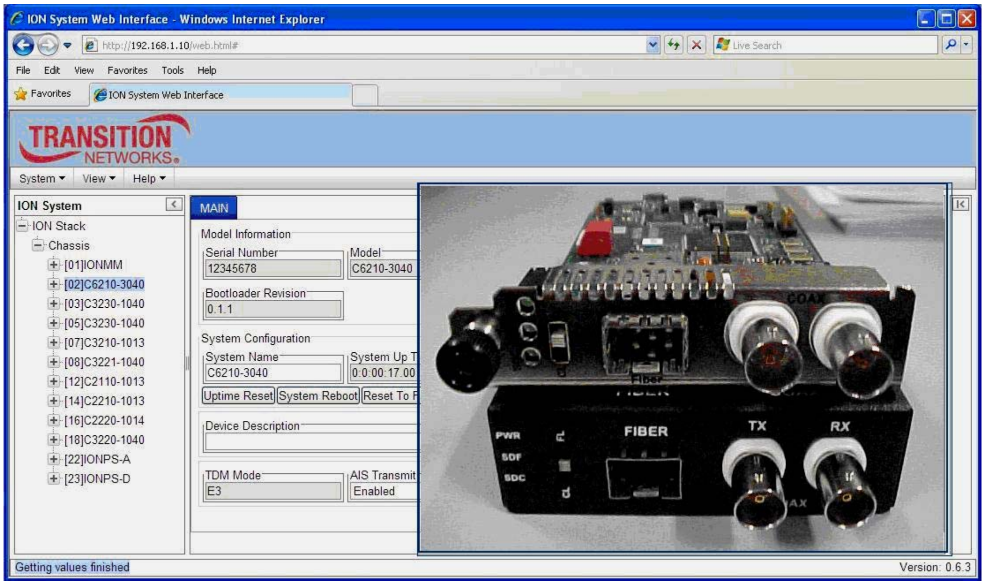
ION System

x6210 Managed DS3-T3/E3 to Fiber

Network Interface Device (NID)



Model Information

Serial Number: 12345678

Model: C6210-3040

Bootloader Revision: 0.1.1

System Configuration

System Name: C6210-3040

System Up T: 0:0:00:17.00

Device Description

TDM Mode: E3

AIS Transmit: Enabled

Getting values finished

Version: 0.6.3

User Guide

33495 Rev. B

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

Printed in the U.S.A.

ION System x6210 Managed DS3-T3/E3 to Fiber NID User Guide

33495 Rev. B

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Revision History

Rev	Date	Description
A	05/01/11	First release for software revision 0.6.5, Hardware Revision 0.0.1, and Bootloader Revision 0.1.1.
B	05/23/12	Revised for software revision 1.2.0.

Cautions and Warnings

Definitions

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. Warnings indicate that there is the possibility of injury to person.

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

Cautions

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

⚠

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

⚠

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

⚠

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

⚠

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

⚠

Caution: Only trained and qualified personnel should install or perform maintenance on the 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 235 for Electrical Safety Warnings translated into multiple languages.

Table of Contents

List of Figures

List of Tables

Section 1: Introduction

Document Overview

This manual provides the user with an understanding of the Transition Networks (TN) 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 utilized 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 serailno, modelno, 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.

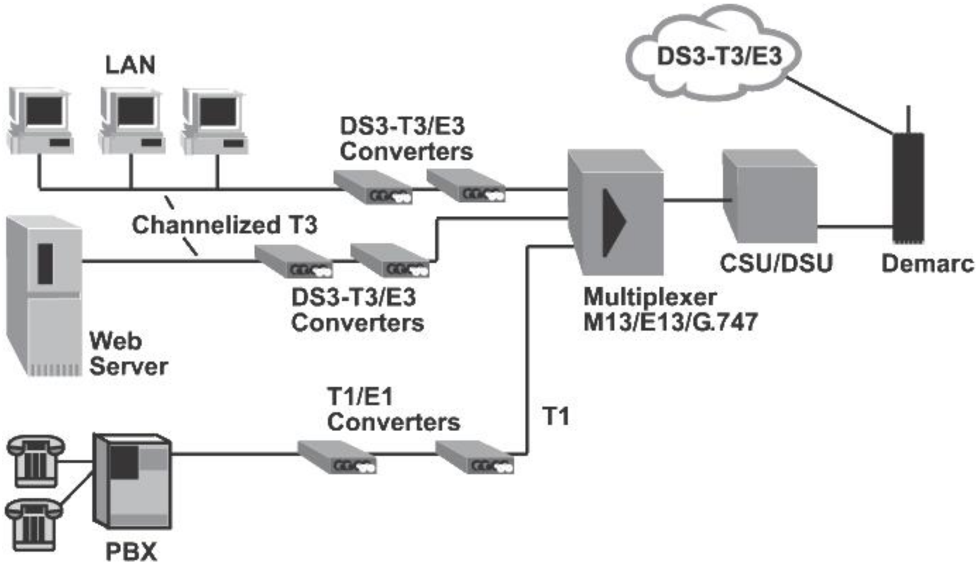


Figure 1a: Typical x6210 User Application (Standalone)

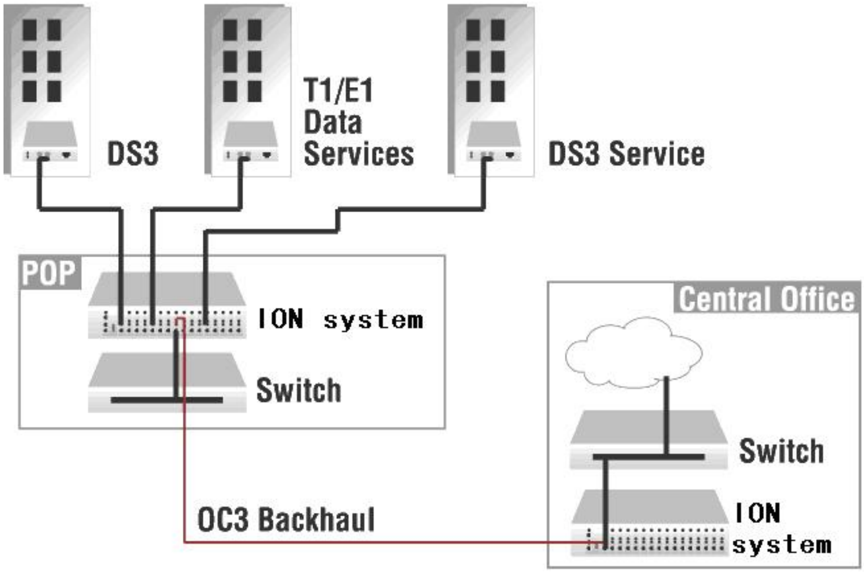


Figure 1b: Typical x6210 User Application (Chassis)

Applicable Standards and RFCs

The x6210 complies with the following hardware standards:

- ANSI T1.102 -1993; ETSI TBR-24
- ITU-T G.703 G.823 for jitter tolerance; G.775 for loss of signal
- GR-499 CORE & GR-253-CORE
- Regulatory Compliance for Emission: EN55022 Class A,FCC Class A
- Regulatory Compliance for Immunity: EN55024
- Safety Compliance: Unit: CE Mark

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 x6210 NID features are described in the following sub-sections.

Compatibility with ION System and Point System

The ION Platform offers backwards compatibility with Transition Networks' Point System family of media converters and NIDs. 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 will power the Point System modules, allowing the module to perform its copper-to-fiber media converter functions. Full read/write management of Point System modules is also available in the ION chassis. This requires the use of a Point System Management Module along with the Point System Adapter Card. By supporting management modules from both the ION Platform and the Point System, you can re-deploy and fully manage their Point System devices, easing your migration to the ION platform. Note the following caveats:

- A C6210 card can only run in an ION chassis system. It is not compatible with TN 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 2.2. 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 can not be managed by FP2.2.
- The ION DS3 (x6210) card can only support 1 level remote management. The maximum cascade level of S6010 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).

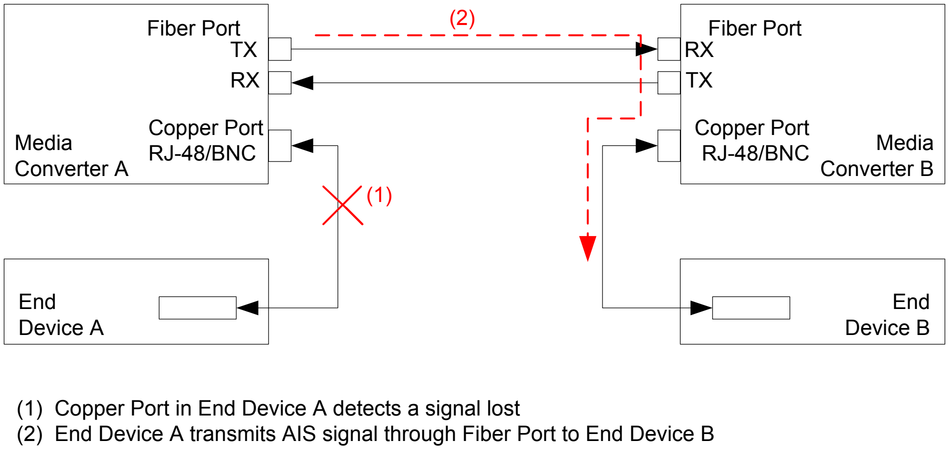


Figure 2: Typical AIS Application

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).

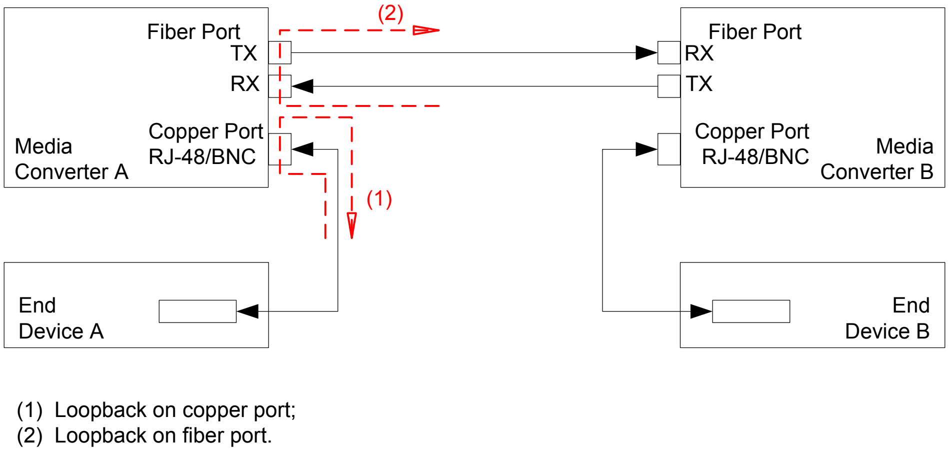


Figure 3: Loopback on Copper and Fiber port of Media Converter A

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 can not 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.

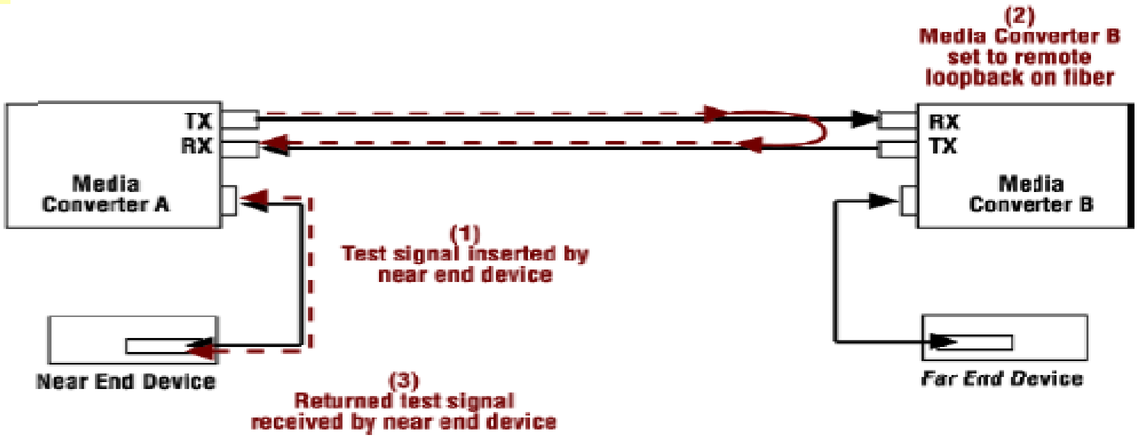


Figure 4: Typical Loopback function on a Fiber port

A typical x6210 Copper port Loopback applications is shown below.

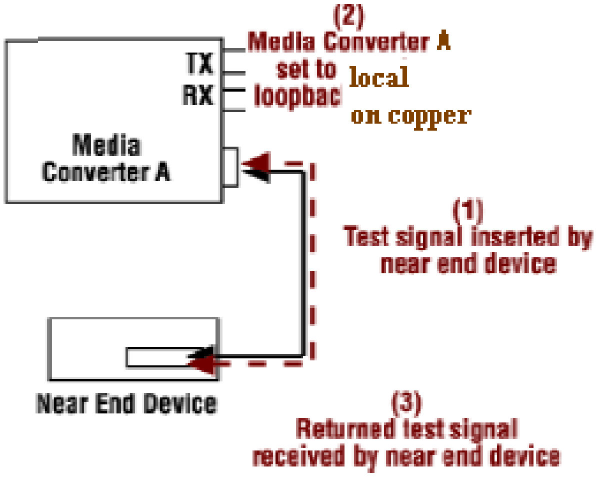


Figure 5: Typical Loopback function on a Copper port

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	

Parameter	Property	Range
Nominal Bit Rate	Read only	
Wavelength	Read only	
Receive Power	Read only	
Receive Power Alarm	Read only	Normal / Low Warning / High Warning / Low Alarm / High Alarm
Rx Power Intrusion Threshold	Read & Write	
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.

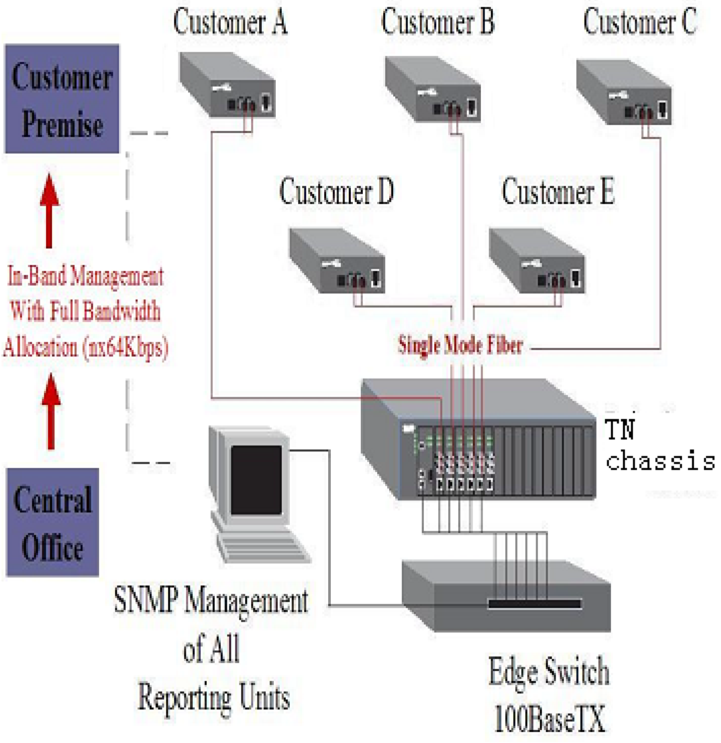


Figure 7: Typical Remote Management Application

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

A remote S6210 device is connected with 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 C6010. Traffic between the IONMM and C6010 is exchanged on the ION chassis' backplane Ethernet bus (BPC), while traffic between the local C6010 and remote S6210 is exchanged on the specific management channel (see figure below).

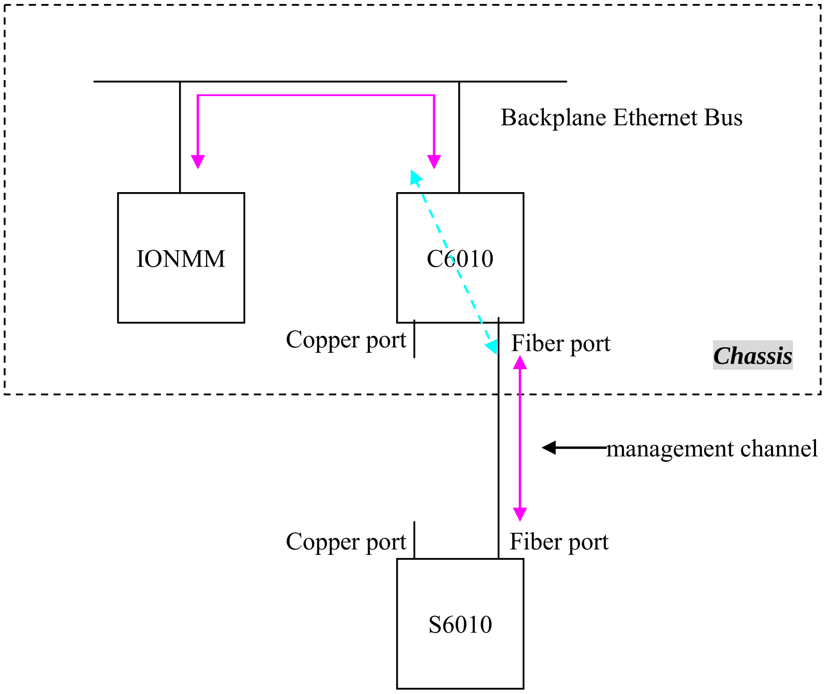


Figure 8: x6210 Remote Management Topology

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 can not 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 through the network.
- Simple Network Management Protocol (SNMP) – both public and private Management Information Bases (MIBs) allowing for a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).

TFTP (Trivial File Transfer Protocol)

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

SNMP MIBs and Traps

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

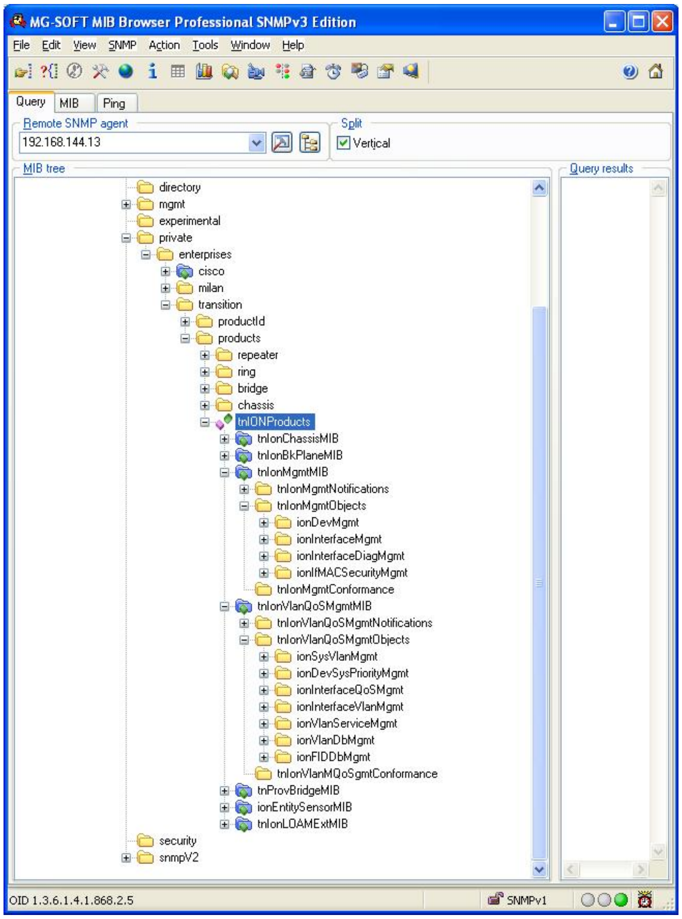
SNMP MIBs

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	ionDMIInfoTable		
5	ionIfLoopbackTable		
6	ionIfTDMTable		Used for ION T1/E1/DS3, including fields such as AIS, LBO, etc.)

An example of a private MIB objects tree is shown in the figure below.



Remote SNMP agent: 192.168.144.13

Split: ☑ Vertical

OID 1.3.6.1.4.1.868.2.5

Figure 9: Private MIB Objects

Trap Functions

The supported Trap MIBs are:

IF-MIB:
    linkDown
    linkup

TN-ION-MGMT-MIB.smi :
    ionDMIRxIntrusionEvt
    ionDMIRxPowerEvt
    ionDMITxPowerEvt
    ionDMITxBiasEvt
    ionDMITemperatureEvt

        ionTDMAISEvt (new)

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 TN software downloads page at http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx and locate the **Management MIB** section.
2. Click the link in the far right column (e.g., **Download mcc16.zip**).
3. At the **File Download** window, click **Save**.
4. At the **Save As** dialog box, verify the filename and **Save in** location (e.g., *C:\TFTP*-Root) and click **Save**.
5. At the **Download complete** dialog click **Close**. The downloaded file is saved to the specified folder location.
6. 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.
7. 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 405.

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.

For Additional MIB Information

For information on traps that the IONMM supports, see "Appendix G: SNMP Traps Supported" on page 243.

For more information on the SNMP Agent, Network Management Station (NMS), MIBS, MIB modules and MIB Variables, the Object ID (OID), the MIB Tree / branch /node, MIB Table Indices, values, notations and transaction types, etc., see the SNMP Primer at http://www.transition.com/pshelp/snmp.html#indices

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).

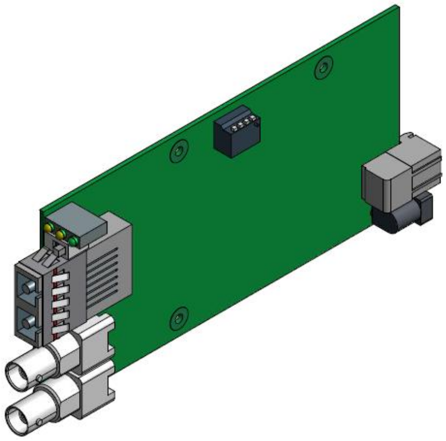
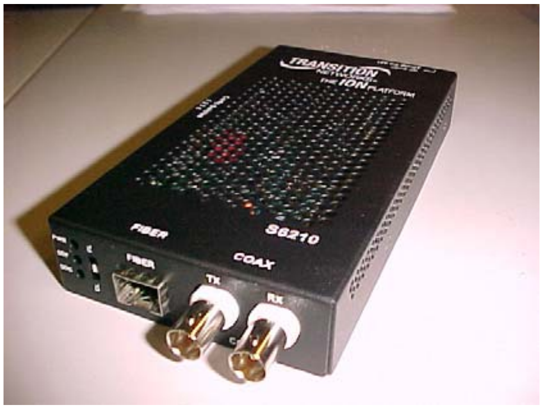
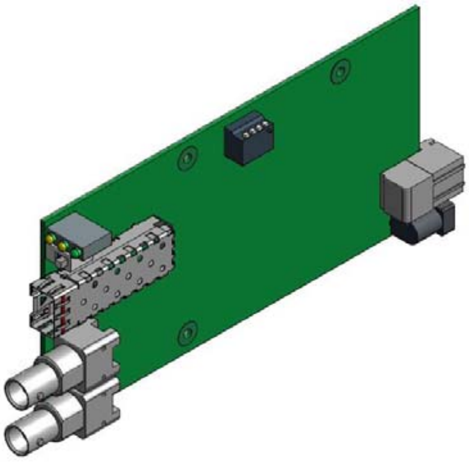
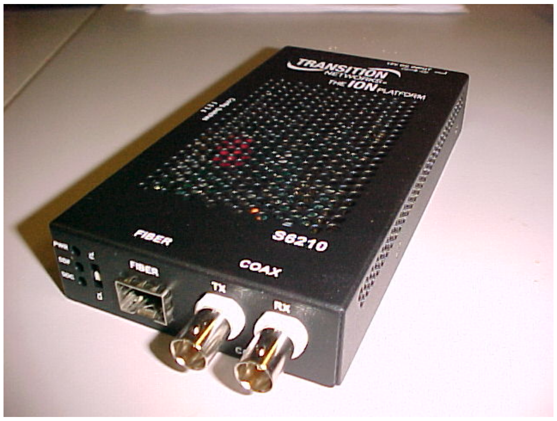
Chassis Models (C6210-xxxx)	Standalone Models (S6210-xxxx)
 **C6210-30xx**	 TRANSITION NETWORKS THE ION PLATFORM FIBER S6210 COAX TX RX **S6210-301x**
 **C6210-3040**	 TRANSITION NETWORKS THE ION PLATFORM FIBER S6210 COAX TX RX **S6210-3040**

Figure 10: x6210 Models

Fiber Specifications

For the latest information go to http://www.transition.com/TransitionNetworks/Landing/SFP-XFP/SFP-XFP.aspx and click on “OPTIC SPECS” and then click on “Download PDF”.

Table 3a: C2010 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

Physical Specifications

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

Table 4: Physical Specifications

Data Speed	E3 = 34.4Mb/s
	DS3 = 44.7Mb/s
	STS-1 = 51.8Mb/s

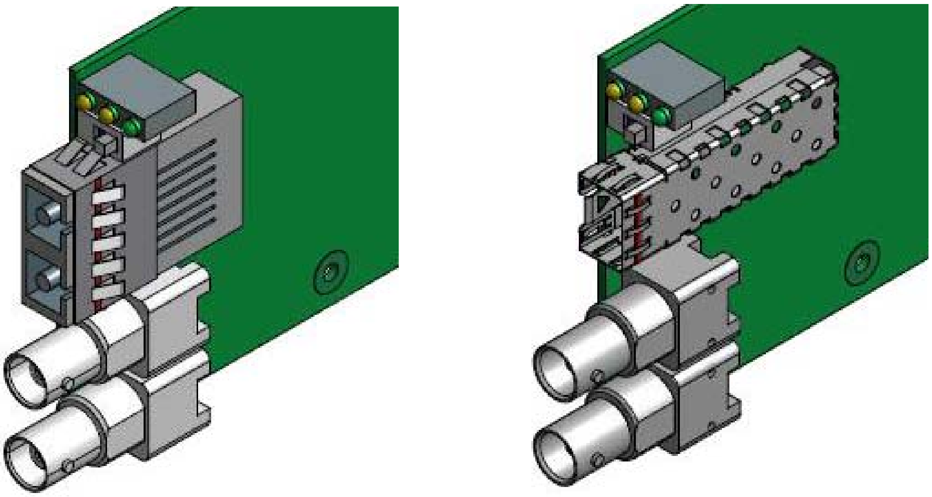
Coax Interface	Two Coax connectors – TX and RX (C6010-3040)
Fiber Port	Connectors supported: 1x9, SFP
Dimensions	Chassis model: 1” x 3.3” x 6.1” (2.54 cm x 8.382 cm x 15.5 cm) HxWxD Standalone model: 0.9” x 3.4” x 6” (2.3 cm x 8.6 cm x 15.2 cm) HxWxD
Power Supply	Chassis model: From ION chassis backplane (slide-in card) Standalone model: 7.5 to 15.9 VDC
Environment	See ION chassis specifications
Shipping Weight	1 lb (0.45 kg)
Warranty	Lifetime

Connectors

The x6210 connectors are described in the table below. For cable specifications see "Appendix D: Cable Specifications" on page 258.

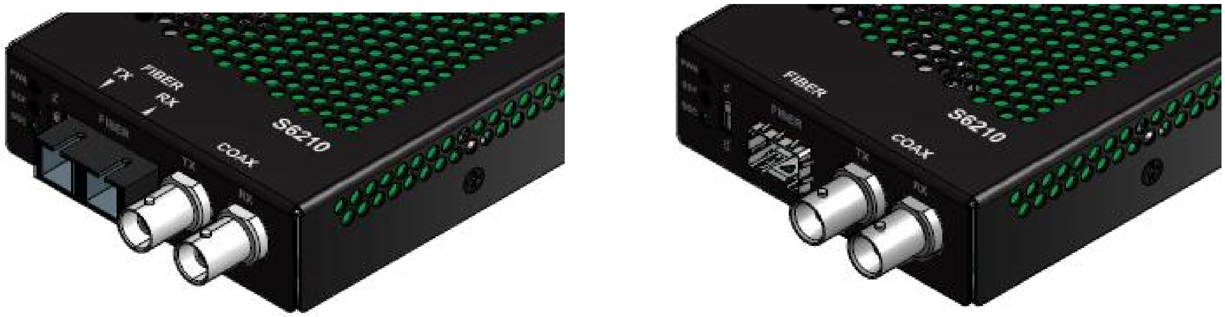
Table 5: x6210 Connector Descriptions

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 and receive connection.



C6210-30xx **C6210-3040**

Figure 11: C6210 Model Connectors



S6210-30xx

S6210-3040

Figure 12: S6210 Model Connectors

LED Descriptions

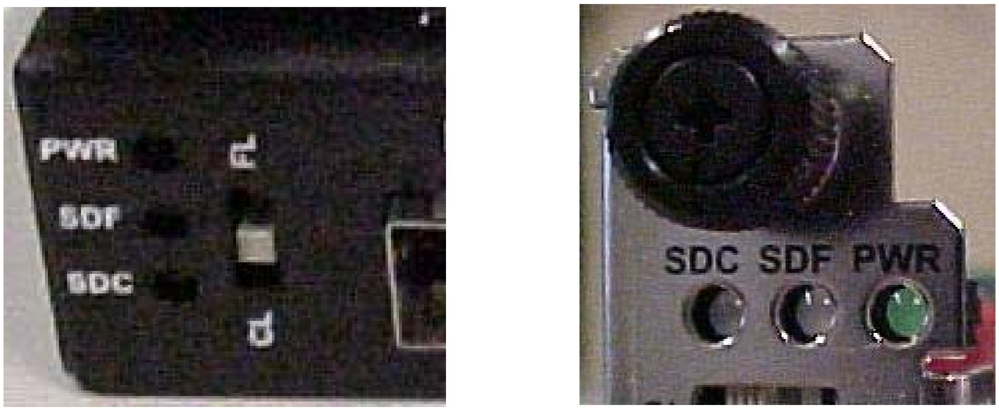
The x6210 LEDs are described below.

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

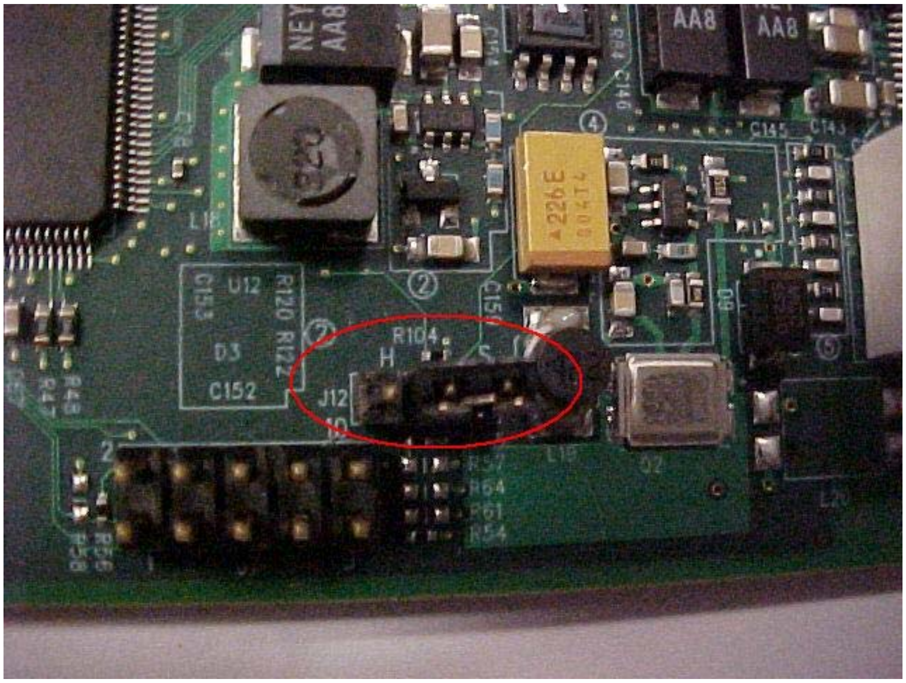
Figure 13: x6210 LEDs

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).



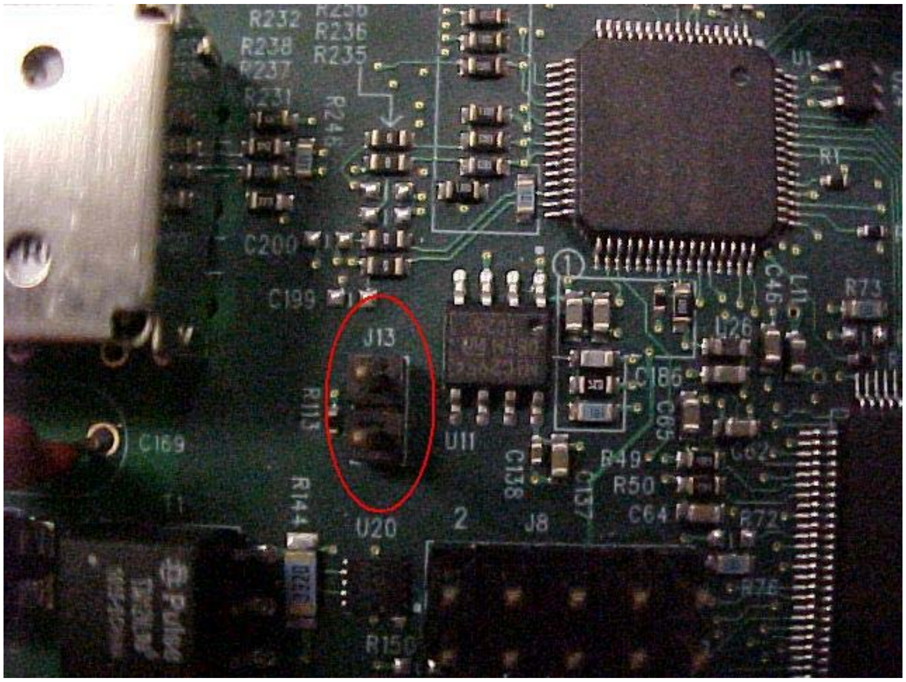
Jumper Pin #s	Sets Mode to	Note
1-2	Hardware mode	Places the x6210 in Hardware operating mode; the hardware can configure the x6210.
2-3	Software mode	Places the x6210 in Software operating mode; the software can configure the x6210 (the default setting).

For more information, see “DIP Switches and Jumper Settings” on page 211.

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 211.

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 211.

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:

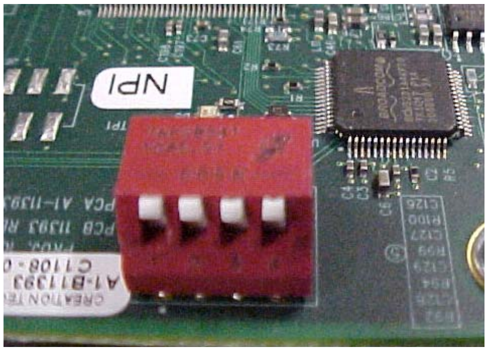
*Up (OPEN) = transmit AIS if receive loss of carrier.

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.



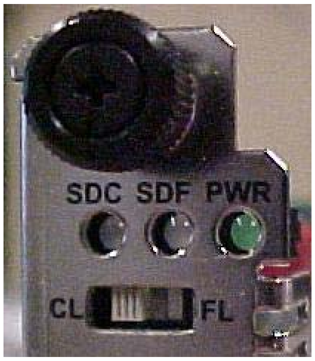
* The SW2 default is all switch positions in the Up (OPEN) position.

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.

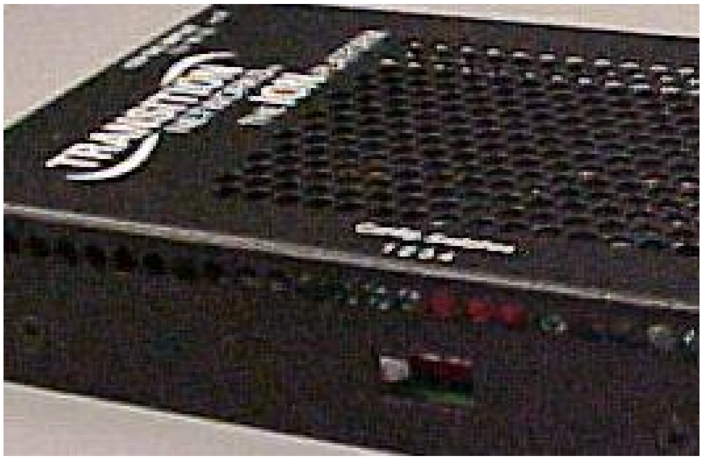


Figure 13: S6210 DIP Switches

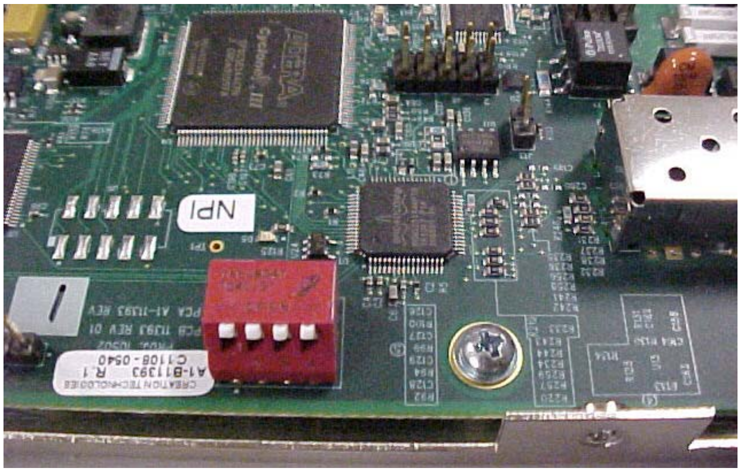


Figure 14 : C6210 DIP Switches

For more information, see "DIP Switches and Jumper Settings" on page 211.

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

Related Manuals and Online Help

A printed documentation card is shipped with each x6210 device. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface. A substantial set of technical documents, white papers, case studies, etc. are available on the Transition Networks web site at www.transition.com. Note that this manual provides links to third part web sites for which Transition Networks is not responsible.

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. SFP manuals (product specific)
6. Release Notes (firmware version specific)

Note: Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version. While all screen examples may not display the latest version number, all of the descriptions and procedures reflect the latest software/firmware version, noted in the Revision History on page 2.

For More Information

Transition Networks 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.

- Advanced Product Features literature on the Transition Networks web site at www.transition.com.
- Transition Networks Learning Center: http://www.transition.com/TransitionNetworks/Learning/Seminar/Description.aspx
- Transition Networks Tech Support:
- http://www.transition.com/TransitionNetworks/TechSupport/Contact.aspx
- 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.

Section 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 Transition Networks ION chassis (ION219-x). For a complete list of ION platform products, go to the Transition Networks website at http://www.transition.com.

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.

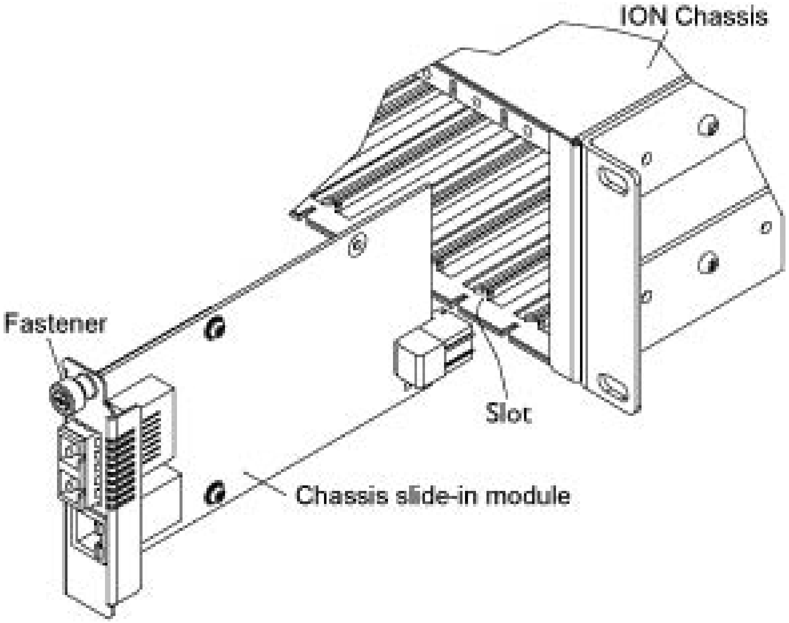


Figure 15: Chassis Installation

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 15: 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 Transition Networks 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.

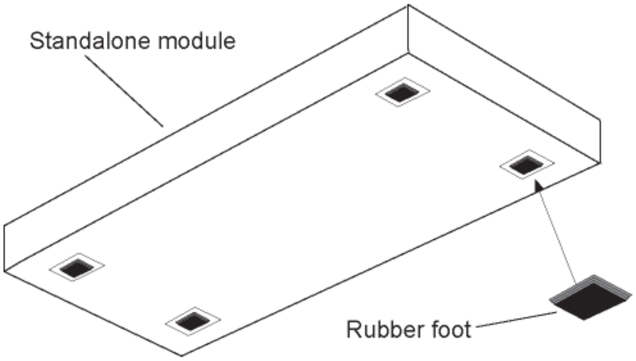


Figure 16: Tabletop Installation

3. Set the S6210in 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.

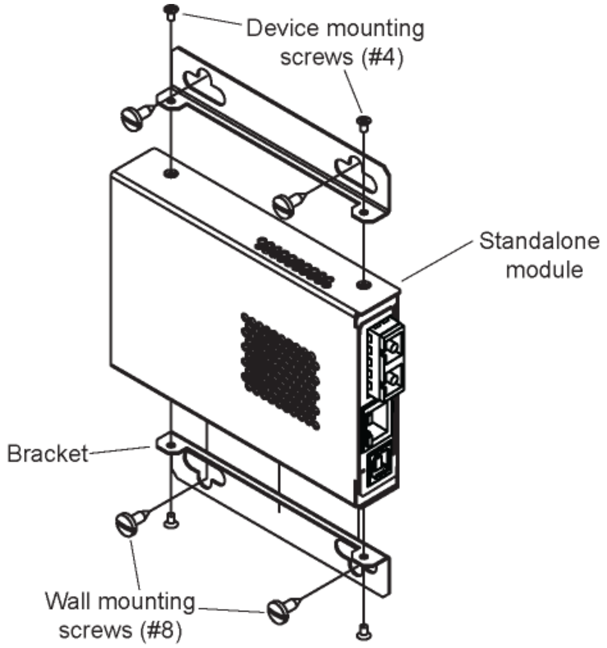


Figure 17: Wall Mount Installation

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 TN#25025).

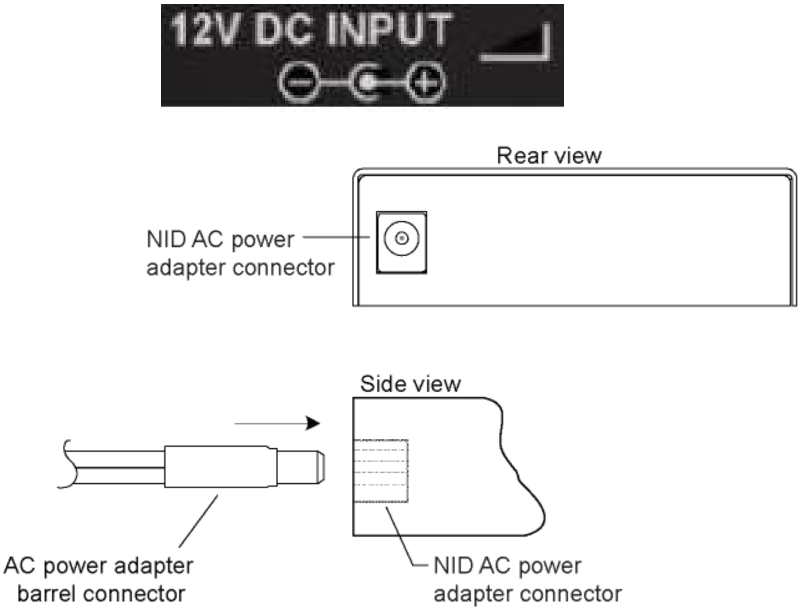

12V DC INPUT
Rear view
NID AC power adapter connector
Side view
AC power adapter barrel connector
NID AC power adapter connector

Figure 18: 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.

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.

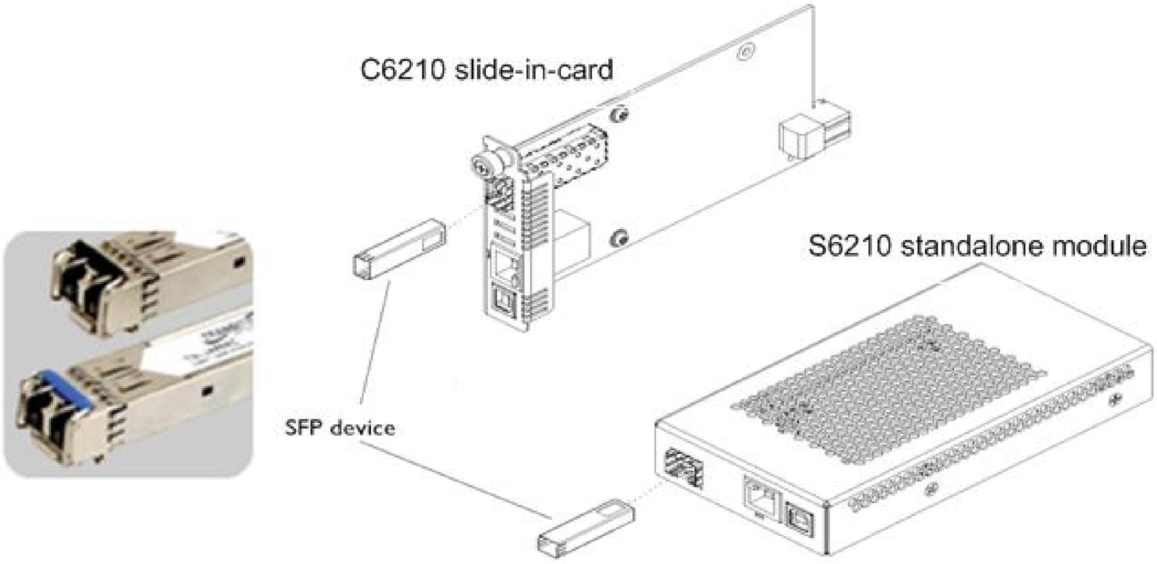


Figure 19: SFP Installation

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 following USB drivers are provided with the ION system on a CD, and are also available at http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx:

Windows® 7	Windows 7 x64	Windows XP® 32 bit
Windows 2000	Windows 2003 32 bit	Windows Vista®
Windows Vista x64	Windows XP 64 bit	

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.

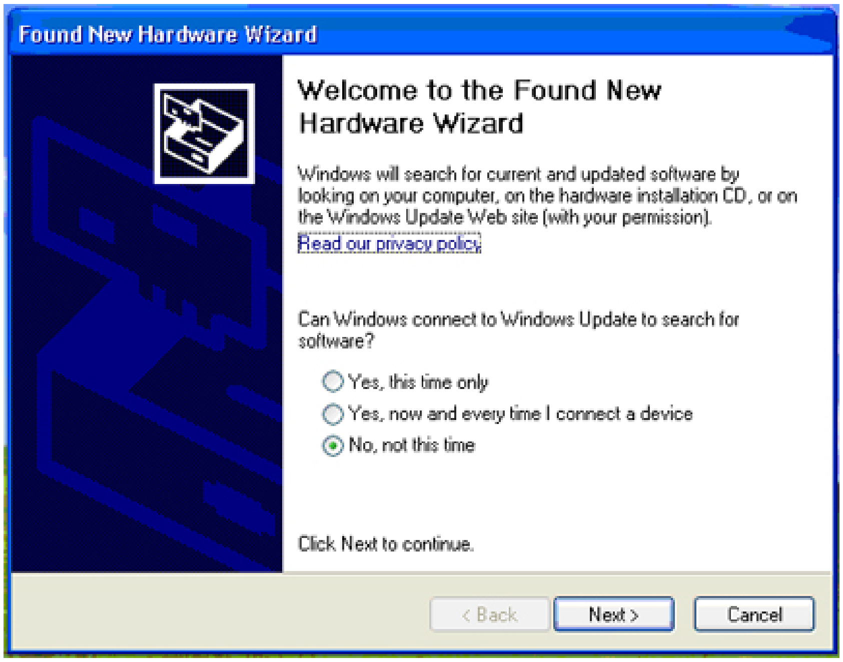
To install the USB driver on a computer running *Windows XP*, do the following.

1. Extract the driver (from the provided CD or 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.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

Can Windows connect to Windows Update to search for software?

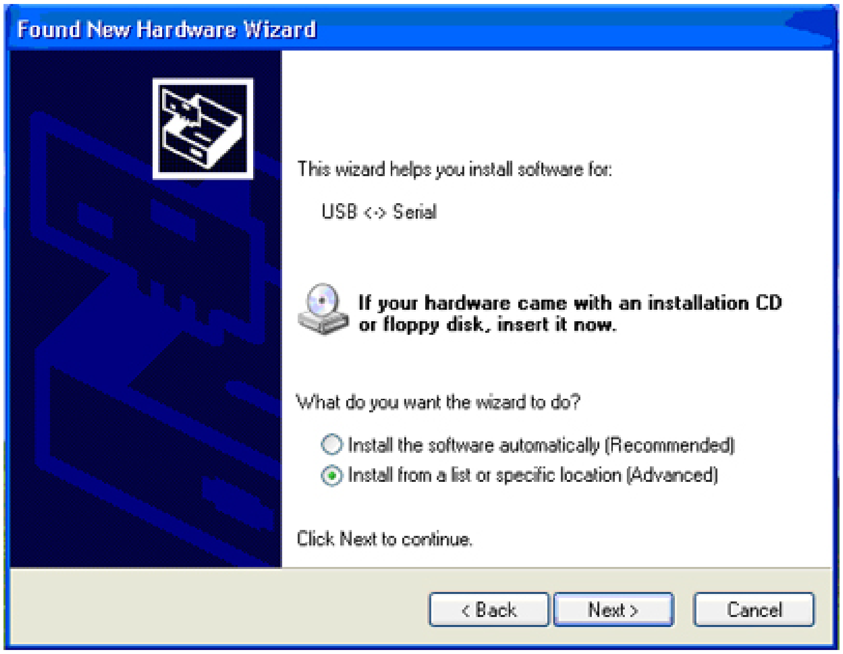
○ Yes, this time only
○ Yes, now and every time I connect a device
● No, not this time

Click Next to continue.

3. Select **No, not this time**.

4. Click **Next**.

The installation options window displays.



Found New Hardware Wizard

This wizard helps you install software for:

USB <-> Serial

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

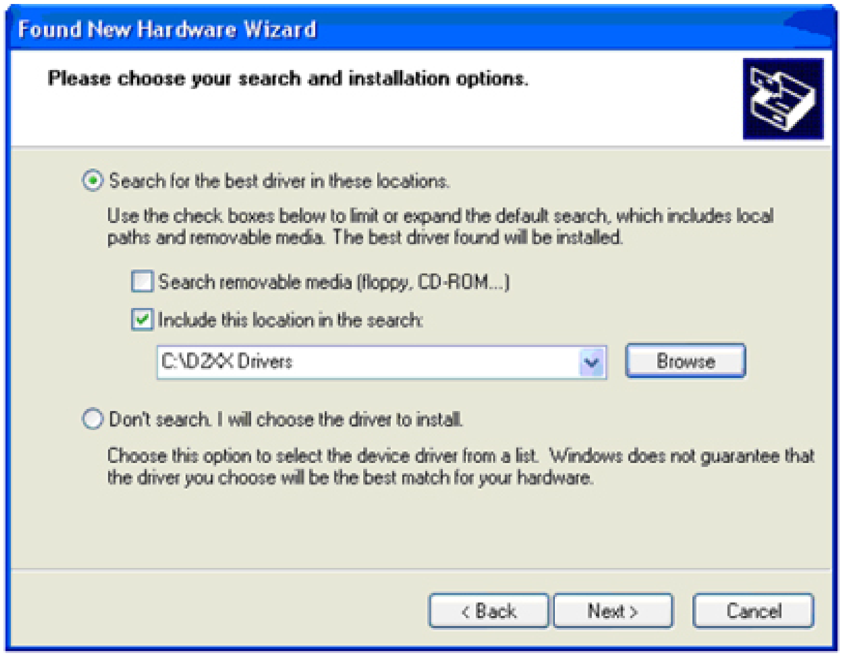
○ Install the software automatically (Recommended)
● Install from a list or specific location (Advanced)

Click Next to continue.

5. Select **Install from a list or specific location (Advanced)**.

6. Click **Next**.

   The driver search installation options window displays.



Found New Hardware Wizard

Please choose your search and installation options.

● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

□ Search removable media (floppy, CD-ROM...)
☑ Include this location in the search:

C:\D2XX Drivers

○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

7. Click **Browse**.

8. Locate and select the USB driver downloaded in step 1 above.

9. Click **Next**.

   Driver installation begins.

10. 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.

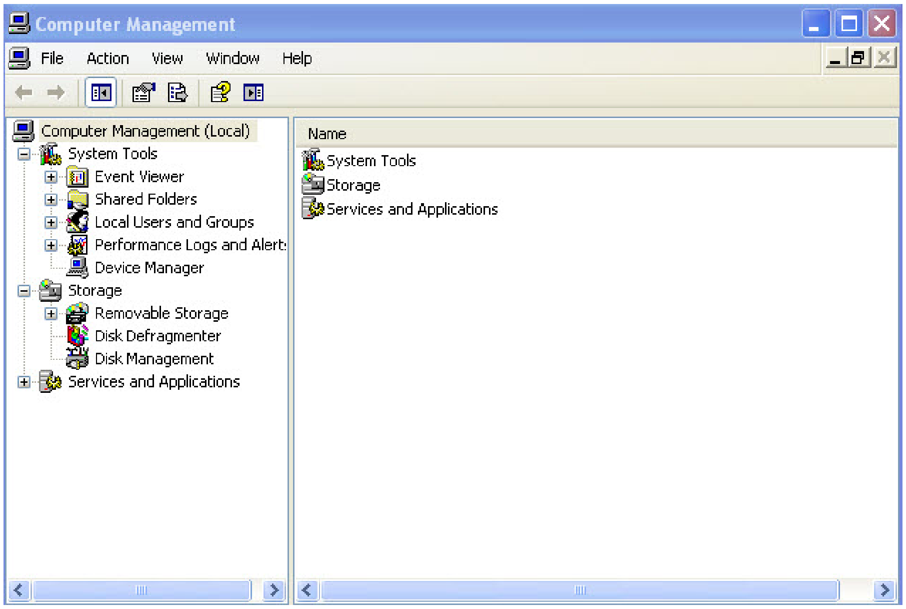
Configuring HyperTerminal

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

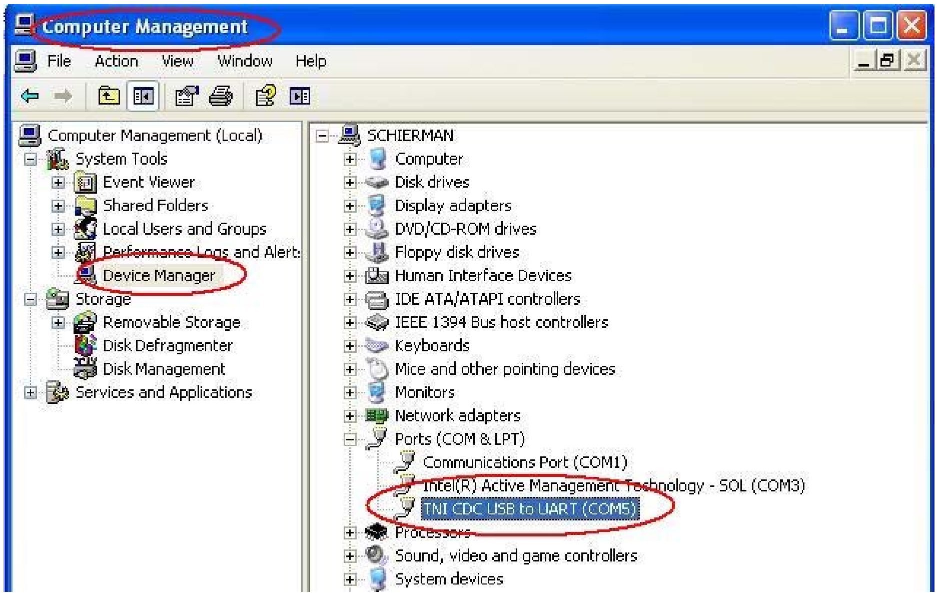
1. On the desktop, right-click on **My Computer**.

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.)


Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Event Viewer
Shared Folders
Local Users and Groups
Performance Logs and Alert:
Device Manager
Storage
Removable Storage
Disk Defragmenter
Disk Management
Services and Applications
SCHIERMAN
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Floppy disk drives
Human Interface Devices
IDE ATA/ATAPI controllers
IEEE 1394 Bus host controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Ports (COM & LPT)
Communications Port (COM1)
Intel(R) Active Management Technology - SOL (COM3)
TNI CDC USB to UART (COM5)
Processors
Sound, video and game controllers
System devices

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 (**COM5** in the example above). You will need to provide this COM port number in step 8.

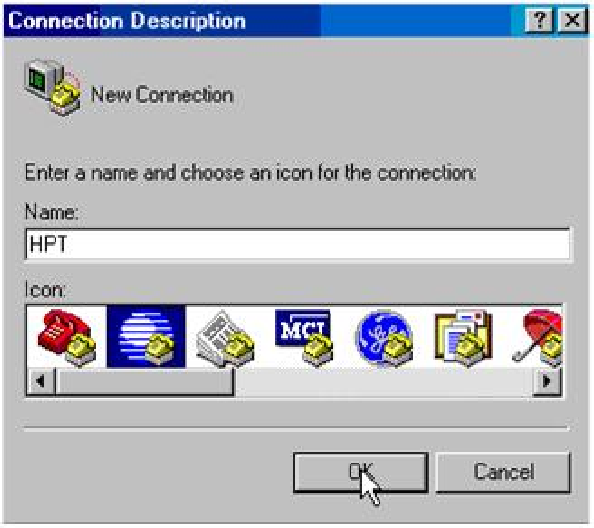
5. Launch the HyperTerminal software.

   a) Click **Start**.

   b) Select: **All Programs > Accessories > Communications**

   c) Click **HyperTerminal**.

   The Connection Description window displays.



Enter a name and choose an icon for the connection:

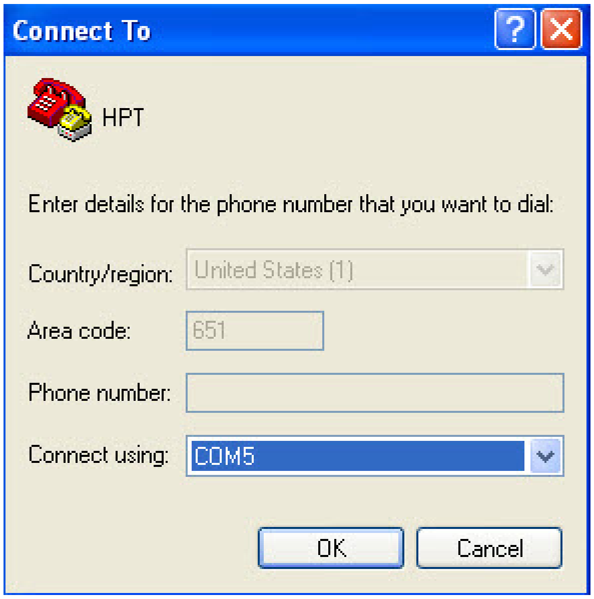
Name: HPT

Icon:

6. Type in a name and select an icon that will be used for this connection.

7. Click **OK**.

   The **Connect To** window displays.



Connect To

HPT

Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 651

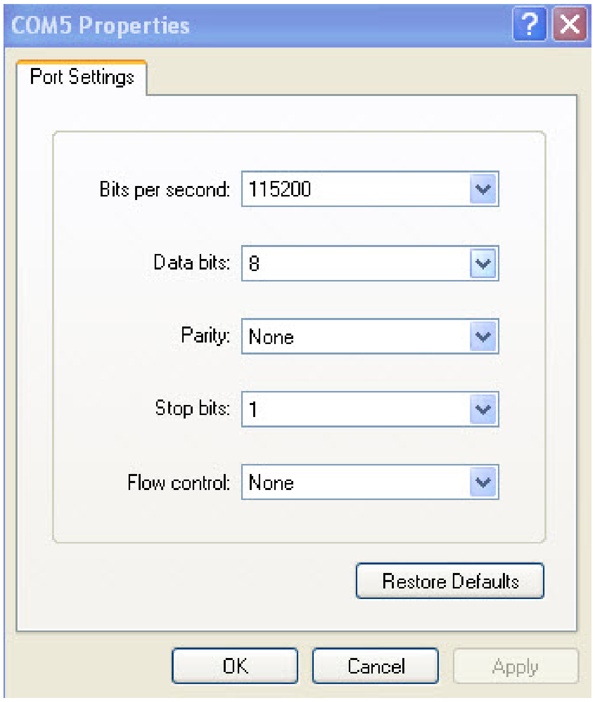
Phone number:

Connect using: COM5

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.



COM5 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

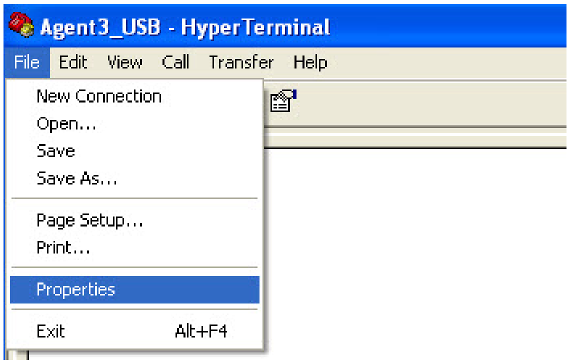
Flow control: None

10. Set the COM port properties as follows:

- Bits per second: **115200**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**
- Flow control: **None**

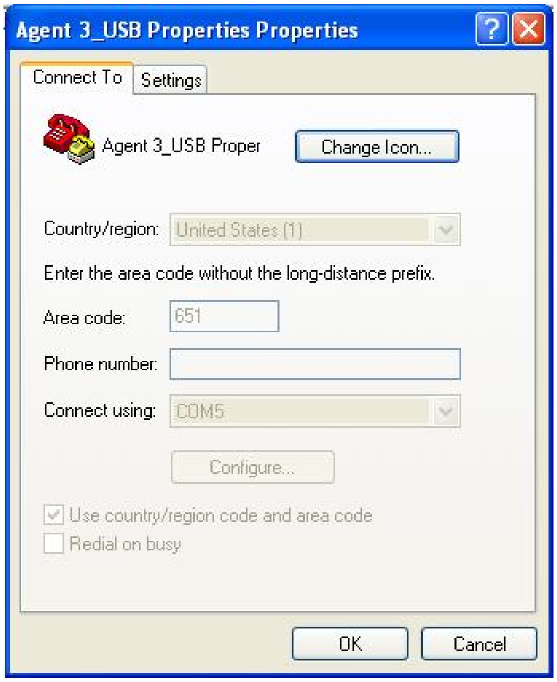
11. Click **OK**.

A blank HyperTerm window displays.



12. In the HyperTerm window, select **File > Properties**.

The Properties window displays the **Connect To** tab.



Country/region: United States (1)

Enter the area code without the long-distance prefix.

Area code: 651

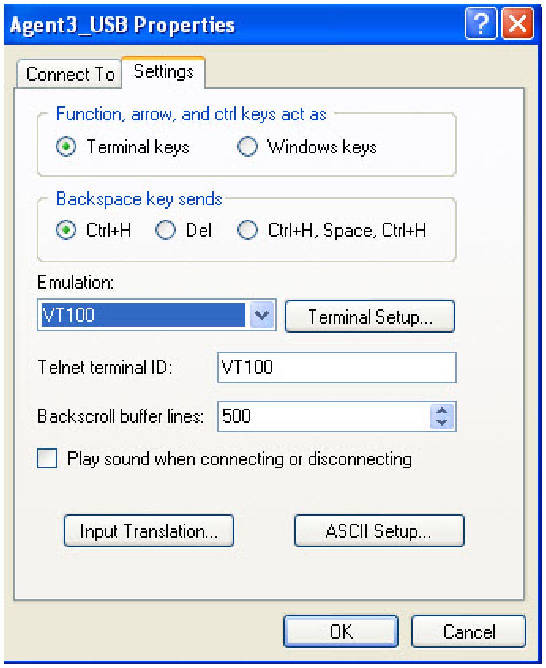
Phone number:

Connect using: COM5

☑ Use country/region code and area code

□ Redial on busy

13. Click the **Settings** tab.



Function, arrow, and ctrl keys act as
● Terminal keys ○ Windows keys

Backspace key sends
● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

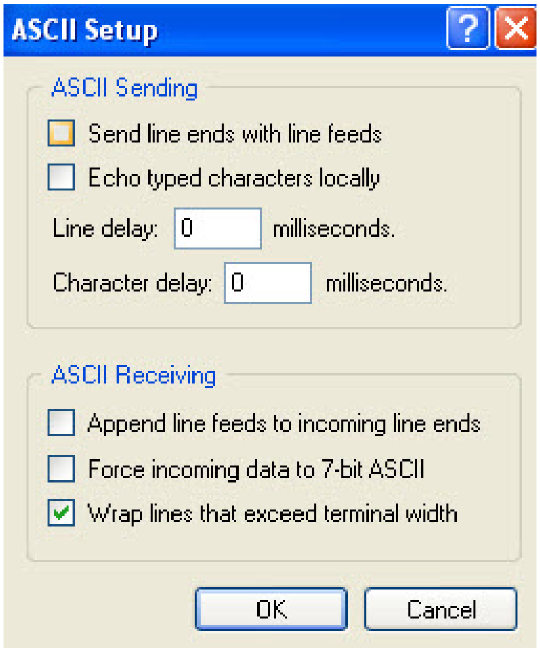
Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

14. In the **Emulation** field, select **VT100**.

15. Click the **ASCII Setup…** button.



ASCII Sending
□ Send line ends with line feeds
□ Echo typed characters locally
Line delay: 0 milliseconds.
Character delay: 0 milliseconds.

ASCII Receiving
□ Append line feeds to incoming line ends
□ Force incoming data to 7-bit ASCII
☑ Wrap lines that exceed terminal width

16. Verify that **Wrap lines that exceed terminal width** is selected.

17. Click:
    - **OK**
    - **OK**
18. Login (see Starting a USB Session below).

Starting a USB Session in HyperTerminal

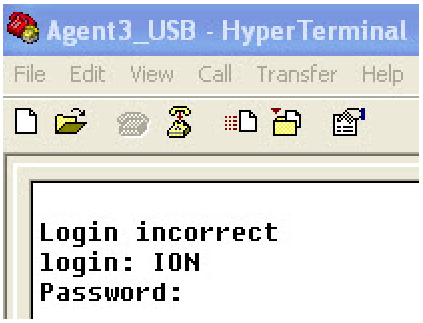
The following describes the procedure to access the NID via a USB connection.

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

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

3. Type your login (the default is **ION**). **Note:** the login is case sensitive.
4. Press **Enter**.

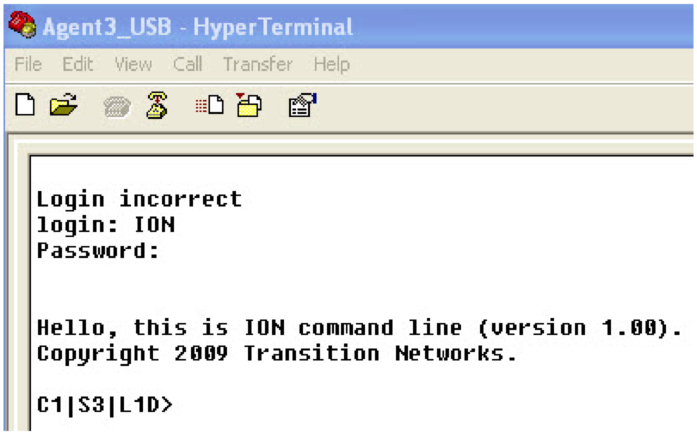
   The password prompt displays. **Note:** if a "*Login incorrect*" message displays, ignore it.



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

5. Type your password (the default is **private**). **Note:** the password is case sensitive.
6. Press **Enter**.

   The HyperTerminal command line prompt displays.



```
Login incorrect
login: ION
Password:


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

C1|S3|L1D>
```

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

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

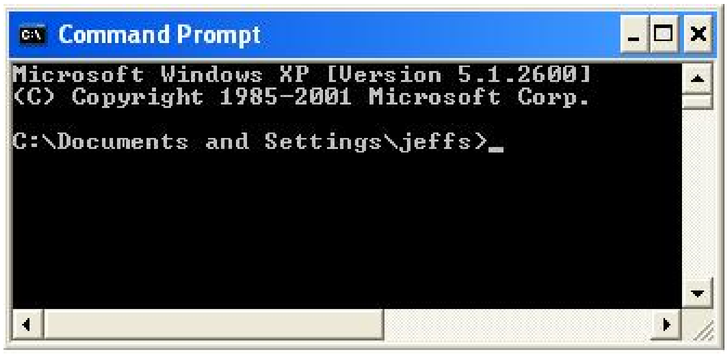
The NID can be managed remotely through the Ethernet network via either a Telnet session or the Web interface. Before this is possible, you must set up the IP configuration for the x6210.

Starting a Telnet Session

The x6210can be controlled from a remote management station via a Telnet session over an Ethernet connection. The x6210is controlled and configured through CLI commands. Use the following procedure to connect to and access the x6210via a Telnet session.

1. Click Windows **Start**.
2. Select **All Programs>Accessories**.
3. Click **Command Prompt**.

The command prompt window displays.



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

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

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 systems uses a security protocol (e.g., RADIUS, etc.), enter the login and password required by that protocol.

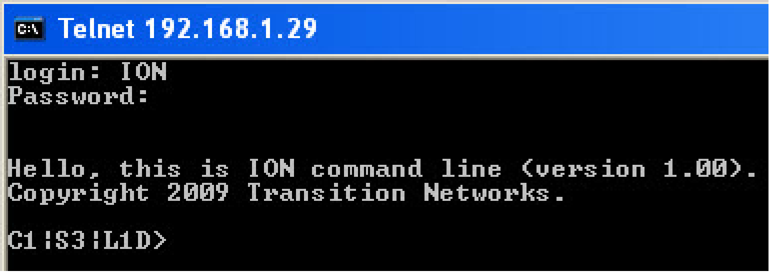
6. Type your login (the default is **ION**). **Note:** the login is case sensitive.
7. Press **Enter**.

   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.



```
login: ION
Password:

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

C1|S3|L1D>
```

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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)

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 following web browsers.

- Firefox (Mozilla Firefox) 3 - 6
- Internet Explorer 6 - 9
- Google Chrome 3 - 13

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 can not be modified.

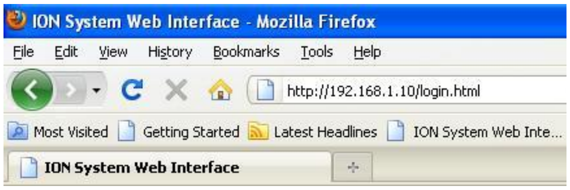
A Web session can be used to connect to and set up the NID.

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.

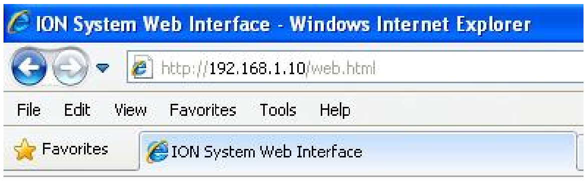
To sign in to the NID via the Web, do the following.

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).



http://192.168.1.10/login.html

ION System Web Interface - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines ION System Web Inte...
ION System Web Interface

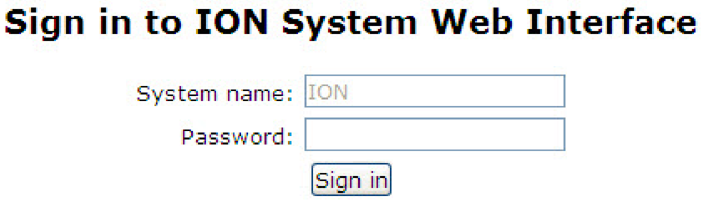


http://192.168.1.10/web.html

ION System Web Interface - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
ION System Web Interface

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

The ION System sign in screen displays.



Sign in to ION System Web Interface

System name: ION

Password:

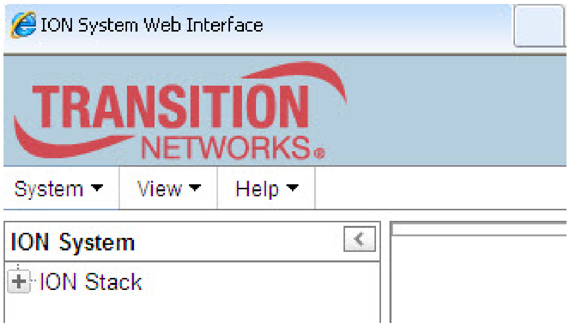
Note: If your systems uses a security protocol (e.g., RADIUS, etc.), you must enter the login and password required by that protocol.

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.

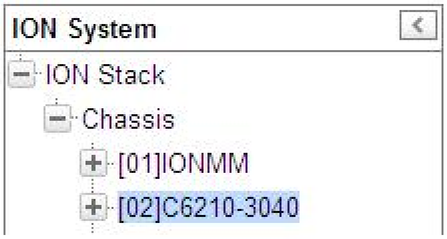
6. Click **Sign in** or press **Enter**.

   The opening screen displays.



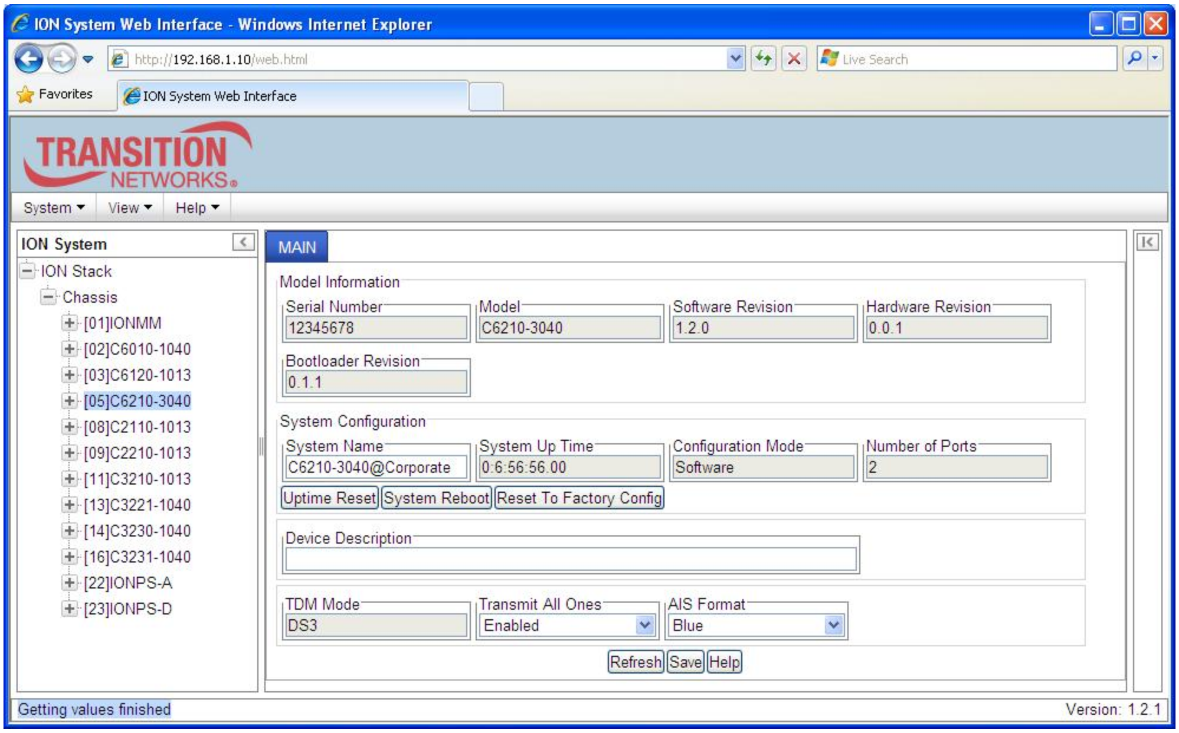
7. Click the plus sign [+] next to **ION Stack**. This unfolds "ION Stack" node in the left tree view and will refresh device status.

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:



Model Information

Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

System Name: C6210-3040@Corporate
System Up Time: 0:6:56:56.00
Configuration Mode: Software
Number of Ports: 2

Device Description:

TDM Mode: DS3
Transmit All Ones: Enabled
AIS Format: Blue

Getting values finished

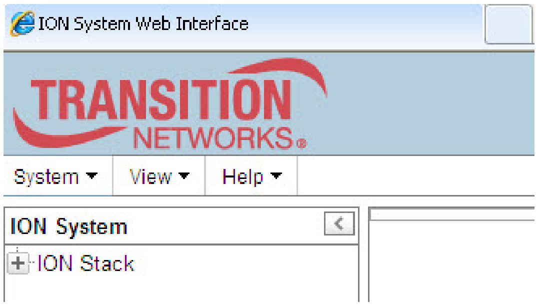
Version: 1.2.1

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.

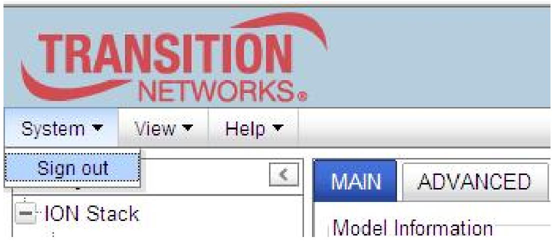
Terminating the Web Interface (Sign Out)

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.

Section 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 x6010 via the CLI or the Web interface.

Managing Slide-In and Remote Modules Using CLI Commands

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

For example:

```
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.

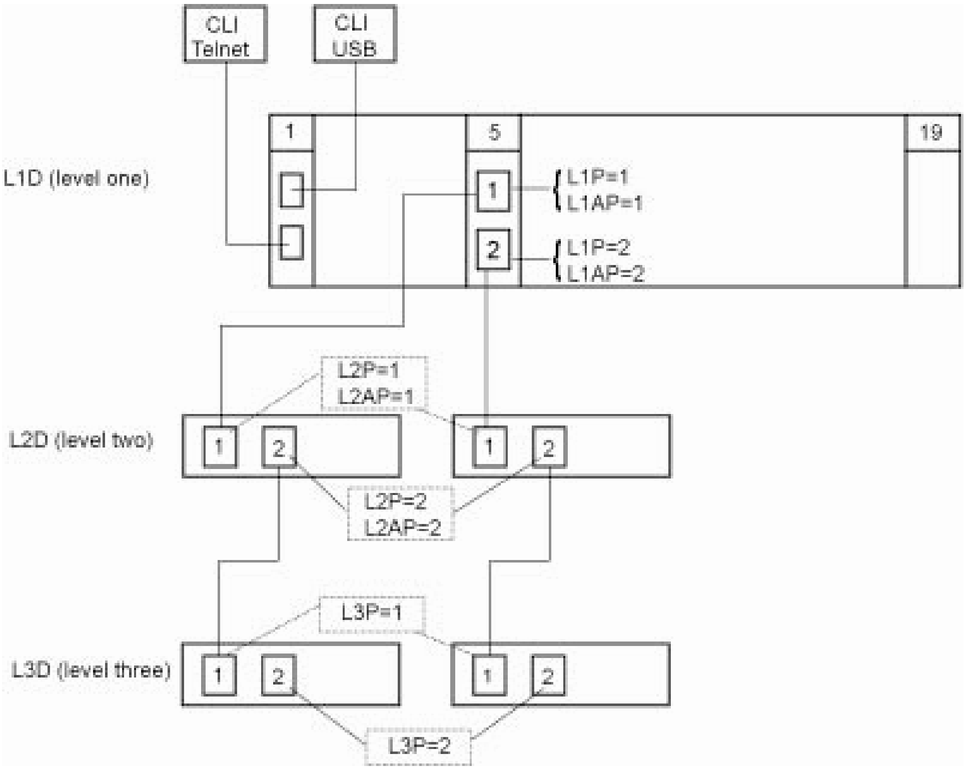


Figure 20: CLI Location Hierarchy

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 **can not** 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 C6010-3040 to its level 2 remotely-connected device (S6010-1040) in the **stat** command example above, you would enter:

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

Command control would be shown by the command line prompt:

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

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

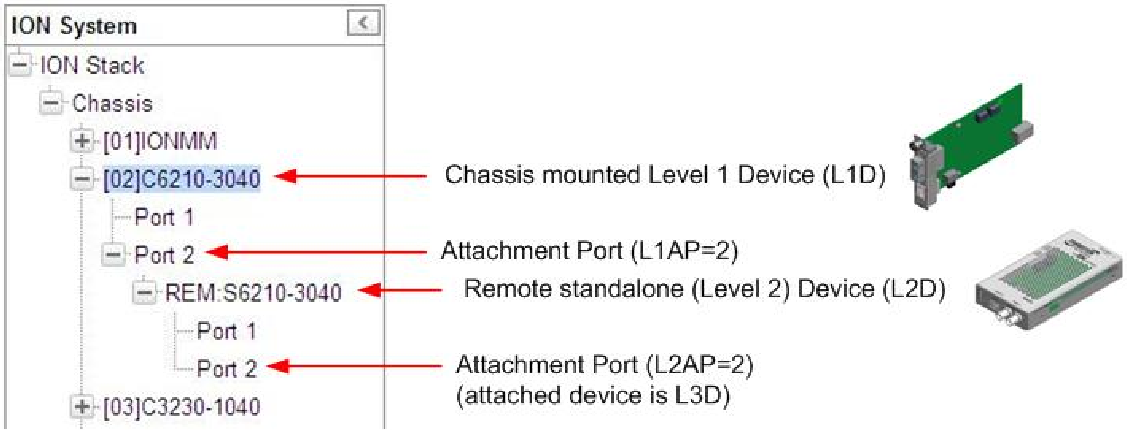
```
C1|S4|L1AP2|L2D>go l2p=1
```

Command control would be shown by the command line prompt:

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

Managing Slide-In and Remote Modules via the Web Interface

1. Access the NID through the Web interface (see “Starting the Web Interface” 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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=
PORT|l1d|l2d|l3d)
```

For example:

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

```
C0|S0|L1D>go l1p=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:

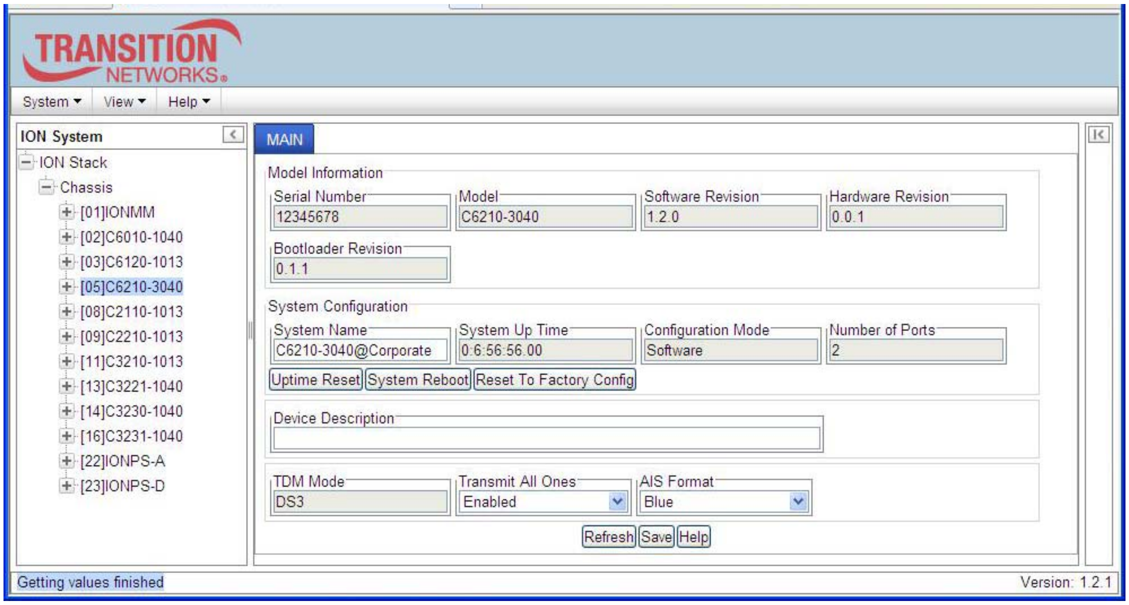
```
C0|S0|L1P1>go l1d
```

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).



Model Information

Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

System Name: C6210-3040@Corporate
System Up Time: 0:6:56:56.00
Configuration Mode: Software
Number of Ports: 2

Device Description:

TDM Mode: DS3
Transmit All Ones: Enabled
AIS Format: Blue

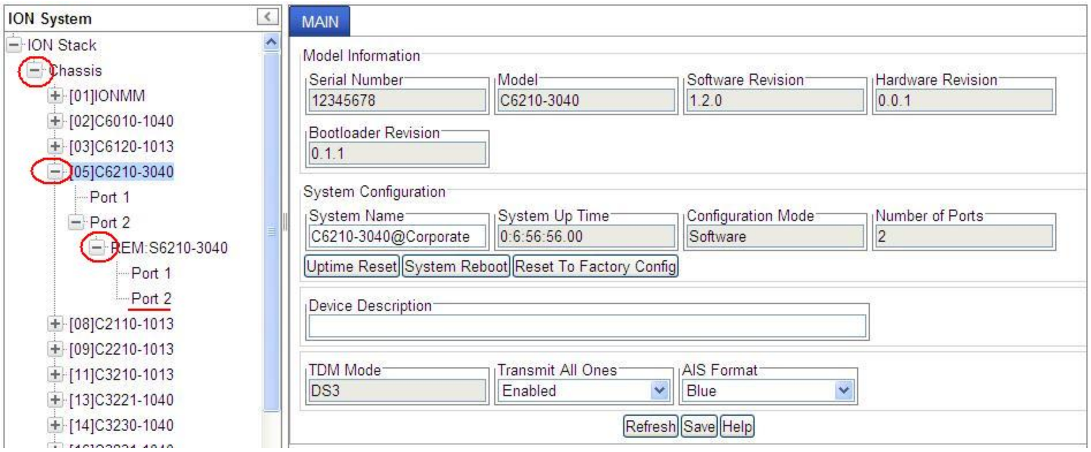
Getting values finished

Version: 1.2.1

2. Click the plus sign [+] next to **ION Stack** to unfold the "**ION Stac**k" 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).



Model Information

Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

System Name: C6210-3040@Corporate
System Up Time: 0:6:56:56.00
Configuration Mode: Software
Number of Ports: 2

Device Description:

TDM Mode: DS3
Transmit All Ones: Enabled
AIS Format: Blue

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	**Stack** - consists of one chassis. The Stack Members table lists the Stack's chassis, type, and description. **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: * 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. **Device** – provides tabs and sub-tabs for the IONMM and NIDs in the ION system. **Port** - provides tabs and sub-tabs for a selected NID port.
System Dropdown	Sign out.
View Dropdown	Refresh.
Help Dropdown	Online Help, ION Product Home Page, About ION System Web Interface.

Device-Level 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: *Refresh, Save, Start, Stop,* and *Help.*
DMI Tab (Port 2 only)	Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length. The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See "DMI (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 "*The DMI feature is not supported on current port*." 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.

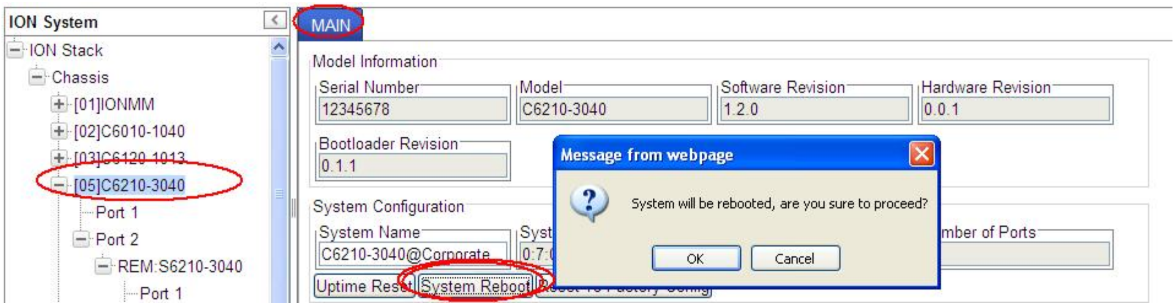
For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- 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.



Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1
System Name: C6210-3040@Corporate
Syst: 0:7:0
mber of Ports

Message from webpage

System will be rebooted, are you sure to proceed?

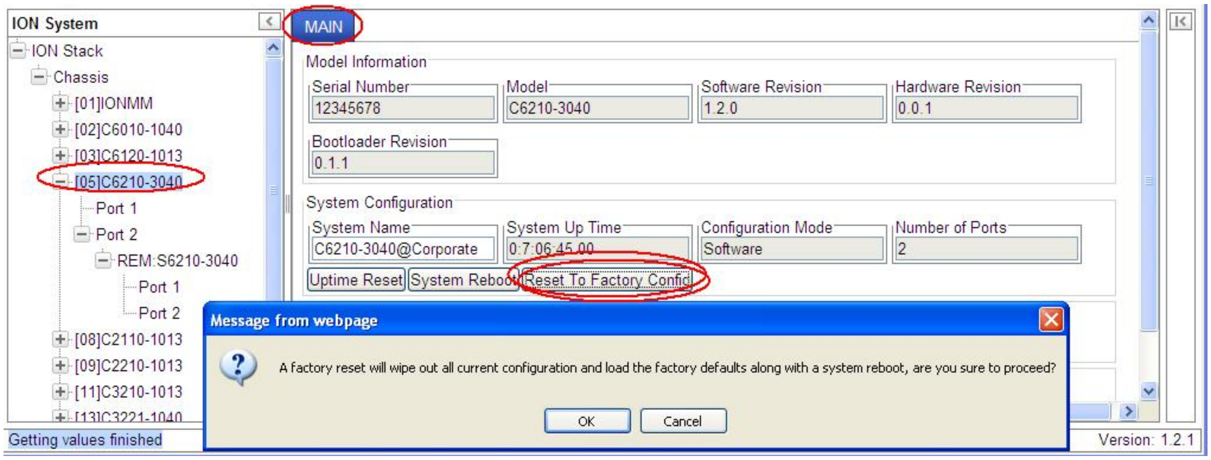
Press the **Cancel** button if you are not sure you want a system reboot to occur.
Press the **OK** button to clear the webpage message and begin the reboot process. The message "*Loading, please wait..*. displays.

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.



Model Information

Serial Number	Model	Software Revision	Hardware Revision
12345678	C6210-3040	1.2.0	0.0.1

Bootloader Revision: 0.1.1

System Configuration

System Name	System Up Time	Configuration Mode	Number of Ports
C6210-3040@Corporate	0:7:06:45.00	Software	2

Message from webpage

A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot, are you sure to proceed?

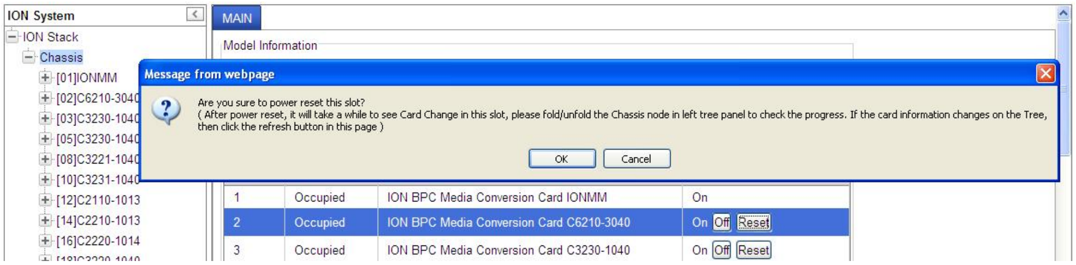
Getting values finished

Version: 1.2.1

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.



Message from webpage

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 left tree panel to check the progress. If the card information changes on the Tree, then click the refresh button in this page)

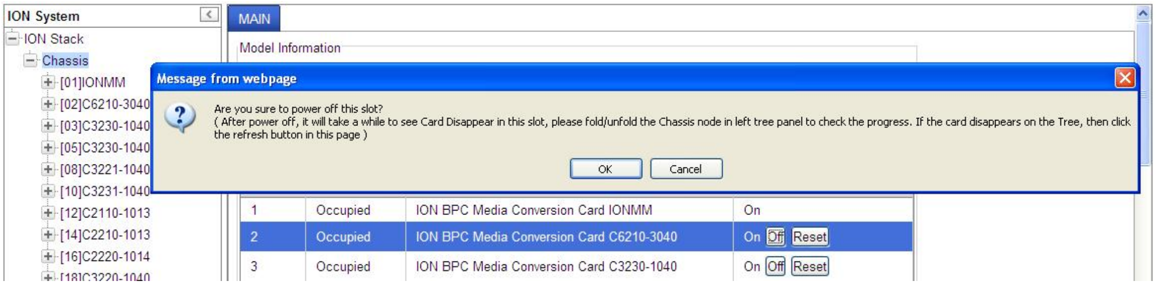
1	Occupied	ION BPC Media Conversion Card IONMM	On
2	Occupied	ION BPC Media Conversion Card C6210-3040	On Off Reset
3	Occupied	ION BPC Media Conversion Card C3230-1040	On Off Reset

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.



Are you sure 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 left tree panel to check the progress. If the card disappears on the Tree, then click the refresh button in this page)

1	Occupied	ION BPC Media Conversion Card IONMM	On
2	Occupied	ION BPC Media Conversion Card C6210-3040	On Off Reset
3	Occupied	ION BPC Media Conversion Card C3230-1040	On Off Reset

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.

Section 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: Transition Networks 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** can not 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>
```

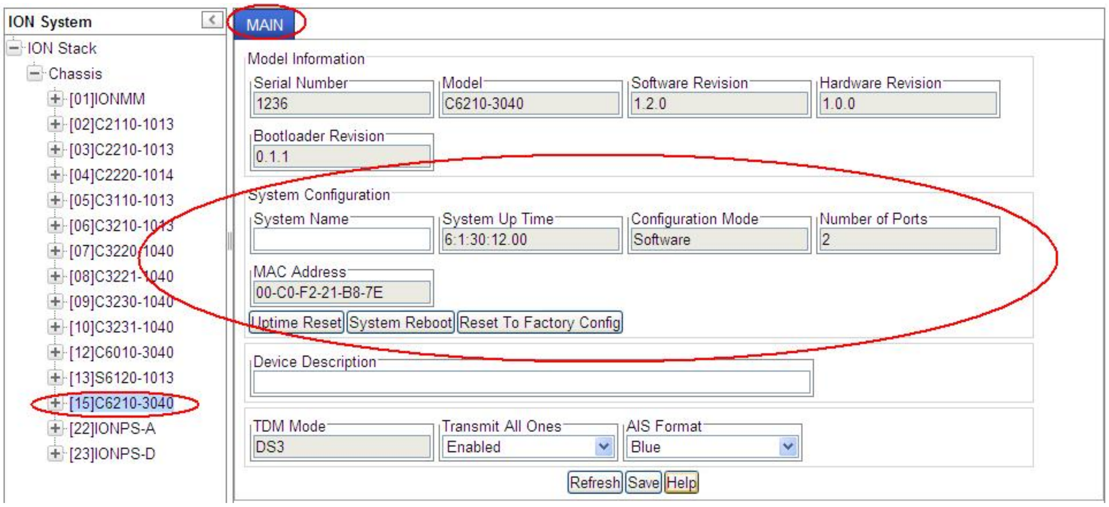
Note: the **show card info** command does not function for a Power Supply module.

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.



Model Information

Serial Number: 1236
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 1.0.0
Bootloader Revision: 0.1.1

System Configuration

System Name:
System Up Time: 6:1:30:12.00
Configuration Mode: Software
Number of Ports: 2
MAC Address: 00-C0-F2-21-B8-7E

Device Description:

TDM Mode: DS3
Transmit All Ones: Enabled
AIS Format: Blue

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** can not 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., 1.1.0 (read only field).
   Hardware Revision - e.g., 0.0.1 (read only field).
   Bootloader Revision - e.g., 0.1.1 (read only field).

   System Name – e.g., 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).
   Transmit All Ones: Enabled or Disabled (read/write field).
   AIS Format: 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:

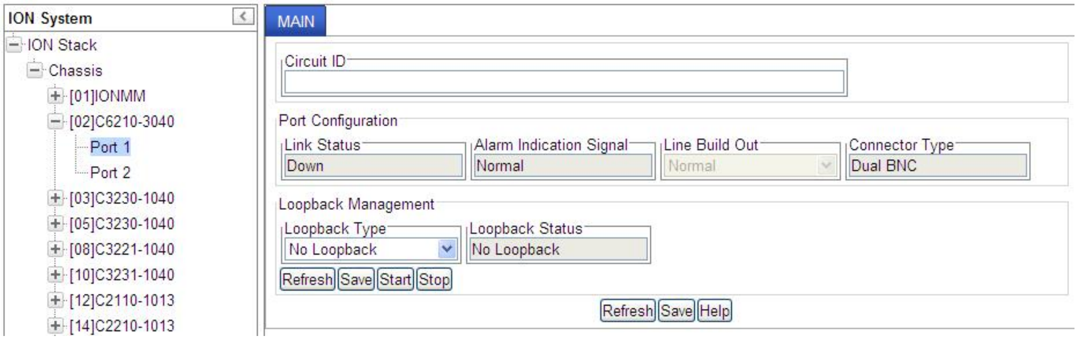
```
AgentIII C1|S3|L1D>set ais transmit=enable
AgentIII C1|S3|L1D>set ais format=blue
AgentIII C1|S3|L1D>set circuit-ID=xx/CD-FDB
AgentIII C1|S3|L1D>show tdm config
ais transmit:                                           enabled
ais format:                                             blue
tdm type:                                               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.



Circuit ID:

Port Configuration

Link Status: Down

Alarm Indication Signal: Normal

Line Build Out: Normal

Connector Type: Dual BNC

Loopback Management

Loopback Type: No Loopback

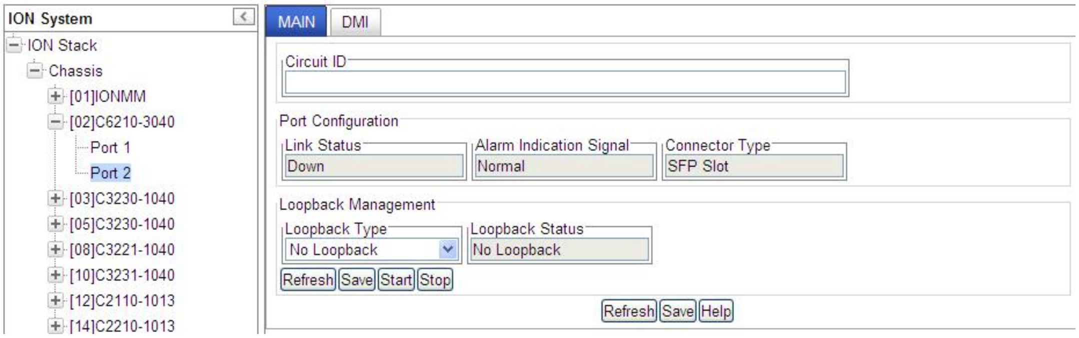
Loopback Status: No Loopback

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**.



Circuit ID:

Port Configuration

Link Status: Down

Alarm Indication Signal: Normal

Connector Type: SFP Slot

Loopback Management

Loopback Type: No Loopback

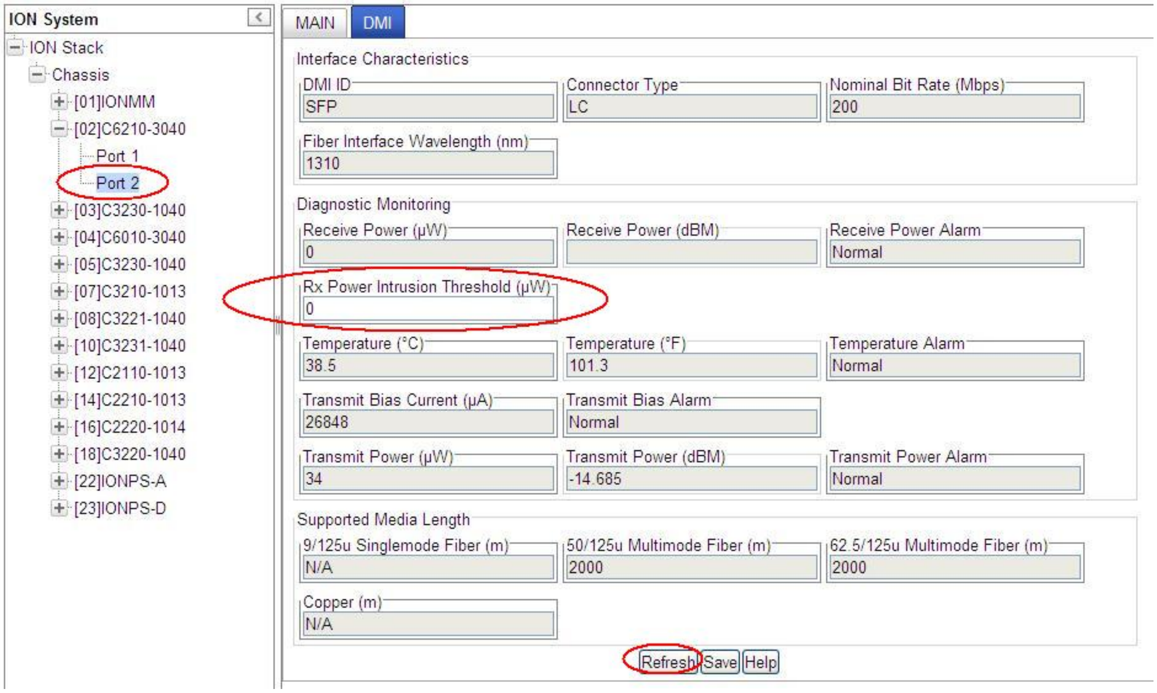
Loopback Status: No Loopback

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).



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

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 x6010 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 x6010 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**=s***top*** 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:

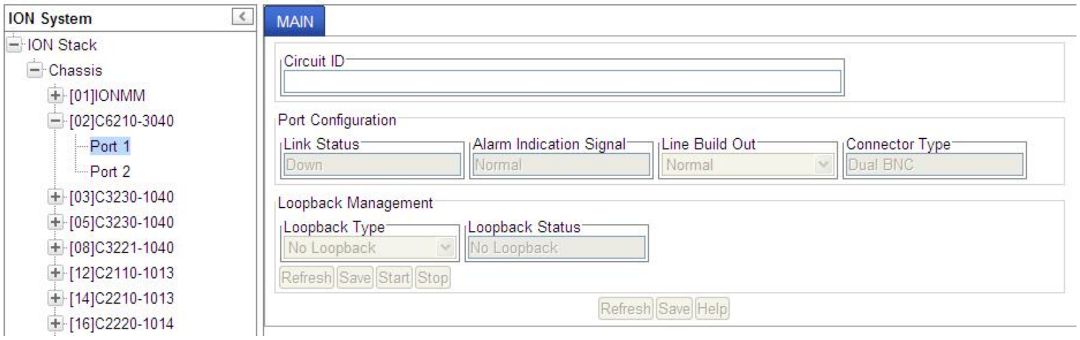
```
AgentIII C1|S3|L1D>show tdm config
ais transmit:                                          enabled
ais format:                                            allones
tdm type:                                              e3
AgentIII C1|S3|L1D>
```

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.



Circuit ID

Port Configuration

Link Status Down

Alarm Indication Signal Normal

Line Build Out Normal

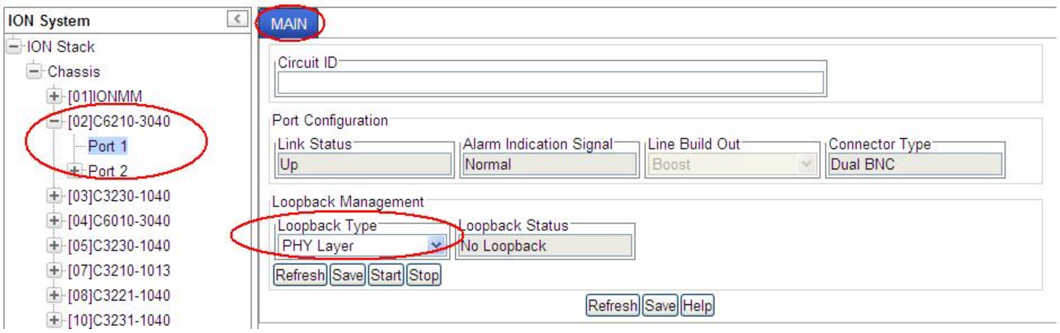
Connector Type Dual BNC

Loopback Management

Loopback Type No Loopback

Loopback Status No Loopback

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



Circuit ID

Port Configuration

Link Status Up

Alarm Indication Signal Normal

Line Build Out Boost

Connector Type Dual BNC

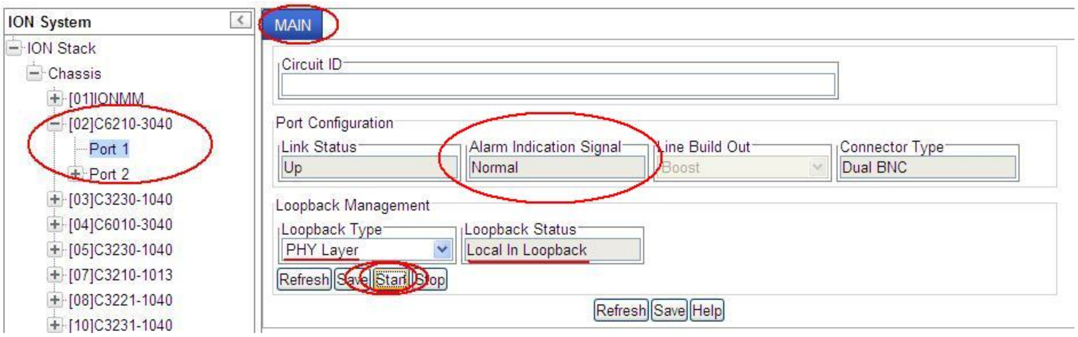
Loopback Management

Loopback Type PHY Layer

Loopback Status No Loopback

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.



Circuit ID

Port Configuration

Link Status Up

Alarm Indication Signal Normal

Line Build Out Boost

Connector Type Dual BNC

Loopback Management

Loopback Type PHY Layer

Loopback Status Local In Loopback

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:

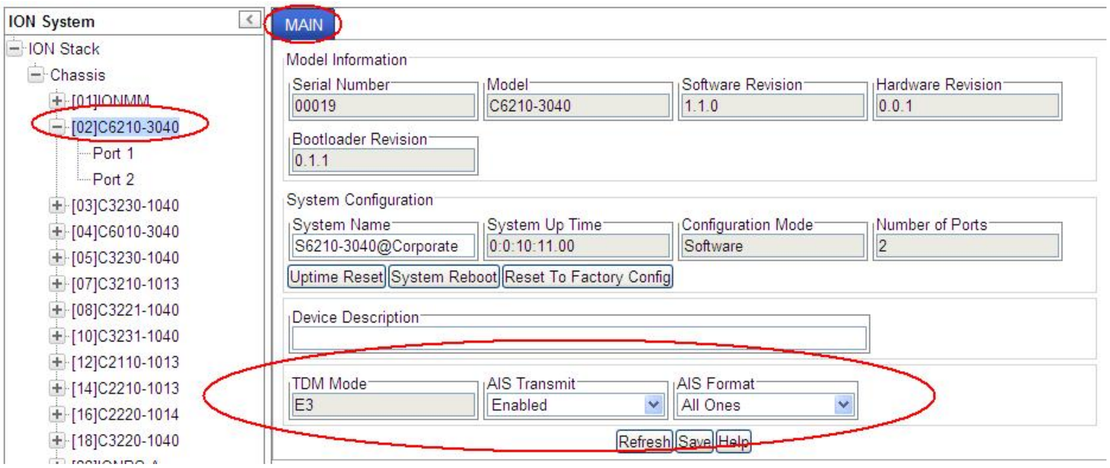
```
C1|S2|L1D>show tdm config
ais transmit:                                        enabled
ais format:                                          blue
tdm type:                                            e3
C1|S2|L1D>set ais transmit ?
  disable
  enable
C1|S2|L1D>
C1|S2|L1D>set ais format ?
  allones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



Model Information
Serial Number: 00019
Model: C6210-3040
Software Revision: 1.1.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration
System Name: S6210-3040@Corporate
System Up Time: 0:0:10:11.00
Configuration Mode: Software
Number of Ports: 2

Device Description:

TDM Mode: E3
AIS Transmit: Enabled
AIS Format: All Ones

3. Click the **Refresh** button if the **TDM Mode** field does not display **E3**.

4. If desired, enter a new **System Name**.

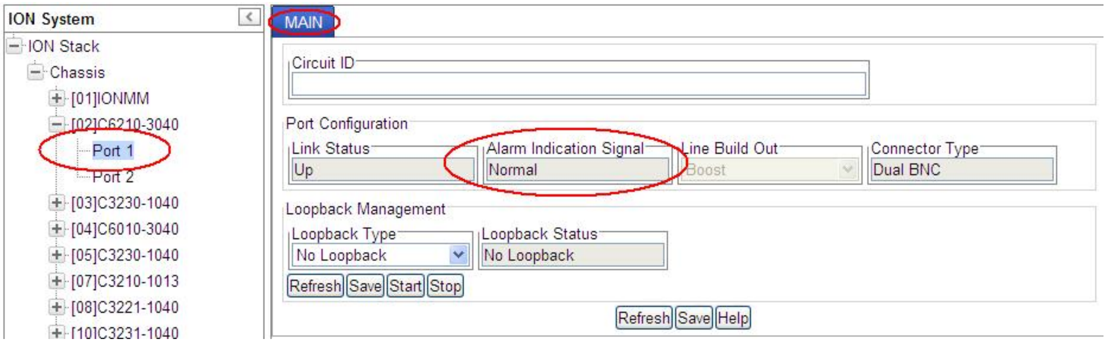
5. If required, enter a **Device Description** of up to 64 characters.

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**.



Circuit ID:

Port Configuration
Link Status: Up
Alarm Indication Signal: Normal
Line Build Out: Boost
Connector Type: Dual BNC

Loopback Management
Loopback Type: No Loopback
Loopback Status: No Loopback

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

Section 5: Operations

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: Transition Networks 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.

Transition Networks 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

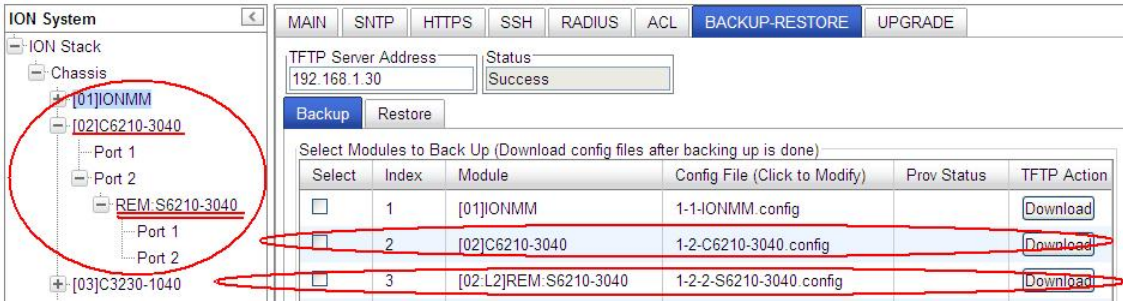
Doing a reboot, a restart or upgrade of the NID, a power restart of the chassis, or a reset to factory settings may cause some configuration backup files, HTTPS certification file, and Syslog file to be lost. Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset 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]C6010-3040** shown below). The second module listed is the standalone (remote) device (e.g., **[04:L2]REM:S6010-1040** shown below).



TFTP Server Address: 192.168.1.30

Status: Success

Select Modules to Back Up (Download config files after backing up is done)

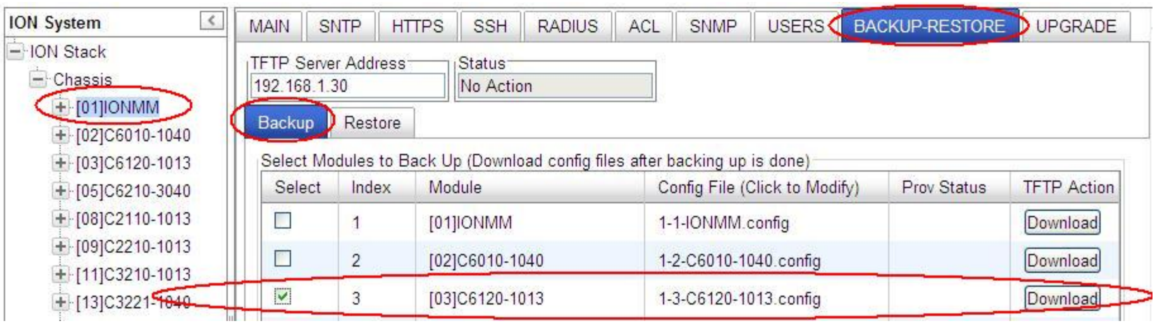
Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Download
□	2	[02]C6210-3040	1-2-C6210-3040.config		Download
□	3	[02:L2]REM:S6210-3040	1-2-2-S6210-3040.config		Download

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.



TFTP Server Address: 192.168.1.30

Status: No Action

Select Modules to Back Up (Download config files after backing up is done)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Download
□	2	[02]C6010-1040	1-2-C6010-1040.config		Download
☑	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.

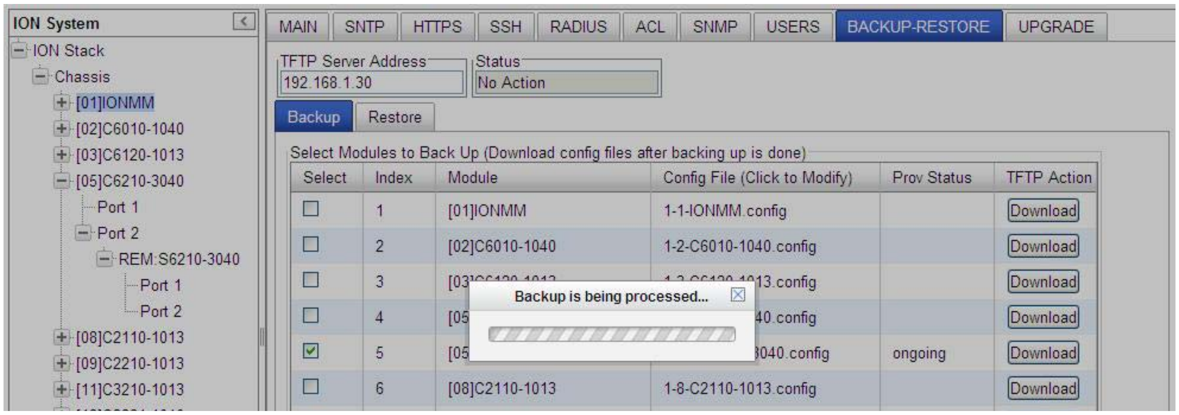
9. Click the **OK** button to clear the web page message.

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*).



TFTP Server Address: 192.168.1.30

Status: No Action

Select Modules to Back Up (Download config files after backing up is done)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Download
□	2	[02]C6010-1040	1-2-C6010-1040.config		Download
□	3	[03]C6120-1013	1-3-C6120-1013.config		Download
□	4	[05	40.config		Download
☑	5	[05	040.config	ongoing	Download
□	6	[08]C2110-1013	1-8-C2110-1013.config		Download

Backup is being processed...

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

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

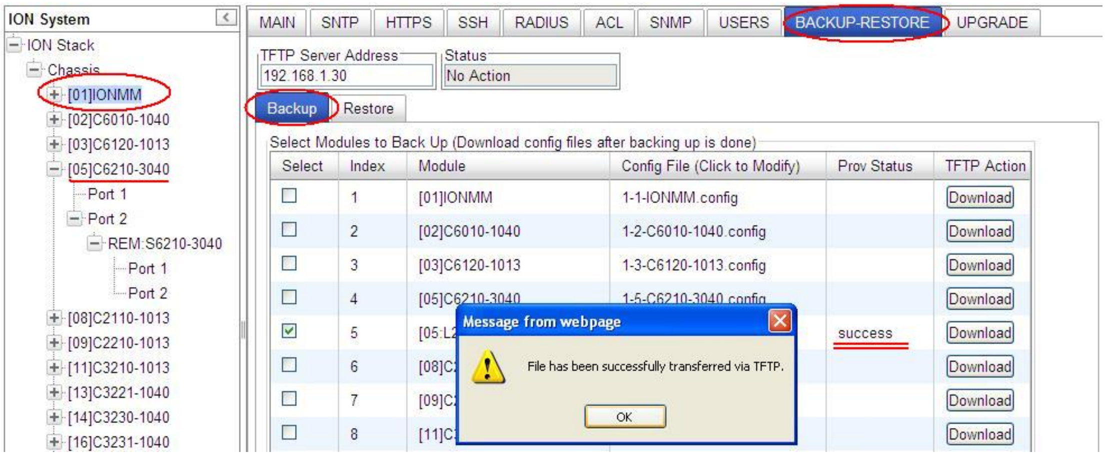
    a. Make sure the TFTP Server is running and configured.

    b. In the **TFTP Server Address** field, enter the IP address of the server.

    c. Click the **Download** button. The message "*File is being transferred*" displays.

    d. When the successful completion message displays, click **OK**. The TFTP Server now contains an emergency backup file for the module specified.

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



ION System
- ION Stack
  - Chassis
    - [01]IONMM
    - [02]C6010-1040
    - [03]C6120-1013
    - [05]C6210-3040
      - Port 1
      - Port 2
        - REM:S6210-3040
          - Port 1
          - Port 2
    - [08]C2110-1013
    - [09]C2210-1013
    - [11]C3210-1013
    - [13]C3221-1040
    - [14]C3230-1040
    - [16]C3231-1040

TFTP Server Address: 192.168.1.30

Status: No Action

Select Modules to Back Up (Download config files after backing up is done)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Download
□	2	[02]C6010-1040	1-2-C6010-1040.config		Download
□	3	[03]C6120-1013	1-3-C6120-1013.config		Download
□	4	[05]C6210-3040	1-5-C6210-3040.config		Download
☑	5	[05:L2		success	Download
□	6	[08]C			Download
□	7	[09]C			Download
□	8	[11]C			Download

Message from webpage

File has been successfully transferred via TFTP.

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 397 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

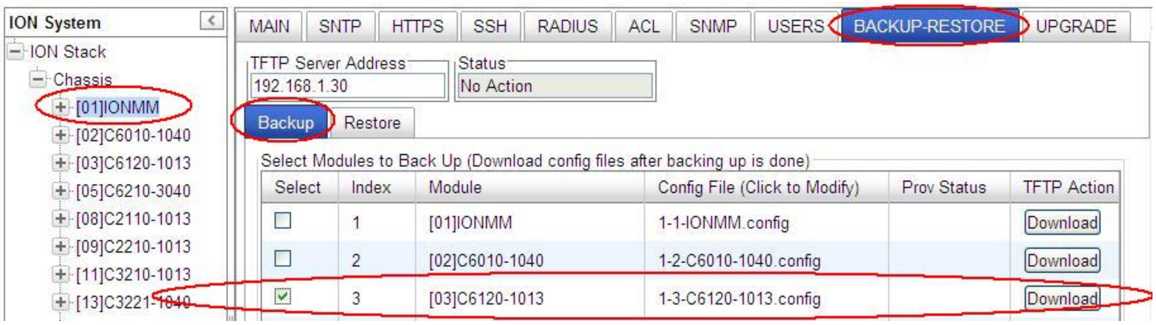
The following procedure describes how to back up the configuration of a standalone module.

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.



TFTP Server Address: 192.168.1.30

Status: No Action

Select Modules to Back Up (Download config files after backing up is done)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Download
□	2	[02]C6010-1040	1-2-C6010-1040.config		Download
☑	3	[03]C6120-1013	1-3-C6120-1013.config		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

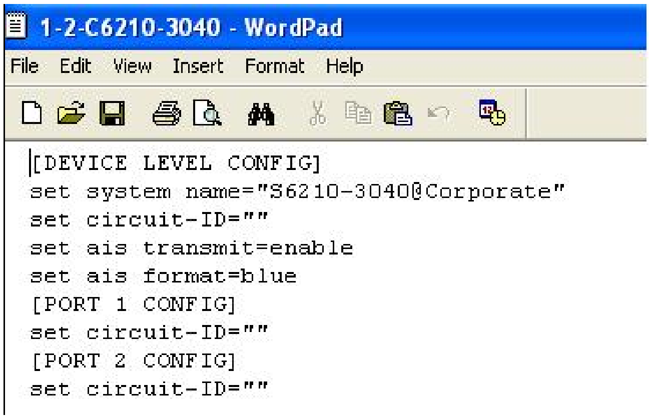
Editing the Config File (Optional)

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- C6010-1040.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.



```
[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.

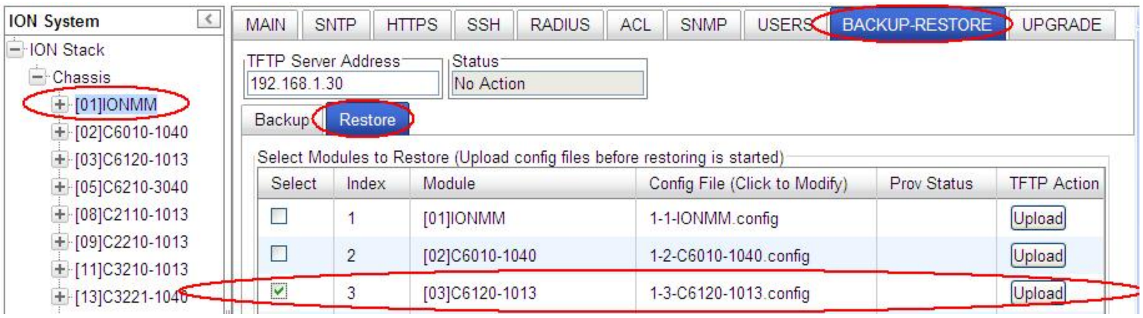
Note: these Restore procedures require that the TFTP server be running and properly configured, and that the backup configuration file is named and located properly.

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.



TFTP Server Address: 192.168.1.30
Status: No Action

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Upload
□	2	[02]C6010-1040	1-2-C6010-1040.config		Upload
☑	3	[03]C6120-1013	1-3-C6120-1013.config		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.*"

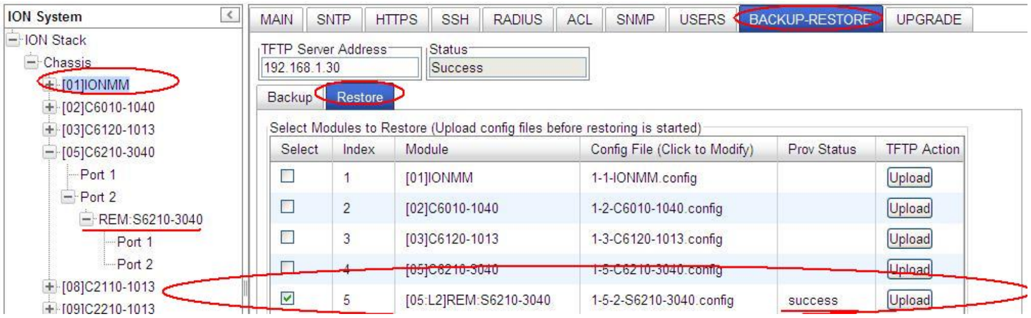
8. Click the **OK** button to clear the Webpage message.

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.



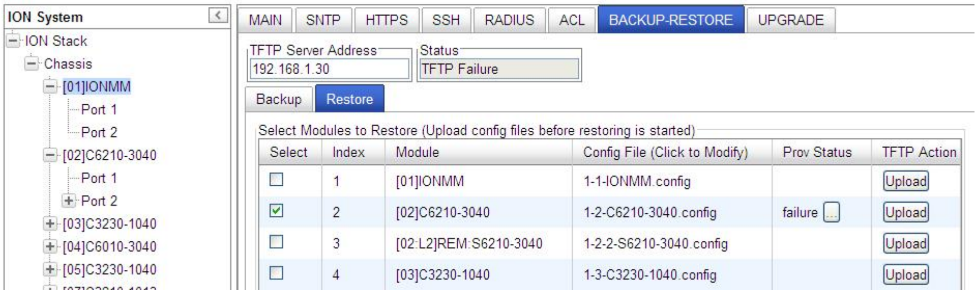
TFTP Server Address: 192.168.1.30

Status: Success

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Upload
□	2	[02]C6010-1040	1-2-C6010-1040.config		Upload
□	3	[03]C6120-1013	1-3-C6120-1013.config		Upload
□	4	[05]C6210-3040	1-5-C6210-3040.config		Upload
☑	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.



TFTP Server Address: 192.168.1.30

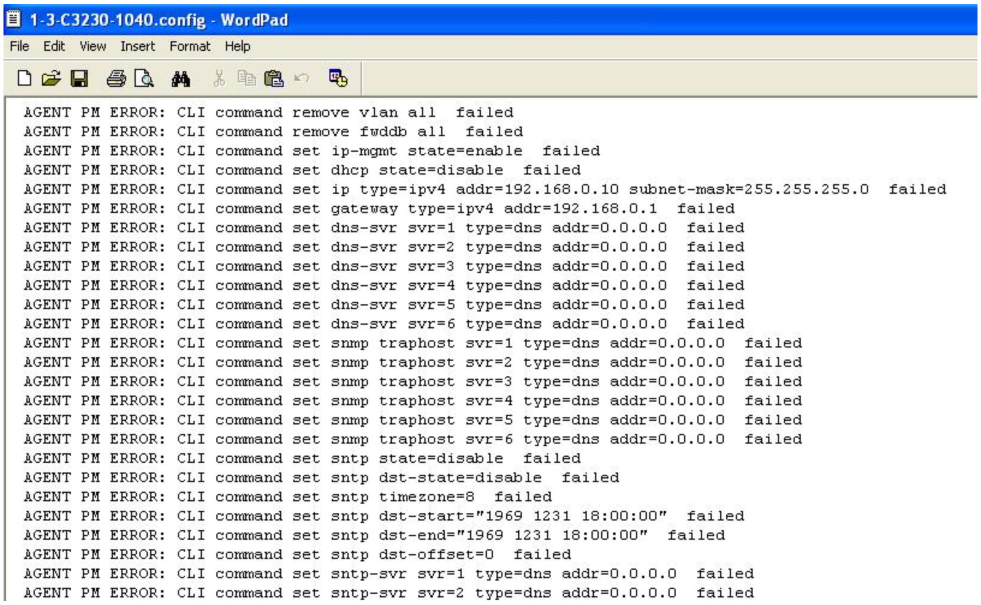
Status: TFTP Failure

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Upload
☑	2	[02]C6210-3040	1-2-C6210-3040.config	failure □	Upload
□	3	[02:L2]REM:S6210-3040	1-2-2-S6210-3040.config		Upload
□	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.



```
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 sntp state=disable  failed
AGENT PM ERROR: CLI command set sntp dst-state=disable  failed
AGENT PM ERROR: CLI command set sntp timezone=8  failed
AGENT PM ERROR: CLI command set sntp dst-start="1969 1231 18:00:00"  failed
AGENT PM ERROR: CLI command set sntp dst-end="1969 1231 18:00:00"  failed
AGENT PM ERROR: CLI command set sntp dst-offset=0  failed
AGENT PM ERROR: CLI command set sntp-svr svr=1 type=dns addr=0.0.0.0  failed
AGENT PM ERROR: CLI command set sntp-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.

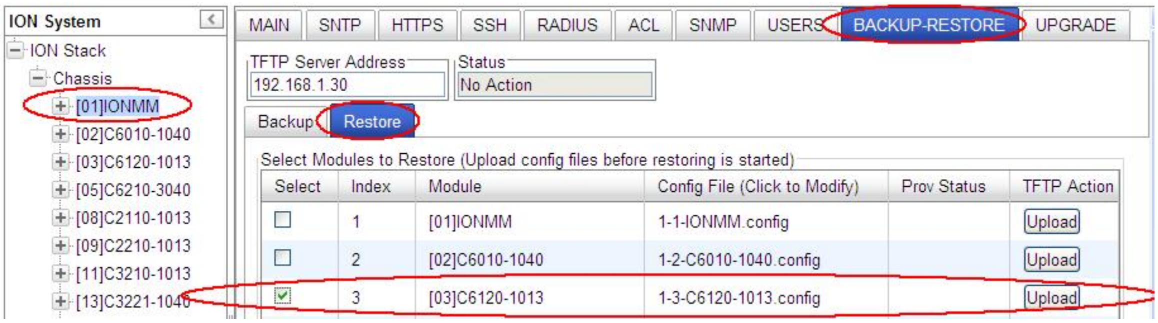
IMPORTANT

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.



TFTP Server Address: 192.168.1.30

Status: No Action

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
☐	1	[01]IONMM	1-1-IONMM.config		Upload
☐	2	[02]C6010-1040	1-2-C6010-1040.config		Upload
☑	3	[03]C6120-1013	1-3-C6120-1013.config		Upload

4. In the **Select** column, check the checkbox of the module to be restored.

5. Is the configuration file to be restored different than the one shown in the **Config File** column?

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

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.

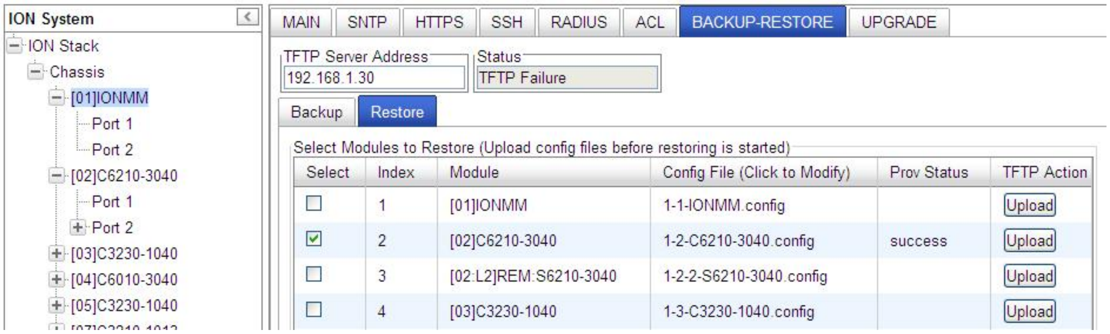
7. Click the **Upload** button. The config file is uploaded via the TFTP server. When done, the message "*File has been successfully transferred via TFTP*."

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.

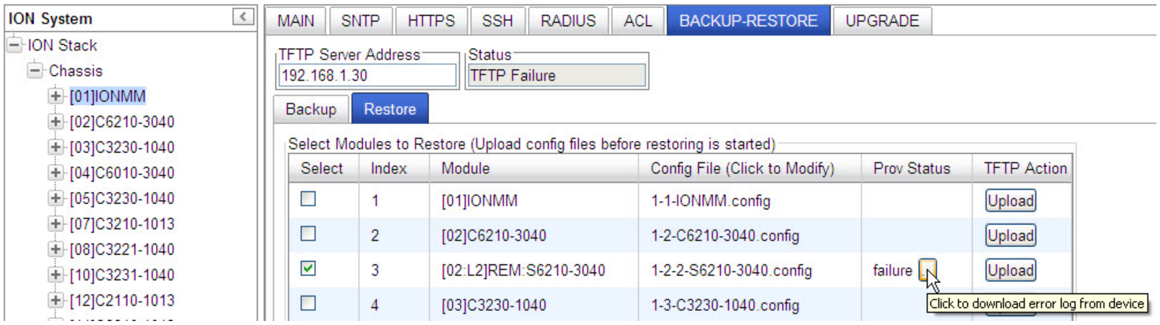


TFTP Server Address: 192.168.1.30
Status: TFTP Failure

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Upload
☑	2	[02]C6210-3040	1-2-C6210-3040.config	success	Upload
□	3	[02:L2]REM:S6210-3040	1-2-2-S6210-3040.config		Upload
□	4	[03]C3230-1040	1-3-C3230-1040.config		Upload

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



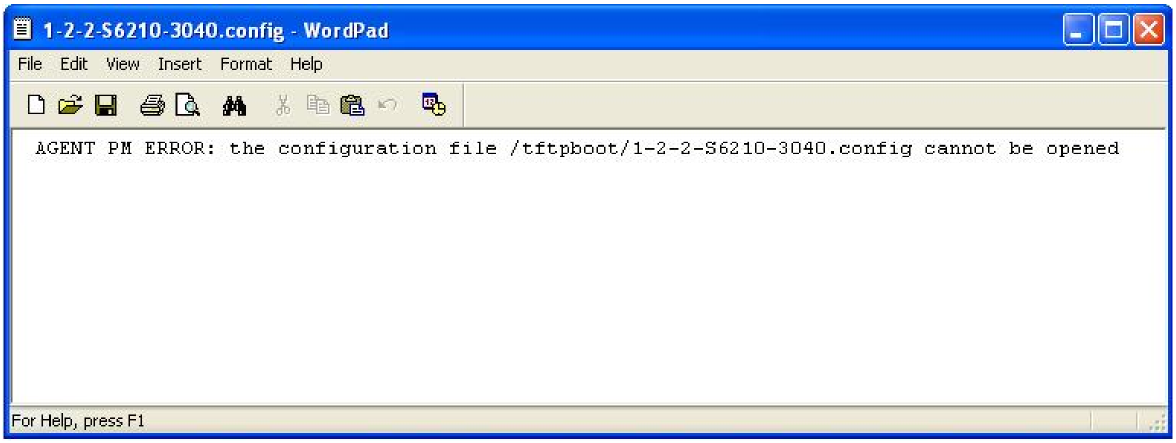
TFTP Server Address: 192.168.1.30
Status: TFTP Failure

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
□	1	[01]IONMM	1-1-IONMM.config		Upload
□	2	[02]C6210-3040	1-2-C6210-3040.config		Upload
☑	3	[02:L2]REM:S6210-3040	1-2-2-S6210-3040.config	failure ...	Upload
□	4	[03]C3230-1040	1-3-C3230-1040.config		

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.



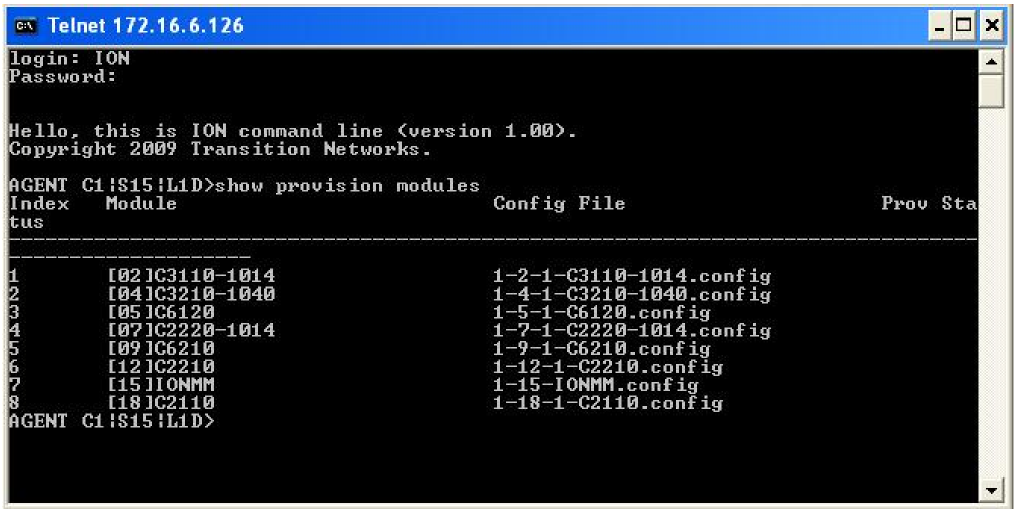
```
AGENT PM ERROR: the configuration file /tftpboot/1-2-2-S6210-3040.config cannot be opened
```

See "The Config Error Log (config.err) File" on page 353 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:



```
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>
```

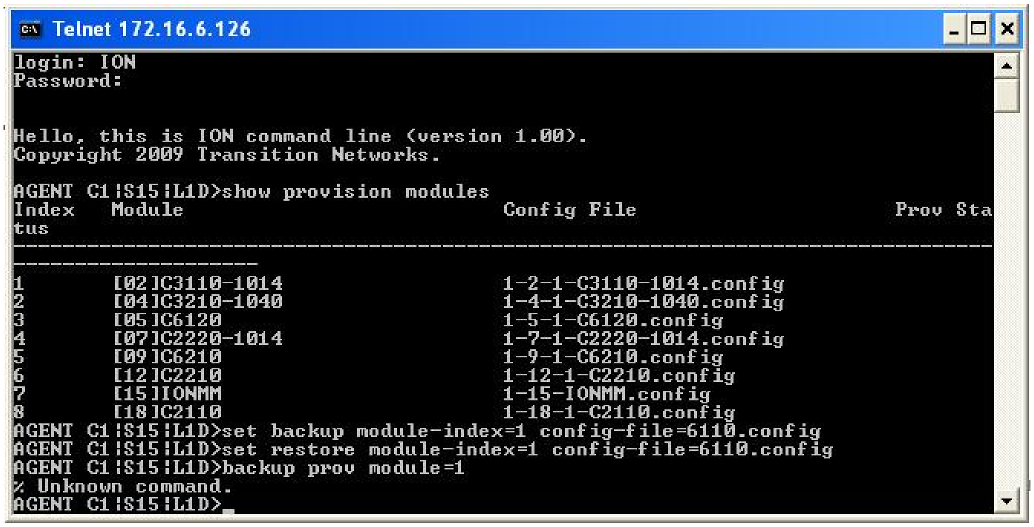
3. Set the Provision module backup configuration.
   Type **set backup module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.

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:



```
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	/tftpboot	Yes - these files are created during Backup operation	No
MIB configuration files	e.g., ‘agent3.conf ’ ‘ifMib.conf ’	The MIB configuration files for SNMP setting	/agent3/conf	No - not needed; the configurations included in this file will be backed up by SNMP set operations	Yes

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 displays:

   ```
   Warning: this command will restart the specified card, connection will be
      lost!
   C1|S2|L1D>
   ```

   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.

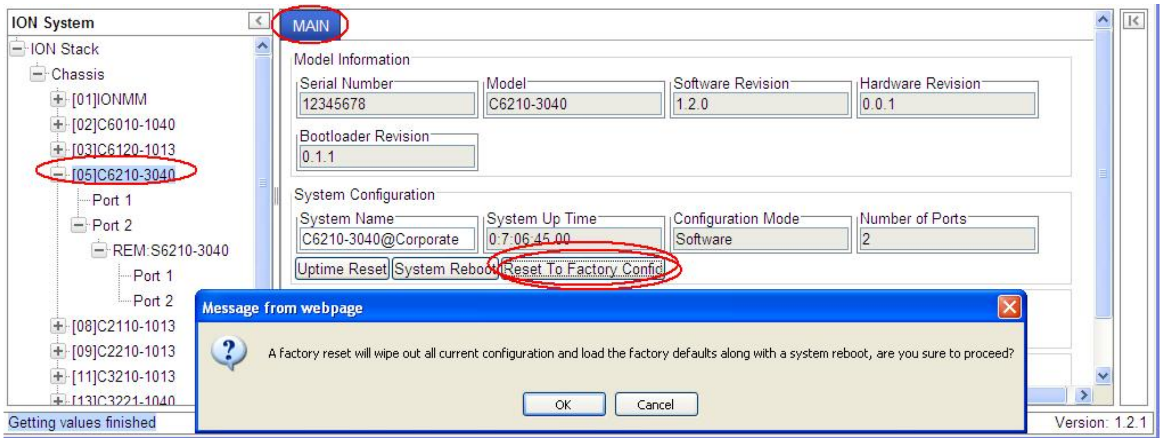
Resetting Defaults – Web Method

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.



Model Information

Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

System Name: C6210-3040@Corporate
System Up Time: 0:7:06:45.00
Configuration Mode: Software
Number of Ports: 2

Message from webpage

A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot, are you sure to proceed?

Getting values finished

Version: 1.2.1

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>
```

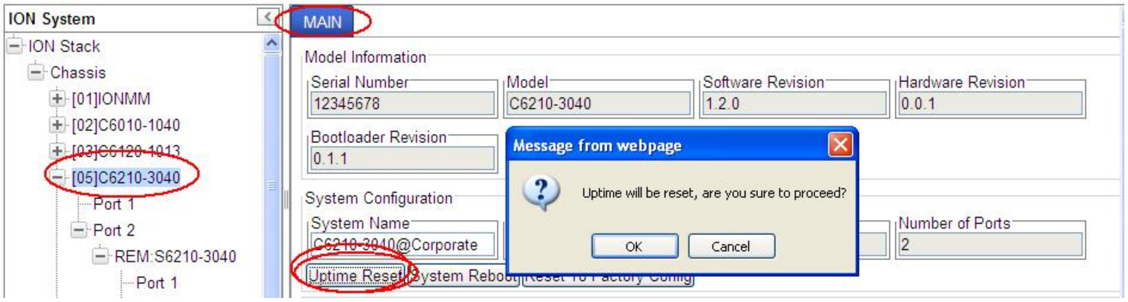
Use the **show card info** command to display the current system uptime.
Note: The **reset uptime** command is not available for all ION system devices.

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.



Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1
System Name: C6210-3040@Corporate
Number of Ports: 2

Message from webpage

Uptime will be reset, are you sure to proceed?

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 S6110 (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

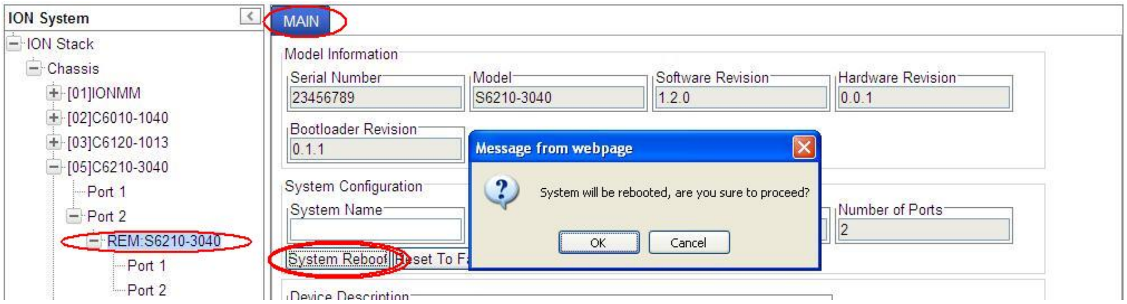
Caution: Doing a system reboot will cause all configuration backup files, HTTPS certification file, and Syslog file to be lost.

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.



Serial Number: 23456789
Model: S6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1
System Name:
Number of Ports: 2

Message from webpage

System will be rebooted, are you sure to proceed?

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 Restore	/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: Transition Networks 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: http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx. 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 can not 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 Transition Networks Software Upgrades web page at http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx.

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**.

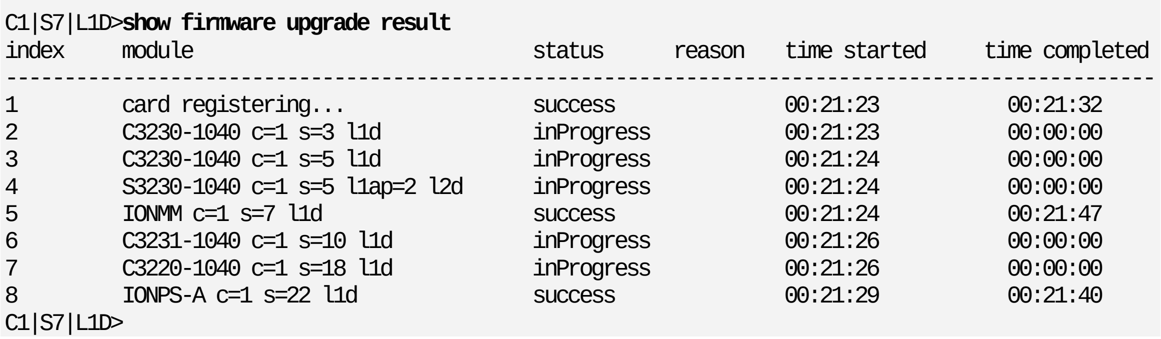
10. Upgrade the module. Type **upgrade module** and press **Enter**.

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             00:21:23        00:21:32
2        C3230-1040 c=1 s=3 l1d         inProgress          00:21:23        00:00:00
3        C3230-1040 c=1 s=5 l1d         inProgress          00:21:24        00:00:00
4        S3230-1040 c=1 s=5 l1ap=2 l2d  inProgress          00:21:24        00:00:00
5        IONMM c=1 s=7 l1d              success             00:21:24        00:21:47
6        C3231-1040 c=1 s=10 l1d        inProgress          00:21:26        00:00:00
7        C3220-1040 c=1 s=18 l1d        inProgress          00:21:26        00:00:00
8        IONPS-A c=1 s=22 l1d           success             00:21:29        00:21:40
C1|S7|L1D>
```

If a module upgrade was unsuccessful, the reason for the failure displays in the "reason" column of the table (e.g., *invalid input file*, *protocol timeout*). See "Section 5 – Troubleshooting" 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 Transition Networks Software Upgrades web page at http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx.
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 can not 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.

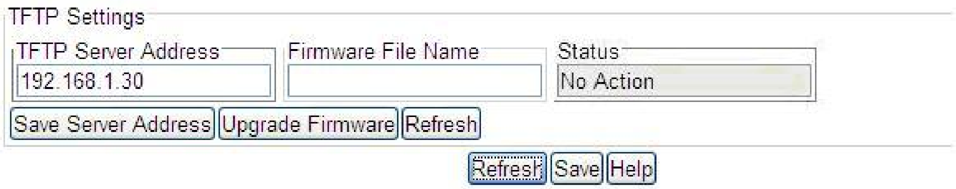
D. Upgrade the IONMM / NID Firmware

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.



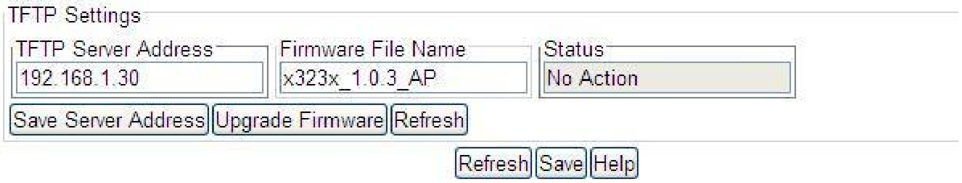
TFTP Settings

TFTP Server Address: 192.168.1.30

Firmware File Name:

Status: No Action

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

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.

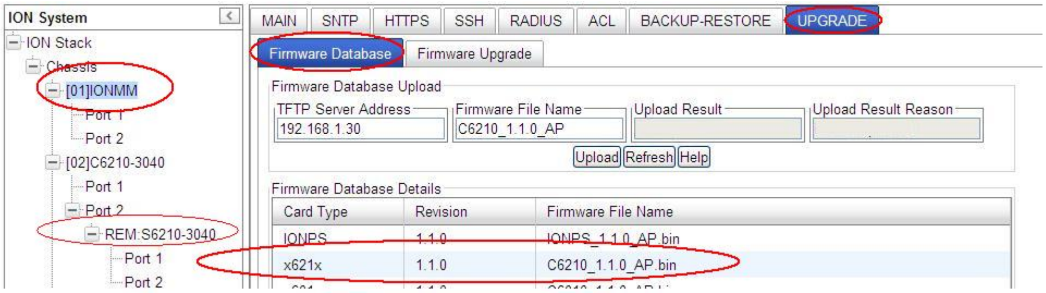
D2. Upgrade IONMM / NID Firmware from the **UPGRADE** Tab

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.



Firmware Database Upload

TFTP Server Address: 192.168.1.30
Firmware File Name: C6210_1.1.0_AP
Upload Result:
Upload Result Reason:

Firmware Database Details

Card Type	Revision	Firmware File Name
IONPS	1.1.0	IONPS_1.1.0_AP.bin
x621x	1.1.0	C6210_1.1.0_AP.bin

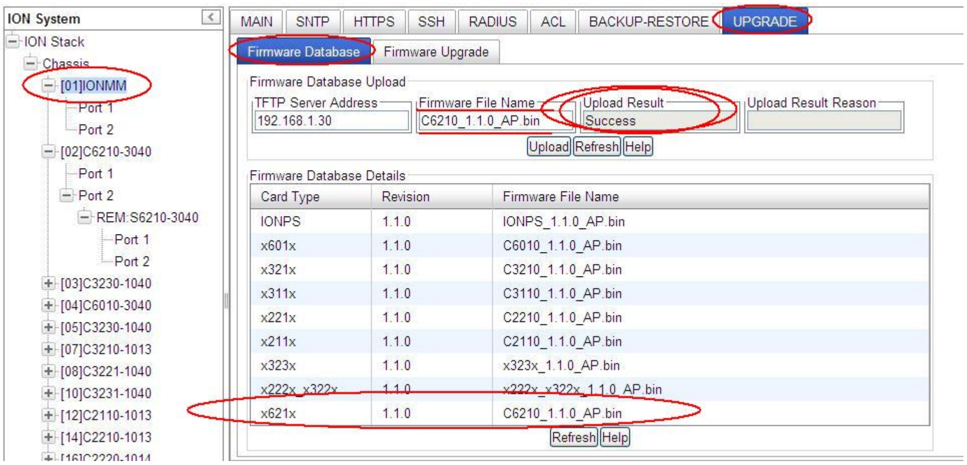
5. Enter the **TFTP Server Address.** This is the IP address of the TFTP Server from step C ("Run TFTP Server") above.

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.



Firmware Database Upload

TFTP Server Address: 192.168.1.30
Firmware File Name: C6210_1.1.0_AP.bin
Upload Result: Success
Upload Result Reason:

Firmware Database Details

Card Type	Revision	Firmware File Name
IONPS	1.1.0	IONPS_1.1.0_AP.bin
x601x	1.1.0	C6010_1.1.0_AP.bin
x321x	1.1.0	C3210_1.1.0_AP.bin
x311x	1.1.0	C3110_1.1.0_AP.bin
x221x	1.1.0	C2210_1.1.0_AP.bin
x211x	1.1.0	C2110_1.1.0_AP.bin
x323x	1.1.0	x323x_1.1.0_AP.bin
x222x_x322x	1.1.0	x222x_x322x_1.1.0_AP.bin
x621x	1.1.0	C6210_1.1.0_AP.bin

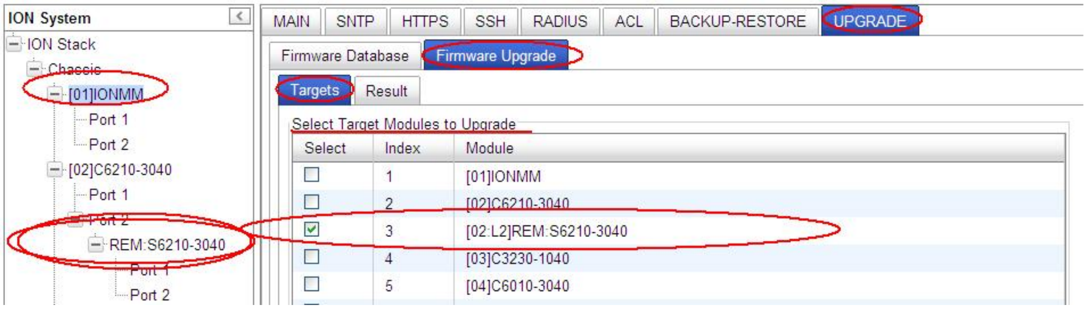
8. If the firmware upload operation failed, the **Upload Result** area displays either:

   - **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.



Select Target Modules to Upgrade

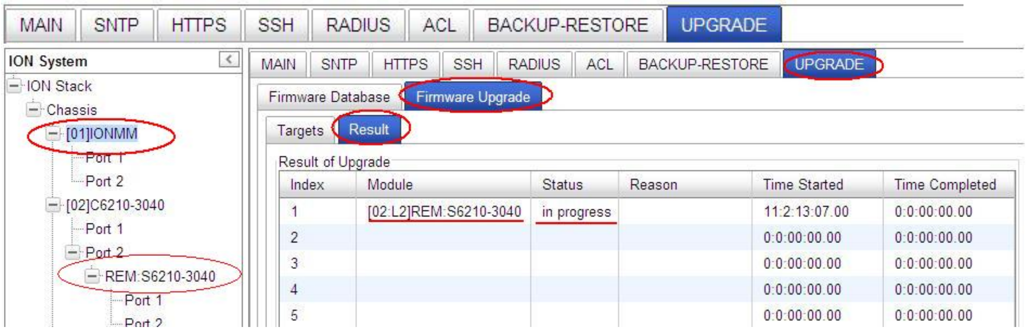
Select	Index	Module
☐	1	[01]IONMM
☐	2	[02]C6210-3040
☑	3	[02:L2]REM:S6210-3040
☐	4	[03]C3230-1040
☐	5	[04]C6010-3040

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.

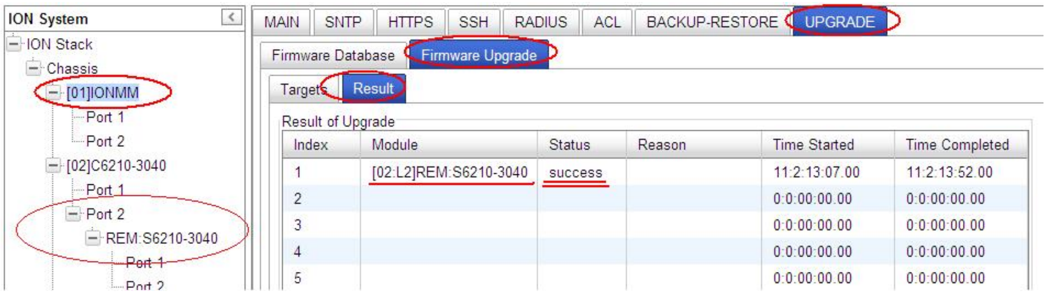
14. Click the **Result** sub-tab. A table displays with upgrade status information.



Result of Upgrade

Index	Module	Status	Reason	Time Started	Time Completed
1	[02:L2]REM:S6210-3040	in progress		11:2:13:07.00	0:0:00:00.00
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

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



Result of Upgrade

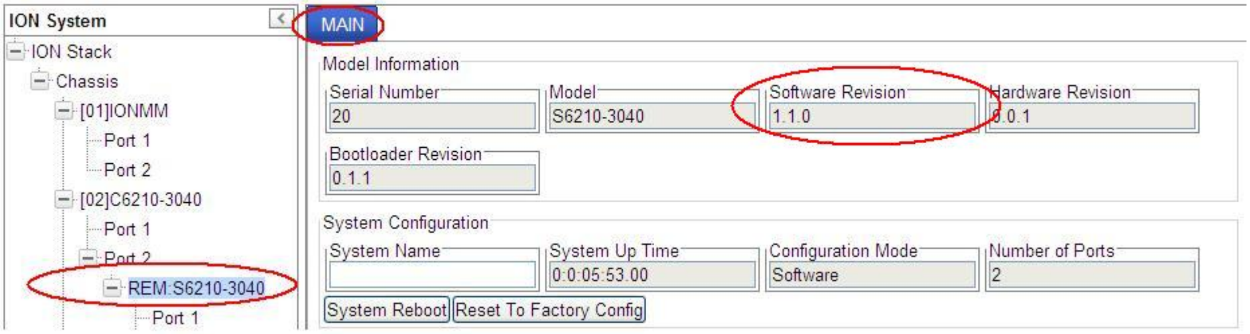
Index	Module	Status	Reason	Time Started	Time Completed
1	[02:L2]REM:S6210-3040	success		11:2:13:07.00	11:2:13:52.00
2				0:0:00:00.00	0:0:00:00.00
3				0:0:00:00.00	0:0:00:00.00
4				0:0:00:00.00	0:0:00:00.00
5				0:0:00:00.00	0:0:00:00.00

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.



Model Information

Serial Number: 20
Model: S6210-3040
Software Revision: 1.1.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

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

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: http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx.
- 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.

```
IONMM        1.1.0   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

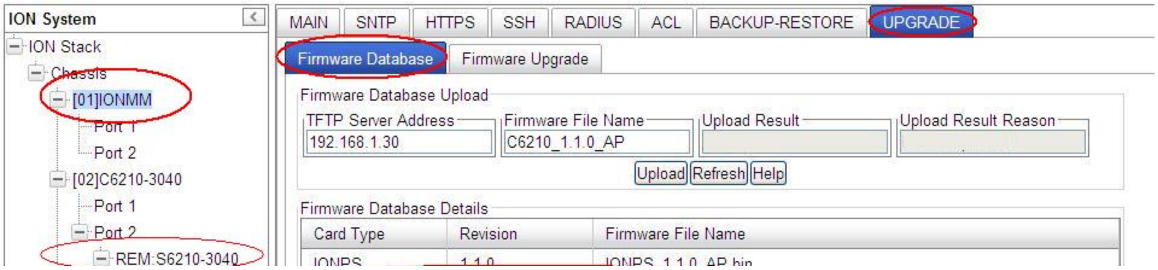
5. Perform the upgrade (see Performing the Module Firmware Upgrade below).

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.



Firmware Database Upload

TFTP Server Address: 192.168.1.30

Firmware File Name: C6210_1.1.0_AP

Upload Result:

Upload Result Reason:

Firmware Database Details

Card Type	Revision	Firmware File Name
IONPS	1.1.0	IONPS_1.1.0_AP.bin

3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP Server where the upgrade (zip) file is located.

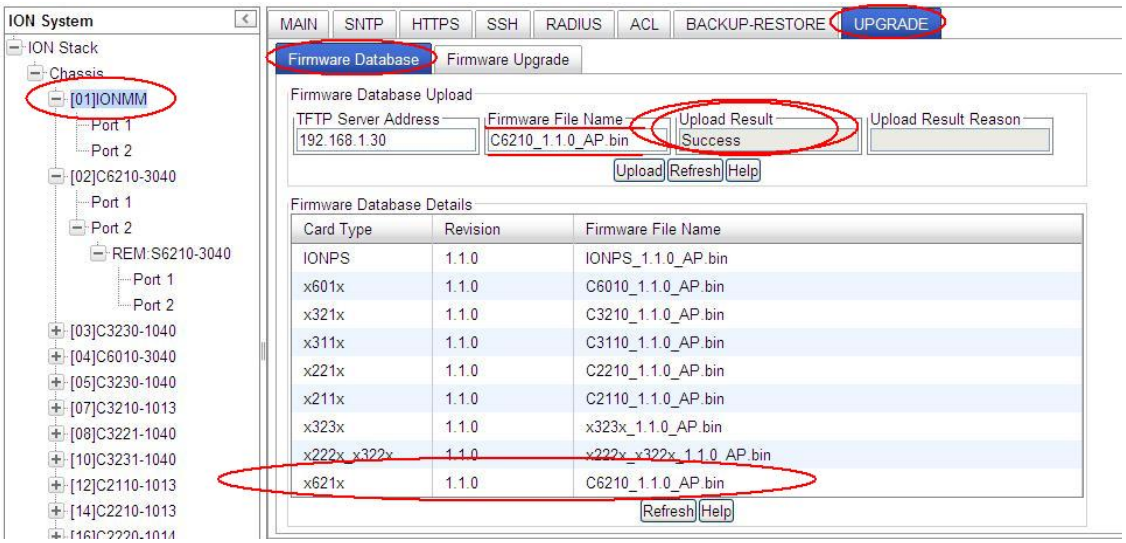
4. In the **Firmware File Name** field, enter the name of the zip file you created (e.g., **C6210.bin0.6.5.zip**). **Note**: Be sure to include the .zip extension in the filename.

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.



Firmware Database Upload

TFTP Server Address: 192.168.1.30

Firmware File Name: C6210_1.1.0_AP.bin

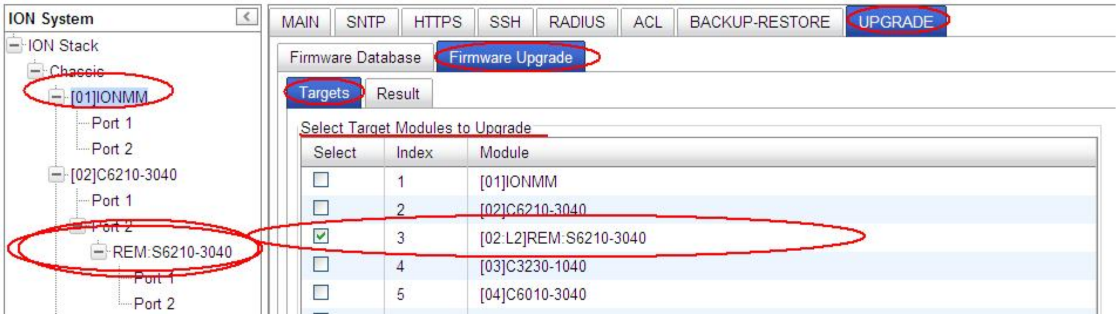
Upload Result: Success

Upload Result Reason:

Firmware Database Details

Card Type	Revision	Firmware File Name
IONPS	1.1.0	IONPS_1.1.0_AP.bin
x601x	1.1.0	C6010_1.1.0_AP.bin
x321x	1.1.0	C3210_1.1.0_AP.bin
x311x	1.1.0	C3110_1.1.0_AP.bin
x221x	1.1.0	C2210_1.1.0_AP.bin
x211x	1.1.0	C2110_1.1.0_AP.bin
x323x	1.1.0	x323x_1.1.0_AP.bin
x222x_x322x	1.1.0	x222x_x322x_1.1.0_AP.bin
x621x	1.1.0	C6210_1.1.0_AP.bin

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



Select Target Modules to Upgrade

Select	Index	Module
☐	1	[01]IONMM
☐	2	[02]C6210-3040
☑	3	[02:L2]REM:S6210-3040
☐	4	[03]C3230-1040
☐	5	[04]C6010-3040

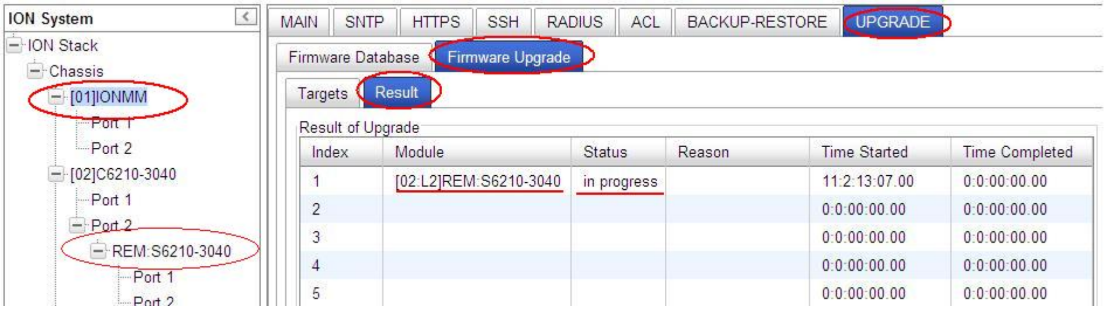
8. In the **Select** column, check the checkbox of each module to be upgraded.

   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**.

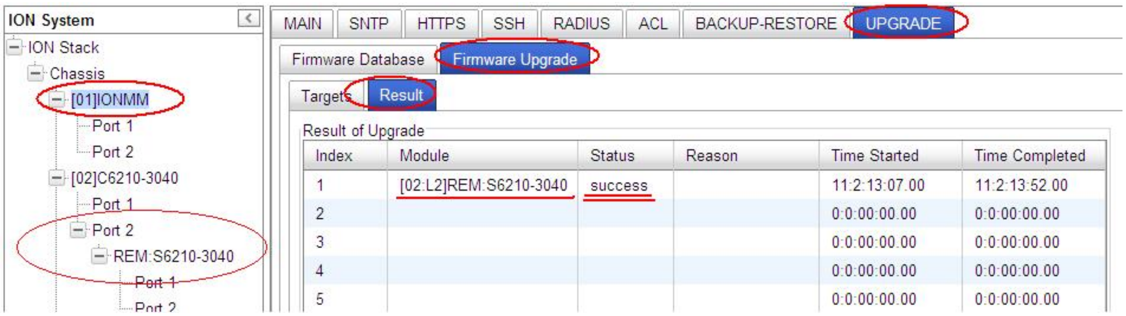
11. To monitor the progress, select the **Result** sub-tab and click **Refresh**.



Result of Upgrade

Index	Module	Status	Reason	Time Started	Time Completed
1	[02:L2]REM:S6210-3040	in progress		11:2:13:07.00	0:0:00:00.00
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

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



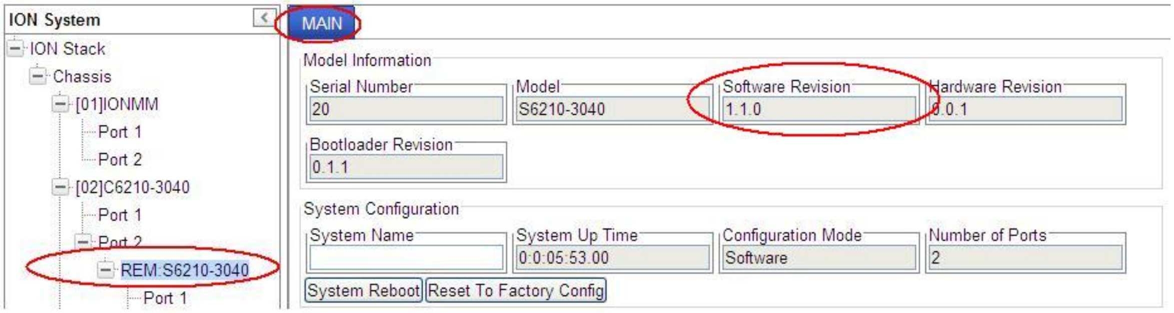
Result of Upgrade

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.

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



Model Information

Serial Number: 20

Model: S6210-3040

Software Revision: 1.1.0

Hardware Revision: 0.0.1

Bootloader Revision: 0.1.1

System Configuration

System Name:

System Up Time: 0:0:05:53.00

Configuration Mode: Software

Number of Ports: 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:

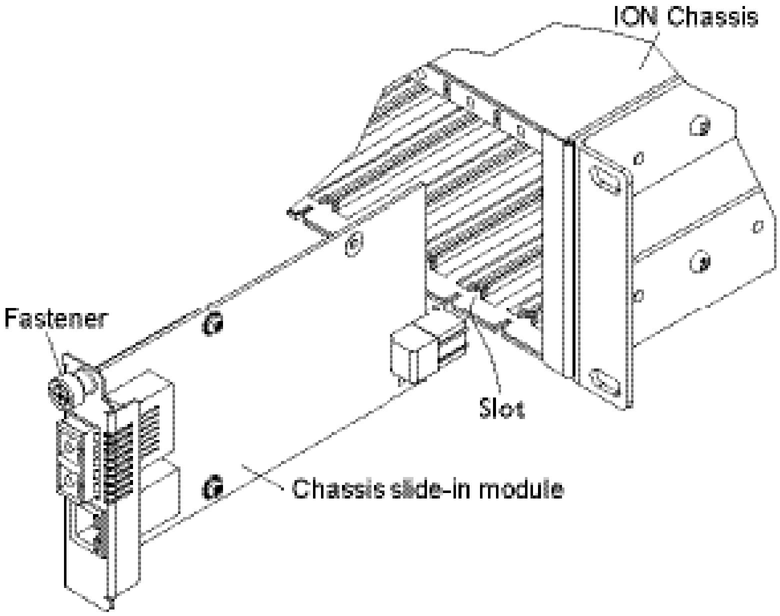
- Upgrade the IONMM and/or NID Firmware.
- Upgrade Slide-In and Remote Modules Firmware via TFTP. This procedure is used to upgrade one or more of the slide-in modules installed in the ION Chassis or a remote module connected to a slide-in module. Requires you to 1) Create Database Index and Archive 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).

Section 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 Transition Networks.

AgentIII C1|S1|L1D>
```

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

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

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

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

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

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

6. Enter CLI commands to set up, configure, operate, and maintain the 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: **Go to another location**

Syntax: **go** <location string>

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

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

Example:

```
AgentIII C1|S3|L1P2>go
Error location parameter number!
Usage: 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)
AgentIII C1|S3|L1P2>go c=1 s=4 l1d
AgentIII C1|S4|L1D>go l1p=1
AgentIII C1|S4|L1P1>go l1p=2
AgentIII C1|S4|L1P2>go c=1 s=3 l1p=1
AgentIII C1|S3|L1P1>
```

Command: **Show DMI Information**

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

Description: A port-level command that displays the Diagnostic Monitoring Interface (DMI) information (the DMI table) for a fiber port (port 2 only)

Example:

```
AgentIII C1|S3|L1P1>show dmi info
DMI is only supported on FIBER port!
AgentIII C1|S3|L1P1>go l1d
AgentIII C1|S3|L1D>show dmi info
Error: this command should be executed on a port!
AgentIII C1|S3|L1D>go l1p=2
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:                                       40.9*C
DMI temperature:                                       105.6*F
DMI temperature alarm:                                 normal
DMI transmit bias current:                             4752*uA
DMI transmit bais alarm:                               normal
DMI Transmit power:                                    252*uW
DMI Transmit power:                                    -5.986*dBM
DMI Transmit power alarm:                              normal
DMI Receive power:                                     0*uW
DMI Receive power alarm:                               normal
DMI Receive power intrusion threshold:                 0*uW
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: 1.3.6.1.2.1.31.1.1.1.18.

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]  C6010-1040
                        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 iptyp**e=<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 Transition Networks.

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
44. 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.

Section 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 200), check T1 Error Events and Alarm Conditions (page 224).

7. Verify that the TN product supports the function you are trying to perform. Your particular TN 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 fixe 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 TN for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED fault and Activity displays (page 142)
- Problem Conditions (page 143)
- CLI Messages (page 156)
- Web Interface Messages (page 159)
- Webpage Messages (page 167)
- Config Error Log (config.err File) Messages (page 174)
- Third Party Tool Messages (HyperTerminal, Ping, and Telnet Messages) (page 182)
- T1 Error Events and Alarm Conditions (page 231)

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):

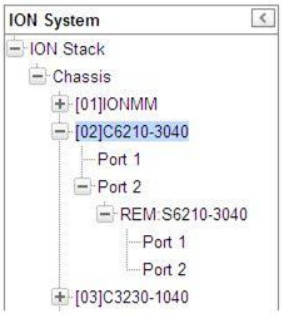
1. Check the **CL - FL** Switch setting.
2. Check twisted pair cables for proper connection.
3. Check the RJ-45 for correct twisted pair cable configuration.
4. Check integrity of device attached to media converter by twisted pair cable.
5. Check if other network devices are working properly.
6. Remove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

TX or RX LED off (not flashing):

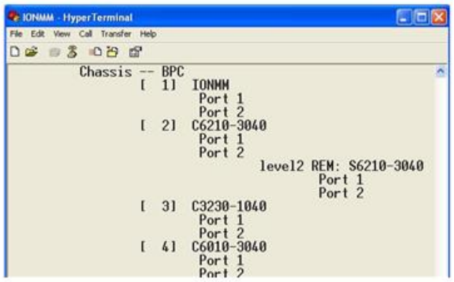
1. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
2. Check if other network devices are working properly.
3. Verify that the ION system devices have the latest firmware versions.
4. Download the latest firmware version and upgrade as necessary.
5. Remove the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

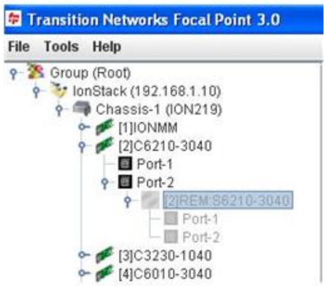


ION System – Web Interface



```
          Chassis -- BPC
                   [  1]  IONMM
                           Port 1
                           Port 2
                   [  2]  C6210-3040
                           Port 1
                           Port 2
                                      level2 REM: S6210-3040
                                                   Port 1
                                                   Port 2
                   [  3]  C3230-1040
                           Port 1
                           Port 2
                   [  4]  C6010-3040
                           Port 1
                           Port 2
```

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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p= PORT|l1d|l2d|l3d)`

3. Power cycle the x6210.

4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=
   PORT|l1d|l2d|l3d)
   ```

3. Power cycle the x6210.

4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 x6210is a remote, power cycle the local x6210.

4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot activate IP-based management

1. Use the **go** command to switch to a device that supports IP configuration.

2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Trap Server does not record traps

1. Ensure the Trap Server application is running.

2. SNMP traps may be blocked by a router or firewall. Consult your Network administrator to determine if this is the case.

3. Check that the correct SNMP trap manager IP address has been defined for the module.

   - For Web Interface – go to the **SNMP Configuration** section on the **MAIN** tab.
   - For CLI – at the device level, type: **show snmp config**.

4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Upgrade fails

1. Check the following:

   - The correct module(s) has been selected.
   - The module selected is listed in the **Card Type** column on the **Firmware Database** sub-tab.
   - A hierarchy conflict does not exist (i.e., trying to upgrade a level 2 module and its level 1 module at the same time).
   - The modules are powered on.

2. Wait two minutes, and then retry the operation. If the operation still fails, continue with step 3 below.

3. Reboot the IONMM and all modules in the upgrade stream.

4. Retry the operation. **Note:** you will have to do another upload of the upgrade files.

5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

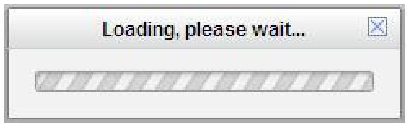
Configuration Mode Mismatch

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 312 for details on hardware mode configuration.

2. Contact Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

loading, please wait ... Displays continuously



Loading, please wait...

1. Wait for one or more minutes for discovery to complete.

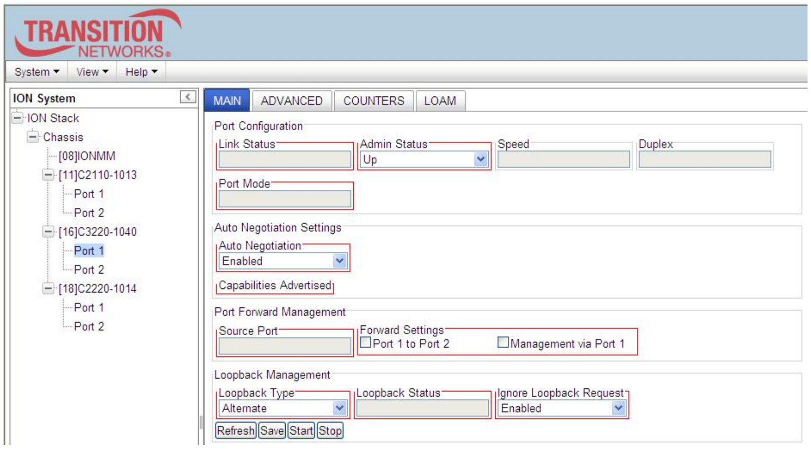
2. Click the ☒ icon to close the message.

3. Check the parameter entries and retry the operation.

4. Click the **Refresh** button and try the operation again.

5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



Port Configuration
Link Status:
Admin Status: Up
Speed:
Duplex:
Port Mode:

Auto Negotiation Settings
Auto Negotiation: Enabled
Capabilities Advertised

Port Forward Management
Source Port:
Forward Settings: □Port 1 to Port 2 □Management via Port 1

Loopback Management
Loopback Type: Alternate
Loopback Status:
Ignore Loopback Request: Enabled

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, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

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 Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

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 Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

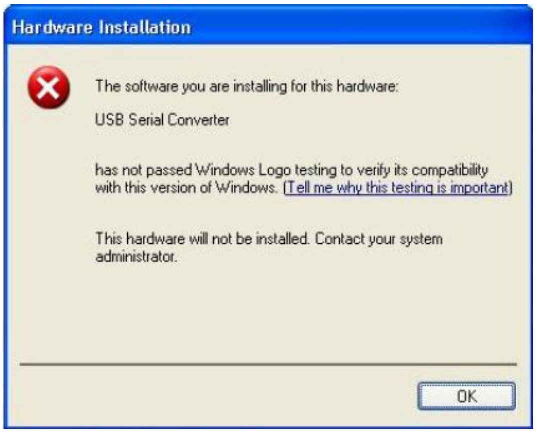
Driver Installation Fails and Windows XP Gives Error Code 10

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 Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

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.


Hardware Installation

The software you are installing for this hardware:

USB Serial Converter

has not passed Windows Logo testing to verify its compatibility with this version of Windows. (Tell me why this testing is important)

This hardware will not be installed. Contact your system administrator.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

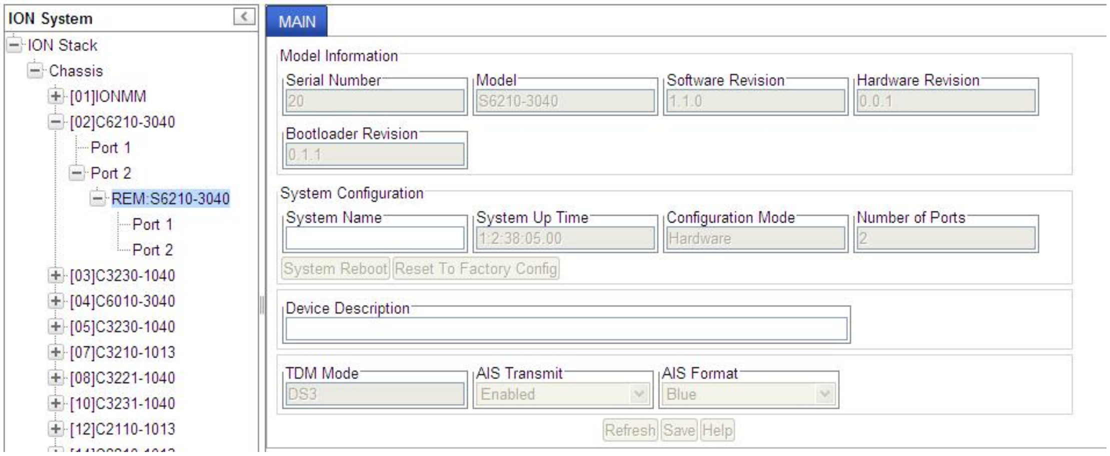
Cannot find new IP address
DHCP issued address is not being displayed
IP Address Wrong

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

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

1. Disable the DHCP client and set the DNS server; the problem resolves. (If you enable the DHCP client and then set the DNS servers via the Web interface, this issue may occur due to the internal sync problem noted above).
2. Contact Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

Cannot make x6210 configuration changes from the Web interface
GUI is not accessible
Web interface screens are all grayed out



Model Information

Serial Number: 20
Model: S6210-3040
Software Revision: 1.1.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

System Name:
System Up Time: 1:2:38:05.00
Configuration Mode: Hardware
Number of Ports: 2

Device Description:

TDM Mode: DS3
AIS Transmit: Enabled
AIS Format: Blue

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 Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

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 the press **Enter**. The valid commands that start with the part of the command you initially entered are displayed.
2. Verify the CLI command syntax.
3. Retry the operation.

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

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See "Section 6: Command Line Interface (CLI) Reference" on page 124.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to get MAC address!

This message indicates that communications to the module can not 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid condition value: xxxx

This message indicates that the input for the value= parameter on the **add acl condition** command in not valid.

1. Verify the value being input; it must match with the value input for type=.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid location parameters, cannot find the physical entity!

This message indicates that the system can not 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 Transition Networks 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.

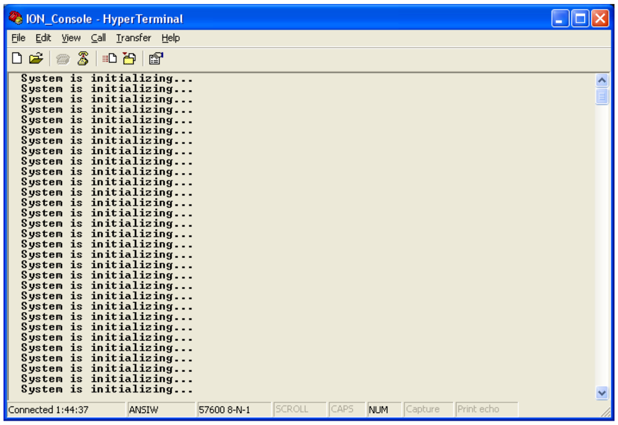
If the value of module, slot and port are not set in later commands, and then you run a device-level command, this error message displays.

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

```
go [c=CHASSIS] [s=SLOT] [l1ap=L0APORT] [l2ap=L1APORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

System is initializing...

CLI is receiving continuous error message "*system is initializing...*"



```
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error location parameter number!

The **go** command you entered had an invalid or missing parameter.

1. Enter the **go** command with all of the location parameters (chassis / slot / port) in the format:

```
go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

tftp get: set address type failed.
tftp put failed.
tftp transfer failed!

1. The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.
2. Verify the CLI command syntax.
3. Verify the firmware version.
4. Be sure the TFTP server is configured and running.
5. Check that the remotefile is in the proper location (e.g., the file *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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Set system name timeout.

You entered a command to define system information, but the information on the card was not accepted. For example:

```
C1|S10|L1D>set system name C3231
Set system name timeout.
```

1. Use the set system name command to enter the System Name information (e.g., **set system name=NAME**) without any special characters (e.g., without the ! or # or % or & characters).
2. Remove and reseat the card.
3. Try the operation again.
4. Select the **MAIN** tab > **System Configuration** section **>** **System Name** field, and verify the name and for the device.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 affect. 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Can not set speed on this port!

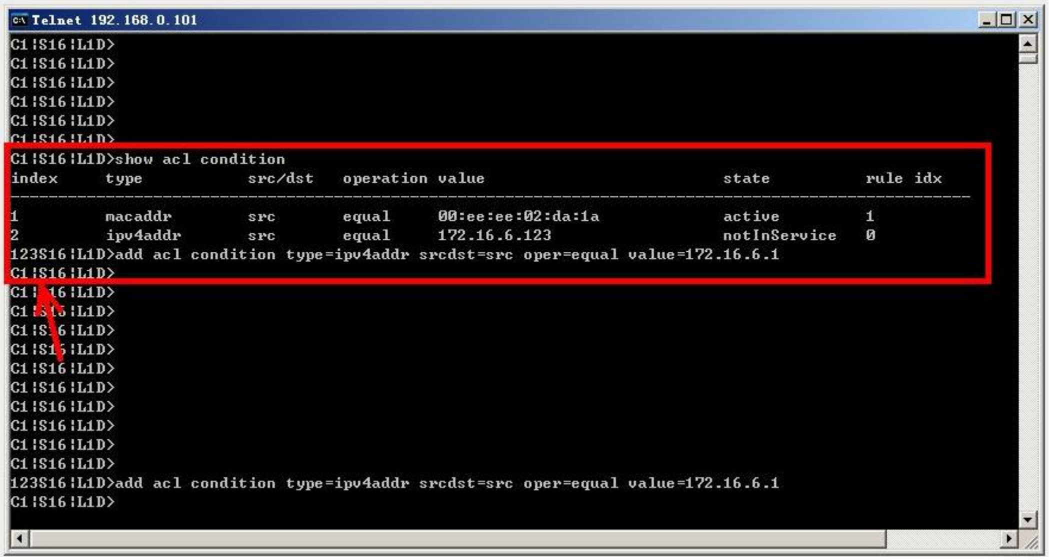
You entered the CLI command to define the NID port's operating speed, but the command failed.
For example:

```
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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Long Command Causes Cursor Wrap to Same Line

When the input command reaches the input max length, the cursor does not return to the next line, but goes back to the beginning of the same line, overwriting the original data.



```
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>show acl condition
index     type           src/dst   operation value                          state          rule idx
----------------------------------------------------------------------------------------------------
1         macaddr        src       equal     00:ee:ee:02:da:1a              active         1
2         ipv4addr       src       equal     172.16.6.123                   notInService   0
123S16¦L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.1
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
C1¦S16¦L1D>
123S16¦L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.1
C1¦S16¦L1D>
```

1. Press the **Enter** key towards the end of the command string and continue entering command text.
2. Try using HyperTerminal or the Web interface, at least temporarily.
3. Contact Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error: parameter out of range, level1 port-id range is (1 .. 15)!
Error: parameter out of range, level2 port-id range is (1 .. 16)!
Error: parameter out of range, level3 port-id range is (1 .. 16)!
Error: parameter out of range, chassis-id range is (1 .. 16)!
Error: parameter out of range, level1 attachment port-id range is (1 .. 16)!
Error: parameter out of range, level2 attachment port-id range is (1 .. 16)!

You used the **go** command to move to a port, but the command was not accepted. For example:

```
C1 S7 L1D>go l1p=0
Error: parameter out of range, level1 port-id range is (1 .. 15)!
C1 S7 L1D>
```

1. Make sure this is the port that you want. See "Managing Device and Port Hierarchy Using CLI Commands" on page 83.

2. Re-enter the **go** command.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

TFTP for Restore upload operation**:**

1. Check:
    - The IP address of the TFTP server is correct.
    - The TFTP server in online and available.
    - The file to be uploaded is in the default directory on the server.
    - The correct module(s) has been selected.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

TFTP operation failed!

This message indicates that the upload portion of an upgrade operation failed.

1. Check:
    - The IP address of the TFTP server is correct.
    - The TFTP server in online and available.
    - The correct file name is specified ("**db.zip**" for Windows XP or "**db**" for Windows 7).
    - The **db.zip** (or **db**) file is in the default directory on the TFTP server.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: The DMI feature is not supported on current port
Meaning: Not all NID models support DMI. Transition Networks 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 321 or page 327, 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

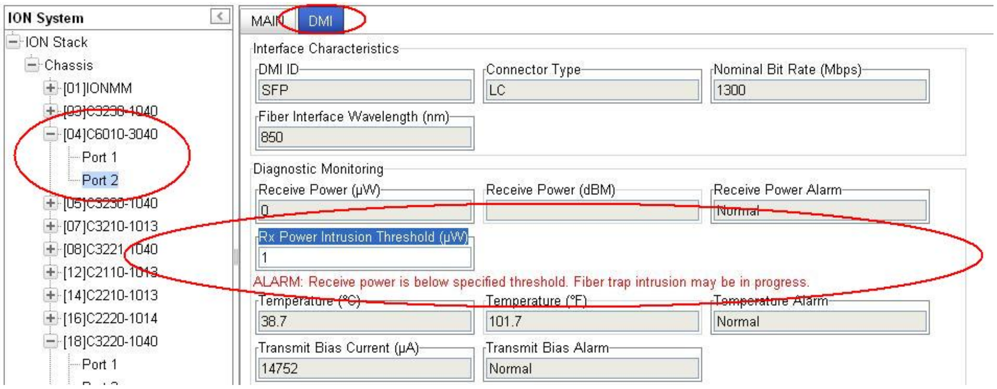
Message: *System initializing or SNMP service busy, please wait...*

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*



Interface Characteristics

DMI ID: SFP

Connector Type: LC

Nominal Bit Rate (Mbps): 1300

Fiber Interface Wavelength (nm): 850

Diagnostic Monitoring

Receive Power (µW): 0

Receive Power (dBM):

Receive Power Alarm: Normal

Rx Power Intrusion Threshold (µW): 1

ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.

Temperature (°C): 38.7

Temperature (°F): 101.7

Temperature Alarm: Normal

Transmit Bias Current (µA): 14752

Transmit Bias Alarm: Normal

Meaning: At **C6010 > Port 2 > DMI** tab, the Rx Power Intrusion Threshold setting was exceeded. With a preset level for Rx Power on the Fiber port, if the DMI read value falls below this preset value, an intrusion is suspected, and a trap is generated. Fiber optic cables can be vulnerable to tapping, with or without physical intrusion into the optic cable light path.

Either the “Rx Power Intrusion Threshold (µW)” setting is too 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:

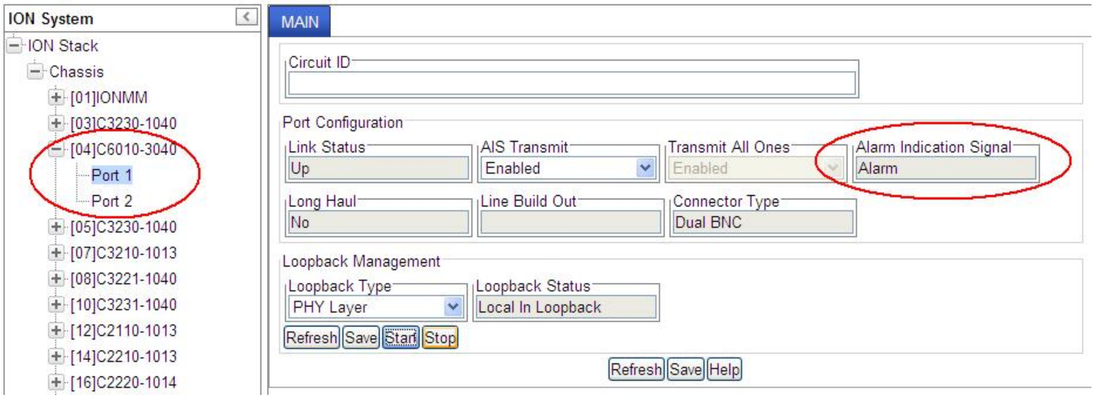
   a. From the x6210 Web interface, at **x6210** > **Port x** (SFP) > **DMI** tab, enter a lower threshold setting and click **Save** and then click **Refresh**.

   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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Alarm condition*



Circuit ID:

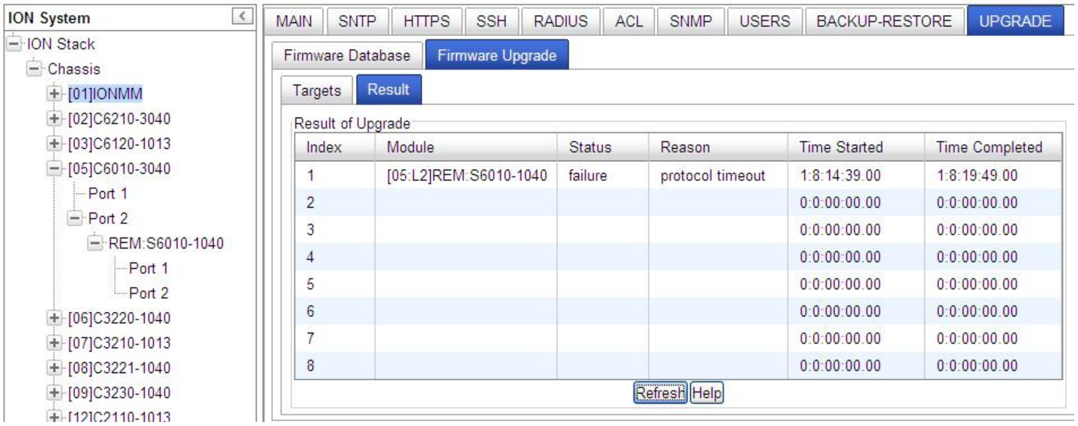
Port Configuration
- Link Status: Up
- AIS Transmit: Enabled
- Transmit All Ones: Enabled
- Alarm Indication Signal: Alarm
- Long Haul: No
- Line Build Out:
- Connector Type: Dual BNC

Loopback Management
- Loopback Type: PHY Layer
- Loopback Status: Local In Loopback

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Remote S6210 Upgrade failure - protocol timeout*



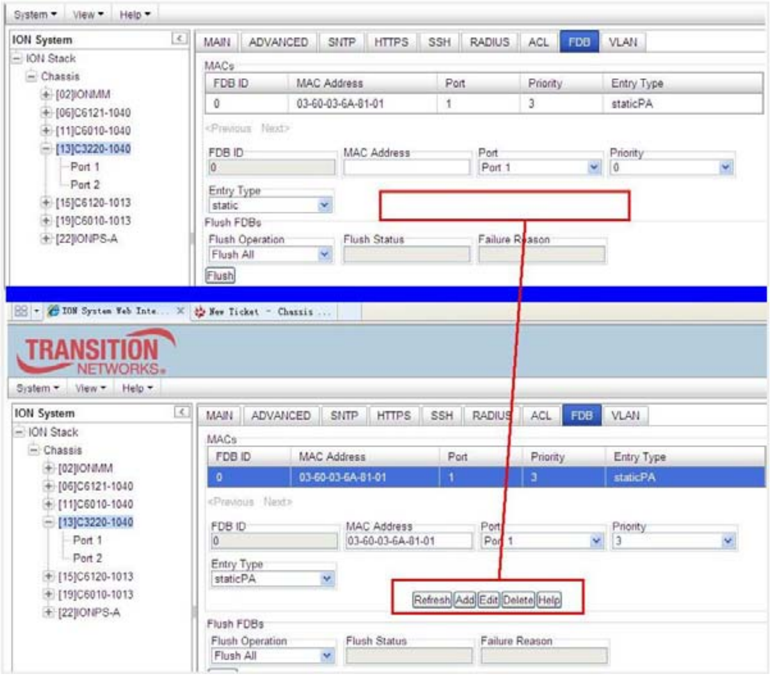
Result of Upgrade

Index	Module	Status	Reason	Time Started	Time Completed
1	[05:L2]REM:S6010-1040	failure	protocol timeout	1:8:14:39.00	1:8:19:49.00
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
6				0:0:00:00.00	0:0:00:00.00
7				0:0:00:00.00	0:0:00:00.00
8				0:0:00:00.00	0:0:00:00.00

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

In IE8 or IE9, the ‘Refresh’, ‘Add’, ‘Edit’, ‘Delete’, ‘Help’ buttons do not display.



MACs

FDB ID	MAC Address	Port	Priority	Entry Type
0	03-60-03-6A-81-01	1	3	staticPA

FDB ID: 0 MAC Address: Port: Port 1 Priority: 0

Entry Type: static

Flush FDBs

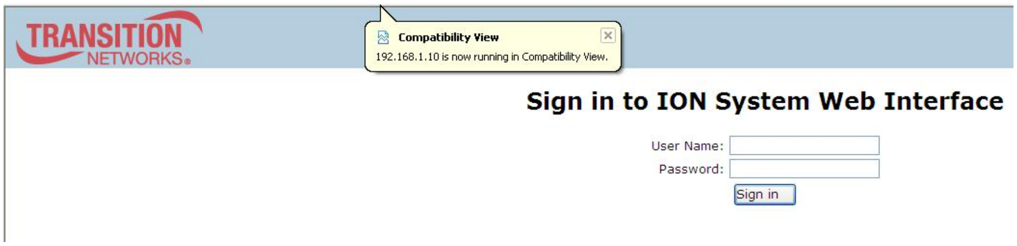
Flush Operation: Flush All Flush Status: Failure Reason:

ION System Web Inte... New Ticket - Chassis ...

FDB ID: 0 MAC Address: 03-60-03-6A-81-01 Port: Port 1 Priority: 3

Entry Type: staticPA

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.



Compatibility View

192.168.1.10 is now running in Compatibility View.

Sign in to ION System Web Interface

User Name:

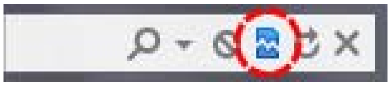
Password:

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.

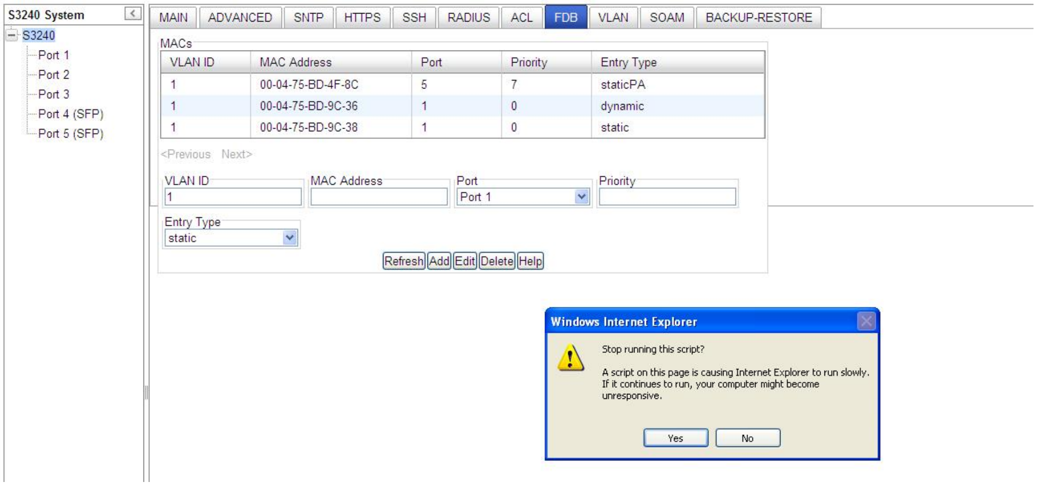
1. In IE8, click the **Stop** button on the right side of the Address bar.
2. If the page has stopped loading, click the **Refresh** button to try again.
3. Click the **Tools** button, and then click **Compatibility View**.



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 occured. Do you wish to Debug?
Done, but with errors on page.



MACs

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

VLAN ID: 1
MAC Address:
Port: Port 1
Priority:
Entry Type: static

Stop running this script?

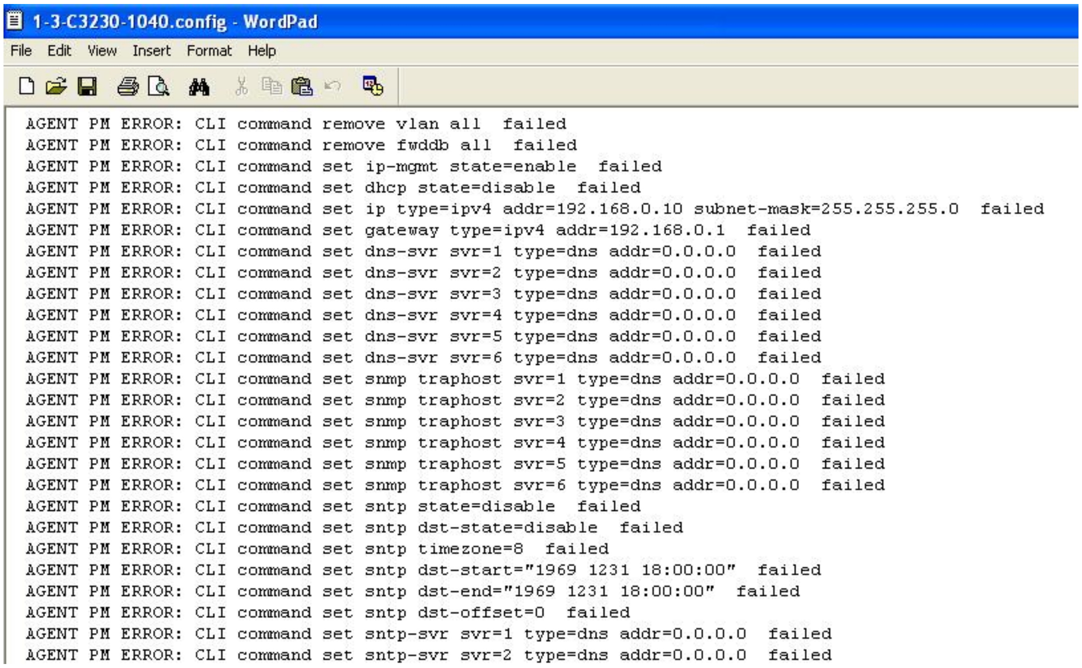
A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer might become unresponsive.

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 sntp state=disable  failed
AGENT PM ERROR: CLI command set sntp dst-state=disable  failed
AGENT PM ERROR: CLI command set sntp timezone=8  failed
AGENT PM ERROR: CLI command set sntp dst-start="1969 1231 18:00:00"  failed
AGENT PM ERROR: CLI command set sntp dst-end="1969 1231 18:00:00"  failed
AGENT PM ERROR: CLI command set sntp dst-offset=0  failed
AGENT PM ERROR: CLI command set sntp-svr svr=1 type=dns addr=0.0.0.0  failed
AGENT PM ERROR: CLI command set sntp-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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set sntp state=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference" on page 124*.. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set sntp dst-state=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference" on page 124*.. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set sntp timezone=8  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference" on page 124*.. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set sntp dst-start="1969 1231 18:00:00"  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference" on page 124*.. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set sntp dst-end="1969 1231 18:00:00"  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *"Section 6: Command Line Interface (CLI) Reference" on page 124*.. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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

Response:

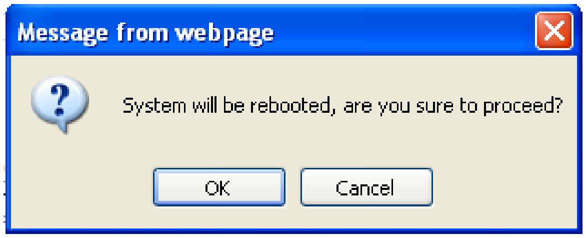
1. Make sure the RFD (Remote Fault Detect) is enabled.
2. Retry the operation.
3. Verify the procedure in "Configuring Selective and Transparent Link Pass Through" on page 204.
4. Restart the system.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.

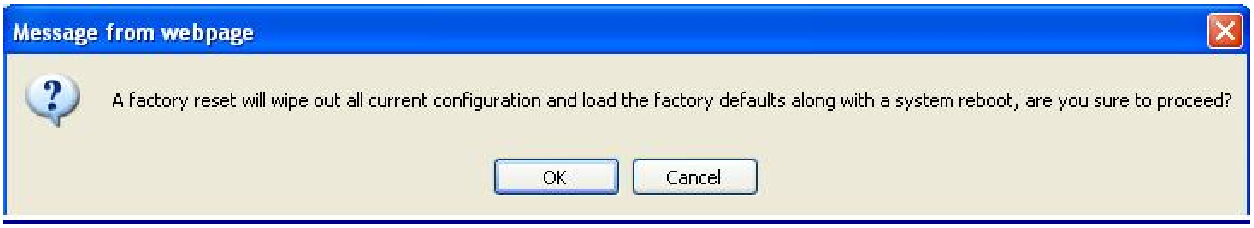
Message: *System will be rebooted, are you sure to proceed*?



System will be rebooted, are you sure to proceed?

Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

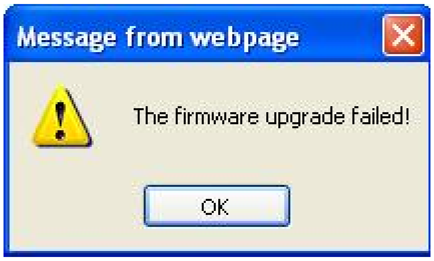
Message: *A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed*?



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*!



Message from webpage

The firmware upgrade failed!

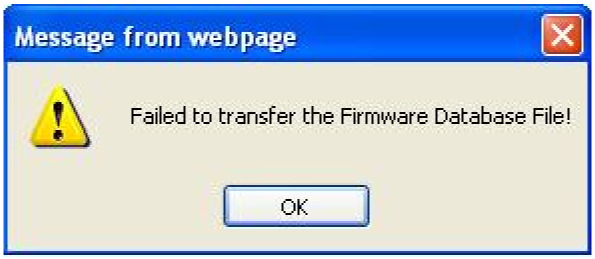
The **MAIN** tab **>** **TFTP Settings** section **Status** area displays "*TFTP Failure*".

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 Transition Networks 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Failed to Transfer the Firmware Database File*!



Message from webpage

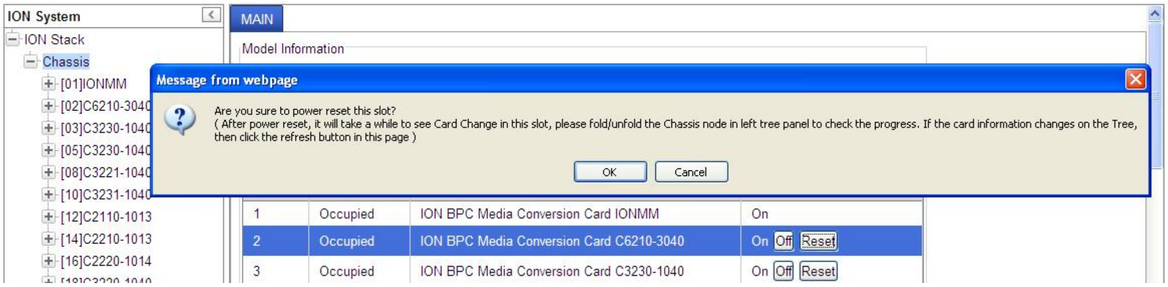
Failed to transfer the Firmware Database File!

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 Transition Networks 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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*.)



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 left tree panel to check the progress. If the card information changes on the Tree, then click the refresh button in this page)

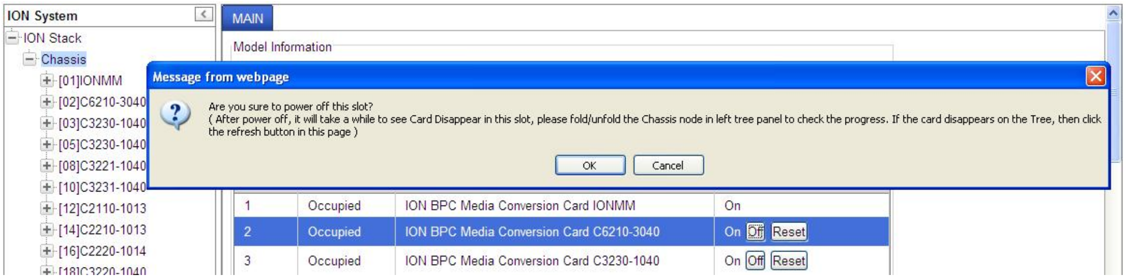
1	Occupied	ION BPC Media Conversion Card IONMM	On
2	Occupied	ION BPC Media Conversion Card C6210-3040	On Off Reset
3	Occupied	ION BPC Media Conversion Card C3230-1040	On Off Reset

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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*.)



Are you sure 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 left tree panel to check the progress. If the card disappears on the Tree, then click the refresh button in this page)

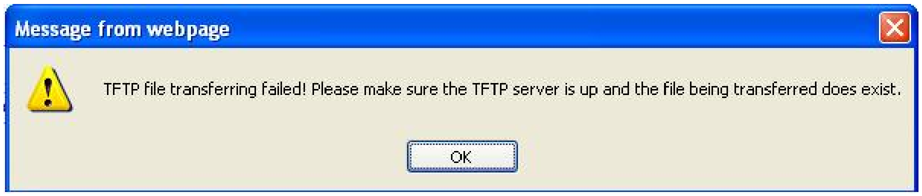
1	Occupied	ION BPC Media Conversion Card IONMM	On
2	Occupied	ION BPC Media Conversion Card C6210-3040	On Off Reset
3	Occupied	ION BPC Media Conversion Card C3230-1040	On Off Reset

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *TFTP file transferring failed!*

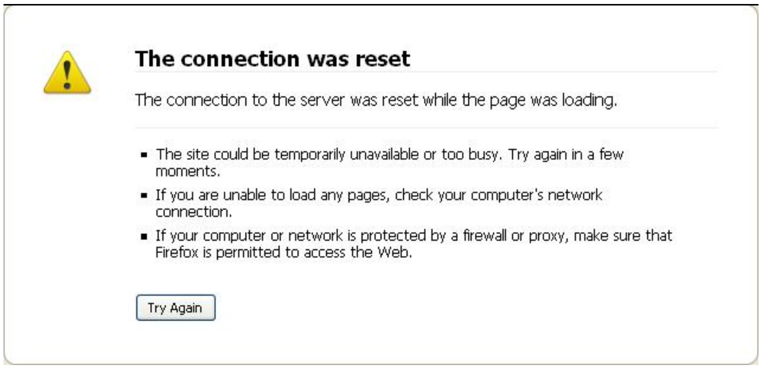


TFTP file transferring failed! Please make sure the TFTP server is up and the file being transferred does exist.

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 TN website at http://transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *The Connection was Reset*



The connection was reset

The connection to the server was reset while the page was loading.

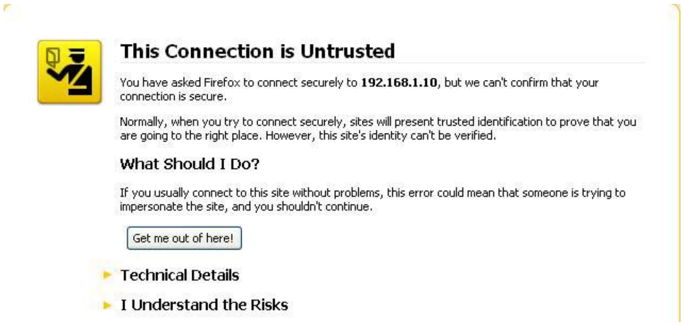
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *This Connection is Untrusted*



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.1.10**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

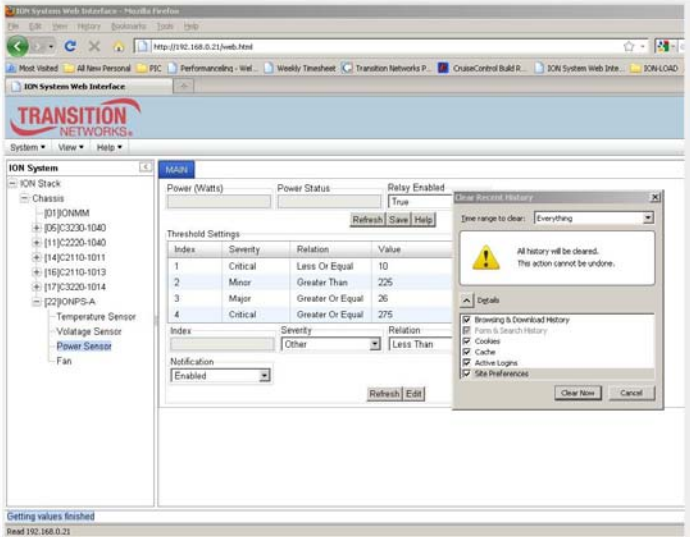
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Clear Recent History*



Power (Watts)

Power Status

Relay Enabled: True

Threshold Settings

Index	Severity	Relation	Value
1	Critical	Less Or Equal	10
2	Minor	Greater Than	225
3	Major	Greater Or Equal	26
4	Critical	Greater Or Equal	275

Index

Severity: Other

Relation: Less Than

Notification: Enabled

Clear Recent History

Time range to clear: Everything

All history will be cleared.
This action cannot be undone.

Details

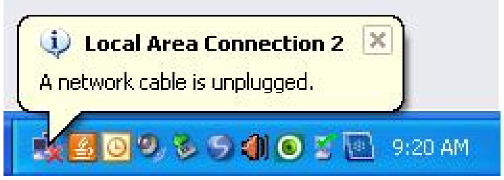
☑ Browsing & Download History
☑ Form & Search History
☑ Cookies
☑ Cache
☑ Active Logins
☑ Site Preferences

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Local Area Connection x – A network cable is unplugged*


Local Area Connection 2

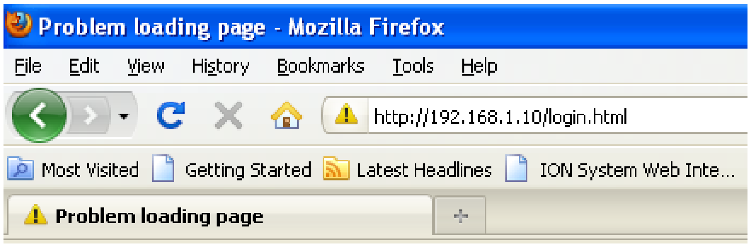
A network cable is unplugged.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Problem loading page – Mozilla Firefox*

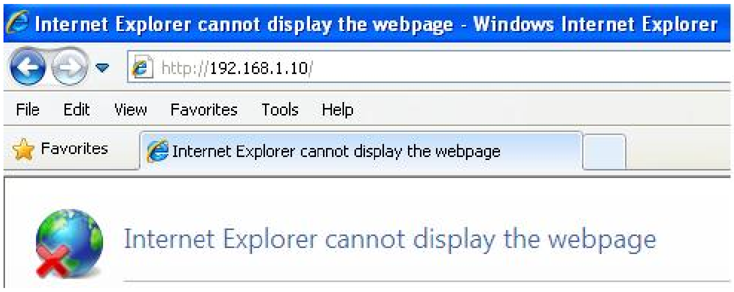

Problem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.10/login.html
Most Visited
Getting Started
Latest Headlines
ION System Web Inte...
Problem loading page

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Internet Explorer cannot display webpage*


Internet Explorer cannot display the webpage - Windows Internet Explorer
http://192.168.1.10/
File Edit View Favorites Tools Help
Favorites
Internet Explorer cannot display the webpage

Internet Explorer cannot display the webpage

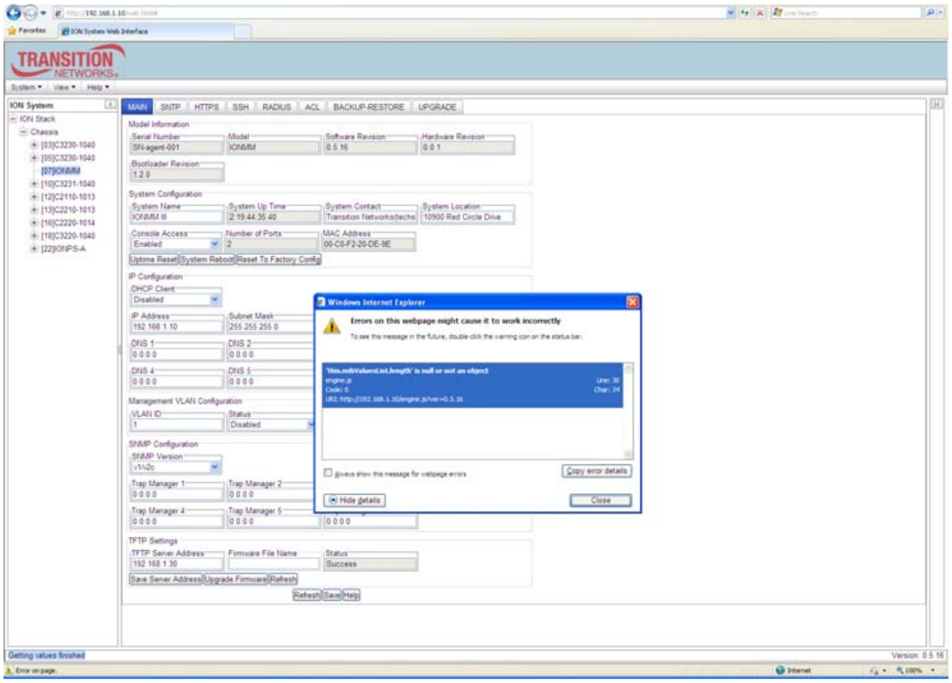
Meaning: You tried to log in to the ION system from IE, but the login failed.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.



Model Information
Serial Number: SN-agent-001
Model: IONMM
Software Revision: 0.5.16
Hardware Revision: 0.0.1
Bootloader Revision: 1.2.0

System Configuration
System Name: IONMM III
System Up Time: 2:19:44:35.40
System Contact: Transition Networks/techs
System Location: 10900 Red Circle Drive
Console Access: Enabled
Number of Ports: 2
MAC Address: 00-C0-F2-20-DE-9E

IP Configuration
DHCP Client: Disabled
IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0
DNS 1: 0.0.0.0
DNS 2: 0.0.0.0
DNS 4: 0.0.0.0
DNS 5: 0.0.0.0

Management VLAN Configuration
VLAN ID: 1
Status: Disabled

SNMP Configuration
SNMP Version: v1/v2c
Trap Manager 1: 0.0.0.0
Trap Manager 2: 0.0.0.0
Trap Manager 4: 0.0.0.0
Trap Manager 5: 0.0.0.0

TFTP Settings
TFTP Server Address: 192.168.1.30
Firmware File Name:
Status: Success

Windows Internet Explorer

Errors on this webpage might cause it to work incorrectly

To see this message in the future, double-click the warning icon on the status bar.

'this.mibValuesList.length' is null or not an object
engine.js Line: 30
Code: 0 Char: 24
URI: http://192.168.1.10/engine.js?ver=0.5.16

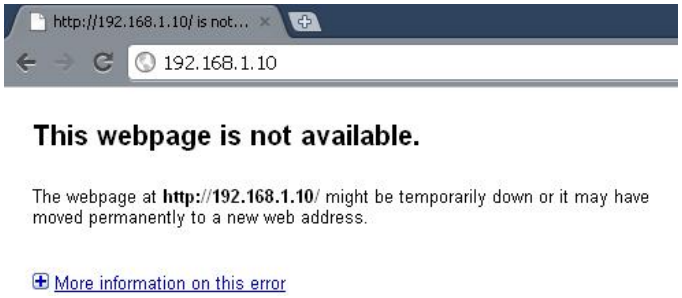
□ Always show this message for webpage errors

Recovery:
1. On the Windows IE error dialog, click the "**Show details button**".
2. Click the "**Copy error details**" button".
3. Click the "**Webpage error details**" button. Additional error information is copied (like doing a **Ctl-C** keyboard command)
4. Paste the error details text (use **Ctl-V** command) into a text file in Notepad, Wordpad, MS Word, etc., and then save the newly created file. For example:

```
User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Tri-
dent/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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *This webpage is not available.*



http://192.168.1.10/ is not...
192.168.1.10

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.

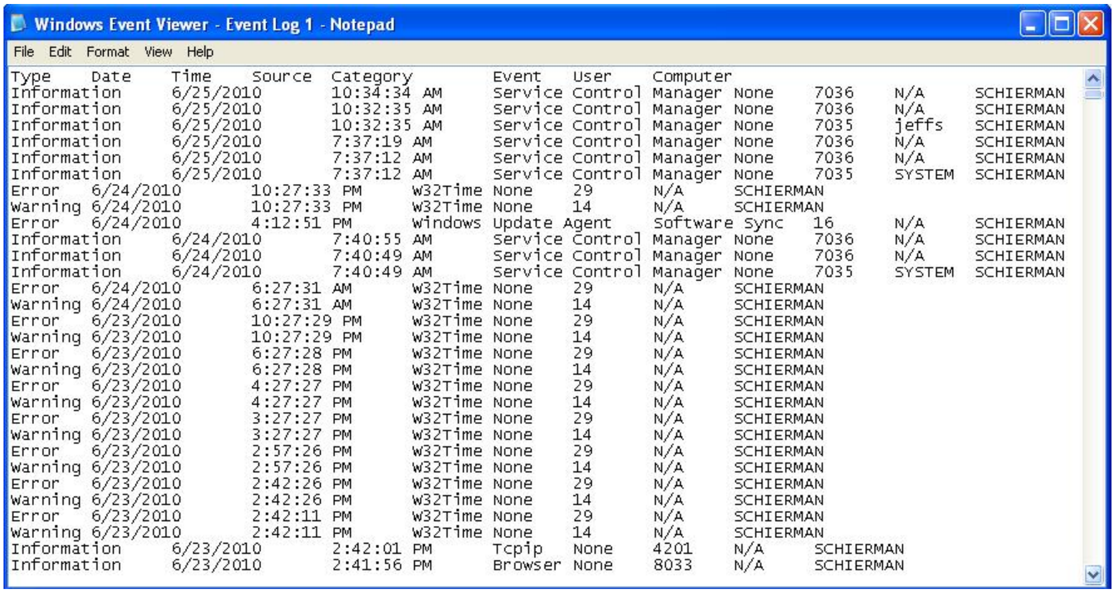
Recovery:

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:


Windows Event Viewer - Event Log 1 - Notepad
File Edit Format View Help

```
Type    Date    Time    Source  Category        Event   User    Computer
Information     6/25/2010       10:34:34 AM     Service Control Manager None    7036    N/A     SCHIERMAN
Information     6/25/2010       10:32:35 AM     Service Control Manager None    7036    N/A     SCHIERMAN
Information     6/25/2010       10:32:35 AM     Service Control Manager None    7035    jeffs   SCHIERMAN
Information     6/25/2010       7:37:19 AM      Service Control Manager None    7036    N/A     SCHIERMAN
Information     6/25/2010       7:37:12 AM      Service Control Manager None    7036    N/A     SCHIERMAN
Information     6/25/2010       7:37:12 AM      Service Control Manager None    7035    SYSTEM  SCHIERMAN
Error   6/24/2010       10:27:33 PM     W32Time None    29      N/A     SCHIERMAN
Warning 6/24/2010       10:27:33 PM     W32Time None    14      N/A     SCHIERMAN
Error   6/24/2010       4:12:51 PM      Windows Update Agent    Software Sync   16      N/A     SCHIERMAN
Information     6/24/2010       7:40:55 AM      Service Control Manager None    7036    N/A     SCHIERMAN
Information     6/24/2010       7:40:49 AM      Service Control Manager None    7036    N/A     SCHIERMAN
Information     6/24/2010       7:40:49 AM      Service Control Manager None    7035    SYSTEM  SCHIERMAN
Error   6/24/2010       6:27:31 AM      W32Time None    29      N/A     SCHIERMAN
Warning 6/24/2010       6:27:31 AM      W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       10:27:29 PM     W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       10:27:29 PM     W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       6:27:28 PM      W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       6:27:28 PM      W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       4:27:27 PM      W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       4:27:27 PM      W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       3:27:27 PM      W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       3:27:27 PM      W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       2:57:26 PM      W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       2:57:26 PM      W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       2:42:26 PM      W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       2:42:26 PM      W32Time None    14      N/A     SCHIERMAN
Error   6/23/2010       2:42:11 PM      W32Time None    29      N/A     SCHIERMAN
Warning 6/23/2010       2:42:11 PM      W32Time None    14      N/A     SCHIERMAN
Information     6/23/2010       2:42:01 PM      Tcpip   None    4201    N/A     SCHIERMAN
Information     6/23/2010       2:41:56 PM      Browser None    8033    N/A     SCHIERMAN
```

Message: `Information   6/25/2010   7:37:12 AM  Service Control Manager  None  7035   SYSTEM`

Meaning: Information message regarding SCM.

Recovery: No action required.

Message: `Error   6/24/2010   10:27:33 PM W32Time   None   29 N/A      SYSTEM`

Meaning: Error level message regarding W32Time.

Recovery: Open the file, examine the number of messages like this, and the potential problem level.

Message: `Warning 6/24/2010   10:27:33 PM W32Time   None   14 N/A      SYSTEM`

Meaning: Warning level message regarding W32Time.

Recovery: Check the other system logs for related messages. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. Transition Networks 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>
```

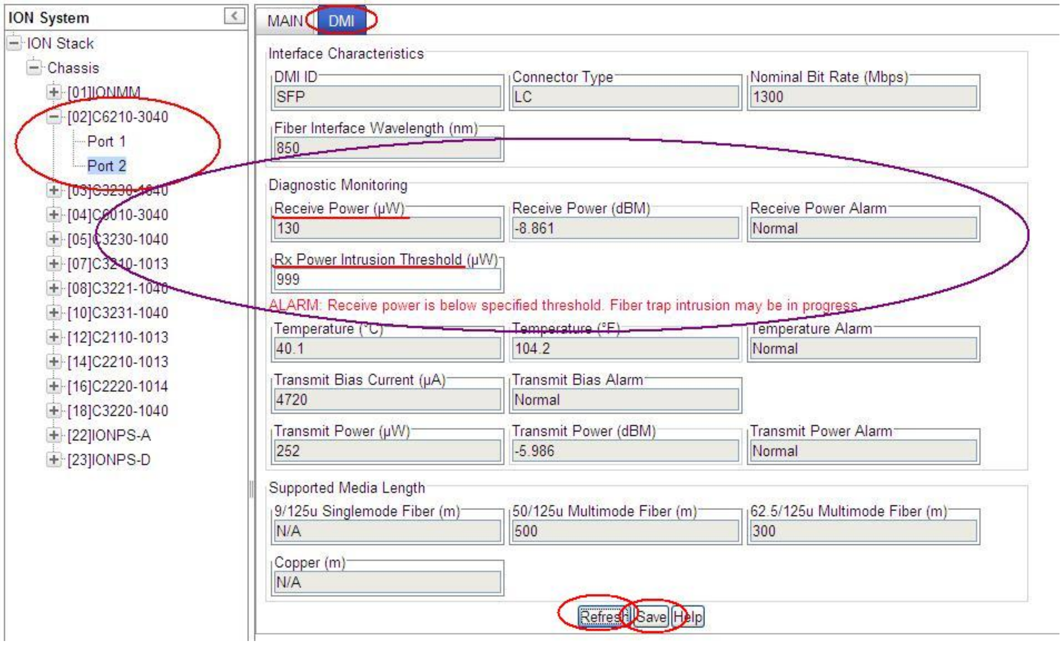
The DMI tab parameters are described in Table 15 later in this section.

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.



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

ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.

Temperature (°C): 40.1
Temperature (°F): 104.2
Temperature Alarm: Normal
Transmit Bias Current (μA): 4720
Transmit Bias Alarm: Normal
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

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 / DMI identifier	Unknown, GBIC, soldered to motherboard, 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	(measured rate)	Bitrate in units of 100Mbps (the sample screen above shows 1300, or 1.3 Gbps).
Fiber Interface Wavelength	(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 µW	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 µW. The default is 0. Displays the message “*ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress*.” if the value falls below the specified threshold.
Temperature (˚C)	(measured temp.)	Temperature of fiber transceiver in tenths of degrees C (Celsius). The sample screen above shows 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 *ionDMITemperatureEvt* event is sent when there is a warning or alarm on DMI temperature
Transmit Bias Current (uA)	(measured current)	Transmit bias current on local fiber interface, in uA (microamperes). The sample screen above shows 15440 uA (microamps).
Transmit Bias Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for transmit bias current on local fiber interface.
Transmit Power (uW)	(measured power)	Transmit power on local fiber measured in microwatts. The sample screen above shows 244 uW (microwatts).
Transmit Power (dBM)	(measured power)	Transmit power on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -6.126 dBM.
Transmit Power Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for transmit power on local fiber.
Supported Media Length	9/125u Singlemode Fiber (m)	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

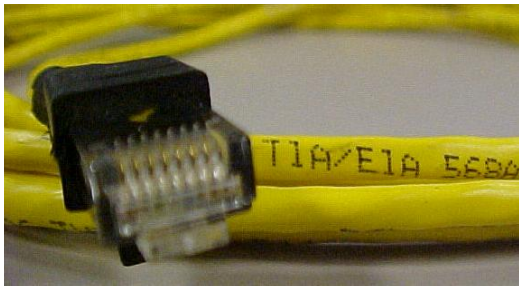
SC

LC

MT-RJ

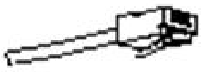
VF-45

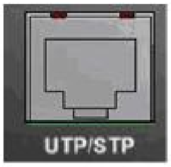
A TIA-EIA 568A CAT 5 cable is shown below.



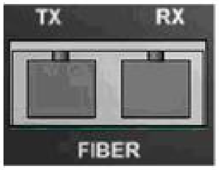
T3/E3 Cable Connectors

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.

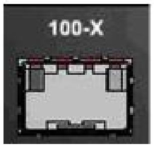




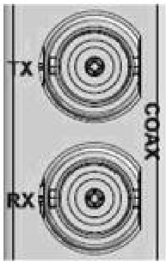
T1 / E1 RJ-45 connector (UTP)
UTP / STP RJ45 copper media connection for shielded twisted pair (STP) or unshielded twisted pair (UTP) media connection.



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 a TN 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 a TN technical support specialist.

x6210 NID

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

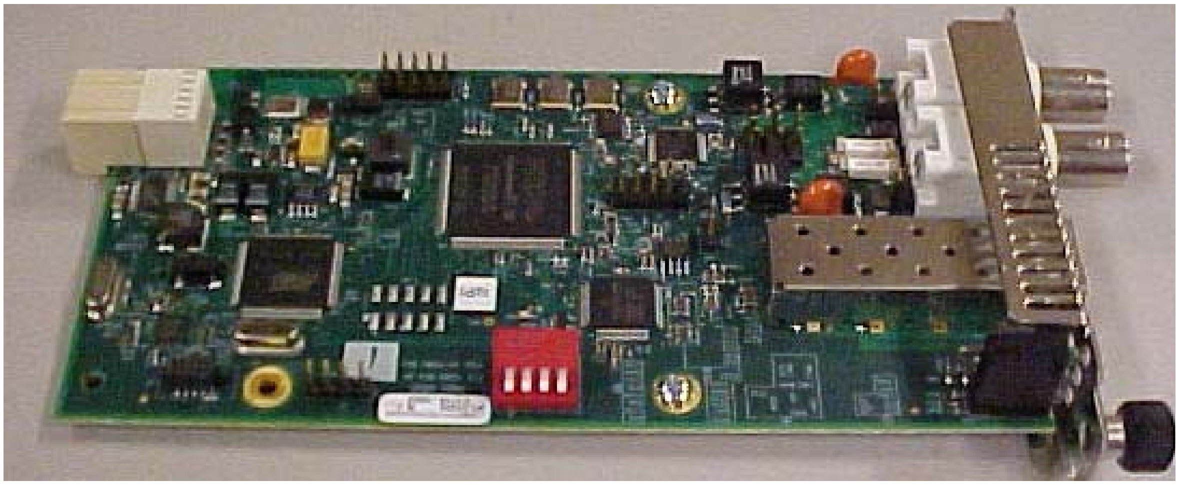
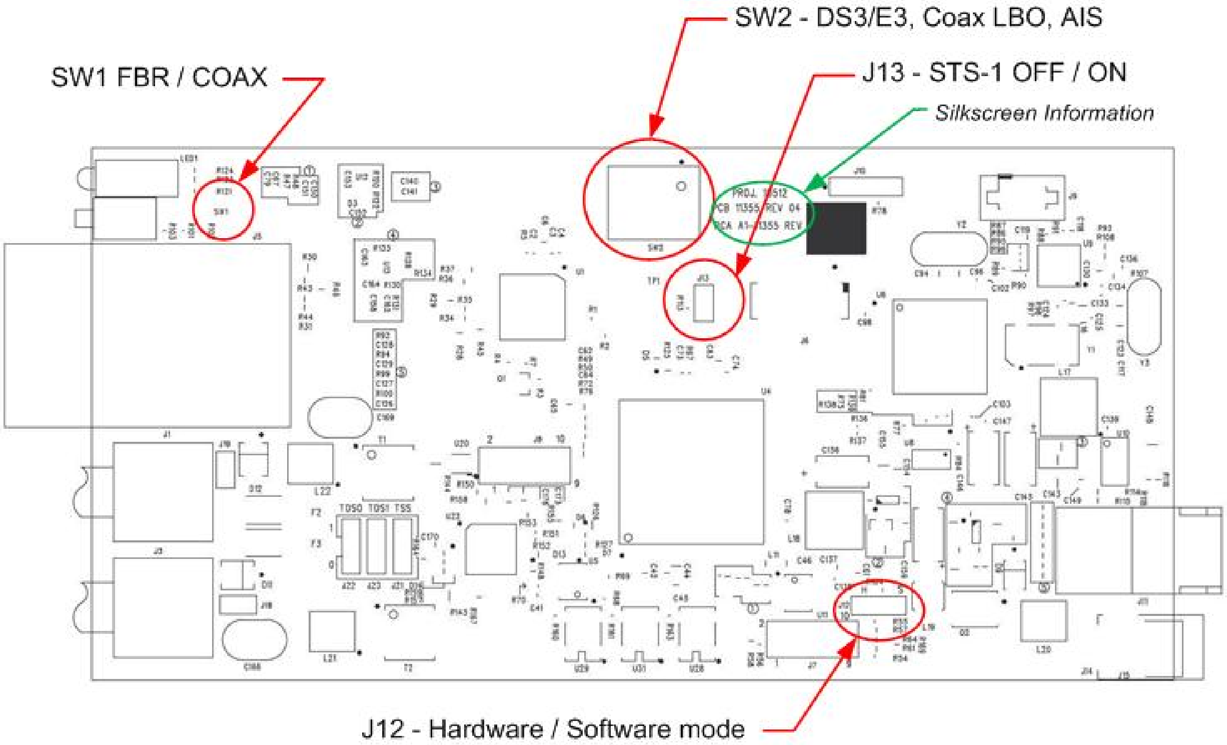


Figure 21: x6210 PCB Layout

The x6210 DIP switches and jumpers are shown below.



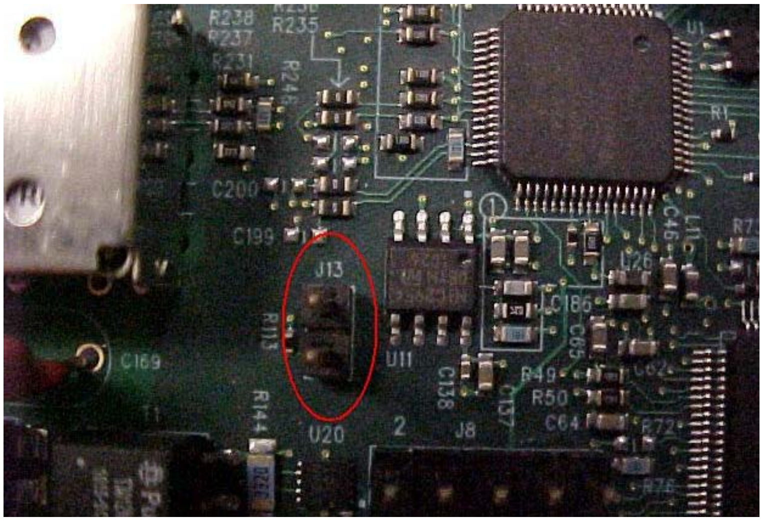
The configurable on-board components (J12, J13, SW1 and SW2) are described bin the following sections.

J12 (Hardware / Software Mode)

Jumper Pin #s	Sets Mode to	Note
1-2	Hardware mode	places the x6210 in Hardware operating mode; the hardware can configure the x6210.
2-3	Software mode	places the x6210 in Hardware operating mode; the software 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	Sets Mode to	Note
1-2 (in)	STS-1 mode off	places the x6210 in DS3 mode.
none (out)	STS-1 mode on	places the x6210 in STS-1 mode (the default setting).

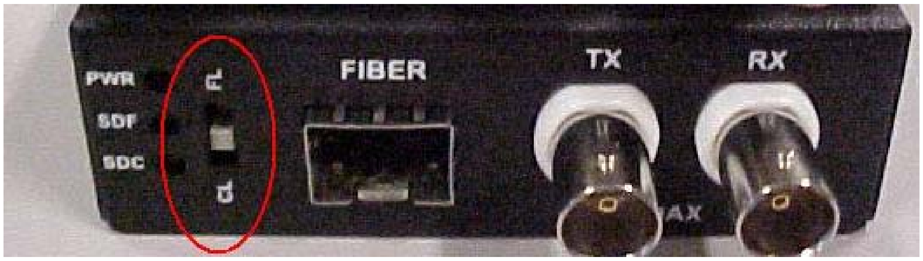
SW1 (CL - Normal - FL)

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 loop-back 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).

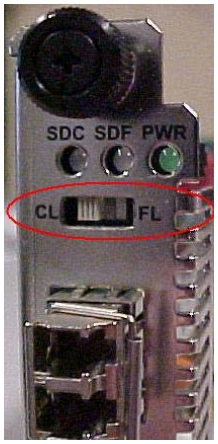
CL / FL Switch SW1 - Loopback test mode:

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.



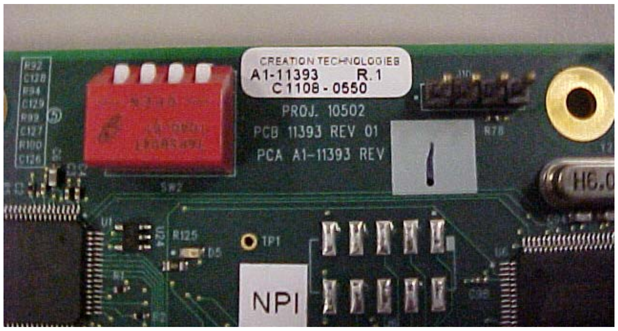
SW2 – DS3/E3, Coax LBO, AIS Xmit, and AIS Format

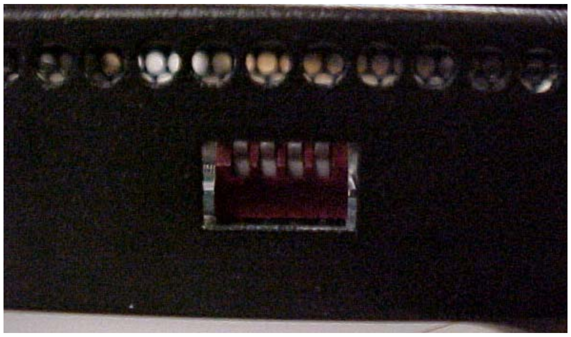
DIP Switch SW2 is used with Jumper J13 to define the x6210 operating mode.

SW2

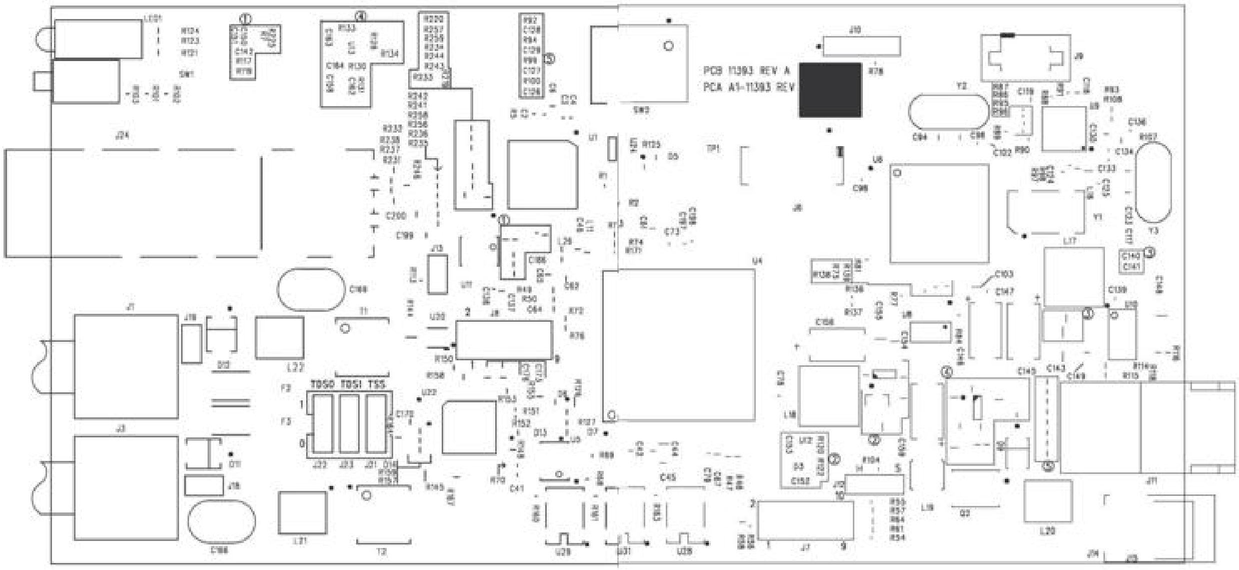
Switch #	Position	Sets Mode to	Note
1	Up (OPEN)	DS3 (or STS-1) mode	** default setting =
1	Down	E3 mode	Up position (OPEN)
2	Up (OPEN)	Coax LBO, less than 255 ft. cable	** default setting =
2	Down	Coax LBO, greater than 255 ft. cable	Up position (OPEN)
3	Up (OPEN)	AIS transmit On	** default setting =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

* 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. Transition Networks 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.

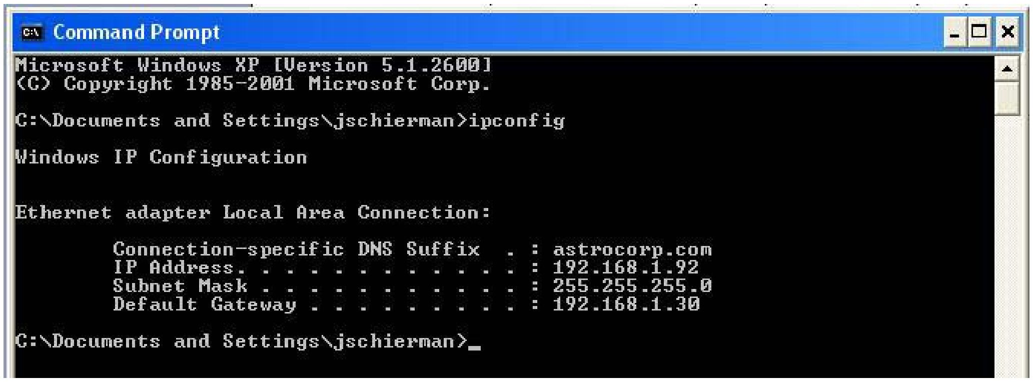
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway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



```
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 **winipcfg** command, which is available in Windows ME, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the **winipcfg** command; however, you can get the equivalent functionality for viewing and renewing an IP address using Windows' Network Connections (see below).

ifconfig

1. Verify that the machine's interfaces are up and have an IP address using the **ifconfig** command:

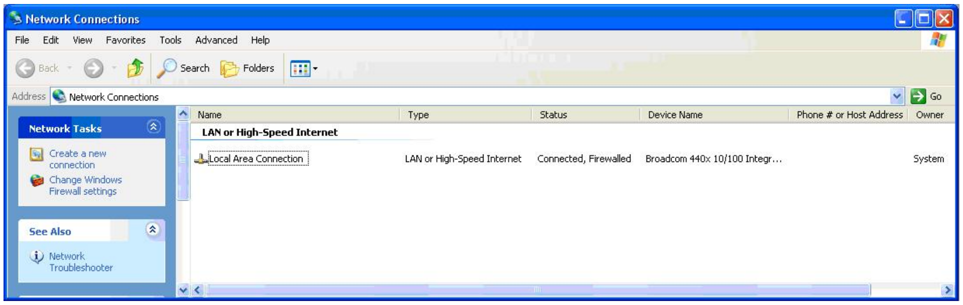
```
[root@sleipnir root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:6E:0A:3D:26
         inet addr:192.168.168.11  Bcast:192.168.168.255
Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:13647 errors:0 dropped:0 overruns:0 frame:0
         TX packets:12020 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:100
         RX bytes:7513605 (7.1 Mb)  TX bytes:1535512 (1.4 Mb)
         Interrupt:10

lo        Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         UP LOOPBACK RUNNING  MTU:16436  Metric:1
         RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:892258 (871.3 Kb)  TX bytes:892258 (871.3 Kb)
```

The above machine is running normally. The first line of output shows that the Ethernet interface eth0 has a layer 2 (MAC or hardware) address of 00:0C:6E:0A:3D:26. This confirms that the device driver is able to connect to the card, as it has read the Ethernet address burned into the network card's ROM. The next line shows that the interface has an IP address of 192.168.168.11, and the subnet mask and broadcast address are consistent with the machine being on network 192.168.168.0.

Windows Network Connections

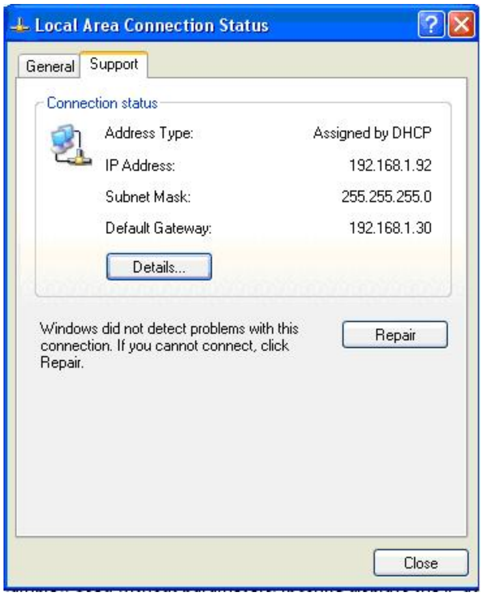
In Windows XP you can view and renew an IP address using Windows Network Connections.

1. Open Network Connections from **Start** → **Control Panel** → **Network Connections**.



Name	Type	Status	Device Name	Phone # or Host Address	Owner
LAN or High-Speed Internet					
Local Area Connection	LAN or High-Speed Internet	Connected, Firewalled	Broadcom 440x 10/100 Integr…		System

2. Right-click a network connection.
3. Click **Status**.
4. Click the **Support** tab. Your connection status information displays.



Connection status

Address Type: Assigned by DHCP
IP Address: 192.168.1.92
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.30

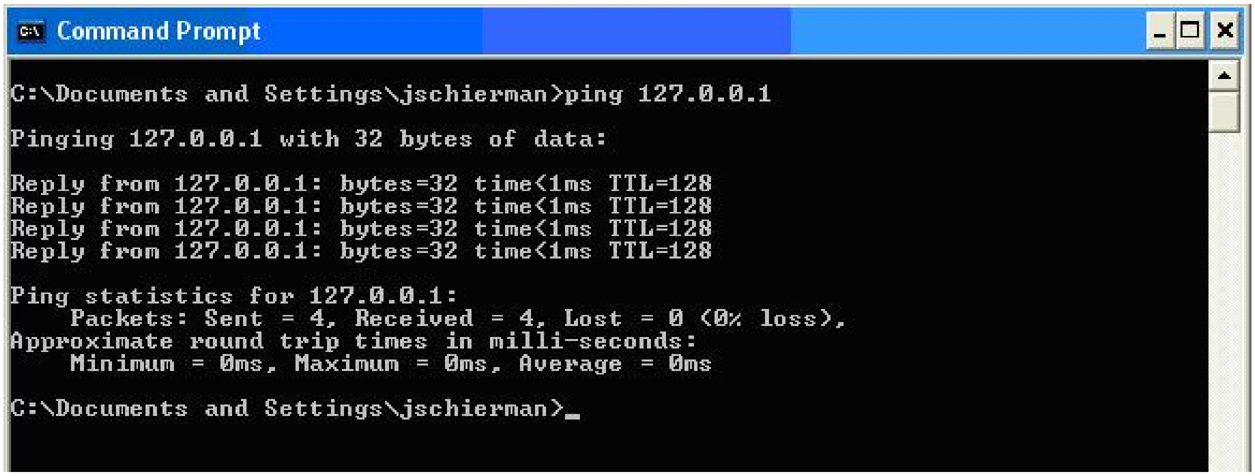
Windows did not detect problems with this connection. If you cannot connect, click Repair.

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**.



```
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
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
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.

After Telnet Client is installed, open it by following the steps below.

1. Clicking the **Start** button, type **Telnet** in the Search box, and then click **OK**.
2. To see the available telnet commands, type a question mark (**?**) and then press **Enter**.

Telnet Server

In Windows Server 2003 for most Telnet Server functions, you do not need to configure Telnet Server options to connect a Telnet client to the Windows Server 2003-based Telnet Server. However, in Windows Server 2003 you must configure Telnet Server options to be able to do certain functions.

For example, the following command uses the credentials of the user who is currently logged on to the client to create a Telnet connection on port 23 with a host named server01 **telnet server01**

The following example creates the same Telnet connection and enables client-side logging to a log file named c:\telnet_logfile **telnet -f c:\telnet_logfile server01**

The connection with the host remains active until you exit the Telnet session (by using the **Exit** command), or you use the Telnet Server administration tool to terminate the Telnet session on the host.

For more information, see the Windows Server TechCenter at http://technet.microsoft.com/en-us/library/cc787407(WS.10).aspx.

1. If you try to enable and install Telnet in Windows 7, and the message "*An error has occurred. Not all of the features were successfully changed*" displays, one workaround is to use a third party Telnet client, such as PuTTY, which also supports recommended SSH client.

PuTTY

PuTTY is a simple, free, but excellent SSH and Telnet replacement for Windows.

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

The PuTTY terminal emulator application also works as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols.

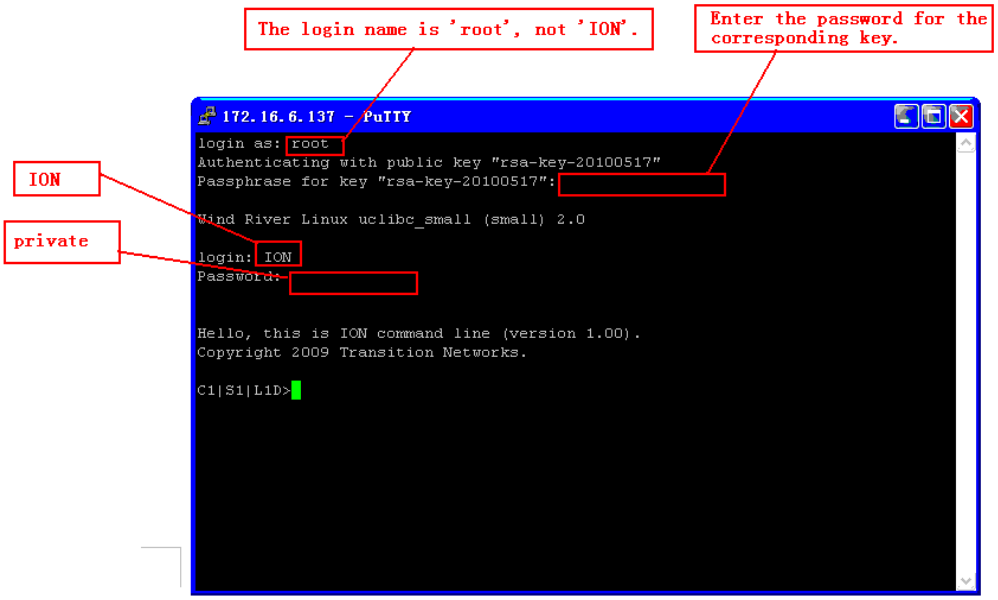
For PuTTY legal and technical details, see the PuTTY download page at http://putty.org/ or at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Note:

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.

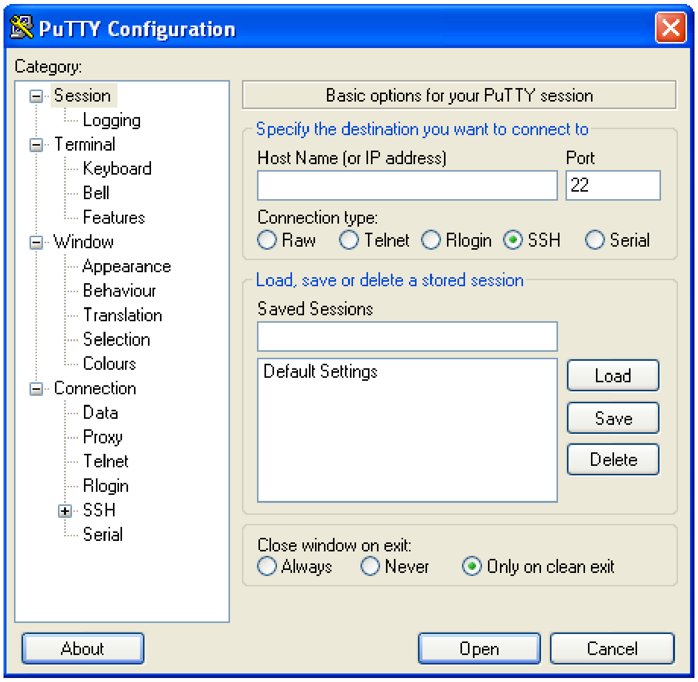
2) The ION system supports SSH2 keys only; SSH1 keys are not supported. When generating using puttyGen.exe, do not select the SSH1 keys.

3) The ION system currently supports one user named 'root' with public key authentication.


The login name is 'root', not 'ION'.
Enter the password for the corresponding key.
ION
private
172.16.6.137 - PuTTY

```
login as: root
Authenticating with public key "rsa-key-20100517"
Passphrase for key "rsa-key-20100517":

Wind River Linux uclibc_small (small) 2.0

login: ION
Password:


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

C1|S1|L1D>
```

PuTTY Basic Options:



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

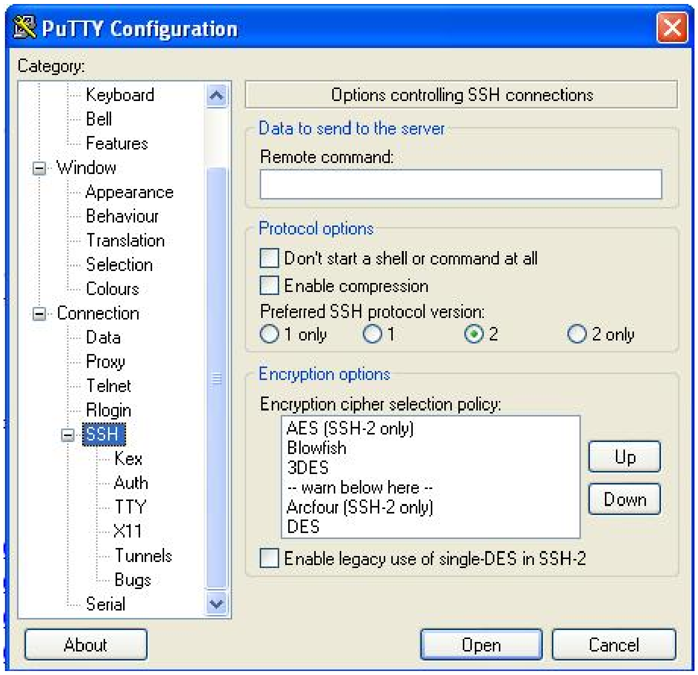
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

PuTTY SSH Options:



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version: ○ 1 only ○ 1 ● 2 ○ 2 only

Encryption options

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
Arcfour (SSH-2 only)
DES

□ Enable legacy use of single-DES in SSH-2

Tracert (Traceroute)

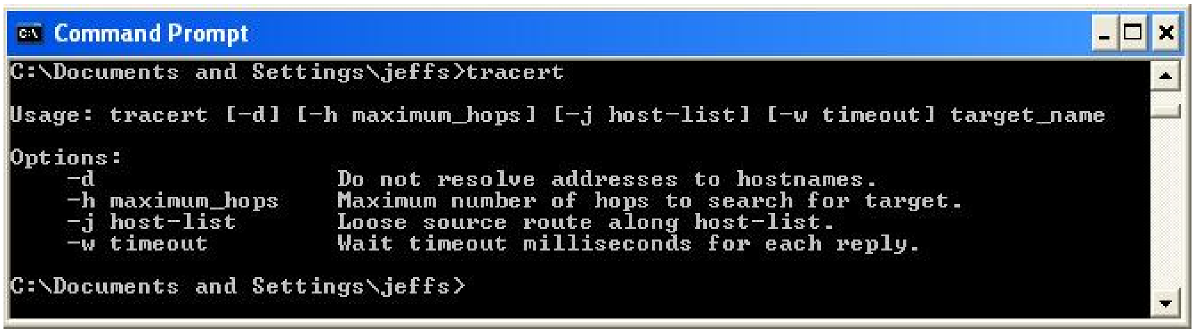
Traceroute is a computer network tool used to determine the route taken by packets across an IP network. 'Tracert" (pronounced "traceroute") sends a test network message from a computer to a designated remote host and tracks the path taken by that message.

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.



```
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>
```

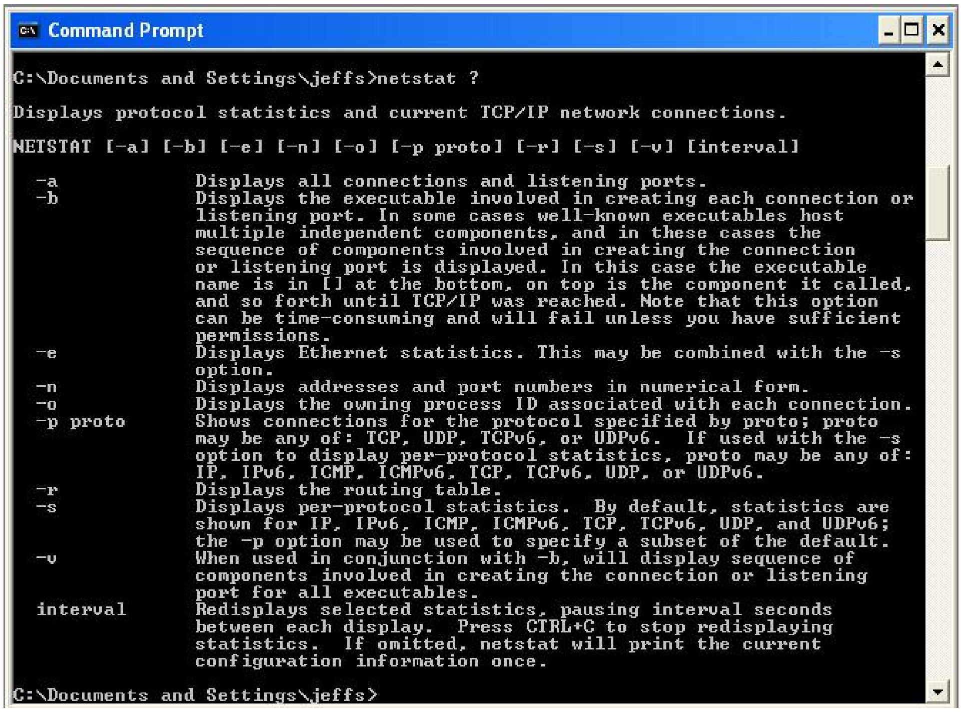
Tracert options include:

-? 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      Redisplays 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.

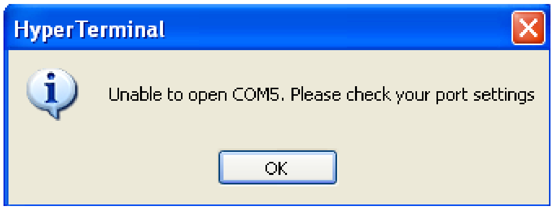
The default Crash Dump path is:
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

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.*

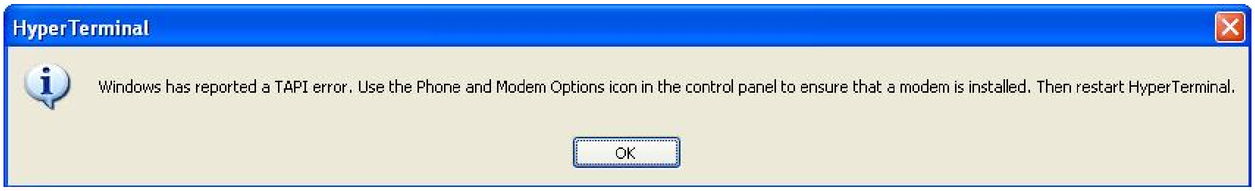


Unable to open COM5. Please check your port settings

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.*

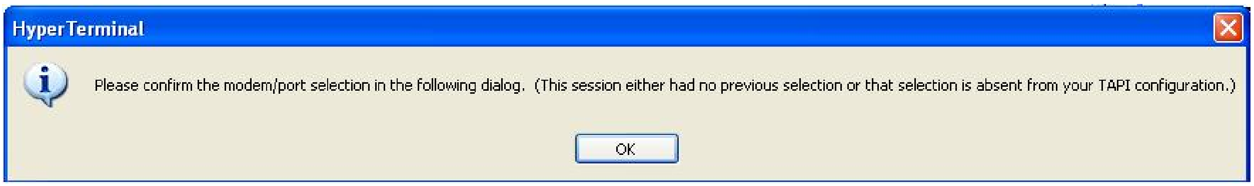


Windows has reported a TAPI error. Use the Phone and Modem Options icon in the control panel to ensure that a modem is installed. Then restart HyperTerminal.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.)*

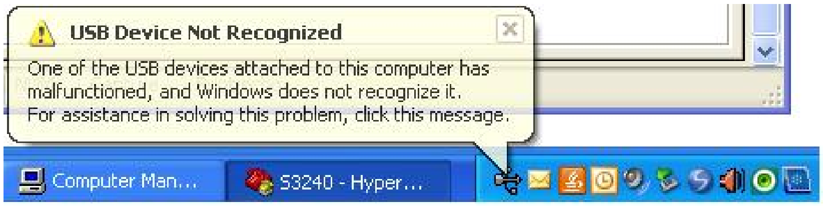


Please confirm the modem/port selection in the following dialog. (This session either had no previous selection or that selection is absent from your TAPI configuration.)

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.

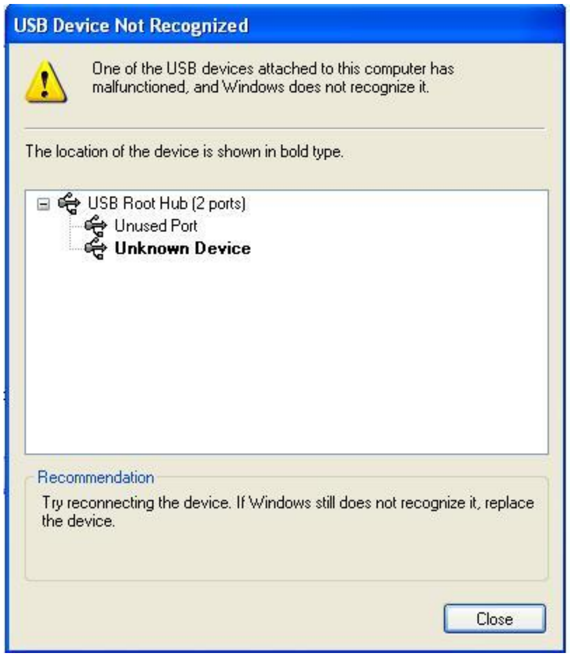


USB Device Not Recognized

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.



USB Device Not Recognized

One of the USB devices attached to this computer has malfunctioned, and Windows does not recognize it.

The location of the device is shown in bold type.

- USB Root Hub (2 ports)
  - Unused Port
  - **Unknown Device**

Recommendation

Try reconnecting the device. If Windows still does not recognize it, replace the device.

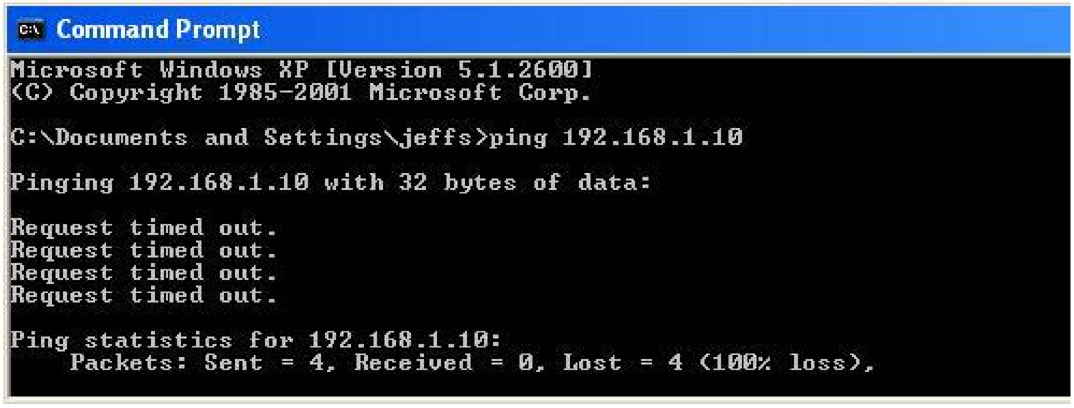
2. Click **Close** to close the dialog.

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.*



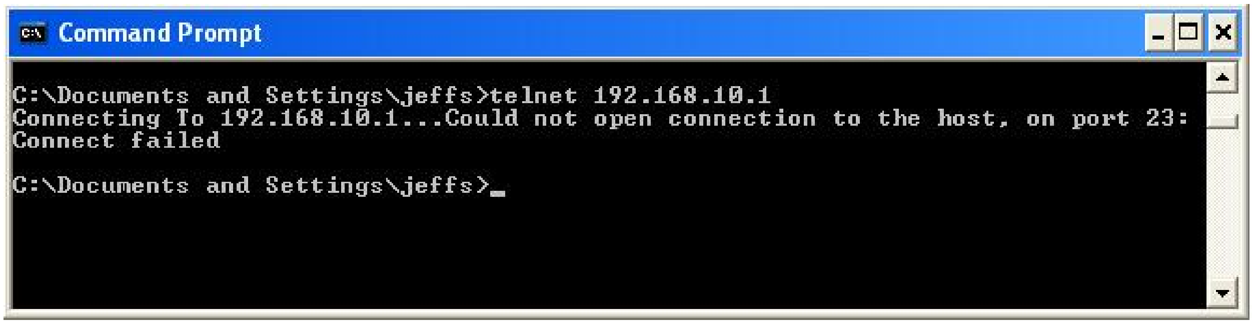
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

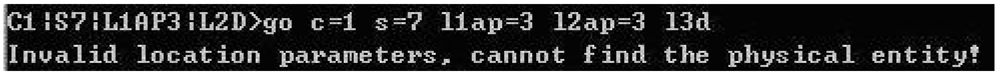
Message: *Could not open connection to the host, on port 23: Connect failed.*



```
C:\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.

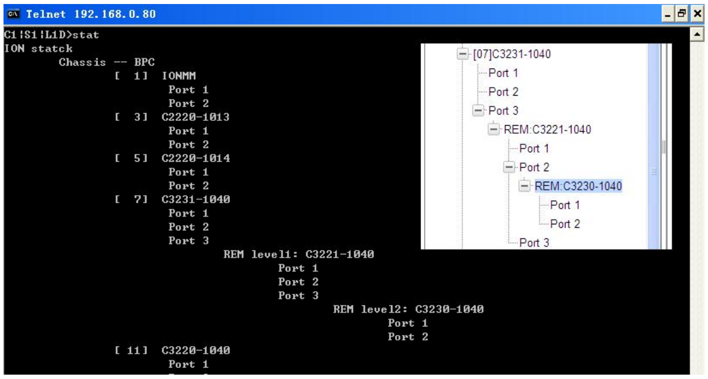
Message: *Invalid location parameters, cannot find the physical entity*!



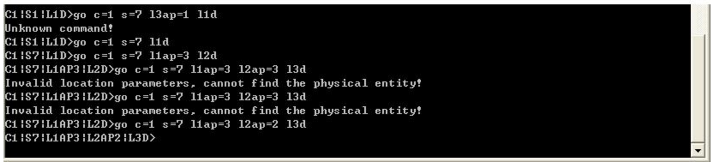
```
C1|S7|L1AP3|L2D>go c=1 s=7 l1ap=3 l2ap=3 l3d
Invalid location parameters, cannot find the physical entity!
```

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.



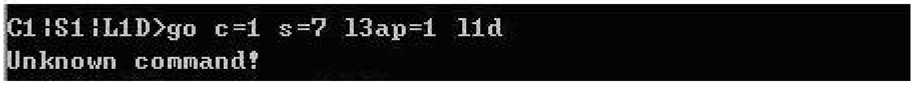
```
C1|S1|L1D>stat
ION statck
        Chassis -- BPC
                [  1]  IONMM
                        Port 1
                        Port 2
                [  3]  C2220-1013
                        Port 1
                        Port 2
                [  5]  C2220-1014
                        Port 1
                        Port 2
                [  7]  C3231-1040
                        Port 1
                        Port 2
                        Port 3
                                REM level1: C3221-1040
                                        Port 1
                                        Port 2
                                        Port 3
                                                REM level2: C3230-1040
                                                        Port 1
                                                        Port 2
                [ 11]  C3220-1040
                        Port 1
```



```
C1|S1|L1D>go c=1 s=7 l3ap=1 l1d
Unknown command!
C1|S1|L1D>go c=1 s=7 l1d
C1|S7|L1D>go c=1 s=7 l1ap=3 l2d
C1|S7|L1AP3|L2D>go c=1 s=7 l1ap=3 l2ap=3 l3d
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!
C1|S7|L1AP3|L2D>go c=1 s=7 l1ap=3 l2ap=2 l3d
C1|S7|L1AP3|L2AP2|L3D>
```

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Unknown command*!



```
C1|S1|L1D>go c=1 s=7 l3ap=1 l1d
Unknown command!
```

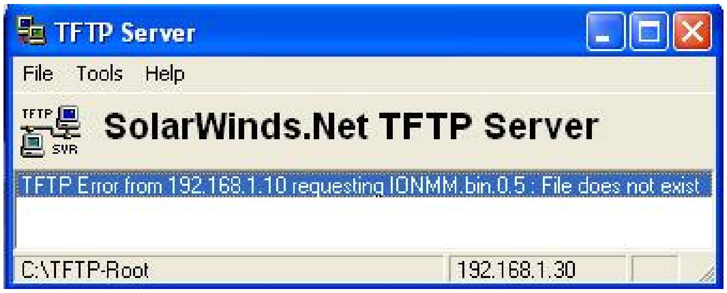
Meaning: The command you entered is not supported, or you entered the wrong command format / syntax.
Recovery:

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.

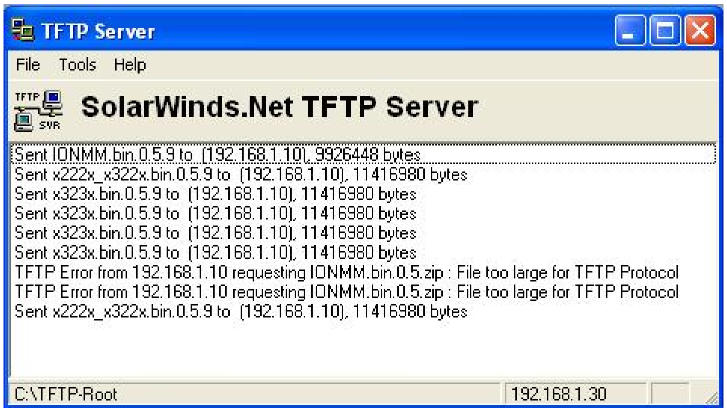
Message: *File does not exist*



```
TFTP Error from 192.168.1.10 requesting IONMM.bin.0.5 : 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*



```
Sent IONMM.bin.0.5.9 to  (192.168.1.10), 9926448 bytes
Sent x222x_x322x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
TFTP Error from 192.168.1.10 requesting IONMM.bin.0.5.zip : File too large for TFTP Protocol
TFTP Error from 192.168.1.10 requesting IONMM.bin.0.5.zip : File too large for TFTP Protocol
Sent x222x_x322x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
```

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 200.
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 200.
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.

Technical Support

Technical support is available 24-hours a day at:

United States:	1-800-260-1312
International:	00-1-952-941-7600

Web-based training

Transition Networks provides 12-16 seminars per month via live web-based training.

Log onto www.transition.com and click the Learning Center link at the top of the page.

E-Mail

Ask a question anytime by sending an e-mail message to our technical support staff: techsupport@transition.com

Address

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343, U.S.A.

Telephone: 952-941-7600

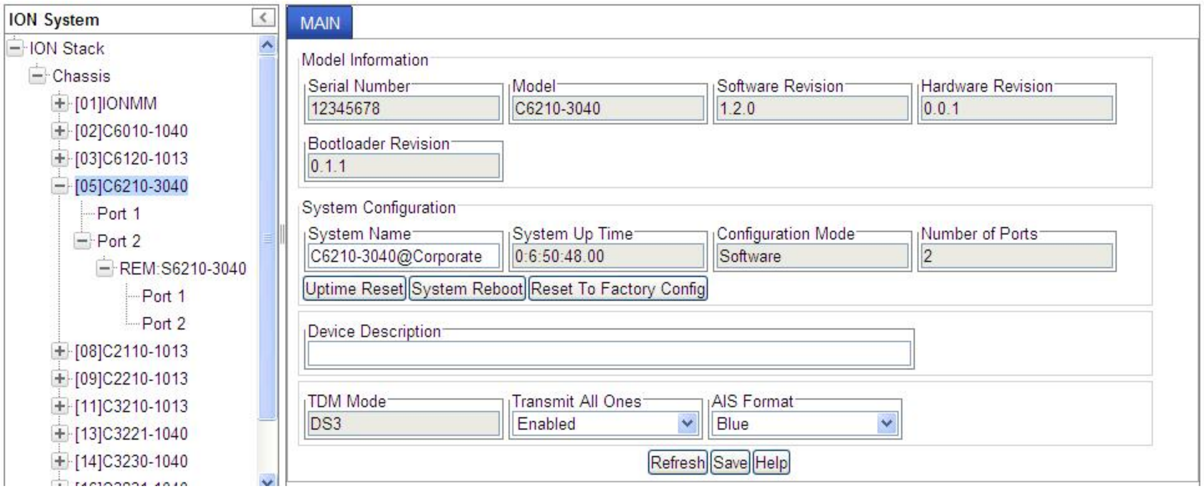
Toll free U.S.A & Canada: 800-526-9267

Fax: 952-941-2322

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 Transition Networks 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.)



Model Information

Serial Number: 12345678
Model: C6210-3040
Software Revision: 1.2.0
Hardware Revision: 0.0.1
Bootloader Revision: 0.1.1

System Configuration

System Name: C6210-3040@Corporate
System Up Time: 0:6:50:48.00
Configuration Mode: Software
Number of Ports: 2

Device Description:

TDM Mode: DS3
Transmit All Ones: Enabled
AIS Format: Blue

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 138.

Your Transition Networks 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 Transition Networks 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: ___________________________

____

Important note on product identification: When the full part number of a ION System device is abbreviated for use in catalogs and marketing literature, the first set of numeric digits in the string is dropped and replaced by the last. In most ION System products, the first set of numeric digits in the full part number is the same as the last, so this process is transparent. With the IONMM, this is not true.

Appendix A: Warranty and Compliance Information

Warranty

This warranty is your only remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Transition Networks is not liable for any special, indirect, incidental or consequential damages or losses, including loss of data, arising from any cause or theory. Authorized resellers are not authorized to extend any different warranty on transition networks' behalf.

Limited Lifetime Warranty

Effective for products shipped May 1, 1999 and after. Every Transition Networks' labeled product purchased after May 1, 1999 will be free from defects in material and workmanship for its lifetime. This warranty covers the original user only and is not transferable.

What the Warranty Does Not Cover

This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside the product's specified rating, or normal wear and tear of mechanical components. If the user is unsure of the proper means of installing or using the equipment, contact Transition Networks' free technical support services.

Establishing Original Ownership

To establish original ownership and provide date of purchase, please complete and return the registration card accompanying the product or register the product on-line on our product registration page.

Transition Networks will at its option:

- Repair the defective product to functional specifications at no charge
- Replace the product with an equivalent functional product
- Refund the purchase price of a defective product

Who to Contact for Returns

To return a defective product for warranty coverage, contact Transition Networks' technical support department for a return authorization number. Transition's technical support department can be reached through any of the following means:

Service Hours

Mon thru Fri 7 AM - 6 PM CST:

Contact Tech Support via telephone at 800-260-1312 or 952-941-7600
Fax 952-941-2322

Email techsupport@transition.com

Live web chat: Transition Now

- Any Other Time
  Voice Mail 800-260-1312 x 579 or 952-941-7600 x 579

How and Where to Send Returns

Send the defective product postage and insurance prepaid to the following address:

Transition Networks, Inc.

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Attn: RETURNS DEPT: CRA/RMA # ___________

Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number.

CRA's are valid for 60 days from the date of issuance. An invoice will be generated for payment on any unit(s) not returned within 60 days.

Upon completion of a demo/ evaluation test period, units must be returned or purchased within 30 days. An invoice will be generated for payment on any unit(s) not returned within 30 days after the demo/ evaluation period has expired.

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

Before making any non-warranty repair, Transition Networks requires a $200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than $200.00, an estimate is issued to the customer for authorization of repair. If no authorization is obtained, or the product is deemed ‘not repairable’, Transition Networks will retain the $200.00 service charge and return the product to the customer not repaired. Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. TRANSITION NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY. AUTHORIZED RESELLERS ARE NOT AUTHORIZED TO EXTEND ANY DIFFERENT WARRANTY ON TRANSITION NETWORKS'S BEHALF.

Customer Pays Non-Compliant Return Costs

The customer must pay the non-compliant product(s) return transportation cost to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for shipping the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

Non-Warranty Repair Costs

Before making any non-warranty repair, Transition Networks requires a $200 charge, plus actual shipping costs to and from the customer. If the repair is greater than $200, an estimate is issued to the customer for authorization before making the repair. If no authorization is obtained, or the product is deemed not repairable, Transition Networks will retain the $200 service charge and return the product to the customer not repaired.

Repaired Non-Warranty Products

Non-warranted products repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as “No Problem Found.”

Compliance Information

Standards

CISPR22/EN55022 Class A, CE Mark

FCC Regulations

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

CE Marking

This is a Class A product. In a domestic environment, this product could cause radio interference; as a result, the customer may be required to take adequate preventative measures.

UL Recognized

Tested and recognized by the Underwriters Laboratories, Inc.

Canadian Regulations

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numériqué de la classe A est conformé à la norme NMB-003 du Canada.

European Regulations

WARNING:

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

Achtung !

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fäll ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention !

Ceci est un produit de Classe A. Dans un environment domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilsateur de prende les measures spécifiques appropriées.

In accordance with European Union Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, Transition Networks will accept post usage returns of this product for proper disposal. The contact information for this activity can be found in the 'Contact Us' portion of this document.

CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.

Der Anschluss dieses Gerätes an ein öffentlickes Telekommunikationsnetz in den EG-Mitgliedstaaten verstösst gegen die jeweligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Declaration of Conformity

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., C6210-3040)
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 (μW)	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

Product	Single/ Multi Mode	Single/ Dual Fiber	DMI Y/N	Distance	Wavelength nm	Data Rate Bit/s	Transmitter Type	TN Part # TX/Transceiver	Spectral Width Max	Min. Tx Pwr
C6210-3011	Multi	Dual	N	2km	1310	100M	InGaAsP LED	13221	400nm FWHM	-19.0 dBm
C6210-3013	Multi	Dual	N	2km	1310	100M	InGaAsP LED	13222	400nm FWHM	-19.0 dBm
C6210-3014	Single	Dual	N	30km	1310	100M	InGaAsP laser	13223	3nm FWHM	-15.0 dBm
C6210-3015	Single	Dual	N	50km	1310	100M		13224	10nm FWHM	-5.0 dBm
C6210-3016	Single	Dual	N	60km	1310	100M	Quantum Well Laser	13226	9.5nm FWHM	-4.0 dBm
C6210-3017	Single	Dual	N	80km	1550	100M	DFB Laser	13225	9.5nm FWHM	-5.0 dBm
C6210-3029-A1	Single	Single	N	20km	1310 TX / 1550 RX	100M	Laser	13229	16nm FWHM	-14.0 dBm
C6210-3029-A2	Single	Single	N	20km	1550 TX / 1310 RX	100M	Laser Diode	13230	10nm FWHM	-14.0 dBm
C6210-3029-B1	Single	Single	N	40km	1310 TX / 1550 RX	100M	Quantum Well DFB Laser	13231	12nm FWHM	-8.0 dBm
C6210-3029-B2	Single	Single	No	40km	1550 TX / 1310 RX	100M	Quantum Well DFB Laser	13232	2nm FWHM	-8.0 dBm
C6210-3040	--------	--------	--------	--------	--------	--------	--------	SFP	--------	--------

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

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

< to be supplied >

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 NOTIFICTION-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
- ionDMIInfoTable
- 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.

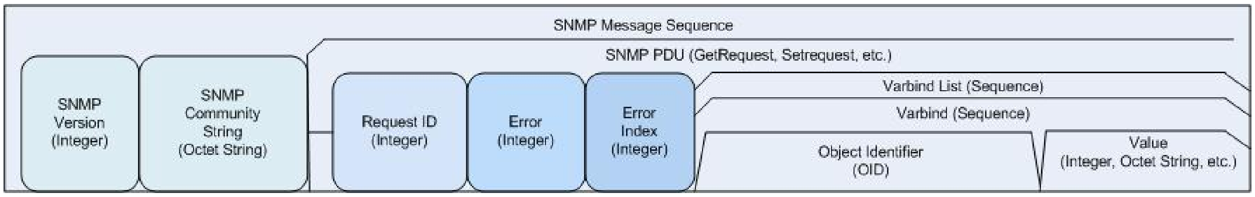


Figure 22: SNMP Message Sequence

MIB Table List / Descriptions

The list of supported MIBs includes:

- ionDevSysCfgTable
- ifTable
- ifXTable
- ionDMIInfoTable
- 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
ionIfTDMAlarmIndicationSignal	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)
ionDMIRxPwrLvlPreset	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)
ionIfTDMAlarmIndicationSignal	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 stsmlh(21), -- ST Singlemode Long Haul stsmelh(22), -- ST Singlemode Extra Long Haul scmm1300(23), -- SC Multimode 1300nm stmm1300(24), -- ST Multimode 1300nm mtrjsm(25), -- MTRJ singlemode fiber serial26(26), -- Universal 26-pin Serial Interface Connector stmmlh(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), -- 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	linkDown	
	linkup	
ifTable		
ifXTable		
ionDMIInfoTable		
ionIfLoopbackTable		
ionIfTDMTable		
TN-ION-MGMT-MIB.smi	ionDMIRxIntrusionEvt	
	ionDMIRxPowerEvt	
	ionDMITxPowerEvt	
	ionDMITxBiasEvt	
	ionDMITemperatureEvt	
xxxxxxxxxxx	ionTDMAISEvt (new)	

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.3.6.1.2.1.47.1.1.1.1.1.134217728 = 134217728 | iso.3.6.1.4.1.868.2.5.2.1.1.1.1.134217728.6 = 6 | iso.3.6.1.4.1.868.2.5.2.1.1.1.2.134217728.6
= 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.transition.productId.chassisProdsId. chassisSlotTypes.chSlcps.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 |
		cgfeb100BiaIndex.1.16 = 1 |
		cgfeb100SlotIndex.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.

Glossary

This section describes many of the terms and mnemonics used in this manual. Note that the use of or description of a term does not in any way imply support of that feature or of any related function(s).

100BASE-FX

100BASE-FX is a version of Fast Ethernet over optical fiber. It uses a 1300 nm near-infrared (NIR) light wavelength transmitted via two strands of optical fiber, one for receive (RX) and the other for transmit (TX). Maximum length is 400 meters (1,310 ft) for half-duplex connections (to ensure collisions are detected), 2 kilometers (6,600 ft) for full-duplex over multimode optical fiber, or 10,000 meters (32,808 feet) for full-duplex single mode optical fiber. 100BASE-FX uses the same 4B5B encoding and NRZI line code that 100BASE-TX does. 100BASE-FX should use SC, ST, or MIC connectors with SC being the preferred option. 100BASE-FX is not compatible with 10BASE-FL, the 10 MBit/s version over optical fiber.

1000BASE-X

Refers to gigabit Ethernet transmission over fiber, where options include 1000BASE-CX, 1000BASE-LX, and 1000BASE-SX, 1000BASE-LX10, 1000BASE-BX10 or the non-standard -ZX implementations.

1000BASE-T

Also called Gigabit (Gb) Ethernet. The 1000BASE designation is an IEEE shorthand identifier. The "1000" in the media type designation refers to the transmission speed of 1000 Mbps. The "BASE" refers to baseband signaling, meaning that only Ethernet signals are carried on the medium. 1000BASE-T is Gigabit Ethernet (1 Gb is 1000 megabits per second) on copper cables, using four pairs of Category 5 UTP wiring to achieve the gigabit data rate. 1000BASE-T is mainly used in data centers for server switching. One advantage of 1000BASE-T is that existing copper cabling can be used instead of having to rewire with optical fiber. Gigabit Ethernet industry offerings include 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-CX, and 1000BASE-T.

AIS

(Alarm Indication Signal) also called “all ones” due to the data / framing pattern, AIS 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.

There are various AIS formats based on the signaling level of the errored circuit. When an element of T-1 or (DS-1) circuit loses signal (LOS) or loses framing (OOF), the device replaces the erroneous data bits with a series of ones. This is where the term All Ones originates (as in “TAOS”.) With Ethernet long-distance data links, a similar Ethernet alarm indication signal (EthAIS) is used.

Alarms

Alarms are normally produced by the receiving terminal equipment when the framing is compromised. There are three defined alarm indication signal states, identified by a legacy color scheme: red, yellow and blue.

Red alarm indicates the alarming equipment is unable to recover the framing reliably. Corruption or loss of the signal will produce “red alarm.” Connectivity has been lost toward the alarming equipment. There is no knowledge of connectivity toward the far end.

Yellow alarm indicates reception from the far end of a data or framing pattern that reports the far end is in “red alarm.” Red alarm and yellow alarm states cannot exist simultaneously on a single piece of equipment because the “yellow alarm” pattern must be received within a framed signal. For ESF framed signals, all bits of the Data Link channel within the framing are set to data “0”; the customer data is undisturbed. For D4 framed signals, the pattern sent to indicate to the far end that inbound framing has been lost is a coercion of the framed data so that bit 2 of each timeslot is set to data “0” for three consecutive frames. Although this works well for voice circuits, the data pattern can occur frequently when carrying digital data and will produce transient “yellow alarm” states, making ESF a better alternative for data circuits.

Blue alarm indicates a disruption in the communication path between the terminal equipment. Communication devices, such as repeaters and multiplexers must see and produce line activity at the DS1 rate. If no signal is received that fills those requirements, the communications device produces a series of pulses on its output side to maintain the required activity. Those pulses represent data “1” in all data and all framing time slots. This signal maintains communication integrity while providing no framing to the terminal equipment. The receiving equipment displays a “red alarm” and sends the signal for “yellow alarm” to the far end because it has no framing, but at maintenance interfaces the equipment will report “AIS” or Alarm Indication Signal. AIS is also called “all ones” because of the data and framing pattern.

These alarm states are also lumped under the term Carrier Group Alarm (CGA). The meaning of CGA is that connectivity on the digital carrier has failed. The result of the CGA condition varies depending on the equipment function. Voice equipment typically coerces the robbed bits for signaling to a state that will result in the far end properly handling the condition, while applying an often different state to the customer equipment connected to the alarmed equipment. Simultaneously, the customer data is often coerced to a 0x7F pattern, signifying a zero-voltage condition on voice equipment. Data equipment usually passes whatever data may be present, if any, leaving it to the customer equipment to deal with the condition.

T1 and E1 Alarms:

Yellow: remote alarm indication (RAI): The RAI (remote alarm indication) signal indicates loss of layer 1 capability at the user-network interface. RAI propagates towards the network if layer 1 capability is lost in the direction of the user, and RAI propagates toward the user if layer 1 capability is lost in the direction of the network.

Blue: alarm indication signal (AIS): The AIS (alarm indication signal) is used to indicate loss of layer 1 capability in the ET-to-TE direction on the network side of the user-network interface. A characteristic of AIS is that its presence indicates that the timing provided to the TE may not be the network clock. AIS is non-framed and coded as all binary Ones.

Red: Loss of signal (LOS): The equipment shall assume "loss of signal" when the incoming signal amplitude is, for a time duration of at least 1 ms, more than 20 dB below the nominal amplitude. The equipment shall react within 12 ms by issuing AIS.

Note: E1s do not use the terms Yellow, Blue, and Red; they are provided here for comparisons with T1.

CSU/DSU Alarms:

AIS: Alarm indication signal that is all ones, unframed -- 11111111. Also known as a Blue Alarm which signals that an upstream failure has occurred

CRC (Cyclic Redundancy Check): A method of detecting errors in the serial transmission of data. A CRC for a block of data is calculated before it is sent, and is then sent along with the data. A new CRC is calculated on the received data. If the new CRC does not match the one that has been sent along with the data then an error has occurred.

Yellow Alarm a yellow alarm indicates a transmission problem at the remote CSU/DSU. A specific bit pattern will identify the alarm, the mechanism differs depending on the frame format. Of course for the remote CSU/DSU to signal an alarm, the basic T1 circuit has to be operational.
Loss of Synchronization if the CSU/DSU can't locate the synchronization flag over some number of frames, it will indicate that it lost "synch" with the remote CSU/DSU.
Red Alarm A red alarm indication warns that the CSU/DSU has lost synchronization over a longer period of time.
Bipolar Violations This indicates that unintentional bipolar violations have been detected on the circuit. This typically is created when one side of the link sends binary data in which the negative and positive states alternate. Used in digital transmission facilities.
Loss of Service- when an insufficient number of '1' bits or pulses are received, the CSU/DSU may declare the circuit to be out of service.

ANSI

(American National Standards Institute) A private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide.

Auto-Negotiation

With Auto-Negotiation in place, Ethernet can determine the common set of options supported between a pair of "link partners." Twisted-pair link partners can use Auto-Negotiation to figure out the highest speed that they each support as well as automatically setting full-duplex operation if both ends support that mode. (AKA, N-WAY Protocol. Standard: IEEE 802.3u.)

BER

(Bit Error Rate) the percentage of bits that have errors relative to the total number of bits received in a telecom transmission, usually expressed as ten to a negative power. For example, a transmission might have a BER of 10 to the minus 6 (10^{-6}), meaning that, out of 1,000,000 bits transmitted, one bit was in error. The BER is an indication of how often a packet or other data unit has to be retransmitted because of an error. Too high a BER indicates that a slower data rate could improve overall transmission time for a given amount of transmitted data since the BER would be reduced, reducing the number of packets to resend. Typical error rates for copper and optical T1 transmissions are in the range $10-^{10}$ to 10^{-14}; BER for wireless networks is typically in the range of 10^{-3} to 10^{-6}. Could also mean “Bit Error Ratio”.

The BER (Bit Error Rate or Bit Error Ratio) is the number of bit errors that occur during transmission. The BER is given as a negative number, (e.g., 10^{-10} indicates a BER of one bit error in 10,000,000,000 bits of transmission).

Big Endian

Bit ordering within a byte where bits are sent serially starting with the MSB (most significant byte) and ending with the LSB (least significant byte). Contrast “Little Endian".

BPC

(Back Plane Controller) the ION chassis component that provides communication between the SIC cards and the IONMM. The BPC is an active device with a microprocessor and management software used to interconnect IONMM and SIC cards via the Ethernet management plane. The BPC has knowledge of the cards that are present in the system, and is responsible for managing the Ethernet switch that interconnects all the chassis slots.

BPDU

(Bridge Protocol Data Unit) Data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go.

BNC

(Bayonet-Neill-Concelman) A bayonet-locking connector used to terminate coaxial cables. A BNC connector has a bayonet-type shell with two small knobs on the female connector which lock into spiral slots in the male connector when twisted on. AKA Bayonet Network Connector, Bayonet Navy Connector, British Naval Connector, Bayonet Nut Connection.

Bridge

A device that connects one local area network (LAN) to another LAN.

CE

A mandatory conformity mark on many products placed on the single market in the European Economic Area (EEA). The CE marking certifies that a product has met EU consumer safety, health or environmental requirements.

CE can also stand for Carrier Ethernet, Circuit Emulation, Customer Edge, or Customer Equipment.

CEPT

Conférence Européenne des Postes et Télécommunications (normalisation) the European Conference on post and telecommunications. A European organization of 26 European Post and Telecommunication governing services that support European advisement by the CCITT. The Conference of European Postal and Telecommunication Administration. Similar to the ITU-T in the U.S.

CEPT-1

(European Digital Signal 1) the European standard for digital physical interface at 2.048 Mbps. The US equivalent acronym is E-1.

CEPT-3

(European Digital Signal 3) the European standard for digital physical interface at 34.368 Mbps. It can simultaneously support 16 E-1/CEPT-1 circuits. The US equivalent acronym is E-3.

CEPT-4

(European Digital Signal 4) the European standard for digital physical interface at 139.264 Mbps. The US equivalent acronym is E-4.

CIR

(Committed Information Rate) The average rate up to which service frames are delivered according to performance objectives (e.g., delay, loss, etc.) associated with the service; the CIR value is always less than or equal to the UNI speed.

EIR

(Excess Information Rate) The max rate over the CIR. The EIR specifies the average rate (greater than or equal to the CIR) up to which service frames are admitted into the Service Provider network. EIR frames are considered EIR-conformant. EIR frames are delivered with no performance guarantees, and are not CIR-conformant (however, service frames that are not EIR-conformant are discarded).

Circuit ID

A company-specific identifier assigned to a data or voice network between two locations. This circuit is then leased to a customer by that ID. If a subscriber has a problem with the circuit, the subscriber contacts the telecommunications provider to provide this circuit ID for action on the designated circuit. Several Circuit ID formats exist (Telephone Number Format, Serial Number Format, Carrier Facility Format and Message Trunk Format). Telecom Circuit ID formats (LEC circuit IDs) provide service codes for DSL, HDSL, ADSL, Digital data, SST Network Trunk, Switched Access, E1, Switched Access, Basic Data and Voice, LAN, SONET, Ethernet, Video, Voice, Digital Transmission, and others.

The C3210 supports the Circuit ID, a company-specific identifier assigned by the user to identify the converter and individual ports in any manner the user chooses. In the ION system, the Circuit ID port identifier is based on the agent-local identifier of the circuit (de-fined in RFC 3046), detected by the agent and associated with a particular port. The C3210 supports a circuit ID of up to 64 bytes at the device level and the port level. The Circuit ID provides the option to configure an ASCII text string up to 63 bytes and override the de-fault circuit ID, which is vlan-module-port in binary format. The C3210 supports the

Circuit ID, a company-specific identifier assigned by the user to identify the converter and individual ports in any manner desired. In the ION system, the Circuit ID port identifier is based on the agent-local identifier of the circuit (defined in RFC 3046), as detected by the agent and associated with a particular port. Demarc Connection Points should be labeled with the Local Access Provider's Circuit ID, Carrier ID Number, and Vendor Cable ID Number. Edge Termination Points should be labeled with the Local Access Provider's Circuit ID, Carrier Circuit ID Number, and Vendor Cable ID Number. The C3210 Circuit ID feature can be configured using either the CLI or Web interface.

CLI

(Command-Line Interface) A mechanism for interacting with a computer operating system or software by typing commands to perform specific tasks. The CLI allows users to set up switch configurations by using simple command phrases through a console / telnet session.

Community

Two levels of ION system access privileges are password protected:

- Read access (Read ONLY) - a Community Name with a particular set of privileges to monitor the network without the right to change any of its configuration.
- Read/Write (Read and make changes) - a Community Name with an extended set of privileges to monitor the network as well as actively change any of its configuration.

Converter

A device that changes: 1) a signal from one transmission media to another (e.g., from copper to optical fiber) or 2) from one signaling type to another (e.g., analog to digital). See also “media converter”.

CSA

(Canadian Standards Association) A not-for-profit membership-based association serving business, industry, government and consumers in Canada and the global marketplace.

D4 Voice and Data Signaling

The transport of signaling states required in switched voice or data (Switched 56K service). Signaling is done with a "Robbed Bit" method where bit 8 of each channel's timeslot is "robbed" to indicate a signaling state in the 6th and 12th frames. The effective throughput for the A signaling bit (Frame 6) is 666.66 Bps. The effective throughput for the B signaling bit (Frame 12) is also 666.66 Bps.

dBm

(DeciBels below 1 Milliwatt) A measurement of power loss in decibels using 1 milliwatt as the reference point. A signal received at 1 milliwatt yields 0 dBm. A signal at .1 milliwatt is a loss of 10 dBm.

DCE

(Data Circuit-terminating Equipment) A device that sits between the data terminal equipment (DTE) and a data transmission circuit. Also called data communications equipment and data carrier equipment.

demarc

(demarcation point) the point where communications facilities owned by one organization interface with those of another organization. In telephone terminology, the interface between customer-premises equipment and network service provider equipment. In telephony, a demarcation point is a point at which the telephone company network ends and connects with the wiring at the customer premises. The demarcation point varies between countries and has changed over time.

In the United States, the modern demarcation point is a device defined by FCC rules (47 C.F.R. Part 68) [1] to allow safe connection of third-party telephone Customer-premises equipment and wiring to the Public Switched Telephone Network (PSTN).The modern demarcation point is the network interface device (NID). The NID is telco property. In Canada, the demarcation point varies between building types and service levels. In simple installations, the demarcation point is a junction block where telephone extensions join to connect to the network. In multi-line installations (e.g., a business or apartment building) the demarcation point may be a punch-down block. In the United Kingdom, a demarcation point occurs within a jack (the master socket), whose wiring is partly owned by the customer, and partly owned by the phone company.

AKA network terminating interface (NTI), demarcation, demark, demarc extension, DMARC, or MPOE (minimum point of entry or main point of entry).

DHCP

(Dynamic Host Configuration Protocol) A protocol for assigning dynamic Intrusion detection

A form of security management for computers and networks that gathers and analyzes information from various areas to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

You can set up x6010 intrusion detection using the CLI command “Rx Power Intrusion Threshold”, or via the web interface from x6010 > Port 2 > DMI tab > Rx Power Intrusion Threshold field. If the threshold is exceeded, the message "ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress." displays. See "DMI (Diagnostic Maintenance Interface) Test" on page 196.

In-band control

A characteristic of network protocols with which data control is regulated. In-band control passes control data on the same connection as main data. Protocols such as HTTP use in-band control (conversely, Out-of-band control is used by protocols such as FTP). One of two common methods of transmitting SNMP requests and responses, by sending them on the same media as the user data. See also "Out-of-band control".

In-band signaling

The sending of metadata and control information in the same band, on the same channel, as used for data. For example, a telephone number is encoded and transmitted across the phone line as DTMF tones. These tones "control" the phone system by telling the telephone company's equipment where to route the call. See also "Out-of-band signaling".

IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. DHCP lets a network administrator supervise and distribute IP addresses from a central point, and automatically sends a new address when a computer is plugged into a different place in the network. (Standard: RFC 2131.)

Discovering / Discovery

Discovery allows a Service OAM capable NID to learn sufficient information (e.g. MAC addresses etc.) regarding other SOAM capable NIDs so that OAM frames can be exchanged with those discovered NIDs.

DMI

(Diagnostic Monitoring Interface) Adds parametric monitoring to SFP devices.

DMM / DMR

(Delay Measurement Message / Delay Measurement Response) DMM/DMR is used to measure single-ended (aka, two-way) Frame Delay (FD) and Frame Delay Variation (FDV, aka, Jitter).

DNS

(Domain Name System) An internet service that translates domain names into IP addresses. DNS allows you to use friendly names, such as www.transition.com, to easily locate computers and other resources on a TCP/IP-based network

DNS is a standard technology for managing the names of Web sites and other Internet domains. DNS lets you type a name into your web browser (e.g., transition.com/TransitionNetworks/Learning/Seminar) to automatically find that address on the Internet.

DNS server

(Domain Name System server) any computer registered to join the Domain Name System. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts.

Dr. Watson

Dr. Watson for Windows is a program error debugger. The information obtained and logged by Dr. Watson is used by technical support groups to diagnose a program error for a computer running Windows. A text file (Drwtsn32.log) is created whenever an error is detected, and can be delivered to support personnel by the method they prefer. There is an option to create a crash dump file, which is a binary file that a programmer can load into a debugger.

DS1

(Digital signal 1), also known as “T1” or "DS-1", is a T-carrier signaling scheme defined by Bell Labs. DS1 is a common telecommunications standard in North America and Japan used to transmit voice and data between devices. E1 is used in place of T1 outside of North America, Japan, and South Korea. Technically, DS1 is the logical bit pattern used over a physical T1 line; however, the terms "DS1" and "T1" are often used interchangeably. Contrast with “DS3”.

DS3 (or DS-3)

(Digital Signal 3) a digital signal level 3 T-carrier (may also be referred to as a T3 line). The data rate for this type of signal is 44.736 Mbit/s. This level of carrier can transport 28 DS1 level signals within its payload (672 DS0 level channels). Bellcore standard GR-139-CORE defines type 734 and 735 cables for this application. Due to losses, there are differing distance limitations for each type of cable. Type 734 has a larger center conductor and insulator for lower losses for a given distance. This level of transport or circuit is mostly used between telephony carriers, both wired and wireless, and typically by OC1 optical connections.

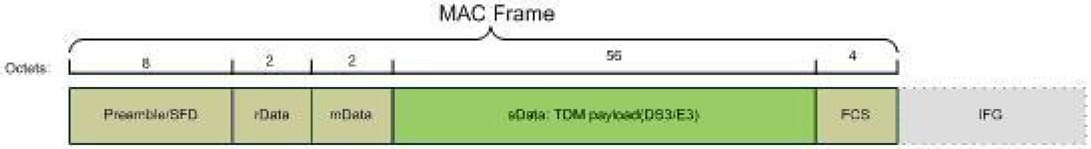
DS3 Frame Format

A DS3 frame consists of six fields:

1. Preamble	7 octets of 1010_1010
2. SFD	1 octet,1010_1011
3. rData	2 octet, reserved data,

4. mData	2 octet, management data
5: sData	(56) octets, TDM Payload data(DS3/E3 or T1/E1);
6. FCS	4 octet, Frame check sequence

A sample DS3 frame is shown below:



Contrast “T1 Frame Format”.

DSx

(Digital Signal Designator) Digital signal X is based on ANSI T1.107 guidelines. The ITU-TS guidelines vary somewhat. The set of signals and related T-carrier and E-carrier systems are summarized below.

DSx	Data Rate	DS0 Multiple	T-Carrier	E-Carrier
DS0	64 Kbps	1	- -	- -
DS1	1.544 Mbps	24	T1	- -
- -	2.048 Mbps	32	- -	E1
DS1C	3.152 Mbps	48	- -	- -
DS2	6.312 Mbps	96	T2	- -
- -	8.448 Mbps	128	- -	E2
- -	34.368 Mbps	512	- -	E3
DS3	44.736 Mbps	672	T3	- -
- -	139.264 Mbps	2048	- -	E4
DS4/NA	139.264 Mbps	2176	- -	- -
DS4	274.176 Mbps	4032	- -	- -
- -	565.148 Mbps	4 E4 channels	- -	E5

The North American signal hierarchy was created by the old US 'Bell system' (AT&T) in the early 1960's and was the world's first digital voice system. It is based on multiples of the DS0 signal. The European digital hierarchy excludes the small North American overhead.

The signal hierarchy defines the levels of multiplexing - the first level of the hierarchy multiplexes (combines) a number of DS0s into a single digital signal (with a DSx designator) which is then placed on a carrier (with a T-x designator). The DSx defines an abstract signal or speed and the T-x defines a physical format or 'pipe'. The DSx and T-x series specifications and most other telecom specifications are standardized by the ANSI accredited Committee T1 (T1E1), which is now part of the Alliance for Telecommunications Industry Solutions (ATIS) which in turn represents the US at ITU standard sessions (via the US Department of State).

DTE

(Data Terminal Equipment) The RS-232C interface that a computer uses to exchange data with a modem or other serial device. An end instrument that converts user information into signals or reconverts received signals (e.g., a terminal).

DWDM

(Dense Wavelength Division Multiplexing) In some optical fiber networks, multiple signals are carried together as separate wavelengths of light in a multiplexed signal using DWDM.

E1 (or E-1)

A type of narrowband transmission facility, used outside of North America, parts of Asia, and Japan. Line Type E1 standards include Signal Standard = 2M, Number of Timeslots = 32, Bit Rate = 2.048 Mbps. Contrast "T1" and "J1" formats.

The European digital transmission format devised by the ITU-TS and given the name by the Conference of European Postal and Telecommunication Administration (CEPT). E1 is the equivalent of the North American T-carrier system format. E2 through E5 are carriers in increasing multiples of the E1 format. E1 signals carry data at a rate of 2.048 Mbps and can carry 32 channels of 64 Kbps each. E1 carries data at a slightly higher data rate than T-1 (which carries 1.544 Mbps) because E1 does not do bit-robbing and all eight bits per channel are used to code the signal (unlike T-1). E1 and T-1 can be interconnected for international use.

E1 Facilities

The International CCITT framing format adopted by Europe, Central/South America, etc.. These facilities operate at 2.048 Mbps. This framing format is actually defined in CCITT Recommendation G.704, although Recommendation G.732 supplements G.704.

- G.704: Synchronous Frame Structures Used and Primary and Secondary Hierarchical Levels
- G.732: Characteristics of Primary PCM Multiplex Equipment Operating at 2048 Kbps.

See also "G.732/G.704 Framing ".

E1 Frame Format

See "T1 frame". Contrast "DS3 Frame Format".

E2 (E-2)

A line that carries four multiplexed E1 signals with a data rate of 8.448 Mbps.

E3 (E-3)

A line that carries 16 E1 signals with a data rate of 34.368 Mbps.

E3 Frame Format

See "DS3 Frame Format".

E4 (E-4)

A line that carries four E3 channels with a data rate of 139.264 Mbps.

EEA

(European Economic Area) Established on 1 January 1994 following an agreement between member states of the European Free Trade Association, the European Community, and all member states of the European Union (EU). It allows these EFTA countries to participate in the European single market without joining the EU.

ESD

(Electrostatic Discharge) a sudden, momentary electric current that flows between two objects.

ESF

(Extended-Superframe Format) in T-carrier, a synchronization frame that delineates 24 DS1 frames ESF requires less frequent synchronization than the T-carrier D-4 superframe format. ESF also facilitates nonchannelized operation and clear-channel operation.

The standard ESF frame is 193 bits long (1 framing bit + 24 8-bit timeslots). Each timeslot is scanned at a rate of 8000 times per second (as in D4/SF). The ESF line rate is 1.544 Mbps, which supports a data "payload" of 1.536 Mbps. There are three types of framing bits; Frame Pattern Sync (FPS), Datalink (DL), and Cyclic Redundancy Check (CRC) bits. Of the 8 Kbps framing bit bandwidth:

- 4 Kbps is allocated to the Datalink
- 2 Kbps is allocated to the CRC-6 character
- 2 Kbps is used for synchronization purposes

Compare to “Superframe”.

ETH-LB

(Ethernet Loopback) - the function used to verify connectivity of a MEP with a MIP or with peer MEP(s). There are two ETH-LB types: Unicast ETH-LB and Multicast ETH-LB.

- Unicast ETH-LB is an on-demand OAM function that can be used to 1) verify bidirectional connectivity of a MEP with a MIP or a peer MEP; or 2) perform a bidirectional in-service or out-of-service diagnostics test between a pair of peer MEPs (bandwidth throughput, detecting bit errors, etc.). Unicast ETH-LB can be used to perform only one of the two applications at any time.

Specific configuration information is required by a MEP to support Unicast ETH-LB. Specific configuration information is required by a MIP to support Unicast ETH-LB

- Multicast ETH-LB is an on-demand OAM function used to verify the bidirectional connectivity of a MEP with its peer MEPs. When a Multicast ETH-LB function is invoked on a MEP, the MEP returns to the initiator of Multicast ETH-LB a list of its peer MEPs with whom the bidirectional connectivity is detected. When Multicast ETH-LB is invoked on a MEP, a Multicast frame with ETH-LB request information is sent from a MEP to other peer MEPs in the same MEG. The MEP expects to receive Unicast frames with ETH-LB reply information from its peer MEPs within a specified period of time. On reception of a Multicast frame with ETH-LB request information, the receiving MEPs validate the Multicast frame with ETH-LB request information and transmit a Unicast frame with ETH-LB reply information after a randomized delay in the range of 0 to 1 seconds.

ETSI

(European Telecommunications Standards Institute) the corresponding body of ANSI in Europe, involved in providing and adapting standards for the European telecommunications. See http://www.etsi.org/.

Event log

A record of events such as port link down, configuration changes, etc. in a database.

FCC

(Federal Communications Commission) An independent United States government agency established by the Communications Act of 1934 that regulates interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

FDL

(Facility Data Link) refers to a repeating, 16-bit ESF data link code word to the T1 remote end requesting that it enter into a network payload loopback. The 16-bit ESF data link code word can be specified as either 00001110 11111111 for FDL ANSI or 00010010 11111111 for FDL Bellcore. This places the remote device into loopback mode per the ANSI T1.403 Specification or per the TR-TSY-000312 Specification.

Two common FDL protocols exist in the extended superframe (ESF) framing mode. One is defined in ANSI document T1.403-1989; the other is defined in AT&T publication TR54016. Depending on the carrier used, either one (or both) of these protocols may be required.

FDM

(Frequency Division Multiplexing) In FDM, multiple channels are combined onto a single aggregate signal for transmission. The channels are separated in the ‘aggregate’ signal by their Frequency. There are always some unused frequency spaces between channels, known as "guard bands". These guard bands reduce the effects of "bleed over" between adjacent channels, a condition more commonly referred to as "crosstalk".

FDM was the first multiplexing scheme to enjoy wide scale network deployment, and such systems are still in use today. However, Time Division Multiplexing is the preferred approach today, due to its ability to support native data I/O (Input/Output) channels.

FDX

(Full Duplex) Communication in both directions simultaneously.

FEF

(Far End Fault) A troubleshooting feature usually used in conjunction with Link Pass Through to notify both end devices of a loss of link.

Firmware

Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Flow Control

Prevents congestion and overloading when a sending port is transmitting more data than a receiving port can receive. (Standard: IEEE 802.3X.)

FPGA

(Field Programmable Gate Array) an integrated circuit that can be configured after manufacturing (thus "field-programmable"). The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC).

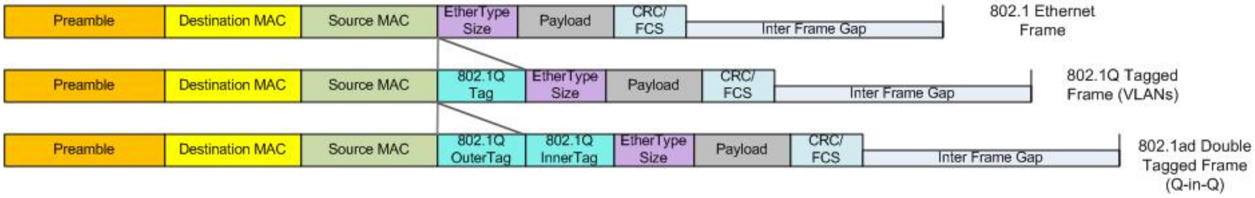
Frame

A unit of data that is transmitted between network points on an Ethernet network. An Ethernet frame has explicit minimum and maximum lengths and a set of required data that must appear within it. Each frame on an IEEE 802 LAN MAC conveys a protocol data unit (PDU) between MAC Service users. There are three types of frame; untagged, VLAN-tagged, and priority-tagged.

Frame Format

In Ethernet, a frame is a way of arranging sections of data for transfer over a computer network. The frame is a key element of an Ethernet system. A typical Ethernet frame is made up of three elements: a pair of addresses, the data itself, and an error checking field.

Frame Formats for 802.1, 802.1Q and 802.1ad are illustrated below.



Frame Loss Ratio

Frame loss ratio is the number of service frames not delivered divided by the total number of service frames during time interval T, where the number of service frames not delivered is the difference between the number of service frames arriving at the ingress ETH flow point and the number of service frames delivered at the egress ETH flow point in a point-to-point ETH connection.

Frame Delay

Frame delay is the round-trip delay for a frame, defined as the time elapsed from the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the loopbacked frame by the same source node, when the loopback is performed at the frame's destination node.

FTP

(File Transfer Protocol) A standard network protocol used to exchange and manipulate files over a TCP/IP based network, such as the Internet. See also TFTP.

G.732/G.704 Framing

The standard G.732/G.704 frame is 32 timeslots, with each timeslot consisting of an 8-bit byte. A Multiframe consists of 16 frames, numbered 0 to 15. The timeslots are numbered 0 to 31. Timeslot 0 is used for:

- Synchronization
- Alarm Transport
- International Carrier use

Timeslot 16 may be used to transmit Channel Associated Signaling (CAS) information. Note that G.732 does not define signaling states, only the transport of the states through the G.732 frame. However, G.704 does recognize the requirement for Common Channel Signaling and also allows the TRANSPARENT End-To-End transport of Timeslot 16. See also "CCITT International E1 Facilities".

GBIC

(Gigabit Interface Converter) A transceiver that converts serial electrical signals to serial optical signals and vice versa. In networking, a GBIC is used to interface a fiber optic system with an Ethernet system, such as Fibre Channel and Gigabit Ethernet.

Gbps

(Gigabits Per Second) Data transfer speeds as measured in gigabits.

GUI

(Graphical User Interface) A type of user interface item that allows people to interact with programs in more ways than typing. A GUI offers graphical icons, and visual indicators, as opposed to text-based interfaces, typed command labels or text navigation to fully represent the information and actions available to a user. The actions are usually performed through direct manipulation of the graphical elements.

HSCP

(High-Security Console Password)

HTML

(HyperText Markup Language) The predominant markup language for web pages. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists etc as well as for links, quotes, and other items.

HTTPS

(Hypertext Transfer Protocol Secure) A combination of the Hypertext Transfer Protocol with the **Error! Reference source not found.**/TLS protocol to provide encryption and secure identification of the server.

IEC

(International Electrotechnical Commission) The world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

IEEE

(Institute of Electrical and Electronics Engineers) An international non-profit, professional organization for the advancement of technology related to electricity.

ION

(Intelligent Optical Networking) the third generation of chassis-based “Intelligent Optical Networking” from Transition Networks. AKA, the ‘ION Platform’ or the ‘ION system’.

Intrusion detection

A form of security management for computers and networks that gathers and analyzes information from various areas to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

You can set up x6010 intrusion detection using the CLI command “Rx Power Intrusion Threshold”, or via the web interface from x6010 > Port 2 > DMI tab > Rx Power Intrusion Threshold field. If the threshold is exceeded, the message "ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress." displays. See "DMI (Diagnostic Maintenance Interface) Test" on page 196.

In-band control

A characteristic of network protocols with which data control is regulated. In-band control passes control data on the same connection as main data. Protocols such as HTTP use in-band control (conversely, Out-of-band control is used by protocols such as FTP). One of two common methods of transmitting SNMP requests and responses, by sending them on the same media as the user data. See also "Out-of-band control".

In-band signaling

The sending of metadata and control information in the same band, on the same channel, as used for data. For example, a telephone number is encoded and transmitted across the phone line as DTMF tones. These tones "control" the phone system by telling the telephone company's equipment where to route the call. See also "Out-of-band signaling".

IP

(Internet Protocol) One of the core protocols of the Internet Protocol Suite. IP is one of the two original components of the suite (the other being TCP), so the entire suite is commonly referred to as TCP/IP. IP is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

ITU

ITU is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services. For nearly 145 years, ITU has coordinated the shared global use of the radio spectrum, worked to improve telecommunication infrastructure in the developing world, and established worldwide standards that foster seamless interconnection of a vast range of communications systems. See http://www.itu.int/net/about/itu-t.aspx.

J1

A type of narrowband transmission facility, used exclusively in Japan, usually between a PBX and a switch. Line Type J1 standards include Signal Standard = Y-1, Number of Timeslots = 32, Bit Rate = 2.048 Mbps. Contrast “T1” and “E1”.

Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size, which is 1518 bytes (1522 if VLAN-tagged). Though this is not a standard, more vendors are adding support for jumbo frames. An initiative to increase the maximum size of the MAC Client Data field from 1500-bytes to 9000-bytes. The initiative was not adopted by the IEEE 802.3 Working Group, but it was endorsed by a number of other companies. Larger frames would provide a more efficient use of the network bandwidth while reducing the number of frames that have to be processed. The Jumbo Frame proposal restricts the use of Jumbo Frames to full-duplex Ethernet links, and defines a "link negotiation" protocol that allows a station to determine if the station on the other end of the segment is capable of supporting Jumbo Frames.

Kbps

(Kilobits Per Second) Data transfer speeds as measured in kilobits.

LAN

(Local Area Network) A group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building).

Last Gasp

This feature enables the device to store a small amount of power to enable it to send out an SNMP trap to alert the management console in the event of a power failure. The notification of an impending power loss before it happens allows for quicker resolution of the power loss.

LBM

(Loopback Message) A unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR.

LBO

(Line Build Out) a device, circuit, or configurable parameter used to reduce the signal strength to the right level for interfacing with terminal equipment. It can also reduce cross talk between pairs sharing the same sheath. It serves to correctly and continuously match the device automatically to any line length and to varying line parameters. The LBO compensates for the length variations ranging from 0 m to 200 meters of the 22 AWG twisted pair cable between a DS-1 line card and the DSX-1 cross-connect. At the cross-connect, the signal must fit into the North American DSX-1 standard pulse-shape mask.

LBR

(Loopback Reply) A unicast CFM PDU transmitted by an MP to a MEP, in response to an LBM received from that MEP.

LED

(Light Emitting Diode) An electronic light source.

Line

A unidirectional E1 or T1 physical connection.

Link

A unidirectional channel residing in one timeslot of a E1 or T1 Line, carrying 64 kbit/s (64'000 bit/s) raw digital data.

Little Endian

Bit ordering within a byte where bits are sent serially starting with the LSB (least significant byte) and ending with the MSB (most significant byte). Ethernet uses Little Endian bit ordering. Contrast "Big Endian".

LLDP

(Link Layer Discovery Protocol) A standard method for Ethernet Network devices such as switches, routers and wireless access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

Long Haul

For Gigabit Ethernet, one of several industry wiring types offered. 1000BASE-LX/LH is a long wavelength used with "long haul" fiber optic cable for a maximum length of 10 kilometers.

Long-haul optics refers to the transmission of visible light signals over optical fiber cable for great distances, especially with no (or minimal) use of repeaters. Fiber optic cable loss takes place because the wavelength determines the index of refraction (observed as a "loss-over-time" effect in long fiber optic cable runs). The energy for each signal can be kept within a narrow range of wavelengths, which has led to the development of WDM (wave-division multiplexing) and DWDM (dense wave-division multiplexing) to minimize loss problems.

On the x6110, a Long Haul cable type is used with Long Haul T1/E1; see Appendix F – Cable Specifications for more information. The x6210 Long Haul function is not applicable in DS3 mode.

Loopback (LB)

The Loopback feature puts a device in a special mode that enables the device to loop back the signal from the RX port to the TX port on either media for testing and troubleshooting purposes. Test signals can then be inserted into the link and looped back as received by a device to test a particular segment of the link (i.e. copper or fiber). Loopback can be either local or remote depending on the location of the converter in the link.

LOS

(Loss of Signal) an indicator on a networking device to indicate that a network signal or connection has been lost. If a LOS is encountered, it is an indication that the cable connected to the network device is bad, has no connection on the other end, network is improperly configured, or the network device itself is bad.

MAC

(Media Access Control) An address that is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN.

MAN

(Metropolitan Area Network) a network that interconnects users with computer resources in a geographic area or region larger than a LAN, but smaller than a WAN. Applies to the interconnection of networks in a city into a single larger network. Can also mean the interconnection of several LANs by bridging them with backbone lines.

Mbps

(Megabits per second) Data transfer speed measured in thousands of bits per second.

MCU (also µC, uC, or MCU)

(Micro-Controller Unit) is a small computer on a single integrated circuit containing a processor core, memory, and programmable input/output peripherals. Program memory in the form of NOR flash or OTP ROM is also often included on chip, an sometimes a small amount of RAM. Microcontrollers are designed for embedded applications (compared to microprocessors used in PCs or other general purpose applications. AKA “"computer on a chip”.

Media Converter

A device that changes: 1) a signal from one transmission media to another (e.g., from copper to optical fiber) or 2) from one signaling type to another (e.g., analog to digital).

Metro Ethernet

The use of Carrier Ethernet technology in a MAN. Since it is typically a collective endeavor with multiple financial contributors, Metro Ethernet offers a more cost-effective, reliable, scalable solution with bandwidth management than proprietary networks.

MIB

(Management Information Base) The set of variables that are used to monitor and control a managed device. A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP.

MIBs stems from the OSI/ISO Network management model and are a type of database used to manage the devices in a communications network. A MIB comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using a subset of Abstract Syntax Notation One (ASN.1) called "Structure of Management Information Version 2 (SMIv2)" RFC 2578. The database is hierarchical (tree-structured) and entries are addressed through object identifiers. IETF RFCs discuss MIBs, notably RFC 1155, "Structure and Identification of Management Information for TCP/IP based internets", RFC 1213, "Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, "A Simple Network Management Protocol".

MIB Module

Strictly speaking, a MIB is just a set of ideas; however, since the MIB Module is the most tangible representation of the MIB, the terms "MIB" and "MIB Module" are used interchangeably by many. To prevent naming conflicts and provide organization, all of the manageable features of all products from all vendors are arranged into one enormous tree structure referred to as the MIB Tree or "The MIB," which is managed by the Internet Assigned Numbers Authority (IANA). Each vendor of SNMP equipment has an exclusive section of The MIB Tree that they control.

MII

(Media Independent Interface) a standard interface used to connect a Fast Ethernet (i.e. 100 Mbit/s) MAC-block to a PHY chip. The MII may be used to connect the MAC to an external PHY via a pluggable connector (see photo), or to connect a MAC chip to a PHY chip on the same printed circuit board. Media independence allows the use of several different types of PHY devices for connecting to different media (i.e. Ethernet, fiber optic, etc.) without changing the MAC hardware. Equivalent MII standards/speeds are: AUI (for 10 megabit Ethernet), GMII (for gigabit Ethernet), and XGMII (for 10 gigabit Ethernet). The MII bus (standardized by IEEE 802.3u) is a generic bus that connects different types of PHYs to the same network Media Access Controller (MAC).

MSA

(Multi-Source Agreement) Common product specifications for pluggable fiber optic transceivers.

MT-RJ

(Mechanical Transfer-Registered Jack) A small form-factor fiber optic connector which resembles the RJ-45 connector used in Ethernet networks.

Multiplexing

The process where multiple channels are combined for transmission over a common transmission path. The two predominant ways of multiplexing are:

- Frequency Division Multiplexing (FDM)
- Time Division Multiplexing (TDM)

Multiplexing involves sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end. See also "TDM" or "DWDM".

NIC

(Network Interface Card or Network Interface Controller) A computer hardware component designed to allow computers to communicate over a computer network. A NIC is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using wireless communications or cables.

NID

(Network Interface Device) A device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In telecommunications, a NID is a device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In fiber-to-the-premises systems, the signal is transmitted to the customer premises using fiber optic technologies.
In general terms, a NID may also be called a Network Interface Unit (NIU), Telephone Network Interface (TNI), Slide-in-card (SIC), or a slide-in-module. See also "NIU".

NIU

(Network Interface Unit) a device that serves as a common interface for various other devices within a local area network (LAN), or as an interface to allow networked computers to connect to an outside network. A network interface card (NIC) is a type of NIU. The NIU converts protocols and associated code and acts as a buffer between connected hardware to enable an interface between a LAN and another network. See also "NID".

NMS

(Network Management Station) A high-end workstation that, like the Managed Device, is also connected to the network. A station on the network that executes network management applications that monitor and control network elements such as hosts, gateways and terminal servers. See also "SNMP".

Non Intrusive test

The ability to troubleshoot a circuit while it is in use.

NTP

(Network Time Protocol) A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

OID

(Object Identifier) Known as a “

MIB object identifier” or “MIB variable” in the SNMP network management protocol, an OID is a number assigned to devices in a network for identification purposes. Each branch of the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an Object ID or OID.

In SNMP, an Object Identifier points to a particular parameter in the SNMP agent.

OSI

(Open Systems Interconnection) A standard description or reference model for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementors so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication.

OUI

(Organizationally Unique Identifier) the Ethernet Vendor Address component. Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits, which specify the interface serial number for that interface vendor. These high-order 3 octets (6 hex digits) are called the Organizationally Unique Identifier or OUI.

Out-of-band control

A characteristic of network protocols with which data control is regulated. Out-of-band control passes control data on a separate connection from main data. Protocols such as FTP use out-of-band control. FTP sends its control information (user ID, password, and put/get commands) on one connection, and sends data files on a separate parallel connection. Since it uses a separate connection for the control information, FTP is considered to use "out-of-band control". See also "In-band control".

Out-of-band signaling

Generally, out-of-band refers to communications which occur outside of a previously established communication method or channel. In telecommunications, out-of-band communication exchanges call control information in a separate band from the data or voice stream, or on an entirely separate, dedicated channel. This is used for separating two different types of data. In computer networking, out-of-band data ("urgent data" in TCP) looks to the application like a separate data stream from the main data stream. Here, the out-of-band data may be lost if the application cannot keep up with it. See also "In-band signaling".

Pause

The Pause feature (data pacing) uses Pause frames for flow control on full duplex Ethernet connections. If a sending device is transmitting data faster than the receiving device can accept it, the receiving station will send a pause frame to halt the transmission of the sender for a specified period of time.

Pause frames are only used on full duplex Ethernet link segments defined by IEEE 802.3x that use MAC control frames to carry the pause commands. Only stations configured for full duplex operation can send pause frames.

PDU

(Protocol Data Units) **1.** Information that is delivered as a unit among peer entities of a network and that may contain control information, address information or data. **2.** In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol control information and possibly user data of that layer.

PHY

(Physical Interface) an abbreviation for the physical layer of the OSI model. An instantiation of PHY connects a link layer device (often called a MAC) to a physical medium such as an optical fiber or copper cable.

PoE

(Power over Ethernet) A system to safely transfer electrical power, along with data, to remote devices over standard category 5 cable in an Ethernet network. It does not require modification of existing Ethernet cabling infrastructure.

PON

(Passive Optical Network) A point-to-multipoint fiber to the premises network architecture using unpowered optical splitters. Passive optical networks do not use electrically powered components to split the signal. Instead, the signal is distributed using beam splitters. Each splitter typically splits the signal from a single fiber into 16, 32, or 64 fibers (depending on the manufacturer).

ITU-T G.983 / 984 sub-types include APON (ATM Passive Optical Network), BPON (Broadband PON), IEEE 802.3ah EPON or GEPON (Ethernet PON), and GPON (Gigabit PON).

Provisioning

In general, "providing" or “making available”. 1) The process of providing users with access to data and technology resources. 2) The process of providing customers or clients with accounts, the appropriate access to those accounts, and the rights associated with those accounts.

The process of preparing / equipping a network to allow it to provide one or more new services to its users (i.e., initial system setup). In telecom services, "provisioning" means "initiation" which includes changing the state of an existing service or capability. The provisioning process 1) monitors access rights and privileges to ensure the security of an enterprise's resources and user privacy, 2) ensures compliance and minimizes the vulnerability of systems to penetration and abuse, and 3) reduces the amount of custom configuration and the number of different configurations involved. Provisioning refers only to the setup or startup part of the service operation.

In the ION system, the prov xxxx commands are typically used for provisioning the system.

Red Alarm

A Red Alarm is declared after detecting a Loss of Signal, a Loss of Frame (a persistent OOF event), or an Alarm Indication Signal (AIS), for at least 2-10 seconds. A Red Alarm is cleared at the onset of 10 consecutive seconds with no SES (severely errored seconds). See also “Alarms”, “LOS”, “AIS”.

RJ-45

The standard connector utilized on 4-pair (8-wire) UTP (Unshielded Twisted Pair) cable. The RJ-45 connector is the standard connector for Ethernet, T1, and modern digital telephone systems.

RMII

(Reduced Media Independent Interface) a standard that addresses the connection of Ethernet physical layer transceivers (PHY) to Ethernet switches. It reduces the number of signals/pins required for connection to the PHY from 16 (for an MII-compliant interface) to between 6 and 10. RMII is capable of supporting 10 and 100 Mbit/s; gigabit interfaces need a wider interface.

RMON

(Remote Network Monitoring) Software that supports the monitoring and protocol analysis of LANs. RMON is a network management protocol that gathers remote network information. (Standard: RFC 1271.) See also “SNMP”.

Router

A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and an ISP/network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding packets, and protocols such as ICMP to communicate with each other and configure the best route between two hosts. Routers do not typically perform much filtering of data. Contrast "Switch".

RS-232

(Recommended Standard 232) A standard for serial binary data signals connecting between a Error! Reference source not found. (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

SDC

(Signal Detect on Copper) a x6210 status LED; when lit indicates twisted-pair copper link is up. Flashing LED (once/second) indicates transmitting on link if other link is down. Flashing LED (5 times/second) indicates All Ones detected on the Link. See also “SDF”.

SDF

(Signal Detect on Fiber) a x6210 status LED when lit indicates fiber link is up. Flashing LED (once/second) indicates transmitting on link if other link is down. Flashing LED (5 times/second) indicates All Ones detected on the Link. See also “SDC”.

SF

(Superframe Format - D4 Framing) The standard SF frame is 193 bits long (1 Framing bit + 24 8-bit timeslots). A Superframe consists of twelve 193-bit frames. A framing bit can support different functions, depending on which of the twelve frames it is in. Contrast “ESF”.

SFP

(Small Form-Factor Pluggable) A compact, hot-pluggable transceiver used in telecommunication and data communications applications. It interfaces a network device mother board (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. The SFP transceiver is specified by a multi-source agreement (MSA) between competing manufacturers. The SFP was designed after the GBIC interface, and allows greater port density (number of transceivers per inch along the edge of a mother board) than the GBIC, thus SFP is also known as “mini-GBIC”. Optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature lets you monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. AKA, Digital Optical Monitoring (DOM), DMI (Diagnostic Monitoring Interface), or DMM (Diagnostic Maintenance Monitoring).

SGMII

(Serial Gigabit Media Independent Interface) A standard Gigabit Ethernet interface used to connect an Ethernet MAC-block to a PHY. To carry frame data and link rate information between a 10/100/1000 PHY and an Ethernet MAC, SGMII uses a different pair for data signals and for clocking signals, with both being present in each direction (i.e., TX and RX).

SMAC

(Static MAC) A MAC address that is manually entered in the address table and must be manually removed. It can be a unicast or multicast address. It does not age and is retained when the switch restarts. You can add and remove static addresses and define the forwarding.

Smart Jack

A device used to test integrity of T-1 circuits remotely from a central office (CO). Installed at the customer premises in the form of a semi-intelligent demarcation point (demarc), the smart jack is completely passive until activated remotely by a digital code, (e.g., "FACILITY 2") sent down the T-1 line. This code activates a relay that breaks the T-1 circuit and closes a receive-to-transmit loop across the T-1 at the customer end, sending the signal back to the CO. This allows the CO to confirm the integrity of the loop without having to dispatch a roll (send a technician to the site).

SNMP

(Simple Network Management Protocol) A request-response protocol that defines network communication between a Managed Device and a Network Management Station (NMS). A set of protocols for managing complex IP networks. (Standard: RFC 1157.)

SNMP Message

A sequence representing the entire SNMP message, which consists of the SNMP version, Community String, and SNMP PDU.

SNMP SMI

(SNMP Structure of Management Information) a collection of managed objects, residing in a virtual information store. The SMI is divided into three parts: module definitions, object definitions, and, notification definitions. There are two types of SMI: SMIv1 and SMIv2. For additional information see IETF RFC 1155 v1 and RFC 2578 v2.

SNMP Version

An integer that identifies the version of SNMP (e.g., SNMPv1 = 0).

SNMP Community String

An octet string that may contain a string used to add security to SNMP devices.

SNMP PDU

An SNMP PDU contains the body of an SNMP message. There are several types of PDUs (e.g., GetRequest, GetResponse, and SetRequest).

SNTP

(Simple Network Time Protocol) A less complicated version of Network Time Protocol (NTP), which is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled via the Internet. SNTP is used to synchronize times on IP devices over a network. (Standard: RFC 2030.)

Static IP addressing

"Static" comes from the word stationary, meaning not moving. A static IP address means it never changes. A static IP address is an IP address permanently assigned to a workstation. If a network uses static addressing, it means that each network interface has an assigned IP address that it always uses whenever it is online. With static addressing, the computer has a well-defined IP address which it uses always and which no other computer ever uses.

Static MAC Entry

Static MAC entry support means that users can manually assign MAC addresses to ports that never age.

STP

(Shielded Twisted Pair) A special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground. Contrast with “UTP”.

STS-1

SONET (Synchronous Optical Networking) and SDH (Synchronous Digital Hierarchy) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or LEDs. The basic unit of framing in SDH is the Synchronous Transport Module, level 1 (STM-1) which operates at 155.52 Mbps. SONET refers to this basic unit as the Synchronous Transport Signal 3, concatenated (STS-3c) or OC-3c, depending on whether the signal is carried electrically (STS) or optically (OC), but its basic functionality, bit rate, and frame size are the same as for STM-1. SONET offers another unit of transmission, the Synchronous Transport Signal 1 (STS-1) or OC-1, operating at 51.84 Mbps. In SONET, the STS-3c/OC-3c signal is composed of three multiplexed STS-1 signals; the STS-3C/OC-3c may be carried on an OC-3 signal. Some manufacturers also support the SDH equivalent of the STS-1/OC-1, known as STM-0.

An STS-1 frame is 810 octets in size, and the STS-1 frame is transmitted as three octets of overhead, followed by 87 octets of payload. This is repeated nine times, until 810 octets have been transmitted, taking 125 μs.

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).

Switch

A networking device that filters and forwards packets between LAN segments. Switches operate at the data link layer (Layer 2) and sometimes the network layer (Layer 3) of the OSI Model, and can support virtually any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs. Contrast "Router".

Syslog

A service run mostly on Unix and Linux systems (but also available for other OSes) to track events that occur on the system. Analysis can be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

T1 (or T-1)

A type of narrowband transmission facility, used primarily in North America and parts of Asia. Line Type E1 standards include Signal Standard = DS1, Number of Timeslots = 24, Bit Rate = 1.544 Mbps. Contrast “E1” and “J1” formats.

T1 Line/ T1 Carrier

A T1 carrier is a commonly-used digital transmission service in the United States, Canada, and Japan. In these countries, a T1 line consists of 24 separate channels using pulse code modulation (PCM) signals with time-division multiplexing (TDM) at an overall rate of 1.544 million bits per second (Mbps). T1 lines originally used copper wire but now also include optical and wireless media. (Contrast with “E1” Line.)

T1 Frame Formats - SF and ESF

North American T1 facilities operate at 1.544 MBPS. Framing may be either Superframe (D4) format or Extended Superframe (ESF) format. A T1/E1 frame includes seven fields:

1. Preamble	7 octets of 1010_1010
2. SFD	1 octet,1010_1011
3. rData	4 octet, reserved data
4. mData	4 octet, management data
5. PAD	48 octet, used for padding purpose
6: sData	4 octets, TDM Payload data (DS3/E3 or T1/E1)
7. FCS	4 octet, Frame check sequence

Contrast “DS3 Frame Format”.

TAOS

(Transmit All Ones) a circuit or device that generates and sends a series of digital "ones" on a line for testing purposes. The x6210 has built-in troubleshooting with the addition of a selectable TAOS (transmit all ones): switch on the fiber and copper interfaces allows the network engineer to test all T1/E1 equipment on that network segment and ensure the network link. The x6210 provides TAOS Enable/Disable on copper and fiber port, which can be managed by x6210 software or hardware DIP switch setting.
The x6210 generates the AIS by transmitting all ones (TAOS).

TIA

(Telecommunications Industry Association) a trade association in the US that represents about 600 telecommunications companies. It helps create universal networking and education standards for the telephony, data networking, and convergence industry. The TIA has helped develop networking standards that have been used worldwide, including:

- TIA/EIA-568-B (telecomm cabling standards used in most voice, video and data networks)
- TIA J-STD-607 (Commercial grounding / Earthing - standards)
- TIA TIA/EIA-598 (Fiber Optic color coding)

TIA 568 Standard

The Commercial Building Telecommunications Wiring Standard commonly used in North America.

TCP

(Transmission Control Protocol) One of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

TCP/IP

(Transmission Control Protocol/Internet Protocol) The basic communication language or protocol of the Internet and/or a private network (either an intranet or an extranet).

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol (TCP), manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol (Intrusion detection

A form of security management for computers and networks that gathers and analyzes information from various areas to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

You can set up x6010 intrusion detection using the CLI command “Rx Power Intrusion Threshold”, or via the web interface from x6010 > Port 2 > DMI tab > Rx Power Intrusion Threshold field. If the threshold is exceeded, the message "ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress." displays. See "DMI (Diagnostic Maintenance Interface) Test" on page 196.

In-band control

A characteristic of network protocols with which data control is regulated. In-band control passes control data on the same connection as main data. Protocols such as HTTP use in-band control (conversely, Out-of-band control is used by protocols such as FTP). One of two common methods of transmitting SNMP requests and responses, by sending them on the same media as the user data. See also "Out-of-band control".

In-band signaling

The sending of metadata and control information in the same band, on the same channel, as used for data. For example, a telephone number is encoded and transmitted across the phone line as DTMF tones. These tones "control" the phone system by telling the telephone company's equipment where to route the call. See also "Out-of-band signaling".

IP), handles the address part of each packet so that it gets to the right destination.

TDM

(Time Division Multiplexing) A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end, based on the timing. TDM provides digital multiplexing where two or more apparently simultaneous channels are derived from a given frequency spectrum (i.e., a bit stream) by interleaving pulses representing bits from different channels. Successive pulses represent bits from successive channels (e.g., voice channels in a T1 system). TDM multiplexing occurs when two or more signals or bit streams are transferred apparently simultaneously as sub-channels in one communication channel, but are physically taking turns on the channel. The time domain is divided into several recurrent timeslots of fixed length, one for each sub-channel. A sample byte or data block of sub-channel 1 is transmitted during timeslot 1, sub-channel 2 during timeslot 2, etc. One TDM frame consists of one timeslot per sub-channel plus a synchronization channel (and possibly an error correction channel) before synchronization. After the last byte (data block), the cycle starts all over again with a new frame, starting with the second sample, byte or data block from sub-channel 1, etc.

TDR

1. (Time Domain Reflectometry) A measurement technique used to determine the characteristics of electrical lines by observing reflected waveforms. **2.** (Time Domain Reflector) An electronic instrument used to characterize and locate faults in metallic cables (for example, twisted wire pairs, coaxial cables). It can also be used to locate discontinuities in a connector, printed circuit board, or any other electrical path.

Telnet

A user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. Telnet is a terminal emulation program for TCP/IP networks that runs on your computer and connects your PC to a switch management. (Standard: RFC 854.)

TFTP

(Trivial File Transfer Protocol) A file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). Due to its simple design, TFTP can be implemented using a very small amount of memory. Because it uses UDP rather than UDP for transport, TFTP is typically used to transfer firmware upgrades to network equipment.

TFTP Download / Upload

The ability to load firmware, configuration files, etc. through a TFTP server. (AKA, TFTP. Standard: RFC 1350.)

TFTP Root Directory

The location on the console device (PC) where files are placed when received, and where files to be transmitted should be placed (e.g., *C:\TFTP-Root*).

TFTP Server

An application that uses the TFTP file transfer protocol to read and write files from/to a remote server. In TFTP, a transfer begins with a request to read or write a file, which also serves to request a connection. If the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and must be acknowledged by an acknowledgment packet before the next packet can be sent. Examples of available packages include Open TFTP Server, Tftpd32, WinAgents TFTP Server for Windows, SolarWinds free TFTP Server, TFTP Server 1.6 for Linux, and TftpServer 3.3.1, a TFTP server enhancement to the standard Mac OSX distribution.

Throughput

The maximum rate at which no frame is dropped. This is typically measured under test conditions.

TIA 568 Standard

The Commercial Building Telecommunications Wiring Standard commonly used in North America.

TLS

(Transport Layer Security) A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (**Error! Reference source not found.**).

TOS

(Type of Service) The ToS byte in the IPv4 header has had several purposes over time, and has been defined in various ways by IETF RFC 791, RFC 1122, RFC 1349, RFC 2474, and RFC 3168. Currently, the ToS byte is a six-bit Differentiated Services Code Point and a two-bit Explicit Congestion Notification field.

The ToS model described in RFC 2474 uses the Differentiated Services Field (DS field) in the IPv4 Header and IPv6 Header. See also CoS and QoS.

Trap

In SNMP, a trap is a type of PDU used to report an alert or other asynchronous event about a managed subsystem.

Also, a place in a program for handling unexpected or unallowable conditions - for example, by sending an error message to a log or to a program user. If a return code from another program was being checked by a calling program, a return code value that was unexpected and unplanned for could cause a branch to a trap that recorded the situation, and take other appropriate action.

An ION system trap is a one-way notification (e.g., from the IONMM to the NMS) that alerts the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the IONMM rather than the NMS. For a management system to understand a trap sent to it by the IONMM, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Trunk

A bidirectional E1 or T1 physical connection.

TCP/UDP Port Prioritization

The ability to prioritize traffic internally based on a TCP or UDP port number. (AKA, Layer 4 Prioritization.)

TTL

(Time to live) an Ethernet counter that records the number of times a transmission is sent/received without errors. TTL specifies how long a datagram is allowed to “live” on the network, in terms of router hops. Each router decrements (reduces by one) the value of the TTL field prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

The default TTL for ION software is 64. This means that a test packet must be successfully sent and received 63 times before a TTL expired message is generated. You can change the TTL value (e.g., a value of 255 is a demanding test because the packet must be sent and received error free 254 times).

UDP

(User Datagram Protocol) A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an Intrusion detection

A form of security management for computers and networks that gathers and analyzes information from various areas to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

You can set up x6010 intrusion detection using the CLI command “Rx Power Intrusion Threshold”, or via the web interface from x6010 > Port 2 > DMI tab > Rx Power Intrusion Threshold field. If the threshold is exceeded, the message "ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress." displays. See "DMI (Diagnostic Maintenance Interface) Test" on page 196.

In-band control

A characteristic of network protocols with which data control is regulated. In-band control passes control data on the same connection as main data. Protocols such as HTTP use in-band control (conversely, Out-of-band control is used by protocols such as FTP). One of two common methods of transmitting SNMP requests and responses, by sending them on the same media as the user data. See also "Out-of-band control".

In-band signaling

The sending of metadata and control information in the same band, on the same channel, as used for data. For example, a telephone number is encoded and transmitted across the phone line as DTMF tones. These tones "control" the phone system by telling the telephone company's equipment where to route the call. See also "Out-of-band signaling".

IP network. It's used primarily for broadcasting messages over a network.

Unicast

One of the four forms of IP addressing, each with its own unique properties. The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient. See also Multicast.

Unicast destination

A host or router that can be identified by a unique unicast IP address. See also Multicast destination.

USB

(Universal Serial Bus) A plug-and-play interface between a computer and add-on devices, such as media players, keyboards, telephones, digital cameras, scanners, flash drives, joysticks and printers.

UTC

(Coordinated Universal Time) A time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich.

UTP

(Unshielded Twisted Pair) The most common form of twisted pair wiring, because it is less expensive and easier to work with than STP (Shielded Twisted Pair). UTP is used in Ethernet 10Base-T and 100Base-T networks, as well as in home and office telephone wiring. The twist in UTP helps to reduce crosstalk interference between wire pairs. Contrast “STP”.

VAC

Volts AC (alternating current, as opposed to DC – direct current).

VCP

(Virtual Com Port) A driver that allows a USB device to appear as an additional COM port. The USB device can be accessed by an application in the same manner as a regular COM port.

Varbind

(Variable bindings) In SNMP, a sequence of two fields, an Object ID and the value for/from that Object ID.. It's the variable number of values that are included in an SNMP packet. Each varbind is made of an OID, type, and value.

VDC

Volts DC (direct current, as opposed to AC – alternating current).

VOIP

(Voice over Internet Protocol) A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks.

Well Known Ethernet Multicast Addresses

Some common Ethernet multicast MAC addresses are shown below with their related Field Type and typical usage.

Ethernet Multicast Address	Usage
01-00-0C-CC-CC-CC	CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)
01-00-0C-CC-CC-CD	Cisco Shared Spanning Tree Protocol Address
01-80-C2-00-00-00	Spanning Tree Protocol (for bridges) (IEEE 802.1D)
01-80-C2-00-00-01	Ethernet OAM Protocol (IEEE 802.3ah)
01-80-C2-00-00-02	IEEE Std 802.3 Slow Protocols multicast address
01-80-C2-00-00-03	IEEE Std 802.1X PAE address
01-80-C2-00-00-04	IEEE MAC-specific control protocols
01-80-C2-00-00-08	Spanning Tree Protocol (for provider bridges) (IEEE 802.1AD)
01-00-5E-xx-xx-xx	IPv4 Multicast (RFC 1112)
33-33-xx-xx-xx-xx	IPv6 Multicast (RFC 2464)

Well Known Ports

The set of all available port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. The Well Known Ports are those from 0 through 1023. The Registered Ports are those from 1024 through 49151. Registered ports require IANA registration. The Dynamic and/or Private Ports are those from 49152 through 65535. Port 443 is reserved for the HTTPS, port 179 for the BGP Border Gateway Protocol, and port 161 for SNMP.

To see all the used and listening ports on your computer, use the **netstat** (or similar) command line command. For further port assignment information, see IETF RFC 1700.

Port Number	Description
20	FTP
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
143	Interim Mail Access Protocol (IMAP)
161	SNMP /TCP
161	SNMP /UDP
161	SNMPTRAP /TCP
162	SNMPTRAP /UDP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
546	DHCP Client
547	DHCP Server

xSTP

Spanning Tree Protocols (multiple variations) defined in MEF specification 17. See also “STP”.

Yellow Alarm

A Yellow Alarm is declared after detecting the Yellow Signal. See ANSI T1.107-1989.

Index

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA

Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Printed in the U.S.A.
ION System x6210 Managed DS3-T3/E3 to Fiber Network Interface Device (NID) User Guide,
33495 Rev. B