LANTRONIX®

x6010 Managed T1/E1-to-Fiber Network Interface Device (NID)

User Guide

Part Number 33493

Revision F June 2023

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.
All other trademarks and trade names are the property of their respective holders.

Patented: https://www.lantronix.com/legal/patents/; additional patents pending.

Warranty

For details on the Lantronix warranty policy, please go to our web site at http://www.lantronix.com/support/warranty.

Contacts

Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev	Description
12/23/16	C	Revised for firmware version 1.2.6 and updated default and LBO settings.
3/3/17	D	Add DoC and update contact information.
11/5/19	E	Updated specifications and added optional accessories. Add Local Management of Cards in a Remote Un-managed Chassis at FW v 1.2.6. Update for FW v 2.0.1.
6/13/23	F	Added fiber specs. Initial Lantronix rebrand. Changed EN 60950-1 to EN62368-1. Added UKCA certification. Removed Glossary and Index.

Cautions and Warnings

Definitions

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. Warnings indicate that there is the possibility of injury to person.
Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons.

Cautions

Do not ship or store devices near strong electrostatic, electromagnetic, magnetic, or radioactive fields.

Caution: When handling chassis Network Interface Devices (NIDs) observe electrostatic discharge precautions. This requires proper grounding (i.e., wear a wrist strap).

Caution: Copper based media ports, e.g., Twisted Pair (TP) Ethernet, USB, RS232, RS422, RS485, DS1, DS3, Video Coax, etc., are intended to be connected to intra-building *(inside plant)* link segments that are not subject to lightening transients or power faults. They are **not** to be connected to inter-building *(outside plant)* link segments that are subject to lightening.

Caution: **Do not** install the NIDs in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor NID performance.

Caution: Read the installation instructions before connecting the chassis to a power source. Failure to observe this caution could result in poor performance or damage to the equipment.

Caution: Only trained and qualified personnel should install or perform maintenance on the x6010. Failure to observe this caution could result in poor performance or damage to the equipment.

Caution: Do not let optical fibers come into physical contact with any bare part of the body since they are fragile, and difficult to detect and remove from the body.

Caution: Do not bend any part of an optical fiber/cable to a diameter that is smaller than the minimum permitted according to the manufacturer's specification (usually about 65 mm or 2.5 in)!

Warnings

Warning: Use of controls, adjustments or the performance of procedures other than those specified herein may result in hazardous radiation exposure.

Warning: Visible and invisible laser radiation when open. **Do not** look into the beam or view the beam directly with optical instruments. Failure to observe this warning could result in an eye injury or blindness.

Warning: DO NOT connect the power supply module to external power before installing it into the chassis. Failure to observe this warning could result in an electrical shock or death.

Warning: Select mounting bracket locations on the chassis that will keep the chassis balanced when mounted in the rack. Failure to observe this warning could allow the chassis to fall, resulting in equipment damage and/or possible injury to persons.

Warning: Do not work on the chassis, connect, or disconnect cables during a storm with lightning. Failure to observe this warning could result in an electrical shock or death.

See Appendix A for Electrical Safety Warnings translated into multiple languages.

Contents

1 Introduction 8
Document Overview 8
Product Overview 8
Features 8
Typical Application 9
Applicable Standards and RFCs 10
Feature Descriptions 10
AIS (Alarm Indication Signal) 10
Loopback Test 11
LOS (Loss of Signal) Detection 12
In-band Fiber Loopback Code Detection 12
HTTP 13
Remote Management 15
Firmware Upgrade 17
Management Access Methods 18
TFTP (Trivial File Transfer Protocol) 18
Optional Accessories (sold separately) 18
Models (Chassis and Standalone) 19
Fiber Cable Specifications 20
Physical Specifications 21
Connectors 22
LED Descriptions 23
Jumper Settings 24
DIP Switches 24
Documentation Conventions 27
Related Manuals and Online Help 28
For More Information 28

2 Installation and System Setup 29
General 29
Installing the Chassis Model (C6010) 29
Installing the Standalone Model (S6010) 30
Rack Mount Installation 30
Tabletop Installation 31
Wall Mount Installation 32
Connecting to AC Power 33
Installing SFPs 34
Connecting the C6010 to the S6010 34
Accessing the NIDs 38
Access via Local Serial Interface (USB) 38
Access via an Ethernet Network 39
Initialization (Default) Configuration 43

3 Management Methods 44
General 44
IONMM Managed x6010 44
Managing Slide-In and Remote Modules Using CLI Commands 44
Managing Slide-In and Remote Modules via the Web Interface 48
Managing Standalone Modules Using CLI Commands 49
Managing Standalone Modules via the IONMM Web Interface 50
Menu Descriptions 52
Reboot, Reset, and Power Off Function Notes 54

4 Configuration 57
General 57

System Configuration 58
System Configuration – CLI Method 58
T1 System Configuration – Web Method 59
T1 Ports Configuration 60
T1 Ports Configuration – CLI Method 60
T1 Ports Configuration – Web Method 61
Port Loopback Tests 64
Port Loopback Test – CLI Method 64
Port Loopback Test – Web Method 66
TDM Mode Configuration 68
Configuring TDM Mode – CLI Method 68
Configuring TDM Mode – Web Method 69

5 Operation 72
General 72
Backup and Restore Operations (Provisioning) 72
Note on Remote (L2D) Module Backup, Restore, and Upgrade 73
Backing Up Slide-In and Remote Module Configuration 73
Backing Up Standalone Modules 76
Editing the Config File (Optional) 78
Restoring Slide-In and Remote Modules' Configuration 79
Restoring Standalone Modules 82
Back Up and Restore File Content and Location 85
IONMM Backup All / Restore All 85
Displaying Information 86
Reset to Factory Defaults 86
Resetting Defaults – CLI Method 86
Resetting Defaults – Web Method 87
File Status after Reset to Factory Defaults 87
Resetting Uptime 88
Reset Uptime – CLI Method 88
Reset Uptime – Web Method 89
Reboot 90
Rebooting – CLI Method 90
Rebooting – Web Method 91
Reboot File Content and Location 92
Upgrade the IONMM and/or NID Firmware 93
Upgrading IONMM and/or NID Firmware – CLI Method 93
Upgrading IONMM and/or NID Firmware – Web Method 95
Upgrading Slide-In and Remote Modules Firmware via TFTP 101
Firmware Upgrade File Content and Location 105
Additional Upgrade Procedures 105
Replacing a Chassis Resident NID 106

6 Command Line Interface (CLI) Reference 107
General 107
Command Line Editing 107
Display Similar Commands 107
Partial Keyword Lookup 107
Recall Commands 107
Keystroke Commands 108
Command Descriptions 109

7 Troubleshooting 125
General 125
Basic ION System Troubleshooting 125
Error Indications and Recovery Procedures 126

LED Fault and Activity Displays 127
Problem Conditions 128
CLI Messages 139
Web Interface Messages 171
The Config Error Log (config.err) File 186
Config.err Messages 187
config.err Message Responses 187
Webpage Messages 190
Windows Event Viewer Messages 200
ION System Tests 201
DMI (Diagnostic Maintenance Interface) Test 201
Set Debug Level 209
DIP Switches and Jumper Settings 210
PCB Identification 210
C6010 PCB 210
S6010 NID Switch Locations 211
X6010-10xx PCB (C6010 with SFP and BNC) 215
In-band Loopback Code Detect Procedure 216
Third Party Troubleshooting Tools 217
Third Party Tool Messages 229
HyperTerminal Messages 229
Ping Command Messages 232
Telnet Messages 232
TFTP Server Messages 234
PuTTY Messages 235
Alarm Indication Signal – Alarm Condition 236
LOS Detection 238
T1 Error Events and Alarm Conditions 238
T1 Error Events 238
D4 and ESF Alarm Conditions 238
Recovery Procedures 239
Recording Model Information and System Information 240

Appendix A Compliance and Safety Information 243
Compliance Information 243
Electrical Safety 246
Elektrische Sicherheit 246
Elektrisk sikkerhed 246
Elektrische veiligheid 246
Sécurité électrique 246
Sähköturvallisuus 246
Sicurezza elettrica 246
Elektrisk sikkerhet 246
Segurança eléctrica 246
Seguridad eléctrica 246
Elsäkerhet 246

Appendix B: Factory Defaults 247
Device-Level Factory Defaults 247
Port-Level Factory Defaults 247
Supported Line Build Out Matrix 248

Appendix C Configuration Quick Reference – CLI 249
For SNMP MIB Trap Information 250

Appendix D Cable Specifications 251
Fiber Cable 251
T1/E1 Cable 251

Twisted-Pair Copper Cable 251
T1 TP/UTP 251
E1 TP/UTP 251

Appendix E Local Management of Cards in a Remote Un-managed Chassis 252

List of Figures

Figure 1: Typical x6010 User Application Scenario 9
Figure 2: Typical AIS Application 10
Figure 3: Loopback on copper and fiber port of Media Converter A 11
Figure 4: Typical Loopback function on a Fiber port 12
Figure 5: Typical Loopback function on a Copper port 12
Figure 7: x6010 Remote Management Topology 16
Figure 8: x6010 Models 19
Figure 9 : C6010 Front Panels 22
Figure 10: S6010 Front Panels 23
Figure 11: S6010 DIP Switches 24
Figure 12: C6010 DIP Switches and Jumpers 25
Figure 13: Chassis Installation 29
Figure 14: Tabletop Installation 31
Figure 15: Wall Mount Installation 32
Figure 16: AC Power Connection 33
Figure 17: SFP Installation 34
Figure 18: CLI Location Hierarchy 45
Figure 19: x6010 PCB Layout 210
Figure 20: x6010 Switch Locations 211
Figure 21: x6010-10xx Layout 215
Figure 22: Initiate a Loopback from a Test Set 216

List of Tables

Table 1: HTTP Parameters 13
Table 2: x6010 Models 20
Table 3: Physical Specifications 21
Table 4: x6010 Connector Descriptions 22
Table 5: Documentation Conventions 27
Table 6: System-Level Menu Description 52
Table 7 : Port-Level Menu Description 53
Table 8: Back Up and Restore File Content and Location 85
Table 9: File Status after a Reset to Factory Defaults 87
Table 10: File Content and Location after a System Reboot 92
Table 11: File Content and Location after a Firmware Upgrade 105
Table 12: Keystroke Editing Commands 108
Table 13: DMI Parameters 203
Table 14: Device-Level Factory Defaults 247
Table 15: Port-Level Factory Defaults 247
Table 16: Line Build Out (LBO) Details 248

1 Introduction

Document Overview

This manual provides the user with an understanding of the Lantronix x6010 Network Interface Device (NID).

Product Overview

The ION T1/E1 model x6010 is a copper-to-fiber NID with remote management that provides a solution to extend T1 or E1 circuits over fiber, and remotely manage them in-band from admin locations.

The x6010 NIDs are designed as either a standalone module (S6010) or a slide-in module (C6010) that is installed in an ION system chassis. In either configuration, these devices are designed to convert the copper ports on T1/E1 devices, such as a PBX or T1/E1 router, to multimode or single mode fiber with advanced services and functions.

The x6010 supports Small Form Pluggable (SFP) transceivers to support a variety of fiber types, distances and wavelengths to provide maximum flexibility across a variety of network topologies. The use of Coarse Wave Division Multiplexing (CWDM) SFPs can be utilized to further increase the bandwidth capacity of the fiber infrastructure. The T1/E1NID must be used in pairs. A typical installation includes a chassis card (C6010) installed in a local ION chassis and a stand-alone device (S6010) installed at a remote location.

Features

The x6010 provides the following services and functions.

- Converts copper ports on T1/E1 devices, such as a PBX or T1/E1 router, to multimode or single mode fiber
- Alarm Indication Signal (AIS) LED
- Can be used with fractional T1/E1 circuits
- Firmware upgrade
- Remote management
- Local or Remote Loopbacks on copper or fiber port
- Switch-selectable RJ-48 connectors for T1 or E1
- Jitter attenuators optimize Bit Error Rate performance
- Network debug procedures make BER testing more convenient
- Built-in troubleshooting with selectable TAOS (Transmit All Ones): a switch on the fiber and copper interfaces allows testing of all T1/E1 equipment on that network segment to ensure the network links

You can manage the following x6010 services and functions via the x6010 application software:

- Report Model information, such as serial number, model number, firmware revision, etc.
- Report link status on copper and fiber ports
- Report LBO, Long Haul, Short Haul status
- Report AIS detected status on copper and fiber port
- Loopback Enable/Disable on copper or fiber port
- TAOS Enable/Disable on copper and fiber port
- Report circuit ID on device and ports
- DMI on Fiber port

Typical Application

The x6010 applications can include:

- Interconnect campus / MAN. A T1 link is a common means of campus / Metropolitan Area Network (MAN) interconnects.
- Extend a T1 to other buildings in a campus or MAN.
- Link two PBXs or extend T1 from a demarc (demarcation point).

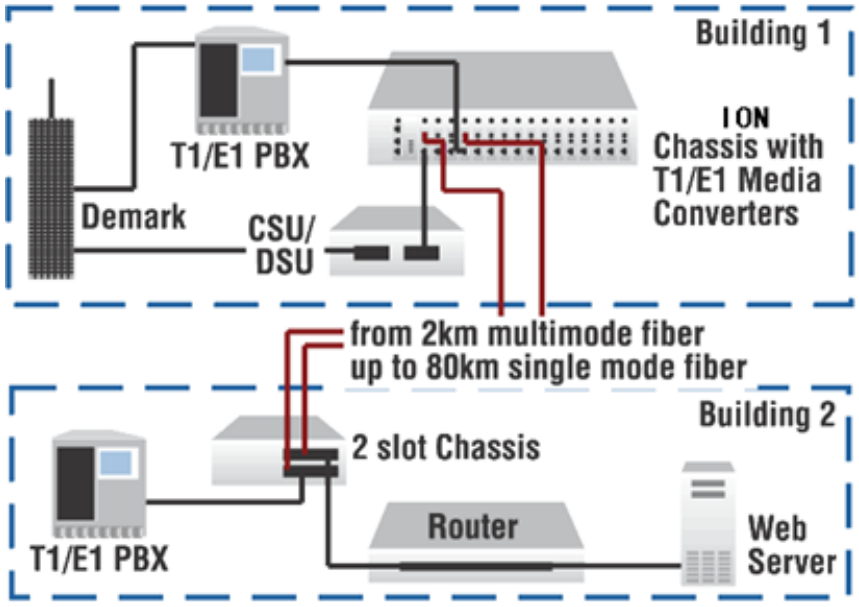


Figure 1: Typical x6010 User Application Scenario

Applicable Standards and RFCs

The x6010 complies with the following hardware standards:

- ANSI T1.102, T1.403, and T1.408
- ITU I.431, G.703, G.736, G.775, and G.823
- ETSI 300-166, 300-233, and TBR12/13
- AT&T Pub 62411
- Regulatory Compliance for Emission: EN 55035/EN55032 Class A, FCC Class A; CE, UKCA, UL (S6010)
- Regulatory Compliance for Immunity: EN55024
- Safety Compliance: Unit: UL listed, CE Mark
- In T1 mode, declaring/clearing AIS detection complies with ANSI T1.231. In E1 mode, declaring/clearing AIS detection complies with ITU G.775 or ETSI 300233, as selected.

The x6010 complies with the following IETF RFCs:

- HTTP protocol: IETF RFC 2616
- SNMP protocol: IETF RFC 1157, RFC 1158, and RFC 2578
- TFTP protocol: IETF RFC 1350

Feature Descriptions

The x6010 features are described in the following sub-sections.

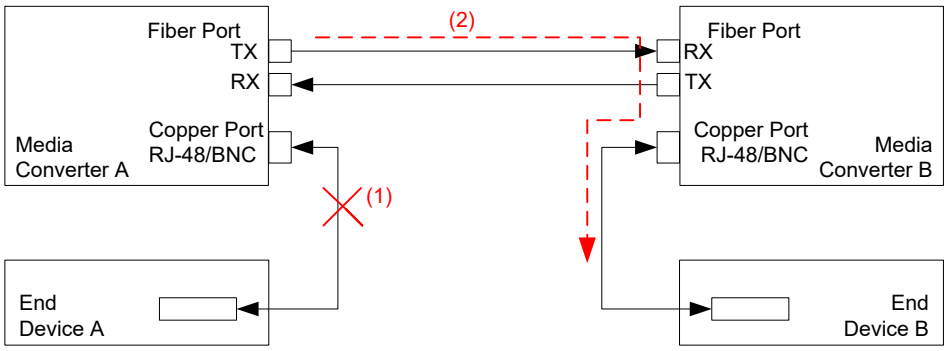
AIS (Alarm Indication Signal)

The x6010 provides AIS (Alarm Indication Signal) support.

When the x6010 detects a signal lost or framing lost on one port's receiving direction, it will send out an Alarm Indication Signal (AIS) through another port to alert the receiving end that a segment of the end-to-end link has failed at a logical or physical level.

The x6010 will generate the AIS by transmitting all ones (TAOS).

You can enable or disable AIS transmit on each x6010 port via the Web interface, FocalPoint (FP), and the Command Line Interface (CLI).



(1) Copper Port in End Device A detects a signal lost
(2) End Device A transmits AIS signal through Fiber Port to End Device B

Figure 2: Typical AIS Application

The AIS transmit function can be enabled or disabled on each port (Copper Port and Fiber Port) by setting TAOS to Enable or Disable. If the AIS transmit function is enabled on one port and signal lost is detected, the x6010 will transmit all ones to the receiving end device; if the AIS function is disabled, no action will be performed.

If the x6010 receives an AIS signal (All Ones frame) from one port, the LED (SDC/SDF- Signal Detect on Copper/Fiber) displays as yellow to indicate AIS is detected on that port (see "LED Descriptions". The x6010 software transmits an AIS detect trap at the same time (see the "SNMP MIBs" section for trap descriptions).

If Media Converter A in Figure 2 above detects a signal lost on a copper port and the AIS function is enabled (TAOS is enabled) on that port, Media Converter A will Transmit All Ones to Media Converter B through the fiber link. Media Converter B's SDF LED will display as yellow to indicate an AIS signal is detected on the fiber port. The AIS signal will then be transmitted to End Device B.

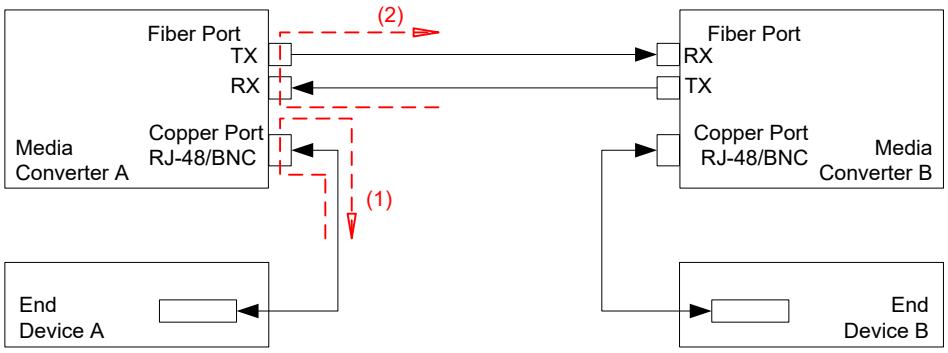
In T1 mode, the criteria for declaring/clearing AIS detection are in compliance with the ANSI T1.231. In E1 mode, the criteria for declaring/clearing AIS detection comply with the ITU G.775 or the ETSI 300233, as selected.

Loopback Test

The x6010 provides Loopback (LB) test support with three different loopback configurations: copper loopback, fiber loopback, and inband loopback.

The Loopback feature puts the x6010 in a mode that lets it loop back the signal from the RX port to the TX port on either media for testing and troubleshooting purposes. You can enable or disable the Loopback function on an x6010 copper port or fiber port via the Web interface, FocalPoint (FP), and the Command Line Interface (CLI).

Test signals from a test device (e.g., Fireberd, etc.) can then be inserted into the link and looped back and received by a device to test a particular segment of the link (i.e., copper or fiber).



(1) Loopback on copper port;
(2) Loopback on fiber port.

Figure 3: Loopback on copper and fiber port of Media Converter A

If the Loopback function is enabled on the copper port of Media Converter A, End Device A is the tester; the test signal is inserted into the copper RX of Media Converter A and then looped back and received by the copper TX of Media Converter A.

If the Loopback function is enabled on the Fiber port of Media Converter A, End Device B is the tester; the test signal will be inserted into the Fiber RX of Media Converter A through Media Converter B and be looped back at Fiber port of Media Converter A and received by End Device B via Media Converter B.

The x6010 Loopback function cannot be enabled on both copper and fiber ports at the same time; an error message displays if attempted.

A typical x6010 Fiber port Loopback applications is shown below.

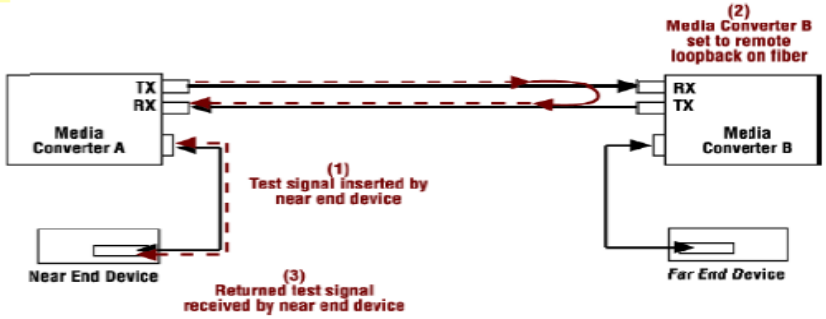


Figure 4: Typical Loopback function on a Fiber port

A typical x6010 Copper port Loopback applications is shown below.

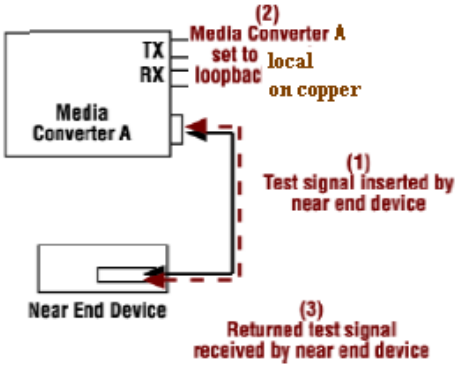


Figure 5: Typical Loopback function on a Copper port

LOS (Loss of Signal) Detection

The x6010 Loss of Signal (LOS) detector monitors the amplitude of the incoming signal level and pulse density of the received TIP/RING signals. A LOS condition is detected when the incoming signal has “no transitions”. The LOS condition is cleared when the incoming signal has “transitions”. In addition, the x6010 application software may get the LOS status via interface with the FPGA. LOS detection is provided on the x6010 coax, fiber and copper interfaces as link down and link up traps and **show** commands.

In-band Fiber Loopback Code Detection

This function enables detection and loopback of the fiber interface based on NIU Facility 2 (FAC2) loopback codes. Certain test devices (e.g., T-BERD 2310) can send in-band loopback codes to the local copper (TP) interface, which are then transmitted to the remote device via the fiber. The remote device can

detect and react to this and activate and de-activate the loopback codes. For detection, these codes must be sent for at least 5 seconds.

The Inband Fiber Loopback Code Detector can track loopback activate/deactivate codes in a framed or unframed T1 data stream. The received data stream is compared with the target activate/deactivate code whose length and the content are pre-defined. When the received data stream matches the target activate/deactivate code and repeats for 4 seconds, this register field indicates the detection of the in-band loopback code.

HTTP

You can manage the x6010 via the IONMM's HTTP service to check all of the configuration parameters and modify some of them via the Web interface.

The table below shows the Global, Fiber port, and Copper port parameters, their Properties, and the valid range of entries supported. The Properties column shows "Read only" (parameters that can only be displayed) or "Read & Write" (parameters that are user-configurable), or "Button".

Table 1: HTTP Parameters

Parameter	Property	Range
Global Parameters		
Serial number	Read only	
Model number	Read only	
Software Revision	Read only	
Hardware Revision	Read only	
Bootloader Revision	Read only	
System Name	Read & Write	Alpha, numeric, and special characters allowed; spaces between characters not allowed.
System Uptime	Read only	
Configuration Mode	Read only	Hardware | Software
Number of Ports	Read only	
System Reboot	Button	
Reset to Factory Defaults	Button	
TDM Mode	Read only	T1 | E1
Device Description	Read & Write	Device description displays string of up to 64 alpha, numeric or special characters.
Fiber Port Parameters		
- Link	Read only	Down | Up
- Transmit All ones	Read & Write	Enable | Disable
- AIS Transmit	Read & Write	Enable | Disable
- Alarm Indication Signal	Read only	Normal | Alarm
- Loopback	Read & Write	No Loopback | PHY Layer
- Connector	Read only	Description string of connector
- Circuit ID	Read & Write	Circuit ID display string
- DMI		

DMI ID	Read only	
Connector Type	Read only	
Nominal Bit Rate	Read only	
Wavelength	Read only	
Receive Power	Read only	
Receive Power Alarm	Read only	Normal | Low Warning | High Warning | Low Alarm | High Alarm
Rx Power Intrusion Threshold	Read & Write	0-65,535
Temperature	Read only	
Temperature Alarm	Read only	Normal | Low warning | high warning | low Alarm | high Alarm
Transmit Bias	Read only	
Transmit Bias Alarm	Read only	Normal | Low warning | high warning | low Alarm | high Alarm
Transmit Power	Read only	
Transmit Power Alarm	Read only	Normal | Low warning | high warning | low Alarm | high Alarm
Length (Single Mode)	Read only	
Length (50um, Multi Mode)	Read only	
Length (62.5 um, Multi Mode)	Read only	
Length (copper)	Read only	
Copper Port		
- Link	Read only	Down | Up
- Transmit All ones	Read & Write	Enable | Disable
- AIS Transmit	Read & Write	Enable | Disable
- Alarm Indication Signal	Read only	Normal | Alarm
- Loopback	Read & Write	No Loopback | PHY Layer
- Long Haul	Read only	Yes | No
- Line build out	Read only	Description string of LBO
- Connector	Read only	Description string of connector
- Circuit ID	Read & Write	Circuit ID display string

Remote Management

Remote Management over fiber allows access to the remote device to obtain status, actively configure remote device features, and perform remote device firmware upgrades.

A typical remote management scenario is shown below.

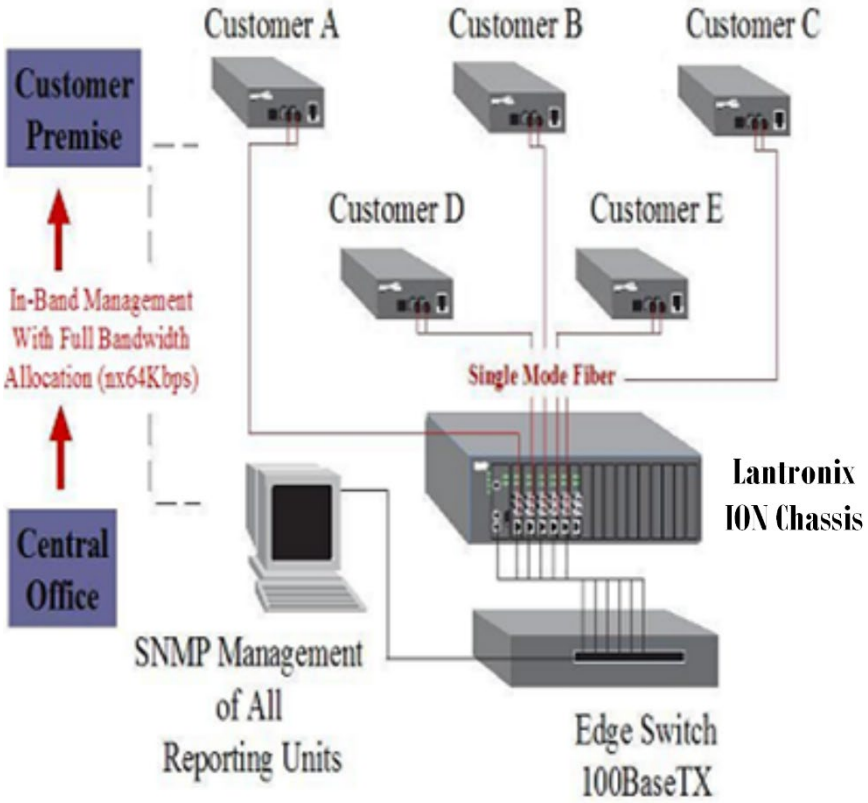


Figure 6: Typical Remote Management Application

In the figure above, devices from Customer A to Customer E can all be remotely managed via the ION Chassis.

A remote S6010 device is connected with local C6010 device through the fiber link, with a specific channel on the fiber link reserved and used for the management traffic. This management channel is independent of the TDM payload channels; the management channel and TDM payload channels will not impact each other.

The x6010 Remote Management (RM) protocol lets applications exchange management traffic between local C6010 and remote S6010 devices. The RM protocol provides the interaction protocol for Packet Handling, BC Packet TX/RX and Remote Packet TX/RX. The RM protocol provides transparent packet forwarding on the C6x10 and packet TX/RX redirection on the S6x10, eliminating the differences between the C6x10 and S6x10 for the IONMM and its upper layer applications.

Note that the current ION platform supports up to one level of x6010 device remote management.

Version 1.2.6 of the x6010 Series supports the management of a C6010 when installed in an unmanaged ION chassis. Management is supported by another C6010 installed in a managed chassis when the two are linked together via a fiber cable. Version 1.2.6 also supports remote firmware upgrades of a C6010 in an unmanaged chassis. See the Release Notes for known Feature limitations.

All management traffic between the IONMM and the remote S6010 are relayed and forwarded through the local C6010. Traffic between the IONMM and C6010 is exchanged on the ION chassis' backplane Ethernet bus (BPC), while traffic between the local C6010 and remote S6010 is exchanged on the specific management channel (see figure below) .

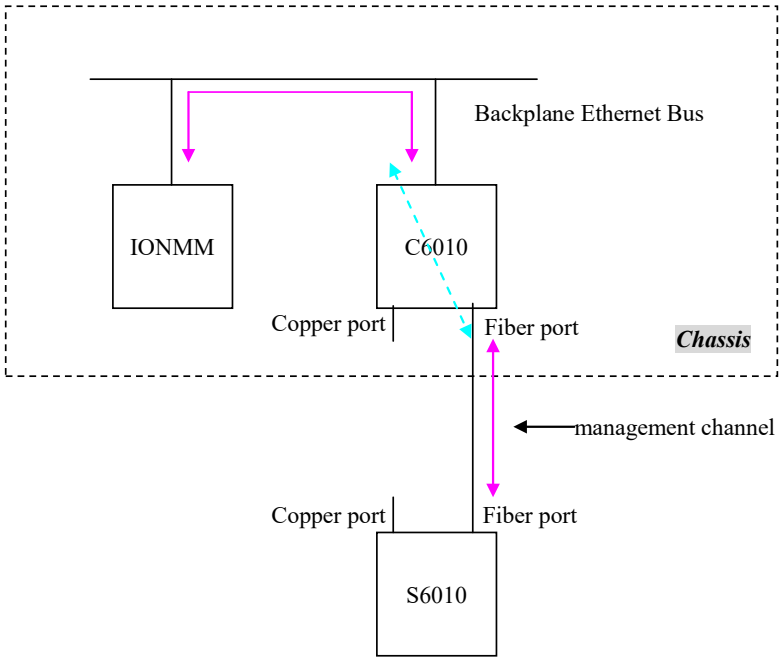


Figure 7: x6010 Remote Management Topology

Remote devices are detected by the IONMM through the internal LLDP protocol. Each time a remote device is powered up, it periodically sends out an LLDP packet to notify the IONMM that it is up.
When the IONMM receives such LLDP packets, it updates the entire ION topology based on the information carried in the LLDP packet.

Firmware Upgrade

The x6010 can be upgraded via an IONMM installed in an ION chassis. You can select the target NID via the Web interface / Focal Point / CLI and start the firmware upgrade operation. After the x6010 finishes upgrading, it will reboot itself to load the new firmware. The upgrades do not require reconfiguration of the SNMP management or converter feature settings.

The x6010 has two parts that need to be upgraded; one is the device firmware (AVR) and the other is the FPGA (Field Programmable Gate Array) firmware. For simplicity, these two parts are combined into one firmware file and upgraded in one step, transparently.

You can upgrade the x6010 to a specific revision via the IONMM, which means the x6010 can be upgraded to a newer revision firmware or can be downgraded to an older revision firmware. (Attempting to upgrade to the existing revision firmware version is not actually performed, and a message displays indicating this.)

Certain conditions will cause the firmware upgrade to fail:

- The communication path between x6010 and IONMM is corrupted, causing an upgrade protocol timeout,
- No valid firmware file stored in the IONMM (e.g., no specified x6010 firmware revision, or a corrupted firmware file).
- The firmware revision is the same.
- Programming the internal Flash fails.

If the x6010 bootloader cannot detect valid firmware installed after device is powered up or rebooted, it enters upgrade mode automatically to request valid firmware from the IONMM. When the x6010 finishes upgrading successfully, it reboots itself and the bootloader checks the firmware again. If it passes, the x6010 loads the new firmware and enters normal operating mode. Otherwise, the x6010 returns to Upgrade mode. **Note**: Only the x6010 in the process of being upgraded will have its FPGA forced into factory mode. The FPGA mode of the connected x6010 remains in application mode. A C6010 can only upgrade a remote S6010 with the same version number.

The three methods of firmware upgrades are:

- Web interface
- Focal Point
- CLI command

A remotely managed x6010 can be upgraded remotely as mentioned above. Note that the current ION platform supports up to one level of x6010 device remote management.

Management Access Methods

Management of the x6010 is accomplished through one of the following methods.

- Universal Serial Bus (USB) – uses a command line interface (CLI) to access and control the x6010 through a locally connected workstation.
- Telnet session – uses the CLI to access and control the x6010 through the network.
- Simple Network Management Protocol (SNMP) – both public and private Management Information Bases (MIBs) allowing for a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).

TFTP (Trivial File Transfer Protocol)

The TFTP client provides uploading and downloading of files out of the device's file system. Typical applications for this protocol on this device include backup of configuration, restore known configuration from a file, firmware image upgrade/downgrade, log files backup, certificate download for SSL applications etc.

Optional Accessories (sold separately)

SFP Modules: SFP port uses standard 100Base-x/oc-3 SFP. See the Lantronix SFP webpage.

Power Supply: SPS-2460-SA Wide Input (24 – 60VDC) Stand-Alone Power Supply included.

Mounting Options:

WMBL Wall Mount Bracket 4" [102 mm]
WMBD DIN Rail Bracket 5" [127 mm]
E-MCR-05 12-Slot Media Converter Rack
RMS19-SA4-02 4-Slot Media Converter Shelf

Country-specific Power Supply: To order the corresponding country specific power supply, add the extension from the list below to the end of the SKU; -NA = Country Code, NA = North America, LA = Latin America, EU = Europe, UK = United Kingdom, SA = South Africa, JP = Japan, OZ = Australia, BR = Brazil.

Models (Chassis and Standalone)

The x6010 models include Chassis (slide in card or SIC) and Standalone models. The Chassis models have a prefix of ***C*** (e.g., C6010) and the Standalone models have a prefix of ***S*** (e.g., S6010).

Standalone Models (S6010-xxxx)

S6010-1011	S6010-1013	S6010-1014	S6010-1040

Chassis Models (C6010-xxxx)

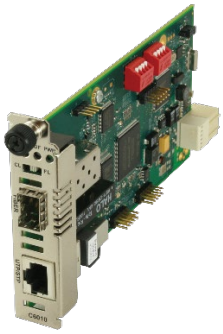
		
C6010-1013	C6010-1014	C6010-1040

Figure 8: x6010 Models

The various x6010 NID models are described in the tables below.

Table 2: x6010 Models

Chassis Model	Copper Conn	Fiber Conn	Mode	Dis-tance (Km)	Transceiver TN#	Notes
C6010-1013	RJ-48	SC	MM	2	13222	TN#13535 with DMI
C6010-1014	RJ-48	SC	SM	20	13223	TN#13402 with DMI
C6010-1040	RJ-48	SFP	SM/MM	2/20	13344/13345	See Note *1

Standalone Model	Copper Conn	Fiber Conn	Mode	Dis-tance (Km)	Transceiver TN#	Notes
S6010-1011	RJ-48	ST	MM	2	13221	TN#13536 with DMI
S6010-1013	RJ-48	SC	MM	2	13222	TN#13535 with DMI
S6010-1014	RJ-48	SC	SM	20	13223	TN#13402 with DMI
S6010-1040	RJ-48	SFP	SM/MM	2/20	13344/13345	See Note *1

Note *1: the module could be used on this card but is not included on standard models of this card.

Fiber Cable Specifications

The fiber cable physical characteristics must meet or exceed IEEE 802.3™ specifications.

The fiber optic transmitters on this device meet Class I Laser safety requirements per IEC-825/CDRH standards and comply with 21 CFR1040.10 and 21CFR1040.11.

Bit Error Rate: <10-9
Single mode fiber (recommended): 9 µm
Multimode fiber (recommended): 62.5/125 µm
Multimode fiber (optional): 50/125 µm

SKU	SM/MM	Fiber	Distance	Wave Length (nm)	Data Rate	Min TX Pwr	Max TX Pwr	RX Sensi-tivity	RX Man In Pwr	Link Budget
C6010-1013	Multi	Dual	2 Km	1310	100M	-19.0 dBm	-14.0 dBm	-30.0 dBm	-14.0 dBm	11.0 dB
C6010-1014	Single	Dual	30 Km	1310	100M	-15.0 dBm	-8.0 dBm	-31.0 dBm	-8.0 dBm	16.0 dB
S6010-1011	Multi	Dual	2 Km	1310	100M	-19.0 dBm	-14.0 dBm	-30.0 dBm	-14.0 dBm	11.0 dB
S6010-1013	Multi	Dual	2 Km	1310	100M	-19.0 dBm	-14.0 dBm	-30.0 dBm	-14.0 dBm	11.0 dB
S6010-1014	Single	Dual	30 Km	1310	100M	-15.0 dBm	-8.0 dBm	-31.0 dBm	-8.0 dBm	16.0 dB

Physical Specifications

The physical specifications for the Chassis and Standalone models are provided in the table below.

Table 3: Physical Specifications

Standards	ANSI T1.102, T1.402, T1.408; ITU I.431, G.703, G.736, G.775; G.823; ETSI 300-166, ETSI 300-233, TBR12/12
Data Rates	T1 = 1.544 Mbps, E1 = 2.048 Mbps
Copper Connectors	RJ-48
Fiber Connectors	SFP: LC connector uses standard 100Base-X/OC-3 SFP Fixed Optics: ST or SC connector
Dimensions	C6010: 1” x 3.3” x 6.1” (2.54 cm x 8.382 cm x 15.5 cm) HxWxD S6010: 0.9” x 3.4” x 6” (2.3 cm x 8.6 cm x 15.2 cm) HxWxD
Power Supply	C6010: From ION chassis backplane (slide-in card) S6010: 7.5 to 15.9 VDC
Power Consumption	2.6 Watts
Environmental	Environment specs depend on the chassis chosen. See ION chassis specs. Operating: 0°C to +50°C (C6010) Operating: -10°C to +65°C (S6010) Humidity: 5% to 95% (non-condensing) Altitude: 0 – 10,000 ft.
Shipping Weight	C6010: 1 lb. (0.45 kg) S6010: 2 lbs. (0.90 kg)
MTBF	With Power Supply: Greater than 41,660 hours (MIL-HDBD-217F) Greater than 114,580 hours (Bellcore) Without Power Supply: Greater than 250,000 hours (MIL-HDBD-217F) Greater than 687,000 hours (Bellcore)
Compliance	EN 55035/EN55032 Class A, FCC Class A; CE, UKCA, UL (S6010)
Warranty	Lifetime

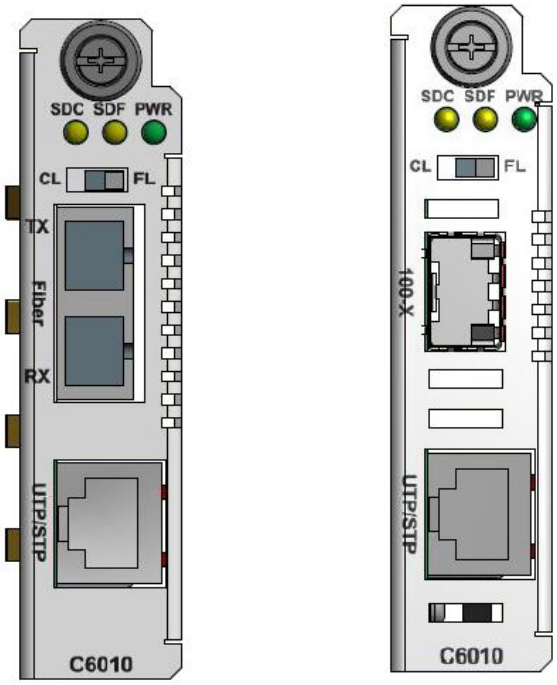
Connectors

The x6010 connectors are described in the table below.

Table 4: x6010 Connector Descriptions

Connector Label	Description
Fiber TX / RX	ST, SC or open SFP for fiber media connection.
UTP / STP	RJ48 copper media connection for shielded twisted pair (STP) or unshielded twisted pair (UTP) media connection.
100-X	PORT 2; open SFP for fiber media connection.

For fiber, coax, and copper cable specifications see "Appendix D: Cable Specifications".



C6010-10xx **C6010-1040**

Figure 9 : C6010 Front Panels

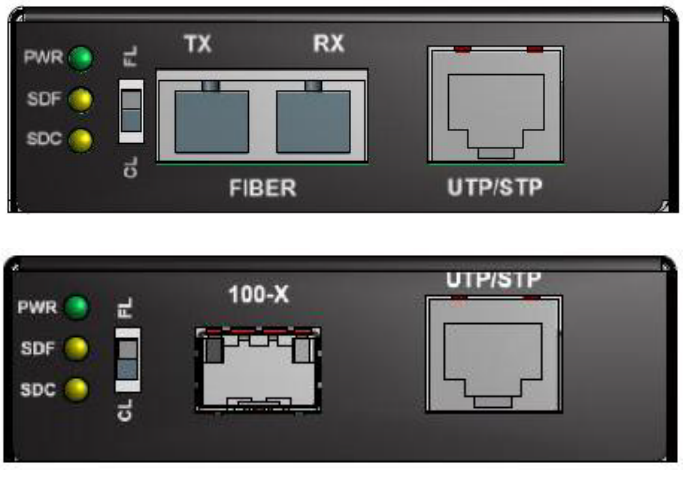


Figure 10: S6010 Front Panels

LED Descriptions

The x6010 LEDs are described below.

PWR Power (Green) on (lit) indicates x6010 power is on.

SDF Signal Detect on Fiber:

- Green, on indicates fiber link is up.
- Green, blinking indicates fiber link is in loopback mode.
- Yellow, on indicates AIS detected on fiber link.

The **SDF** LED when lit indicates fiber link is up. Flashing **SDF** LED (once/second) indicates transmitting on link if other link is down. Flashing **SDF** LED (5 times/second) indicates 'All Ones' detected on the fiber link.

SDC Signal Detect on Copper:

- Green, on (lit) indicates copper link is up.
- Green, blinking indicates copper link is in loopback mode.
- Yellow, on (lit) indicates AIS detected on copper link.

The **SDC** LED, when lit indicates twisted-pair copper link is up. Flashing SDC LED (once/second) indicates transmitting on link if other link is down. Flashing SDC LED (5 times/second) indicates All Ones detected on the Link.

Jumper Settings

The x6010 jumper settings are described below.

Jumper J8 – Configuration mode (HW / SW Mode): Jumper J8 defines the x6010 PCB's Hardware / Software mode setting.

- 1-2: Hardware mode; the x6010 configuration is controlled by hardware. Use the shorting plug to jumper (short) pins 1 and 2 for Hardware Mode.
- 2-3: Software mode; the x6010 configuration is controlled by software (default). Use the shorting plug to jumper (short) pins 2 and 3 for Software Mode.

The factory default setting is Software mode (pins 2 and 3 jumpered) as shown above. Note that in Hardware mode you cannot make x6010 configuration changes from the Web interface, as the screen fields are all grayed out. You can enter CLI commands with the x6010 in Hardware mode.

For more information, see "DIP Switches and Jumper Settings".

DIP Switches

Several multi-position DIP switches allow the network administrator to configure the x6010 for network conditions. Use a small flat blade screwdriver or similar device to set these switches for site installation.

The x6010 DIP switches and jumpers are summarized below. The x6010 DIP switch settings are described below. For more information, see "DIP Switches and Jumper Settings".

DIP Switch Locations

The S6010 DIP switch locations are shown below.

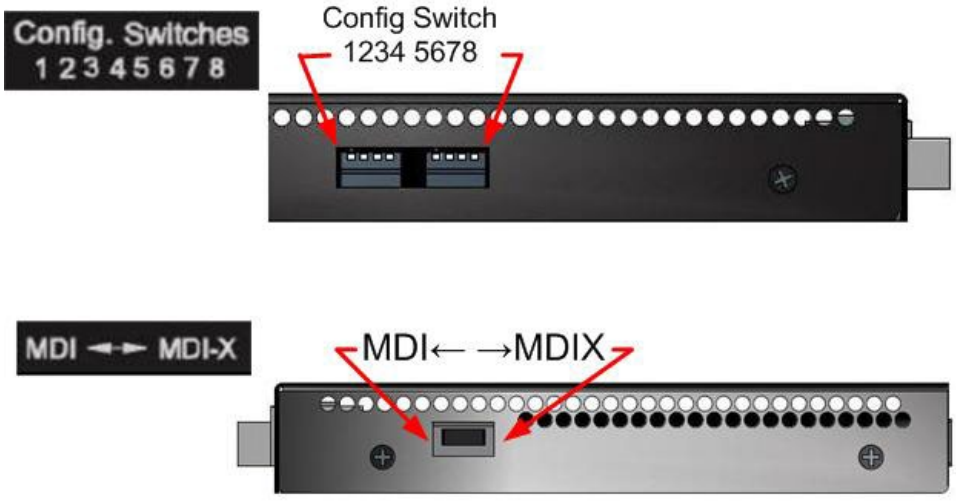


Figure 11: S6010 DIP Switches

The C6010 DIP switch and jumper locations are shown in the figure below.

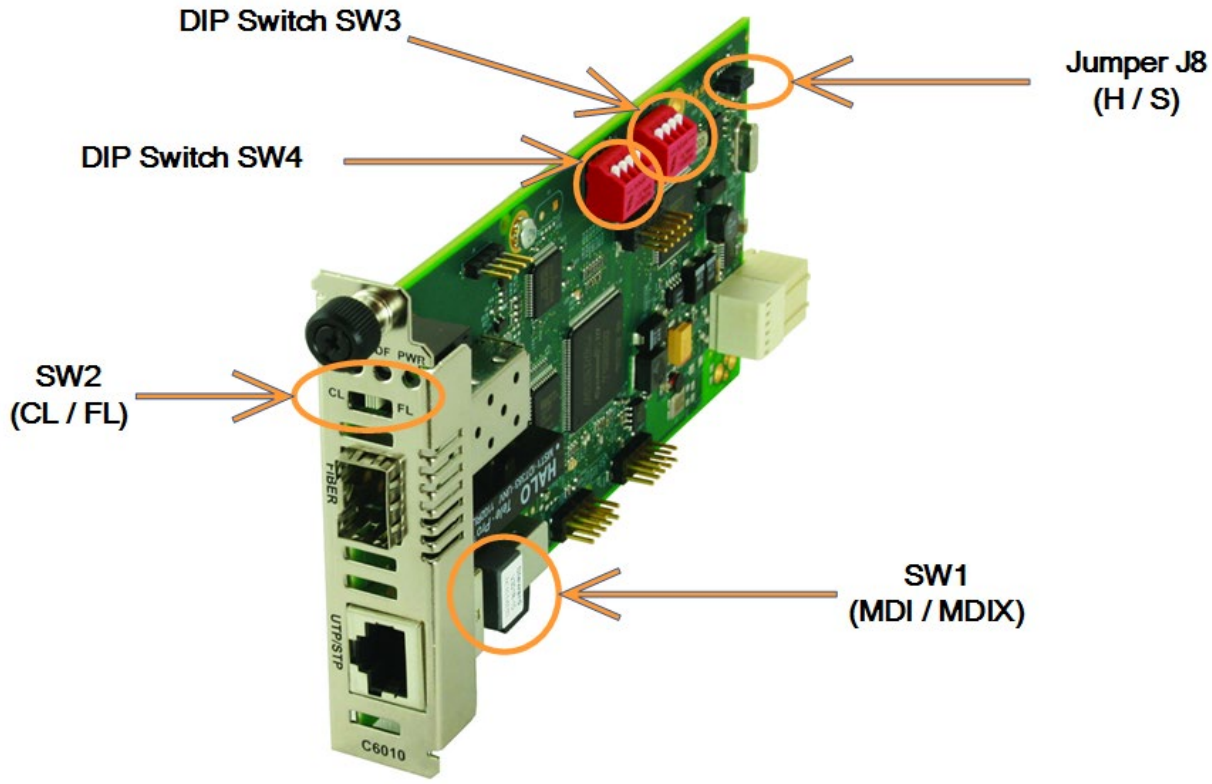


Figure 12: C6010 DIP Switches and Jumpers

DIP Switch Settings

The x6010 DIP switch settings are described below.

MDI ← → MDI-x Switch – DIP Switch **SW1**

Switch1 MDI/MDI-X selection for T1/E1 cable:

- MDI: Straight-Through cable.
- MDI-X: Crossover cable.

CL – FL Switch – DIP Switch **SW2**

Switch2 Copper/Fiber loopback:

- **CL**: Enable loopback on the local copper interface.
- (Center position): Normal operation (no loopback) (default).
- **FL**: Enable loopback on the local fiber interface.

Config Switch 12345678 – DIP Switch **SW3** and **SW4**

Switch 3-1 Line configuration setting in T1 mode (see table below).
Switch 3-2 Line configuration setting in T1 mode (see table below).
Switch 3-3 Line configuration setting in T1 mode (see table below).

Switch 3-4 Inband loopback selection:

- Up: Disabled (default)
- Down: Enabled

Switch 4-1 TAOS on copper port:

- Up: Disabled (default)
- Down: Enabled

Switch 4-2 TAOS on fiber port:

- Up: Disabled (default)
- Down: Enabled

Switch 4-3 Long haul or short haul mode (only valid for T1 mode):

- Up: Short haul (default)
- Down: Long haul

Switch 4-4 T1/E1 mode selection:

- Up: T1 mode (default)
- Down: E1 mode (cable configuration is automatically set to 120 ohms)

SW4-4: up, SW4-3: up. T1/Short Haul (SW3-4 is not used in Short Haul mode):

SW3-1	SW3-2	SW3-3	DSX-1 Condition
Up	Up	Up	J1 Mode, 110 ohm cable (Optional)
Up	Up	Down	DSX-1, 162.5-200m,(533-655') 100 ohm cable
Up	Down	Up	DSX-1, 121.6-162.5m,(399-533') 100 ohm cable
Up	Down	Down	DSX-1, 81-121.6m,(266-399') 100 ohm cable
Down	Up	Up	DSX-1, 40.5-81m,(133-266') 100 ohm cable
Down	Up	Down	DSX-1, 0-40.5m,(0-133') 100 ohm cable
Down	Down	X	Do Not Care

SW4-4: Up, SW4-3: Down. T1/ Long Haul (SW3-3, SW3-4 are not used in Long Haul mode):

SW3-1	SW3-2	DS-1 Condition
Up	Up	-22.5db 100ohm cable
Up	Down	-15.0db 100ohm cable
Down	Up	-7.5db 100ohm cable
Down	Down	0.0db 100ohm cable

See "Section 4: Configuration" for more configuration information.
See "Appendix B: Factory Defaults" for a summary of default and optional settings.

Documentation Conventions

The conventions used within this manual for commands/input entries are described in the table below.

Table 5: Documentation Conventions

Convention	Meaning
Boldface text	Indicates the entry must be made as shown. For example: **ipaddr=<**addr> In the above, only **ipaddr=** must be entered exactly as you see it, including the equal sign (=).
< >	Arrow brackets indicate a value that must be supplied by you. Do not enter the symbols < >. For example: **ipaddr=<**addr> In place of <addr> you must enter a valid IP address.
[ ]	Indicates an optional keyword or parameter. For example: **go** [**s=**<xx>] In the above, **go** must be entered, but **s=** does not have to be.
{ } |	Indicates that a choice must be made between the items shown in the braces. The choices are separated by the | symbol. For example: **state=**{**enable** | **disable**} Enter **state=enable** or state**=disable**.
“ ”	Indicates that the parameter must be entered in quotes. For example: **time=**<**“**value**”**> Enter **time=”20100115 13:15:00”**.
>	Indicates a selection string. For example: Select **File > Save**. This means to first select/click **File** then select/click **Save**.

Related Manuals and Online Help

A printed documentation card is shipped with each x6010 device. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface.

For Lantronix Drivers, Firmware, Manuals, Product Notifications, Warranty Policy & Procedures, etc. go to the Lantronix Technical Resource Center.

Note that this manual provides links to third part web sites for which Lantronix is not responsible.

Other ION system and related device manuals are listed below.

1. ION System x6010 Managed T1/E1-to-Fiber NID User Guide, 33493 (this manual)
2. ION Management Module (IONMM) User Guide, 33457
3. ION System CLI Reference Manual, 33461
4. ION219-A 19-Slot Chassis Installation Guide, 33412
5. ION106-x Six Slot Chassis User Guide, 33658
6. IONPS-A-R1 Power Supply User Guide, 33614
7. IONPS-D-R1 Power Supply User Guide, 33707
8. SPS-2460-xx External Power Supply User's Guide, 33455
9. SFP manuals (product specific)
10. Release Notes (firmware version specific)

Note: Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version. While all screen examples may not display the latest version number, all of the descriptions and procedures reflect the latest software/firmware version, noted in the Revision History on page 2. Transition Networks is now Lantronix. Some products/firmware items are still in process of being re-branded and may still reflect the Transition Networks name/logo.

For More Information

Lantronix has designed their full-featured products to include the most advanced features on the market today. Please use the following resources to learn more about these advanced features.

- ANSI T1.403-1999 – Network and Customer Installation Interface info@ansi.org
- ITU-T Recommendations page.
- IEEE 802 Standards page
- Metro Ethernet Forum – MEF Specifications page.
- IETF – Request for Comments (RFC) page.
- The TIA (Telecommunications Industry Association) Standards page.

2 Installation and System Setup

General

This section describes how to install the x6010 and the procedures to access and initially set up the x6010 through either a local serial interface (USB) or a remote Ethernet connection (Telnet session or Web interface).

Installing the Chassis Model (C6010)

The C6010 is a slide-in module that can only be installed in a Lantronix ION chassis (ION001-x and ION219-x). For a list of ION platform products, go to https://www.lantronix.com/products-class/chassis/.

The following describes how to install the C6010 in the ION chassis.

Caution: Failure to wear a grounding device and observe electrostatic discharge precautions when installing the C6010 could result in damage or failure of the module.

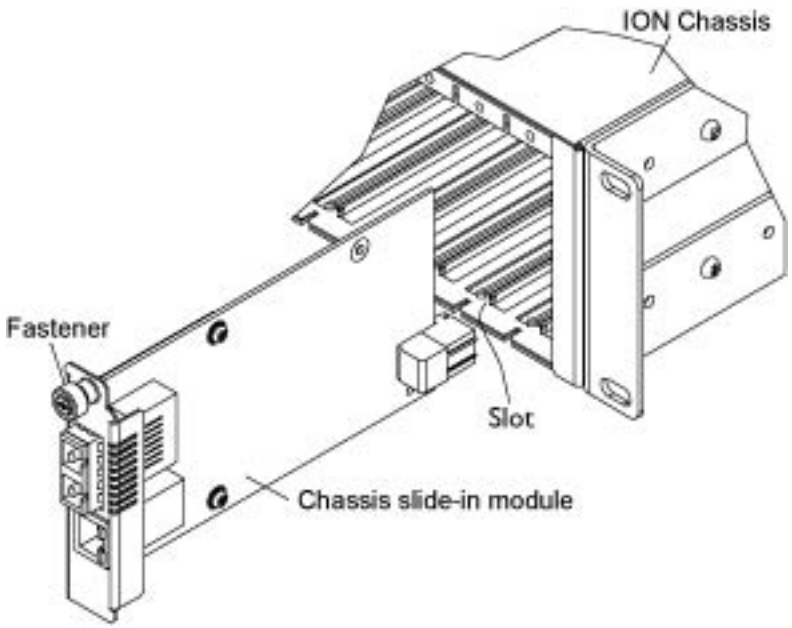


Figure 13: Chassis Installation

IMPORTANT

The C6010 slide-in-card is a “hot swappable” device and can be installed with chassis power on.

1. Locate an empty slot in the ION System chassis.
2. Grasp the edges of the C6010 card by its front panel.
3. Align the card with the upper and lower slot guides, and carefully insert the C6010 into the installation slot.
4. Firmly seat the card against the chassis back panel.
5. Push in and rotate clockwise the panel fastener screw to secure the card to the chassis (see Figure 13: Chassis Installation on the previous page).
6. Note that the C6010 card’s Power LED lights. See Accessing the NIDs.

Installing the Standalone Model (S6010)

The standalone model (S6010) can be installed in any of the following ways.

- Rack mounted
- Table top
- Wall mounted

Rack Mount Installation

The x6010 standalone module can be mounted into a Lantronix E-MCR-05 media converter rack, which can be installed on a tabletop or in a standard site rack. For installation details, see the *E-MCR-05 Media Converter Rack User Guide, 33392*.

Tabletop Installation

The S6010 is shipped with four rubber feet for optional installation on a table or other flat, stable surface in a well-ventilated area.

1. Remove the rubber feet from the card.
2. On the bottom of the S6010, place one rubber foot in each corner of the S6010.

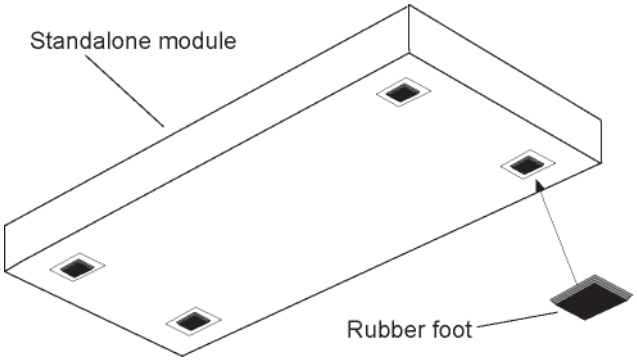


Figure 14: Tabletop Installation

3. Set the S6010 in place and connect the AC power adapter (see Connecting to AC Power).

Wall Mount Installation

1. Remove the four #4 Philips head screws securing the cover to the S6010 and orient the device as shown in the figure below.

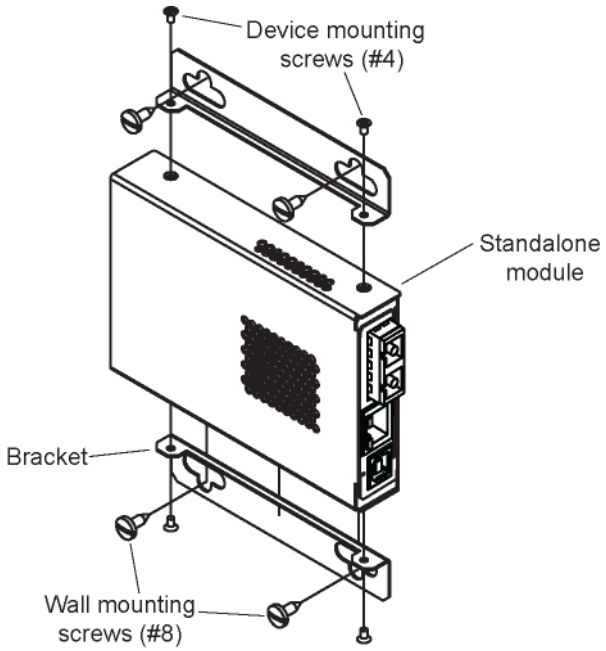


Figure 15: Wall Mount Installation

2. Mount one of the bracket assemblies to the S6010 using two of the #4 Philips head screws.
3. Mount the other bracket assembly to the other side of the S6010 using the other two #4 Philips head screws.
4. Position the S6010 on the mounting surface.
5. Use the four #8 screws to mount the bracket to the mounting surface.
6. Connect the AC power adapter (see Connecting to AC Power).

Connecting to AC Power

After the standalone S6010 has been installed, connect it to the supplied AC-DC power adapter as follows. Use the AC power adapter shipped with the S6010 (# SPS-2460-SA). See the related manual for specifics.

Warning: Risk of electrical shock.

1. Insert the barrel connector of the AC power adapter to the power inlet marked **12V DC INPUT** on the back of the standalone S6010.

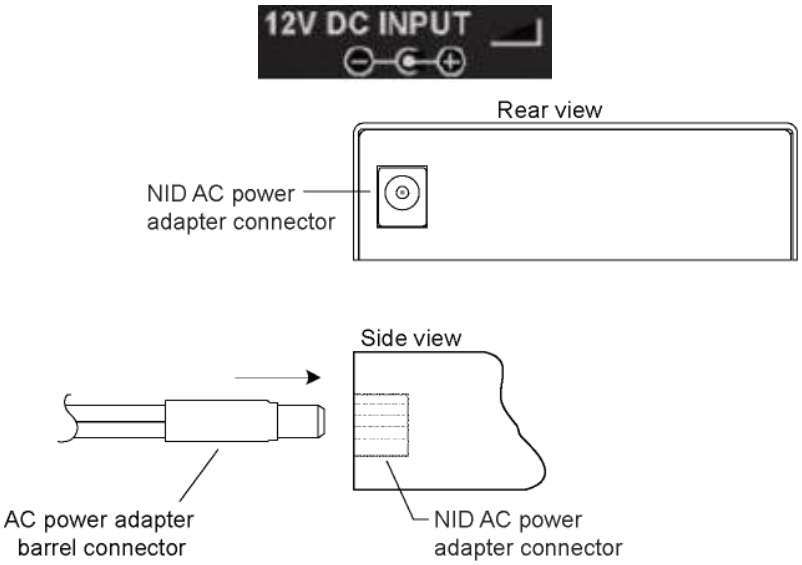


Figure 16: AC Power Connection

2. Plug the AC power adapter plug into AC power at an appropriate AC outlet. Note that the standalone S6010 front Power (PWR) LED lights.

Installing SFPs

Some models allow you to install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection. The x61x0-1040 models have a single SFP port. The x61xx-x040 models have two SFP ports. See the SFP manual for cautions and warnings.

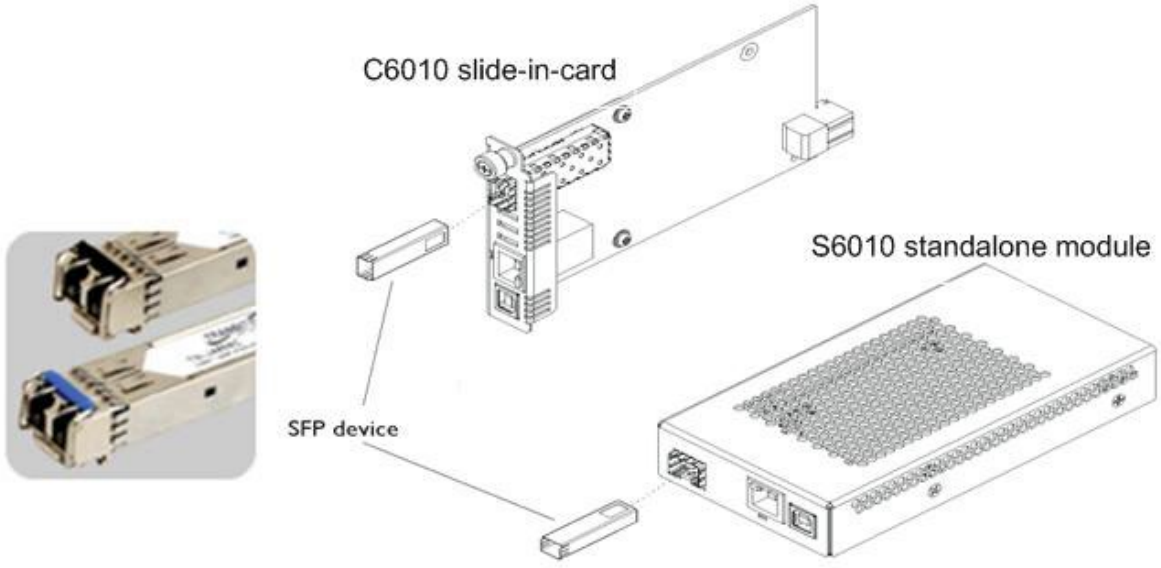


Figure 17: SFP Installation

1. Position the SFP device at either installation slot, with the label facing up (on the S6010) or to the right (on the C6010).
2. Carefully slide the SFP device into the slot, aligning it with the internal installation guides.
3. Ensure that the SFP device is firmly seated against the internal mating connector.
4. Connect the fiber cable to the fiber port connector of the SFP device.

Note: Make sure the SFP release latch is in the up (closed) position when you insert the cable connector into the SFP at the fiber port. (There should be a slight 'click' when connected.)

Connecting the C6010 to the S6010

Connect the C6010 to the S6010 using fiber ports. If two fiber lines are supported, connect the local and remote device's primary lines together, and then connect the secondary lines together.

Installing the USB Driver

IMPORTANT

The following driver installation instructions are for the *Windows XP* operating system only. Installing the USB driver using another operating system is similar, but not necessarily identical to the following procedure.

To install the USB driver on a computer running *Windows XP*, do the following.

1. Extract the driver from the website and place it in an accessible folder on the local drive of the PC.
2. Connect the NID to the USB port on the PC.

   Note: for slide-in modules installed in an ION Chassis, the USB connection will be made to the ION Management Module if one is installed in the chassis.

   The *Welcome to the Found New Hardware Wizard* window displays.
3. Select **No, not this time**.
4. Click **Next**. The installation options window displays.
5. Select **Install from a list or specific location (Advanced)**.
6. Click **Next**. The driver search installation options window displays.
7. Click **Browse**. Locate and select the USB driver downloaded in step 1 above.
8. Click **Next**. Driver installation begins.
9. When the finished installing screen displays, click **Finish**.

The USB driver installation is complete. You must now configure the COM port to be used by the terminal emulator.

Configuring HyperTerminal

After the USB driver has been installed, you must set up the terminal emulator software (e.g., HyperTerminal) to use the USB COM port.

1. On the desktop, right-click on **My Computer**.
2. Select **Manage**. The **Computer Management** window displays.
3. Click on **Device Manager** to open the Device Manager panel. (If a Device Manager message displays, click **OK** and continue.)
4. In the right panel, expand the list for **Ports (COM & LPT)**.

   Write down the USB COM port number for the "*TNI CDC USB to UART*" listing (e.g., **COM5**). You will need to provide this COM port number in step 8.
5. Launch the HyperTerminal software.

   a) Click **Start**.
   b) Select: **All Programs > Accessories > Communications**
   c) Click **HyperTerminal**.

   The Connection Description window displays.
6. Type in a name and select an icon that will be used for this connection.
7. Click **OK**. The **Connect To** window displays.
8. From the drop-down list in the **Connect using** field, select the COM port noted in step 4.
9. Click **OK**. The **Port Settings** window displays.
10. Set the COM port properties as follows:

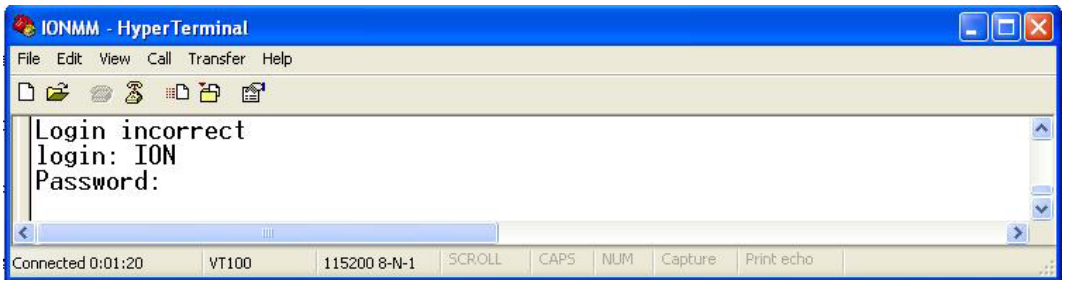
    - Bits per second: **115200**
    - Data bits: **8**
    - Parity: **None**
    - Stop bits: **1**
    - Flow control: **None**
11. Click **OK**. A blank HyperTerm window displays.
12. In the HyperTerm window, select **File > Properties**. The Properties window displays the **Connect To** tab.
13. Click the **Settings** tab. The Settings tab displays.
14. In the **Emulation** field, select **VT100**.
15. Click the **ASCII Setup…** button. The ASCII Setup window displays.
16. Verify that **Wrap lines that exceed terminal width** checkbox is checked.
17. Click **OK**, and then click **OK** again.
18. Login (see Starting a USB Session below).

Starting a USB Session in HyperTerminal

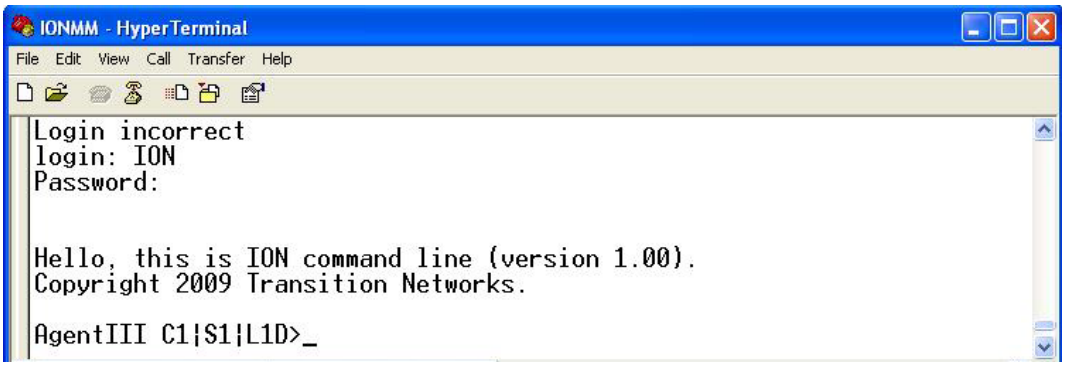
The following describes the procedure to access the NID via a USB connection.

1. Start the terminal emulator program (e.g., HyperTerminal).
2. When the emulator screen displays, press **Enter**. The login prompt displays.
   If the login prompt does not display, try unplugging and re-plugging the USB cable at the IONMM.

   Note: If your system uses a security protocol (e.g., RADIUS, etc.), you must enter the login and password required by that protocol.
3. Type your login (the default is **ION**). **Note:** the login is case sensitive.
4. Press **Enter**. The password prompt displays. **Note:** if a "*Login incorrect*" message displays, ignore it.



5. Type your password (the default is **private**). **Note:** the password is case sensitive.
6. Press **Enter**. The HyperTerminal command line prompt displays.



7. Enter a **go** command to change the location for the command prompt. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)
8. Enter commands to set up the various configurations for the NID. For configuration information, see "Section 4: Configuration" . For a description of all available CLI commands see "Section 6: Command Line Interface (CLI) Reference".

Note: If required by your organization's security policies and procedures, use the CLI command **set community write=<xx>** to change the default password. For a description of all available CLI commands see "Section 6: Command Line Interface (CLI) Reference".

Terminating a USB Connection from HyperTerminal

To terminate the USB connection, do the following.

1. At the command prompt, type **quit**.
2. Press **Enter**.
3. Click **Call** > **Disconnect**.
4. Click **File** > **Exit**.

Accessing the NIDs

The x6010 NIDs can be accessed through either a local serial interface via a USB connection or through an Ethernet network connection. The network connection can be done via a Telnet session or a Web graphical user interface (GUI).

Access via Local Serial Interface (USB)

The x6010 NIDs can be connected to a local management station (PC) through a serial interface using a USB connection. The NID is controlled by entering command line interface (CLI) commands at the local management station. To use the serial interface (USB) the following is required:

- Personal computer (PC)
- USB cable (type A male connector on one end and type B male connector on the other)
- Terminal emulator program (e.g., HyperTerminal) on the PC
- USB driver installed on the PC
- Configured COM port

IMPORTANT

In order to control the chassis slide-in module through a USB serial interface, the command line prompt must be showing the location of the module to be managed.

Operating Systems Supported

The following USB drivers are available at the Lantronix ION Products page.

Windows® 7	Windows 7 x64	Windows XP® 32 bit
Windows 2000	Windows 2003 32 bit	Windows Vista®
Windows Vista x64	Windows 8 and 8.1	Windows 10

Virtual COM port (VCP) drivers make the USB device appear as an additional COM port available to the PC. Application software can access the USB device in the same way as it would access a standard COM port.

Access via an Ethernet Network

The NID can be managed remotely through the Ethernet network via either a Telnet session or the Web interface. Before this is possible, you must set up the IP configuration for the x6010.

Starting a Telnet Session

The x6010 can be controlled from a remote management station via a Telnet session over an Ethernet connection. The x6010 is controlled and configured through CLI commands. Use the following procedure to connect to and access the x6010via a Telnet session.

1. Click **Start**.
2. Select **All Programs>Accessories**.
3. Click **Command Prompt**. The command prompt window displays.
4. At the command line type: **telnet** <xx> where:

   xx = IP address of the x6010
5. Press **Enter**. The login prompt displays. **Note**: If your systems uses a security protocol (e.g., RADIUS, etc.), enter the login and password required by that protocol.
6. Type your login (the default is **ION**). **Note:** the login is case sensitive – all upper case).
7. Press **Enter**. The password prompt displays.
8. Type your password (the default is **private**). The password is case sensitive - all lower case.
9. Press **Enter**. The command line prompt displays.
10. Enter a **go** command to change the location for the command prompt. The format is:
    go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
11. Press the **Enter** key.
12. Enter commands to set up the various configurations for the NID. For configuration information, see Section 4: "Configuration" . For a description of all available CLI commands see "Section 6: Command Line Interface (CLI) Reference".

Note: If required by your organization's security policies and procedures, use the CLI command **set community write=<xx>** to change the default password. See "Section 6: Command Line Interface (CLI) Reference".

Terminating a Telnet Session

To terminate the Telnet session:

1. Type **quit**.
2. Press the **Enter** key.

Web Browsers Supported

The ION system supports current versions of most popular web browsers (e.g., Mozilla Firefox, Internet Explorer, Google Chrome).

Starting the Web Interface

The NID can be controlled and configured from a remote management station via a Web graphical user interface (GUI) over an Ethernet connection. Information is entered into fields on the various screens of the interface. **Note:** fields that have a grey background cannot be modified.

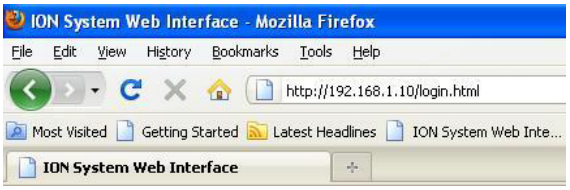
A Web session can be used to connect to and set up the x6010.

IMPORTANT

- Do not use the browser's back button to navigate screens – it causes the web connection to drop.
- Do not use the keyboard back space key in grayed out fields. This causes the web connection to drop.

To sign in to the NID via the Web, do the following.

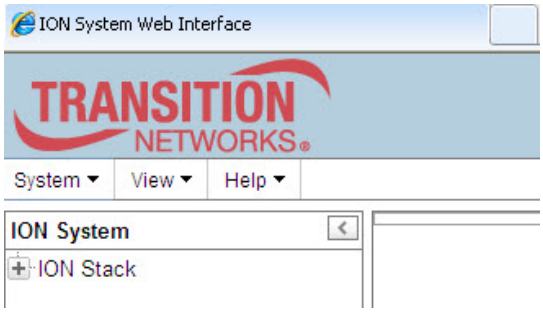
1. Open a web browser.
2. In the address (URL) block, type the IP address of the NID (the default address is 192.168.0.10).



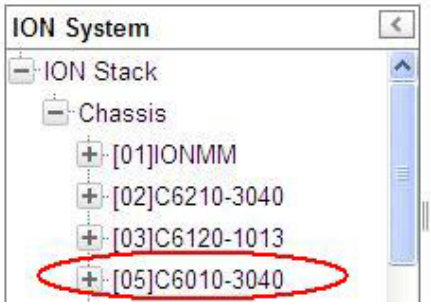
3. Click **Go** or press **Enter**. The ION System sign in screen displays.

Note: If your systems uses a security protocol (e.g., RADIUS, etc.), you must enter the login and password required by that protocol.

4. Type the User Name (the default is **ION**). **Note:** the System name is case sensitive – all upper case.
5. Type the Password (the default is **private**). **Note:** the password is case sensitive – all lower case.
6. Click **Sign in** or press **Enter**. The opening screen displays the ION System / ION Stack.

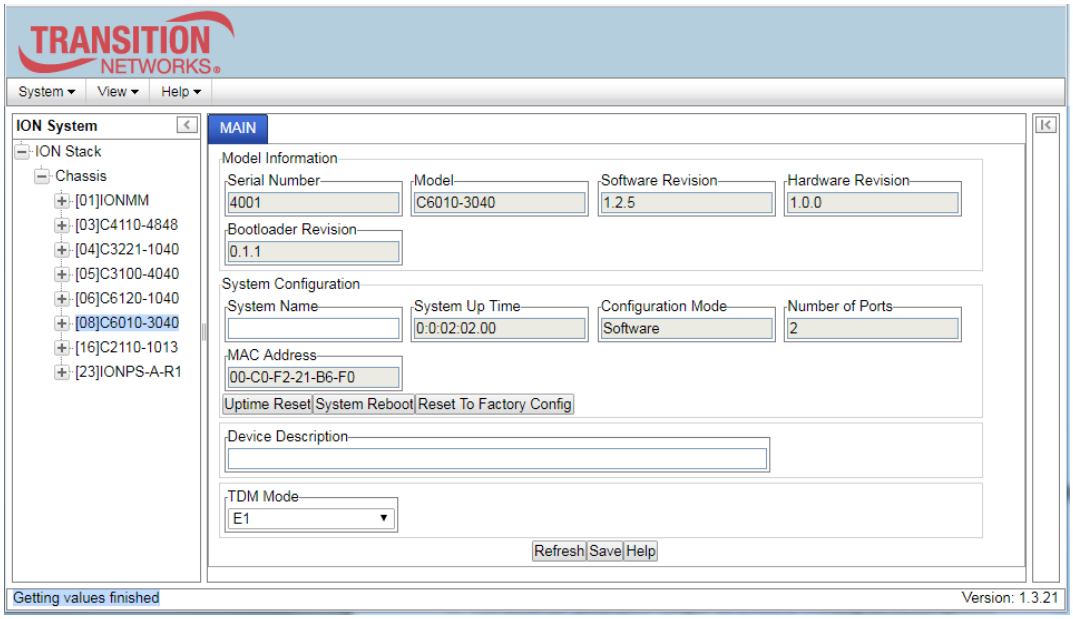


7. Click the plus sign **[+]** next to **ION Stack**. This unfolds "ION Stack" node in the left tree view and will refresh device status.
8. Click the plus sign **[+]** next to **Chassis** to unfold the chassis devices.



9. Select the appropriate NID. The **MAIN** screen displays for the selected NID.

   The Model C6010-1040 **MAIN** tab screen is shown below.

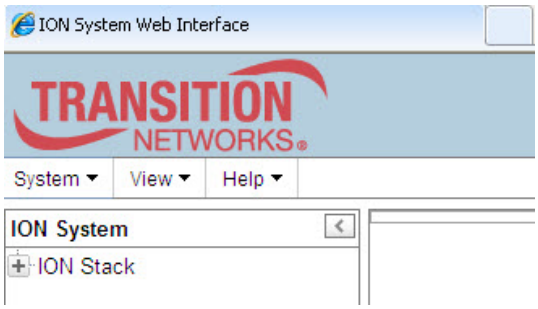


10. You can use the various tabs to configure the system, devices and ports. For configuration information, see "Section 4: Configuration".

Note: If required, use the **set community** CLI command to change the default password according to your organization's security policies and procedures.

Terminating the Web Interface (Sign Out)

To sign out from the Web interface, in the upper left:



1. Click **System** ▾. The **Sign out** selection drops down.
2. Click **Sign out**.

The sign in screen displays.

Note: The x6010 does not automatically sign out upon exit or after a timeout period, which could leave it vulnerable if left unattended. Follow your organizational policy on when to log out.

Initialization (Default) Configuration

The x6010 assumes the following operating characteristics on initial startup. These are the default initialization parameter values for the x6010. See Appendix B: Factory Defaults for a summary of all of the default settings.

Parameter	Property	Default Value
T1/E1 Model	Read only	T1
Configuration Mode	Read only	SW
Fiber Port		
• Link	Read only	Down
• Transmit All Ones	Read & Write	Enabled
• Alarm Indication Signal	Read only	Normal
• Loopback	Read & Write	Disabled
Copper Port		
• Link	Read only	Down
• Transmit All Ones	Read & Write	Enabled
• Alarm Indication Signal	Read only	Normal
• Loopback	Read & Write	Disabled
• Long Haul	Read only	No

See section 4 Configuration for the procedures used to change these default settings.

3 Management Methods

General

The x6010 NIDs are managed through the IONMM using one of the following methods.

- Simple Network Management Protocol (SNMP) – both public and private Management Information Bases (MIBs) allowing for a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).
- Telnet session – uses a command line interface (CLI) to access and control the IONMM via the network.
- Universal Serial Bus (USB) – uses a CLI to access and control the IONMM through a locally connected workstation.
- Web-browser – access and control the IONMM using a standard web browser and a graphical user interface (GUI).

The x6010 NIDs cannot be remotely managed directly (i.e., only through IONMM).

IONMM Managed x6010

NIDS that are managed through the IONMM are either chassis resident (C6010) or standalone modules (S6010) that are connected as remotes to chassis resident modules. Communications between the IONMM and each x6010 is through the ION Chassis backplane.

You can manage and configure the x6010 via the CLI or the Web interface.

Managing Slide-In and Remote Modules Using CLI Commands

Management of modules other than the IONMM can be accomplished by entering CLI commands through either the local USB serial interface or a remote Telnet session. CLI commands can operate on the device level or port level. This is indicated by the status of the command prompt's preamble.

For example:

```
AgentIII C1|S1|L1D>
```

or just:

```
C1|S1|L1D>
```

This prompt indicates that any subsequent commands entered are for the module located in chassis 1/slot1. In order to enter a command for a different device or port in the ION system, you must change the location of the command prompt. The **go** command lets you change the hierarchical location of the command prompt. Before using the command, a familiarity with the hierarchy structure in the ION system is essential.

The ION system hierarchy is shown in the figure below.

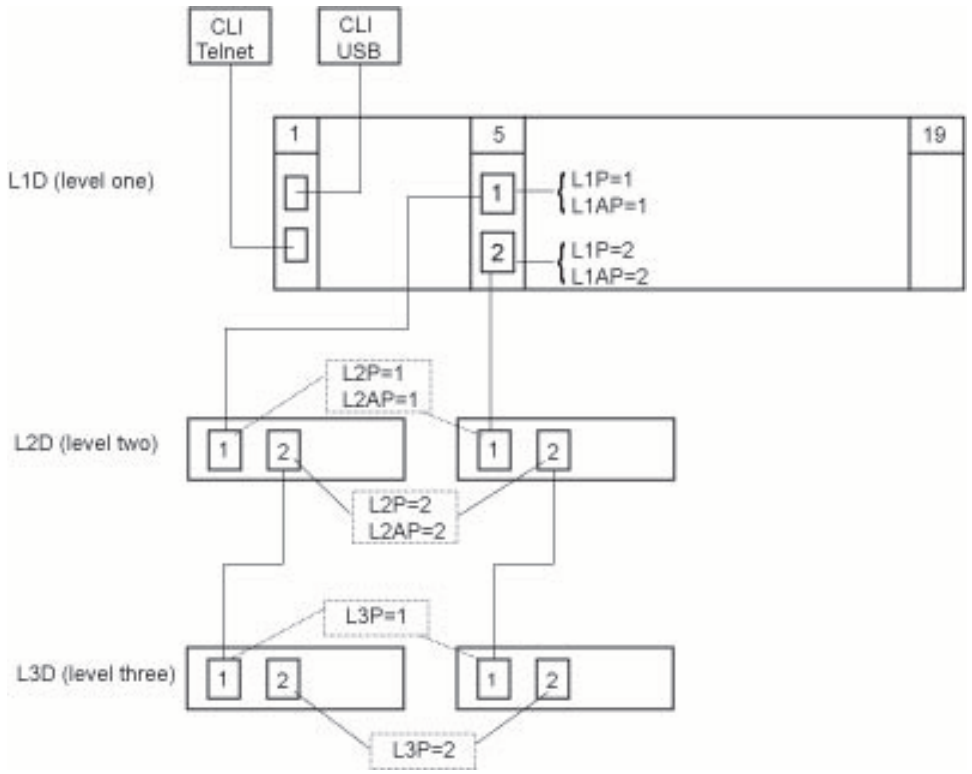


Figure 18: CLI Location Hierarchy

In the above figure, there are three levels of devices:

- L1D (level one device) refers to devices (IONMM and other NIDs) that are installed in the chassis.
- L2D (level two device) refers to a device that is directly connected to a port in a NID in the chassis and has other devices connected to it.
- L3D (level three device) refers to a device that is directly connected to a port in a level one device.

The ports on a device are divided into two categories: Device ports and Attachment ports.

- Device ports – These are ports on a specified device that are used as service ports for either customer or network connections, and are typically attached to routers or switches. These ports are labeled L1P=, L2P= and L3P=. The L1, L2, and L3 indicate the level of the device that the port is on. Devices attached to a port with this designation **cannot** be managed by the IONMM.
- Attachment port – These are also ports on a specified device; they are labeled L1AP= and L2AP= and indicate an attachment point for another ION family device that **can** be managed by the IONMM.

Physically these are the same port. That is, L1P1 and L1AP1 are both port one on a level one device. However, it is how they are used that determines their syntax. For example, L1P1 indicates that the port is used to connect to a service device that is not managed by the IONMM. L1AP1 (level 1 attachment

port 1) indicates that the port is used to connect to a level two device that can be managed by the IONMM.

Example 1

In the CLI location hierarchy, to go to the first port (L3P1) on device L3D in the network topology shown in Figure 20, you would enter the following command from the base prompt.

```
C1|S1|L1D>go s=5 l1ap=2 l2ap=1 l3p=1
```

The resulting command line prompt would be:

```
C1|S5|L1AP2|L2AP1|L3P1>
```

Any CLI command appropriate for the port can now be entered.

Example 2

In the CLI location hierarchy, to go to device L2D in the network topology shown in Figure 19, you would enter the following command from the base prompt.

```
C1|S1|L1D>go s=5 l1ap=2 l2d=1
```

The resulting command line prompt would be:

```
C1|S5|L1AP1|L2D>
```

Any CLI command appropriate for the device can now be entered.

The following describes the procedure for using CLI commands to manage the NIDs.

1. Access the NID through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. Use the **go** command to change the operational location to the device/port to be managed. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
3. Configure the NID using the appropriate commands. See "Section 6: Command Line Interface (CLI) Reference".
4. To return the location to the IONMM, type **home** and press **Enter**.

Note: Use the **stat** command to display the current ION chassis/card/port/remote device configuration.

```
AgentIII C1|S1|L1D>stat
ION statck
        Chassis – BPC
                [  1]  IONMM
                        Port 1
                        Port 2
                [  2]  C6210-3040
                        Port 1
                        Port 2
                [  3]  C6120-1013
                        Port 1
                        Port 2
                        Port 3
                        Port 4
                        Port 5
                        Port 6
                [  5]  C6010-3040
                        Port 1
                        Port 2
                                level2 REM: S6010-1040
                                        Port 1
                                        Port 2
```

For more information, see the Status check (**stat**) command in "Section 6: Command Line Interface (CLI) Reference".

To switch command control from the local slot 4 C6010-3040 to its level 2 remotely-connected device (S6010-1040) in the **stat** command example above, you would enter:

```
C1|S4|L1D>go c=1 s=4 l1ap=2 l2d
```

Command control would be shown by the command line prompt:

```
C1|S4|L1AP2|L2D>
```

To switch command control to port 1 of the level2 REM: S6010-1040 above, you would enter:

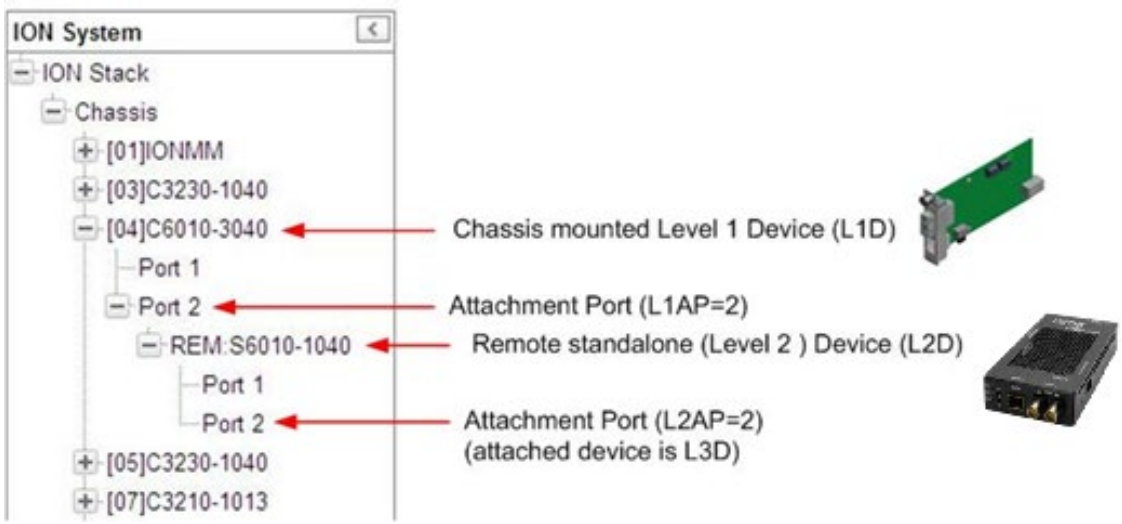
```
C1|S4|L1AP2|L2D>go l2p=1
```

Command control would be shown by the command line prompt:

```
C1|S4|L1AP2|L2P1>
```

Managing Slide-In and Remote Modules via the Web Interface

1. Access the NID through the Web interface (see "Starting the Web Interface").
2. Click on the slide-in module or port to be managed.



3. Click on the ( ) for a particular device and click on the port to be managed.
4. The operations that can be performed depend on the type of device or port selected. Refer to the specific product documentation for other device information. See the "Related Manuals" section.

Managing Standalone Modules Using CLI Commands

Management of standalone modules can be accomplished by entering CLI commands through either the local USB serial interface or a remote Telnet session. CLI commands can operate on the device level or port level. This is indicated by the status of the command prompt's preamble.

For example:

```
AgentIII C1|S5|L1D>
```

or just:

```
C1|S5|L1D>
```

This prompt indicates that any subsequent commands entered are for the device instead of a port. In order to enter a command for a port, you must change the location of the command prompt. The **go** command allows you to change the hierarchical location of the command prompt.

The **go** command format is:
go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)

For example:

In the CLI location hierarchy, to go to port 1 on a device, you would enter the following command from the base prompt:

```
C1|S5|L1D>go l1p=1
```

The resulting command line prompt would be:

```
C1|S5|L1P1>
```

Any CLI command appropriate for the port can now be entered.

Subsequently, to return to the device level, you would enter the following:

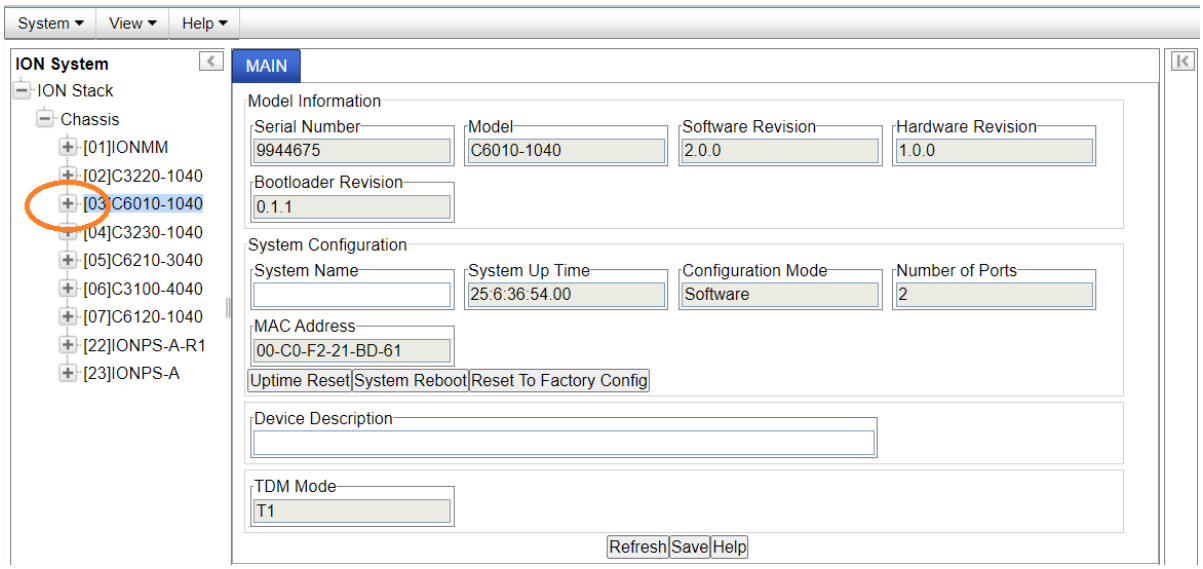
```
C1|S5|L1P1>go l1d
```

The resulting command line prompt would be:

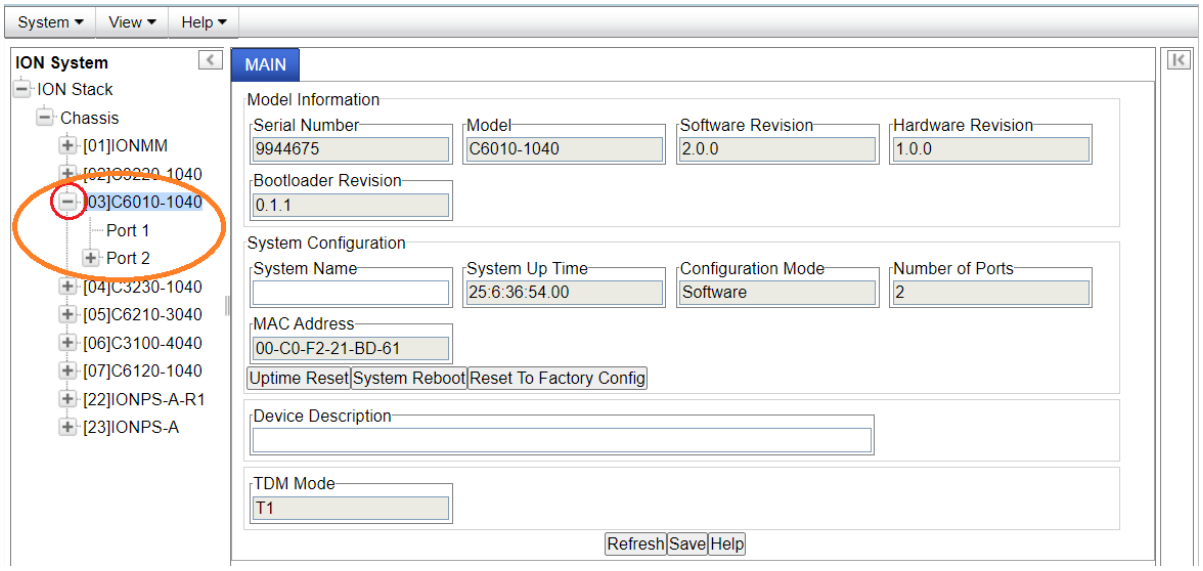
```
C1|S5|L1D>
```

Managing Standalone Modules via the IONMM Web Interface

1. Access the x6010 through the Web interface (see "Starting the Web Interface").
2. Click the plus sign ( ) next to **ION Stack** to unfold the "**ION Stack**" node in the left tree view if not already done.
3. Click the plus sign ( ) next to **Chassis** and click the plus sign ( ) next to a module.

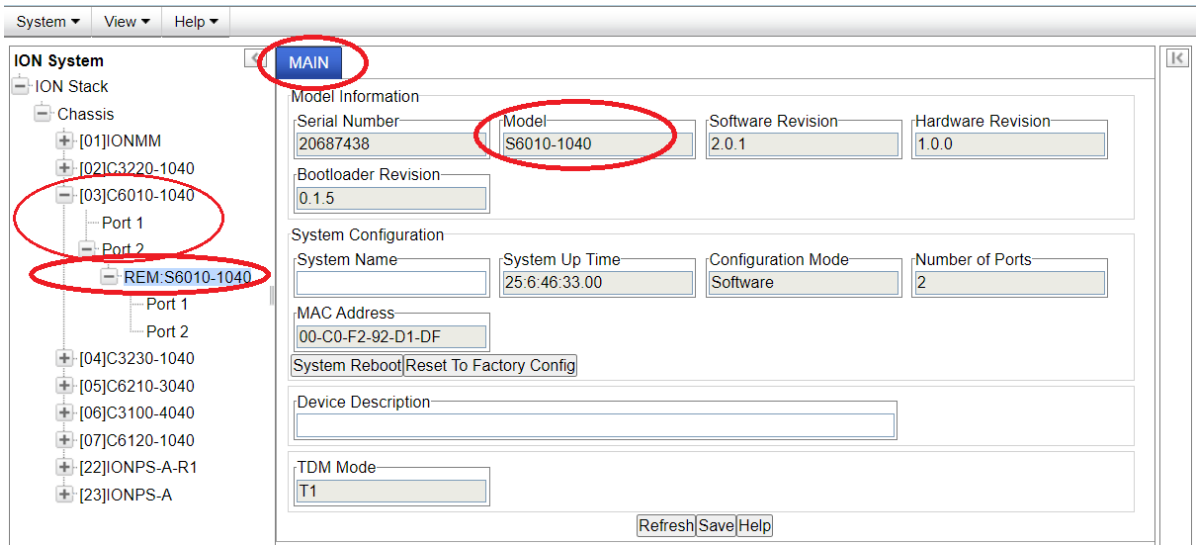


4. Click on the desired module (e.g., **[03]C6010-1040]** on the screen above).



5. Click on the plus sign ( ) next to the attachment port to be managed **(Port 2** above).

The remote device's MAIN tab displays.



6. Click on the **[+]** next to the remote device to be managed (**REM:S6010-1040** above).
7. Select the various ports / fields to perform the desired operations.

Menu Descriptions

This section describes the ION Web interface in terms of its system-level, device-level, and port-level menus. Note that menus and tabs vary slightly by model.

System-Level Menus

The table below describes the ION Web interface in terms of its system-level pane, dropdowns, tabs and sub-tabs. Note that menus and tabs vary slightly by model.

Table 6: System-Level Menu Description

Dropdown / Tab	Description
ION System pane	**Stack** – consists of one to many chassis or one standalone. The Stack Members table lists the Stack's chassis and its type. **Chassis** – the ION System family of products, multiple chassis may be connected together via Inter-Chassis Interface cables and managed by a single ION System SNMP Agent. The Chassis View shows a summary view of one such chassis. Model Information includes: * Serial Number – The serial number of the chassis itself. Individual NIDs also have their own serial numbers. * Model Name – The exact model name of this device. When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number. * Software, Revision, and Bootloader Revision. * Chassis Members table – lists local physical components in slots 1 to 19. **Device** – provides tabs and sub-tabs for the IONMM and NIDs in the ION system. **Port** – provides tabs and sub-tabs for the IONMM or a selected NID port.
System Dropdown	Sign out.
View Dropdown	Refresh.
Help Dropdown	Online Help, ION Product Home Page, About ION System Web Interface.

Device-Level Menus

The table below describes the ION Web interface in terms of its device-level pane, dropdowns, tabs and sub-tabs. Note that menus and tabs vary slightly by model.

Tab	Description
MAIN Tab	Sections: Model Information, System Configuration, Device Description, and TDM Mode sections. Buttons: *Uptime Reset*, *System Reboot*, and *Reset to Factory Config*. *Refresh, Save,* and *Help.*

Port-Level Menus

The table below describes the ION Web interface in terms of its port-level tabs and sub-tabs.

Table 7 : Port-Level Menu Description

Tab	Description
MAIN Tab	Sections: Circuit ID, Port Configuration, and Loopback Management. Port 1 Fields: Link Status, AIS Transmit, Transmit All Ones, Alarm Indication Signal, Long Haul, Line Build Out, Connector Type, Loopback Type, Loopback Status. Port 2 Fields: Link Status, AIS Transmit, Transmit All Ones, Alarm Indication Signal, Connector Type, Loopback Type, Loopback Status. Buttons: *Refresh, Save, Start, Stop,* and *Help.*
DMI Tab (Port 2 only)	Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length. The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See "DMI Test" for more information. **Note**: not all NID or SFP models support DMI. If you click the DMI tab on a NID model that does not support DMI, the message "*The DMI feature is not supported on current port*."

Reboot, Reset, and Power Off Function Notes

Certain functions such as a System Reboot, Reset to Factory Configuration, Reset Power to a Slot, and Power Off a Slot) cause the system to delete certain stored files. ***Caution***: In some circumstances, these stored files are lost unless you first perform a System Backup. See the "Backup and Restore Operations" section for information on how to save the stored files from deletion.

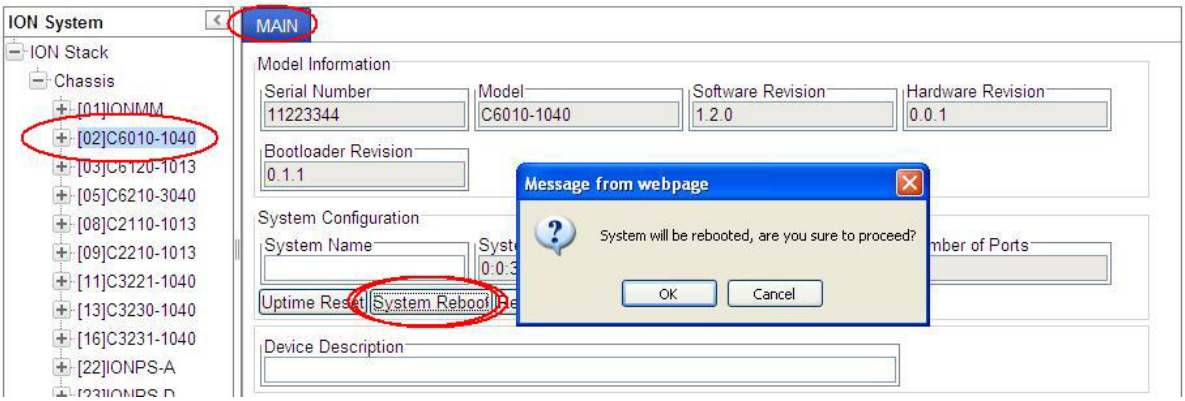
For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- Table 17. Back Up and Restore File Content and Location
- Table 18. File Status after a Reset to Factory Defaults
- Table 19. File Content and Location after a System Reboot
- Table 20. File Content and Location after a Firmware Upgrade

Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory removes temporary files (e.g. configuration backup files, Syslog file). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key).

System Reboot

Clicking the **System Reboot** button resets all system states and reinitializes the system; all configuration data is saved during a restart.



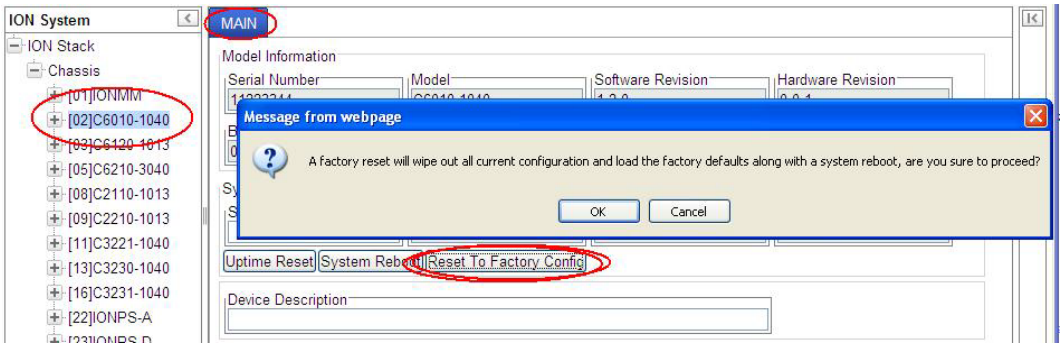
Press the **Cancel** button if you are not sure you want a system reboot to occur.
Press the **OK** button to clear the webpage message and begin the reboot process. The message "*Loading, please wait...* displays.

Note that a System Reboot can take several minutes.

Reset To Factory Config

Clicking the **Reset To Factory Config** button resets the entire system configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the system configuration with the factory default settings.

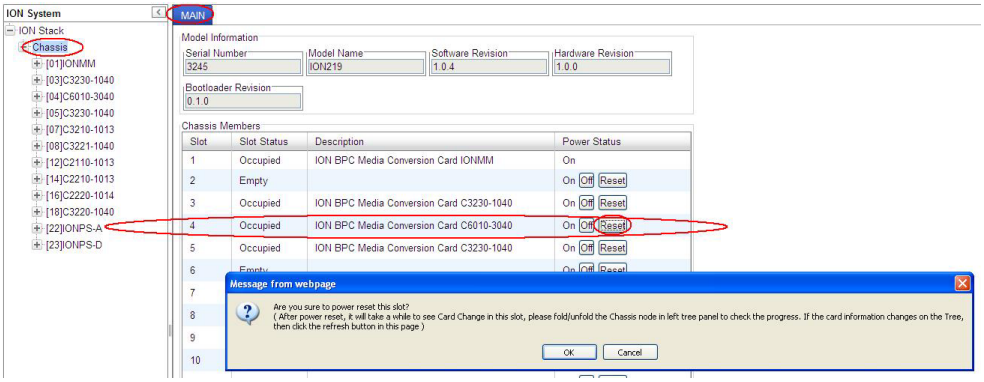
The message "*A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*" displays.



You should only click **OK** if you wish to reboot. Otherwise, click **Cancel** if you are not sure you want a factory reset / reboot to occur.

Reset Power to a Slot

The x6010 provides two Reset functions: a software reset and hardware reset. At the **Chassis** > **MAIN** tab, you can click the **Reset** button to reset power for a specific slot in the chassis. The message "*Are you sure to power reset this slot?*" displays.

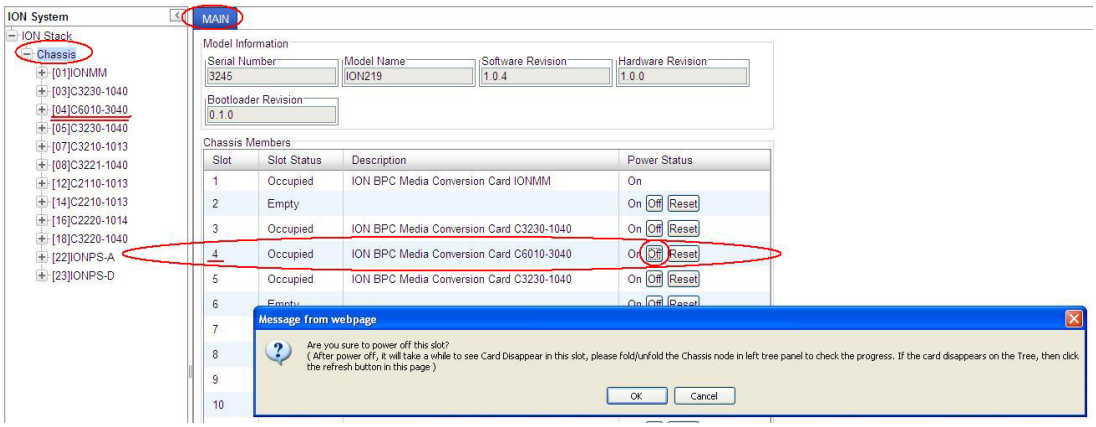


After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page.

If you are not sure that you want to reset this chassis, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.

Power Off a Slot

At the **Chassis** > **MAIN** tab, you can click the **Off** button to remove power to a specific slot in the chassis. The message "*Are you sure to power off this slot?*" displays.



If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.

After power off, it will take a while for the card to disappear from this slot. Fold and then unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page.

4 Configuration

General

After the NID has been installed and access has been established, the device and its ports must be configured to operate within your network. The configuration establishes operating characteristics of the device and the ports associated with the NID.

Configurations can be done either by entering CLI commands (USB / Telnet) or through a Web interface. For complete descriptions of all CLI commands, see “Section 6: Command Line Interface (CLI) Reference”.

The operating characteristics that can be defined for the NID are:

- System setup
- Features
  - Interface *(*AIS, TDM, Loopback modes)
- Security

Note: Lantronix recommends as a “best practice” to back up each SIC card’s configuration after it is fully configured so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored.

System Configuration

The system configuration defines a name for the NID, and (optionally) a Device Description.

The system configuration can be defined via the CLI or the Web interface.

System Configuration – CLI Method

The system information can be alphabetic, numeric or a combination. See "Section 6: Command Line Interface (CLI) Reference" for individual CLI command details.

1. Set the x6010 DIP switches and jumpers for your environment. See "Jumper Settings" and "DIP Switch Settings".
2. Access the NID through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
3. Type **set system name**=NAME, where NAME is the new system name, and press **Enter**.
   For example:

```
AgentIII C1|S5|L1D>set system name=C6010-3040
```

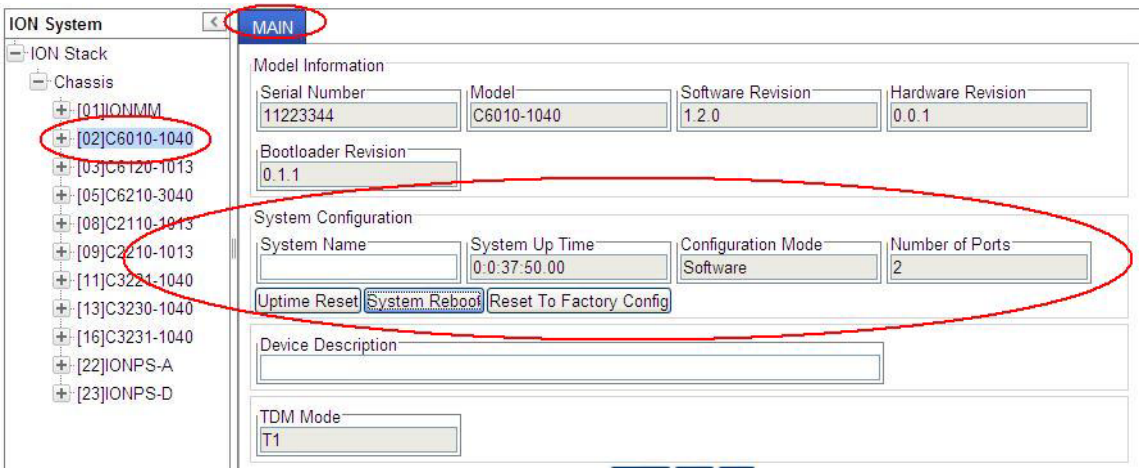
4. Verify the new system definition. Type **show card info** and press **Enter**. For example:

```
AgentIII C1|S5|L1D>show card info
System name:        C6010-3040
Uptime:             21:03:26
Port number:        2
Serial number:      12345678
Config mode:        software
Software:           1.2.5
Bootloader:         0.1.1
Hardware:           1.0.0
Agent III C1|S2|L1D>
```

Note: the **show card info** command does not function for a Power Supply module.

T1 System Configuration – Web Method

1. Set the x6010 DIP switches and jumpers for your environment. See "Jumper Settings" and "DIP Switch Settings".
2. Access the x6010 via the Web interface (see "Starting the Web Interface").
3. Locate the **System Configuration** section.



4. In the **System Name** field, enter the name and for the x6010 device. The name can be alphabetic, numeric or a combination. Do not enter spaces in the **System Name** field.
5. Enter a **Device Description** of up to 64 characters, as required.
6. Scroll to the bottom and click **Save**.
7. Verify the device-level configuration settings:

   Serial Number – e.g., 12345678 (read only field).
   Model – e.g., C6010-3040 (read only field).
   Software Revision – e.g., 1.2.5 (read only field).
   Hardware Revision – e.g., 0.0.1 (read only field).
   Bootloader Revision – e.g., 0.1.1 (read only field).

   System Name – e.g., C6010-3040 (read/write field).
   System Up Time: e.g., 5:5:59:26.00 (read only field).
   Configuration Mode: Hardware or Software (read only field).
   Number of Ports: e.g., 2 (read only field).

   Device Description: blank or as entered (read/write field).

   TDM Mode: e.g., T1 or E1 (dropdown)

T1 Ports Configuration

The x60xx ports configuration sets Port 1 and Port 2 Circuit ID, AIS Transmit and TDM Loopback type. You can configure the x60xx ports via the CLI or the Web interface.

T1 Ports Configuration – CLI Method

The port information can be alphabetic, numeric or a combination. See "Section 6: Command Line Interface (CLI) Reference" for individual CLI command details.

1. Access the x60xx through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. Configure the Port 1 Circuit ID. At the command prompt type **set circuit-ID=xx** (up to 64 alphanumeric characters) and press **Enter**.
3. Configure the Port 1 Loopback Type. Type **set tdm loopback type**=***phylayer*** and press **Enter**.
4. Use the **go** command to switch to Port 2.
5. Repeat steps 2-3 above to configure the Port 2 Circuit ID, AIS Transmit, and Loopback Type.
6. Configure the Port 2 DMI function (optional – if supported). See "DMI (Diagnostic Maintenance Interface) Test" for more information.
7. Click the **Save** button when done. For example:

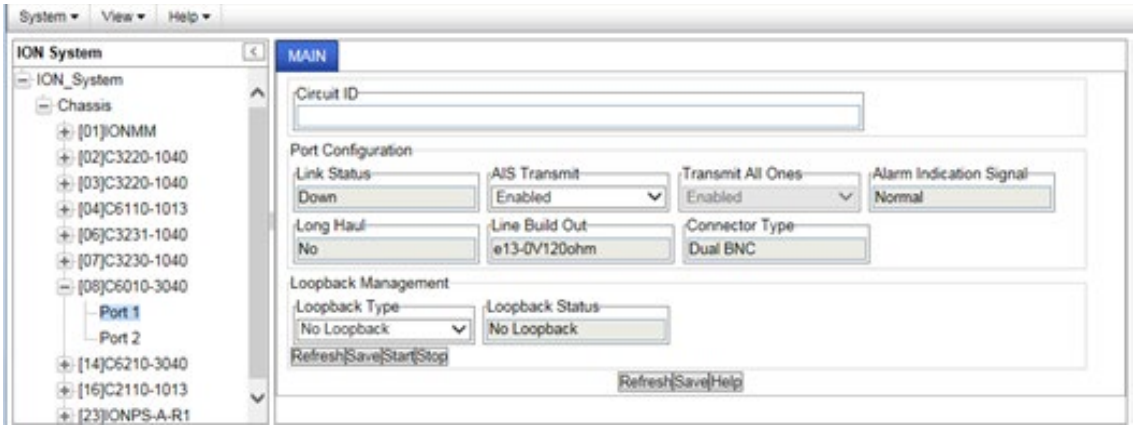
```
AgentIII C1|S5|L1P1>set ais transmit=enable
AgentIII C1|S5|L1P1>set tdm loopback type=phylayer
AgentIII C1|S5|L1P1>go l1p=2
AgentIII C1|S5|L1P2>set ais transmit=enable
AgentIII C1|S5|L1P2>set tdm loopback type=phylayer
```

10. Verify each port's configuration. For example:

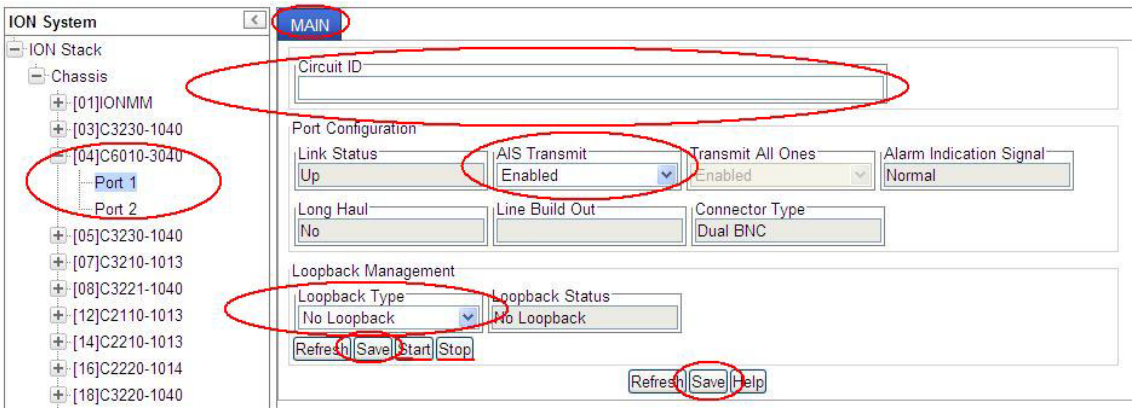
```
AgentIII C1|S5|L1D>go l1p=1
AgentIII C1|S5|L1P1>show tdm port config
link oper status:                                   up
alarm indication signal:                            normal
taos transmit:                                      enabled
longhaul:                                           no
lbo status:                                         unknown
connector:                                          Dual BNC
AgentIII C1|S5|L1P1>go l1p=2
AgentIII C1|S5|L1P2>show tdm port config
link oper status:                                   up
alarm indication signal:                            alarm
taos transmit:                                      enabled
connector:                                          SFP Slot
AgentIII C1|S5|L1P2>
```

T1 Ports Configuration – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface").
2. Select Port 1.

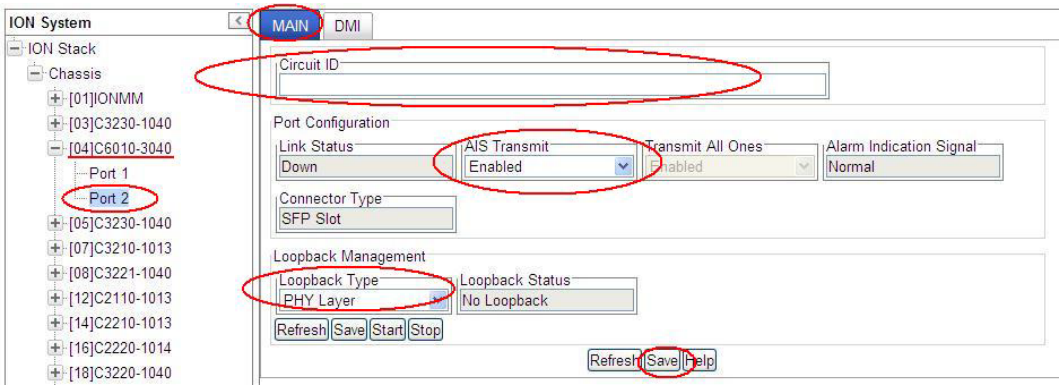


3. In the Port 1 **MAIN** tab, in the **Circuit ID** field, enter up to 64 alphanumeric characters as required.
4. In the **Port Configuration** section in the **AIS Transmit** field, select **Enabled** or **Disabled**.

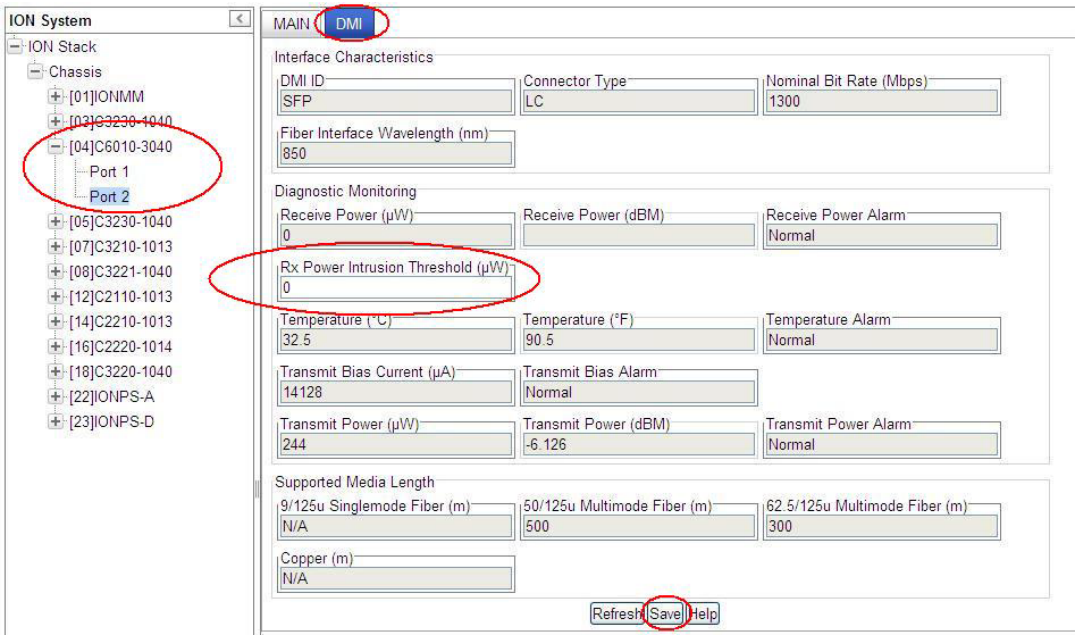


5. In the **Loopback Management** section in the **Loopback Type** field, select N**o Loopback** or **PHY Layer**. See "Ports Loopback Test" for the PHY layer loopback test procedure.
6. Click the **Save** button when done.

7. Select **Port 2**.



8. At the Port 2 **MAIN** tab, in the **Circuit ID** field, enter up to 64 alphanumeric characters as required.
9. In the **AIS Transmit** field, select **Enabled** or **Disabled**.
10. In the **Loopback Type** field, select **No Loopback** or **PHY Layer**.
11. Click the **Save** button when done.
12. Select the Port 2 **DMI** tab (optional – only if DMI is used).



13. Set the **Rx Power Intrusion Threshold** (0-65535 µW). The default is 0 uW.
14. Click the **Refresh** button and verify the DMI status. See "DMI (Diagnostic Maintenance Interface) Test" for more information.
15. Click the **Save** button when done.
16. Verify the C6010 **Port 1** (copper port) configuration settings:

Circuit ID – either blank or the information entered earlier displays (read/write field).

Link Status – either **Down** or **Up** displayed (read only field).

AIS Transmit – Select **All Ones** or **Blue** on the Port 1 copper interface as an error signal when the copper interface is down. When this error signal is transmitted, the AIS of the device on the other end is activated, if supported (read/write field).

Transmit All Ones – Transmit AIS (All Ones:1111... sequence / BLUE:0101... sequence) on the Port 1 copper interface as an error signal for the DS3/E3/STS-1 port.

Alarm Indication Signal – When "***Alarm***" displays, this means that the other end has TAOS enabled and is currently transmitting an alarm condition. When "***Normal***" displays, this means no alarm (read only field).

Long Haul – This variable indicates the current position of the remote device's Short/Long haul configuration switch (read only field).

TDM Mode – This variable indicates the type of the current device. T1=1.544MHz; E1=2.048MHz; E3=34.4Mb/s; DS3 = 44.7Mbps; STS-1 = 51.8Mbps.

Line Build Out – The characteristics of the x6010's copper interface (read only field) as defined by DIP switch. An x60xx with Coax interface works in E1 mode only; in this mode the Line Build Out is e12-37V75ohms.

Connector Type – RJ45, SFP ~~Dual BNC~~, etc. – model dependent (read only field).

Loopback Type – either "No Loopback" or "PHY layer" loopback displayed.

Loopback Status – either "**Local In Loopback**" or "**No Loopback**" displayed.

17. Verify the C6010 **Port 2** (fiber port) configuration settings:

Circuit ID – either blank or the information entered earlier displays.

Link Status – either **Down** or **Up** displayed (read only field).

AIS Transmit – Select **All One**s or **Blue** on the Port 2 fiber interface as an error signal when the Port 2 fiber interface is down. When this error signal is transmitted, the AIS of the device on the other end is activated, if supported (read/write field).

Transmit All Ones – Transmit AIS (All Ones:1111... sequence / BLUE:0101... sequence) on the Port 2 fiber interface as an error signal for the DS3/E3/STS-1 port (read only field).

Alarm Indication Signal – When "***Alarm***" displays, this means that the other end has TAOS enabled and is currently transmitting an alarm condition. When "***Normal***" displays, this means no alarm (read only field).

Connector Type –SFP Slot, etc. – model dependent (read only field).

Loopback Type – either "**No Loopback**" or "**PHY layer**" loopback displayed (read/write field).

Loopback Status – either "**Local In Loopback**" or "**No Loopback**" displayed.

Rx Power Intrusion Threshold – from 0-65535 µW. The default is 0 uW. (DMI tab)

Port Loopback Tests

Each port lets you configure, start, and stop a PHY Layer local loopback test and display status. Note that you can run just one port's loopback test at a time.

With the x60xx in Hardware mode, just set the x60xx front panel **CL** – **FL** switch to the **CL** (copper loopback mode) position to start and stop the loopback test.

In SW mode, the front panel **CL**- **FL** switch position is ignored. You can run the port loopback test via either the CLI or the Web interface.

Port Loopback Test – CLI Method

1. Access the x60xx through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. At the x60xx CLI command prompt, use the **go** command to switch to Port 1. Type **go c1 s*x* l1p=1** and press **Enter** (where x is the slot where the x6010 is located in the ION chassis). To control S6010 loopback, type **go c1 sx l1ap=2 l2p=1** and press **Enter**.
3. Set the TDM Loopback type to PHY layer. Type ***set tdm loopback type=phylayer*** and press **Enter**.
4. Start the Port 1 Loopback operation. Type **set tdm loopback oper**=***init*** and press **Enter**.
5. Stop the Port 1 Loopback operation. Type **set tdm loopback oper**=s***top*** and press **Enter**.
6. Set the x6010 front panel **CL** – **FL** switch to the **FL** (Fiber Loopback mode) position.
7. Use the **go** command to switch to Port 2.
8. Repeat steps 1-5 above for Port 2. For example:

```
C1|S4|L1P2>set tdm loopback type phylayer
C1|S4|L1P2>set tdm loopback oper init
C1|S4|L1P2>set tdm loopback oper stop
C1|S4|L1P2>show tdm loopback capability
Loopback capability: phyLayer
C1|S4|L1P2>show tdm loopback state
Loopback type: phylayer
Loopback state: noLoopback
```

9. Use the **show tdm config** command to display and verify the device-level TDM configuration:

```
C1|S4|L1D>show tdm config
tdm type:                                          t1
```

10. Use the **show tdm port config** command to display and verify the port-level TDM configuration for each port.

Example 1:

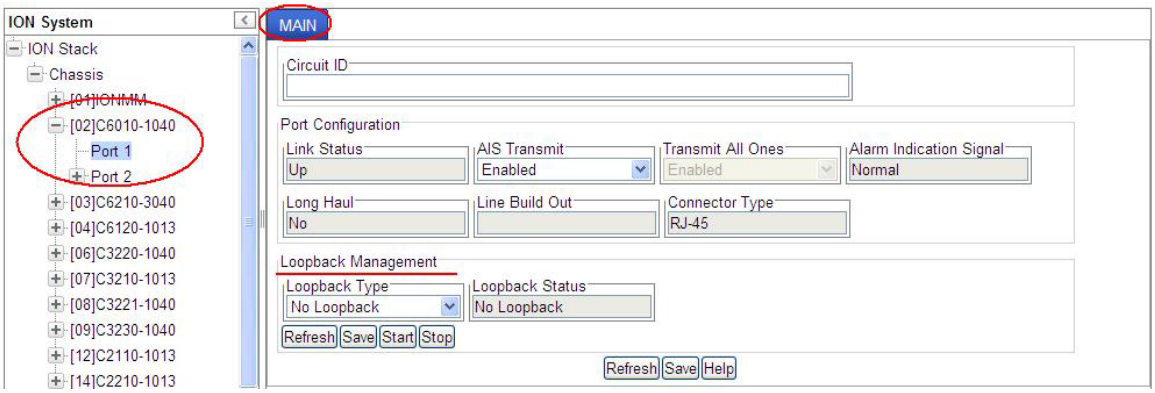
```
C1|S4|L1P1>show tdm port config
link oper status:                                up
alarm indication signal:                         normal
taos transmit:                                   enabled
lbo status:                                      unknown
longhaul:                                        no
connector:                                       Dual BNC
C1|S4|L1P1>go l1p=2
C1|S4|L1P2>show tdm port config
link oper status:                                down
alarm indication signal:                         normal
taos transmit:                                   enabled
connector:                                       SFP Slot
C1|S4|L1P2>
```

Example 2:

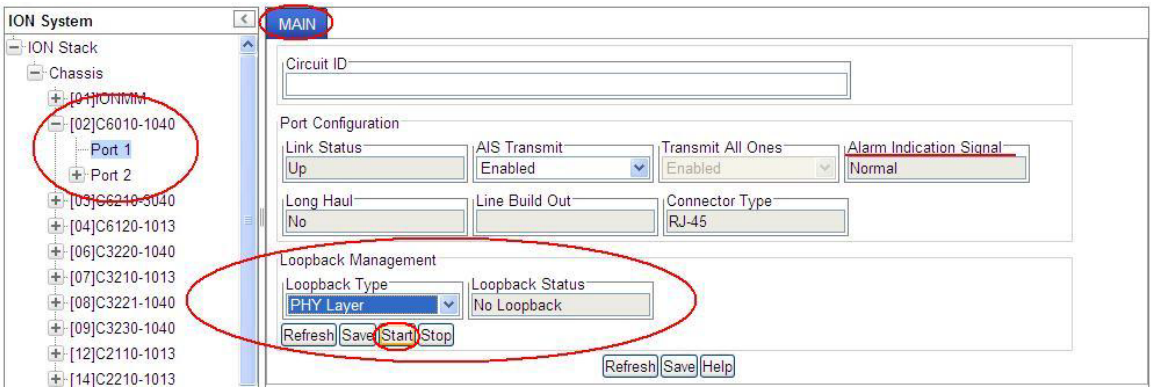
```
C1|S4|L1P1>show tdm port config
link oper status:                                up
alarm indication signal:                         normal
taos transmit:                                   enabled
lbo status:                                      t1LH-m22-5dB
longhaul:                                        yes
connector:                                       Dual BNC
C1|S4|L1P1>go l1p=2
C1|S4|L1P2>show tdm port config
link oper status:                                down
alarm indication signal:                         normal
taos transmit:                                   enabled
connector:                                       SFP Slot
C1|S4|L1P2>
```

Port Loopback Test – Web Method

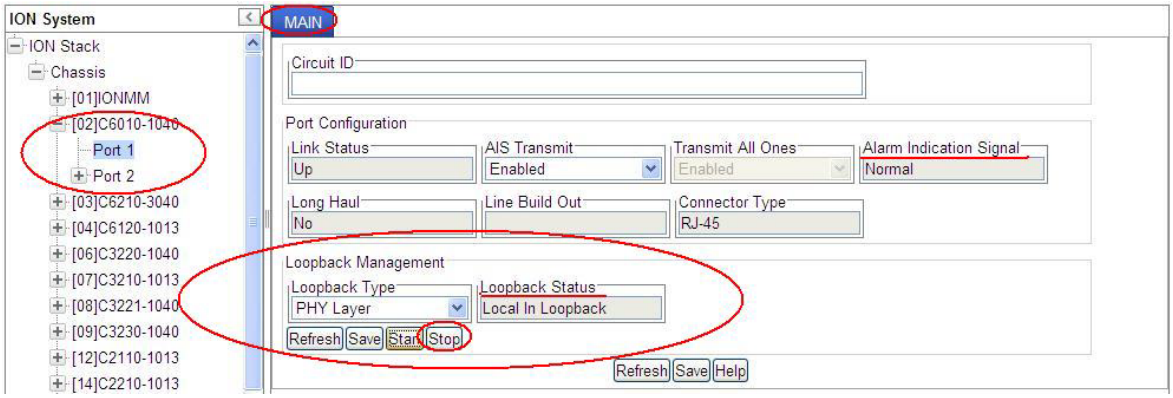
1. Go to the **x6010** > **Port 1** > **MAIN** > **Loopback Management** section.



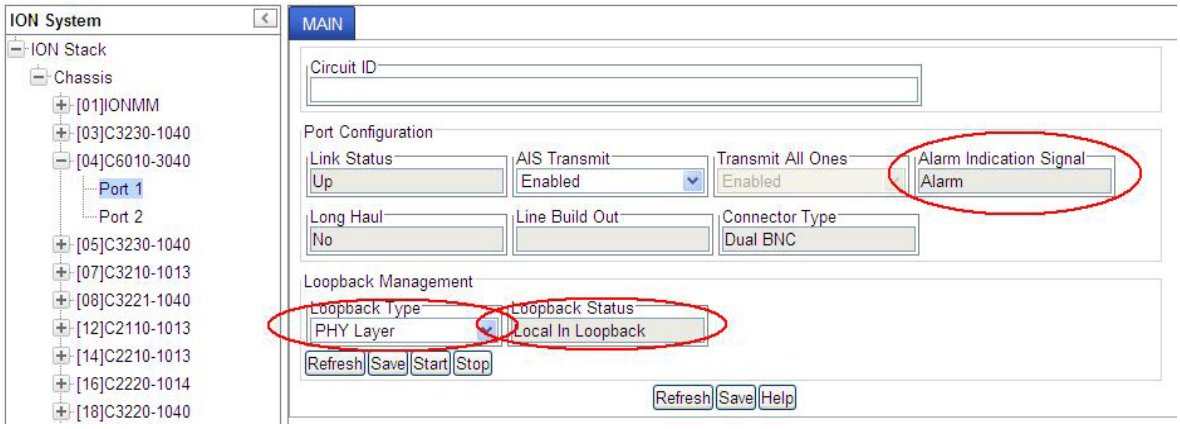
2. In the **Loopback Type field**, select **PHY Layer**.



3. Click the **Start** button. The **Loopback Status** field displays "**Local In Loopback**".



4. Click the **Refresh** button. Check if the **Alarm Indication Signal** field changes from "**Normal**" to "**Alarm**", as shown below.



Note that the Alarm Indication Signal field is not changed directly by this operation. However, in some cases, the Alarm Indication Signal field does change, because the AIS signal also does a loopback, and the loopback AIS signal is detected again by the FPGA.

5. Click the **Stop** button. The **Loopback Status** field displays "**No Loopback**" again.
6. Click the **Loopback Management** section's **Save** button.
7. Click the **Refresh** button.
8. Verify the configuration.
9. Click the Port 1 **MAIN** tab's **Save** button when done.
10. Select **Port 2** and repeat steps 2-9 above.

TDM Mode Configuration

The x6010 is shipped from the factory in T1 mode. Use the procedure below to configure E1 mode.

You can configure E1 mode via either the CLI or the Web interface.

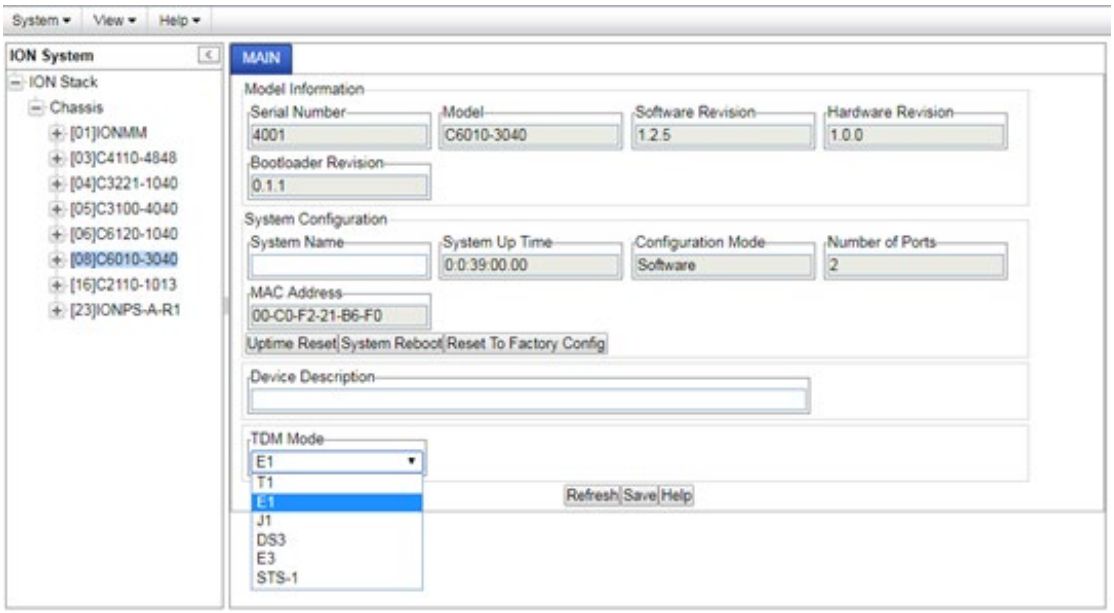
Configuring TDM Mode – CLI Method

1. Set DIP Switch SW4 switch #4 to the Down position. See "DIP Switches".
2. Install the x6010 as described in "Section 2: Installation and System Setup".
3. Access the x6010 through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
4. At the x6010 CLI command prompt, use the **go** command to switch to Port 1.
   Type **go c**=1 **s**=*x* **l1p**=1 and press **Enter** (where x is the x6010 slot location in the ION chassis).
5. If required, enter a Circuit ID of up to 64 characters using the **set circuit-ID** command.
6. Configure the Loopback Management section as required using the **set tdm loopback oper** and the **set tdm loopback oper type** commands.
7. Configure TAOS Transmit. Type **set taos transmit**={disable|enable} and press **Enter**.
8. Verify the E1 mode configuration. For example:

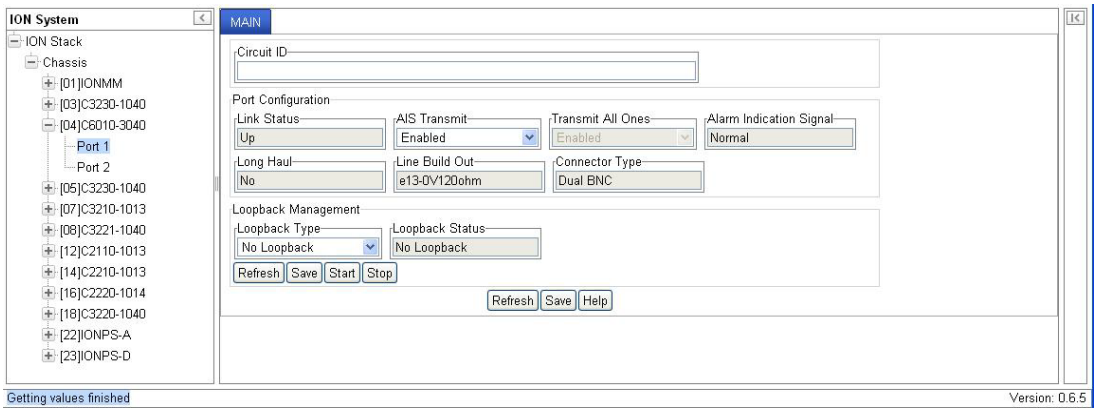
```
C1|S4|L1D>show tdm config
tdm type:                                          e1
C1|S4|L1D>go l1p=1
C1|S4|L1P1>set tdm loopback type phylayer
C1|S4|L1P1>show tdm ?
  config
  loopback
  port
C1|S4|L1P1>show tdm port config
link oper status:                                  up
alarm indication signal:                           normal
taos transmit:                                     enabled
lbo status:                                        e13-0V120ohm
longhaul:                                          no
connector:                                         Dual BNC
C1|S4|L1P1>
C1|S4|L1D>go l1p=2
C1|S4|L1P2>show tdm port config
link oper status:                                  down
alarm indication signal:                           normal
taos transmit:                                     enabled
connector:                                         SFP Slot
C1|S4|L1P2>
```

Configuring TDM Mode – Web Method

1. Set DIP Switch SW4 switch #4 to the Down position for E1 mode. See "DIP Switches".
2. Go to the x6010 **MAIN** tab and locate the **TDM Mode** field.

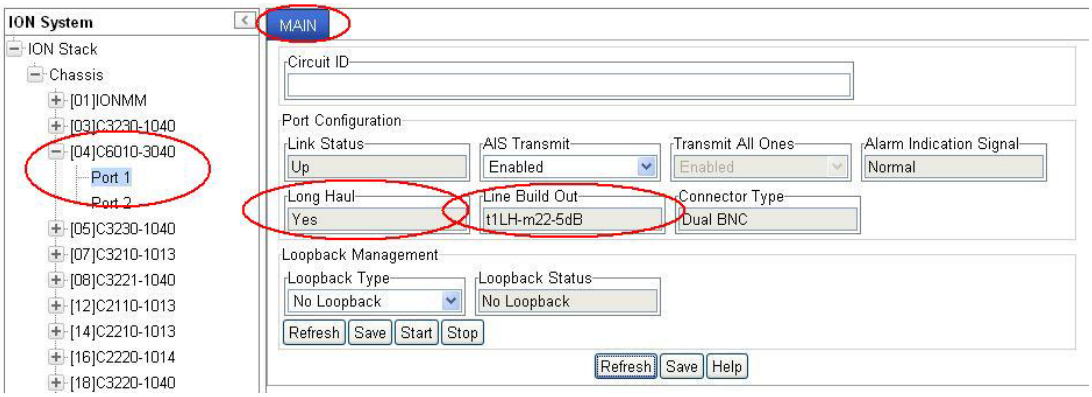


3. At the **TDM Mode** dropdown, select the desired TDM mode. This is the current operating mode of the x6010, either **T1** or **E1**. The operating characteristics include T1=1.544 MHz; E1=2.048 MHz; E3=34.4Mbps; DS3=44.7Mbps; STS-1=51.8Mbps.
4. If desired, enter a new **System Name**.
5. If required, enter a **Device Description** of up to 64 characters.
6. Click the **Save** button.
7. Select **Port 1**.



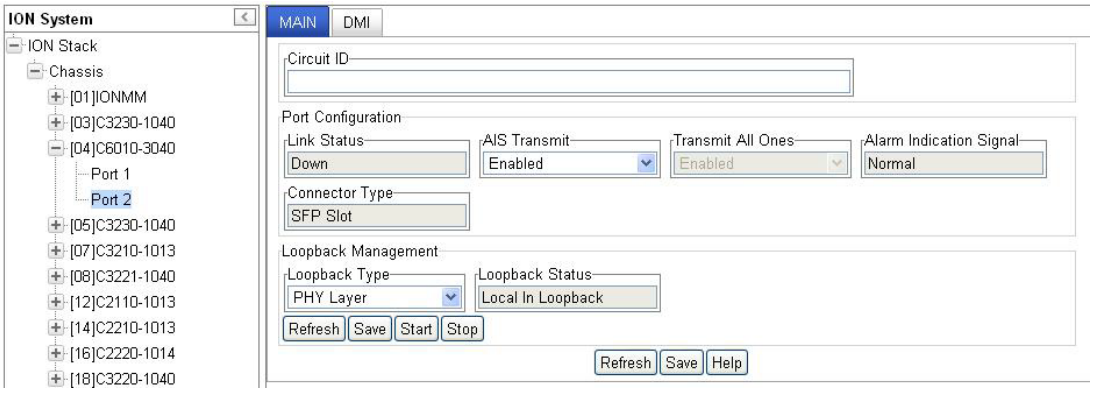
8. If required, enter a **Circuit ID** of up to 64 characters.
9. Configure the **Loopback Management** section as required.

10. Note the **Long Haul**, **Line Build Out** and **Connector Type** field settings. Change the DIP switch settings as required for your particular site configuration.



11. Click the **Save** button at the bottom of the screen when done.

12. Select **Port 2**.



13. If required, enter a **Circuit ID** of up to 64 characters.

14. In the **AIS Transmit** section select **Enabled** or **Disabled**.

15. Note the **Alarm Indication Signal** field setting.

16. Click the **Save** button at the bottom of the screen when done.

17. Verify the x6010 **Port 1** (copper port) configuration settings:

    Circuit ID – either blank or the information entered earlier displays (read/write field).

    Link Status – either **Down** or **Up** displayed (read only field).

    AIS Transmit – Select **Enabled** or **Disabled** as required (read/write field).

    Transmit All Ones – Displays the port's TAOS status **Enabled** or **Disabled** (read only field).

    Alarm Indication Signal – When "***Alarm***" displays, the other end has TAOS enabled and is currently transmitting an alarm condition. When "***Normal***" displays, there is no alarm (read only field).

    Long Haul – Indicates the current position of the remote device's Short/Long haul configuration switch (read only field, e.g., **Yes** or **No**).

TDM Mode – Indicates the type of the current device. **T1=1.544MHz**; T**1=2.048MHz**; **E3=34.4Mb/s**; **DS3 = 44.7Mbps**; **STS-1 = 51.8Mbps**.

Line Build Out – The characteristics of the T1/E1 card's copper interface (read only field, e.g., **e13-0V120ohm**).

Connector Type – **Dual BNC**, **SFP Slot**, etc. (model dependent – read only field).

Loopback Type – either "**No Loopback**" or "**PHY layer**" loopback displayed.

Loopback Status – either "**Local In Loopback**" or "**No Loopback**" displayed.

18. Verify the x6010 **Port 2** (fiber port) configuration settings:

    Circuit ID – either blank or the information entered earlier displays.

    Link Status – either **Down** or **Up** displayed (read only field).

    AIS Transmit – Select **All One**s or **Blue** on the Port 2 fiber interface as an error signal when the Port 2 fiber interface is down. When this error signal is transmitted, the AIS of the device on the other end is activated, if supported (read/write field).

    Transmit All Ones – displays the Transmit All Ones status – either **Enabled** or **Disabled** (read only field).

    Alarm Indication Signal – Either "**Alarm**" or "**Normal**". When "***Alarm***" displays, this means that the other end has TAOS enabled and is currently transmitting an alarm condition. When "***Normal***" displays, this means no alarm (read only field).

    Connector Type –SFP Slot, Dual BNC, etc. – model dependent (read only field).

    Loopback Type – either "**No Loopback**" or "**PHY Layer**" loopback displayed (read/write field).

    Loopback Status – either "**Local In Loopback**" or "**No Loopback**" displayed.

19. At the DMI tab (if supported and configured) set the **Rx Power Intrusion Threshold** (0-65535 µW). The default is 0 uW (microwatts).

20. Click the **Refresh** button and verify the DMI status. See "DMI (Diagnostic Maintenance Interface) Test" for more information.

5 Operation

General

This section describes x6010 non-configuration operations (e.g., Backup, Restore, Reset, Upgrade, Reboot, Replace, etc.).

Backup and Restore Operations (Provisioning)

Through the Web interface you can back up and restore the configuration information for the IONMM and any or all of the NIDs in the ION system.

A Backup is used to get the SIC card running configuration, convert it to CLI commands, and save those CLI commands into the backup file. The backup file is stored in the IONMM. **Note**: Lantronix recommends as a "best practice" to back up each SIC card's configuration after it is fully configured, so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored.

A Restore is used to send the CLI commands in the configuration file to a SIC after removing the current SIC running configuration. If a problem causes the SIC card configuration restoration to stop (e.g., due to a lost network connection between the PC host and Agent card) the SIC card will use the previous configuration to run the traffic. If the IONMM card is downloading the restore configuration data to the SIC card, and the SIC card is physically removed from the chassis, the SIC card will use the factory default configuration setting when it is re-inserted into the chassis.

Lantronix recommends that you to enter a "**show card info**" CLI command to view the NID's current configuration before a backup/restore operation to verify the desired configuration settings. There are several CLI **show** commands that allow you to display (show) information about a SIC card's configuration. For a complete description of these and other CLI commands see "Section 6: Command Line Interface (CLI) Reference".

Note: Disable the DHCP client for each device that you backup/restore.

IMPORTANT

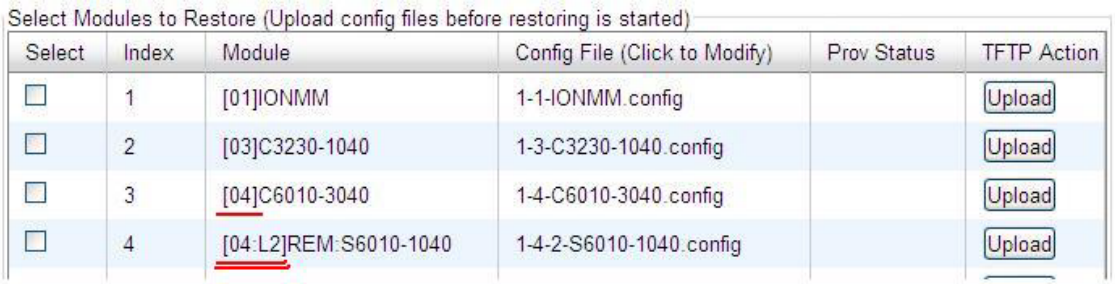
Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory removes temporary files (e.g. configuration backup files, Syslog file). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key).

For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- Table 17. Back Up and Restore File Content and Location
- Table 18. File Status after a Reset to Factory Defaults
- Table 19. File Content and Location after a System Reboot
- Table 20. File Content and Location after a Firmware Upgrade

Note on Remote (L2D) Module Backup, Restore, and Upgrade

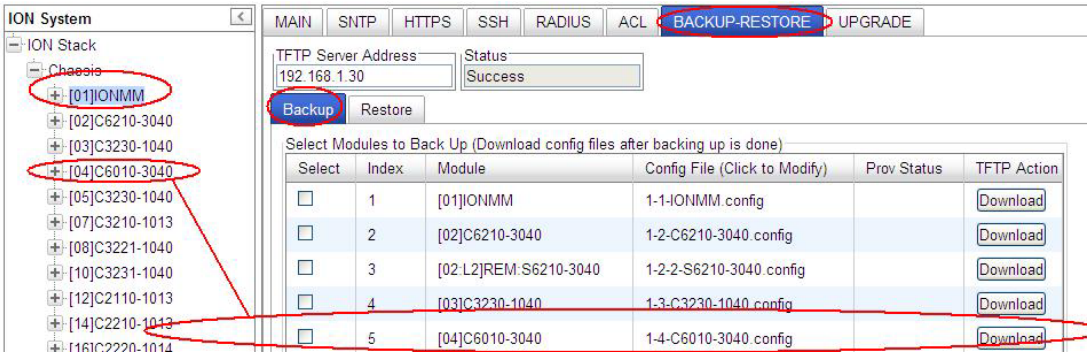
When doing a remote (L2) module backup, restore, or upgrade, the related table displays two Module numbers for the same slot. The first module is the chassis (local) device (e.g., **[04]C6010-3040** shown below). The second module listed is the standalone (remote) device (e.g., **[04:L2]REM:S6010-1040** shown below).



Backing Up Slide-In and Remote Module Configuration

The following procedure describes how to back up the configuration of one or more slide-in or remote modules in the ION system. The backup file is stored in x6010 memory.

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **BACKUP-RESTORE** tab. Select the **Backup** sub-tab if not already displayed.



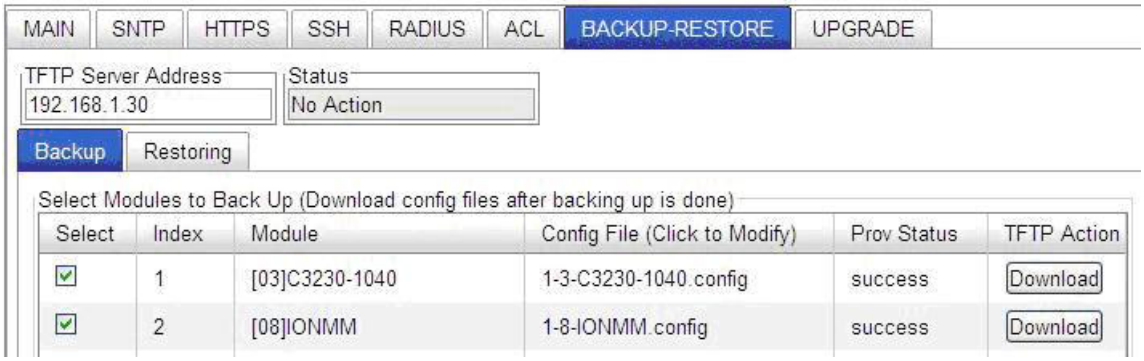
3. Verify that the TFTP Server address shown is correct, that the TFTP Server is running and configured, and that the file to be downloaded is located correctly (e.g., at *C:\TFTP-Root*).
4. Verify that the card list shown in the table is correct; if not correct, fold and then unfold the "ION Stack" node in the left tree view to refresh.
5. Note the **Prov Status** field message (*Wrong Firmware*, *No Action*, etc.).
6. In the **Select** column, check the checkbox of each module to be backed up.

7. Do you want to rename the backup file?

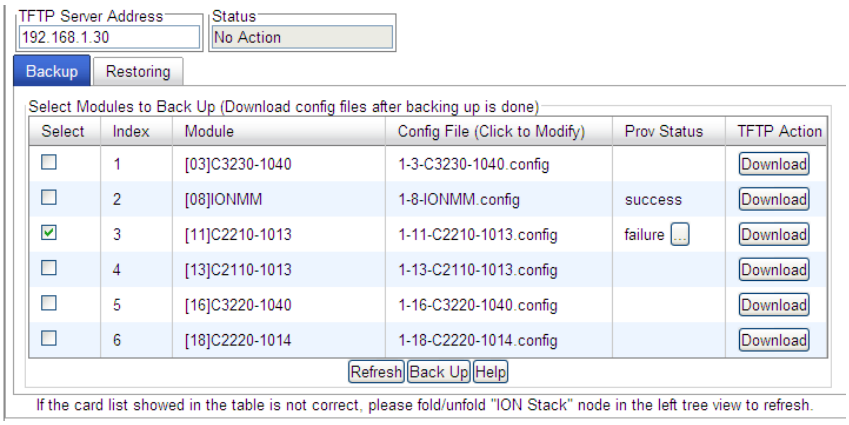
Yes	No
a) In the **Config File** column, click the file name. b) Type a new name for the backup file. **Note:** the file name must be 1–63 characters long and must end with **.config**. c) Continue with step 8 below.	Continue with step 8 below.

8. Click the **Download** button. When completed, the message "*File has successfully transferred via TFTP*" displays.
9. Click the **OK** button to clear the web page message.
10. Click the **Back Up** button. The message "*Backup is being processed ...*" displays. The Back Up operation can take several minutes.
11. At the confirmation message, click **OK**. The message "*Backup is being processed ...*" displays. The Back Up operation can take several minutes.
12. When the confirmation window displays, click **OK**. The backup file is saved in the IONMM.

    The **Prov Status** column displays the provision operation result (*ongoing*, *success*, or *fail*).



13. If the Back Up operation fails, go to step 15 below.
14. To send a copy of the backup file to the TFTP Server:
    a. Make sure the TFTP Server is running and configured.
    b. In the **TFTP Server Address** field, enter the IP address of the server.
    c. Click the **Download** button. The message "*File is being transferred*" displays.
    d. When the successful completion message displays, click **OK**. The TFTP Server now contains an emergency backup file for the module specified.
15. If the **Backup** operation fails, the **Prov Status** column displays failure . Click the box to download an error log from the device.



The error (.ERR) log file is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as *1-11-C6010-1040.config*. You can open the file in WordPad. See "The Config Error Log (config.err) File" section for error messages and possible recovery procedures.

When the Back Up is successfully completed, you can edit the Config file (optional) or continue with the applicable Restore procedure. See:

- Editing the Config File (Optional)
- Restoring Slide-In and Remote Modules
- Restoring Standalone Modules

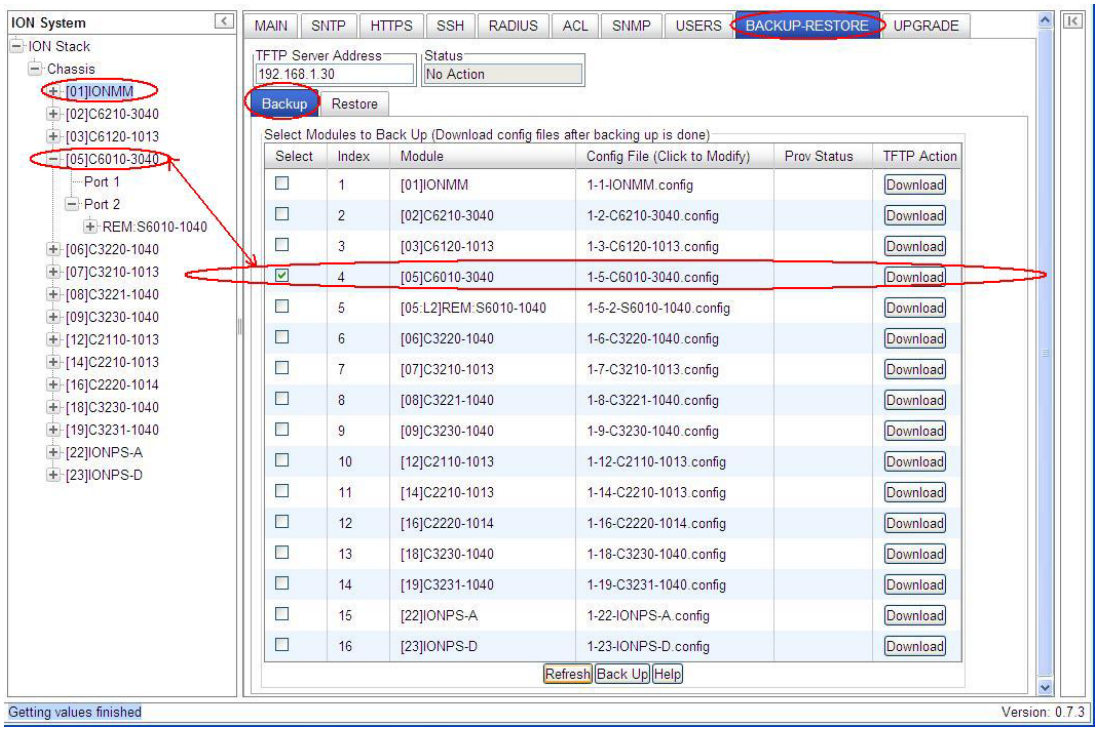
Backing Up Standalone Modules

The following procedure describes how to back up the configuration of a standalone module.

IMPORTANT

Doing a reboot, restart, an upgrade or a reset to factory settings may cause some configuration backup files, HTTPS certification file, and Syslog file to be lost. Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory removes temporary files (e.g. configuration backup files, Syslog file). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key).

1. Access the IONMM module through the Web interface (see "Starting the Web Interface").
2. Select the **BACKUP-RESTORE** tab.



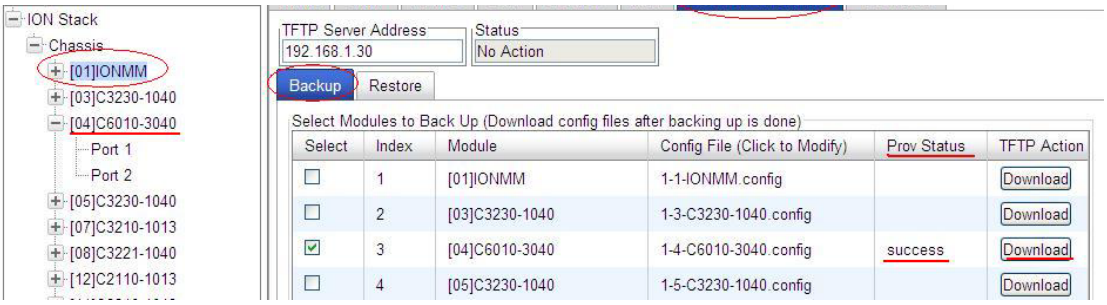
3. In the **Select** column, check the checkbox of the module to be backed up (C6010-3040 in slot 05 – Index #4 in the screen above). The attached standalone is REM S6010-1040 in slot 05 – Index #5

4. Do you want to rename the backup file?

Yes	No
a) In the **Config File** column, click the file name. b) Type a new name for the backup file. **Note:** the file name must be from 1–63 characters in length and must end with **.config**. c) Continue with step 5.	Continue with step 5.

5. Click the **Back Up** button.
6. When the confirmation window displays, click **OK**.

   The backup file is saved in the IONMM module.
7. Click the **Download** button. When completed, the message "*File has successfully transferred via TFTP*" displays, and the Prov Status column displays "success".



8. Click the **OK** button to clear the web page message.
9. To send a copy of the backup file to the TFTP server:
   a. Make sure the TFTP Server is running and configured.
   b. In the **TFTP Server Address** field, enter the IP address of the TFTP server.
   c. Click the **Download** button.
   d. When the successful completion message displays, click **OK**.

When the Back Up is successfully completed, you can edit the Config file (optional) or continue with the applicable Restore procedure:

- Editing the Config File (Optional)
- Restoring Slide-In and Remote Modules
- Restoring Standalone Modules

Editing the Config File (Optional)

In some circumstances you may need to edit the backup Config file before restoring it. For example, you may want to globally change the FDB IDs or other addressing.

The procedure below provides steps typically used in editing a Config file.

1. Complete the applicable Backup procedure from the previous section.
2. Open the Config file (in Notepad, WordPad, Word, OpenOffice Writer, etc.) from the TFTP server location (e.g., C:*TFTP-Root**1-9-C6010-1040.config*).
3. Edit the Config file sections. Each Config file contains a DEVICE LEVEL CONFIG section and two PORT x CONFIG sections.
4. Save the edited Config file back to the TFTP server location (e.g., C:*TFTP-Root**1-9- C6010-1040.config*).
5. Continue with the applicable Restore procedure from the following section using the edited Config file.

A sample portion of a typical Config file is shown below.

```
[DEVICE LEVEL CONFIG]
set system name=”C6010-1040”
set circuit-ID=””
[PORT 1 CONFIG]
set taos transmit=enable
set circuit-ID=””
[PORT 2 CONFIG]
set taos transmit=enable
set circuit-ID=””
```

Restoring Slide-In and Remote Modules' Configuration

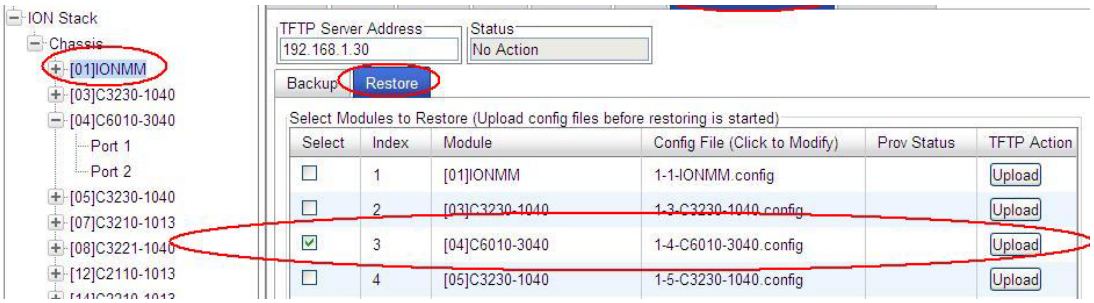
The following procedure describes how to restore the configuration of one or more slide-in or remote modules in the ION system.

Note: these Restore procedures require that the TFTP server be running and properly configured, and that the backup configuration file is named and located properly.

IMPORTANT

A restore operation can only be performed for a module that had its configuration file backed up (see Backing Up Standalone Modules).

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. At the **BACKUP-RESTORE** tab, select the **Restore** sub-tab. The "Modules to Restore" table displays.



3. If the card list shown in the table is not correct, unfold the ION Stack in the left tree view, and then refold it to refresh the table information.
4. In the **Select** column, check the checkbox of each module to be restored.
5. Is the configuration file to be restored different than the one shown in the Config File column?

Yes	**No**
a) In the **Config File** column, click the file name. b) Type the name of the backup file to be restored. **Note:** the file name must end with **.config**. c) Continue with step 6.	Continue with step 6.

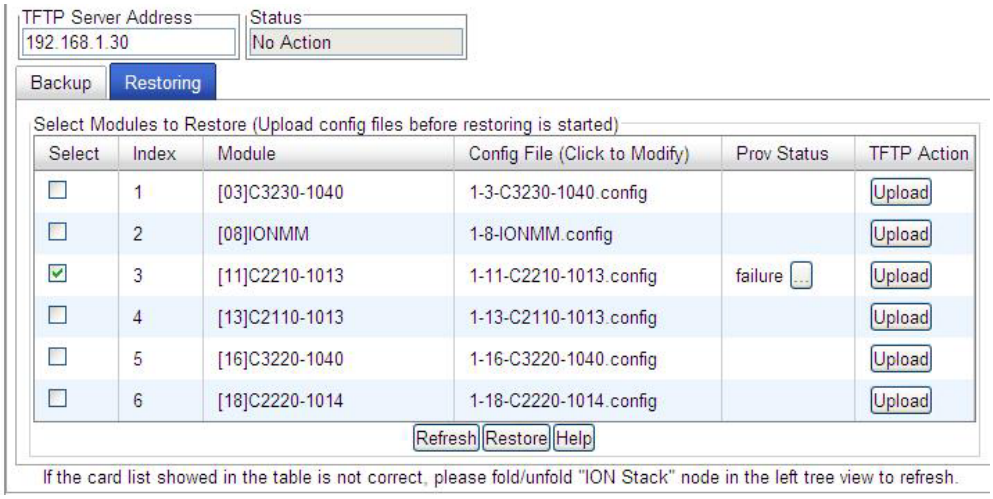
6. Does the configuration file need to be retrieved from the TFTP server?

Yes	No
a) In the **TFTP Server Address** field, enter the IP address of the server. b) Click **Upload**. c) When the successful transfer message displays, click **OK**. d) Continue with step 7.	Continue with step 7.

7. Click the **Upload** button. The config file is uploaded via the TFTP server. When done, the message "*File has been successfully transferred via TFTP.*"
8. Click the **OK** button to clear the Webpage message.
9. Click the **Restore** button.
10. When the confirmation window displays, click **OK**.

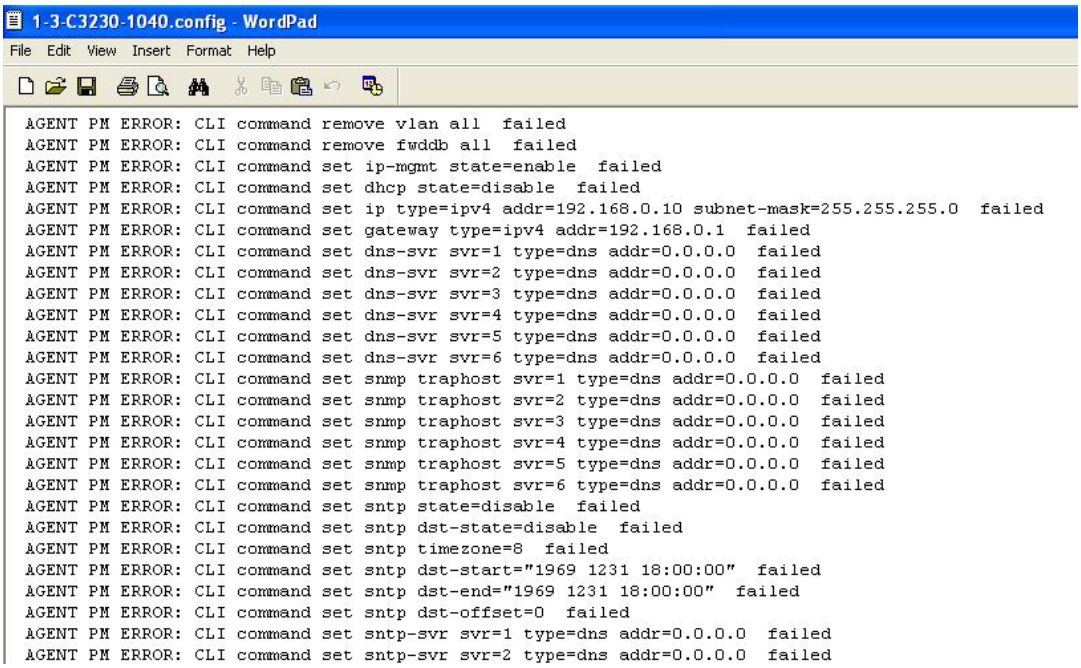
    The configuration will be restored from the specified file. During the Restore operation the message "*Restoring is being processed ...*" displays, and the **Prov Status** column displays "ongoing".
    When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.

11. If the **Restore** operation fails, the **Prov Status** column displays failure ... Click the box to download an error log from the device.



The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad or a text editor.

A sample portion of an error log file (.ERR file) is shown below.



See "The Config Error Log (config.err) File" section for error messages and possible recovery procedures.

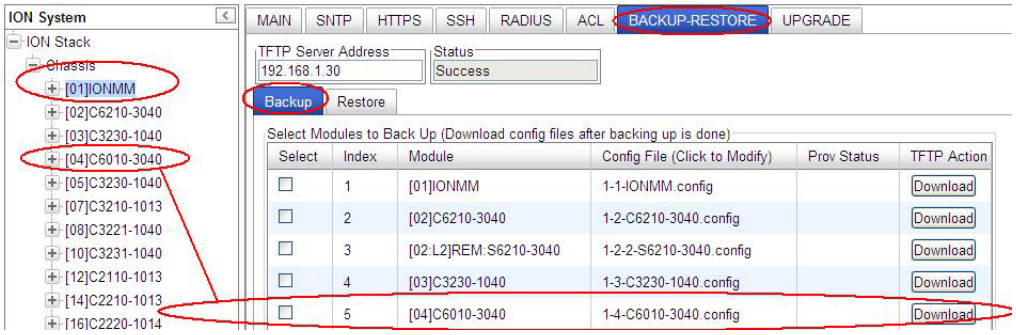
Restoring Standalone Modules

The following procedure describes how to restore the configuration of a standalone module.

IMPORTANT

A restore operation can only be performed for a module that had its configuration file backed up (see Backing Up Standalone Modules).

1. Access the IONMM module through the Web interface (see "Starting the Web Interface").
2. Select the **BACKUP-RESTORE** tab.
3. Select the **Restore** sub-tab. The "Modules to Restore" table displays.



4. In the **Select** column, check the checkbox of the module to be restored.
5. Is the configuration file to be restored different than the one shown in the **Config File** column?

Yes	**No**
a) In the **Config File** column, click the file name. b) Type the name of the backup file to be restored. **Note:** the file name must end with **.config**. c) Continue with step 5.	Continue with step 6.

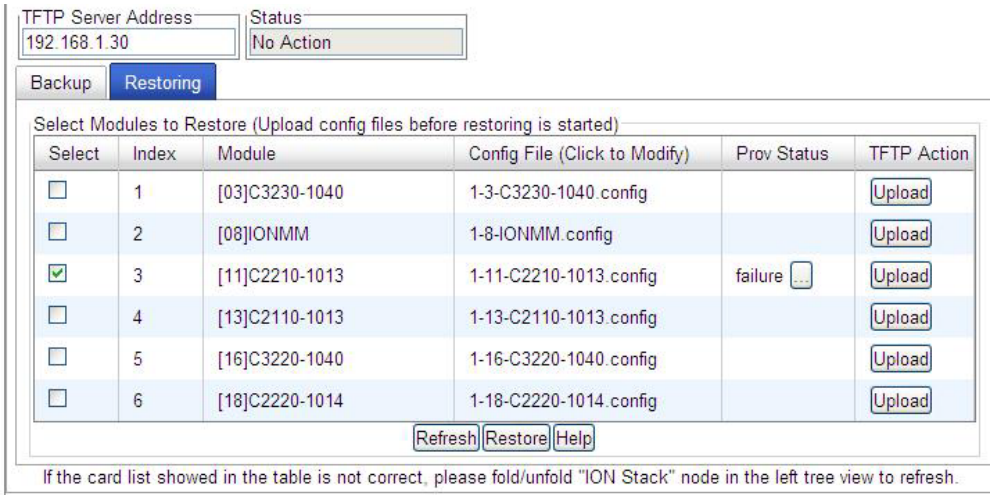
6. Does the configuration file need to be retrieved from the TFTP server?

Yes	No
a) In the **TFTP Server Address** field, enter the IP address of the server. b) Click **Upload**. c) When the successful transfer message displays, click **OK**. d) Continue with step 6.	Continue with step 7.

7. Click the **Upload** button. The config file is uploaded via the TFTP server. When done, the message "*File has been successfully transferred via TFTP.*"
8. Click the **OK** button to clear the Webpage message.
9. Click the **Restore** button.
10. When the confirmation window displays, click **OK**.

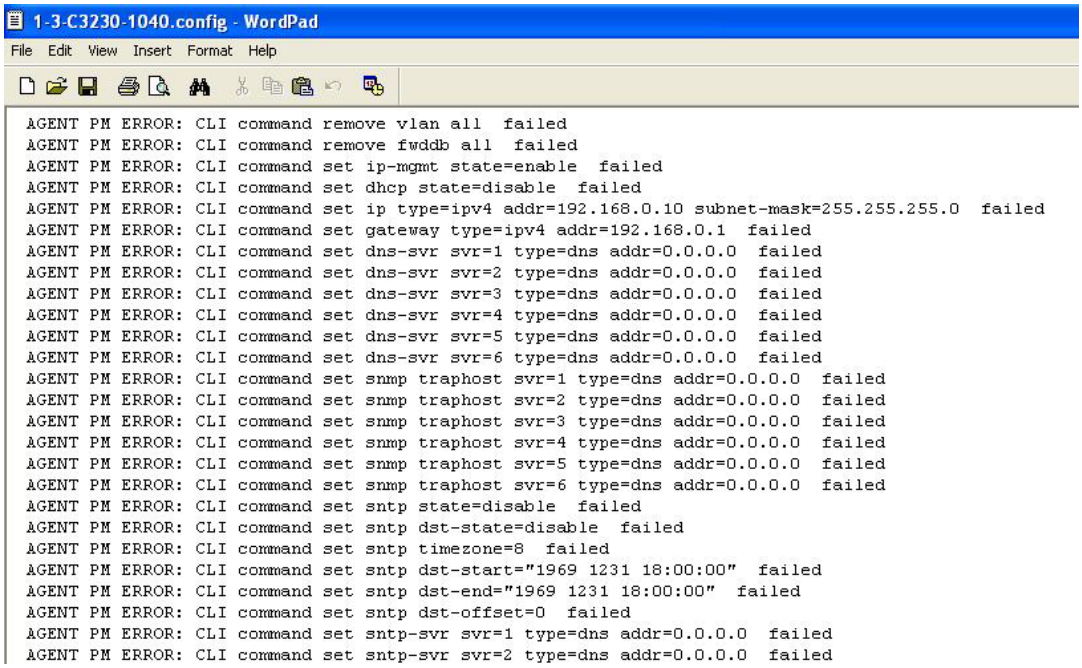
    The configuration will be restored from the specified file. During the Restore operation the message "*Restoring is being processed ...*" displays, and the **Prov Status** column displays "ongoing".
    When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.

11. If the **Restore** operation fails, the **Prov Status** column displays failure [...]. Click the box to download an error log from the device.



The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad or a text editor.

A sample portion of an error log file (.ERR file) is shown below.



See “The Config Error Log (config.err) File” for message descriptions.

Back Up and Restore File Content and Location

The IONMM card stores all configuration backup files, HTTPS certification file, and Syslog file.

Note: Doing a reboot, restart, an upgrade or a reset to factory settings may cause some configuration backup files, HTTPS certification file, and Syslog files to be lost. Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory removes temporary files (e.g. configuration backup files, Syslog file). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key).

The back Up operation backs up all of the SNMP settings (the same as what can be set via the Web interface / CLI) for one SIC into a file containing a list of CLI commands. This file can be downloaded from IONMM. When restoring for one SIC, you can upload a provisioning backup file (this file must have been made via the Backup operation and must be for the same SIC type) to the IONMM and do a Restore. See the IONMM Backup-Restore (**provisioning)** tab description. Currently, the Backup content includes configuration files, HTTPS certification file, the Syslog file, and certain other files, as outlined in the table below.

Table 8: Back Up and Restore File Content and Location

File Type	Filename	File Description	Stored Directory	Backed up? (Y/N)	Changed after Restore? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes – these files are created during Backup operation	No
MIB configuration files	e.g., 'agent3.conf ' 'ifMib.conf '	The MIB configuration files for SNMP setting	/agent3/conf	No – not needed; the configurations included in this file will be backed up by SNMP set operations	Yes

IONMM Backup All / Restore All

IONMM v 1.4.0 adds Backup All and Restore All capabilities. The new Backup All and Restore All features can be configured via the ION System Web GUI or CLI commands. The Backup/Restore feature provides Automatic TFTP transfer, Backup and restore of up to 41 modules at one time, Time-stamped filenames that include the stackname and index number, and Time-stamped tarfile containing all the config files. See the IONMM User Guide for details.

Displaying Information

There are several CLI commands that allow you to display (show) information about the NID configuration. For a complete description of these and other CLI commands see "Section 6: Command Line Interface (CLI) Reference".

Reset to Factory Defaults

If need be, you can reset all configurations in the IONMM back to their original factory defaults. This operation can be accomplished through either the CLI or Web method.

IMPORTANT

This operation deletes **all** configuration information that was saved in the IONMM.

Resetting Defaults – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" 1) or a Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **reset factory**
3. Press **Enter**. The following displays:

```
Warning: this command will restart the specified card, connection will be lost!
C1|S18|L1D>
```

   All configuration parameters will be reset to their factory values. For a list of all factory defaults, see "Appendix B: Factory Defaults").

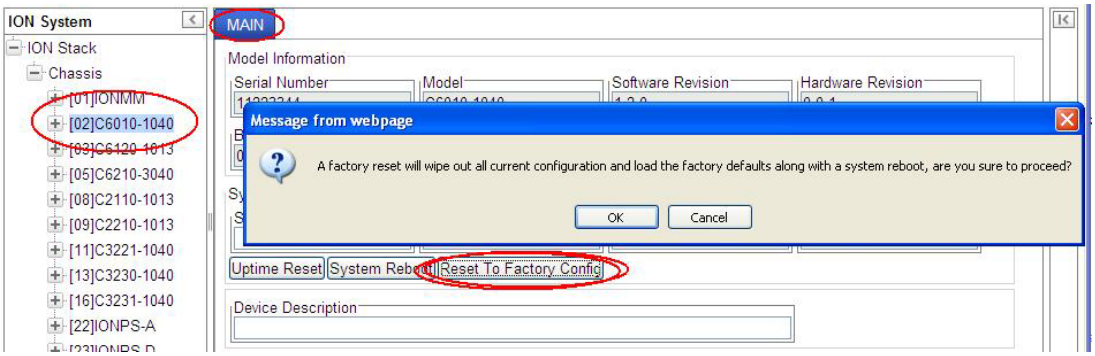
   Note: Your USB and/or Telnet session will be disconnected.

4. Set the IP configuration (see "Doing the Initial System Setup").

Resetting Defaults – Web Method

Caution: This operation deletes all configuration information that was saved in the x6010, including the IP address you assigned to the x6010.

1. Access the NID through the Web interface (see "Starting the Web Interface").
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.
4. Click the **Reset to Factory Config** button. The message "*A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*" displays.



5. Click **Cancel** if you are sure you want to proceed with the Reboot. Click **OK** only if you wish to reboot.

   All configuration parameters will be reset to their factory values. For a list of all factory defaults, see "Appendix B: Factory Defaults").

   Note: Your Web session will be discontinued.

File Status after Reset to Factory Defaults

The table below shows the status of various system files after a reset to factory defaults.

Table 9: File Status after a Reset to Factory Defaults

File Type	Filename	File Description	Stored Directory	Status after Reset to Factory Default
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Lost
MIB 87config-uration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	Restored to factory configuration (lost)

Resetting Uptime

The device uptime field displays the amount of time that the ION system device has been in operation.

The System Up Time is displayed in the format days:hours:minutes:seconds.milliseconds. For example, a **System Up Time** field display of **9:8:15:18.26** indicates the ION system has been running for 9 days, 8 hours, 15 minutes, 18 seconds, and 26 milliseconds.

The ION **System Up Time** counter can be reset via the CLI or Web method.

Reset Uptime – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **reset uptime** and press **Enter**.

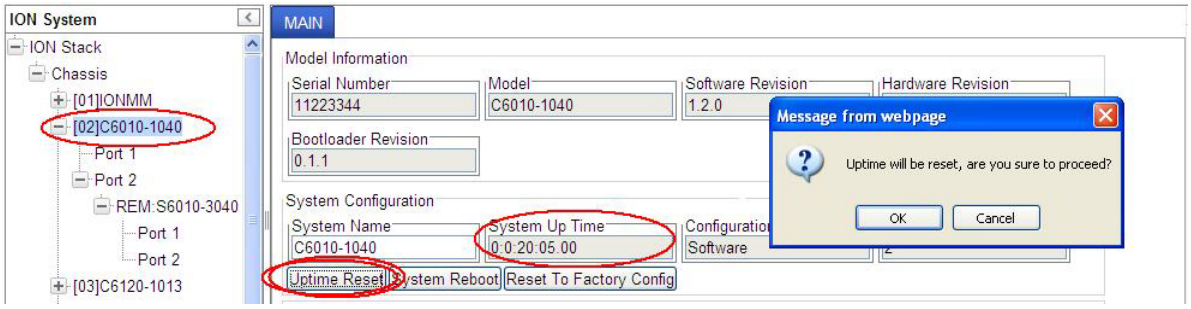
   The System Up Time field resets to zero, and immediately begins to increment. For example:

```
C1|S4|L1D>reset uptime
C1|S4|L1D>
```

Use the **show card info** command to display the current device uptime.
Note: The **reset uptime** command is not available for all ION system devices.

Reset Uptime – Web Method

1. Access the x6010 through the Web interface (see "Starting the Web Interface").
2. At the **MAIN** tab, locate the **System Configuration** section.



3. If desired, observe and record the **System Up Time** field count.
4. Click the **Uptime Reset** button. The message "*Uptime reset, are you sure*" window displays.
5. Click **OK** to reset the system up time. The message "*Setting values succeeded*" displays at the bottom left of the screen when the Uptime reset is done.
6. Click the **Refresh** button at the bottom of the screen. The **System Up Time** field resets to zero, and immediately begins to increment.

Note: The System Up Time cannot be reset on a Remote S6210 (level 2 device) via the Web interface. If you Reset uptime on the connected (local) chassis device, the remote device's uptime counters are not reset.

Reboot

At times you may have to reboot (restart) the ION system. This operation can be accomplished by either the CLI or Web method.

Note: this operation can take several minutes. The amount of time for the reboot to complete depends on the ION system configuration. When the reboot is finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The 'red box' condition occurs while the devices are resetting; this condition can continue several minutes after the reboot.

See Table 19 in this section for file content and location after a System Reboot.

IMPORTANT

Doing a system reboot, restart, upgrade, or a reset to factory settings may cause some configuration backup files, HTTPS certification file, and Syslog file to be deleted.

Rebooting – CLI Method

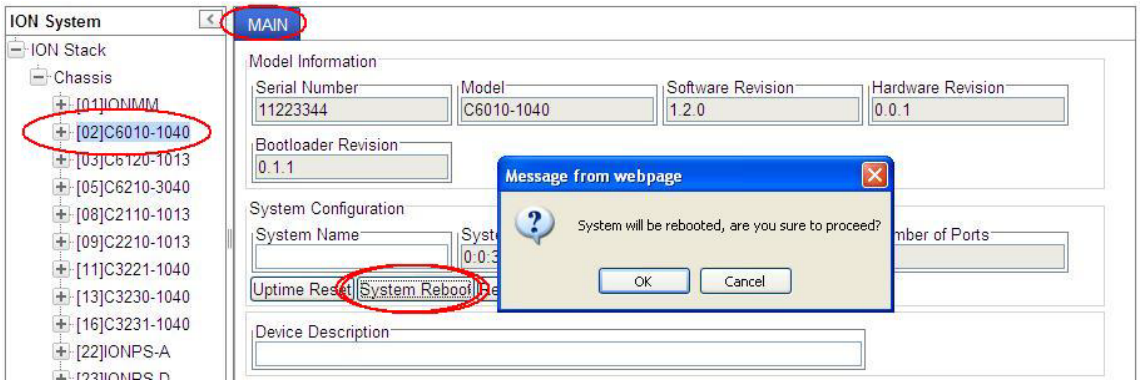
1. Access the NID through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login again!* The ION system device reboots. If this operation is performed on a standalone module, the connection / session is terminated.
3. To reestablish the connection / session, wait about one minute, and then:
   - For a USB connection
     a) Select **Call > Disconnect**.
     b) Select **File > Exit**.
     c) Disconnect then reconnect one end of the USB cable.
     d) Start a USB session (see "Starting a USB Session").
   - For a Telnet session
     a) Press **Enter**.
     b) Start a Telnet session (see "Starting a Telnet Session").

Rebooting – Web Method

Caution: Doing a system reboot may cause some configuration backup files, HTTPS certification file, and Syslog file to be lost.

Note: If you have a USB or Telnet session established, terminate the session before doing the reboot.

1. Access the x6010 through the Web interface (see "Starting the Web Interface").
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.
4. Click the **System Reboot** button. The confirmation message "*System will be rebooted, are you sure to proceed?*" displays.



5. At the confirmation window, click the **OK** button to start the reboot, or click **Cancel** to quit the reboot.

   The x6010 will restart and will be available for operations after about one minute.

Reboot File Content and Location

The table below shows file content and location resulting from a system re-boot.

Table 10: File Content and Location after a System Reboot

File Type	Filename	File Description	Stored Directory	Lost after Reboot? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Re-store	/tftpboot	Yes
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

Upgrade the IONMM and/or NID Firmware

Occasionally changes must be made to the firmware version that is currently stored in IONMM or NID memory. This could occur because of features, fixes or enhancements being added.

Note: Lantronix recommends that before completing any steps on an install that you verify that the IONMM and NIDs have the latest firmware version installed and running.

Ideally, all the cards in a chassis will be upgraded to the latest versions at the same time; running devices with a mix of old and new firmware can cause a "red box" condition. See "Section 6: Troubleshooting".
Note: You cannot upgrade a module with multiple BIN files.

Upgrading modules via the IONMM will cause all configuration backup files to be lost.

You can upgrade the IONMM and/or NID Firmware from the Command Line Interface (CLI) or via the Web interface.

Upgrading IONMM and/or NID Firmware – CLI Method

Perform this procedure to upgrade the IONMM Firmware from the CLI.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. Display the current version of the IONMM firmware. Type **show card info** and press **Enter**.
3. Determine the current TFTP server address using the **prov** command and press **Enter**.
   For example:

   prov get tftp svr addr
   prov set tftp svr type=(ipv4|dns) addr=ADDR
4. Go to the Lantronix Software Upgrades web page.
5. Locate the "**Agent Firmware**" section and click the link in the right hand column (e.g., "**Download IONMM.bin.1.0.5.bin**" or "**Download C6010_0.6.7_AP.bin"** and "**Download C6010_0.6.7_FPGA_AP.bin**").
6. Zip the downloaded file.
7. Retrieve the firmware database file using the **tftp get** command to get the file from the TFTP Server, and then press **Enter**. For example:

   tftp get iptype=(ipv4 |dns) **ipaddr**=ADDR **remotefile**=RFILE [**localfile**=LFILE]
   tftp put iptype=(ipv4|dns) **ipaddr**=ADDR **localfile**=LFILE [**remotefile**=RFILE]
8. Unzip the file. Type **update firmware-db file=FILENAME** and press **Enter**.
9. Verify the Update results. Type **show firmware-db update result** and press **Enter**.
10. Upgrade the module. Type **upgrade module** and press **Enter**.

11. A table of available modules displays with upgrade instructions.

```
C1|S7|L1D>upgrade module
Available modules:

index     module                                    loc
1         ION219                                    c=1 s=0 l1d
2         C3230-1040                                c=1 s=3 l1d
3         C3230-1040                                c=1 s=5 l1d
4         S3230-1040                                c=1 s=5 l1ap=2 l2d
5         IONMM                                     c=1 s=7 l1d
6         C3231-1040                                c=1 s=10 l1d
7         C2110-1013                                c=1 s=12 l1d
8         C2210-1013                                c=1 s=13 l1d
9         C2220-1014                                c=1 s=16 l1d
10        C3220-1040                                c=1 s=18 l1d
11        IONPS-A                                   c=1 s=22 l1d

Choose the module you want to upgrade: (eg. 1,3,16; at most 8 modules to
   upgrade, press 'q' to exit upgrade)
1,2,3,4,5,6,10,11

It may take some time to finish the task, you can continue with other works,
   then use "show firmware upgrade result" to check result.
```

12. Choose the module(s) to upgrade (**# 1-6,10,11** in the example above) and press **Enter**.

13. Verify the Upgrade results. Type **show firmware upgrade result** and press **Enter**.
The firmware upgrade results are displayed in a table. If the firmware upgrade was successful, the *time started* and *time completed* display.

```
C1|S7|L1D>show firmware upgrade result
index     module                          status      reason    time started     time completed
1         card registering...             success               00:21:23          00:21:32
2         C3230-1040 c=1 s=3 l1d          inProgress            00:21:23          00:00:00
3         C3230-1040 c=1 s=5 l1d          inProgress            00:21:24          00:00:00
4         S3230-1040 c=1 s=5 l1ap=2 l2d   inProgress            00:21:24          00:00:00
5         IONMM c=1 s=7 l1d               success               00:21:24          00:21:47
6         C3231-1040 c=1 s=10 l1d         inProgress            00:21:26          00:00:00
7         C3220-1040 c=1 s=18 l1d         inProgress            00:21:26          00:00:00
8         IONPS-A c=1 s=22 l1d            success               00:21:29          00:21:40
C1|S7|L1D>
```

If a module upgrade was unsuccessful, the reason for the failure displays in the "reason" column of the table (e.g., *invalid input file*, *protocol timeout*). See "Section 5 – Troubleshooting" for error messages and recovery procedures.

Upgrading IONMM and/or NID Firmware – Web Method

The following describes the procedure for upgrading the firmware in the IONMM through the Web Interface. If the IONMM is to be upgraded at the same time as other modules in the ION Chassis, see Upgrading Slide-In and Remote Modules.

Note: Doing an IONMM / NID firmware upgrade may cause configuration backup files to be lost.

The steps involved include **A**. Verify the current IONMM / NID Firmware version, **B**. Locate the current IONMM / NID Firmware version, **C**. Run the TFTP Server, and **D**, either 1. Upgrade IONMM / NID Firmware from the **MAIN** tab, or 2. Upgrade IONMM / NID Firmware from the **UPGRADE** tab.

1) Verify the Current IONMM / NID Firmware Version

Perform this procedure to display the current version of the IONMM firmware via the web interface.

1. Access the IONMM via the Web interface (see "Starting the Web Interface").
2. Select the **MAIN** tab and locate the **Software Revision** area in the **Model Information** section. (You can also use the **Help** dropdown and select **About ION System Web Interface** to determine the current firmware version.)
3. Note the current version of the x6010 NID or IONMM firmware for use in steps D1 and D2 below.

B. Locate and Download the New IONMM / NID Firmware Version

Perform this procedure to locate the IONMM Firmware version via the Web interface.

1. Go to the Lantronix Software Upgrades web page.
2. Locate the "**Agent Firmware**" section and examine the link in the right hand column (e.g., "**Download x6010_1.0.5_AP.bin**").
3. Compare the IONMM / NID version displayed in the **MAIN** tab **Software Revision** area with the version number on the web site, and continue if the web site version is newer than the current (running) version.
4. Click the link located in step 1 above to download the new firmware files (e.g. "C6010_0.6.7_AP.bin" and "C6010_0.6.7_FPGA_AP.bin").

C. Run TFTP Server

This process requires a TFTP Server to load the new firmware. **Note**: A TFTP Server is not the same as an FTP server; they use different protocols. You cannot connect to the TFTP Server with an FTP client.

1. Install, run and configure the TFTP Server.
2. Copy the file downloaded in step 4 above to the required TFTP Server location.
   Note: the upgrade file must be resident in the default directory on the TFTP server (normally *C:TFTP-Root*).
3. Note the location of the downloaded file and its filename for use in steps D1 and D2 below.

D. Upgrade the IONMM / NID Firmware

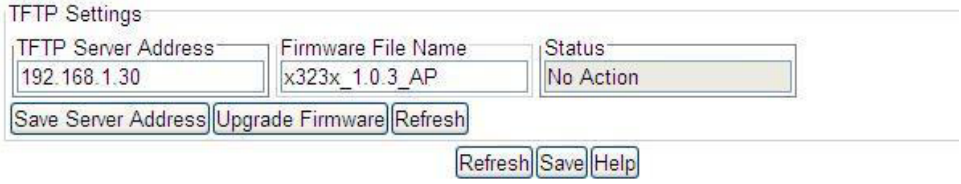
Perform this procedure to upgrade the IONMM / NID Firmware from either

- the IONMM **MAIN** tab (step D1) or
- the **UPGRADE** tab (step D2).

D1. Upgrade IONMM / NID Firmware from the **MAIN** Tab.

1. Access the IONMM card through the Web interface (see "Starting the Web Interface").
2. Select the **MAIN** tab.
3. Locate the **TFTP Settings** section at the bottom of the screen.

4. Enter the **TFTP Server Address.** This is the IP address of the TFTP Server from step C ("Run TFTP Server") above.
5. Enter the **Firmware File Name**. This is the name of the firmware file from step C sub-step 2 above.



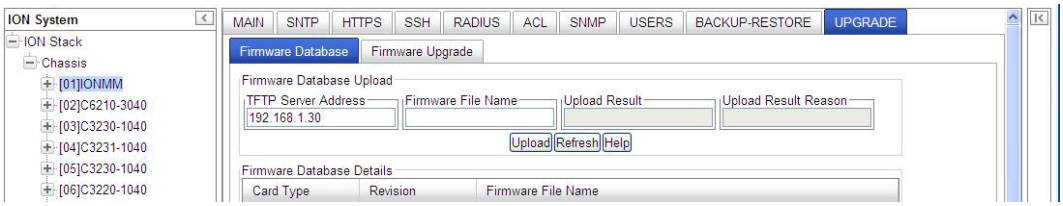
6. Click the **Upgrade Firmware** button.

   The message "*The specified firmware on the TFTP Server will be upgraded to the current module; are you sure to proceed?*" displays.

7. Click **OK**.
   The file is downloaded and the x6010 and/or IONMM reboots. When the reboot is complete, the message "*[xx]IONMM rebooting finished*" displays.
8. Click the **Refresh** button. The **Software Revision** area is updated from the old version number to the new version number (e.g., from 1.0.3 to 1.0.5).
9. If you will be using the same TFTP Server Address for future upgrades, click the **Save Server Address** button.

D2. Upgrade IONMM / NID Firmware from the **UPGRADE** Tab

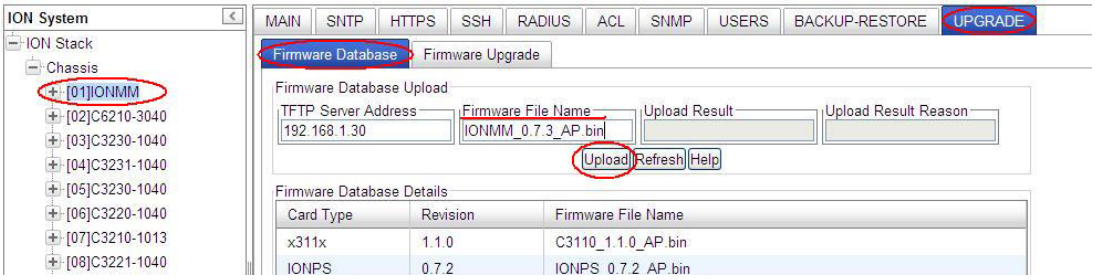
1. Access the IONMM card through the Web interface (see “Starting the Web Interface”).
2. Select the **UPGRADE** tab.
3. Select the **Firmware Database** sub-tab if not already selected.
4. Locate the **Firmware Database Upload** section.



5. Enter the **TFTP Server Address.** This is the IP address of the TFTP Server from step C (“Run TFTP Server”) above.
6. Enter the **Firmware File Name**. This is the name of the firmware file from step C sub-step 5 above.
7. Click the **Upload** button.

   The message “*The Firmware Database File is being transferred.*” Displays during the upload, and the **Upload Result** area displays *In Progress*.

   When successfully completed, the message “*Getting all records finished*” displays, the **Upload Result** area displays “*Success*”, and the **Firmware Database Details** section displays updated firmware information.

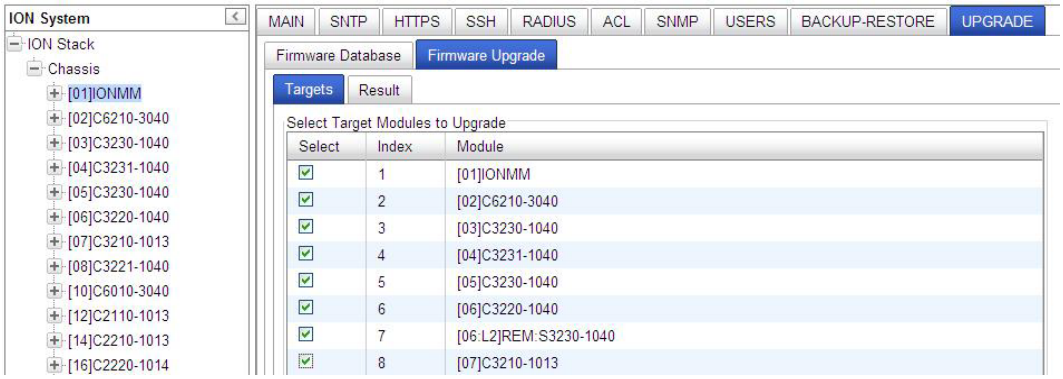


8. If the firmware upload operation failed, the **Upload Result** area displays either:
   - **None**: no operation was performed, or
   - **Failure**: the specified operation has failed.

   The **Upload Result Reason** area displays a description of the cause of the upload ‘Failure’. This area is blank if the **Upload Result** displayed is anything other than ‘Failure’.

9. Click the **Firmware Upgrade** sub-tab.

10. Click the **Targets** sub-tab if not already displayed. The modules available to be upgraded display in a table.

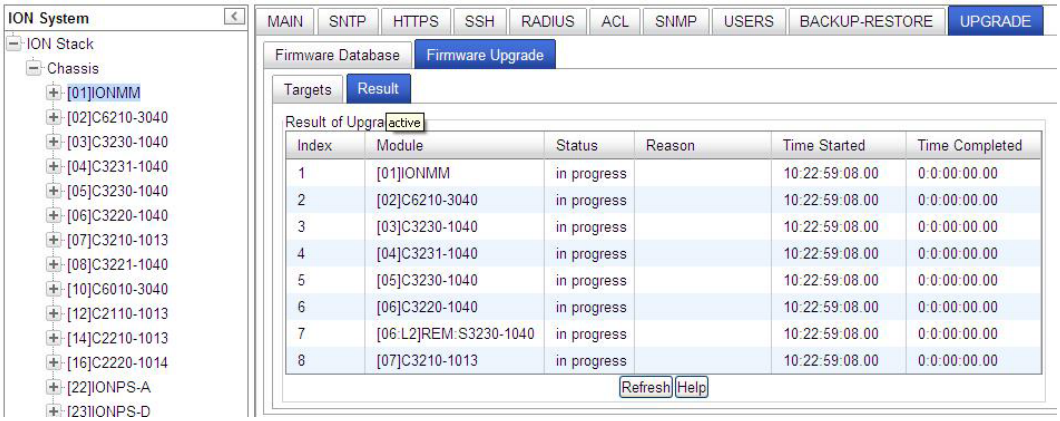


11. In the **Select** column, check the **IONMM** and/or one or more NIDs as the Target Module(s) to be upgraded.

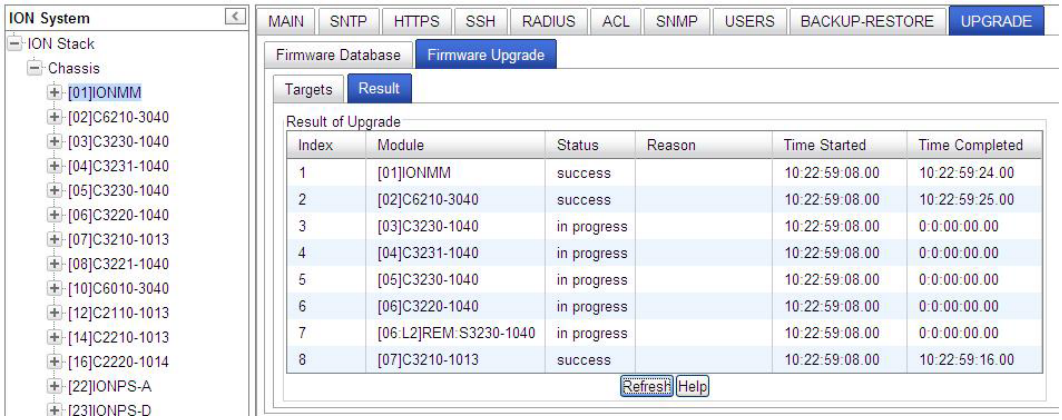
12. Click the **Upgrade** button.

13. Click the **OK** button to proceed.
    During the upload, the message "*Getting records in progress...*" displays.
    If the upload was successful, the message "*Getting all records finished*" displays.
    If the upload was unsuccessful, "*Getting records failed (http server error)*" displays.

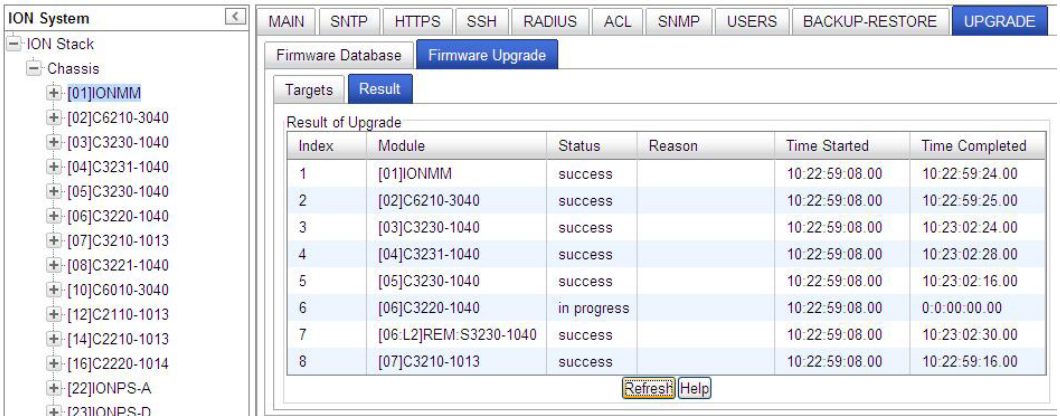
14. Click the **Result** sub-tab. A table displays with upgrade status information.



15. Click the **Refresh** button.



16. If upgrading more than one device, you may have to click **Refresh** again.

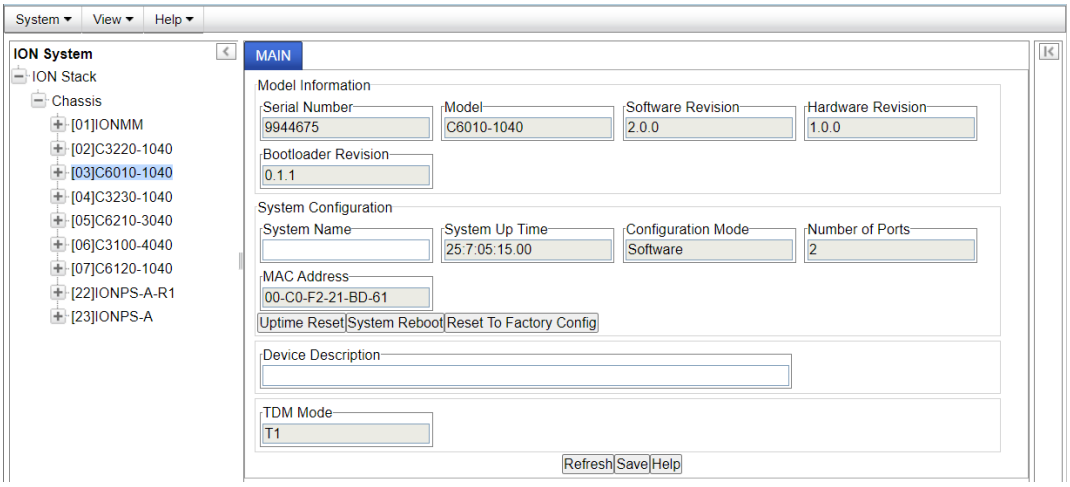


Note: the upgrade will take one or more minutes to complete. The exact amount of time for the upgrade depends on the number of modules being upgraded.

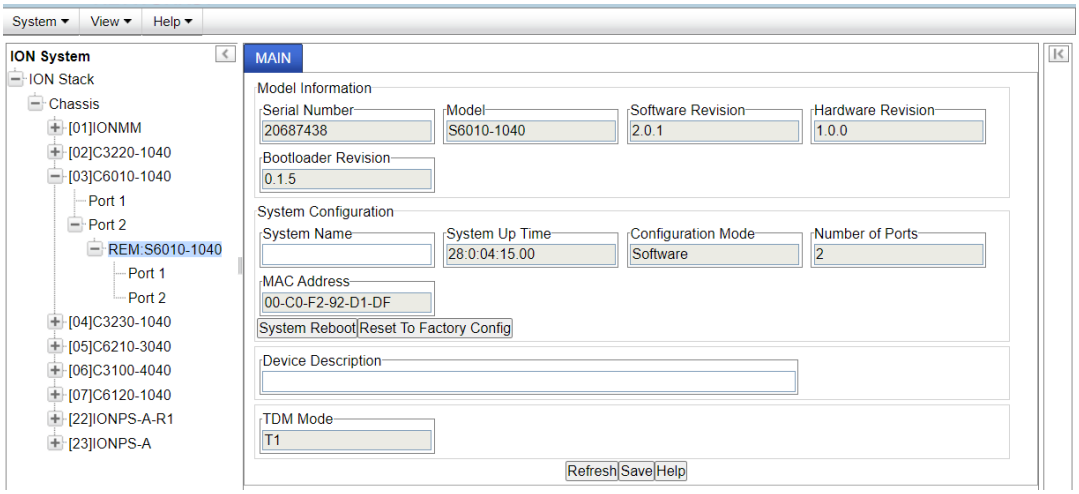
17. After the upgrade has successfully completed, "*success*" displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See "Section 5 – Troubleshooting" for error messages and recovery procedures.

    Check the **MAIN** tab for each upgraded module to ensure that the correct revision level is displayed in the **Software Revision** field. You may have to click **Refresh** to display the updated Software Revision level.

The sample screen above shows a C6010-3040 **MAIN** tab with the Software Revision field indicating a successful firmware upgrade to revision 2.0.0.



The sample screen below shows a remote S6010-1040 upgraded to revision 2.0.1.



Upgrading Slide-In and Remote Modules Firmware via TFTP

This procedure is used to upgrade one or more of the slide-in modules installed in the ION Chassis or a remote module connected to a slide-in module.

Before you can upgrade the firmware in the ION system modules you must do the following:

- Have the upgrade files resident in the default directory on the TFTP Server (normally *C:/TFTP-Root*). To find the latest version of the firmware, go to: https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/1845100581/Latest+firmware+for+the+S6010+Series.
- Create the Database Index and Archive Files (below).
- Perform the Module Firmware Upgrade (page 249).

Creating the Database Index and Archive Files

The database index file is a listing of the modules that can be upgraded and the firmware file that will be used to upgrade each module. The index file must be named **db.idx**. The archive file is a zip file containing the index file and the firmware upgrade files. The archive file must be named **db.zip** in Windows XP. If using Windows 7, name the index file just "**db**".

The following describes the procedure for creating the firmware database index and archive files.

1. Launch the program that will be used to create the index file (**db.idx**).

   Note: a program such as Notepad can be used to create the file.

2. Make an entry for each firmware file to be used for the upgrade in the following format:

   model rev file

   Where:

   model = name of the module
   rev = revision level of the firmware upgrade file
   file = name of the firmware upgrade file

Note: Each of the three fields must be separated by a single space or a single tab.

EXAMPLE

Below is a sample **db.idx** file that upgrades two chassis-resident modules (IONMM and C6010-3040). Note that two upgrade files are required for the x6010 upgrade process.

```
IONMM1.1.0    IONMM.bin.1.0.5_AP
C6010-3040    1.1.0    C6010_0.6.6_FPGA_AP
C6010-3040    1.1.0    C6010_0.6.6_AP
```

3. Save the file as **db.idx**.

   Note: if you used a program, such as Notepad, that does not allow you to save the file as .idx, then save it as a text file and rename it (i.e., change *db.txt* to *db.idx*).

4. Create a zip file that contains each of the upgrade files and the index file. Save the .zip file to the TFTP Server root directory (e.g., filename of **x6010.bin.1.2.5.zip**).

For example, using the files listed in the EXAMPLE above, the db.zip file would contain the following four files:

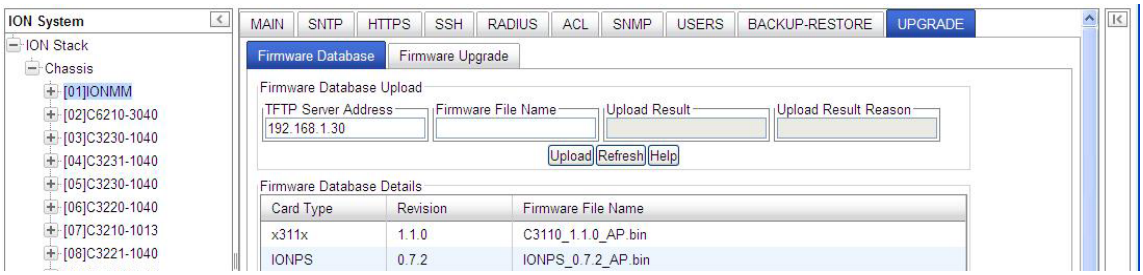
- db.idx
- IONMM.bin.1.1.0
- C6010_1.1.0_FPGA_AP
- C6010_1.1.0_AP

5. Perform the upgrade (see Performing the Module Firmware Upgrade below).

Performing the Module Firmware Upgrade

The upgrade consists of two parts: uploading the archive file to the IONMM, and then loading the upgrade file into the appropriate modules. The following procedure is for upgrading the ION family modules. This procedure assumes that the TFTP server is running and is configured to send and receive transmissions, and that it contains the .zip file created on the previous page.

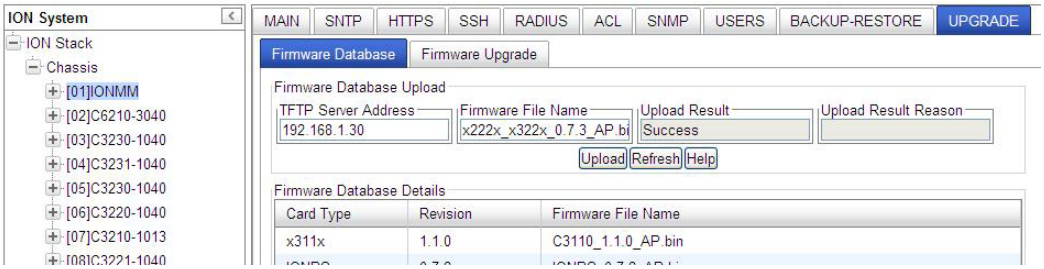
1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **Upgrade** tab. The **Firmware Database** sub-tab displays.



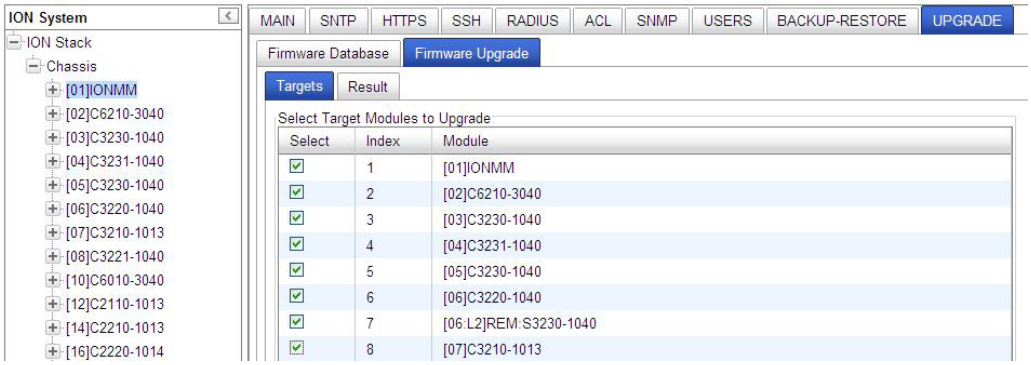
3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP Server where the upgrade (zip) file is located.
4. In the **Firmware File Name** field, enter the name of the zip file you created (e.g., **x6010.bin1.0.5.zip**). **Note**: Be sure to include the .zip extension in the filename.
5. Click the **Upload** button.

   The firmware file is uploaded from the TFTP server. **Note:** this operation can take several minutes. The amount of time for the upload to complete depends on the size of the file. The messages "*Getting values in progress*" and "*Getting values finished*" display during the upload process.
6. Wait for the file to successfully upload. The messages "*The Firmware Database File is being transferred....*" and "*Getting all records finished*" display during the upload process.

   The message "*Success*" displays in the **Upload Result** field and the modules listed in the **db.idx** file will be listed in the **Firmware Database Details** section.



7. Select the **Firmware Upgrade** sub-tab. The **Targets** sub-tab displays.



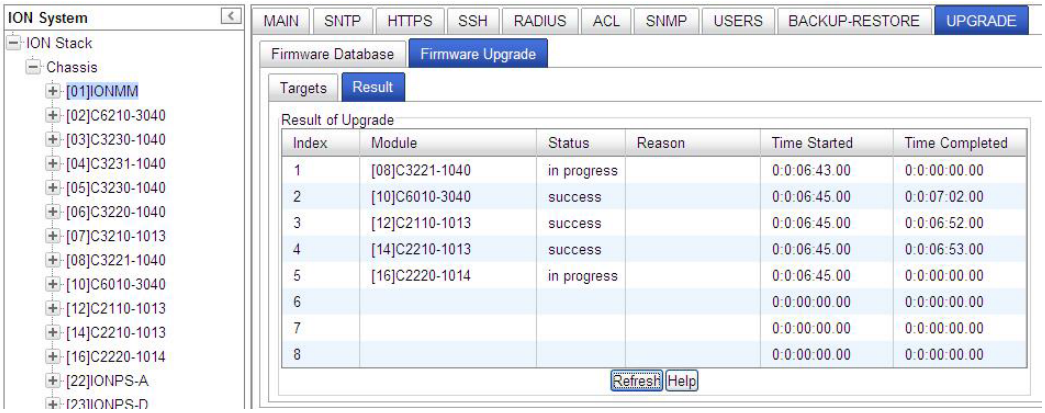
8. In the **Select** column, check the checkbox of each module to be upgraded.

   Note: You can**not** upgrade a module and a remote module connected to it at the same time. In order to upgrade both, you must first do one and then the other.

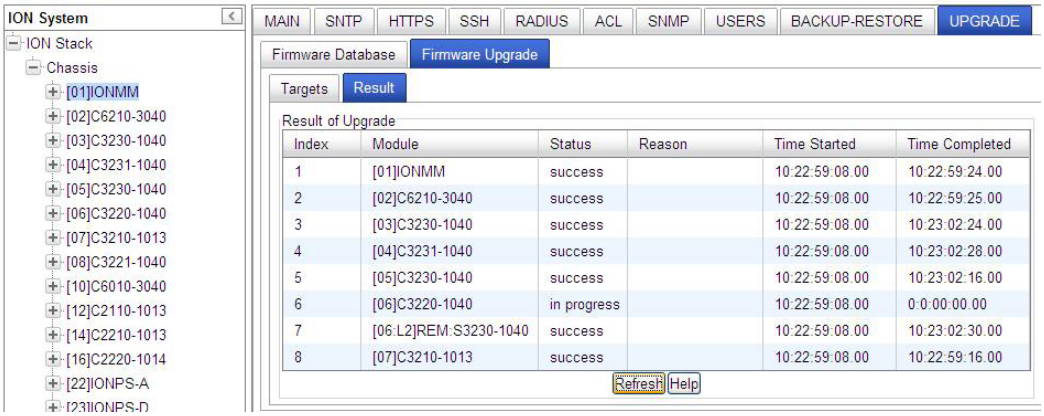
9. Click the **Upgrade** button at the bottom of the screen.

10. When the confirmation window displays, click the **OK** button.

11. To monitor the progress, select the **Result** sub-tab and click **Refresh**.



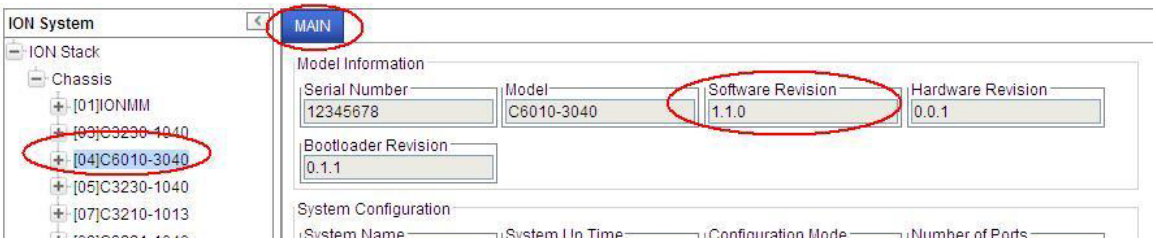
If the Status *in progress* displays, click **Refresh** again; the Status *success* displays.



Note: the upgrade will take one or more minutes to complete. The exact amount of time for the upgrade depends on the number of modules being upgraded.

After the upgrade has successfully completed, "*success*" displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See "Section 5 – Troubleshooting" for error messages and recovery procedures.

12. Check the **MAIN** tab for each module to ensure that the correct revision level is displayed in the **Software Revision** field.



The sample screen above shows the C6010-3040 **MAIN** tab with the **Software Revision** field indicating a successful firmware upgrade to version **1.1.0**.

Firmware Upgrade File Content and Location

The table below shows file content and location resulting from a firmware upgrade.

Table 11: File Content and Location after a Firmware Upgrade

File Type	Filename	File Description	Stored Directory	Lost after Firmware Upgrade? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes
MIB 105con-figuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configura-tion files for SNMP setting	/agent3/conf	No

Additional Upgrade Procedures

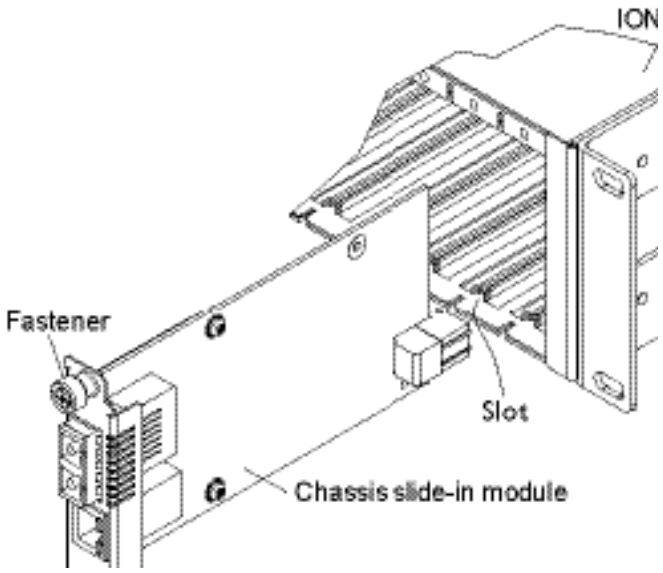
Additional upgrade procedures are available for the ION system. Refer to the *IONMM User Guide* for these IONMM upgrade procedures:

- Upgrade the IONMM and/or NID Firmware.
- Upgrade Slide-In and Remote Modules Firmware via TFTP. This procedure is used to upgrade one or more of the slide-in modules installed in the ION Chassis or a remote module connected to a slide-in module. Requires you to 1) Create Database Index and Archive Files, and 2) Perform the Module Firmware Upgrade.
- Perform the Module Firmware Upgrade – the upgrade consists of two parts: uploading the ar-chive file to the IONMM, and then loading the upgrade file into the appropriate modules. This procedure is for upgrading the ION system modules.

Replacing a Chassis Resident NID

The x6010 is a “hot swappable” device (it can be removed and installed while the chassis is powered on). To replace a chassis resident x6010, do the following.

1. Backup the configuration (see Backing Up Slide-In and Remote Modules.
2. Disconnect any cables attached to the x6010.



3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the x6010 from the Chassis.
5. Carefully slide the new x6010 fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the x6010 to the chassis.
7. Connect the appropriate cables to the x6010.
8. Load (restore) the configuration into the new x6010 (see Restoring Slide-In and Remote Modules).

6 Command Line Interface (CLI) Reference

General

This section describes CLI use and the commands for the x6010.

Command Line Editing

This section describes how to enter CLI commands.

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters.

Display Similar Commands

At the command line, you can use the keyboard Tab key or **?** Key to show available commands in a category of commands after entering a part of the command.

For example, use the Tab key to enter part of the command (**show ether** in this example) to display all of the available commands that start with **show ether**. The commands display in a single row.

```
C1|S8|L1D>show tdm <tab key>
config    loopback  port
C1|S8|L1D>
```

Use the **?** key after a partial CLI command entry to display all of the available commands that start with **show ether**, but in a single column:

```
  C1|S8|L1D>show tdm ?
    config
    loopback
    port
  C1|S8|L1D>
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember to not leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "**s**."

Recall Commands

To recall recently-entered commands from the command history, perform one of the optional actions below:

Ctrl-P or **Up arrow** (↑) key: Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

Ctrl-N or **Down arrow** (↓) key: Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up arrow key. Repeat the key sequence to recall successively more recent commands.

Keystroke Commands

The table below shows the optional keystrokes available to edit command lines (*indicates HyperTerm support, ** indicates command prompt support, *** indicates both HT and command prompt support by this keystroke).

Table 12: Keystroke Editing Commands

Capability	Keystroke	Purpose
Move the command line around to make changes or corrections	Ctrl-B *** or left (←) arrow key ***	Move the cursor back one character.
	Ctrl-F *** or right (→) arrow key ***	Move the cursor forward one character.
	Ctrl-A ***	Move the cursor to the beginning of the command line.
	Ctrl-E ***	Move the cursor to the end of the command line.
Recall commands from the buffer and paste them in the command line	Ctrl-Y ***	Recall the most recent entry in the buffer.
	Ctrl-T **	Transpose the character to the left of the cursor with the character located at the cursor.
	Ctrl-Y **	Recall the most recent entry in the buffer.
Delete entries (if you make a mistake or change your mind)	Delete key *** or Backspace key ***	Erase the character to the left of the cursor.
	Ctrl-D ***	Delete the character at the cursor.
	Ctrl-K ***	Delete all characters from the cursor to the end of the command line.
	Ctrl-U *** or Ctrl-X ***	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W ***	Delete the word to the left of the cursor
	Esc D **	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters	Esc C *	Change case from capital to lower-case (or lower-case to capital) at the cursor.
Redisplay the current command line if the switch unexpectedly sends a message to your screen	Ctrl-L *** or Ctrl-R ***	Redisplay the current command line (reverse-i-search).

Command Descriptions

This section defines the x6010 CLI commands in terms of syntax, descriptions, and examples.

Command: **Password for Login / Access**

Syntax: Password: **private**

Description: The default device CLI password. CLI entry requires a successful password entry.

Example:

```
Password:
Login incorrect
login: ION
Password:private

Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

AgentIII C1|S1|L1D>
```

In order to control the NIDs via a USB interface, the command line prompt must be showing the location of the module to be managed. Use the procedure below to access the NID and login via USB connection.

1. Start the terminal emulator program (e.g., HyperTerminal).

2. When the emulator screen displays, press **Enter**. The login prompt displays. If your system uses a security protocol (e.g., RADIUS, SSH, etc.), you must enter the login and password required by that protocol.

3. Type **ION** (all upper case) and press **Enter**. The password prompt displays. If a "Login incorrect" message displays, ignore it.

4. Type your password. The default is **private** (all lower case).

5. Press **Enter**. The HyperTerminal command line prompt displays (C1|S3|L1D>).

6. Enter CLI commands to set up, configure, operate, and maintain the x6010.

Command: **Log Out (Quit)**

Syntax : **q**(uit)

Description: Exit the current mode and return to the previous mode (the command line prompt).

Example :
```
C1|S3|L1D>q
login:
```

Note: At IONMM FW v 1.3.14 and before, the ION System does not automatically log out upon exit or after a timeout period, which could leave it vulnerable if left unattended. Follow your organizational policy on when to sign out.

At IONMM FW v 1.3.15 and above, a 15 minute inactivity timeout was added. Also note that at login, a timestamp is shown while the page loads.

Command: **Help (?)**

Syntax: **?**

Description:Displays all available command line commands.

Example: A **?** (Help) command listing is shown below.

```
C1|S4|L1D>?
  add       Add a ACL condition.
  Clear     Clear all counters of the specified Ethernet port.
  Cls       Clear the screen.
  Go        Set the location to device/port of the SIC to be operated.
  Home      Go back to the IONMM card.
  List      Display a list of all available commands.
  Ping      Send ICMP ECHO-REQUEST to network hosts.
  Prov      Get / set current TFTP server address.
  Ps        Report a snapshot of the current processes.
  Pwd       Show current directory.
  Quit      Exit current mode and down to previous mode.
  Reboot    Warm start the system.
  Reset     Reset all ports counters/factory defaults/uptime.
  Set       Set AIS, Circuit-ID, DMI, etc.
  show      Show AIS, DMI, TDM information.
  Start     Start TDR test of the specified Ethernet port.
  Stat      Show topology information of the chassis.
  Tftp      Get/put/upgrade a file from via TFTP server.
  Update    Update a firmware database file.
  Upgrade   Upgrade firmware modules.
C1|S4|L1D>
```

Command: **Go to another location**

Syntax: **go** <location string>

Description:Set the location to device/port of the SIC to be operated.

Usage: **go** [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>||l2p=<1-15>||l3p=<115>||l1d||l2d||l3d)

Example:
```
C1|S1|L1D>go c=1 s=4 l1d
C1|S4|L1D>go c=1 s=6 l1d
Invalid location parameters, cannot find the physical entity!
C1|S4|L1D>go c=1 s=8 l1d
C1|S8|L1D>go c=1 s=8 l1p=1
C1|S8|L1P1>
```

Command: **Show TDM Configuration**

Syntax: **show tdm config** <cr>

Description: A system-level command that displays the x6010 TDM type (the current x6010 device's operating mode, either ***T1*** or ***E1***). **Note**: at the port level, use the **show tdm port conf**ig command.

Example:
```
Agent III C1|S2|L1D>show tdm ?
  config
  inband
  loopback
  peer
  port
Agent III C1|S2|L1D>show tdm config
tdm type:                                                t1
Agent III C1|S2|L1D>
```

Command: **Show TDM Loopback Capability**

Syntax: **show tdm loopback capability** <cr>

Description: A port-level command that displays the port's TDM loopback setting (either noLoopback or phyLayer).

Example:
```
Agent III C1|S2|L1D>show tdm loopback capability
Error: this command should be executed on a port!
Agent III C1|S2|L1D>go l1p=1
Agent III C1|S2|L1P1>show tdm loopback capability
Loopback capability: phyLayer
Agent III C1|S2|L1P1>go l1p=2
Agent III C1|S2|L1P2>show tdm loopback capability
Loopback capability: phyLayer
Agent III C1|S2|L1P2>
```

Command: **Show TDM Loopback State**

Syntax: **show tdm loopback state** <cr>

Description: A port-level command that displays the port's TDM loopback type and state.

Example:

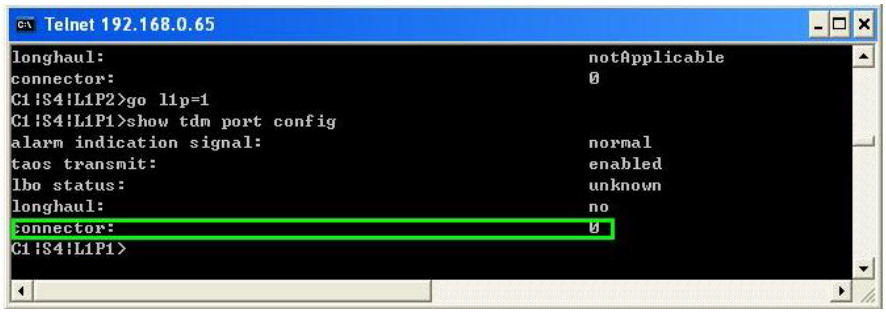
```
Agent III C1|S2|L1P2>show tdm loopback state
Loopback type: phylayer
Loopback state: noLoopback
Agent III C1|S2|L1P2>show tdm loopback state
Loopback type: phylayer
Loopback state: noLoopback
Agent III C1|S2|L1P2>set tdm loopback oper init
Agent III C1|S2|L1P2>show tdm loopback state
Loopback type: phylayer
Loopback state: localInLoopback
Agent III C1|S2|L1P2>
Agent III C1|S2|L1P2>go l1p=1
Agent III C1|S2|L1P1>show tdm loopback state
Loopback type: phylayer
Loopback state: noLoopback
Agent III C1|S2|L1P1>
```

Command: **Show TDM Port Configuration**

Syntax: **show tdm port config** <cr>

Description: A port-level command that displays the x6010 TDM table containing the current x6010 device port's TDM configuration settings. **Note**: at the device level, use the **show tdm config** command.

Example 1: (Telnet example)



Example 2:

```
C1|S4|L1P2>show tdm port config
link oper status:                          down
alarm indication signal:                 normal
taos transmit:                             enabled
connector:                                 SFP Slot
C1|S4|L1P2>
```

Example 3:

```
C1|S4|L1P1>show tdm port config
link oper status:                          up
alarm indication signal:                 normal
taos transmit:                             enabled
lbo status:                                unknown
longhaul:                                  no
connector:                                 Dual BNC
C1|S4|L1P1>
```

Example 4:

```
C1|S4|L1P1>show tdm port config
link oper status:                        down
alarm indication signal:                 normal
taos transmit:                           enabled
lbo status:                              e13-0V120ohm
longhaul:                                no
connector:                               Dual BNC
C1|S4|L1P1>
```

Messages: *Error: Get Alarm Indication Signal no such object.*

Command: **TAOS Transmit Enable/Disable**

Syntax: **set taos transmit**=(enable|disable)

Description: A port-level command that defines the current x6010 port's ability to send TAOS (Transmit All OneS) signals. Defines the port's ability to Transmit an All Ones pattern. The default setting is enabled.

Example:

```
C1|S4|L1D>set taos ?
  transmit
C1|S4|L1D>set taos transmit ?
  disable
  enable
C1|S4|L1D>set taos transmit enable
Error: this command should be executed on a port!
C1|S4|L1D>go l1p=1
C1|S4|L1P1>set taos transmit enable
C1|S4|L1P1>go l1p=2
C1|S4|L1P2>set taos transmit enable
C1|S4|L1P2>
```

Note: Use the **show tdm port config** command to display the current TAOS status.

Command: **Show DMI Information**

Syntax: **show dmi info** <cr>

Description: Displays the Diagnostic Monitoring Interface (DMI) information (dmi table) for a fiber port.

Example:

```
Agent III C1|S2|L1P2>show dmi info
Diagnostic monitoring interface information:
DMI connector type:                                 LC
DMI indentifier:                                    SFP
DMI Nominal bit rate:                               1300*Mbps
DMI 9/125u Singlemode Fiber (m):                    N/A
DMI 50/125u Multimode Fiber (m):                    500*m
DMI 62.5/125u Multimode Fiber (m):                  30*10m
Copper(m):                                          N/A
DMI fiber interface wavelength:                     850*nm
DMI temperature:                                    40.8*C
DMI temperature:                                    105.4*F
DMI temperature alarm:                              normal
DMI transmit bias current:                          4784*uA
DMI transmit bais alarm:                            normal
DMI Transmit power:                                 252*uW
DMI Transmit power:                                 -5.986*dBM
DMI Transmit power alarm:                           normal
DMI Receive power:                                  242*uW
DMI Receive power:                                  -6.162*dBM
DMI Receive power alarm:                            normal
DMI Receive power intrusion threshold:              0*uW
Agent III C1|S2|L1P2>
```

Command: **Set DMI Receive Power Preset Level**

Syntax: **set dmi rx–power–preset–level**=<x> ??

Description: Defines a fiber port's current RX power threshold.

Where x = <0-10>

Example:
```
C1|S4|L1D>set dmi ?
  rx-power-preset-level
C1|S4|L1D>set dmi rx-power-preset-level 5
Error: this command should be executed on a port!
C1|S4|L1D>go l1p=1
C1|S4|L1P1>set dmi rx-power-preset-level 5
DMI is only supported on FIBER port!
C1|S4|L1P1>go l1p=2
C1|S4|L1P2>set dmi rx-power-preset-level 5
C1|S4|L1P2>
```

Note: use the **show dmi info** command to display the current Diagnostic monitoring interface information.

Command: **Set TDM Loopback Operation**

Syntax: **set tdm loopback operation**=<init|stop> <cr>

Description: Defines the current port's TDM loopback operating configuration to either ***init*** (start) or ***stop***.

Example:
```
C1|S4|L1P2>set tdm ?
  loopback
C1|S4|L1P2>set tdm loopback ?
  oper
  type
C1|S4|L1P2>set tdm loopback oper ?
  init
  stop
C1|S4|L1P2>set tdm loopback oper init
C1|S4|L1P2>set tdm loopback oper stop
C1|S4|L1P2>
```

Command: **Set TDM Loopback Type**

Syntax: **set tdm loopback type**=<x> <cr>

Description: Defines the current port-level TDM loopback operating configuration to either no loopback or phylayer loopback.

Example:
```
C1|S4|L1P2>set tdm ?
  loopback
C1|S4|L1P2>set tdm loopback ?
  oper
  type
C1|S4|L1P2>set tdm loopback type ?
  noloopback
  phylayer
C1|S4|L1P2>set tdm loopback type noloopback
C1|S4|L1P2>set tdm loopback type phylayer
C1|S4|L1P2>
```

Command: **Set System Name**

Syntax: **set system name**=(name) <cr>

Description: Changes the name assigned to the x6010 device. The default setting is blank.

Example:
```
C1|S4|L1D>set system name=C6010@Corporate
C1|S4|L1D>show card info
System name:        C6010@Corporate
Uptime:             1 day, 00:43:51
Port number:        2
Serial number:      12345678
Config mode:        software
Software:           1.1.0
Bootloader:         0.1.1
Hardware:           0.0.1
C1|S4|L1D>
```

The system name default is x6010 (case sensitive – the S or C in capitals). The **show card info** command displays the system name and other descriptive information.

Command: **Show Card Information**

Syntax: **show card info**

Description: Displays the device information (*sys config table*) for the x6010.

Example:
```
Agent III C1|S8|L1D>show card info
System name:
Uptime:              00:02:17
MAC:                 00-c0-f2-21-b6-f0
Port number:         2
Serial number:       4001
Config mode:         software
Software:            1.2.5
Bootloader:          0.1.1
Hardware:            1.0.0
Agent III C1|S8|L1D>
```

Command: **Show Card Type**

Syntax: **show cardtype**

Description: Displays the model number of the device.

Example:
```
Agent III C1|S8|L1D>show cardtype
Card type:                    C6010-3040
Agent III C1|S8|L1D>
```

Command: **Show Firmware Upgrade Result**

Syntax: **show firmware upgrade result**

Description: Used to verify the IONMM Upgrade results. Type **show firmware upgrade result** and press **Enter**. The firmware upgrade results are displayed in a table. If the firmware upgrade was successful, the time started and time completed display.

See the IONMM User Guide for specifics. See the "Upgrade" section for the procedure. See "Section 5 – Troubleshooting" for error messages and recovery procedures.

Command: **Show Firmware Database Update Result**

Syntax: **show firmware-db update result**

Description: See the IONMM User Guide for specifics. See the "Upgrade" section for the procedure. See "Section 5 – Troubleshooting" for error messages and recovery procedures.

Command: **Prov Get TFTP Server Address**

Syntax: **prov get tftp svr addr**

Description: Accesses the TFTP server's IP address.

Example:
```
C1|S4|L1AP2|L2D>prov get tftp svr addr
C1|S4|L1AP2|L2D>
```

Command: **Prov Set TFTP Server Address**

Syntax: **prov set tftp svr type**

Description: Defines the TFTP Server IP address for TFTP server operations.

Example:
```
C1|S4|L1AP2|L2D>prov set tftp svr type ipv4 addr 192.168.1.30
C1|S4|L1AP2|L2D>
```

Command: **Set Circuit ID**

Syntax: **set circuit-ID**=<xx> <cr>

Description: Lets you define an ASCII text string up to 63 bytes and override the default Circuit ID, which is vlan-module-port in binary format, for a device and/or device ports, where:

xx = an ASCII text string up to 63 bytes

Example:
```
C1|S4|L1D>set circuit XX/YYYY/000000/111/CC/SEG
C1|S4|L1D>show circuit-ID
Circuit-ID:          XX/YYYY/000000/111/CC/SEG
```

The default setting is 'blank' (no data entered).

Note: Use the **show circuit-ID** command to display the Circuit ID information for a device or port.

Command: **Show Circuit ID**

Syntax: **show circuit-ID** <cr>

Description: Displays the current Circuit ID (ifxtable or system table) for the device or port. Use the **set circuit-ID** command to change the current Circuit ID information defined for a device or port.

Example:
```
C1|S4|L1D>set circuit XX/YYYY/000000/111/CC/SEG
C1|S4|L1D>show circuit-ID
Circuit-ID:          XX/YYYY/000000/111/CC/SEG
```

Note: If no circuit ID has been defined via the set circuit-ID= command, nothing displays after the "Circuit-ID:".

Command: **Status Check**

Syntax: **stat**

Description: Displays the current chassis configuration.

Example:

```
C1|S4|L1D>stat
ION statck
        Chassis – BPC
                [  1]  IONMM
                        Port 1
                        Port 2
                [  3]  C3230-1040
                        Port 1
                        Port 2
                [  4]  C6010-3040
                        Port 1
                        Port 2
                                level2 REM: S6010-1040
                                        Port 1
                                        Port 2
                [  5]  C3230-1040
                        Port 1
                        Port 2
                [  7]  C3210-1013
                        Port 1
                        Port 2
                [  8]  C3221-1040
                        Port 1
                        Port 2
                        Port 3
                [ 10]  C3231-1040
                        Port 1
                        Port 2
                        Port 3
                [ 12]  C2110-1013
                        Port 1
                        Port 2
                [ 14]  C2210-1013
                        Port 1
                        Port 2
                  [ 22]  IONPS-A
                        Temperature Sensor
                        Voltage Sensor
                        Power Sensor
                        Fan-1
                        Fan-2
                [ 23]  IONPS-D
                        Temperature Sensor
                        Voltage Sensor
                        Power Sensor
                        Fan-1
                        Fan-2
C1|S4|L1D>
```

Command: **TFTP Get**

Syntax: **tftp get iptype**=<ww> **ipaddr**=<xx> **remotefile**=<yy> **[localfile**=<zz>]

Description:Gets (retrieves) a file from the default directory on the TFTP server and puts it in the IONMM

where:

ww = IP address format; valid choices are:

- ipv4 (32-bit address format)
- dns (domain name address format)

xx = IP address of the TFTP server where the file is located

yy = name of the file to "get"

zz = optional; name that the file is to be saved as on the IONMM or NID.

Example:

```
C1|S3|L1D>tftp get iptype=ipv4 ipaddr=192.168.1.30 remotefile=cert localfile=cert
TFTP transferring...
File transfer successful!
```

Command: **TFTP Put**

Syntax: **tftp put iptype**=<ww> **ipaddr**=<xx> **localfile**=<yy> [**remotefile**=<zz>]

Description:Puts (sends) a local file from the IONMM to the default directory on the TFTP server.

Where:

ww = IP address format; valid choices are:

- ipv4 (32-bit address format)
- dns (domain name address format)

xx = IP address of the TFTP server where the file is to be sent

yy = name of the file to send ("put")

zz = optional; name the file is to be saved as on the TFTP server

Example:

```
C1|S4|L1D>tftp put iptype ipv4 ipaddr 192.168.1.30 localfile readme
tftp put failed.
```

Command: **TFTP Upgrade**

Syntax: **tftp upgrade iptype**=(ipv4) ipaddr=ADDR remotefile=RFILE

Description: Upgrades IONMM card with IONMM firmware from a TFTP server. The TFTP server must be configured and running and the remotefile must be in the proper location (e.g., *C:\TFTP-Root*).

Where:

xx = iptype=(ipv4) , the TFTP server address type

yy = ipaddr=ADDR, the TFTP server address

zz = RFILE, the remote firmware file name

Example:

```
C1|S1|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remotefile 1-3-C3230-
1040.config
Processing...
Wrong firmware for upgrading!
C1|S1|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remotefile IONMM_0.6.5_AP.bin

Processing...

TFTP upgrade succeeded!
C1|S1|L1D>
```

Command: **Reboot (Warm Start) the C6010**

Syntax: **reboot**

Description: Performs a reboot ("cold start the system") of the device in the command line prompt.

Warning: Doing a reboot or restart of a NID or the IONMM may cause some configuration backup files to be lost and the USB or Telnet session to drop. Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory removes temporary files (e.g. configuration backup files, Syslog file). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key).

Example 1 (C6010):

```
C1|S18|L1D>reboot
Warning: this command will restart system, connection will be lost and please login
again!

Login: ION
Password:private

Hello, this is ION command line (version 1.00).
Copyright 2009 Lantronix.

C1|S1|L1D>
```

The HyperTerminal connection closes and the Windows Taskbar Notification area displays the message "*A network cable is unplugged!*. "

To recover: 1. Close the Windows Taskbar message. 2. Disconnect and close HyperTerminal. 3. Re-open HyperTerminal. 4. Re-open the HT session. 5. Log back in to the x6010.

Example 2 (S6010):

```
C1|S4|L1AP2|L2P2>reboot
Warning: this command will restart system, connection will be lost and please login again!
Warm start failed.
C1|S4|L1AP2|L2P2>
```

Reset System Uptime

Syntax: **reset uptime**

Description: Resets the System Up Time counter to zero, and immediately begins to increment.

Example:
```
C1|S18|L1D>reset uptime
C1|S18|L1D>
```

Note: If you reset uptime on the connected (local) chassis device, the remote device's uptime counters are reset as well.
Note: Use the **show system info** command to display the current device uptime.
Note: the **reset uptime** command is not available for the Power Supply modules.

Command: **Reset to Factory Default Configuration**

Syntax: **reset factory**

Description: Resets a card to its factory default configuration.

Warning: doing a reboot or restart of the IONMM or NID may cause some configuration backup files to be lost and the USB or Telnet session to drop. Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory removes temporary files (e.g. configuration backup files, Syslog file). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key).

Example 1:

```
C1|S18|L1D>reset factory
Warning: this command will restart the specified card, connection will be lost!
C1|S18|L1D>
```

The HyperTerminal connection closes and the Windows Taskbar Notification area displays the message "*A network cable is unplugged!*."

To recover: 1. Close the Windows Taskbar message. 2. Disconnect and close HyperTerminal. 3. Re-open HyperTerminal. 4. Re-open the HT session. 5. Log back in to the x6010.

Example 2:

```
C1|S4|L1AP2|L2D>reset factory
Warning: this command will restart the specified card, connection will be lost!
C1|S4|L1AP2|L2D>
```

Command: **Reset (Clear) All Ports Counters**

Syntax: **reset all ports counters**

Description: Resets all counters on all ports of the specified Ethernet device. The device's counters (RMON statistics counters, dot3 counters etc.) are reset to zero and begin incrementing immediately.

Example:
C1|S5|L1D>**reset all ports counters**
C1|S5|L1D>

Command: **List All Commands**

Syntax: l**ist** <cr>

Description:Displays all of the available CLI commands.

Example:

```
C1|S2|L1D>list
    go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-
    15>|l1d|l2d|l3d)
    home
    list
    prov get tftp svr addr
    prov set tftp svr type=(ipv4|dns) addr=ADDR
    quit
    reboot
    reset all ports counters
    reset factory
    reset uptime
    set circuit-ID=CIRCUIT
    set community read=COMMUNITY
    set community write=COMMUNITY
    set dbg level=<0-2>
    set dmi rx-power-preset-level=POWER
    set system name=NAME
    set taos transmit=(enable|disable)
    set tdm loopback oper=(init|stop)
    set tdm loopback type=(noloopback|phylayer)
    show card info
    show cardtype
    show circuit-ID
    show dmi info
    show firmware upgrade result
    show firmware-db update result
    show tdm config
    show tdm loopback capability
    show tdm loopback state
    show tdm port config
    stat
    tftp get iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
    tftp put iptype=(ipv4|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
    tftp upgrade iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE
    upgrade module
C1|S2|L1D>
```

Note that not all of the commands listed are necessarily operational on the x6010 models.

7 Troubleshooting

General

This section provides basic and specific problem determination processes, and a description of problem conditions that may occur or messages that may be displayed. This section also documents ION system tests, x6010 jumpers, and describes where and how to get technical support.

IMPORTANT

For each procedure described in this section, do each step sequentially as indicated. If the result of a step causes the problem to be corrected, **do not** continue with the other steps in the procedure.

Basic ION System Troubleshooting

This basic process is intended to provide some high-level techniques that have been found useful in isolating ION problems. This process is not a comprehensive guide to troubleshooting the ION system. The intent here is to 1) avoid missing any important information, 2) simplify analysis of captured information, and 3) improve accuracy in finding and explaining problem causes and solutions.

This basic process applies to these ION system and related components:

- ION Chassis
- ION NIDs (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web interface or ION command line interface – CLI).
- ION power supply
- ION Options (ION SFPs, ION LG Kit, etc.)
- Data cables, electrical cables, and electrical outlets
- Third party network equipment (circuit protection equipment, battery backup, 3rd party client or server software –TFTP, etc.)

When troubleshooting an ION system / network problem on site:

1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the simplest and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the NIDs are seated properly, view the CLI **show** command output, run ION System Tests (page 203), In-band Loopback Code Detect Procedure (page 210), and check DIP Switch and Jumper Settings (page 211).
6. Write down your initial 2-3 guesses as to the cause of the problem.
7. Verify that the Lantronix product supports the function you are trying to perform. Your particular Lantronix product or firmware version may not support all the features documented for this

module. For the latest feature information and caveats, see the release notes for your particular device/system and firmware release.

8. Compare the results of an operation via each user interface (Web interface, CLI, Focal Point 3).
9. Use the Web interface or command line interface (CLI) to obtain all possible operating status information (log files, test results, **show** command outputs, counters, etc.)
10. Use the ION system manual procedure to retry the failed function or operation.
11. For the failed function or operation, verify that you entered valid parameters using the cursor-over-help (COH) and/or the ION system manual.
12. Based on the symptoms recorded, work back through each step in the process or operation to recall a point at which the problem occurred, and examine for a possible failure point and fixe for each.
13. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
14. Isolate the 1-2 most likely root causes of what went wrong, and gain as much information as you can to prove the suspected cause(s).
15. If you find a sequence of actions that causes the problem to recur, replicate the full sequence several times and document it if possible.
16. Review your system log information and add any other comments that occur to you about what has taken place in terms of system behavior and suspected problem causes and solutions.
17. Review the "Recording Model Information and System Information" section before calling Lantronix for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED fault and activity displays (page 129)
- Problem Conditions (page 130)
- CLI Messages (page 143)
- Web Interface Messages (page 145)
- Webpage Messages (page 154)
- Config Error Log (config.err File) Messages (page 160)
- Third Party Tool Messages (HyperTerminal, Ping, and Telnet Messages) (page 169)
- T1 Error Events and Alarm Conditions (page 219)

These message types and their recommended recovery procedures are covered in the following subsections.

LED Fault and Activity Displays

Refer to this section if the LEDs indicate a problem. For any LED problem indication, review the "Front Panel Connections and LEDs" section, and then perform the following steps.

1. Check the power cord connections and power outlet.
2. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
3. Make sure the USB cable is properly connected.
4. Check the power supply voltages (see related documentation).
5. Verify that the ION system devices have the latest firmware versions. Download the latest firmware version and upgrade as necessary.
6. Check if other network devices are working properly.

Power (PWR) LED is off (not lit):

1. Check at both ends for a loose power cord.
2. Check for a power supply failure. Replace power supply if failed.
3. Make sure all circuit protection and connection equipment and devices are working.
4. Verify that the ION system power supply is within operating range.
5. Remove the card from the chassis and re-insert it. Replace if failed.
6. Make sure the mode displayed matches the hardware setting on the device. See the "Jumper Settings" section.

SDF (Signal Detect/Fiber) LED off (not lit):

1. Check the **CL** – **FL** Switch setting.
2. Check fiber cables for proper connection.
3. Verify that the TX and RX cables are connected to RX and TX ports, respectively, on the far end device.
4. Check if other network devices are working properly.
5. Remove the suspect x6010 from the chassis and re-insert it.

SDC (Signal Detect/Copper) LED off (not lit):

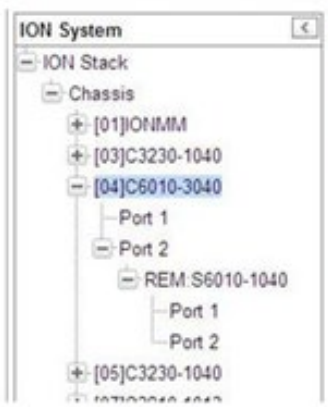
1. Check the **CL** – **FL** Switch setting.
2. Check twisted pair cables for proper connection.
3. Check RJ-45 connectors and cables for correct twisted pair cable configuration.
4. Check integrity of device attached to the x6010 by twisted pair cable.
5. Check if other network devices are working properly.
6. Remove the suspect x6010 from the chassis and re-insert it.

TX or RX LED off (not flashing):

1. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
2. Check if other network devices are working properly.
3. Remove the card from the chassis and re-insert it.
4. Verify that the ION system devices have the latest firmware versions.
5. Download the latest firmware version and upgrade as necessary.

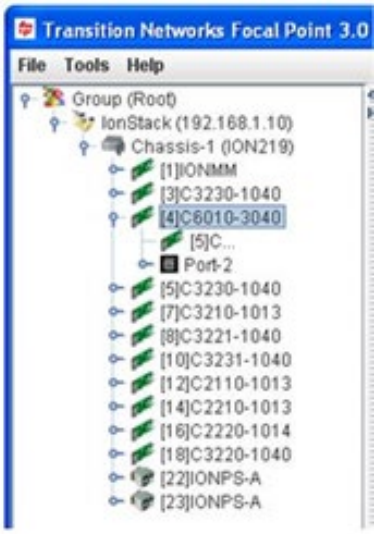
Problem Conditions

You can access the x6010 via the Web interface, Focal Point, and the CLI. Comparing the results of an operation via each user interface is an initial step in troubleshooting.



ION System – Web Interface

ION System – Command Line Interface (CLI



Focal Point – Web Interface

1. Verify the overall ION system configuration.
2. Compare the ION configuration via each user interface (Web interface, CLI, Focal Point 3).
3. Locate the specific error condition or message in the following sections.

Cannot access the NID via USB port

1. If you can access the IONMM, continue with step 2 below. If you cannot access the IONMM, see the IONMM User Guide.
2. Check that the syntax for the **go** command is correct. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
3. Power cycle the NID.
4. If the problem persists, contact Technical Support.

Cannot access the NID via Telnet

1. If you can access the IONMM, continue with step 2 below. If you cannot access the IONMM, see the IONMM User Guide.
2. Check that the syntax used for the **go** command is correct. The **go** command syntax is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
3. Power cycle the NID.
4. If the problem persists, contact Technical Support.

Cannot access the NID via the Web

1. If you can access the IONMM, continue with step 2 below. If you cannot access the IONMM, see the IONMM User Guide.
2. Make sure that RADIUS client and HTTPS state are all set to disabled.
3. Power cycle the NID.
4. If the NID is a remote, power cycle the local NID.
5. If the problem persists, contact Technical Support.

Cannot activate IP-based management

1. Verify that the IP, gateway, and subnet mask are configured correctly.
2. With DHCP enabled, DHCP could have failed leaving the system with the old static IP configuration. Check the configuration via the USB port.
   a) Access the IONMM through a USB connection (see "Starting a USB Session").
   b) At the command prompt, type: **show ip–129nter config**.
   c) Press **Enter**.
3. If the problem persists, contact Technical Support.

Cannot upgrade modules

See Upgrade fails.

Cannot upload upgrade files

See Upload fails.

Telnet connection is lost after a CLI command is executed

1. If you can connect to the IONMM through the Web interface (see "Starting the Web Interface"), go to step 3 below. If you cannot connect to the IONMM through the Web interface, continue with step 3 below.
2. Check the following:
   - the IONMM is seated properly in the chassis
   - the IONMM is powered up
   - the network cable is seated
   - the network is operational
3. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
4. Cycle power for the module in question. **Note**: for slide-in cards, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. If the problem persists, contact Technical Support.

Trap Server does not record traps

1. Ensure the Trap Server application is running.
2. SNMP traps may be blocked by a router or firewall. Consult your Network administrator to determine if this is the case.
3. Check that the correct SNMP trap manager IP address has been defined for the module.
   - For Web Interface – go to the **SNMP Configuration** section on the **MAIN** tab.
   - For CLI – at the device level, type: **show snmp config**.
4. If the problem persists, contact Technical Support.

Upgrade fails

1. Check the following:
   - The correct module(s) has been selected.
   - The module selected is listed in the **Card Type** column on the **Firmware Database** sub-tab.
   - A hierarchy conflict does not exist (i.e., trying to upgrade a level 2 module and its level 1 module at the same time).
   - The modules are powered on.
2. Wait two minutes, and then retry the operation. If the operation still fails, continue with step 3 below.
3. Reboot the IONMM and all modules in the upgrade stream.
4. Retry the operation. **Note:** you will have to do another upload of the upgrade files.
5. If the problem persists, contact Technical Support.

Upload fails

1. Check the following:
   - The IONMM is powered on.
   - The IP address of the TFTP server is correct.
   - The TFTP server is online and available.
   - The correct file name, **db.zip**, is specified (including the .zip extension for Windows XP). If using Windows 7, name the file just "**db**".
   - The **db.zip** file is in the default directory on the TFTP server.
   - The **db.zip** (or **db**) file contains the db.idx file and the upgrade files.
   - The **db.idx** file is formatted correctly ("Creating the Database Index and Archive Files").
2. Wait three minutes then retry the operation. If the operation still fails, continue with step 3.
3. Reboot the IONMM.
4. Retry the upload operation.
5. If the problem persists, contact Technical Support.

USB connection resets after a CLI command is executed

1. If you can connect to the IONMM through the Web interface (see "Starting the Web Interface"), go to step 4 of "Telnet connection is lost after a CLI command is executed".
   If you cannot connect to the IONMM through the Web interface, continue with step 2 below.
2. Check the following:
   - the IONMM is seated properly in the chassis
   - the IONMM is powered up
   - the network cable is seated
   - the network is operational
3. For all modules (slide-in and remote) check the following:
   - the module is properly seated/connected
   - the module is powered up
4. Cycle power for the module in question.
5. If the problem persists, contact Technical Support.

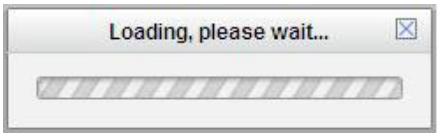
Configuration Mode Mismatch

On the device **MAIN** tab, in the **System Configuration** section in the **Configuration Mode** box, the mode displayed does not match the hardware setting on the device.

The device may have a jumper or switch that disables software management of the device. When Configuration Mode is **hardware**, the devices take some of the configurations from DIP switches or jumpers on the device. In **software** mode, configuration is controlled by management.

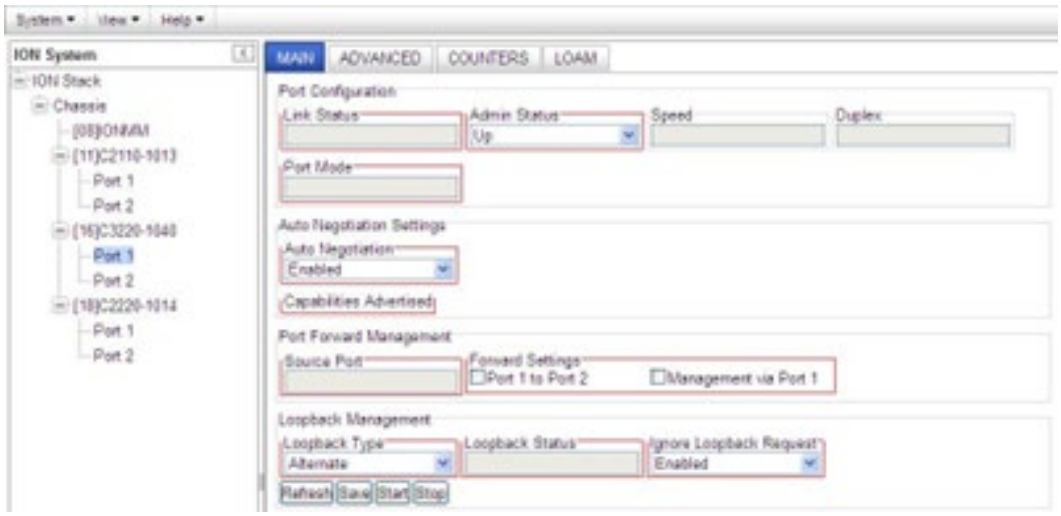
1. Refer to the "DIP Switches and Jumper Settings" section for details on hardware mode configuration.
2. Contact Lantronix for more information.

***Loading, please wait ...* Displays continuously**



1. Wait for one or more minutes for discovery to complete.
2. Click the ☒ icon to close the message.
3. Check the parameter entries and retry the operation.
4. Click the **Refresh** button and try the operation again.
5. If the problem persists, contact Technical Support.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



1. Check if the device is physically connected and powered on.
2. If the "*Getting values failed*" message also displays, refresh the device by clicking the **Refresh** key.
3. Collapse and then expand the ION System tree (i.e., fold and then unfold the "ION Stack" node in the left tree view) to refresh.
4. Cycle power for the x6010 in question.
5. Reboot the x6010 by clicking the **Reboot** key. See the Reboot section. Check if the parameter boxes are again outlined in black and that you can enter parameters.
6. Upgrade the device(s) to the latest software version.
7. If the problem persists, contact Technical Support.

Red Box Condition

When certain operations (e.g., a reboot) are finished, some devices (usually remote devices) will show the error condition of a “red box” around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The ‘red box’ condition occurs while the devices are resetting; this condition can continue several minutes after the reboot. Until the system is ready to be fully managed, certain fields may display within “red boxes”. The “red boxes” will disappear when the system is ready to be fully managed.

1. Wait a couple of minutes for the current operation to complete, and then continue operation.
2. Check the devices’ firmware versions. For example, a NID has only certain items ‘red boxed’. The IONMM in this case is at latest version and shows certain new functions on the GUI, while the NID is at an older version and shows the newer functions as ‘red boxed’. Since the older version of NID does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as ‘red boxed’. Upgrade the devices to the latest software version.
3. Reboot the system. See the “Reboot” section for more information.
4. Contact Lantronix for more information.

TFTP Server Address is empty or invalid!

1. On a device **MAIN** tab, in the **TFTP Settings** section, you clicked the **Save Server Address** button with no TFTP Server Address entered, or with an invalid TFTP Server Address entered.
2. Enter a valid **TFTP Server Address** and click the **Save Server Address** button.

Windows XP Cannot Find Drivers For My Device

This error can occur if the information programmed into the device EEPROM do not match those listed in the INF files for the driver. If they do not match, the driver cannot be installed for that device without either reprogramming the device EEPROM or modifying the INF files.

1. Contact Lantronix for more information.

Windows XP Forces a Reboot after Installing a Device

This problem can occur if an application is accessing a file while the New Hardware Wizard is trying to copy it. This usually occurs with the FTD2XX.DLL file.

1. Select not to restart the computer and then unplug and re-plug the device. This may allow the device to function properly without restarting.
2. Restart the computer to allow the device to work correctly.
3. Contact Lantronix for more information.

Driver Installation Fails and Windows XP Gives Error Code 10

Windows error code 10 indicates a hardware error or failed driver installation. This error may appear if a device has insufficient power to operate correctly (e.g. plugged into a bus powered hub with other devices), or may indicate a more serious hardware problem. Also, it may be indicative of USB root hub drivers being incorrectly installed.

1. Contact Lantronix for more information.

Windows XP Displays an Error and then Terminates Installation

If the following screen is displayed with this message, Windows XP has been configured to block the installation of any drivers that are not WHQL certified.

To successfully install the device, you must change the driver signing options to either warn or ignore to allow the installation to complete.

1. To change the current driver signing setting, in Windows XP, go to “Control Panel\System”, click on the “Hardware” tab and then click “Driver Signing”.
2. Select the desired signing option.

For other USB Driver / OS Messages (Win2K, Vista, Windows 7, Linux, Mac) refer to the separate document with Driver / OS install, uninstall and troubleshooting information.

Kernel panic – not syncing: Aiee, killing interrupt handler!

After a successful CLI command entry, the system crashes and the message displays. For ex-ample:

1. Upgrade to the S6010 bootloader and Uboot was successful.
2. The S6010 Web interface HTTP shows as failed.
3. Log into the USB console, and enter the command **show ip config**. For example:

```
>show ip config
IP management configuration:
IP management state no such object.
>show i
```

4. After entering "**show I**", the system crashes.

A 'kernel panic' is an error from which the OS cannot quickly or easily recover. It applies primarily to Unix-based systems. In other systems, the equivalent of a kernel panic is known as blue screen of death, sad Mac, or bomb. In Windows 3.x, this sort of error was called a 'general protection fault'.

To recover:
1. Check for these kernel panic causes:
   a. An inappropriate attempt by the OS to access or write to memory,
   b. A software bug or malware,
   c. Failure or improper installation of RAM chips, hard disk damage or data corruption, or
   d. A defective microprocessor chip or incompatible device drivers.
2. If the problem persists, contact Technical Support.

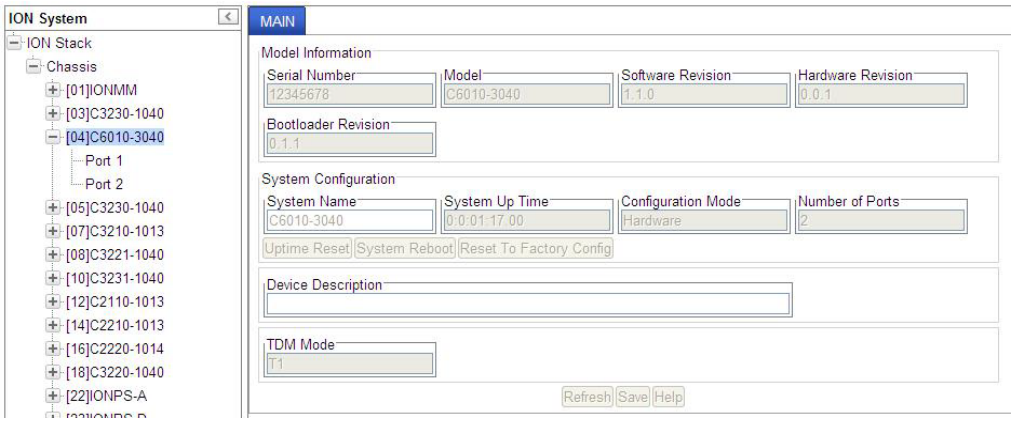
Cannot find new IP address
DHCP issued address is not being displayed
IP Address Wrong

If the DHCP client is enabled on the IONMM **MAIN** page, there is no easy way to determine the new IP address. If DHCP client status set to "enable", the value of "ip address" shows the last IP address, not the current dynamic allocation IP address.

When a "**show ip-mgmt config**" command is entered on the CLI, the previous "fixed" IP address is still returned. If a Fully Qualified Domain Name is used on any of the IONMM pages to access other devices (TFTP, SNTP, or Radius), or to ping another PC, they will fail because of an internal sync problem when getting the IP settings from the ION system when the DHCP client is enabled.

1. Disable the DHCP client and set the DNS server; the problem resolves. (If you enable the DHCP client and then set the DNS servers via the Web interface, this issue may occur due to the internal sync problem noted above).
2. Contact Lantronix for more information.

Cannot make x6010 configuration changes from the Web interface
GUI is not accessible
Web interface screens are all grayed out



With the x6010 in Hardware mode, you cannot make x6010 configuration changes from the Web interface, as the screen fields are all grayed out.

1. Change the x6010 PCB J8 jumper setting. Jumper J8 sets the x6010 PCB's Hardware / Software mode. Use the shorting plug to jumper (short) pins 2 and 3 for Software Mode. See "Jumper Setings".
2. Collapse and then expand the ION System tree (i.e., fold and then unfold the "ION Stack" node in the left tree view) to refresh.
3. Select the x6010 again, and continue operation.
4. Use CLI commands for configuration and operation. See "Section 6: Command Line Interface (CLI) Reference".
5. Contact Lantronix for more information.

Discovery not taking place for remote S6xxx device
ION Can't Discover Remote x6xxx
Remote ION x6xxx device does not display
System cannot discover remote ION x6xxx device

The local (chassis-based) C6xxx does not show a connection to the remote S6xxx device.
The ION Chassis view displays the local (chassis-based) C6xxx but when expanded, does not show the remote S6xxx device.

This is sometimes caused by the local and remote ION devices having different firmware versions, or different DIP switch settings.

1. Make sure the remote x6xxx is powered on.
2. Make sure the local and remote S6xxx devices have the same DIP switch settings and jumper settings. If necessary, change DIP switch settings on one or both x6xxx devices so that the local and remote devices match. See "Jumper Settings" and "DIP Switch Settings".
3. Make sure the local and remote S6xxx devices have the same (latest) Firmware versions.
   If necessary, upgrade the firmware version on one or both x6xxx devices so that the local and remote devices match. See "Upgrade the IONMM and/or NID Firmware".
4. Click the **Refresh** button.
5. Contract and then expand the ION Stack tree.
6. Unplug and then re-plug the USB cable at the IONMM.
7. Unplug and then re-plug the Ethernet cable at the IONMM.
8. Log out of the ION system and then log back in.

CLI Messages

The following are messages that may appear during CLI (Command Line Interface) operations.

Ambiguous command

2) This message indicates either a) the input for one of the parameters is incorrect, or b) a hyphen is missing between two parts of the command.

1. Verify the CLI command syntax.
2. Retry the operation.

B. You typed part of a valid CLI command and pressed **Enter** before completing the command syntax. For example, if you type

```
C1|S7|L1D>add v
```

and then press the **Enter** key, the message "*% Ambiguous command.*" Displays.

1. Type the part of the command that failed (**add v** in the example above), type a question mark (**?**), and the press **Enter**. The valid commands that start with the part of the command you initially entered are displayed.
2. Verify the CLI command syntax.
3. Retry the operation.

C. The system was unable to resolve the desired command based on the portion of the command entered. For example, you entered the following: C1|S7|L1D>**set dot1**

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See "Section 6: Command Line Interface (CLI) Reference".
4. If the problem persists, contact Technical Support.

Bad advertisement capability!

This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability command are not valid choices.

1. Verify the command syntax.
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Cannot get link pass through information on this card

This message indicates that a link pass through (LPT) CLI command was entered for an IONMM. CLI commands for LPT operations are only valid for slide-in modules other than the IONMM. For example:

```
C1|S7|L1D>show lpt config
Cannot get link pass through information on this card!
C1|S7|L1D>
```

1. Use the **go** command to change from the IONMM to the specific slide-in module. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Cannot get LOAM configuration on this port!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Cannot get port security on this port!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Command incomplete

This message indicates that not all of the required fields were entered for the CLI command.

1. Verify the command syntax. Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference.
3. If the problem persists, contact Technical Support.

Could not open connection to the host on port 23. Connection failed.

This message indicates that the Telnet server and client are configured for different ports. For Telnet operations the default port is 23.

1. Ensure that the Telnet port is set to 23 for both the server and the client. This will require someone with administrative rights in order to make a change.
2. Add the port number to the Telnet command. Example:

   Telnet <ipaddr> <port#>

3. If the problem persists, contact Technical Support.

Error: this command should be executed on a device

This message indicates that the CLI command was entered for a port and it only applies to a device.

1. Use the **go** command to change location of where the command operates. The format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Error: this command should be executed on a port

This message indicates that the CLI command was entered for a card and it is only applicable for a port.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Fail to get MAC address!

This message indicates that communications to the module cannot be established.

1. Verify that the correct hierarchy has been specified in the command (see "Managing Slide-In and Remote Modules Using CLI Commands").
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
6. If the problem persists, contact Technical Support.

Fail to get port type!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the **go** command to change location of where the command operates.
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Failed to set DHCP client state!

This message may indicate a problem in the IONMM DHCP setup / configuration.

1. Verify the operation in the "Assigning a Dynamic IP Address" section of the IONMM User Guide.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Failed to set current time
Failed to set SNTP state!
Failed to set SNTP daylight savings time state!
Failed to set timezone!
Failed to set SNTP server
Failed to set SNTP server!
Failed to set system contact
Failed to set system name
Failed to set system location!

These messages indicate a problem in the IONMM SNTP setup / configuration.

1. Verify the operation in the "Configuring SNTP" section of the IONMM User Guide.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Incomplete location command!
Incomplete location parameters, lack of level1 attachment port!

This message indicates that one or more parameters for the **go** command are missing. The **go** command was entered to set location parameters, but the module, slot and/or port value(s) were not included in the command string.

The **go** command can operate on a local or remote card/port, and you must give the last parameter to specify the target is a port or device. For example, the input go c=1 s=14 does not include the port parameter, so the CLI module displays "Incomplete location parameters".

1. Verify the command syntax.
2. Re-enter the **go** command and be sure to include all of the location parameters:

```
go[c=CHASSIS][s=SLOT][1ap=L0APORT][2ap=L1APORT](1p=PORT|2p=PORT|3p=PORT|1d|2d|3d)
```

3. If the problem persists, contact Technical Support.

Invalid condition value: xxxx

This message indicates that the input for the value= parameter on the command in not valid.

1. Verify the value being input; it must match with the value input for **type**=.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid location parameters, cannot find the physical entity!

This message indicates that the system cannot detect the presence of the device or port specified in the **go** command.

1. Verify that the correct hierarchy has been specified in the command (see "Managing Slide-In and Remote Modules Using CLI Commands").
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation.
6. If the problem persists, contact Technical Support.

Invalid user!

This message indicates that the specified user is not valid.

1. Verify the user.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Login incorrect

This message indicates that either the login or password entered while trying to establish a USB or Telnet connection is incorrect.

1. Verify the login/password. **Note:** the login and password are case sensitive. The default login is **ION** and the default password is **private**.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

No DMI support on this port!

This message indicates that you entered a DMI command for a port that does not support DMI.

1. Verify that the port and SFP support DMI. For Lantronix NIDs and SFPs, the model number will have a “D” at the end.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

There is no matched command

This message indicates that there is no such command available on this system.

1. Verify the command syntax.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Unable to open xx. Please check your port settings.

This message indicates that HyperTerminal no longer recognizes which COM port to use for its connection.

1. Check that the USB cable is connected to the management station and the IONMM or NID.
2. Check that the COM port is listed for the device manager on the management station.
   a) On the desktop, right-click on **My Computer**.
   b) Select **Manage**.
   c) Click **Device Manager**.
   d) In the right panel, expand the list for **Ports** (**COM & LPT)**.
3. Is the COM port in the list?

Yes	**No**
Continue with step 4.	Restart the Management station (PC).

4. In the HyperTerminal window, select **File>Properties**.
5. Check that the correct port is listed in the **Connect using** field.
6. Restart the Management station (PC).
7. Reboot the IONMM or NID.
8. If the problem persists, contact Technical Support.

Error, you should first give full location parameters

The location value is incomplete; it is missing the module, slot and/or port value(s). This message can display when a device-level command is entered (e.g., **show lpt config**).

When you change a bigger container, the value of smaller object is cleared. For example, originally the operated object is Chassis=1, slot=4, L1AP=1 L2AP=2 L3D, and then when the command chassis 3 is entered. This automatically sets the value of module, slot and port to 0.

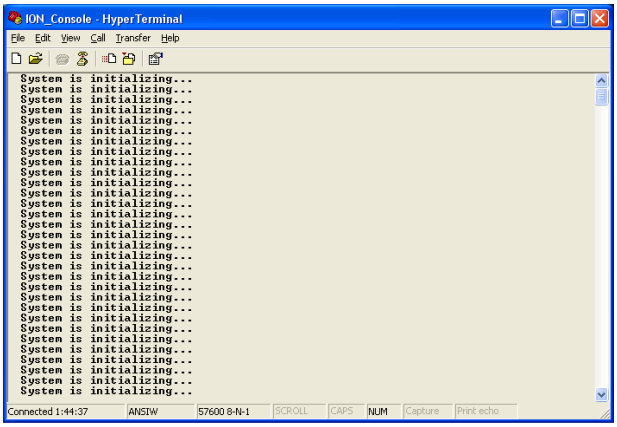
If the value of module, slot and port are not set in later commands, and then you run a device-level command (e.g., **show lpt config**), this error message displays.

Enter the **go** command and be sure to include all of the location parameters.

Go[c=CHASSIS][s=SLOT][l1ap=L0APORT][l2ap=L1APORT](l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)

System is initializing...

CLI is receiving continuous error message "*system is initializing...*"



1. Wait for a few minutes for the message to clear.
2. Cycle power to the IONMM.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

This command is only available on <x6010> card!

1. Verify the command entered is the one you want.
2. Verify that the device for the command entered can support the function of the command (e.g., SOAM functions / commands are only supported by model S323x / C323x NIDs).
3. Retry the operation (e.g., type **show soam port** and press **Enter**).
4. If the problem persists, contact Technical Support.

Error: this command should be executed on a device!

1. Verify the command entered is the one you want.
2. Change to the device level; enter the **home** command, or enter the **go** command with all of the location parameters (chassis / slot / port).
3. Retry the operation from the device level prompt (***S6010>***).
4. If the problem persists, contact Technical Support.

Error: this command should be executed on a port!

1. Verify the command entered is the one you want.
2. Change to the desired port; enter the **go** command with all of the location parameters (chassis / slot / port).
3. Retry the operation from the port (i.e., type **show fwd portlist** and press **Enter**).
4. If the problem persists, contact Technical Support.

Unknown command!

The command you entered is not supported, or you entered the wrong command format / syntax.

1. Verify the CLI command syntax.
2. Retry the operation.
3. See "Section 6: Command Line Interface (CLI) Reference".
4. If the problem persists, contact Technical Support.

There is no matched command.

The command you entered is not supported, or you entered the wrong command format / syntax.

1. Verify the CLI command syntax.
2. Retry the operation.
3. See "Section 6: Command Line Interface (CLI) Reference".
4. If the problem persists, contact Technical Support.

Error location parameter number!

The **go** command you entered had an invalid or missing parameter.

1. Enter the **go** command with all of the location parameters (chassis / slot / port) in the format:

   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)

tftp get: set address type failed.
Tftp put failed.
Tftp transfer failed!

1. The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.
2. Verify the CLI command syntax.
3. Verify the firmware version.
4. Be sure the TFTP server is configured and running.
5. Check that the remotefile is in the proper location (e.g., the file *x6010.bin.0.5.4* is at *C:\TFTP-Root*).
6. Retry the operation. See the **tftp upgrade** command in "Section 6: Command Line Interface (CLI) Reference".
7. If the problem persists, contact Technical Support.

Fail to transfer the file!

The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., **tftp get** or **tftp put** or **tftp transfer**).

1. Check the command syntax. See "TFTP Commands" page.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support.

Redundancy is not supported on this card!

The attempt to set or show fiber redundancy failed. For example, you entered the command **show redundancy info**, but the device does not support fiber redundancy.

1. Verify that the NID you entered the command on supports this function (must have at least 2 fiber ports).
2. Retry the operation on a card that supports this function. See the "Fiber Redundancy Commands" section.
3. If the problem persists, contact Technical Support.

Invalid user!

You entered a show command, but specified the wrong user (e.g., you typed **admin** instead of **root**).

1. Retry the operation using the correct user information.
2. If the problem persists, contact Technical Support.

Upgrade is only supported on IONMM card!

You entered a firmware *upgrade* or firmware *update* command from a device other than the IONMM. For example:

```
C1|S3|L1D>show firmware upgrade result
C1|S3|L1D>show firmware-db update result
C1|S3|L1D>show upgrade firmware file
C1|S3|L1D>update firmware-db file cert
C1|S3|L1D>upgrade module
```

1. Make sure of the command you want to enter. See "Firmware Upgrade Commands".
2. Use the **home** command to go to the IONMM device.
3. Re-enter the firmware upgrade command from the IONMM.
4. If the problem persists, contact Technical Support.

Cannot set bandwidth alloc type on this card!

You entered the command **set bw alloc-type=countAllLayerx** on a card that does not support it. For example:

```
C1|S7|L1P1>set bw alloc-type countAllLayer2
Cannot set bandwidth alloc type on this card!
```

1. Verify if the card supports bandwidth allocation.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands".
4. If the problem persists, contact Technical Support.

Cannot set ingress and egress rate on this card!

You entered the command **set irate=xx erate=xx** on a card that does not support it. For example:

```
C1|S7|L1P1>set irate noLimit erate noLimit
Cannot set ingress and egress rate on this card!
```

1. Verify if the card supports rate limiting. Try the syntax **set irate=unLimit erate=unLimit**.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands".
4. If the problem persists, contact Technical Support.

DMI is only supported on FIBER port!

You entered the command **show dmi info** on a card that does not support it. For example:

```
C1|S7|L1P1>show dmi info
DMI is only supported on FIBER port!
```

1. Verify if the card supports DMI.
2. Use the **go** command to switch to a different card port supporting Fiber.
3. Verify the command entry. See "DMI Commands" .
4. If the problem persists, contact Technical Support.

Link OAM is not supported on this card!

You entered the command **show loam rx loopback control** on a card that does not support it. For example:

```
C1|S7|L1P1>show loam rx loopback control
Link OAM is not supported on this card!
```

1. Verify if the card supports loopback.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. See "LOAM Commands".
4. If the problem persists, contact Technical Support.

Cannot clear loopback counters on this card!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set autocross on this card!
Cannot set auto negotiation state on this port!
Cannot set Ethernet port speed for this card!
Cannot set Ether port duplex mode on this card!
Cannot set far end fault on this card!
Cannot set filter unknown dest multicast frames on this port!
Cannot set filter unknown dest unicast frames on this port!
Cannot set pause on this port!
Cannot set source address lock action on this port!

You entered a command (e.g., **clear loopback counters**) for a function not supported on the card or port.

1. Verify if the card supports the desired function. See Table 3 in the section "Ethernet Port Commands".
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry.
4. If the problem persists, contact Technical Support.

No Time-domain reflectometer support on this card!
Cannot get port security configuration on this port!
Fail to get MAC control frames statistics!
Fail to get auto-negotiation state!
Cannot show forwarding port list on this card!
Cannot show slot info on this card!
Cannot show USB port state on this card!
Cannot show USB port configure on this card!
Cannot show TP port cable length on this card!
Cannot set management VLAN on this card!
Cannot clear counters on this port!
Cannot reset all ports' counters on this cards!
Cannot set aging time on this card!
Cannot show aging time on this card!

You entered a command for a function not supported on the card. For example:

```
C1|S7|L1P1>clear ether all counters
Cannot clear loopback counters on this card!
```

1. Verify if the card supports the desired function. See Table 3 in the section "Ethernet Port Commands".
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. The command functions may include 1) admin, 2) adv-cap, 3) autocross, 4) autoneg, 5) duplex, 6) fef, 7) filter-unknown-multicast, 8) filter-unknown-unicast, 9) loopback, 10) pause, 11) speed, and 12) src-addr-lock, 13) tdr, 14) ether security config, 15) fwddb, etc.
5. If the problem persists, contact Technical Support.

Fail to get system name!
You entered a command for system information, but the information on the card was not available.
For example:

```
C1|S10|L1D>show card info
Fail to get system name!
```

1. Try entering the **show cardtype** command.
2. Select the **MAIN** tab > **System Configuration** section **> System Name** field, and verify the name and for the device.
3. Use the set system name command to enter the **System Name** information (e.g., **set system name**=NAME).
4. Remove and reset the card.
5. Try the operation again.
6. If the problem persists, contact Technical Support.

Set system name timeout.

You entered a command to define system information, but the information on the card was not accepted.
For example:

```
C1|S10|L1D>set system name C3231
Set system name timeout.
```

1. Use the set system name command to enter the System Name information (e.g., **set system name=NAME**) without any special characters (e.g., without the ! or # or % or & characters).
2. Remove and reseat the card.
3. Try the operation again.
4. Select the **MAIN** tab > **System Configuration** section **> System Name** field, and verify the name and for the device.
5. If the problem persists, contact Technical Support.

System is busy, please retry this command later!

You entered a **show** or **set** command, but the command was not accepted by the system. For example:

```
C1|S10|L1D>show https config
System is busy, please retry this command later!
C1|S10|L1D>
```

1. Wait 1-2 minutes and then retry the command.
2. Reboot the system and then retry the command.
3. If the problem persists, contact Technical Support.

Get HTTPS state no such object.
IP management state no such object.

You entered a **show** or **get** command, but the command was not accepted by the system. For example:

```
C1|S10|L1D>show https config
HTTPS configuration:
Get HTTPS state no such object.

C1|S10|L1D>show ip-mgmt config
IP management configuration:
IP management state no such object.
```

1. Verify that the command is supported.
2. Wait 1-2 minutes and then retry the command.
3. Retry the command with different parameters or use the go command to switch to a device that supports the desired command.
4. If the problem persists, contact Technical Support.

Warning: this command will restart system, connection will be lost and please login again!
Warm start failed.

You entered a **reboot** command, but the reboot was unsuccessful.

1. Wait 1-2 minutes and then retry the command.
2. If the problem persists, contact Technical Support.

4 packets transmitted, 0 packets received, 100% packet loss

The attempted ping command failed. For example:

```
PING 192.168.1.10 (192.168.1.10): 56 data bytes
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

1. Verify the IP address.
2. Check the cable connection.
3. Refer to the **Ping** command section.
4. Retry the command.
5. If the problem persists, contact Technical Support.

Ping command can only be used on management card!

The attempted ping command was not accepted by the system. For example:

```
C1|S5|L1D>ping 192.168.1.30
Ping command can only be used on management card!
```

1. Use the **go** command to switch to the IONMM card.
2. Refer to the **Ping** command section.
3. Retry the command.
4. If the problem persists, contact Technical Support.

Only 100M fiber port can set far end fault!

The attempted far end fault command was not accepted by the system. For example:

```
C1|S16|L1P1>set ether fef enable
Only 100M fiber port can set far end fault!
```

1. Use the **go** command to switch to the 100M fiber port.
2. Re-enter the **fef** command.
3. Use an alternate Ethernet test command in place of the **fef** command.
4. If the problem persists, contact Technical Support.

Cannot set 1000M speed for this card!

You tried to use the **set ether speed** command to set the device's speed to 1000 Mbps (1 Gbps), but the card you entered the command on does not support this speed. For example:

```
C1|S16|L1P1>set ether speed=1000M
Can not set 1000M speed for this card!
C1|S16|L1P1>
```

1. Use the **set ether speed ?** command to determine the card's speed capabilities.
2. Re-enter the **set ether speed= command** with a speed supported by the card.
3. Use another (supported) command, or use the go command to switch to a device that supports this function.
4. If the problem persists, contact Technical Support.

Set Ethernet port loopback type failed.

You tried to use the **set oam loopback type** command to set the device's type of loopback support, but the command was not accepted. For example:

```
C1|S16|L1P1>set oam loopback type=phylayer
Set Ethernet port loopback type failed.
C1|S16|L1P1>
```

1. Verify the command syntax.
2. Use another (supported) command, or use the go command to switch to a device that supports this function.
3. If the problem persists, contact Technical Support.

Cannot show system information on this card!

You entered the **show system information** command from an unsupported device. For example:

```
C1|S22|L1D>show system information
Cannot show system information on this card!
```

1. Try using the **show card info** command.
2. Use the **go** command to switch to a different device (e.g., from the Power Supply to the IONMM or an x6010 card).
3. If the problem persists, contact Technical Support.

L2CP is not supported on this card!

You tried to perform an L2CP function but the device does not support L2CP.

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports L2CP.
3. Try entering the command again. See "Configuring L2CP".
4. If the problem persists, contact Technical Support.

Cannot show circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.
1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports Circuit ID display.
3. Try entering the command again. See "Circuit ID".
4. If the problem persists, contact Technical Support.

Cannot set circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.
1. Verify the Circuit ID parameters. See "Circuit ID".
2. Try entering the command again.
3. If the problem persists, contact Technical Support.

Please reboot the card for the changes to take effect!
You made a change that requires a system reboot in order for the change to take effect. For example:

```
C1|S5|L1D>set snmp traphost svr 1 type ipv4 addr 192.168.1.30
Please reboot the card for the changes to take effect!
C1|S5|L1D>
```

1. Reboot the card. See the "Reboot" section.
2. Continue the operation.
3. If a problem persists, contact Technical Support.

Get DMI identifier no such object.

You entered the CLI command to display DMI information, but it was not available. For example:

```
C1|S3|L1P2>show dmi info
Get DMI identifier no such object.
C1|S3|L1P2>
```

1. Make sure this is the command / function that you wanted.
2. Try entering the command again. See "DMI (Diagnostic Maintenance Interface) Parameters".
3. If a problem persists, contact Technical Support.

Get SNMP version no such object.

You entered the CLI command to display SNMP configuration information, but it was not available. For example:

```
C1|S3|L1D>show snmp config
SNMP configuration:
Get SNMP version no such object.
C1|S3|L1D>
```

1. Make sure this is the command / function that you wanted.
2. Verify the command syntax. See "Configuring SNMP" .
3. For complete command descriptions, see "Command Line Interface (CLI) Reference".
4. Try entering the command again. See "DMI (Diagnostic Maintenance Interface) Parameters".
5. If a problem persists, contact Technical Support.

Fail to set Ethernet port loopback operation, please check if Link OAM admin state of remote peer port is enabled, link status and other issues.

You entered the CLI command to define the type of Ethernet loopback test, but the command failed. For example:

```
C1|S5|L1P2>set oam loopback oper init
Fail to set Ethernet port loopback operation, please check if Link OAM admin state of remote peer port is enabled, link status and other issues.
C1|S5|L1P2>
```

1. Make sure the LOAM admin state of remote peer port is enabled (see "**set loam admin state**" command).
2. Verify the command syntax.
3. Use the **set oam loopback ?** command to display the card's loopback capabilities. For example:

```
C1:S7:L1P1>set oam loopback type ?
 alternate
 noloopback
 remote
```

4. Re-enter the **set oam loopback=** command with a loopback capability supported by the card.
5. Verify the loopback capability with the **show oam loopback capability** command. For example:

```
C1|S5|L1P2>show oam loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P2>
```

6. Use another (supported) command, or use the go command to switch to a device that supports this function.
7. If the problem persists, contact Technical Support.

Cannot set speed on this port!
You entered the CLI command to define the NID port's operating speed, but the command failed. For example:

```
C1|S5|L1P2>set ether speed 100M
Can not set speed on this port!
C1|S5|L1P2>
```

1. Verify the NID supports this speed.
2. Verify the command syntax.
3. Re-enter the **set ether speed=** command with a speed supported by the card.
4. If the problem persists, contact Technical Support.

Fail to set port advertisement capability!

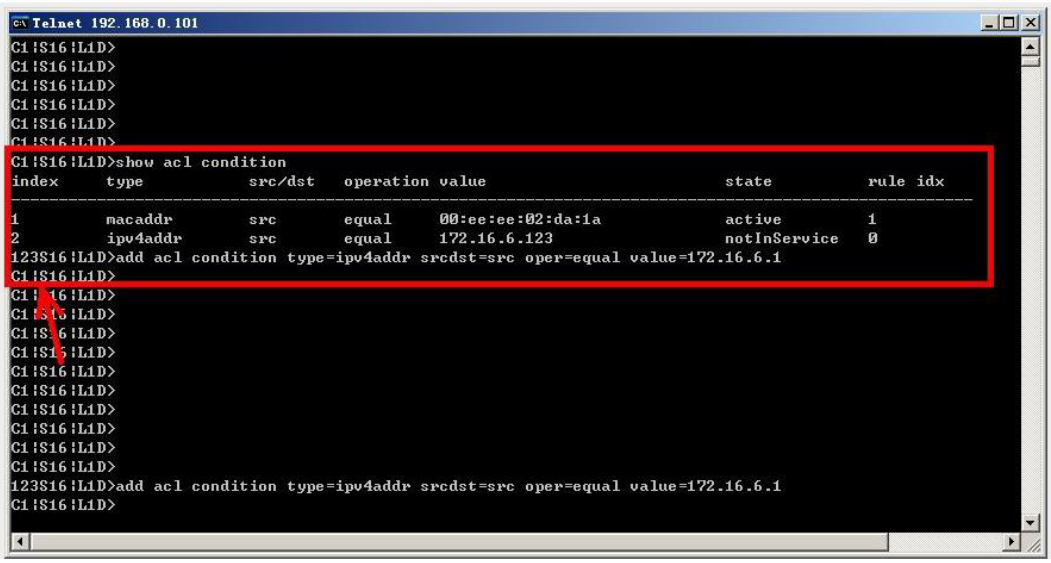
This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability (set ether adv-cap) command are not valid choices. For example:

```
C1|S5|L1P2>set ether adv-cap 1000XFD
C1|S5|L1P2>set ether adv-cap 1000XHD
Fail to set port advertisement capability!
C1|S5|L1P2>
```

1. Verify the x6010 supports this capability.
2. Verify the command syntax.
3. Retry the operation. For a complete list of the available commands, see "Section 6: CLI Reference".
4. Use another (supported) command, or use the go command to switch to a device that supports this function.
5. If the problem persists, contact Technical Support.

Long Command Causes Cursor Wrap to Same Line

When the input command reaches the input max length, the cursor does not return to the next line, but goes back to the beginning of the same line, overwriting the original data.



1. Press the **Enter** key towards the end of the command string and continue entering command text.
2. Try using HyperTerminal or the Web interface, at least temporarily.
3. Contact Lantronix for more information.

Cannot create VLAN database on this card!

This model of NID does not support the VLAN database. For example:

```
C1|S7|L1D>add vlan-db vid 2 priority=5 pri-override=enable
Cannot create VLAN database on this card!
C1|S7|L1D>
```

1. Make sure this is the function that you want.
2. Use the go command to switch to a NID that supports the VLAN database.
3. Re-enter the **add vlan-db** command.
4. If the problem persists, contact Technical Support.

Cannot remove vlan on this card!

You entered a command to delete one or all VLANs from the NID, but the action cannot be performed. For example:

```
C1|S7|L1D>remove vlan all
Cannot remove vlan on this card!
C1|S7|L1D>remove vlan vid=3
Cannot remove vlan on this card!
C1|S7|L1D>
```

1. Make sure this is the function that you want.
2. Use the **go** command to switch to a NID that supports the VLAN database.
3. Use the **add vlan-db** command to add a VLAN VID if needed.
4. If the problem persists, contact Technical Support.

Cannot remove forward database rows on this card!

You entered a command to delete a VLAN forward database VID (forward database row) from the NID, but the action cannot be performed. For example:

```
C1|S7|L1D>remove vlan-db vid 3
Cannot remove forward database rows on this card!
C1|S7|L1D>
```

1. Make sure this is the function that you want.
2. Use the **go** command to switch to a NID that supports the VLAN FDB.
3. If the problem persists, contact Technical Support.

Error: location parameter should be digital number!
You entered a letter or special character as part of the **go** command. For example:

```
C1|S7|L1P2>go c=s s=5 l1d
Error: location parameter should be digital number!
C1|S7|L1P2>
```

1. Re-enter the **go** command with the correct syntax (e.g., change the letter **s** to a number in the example above).
2. Retry the operation. See "Section 6: Command Line Interface (CLI) Reference".
3. If the problem persists, contact Technical Support.

Error: parameter out of range, level1 port-id range is (1 .. 15)!
Error: parameter out of range, level2 port-id range is (1 .. 16)!
Error: parameter out of range, level3 port-id range is (1 .. 16)!
Error: parameter out of range, chassis-id range is (1 .. 16)!
Error: parameter out of range, level1 attachment port-id range is (1 .. 16)!
Error: parameter out of range, level2 attachment port-id range is (1 .. 16)!

You used the **go** command to move to a port, but the command was not accepted. For example:

```
C1 S7 L1D>go l1p=0
Error: parameter out of range, level1 port-id range is (1 .. 15)!
C1 S7 L1D>
```

1. Make sure this is the port that you want. See "Managing Device and Port Hierarchy Using CLI Commands".
2. Re-enter the **go** command.
3. If the problem persists, contact Technical Support.

Cannot show cable length for fiber port!

You entered the command to display the length of the copper cable for a port that does not support it.

1. Make sure the NID supports the **show cable length** command (only for x2110).
2. Verify the command syntax. See the related *User Guide* manual.
3. Type **show ether config** to show the Ethernet port's configuration.
4. If the problem persists, contact Technical Support.

Auto-negotiation is enabled, you can not set port duplex now!

You entered the command to assign a duplex mode, but the command is not functional if Auto-negotiation is currently enabled.

1. Either leave the Auto-negotiation setting and use the current duplex setting, or disable AutoNegotiation and set the Duplex mode as required.
2. Use the **show ether config** command to display the current Auto-negotiation and Duplex settings.
3. If the problem persists, contact Technical Support.

TDM config is not supported on this card!

You entered the command to configure TDM, but the command is not functional on the NID model.

1. Use the **show tdm config** command to display the current config settings.
2. Either use a different (supported) command, or change to another NID card that supports the TDM function.
3. If the problem persists, contact Technical Support.

TDM port config is not supported on this card!

You entered the command to configure TDM, but the command is not functional on the port.

1. Use the **show tdm config** command to display the current config settings.
2. Either use a different (supported) command, or change to another port that supports the TDM function.
3. If the problem persists, contact Technical Support.

Set tdm port loopback operation failed

You enabled the loopback function on both copper and fiber ports at same time, which is not allowed.

1. Make sure the LOAM Admin state for this port is enabled (active). See the **set loam admin state** command.
2. Make sure LOAM is enabled on both ends of the link.
3. Enable the loopback function on either the copper port or the fiber port (but not both ports at the same time).

Set port TAOS Status Failure!

You entered the command to configure TAOS, but the command is not functional on this x6010 port.

1. Use the **show taos config** command to display the current config settings.
2. Either use a different (supported) command, or change to another NID port that supports the TAOS function.
3. If the problem persists, contact Technical Support.

Set AIS format Failure!

You entered the command to configure AIS, but the command is not functional on this x6010 port.

1. Use the **show ais config** command to display the current config settings.
2. Verify the command syntax and re-enter the command to configure AIS
3. Either use a different (supported) command, or change to another NID port that supports the TAOS function.
4. If the problem persists, contact Technical Support.

AIS transmit setting is not supported on this card!

You entered a command to enable or configure AIS, but the device does not support the AIS function. For example:

```
C1|S3|L1D>set ais transmit=enable
AIS transmit setting is not supported on this card!
C1|S3|L1D>
```

1. Verify that this is the command you want. See "TAOS and AIS Commands".
2. Either select another device that supports AIS, or enter another command that this device supports.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

TAOS status setting is not supported on this card!

You entered a command to configure TAOS, but the command is not functional on this NID model.

1. Use the **show taos config** command to display the current config settings.
2. Either use a different (supported) command, or change to another NID card that supports the TAOS function.
3. If the problem persists, contact Technical Support.

Cannot get port security configuration on this port!
Cannot set transparent link pass through on this card!
Cannot show Ethernet statistics on this port!
Can not show ether configure on this card!
IP management is not supported on this card!
No loopback supported on this card!
No Time-domain reflectometer support on this card!
No TDR support on this card!
No loopback supported on this card!
TAOS status setting is not supported on this card!

You entered a command for a function that is not supported on the x6010. For example:

```
C1|S15|L1D>set dhcp state disable
IP management is not supported on this card!
C1|S15|L1D>
```

1. Use a **show *xxxx* config** command to display the current xxxx settings.
2. Try another (supported) command on the x6010. See "Section 6: Command Line Interface (CLI) Reference".
3. Try the failed command on another card that supports the attempted function.
4. If the problem persists, contact Technical Support.

Cannot set if this port can be managed by CPU on this card!
You entered a command to change console access to the device, but the command was rejected. For example:

```
C1|S4|L1AP2|L2P1>set port mgmtaccess enable
Cannot set if this port can be managed by CPU on this card!
C1|S4|L1AP2|L2P1>
```

1. Use a **show *xxxx* config** command to display the current xxxx settings.
2. Try another (supported) command on the x6010. See "Section 6: Command Line Interface (CLI) Reference".
3. Try the failed command on another card that supports the attempted function.
4. If the problem persists, contact Technical Support.

TLPT is not supported if no ethernet port
VLAN is not supported if no ethernet port

You entered a command on a x60xx device that does not support the attempted function.

1. Either use a different (supported) command or change to another NID card that supports the TLPT or VLAN function.
2. If the problem persists, contact Technical Support.

Software version of this card is too old, please upgrade it!
ERROR Software version of this card (1.1.0) is not supported, please upgrade to the same version as the IONMM

You entered a command on a x60xx device that does not support the attempted function.

1. Either use a different (supported) command, or change to another NID card that supports the function.
2. Upgrade the x60xx firmware. See “Upgrade the IONMM and/or NID Firmware”.
3. If the problem persists, contact Technical Support.

Fail to set card entity index!
At one time we can only backup at most 10 cards!
At one time we can only restore at most 10 cards!
Backup finished
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Fail to set card entity index!
Processing...
The MAX provision configure file name is 64!
The specified module does not exist!

You entered a "**prov**" command to do a Backup or Restore function, but a problem was encountered or the process is not yet finished.

1. Wait a few moments for the command to complete and the "*Restore finished*" or "*Backup finished* " message to display.
2. Retry the backup or restore operation with 10 or fewer devices listed.
3. Use the **go** command to switch to the device level of a supported device and re-enter the command.
4. Enter a filename of 64 characters or less in length.
5. Specify an existing module name.
6. If the problem persists, contact Technical Support.

Cannot get dot1bridge state on this port!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set default VLAN id on this port!
Cannot set Ether port duplex mode on this port!
Cannot set pause on this port!
Cannot set VLAN network tagging on this port!
Cannot show VLAN tag config on this port!
Fail to get port type!

You entered a command not supported on the C6120 TP port.

1. Either use a different (supported) command, or change to another NID that supports the desired function.
2. If the problem persists, contact Technical Support.

Error: pattern string is not regular!
Error: this command is not supported on this port!
OID error, module=%d, leaf=%d%s
Set loopback type of the specified TDM port\n
Show TDM information of a specific port\n

You entered a **tdm inband config** command but the command failed.

1. Make sure the TDM configuration is correct. See "Section 6: Command Line Interface (CLI) Reference".
2. Either use a different (supported) command, or change to another NID or port that supports the desired function.
3. If the problem persists, contact Technical Support.

No loopback supported on this card!
No TDM loopback supported on this card!
TDM inband config is not supported on this card!
TDM port config is not supported on this card!

You entered a **tdm inband config** command but the command failed.

1. Make sure the TDM configuration is correct. See "Section 6: Command Line Interface (CLI) Reference".
2. Either use a different (supported) command, or change to another NID that supports the desired function.
3. If the problem persists, contact Technical Support.

Get inband loopback status fail!
Get inband loopback start pattern fail!
Get inband loopback stop pattern fail!

You entered a **show tdm inband config** command but the command failed.

1. Make sure the TDM configuration is correct. See "Section 6: Command Line Interface (CLI) Reference".
2. Either use a different (supported) command, or change to another NID card that supports the desired function.
3. If the problem persists, contact Technical Support.

Get peer inband loopback start pattern fail!
Get peer inband loopback status fail!

You entered a **show tdm peer inband config** command, but the command failed.

1. Make sure the TDM configuration is correct. See "Section 6: Command Line Interface (CLI) Reference". Either use a different (supported) command or change to another NID that supports the desired function.
2. If the problem persists, contact Technical Support.

Set inband loopback start pattern fail!
Set inband loopback stop pattern fail!

You entered a **set tdm inband stop pattern**= command but the command failed.

1. Make sure the TDM configuration is correct. See "Section 6: Command Line Interface (CLI) Reference".
2. Either use a different (supported) command or change to another NID that supports the desired function.
3. If the problem persists, contact Technical Support.

This card is in hardware mode and no setting allowed!

You tried to make a configuration change via the Web interface or the CLI, but the action was rejected. For example:

```
AgentIII C1|S3|L1D>set tdm inband enable
This card is in hardware mode and no setting allowed!
AgentIII C1|S3|L1D>
```

The device may have a jumper or switch that disables software management of the device. When Configuration Mode is hardware, the devices take some of the configurations from DIP switches or jumpers on the device. In software mode, configuration is controlled by management.

1. Make the required changes via DIP switch configuration. See the related section of the manual.
2. Change the Hardware/Software Jumper setting to Software mode.
3. Retry the configuration change via the Web interface or the CLI.
4. Contact Lantronix for more information.

Cannot show slot info on this card!

You entered a "**show slot info**" command on an ION card other than an IONMM card.

1. Enter another (supported) show command on this card or use the "**go**" command to switch to the IONMM.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

ERROR Software version of this card ("cardVersion") is not supported, please upgrade to the same version as the IONMM
Getting card version failed
The failure get template config handler was called.

You attempted a function that is not supported by this version of firmware.

1. Enter another (supported) function at this card's firmware version or use the "**go**" command to switch to another card.
2. Upgrade to a newer firmware version. See "TFTP Transfer / Upgrade Commands" or "Upgrade / Update Firmware Commands".
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Error: this command is not supported on this port!
Error: this command should be executed on a device!
Get AIS Transmit no such object.
Get Channel Alarm Indication Signal no such object.
Get link status no such object.

You entered a command at the wrong level (device or port level), or a command that is not supported by this device or port. For example:

```
AgentIII C1|S3|L1P1>show tdm config
Error: this command should be executed on a device!
AgentIII C1|S3|L1P1>go l1d
AgentIII C1|S3|L1D>show tdm config
Get AIS Transmit no such object.
AgentIII C1|S3|L1D>go l1p=1
AgentIII C1|S3|L1P1>show tdm port config
Get Channel Alarm Indication Signal no such object.
AgentIII C1|S3|L1P1>go l1p=3
AgentIII C1|S3|L1P3>show tdm port config
Get link status no such object.
AgentIII C1|S3|L1P5>go l1p=6
AgentIII C1|S3|L1P6>show tdm port config
Error: this command is not supported on this port!
AgentIII C1|S3|L1P6>
```

1. Make sure this is the command / function that you want.

2. Enter another (supported) function at this card's firmware version, or use the "**go**" command to switch to the appropriate device and/or port.
3. Upgrade to a newer firmware version. See "TFTP Transfer / Upgrade Commands" or "Upgrade / Update Firmware Commands".
4. Retry the operation.
5. If the problem persists, contact Technical Support.

Web Interface Messages

IMPORTANT

For each procedure described below, do each step sequentially as indicated. If the result of a step causes the problem to be corrected, **do not** continue with the other steps in the procedure.

Cannot Ping IONMM Device

1. Check the IONMM and x6010 cabling.
2. Make sure IONMM and x6010 are securely seated.
3. Reset the IONMM.
4. Unplug and then re-plug the USB cable at the IONMM.
5. Unplug and then re-plug the Ethernet cable at the IONMM.
6. If the problem persists, contact Technical Support.

Getting values failed (snmp operation timeout)

This message indicates that you entered an invalid parameter value.

1. Click the **Refresh** button to clear the message.
2. Verify the recent parameter entries. Refer to the related CoH (cursor-over-help) and then revise parameter entries as needed.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Firmware DB operation failed, unzip failed.

This message indicates that the upload of the upgrade file failed.

1. Check that the **db.zip** file was specified in the **Database File Name** field for Windows XP; for Windows 7, specify just "**db**".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid input file

This message displays in the "**Upload Result Reason**" field at **IONMM** > **Upgrade** tab> **Firmware database** sub-tab if the "Firmware File Name" entered had an incorrect filename format.

1. Verify the parameter value entered; see "Upgrading IONMM Firmware – Web Method" for valid input information.
2. Retry the operation with a valid firmware file name (e.g., *IONMM.bin.1.0.5*, or *x6010.bin.1.0.5*).
3. If the problem persists, contact Technical Support.

Invalid input found!

This message indicates that you entered a parameter outside the valid range (e,g, VLAN ID = 0).

1. Verify the parameter value to be entered; check the online Help for valid input information.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid password!

This message indicates that the password entered during sign on is not valid.

1. Sign in using the correct password. The default password is **private**.

   Note: the password is case sensitive. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. If the problem persists, contact Technical Support.

Failed to retrieve DMI info on current port.

You clicked the Device port's DMI tab, but the device does not support DMI. Not all NID models/ports support DMI. The NIDs that support DMI have a "D" at the end of the model number.

1. Verify that the NID supports DMI.
2. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Admin Status: Down (or **Testing)**

In the device's port, at the **MAIN** tab in the **Port Configuration** section, the Admin Status field displays "Down". Typically, if 'Admin Status' is Down, then 'Link Status' is also Down.

The status here is the desired state of the interface. The "Testing" status indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with 'Admin Status' in the Down state. As a result of either explicit management action or per configuration information retained by the managed system, 'Admin Status' is then changed to either the Up or Testing states, or remains in the Down state.

1. Verify the initialization process; see "Section 2: Installation and System Setup".
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization and discovery to take place.
4. If the problem persists, contact Technical Support.

Link Status: Down (or **Testing** or **Dormant,** or **NotPresent)**

This is the current operational state of the interface.

The 'Link Status' Testing state indicates that no operational packets can be passed.

If 'Admin Status' is Down then 'Link Status' likely will be Down.

If 'Admin Status' is changed to Up, then 'Link Status' should change to Up if the interface is ready to transmit and receive network traffic.

'Link Status' should change to Dormant if the interface is waiting for external actions (such as a serial line waiting for an incoming connection);

'Link Status' should remain in the Down state if and only if there is a fault that prevents it from going to the Up state;

'Link Status' should remain in the NotPresent state if the interface has missing (typically, hardware) components.

Link Status: *Down*: The ION system interface is not ready to transmit and receive network traffic due a fault.

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see "Section 2: Installation and System Setup".
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization and discovery to take place.
5. If the problem persists, contact Technical Support.

Link Status: *Dormant*: The ION system interface is waiting for external actions (such as a serial line waiting for an incoming connection).

1. Wait several minutes for initialization and discovery to take place, and then retry the operation.
2. If the problem persists, contact Technical Support.

Link Status: *NotPresent*: the interface has missing components (typically hardware).

1. Verify the ION system installation; see "Section 2: Installation and System Setup".
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

Link Status: *Testing*: The ION system interface can not pass operational packets.

1. Verify that diagnostic tests were run properly and completed successfully.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

Setting values failed (http server error)

This message indicates a configuration entry error (e.g., https).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See "Configuring HTTPS".
3. If the problem persists, contact Technical Support.

Setting values failed (snmp operation error)

This message indicates that the SNMP Configuration entered had an invalid SNMP entry (e.g., an unrecognized Trap Manager address entry).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See the related section of this manual.
3. If the problem persists, contact Technical Support.

TFTP file transferring failed!

This message indicates that a TFTP operation could not be completed.

TFTP for Backup download operation:

1. Verify that:
   a. The correct module(s) has been selected.
   b. The IP address of the TFTP server is correct.
   c. The TFTP server is online and available.
2. Perform a backup of the module(s) for which the download operation was intended. Make sure that the status of the backup operation for each module is "*Success*".
3. Retry the operation.
4. If the problem persists, contact Technical Support.

TFTP for Restore upload operation**:**

1. Check:
   - The IP address of the TFTP server is correct.
   - The TFTP server in online and available.
   - The file to be uploaded is in the default directory on the server.
   - The correct module(s) has been selected.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

TFTP operation failed!

This message indicates that the upload portion of an upgrade operation failed.

1. Check:
   - The IP address of the TFTP server is correct.
   - The TFTP server in online and available.
   - The correct file name is specified ("**db.zip**" for Windows XP or "**db**" for Windows 7).
   - The **db.zip** (or **db**) file is in the default directory on the TFTP server.
2. If the problem persists, contact Technical Support.

There is a problem with this website's security certificate.

This message indicates that the security certificate presented by this website was changed.

1. Click the Continue to this website... selection.
2. See the "Configuring HTTPS" section.
3. If the problem persists, contact Technical Support.

Web UI Management connection Lost

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails.
   The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic.
   The PC can ping to S2220-1013 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support.

Current power status of this slot is off, please turn it on before you reset it!

The reset function only works when the slot power is in the On position to have the unit to reboot/reset.

1. At Chassis > MAIN > Chassis Members click the "On" button in the Power Status column of the device before you click the "Reset" button.
2. If the problem persists, contact Technical Support.

Message: "*Setting values in progress ...*" displays continuously

The message "Setting values in progress ..." displays for over 10 minutes after you set up a VLAN 100, then set Management VLAN to Enabled and clicked Save.

Getting values failed (http server error) then displays.

Loading Template agent_main_view.htm failed displays:

MAIN tab displayed is blank after you close the **Loading ...** dialog box.

Meaning: These messages display after you turn on the Management VLAN function either via the ION Web interface or the CLI. (The CLI command is **set inter vlan state=enable**, and the Web interface is from the IONMM **MAIN** screen in the **Management VLAN Configuration** section, where the **Status** field is set to **Enabled**. In both cases, management control is given to the Management VLAN that you enabled.

Recovery: The recovery (re-gaining control from the CLI or Web interface) is to turn off Management VLAN via the CLI (**set 177nter vlan state=enable**) or via the Web interface (IONMM **MAIN** > **Management VLAN Configuration** > **Status** > **Enabled**).

Message: *The DMI feature is not supported on current port*

Meaning: Not all NID models support DMI. Lantronix NIDs that support DMI have a "D" at the end of the model number. If you click the DMI tab on a NID model that does not support DMI, the message "*The DMI feature is not supported on current port*."

The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.

Recovery: 1. Verify that the device and port support DMI. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information.

2. Switch to a NID / port that supports the DMI feature.

3. Retry the operation.

Message: *priority is empty or invalid*

Meaning: Can't change ACL status to enable, message box show "priority is empty or invalid"

Recovery: 1. Review the ACL entries. See "Configuring an ACL".

3) If the problem persists, contact Technical Support.

Message: *Loading template config file succeeded* displays but the ION Stack node won't expand.

Meaning: Either the loading or the discovery process may be hung up.

Recovery: 1. Click the checkbox to close the "*Loading, please wait ...*" dialog box (if displayed).

2. Contract and expand the ION Stack node again.

3. If the message "*Discovering succeeded*" displays, but the ION Stack node won't expand:

a) Sign out and sign back in to the ION system

b) Cycle power to the ION system.

c) Disconnect and then re-connect the USB cable at the IONMM.

4. If the problem persists, contact Technical Support.

Message: *Getting Records failed (snmp operation timeout)*
Message: *Getting records failed (http server error)*

Meaning: The NID could not find the records associated with the operation attempted.

Recovery: 1.Verify the attempted operation was performed correctly.

4) Retry the operation. See the applicable section (e.g., "Upgrade" section or "Backup and Restore Operations (Provisioning)".

1. Reboot the x6010. See "Reboot".

5) If the problem persists, contact Technical Support.

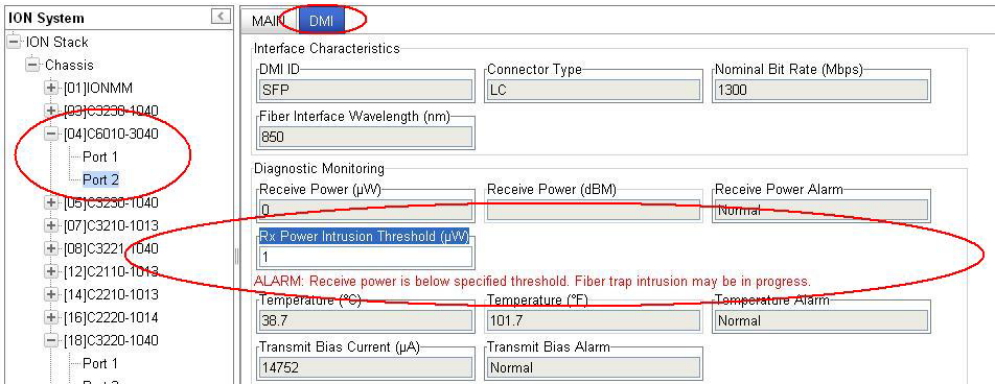
Message: *System initializing or SNMP service busy, please wait...*

Meaning: The system password was accepted, but the system

Recovery: Sign in using the correct password. The default password is private. Note that the password is case sensitive.

1. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. Verify the SNMP configuration.
4. If the problem persists, contact Technical Support.

Message: *ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*



Meaning: At **C6010 > Port 2 > DMI** tab, the Rx Power Intrusion Threshold setting was exceeded. With a preset level for Rx Power on the Fiber port, if the DMI read value falls below this preset value, an intrusion is suspected, and a trap is generated. Fiber optic cables can be vulnerable to tapping, with or without physical intrusion into the optic cable light path.

Either the "Rx Power Intrusion Threshold (µW)" setting is too high, or an optical fiber may have been tapped, which could allow the data stream to be intercepted.

Recovery:

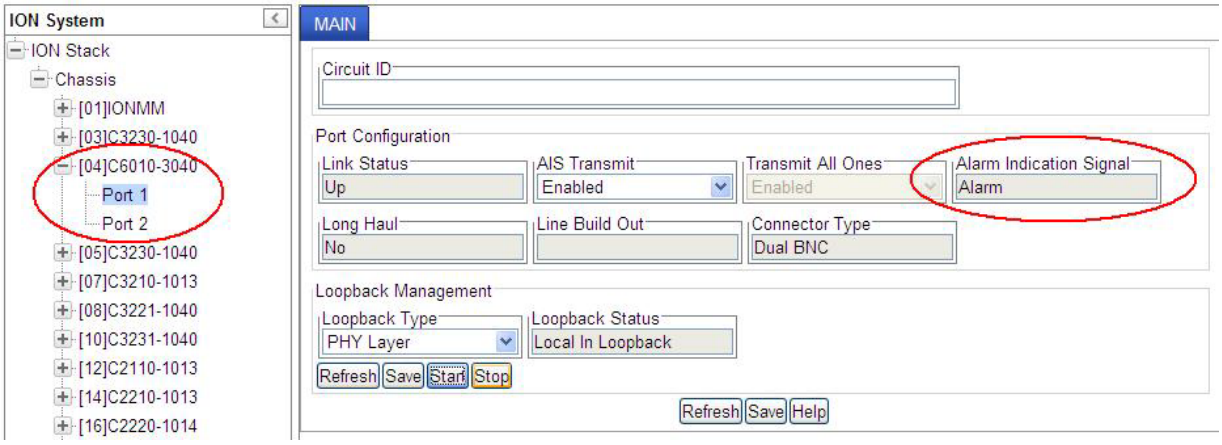
1. Make sure that an intrusion did not cause the alarm; check with your organization's security staff.
2. Change the **Rx Power Intrusion Threshold** setting to a higher value:

   a. From the x6010 Web interface, at **x6010** > **Port x** (SFP) > **DMI** tab, enter a lower threshold setting and click **Save** and then click **Refresh**.

   b. From the x6010 CLI, enter the **set dmi rx-power-preset-level**=xx command where xx is a lower setting, and press the **Enter** key. See "DMI (Diagnostic Maintenance Interface) Parameters".

3. From the CLI, enter the command **reset all ports counters** and press the **Enter** key.
4. If the problem persists, contact Technical Support.

Alarm condition

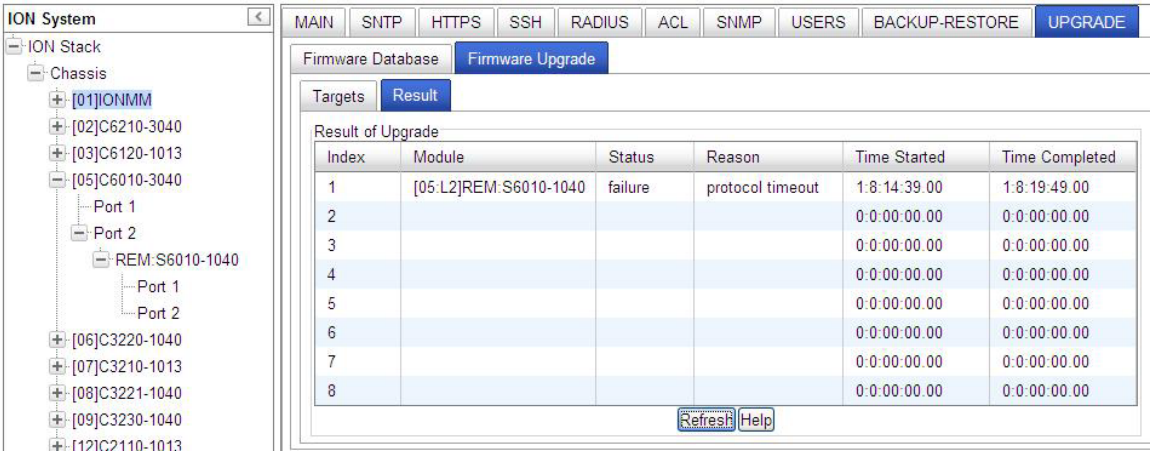


Meaning: The Alarm Indication Signal field displays "Alarm", which means that the other end has TAOS enabled and is currently transmitting an alarm condition.

Recovery:

1. Click the **Refresh** button.
2. Click the **Stop** button.
3. Change the **Loopback Type** selection to **No Loopback** and click the **Save** button.
4. For more information see "AIS (Alarm Indication Signal)".
5. See "Alarm Indication Signal – Alarm Condition".
6. If the problem persists, contact Technical Support.

Message: *Remote S6010 Upgrade failure – protocol timeout*

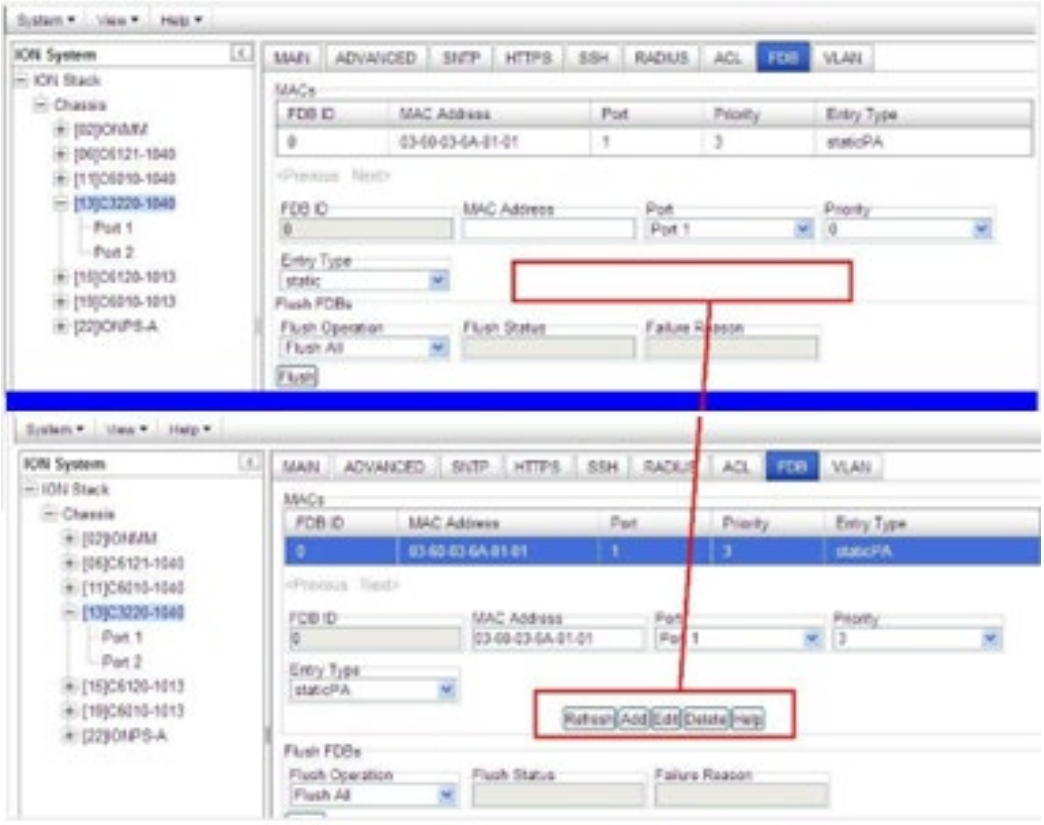


Meaning: At the **IONMM > Upgrade > Firmware Upgrade > Results** subtab, the "protocol timeout" Reason displays with "failure" displayed in the Status column. The probable cause was a temporary line fault.

Recovery:

1. Check the IONMM, C6010, and S6010 cabling and connections.
2. Try the upgrade procedure again.
3. If the problem persists, contact Technical Support.

In IE8 or IE9, the 'Refresh', 'Add', 'Edit', 'Delete', 'Help' buttons of FDB do not display.



6) Select IE8 **Tools** > **Compatibility Mode** to use the IE8 'Compatibility View'. The message "***Compatibility View*** *– 192.168.1.10 is now running in Compatibility View.*' Displays.

2. Log in to the ION system again.
3. Select the **FDB** tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
4. Click one existing MAC address in the MAC address list.

Website displays incorrectly in Internet Explorer 8 or 9

Websites that were designed for earlier versions of Internet Explorer might not display correctly in the current version. However, you can often improve how a website will look in Internet Explorer by using the new 'Compatibility View' feature. When you turn on Compatibility View, the webpage displayed (and any other webpages within the website's domain) will display as if you were using an earlier version of Internet Explorer.

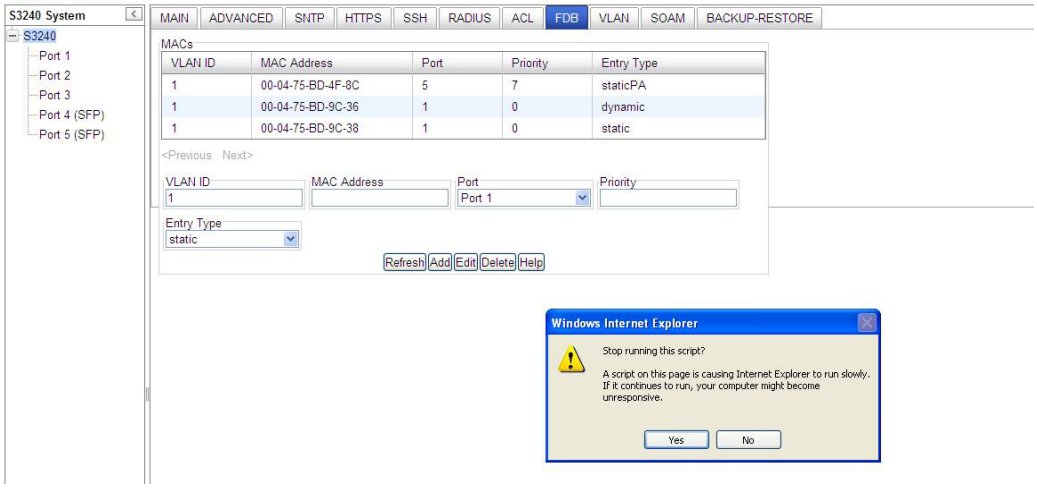
1. In IE8, click the **Stop** button on the right side of the Address bar.
2. If the page has stopped loading, click the **Refresh** button to try again.
3. Click the **Tools** button, and then click **Compatibility View**.

If Internet Explorer recognizes a webpage that is not compatible, the **Compatibility View** button displays on the Address bar. To turn Compatibility View on, click the **Compatibility View** button. From now on, whenever you visit this website, it will be displayed in Compatibility View. However, if the website receives updates to display correctly in the current version of Internet Explorer, Compatibility View will automatically turn off. Note that not all website display problems are caused by browser incompatibility. Interrupted Internet connections, heavy traffic, or website bugs can also affect how a webpage is displayed. To go back to browsing with Internet Explorer 8 on that site, click the **Compatibility View** button again.

4. Check your ION firmware version and upgrade to the latest if outdated. See the "Upgrade" section.
5. Check the Microsoft Support Online website http://support.microsoft.com/ph/807/en-us/#tab0 for more information.
6. See also: http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx
http://support.microsoft.com/kb/960321
http://blogs.msdn.com/b/ie/archive/2008/08/27/introducing-compatibility-view.aspx

7) In IE9, click the **Compatibility View** toolbar button on the Address bar to display the website as if you were using an earlier version of Internet Explorer. See the Microsoft Support website Article ID: 956197 at http://support.microsoft.com/kb/956197.

Script error message received.
Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No
Error: Object doesn't support this property or method.
A Runtime Error has I. Do you wish to Debug?
Done, but with errors on page.

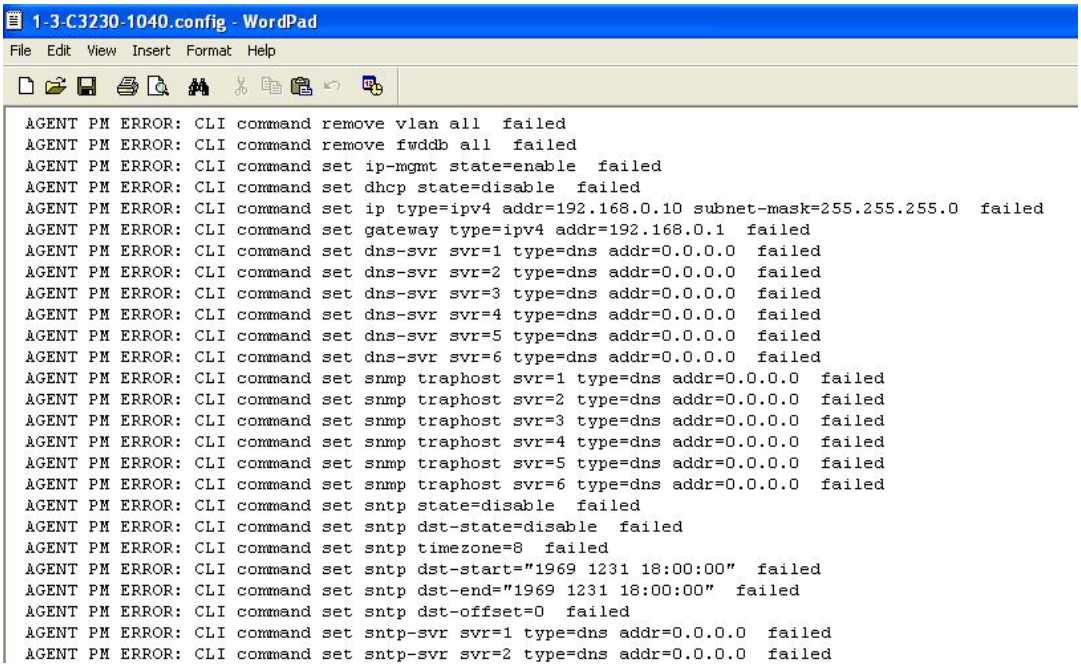


1. Click the **Yes** button to stop the script.
2. Click **Show Details** to display error details.
3. Disable script debugging.
4. Test a Web page from another user account, another browser, and another computer.
5. Verify that Active Scripting, ActiveX, and Java are not being blocked by Internet Explorer.
6. Remove all the temporary Internet-related files.
7. Install the latest Internet Explorer service pack and software updates.
8. For more advanced troubleshooting, see the Microsoft Support Article ID 308260 at http://support.microsoft.com/kb/308260.

The Config Error Log (config.err) File

The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root, with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad or a text editor. The config.err messages are failed web interface functions that were attempted, translated into CLI commands.

A sample portion of an error log file (.ERR file) is shown below.



These messages show a translation of failed web interface functions that were attempted, translated into their equivalent CLI commands.

The config.err files are saved in the TFTP server location specified (typically *C:\TFTP-Root*) with a file name something like: *1-2-2-C3220-1040_20100608.config.err*. Each message is prefixed by the words "*AGENT PM ERROR: CLI command*". The remaining words and phrases are explained below:

1. The first word in the message (e.g., *add*, *set*, *remove*) shows the type of action attempted.
2. The second word or phrase in the message (e.g., *dhcp state, fwddb*, *gateway type*, *vlan-db vid*, etc.) lists the general function attempted. This is the part of the message immediately preceding the = sign.
3. The next word or phrase in the message is the specific function attempted that immediately follows the = sign or the second word of the message (e.g., all, =enable, =disable, =8, =dns addr=0.0.0.0, etc.). This part of the error message may include several segments with = signs (e.g., =0.0.0.0 retry=3 timeout=30.
4. The final word in the message line is the word "failed".

Config.err Messages

Sample config.err file information is provided below.

1-2-2-C3220-1040_20100608.config.err

Line
1 AGENT PM ERROR- CLI command remove vlan all failed
2 AGENT PM ERROR- CLI command remove fwddb all failed
3 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed
4 AGENT PM ERROR- CLI command remove vlan all failed
5 AGENT PM ERROR- CLI command remove fwddb all failed
6 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-02 conn-port=1 priority=1 type=staticNRL failed
7 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-03 conn-port=1 priority=1 type=staticNRL failed
8 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-04 conn-port=1 priority=1 type=staticNRL failed
9 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-05 conn-port=1 priority=1 type=staticNRL failed
10 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-06 conn-port=1 priority=1 type=staticNRL failed
11 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-07 conn-port=1 priority=1 type=staticNRL failed
12 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-08 conn-port=1 priority=1 type=staticNRL failed
13 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-09 conn-port=1 priority=1 type=staticNRL failed
14 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed
15 AGENT PM ERROR- CLI command remove vlan all failed
16 AGENT PM ERROR- CLI command remove fwddb all failed
17 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-02 conn-port=1 priority=1 type=staticNRL failed
18 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-03 conn-port=1 priority=1 type=staticNRL failed
19 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-04 conn-port=1 priority=1 type=staticNRL failed
20 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-05 conn-port=1 priority=1 type=staticNRL failed
21 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-06 conn-port=1 priority=1 type=staticNRL failed
22 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-07 conn-port=1 priority=1 type=staticNRL failed
23 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-08 conn-port=1 priority=1 type=staticNRL failed
24 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-09 conn-port=1 priority=1 type=staticNRL failed
25 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed
26 AGENT PM ERROR- CLI command remove vlan all failed
27 AGENT PM ERROR- CLI command remove fwddb all failed
28 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed

config.err Message Responses

Some typical error log file messages and the recommended responses are provided below (without the prefix of "AGENT PM ERROR: CLI command").

Message: set ip-mgmt state=enable failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related DHCP command in "Section 6: Command Line Interface (CLI) Reference". 4. If the problem persists, contact Technical Support.

Message: set dhcp state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the DHCP operation in the related section of this manual. Retry the DHCP operation. 3. See the related DHCP command in "Section 6: Command Line Interface (CLI) Reference". 4. If the problem persists, contact Technical Support.

Message: set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in "Section 6: Command Line Interface (CLI) Reference". 4. If the problem persists, contact Technical Support.

Message: set gateway type=ipv4 addr=192.168.0.1 failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in *"Section 6: Command Line Interface (CLI) Reference".* 4. If the problem persists, contact Technical Support.

Message: set dns-svr svr=1 type=dns addr=0.0.0.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the DNS Server operation in the related section of this manual. Retry the operation. 3. See the related DNS server command in "Section 6: Command Line Interface (CLI) Reference". 4. If the problem persists, contact Technical Support.

Message: set snmp traphost svr=1 type=dns addr=0.0.0.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in "Section 6: Command Line Interface (CLI) Reference". 4. If the problem persists, contact Technical Support.

Message: set sntp state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference".* 4. If the problem persists, contact Technical Support.

Message: set sntp dst-state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference".* 4. If the problem persists, contact Technical Support.

Message: set sntp timezone=8 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference".* 4. If the problem persists, contact Technical Support.

Message: set sntp dst-start="1969 1231 18:00:00" failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference".* 4. If the problem persists, contact Technical Support.

Message: set sntp dst-end=”1969 1231 18:00:00” failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *“Section 6: Command Line Interface (CLI) Reference”.* 4. If the problem persists, contact Technical Support.

Message: set sntp dst-offset=0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *“Section 6: Command Line Interface (CLI) Reference”.* 4. If the problem persists, contact Technical Support.

Message: set sntp-svr svr=1 type=dns addr=0.0.0.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *“Section 6: Command Line Interface (CLI) Reference”.* 4. If the problem persists, contact Technical Support.

Message: AGENT PM ERROR: CLI command set rfd state=configuration. Failed

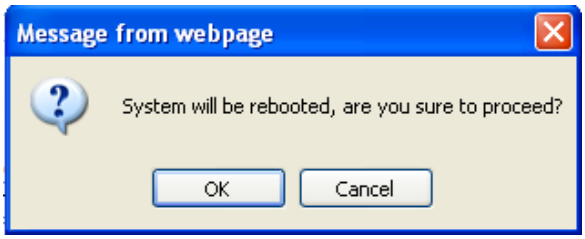
Response: Make sure the RFD (Remote Fault Detect) is enabled. 2. Retry the operation. 3. Restart the system. 4. If the problem persists, contact Technical Support.

Webpage Messages

Certain menu operations will display a webpage verification message to verify that you want to proceed. These messages also provide information on the effect that the operation will have if you continue. These messages display for operations such as **Reset to Factory Config**, **Reboot the System,** or other operational confirmation messages.

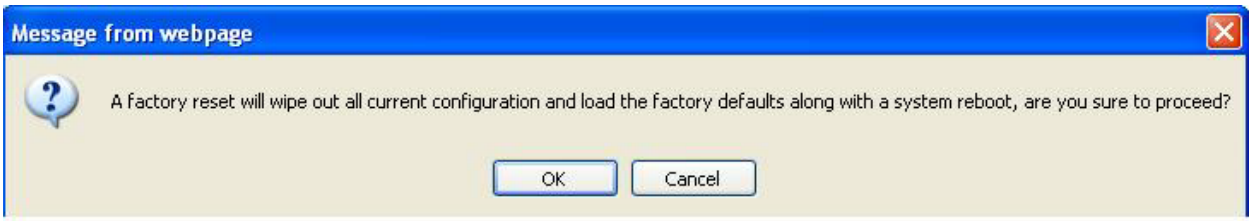
See Menu System Notes for more information.

Message: *System will be rebooted, are you sure to proceed*?



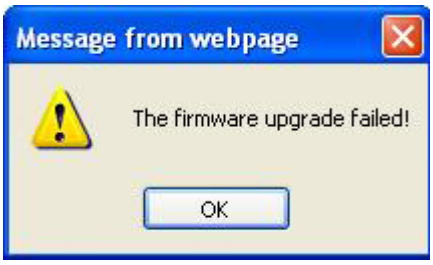
Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

Message: *A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed*?



Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

Message*: The firmware upgrade failed*!



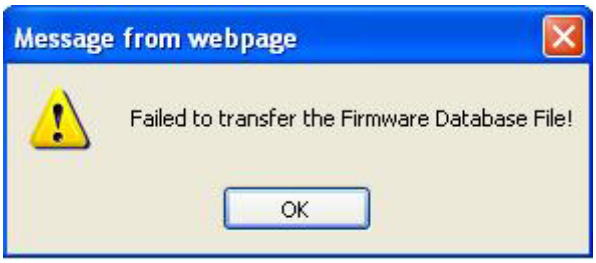
The **MAIN** tab **> TFTP Settings** section **Status** area displays "*TFTP Failure*".

Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the Upgrade the IONMM Firmware section.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Lantronix web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.1.0.5**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.1.0.5 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Make sure that the Management VLAN function is disabled.
8. Reset the device. The **TFTP Settings** section **Status** area should display "*Success*" when done.
9. Check the "TFTP Server Messages" sub-section in the "Third Party Tool Messages" section.
10. If the problem persists, contact Technical Support.

Message*: Failed to Transfer the Firmware Database File*!

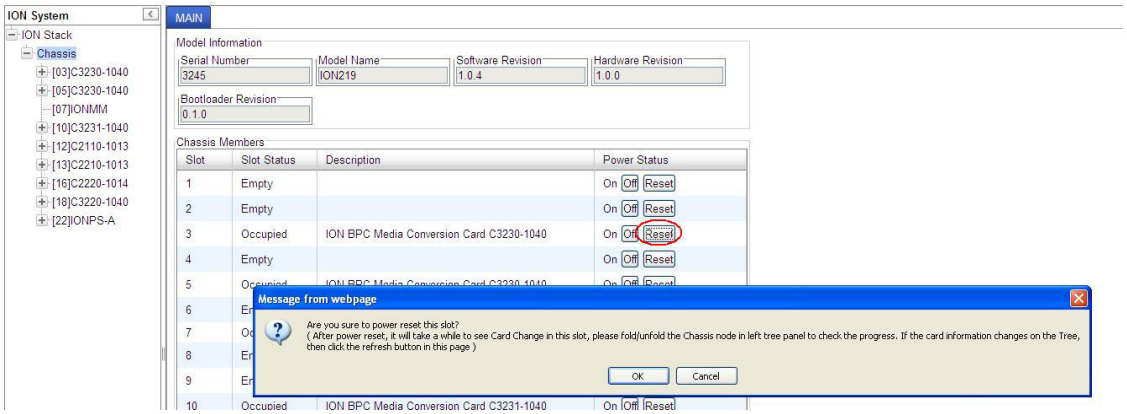


Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the Upgrade the IONMM Firmware section.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Lantronix web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.1.0.5**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.1.0.5 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Reset the device. The **TFTP Settings** section **Status** area should display "*Success*" when done.
8. Check the "TFTP Server Messages" sub-section in the "Third Party Tool Messages" section.
9. If the problem persists, contact Technical Support.

Message: *Are you sure to power reset this slot? (After power reset, it will take a while to see card change in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page*.)

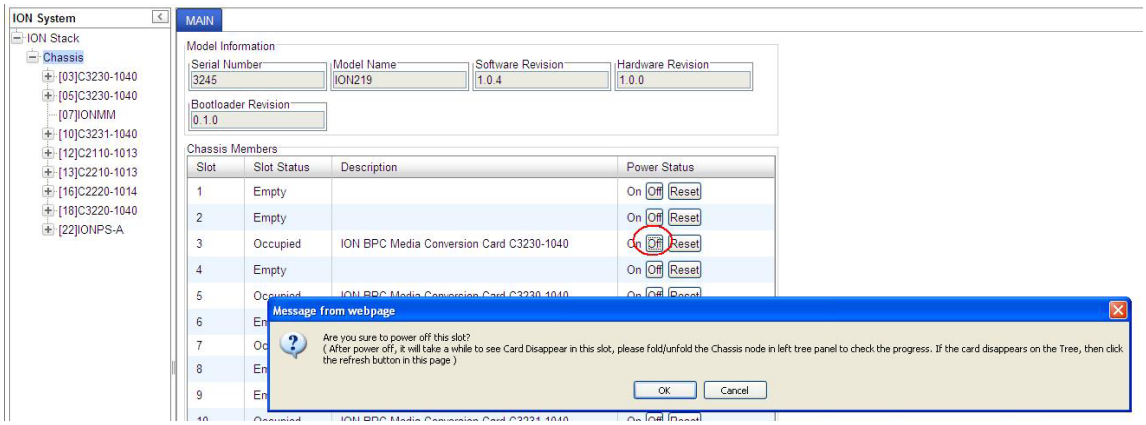


Meaning: A caution message generated at the **Chassis** > **MAIN** tab. You clicked the **Reset** button for a particular slot.

Recovery:

1. If you are not sure that you want to reset this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to reset this chassis, click the **OK** button to clear the message and reset power to the slot.
3. At the **Chassis** > **MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See the "Menu System Notes" section.
6. If the problem persists, contact Technical Support.

Message: *Are you sure you want to power off this slot? (After power off, it will take a while to see Card Disappear in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page*.)



Meaning: A caution message generated at the **Chassis** > **MAIN** tab. You clicked the **Off** button for a particular slot.

Recovery:

1. If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to power off this slot, click the **OK** button to clear the message and remove power to the slot.
3. At the **Chassis** > **MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See the "Menu System Notes" section.
6. If the problem persists, contact Technical Support.

Message: *TFTP file transferring failed!*

Meaning: Either the TFTP Server is not running, or the filename entered was incorrect or not found. See the "Backup/Restore Operations" section.

Recovery: 1. Start the TFTP Server and verify the name and location of the file to be transferred. If the file does not exist (e.g., at *C:\TFTP-Root*), then download the file from the Lantronix website.
2. If the problem persists, contact Technical Support.

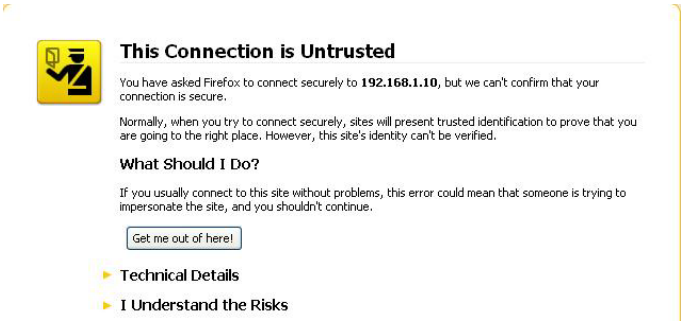
Message: *The Connection was Reset*

Meaning: The Firefox web browser connection failed to load the page.

Recovery:

1. Verify the URL (e.g., *http://* versus *https://*).
2. Check if the applicable server is running (TFTP, Syslog, HTTPS server) in the expected location.
3. Click the **Try again** button to retry the operation.
4. If the problem persists, contact Technical Support.

Message: *This Connection is Untrusted*

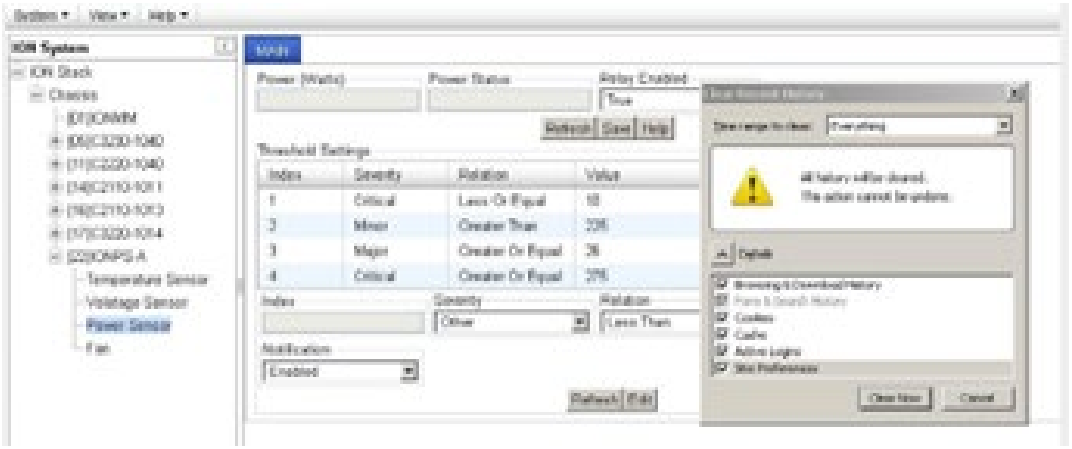


Meaning: You tried to connect via Firefox to a URL, but the Firefox web browser did not find a trusted certificate for that site.

Recovery: 1. Click **Technical Details** for details, or click **I Understand the Risks** to continue operation.

8) If the problem persists, contact Technical Support.

Message: *Clear Recent History*

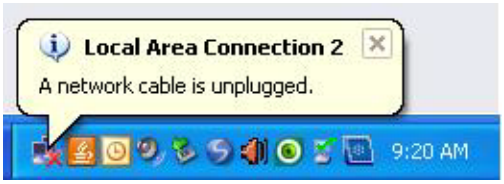


Meaning: You tried to display the Power Supply's temperature, fan, voltage or power sensor sub-menu in the Mozilla Firefox browser.

Recovery:

1. Click **Cancel** / Click **Clear Now** to clear the error dialog.
2. Make sure the latest firmware is running. See "Upgrade the IONMM and/or NID Firmware" on page 93. Upgrade the firmware version if needed.
3. Expand and contract the ION Stack.
4. Retry the operation.
5. If the problem persists, contact Technical Support.

Message: *Local Area Connection x – A network cable is unplugged*

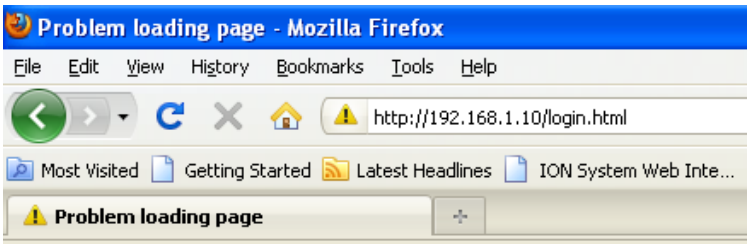


Meaning: You unplugged the USB cable at the NID or IONMM, or the NID or IONMM was unplugged from the ION chassis, or you pressed the **RESET** button on the IONMM.

Recovery:

1. If you pressed the **RESET** button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM's **USB-DEVICE** connector, or plug the USB cable back into the NID's **USB** connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support.

Message: *Problem loading page – Mozilla Firefox*

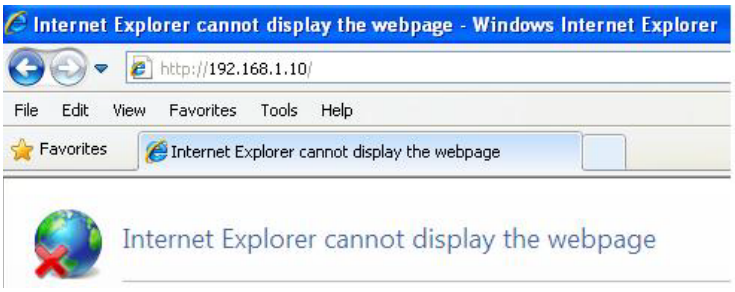


Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See "Web Browsers Supported".
2. Verify the URL entered.
3. Verify NID access. See "Accessing the NIDs".
4. Verify the IP address setting. See "Setting the IP Addressing".
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

Message: *Internet Explorer cannot display webpage*



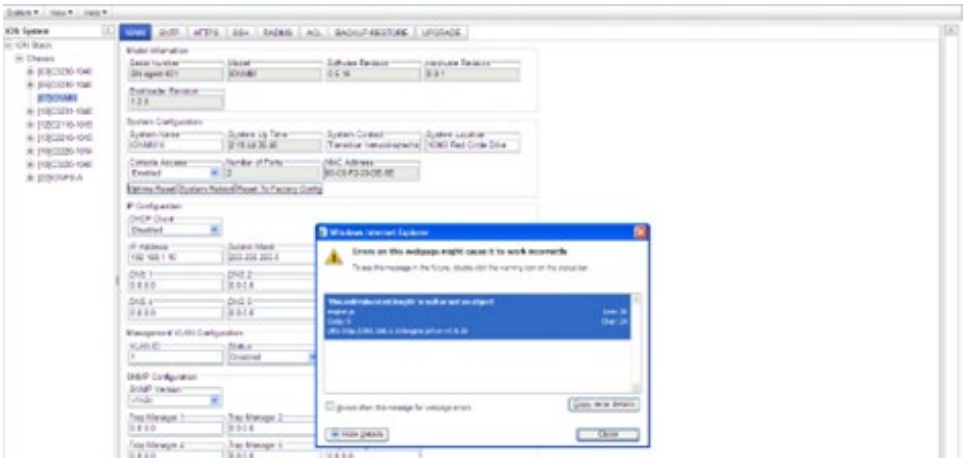
Meaning: You tried to log in to the ION system from IE, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See "Web Browsers Supported".
2. Verify the URL entered (e.g., http:// versus https://).
3. Verify NID access. See "Accessing the NIDs".
4. Verify the IP address setting. See "Setting the IP Addressing" in the IONMM User Guide.
5. Make sure HTTPS, SSH, and/or RADIUS servers are not enabled in the ION system / device configuration.
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

Message: *Error on page.*
Message: *Errors on this webpage might cause it to work incorrectly.*
Message: *'this.mibValuesList.length' is null or not an object*

Meaning: In Windows IE, the message displays in the lower left corner of the screen after some amount of inactivity.



Recovery:
1. On the Windows IE error dialog, click the "**Show details button**".
2. Click the "**Copy error details**" button".
3. Click the "**Webpage error details**" button. Additional error information is copied (like doing a **Ctl-C** keyboard command)
4. Paste the error details text (use **Ctl-V** command) into a text file in Notepad, Wordpad, MS Word, etc., and then save the newly created file. For example:

> User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
> Timestamp: Mon, 6 Dec 2010 14:20:17 UTC
>
> Message: 'this.mibValuesList.length' is null or not an object
> Line: 30
> Char: 24
> Code: 0
> URI: http://192.168.1.10/engine.js?ver=0.5.16

5. Click the **Close** button to close the Windows IE error dialog.
6. Click the ION system **Refresh** button.
7. Retry the operation.
8. If the problem persists, contact Technical Support.

Message: *This webpage is not available.*

Meaning: You tried to display the ION system web interface in Google Chrome, but could not access the webpage. (You tried to log in to the ION system from IE, but the login failed.

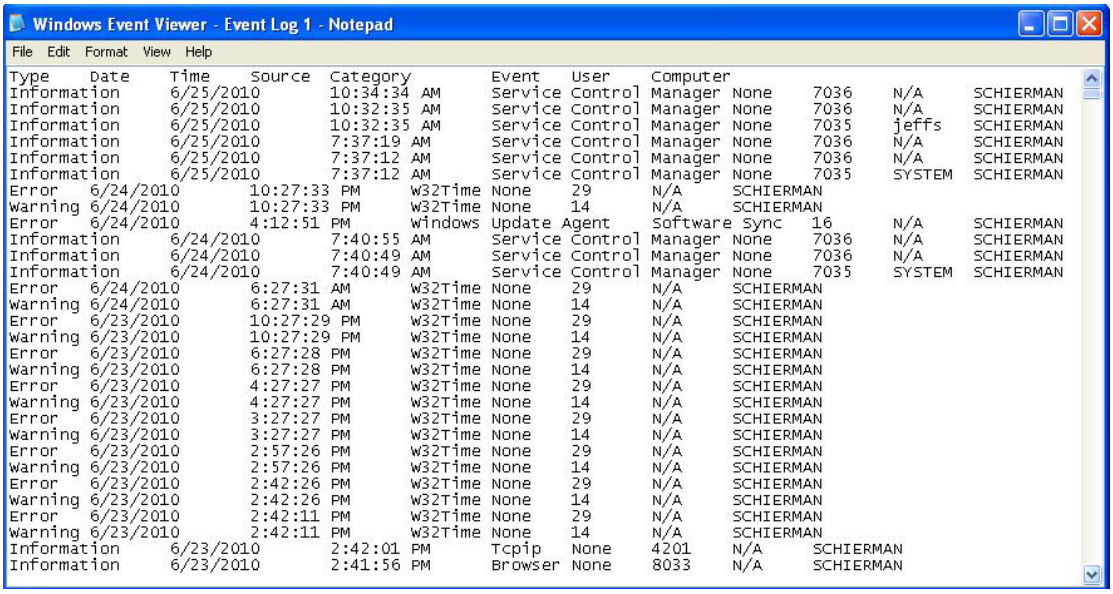
Recovery:

1. Make sure the web browser / version you are using is supported. See "Web Browsers Supported".
2. Verify the URL entered (e.g., http:// versus https://).
3. Verify NID access. See "Accessing the NIDs".
4. Verify the IP address setting. See "Setting the IP Addressing" in the IONMM User Guide.
5. Click on "More information on this error.".
6. Make sure HTTPS, SSH, and/or RADIUS server are not enabled in the ION system / device configuration.
7. Try to log in to the ION system again.
8. If the problem persists, contact Technical Support.

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer – Event Log 1:



Windows Event Viewer - Event Log 1 - Notepad

File Edit Format View Help

Type	Date	Time	Source	Category	Event	User	Computer			
Information	6/25/2010	10:34:34 AM		Service Control Manager	None	7036	N/A	SCHIERMAN		
Information	6/25/2010	10:32:35 AM		Service Control Manager	None	7036	N/A	SCHIERMAN		
Information	6/25/2010	10:32:35 AM		Service Control Manager	None	7035	jeffs	SCHIERMAN		
Information	6/25/2010	7:37:19 AM		Service Control Manager	None	7036	N/A	SCHIERMAN		
Information	6/25/2010	7:37:12 AM		Service Control Manager	None	7036	N/A	SCHIERMAN		
Information	6/25/2010	7:37:12 AM		Service Control Manager	None	7035	SYSTEM	SCHIERMAN		
Error	6/24/2010	10:27:33 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/24/2010	10:27:33 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/24/2010	4:12:51 PM	Windows Update Agent		Software Sync	16	N/A	SCHIERMAN		
Information	6/24/2010	7:40:55 AM		Service Control Manager	None	7036	N/A	SCHIERMAN		
Information	6/24/2010	7:40:49 AM		Service Control Manager	None	7036	N/A	SCHIERMAN		
Information	6/24/2010	7:40:49 AM		Service Control Manager	None	7035	SYSTEM	SCHIERMAN		
Error	6/24/2010	6:27:31 AM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/24/2010	6:27:31 AM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	10:27:29 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	10:27:29 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	6:27:28 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	6:27:28 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	4:27:27 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	4:27:27 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	3:27:27 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	3:27:27 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	2:57:26 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	2:57:26 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	2:42:26 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	2:42:26 PM	W32Time	None	14	N/A	SCHIERMAN			
Error	6/23/2010	2:42:11 PM	W32Time	None	29	N/A	SCHIERMAN			
Warning	6/23/2010	2:42:11 PM	W32Time	None	14	N/A	SCHIERMAN			
Information	6/23/2010	2:42:01 PM	Tcpip	None	4201	N/A	SCHIERMAN			
Information	6/23/2010	2:41:56 PM	Browser	None	8033	N/A	SCHIERMAN			

Message: Information 6/25/2010 7:37:12 AM Service Control Manager None 7035 SYSTEM

Meaning: Information message regarding SCM.

Recovery: No action required.

Message: Error 6/24/2010 10:27:33 PM W32Time None 29 N/A SYSTEM

Meaning: Error level message regarding W32Time.

Recovery: Open the file, examine the number of messages like this, and the potential problem level.

Message: Warning 6/24/2010 10:27:33 PM W32Time None 14 N/A SYSTEM

Meaning: Warning level message regarding W32Time.

Recovery: Check the other system logs for related messages. If the problem persists, contact Technical Support.

ION System Tests

This section describes x6010 DMI and debug functions, PCB configurables, and related test functions.

DMI (Diagnostic Maintenance Interface) Test

The DMI (Diagnostic Maintenance Interface) function displays x6010 diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. You can set the fiber port's "Rx Power Intrusion Threshold" to a setting of 0 to 65,535 uW to meet your organization's intrusion detection requirements.

Note: only certain Lantronix NID and SFP models support DMI. NIDs that support DMI have a "D" at the end of the model number.

DMI can be configured in the NID using either the CLI or Web method.

DMI Config – CLI Method

1. Access the x6010 through either a USB connection (see "Starting a USB Session") or a Telnet session (see "Starting a Telnet Session").
2. Set the Diagnostic Monitoring Interface receive preset power level for a fiber port. Type:

   set dmi rx-power-preset-level=xx

   where: xx is a preset level for Rx Power on the Fiber port, in the range of 1 to 65,535.
3. Press **Enter**. For example: **set dmi rx-preset-power-level=10** and press **Enter**.
4. Display the DMI information. Type: **show dmi info** and press **Enter**. For example:

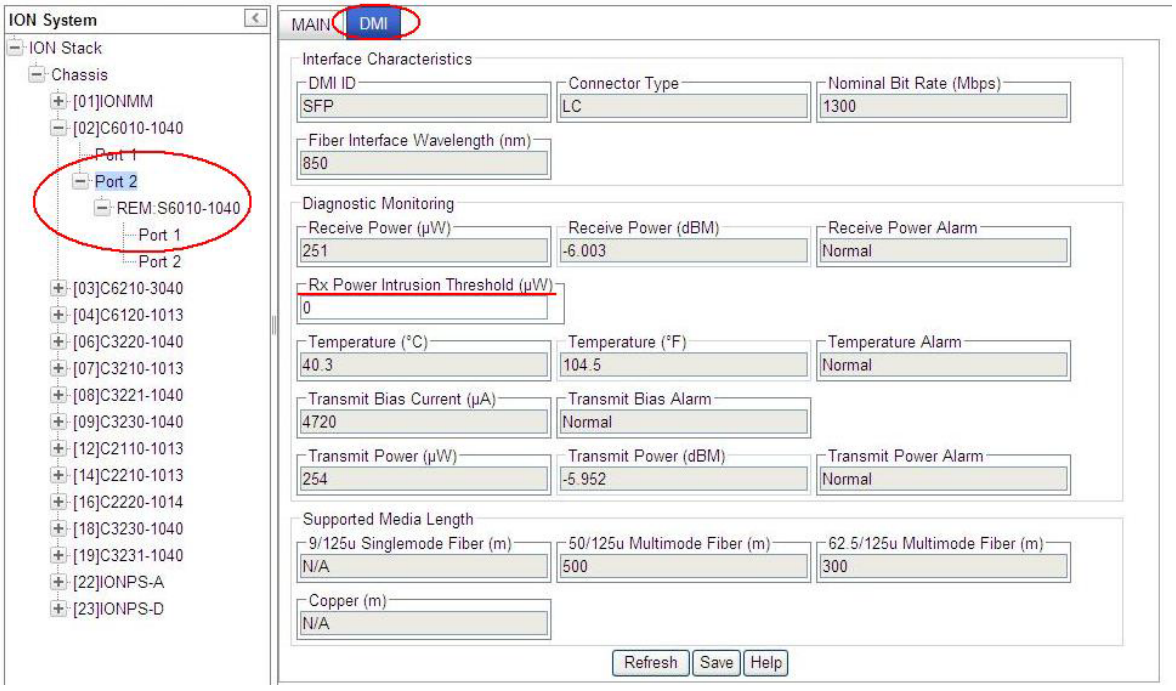
```
Agent III C1|S8|L1P2>set dmi rx-power-preset-level 10
Agent III C1|S8|L1P2>show dmi info
Diagnostic monitoring interface information:
DMI connector type:                     LC
DMI indentifier:                        SFP/SFP+/SFP28
DMI Nominal bit rate:                   1300*Mbps
DMI 9/125u Singlemode Fiber (k):        N/A
DMI 9/125u Singlemode Fiber (m):        N/A
DMI 50/125u Multimode Fiber (m):        500*m
DMI 62.5/125u Multimode Fiber (m):      30*10m
Copper(m):                              N/A
DMI fiber interface wavelength:         850*nm
DMI temperature:                        34.7*C
DMI temperature:                        94.5*F
DMI temperature alarm:                  normal
DMI transmit bias current:              4144*uA
DMI transmit bais alarm:                normal
DMI Transmit power:                     204*uW
DMI Transmit power:                     -6.904*dBM
DMI Transmit power alarm:               normal
DMI Receive power:                      0*uW
DMI Receive power alarm:                normal
Error: Get DMI Vendor name no such object.
Error: Get DMI Vendor Part Number no such object.
Error: Get DMI Vendor serial number no such object.
```

```
Error: Get DMI Vendor revision no such object.
Error: Get DMI Vendor date code no such object.
Error: Get DMI Vendor SFP type no such object.
Error: Get DMI Vendor OUI no such object.
DMI Receive power intrusion threshold:  10*uW
Agent III C1|S8|L1P2>
```

The DMI tab fields are described in Table 14 later in this section.

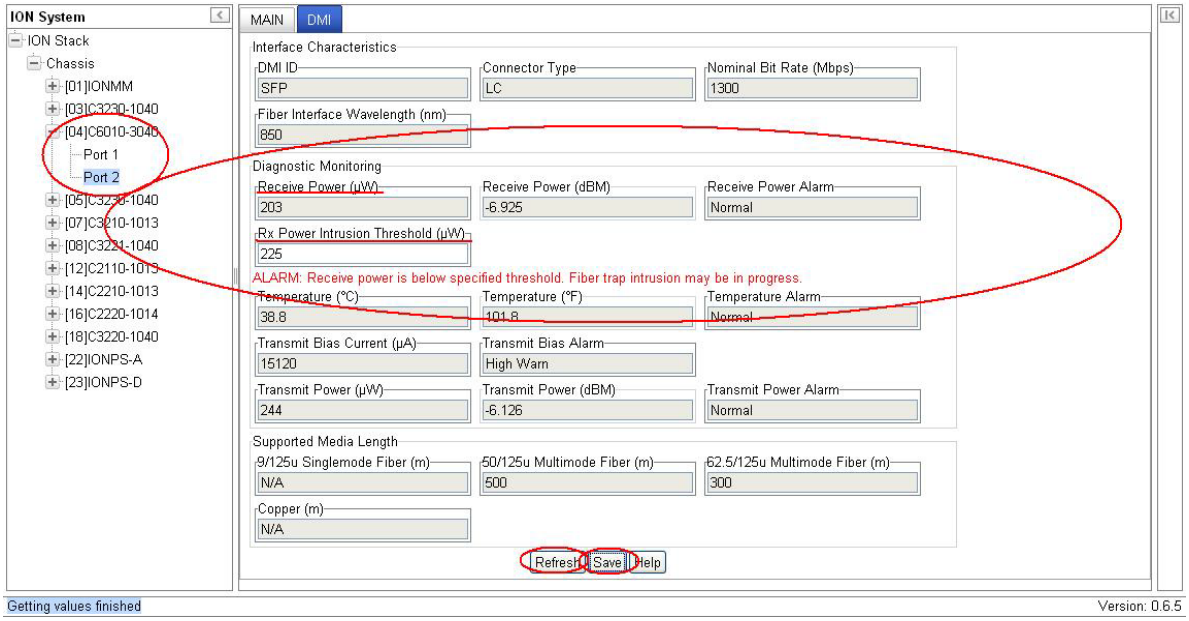
DMI Config – Web Method

1. Access the x6010 through the Web interface (see "Starting the Web Interface").
2. Select the desired device and port.
3. Select the **DMI** tab.



The Interface Characteristics, Diagnostic Monitoring, and Supported Media Length sections display. See the table below for individual field / parameter descriptions.

4. Set the "**Rx Power Intrusion Threshold**" as required. This is a preset level for Rx Power on the Fiber port; if the DMI read value falls below the preset value, a potential intrusion is detected, and a trap is generated. The valid range is 0 – 65535 µW. The default is 0.
5. Click the **Save** button to save any updated information.
6. Click the **Refresh** button to update the information displayed.
7. If the message "*ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*" Displays, follow your organization's process for intrusion detection.



The **DMI** tab parameters are described in the table below.

Table 13: DMI Parameters

Parameter	Possible Values	Description
Interface Characteristics		
DMI ID	Unknown, SFP/SFP+/SFP28, GBIC, SFP, Reserved, vendor-specific	Specifies the physical device from SFF-8472 Rev 9.5 Standard: 00h Unknown or unspecified 01h GBIC 02h Module/connector soldered to motherboard 03h SFP 04-7Fh Reserved 80-FFh Vendor specific
Connector Type	LC, MT-RJ LC, SC, ST, RJ-45, or VF-45, or unknown	The external optical or electrical cable connector provided as the interface. * MT-RJ: Media Termination – Recommended Jack for Duplex multimode connections. * LC: Lucent Connector or Local Connector for High-density connections, SFP transceivers. * SC: Subscriber Connector for Datacomm and Telecomm. * ST: BFOC Straight Tip / Bayonet Fiber Optic Connector for Multimode – rarely Singlemode (APC not possible). * VF-45: Snap connector for Datacom uses. See "Connector Types" section below.
Nominal Bit Rate Mbps)	(measured rate)	Bitrate in units of 100Mbps (the sample screen above shows 1300, or 1.3 Gbps).
Fiber Interface Wavelength (nM)	(measured wavelength)	The Nominal transmitter output wavelength at room temperature. The unit of measure is nanometers (the sample screen above shows 850 nm).
Diagnostic Monitoring		
Receive Power (uW)	(measured power measurement)	Receive power on local fiber measured in microwatts (the sample screen above shows 203 uW).
Receive Power (dBM)	(measured signal strength)	Receive power on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -6.925dBM.
Receive Power Alarm	Normal -1, Not Supported – 2, Low Warn – 3, High Warn – 4, Low Alarm – 6 High Alarm – 7	Alarm status for receive power on local fiber.
Rx Power Intrusion Threshold (uW)	0 – 65535 µW	A configurable level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated. The valid range is 0 – 65535 µW. The default is 0. Displays the message "*ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*" If the value falls below the specified threshold.
Temperature (˚C)	(measured temp.)	Temperature of fiber transceiver in tenths of degrees C (Celsius). The sample screen above shows 38.0˚C.
Temperature (˚F)	(measured temp.)	Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). The sample screen above shows 101.8 ˚F.

Temperature Alarm	Normal -1, Not Supported – 2, Low Warn – 3, High Warn – 4, Low Alarm – 6 High Alarm – 7	Alarm status for temperature of fiber transceiver. An *ionDMITemperatureEvt* event is sent when there is a warning or alarm on DMI temperature
Transmit Bias Current (uA)	(measured current)	Transmit bias current on local fiber interface, in uA (microamperes). The sample screen above shows 15440 uA (microamps).
Transmit Bias Alarm	Normal -1, Not Supported – 2, Low Warn – 3, High Warn – 4, Low Alarm – 6 High Alarm – 7	Alarm status for transmit bias current on local fiber interface.
Transmit Power (uW)	(measured power)	Transmit power on local fiber measured in microwatts. The sample screen above shows 244 uW (microwatts).
Transmit Power (dBM)	(measured power)	Transmit power on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -6.126 dBM.
Transmit Power Alarm	Normal -1, Not Supported – 2, Low Warn – 3, High Warn – 4, Low Alarm – 6 High Alarm – 7	Alarm status for transmit power on local fiber.

Supported Media Length		
9/125u Singlemode Fiber (m)	SM fiber length in meters or N/A	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). The sample screen above shows N/A, indicating the media is not applicable.
50/125u Multimode Fiber (m)	MM fiber length in meters or N/A	Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 500 meters as the supported media length.
62.5/125u MM Fiber (m)	MM fiber length in meters or N/A	Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 300 meters as the supported media length.
Copper (m)	Copper cable length in meters or N/A	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters. The sample screen above shows N/A, indicating the media is not applicable.

Connector Types

The DMI **Connector Type** field indicates the external optical or electrical cable connector provided as the interface. The information below is from SFF 8472 Rev 9.5.

Value	Description of connector
00h	Unknown or unspecified
01h	SC
02h	Fibre Channel Style 1 copper connector
03h	Fibre Channel Style 2 copper connector
04h	BNC/TNC
05h	Fibre Channel coaxial headers
06h	FiberJack
07h	LC
08h	MT-RJ
09h	MU
0Ah	SG
0Bh	Optical pigtail
0C-1Fh	Reserved
20h	HSSDC II
21h	Copper Pigtail
22h-7Fh	Reserved
80-FFh	Vendor specific

The LC, MT-RJ LC, SC, ST, and VF-45 connector types (jacks) are shown below.

ST

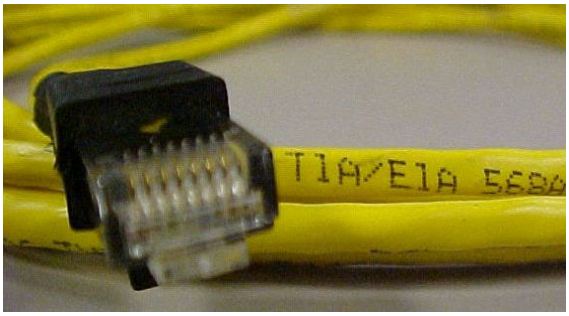
SC

LC

MT-RJ

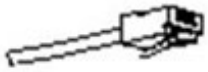
VF-45

A TIA-EIA 568A CAT 5 cable is shown below.

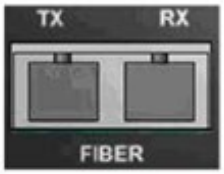


T1/E1/J1 Cable Connectors

Narrowband transmission facilities can be connected with a variety of cable connectors, depending on the type of equipment being installed. The various cable connectors used with narrowband transmission facilities are shown below.



T1 / E1 RJ-45 connector (UTP)
UTP / STP RJ45 copper media connection for shielded twisted pair (STP) or unshielded twisted pair (UTP) media connection.



T1 / E1 SFP connector (Fiber)
FIBER TX / RX: ST, SC or open SFP for fiber media connection.

100-X PORT 2; open SFP for fiber media connection.

T1 often uses DB-15 connectors or RJ-48 connectors if a high density of interfaces is required.

E1 systems commonly use a pair of BNC connectors (one for transmit, one for receive); E1 can also use DB-15 or RJ-48 connectors.

J1 facilities typically use DB-15 connectors.

Set Debug Level

You can use the CLI method to define the system debug level.

1. Access the NID through either a USB connection (see “Starting a USB Session”) or a Telnet session (see “Starting a Telnet Session”).
2. Set the desired debug level. Type:

   set dbg level=<0-2>

   where:

   0=debug Severity level 0 (Emergency: system is unusable – e.g., serious hardware failure or imminent power failure).
   1=debug Severity level 1 (Alert: action must be taken immediately).
   2=debug Severity level 2 (Critical condition).

3. Press **Enter**. For example:

```
C1|S5|L1D>set dbg level 0
C1|S5|L1D>set dbg level 1
C1|S5|L1D>set dbg level 2
C1|S5|L1D>
```

DIP Switches and Jumper Settings

The x6010 NID has on-board components that can be used to configure device operation, typically at the direction of a Lantronix technical support specialist. In most cases, the factory default settings provide optimal configuration settings; however, DIP switch and/or jumper setting changes may be required for operating mode changes or troubleshooting purposes. Multi-position DIP switches allow configuring the x6010 for varying network conditions. Use a small flat blade screwdriver or similar device to change DIP switch settings for on-site configuration.

PCB Identification

This section covers the following PCBs (printed circuit boards):

1. **x6010** SIC – PCB 11354 Rev. 05 (this information is silkscreened at the top center of the PCB).
2. **x6010** NID – PCB 11354 Rev. A (this information is silkscreened at the top center of the PCB).
3. **x6010-10xx** – PCB 11381 Rev. A (this information is silkscreened at the top center of the PCB).

Note: Do not change the configurable items except at the direction of a Lantronix technical support specialist.

C6010 PCB

PCB: 11354 Rev. A (information is silkscreened at the top center of the PCB).

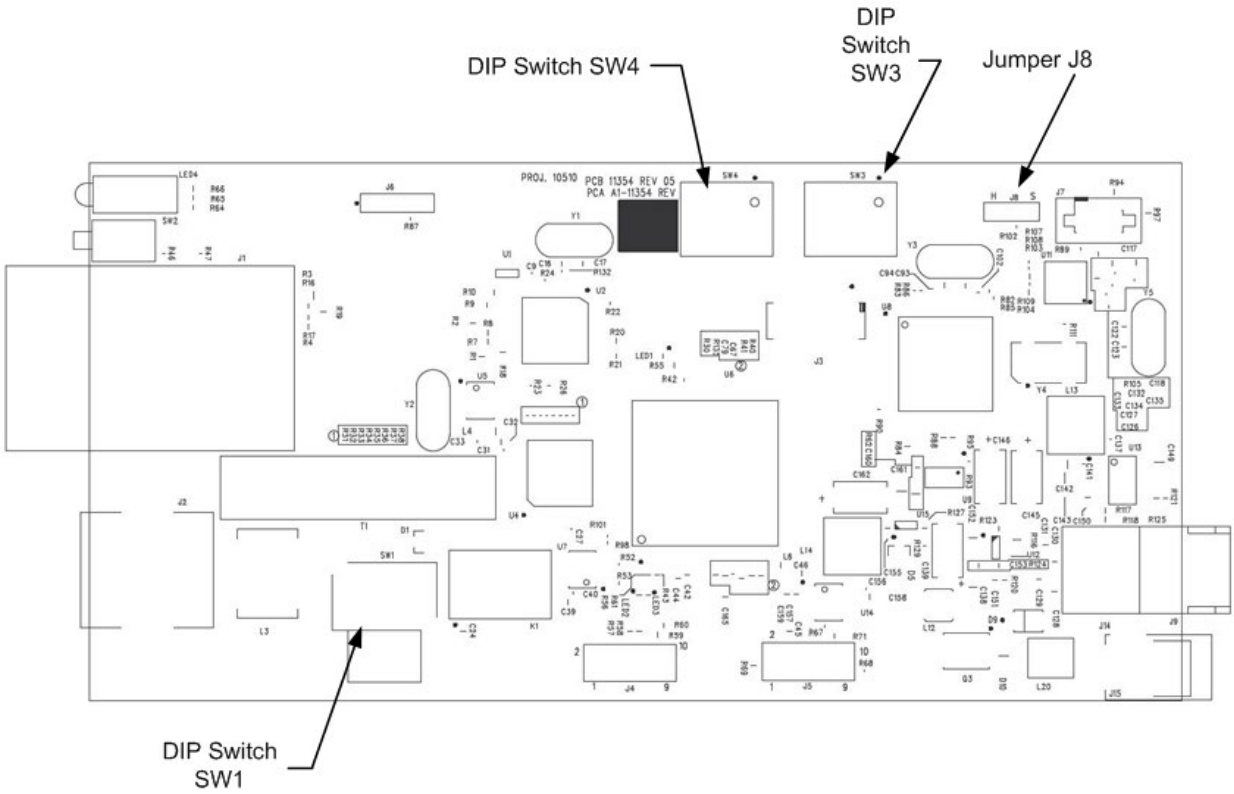


Figure 19: x6010 PCB Layout

S6010 NID Switch Locations

The S6010 configuration information is silkscreened on the top of the NID.

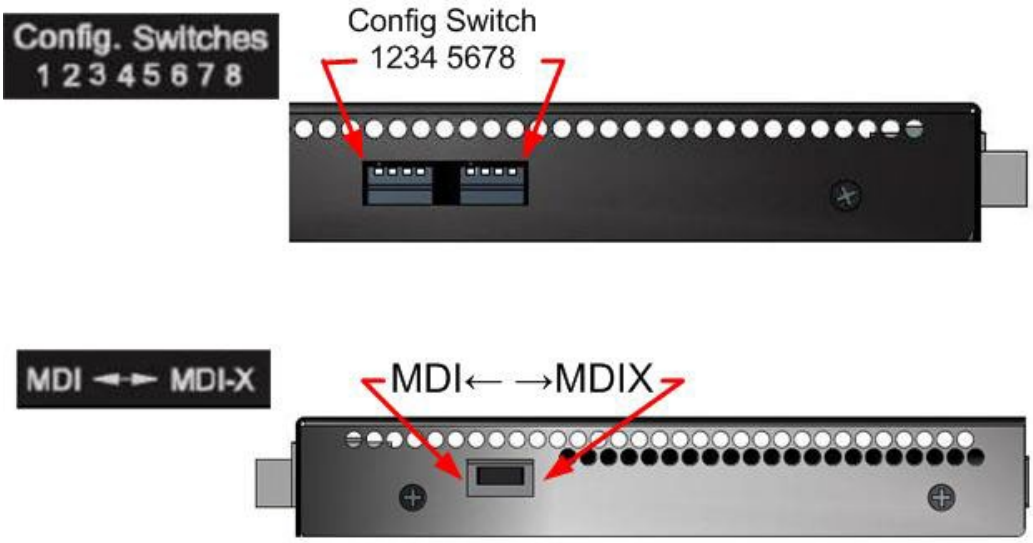


Figure 20: x6010 Switch Locations

DIP Switch SW1 – MDI ← → MDI-x Switch

MDI (Media Dependent Interface) is the standard wiring for end stations, and MDIX (Media Dependent Interface with Crossover) is the standard wiring for hubs and switches. The x6010 device's AutoCross feature makes it possible for hardware to automatically correct errors in cable selection.

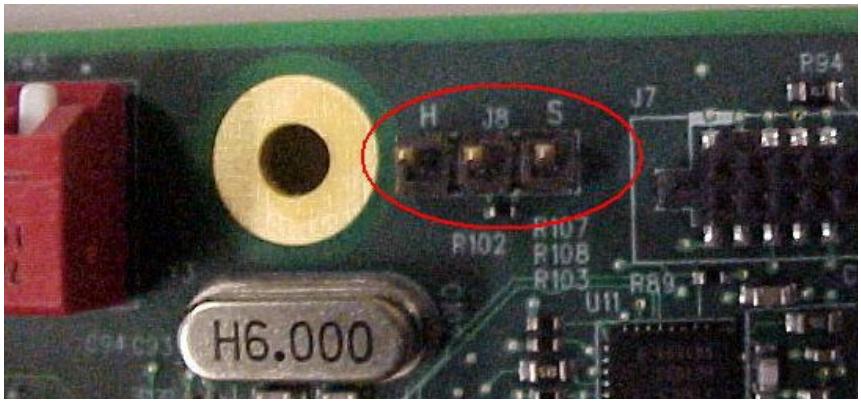
MDI/MDI-X selection for T1/E1 cable:

- MDI (left position): Straight-Through cable.
- MDI-X (right position): Crossover cable.

J8 – HW-SW Mode Jumper

Jumper J8 defines the x6010 Hardware / Software mode setting. Use the shorting plug to jumper (short):

- Pins 1 and 2 for Hardware Mode. In this mode, the hardware defines the x6010 configuration.
- Pins 2 and 3 for Software Mode. In this mode, the software defines the x6010 configuration (the default setting).

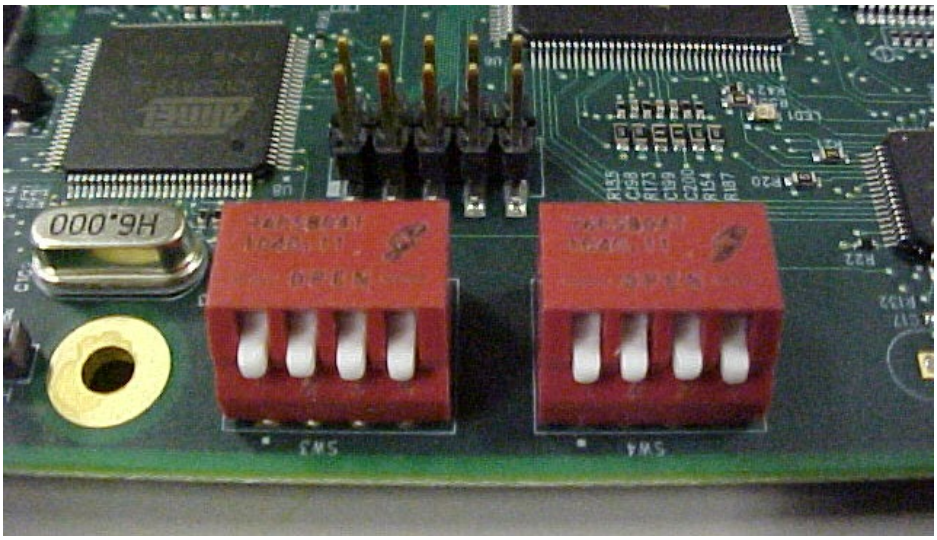


The J8 factory default setting is Software mode (pins 2 and 3 jumpered) as shown above.

Note that in Hardware mode you cannot make x6010 configuration changes from the Web interface, as the screen fields are all grayed out. You can enter CLI commands with the x6010 in Hardware mode.

DIP Switch SW3 – LBO

DIP Switch SW3 defines LBO. The FCC Part 68 Regulation specifies four grades of attenuation with a step of 7.5 dB. Three LBOs are used to implement the pulse attenuation.



DIP Switch SW3 (left) – LBO

SW3-1, SW3-2, SW3-3: Line configuration setting in T1 mode (see "DIP Switch SW4" below)

T1/Short Haul Mode (when SW4-4 = H (Up), SW4-3 = H (Up))

SW3-1, SW3-2, SW3-3: DSX-1 condition

Up, Up, Up: J1 Mode, 110ohm cable (future support);
Up, Up, Down: DSX-1, 162.5-200m,(533-655') 100ohm cable;
Up, Down, Up: DSX-1, 121.6-162.5m (399-533') 100ohm cable;
Up, Down, Down: DSX-1, 81-121.6m (266-399') 100ohm cable;
Down, Up, Up: DSX-1, 40.5-81m (133-266') 100ohm cable;
Down, Up, Down: DSX-1, 0-40.5m (0-133') 100ohm cable;
Down, Down, *X*: Do NOT Care.

T1/Long Haul Mode (when SW4-4 = H (Up), SW4-3 = L (Down))

SW3-1, SW3-2: DS-1 condition

Up, Up: -22.5db 100ohm cable;
Up, Down: -15.0db 100ohm cable;
Down, Up: -7.5db 100ohm cable;
L, L: 0.0db 100ohm cable.

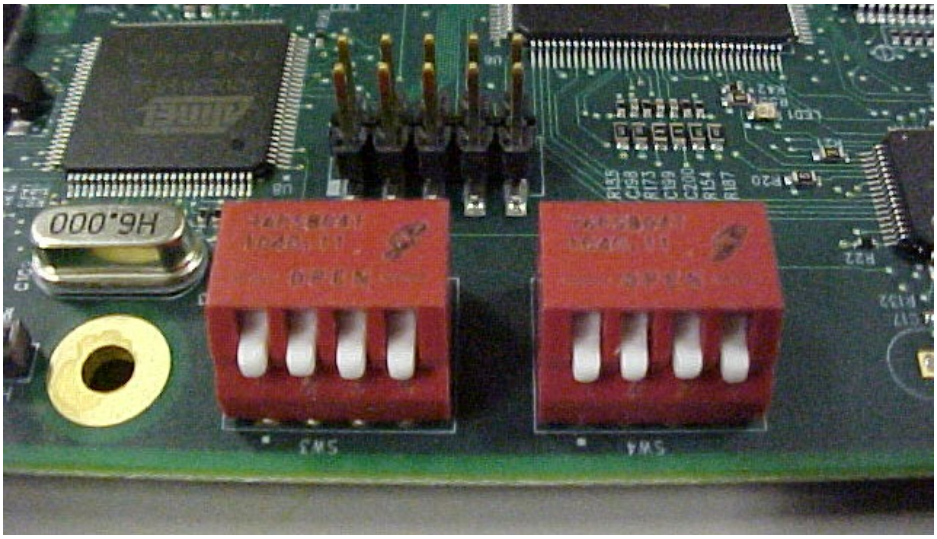
Switch3-4 Inband loopback selection:

Up (H): Disabled
Down (L): Enabled

Note that PCB builds may vary, and that the particular DIP switch used on your PCB may be labeled differently than shown here. The DIP switch labels **UP**, **H**(igh) and **OPEN** typically indicate the same setting, while **Down**, **L**(ow), and **Closed** all indicate the same configuration setting.

DIP Switch SW4 – TAOS – T1-E1 Mode Select

DIP switch SW4 defines TAOS, T1-E1 Mode, T1 Lon/Short Haul, and T1/E1 Mode selection.



DIP Switch SW4 – TAOS (right)

SW4-1 : TAOS on Copper port :
Up = Disable,
Down = Enable;

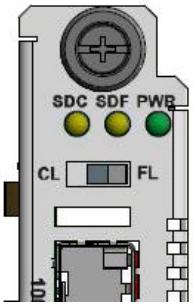
SW4-2: TAOS on fiber port:
Up = Disable,
Down = Enable;

SW4-3: Long haul or Short haul selection; only valid for T1 mode:
Up = Short haul,
Down = Long haul;

SW4-4 : T1/E1 Mode selection :
Up = T1,
Down = E1; in E1 mode, cable configuration is automatically set to 120 ohms.

DIP Switch SW2 – Fiber Loopback Test –Normal - - Copper Loopback Test Mode

DIP Switch SW2 selects between Fiber Loopback test mode, Normal operating mode, and Copper Loopback test mode. The Normal (center) position is the default setting.



SW2 Loopback Switch:

1 – Copper Loopback (**CL**).
2 – Normal Operation (center position). No loopback (default setting).
3 – Fiber Loopback (**FL**). Enable loopback on the local fiber interface.

Jumpers J1, J5, J9, J14, and J15 are not configurable in the field.

X6010-10xx PCB (C6010 with SFP and BNC)

PCB: 11381 Rev. A (information is silkscreened at the top center of the PCB).

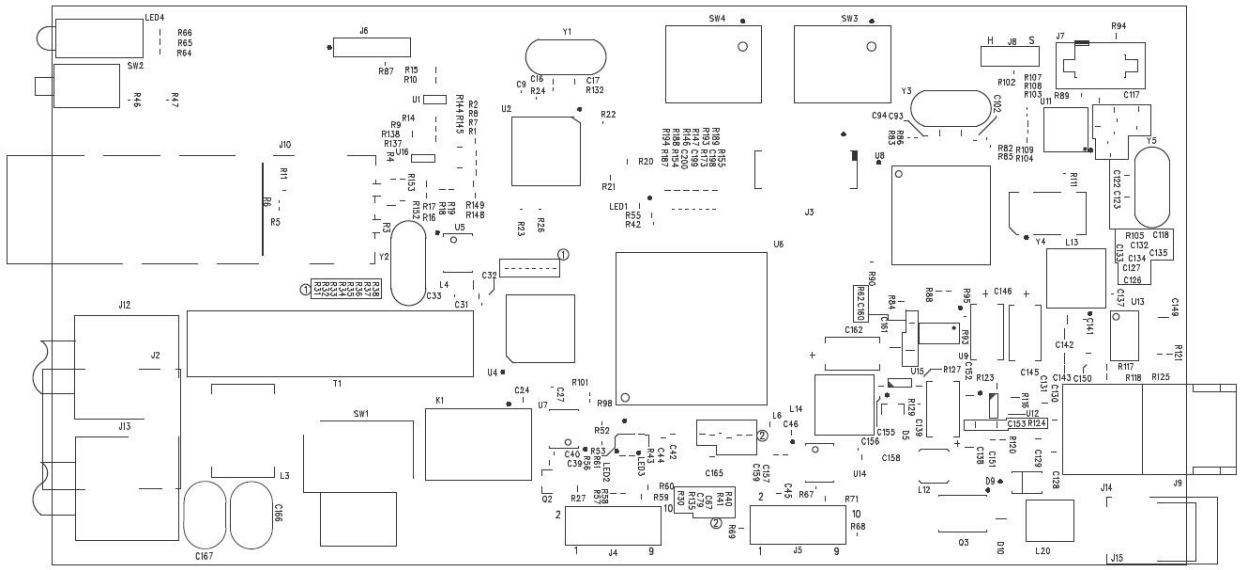


Figure 21: x6010-10xx Layout

Differences from 11354_03: 1. Add BNC connector; 2. Change Fiber connector to SFP; 3. Add R143. See the previous section for DIP switch and Jumper information.

In-band Loopback Code Detect Procedure

This function enables detection and loopback of the fiber interface based on NIU Facility 2 (FAC2) loopback codes. Certain test devices (e.g., T-BERD 2310) can send in-band loopback codes to the local copper (TP) interface, which are then transmitted to the remote device via the fiber. The remote device can detect and react to this and activate and de-activate the loopback codes. For detection, these codes must be sent for at least 5 seconds. Bit 5 loop codes are as follows:

- Loop UP code: 5-bit '11000'
- Loop DOWN code: 5-bit '11100'

The figure below shows data paths after the remote device receives the loop activate code (5-bit 11000) for 5 seconds with SW 3 Switch 3-4 in the DOWN position.

Figure 22: Initiate a Loopback from a Test Set

The Inband Loopback Code Detector can track loopback activate/deactivate codes in a framed or unframed T1/J1 data stream. The received data stream is compared with the target activate/deactivate code whose length and the content are pre-defined. When the received data stream matches the target activate/deactivate code and repeats for 4 seconds, this register field indicates the detection of the inband loopback code.

Register fields IBLBA_S and IBLBD_S: In-band Loopback activate / deactivate code receive (from fiber) status:

0: No Inband Loopback deactivate signal is detected (default0

1: The Inband Loopback deactivate signal is detected and then received over a period of more than 40 ms (T1) or 30ms (E1) with BER < 0.01.

The default setting is 0 (No Inband Loopback deactivate signal is detected).

1. Set DIP Switch SW3 Switch 3-4 (Inband loopback selection) to the Down (L): Enabled position.
2. See the specific test device (e.g., T-BERD 2310) documentation for the procedure to send in-band loopback codes to the local copper (TP) interface.

Third Party Troubleshooting Tools

This section provides information on third party troubleshooting tools for Windows, Linux, etc. Note that this section may provide links to third party web sites. Lantronix is not responsible for any third party web site content or application. The web site information was accurate at the time of publication, but may have changed in the interim.

- Ipconfig and ifconfig
- Windows Network Connections
- Ping
- Telnet
- PuTTy
- Tracert (Traceroute)
- Netstat
- Winipcfg
- Nslookup
- Dr. Watson

Note: IETF RFC 2151 is a good source for information on Internet and TCP/IP tools at ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt.

Ipconfig

Ipconfig (Windows Vista): Use the procedure below to find your IP address, MAC (hardware) address, DHCP server, DNS server and other useful information under Windows Vista.

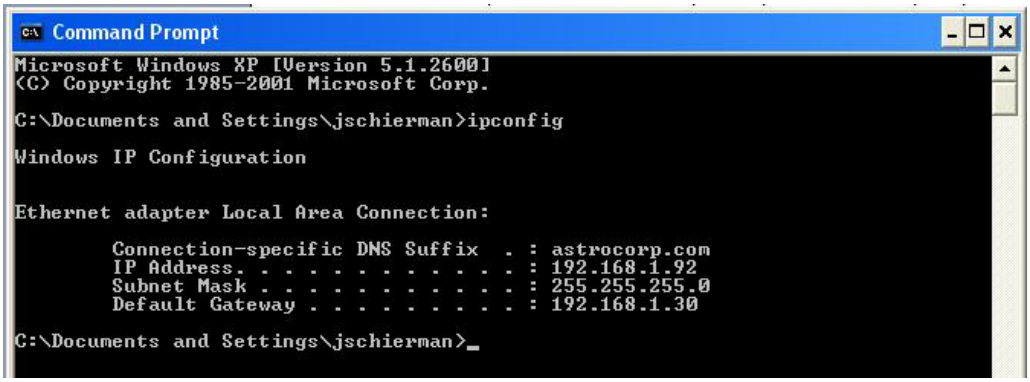
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway display. If your IP address is 192.168.x.x, 10.x.x.x, or 172.16.x.x, then you are receiving an internal IP address from a router or other device.
4. For more detailed information, type **ipconfig /all** at the prompt. Here you can get the same information as **ipconfig** plus your MAC (hardware) address, DNS and DHCP server addresses, IP lease information, etc.

Note: If you are receiving a 169.254.x.x address, this is a Windows address that generally means your network connection is not working properly.

Ipconfig (Windows XP): **ipconfig** (Internet Protocol Configuration) in Windows is a console application that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.

Use the **ipconfig** command to quickly obtain the TCP/IP configuration of a computer.

1. Open a Command Prompt. Click Start, point to Programs, point to Accessories, and then click Command Prompt.
2. Type **ipconfig** and press Enter. The Windows IP Configuration displays:



3. Make sure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
4. For more information, use the /all parameter (type **ipconfig /all** and press **Enter**).

The **ipconfig** command is the command-line equivalent to the **winipcfg** command, which is available in Windows ME, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the **winipcfg** command; however, you can get the equivalent functionality for viewing and renewing an IP address using Windows' Network Connections (see below).

Ifconfig

1. Verify that the machine's interfaces are up and have an IP address using the **ifconfig** command:

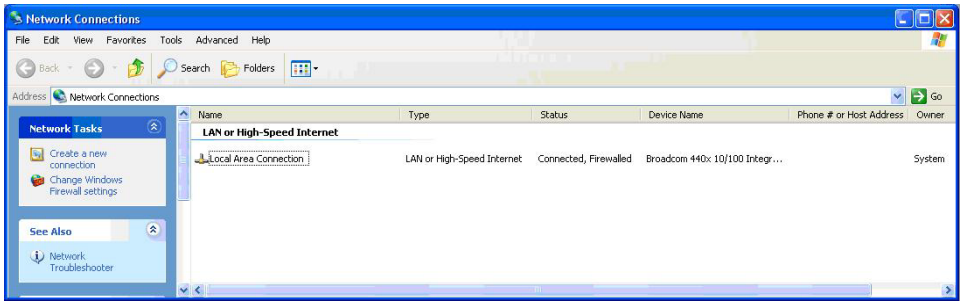
```
[root@sleipnir root]# ifconfig
eth0      Link encap:Ethernet  Hwaddr 00:0C:6E:0A:3D:26
          inet addr:192.168.168.11  Bcast:192.168.168.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13647 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12020 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:7513605 (7.1 Mb)  TX bytes:1535512 (1.4 Mb)
          Interrupt:10

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:892258 (871.3 Kb)  TX bytes:892258 (871.3 Kb)
```

The above machine is running normally. The first line of output shows that the Ethernet interface eth0 has a layer 2 (MAC or hardware) address of 00:0C:6E:0A:3D:26. This confirms that the device driver is able to connect to the card, as it has read the Ethernet address burned into the network card's ROM. The next line shows that the interface has an IP address of 192.168.168.11, and the subnet mask and broadcast address are consistent with the machine being on network 192.168.168.0.

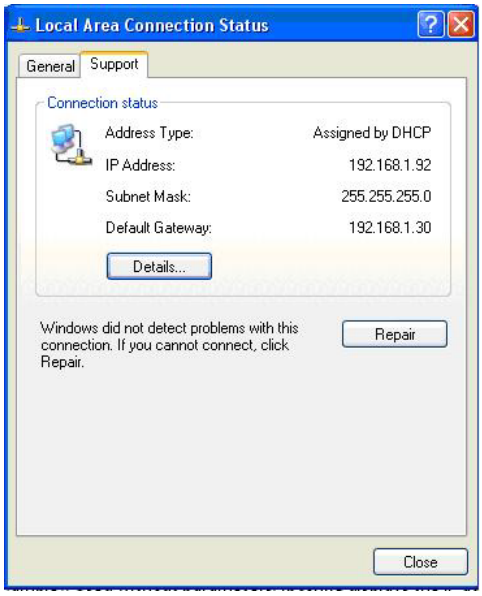
Windows Network Connections

In Windows XP you can view and renew an IP address using Windows Network Connections.

1. Open Network Connections from **Start** → **Control Panel** → **Network Connections**.



2. Right-click a network connection.
3. Click **Status**.
4. Click the **Support** tab. Your connection status information displays.

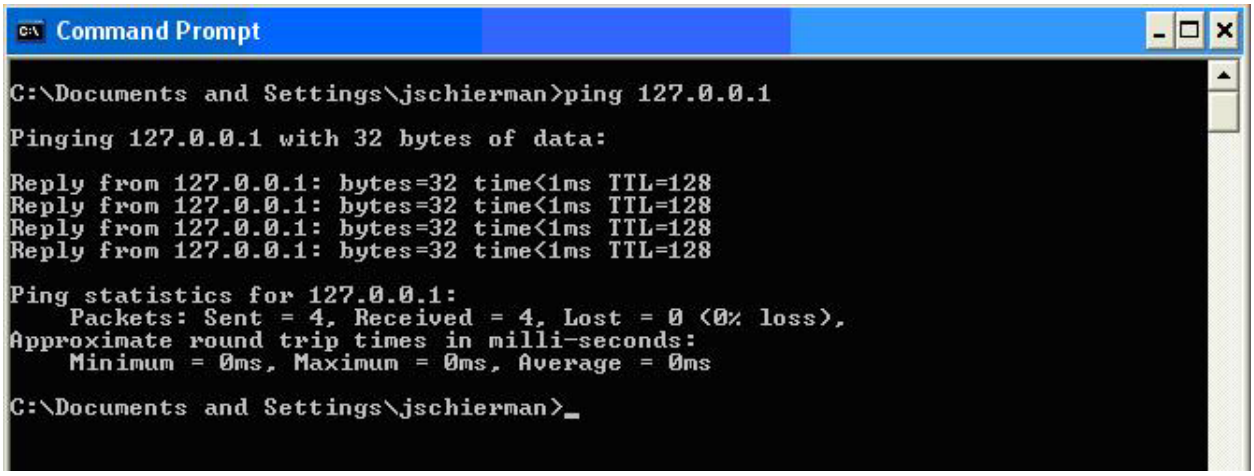


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

Ping

Use the **ping** command to test a TCP/IP configuration by using the ping command (in Windows XP Professional in this example). Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

1. Open a Command Prompt**.** To open a command prompt, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, ping the loopback address by typing **ping 127.0.0.1**.



3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the **ping** command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host on a different subnet). If the **ping** command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server. If the **ping** command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

If the **ping** command is not found or the command fails, you can use Event Viewer to check the System Log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.

The **ping** command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

Telnet

Telnet is a simple, text-based program that lets you connect to another computer via the Internet. If you've been granted the right to connect to that computer by that computer's owner or administrator, Telnet will let you enter commands used to access programs and services that are on the remote computer, as if you were sitting right in front of it.

The Telnet command prompt tool is included with the Windows Server 2003 and Windows XP operating systems. See the related OS documentation and helps for more information. Note that if you are only using computers running Windows, it may be easier to use the Windows Remote Desktop feature. For more information about Remote Desktop, see the related OS documentation and helps.

Telnet Client

By default, Telnet is not installed with Windows Vista or Windows 7, but you can install it by following the steps below.

1. Click the **Start** button, click **Control Panel**, click **Programs**, and then select **Turn Windows features on or off**. If prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In the **Windows Features** dialog box, check the **Telnet Client** checkbox.
3. Click **OK**. The installation might take several minutes.

After Telnet Client is installed, open it by following the steps below.

1. Clicking the **Start** button, type **Telnet** in the Search box, and then click **OK**.
2. To see the available telnet commands, type a question mark (**?**) and then press **Enter**.

Telnet Server

In Windows Server 2003 for most Telnet Server functions, you do not need to configure Telnet Server options to connect a Telnet client to the Windows Server 2003-based Telnet Server. However, in Windows Server 2003 you must configure Telnet Server options to be able to do certain functions.

For example, the following command uses the credentials of the user who is currently logged on to the client to create a Telnet connection on port 23 with a host named server01 **telnet server01**

The following example creates the same Telnet connection and enables client-side logging to a log file named c:\telnet_logfile **telnet -f c:\telnet_logfile server01**

The connection with the host remains active until you exit the Telnet session (by using the **Exit** command), or you use the Telnet Server administration tool to terminate the Telnet session on the host.

For more information, see the Windows Server TechCenter at http://technet.microsoft.com/en-us/library/cc787407(WS.10).aspx.

1. If you try to enable and install Telnet in Windows 7, and the message "*An error has occurred. Not all of the features were successfully changed*" displays, one workaround is to use a third party Telnet client, such as PuTTY, which also supports recommended SSH client.

PuTTY

PuTTY is a simple, free, but excellent SSH and Telnet replacement for Windows. The PuTTY SSH and telnet client was developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is developed and supported by a group of volunteers. PuTTY has been ported to various other operating systems. Official versions exist for some Unix-like platforms, with on-going ports to Mac OS and Mac OS X.

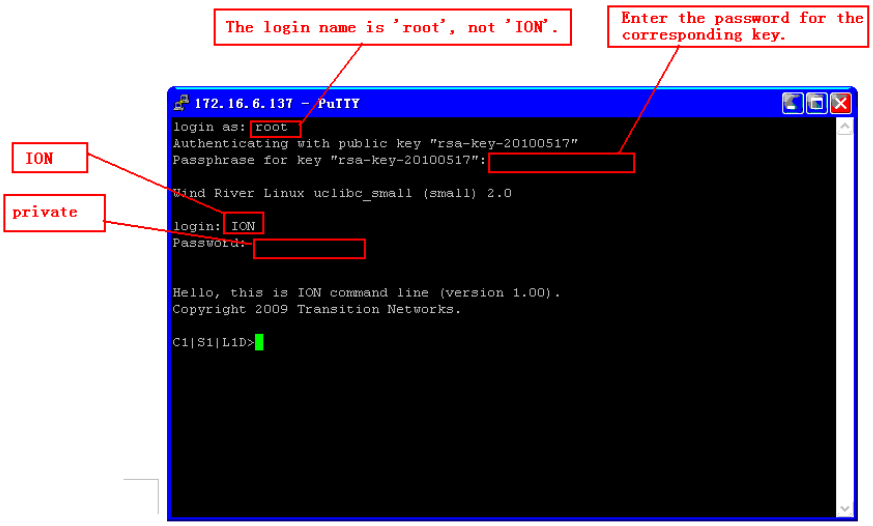
The PuTTY terminal emulator application also works as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols. For PuTTY legal and technical details, see the PuTTY download page at http://putty.org/ or at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Note:

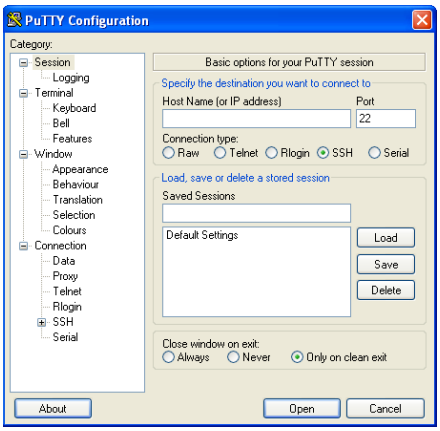
9) When the user-public key is loaded into the IONMM successfully, the key will take effect immediately; you do not need to restart the SSH server.

10) The ION system supports SSH2 keys only; SSH1 keys are not supported. When generating using puttyGen.exe, do not select the SSH1 keys.

11) The ION system currently supports one user named 'root' with public key authentication.



PuTTY Basic Options:



PuTTY SSH Options:

Tracert (Traceroute)

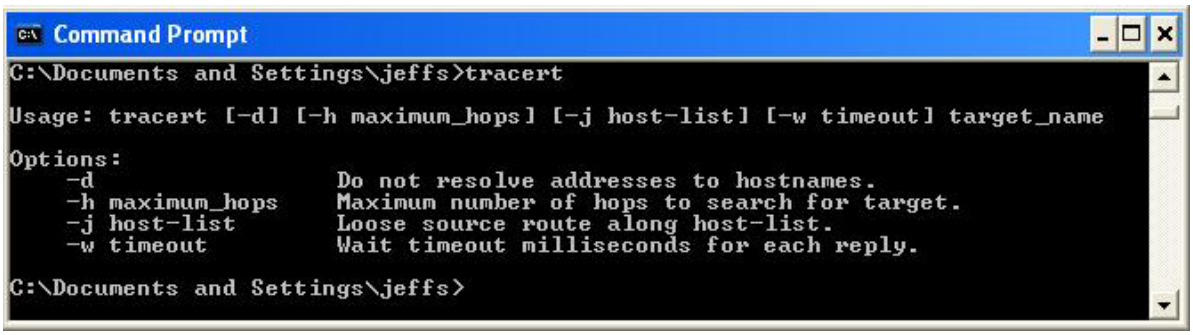
Traceroute is a computer network tool used to determine the route taken by packets across an IP network. 'Tracert" (pronounced "traceroute") sends a test network message from a computer to a designated remote host and tracks the path taken by that message.

Tracert is a Windows based tool that helps test your network infrastructure. In this article we will look at how to use tracert while trying to troubleshoot real world problems. This will help to reinforce the tool's usefulness and show you ways in which to use it when working on your own networks.

The traceroute tool is available on almost all Unix-like operating systems. Variants with similar functionality are also available, such as tracepath on modern Linux installations and tracert on Microsoft Windows operating systems. Windows NT-based operating systems also provide **pathping**, which provides similar functionality.

The tracert TCP/IP utility allows you to determine the route packets take through a network to reach a particular host that you specify. Tracert works by increasing the "time to live" (TTL) value of each successive packet sent. When a packet passes through a host, the host decrements the TTL value by one and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded. Tracert, if used properly, can help you find points in your network that are either routed incorrectly or are not existent at all.

The Tracert Windows based command-line tool lets you trace the path that an IP packet takes to its destination from a source. Tracert determines the path taken to a destination by sending ICMP (Internet Control Message Protocol) Echo Request messages to the destination. When sending traffic to the destination, it incrementally increases the TTL (Time to Live) field values to help find the path taken to that destination address.



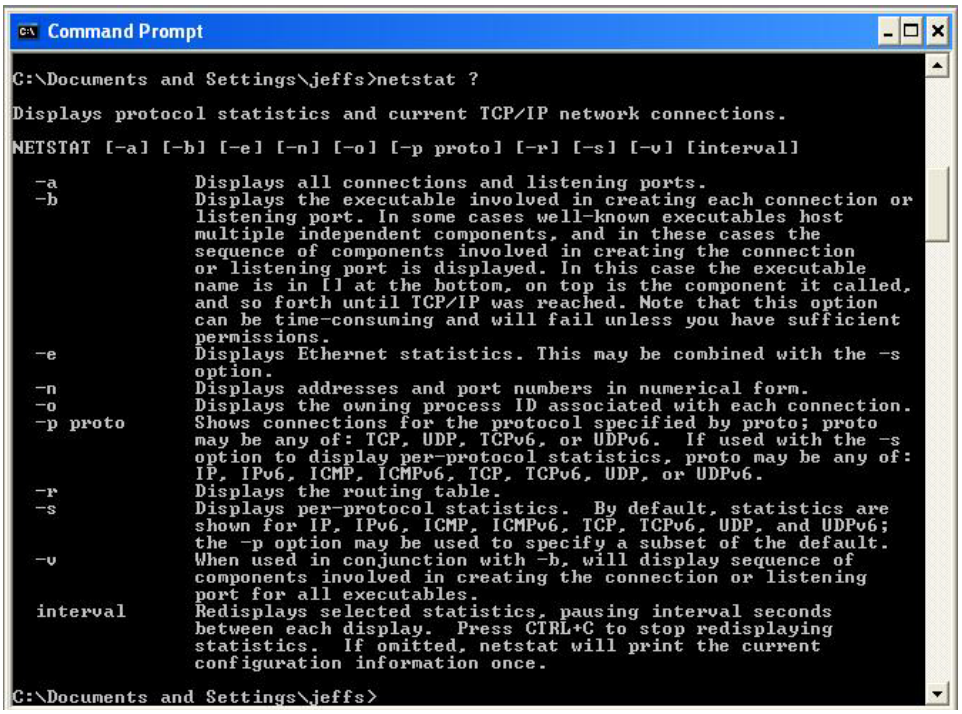
Tracert options include:

-? Which displays help at the command prompt.
-d which prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names (this speeds up the display of tracert results). Using the **–d** option helps when you want to remove DNS resolution. Name servers are helpful, but if not available, incorrectly set, or if you just want the IP address of the host, use the **–d** option.

Netstat

Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on UNIX, Unix-like, and Windows NT-based operating systems.

The **netstat** tool is used for finding network problems and determining the amount of traffic on the network as a performance measurement. It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, Ipv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and Ipv6 statistics (for the Ipv6, ICMPv6, TCP over Ipv6, and UDP over Ipv6 protocols). When used without parameters, **netstat** displays active TCP connections.



Note: parameters used with this command must be prefixed with a hyphen (**-**) and NOT a slash (/):
-a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-b Displays the binary (executable) program's name involved in creating each connection or listening port. (Windows XP, 2003 Server only – not Microsoft Windows 2000 or other non-Windows operating systems).
-e Displays Ethernet statistics, such as the number of bytes and packets sent and received.
-f Displays fully qualified domain names (FQDN) for foreign addresses.(not available under Windows)
-I Displays network interfaces and their statistics (not available under Windows).
-o Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).
-p (Windows): Protocol : Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with **-s** to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
-p (Linux) Process : Show which processes are using which sockets (you must be root to do this).

Winipcfg

The **winipcfg** command is available in Windows ME, Windows 98, and Windows 95 to review your current TCP/IP network protocol settings. Follow these steps to view your current TCP/IP settings using **winipcfg**:

1. Click the **Start** button and then click **Run**.
2. Type **winipcfg** in the **Open** box, and then click **OK**. Your current TCP/IP settings are displayed.
3. To view additional information, click **More Info**.

Note: The Winipcfg display is not updated dynamically. To view changes, quit **winipcfg** and then run it again. If your IP address was dynamically allocated by a DHCP server, you can use the Release and Renew buttons to release and renew the IP address.

The following information is displayed by the **winipcfg** tool.

Adapter Address: This string of hexadecimal numbers represents the hard-coded identification number assigned to the network adapter when it was manufactured. When you are viewing the IP configuration for a PPP connection using Dial-Up Networking, the number is set to a default, meaningless value (because modems are not hard-coded with this type of address).

IP Address: This is the actual IP networking address that the computer is set to. It is either dynamically assigned to the computer upon connection to the network, or a static value that is manually entered in TCP/IP properties.

Subnet Mask: The subnet mask is used to "mask" a portion of an IP address so that TCP/IP can determine whether any given IP address is on a local or remote network. Each computer configured with TCP/IP must have a subnet mask defined.

Default Gateway: This specifies the IP address of the host on the local subnet that provides the physical connection to remote networks, and is used by default when TCP/IP needs to communicate with computers on other subnets.

Click **More Info** to display the following settings:

DHCP Server: This specifies the IP address of the DHCP server. The DHCP server provides the computer with a dynamically assigned IP address upon connection to the network. Clicking the Release and Renew buttons releases the IP address to the DHCP server and requests a new IP address from the DHCP server.

Primary and Secondary WINS Server: These settings specify the IP address of the Primary and Secondary WINS servers (if available on the network). WINS servers provide a service translating NetBIOS names (the alphanumeric computer names seen in the user interface) to their corresponding IP address.

Lease Obtained and Lease Expires: These values show when the current IP address was obtained, and when the current IP address is due to expire. You can use the Release and Renew buttons to release and renew the current IP address, but this is not necessary because the DHCP client automatically attempts to renew the lease when 50 % of the lease time has expired.

Nslookup

nslookup is a computer program used in Windows and Unix to query DNS (Domain Name System) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The name nslookup means "name server lookup". A common version of the program is included as part of the BIND package.

Microsoft Windows 2000 Server, Windows 2000 Advanced Server, and Windows NT Server 4.0 Standard Edition provide the **nslookup** tool.

Windows' nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through the Control Panel.

Nslookup.exe can be run in two modes: interactive and noninteractive. Noninteractive mode is used when just a single piece of data is needed.

1. The syntax for noninteractive mode is:

   nslookup [-option] [hostname] [server]

2. To start Nslookup.exe in interactive mode, simply type "**nslookup**" at the command prompt:

   C:\> nslookup
   Default Server: nameserver1.domain.com
   Address: 10.0.0.1

3. Type "**help**" or "**?**" at the command prompt to generate a list of available commands.

Notes:

- The TCP/IP protocol must be installed on the computer running Nslookup.exe.
- At least one DNS server must be specified when you run the IPCONFIG /ALL command from a command prompt.
- Nslookup will always devolve the name from the current context. If you fail to fully qualify a name query (i.e., use a trailing dot), the query will be appended to the current context. For example, if the current DNS settings are att.com and a query is performed on www.microsoft.com; the first query will go out as www.microsoft.com.att.com because of the query being unqualified. This behavior may be inconsistent with other vendor's versions of Nslookup.

Dr. Watson

Dr. Watson detects information about Windows system and program failures and records the information in a log file. Dr. Watson starts automatically at the event of a program error. To start Dr. Watson, click **Start**, click **Run**, and then type **drwtsn32**. To start Dr. Watson from a command prompt, change to the root directory, and then type **drwtsn32**.

When a program error occurs, Dr. Watson creates a log file (Drwtsn32.log) which contains:

- The line *Application exception occurred*:.
- Program error information.
- System information about the user and the computer on which the program error occurred.
- The list of tasks that were running on the system at the time that the program error occurred.
- The list of modules that the program loaded.
- The state dump for the thread ID that is listed.
- The state dump's register dump.
- The state dump's instruction disassembly.
- The state dump's stack back trace.
- The state dump's raw stack dump.
- The symbol table.

The default log file path is:
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson.

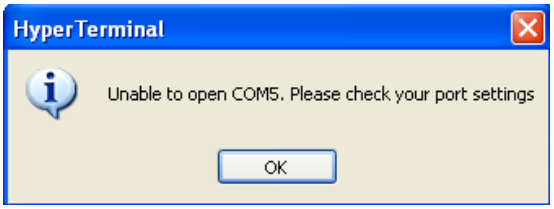
The default Crash Dump path is:
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

Third Party Tool Messages

This section discusses messages generated by HyperTerminal, Ping, and Telnet during ION system installation, operation and configuration.

HyperTerminal Messages

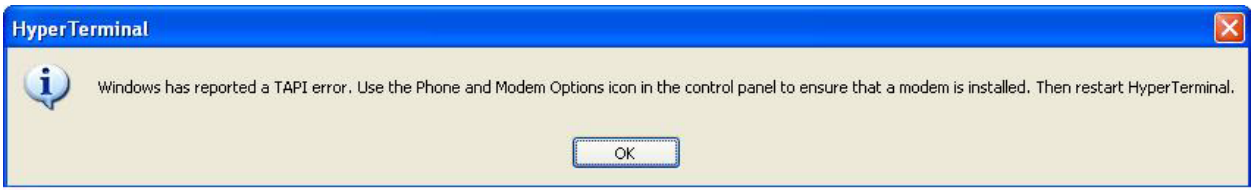
Message: *Unable to open COM x. Please check your port settings*.



Response:

1. Verify your computer's **Ports (COM & LPT)** setting. See "Configuring HyperTerminal".
2. Use the **Computer Management > Device Manager** > **Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support.

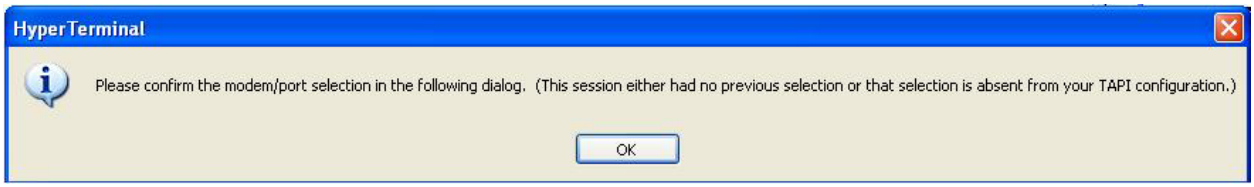
Message: *Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal*.



Response:

1. Click **OK** to close the HyperTerminal error dialog box.
2. Try opening an existing HyperTerminal connection (**File** > **Open**).
3. Verify your computer's **Ports (COM & LPT)** setting. See "Configuring HyperTerminal".
4. Use the **Computer Management > Device Manager** > **Troubleshooter** button on the **General** tab in **Properties**.
5. Unplug and re-plug the USB connector on the IONMM card.
6. If the problem persists, contact Technical Support.

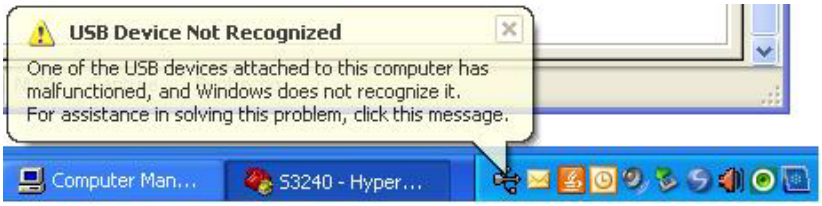
Message: *Please confirm the modem/port selection in the following dialog. (This session either had no previous selection or that selection is absent from your TAPI configuration.)*



Response:

1. Verify the HyperTerminal configuration. See "Configuring HyperTerminal "(e.g., verify your **computer's Ports (COM & LPT**) setting).
2. Use the **Computer Management > Device Manager** > **Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the NID.
4. Retry the operation. See "Start a USB Session in HyperTerminal and Log In ".
5. If the problem persists, contact Technical Support.

Message: *USB Device Not Recognized*
One of the USB devices attached to this computer has malfunctioned, and Windows does not recognize it. For assistance in solving this problem, click this message.



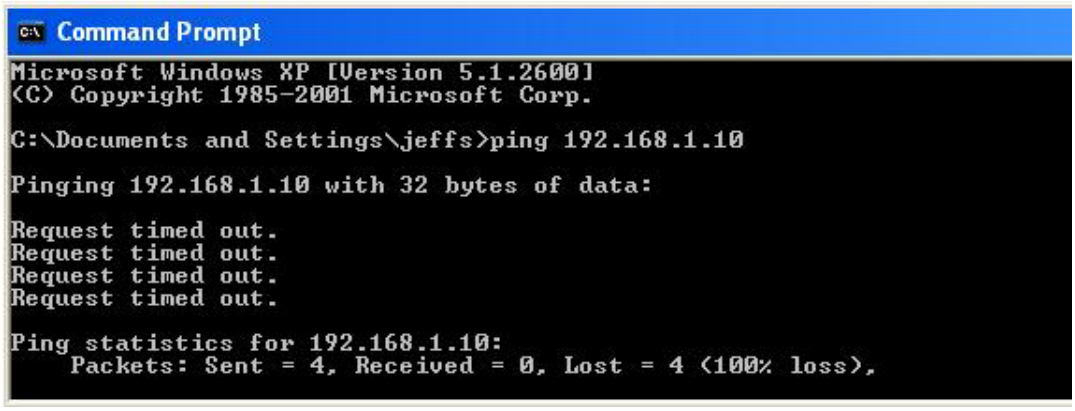
Response:

1. Click message icon in the tray. A Windows recommendation dialog displays.

2. Click **Close** to close the dialog.
3. Try reconnecting the device to the same USB port on the console device (PC).
4. Try reconnecting the device to a different USB port on the console device (PC) if available.

Ping Command Messages

Message: *Request timed out*.

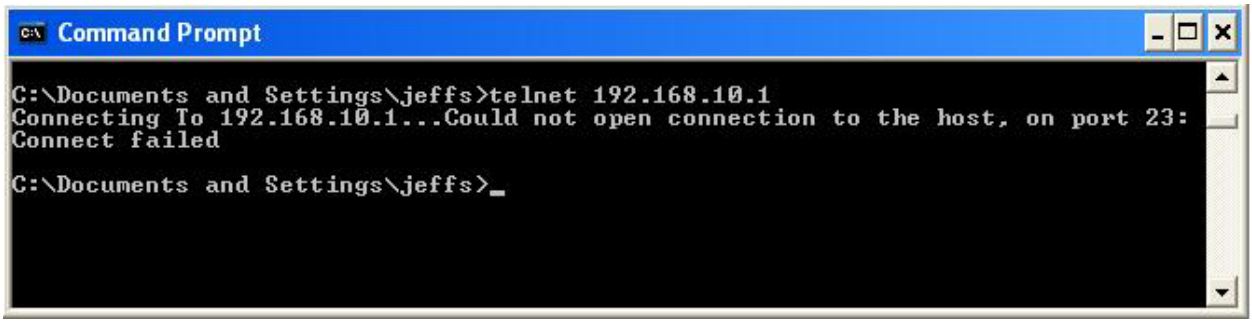


Meaning: The Ping command failed.
Recovery:

1. Verify the connection, verify correct IP address entry, and retry the operation.
2. Verify if the default IP address has changed using the Ipconfig (or similar) command.

Telnet Messages

Message: *Could not open connection to the host, on port 23: Connect failed*.



Meaning: The attempted Telnet connection failed.
Recovery:

1. Verify the physical connection, verify correct IP address entry, and retry the operation.
2. Check if the default IP address has changed using the Ipconfig (or similar) command.

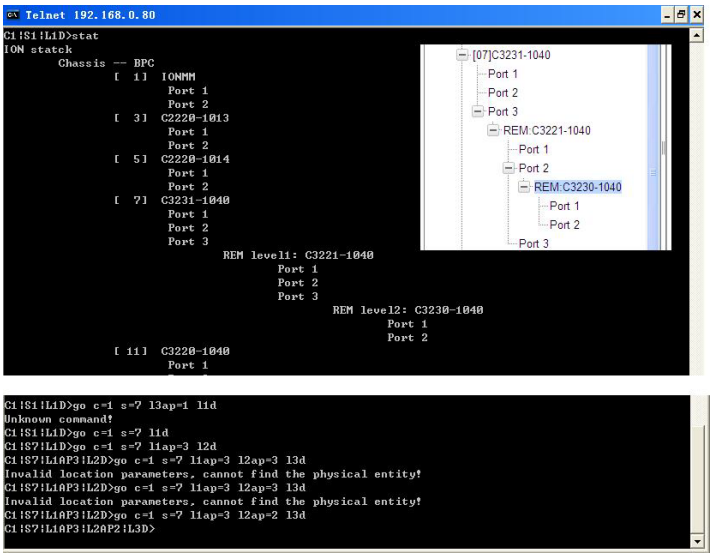
Message*: Invalid location parameters, cannot find the physical entity*!

```
C1!S7!L1AP3!L2D>go c=1 s=7 l1ap=3 l2ap=3 l3d
Invalid location parameters, cannot find the physical entity!
```

Meaning: 1) The **go** command you entered includes a location that does not exist or that you entered incorrectly. 2) The NID is in the process of a reset operation; wait one minute and then re-try the function.

Recovery:

1. Run the **stat** command to verify your configuration.
2. Click the plus sign [**+**] next to **ION Stack** to unfold the "ION Stack" node in the left tree view to refresh device status.
3. Click the plus sign [+] next to **Chassis** to unfold the chassis devices.



4. Compare the **stat** command results to the Web interface tree view configuration information.
5. Re-run the **stat** command with the correct location parameters.
6. Ping the device in question.
7. Unplug and re-plug the USB connector on the IONMM card.
8. If the problem persists, contact Technical Support.

Message: *Unknown command*!

```
C1!S1!L1D>go c=1 s=7 l3ap=1 l1d
Unknown command!
```

Meaning: The command you entered is not supported, or you entered the wrong command format / syntax.

Recovery:

1. Verify the CLI command syntax.
2. See "Section 6: Command Line Interface (CLI) Reference".

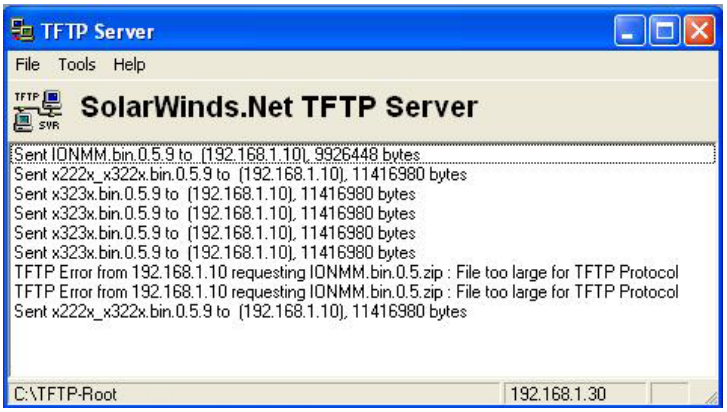
TFTP Server Messages

Messages like the ones below may display during TFTP Server operation, depending on the TFTP Server package that you selected.

Message: *File does not exist*

Meaning: A TFTP Server error – the TFTP Server Address that you specified does not contain the Firmware File Name specified.
Recovery:
1) Verify the TFTP server's correct file location (e.g., local disk at *C:\TFTP-Root*).
2) Verify the filename / extension.
3) Check the TFTP Server's online helps for suggestions.

Message: *File too large for TFTP Protocol*



Meaning: A TFTP Server error – you tried to upload a file (e.g., IONMM.bin.0.5 – 50Mb) but the TFTP server failed. The file you tried to upload via the TFTP server exceeded the file size capability.
Recovery:
1) Check if some extra files ended up in the zip folder – some repeated – 6 FW files total.
2) Remove some of the files from the zip folder and try the upload again.
3) Send the remaining files in a separate file.
4) Check the TFTP Server's online helps for suggestions.

PuTTY Messages

Messages like the ones below may display during PuTTY (or similar package) operation, depending on the package that you selected.

Message: *Server refused key*
Meaning: You can connect to a secure telnet session using password authentication, but when you try to connect using public key authentication, you receive a "*Server refused our key*" message on the client (PuTTy) session. For example, you generated a public/private key (using Puttygen) and saved them, loaded the client public key into the IONMM via TFTP, and enabled SSH. The PuTTY SSH Authentication pointed to the saved private key. You set the auto-log on user name to root as suggested, but when you activated PuTTY, after 20-30 seconds, the refusal message displayed and PuTTY reverted back to password authentication (the default).
Recovery:

1. When generating using *puttyGen.exe*, select the SSH2 keys – do not select the SSH1 keys.
2. Log in to PuTTy as '*root*' with the public key authentication.
3. Use the online helps and documentation to set up Putty as suggested.
4. See the "PuTTY" section notes.

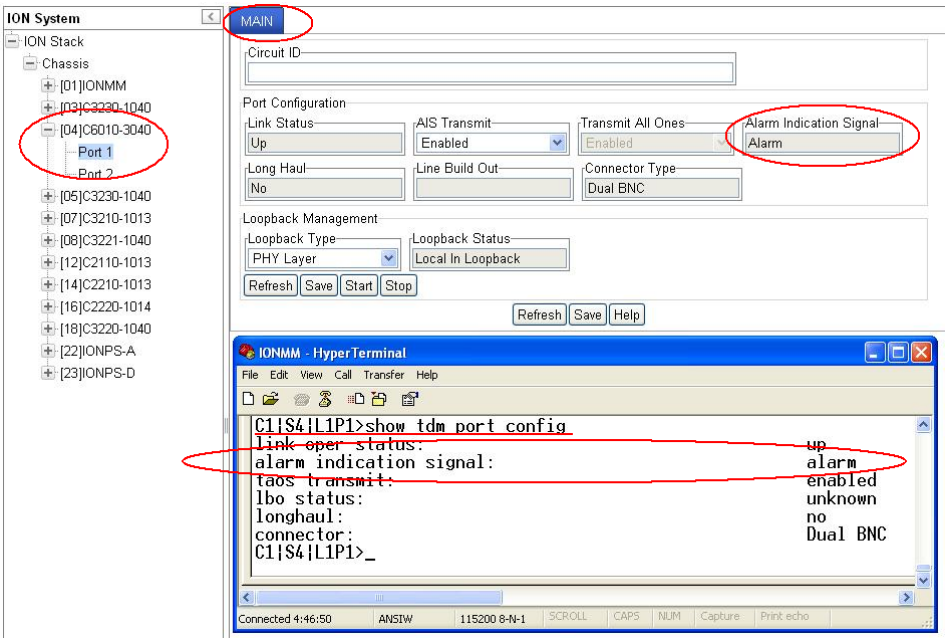
Alarm Indication Signal – Alarm Condition

In T1 mode, the criteria for declaring/clearing AIS detection are in compliance with the ANSI T1.231.

In E1 mode, the criteria for declaring/clearing AIS detection comply with the ITU G.775 or the ETSI 300233, as selected. The function is implemented in the LIU chip. When in E1 mode, application software may select the AIS condition by changing the value in the LIU register accordingly. The criteria for AIS detection declaring and clearing is shown below.

	ITU G.755 for E1 (LAC bit is set to '0' by default)	ETSI 300233 for E1 (LAC bit is set to '1')	ANSI T1.231 for T1/J1
AIS detected	Less than 3 zeros contained in each of two consecutive 512-bit streams are received	Less than 3 zeros contained in a 512-bit stream are received	Less than 9 zeros contained in an 8192-bit stream (a ones density of 99.9% over a period of 5.3 ms)
AIS cleared	3 or more zeros contained in each of two consecutive 512-bit streams are received	3 or more zeros contained in a 512-bit stream are received	9 or more zeros contained in an 8192-bit stream are received

The x6010 AIS **Alarm** condition is shown below for both the CLI and the Web interface.



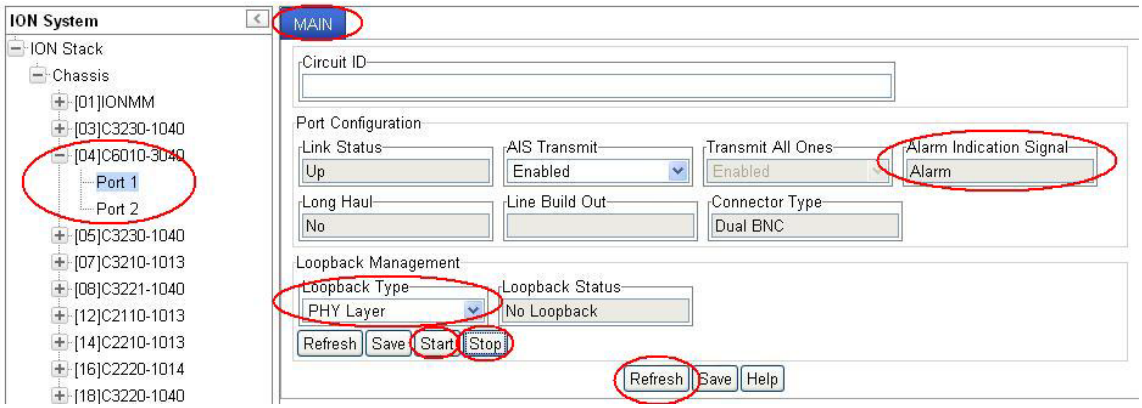
To clear the AIS **Alarm** condition from the CLI:

1. Start (initiate) the TDM Loopback operation. Type **set tdm loopback oper=init** and press **Enter**.
2. Stop the TDM Loopback operation. Type **set tdm loopback oper stop** and press **Enter**.
3. Verify that the condition changed from ***alarm*** to ***normal***. Type **show tdm port config** and press **Enter**.

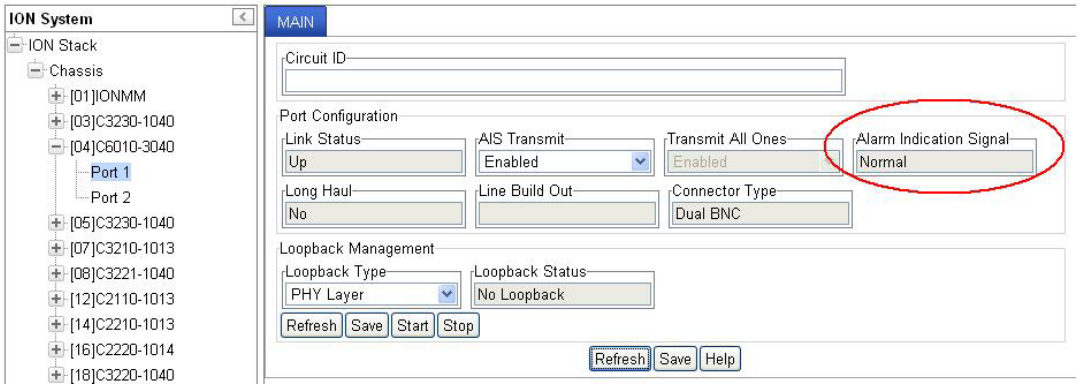
For example:

```
C1|S4|L1P1>set tdm loopback oper init
C1|S4|L1P1>set tdm loopback oper stop
C1|S4|L1P1>show tdm port config
link oper status:                                       up
alarm indication signal:                                normal
taos transmit:                                          enabled
lbo status:                                             unknown
longhaul:                                               no
connector:                                              Dual BNC
C1|S4|L1P1>
```

To clear the AIS **Alarm** condition via the Web interface:



1. In the **Loopback Type** field select **PHY Layer**.
2. Click the **Start** button.
3. Click the **Stop** button.
4. Click the **Refresh** button.



5. Verify that the **Alarm Indication Signal** field has changed from **Alarm** to **Normal**.

LOS Detection

The x6010 LOS (Loss of Signal) detector monitors the amplitude of the incoming signal level and pulse density of the received TIP/RING signals. A LOS is detected when the incoming signal has “no transitions”. The LOS is cleared when the incoming signal has “transitions”. The x6010 LOS function is implemented in the LIU chip, but the x6010 application software may get the LOS status via interface with the FPGA. The x6010 LOS detection is provided via link down and link up traps and **show** commands.

T1 Error Events and Alarm Conditions

There are error events specific to T1, and alarm conditions specific to DS4 / ESF that are generated at the system level. Basic responses include:

1. Check all available logs and reports for related troubleshooting information.
2. Check the x6010 NID connections (see “Section 2: Installation and System Setup”) at the near-end and far-end.
3. Check all cable runs for damaged cable, etc.
4. Verify proper operation of other network devices.
5. Check the x6010 NID configuration; see “Section 4: Configuration”.

T1 Error Events

ANSI T1.403 terminal equipment (CSU) transmits Performance Report messages towards the network every second. The following Error Events can be reported in the Performance Report Message:

CRC Errors – event occurs when the received CRC code does not match that CRC code calculated locally.

Severe Errors – event occurs when two or more framing bit errors are detected in any 3 mSec window. Alternatively, existing 2 of 4, 2 of 5, or 3 of 5 errored framing bit criteria can be used to declare a Severe Error (SE). When a Severe Error is reported, the FE (Frame Bit Errors) count is set to 0.

Frame Bit Errors – event occurs whenever an incorrect or unexpected framing bit is received. When a FE error count is transmitted, the Severe Error (SE) count is set to 0.

Line Code Violations – event occurs whenever an invalid line violation (bipolar violation) occurs.

Controlled Slip Events – event occurs when frames are repeated or deleted at the receiving terminal to compensate for clocking differences between the Carrier and the Terminal equipment.

D4 and ESF Alarm Conditions

The following D4 / ESF Alarm Conditions can be reported:

AIS CFA (Alarm Indication Signal – Carrier Failure Alarm) – also known as a “Keep Alive” or “Blue Alarm” signal; consists of an unframed all-ones signal sent to maintain transmission continuity. The AIS CFA signal is declared when both the AIS state and Red CFA persist simultaneously.

OOF (Out-Of-Frame) Condition – occurs whenever Network or DTE equipment senses errors in the incoming framing pattern. Depending on the equipment, this can occur when 2 of 4, 2 of 5, or 3 of 5 framing bits are in error. A reframe clears the OOF condition.

Red CFA (Carrier Failure Alarm) – occurs after detection of a Continuous OOF condition for 2.5 seconds. This alarm state is cleared when no OOF conditions occur for at least 1 second. Some applications (AT&T DACS services) may not clear the CFA state for up to 15 seconds of no Out-Of-Frame occurrences.

Yellow CFA (Carrier Failure Alarm) – when a Terminal/Network equipment enters a Red CFA state, it transmits a "Yellow Alarm" in the opposite direction. A Yellow Alarm is transmitted by setting Bit #2 of each timeslot to a 0 (zero), Space state for D4 Framed facilities. For ESF facilities, a Yellow Alarm is transmitted by sending a repetitive 16-bit pattern consisting of 8 Marks (1) followed by 8 Spaces (0) in the Datalink bits. This is transmitted for a minimum of 1 second.
For D4 facilities, the minimum Yellow Alarm detection time is 335 mSec. Trunk conditioning should occur within 335 to 1000 mSec.
For ESF facilities, the minimum detection time is 28 mSec. (Note that 335 mSec equates to 2680 D4-type frames.)

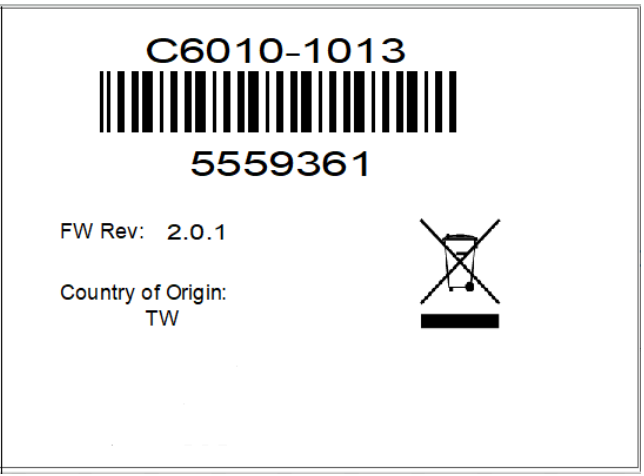
LOS (Loss Of Signal) – a condition that is declared when no pulses have been detected in a 175 +/- 75 pulse window (100 to 250 bit times).

Recovery Procedures

1. Ensure that the T1 or E1 is running properly on both ends.
2. Use the **show tdm config**, **show tdm loopback**, and **show tdm port** commands to verify that the configuration of the line matches that of the remote end.
3. Ensure that the cable between the interface port and the T1 or E1 service provider equipment or remote E3 terminal equipment connects correctly.
4. Ensure that the cable is connected to the correct port. Correct the cable connections as required.
5. Check all cables integrity. Look for breaks or other physical abnormalities in the cable. Replace the cable if necessary.
6. Check x6010 DIP Switches and Jumper Settings (page 210).
7. Run ION System Tests (page 201).
8. Run the In-band Loopback Code Detect Procedure (page 216).
9. Check with your provider to make sure the framing format configured on the port matches the framing format on the line. Try another framing format and see if the alarm clears.
10. Work with your provider to configure a remote loopback on the affected interface.

Device Label and Box Label

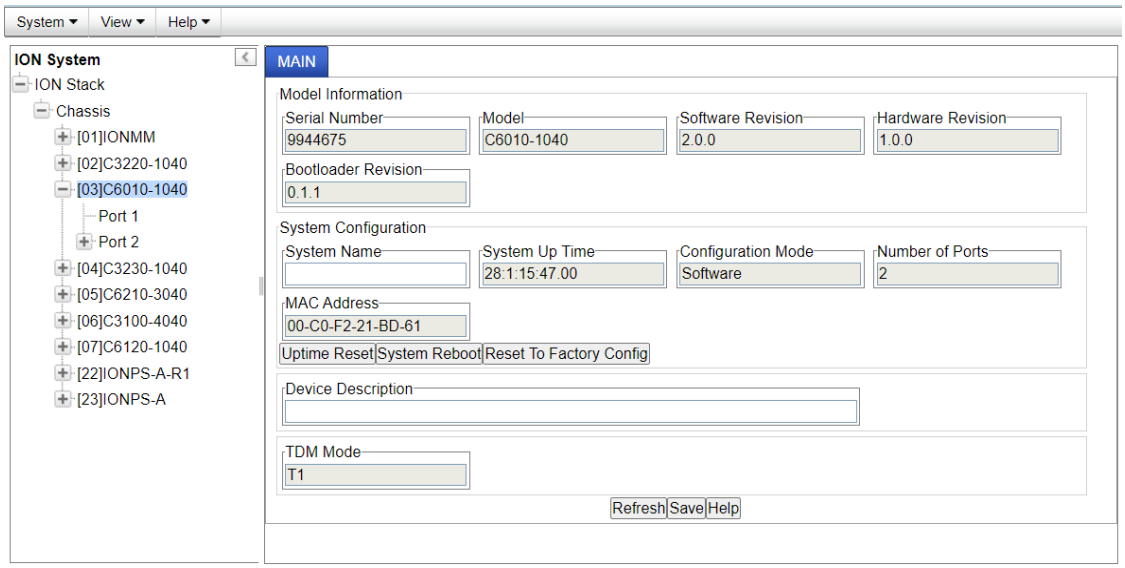
The labels on the device and on the shipping carton can provide helpful information when calling Technical Support.

Device Label	Box Label
	

Recording Model Information and System Information

After performing the troubleshooting procedures, and before contacting Technical Support, please record as much information as possible to help the Technical Support Specialist.

1. Select the ION system device **MAIN** tab. (From the CLI, use the commands needed to gather the information requested below. This could include commands such as **show card info**, **show tdm info**, **show tdm port config**, or others as request by the Support Specialist.



2. Record the x6010 **Model Information**.

   Serial Number: _____ Model: _____

   Software Revision: _____ Hardware Revision: _____

   Bootloader Revision: _____

3. Record the x6010 **System Configuration** information.

   System Up Time: _____ Configuration Mode: _____

   Number of Ports: _____ Device Description: _____

   TDM Mode: _____

4. Provide additional Model and System information to your Technical Support Specialist. See "Basic ION System Troubleshooting".

   Your Lantronix service contract number: _____

   Describe the failure: _____

   Describe any action(s) already taken to resolve the problem (e.g., changing switch mode, rebooting, etc.): _____

   The serial # and revision # of each involved Lantronix product in the network:

   _____

Describe your network environment (layout, cable type, etc.): _____

Network load and frame size at the time of trouble (if known): _____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

_____

Any previous Return Material Authorization (RMA) numbers: _____

Appendix A Compliance and Safety Information

Compliance Information

Standards CISPR22/EN55022 Class A, CE Mark

FCC Regulations NOTE: 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 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 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 the user will be required to correct the interference at his own expense.

CE Marking: This is a Class A product. In a domestic environment, this product could cause radio interference; as a result, the customer may be required to take adequate preventative measures.

UL Recognized Tested and recognized by the Underwriters Laboratories, Inc.

Canadian Regulations This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numériqué de la classe [*] est conformé à la norme NMB-003 du Canada.

European Regulations

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

Achtung ! Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fäll ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention ! Ceci est un produit de Classe A. Dans un environment domestique, ce produit 243nterf de créer des 243nterferences radioélectriques, il appartiendra alors à l'utilsateur de prende les measures spécifiques appropriées.

In accordance with European Union Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, Lantronix will accept post usage returns of this product for proper disposal. The contact information for this activity can be found in the 'Contact Us' portion of this document.

CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.

Der Anschluss dieses Gerätes an ein öffentlickes Telekommunikationsnetz in den EG-Mitgliedstaaten verstösst gegen die jeweligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

EU Declaration of Conformity

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Product Name: Network Interface Device
Model Number: C6010-1040, C6010-101X, S6010-1040, S6010-101X (X can be 0-9)

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)

- **EN IEC 62368-1:2020, EN IEC 62368-1:2020/A11:2020**

EMC Directive (2014/30/EU)

- **EN 55032:2015/A1:2020 (Class A)**
- **EN 55035:2017+A11:2020**

EU Directive 2011/65/EU for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I

- **EN IEC 63000:2018**

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: Eric Bass Date: 19 May 2023

Name: Eric Bass Title: VP of Engineering

UK Declaration of Conformity

LANTRONIX®

UK CA

UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Product Name: Network Interface Device
Model Number: C6010-1040, C6010-101X, S6010-1040, S6010-101X (X can be 0-9)

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Electrical Equipment Regulations (Safety)

- **EN IEC 62368-1:2020, EN IEC 62368-1:2020/A11:2020**

Electromagnetic Compatibility Regulations (EMC)

- **BS EN 55032:2015/A1:2020 (Class A)**
- **BS EN 55035:2017+A11:2020**

UK SI 2012 No. 3032 for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and 6(c).
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU[7(c)-I] and 2018/741/EU[6(c)]
BS EN IEC 63000 : 2018

Statement of Conformity: The product specified above meets the test requirements of the relevant legislation of United Kingdom, including the application of sound engineering practice.

Signature: Eric Bass Date: 19 May 2023

Name: Eric Bass Title: VP of Engineering

Electrical Safety Warnings

Electrical Safety

IMPORTANT: This equipment must be installed in accordance with safety precautions.

Elektrische Sicherheit

WICHTIG: Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

Elektrisk sikkerhed

VIGTIGT: Dette udstyr skal installeres i overensstemmelse med sikkerhedsadvarslerne.

Elektrische veiligheid

BELANGRIJK: Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

Sécurité électrique

IMPORTANT: Cet équipement doit être utilisé conformément aux instructions de sécurité.

Sähköturvallisuus

TÄRKEÄÄ: Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

IMPORTANTE: questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal installeres i samsvar med sikkerhetsregler.

Segurança eléctrica

IMPORTANTE: Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

Seguridad eléctrica

IMPORTANTE: La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

Elsäkerhet

OBS! Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.

Appendix B: Factory Defaults

The x6010 NID *Device* Level Factory Defaults are shown in the tables below. **Note**: The default settings shown are as seen in the tabs/fields of the x6010 Web interface.

Device-Level Factory Defaults

Table 14: Device-Level Factory Defaults

Hardware Mode		
System Level		
Login / Password	ION / private	
System Name	Device dependent (e.g., C6010-3040)	
Device Description	<null string>	
TDM mode	Depends on DIP switch position	DIP switch 4-4, UP: T1, Down:E1
In-band Loopback Selection	Depends on DIP switch position	DIP switch 3-4, UP: Disabled, Down: Enabled. Start Pattern: “11000” Stop Pattern: “11100”

Port-Level Factory Defaults

Table 15: Port-Level Factory Defaults

Port 1		
Circuit ID	<null string>	
AIS Transmit	Depends on DIP switch position	DIP switch 4-1, UP: Disable, Down: Enable
Transmit All Ones	Enabled	
Long Haul	Depends on DIP switch position Valid on T1 only	DIP switch 4-3, UP: No, Down: Yes
Line Build Out	Depends on TDM mode & DIP switch position	See Table 17 below.
Loopback Type	Depends on front panel DIP switch.	Switch 2, CL: PHY Layer, Middle: No Loopback
Loopback Status	Depends on front panel DIP switch.	Switch 2, CL: Local in Loopback, Middle: No Loopback
Port 2		
Circuit ID	<null string>	
AIS Transmit	Depends on DIP switch position	DIP switch 4-2, UP: Disable, Down: Enable
Transmit All Ones	Enabled	
Loopback Type	Depends on front panel DIP switch.	Switch 2, FL: PHY Layer, Middle: No Loopback
Loopback Status	Depends on front panel DIP switch.	Switch 2, FL: Local in Loopback, Middle: No Loopback

Software Mode		
System Level		
Device Description	<null string>	
TDM mode	Depends on DIP switch position	DIP switch 4-4, UP: T1, Down:E1
In-band Loopback Selection	Depends on DIP switch position	DIP switch 3-4, UP: Disabled, Down: Enabled. Start Pattern: “11000” Stop Pattern: “11100”
Port 1		
Circuit ID	<null string>	
AIS Transmit	Enabled	
Transmit All Ones	Enabled	
Long Haul	Depends on DIP switch position Valid on T1 only	DIP switch 4-3, UP: No, Down: Yes
Line Build Out	Depends on TDM mode & DIP switch position	See Table 17 below.
Loopback Type	No Loopback	
Loopback Status	No Loopback	
Port 2		
Circuit ID	<null string>	
AIS Transmit	Enabled	
Transmit All Ones	Enabled	
Loopback Type	No Loopback	
Loopback Status	No Loopback	

Supported Line Build Out Matrix

Table 16: Line Build Out (LBO) Details

Switch 4-4 (TDM mode)	Switch 4-3 (Long Haul)	Switch 3-1	Switch 3-2	Switch 3-3	Line Build Out
UP	UP	UP	UP	Down	t1SH-DSX-533-655
UP	UP	Up	Down	UP	t1SH-DSX-399-533
UP	UP	Up	Down	Down	t1SH-DSX-266-399
UP	UP	Down	UP	Up	t1SH-DSX-133-266
UP	UP	Down	UP	Down	t1SH-DSX-0-133ANSIT1403
UP	Down	UP	UP	X	t1LH-m22-5dB
UP	Down	UP	Down	X	t1LH-m15dB
UP	Down	Down	UP	X	t1LH-m7-5dB
UP	Down	Down	Down	X	t1LH-0dB
Down	X	X	X	X	x6010 with BNC: e12-37V75ohm x6010 with RJ-48: e13-0V120ohm

X = does not care

Appendix C Configuration Quick Reference – CLI

T1 Ports Configuration

1. Access the x60xx through either a USB connection or a Telnet session.
2. Configure the Port 1 Circuit ID.
   Type **set circuit-ID=xx**.
3. Configure the Port 1 Loopback Type.
   Type **set tdm loopback type=phylayer**.
4. Use the **go** command to switch to Port 2.
5. Repeat steps 2-3 above to configure the Port 2 Circuit ID, AIS Transmit, and Loopback Type.
6. Configure the Port 2 DMI function (optional - if supported).
7. Click the **Save** button when done.
8. Verify each port's configuration.
   Type **show tdm port config**.

Port Loopback Test –T1 and E1 Modes

1. Place the x6010 in Hardware mode and set the x6010 front panel **CL** – **FL** switch to the **CL** position.
2. Access the x6010 through either a USB connection or a Telnet session.
3. Use the **go** command to switch to Port 1.
   Type **go c1 sx l1p=1** and press **Enter**.
4. Set the Port 1TDM Loopback type to PHY layer.
   Type **set tdm loopback type=phylayer** and press **Enter**.
5. Start the Port 1 Loopback operation.
   Type **set tdm loopback oper=init** and press **Enter**.
6. Stop the Port 1 Loopback operation.
   Type **set tdm loopback oper=stop** and press **Enter**.
7. Set the x6010 front panel **CL** – **FL** switch to the **FL** position.
8. Use the **go** command to switch to Port 2.
9. Repeat steps 4-6 for Port 2.

E1 Mode Configuration

1. Set DIP Switch SW4 switch #4 to the Down position.
2. Access the x6010 through either a USB connection or a Telnet session.
3. Use the **go** command to switch to Port 1.
   Type **go c=1 s=x l1p=1**.
4. If required, enter a Circuit ID of up to 64 characters using the **set circuit-ID** command.
5. Configure Loopback management as required.
   Type **set tdm loopback oper**=xx and **set tdm loopback oper type=xx**.
6. Configure TAOS Transmit.
   Type **set taos transmit=enable**.
7. Verify the E1 mode configuration.
   Type **show tdm config**.

For SNMP MIB Trap Information

For information on Network Management for Microsoft Networks Using SNMP, see the MSDN Library or http://technet.microsoft.com/en-us/library/cc723469.aspx.

The notification MIB is described in section 4.2 and section 7.2 of RFC 2573, available from the IETF web site at http://www.ietf.org/rfc/rfc2573.txt.

Appendix D Cable Specifications

This appendix provides fiber and twisted-pair copper cable specifications.

Fiber Cable

Bit Error Rate: <10-9
Single mode fiber *(recommended)*: 9 µm
Multimode fiber *(recommended):* 62.5/125 µm
Multimode fiber *(optional)*: 100/140, 85/140, 50/125 µm

T1/E1 Cable

Category 3: (minimum requirement)
Connector: RJ-48C
Electrical network connection: Single 4-wire (Tip/Ring - Tip1/Ring1)
Mechanical arrangement: 8-position miniature modular jack
Usage: 1.544 Mb/s access lines
Interface codes: 04DU9 (any applicable)
Cable types:

- ☐ Long Haul T1/E1: 0db, -7.5dp, -15db, -22db
- ☐ E1: E1 3.0V, 120 ohm
- ☐ J1: 0-655', 110 ohm (future support)
- ☐ DSX-1: 0-133', 133-266', 266-399', 399-533', 533-655', 100 ohm

Twisted-Pair Copper Cable

Twisted pair connection requires two active pairs. The two active pairs in a T1/E1 network are pins 1 & 2 and pins 4 & 5. Use only dedicated wire pairs (such as blue/white & white/blue, orange/white & white/orange) for the active pins. Category 3 or better twisted-pair copper wire is required. Either shielded twisted-pair (STP) or unshielded twisted-pair (UTP) can be used.

T1 TP/UTP

Gauge 24 to 22 AWG
Attenuation 2.6 dB/100 meters @ 1.0 MHz
Differential Characteristic Impedance 100 Ω ±10%

E1 TP/UTP

Gauge 24 to 22 AWG
Attenuation 2.6 dB/100 meters @ 1.0 MHz
Differential Characteristic Impedance 120 Ω ±10%

The physical characteristics must meet or exceed ITU specifications.

Appendix E Local Management of Cards in a Remote Un-managed Chassis

This appendix discusses managing the link between an ION Managed Chassis (MC) and an Un-managed Chassis (UC), and performing remote firmware upgrades.

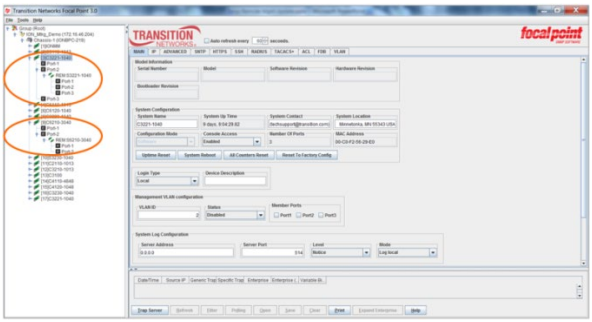
ION x6210 FW v1.2.6 adds support for management of a C6210 when installed in an unmanaged ION chassis. Management is supported by another C6210 installed in a managed chassis when the two are linked together via a fiber cable. FW v1.2.6 also adds support for remote firmware upgrades of a C6210 in an unmanaged chassis.

Previous Status

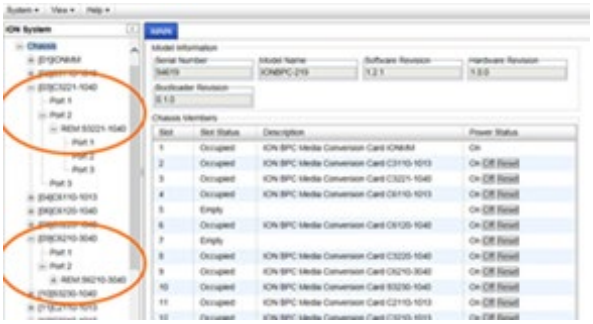
In previous firmware versions (e.g., x6010 / x6020 before v 1.2.6):

- All cards in an ION chassis can be managed via the IONMM.
- Some cards support remote management of a linked stand-alone, in-band, over the fiber, by the card in a local Managed Chassis (MC):
  - Ethernet: x2220, x3220, x3230, x4120
  - TDM: x6010, x6110, x6120, x6210
- Some cards do not support remote management of a linked stand-alone:
  - x2110, x2210, x3100, x3110, x3210, x4110

Local Management of a Remote Unit:



Focal Point



ION System

In firmware versions before v 1.2.6, support includes:

- A local Managed Chassis with an IONMM can manage a remotely managed standalone
- A local Managed Chassis with an IONMM can manage a remotely managed card in a 1- or 2-Slot ION Chassis

Not supported in firmware versions before v 1.2.6:

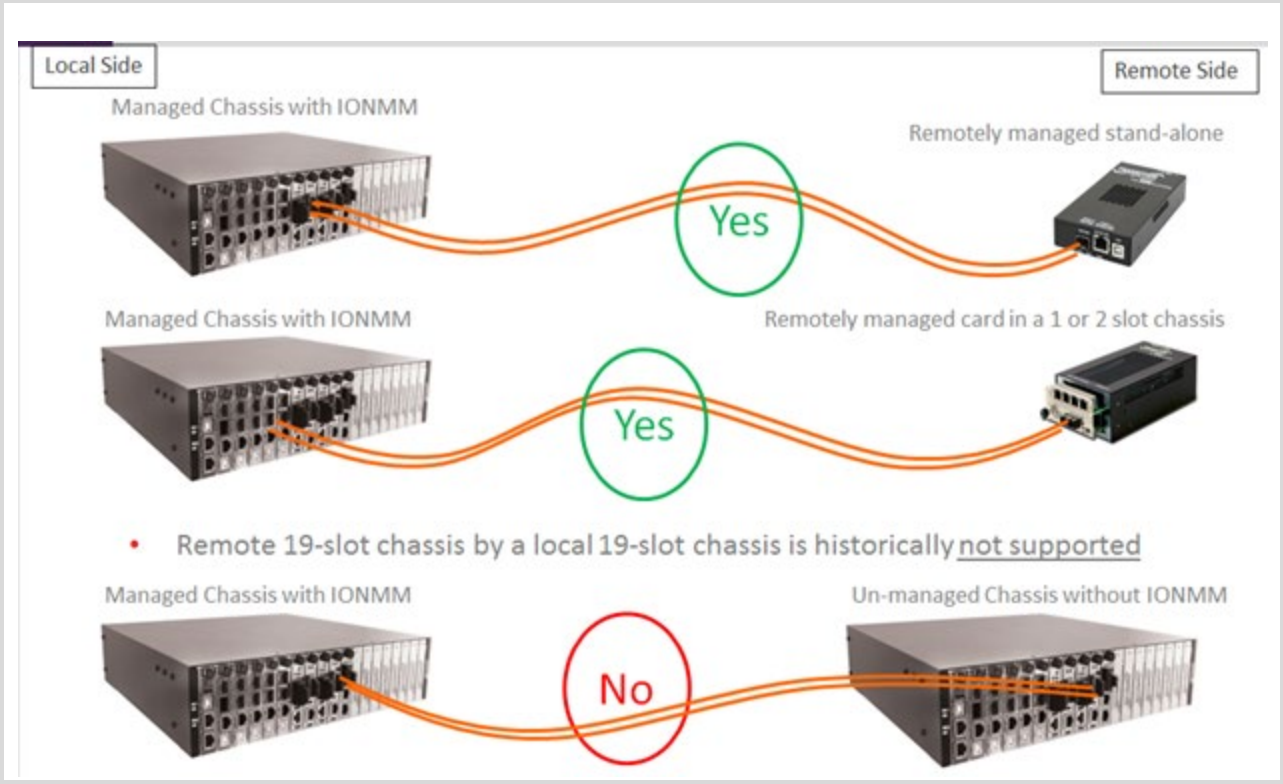
- Remote 19-slot Managed Chassis cannot manage a remote Un-managed Chassis that has no IONMM

In x6010 / x6020 firmware versions v 1.2.6 and after, Managed Chassis (MC) to Un-managed Chassis (UC) is supported with a firmware upgrade to the slide-in-card (S6010/S6020 v 1.2.6).

Note that no firmware upgrade to the IONMM is required.

Previous Management of a Managed Chassis

Previously supported and un-supported configurations are shown below.



New Chassis-to-Chassis Operation

Managed Chassis (MC) to Un-managed Chassis (UC) is now supported with a firmware upgrade to the slide-in-cards. No firmware upgrade to IONMM is required.

1. When a chassis is first powered up, the IONMM boots and sends LLDP discovery packets out to the chassis backplane to let the cards know that this is a managed chassis
   a) If IONMM exists: cards enter normal local management mode
   b) If no IONMM exists: cards enter remote management mode
2. When a managed chassis (MC) is first powered up:
   a) In approximately 40 seconds, the IONMM boots and the x6110 / x6120 / C4120 cards display in the Management interface.
   b) In 50 seconds to 1:25 minutes, the IONMM boots and the OAM Ethernet cards display in the Management interface.
3. During power up of an Un-managed Chassis (UC), the discovery (or non-discovery) of a Management Module takes time:
   a) Time for the TDM cards in the UC to be displayed in the MC: 1:05 minutes.
   b) Time for the remote cards in the UC to show up in the management interface of the MC: 3:40 minutes.

Remote Firmware Upgrade

Remote firmware upgrade of cards in an UC is also supported. **Note** that:

- OAM Ethernet cards are easily upgraded in the field.
- TDM cards and x602x require a boot loader upgrade first:
  - Can only be done in the factory
  - Only needs to be done once, but is required to support future firmware upgrades in the field:
    - C6010: Bootloader 0.1.2
    - C6110/C6120: Bootloader 0.1.3
    - C6210: Bootloader 0.1.2
    - C4120: Bootloader 0.1.3
  - Field firmware upgrades can be done in a MC, and then the cards can be moved to the UC.
  - Field firmware upgrades in the UC cannot be done until the boot loader is upgraded at the factory.

C6010 Series (T1/E1 Copper to Fiber Media Converter):

- Firmware needed: x6010_1.2.6_AP.bin
- Bootloader upgrade is required (x6010_0.1.2_BL.bin)
- Time required for a card to be displayed in the Management interface:
  - Managed Chassis (MC)
    - Inserting a card in a MC takes 0:10 – 0:20 seconds
    - On chassis power up, cards appear in 0:40 – 0:59 seconds
  - Un-managed Chassis (UC)
    - Inserting a card in an UC takes 1:10 minutes
    - Upgrading a card in an UC takes 0:45 seconds

Issues

1. The bootloader upgrade requirement only affects cards in the field.
   a) New production units will already have the bootloader upgrade done in the factory.
2. On initial power up of chassis:
   a) The remote cards will take a few minutes longer to show up in the management display.
   b) Accessing management at a later date, on a chassis that is already powered up is much quicker; delays only occur on initial power up.
3. Adding at card to an already powered up chassis is 40 seconds quicker that times listed, because the IONMM is already booted up.
4. If a chassis is up and running as a remotely located, un-managed chassis, and you decide at a later date to add an IONMM, the chassis will have to be power cycled in order for the cards to report their status to the new local management module.

Default configurations

Default configurations for ION cards are as follows:

Chassis cards (e.g., C2220, C3220, C3221 ...) defaults:

- Remote mode so the IONMM can see them.
- The IP stack is disabled so they don't have an IP address.
- USB is enabled.

Standalone cards S2220, S3220, S3230 defaults:

- Local mode.
- The IP stack is enabled.
- The local IP address is 192.168.0.10.
- USB is enabled.

Standalone cards S3221 and S3221 defaults:

- Remote mode so they can be seen by the IONMM hanging off a port of the local card.
- The IP stack is disabled so they don't have an IP address.
- USB is enabled.

Note: For the Local Management of Cards in a Remote Un-managed Chassis feature to work the card in the remote chassis must be set to "Remote" mode so the IONMM in the local chassis can see it hanging off the port of the local card.

Changing Switch Mode (Local / Remote)

The NID default is changed to Local mode (instead of Remote mode) at ION v 1.3.10. When an ION NID is powered up, it will no longer come up in Remote mode. Instead it will come up in Local mode with DHCP enabled. If a DHCP server is not accessible, it will timeout and revert to the default static IP address 192.168.0.10.

Management and configuration control can be switched between local management control (via CLI, Telnet or Web) or remote management control (via the IONMM). By default, the NID is managed by the IONMM.

The switch mode can only be changed for the NID using the CLI method.

The CLI command **set switch mode={local | remote}** changes the operating mode of a standalone device.

Remote Mode (default mode): the device can only be managed and configured via the IONMM. Setting the switch mode to remote indicates that the device is managed through the IONMM. The device cannot perform any IP management when in 'remote' mode.

Local Mode: the device can only be configured and managed directly via CLI, Telnet or Web. Setting the mode to **local** indicates that the device is managed through either a direct USB connection or a direct network connection via Telnet or the Web interface (i.e., the device is no longer managed by the IONMM).

Note: The x323x NIDs are shipped with switch mode set to "remote."

To change the device switch mode to local, do the following:

1. Start a USB session.
2. At the command prompt type **set switch mode=local**.
3. Press the **Enter** key.
4. Reboot the card for the changes to take effect. At the command prompt type **reboot**.

   Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory remove temporary files (e.g. configuration backup files, Syslog file).
5. Press the **Enter** key to reboot the module.
6. At the command prompt type **show switch mode**.
7. Press the **Enter** key. This displays the device's management mode - local or remote - indicating where the device is managed:
   - **local** – device is managed through direct connection to the device.
   - **remote** – device is managed through the IONMM.

Note: The system cannot show the switch mode on all card types.

Troubleshooting

Message: *Error: System is busy, please retry this command later!*

Symptom: long delay in CLI response for a C601x in a 1 or 2 slot ION chassis.

Meaning: C601x software v1.3.13 adds a new feature that allows a chassis card to be seen in an unmanaged chassis. The card looks for an IONMM in the chassis before completing its initialization, and in a 1 or 2 slot chassis it delays the longest before deciding there isn't an IONMM present.
When setting the card to **Local** mode you must wait for a timeout period of up to 5 minutes.
After the 5 minutes the card comes back and you can set the IP address to static and you will no longer get the error message of the card being “busy”.

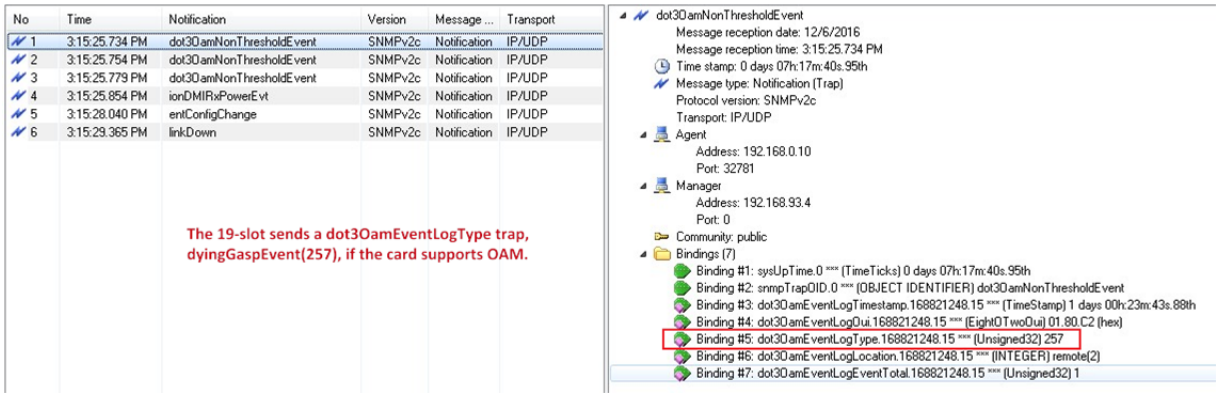
Example:

```
C0|S0|L1D>set switch mode local
Please reboot the card for the changes to take effect!
C0|S0|L1D>reboot
Warning: this command will restart system, connection will be lost and

please login again!

login: ION
Password:
Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C0|S0|L1D>set curr-time="20180118 9:44:50"
Error: System is busy, please retry this command later!
C0|S0|L1D>show ip-mgmt cond fig
Error: System is busy, please retry this command later!
C0|S0|L1D>show system info
Error: System is busy, please retry this command later!

**************************************************
It takes 5 minutes to display the following response:
**************************************************

C0|S0|L1D>
```

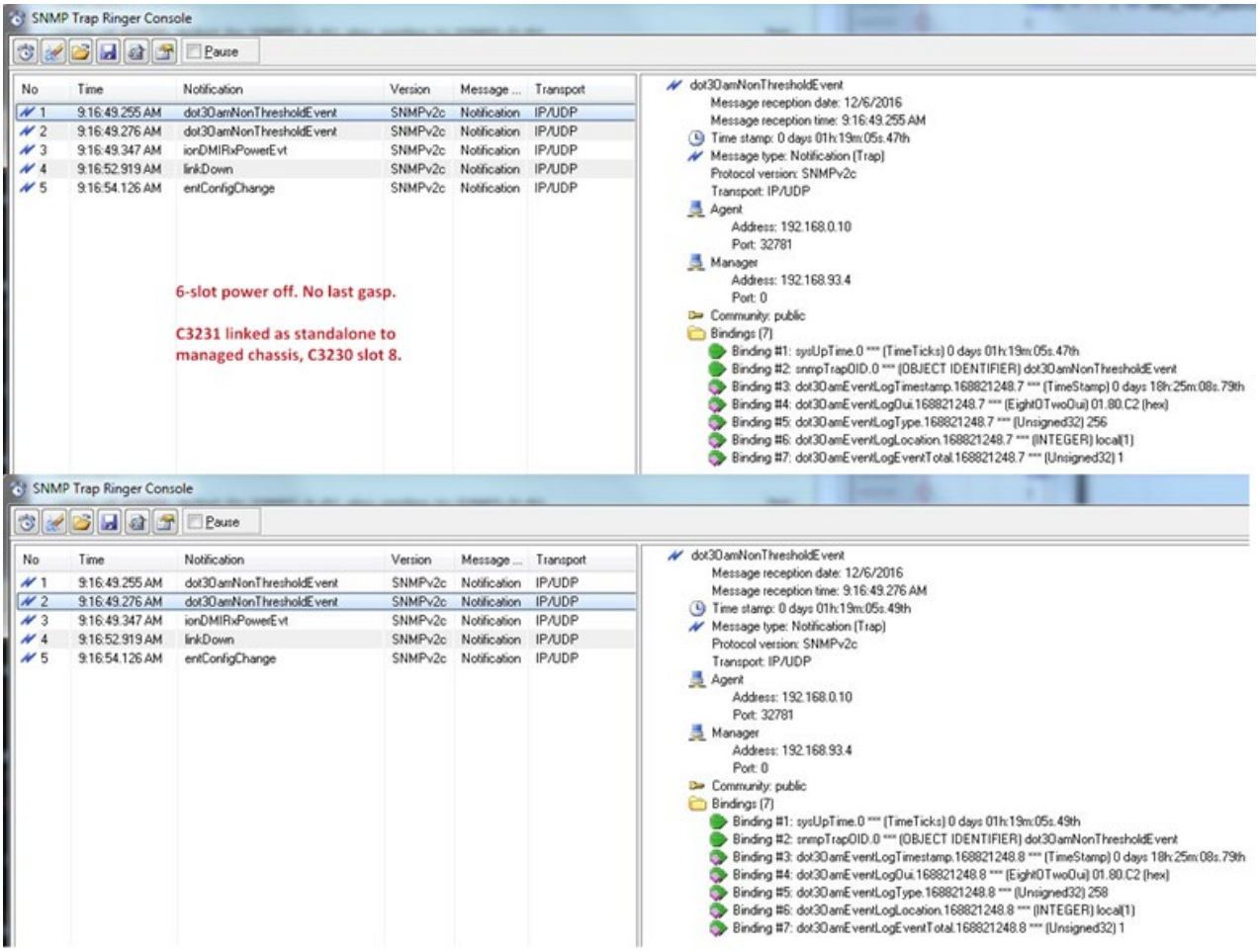
Recovery: Wait 5 minutes for the card to come back and the command prompt to display again.

Traps

The 19-Slot as a Remote Chassis: The ION219-x sends a *dot3OamEventLogType* trap; it also sends a *dyingGaspEvent(257)* **if** the card supports OAM.

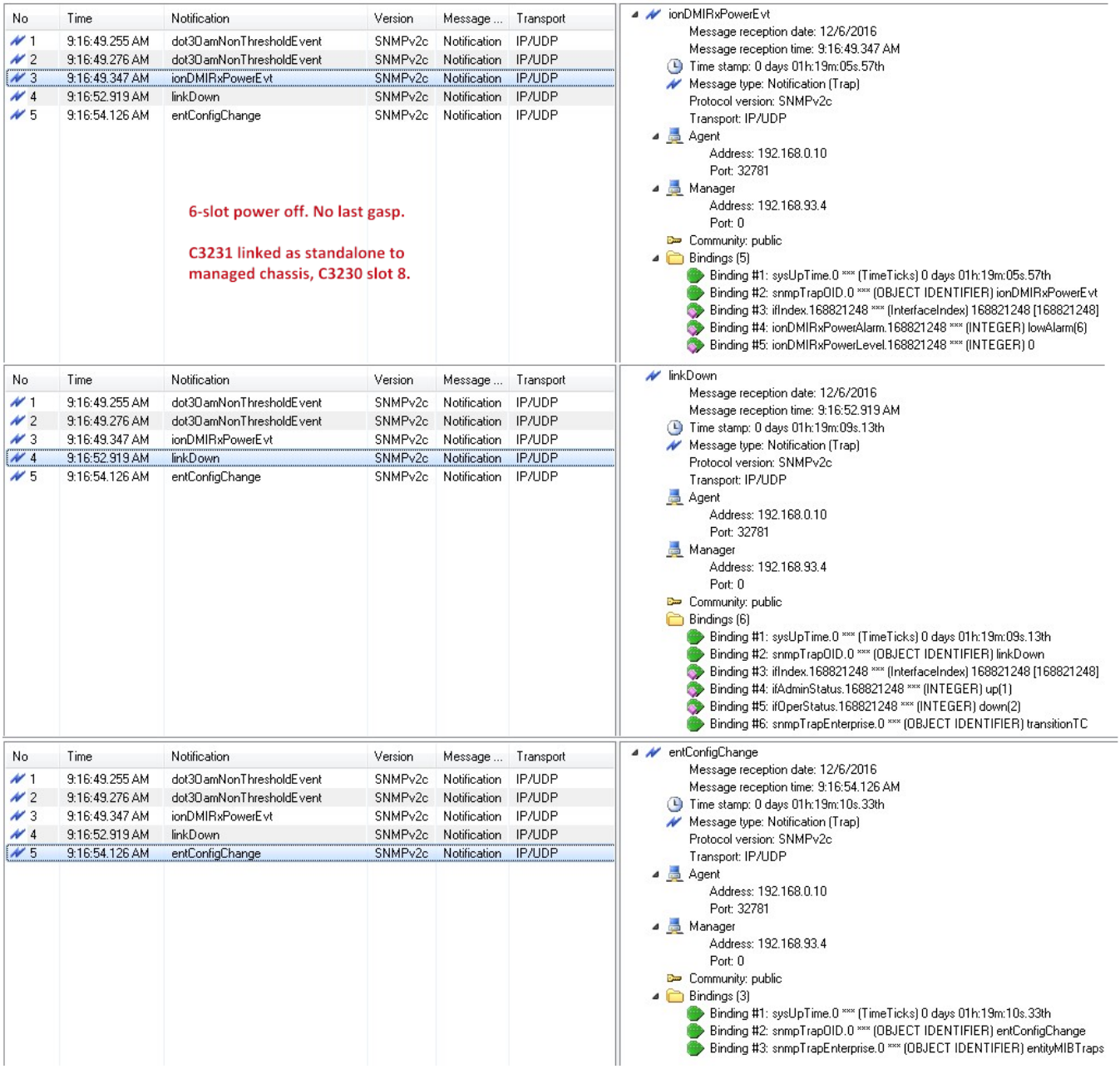


Unmanaged 6-slot with remote C3231 connected to a managed 19-slot, C3230 slot 8. Below are the traps seen by MG-Soft when the ION106-x lost power. There is no last gasp trap.

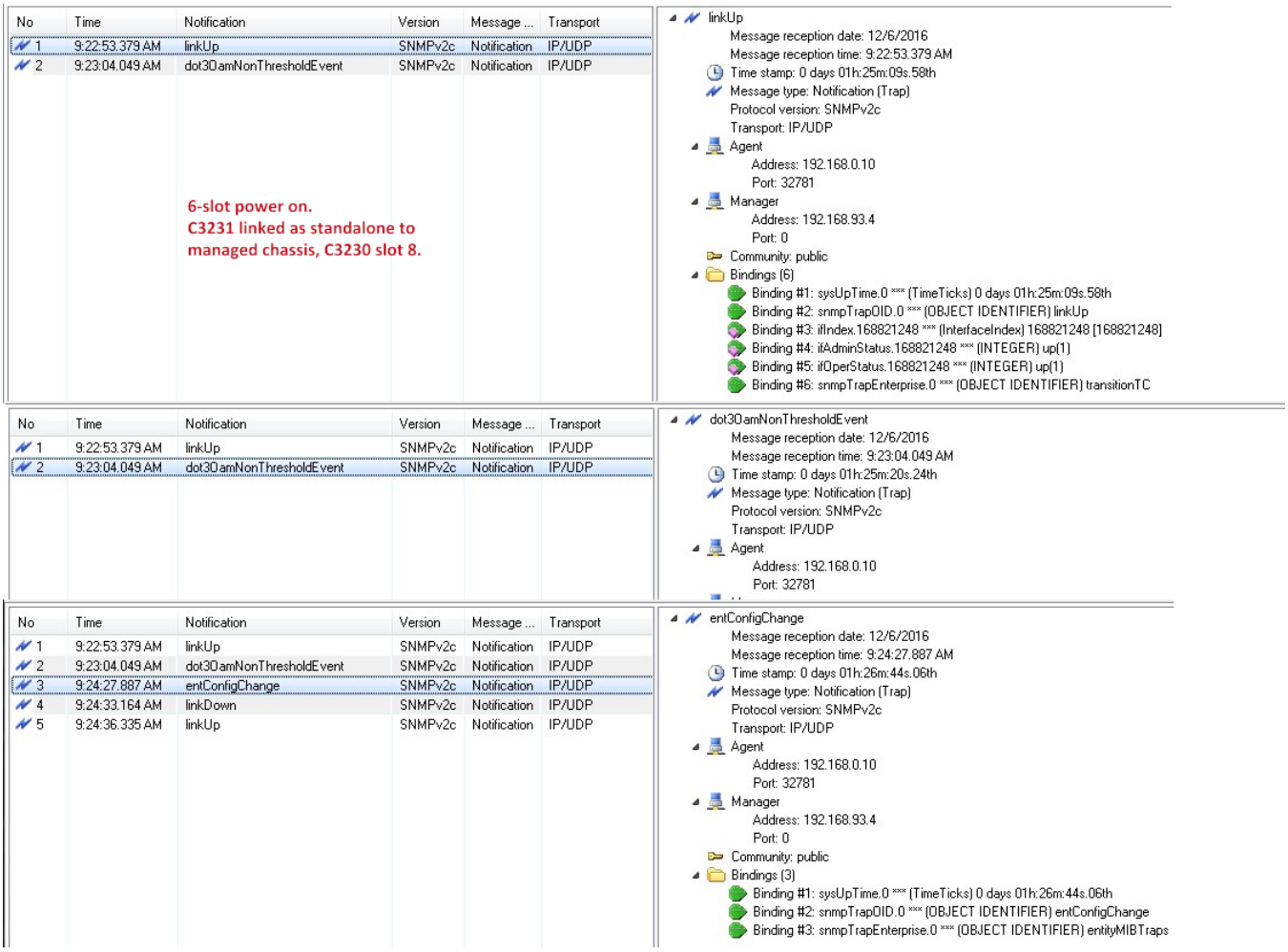


ION106-x power off. No last gasp. C3231 linked as standalone to managed chassis; C3230 in slot 8.

ION106-x power off. No last gasp. C3231 linked as standalone to managed chassis; C3230 in slot 8.



ION106-x power on. C3231 linked as standalone to managed chassis; C3230 in slot 8.



Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.