



ION System x6210 Managed DS3-T3/E3 to Fiber Network Interface Device (NID)

User Guide

Part Number 33495
Revision C September 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 the Lantronix web site at 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	Notes
A	05/01/11	First release for SW Rev 0.6.5, HW Rev 0.0.1, and Bootloader Rev 0.1.1.
B	05/23/12	Revised for software revision 1.2.0.
C	10/6/23	FW v 1.2.5: fix remote device visibility, fix MAC address display after power is lost then restored, and fix loss of SNMP to device. Add support for C6210 management when installed in an unmanaged ION chassis. Management is supported by another C6210 installed in a managed chassis when the two are linked via a fiber cable; add support for remote firmware upgrades of a C6210 in an unmanaged chassis. Add Port description (Copper, Fiber). Enhance recovery time of C612x in a managed chassis in the event of a power outage. FW v 2.0.0: fix chassis slot number was reporting. Add DoC and update specs. Display IONMM system name in ION Stack field. Initial Lantronix rebrand. Change EN 60950-1 to EN 62368-1. Update contact information. Remove 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 lightning transients or power faults. **Do not** connect to inter-building (*outside plant*) link segments subject to lightning.

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 x6210. 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](#) on page 236 for Electrical Safety Warnings translated into multiple languages.

Contents

Cautions and Warnings	3
1: Introduction	8
Typical Application	9
Applicable Standards and RFCs	10
AIS (Alarm Indication Signal)	11
HTTP	14
SNMP MIBs and Traps	19
Models (Chassis and Standalone)	23
S6210 Optional Accessories (sold separately)	24
C6210 Optional Accessories (sold separately)	24
Fiber Specifications	24
Physical Specifications	26
LED Descriptions	28
Jumper Settings	29
DIP Switch Settings	31
Documentation Conventions	33
Related Manuals and Online Help	34
For More Information	34
2: Installation and System Setup	35
General	35
Installing the Chassis Model (C6210)	35
Installing the Standalone Model (S6210)	36
Tabletop Installation	37
Connecting to AC Power	39
Installing SFPs	40
Connecting the C6210 to the S6210	40
Accessing the NIDs	41
Access via Local Serial Interface (USB)	41
Initialization (Default) Configuration	52
3: Management Methods	53
General	53
IONMM Managed x6210s	53
4: Configuration	65
General	65
System Configuration	66
Ports Configuration	68
Port 1 and 2 Configuration – Web Method	69
Port Loopback Tests	71
E3 TDM Mode Configuration	75
Configuring E3 Mode – CLI Method	75
Configuring E3 Mode – Web Method	76
5: Operation	77
General	77
Backup and Restore Operations	77
Note on Remote (L2D) Module Backup, Restore, and Upgrade	78
Backing Up Slide-In and Remote Module Configuration	78
Backing Up Standalone Modules	81
Editing the Config File (Optional)	83
Restoring Slide-In and Remote Modules' Configuration	84
Restoring Standalone Modules	87
Configure / Backup / Restore Provision Module(s) - CLI Method	90

Back Up and Restore File Content and Location	91
Displaying Information	92
Reset to Factory Defaults	92
Resetting Defaults – CLI Method	92
Resetting Defaults – Web Method	93
File Status after Reset to Factory Defaults	94
Resetting Uptime	95
Reset System Uptime – CLI Method	95
Reset System Uptime – Web Method	96
Rebooting – CLI Method	97
Rebooting – Web Method	98
Reboot File Content and Location	99
Upgrade the IONMM and/or NID Firmware	100
Upgrading IONMM and/or NID Firmware – CLI Method	100
Upgrading IONMM and/or NID Firmware – Web Method	102
Upgrading Slide-In and Remote Modules Firmware via TFTP	107
Firmware Upgrade File Content and Location	111
Additional Upgrade Procedures	111
Replacing a Chassis Resident NID	112
6: Command Line Interface (CLI) Reference	113
Command Line Editing	113
Display Similar Commands	113
Partial Keyword Lookup	113
Recall Commands	113
Keystroke Commands	114
Command Descriptions	115
7: Troubleshooting.....	132
Basic ION System Troubleshooting.....	132
Error Indications and Recovery Procedures.....	133
LED Fault and Activity Displays.....	134
Problem Conditions	135
CLI Messages	146
Web Interface Messages.....	170
The Config Error Log (config.err) File.....	182
config.err Messages	183
config.err Message Responses.....	183
Webpage Messages	186
Windows Event Viewer Messages.....	196
ION System Tests.....	197
DMI (Diagnostic Maintenance Interface).....	197
Set Debug Level.....	203
DIP Switches and Jumper Settings	204
PCB Identification	204
x6210 NID.....	204
C6210 NID - PCB 11393 Rev A	209
Third Party Troubleshooting Tools.....	210
Third Party Tool Messages.....	223
HyperTerminal Messages	223
Ping Command Messages	226
Telnet Messages	226
TFTP Server Messages	228
PuTTY Messages	229
DS3-E3 Error Events and Alarm Conditions.....	230
Recording Model Information and System Information	231

Appendix A: Compliance Information	233
Compliance Information.....	233
Declaration of Conformity.....	234
Electrical Safety.....	235
Elektrische Sicherheit.....	235
Elektrisk sikkerhed.....	235
Elektrische veiligheid.....	235
Sécurité électrique.....	235
Sähköturvallisuus.....	235
Sicurezza elettrica.....	235
Elektrisk sikkerhet.....	235
Segurança eléctrica.....	235
Seguridad eléctrica.....	235
Elsäkerhet.....	235
Appendix B: Factory Defaults	236
Appendix C: Configuration Quick Reference – CLI	237
Port Loopback Test – Web Method – T1 and E1 Modes.....	237
Appendix D: Cable Specifications	238
Fiber Cable.....	238
Twisted-Pair Copper Cable.....	238
DS-3 Cable.....	238
E3 Cable.....	238
Appendix E: SNMP MIB Trap Support	239
MIBs List.....	239
MIB Table List / Descriptions.....	240
ifTable.....	240
ionDevSysCfgTable.....	241
ionIfLoopbackTable.....	241
ionIfDMAISTrapTable.....	241
ionDMInfoTable.....	242
ionIfTDMTable.....	243
MIB Traps Summary.....	245
Trap Server Log.....	246
For Additional SNMP MIB Trap Information.....	247

List of Figures

Figure 1a: Typical x6210 User Application (Standalone).....	9
Figure 1b: Typical x6210 User Application (Chassis).....	9
Figure 2: Typical AIS Application.....	11
Figure 3: Loopback on Copper and Fiber port of Media Converter A.....	12
Figure 4: Typical Loopback function on a Fiber port.....	13
Figure 5: Typical Loopback function on a Copper port.....	13
Figure 7: Typical Remote Management Application.....	16
Figure 8: x6210 Remote Management Topology.....	17
Figure 9: Private MIB Objects.....	20
Figure 10: x6210 Models.....	23
Figure 11: C6210 Model Connectors.....	27
Figure 12: S6210 Model Connectors.....	27
Figure 13: x6210 LEDs.....	28
Figure 14: S6210 DIP Switches.....	32
Figure 15 : C6210 DIP Switches.....	32

Figure 16: Chassis Installation	35
Figure 17: Tabletop Installation	37
Figure 18: Wall Mount Installation	38
Figure 19: AC Power Connection	39
Figure 20: SFP Installation	40
Figure 21: CLI Location Hierarchy	54
Figure 22: x6210 PCB Layout	204
Figure 23: SNMP Message Sequence	239

List of Tables

Table 1: HTTP Parameters	14
Table 2: Supported MIBs	19
Table 3a: C6210 Fiber Specifications	24
Table 3b: S6210 Fiber Specifications	25
Table 4: Physical Specifications	26
Table 5: x6210 Connector Descriptions	27
Table 6: Documentation Conventions	33
Table 7: System-Level Menu Description	60
Table 8: Port-Level Menu Description	61
Table 9: Back Up and Restore File Content and Location	91
Table 10: File Status after a Reset to Factory Defaults	94
Table 11: File Content and Location after a System Reboot	99
Table 12: File Content and Location after a Firmware Upgrade	111
Table 13: Keystroke Editing Commands	114
Table 15: DMI Parameters	199
Table 16: Connector Types	201
Table 17: Device-Level Factory Defaults	236
Table 18: Port-Level Factory Defaults	236
Table 19: Supported MIBs	240
Table 20: MIB Traps Summary	245
Table 21: Trap Server Log File Description	247

1: Introduction

Document Overview

This manual provides the user with an understanding of the Lantronix x6210 Network Interface Device (NID).

Product Overview

The ION DS3 (x6210) copper-to-fiber with remote management NID card is a copper-to-fiber NID that can extend the point of presence of a DS3 or E3 connection or connect remote locations via T3/E3.

The x6210 NIDs are designed as either a standalone module (S6210) or a slide-in / chassis-mount module (C6210) that is installed in an ION system chassis. The x6210 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 used to further increase the bandwidth capacity of the fiber infrastructure.

The x6210 NIDs must be used in pairs. A typical installation will include a chassis card installed in the ION Platform locally and a stand-alone device installed at the remote location.

Features

The x6210 provides the following services and functions.

- AIS (Alarm Indication Signal): all ones or blue detected on both ports
- AIS generated in both directions: selectable blue or all ones
- Loopback on fiber or copper ports
- Coax line build out
- Switch selectable DS3/T3 or E3 rate
- Firmware upgrade
- Remote management
- LED indications for all operation modes
- Supports fractional/channelized DS3/E3

You can manage the following x6210 services and functions via the software:

- Report Model information, such as serial no, model no, firmware revision, etc.
- Report link status on copper and fiber port
- Report LBO status
- Report AIS detected status on copper and fiber port
- Loopback enable/disable on copper or fiber port
- AIS enable/disable on copper and fiber port
- AIS signal format selectable: all ones or blue
- DMI on Fiber port

Typical Application

The x6210 applications shown below include a chassis-based (C6210) environment and a standalone (S6210) environment.

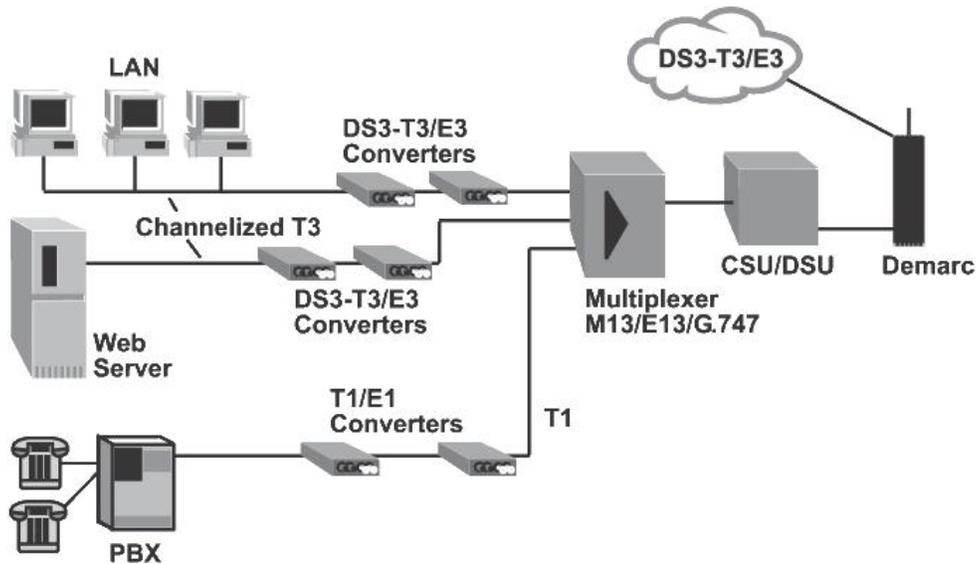


Figure 1a: Typical x6210 User Application (Standalone)

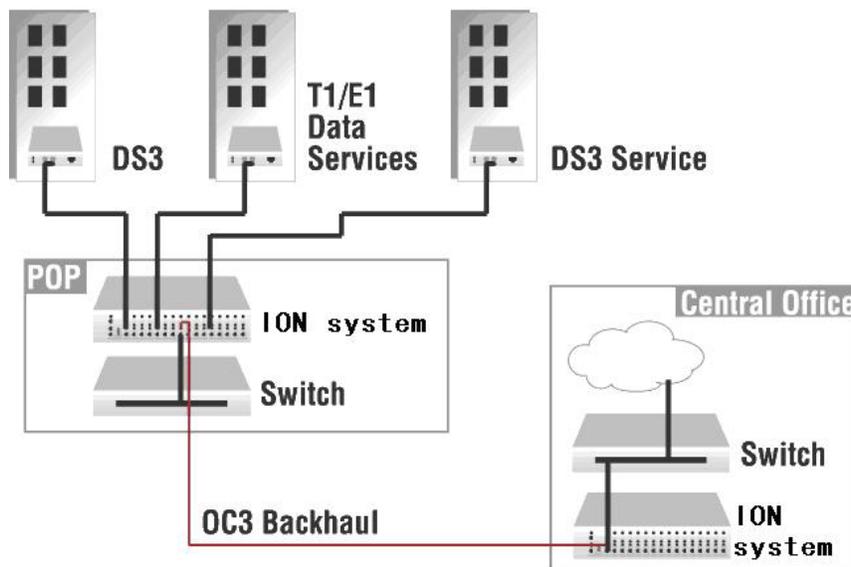


Figure 1b: Typical x6210 User Application (Chassis)

Applicable Standards and RFCs

The x6210 complies with the following hardware standards:

- ANSI T1.102 -1993; ETSI TBR-24
- ITU-T G.823 for jitter tolerance; G.775 for loss of signal
- GR-499 CORE & GR-253-CORE
- Regulatory Compliance for Emission: CISPR/EN55022 Class A, FCC Class A
- Regulatory Compliance for Immunity: EN55024
- Safety Compliance: Unit: CE Mark, EN 62368-1

The x6210 complies with the following IETF RFCs:

- HTTP protocol per RFC 2616
- SNMP protocol per RFC 1157, RFC 1158, RFC 2578
- TFTP protocol per RFC 1350

Feature Descriptions

The ION x6210 features are described in the following sub-sections.

Compatibility with ION System and Point System

An ION module can be linked to a Point System Module over fiber, and Point System modules can be installed in an ION chassis by using a Point System Adapter Card.

The ION chassis backplane powers the Point System modules, allowing the module to perform its copper-to-fiber media converter functions. Note the following caveats:

- A C6210 card can only run in an ION chassis system. It is not compatible with Point System.
- An S6210 is used as a remote device and can only be remotely managed by an ION system that is operating in software mode.
- A Point System DS3 card can be inserted into an ION chassis with the Point System Adapter Card, but it can only pass data and it can only be managed by the Point System web interface or Focal Point. The ION web interface and FP 3.0 do not provide support to manage the Point System DS3 card.
- The fiber link connection between a Point System CCSCF3013-110 and the ION S6210-3013 is not supported.
- A C6210 card can only be managed by FP3.0. It cannot be managed by FP2.2.
- The ION DS3 (x6210) card can only support 1 level remote management. The maximum cascade level of S6210 is 1 level (up to level-2). The maximum Coax line length is 1000 feet.

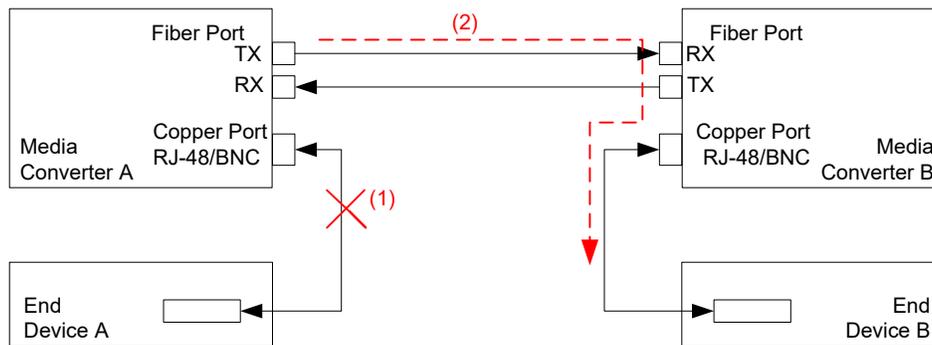
AIS (Alarm Indication Signal)

The x6210 provides AIS (Alarm Indication Signal) support.

When the x6210 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 x6210 can generate the AIS with two formats: All ones (1111... sequence), or Blue (1010... sequence).

You can enable or disable AIS transmit on each x6210 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

If AIS transmit is enabled, both the Copper port and the Fiber port will transmit an AIS signal if it detects signal lost; otherwise, both Copper and Fiber ports will not transmit AIS signal if AIS transmit is disabled. See the “[LED Descriptions](#)” section on page 30.

If the AIS transmit function is enabled and one port detects signal loss, the x6210 will transmit AIS signal to the receiving End Device, using the selected AIS format (All ones or Blue); if AIS function is disabled, no action is performed.

If the x6210 receives an AIS signal from one port, the SDC/SDF (Signal Detect on Copper/Fiber) LED displays as yellow to indicate AIS is detected on that port. See the “[LED Descriptions](#)” section on page 30. Software will send out AIS detected trap at the same time.

As shown in Figure 2 above, if Media Converter A detects a signal lost on the Copper port and the AIS function is enabled on that port, Media Converter A will transmit the AIS signal to Media Converter B via 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.

Loopback Test

The x6210 provides Loopback (LB) test support. The Loopback feature puts the x6210 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 x6210 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).

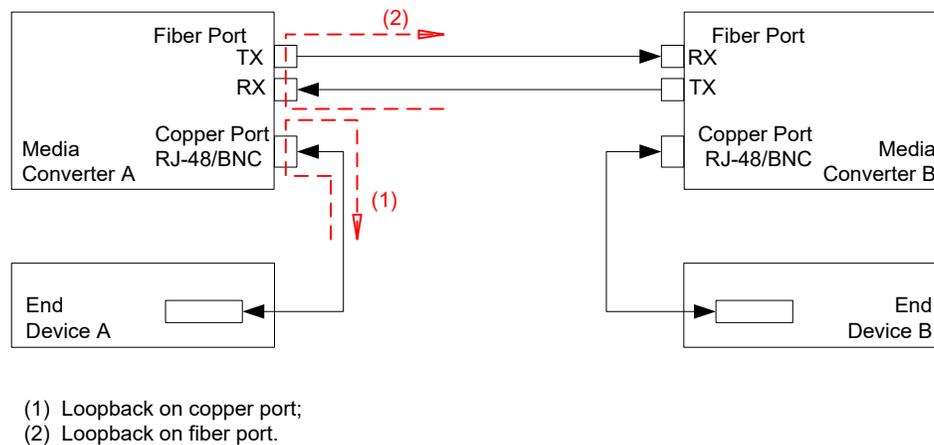


Figure 3: Loopback on Copper and Fiber port of Media Converter A

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 x6210 Loopback function cannot be enabled on both copper and fiber ports at the same time; an error message displays if attempted.

A typical x6210 Fiber port Loopback applications is shown below.

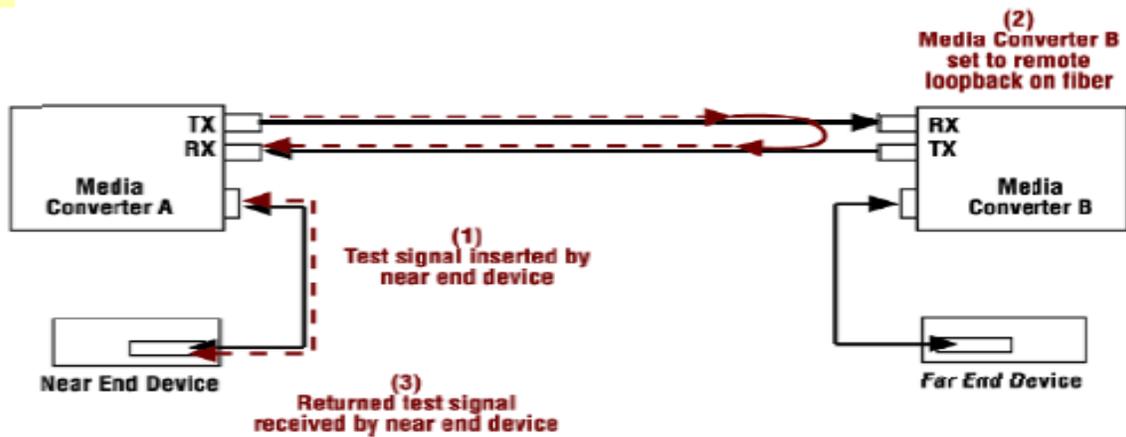


Figure 4: Typical Loopback function on a Fiber port

A typical x6210 Copper port Loopback applications is shown below.

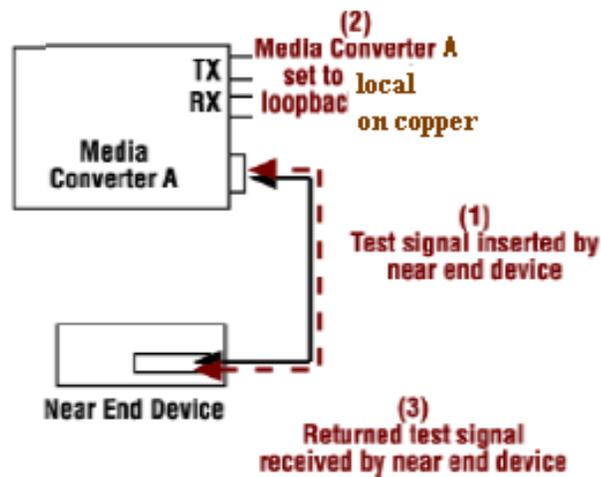


Figure 5: Typical Loopback function on a Copper port

HTTP

You can manage the x6210 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		
Serial number	Read only	
Model number	Read only	
Software Revision	Read only	
Hardware Revision	Read only	
Bootloader Revision	Read only	
System Name	Read & Write	
System Uptime	Read only	
Configuration Mode	Read only	Hardware / Software
Number of Ports	Read only	
System Reboot	Button	
Reset to Factory Defaults	Button	
DS3 mode	Read only	DS3 / E3 / STS-1
- AIS transmit	Read & Write	Enable / Disable
- AIS format	Read & Write	All Ones / Blue
Fiber Port		
- Link	Read only	Down / Up
- Alarm Indication Signal	Read only	Normal / Alarm
- Loopback	Read & Write	Enable / Disable
- Connector	Read only	Connector description string
- DMI		
DMI ID	Read only	
Connector Type	Read only	
Nominal Bit Rate	Read only	

Parameter	Property	Range
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	
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
- Alarm Indication Signal	Read only	Normal / Alarm
- Loopback	Read & Write	Enable / Disable
- Line build out	Read only	LBO description string
- Connector	Read only	Connector description 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.

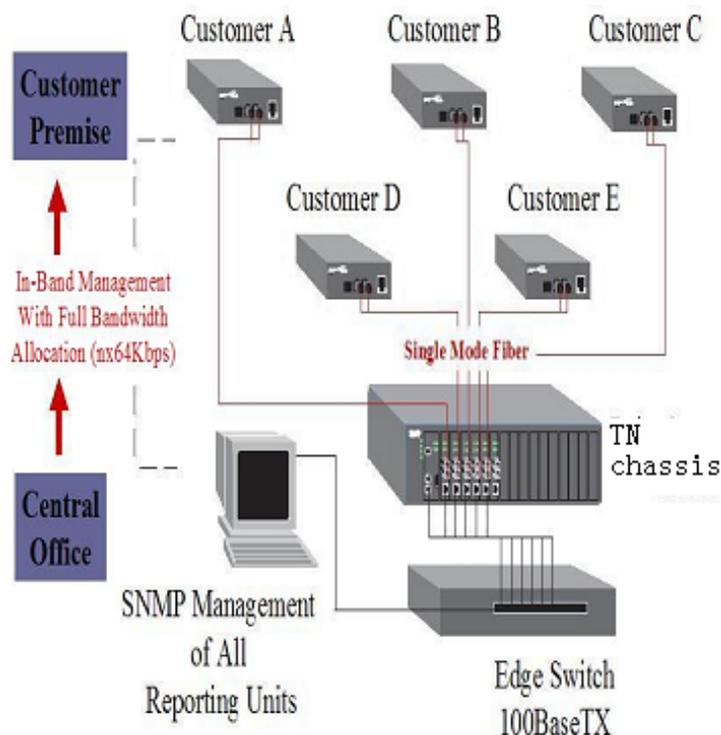


Figure 7: Typical Remote Management Application

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

A remote S6210 device connects to a local C6210 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 x6210 Remote Management (RM) protocol lets applications exchange management traffic between local C6210 and remote S6210 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 C6210 and packet TX/RX redirection on the S6210, eliminating the differences between the C6210 and S6210 for the IONMM and its upper layer applications.

Note that the current ION platform supports up to one level of x6210 device remote management.

All management traffic between the IONMM and the remote S6210 are relayed and forwarded through the local C6210. Traffic between the IONMM and C6210 is exchanged on the ION chassis' backplane Ethernet bus (BPC), while traffic between the local C6210 and remote S6210 is exchanged on the specific management channel (see figure below).

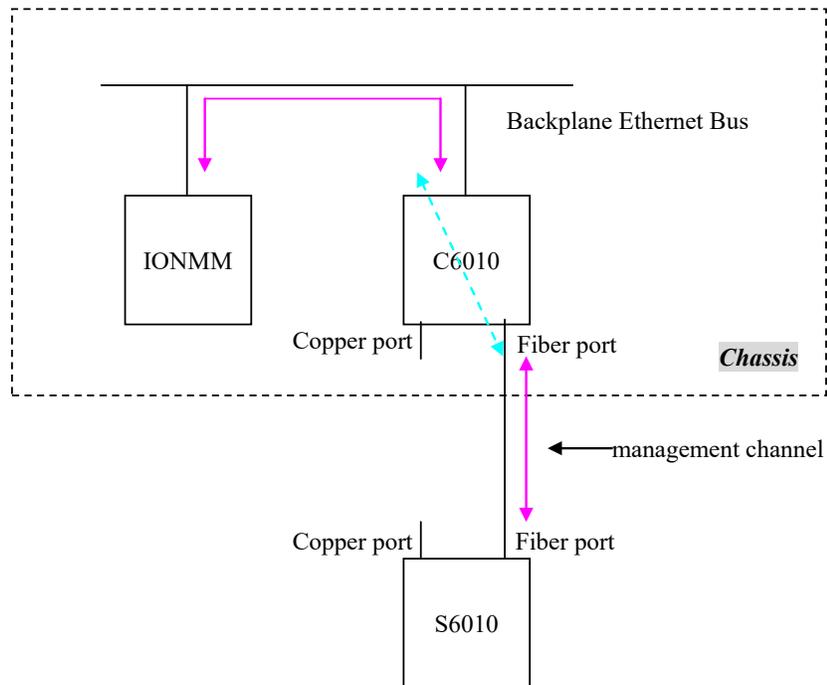


Figure 8: x6210 Remote Management Topology

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 x6210 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 x6210 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 x6210 has two parts that need to be upgraded; one is the device firmware 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 x6210 to a specific revision via the IONMM, which means the x6210 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 x6210 and IONMM is corrupted, causing an upgrade protocol timeout.
- No valid firmware file stored in the IONMM (e.g., no specified x6210 firmware revision, or a corrupted firmware file).
- The firmware revision is same.
- Programming the internal Flash fails.

If the x6210 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 x6210 finishes upgrading successfully, it reboots itself and the bootloader checks the firmware again. If it passes, the x6210 loads the new firmware and enters normal operating mode. Otherwise, the x6210 returns to Upgrade mode.

The three methods of x6210 firmware upgrades are:

- Web interface
- Focal Point
- CLI command

A remotely-managed x6210 can be upgraded remotely as mentioned above. Note that the current ION platform supports up to one level of x6210 device remote management.

Management Access Methods

Management of the x6210 is accomplished through one of the following methods.

- Universal Serial Bus (USB) – uses a command line interface (CLI) to access and control the x6210 through a locally connected workstation.
- Telnet session – uses the CLI to access and control the x6210 via 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.

SNMP MIBs and Traps

The x6210 can be managed with the SNMP v1 or v2 protocol via the IONMM.

SNMP MIBs

The x6210 NID provides complete management through the SNMP interface. It supports the following standard MIBs for management using SNMPv1/v2 as shown in the table below.

Table 2: Supported MIBs

#	MIB	RFC # or Private	Description
1	ionDevSysCfgTable		
2	ifTable		
3	ifXTable		
4	ionDMInfoTable		
5	ionIfLoopbackTable		
6	ionIfTDMTable		Used for ION T1/E1/DS3, including fields such as AIS, LBO, etc.)

The Trap functions and status reporting is described below.

1) Link status change on copper and fiber ports:

- The x6210 sends a **link up** trap only once if the Copper/Fiber port link status changes from link down to up;
- The x6210 sends a **link down** trap only once if the Copper/Fiber port link status changes from link up to down.

2) AIS detected on copper and fiber ports:

- The x6210 sends an **AIS trap** only once if the Copper/Fiber port detects an AIS signal; a parameter indicates AIS detected should be carried in trap message.
- The x6210 sends an **AIS trap** only once if the Copper/Fiber port detects the AIS signal has disappeared; a parameter indicates AIS disappeared should be carried in trap message.

3) DMI trap:

- An *ionDMIRxIntrusionEvt* event is sent if the *ionDMIRxPowerLevel* falls below the *ionDMIRxPwrLvlPreset* indicating an intrusion on the fiber.
- An *ionDMIRxPowerEvt* event is sent when there is a warning or alarm on Rx Power.
- An *ionDMITxPowerEvt* event is sent when there is a warning or alarm on Tx Power.
- An *ionDMITxBiasEvt* event is sent when there is a warning or alarm on Tx Bias current.
- An *ionDMITemperatureEvt* event is sent when there is a warning or alarm on DMI temperature.

The x6210 will keep sending **DMI** traps until it becomes normal. Like the other ION SICS, the x6210 will periodically send out the specific trap every 3 seconds until the trap event condition is not met.

The Focal Point (FP) integrated SNMP management / Trap server tool is not launched in the FP initialization procedure. You can launch this function when needed. The FP SNMP tool shows the traps it receives; no further action is performed in terms of notification of trap events.

The FP Trap messages include following content:

Date/Time	SourceIP	Generic Trap	Specific Trap	Enterprise	Variable Bindings
-----------	----------	--------------	---------------	------------	-------------------

The FP display format is:

Date/Time	SourceIP	Generic Trap	Specific Trap	Enterprise	Variable Bindings
Fri Apr 17:43:35 2010	172.16.6.3	Notification	Linkup		...
Fri Apr 17:44:45 2010	172.16.6.3	Notification	Linkdown		...

Downloading, Compiling and Integrating MIBs

You can download industry standard MIBs from <http://www.ietf.org>. To download ION system private MIBs:

1. Go to the [ION downloads page](#) and select **SNMP MIBs**.
2. In the search box, enter the model number.
3. Click the linked MIB Name (e.g., **MIBs v1.3.8**).
4. At the **File Download** window, click **Save As**.
5. Navigate to the desired save location and click **Save**. The downloaded file is saved to the specified folder location.
6. At the specified file location, extract /unzip the MIB file.
7. If you plan to integrate the ION system with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView, you must compile the ION system MIBs with the HP OpenView NMS (Network Management System). See the NMS documentation for compiler instructions.
8. While working with MIBs, be aware that:
 - a. Mismatches on datatype definitions can cause compiler errors or warning messages.
 - b. The MIB datatype definitions are not mismatched; however, some standard RFC MIBs do mismatch.
 - c. If your MIB compiler treats a mismatch as an error, or if you want to delete the warning message, refer to the “[Technical Support](#)” section on page 235.

Set up your ION system SNMP configuration via the command line interface (CLI). Refer to “[Configuring SNMP](#)” on page 214. See “[Section 6: Command Line Interface \(CLI\) Reference](#)” on page 125.

See also “[Appendix E: SNMP MIB Trap Support](#)” on page 246.

Models (Chassis and Standalone)

The x6210 models include Chassis (slide in card or SIC) and Standalone models. The Chassis models have a prefix of **C** (e.g., C6210) and the Standalone models have a prefix of **S** (e.g., S6210).

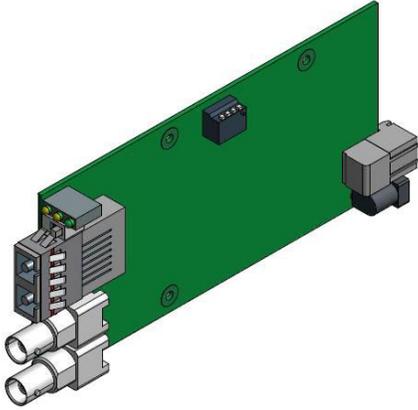
Chassis Models (C6210-xxxx)	Standalone Models (S6210-xxxx)
 <p data-bbox="423 879 570 909">C6210-30xx</p>	 <p data-bbox="1045 873 1192 903">S6210-301x</p>
 <p data-bbox="423 1394 570 1423">C6210-3040</p>	 <p data-bbox="1045 1386 1192 1415">S6210-3040</p>

Figure 10: x6210 Models

S6210 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 ([SPS-2460-SA](#)).

Wall Mounting: WMBL Wall Mount Bracket 4" [102 mm] ([WMBL](#)).

Wall Mounting: WMBD DIN Rail Bracket 5" [127 mm] ([WMBD](#)).

Rack: E-MCR-05 12-Slot Media Converter Rack ([E-MCR-05](#)).

Shelf: RMS19-SA4-02 4-Slot Media Converter Shelf ([RMS19-SA4-02](#)).

C6210 Optional Accessories (sold separately)

SFP Modules: SFP port uses standard 100Base-x/oc-3 SFP. See the [Lantronix SFP webpage](#).

Fiber Specifications

For the latest information go to the Lantronix [Optical Devices SFP Specifications](#) page to display the specs.

You can also view our full [Optical Devices Product Catalog](#).

Table 3a: C6210 Fiber Specifications

Model	Description	Fiber Connector
C6210-3011	1300nm multimode (ST) [2 km/1.2 miles]	TN#13221 (1x9, 1310nm, ST, MM, 3.3V)
C6210-3013	1300nm multimode (SC) [2 km/1.2 miles]	TN#13222 (1x9, 1310nm, SC, MM, 3.3V)
C6210-3014	1310nm single mode (SC) [20 km/12.4 miles]	TN#13223 (1x9, 1310nm, SC, SM, 3.3V)
C6210-3015	1310nm single mode (SC) [40 km/24.9 miles]	TN#13224 (1x9, 1310nm, SC, SM LH, 3.3V)
C6210-3016	1310nm single mode (SC) [60 km/37.3 miles]	TN#13226 (1x9, 1310nm, SC, SM XL, 3.3V)
C6210-3017	1550nm single mode (SC) [80 km/49.7 miles]	TN#13225 (1x9, 1550nm, SC, SM LW, 3.3V)
C6210-3029-A1	1310nm TX / 1550nm RX single fiber single mode (SC) [20km/12.4 miles]	TN#13229 (1x9, 1550nm, SC, SM XXL, 3.3V)
C6210-3029-A2	1550nm TX / 1310nm RX single fiber single mode (SC) [20 km/12.4 miles]	TN#13230 (1x9, 1550nmTX/1310nmRX, SC, SM SF 20K, 3.3V)
C6210-3029-B1	1310nm TX / 1550nm RX single fiber single mode (SC) [40 km/24.9 miles]	TN#13231
C6210-3029-B2	1550nm TX / 1310nm RX single fiber single mode (SC) [40 km/24.9 miles]	TN#13232
C6210-3040	SFP version	NA

Fiber Connectors with SFF-8472 DMI management:

TN#xxxxx 12-Pin, 1310nm, SC, SM, 3.3V, SFF-8472

TN#xxxxx 12-Pin, 1550nmTX/1310nmRX, SC, SM SF 20K, 3.3V, SFF-8472

TN#xxxxx 12-Pin, 1310nmTX/1550nmRX, SC, SM SF 20K, 3.3V, SFF-8472

Table 3b: S6210 Fiber Specifications

Model	Description	Fiber Connector
S6210-3011	1300nm multimode (ST) [2 km/1.2 miles]	TN#13221 (1x9, 1310nm, ST, MM, 3.3V)
S6210-3013	1300nm multimode (SC) [2 km/1.2 miles]	TN#13222 (1x9, 1310nm, SC, MM, 3.3V)
S6210-3014	1310nm single mode (SC) [20 km/12.4 miles]	TN#13223 (1x9, 1310nm, SC, SM, 3.3V)
S6210-3015	1310nm single mode (SC) [40 km/24.9 miles]	TN#13224 (1x9, 1310nm, SC, SM LH, 3.3V)
S6210-3016	1310nm single mode (SC) [60 km/37.3 miles]	TN#13226 (1x9, 1310nm, SC, SM XL, 3.3V)
S6210-3017	1550nm single mode (SC) [80 km/49.7 miles]	TN#13225 (1x9, 1550nm, SC, SM LW, 3.3V)
S6210-3029-A1	1310nm TX / 1550nm RX single fiber single mode (SC) [20 km/12.4 miles]	TN#13229 (1x9, 1550nm, SC, SM XXL, 3.3V)
S6210-3029-A2	1550nm TX / 1310nm RX single fiber single mode (SC) [20 km/12.4 miles]	TN#13230 (1x9, 1550nmTX/1310nmRX, SC, SM SF 20K, 3.3V)
S6210-3029-B1	1310nm TX / 1550nm RX single fiber single mode (SC) [40 km/24.9 miles]	TN#13231
S6210-3029-B2	1550nm TX / 1310nm RX single fiber single mode (SC) [40 km/24.9 miles]	TN#13232
S6210-3040	SFP port	NA

Fiber Connectors with SFF-8472 DMI management:

TN#xxxxx 12-Pin, 1310nm, SC, SM, 3.3V, SFF-8472

TN#xxxxx 12-Pin, 1550nmTX/1310nmRX, SC, SM SF 20K, 3.3V, SFF-8472

TN#xxxxx 12-Pin, 1310nmTX/1550nmRX, SC, SM SF 20K, 3.3V, SFF-8472

See “[Appendix D: Cable Specifications](#)” on page 244 for more fiber specs.

Physical Specifications

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

Table 4: Physical Specifications

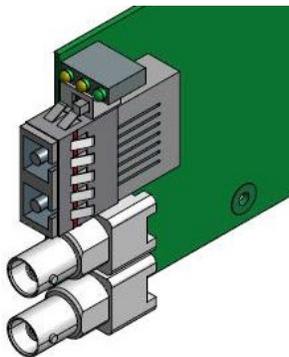
Data Rates	E3 = 34.4 Mb/s DS3 = 44.7 Mb/s STS-1 = 51.8 Mb/s
Coax Interface	Two 75 ohm Coax connectors – TX and RX
Fiber Port	Connectors supported: 1x9, SFP Fiber Connectors SFP: LC connector Uses standard 100Base-X/OC-3 SFP Fixed Optics: ST or SC connector
Dimensions	C6210: 1" x 3.3" x 6.1" (2.54 cm x 8.382 cm x 15.5 cm) HxWxD S6210: 0.9" x 3.4" x 6" (2.3 cm x 8.6 cm x 15.2 cm) HxWxD
Power Consumption	C6210: 2.5 Watts S6210: 2.4 Watts
Power Supply	C6210: From ION chassis backplane (slide-in card) S6210: 7.5 to 15.9 VDC (SPS-2460-SA)
Environment	C6210: See ION chassis specifications S6210: Operating Temp: -10°C to +65°C. Humidity: 5% to 95% (non-condensing). Altitude: 0 – 10,000 ft.
Shipping Weight	C6210: 1 lb. (0.45 kg.) S6210: 2 lbs. [0.90 kg]
MTBF	C6210: Greater than 250,000 hours (MIL-HDBD-217F). Greater than 687,000 hours (Bellcore) (C6210-3040 (1DS3 & SFP port; up to OC3 rate). S6210: 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).
Warranty	Lifetime

Connectors

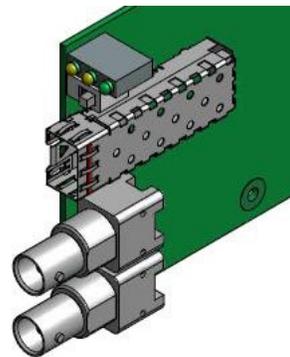
The x6210 connectors are described in the table below. For cable specifications see “[Appendix D: Cable Specifications](#)” on page 242.

Table 5: x6210 Connector Descriptions

Connector Label	Description
FIBER TX / RX	ST or SC for fiber media connection. Fiber is only supported on models with SFP.
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.
COAX TX / RX	PORT 1; Two BNC connectors: Coax ports for Coaxial cable transmit & receive connection.



C6210-30xx



C6210-3040

Figure 11: C6210 Model Connectors



S6210-30xx



S6210-3040

Figure 12: S6210 Model Connectors

LED Descriptions

The x6210 LEDs are described below.

PWR (Power)	Device Power on/off indication: Green – On (lit) when power is applied to the board.
SDF (Fiber)	Fiber Signal Detect/AIS: Green – On (lit) if Fiber link is up Green – Blinking indicates Fiber is in fiber loopback mode Yellow – On (lit) for AIS (unframed) detected
SDC (Copper)	Coax Signal Detect/AIS: Green – ON indicates Coax link is up Green – Blink indicates Coax is in copper loopback mode Yellow – ON for AIS (unframed) detected

The x6210 LEDs are shown below.



S6210 LEDs



C6210 LEDs

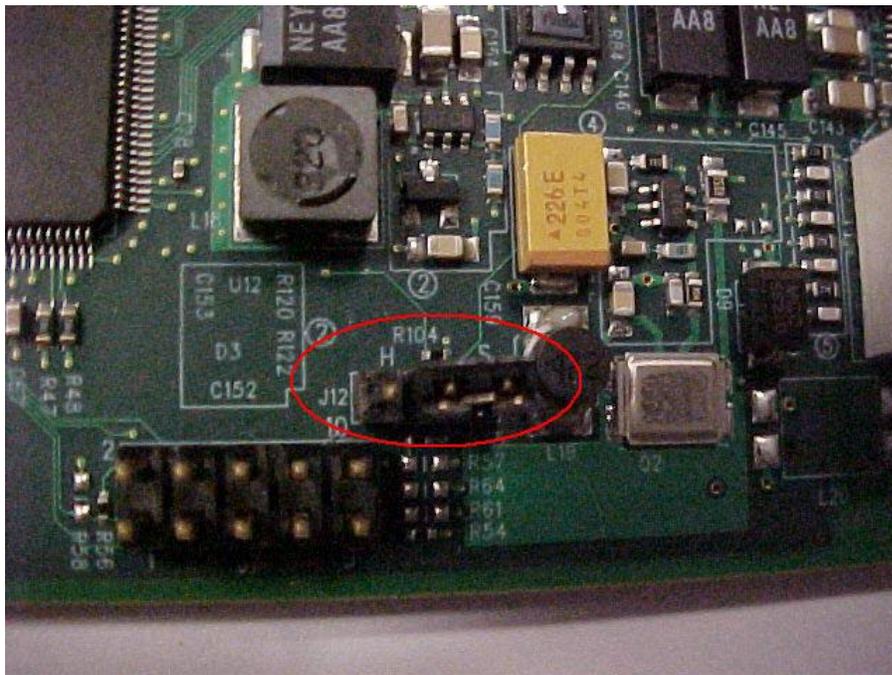
Figure 13: x6210 LEDs

Jumper Settings

The x6210 jumper settings are shown and described below.

Jumper J12 (Hardware/Software Configuration Mode)

Jumper J12 sets the x6210 operating mode to either hardware or software configuration control mode. The default setting is Software operating mode (J12 pins 2 and 3 jumpered).



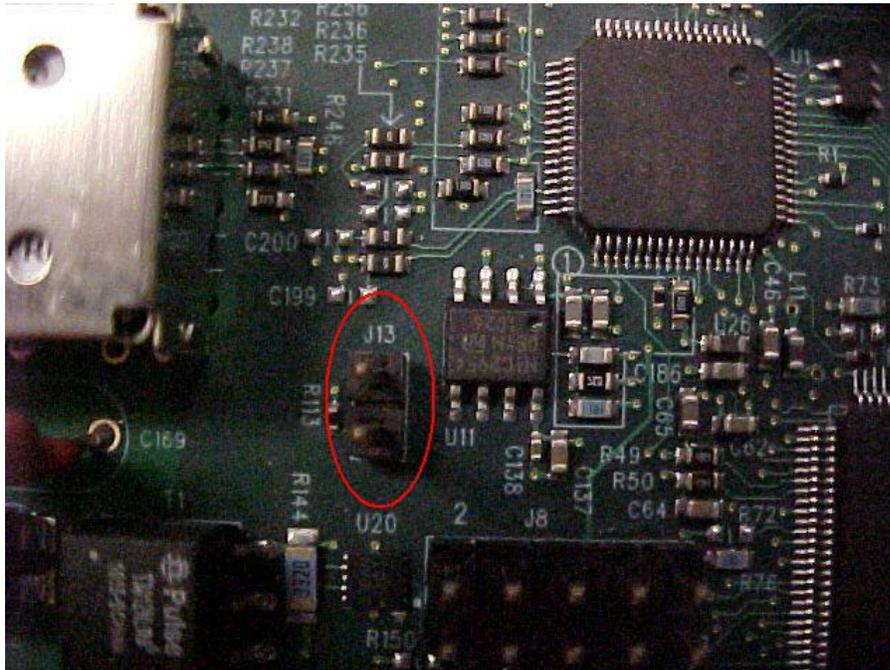
<u>Jumper Pin #s</u>	<u>Sets Mode to</u>	<u>Note</u>
1-2	Hardware mode	Places the x6210 in Hardware operating mode; the <u>hardware</u> can configure the x6210.
2-3	Software mode	Places the x6210 in Software operating mode; the <u>software</u> can configure the x6210 (the default setting).

For more information, see “[DIP Switches and Jumper Settings](#)” on page 206.

Jumper J13 (DS3 / STS-1 Mode Select)

Jumper J13 sets the x6210 STS-1 on or off. The default is STS-1 Off (not jumpered). The SW-1 (position-1) is used with J13 to define the x6210 operating mode.

Synchronous Transport Signal 1 (STS-1) or OC-1, operates at 51.84 Mbps. STS-1 is one of several x6210 TDM / device type options; the STS-1 rate is 51.8Mbps (the other rate options are T1=1.544MHz, E1=2.048MHz, E3 = 34.4Mbps, and DS3 = 44.7Mbps). Note: STS-1 mode is not currently supported.



J13 Pins 1 & 2	Mode	Note
Not jumpered	STS-1 Off	DS3 selected (the default setting).
Jumpered	STS-1 On	STS-1 selected (shorting plug installed - not currently supported).

For more information, see “[DIP Switches and Jumper Settings](#)” on page 206.

DIP Switch Settings

A multi-position DIP switch allows the network administrator to configure the x6210 for network conditions. Use a small flat blade screwdriver or similar device to set these switches for site installation. For more information, see “[DIP Switches and Jumper Settings](#)” on page 206.

The x6210 DIP switch settings are described below.

4-Position DIP Switch SW2

SW1 – DS3/E3: used with Jumper J13 to define the x6210 operating mode.

*Up (OPEN) = DS3 mode.

Down = E3 mode.

SW2 – Coax Line Build Out:

*Up (OPEN) = less than 255 feet of cable.

Down = greater than 255 feet of cable.

SW3 – AIS transmit:

*Up (OPEN) = transmit AIS if receive loss of carrier.

Down = don't transmit AIS.

SW4 – AIS Format - AIS Blue / AIS All 1s:

*Up (OPEN) = AIS Blue = a sequence of alternating 1s and 0s (e.g., 1010... sequence).

Down = AIS All 1s = a pattern of an unframed all-ones signal to maintain transmission continuity.

* The SW2 default is all switch positions in the Up (OPEN) position.



CL / FL Switch SW1 - Loopback mode:

Left (**CL**) = Coax loopback mode.

Right (**FL**) = Fiber loopback mode.

*Center = Normal operating mode (*default setting).



The S6210 and C6210 DIP switch locations are shown below.



Figure 14: S6210 DIP Switches



Figure 15 : C6210 DIP Switches

For more information, see “[DIP Switches and Jumper Settings](#)” on page 206.

Documentation Conventions

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

Table 6: Documentation Conventions

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

Related Manuals and Online Help

A printed documentation card is shipped with each x6210 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](#).

Other ION system and related device manuals are listed below.

1. ION System x6210 Managed DS3-T3/E3 to Fiber NID User Guide, 33495 (this manual)
2. ION219-A 19-Slot Chassis Installation Guide, 33412
3. IONMM Management Module Install Guide, 33420
4. ION Management Module (IONMM) User Guide, 33457
5. ION106-x Six Slot Chassis User Guide, 33658
6. SPS-2460-SA Power Supply User Guide, 33455
7. SFP manuals (product specific)
8. 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 the descriptions and procedures reflect the latest software/firmware version, noted in the [Revision History](#) on page 2.

Note that this manual provides links to third part web sites for which Lantronix is not responsible. Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

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 x6210 and the procedures to access and initially set up the NID through either a local serial interface (USB) or a remote Ethernet connection (Telnet session or Web interface).

Installing the Chassis Model (C6210)

The C6210 is a slide-in module that can only be installed in a Lantronix ION chassis (ION219-x). For a complete list of ION platform products, go to the Lantronix [website](#).

The following describes how to install the C6210 in the ION chassis.



Caution: Failure to wear a grounding device and observe electrostatic discharge precautions when installing the C6210 could result in damage or failure of the module.

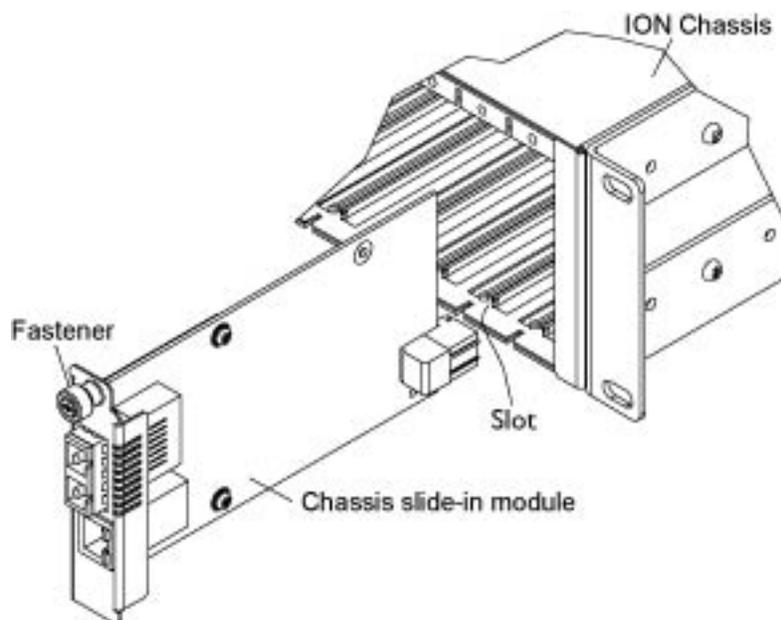


Figure 16: Chassis Installation

IMPORTANT

The C6210 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 C6210 card by its front panel.
3. Align the card with the upper and lower slot guides, and carefully insert the C6210 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 16: Chassis Installation](#) on the previous page).
6. Note that the C6210 card’s Power LED lights. See [Accessing the NIDs](#) on page 39.

Installing the Standalone Model (S6210)

The standalone model (S6210) can be installed in any of the following ways.

- Rack mounted
- Table top
- Wall mounted

Rack Mount Installation

The x6210 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 S6210 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 S6210, place one rubber foot in each corner of the NID.

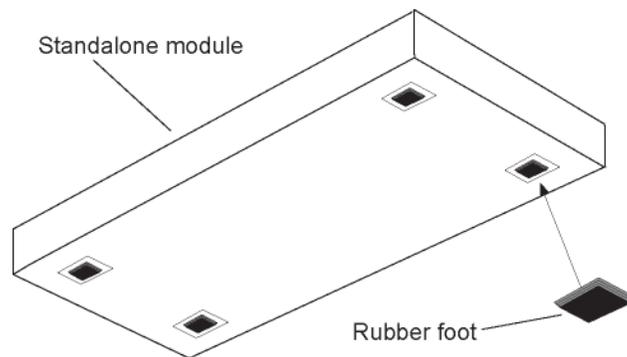


Figure 17: Tabletop Installation

3. Set the S6210 in place and connect the AC power adapter (see Connecting to AC Power on page 39).

Wall Mount Installation

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

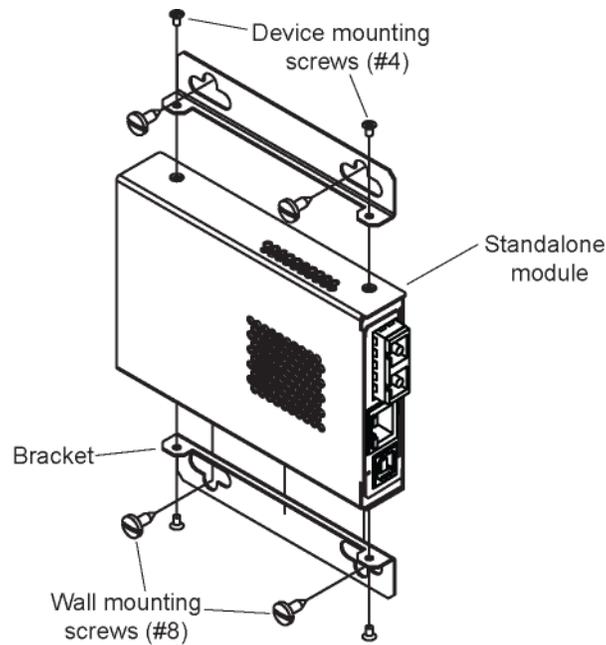


Figure 18: Wall Mount Installation

2. Mount one of the bracket assemblies to the device using two of the #4 Philips head screws.
3. Mount the other bracket assembly to the other side of the device using the other two #4 Philips head screws.
4. Position the device 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](#) on page 39).

Connecting to AC Power

After the standalone S6210 has been installed, connect the S6210 to the AC power adapter that came with the S6210.



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 S6210 (AC-DC adapter 25025).

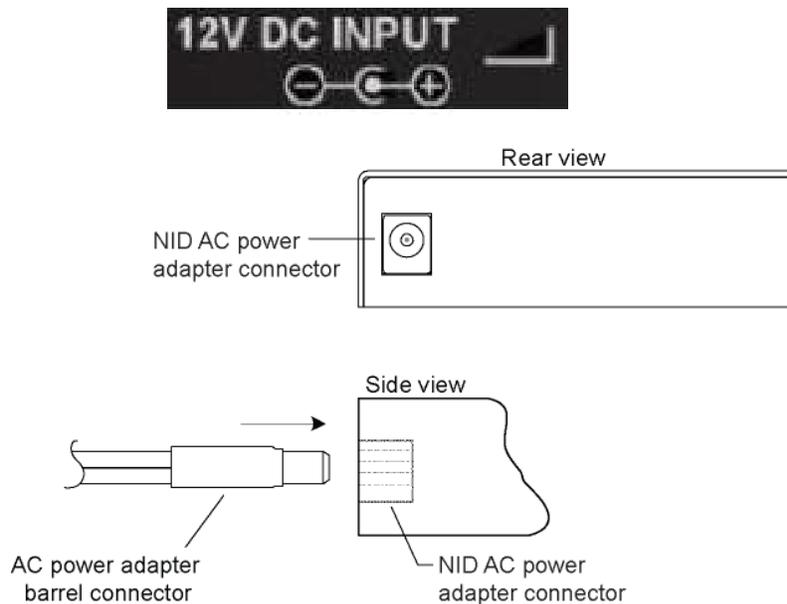


Figure 19: AC Power Connection

2. Plug the Power adapter plug into AC power at an appropriate AC outlet. Note that the S6210 front Power (PWR) LED lights.

Firmware version 1.2.5 allows for a power outage on the 6-slot and 19-slot chassis with an IONMM. The C601x, C611x, C612x, and C6210 find the agent at ~47 seconds after power is restored on the ION219 chassis. On the ION106-x chassis it's about 45 seconds.

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 C6210-3040 and C6210-1040 each have a single SFP port. The SFP port uses standard 100Base-x/oc-3 SFP.

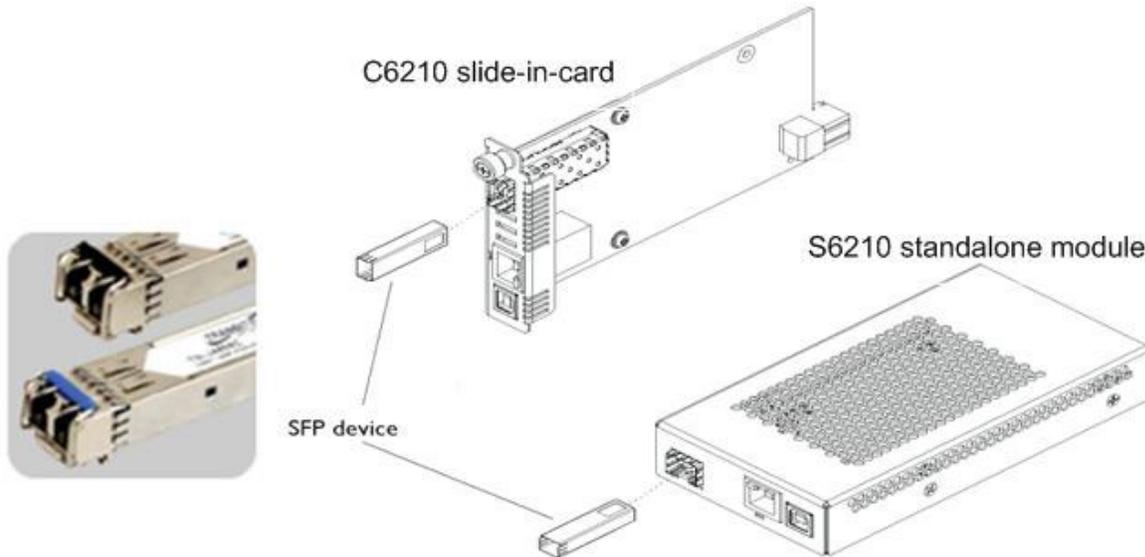


Figure 20: SFP Installation

1. Position the SFP device at either installation slot, with the label facing up.
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 Port 4 or Port 5. (There should be a slight 'click' when connected.)

Connecting the C6210 to the S6210

Connect the local C6210 to the remote S6210 using fiber ports. If two fiber lines are supported, connect the local and remote device's primary lines together, and connect the secondary lines together. Make sure the C6210 and S6210 are set to the same mode (DS3 or E3).

Accessing the NIDs

The x6210 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 x6210 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

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 USB drivers are available at <https://www.lantronix.com/products/c6210-series/>. 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.

Installing the USB Driver (Windows XP)

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 must 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.
14. In the **Emulation** field, select **VT100**.
15. Click the **ASCII Setup...** button.
16. Verify that **Wrap lines that exceed terminal width** is selected.
17. Click **OK** twice.
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.

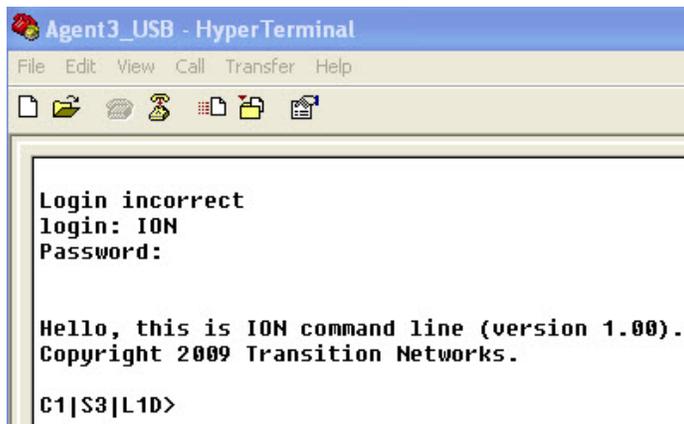
1. Start the terminal emulator program (e.g., HyperTerminal).
2. When the emulator screen displays, press **Enter**. The login prompt displays.
If the login prompt does not display, try unplugging and re-plugging the USB cable at the IONMM.

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 “Login incorrect” 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. Is the NID controlled by the ION Management Module?

Yes	No
Continue with step 8 .	Go to step 9 .

8. Enter a **go** command to change the location for the command prompt; the format is:
go [c=CHASSIS] [s=SLOT] [I1ap=PORT] [I2ap=PORT] (I1p=PORT|I2p=PORT|I3p=PORT|I1d|I2d|I3d)
9. Enter commands to set up the various configurations for the NID. For configuration information, see “[Section 4: Configuration](#)” on page 55. For a description of all available CLI commands see “[Section 6: Command Line Interface \(CLI\) Reference](#)” on page 126.

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](#)” on page 126.

Terminating a USB Connection from HyperTerminal

To terminate the USB connection, do the following.

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

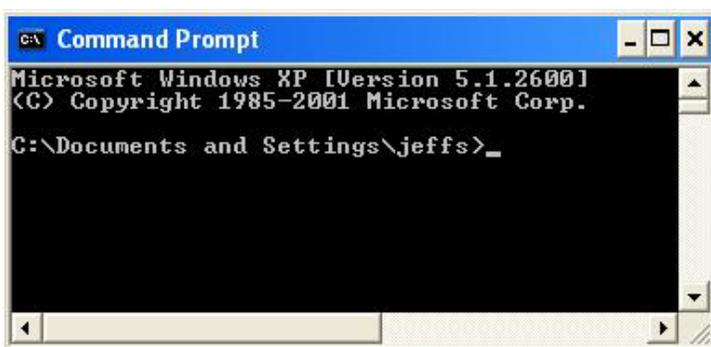
Access via an Ethernet Network

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 x6210.

Starting a Telnet Session

The x6210 can be controlled from a remote management station via a Telnet session over an Ethernet connection. The x6210 is controlled and configured through CLI commands. Use the following procedure to connect to and access the x6210 via a Telnet session.

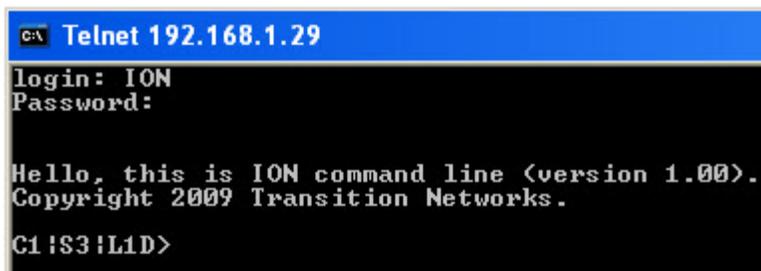
1. Click Windows **Start**.
2. Select **All Programs>Accessories**.
3. Click **Command Prompt**. The command prompt window displays.



4. At the command line type: **telnet <xx>** where:
xx = IP address of the x6210
5. Press **Enter**. The login prompt displays.

Note: If your system 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.
7. Press **Enter**. The password prompt displays.
8. Type your password (the default is **private**). **Note:** the password is case sensitive.
9. Press **Enter**. The command line prompt displays.



10. Is the NID controlled by the ION Management Module?

Yes	No
Continue with step 11 .	Go to step 12 .

11. Enter a **go** command to change the location for the command prompt. The **go** command format is:

```
go [c=CHASSIS] [s=SLOT] [I1ap=PORT] [I2ap=PORT] (I1p=PORT | I2p=PORT | I3p=PORT | I1d | I2d | I3d)
```

12. Enter commands to set up the various configurations for the NID. For configuration information, see [Section 4: "Configuration"](#) on page 55. For a description of all available CLI commands see ["Section 6: Command Line Interface \(CLI\) Reference"](#) on page 126.

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"](#) on page 126.

Terminating a Telnet Session

To terminate the Telnet session:

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

Web Browsers Supported

The ION system supports the latest version of most popular web browsers.

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.

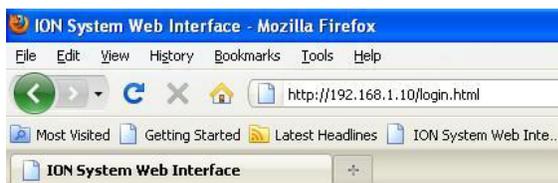
A Web session can be used to connect to and set up the NID.

IMPORTANT

- Do not use the browser back button to navigate the screens. This causes the connection to drop.
 - Do not use the keyboard back space key in grayed out fields. It causes the 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 192.168.1.10).



3. Click **Go** or press **Enter**.

The ION System sign in screen displays.

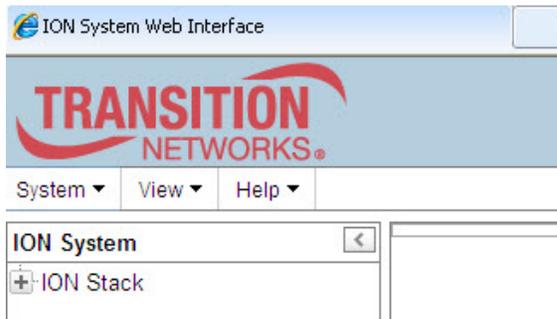
Sign in to ION System Web Interface

System name:

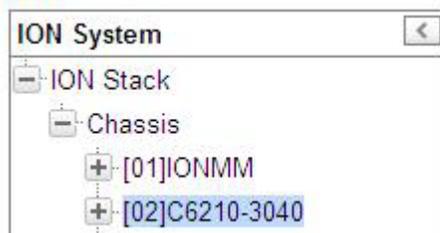
Password:

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 System name (the default is **ION**). **Note:** the System name is case sensitive.
5. Type the password (the default is **private**). **Note:** the password is case sensitive.
6. Click **Sign in** or press **Enter**. The opening screen displays.



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 C6210-3040 **MAIN** tab screen is shown below:

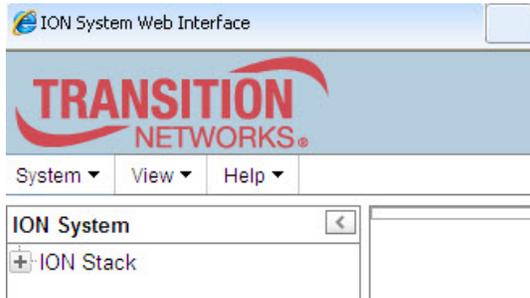
The screenshot displays the Lantronix ION System configuration interface. The top left features the 'TRANSITION NETWORKS' logo and a menu bar with 'System', 'View', and 'Help' options. A navigation tree on the left shows the 'ION Stack' with a 'Chassis' section containing various device models, with '[09]C6210-3040' selected. The main area is titled 'MAIN' and contains several configuration sections: 'Model Information' with fields for Serial Number (10134184), Model (C6210-3040), Software Revision (1.2.4), Hardware Revision (1.0.0), and Bootloader Revision (0.1.1); 'System Configuration' with fields for System Name, System Up Time (124:1:03:56:00), Configuration Mode (Software), and Number of Ports (2), along with a MAC Address field (00-C0-F2-22-7A-BE) and buttons for Uptime Reset, System Reboot, and Reset To Factory Config; 'Device Description' with an empty text box; and 'TDM Mode' with a dropdown set to DS3, Transmit All Ones set to Enabled, and AIS Format set to Blue. At the bottom of the main area are buttons for Refresh, Save, and Help. The status bar at the bottom left shows 'Getting values finished' and the bottom right shows 'Version: 1.3.19'.

10. You can use the various tabs to configure the system, devices and ports. For configuration information, see “[Section 4: Configuration](#)” on page 65.

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**.
2. Click **Sign out**.



The sign in screen displays again.

Note: The x621x 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 log out.

Initialization (Default) Configuration

The x6210 assumes the following operating characteristics on initial startup. These are the default initialization parameter values for the x6210.

Parameter	Property	Default setting
DS3/E3 model	Read only	DS3
Configuration mode	Read only	SW
AIS transmit	Read & Write	Enable
AIS format	Read & Write	Blue
Fiber Port		
* Link	Read only	Down
* Alarm Indication Signal	Read only	Normal
* Loopback	Read & Write	Disable
Copper Port		
* Link	Read only	Down
* Alarm Indication Signal	Read only	Normal
* Loopback	Read & Write	Disable
* DS3 Line build out	Read only	On

See [Section 4: Configuration](#) for the procedures used to change these default settings.

3: Management Methods

General

The x6210 NIDs are managed either directly or through the IONMM. Whether the NID is managed directly or indirectly, management is accomplished through 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 through 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 x6210 NIDs can be remotely managed directly (i.e., only through IONMM).

IONMM Managed x6210s

NIDS that are managed through the IONMM are either chassis resident (C6210) or standalone modules (S6210) that are connected as remotes to chassis resident modules. Communications between the IONMM and each x6210 is through the ION Chassis backplane.

You can manage and configure the x6210 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:

```
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.

A representation of the hierarchy is shown in the figure below.

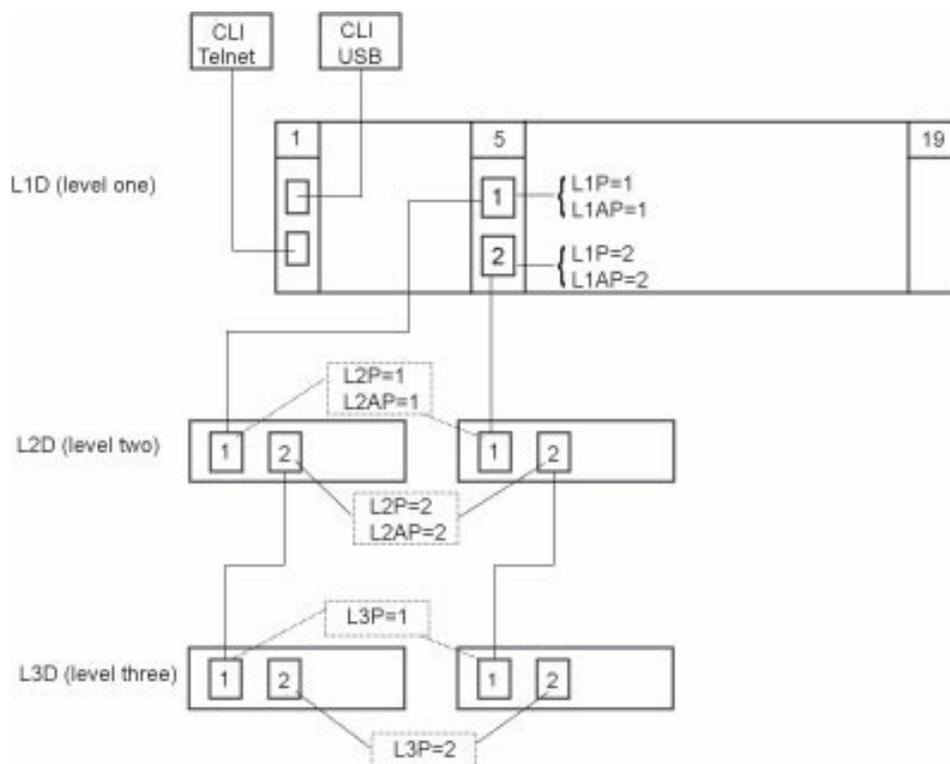


Figure 21: CLI Location Hierarchy

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

- L1D, or level one device, refers to devices (IONMM and other NIDs) that are installed in the chassis.
- L2D, or 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, or 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 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 19, 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 20, 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”](#) on page 41) or a Telnet session (see [“Starting a Telnet Session”](#) on page 43).
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”](#) on page 125.
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.

```
C1|S2|L1D>stat
ION statck
  Chassis -- BPC
    [ 1] IONMM
        Port 1
        Port 2
    [ 2] C6210-3040
        Port 1
        Port 2
                Level2 REM: S6210-3040
                    Port 1
                    Port 2
```

For more information, see the Status check (**stat**) command in “[Section 6: Command Line Interface \(CLI\) Reference](#)” on page 125.

To switch command control from the local slot 4 C6210-3040 to its level 2 remotely-connected device (S6210-1040) 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: S6210-1040 above, you would enter:

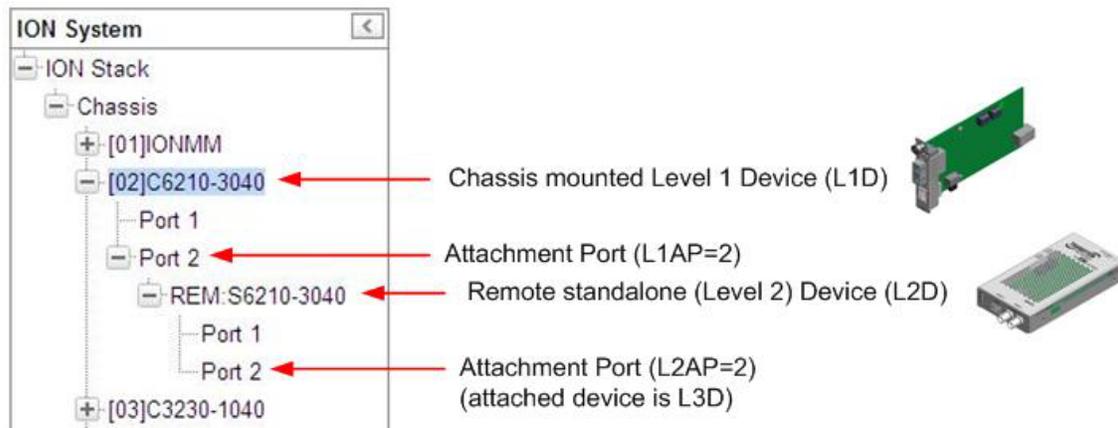
```
C1|S4|L1AP2|L2D>go l2p=1
```

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” on page 45).



2. Click on the slide-in module or port to be managed.
3. The operations that can be performed depend on the type of slide-in module. Refer to the product documentation for the information. See the “Related Manuals” section on page 38.

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:

```
C0|S0|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] [11ap=PORT] [12ap=PORT] (11p=PORT|12p=PORT|13p=PORT|11d|12d|13d)
```

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:

```
C0|S0|L1D>go 11p=1
```

The resulting command line prompt would be:

```
C0|S0|L1P1>
```

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

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

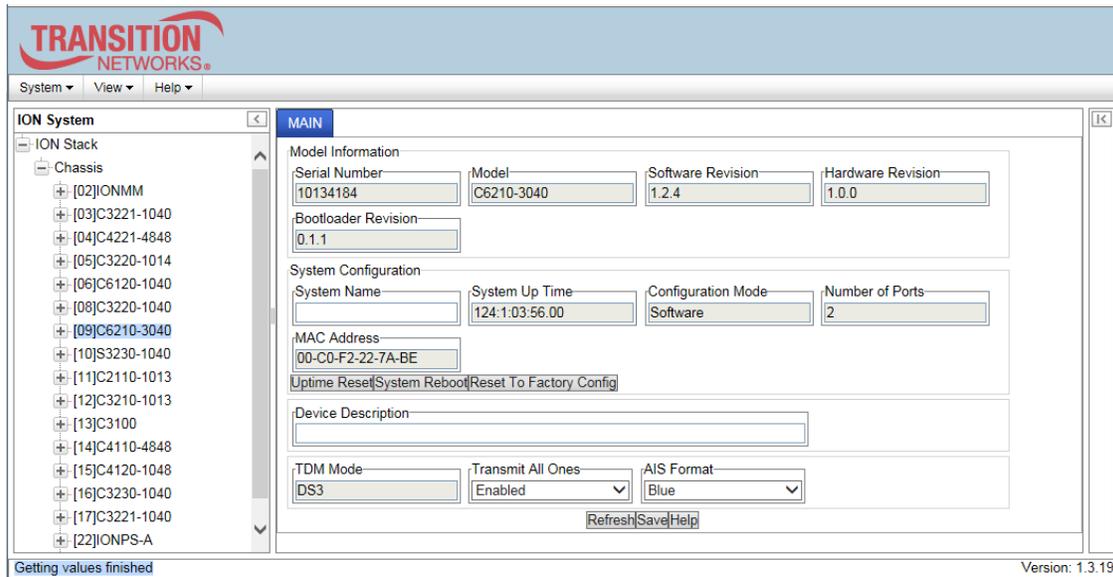
```
C0|S0|L1P1>go 11d
```

The resulting command line prompt would be:

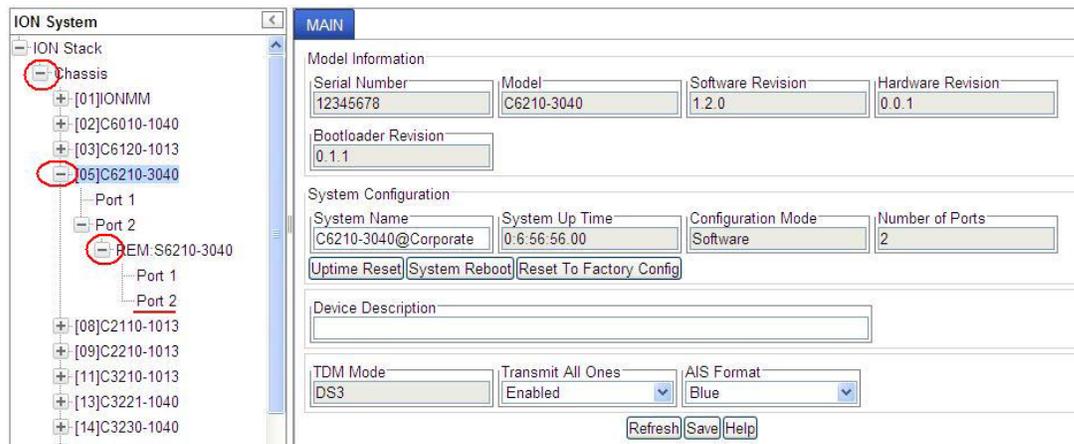
```
C0|S0|L1D>
```

Managing Standalone Modules via the IONMM Web Interface

1. Access the C6210 through the Web interface (see “Starting the Web Interface” on page 45).



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 (e.g., **[02:C6210-3040]** shown above).
4. Click on the desired module (e.g., **[02:C6210-3040]** on the screen above).



5. Click on the **[+]** next to the attachment port to be managed (**Port 2** above).
6. Click on the **[+]** next to the remote device to be managed (**REM:S6210-3040** 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 x6210 Web interface in terms of its system-level pane, dropdowns, tabs and sub-tabs. Note that menus and tabs vary slightly by model.

Table 7: System-Level Menu Description

Dropdown / Tab	Description
ION System pane	<p>Stack - consists of one chassis. The Stack Members table lists the Stack's chassis, type, and description.</p> <p>Chassis - the ION System set of devices; the Chassis View shows a summary view of one chassis and its member devices. The Model Information includes:</p> <ul style="list-style-type: none"> * Serial Number - The serial number of the chassis itself. Individual NIDs also have their own serial numbers. * Model - The exact model number of this device. When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number. * Software Revision, Hardware Revision, and Bootloader Revision. * Chassis Members table - lists local physical components in slots 1 to 19. <p>Device – provides tabs and sub-tabs for the IONMM and NIDs in the ION system.</p> <p>Port - provides tabs and sub-tabs for a selected NID port.</p>
System Dropdown	Sign out.
View Dropdown	Refresh.
Help Dropdown	Online Help, ION Product Home Page, About ION System Web Interface.

Device-Level Menu

The table below describes the C6210 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	C6210 Model Information, System Configuration, Device Description, TDM Mode, Transmit All Ones, and AIS Format sections. Uptime Reset, System Reboot, and Reset to Factory Config buttons.

Port-Level Menus

The table below describes the x6210 Web interface in terms of its port-level tabs and sub-tabs.

Table 8: Port-Level Menu Description

Tab	Description
MAIN Tab	Sections: Circuit ID, Port Configuration, and Loopback Management. Fields: Link Status, Alarm Indication Signal, Line Build Out, Connector Type, Loopback Type, and Loopback Status. Buttons: <i>Refresh, Save, Start, Stop, and Help.</i>
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 (Diagnostic Maintenance Interface) Parameters ” on page 248 for more information. Note: not all NID / SFP models support DMI. If you click the DMI tab on a NID model that does not support DMI, the message “ <i>The DMI feature is not supported on current port.</i> ” displays.

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 starting on page 86 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:

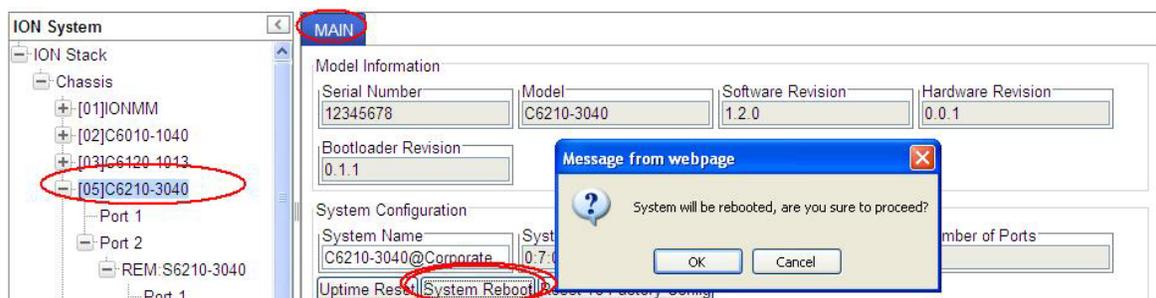
- Table 9. [Back Up and Restore File Content and Location](#) on page 97
- Table 10. [File Status after a Reset to Factory Defaults](#) on page 100
- Table 11. [File Content and Location after a System Reboot](#) on page 105
- Table 12. [File Content and Location after a Firmware Upgrade](#) on page 117



Doing a reboot, restart, or upgrade of the IONMM, a chassis power restart, or a reset to factory settings may cause configuration backup files, HTTPS certification file, and/or 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).

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.

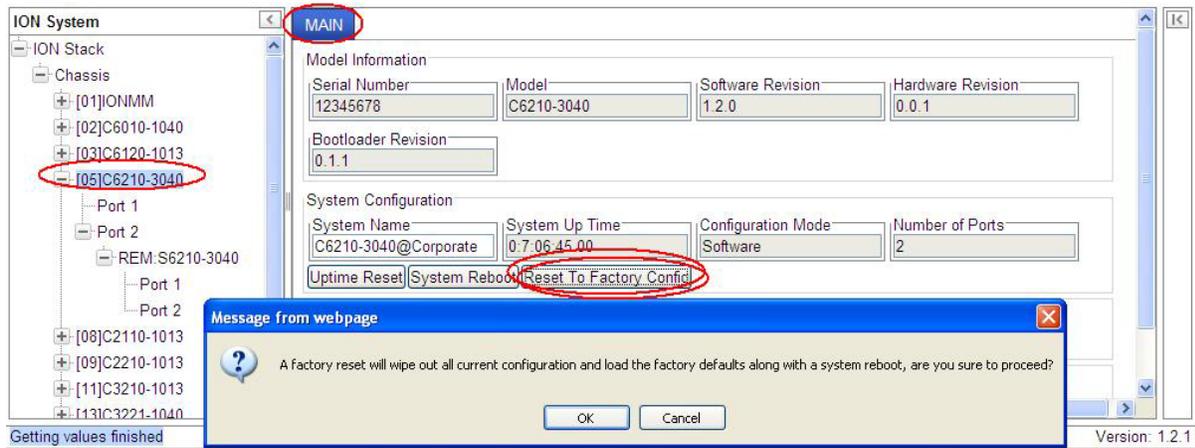
Press the **OK** button to clear the webpage message and begin the reboot process. The message “*Loading, please wait...*” displays.

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.

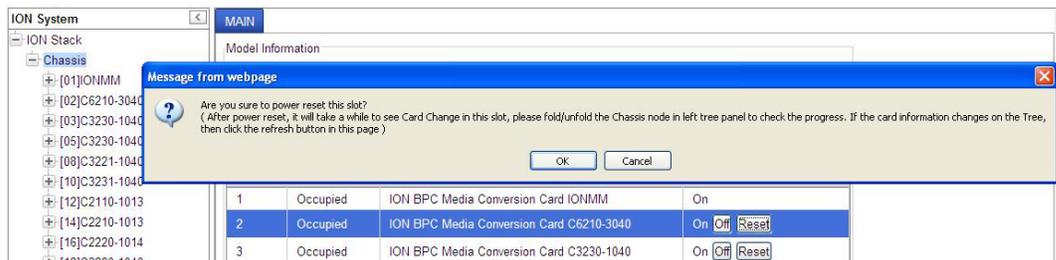
The message *“A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?”* displays.



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 x6210 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.

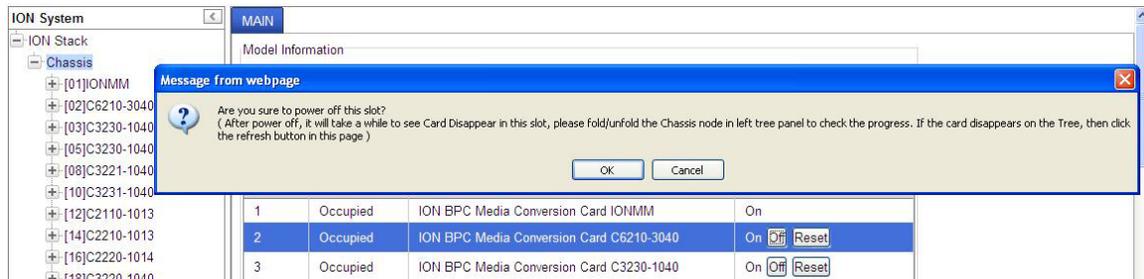


After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page.

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 x6210 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 x6210.

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](#)” on page 124.

The operating characteristics that can be defined for the x6210 are:

- System configuration / System Name
- Device Description / Circuit ID
- Features
 - TDM
 - AIS
 - Loopback Type
 - DMI

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

During system configuration, you define a name for the x6200, and define AIS operation.

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

System Configuration – CLI Method

1. Set the x6210 DIP switches and jumpers for your environment. See “[Jumper Settings](#)” on page 31 and “[DIP Switch Settings](#)” on page 33.
2. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
3. Define a new system name if desired. Type **set system name=x**, where x is the new system name, and press **Enter**. The **System Name** cannot contain any spaces between characters.
4. Enter a **Device Description** of up to 64 alphanumeric characters, as needed.
5. Define the AIS Transmit mode. Type **set ais transmit=enable** and press **Enter**.
6. Define the AIS Format to be used. Type **set ais format={allones|blue}** and press **Enter**. Note that this command is case sensitive.
7. Verify the new system definition. Type **show card info** and press **Enter**. For example:

```
AgentIII C1|S3|L1D>set system name=C6210-3040@Corporate
AgentIII C1|S3|L1D>set ais transmit=enable
AgentIII C1|S3|L1D>set ais format=blue
AgentIII C1|S3|L1D>show card info
System name:      C6210-3040@Corporate
Uptime:          02:17:49
Port number:     2
Serial number:   12345678
Config mode:    software
Software:       0.7.4
Bootloader:     0.1.1
Hardware:       0.0.1
AgentIII C1|S3|L1D>show tdm config
ais transmit:    enabled
ais format:     blue
tdm type:       e3
AgentIII C1|S3|L1D>
```

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

System Configuration – Web Method

1. Set the x6210 DIP switches and jumpers for your environment. See “[Jumper Settings](#)” on page 31 and “[DIP Switch Settings](#)” on page 33.
2. Access the NID through the Web interface (see “[Starting the Web Interface](#)” on page 45).
3. At the **MAIN** tab, locate the **System Configuration** section.

The screenshot shows the web interface for a Transition Networks device. The main content area is titled 'MAIN' and contains several sections:

- Model Information:** Serial Number (10134184), Model (C6210-3040), Software Revision (1.2.4), Hardware Revision (1.0.0), and Bootloader Revision (0.1.1).
- System Configuration:** System Name (empty), System Up Time (125:3:26:03.00), Configuration Mode (Software), and Number of Ports (2).
- MAC Address:** 00-C0-F2-22-7A-BE.
- Device Description:** A text input field.
- TDM Mode:** DS3.
- AIS Transmit:** Enabled.
- AIS Format:** Blue.

At the bottom of the form are buttons for 'Refresh', 'Save', and 'Help'. The status bar at the very bottom shows 'Getting values finished' and 'Version: 1.3.19'.

4. In the **System Name** field, enter the name and for the x6210 device. The name can be alphabetic, numeric or a combination. The **System Name** cannot contain any spaces between characters.
5. Scroll to the bottom and click the **Save** button when done.
6. Verify the x6210 device **MAIN** tab configuration.

Serial Number – e.g., 00019 (read only field).

Model – e.g., C6210-3040 (read only field).

Software Revision – e.g., 1.2.4 (read only field).

Hardware Revision - e.g., 1.0.0 (read only field).

Bootloader Revision - e.g., 0.1.1 (read only field).

System Name – e.g., C6210-3040 (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).

MAC Address: e.g., 00-C0-F2-21-B8-7E (read only field).

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

TDM Mode: DS3 or E3 (read only field).

AIS Transmit: dropdown to select Enabled or Disabled (read/write field).

AIS Format: dropdown to select All Ones or Blue (read/write field).

Ports Configuration

The ports configuration defines x6210 port Circuit ID, AIS Transmit, and Loopback Management. You can configure the x6210 ports via the CLI or the Web interface.

Port Configuration – CLI Method

The port information can be alphabetic, numeric or a combination. See “[Section 6: Command Line Interface \(CLI\) Reference](#)” on page 127 for individual CLI command details.

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Configure the Port 1 Circuit ID. At the command prompt type up to 64 characters and press **Enter**.
3. Configure the device-level AIS Transmit. Type **set ais transmit=enable** and press **Enter**.
4. Configure the device-level AIS Format. Type **set ais format-<allones|blue>** and press **Enter**.
allones = a pattern of an all-ones signal.
blue = a pattern of an unframed all-ones signal to maintain transmission continuity; a sequence of alternating 1s and 0s (e.g., 1010... sequence).
5. Configure the Port 1 Loopback Type. Type **set tdm loopback type=phylayer** and press **Enter**.
6. Use the **go** command to switch to Port 2. Type **go l1p2** and press **Enter**.
7. Repeat steps 3-6 above for Port 2.
8. Configure the Port 2 DMI function (optional - if supported / required).
9. Click the **Save** button when done.
10. Verify the x6210 configuration. For example:

```
AgentIII C1|S3|L1D>set ais transmit=enable
AgentIII C1|S3|L1D>set ais format=blue
AgentIII C1|S3|L1D>set circuit-ID=xx/CD-FDB
AgentIII C1|S3|L1D>show tdm config
ais transmit:                enabled
ais format:                  blue
tdm type:                    e3
AgentIII C1|S3|L1D>go l1p=1
AgentIII C1|S3|L1P1>set tdm loopback type ?
  maclayer
  noloopback
  phylayer
AgentIII C1|S3|L1P1>set tdm loopback type=maclayer
Set TDM port loopback type failed.
AgentIII C1|S3|L1P1>set tdm loopback type=phylayer
AgentIII C1|S3|L1P1>show tdm port config
link oper status:            down
alarm indication signal:    normal
lbo status:                  boost
connector:                   Dual BNC
AgentIII C1|S3|L1P1>
```

Port 1 and 2 Configuration – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. In the Port 1 **MAIN** tab, in the **Circuit ID** field, enter up to 64 characters as required.

3. In the **Port Configuration** section in the **AIS Transmit** field, select **Enabled** or **Disabled**.
4. In the **Loopback Management** section in the **Loopback Type** field, select **No Loopback** or **PHY Layer**.
5. Click the **Save** button when done.
6. Select **Port 2**.

7. At the **MAIN** tab, in the **Circuit ID** field, enter up to 64 characters as required.
8. In the **Loopback Type** field, select **No Loopback** or **PHY Layer**.
9. Click the **Save** button when done.

10. Select the Port 2 **DMI** tab (optional – only if DMI is supported).

The screenshot shows the ION System configuration window with the DMI tab selected. The left sidebar shows a tree view of the ION Stack, with 'Port 2' selected. The main area displays the following configuration fields:

Interface Characteristics		
DMI ID	Connector Type	Nominal Bit Rate (Mbps)
SFP	LC	200
Fiber Interface Wavelength (nm)		
1310		
Diagnostic Monitoring		
Receive Power (µW)	Receive Power (dBm)	Receive Power Alarm
0		Normal
Rx Power Intrusion Threshold (µW)		
0		
Temperature (°C)	Temperature (°F)	Temperature Alarm
38.5	101.3	Normal
Transmit Bias Current (µA)	Transmit Bias Alarm	
26848	Normal	
Transmit Power (µW)	Transmit Power (dBm)	Transmit Power Alarm
34	-14.685	Normal
Supported Media Length		
9/125u Singlemode Fiber (m)	50/125u Multimode Fiber (m)	62.5/125u Multimode Fiber (m)
N/A	2000	2000
Copper (m)		
N/A		

At the bottom right, there are buttons for 'Refresh', 'Save', and 'Help'. The 'Save' button is highlighted with a red circle.

11. Set the **Rx Power Intrusion Threshold** (0-65535 µW). The default is 0 uW (microWatts).

12. Click the **Save** button when done.

13. Verify the x6210 Port 1 and Port 2 configurations.

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

Link Status: either Down or Up displayed (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).

Loopback Type: either “No Loopback” or “PHY layer” loopback displayed.

Line Build Out: The characteristics of the T1/E1 card's copper interface (read only field) as defined by DIP switch.

Connector Type –SFP Slot, LC, 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.

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 x6210 in Hardware mode, just set the x6210 front panel **CL – FL** switch to the **CL** (copper loopback mode) position to start and stop the loopback test.

In Software 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 x6210 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the x6210 CLI command prompt, use the **go** command to switch to Port 1. Type **go c1 sx l1p=1** and press **Enter** (where x is the slot where the x6210 is located in the ION chassis). To control S6210 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=stop** and press **Enter**.
6. Set the x6210 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:

```
AgentIII C1|S3|L1D>set tdm loopback type phylayer
AgentIII C1|S3|L1D>set tdm loopback oper init
AgentIII C1|S3|L1D>set tdm loopback oper stop
AgentIII C1|S3|L1D>show tdm loopback capability
Loopback capability: phyLayer
AgentIII C1|S3|L1D>show tdm loopback state
Loopback type: phylayer
Loopback state: noLoopback
AgentIII C1|S3|L1D>
```

9. Use the **show tdm config** command to display and verify the device-level TDM configuration. In DS3 mode, for example:

```
AgentIII C1|S3|L1D>show tdm config
ais transmit:                enabled
ais format:                   blue
tdm type:                     dS3
AgentIII C1|S3|L1D>
```

In E3 mode, for example:

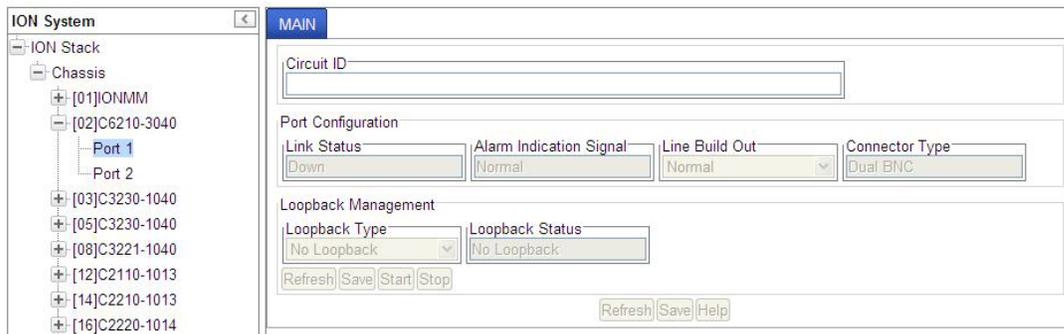
```
AgentIII C1|S3|L1D>show tdm config
ais transmit:                enabled
ais format:                  allones
tdm type:                    e3
AgentIII C1|S3|L1D>
```

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

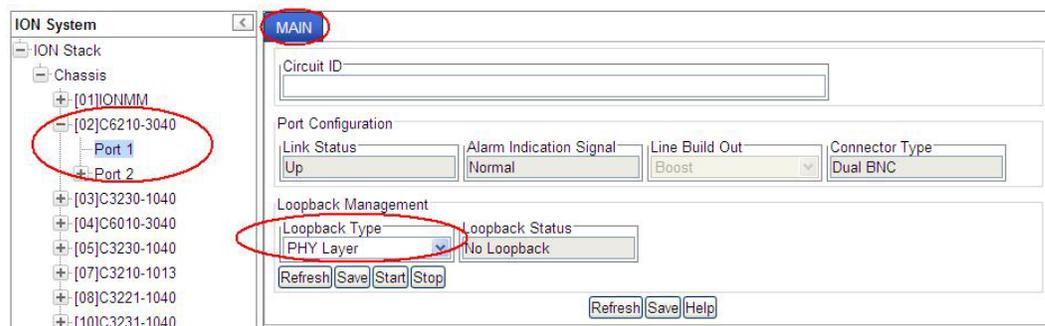
```
AgentIII C1|S3|L1D>show tdm port config
link oper status:            up
alarm indication signal:    normal
lbo status:                  boost
connector:                   Dual BNC
AgentIII C1|S3|L1D>go l1p=2
C1|S2|L1P2>show tdm port config
link oper status:            up
alarm indication signal:    normal
connector:                   SFP Slot
AgentIII C1|S3|L1D>go l1p=1
AgentIII C1|S3|L1P1>show tdm port config
link oper status:            down
alarm indication signal:    normal
lbo status:                  boost
connector:                   Dual BNC
AgentIII C1|S3|L1P1>go l1p=2
AgentIII C1|S3|L1P2>show tdm port config
link oper status:            down
alarm indication signal:    normal
connector:                   SFP Slot
AgentIII C1|S3|L1P2>
```

Port Loopback Test – Web Method

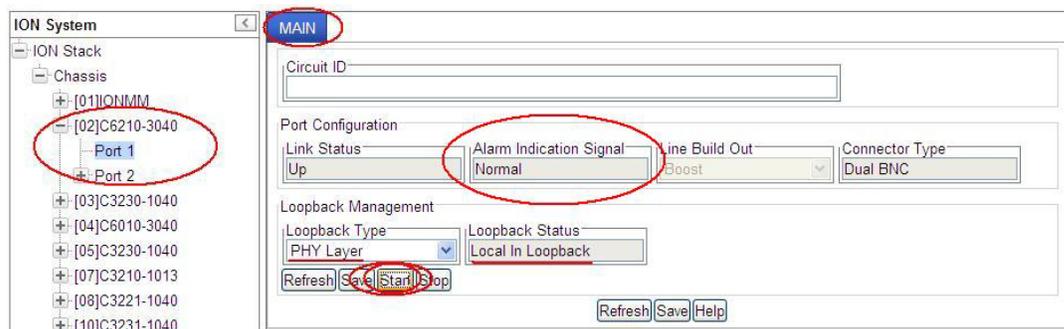
1. Go to the **x6210 > Port 1 > MAIN > Loopback Management** section.



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.

Note: If you Start a loopback test on both ports at the same time, the message *“Setting values failed (snmp operation error)”* displays and you must Stop one of the loopback tests to clear the message.

E3 TDM Mode Configuration

The x6210 is shipped from the factory in DS3 mode. Use the procedure below to configure E3 mode. Note that the System Up Time counter is reset to 0 when you change the TDM Mode to 'E3'.

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

Configuring E3 Mode – CLI Method

1. Set x6210 DIP Switch SW1 – DS3/E3 to the Down (closed) position to select E3 mode. See “DIP Switches” on page 33.
2. Access the x6210 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
3. If required, enter a Circuit ID of up to 64 characters using the **set circuit-ID** command.
4. Select an AIS Format (either All Ones or Blue). Type **set ais format={allones|blue}** and press **Enter**.
5. Configure the AIS transmit. Type **set ais transmit=enable** and press **Enter**.
6. Verify the configuration. Type **show tdm config** and press **Enter**. For example:

```
C1|S2|L1D>show tdm config
ais transmit:                enabled
ais format:                  blue
tdm type:                    e3
C1|S2|L1D>set ais transmit ?
  disable
  enable
C1|S2|L1D>
C1|S2|L1D>set ais format ?
  allones
  blue
C1|S2|L1D>
```

7. At the x6210 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 x6210 slot location in the ION chassis).

Configuring E3 Mode – Web Method

1. Set x6210 DIP Switch SW1 – DS3/E3 to the Down (closed) position to select E3 mode. See “[DIP Switches](#)” on page 33.
2. Go to the x6210 **MAIN** tab and verify that the **TDM Mode** field displays **E3**.

The screenshot shows the ION System web interface. The left sidebar displays the ION Stack hierarchy, with the [02]C6210-3040 node selected. The main content area is titled 'MAIN' and contains the following sections:

- Model Information:** Serial Number (00019), Model (C6210-3040), Software Revision (1.1.0), Hardware Revision (0.0.1), and Bootloader Revision (0.1.1).
- System Configuration:** System Name (S6210-3040@Corporate), System Up Time (0:0:10:11:00), Configuration Mode (Software), and Number of Ports (2). Buttons for Uptime Reset, System Reboot, and Reset To Factory Config are present.
- Device Description:** A text input field.
- TDM Mode:** Set to E3.
- AIS Transmit:** Set to Enabled.
- AIS Format:** Set to All Ones.

Buttons for Refresh, Save, and Help are located at the bottom right of the configuration area.

3. Click the **Refresh** button if the **TDM Mode** field does not display **E3**.
4. If desired, enter a new **System Name**.
5. If required, enter a **Device Description** of up to 64 characters.
6. At the **AIS Transmit** dropdown, select **Enabled**.
7. At the **AIS Format** dropdown, select **All Ones** or **Blue**.
8. Click the **Save** button when done.
9. Select **Port 1** and verify that the **Alarm Indication Signal** field displays **Normal**.

The screenshot shows the ION System web interface. The left sidebar displays the ION Stack hierarchy, with the [02]C6210-3040 node selected and Port 1 highlighted. The main content area is titled 'MAIN' and contains the following sections:

- Circuit ID:** A text input field.
- Port Configuration:** Link Status (Up), Alarm Indication Signal (Normal), Line Build Out (Boost), and Connector Type (Dual BNC).
- Loopback Management:** Loopback Type (No Loopback) and Loopback Status (No Loopback).

Buttons for Refresh, Save, Start, and Stop are located at the bottom right of the configuration area.

10. Select **Port 2** and verify that the **Alarm Indication Signal** field displays **Normal**.

5: Operation

General

This section describes the non-configuration operations that can be performed for the x6210.

Backup and Restore Operations

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 x6210.

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](#)” on page 124.

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

IMPORTANT



Doing a reboot, a restart or upgrade of the NID, a power restart of the chassis, 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).

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

- Table 9. [Back Up and Restore File Content and Location](#) on page 97
- Table 10. [File Status after a Reset to Factory Defaults](#) on page 100
- Table 11. [File Content and Location after a System Reboot](#) on page 105
- Table 12. [File Content and Location after a Firmware Upgrade](#) on page 117

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]C6210-3040 shown below). The second module listed is the standalone (remote) device (e.g., [04:L2]REM:S6210-1040 shown below).

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		Download
<input type="checkbox"/>	2	[02]C6210-3040	1-2-C6210-3040.config		Download
<input type="checkbox"/>	3	[02:L2]REM:S6210-3040	1-2-2-S6210-3040.config		Download

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 x6210 memory.

1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **BACKUP-RESTORE** tab. Select the **Backup** sub-tab if not already displayed.

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		Download
<input type="checkbox"/>	2	[02]C6010-1040	1-2-C6010-1040.config		Download
<input checked="" type="checkbox"/>	3	[03]C6120-1013	1-3-C6120-1013.config		Download

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 **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.

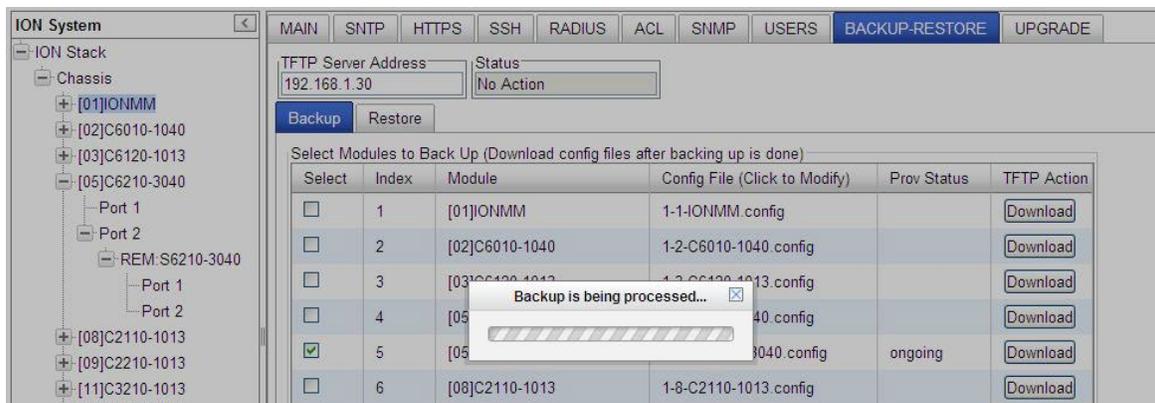
9. Click the **OK** button to clear the web page message.

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*).

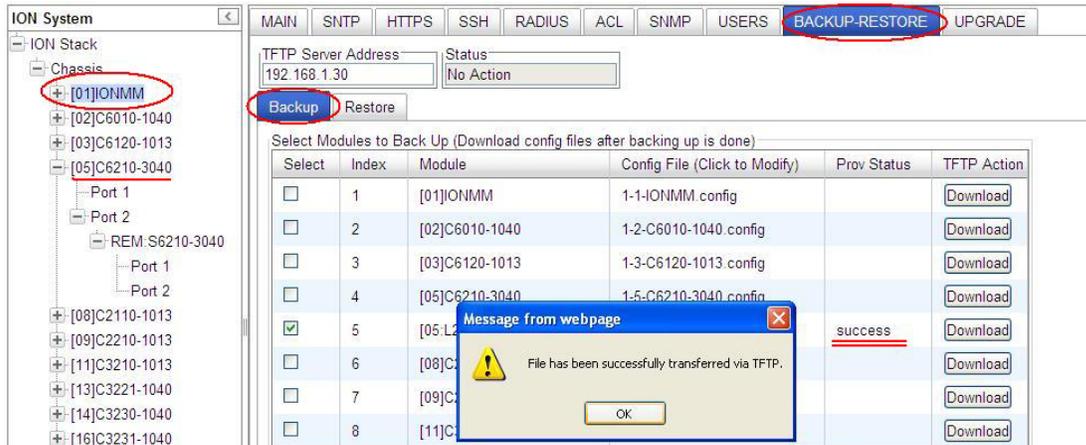


13. If the Back Up operation fails, go to step 15 below.

14. To send a copy of the backup file to the TFTP Server:

- Make sure the TFTP Server is running and configured.
- In the **TFTP Server Address** field, enter the IP address of the server.
- Click the **Download** button. The message “*File is being transferred*” displays.
- 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 . Click the  box to download an error log from the device.



The screenshot shows the ION System web interface. The 'ION Stack' tree on the left includes modules like [01]IONMM, [02]C6010-1040, [03]C6120-1013, and [05]C6210-3040. The 'MAIN' menu is active, and the 'BACKUP-RESTORE' tab is selected. The 'TFTP Server Address' is 192.168.1.30. The 'Backup' button is highlighted. Below it, a table lists modules for backup:

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		<input type="button" value="Download"/>
<input type="checkbox"/>	2	[02]C6010-1040	1-2-C6010-1040.config		<input type="button" value="Download"/>
<input type="checkbox"/>	3	[03]C6120-1013	1-3-C6120-1013.config		<input type="button" value="Download"/>
<input type="checkbox"/>	4	[05]C6210-3040	1-5-C6210-3040.config		<input type="button" value="Download"/>
<input checked="" type="checkbox"/>	5	[05]C6210-3040		success	<input type="button" value="Download"/>
<input type="checkbox"/>	6	[08]C2110-1013			<input type="button" value="Download"/>
<input type="checkbox"/>	7	[09]C2210-1013			<input type="button" value="Download"/>
<input type="checkbox"/>	8	[11]C3210-1013			<input type="button" value="Download"/>

A 'Message from webpage' dialog box is displayed, stating: 'File has been successfully transferred via TFTP.' with an 'OK' button.

The error (.ERR) log 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. See “[The Config Error Log \(config.err\) File](#)” section on page 190 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 \(Optional\)](#) on page 91
- [Restoring Slide-In and Remote Modules](#) on page 93
- [Restoring Standalone Modules](#) on page 95

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.

1. Access the IONMM module through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **BACKUP-RESTORE** tab.

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		<input type="button" value="Download"/>
<input type="checkbox"/>	2	[02]C6010-1040	1-2-C6010-1040.config		<input type="button" value="Download"/>
<input checked="" type="checkbox"/>	3	[03]C6120-1013	1-3-C6120-1013.config		<input type="button" value="Download"/>

3. In the **Select** column, check the checkbox of the module to be backed up.
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.
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 \(Optional\)](#) on page 91
- [Restoring Slide-In and Remote Modules](#) on page 92
- [Restoring Standalone Modules](#) on page 95

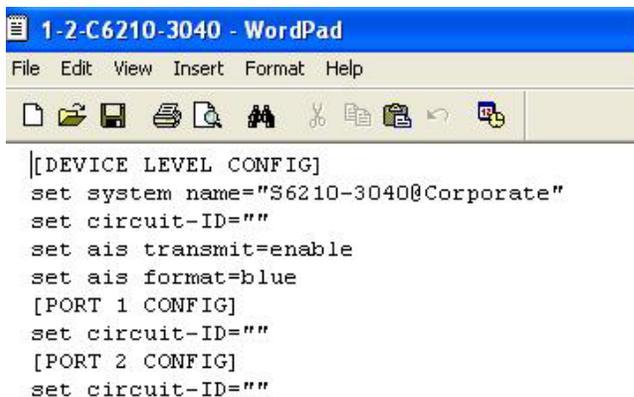
Editing the Config File (Optional)

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- C6210-1040.config*).
3. Edit the Config file sections. Each Config file contains a DEVICE LEVEL CONFIG section and two PORT x CONFIG sections (three PORT x CONFIG sections for the model x601x NIDs).
4. Save the edited Config file back to the TFTP server location (e.g., *C:\TFTP-Root\1-2-C6210-3040.config*).
5. Continue with the applicable Restore procedure from the following section using the edited Config file.

A sample portion of a typical x6210 Config file (*1-2-C6210-3040*) is shown below.

A screenshot of a WordPad window titled "1-2-C6210-3040 - WordPad". The window has a menu bar with "File", "Edit", "View", "Insert", "Format", and "Help". Below the menu bar is a toolbar with various icons for file operations and editing. The main text area contains the following configuration text:

```
[DEVICE LEVEL CONFIG]
set system name="S6210-3040@Corporate"
set circuit-ID=""
set ais transmit=enable
set ais format=blue
[PORT 1 CONFIG]
set circuit-ID=""
[PORT 2 CONFIG]
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](#) on page 252).

1. Access the IONMM through the Web interface (see [“Starting the Web Interface”](#) on page 45).
2. At the **BACKUP-RESTORE** tab, select the **Restore** sub-tab. The “Modules to Restore” table displays.

The screenshot shows the ION System Web interface. The left sidebar displays the ION Stack tree view with the following items: Chassis, [01]IONMM, [02]C6010-1040, [03]C6120-1013, [05]C6210-3040, [08]C2110-1013, [09]C2210-1013, [11]C3210-1013, and [13]C3221-1040. The [01]IONMM item is circled in red. The main content area has tabs for MAIN, SNTP, HTTPS, SSH, RADIUS, ACL, SNMP, USERS, **BACKUP-RESTORE**, and UPGRADE. The BACKUP-RESTORE tab is active, and the Restore sub-tab is selected. The TFTP Server Address is 192.168.1.30 and the Status is No Action. The Backup section has a Restore button circled in red. Below is the 'Select Modules to Restore' table:

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		<input type="button" value="Upload"/>
<input type="checkbox"/>	2	[02]C6010-1040	1-2-C6010-1040.config		<input type="button" value="Upload"/>
<input checked="" type="checkbox"/>	3	[03]C6120-1013	1-3-C6120-1013.config		<input type="button" value="Upload"/>

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.

The screenshot shows the ION System Backup/Restore interface. The left pane displays the ION Stack hierarchy with [01]IONMM selected. The main pane shows the Backup/Restore configuration with the TFTP Server Address set to 192.168.1.30 and Status set to Success. The Restore button is highlighted. Below, a table lists modules to restore:

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		Upload
<input type="checkbox"/>	2	[02]C6010-1040	1-2-C6010-1040.config		Upload
<input type="checkbox"/>	3	[03]C6120-1013	1-3-C6120-1013.config		Upload
<input type="checkbox"/>	4	[05]C6210-3040	1-5-C6210-3040.config		Upload
<input checked="" type="checkbox"/>	5	[05:L2]REM:S6210-3040	1-5-2-S6210-3040.config	success	Upload

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

The screenshot shows the ION System Backup/Restore interface with the TFTP Server Address set to 192.168.1.30 and Status set to TFTP Failure. The Restore button is highlighted. Below, a table lists modules to restore:

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		Upload
<input checked="" type="checkbox"/>	2	[02]C6210-3040	1-2-C6210-3040.config	failure 	Upload
<input type="checkbox"/>	3	[02:L2]REM:S6210-3040	1-2-2-S6210-3040.config		Upload
<input type="checkbox"/>	4	[03]C3230-1040	1-3-C3230-1040.config		Upload

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.

```

1-3-C3230-1040.config - WordPad
File Edit View Insert Format Help
AGENT PH ERROR: CLI command remove vlan all failed
AGENT PH ERROR: CLI command remove fwddb all failed
AGENT PH ERROR: CLI command set ip-mgmt state=enable failed
AGENT PH ERROR: CLI command set dhcp state=disable failed
AGENT PH ERROR: CLI command set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed
AGENT PH ERROR: CLI command set gateway type=ipv4 addr=192.168.0.1 failed
AGENT PH ERROR: CLI command set dns-svr svr=1 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set dns-svr svr=2 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set dns-svr svr=3 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set dns-svr svr=4 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set dns-svr svr=5 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set dns-svr svr=6 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp traphost svr=1 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp traphost svr=2 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp traphost svr=3 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp traphost svr=4 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp traphost svr=5 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp traphost svr=6 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp state=disable failed
AGENT PH ERROR: CLI command set snmp dst-state=disable failed
AGENT PH ERROR: CLI command set snmp timezone=8 failed
AGENT PH ERROR: CLI command set snmp dst-start="1969 1231 18:00:00" failed
AGENT PH ERROR: CLI command set snmp dst-end="1969 1231 18:00:00" failed
AGENT PH ERROR: CLI command set snmp dst-offset=0 failed
AGENT PH ERROR: CLI command set snmp-svr svr=1 type=dns addr=0.0.0.0 failed
AGENT PH ERROR: CLI command set snmp-svr svr=2 type=dns addr=0.0.0.0 failed
  
```

See “[The Config Error Log \(config.err\) File](#)” section on page 197 for error messages and possible recovery procedures.

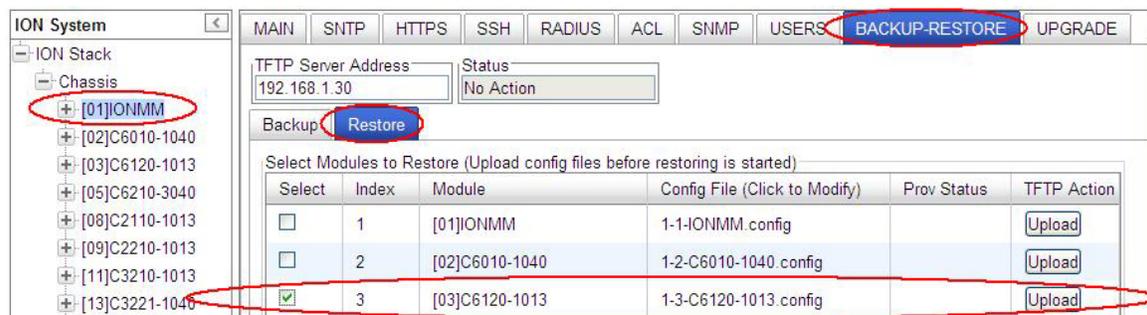
Restoring Standalone Modules

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](#) on page 152).

1. Access the IONMM module through the Web interface (see [“Starting the Web Interface”](#) on page 45).
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
<p>a) In the Config File column, click the file name.</p> <p>b) Type the name of the backup file to be restored. Note: the file name must end with .config.</p> <p>c) Continue with step 6.</p>	<p>Continue with step 6.</p>

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 6.

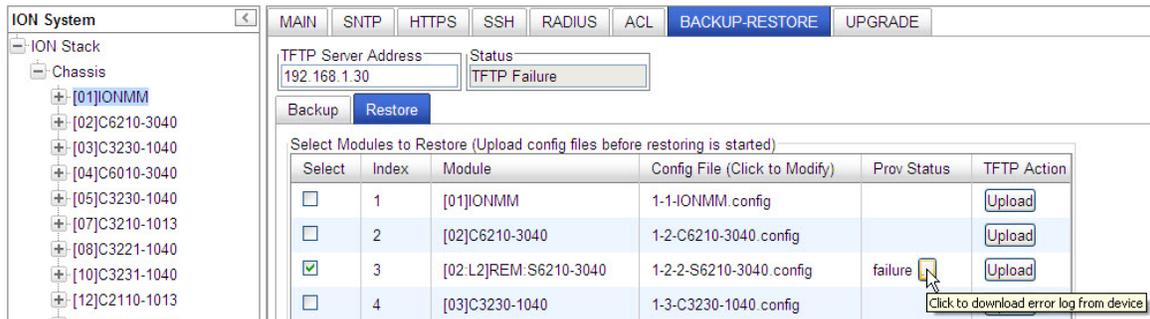
7. Click the **Upload** button. The config file is uploaded via the TFTP server. When done, the message *"File has been successfully transferred via TFTP."*
8. Click the **OK** button to clear the Webpage message.
9. Click the **Restore** button.
10. When the confirmation window displays, click **OK**.

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.

The screenshot shows the ION System configuration interface. The left pane displays a tree view of the system components, including the ION Stack, Chassis, and various modules like [01]IONMM, [02]C6210-3040, [03]C3230-1040, [04]C6010-3040, and [05]C3230-1040. The right pane shows the configuration for the Backup-Restore section. The TFTP Server Address is set to 192.168.1.30, and the Status is TFTP Failure. Below this, there are buttons for Backup and Restore. A table titled "Select Modules to Restore (Upload config files before restoring is started)" is displayed, with the following data:

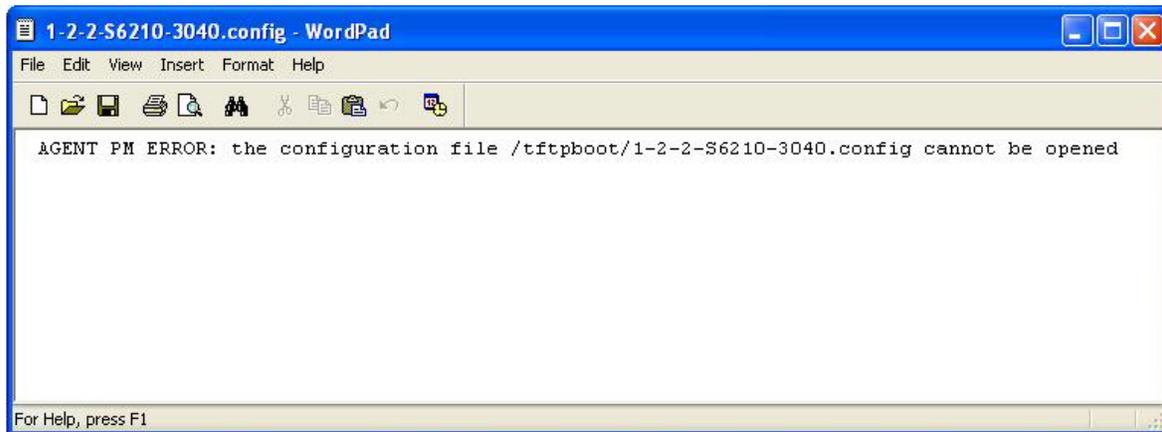
Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		<input type="button" value="Upload"/>
<input checked="" type="checkbox"/>	2	[02]C6210-3040	1-2-C6210-3040.config	success	<input type="button" value="Upload"/>
<input type="checkbox"/>	3	[02-L2]REM:S6210-3040	1-2-2-S6210-3040.config		<input type="button" value="Upload"/>
<input type="checkbox"/>	4	[03]C3230-1040	1-3-C3230-1040.config		<input type="button" value="Upload"/>

11. If the **Restore** operation fails, the **Prov Status** column displays . Click the  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 *1-2-2-S6210-3040.config*. You can open the file in WordPad or a text editor.

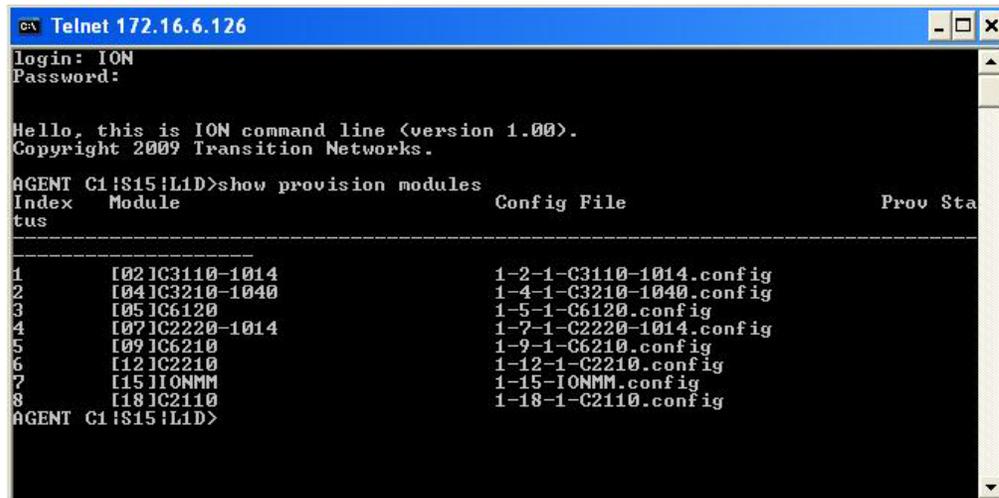
A sample portion of an error log file (.ERR file) is shown below.



See “[The Config Error Log \(config.err\) File](#)” on page 190 for message descriptions.

Configure / Backup / Restore Provision Module(s) - CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the command prompt, check the current provisioning status. Type **show provision modules** and press **Enter**. The status displays:



```

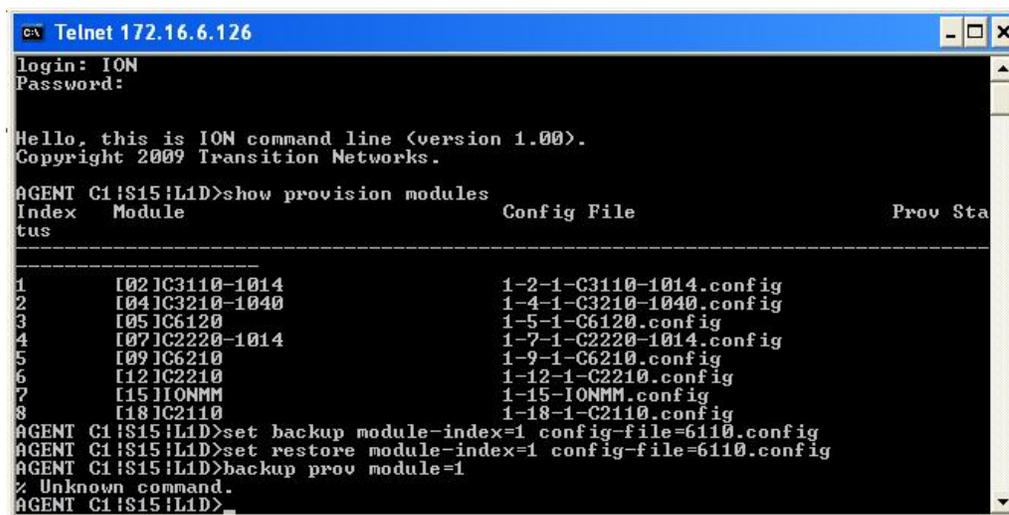
Telnet 172.16.6.126
login: ION
Password:

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

AGENT C1!S15!L1D>show provision modules
Index  Module                               Config File                               Prov Sta
tus
-----
1      [02]C3110-1014                          1-2-1-C3110-1014.config
2      [04]C3210-1040                          1-4-1-C3210-1040.config
3      [05]C6120                               1-5-1-C6120.config
4      [07]C2220-1014                          1-7-1-C2220-1014.config
5      [09]C6210                               1-9-1-C6210.config
6      [12]C2210                               1-12-1-C2210.config
7      [15]IONMM                               1-15-IONMM.config
8      [18]C2110                               1-18-1-C2110.config
AGENT C1!S15!L1D>

```

3. Set the Provision module backup configuration.
Type **set backup module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.
4. Set the Provision module Restore configuration.
Type **set restore module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.
5. Specify 1-10 provision modules to be backed up. Type **backup prov module=x** and press **Enter**.
6. Specify 1-10 provision modules to be restored. Type **restore prov module =x** and press **Enter**.
7. Verify the configuration. Type **show provision modules** and press **Enter**. For example:



```

Telnet 172.16.6.126
login: ION
Password:

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

AGENT C1!S15!L1D>show provision modules
Index  Module                               Config File                               Prov Sta
tus
-----
1      [02]C3110-1014                          1-2-1-C3110-1014.config
2      [04]C3210-1040                          1-4-1-C3210-1040.config
3      [05]C6120                               1-5-1-C6120.config
4      [07]C2220-1014                          1-7-1-C2220-1014.config
5      [09]C6210                               1-9-1-C6210.config
6      [12]C2210                               1-12-1-C2210.config
7      [15]IONMM                               1-15-IONMM.config
8      [18]C2110                               1-18-1-C2110.config
AGENT C1!S15!L1D>set backup module-index=1 config-file=6110.config
AGENT C1!S15!L1D>set restore module-index=1 config-file=6110.config
AGENT C1!S15!L1D>backup prov module=1
% Unknown command.
AGENT C1!S15!L1D>

```

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 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 9: 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	/ftptboot	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

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](#)” on page 124.

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, including the IP address you assigned to the IONMM.

Resetting Defaults – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the command prompt type: **reset factory**.
3. Press **Enter**. The following message displays:

```
Warning: this command will restart the specified card, connection will be lost!
```

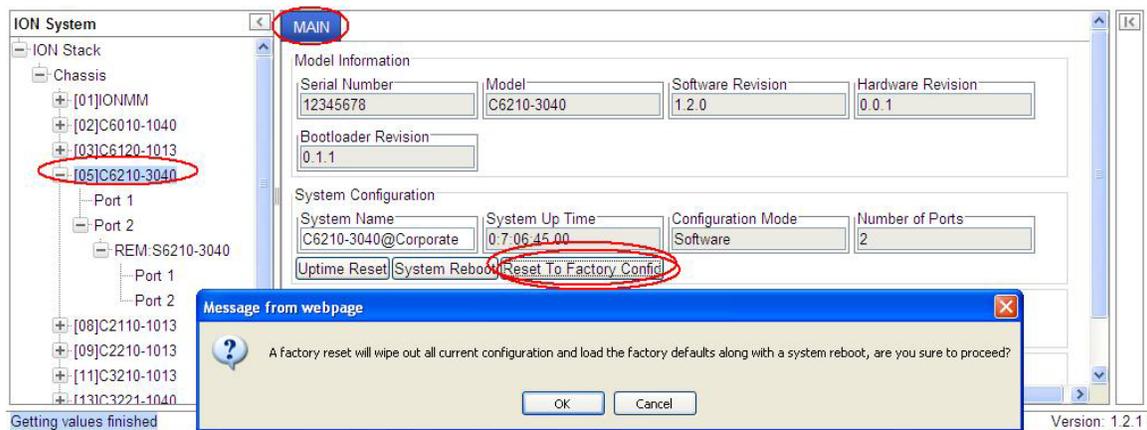
All configuration parameters will be reset to their factory values. For a list of all factory defaults, see “[Appendix B: Factory Defaults](#)” on page 179).

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

Resetting Defaults – Web Method

Caution: This operation deletes all configuration information that was saved in the x6210, including the IP address you assigned to the x6210.

1. Access the x6210 through the Web interface (see “Starting the Web Interface” on page 45).
2. At the **MAIN** tab, locate the **System Configuration** section.
3. 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.



4. Click **Cancel** if you are not 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” on page 179).

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 10: 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 configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	Restored to factory configuration (lost)

Resetting Uptime

The ION system uptime field displays the amount of time that the ION system 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 Reset Uptime function changes the x6210 device's system uptime, zeros out the counters, and starts incrementing again. The System Up Time can be set on a Remote S6210 (level 2 device) via the Web interface. Reset uptime on the connected (local) chassis device will not reset the remote device's uptime counters.

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

Reset System Uptime – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
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:

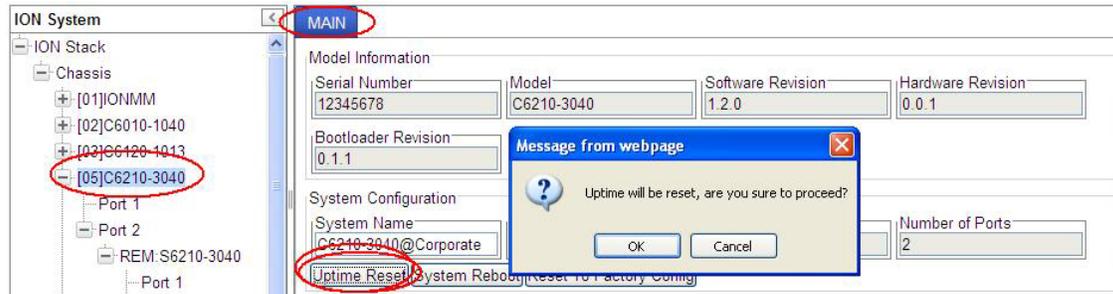
```
C1 | S13 | L1P2 > reset uptime
C1 | S13 | L1P2 >
```

Use the **show card info** command to display the current system uptime.

Note: The **reset uptime** command is not available for all ION system devices.

Reset System Uptime – Web Method

1. Access the C6210 through the Web interface (see “Starting the Web Interface” on page 26).
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 will be reset, are you sure to proceed” message 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 can be set on a Remote S6210 (level 2 device) via the Web interface. Reset uptime on the connected (local) chassis device will not reset the remote device’s uptime counters.

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

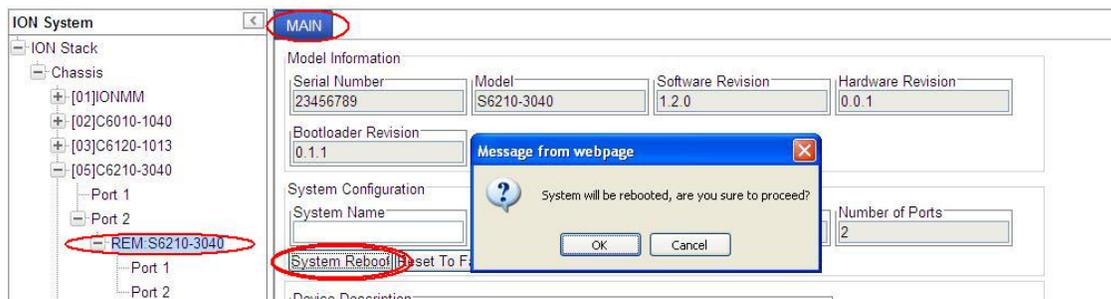
1. Access the x6210 through either a USB connection (see [“Starting a USB Session”](#) on page 41) or a Telnet session (see [“Starting a Telnet Session”](#) on page 43).
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login again!* The ION system reboots. If this operation is performed on a standalone module, the connection / session is terminated. After an x61xx reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.
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”](#) on page 41).
 - For a Telnet session
 - a) Press **Enter**.
 - b) Start a Telnet session (see [“Starting a Telnet Session”](#) on page 43).

Rebooting – Web Method

Caution: Doing a system reboot will cause all 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 x6210 through the Web interface (see “Starting the Web Interface” on page 45).
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 x6210 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 11: 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. The latest firmware version is at <https://www.lantronix.com/products/c6210-series/>. 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” on page 332.

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” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
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 at <https://www.lantronix.com/products/c6210-series/>
5. Locate the “Agent Firmware” section and click the link in the right hand column (e.g., “Download IONMM.bin.1.0.5.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
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](#)” on page [301](#) 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 will cause all 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.

A. 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](#)” on page 45).
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 x6210 NID or IONMM firmware for use in steps D1 and D2 below.

B. Locate the New IONMM / NID Firmware Version

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

1. Go to the Lantronix web page at <https://www.lantronix.com/products/c6210-series/>.
2. Locate the “**Agent Firmware**” section and examine the link in the right hand column (e.g., “**Download x6210_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 file.

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](#)” on page 45).
2. Select the **MAIN** tab.
3. Locate the **TFTP Settings** section at the bottom of the screen.

TFTP Settings

TFTP Server Address 192.168.1.30	Firmware File Name 	Status No Action
Save Server Address	Upgrade Firmware	Refresh

Refresh Save Help

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.

TFTP Settings

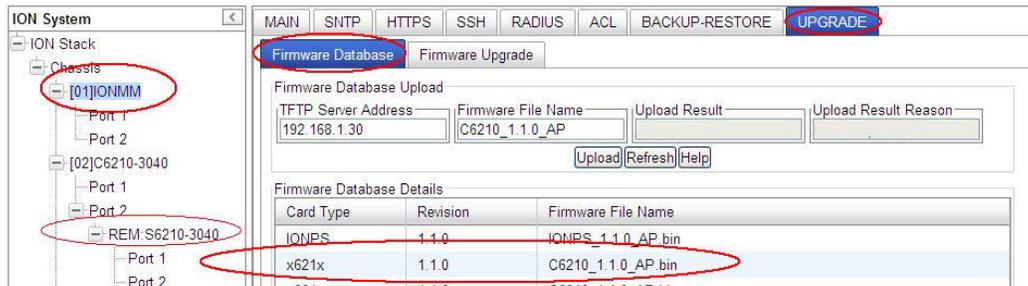
TFTP Server Address 192.168.1.30	Firmware File Name x323x_1.0.3_AP	Status No Action
Save Server Address	Upgrade Firmware	Refresh

Refresh Save Help

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 x6210 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.

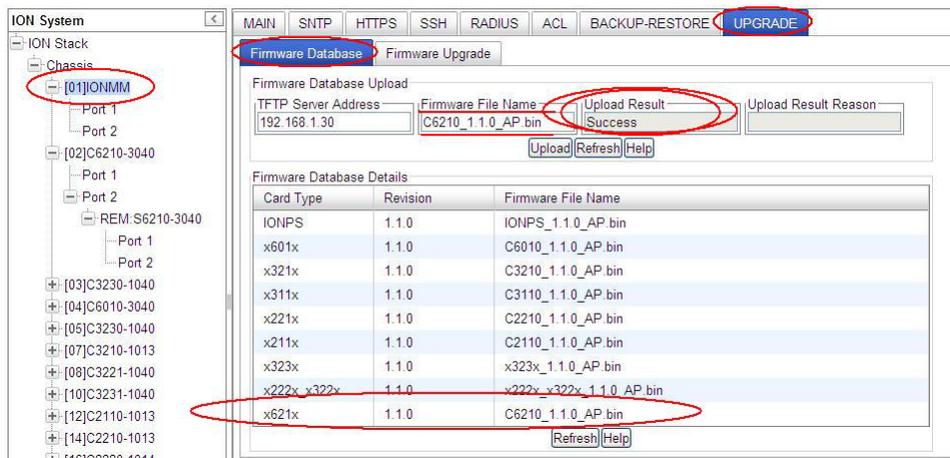
D2. Upgrade IONMM / NID Firmware from the **UPGRADE** Tab

1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 45).
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*.

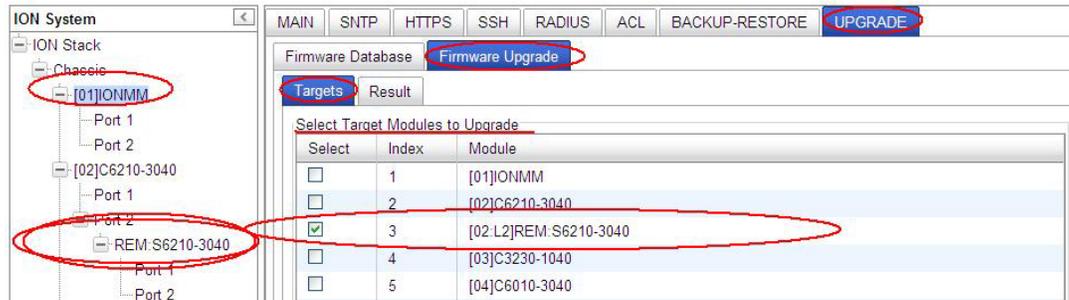
When successfully completed, the message “Getting all records finished” displays, the **Upload Result** area displays “Success”, and the **Firmware Database Details** section displays updated firmware information.



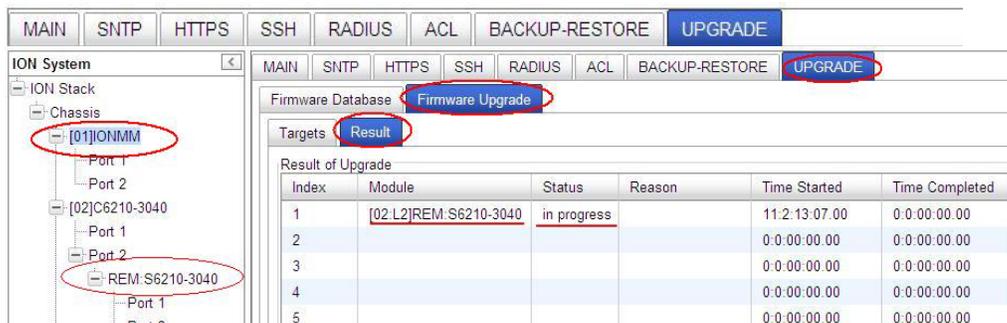
8. If the firmware upload operation failed, the **Upload Result** area displays either:
 - **None**: no operation was performed, or
 - **Failure**: the specified operation has failed.

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'.

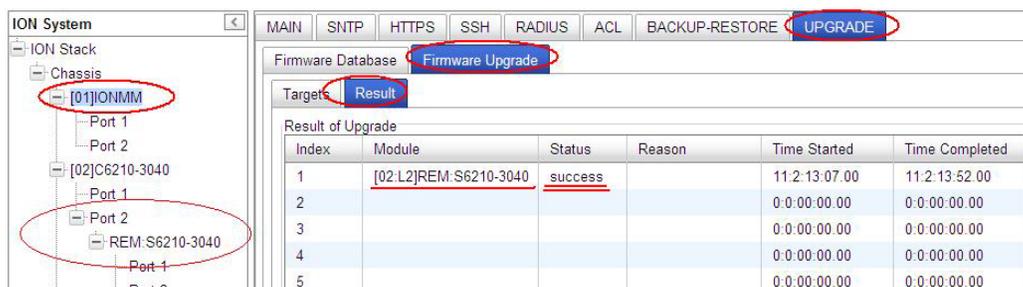
9. Click the **Firmware Upgrade** sub-tab.
10. Click the **Targets** sub-tab if not already displayed.
The modules that are available to be upgraded display in a table.



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. A confirmation message displays.
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.



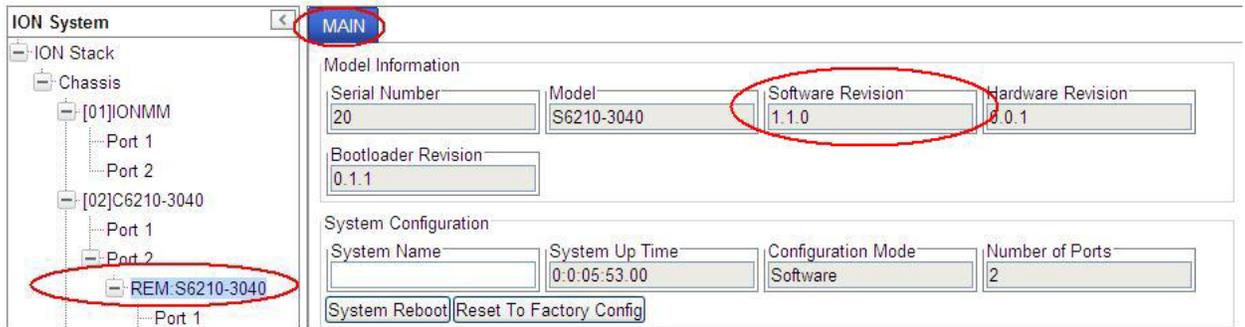
15. Click the **Refresh** button. The **Status** column displays *"success"*.



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](#)” on page 301 for error messages and recovery procedures.
18. Check the **MAIN** tab for each upgraded module to ensure that the correct revision level is displayed in the **Software Revision** field. You may need to click the **Refresh** button.



The sample screen above shows the remote S6210 **MAIN** tab with the **Software Revision** field indicating a successful firmware upgrade to version **1.1.0**.

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 C6210 [latest firmware page](#).
- Create the Database Index and Archive Files (below).
- Perform the Module Firmware Upgrade (page 114).

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 for an upgrade of two chassis-resident modules (IONMM and C6210-1040), and no second level remotes.

```

IONMM1.1.0  IONMM.bin.1.0.5_AP
C6210-1040  1.1.0  C6210_1.1.0_AP
C6210-1040  1.1.0  C6210_1.1.0_FPGA_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 **C6210.bin.0.6.5.zip**).

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

- db.idx

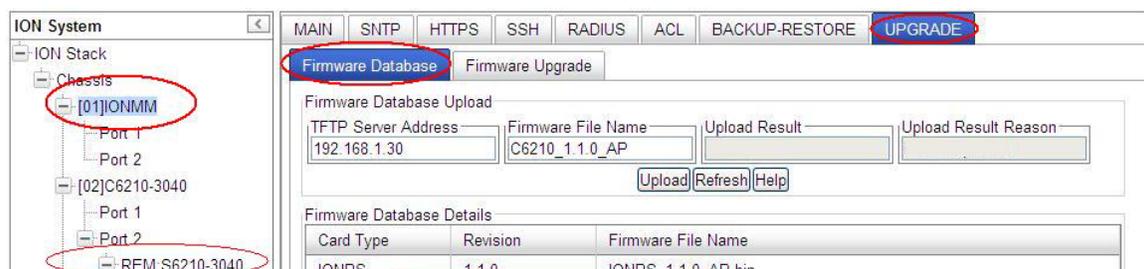
- IONMM.bin. 1.1.0
- C6210_1.1.0_AP
- C6210_1.1.0_FPGA_AP

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”](#) on page 45).
2. Select the **Upgrade** tab. The **Firmware Database** sub-tab displays.

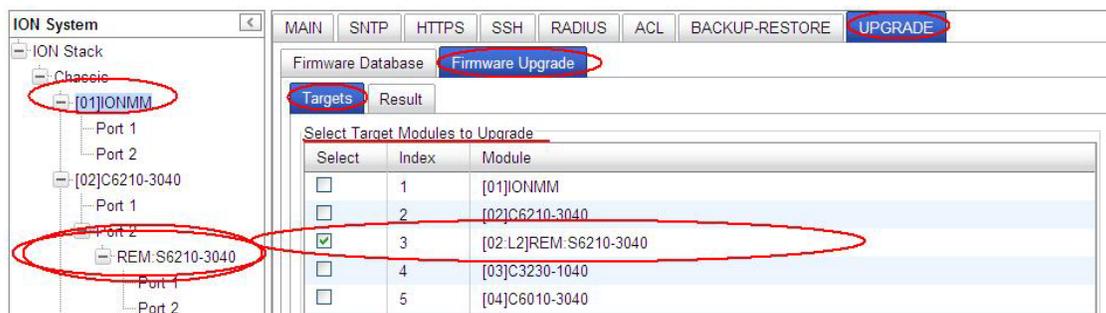


3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP Server where the upgrade (zip) file is located.
4. In the **Firmware File Name** field, enter the name of the zip file you created (e.g., **C6210.bin0.6.5.zip**). **Note:** Be sure to include the .zip extension in the filename.
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.



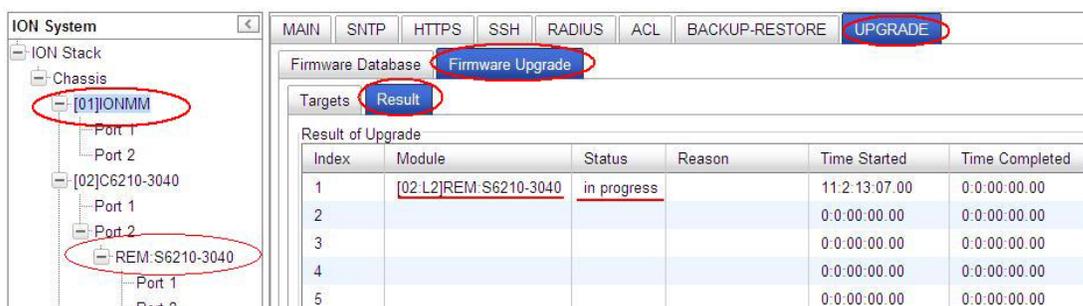
8. In the **Select** column, check the checkbox of each module to be upgraded.

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.

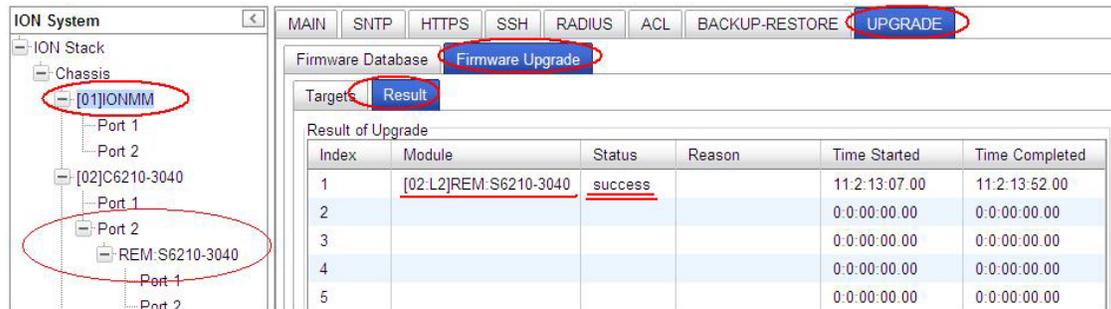
9. Click the **Upgrade** button.

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

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.



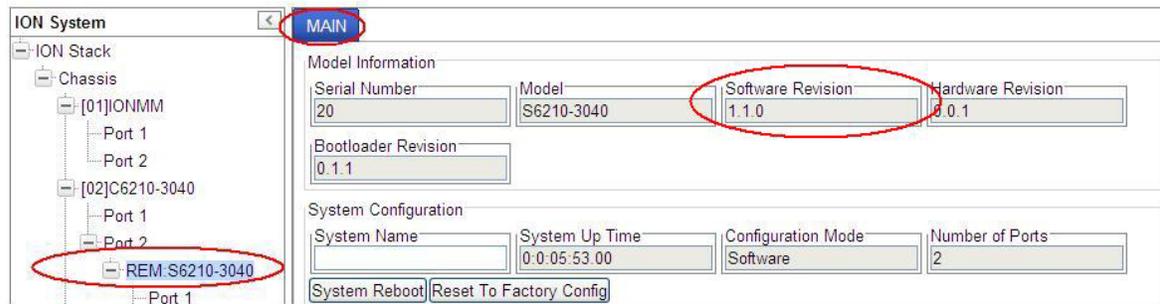
The screenshot shows the ION System interface with the 'UPGRADE' tab selected. The 'Firmware Upgrade' sub-tab is active, displaying a table of upgrade results. The table has columns for Index, Module, Status, Reason, Time Started, and Time Completed. The first row shows a successful upgrade for module [02:L2]REM-S6210-3040.

Index	Module	Status	Reason	Time Started	Time Completed
1	[02:L2]REM-S6210-3040	success		11:2:13:07.00	11:2:13:52.00
2				0:0:00:00.00	0:0:00:00.00
3				0:0:00:00.00	0:0:00:00.00
4				0:0:00:00.00	0:0:00:00.00
5				0:0:00:00.00	0:0:00:00.00

Note: the upgrade will take one or more minutes to complete. The exact amount of time for the upgrade depends on the number and models 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](#)” on page 261 for error messages and recovery procedures.

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



The screenshot shows the ION System interface with the 'MAIN' tab selected for the remote S6210-3040 module. The 'Model Information' section displays the following fields:

Serial Number	Model	Software Revision	Hardware Revision
20	S6210-3040	1.1.0	0.0.1

The 'Software Revision' field is highlighted, showing the value 1.1.0. The 'System Configuration' section displays the following fields:

System Name	System Up Time	Configuration Mode	Number of Ports
	0:0:05:53.00	Software	2

The screen above shows the remote S6210 **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 12: 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 configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

Additional Upgrade Procedures

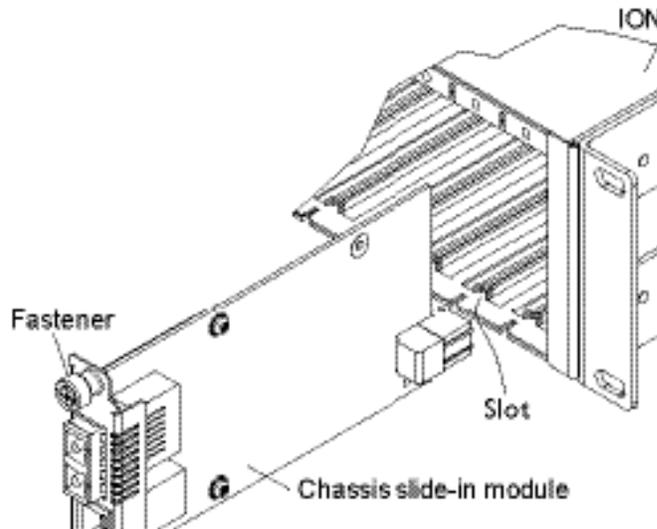
Additional upgrade procedures are available for the ION system. Refer to the *IONMM User Guide* for these IONMM upgrade procedures:

- 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 archive 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 x6210 is a “hot swappable” device (it can be removed and installed while the chassis is powered on). To replace a chassis resident x6210, do the following.

1. Backup the configuration (see [Backing Up Slide-In and Remote Modules](#) on page 150).
2. Disconnect any cables attached to the x6210.



3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the old x6210 from the Chassis.
5. Carefully slide the new x6210 fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the x6210 to the chassis.
7. Connect the appropriate cables to the x6210.
8. Load (restore) the configuration into the new x6210 (see [Restoring Slide-In and Remote Modules](#) on page 114).

6: Command Line Interface (CLI) Reference

General

This section describes CLI use and the commands for the x6210.

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.

```
X6210>show tdm <tab key>
config      loopback   port
```

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

```
Agent III C1|S5|L1D>show tdm ?
config
inband
loopback
peer
port
Agent III C1|S5|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 13: 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 x6210 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 Lantronix.

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 NID.

Command: Log Out (Quit)

Syntax : q(uit)

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

```
Example : Agent III C1|S5|L1D>q

login:
```

Note: The NID 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 log out.

Command: Help (?)

Syntax: ? <cr>

Description: Displays all available command line commands.

Example: A sample ? (help) command listing is shown below.

```
AgentIII C1|S3|L1P2>?
add          Add a ACL condition
backup      Backup specified provision modules.
cat         Show the content of the FILES
cd          Change to another directory
clear       Clear all counters of the specified Ethernet port
cls         Clear the screen.
flush       Flush VLAN db.
generate    Generate the specified SSH host key.
go          set location to device/port of the SIC to be operated.
home        go back to IONMM card
list        Print command list
ls          List the information about the FILES
more        A filter for paging through text one screenful at a time.
ping        Send ICMP ECHO-REQUEST to network hosts.
prov        Get 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.
remove      Remove all ACL conditions
reset       Reset all ports' counters of the specified Ethernet port
restart     Restart ACL
restore     Restore specified provision modules.
send        Initiates the delay measurement for a given MEP. Please note that
            only one DM request is supported at a time for a given MEP.
serial      transfer file through a serial line.
set         Set bakup/restore configuration file name for a specified
            provisionmodule.
show        Show ACL chains
start       Start TDR test of the specified Ethernet port
stat        Show topology information of a chassis.
tftp        Get a file from a TFTP server.
update      Update fireware database
upgrade     Upgrade firmware modules
AgentIII C1|S3|L1P2>
```


Command: Set DMI Receive Power Preset Level

Syntax: set dmi rx-power-preset-level=<x>

Description: Defines the current

where x = <0-65,535>

```
Example: AgentIII C1|S3|L1D>go l1p=1
AgentIII C1|S3|L1P1>set dmi rx-power-preset-level 3
DMI is only supported on FIBER port!
AgentIII C1|S3|L1P1>go l1p=2
AgentIII C1|S3|L1P2>set dmi rx-power-preset-level 3
```

Command: Show Card Type

Syntax: show cardtype

Description: Displays the device (card) information for the x6210.

```
Example: AgentIII C1|S3|L1D>show cardtype
Card type: C6210-3040
AgentIII C1|S3|L1D>
```

Command: Show Card Information

Syntax: show card info

Description: Displays the system information (sys config table) for the x6210.

```
Example: Agent III C1|S5|L1D>show card info
System name: C6210-3040@Corporate
Uptime: 07:52:27
Port number: 2
Serial number: 12345678
Config mode: software
Software: 1.2.0
Bootloader: 0.1.1
Hardware: 0.0.1
Agent III C1|S5|L1D>
```

Command: Set System Name**Syntax:** set system name=(name) <cr>**Description:** Changes the name assigned to the x6210 device. The default setting is blank.

```

Example: AgentIII C1|S3|L1D>set system name=S6210-32@Corporate
AgentIII C1|S3|L1D>show card info
System name:      S6210-32@Corporate
Uptime:          01:17:55
Port number:     2
Serial number:   12345678
Config mode:    software
Software:       0.7.4
Bootloader:     0.1.1
Hardware:       0.0.1
AgentIII C1|S3|L1D>

```

The system name default is x6210 (case sensitive – the S or C in capitals). The **show card info** command displays the system name, uptime, number of ports, software version, and other device information.

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: AgentIII C1|S3|L1D>show circuit-ID
Circuit-ID:      xx/CD-FDB
AgentIII C1|S3|L1D>set circuit XX/YYYY/000000/111/CC/SEG
AgentIII C1|S3|L1D>show circuit-ID
Circuit-ID:      XX/YYYY/000000/111/CC/SEG
AgentIII C1|S3|L1D>

```

The default setting is an empty field. The Device Description / Circuit ID is an ASCII text string up to 63 bytes that overrides the default Circuit ID, which is the vlan-module-port in binary format. At the ION system device level it is displayed as ‘Device Description’, MIB variable is ‘sysName’ in ‘system public mib, oid: 1.3.6.1.2.1.1.5. At the ION system port level it is displayed as ‘Circuit ID’, MIB variable is ‘ifAlias’ in ‘ifXTable’ public mib, oid: 1.3.6.1.2.1.31.1.1.18.

Note: the dash (“-”) is required, and the letters “ID” must be upper-case. 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: AgentIII C1|S3|L1D>show circuit-ID
Circuit-ID:      xx/CD-FDB
AgentIII C1|S3|L1D>set circuit XX/YYYY/000000/111/CC/SEG
AgentIII C1|S3|L1D>show circuit-ID
Circuit-ID:      XX/YYYY/000000/111/CC/SEG
AgentIII C1|S3|L1D>
```

Note: the dash ("-") is required, and the letters "ID" must be upper-case. If no circuit ID has been defined via the set circuit-ID= command, nothing displays after the "Circuit-ID".

Command: Prov Get TFTP Server Address

Syntax: prov get tftp svr addr

Description: Accesses the TFTP server's IP address.

```
Example: AgentIII C1|S3|L1D>prov get tftp svr addr
AgentIII C1|S3|L1D>
```

Command: Prov Set TFTP Server Address

Syntax: prov set tftp svr type

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

```
Example: AgentIII C1|S3|L1D>prov set tftp svr type ipv4 addr 192.168.1.30
AgentIII C1|S3|L1D>
```

TAOS and AIS Commands

The TAOS (Transmit All Ones) and AIS (Alarm Indication Signal) commands generate a pre-defined signal.

AIS, also called “all ones” due to its data / framing pattern, is a signal transmitted by an intermediate element of a multi-node transport circuit that is part of a concatenated telecommunications system to alert the receiving end of the circuit that a segment of the end-to-end link has failed at a logical or physical level, even if the system it is directly connected to is still working. The AIS replaces the failed data, allowing the higher order system in the concatenation to maintain its transmission framing integrity. Downstream intermediate elements of the transport circuit propagate the AIS onwards to the destination element. All ones is an OAM function type used for fault management (see also CC, RDI). All 1's, also called Blue Alarm, is used as a ‘keep alive’ signal.

TAOS (Transmit All Ones) is a circuit or device that generates and sends a series of digital "ones" on a line for testing purposes. The x6210 has configurable TAOS (transmit all ones) on the fiber and copper interfaces to test all T1/E1 equipment on that network segment and ensure the network link. The x6210 TAOS Enable/Disable on copper and fiber port can be managed by x6210 software or hardware DIP switch setting. The x6210 generates the AIS by transmitting all ones (TAOS).

The following commands are used for TAOS and AIS operations.

Command: **Enable/Disable TAOS Transmitting**

Syntax: **set taos transmit=<enable|disable>**

Description: A port-level command that defines the current x6210 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 enable.

```
Example: AgentIII C1|S3|L1D>set taos transmit enable
Error: this command should be executed on a port!
AgentIII C1|S3|L1D>go l1p=1
AgentIII C1|S3|L1P1>set taos transmit enable
TAOS status setting is not supported on this card!
AgentIII C1|S3|L1P1>go l1p=2
AgentIII C1|S3|L1P2>set taos transmit enable
TAOS status setting is not supported on this card!
AgentIII C1|S3|L1P2>
```

Command: Enable / Disable AIS Transmitting**Syntax:** `set ais transmit=<x> <cr>`**Description:** Device-level command used to define the device's AIS (Alarm Indication Signal) operating state, where x = <enable|disable >.

```

Example: AgentIII C1|S3|L1D>set ais transmit ?
            disable
            enable
AgentIII C1|S3|L1D>set ais transmit enable
AgentIII C1|S3|L1D>set ais transmit enable
AgentIII C1|S3|L1D>set ais transmit disable
AgentIII C1|S3|L1D>

```

The message “AIS transmit setting is not supported on this card!” displays if the AIS function is not configurable on a specific device.

Command: Set AIS Format**Syntax:** `set ais format={allones|blue}`**Description:** A device-level command that displays the current x6210 port's AIS format setting (either **blue** or **allones**). The default setting is blue. Defines the device's AIS (Alarm Indication Signal) formatting,
where:

allones = use a pattern of all ones (11111) to replace the failed data.

blue = use a pattern of an unframed all-ones signal to maintain transmission continuity.

```

Example: AgentIII C1|S3|L1P1>set ais format ?
            allones
            blue
AgentIII C1|S3|L1P1>set ais format allones
Error: this command should be executed on a device!
AgentIII C1|S3|L1P1>go l1d
AgentIII C1|S3|L1D>set ais format allones
AgentIII C1|S3|L1D>set ais format blue
AgentIII C1|S3|L1D>

```

TDM Commands

The TDM commands let you set the loopback test type, initiate and stop the loopback test process, and display the current loopback capability.

The following commands are used for TDM operations.

Command: Set Loopback Type of Specified TDM Port

Syntax: `set tdm loopback type=(noloopback|phylayer) <cr>`

Description: Defines the type of loopback for a specified TDM port to either no loopback support, or to Phy Layer loopback support.

where:

x= (noloopback|phylayer)

```

Example: AgentIII C1|S3|L1P2>set tdm loopback type ?
        maclayer
        noloopback
        phylayer
AgentIII C1|S3|L1P2>set tdm loopback type=maclayer
Set TDM port loopback type failed.
AgentIII C1|S3|L1P2>set tdm loopback type=phylayer
AgentIII C1|S3|L1P2>set tdm loopback type=noloopback
AgentIII C1|S3|L1P2>go l1p=1
AgentIII C1|S3|L1P1>set tdm loopback type=noloopback
AgentIII C1|S3|L1P1>set tdm loopback type=phylayer
AgentIII C1|S3|L1P1>set tdm loopback type=maclayer
Set TDM port loopback type failed.
AgentIII C1|S3|L1P1>

```

Command: Set TDM Loopback Operation

Syntax: `set tdm loopback oper=<init|stop> <cr>`

Description: Starts and stops the current loopback test.

```

Example: AgentIII C1|S3|L1P1>set tdm loopback oper=init
AgentIII C1|S3|L1P1>set tdm loopback oper=stop
AgentIII C1|S3|L1P1>

```

Command: Show Loopback Capability of Specified TDM Port**Syntax:** `show tdm loopback capability <cr>`**Description:** Displays the current loopback functionality that has been set for the port specified in the command. The loopback capabilities that can display are "noloopback", "phyLayer", "macLayer", "alternate", or "remotePeer".

```

Example: AgentIII C1|S3|L1P1>show tdm loopback capability
Loopback capability: phyLayer
AgentIII C1|S3|L1P1>go l1p=2
AgentIII C1|S3|L1P2>show tdm loopback capability
Loopback capability: phyLayer
AgentIII C1|S3|L1P2>

```

Command: Show TDM Loopback State**Syntax:** `show tdm loopback state <cr>`**Description:** Displays the current loopback operating state for the port entering the command. The loopback capabilities that can display are ""noLoopback", "intiateLoopback", "terminateLoopback", "inProcess", "localInLoopback", or "remoteInLoopback".

```

Example: AgentIII C1|S3|L1P1>show tdm loopback state
Loopback type: phylayer
Loopback state: noLoopback
Agent III C1|S5|L1P1>set tdm loopback oper=init
Agent III C1|S5|L1P1>show tdm loopback state
Loopback type: phylayer
Loopback state: localInLoopback
Agent III C1|S5|L1P1>

```

Command: Show TDM Configuration**Syntax:** `show tdm config <cr>`**Description:** A device-level command that displays the x6210 TDM table containing the x6210 device's current TDM configuration settings.

```

Example 1: AgentIII C1|S3|L1D>show tdm config
ais transmit:                disabled
ais format:                  blue
tdm type:                    e3
AgentIII C1|S3|L1D>

```

```

Example 2: AgentIII C1|S3|L1D>set ais transmit enable
AgentIII C1|S3|L1D>set ais format allones
AgentIII C1|S3|L1D>show tdm config
ais transmit:                enabled
ais format:                  allones
tdm type:                    e3
AgentIII C1|S3|L1D>

```

Command: Show TDM Port Configuration

Syntax: show tdm port config <cr>

Description: A port-level command that displays the x6210 TDM table containing the current x6210 device port's TDM configuration settings.

```
Example: AgentIII C1|S3|L1P1>show tdm port config
link oper status: down
alarm indication signal: normal
lbo status: normal
connector: Dual BNC
AgentIII C1|S3|L1P1>go l1p=2
AgentIII C1|S3|L1P2>show tdm port config
link oper status: down
alarm indication signal: normal
connector: SFP Slot
AgentIII C1|S3|L1P2>
```

Command: Status Check - Chassis Configuration

Syntax: stat

Description: Displays the current chassis configuration in terms of local and remote devices.

Example:

```
AgentIII C1|S3|L1D>stat
ION statck
    Chassis -- BPC
        [ 1] IONMM
            Port 1
            Port 2
        [ 2] C6210-1040
            Port 1
            Port 2
        [ 3] C6210-3040
            Port 1
            Port 2
        [ 4] C6120-1013
            Port 1
            Port 2
            Port 3
            Port 4
            Port 5
            Port 6
        [ 6] C3220-1040
            Port 1
            Port 2
        [ 7] C3210-1013
            Port 1
            Port 2
        [ 8] C3221-1040
            Port 1
            Port 2
            Port 3
        [ 9] C3230-1040
            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
AgentIII C1|S3|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

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 C6210

Syntax: reboot

Description: Performs a reboot (“warm 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).

Example 1 C6210):

```
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 x6210.

Example 2 (S6210):

```
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 reset to factory removes temporary files (e.g. configuration backup files, Syslog file) and 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 x6210.

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: list

Description: Displays all of the available x6210 CLI commands. For example:

```
C1|S2|L1D>list
1. clear ether all counters
2. cls
3. 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)
4. home
5. list
6. ls [OPTION] [FILES]
7. more [OPTION] [+linenum] FILE ...
8. ping [-c COUNT] [-t TTL] A.B.C.D
9. prov get tftp svr addr
10. prov set tftp svr type=(ipv4|dns) addr=ADDR
11. ps [OPTION]
12. pwd
13. quit
14. reboot
15. reset all ports counters
16. reset factory
17. reset uptime
18. set ais format=(blue|allones)
19. set ais transmit=(enable|disable)
20. set circuit-ID=CIRCUIT
21. set community read=COMMUNITY
22. set community write=COMMUNITY
23. set dbg level=<0-2>
24. set dmi rx-power-preset-level=POWER
25. set system name=NAME
26. set taos transmit=(enable|disable)
27. set tdm loopback oper=(init|stop)
28. set tdm loopback type=(noloopback|phylayer)
29. show card info
30. show cardtype
31. show circuit-ID
32. show dmi info
33. show firmware upgrade result (IONMM only)
34. show firmware-db update result (IONMM only)
35. show tdm config
36. show tdm loopback capability
37. show tdm loopback state
38. show tdm port config
39. stat
40. tftp get iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
41. tftp put iptype=(ipv4|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
42. tftp upgrade iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE
43. upgrade module
C1|S2|L1D>
```

Note: the numbers in the list of commands are for reference only.

Note that not all of the commands listed are necessarily operational on the x6210 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, x6210 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. Write down your initial 2-3 guesses as to the cause of the problem.
6. Start with the most simple 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, etc., and then run ION System Tests ([page 193](#)), check DIP Switches and Jumper Settings ([page 206](#)), check DS3-E3 Error Events and Alarm Conditions on [page 238](#)).

7. Verify that the product supports the function you are trying to perform. Your particular 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. 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.)
9. Use the ION system manual procedure to retry the failed function or operation.
10. For the failed function or operation, verify that you entered valid parameters using the cursor-over-help (COH) and/or the ION system manual.
11. 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 fix for each.
12. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
13. 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).
14. If you find a sequence of actions that causes the problem to recur, replicate the full sequence several times and document it if possible.
15. Review your logged 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.
16. Review the “[Recording Model Information and System Information](#)” section on page 238 before calling for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED fault and Activity displays ([page 134](#))
- Problem Conditions ([page 136](#))
- CLI Messages ([page 154](#))
- Web Interface Messages ([page 153](#))
- Webpage Messages ([page 151](#))
- Config Error Log (config.err File) Messages ([page 164](#))
- Third Party Tool Messages (HyperTerminal, Ping, and Telnet Messages) ([page 172](#))
- T1 Error Events and Alarm Conditions ([page 225](#))

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 on page 54, 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 if other network devices are working properly.
5. Check the power supply voltages (see related documentation).
6. Verify that the ION system devices have the latest firmware versions. Download the latest firmware version and upgrade as necessary.

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

1. Check at both ends for a loose power cord.
2. Make sure all circuit protection and connection equipment and devices are working.
3. Verify that the ION system power supply is within operating range.
4. Remove the power supply from the chassis and re-insert it. Replace if failed.
5. Make sure the mode displayed matches the hardware setting on the device. See the “[Jumper Settings](#)” section on page 212.

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 TX and RX cables on media converter are connected to RX and TX ports, respectively, on other media converter.
4. Check if other network devices are working properly.
5. Remove the suspect card from the chassis and re-insert it.

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

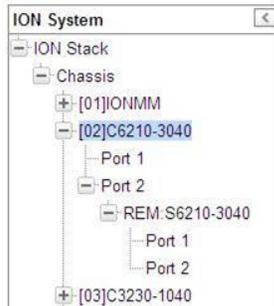
1. Check the **CL - FL** Switch setting.
2. Check twisted pair cables for proper connection.
3. Check the RJ-45 for correct twisted pair cable configuration.
4. Check integrity of device attached to media converter by twisted pair cable.
5. Check if other network devices are working properly.
6. Remove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

TX or RX LED off (not flashing):

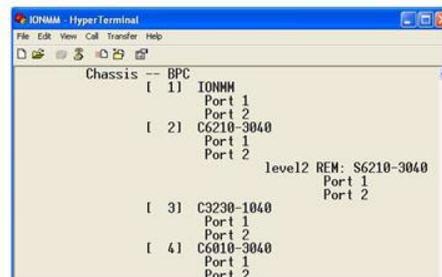
1. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
2. Check if other network devices are working properly.
3. Verify that the ION system devices have the latest firmware versions.
4. Download the latest firmware version and upgrade as necessary.
5. Remove the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

Problem Conditions

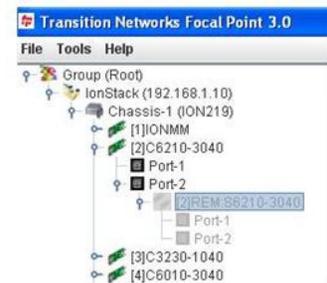
You can access the x6210 via the ION Web interface, the ION CLI, and Focal Point 3. Comparing the results of an operation via each user interface is an initial step in troubleshooting.



ION System – Web Interface



ION System – Command Line Interface (CLI)



Focal Point 3.0 – Web Interface

1. Verify the overall ION system configuration.
2. Compare the ION configuration via each user interface (ION Web interface, ION 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 can not 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] [I1ap=PORT] [I2ap=PORT] (I1p=PORT | I2p=PORT | I3p=PORT | I1d | I2d | I3d)
3. Power cycle the x6210.
4. If the problem persists, see [Contact Us](#) on page 233.

Cannot access the x6210 via Telnet

1. If you can access the IONMM, continue with step 2 below. If you can not 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] [I1ap=PORT] [I2ap=PORT] (I1p=PORT|I2p=PORT|I3p=PORT|I1d|I2d|I3d)`
3. Power cycle the x6210.
4. If the problem persists, see [Contact Us](#) on page 233.

Cannot access the x6210 via the Web

1. If you can access the IONMM, continue with step 2 below. If you can not access the IONMM, see the IONMM User Guide.
2. Check the hardware settings on the x6210. See “[Jumper Settings](#)” on page 31 and “[DIP Switch Settings](#)” on page 33.
3. Power cycle the x6210. If the x6210 is a remote, power cycle the local x6210.
4. If the problem persists, see [Contact Us](#) on page 233.

Cannot activate IP-based management

1. Use the **go** command to switch to a device that supports IP configuration.
2. If the problem persists, see [Contact Us](#) on page 233.

Cannot upgrade modules

See [Upgrade fails](#) on page 177.

Cannot upload upgrade files

See [Upload fails](#) on page 177.

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”](#) on page 45), 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, see [Contact Us](#) on page 233.

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, see [Contact Us](#) on page 233.

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, see [Contact Us](#) on page 233.

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](#)" on page 148).
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, see [Contact Us](#) on page 233.

USB connection resets after a CLI command is executed

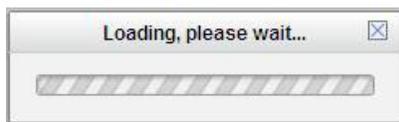
1. If you can connect to the IONMM through the Web interface (see [“Starting the Web Interface”](#) on page 45), go to step 4 of [“Telnet connection is lost after a CLI command is executed”](#) on page 168. If you can not connect to the IONMM through the Web interface, continue with step 2 below.
2. 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, see [Contact Us](#) on page 233.

Configuration Mode Mismatch

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.

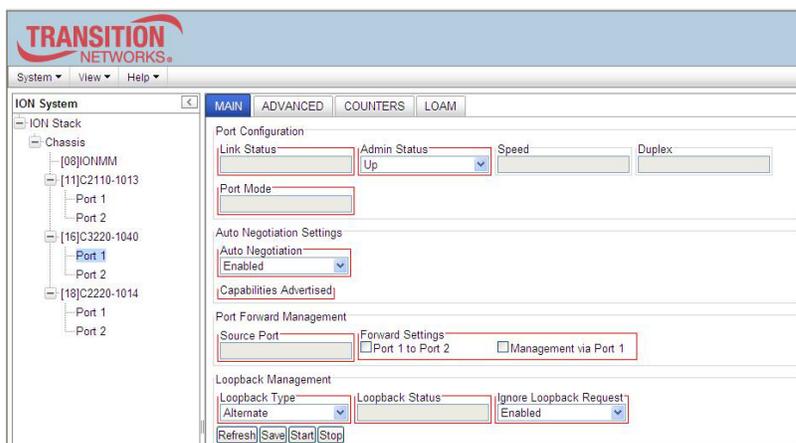
1. Refer to the [“DIP Switches and Jumper Settings”](#) section on page 206 for details on hardware mode configuration.
2. Contact Lantronix for more information.

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, see [Contact Us](#) on page 233.

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 device in question.
5. Reboot the x6210 by clicking the **Reboot** key. 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, see [Contact Us](#) on page 233.

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 C6210 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 C6210 is at an older version and shows the newer functions as 'red boxed'. Since the older version of C6210 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 on page [285](#) 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!

Meaning: after a successful CLI command entry, the system crashes and the message displays. For example:

1. Upgrade to the S3240 bootloader and Uboot was successful.
2. The S3240 Web interface HTTP shows as failed.
3. Log into the USB console, and enter the command show ip config. For example:

```
AgentIII C1|S3|L1D>show ip config
IP management configuration:
-----
IP management state no such object.
AgentIII C1|S3|L1D>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

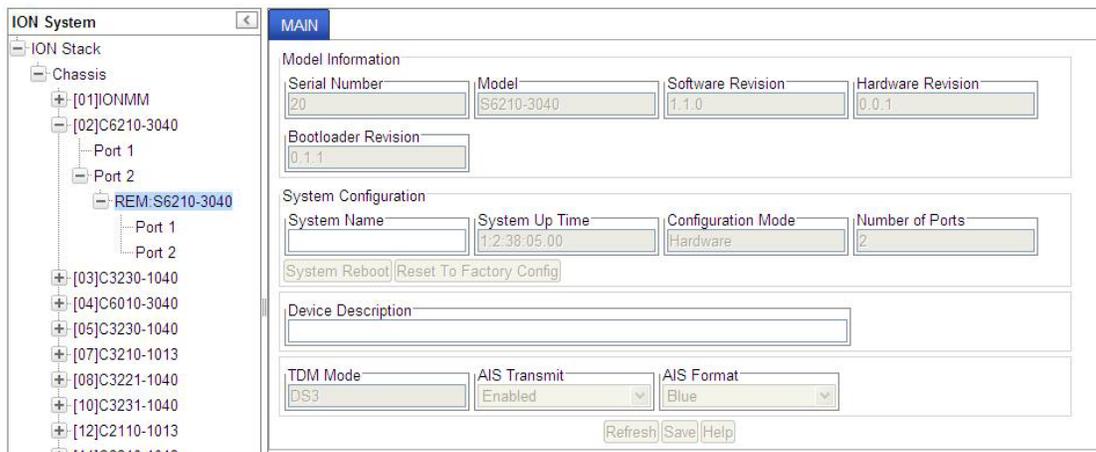
IP Address Wrong

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, SNMP, 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 x6210 configuration changes from the Web interface
GUI is not accessible
Web interface screens are all grayed out**



With the x6210 in Hardware mode, you cannot make x6210 configuration changes from the Web interface, as the screen fields are all grayed out.

1. Change the x6210 PCB J12 jumper setting. Jumper J12 sets the x6210 PCB's Hardware / Software mode. Use the shorting plug to jumper (short) pins 2 and 3 for Software Mode. See "[Jumper Settings](#)" on page 30.
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 x6210 again, and continue operation.
4. Use CLI commands for configuration and operation. See "[Section 6: Command Line Interface \(CLI\) Reference](#)" on page 120.
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 can be 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](#)" on page 31 and "[DIP Switch Settings](#)" on page 33.
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](#)" on page 108.
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

A. 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 then 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](#)” on page 124.
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](#)” on page 125.
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](#)” on page 125.
3. If the problem persists, contact Technical Support.

Cannot get LOAM configuration on this port!

Indicates that a command was entered on the x6210 but the command is not valid for the x6210.

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. If the problem persists, contact Technical Support.

Cannot get port security on this port!

Indicates that a command was entered for the x6210 but the command is not valid for the x6210.

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. 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](#)” on page 125.
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 is only applicable for a device.

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](#)” on page 125.
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” on page 125.
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](#)” on page 49).
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](#)” on page 125.
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 NID 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](#)” on page 125.
3. If the problem persists, contact Technical Support.

Failed to set DHCP client state!

This message indicates a problem in the DHCP setup / configuration.

1. Use the **go** command to switch to a device that supports this function.
2. 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 SNTP setup / configuration.

1. Use the **go** command to switch to a device that supports this function.
2. 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] [l1ap=L0APORT] [l2ap=L1APORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

3. If the problem persists, contact Technical Support.

Invalid condition value: xxxx

This message indicates that the input for the value= parameter on the **add acl condition** command is 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”](#) on page 49).
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 supports 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. Use the **go** command to switch to a device that supports this function.
4. 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.
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.
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.

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.

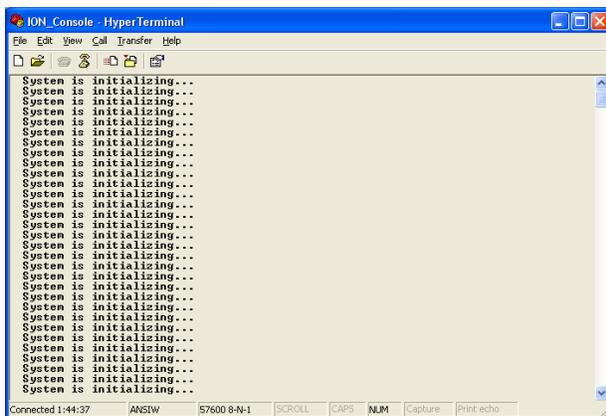
If the value of module, slot and port are not set in later commands, and then you run a device-level command, this error message displays.

Enter the **go** command and be sure to include all of the location parameters.

```
go [c=CHASSIS] [s=SLOT] [l1ap=L1APORT] [l2ap=L2APORT] (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 <x6210> 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.
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 (**X6210>**).
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.
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](#)” on page 125.
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. See “[Section 6: Command Line Interface \(CLI\) Reference](#)” on page 125.
3. Use the **go** command to switch to a device that supports this function.
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] [11ap=PORT] [12ap=PORT] (11p=PORT|12p=PORT|13p=PORT|11d|12d|13d)
```

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 *x6210.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](#)” on page 124.
7. 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.
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.

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 on page 157.
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.

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](#)” on page 167.
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. 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. 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. 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. 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](#)” on page 64.
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](#)” on page 64.
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.
4. 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 reseal 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.

**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.

Can not set Ethernet port 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. If the problem persists, contact Technical Support.

Set Ethernet port loopback type failed.

You tried to use the **set loam 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 the **set loam loopback type** command to set the device's type of loopback support (alternate, noloopback, or remote).
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. Use the **go** command to switch to a different device (e.g., from the Power Supply to the IONMM or an x6210 card).
2. Try entering the **show card info** command.
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. If the problem persists, contact Technical Support.

Please give parameters for L2CP configuration:%s

You tried to perform an L2CP function but have not defined the L2CP parameter(s).

1. Use the `go` command to switch to a device that supports L2CP.
2. Try entering the command again.
3. 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.
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.
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 on page [192](#).
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](#)” on page 195.
3. If a problem persists, contact Technical Support.

Can not 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. Use the `go` command to switch to a device that supports the command.
2. Re-enter the `set ether speed=` command with a speed supported by the card.
3. If the problem persists, contact Technical Support.

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](#)” on page 125.
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 11p=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](#)" on page 83.
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.

Can not set switch mode on this card!

You entered the command to configure the switch mode, but the command does not work on this model.

1. Either use a different (supported) command, or change to another NID card that supports the function.
3. If the problem persists, contact Technical Support.

TDM config is not supported on this card!**TDM inband config is not supported on this card!****TDM peer inband config is not supported on this card!**

You entered a 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 x6210 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 x6210 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](#)” on page 194.
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.

IP management is not 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 x6210. For example:

```
C1|S15|L1D>set dhcp state disable
IP management is not supported on this card!
C1|S15|L1D>
```

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. Try the command on another card that supports the attempted function.
4. 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 x6210 cabling.
2. Make sure IONMM and x6210 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](#)” on page 150 for valid input information.
2. Retry the operation with a valid firmware file name (e.g., *IONMM.bin.1.0.5*, or *x6210.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 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](#)” on page 148 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](#)" on page 40.
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](#)" on page 40.
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](#)” on page 40.
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.

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 is 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 is 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. Continue with the operation.
3. If the problem persists, contact Technical Support.

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](#)” on page 248 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](#)” on page 201.

2. 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 (e.g., Policy/ Rule type drop down on the ACL page).

1. Retry the operation. See the applicable section (e.g., “[Upgrade](#)” section on page [221](#) or page [227](#), or “[Backup and Restore Operations \(Provisioning\)](#)” on page [296](#)).

2. Reboot the NID. See “[Reboot](#)” on page [317](#).

3. 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.

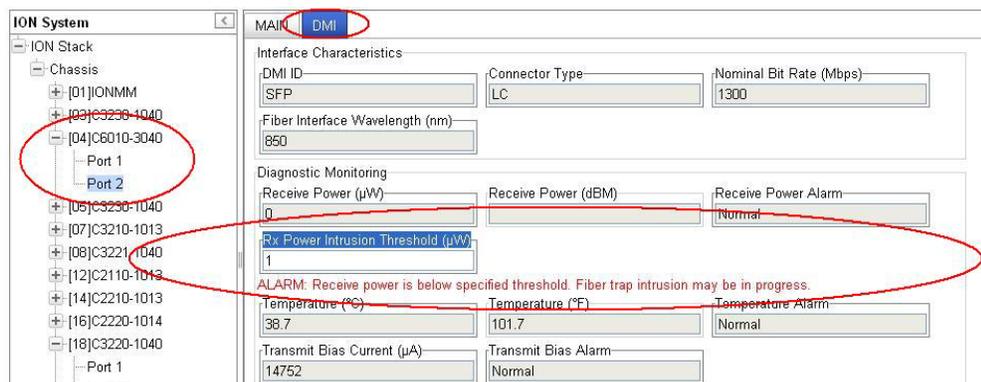
1. Make sure the keyboard’s “Caps Lock” is off.

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.*

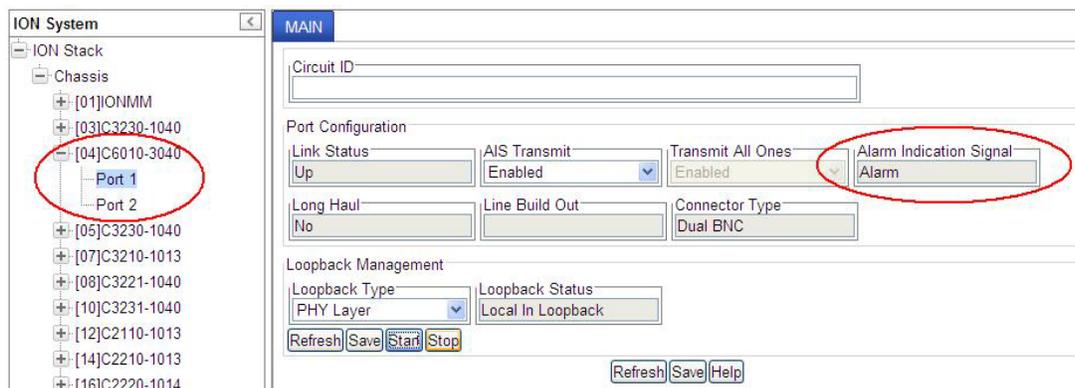


Meaning: At **C6210 > Port 2 > DMI** tab, the Rx Power Intrusion Threshold setting was exceeded. With a preset level for Rx Power on the Fiber port, if the DMI read value falls below this preset value, an intrusion is suspected, and a trap is generated. Fiber optic cables can be vulnerable to tapping, with or without physical intrusion into the optic cable light path.

Either the “Rx Power Intrusion Threshold (μW)” setting is too low, or an optical fiber may have been tapped, which could allow the data stream to be intercepted.

Recovery:

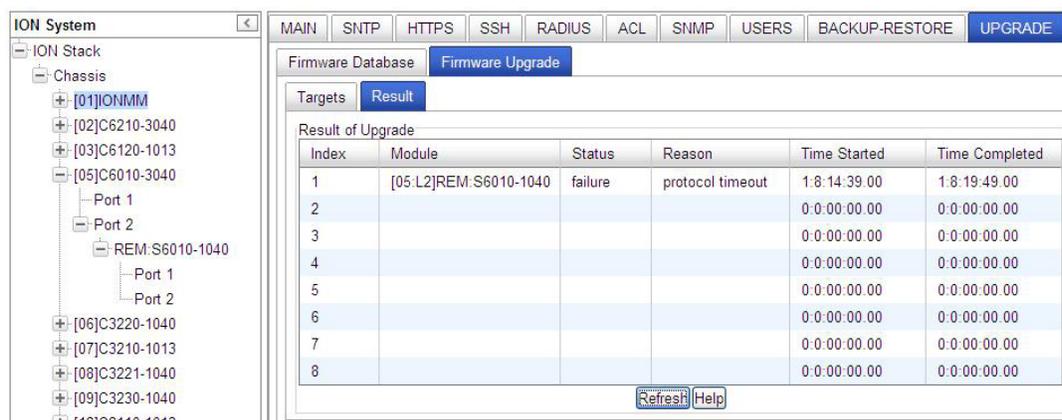
1. Make sure that an intrusion did not cause the alarm; check with your organization’s security staff.
2. Change the Rx Power Intrusion Threshold setting to a higher value:
 - a. From the x6210 Web interface, at **x6210 > Port x (SFP) > DMI** tab, enter a lower threshold setting and click **Save** and then click **Refresh**.
 - b. From the x6210 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](#)” on page 450.
3. From the CLI, enter the command **reset all ports counters** and press the **Enter** key.
4. If the problem persists, contact Technical Support.

Message: *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 \(Alarm Indication Signal\)](#)” on page 13.
5. See “[Alarm Indication Signal – Alarm Condition](#)” on page 233.
6. If the problem persists, contact Technical Support.

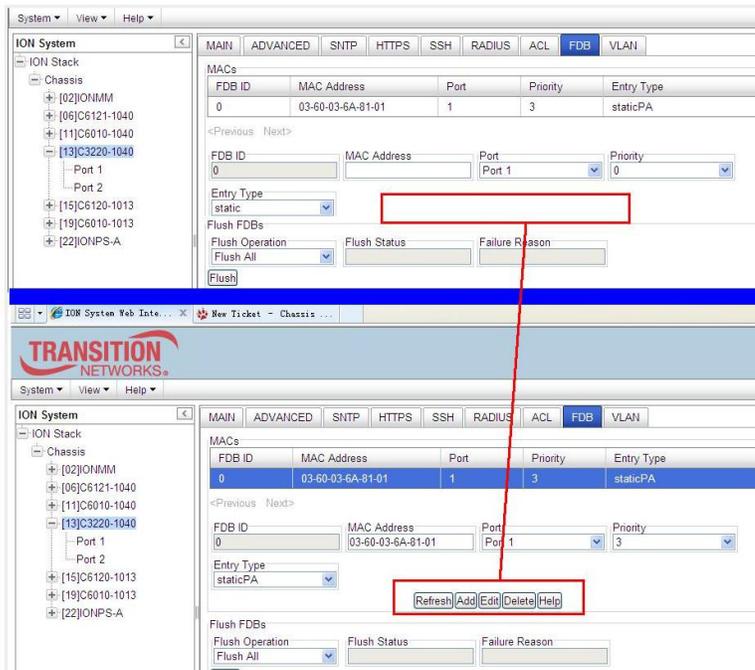
Message: *Remote S6210 Upgrade failure - protocol timeout*

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, C6210, and S6210 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 do not display.



1. 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.

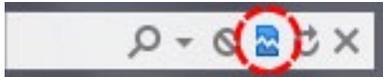


2. Log in to the ION system again.
3. Select the **FDB** tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
4. Click one existing MAC address in the MAC address list.

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 on page 266.
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 occurred. Do you wish to Debug?

Done, but with errors on page.

The screenshot shows a network management interface for 'S3240 System'. The 'FDB' tab is active, displaying a table of MAC addresses. Below the table are input fields for adding a new entry. A Windows Internet Explorer error dialog box is overlaid on the interface, displaying a warning icon and the following text:

Windows Internet Explorer
 Stop running this script?
 A script on this page is causing Internet Explorer to run slowly.
 If it continues to run, your computer might become unresponsive.
 Yes No

VLAN ID	MAC Address	Port	Priority	Entry Type
1	00-04-75-BD-4F-8C	5	7	staticPA
1	00-04-75-BD-9C-36	1	0	dynamic
1	00-04-75-BD-9C-38	1	0	static

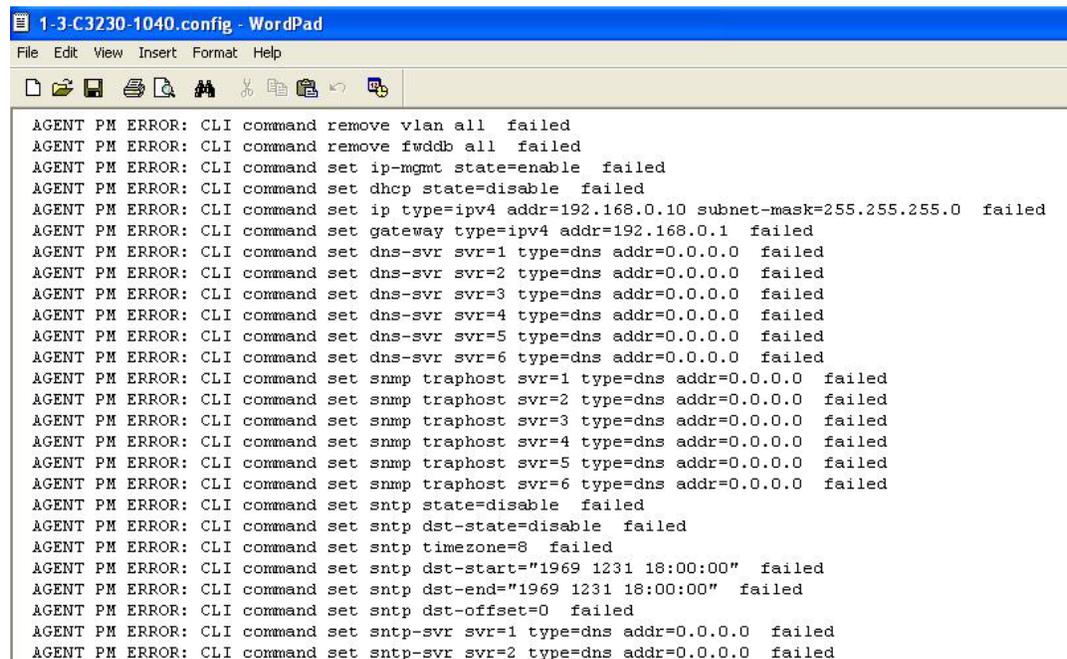
Below the table, there are input fields for VLAN ID (1), MAC Address, Port (Port 1), and Priority. The Entry Type is set to static. Buttons for Refresh, Add, Edit, Delete, and Help are visible.

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-C6210-1013.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.



```

1-3-C3230-1040.config - WordPad
File Edit View Insert Format Help
AGENT PM ERROR: CLI command remove vlan all failed
AGENT PM ERROR: CLI command remove fwddb all failed
AGENT PM ERROR: CLI command set ip-mgmt state=enable failed
AGENT PM ERROR: CLI command set dhcp state=disable failed
AGENT PM ERROR: CLI command set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed
AGENT PM ERROR: CLI command set gateway type=ipv4 addr=192.168.0.1 failed
AGENT PM ERROR: CLI command set dns-svr svr=1 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=2 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=3 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=4 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=5 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=6 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=1 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=2 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=3 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=4 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=5 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=6 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp state=disable failed
AGENT PM ERROR: CLI command set snmp dst-state=disable failed
AGENT PM ERROR: CLI command set snmp timezone=8 failed
AGENT PM ERROR: CLI command set snmp dst-start="1969 1231 18:00:00" failed
AGENT PM ERROR: CLI command set snmp dst-end="1969 1231 18:00:00" failed
AGENT PM ERROR: CLI command set snmp dst-offset=0 failed
AGENT PM ERROR: CLI command set snmp-svr svr=1 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp-svr svr=2 type=dns addr=0.0.0.0 failed

```

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-C6210-1040_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](#)” on page 124. 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](#)” on page 124.. 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” on page 124.. 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](#)” on page 124.. 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](#)” on page 124.. 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](#)” on page 124.. 4. If the problem persists, contact Technical Support.

Message: set snmp 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](#)” on page 124.. 4. If the problem persists, contact Technical Support.

Message: set snmp 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](#)” on page 124.. 4. If the problem persists, contact Technical Support.

Message: set snmp 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](#)” on page 124.. 4. If the problem persists, contact Technical Support.

Message: set snmp 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](#)” on page 124.. 4. If the problem persists, contact Technical Support.

Message: set snmp 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](#)" on page 124.. 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](#)" on page 124.. 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](#)" on page 124. 4. If the problem persists, contact Technical Support.

Message: AGENT PM ERROR: CLI command set rfd state=configuration. failed

Response:

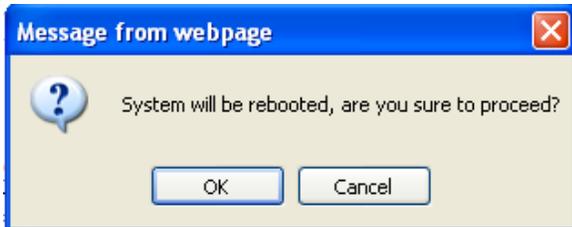
1. Make sure the RFD (Remote Fault Detect) is enabled.
2. Retry the operation.
3. Verify the procedure in "[Configuring Selective and Transparent Link Pass Through](#)" on page 204.
4. Restart the system.
5. If the problem persists, contact Technical Support.

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.

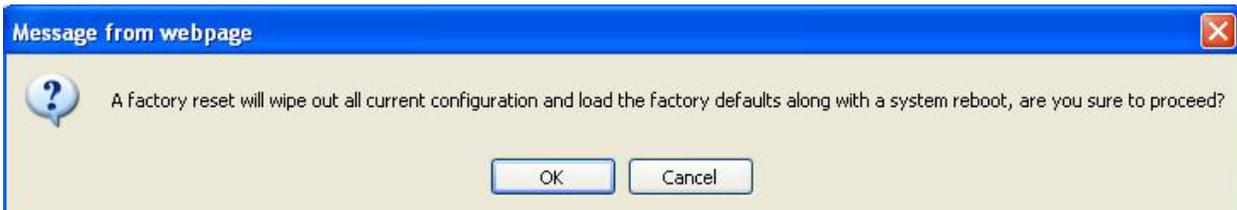
See [Menu System Notes](#) on page 79 for more information.

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 on page 205.

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 on page 215.
10. If the problem persists, contact Technical Support.

Message: Failed to Transfer the Firmware Database File!

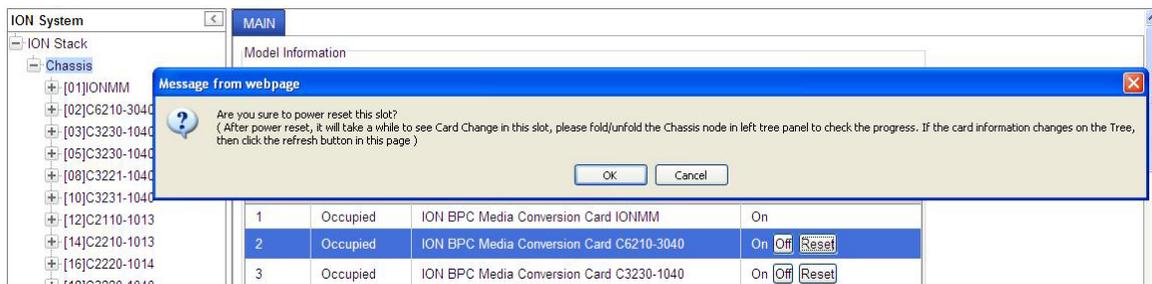


Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the [Upgrade the IONMM Firmware](#) section on page 205.

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 on page 415.
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.)*

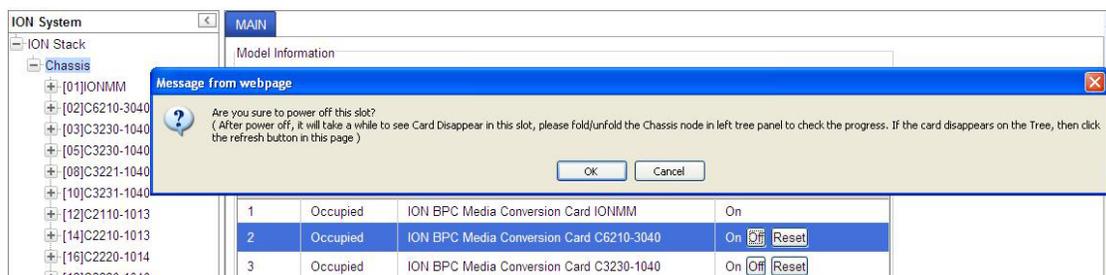


Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Reset** button for a particular slot.

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 on page 77.
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.)*

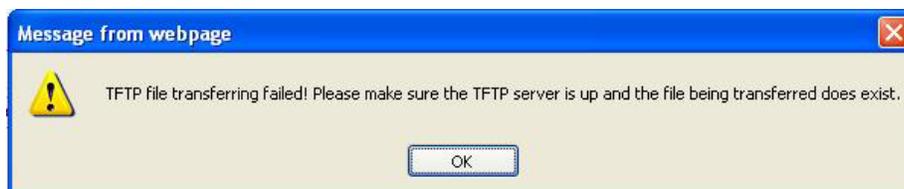


Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Off** button for a particular slot.

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 on page 77.
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 on page 218.

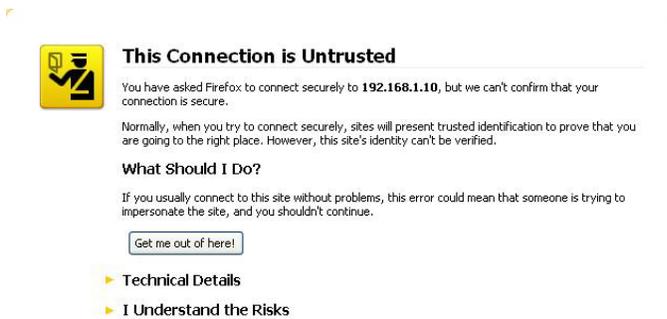
- Recovery:**
1. Start the TFTP Server and verify the name and location of the file to be transferred. If the file does not exist (e.g., at `C:\TFTP-Root`), then download the file from the Lantronix website.
 2. If the problem persists, contact Technical Support.

Message: *The Connection was Reset*

Meaning: The FireFox web browser connection failed to load the page.

Recovery:

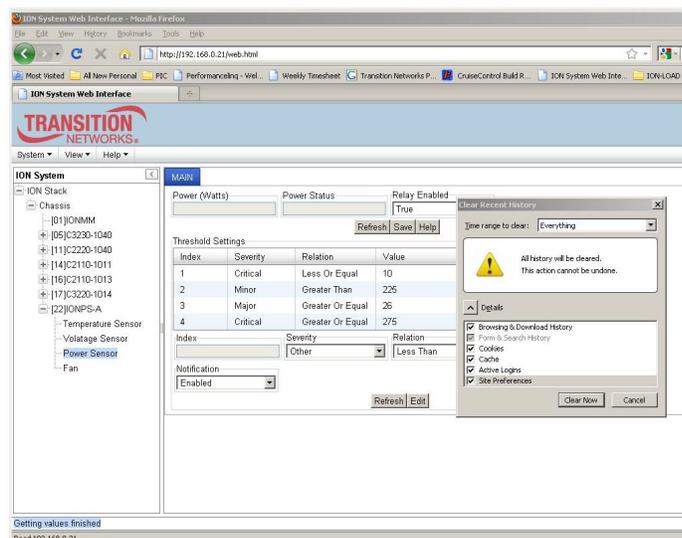
1. Verify the URL (e.g., *http://* versus *https://*).
2. Check if the applicable server is running (TFTP, Syslog, HTTPS server) in the expected location.
3. Click the **Try again** button to retry the operation.
4. If the problem persists, contact Technical Support.

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.

2. 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:

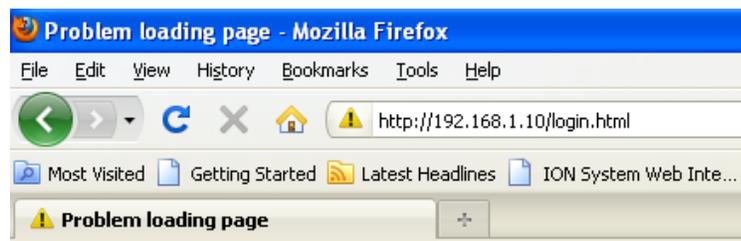
1. Click **Cancel** / Click **Clear Now** to clear the error dialog.
2. Make sure the latest firmware is running. See “[Upgrade the IONMM and/or NID Firmware](#)” on [page 210](#). Upgrade the firmware version if needed.
3. Expand and contract the ION Stack.
4. Retry the operation.
5. If the problem 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:

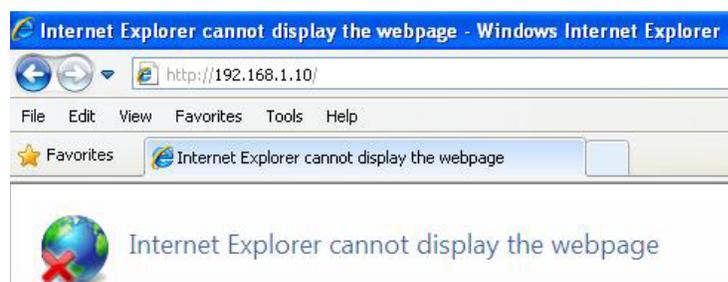
1. If you pressed the **RESET** button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM’s **USB-DEVICE** connector, or plug the USB cable back into the NID’s **USB** connector.
3. Try the operation again.
4. If the problem persists, contact Technical 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](#)” on page 72.
2. Verify the URL entered.
3. Verify NID access. See “[Accessing the NIDs](#)” on page 60.
4. Verify the URL (e.g., http:// versus https://).
5. Try to log in to the ION system again.
6. 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:

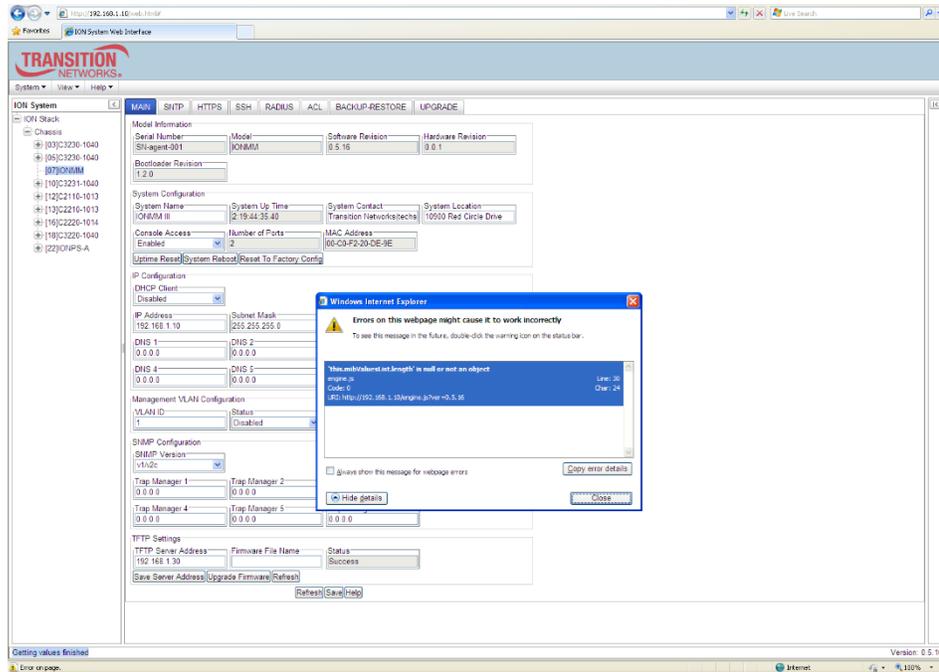
1. Make sure the web browser / version you are using is supported. See “[Web Browsers Supported](#)” on page 72.
2. Verify the URL entered (e.g., http:// versus https://).
3. Verify NID access. See “[Accessing the NIDs](#)” on page 60.
4. Try to log in to the ION system again.
5. If the problem persists, 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 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 **Ctrl-C** keyboard command)
4. Paste the error details text (use **Ctrl-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.*



This webpage is not available.

The webpage at **http://192.168.1.10/** might be temporarily down or it may have moved permanently to a new web address.

[+ More information on this error](#)

Meaning: You tried to display the ION system web interface in Google Chrome, but could not access the webpage.

Recovery:

1. Make sure the web browser / version you are using is supported. See “[Web Browsers Supported](#)” on page [72](#).
2. Verify the URL entered (e.g., http:// versus https://).
3. Verify NID access. See “[Accessing the NIDs](#)” on page [60](#).
4. Click on “[More information on this error.](#)”
5. Make sure HTTPS, SSH, and/or RADIUS server 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.

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:

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 7036 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 the x6210 DMI functions, debug function, PCB configurables, and related tests.

DMI (Diagnostic Maintenance Interface)

The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. **Note:** only certain NID / SFP models support DMI. Lantronix SFPs 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 x6210 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

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 preset-power-level=10`.
4. Display the DMI information. Type: `show dmi info` and press **Enter**. For example:

```
AgentIII C1|S3|L1P2>set dmi rx-power-preset-level 10
AgentIII C1|S3|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:                   41.1*C
DMI temperature:                   106.0*F
DMI temperature alarm:             normal
DMI transmit bias current:         4720*uA
DMI transmit bais alarm:           normal
DMI Transmit power:                255*uW
DMI Transmit power:                -5.935*dBM
DMI Transmit power alarm:          normal
DMI Receive power:                 0*uW
DMI Receive power alarm:           normal
DMI Receive power intrusion threshold: 10*uW
AgentIII C1|S3|L1P2>
```

The DMI tab parameters are described in Table 15 later in this section.

DMI Config – Web Method

1. Access the x6210 through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired device and port.
3. Select the **DMI** tab.

The screenshot shows the ION System web interface. On the left, a tree view under 'ION Stack' shows a hierarchy: Chassis > [01]IONMM > [02]C6210-3040 > Port 2. The 'DMI' tab is selected in the top navigation bar. The main content area displays configuration fields for the selected port:

- Interface Characteristics:** DMI ID (SFP), Connector Type (LC), Nominal Bit Rate (Mbps) (1300), Fiber Interface Wavelength (nm) (850).
- Diagnostic Monitoring:** Receive Power (μW) (130), Receive Power (dBm) (-8.861), Receive Power Alarm (Normal), Rx Power Intrusion Threshold (μW) (999). An alarm message is displayed: "ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress".
- Temperature:** Temperature (°C) (40.1), Temperature (°F) (104.2), Temperature Alarm (Normal).
- Transmit Bias Current:** Transmit Bias Current (μA) (4720), Transmit Bias Alarm (Normal).
- Transmit Power:** Transmit Power (μW) (252), Transmit Power (dBm) (-5.986), Transmit Power Alarm (Normal).
- Supported Media Length:** 9/125u Singlemode Fiber (m) (N/A), 50/125u Multimode Fiber (m) (500), 62.5/125u Multimode Fiber (m) (300), Copper (m) (N/A).

At the bottom of the interface, there are three buttons: Refresh, Save, and Help.

The Interface Characteristics, Diagnostic Monitoring, and Supported Media Length information fields display. See the table below for parameter descriptions.

4. Set the “**Rx Power Intrusion Threshold**” as required. This is a specified level for Receive Power on the Fiber port; if the DMI read value falls below the specified value, a potential intrusion is detected, and a trap is generated. The valid range is 0 - 65535 μW. The default is 0 uW (microwatts).

If the DMI read value falls below the preset value, the message “*ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*” displays to indicate that a potential intrusion is detected.

5. Click the **Save** button to save any updated information.
6. Click the **Refresh** button to update the information displayed.

The **DMI** tab parameters are described in the table below.

Table 15: DMI Parameters

Parameter	Possible Values	Description
DMI ID	Unknown, GBIC, SFP/SFP+/SFP28, 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, RJ-45, ST, 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).
Receive Power (uW)	(measured power measurement)	Receive power on local fiber measured in microwatts (the sample screen above shows 240 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 -6.198 dBm.
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 μ W	A preset 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 μ W. The default is 0. Displays the message " <i>ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.</i> " 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 46.1°C.

Temperature (°F)	(measured temp.)	Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). The sample screen above shows 115.2 °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 <i>ionDMITemperatureEvt</i> 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)	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.
Supported Media Length	50/125u Multimode Fiber (m)	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.
Supported Media Length	62.5/125u MM Fiber (m)	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.
Supported Media Length	Copper (m)	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.

Table 16: Connector Types

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

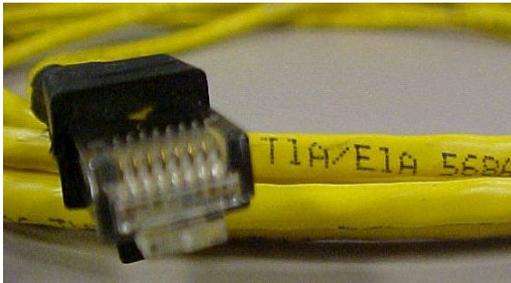


MT-RJ



VF-45

A TIA-EIA 568A CAT 5 cable is shown below.



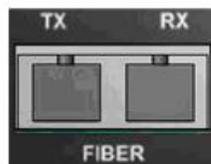
T3/E3 Cable Connectors

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.



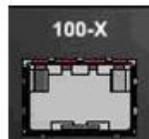
T1 / E1 RJ-45 connector (UTP)

UTP / STP RJ45 copper media connection for shielded twisted pair (STP) or unshielded twisted pair (UTP) media connection.

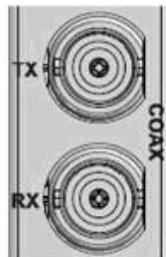


T1 / E1 SFP connector (Fiber)

FIBER TX / RX: ST, SC or open SFP for fiber media connection.



100-X PORT 2; open SFP for fiber media connection.



E1 BNC connector (75-ohm coax)

COAX TX RX: PORT 1; Two BNC connectors: Coaxial cable ports for Coax Tx and Rx connections.

Coax is only supported on models with SFP.

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](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
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:

```
AgentIII C1|S3|L1D>set dbg level ?  
<0-2>  
AgentIII C1|S3|L1D>set dbg level 1  
AgentIII C1|S3|L1D>set dbg level 2  
AgentIII C1|S3|L1D>set dbg level 3  
% Parameter value is out of range.  
AgentIII C1|S3|L1D>set dbg level 0  
AgentIII C1|S3|L1D>
```

DIP Switches and Jumper Settings

The x6210 NID has on-board components that can be used to configure device operation, typically at the direction of the 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 x6210 for varying network conditions. Use a small flat blade screwdriver or similar tool to change DIP switch settings for on-site configuration.

PCB Identification

This section covers the following PCBs (printed circuit boards):

1. **C6210** SIC - PCB 11355 Rev. 04 (this information is silkscreened at the top center of the PCB).
2. **S6210** NID - PCB 11355 Rev. 04 (this information is silkscreened at the top center of the PCB).
3. **C6210** NID - PCB 11393 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 the technical support specialist.

x6210 NID

PCB: 11355 Rev. 04 (information is silkscreened at the top center of the PCB).

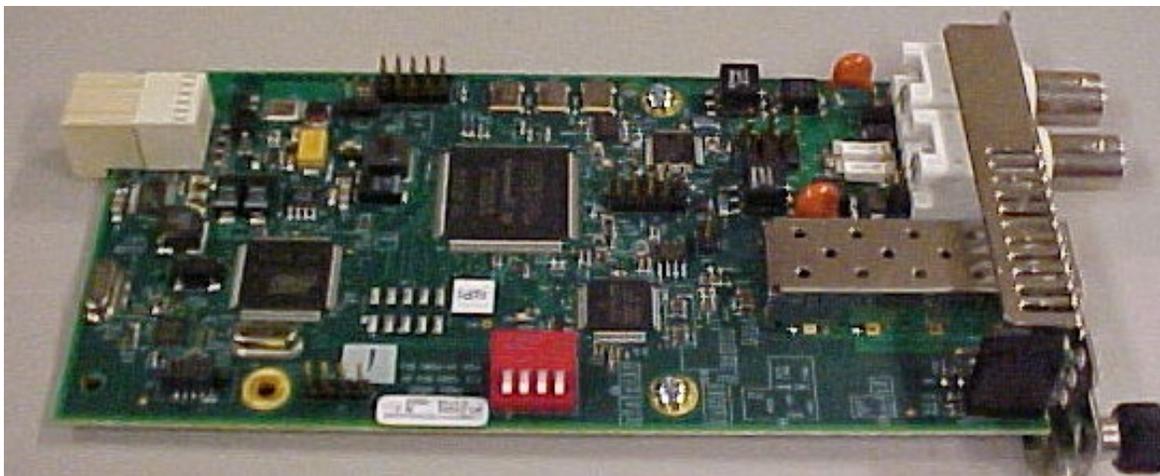
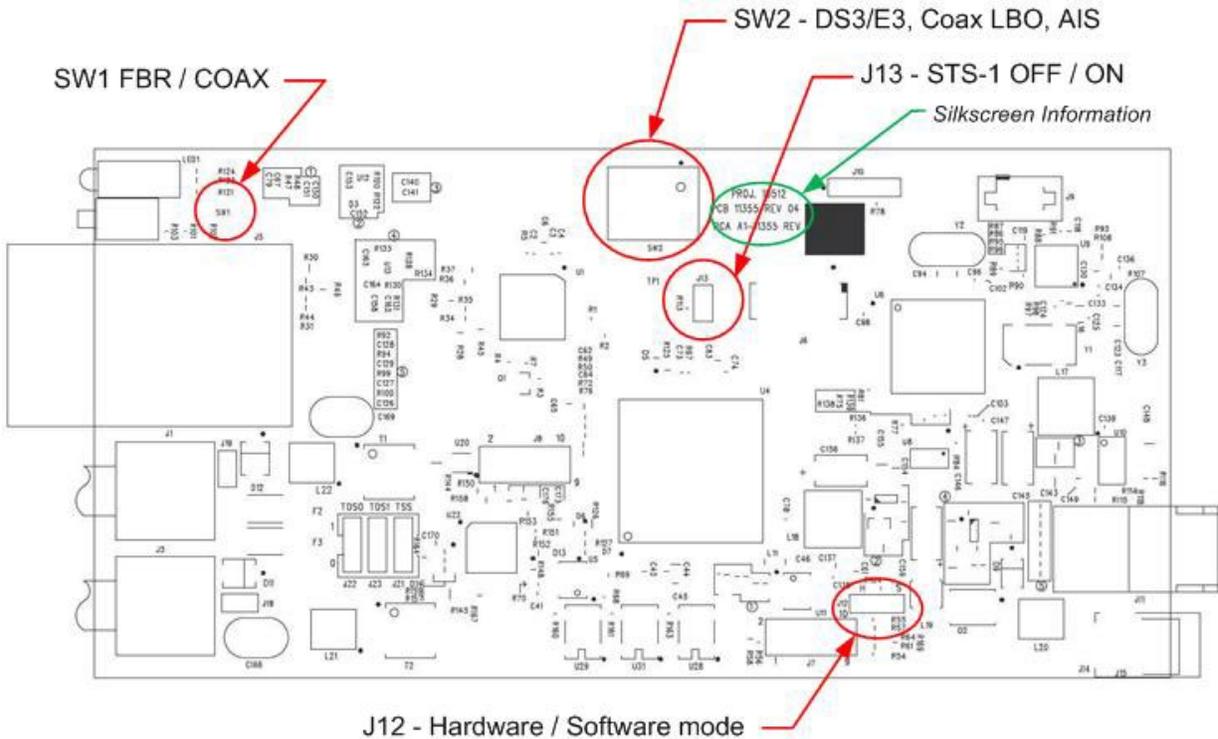


Figure 22: x6210 PCB Layout

The x6210 DIP switches and jumpers are shown below.



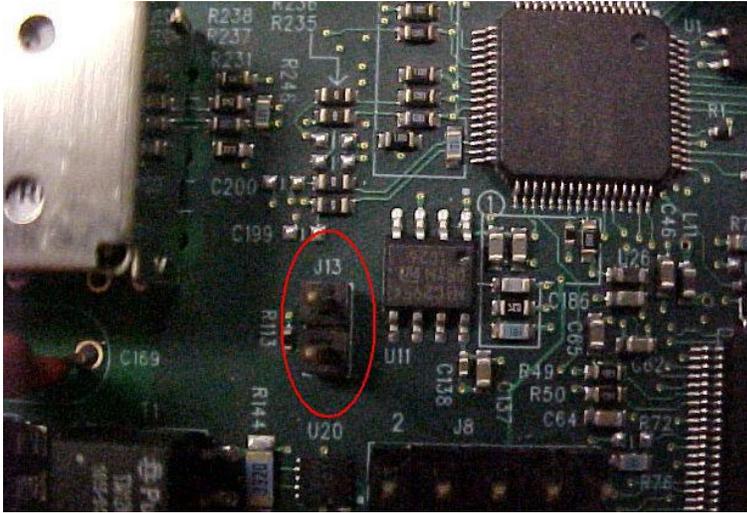
The configurable on-board components (J12, J13, SW1 and SW2) are described in the following sections.

J12 (Hardware / Software Mode)

<u>Jumper Pin #s</u>	<u>Sets Mode to</u>	<u>Note</u>
1-2	Hardware mode	Places the x6210 in Hardware operating mode; the <u>hardware</u> can configure the x6210.
2-3	Software mode	Places the x6210 in Hardware operating mode; the <u>software</u> can configure the x6210 (default setting).

J13 (DS3/STS-1 Mode)

Jumper J13 is used with DIP Switch SW2 to define the x6210 operating mode.

**Jumper Pin #s**

1-2 (in)

none (out)

Sets Mode to

STS-1 mode off

STS-1 mode on

Note

places the x6210 in DS3 mode.

places the x6210 in STS-1 mode (the default setting).

SW1 (CL - Normal - FL)

Each x6210 port lets you configure, start, and stop a PHY Layer local loopback test and display the status. Note that you can run just one port's loopback test at a time. With the x6210 in Hardware mode, set the x6210 front panel CL – FL switch to the CL (Copper Loopback mode) position to start and stop the loopback test.

With the x6210 in Software mode, the front panel CL- FL switch position is ignored. Jumper J12 sets the x6210 operating mode to either Hardware or Software configuration control mode. The default setting is Software operating mode (J12 pins 2 and 3 jumpered).

CL / FL Switch SW1 - Loopback test mode:

SW1 Position	Sets Mode to	Note
UP	FL - Fiber loopback mode	Places the S6210 in Fiber loopback test mode.
*Center	* Normal operating mode	Default setting* - Normal (non-loopback test) mode.
DOWN	CL - Coax loopback mode	Places the S6210 in Coax loopback test mode.



CL / FL Switch SW1 - Loopback test mode:

SW1 Position	Sets Mode to	Note
Left	CL = Coax loopback mode.	Places the C6210 in Coax loopback test mode.
Right	FL = Fiber loopback mode.	Places the C6210 in Fiber loopback test mode.
*Center	* Normal operating mode	Default setting* - Normal (non-loopback test) mode.



SW2 – DS3/E3, Coax LBO, AIS Xmit, and AIS Format

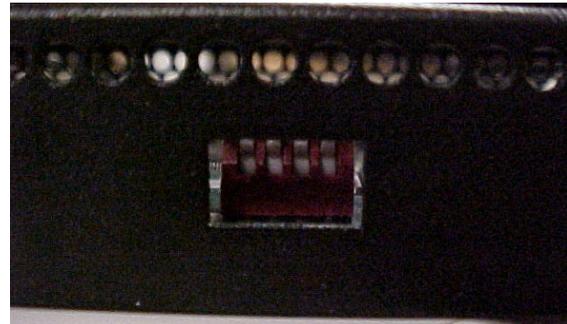
DIP Switch SW2 is used with Jumper J13 to define the x6210 operating mode.

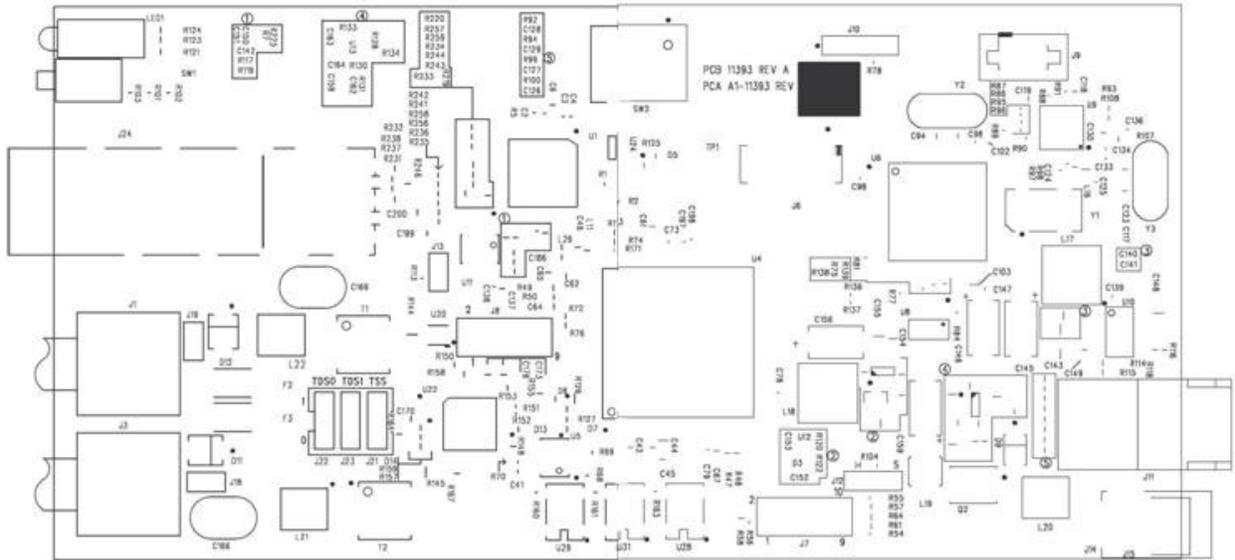
SW2

Switch #	Position	Sets Mode to	Note
1	Up (OPEN)	DS3 (or STS-1) mode	** default setting = Up position (OPEN)
1	Down	E3 mode	
2	Up (OPEN)	Coax LBO, less than 255 ft. cable	** default setting = Up position (OPEN)
2	Down	Coax LBO, greater than 255 ft. cable	
3	Up (OPEN)	AIS transmit On	** default setting = Up position (OPEN)
3	Down	AIS transmit Off	
4	AIS is defined as Blue/AIS All 1's (unframed):		
4	Up (OPEN)	AIS blue (pattern of alternating 1s and 0s)	** default setting = Up position (OPEN)
4	Down	AIS all ones (pattern of all 1s) (unframed)	

* Both the local C6210 and the remote S6210 must have the same DS3/E3 mode setting.

**The SW2 default is all 4 switches in the Up (OPEN) position.



C6210 NID - PCB 11393 Rev A

Minor differences from PCB 11355 Rev. 04: See the previous section for DIP switch and Jumper information.

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.

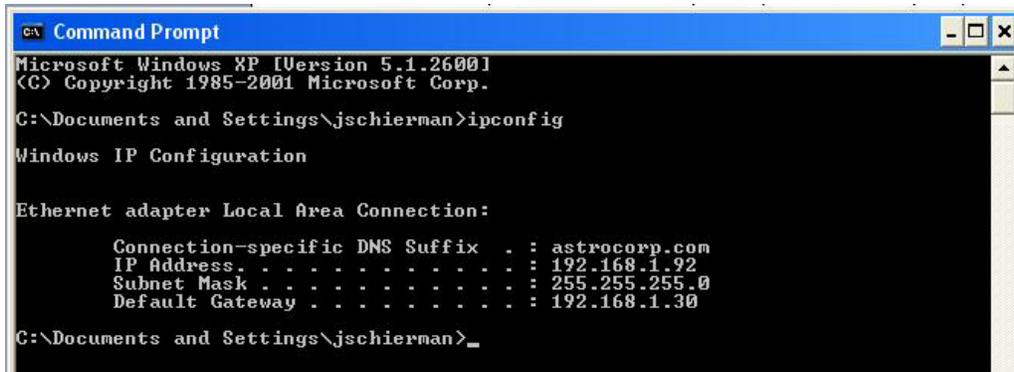
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway 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:



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\jschierman>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : astrocorp.com
    IP Address. . . . .               : 192.168.1.92
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.30

C:\Documents and Settings\jschierman>
```

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 **wipcfg** command, which is available in Windows ME, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the **wipcfg** 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.

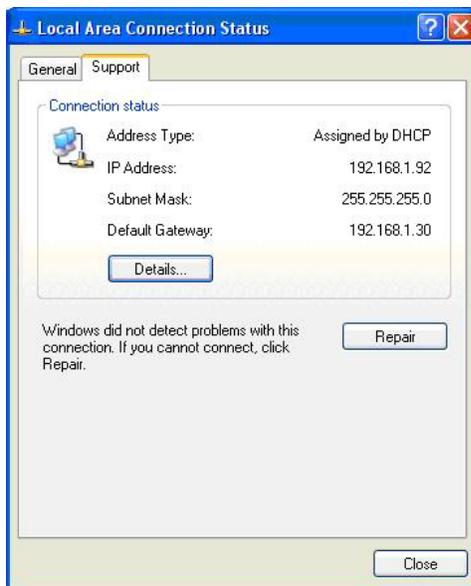
Windows Network Connections

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.

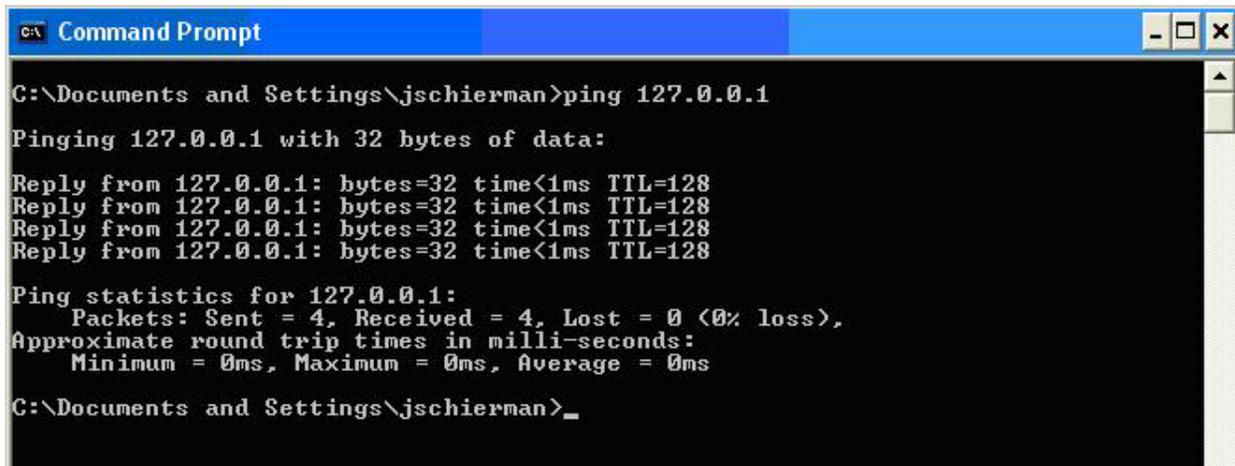


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

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**.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt" and the address bar shows "C:\Documents and Settings\jschierman". The command prompt displays the following text:

```
C:\Documents and Settings\jschierman>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\jschierman>_
```

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.
4. After Telnet Client is installed, open it by following the steps below.
5. Clicking the **Start** button, type **Telnet** in the Search box, and then click **OK**.
6. 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](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.

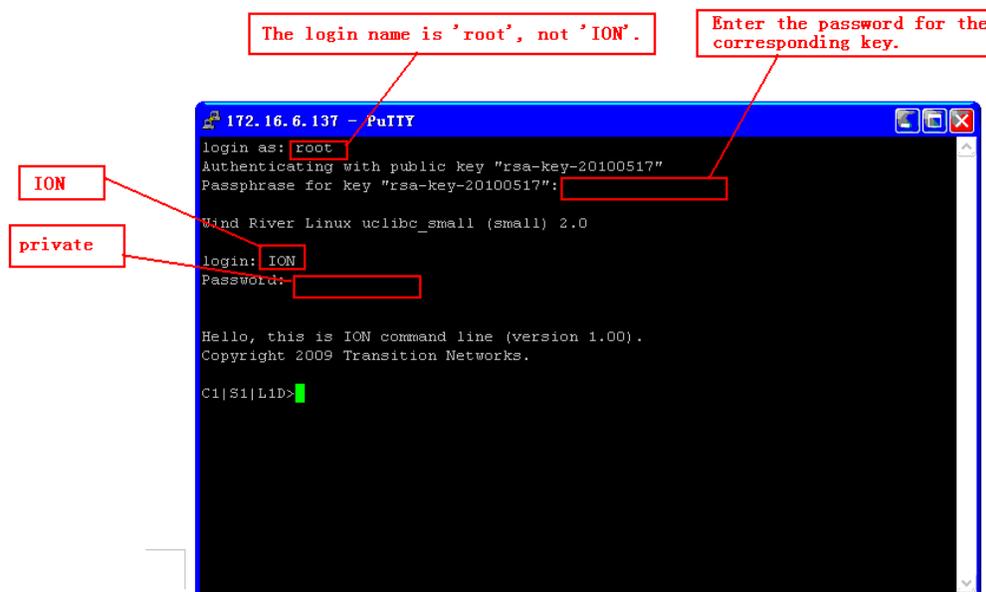
The PuTTY SSH and telnet client was developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is developed and supported by a group of volunteers. PuTTY has been ported to various other operating systems. Official versions exist for some Unix-like platforms, with 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.

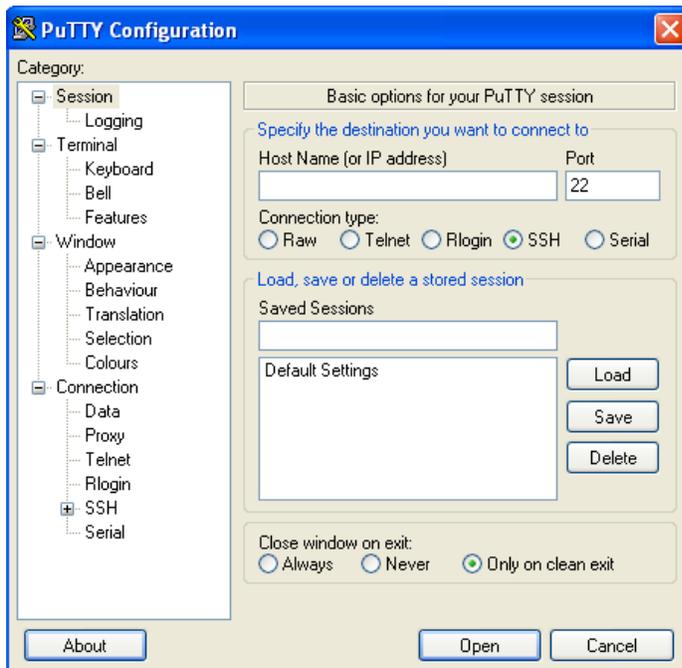
For PuTTY legal and technical details, see the PuTTY download page at <http://putty.org/> or at <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

Note:

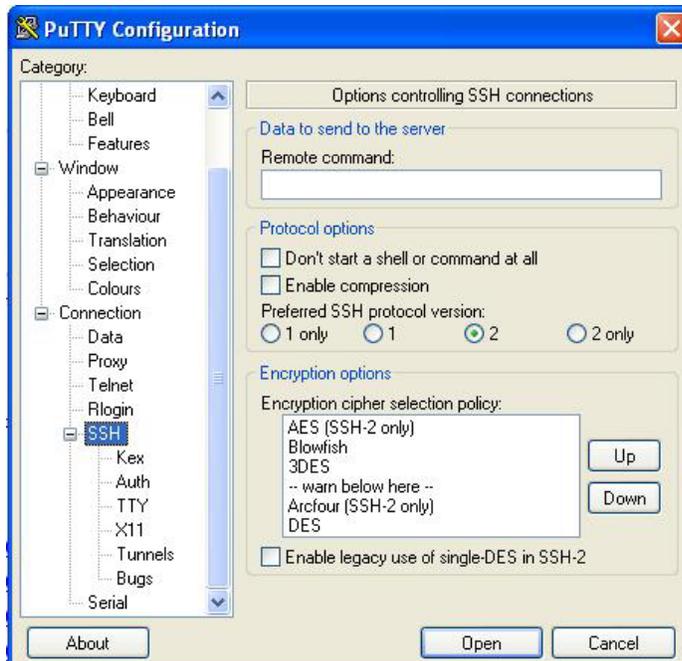
- 1) When the user-public key is loaded into the IONMM successfully, the key will take effect immediately; you do not need to restart the SSH server.
- 2) The ION system supports SSH2 keys only; SSH1 keys are not supported. When generating using puttyGen.exe, do not select the SSH1 keys.
- 3) The ION system currently supports one user named 'root' with public key authentication.



PuTTY Basic Options:



PuTTY SSH Options:



Tracert (Traceroute)

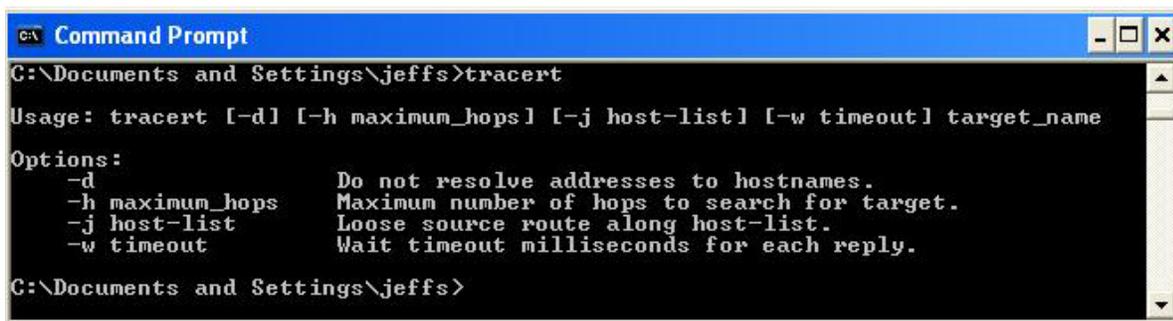
Traceroute is a computer network tool used to determine the route taken by packets across an IP network. "Tracert" (pronounced "traceroute") sends a test network message from a computer to a designated remote host and tracks the path taken by that message.

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.



```
Command Prompt
C:\Documents and Settings\jeffs>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
  -d          Do not resolve addresses to hostnames.
  -h maximum_hops  Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list.
  -w timeout    Wait timeout milliseconds for each reply.

C:\Documents and Settings\jeffs>
```

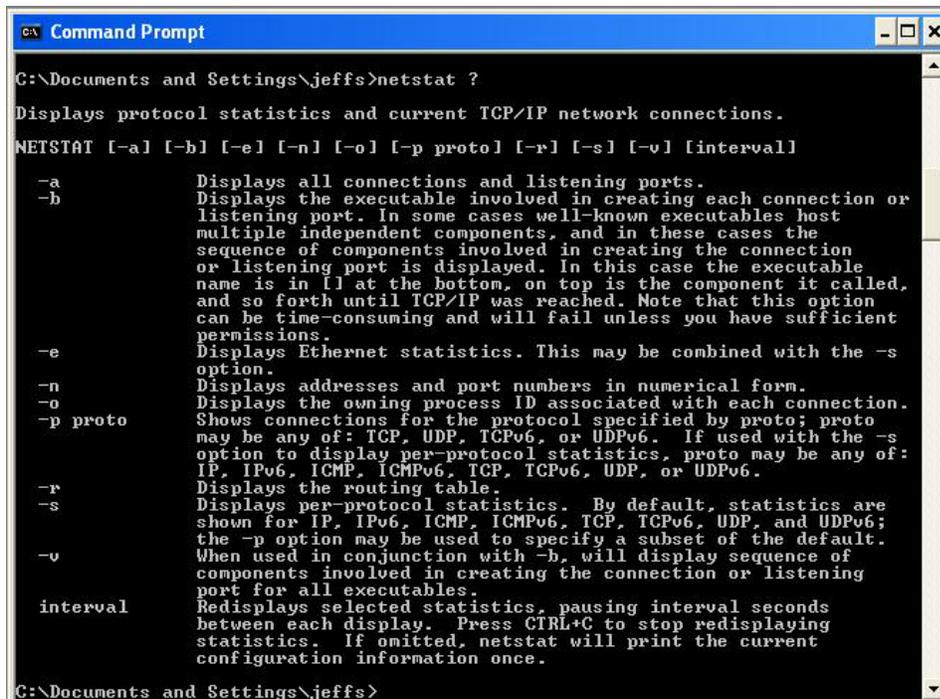
Tracert options include:

- ? 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.



```

C:\Documents and Settings\jeffs>netstat ?
Displays protocol statistics and current TCP/IP network connections.
NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables host
           multiple independent components, and in these cases the
           sequence of components involved in creating the connection
           or listening port is displayed. In this case the executable
           name is in [] at the bottom, on top is the component it called,
           and so forth until TCP/IP was reached. Note that this option
           can be time-consuming and will fail unless you have sufficient
           permissions.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
           the -p option may be used to specify a subset of the default.
-v          When used in conjunction with -b, will display sequence of
           components involved in creating the connection or listening
           port for all executables.
interval   Redispays selected statistics, pausing interval seconds
           between each display. Press CTRL+C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.

C:\Documents and Settings\jeffs>

```

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:

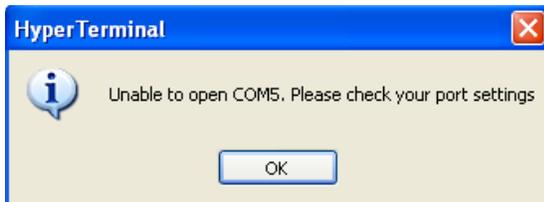
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

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](#)" on page 53.
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.

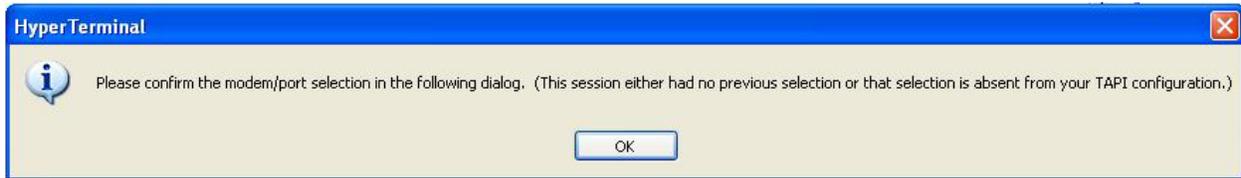
Message: *Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal.*



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](#)" on page 53.
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:

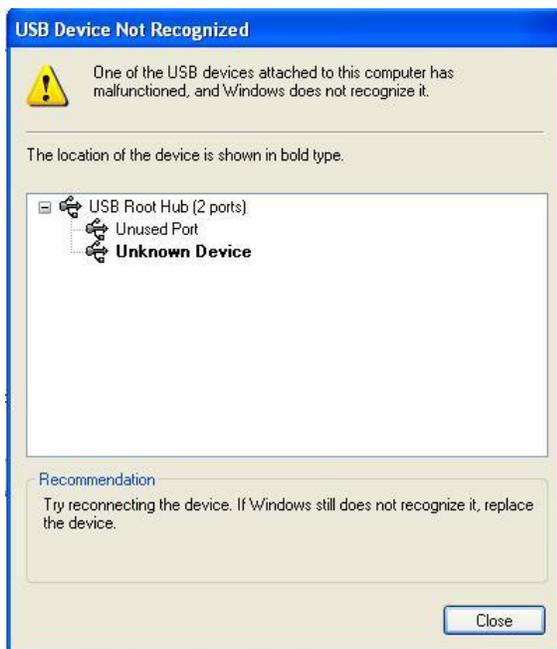
1. Verify the HyperTerminal configuration. See “[Configuring HyperTerminal](#)” on page 65 (e.g., verify your **computer’s Ports (COM & LPT)** setting).
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the x6210.
4. Retry the operation. See “[Start a USB Session in HyperTerminal and Log In](#)” on page 72.
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:**

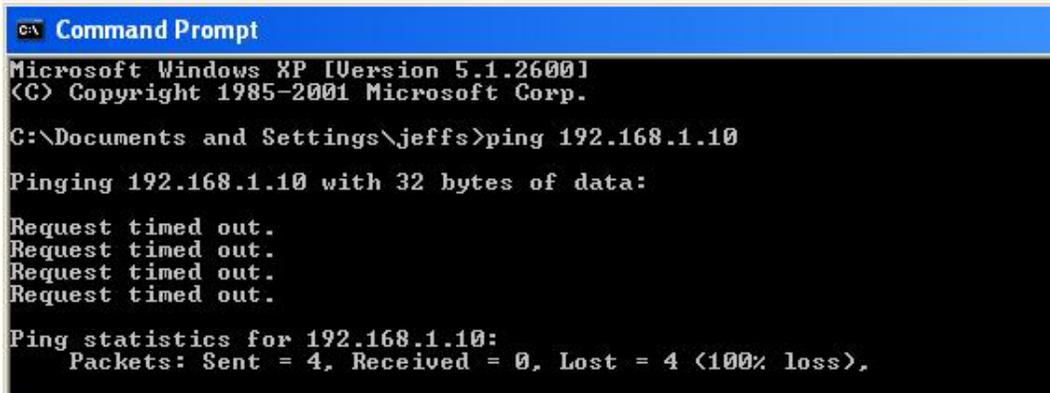
1. Click message icon in the tray. A Windows recommendation dialog displays.



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.*



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jeffs>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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.*



```
C:\ Command Prompt

C:\Documents and Settings\jeffs>telnet 192.168.10.1
Connecting To 192.168.10.1...Could not open connection to the host, on port 23:
Connect failed

C:\Documents and Settings\jeffs>_
```

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.

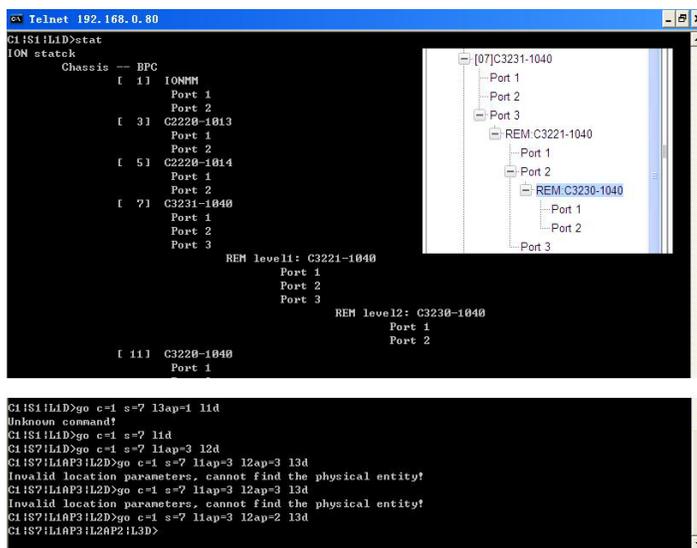
Message: *Invalid location parameters, cannot find the physical entity!*

```
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](#)” on page 125.

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*

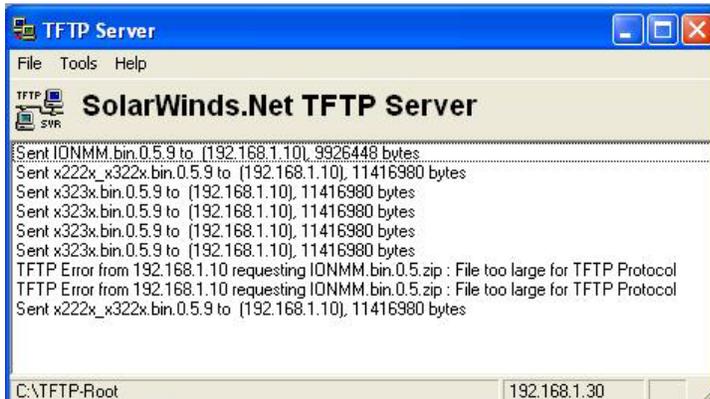


Meaning: A TFTP Server error - the TFTP Server Address that you specified does not contain the Firmware File Name specified.

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 on page [408](#).

DS3-E3 Error Events and Alarm Conditions

These are error events and alarm conditions specific to DS3 and E3 that are generated at the system level. Basic responses include:

1. Check all available logs and reports for related troubleshooting information.
2. Check the x6210 NID connections (see “[Section 2: Installation and System Setup](#)” on page 36) at the near-end and far-end.
3. Check all cable runs for damaged cable, etc.
4. Use the DMI function to make sure the cable runs are within the Supported Media Lengths. See “[DMI \(Diagnostic Maintenance Interface\)](#)” on page 194.
5. Verify proper operation of other network devices.
6. Check the x6210 NID configuration; see “[Section 4: Configuration](#)” on page 72.

The following section lists specific DS3 / E3 Alarm Conditions that can be reported, and the recommended recovery procedures.

Alarm Indication Signal (AIS) indicates an alarm raised on a line upstream from the x6210. To recover:

1. Use the **show** commands to verify that the configuration of the line matches that of the remote end.
2. Check the LBO setting. You may have to reduce the transmit level of the device attached to the x6210 by adjusting its Line Build Out (LBO) configuration setting.
3. Check the x6210 PCB configuration. See “[DIP Switches and Jumper Settings](#)” on page 206.
4. Run the x6210 Loopback Tests for the copper and fiber links.
5. Check the status of the adjacent network devices.
6. Ask your service provider to trace the source of the AIS signal.

Loss of Frame (LOF) condition usually means either 1) the configuration settings on the port are not correct for the line, or 2) the port configuration is correct, but the line is experiencing other errors causing the LOF alarm. To recover:

1. Use the **show** commands to verify that the configuration of the line matches that of the remote end.
2. Ensure that the cable between the interface port and the E3 service provider equipment or remote E3 terminal equipment connects correctly.
3. Ensure that the cable is connected to the correct port. Correct the cable connections as required.
4. Check the 75 ohm coax cable integrity. Look for breaks or other physical abnormalities in the cable. Replace the cable if necessary.
5. Check the x6210 PCB configuration. See “[DIP Switches and Jumper Settings](#)” on page 206.
6. Run the x6210 Loopback Tests for the copper and fiber links.
7. Check with your provider to see if the framing format configured on the port matches the framing format on the line. Try another framing format and see if the alarm clears.
8. Work with your provider to configure a remote loopback on the affected interface.

Recording Model Information and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible in order to help the Lantronix Technical Support Specialist.

2. 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 ais config**, **show tdm port config**, or others as request by the Support Specialist.)

The screenshot shows the ION System configuration interface. On the left is a tree view of the ION Stack, with the [05]C6210-3040 device selected. The main panel is titled 'MAIN' and contains the following sections:

- Model Information:** Serial Number (12345678), Model (C6210-3040), Software Revision (1.2.0), Hardware Revision (0.0.1), and Bootloader Revision (0.1.1).
- System Configuration:** System Name (C6210-3040@Corporate), System Up Time (0:6:50:48.00), Configuration Mode (Software), and Number of Ports (2). It also features buttons for Uptime Reset, System Reboot, and Reset To Factory Config.
- Device Description:** An empty text field.
- TDM Mode:** DS3, Transmit All Ones (Enabled), and AIS Format (Blue).

At the bottom right of the main panel are buttons for Refresh, Save, and Help.

3. Record the **Model Information** for your system.

Serial Number: _____ Model: _____
 Software Revision: _____ Hardware Revision: _____
 Bootloader Revision: _____

4. Record the **System Configuration** information for your system.

System Up Time: _____ Configuration Mode: _____
 Device Description: _____ TDM Mode: _____
 AIS Transmit: _____ AIS Format: _____

5. Provide additional Model and System information to your Technical Support Specialist. See “[Basic ION System Troubleshooting](#)” on page 140.

Your Lantronix service contract number: _____

A description of the failure: _____

A description of any action(s) already taken to resolve the problem (e.g., changing modes, rebooting, etc.):

The serial # and revision # of each involved Lantronix product in the network:

A description of 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 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 numéroté de la classe A est conforme 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 Fall ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention !

Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures 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 öffentliches Telekommunikationsnetz in den EG-Mitgliedstaaten verstößt gegen die jeweiligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Declaration of Conformity

Manufacture's Name: Lantronix, Inc.

Manufacture's Address: 48 Discovery, Suite 250, Irvine, California 92618 USA

Declares that the products:

C6010-30xx, S6010-30xx, C6010-10xx, S6010-10xx

Conform to the following Product Regulations:

FCC Part 15 Class A, EN 55032:2012, EN 55024:2010

Directive 2014/30/EU

Low-Voltage Directive 2014/35/EU

EN 62368-1:2014+A11:2017

2011/65/EU EN 50581:2012

With the technical construction on file at the above address, this product carries the CE Mark

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

Place: Irvine, California

Date: April 27, 2023

Signature: *Eric Bass*

Full Name: Eric Bass

Position: Vice President 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

Note: The default settings shown are as seen in the tabs/fields of the Web interface.

Table 17: Device-Level Factory Defaults

Item/Field	Default Setting
Telnet/USB Login	ION
Telnet/USB/Web Password	private
System Name	x6210 (e.g., C6210-1040)
Device Description	blank
TDM Mode	E3
AIS Transmit	Enabled
AIS Format	All Ones

Table 18: Port-Level Factory Defaults

Item/Field	Default Setting
MAIN Tab	
Circuit ID	blank
Link Status	Up
AIS Transmit	Enabled
Transmit All Ones	Enabled
Alarm Indication Signal	Normal
Long Haul	No
Line Build Out	blank or Normal
Connector Type	Dual BNC (Port 1) ; SFP slot (Port 2)
Loopback Type	No Loopback
Loopback Status	No Loopback
DMI Tab (Port 2 only)	
Rx Power Intrusion Threshold (μ W)	0

Appendix C: Configuration Quick Reference – CLI

Port Loopback Test – Web Method – T1 and E1 Modes

1. Place the x6210 in Hardware mode.
2. Set the x6210 **CL – FL** switch to the **CL** position.
3. Access the x6210 through either a USB connection or a Telnet session.
4. Use the **go** command to switch to Port 1. Type **go c1 sx l1p=1** and press **Enter**.
5. Set the Port 1TDM Loopback type to PHY layer. Type **set tdm loopback type=phylayer** and press **Enter**.
6. Start the Port 1 Loopback operation. Type **set tdm loopback oper=init** and press **Enter**.
7. Stop the Port 1 Loopback operation. Type **set tdm loopback oper=stop** and press **Enter**.
8. Set the x6210 **CL – FL** switch to the **FL** position.
9. Use the **go** command to switch to Port 2.
10. Repeat steps 5-7 for Port 2.

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

SKU	Single / Multi Mode	Single / Dual Fiber	Distance	Wave-length (nm)	Data Rate	Spectral Width Max	Min. TX Power
C6210-3011	Multi	Dual	2 Km	1310	100M	400nm FWHM	-19.0dBm
C6210-3013	Multi	Dual	2 Km	1310	100M	400nm FWHM	-19.0dBm
C6210-3014	Single	Dual	30 Km	1310	100M	3nm FWHM	-15.0dBm
C6210-3015	Single	Dual	50 Km	1310	100M	10nm FWHM	-5.0dBm
C6210-3016	Single	Dual	60 Km	1310	100M	9.5nm FWHM	-4dBm
C6210-3017	Single	Dual	80 Km	1550	100M	9.5nm FWHM	-5dBm
C6210-3029-A1	Single	Single	20 Km	1310 Tx / 1550 Rx	100M	16nm FWHM	-14dBm
C6210-3029-A2	Single	Single	20 Km	1550 Tx / 1310 Rx	100M	10 nm FWHM	-14 dBm
C6210-3029-B1	Single	Single	40 Km	1310 Tx / 1550 Rx	100M	12 nm FWHM	-9 dBm
C6210-3029-B2	Single	Single	40 Km	1550 Tx / 1310 Rx	100M	2 nm FWHM	-8 dBm

*Actual 'Maximum Cable Distance' distances depend on network installation physical characteristics.

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.

DS-3 Cable

Bellcore GR-139-CORE (Generic Requirements for Central Office Coaxial Cable) contains and defines the requirements for coax cable utilized in DS-3 systems. 734A*, 734D*, and 735A* are industry references for coax made for Central Office applications in general, and Digital Signal Cross-connect (DSX) applications in particular. DS-3 coax cables must conform to the requirements of Bellcore GR-139-CORE.

E3 Cable

See the cable supplier's documentation. Refer to the [ANSI standards](#) page. The physical characteristics must meet or exceed ITU specifications.

Appendix E: SNMP MIB Trap Support

This appendix provides information on SNMP traps supported on the IONMM, including when a trap is generated and what information is in each trap.

All ION system critical events are reported via SNMP Traps. The ION system uses only SNMPv2 traps, with the definition of NOTIFICATION-TYPE in the MIB (Management Information Base).

See the “Supported MIBs” section on page 32 for information on support for public (standard) and private MIBs. For information on “Configuring SNMP” see page 234. See the *ION Management Module (IONMM) User Guide* manual for SNMP traps supported on the IONMM.

Traps are generated when a condition has been met on the SNMP agent. These conditions are defined in the Management Information Base (MIB). The administrator then defines thresholds, or limits to the conditions, that are to generate a trap. Conditions range from preset thresholds to a restart.

All of the values that SNMP reports are dynamic. The information needed to get the specified values that SNMP reports is stored in the MIB. This information includes Object IDs (OIDs), Protocol Data Units (PDUs), etc. The MIBs must be located at both the agent and the manager to work effectively.

MIBs List

For SNMP configuration/management function, the ION X6210 will realize these MIBs:

- ionDevSysCfgTable
- ifTable
- ifXTable
- ionDMIIInfoTable
- ionIfLoopbackTable
- ionIfTDMTable (used for ION T1/E1/DS3, including fields such as AIS, LBO, etc.)

All ION system SNMP Trap messages conform to SNMPv2 MIB RFC-2573.

See the “Supported MIBs” section on page 32 for information on the x6210 NIDs support for public (standard) and private MIBs.

For information on “Configuring SNMP” see page 234, see the *ION Management Module (IONMM) User Guide* manual for SNMP traps supported on the IONMM.

A sample SNMP Message sequence is shown below.

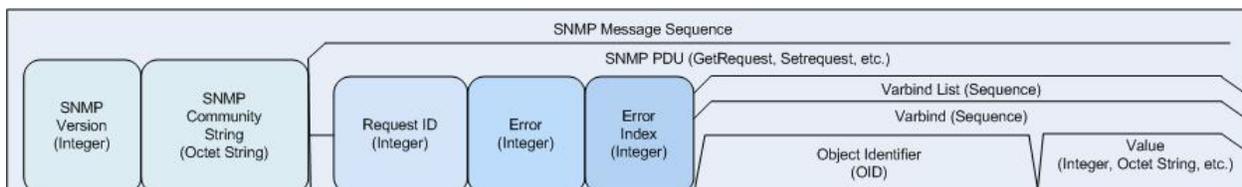


Figure 23: SNMP Message Sequence

MIB Table List / Descriptions

The list of supported MIBs includes:

- ionDevSysCfgTable
- ifTable
- ifXTable
- ionDMIIInfoTable
- ionIfLoopbackTable
- ionIfTDMTable

These MIBs are described in the following sections.

ifTable

This table is partly applicable for TDM card.

Table 19: Supported MIBs

Parameter	Property	Range
ifIndex	Read only	Integer32
ifDescr	Read only	String SIZE (0..255)
ifType	Read only	1~32
ifMtu	Read only	Integer32
ifSpeed	Read only	Gauge (32 bit)
ifPhysAddress	Read only	Octets
ifAdminStatus	Read & Write	Up(1) down(2) testing(3)
ifOperStatus	Read only	up(1), down(2), testing(3), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7)
ifLastChange	Read only	
ifInOctets	Read only	Counter (32 bit)
ifInUcastPkts	Read only	Counter (32 bit)
ifInNUcastPkts	Read only	Counter (32 bit)
ifInDiscards	Read only	Counter (32 bit)
ifInErrors	Read only	Counter (32 bit)
ifInUnknownProtos	Read only	Counter (32 bit)
ifOutOctets	Read only	Counter (32 bit)
ifOutUcastPkts	Read only	Counter (32 bit)
ifOutNUcastPkts	Read only	Counter (32 bit)
ifOutDiscards	Read only	Counter (32 bit)
ifOutErrors	Read only	Counter (32 bit)
ifOutQLen	Read only	Gauge (32 bit)
ifSpecific	Read only	

ionDevSysCfgTable

Parameter	Property	Range
ionDevSysName	Read & Write	SIZE (0..64)
ionDevSysUptime	Read only	
ionDevSysUptimeReset	Read & Write	1: reset(1) 2: doNothing(2)
ionDevSysReset	Read & Write	1: running(1) 2: coldStart(2) 3: warmStart(3)
ionDevNumOfPorts	Read only	2 (ports) for TDM card
ionDevClearCounters	Read & Write	1: perform(1) 2: doNothing(2)
ionDevResetToFactoryConfig	Read & Write	1: perform(1) 2: doNothing(2)
ionDevConfigurationMode	Read only	1: software(1) 2: hardware(2)

ionIfLoopbackTable

Parameter	Property	Range
ionIfLoopbackCapability	Read only	Unused(0) phyLayerLoopbackCapable(1)
ionIfLoopbackInit	Read & Write	phyLayer
ionIfLoopbackStatus	Read & Write	localInLoopback(5) no Loopback(1)
ionIfClearCounters	Read & Write	1: reset(1) 2: doNothing(2)

ionIfTDMAISTrapTable

Parameter	Property	Range
ifIndex	Read only	Integer32
ionIfTDMAAlarmIndicationSignal	Read only	alarm(1), normal(2)

ionDMIInfoTable

Parameter	Property	Range
ionDMIConnectorType	Read only	unknownUnspecified(0), sc(1), fibreChannelStyle1Copper(2), fibreChannelStyle2Copper(3), bncTnc(4), fibreChannelCoaxHeader(5), fiberJack(6), lc(7), mtrj(8), mu(9), sg(10), opticalPigtail(11), hssdcII(32), copperPigtail(33)
ionDMIBitRate	Read only	Integer32
ionDMILenFor9x125umKM	Read only	Integer32
ionDMILenFor9x125um100M	Read only	Integer32
ionDMILenFor50x125um10M	Read only	Integer32
ionDMILenFor625x125um10M	Read only	Integer32
ionDMILenForCopper	Read only	Integer32
ionDMIId	Read only	Integer32
ionDMILaserWavelength	Read only	Integer32
ionDMITemperature	Read only	Integer32
ionDMITempAlarm	Read only	normal(1), notSupported(2), lowWarn(3), highWarn(4), lowAlarm(5), highAlarm(6)
ionDMITxBiasCurrent	Read only	
ionDMITxBiasAlarm	Read only	normal(1), notSupported(2), lowWarn(3), highWarn(4), lowAlarm(5), highAlarm(6)
ionDMITxPowerLevel	Read only	
ionDMITxPowerAlarm	Read only	normal(1), notSupported(2), lowWarn(3), highWarn(4), lowAlarm(5), highAlarm(6)
ionDMIRxPowerLevel	Read only	
ionDMIRxPowerAlarm	Read only	normal(1), notSupported(2), lowWarn(3), highWarn(4), lowAlarm(5), highAlarm(6)
ionDMIRxPwrLvIPreset	Read & Write	Integer32(0 ~ 65535)

ionIfTDMTable

Parameter	Property	Range
ionIfTDMAISTransmit	Read & Write	enabled(1), disabled(2), notApplicable(3)
ionIfTDMAISFormat	Read & Write	allones(1), blue(2), notApplicable(3)
ionIfTDMAAlarmIndicationSignal	Read only	alarm(1), normal(2)
ionIfTDMLongHaul	Read only	yes(1), no(2) –only supported on copper, notApplicable(3)
ionIfTDMType	Read only	Unknown(0), T1(1),E1(2),J1(3), DS3(4),E3(5),STS-1(6)
ionIfTDMT1E1IfLineBuildout	Read only	Unknown(0), e13-0V120ohm(1), e12-37V75ohm(2), t1SH-DSX-0-133ANSIT1403(3), t1SH-DSX-133-266(4), t1SH-DSX-266-399(5), t1SH-DSX-399-533(6), t1SH-DSX-533-655(7), t1SH-DSX-6V(8), t1LH-0dB(9), t1LH-m7-5dB(10), t1LH-m15dB(11), t1LH-m22-5dB(12) – only supported on copper
ionIfTDMDS3E3LineBuildout	Read & Write	Unknown(0),Boost(1), Normal(2)
ionIfTDMConnectorType	Read only	rj-48(10), -- RJ-45, unshielded twisted pair stmm(11), -- ST fiber, multimode stsm(12), -- ST fiber, Singlemode scmm(13), -- SC fiber, multimode scsm(14), -- SC fiber, Singlemode scsmlh(15), -- SC fiber, singlemode, long haul scsmelh(16), -- SC fiber, singlemode, extra long haul scsmlhlw(17), -- SC fiber, long haul, long wavelength mtrjmm(18), -- MT-RJ multimode fiber lc(19), -- LC fiber, singlemode bnc(20), -- BNC coax stsmhl(21), -- ST Singlemode Long Haul stsmelh(22), -- ST Singlemode Extra Long Haul scmm1300(23), -- SC Multimode 1300nm stmm1300(24), -- ST Multimode 1300nm mtrjmm(25), -- MTRJ singlemode fiber serial26(26), -- Universal 26-pin Serial Interface Connector stmmhl(27), -- ST Multimode Long Haul scsmsh(28), -- SC Singlemode Short Haul scsimplex(29), -- SC Simplex bncdual(30), -- Dual BNC coax connectors db9rsxxx(31), -- DB9 for RS232 and RS485 termblock(32),

		<ul style="list-style-type: none">-- Terminal Block for RS485 rj11(33),-- RJ-11, unshielded twisted pair sc40km(34),-- SC fiber, 1550nm 40km din6(38),-- DIN 6-Pin for RS232 lcmm(39),-- LC Multimode Fiber sfp(40),-- SFP Small Form Factor Pluggable sfmmlh(42),-- Single-Fiber Multimode scmmlh(43),-- SC Multimode (long haul)lcmmlh(44)-- LC Singlemode (long haul)
--	--	--

MIB Traps Summary

The x6210 Trap MIBs include:

IF-MIB:

linkDown

linkup

TN-ION-MGMT-MIB.smi :

ionDMIRxIntrusionEvt

ionDMIRxPowerEvt

ionDMITxPowerEvt

ionDMITxBiasEvt

ionDMITemperatureEvt

ionTDMAISEvt (new)

The ION system MIB Traps are summarized in the table below in terms of related MIBs and varbinds.

Table 20: MIB Traps Summary

MIB (linked to section)	Trap (linked to section)	VarBinds
ionDevSysCfgTable	<u>linkDown</u>	
	<u>linkup</u>	
ifTable		
ifXTable		
ionDMInfoTable		
ionIfLoopbackTable		
ionIfTDMTable		
TN-ION-MGMT-MIB.smi	<u>ionDMIRxIntrusionEvt</u>	
	<u>ionDMIRxPowerEvt</u>	
	<u>ionDMITxPowerEvt</u>	
	<u>ionDMITxBiasEvt</u>	
	<u>ionDMITemperatureEvt</u>	
xxxxxxxxxxx	<u>ionTDMAISEvt (new)</u>	

Trap Server Log

The Trap Server log file contains information presented to the trap server by ION devices.

A sample part of a trap server log file is shown below.

```
Line
1
2
3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
12
13 E=
14 Ebig=
15 IP=192.251.144.220
16 com=trap
17 GT=Notification
18 ST=
19 TS=Thu May 13 10:06:42 2010
20 VB-Count=3
21 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266790) 326 days, 15:37:47.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
22
23 E=
24 Ebig=
25 IP=192.251.144.220
26 com=trap
27 GT=Notification
28 ST=
29 TS=Thu May 13 10:10:17 2010
30 VB-Count=3
31 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288348) 326 days, 15:41:23.48 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
32
33 E=
34 Ebig=
35 IP=192.251.144.220
36 com=trap
37 GT=Notification
38 ST=
39 TS=Thu May 13 10:10:18 2010
40 VB-Count=5
41 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288428) 326 days, 15:41:24.28 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.4.1.868.2.5.2.0.1 |
iso.3.6.1.2.1.47.1.1.1.1.134217728 = 134217728 | iso.3.6.1.4.1.868.2.5.2.1.1.1.134217728.6 = 6 |
iso.3.6.1.4.1.868.2.5.2.1.1.2.134217728.6 = 1
```

These trap server log file lines are described in the table below.

```

3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 =

```

Table 21: Trap Server Log File Description

Category	Meaning	Example
E=	Endian	cpsmM100Id
Ebig=	bigEndian	enterprises.transi- tion.productId.chassisProdsId. chassisSlot- Types.chSlcpcs.cpsmM100Id
IP=	IP address	192.251.144.199
com=	public	
GT=	Generic Trap	Enterprise Specific
ST=	Specific Trap	pSDeviceRemoved (114)
TS=	Timestamp – the log date that the file was recorded	Thu May 26 11:00:00 2011
VB-Count=	The number of Varbinds (Variable bindings)	3
Vars=	Varbinds (Variable bindings) - the variable number of values that are included in an SNMP packet. Each varbind has an OID, type, and value (the value for/from that Object ID).	cpsModuleModel.1.16 = cgfeb100Id cgfeb100Bialn- dex.1.16 = 1 cgfeb100SlotIn- dex.1.16 = 16
Timeticks:	(2822266290) 326 days, 15:37:42.90	
iso.3.6.1.6.3.1.1.4.1.0 =	iso.3.6.1.2.1.47.2.0.1	
iso.3.6.1.6.3.1.1.4.3.0 =	iso.3.6.1.2.1.47.2	

For Additional SNMP MIB Trap Information

For information on Network Management for Microsoft Networks Using SNMP, see <http://technet.microsoft.com/en-us/library/cc723469.aspx> or the [MSDN Library](#).

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>.



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.