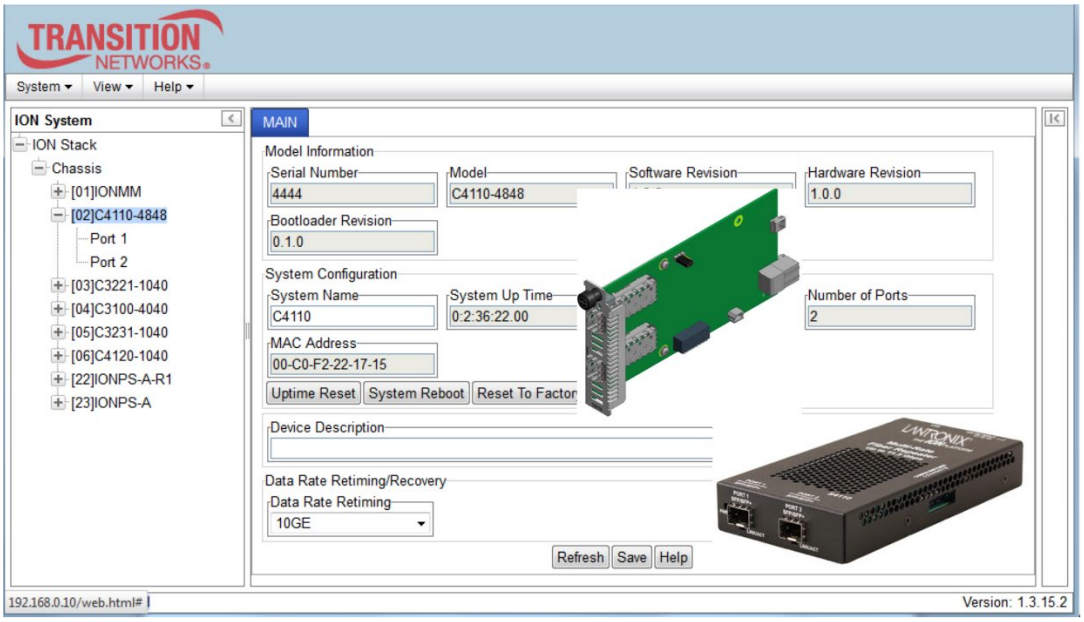
LANTRONIX®




# ION System

## x4110

### 10 Gbps Fiber-to-Fiber Converter

### Slide-in-Module and NID

## Web User Guide

**Part Number 33574**
**Revision E August 2023**

## Intellectual Property



## Warranty

For details on the Lantronix warranty policy, go to http://www.lantronix.com/support/warranty.

## Contacts

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

**Technical Support**

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

**Sales Offices**

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

## Disclaimer

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

## Revision History

| Rev | Date | Description |
|---|---|---|
| A | 3/2/15 | Initial release for v 1.2.4. |
| B | 9/12/16 | Update for C4110 v1.2.6; add Vendor Specific Info to DMI; add C4110 support in Focal Point; update driver installation and contact information. |
| C | 12/6/17 | Remove Loopback and update LPT description. |
| D | 3/30/23 | Initial Lantronix re-brand. Remove Glossary, Index, Warranty, and Compliance information. |
| E | 8/22/23 | Update to FW v2.0.5:<br>• Reset input and output buffers on LOS signal detect.<br>• Correctly report SFP vendor specific info in DMI statistics of web UI.<br>• C4110 updates will work with IONMM v 1.4.3 or higher.<br>• Allow time to check link status and send traps. |

# Contents

# 1: Introduction

## Document Overview

The purpose of this manual is to provide the user with an understanding of the Lantronix x4110 Ethernet media converter's web interface. For S4110 and C4110 models, product description, features, applications, manageable features and protocols, see the model-specific Install Guide.

## Related Manuals and Online Help

A printed documentation card is shipped with each x4110 device. Note that this manual provides links to third party web sites for which Lantronix is not responsible. Other ION system and related device manuals are listed below.

- Product Documentation Postcard, 33504
- ION C4110 Install Guide, 33572 (this manual)
- ION S4110 Install Guide, 33573
- ION x4110 Web User Guide, 33574
- ION x4110 CLI Reference, 33575
- ION Management Module (IONMM) Install Guide, 33420 and User Guide, 33457
- 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 Record of Revisions on page 2. Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

## For More Information

For Lantronix Documentation, Firmware, App Notes, etc. go to https://www.lantronix.com/technical-support/. Note that this manual provides links to third party web sites for which Lantronix is not responsible.

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

For Lantronix Warranty Policy & Procedure information go to https://www.lantronix.com/technical-support/warranty/.

See the related Install Guide for Safety Warnings and Cautions, Safety Statements, Application Examples, Network Scenarios, Pre-Installation, DIP Switch and Jumper settings, and other important information.

## Starting the Web Interface

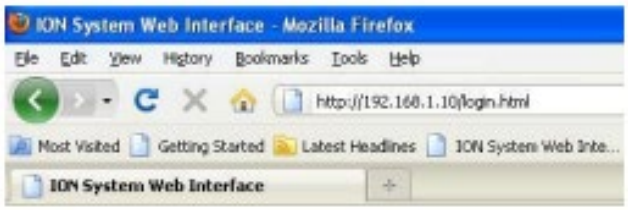
The C4110 can be controlled and configured from a remote management station via the Web UI over an Ethernet connection. Information is entered into fields on the various screens of the interface. Note: fields that have a grey background cannot be modified.

**Important**

- Do not use the browser's back button to navigate the screens. This causes the connection to drop.
- Do not use the keyboard's back space key in grayed out fields. This causes the connection to drop.
- For DHCP operations, a DHCP server must be on the network and available.

**To sign in to the C4110 via the Web:**

1. Open a web browser.



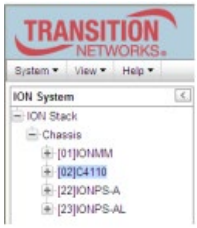


2. In the address (URL) block, type the IP address of the IONMM (the default address is 192.168.1.10).
3. Click Go or press Enter. The ION System sign in screen displays.

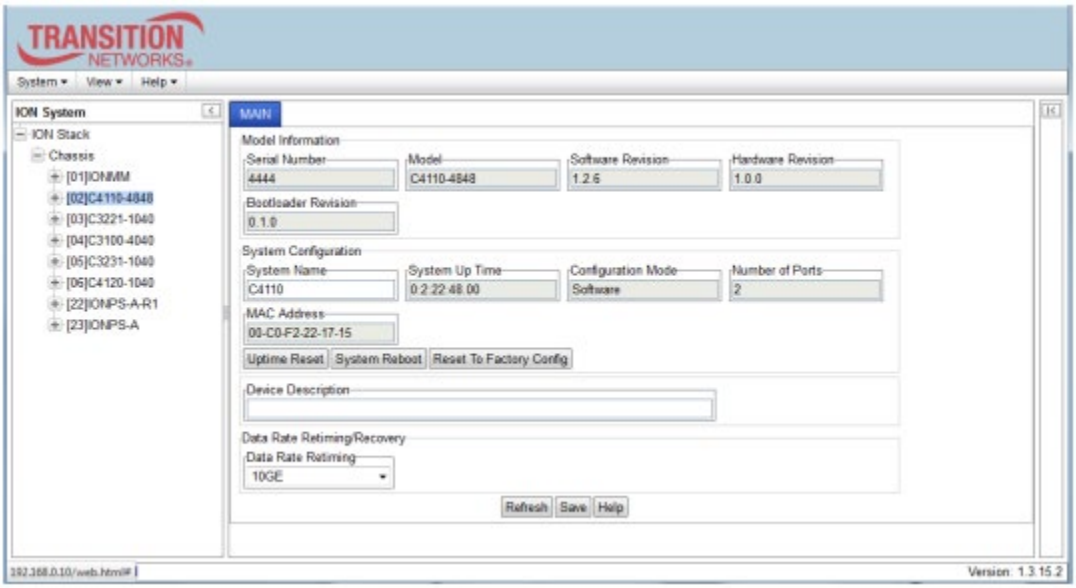

**Note**: If your systems uses a security protocol (e.g., RADIUS, SSH, etc.), you must enter the login and password required by that protocol.

1. Type the System name (the default is ION). Note: the System name is case sensitive - all upper case.
2. Type the password (the default is private). Note: the password is case sensitive - all lower case.
3. Click Sign in or press Enter. The opening screen displays.


4. Click the plus sign [+] next to ION Stack to unfold "ION Stack" node in left tree view and refresh device status.
5. Click the plus sign [+] next to Chassis to unfold the chassis devices.




6. Select the appropriate C4110-4848 device. The MAIN screen displays for the selected C4110.




7. You can use the various fields to configure the device and ports as described in the following sections.

**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

To sign out from the Web UI, in the upper left corner of the ION System Web Interface:

1. Click the System dropdown.
2. Click Sign out. The ION sign- in screen displays.

**Note**: The C4110 does not automatically log out upon exit or after a timeout period, which could leave it vulnerable if left unattended. Follow your organizational policy on when to sign out from the ION System via the Web Interface.

## Documentation Conventions

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

**Table 1: Documentation Conventions**

| Convention | Meaning |
|---|---|
| **Boldface** text | Indicates the entry must be made as shown. For example:<br>ipaddr=<addr><br>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:<br>ipaddr=<addr><br>In place of <addr> you must enter a valid IP address. |
| [ ] | Indicates an optional keyword or parameter. For example:<br>go [s=<xx>]<br>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:<br>state={enable \| disable}<br>Enter state=enable or state=disable. |
| “ ” | Indicates that the parameter must be entered in quotes. For example:<br>time=<“value”><br>Enter time=”20100115 13:15:00”. |
| > | Indicates a selection string. For example:<br>Select File > Save.<br>This means to first select/click File then select/click Save |

# 2. Management Methods

## General

The x4110s are managed either directly or through the IONMM. Whether the x4110is managed directly or indirectly, management is accomplished through one of the following methods.

- 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 x4110 can be remotely managed directly (i.e., not through IONMM). This enables administrators to monitor and configure remote stand-alone x4110s straight from the Network Management Station (NMS) without leaving the office.

## IONMM Managed Devices

IONMM devices that are managed through the IONMM are either chassis resident (x4110) or standalone modules (S32xx or media converters) that are connected as remotes to chassis resident modules.

Communications between the IONMM and remote devices is through the ION Chassis backplane. See the IONMM User Guide for details.

### Managing Slide-In and Remote Modules via the Web Interface

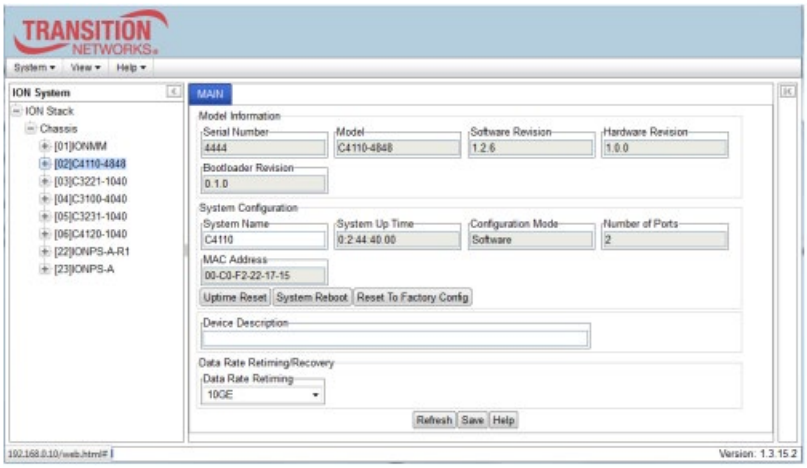
1. Access the x4110 via the Web interface (see “Starting the Web Interface”).
2. Click on the slide-in module or port to be managed.
3. The operations that can be performed depend on the type of slide-in module. Refer to the product documentation for the information. See the “Related Manuals and Online Helps” section.

## Direct Managed Devices

Direct management is for standalone devices that are not connected to a module that is managed through the ION Management Module (IONMM). In direct management, the network and/or USB cable is connected directly to the module to be managed.

### Managing Standalone Modules via the IONMM Web Interface

1. Access the x4110 through the Web interface (see “Starting the Web Interface”).
2. Click the plus sign [+] next to ION Stack to unfold the "ION Stack" node in the left tree view if not already done.
3. Click the plus sign [+] next to Chassis and click the plus sign [+] next to a module.




4. Click on the module to be managed (e.g., the C4110-4848 module above).
5. Select the various tabs to perform the applicable operations.

## Menu System Descriptions

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

**Table 2: System-Level Menu Description**

| Dropdown / Tab | Description |
|---|---|
| **ION System pane** | **ION Stack** - consists of one chassis or one standalone device. The Stack Members table lists the Stack's chassis and its type.<br>**Chassis** - the ION System family of products; the Chassis View shows a summary view of one such chassis. Model Information includes:<br>* Serial Number - The serial number of the chassis itself. Individual x4110s also have their own serial numbers.<br>* Model Name - The exact model name of this device (e.g., ION219). When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number.<br>* Software Revision, Hardware Revision, and Bootloader Revision.<br>* Chassis Members table - lists local physical components in slots 1 to 19.<br>**Device** – provides tabs and sub-tabs for the IONMM and x4110s in the ION system.<br>**Port** - provides tabs and sub-tabs for a selected x4110 port. |
| **System** Dropdown | Sign out |
| **View** Dropdown | Refresh |
| **Help** Dropdown | Online Help, ION Product Home Page, and About ION System Web Interface. |
| **MAIN** Tab | **Sections**: Model Information, System Configuration, Device Description, and Data Rate Timing/Recovery sections.<br>**Buttons**: Uptime Reset, System Reboot, Reset To Factory Config buttons. Refresh, Save, and Help buttons |

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

**Table 3: Port-Level Menu Description**

| Tab | Description |
|---|---|
| **Main** tab | Sections: Circuit ID and Port Configuration.<br>Buttons: Refresh, Save, and Help. |
| **DMI** tab | Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length, and Vendor Specific Information.<br>The DMI (Diagnostic Maintenance Interface) function displays x4110 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information.<br>**Note**: not all SFP models support DMI. Models that support DMI have a "D" at the end of the model number. If you click the DMI tab on a x4110 model that does not support DMI, the message "*The DMI feature is not supported on current port*."<br>Buttons: Refresh, Save, and Help. |

### Reboot, Reset, and Power Off Function Notes

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

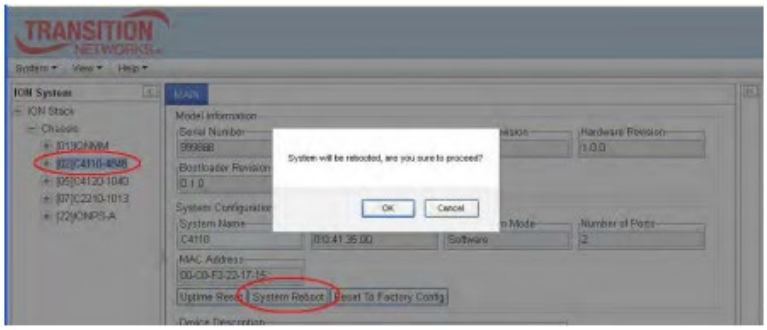
For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- Table 5: File Status after a Reset to Factory Defaults on age 24
- Table 6: File Content and Location after a System Reboot on page 27

**Caution**: 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. Note that a System Reboot can take several minutes.




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 *[02]C4110-4848 is rebooting...* displays for a while; when done, the message *[02]C4110-4848 rebooting finished*" displays. You can click the **Refresh** button to clear the message.

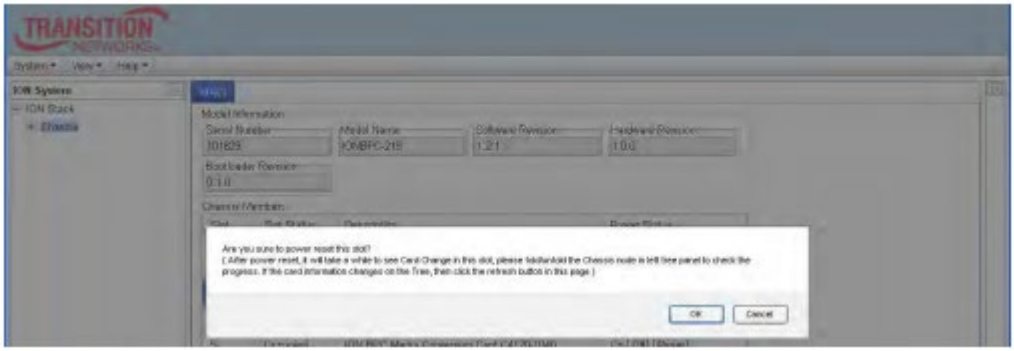
## Reset To Factory Config

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

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

## Reset Power to a Slot

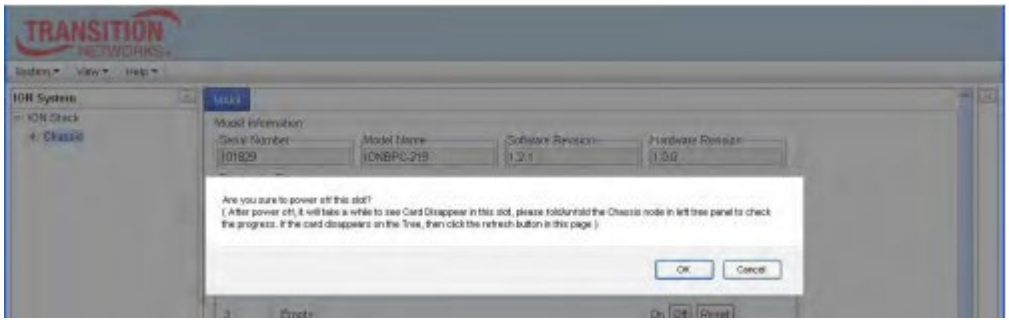
At the Chassis > MAIN tab, you can click the Reset button to reset power for the selected slot in the chassis. The message "Are you sure to power reset this slot?" displays.



After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page. If you are not sure that you want to reset this chassis, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot

## Power Off a Slot

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



If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot. After power off, it will take a while for the card to disappear from this slot; fold/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.

# 3: Configuration

## General

After the x4110 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 x4110. Configurations can be done either by entering CLI commands (USB / Telnet) or through a Web interface. For complete descriptions of all CLI commands, see the x4110 CLI Reference.

The operating characteristics that can be defined for the x4110 are:

- System name
- Features
  - Device Description
  - Data Rate Retiming
- Port setup
  - Circuit ID
- DMI (Diagnostic Monitoring Interface)
  - Rx Power Intrusion Threshold (µW)

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

## System Configuration

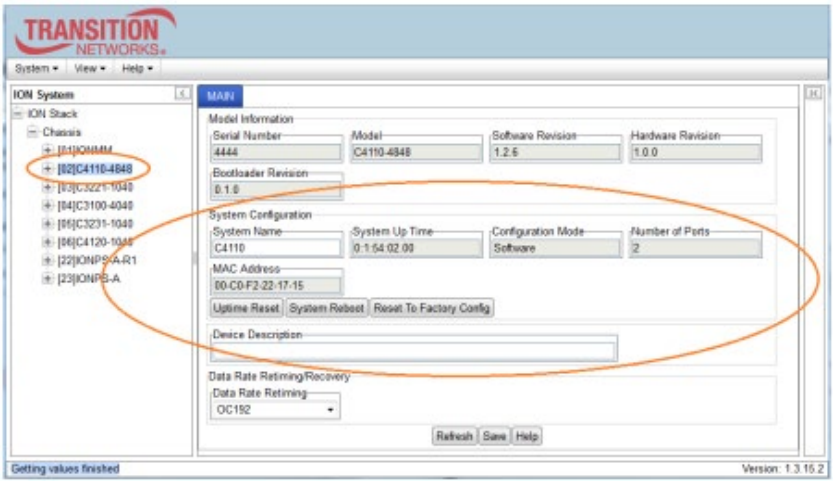
The system configuration defines:

- a name for the C4110
- a device description (optional)

The entry for the system name must be a text string with no spaces between characters. Note that numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed. The system configuration can be defined via the Web interface as described below.

### System Configuration – Web Method

1. Access the x4110 via the Web interface.
2. At the device's MAIN tab, locate the System Configuration section.



3. In the System Name field, enter the name and for the x4110. The name can be alphabetic, numeric or a combination, but cannot contain any spaces between the characters.
4. Scroll to the bottom and click Save.

## Device Description Configuration

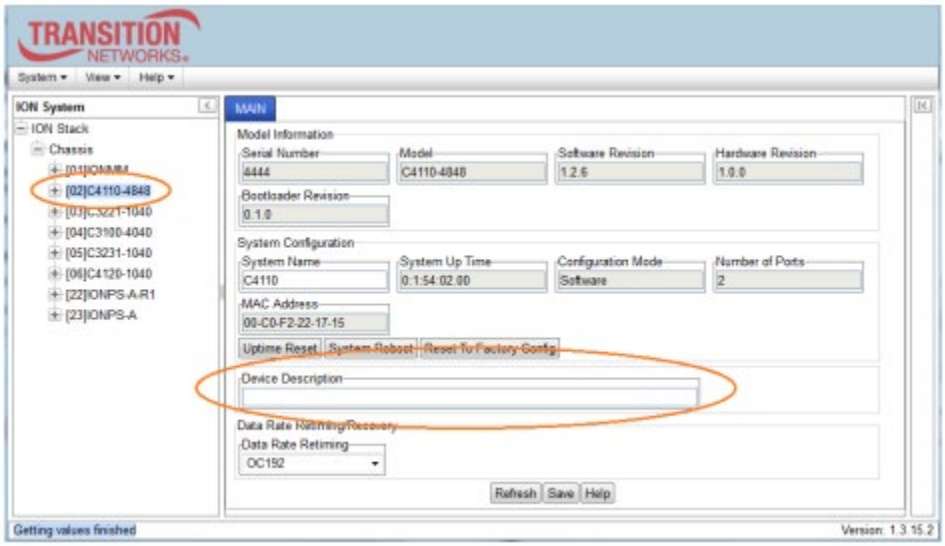
The x4110 supports a Device Description at the device level and a Circuit ID at the port level.

The Device Description provides the option to configure an ASCII text string up to 63 bytes and override the default information, which is vlan-module-port in binary format.

The Device Description can be configured in the x4110 via the Web a follows.

**Device Description Config – Web Method**

1. Access the x4110 via the Web interface.
2. At the x4110 MAIN tab, locate the Device Description section.
3. Enter the Device Description of up to 64 bytes for the device.




4. Scroll to the bottom and click the **Save** button.

If you enter more than 64 characters for the Device Description and then click Save, the characters entered display in red, and the message “Invalid input found!” displays in the lower left corner of the Web interface.

To recover:

a) Click Refresh, and re-enter a Device Description of 64 or fewer characters and click Save.

b) The message “Setting values succeeded” displays in the lower left corner of the Web interface.

## Data Rate Timing/Recovery Configuration

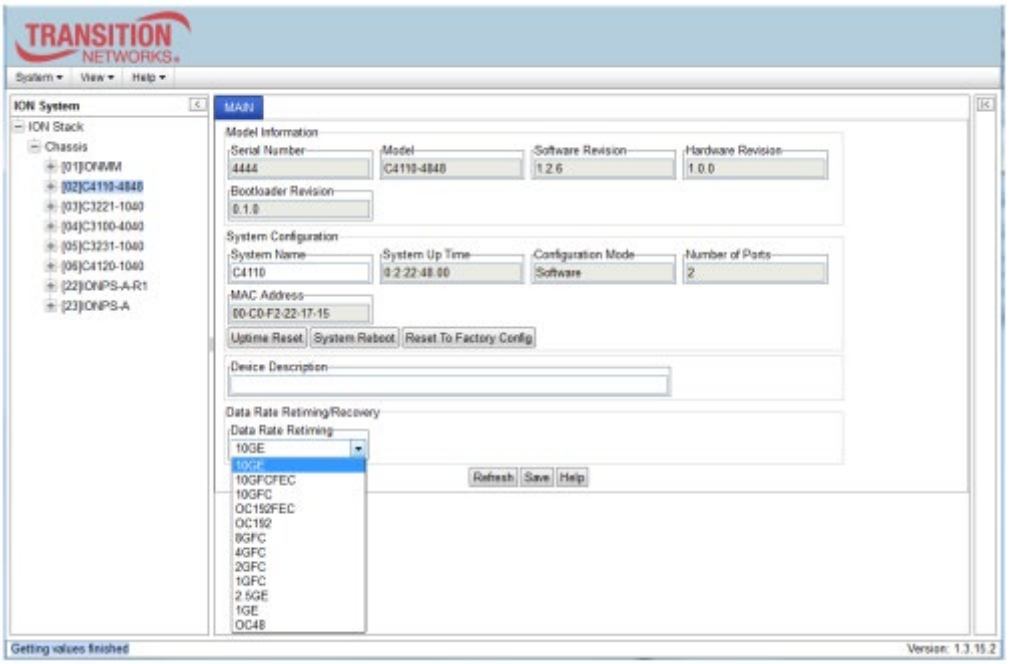
The C4110 can be used in applications where links supporting data rates from 1Gig to 10Gig require fiber extension or where 10Gig links require an interface between two fiber networks. It performs 3R (reamplify, re-shape, re-time) signal regeneration. The S4110 is protocol 'agnostic', supporting a wide variety of protocols in a network; from 1 to 11.5Gbps, including 10G LAN, 10G WAN, 10G Fiber Channel, SONET OC192, 10G OTN (G.709), 1/2/4/8 Gig Fiber Channel, 1 Gig Ethernet, or Sonet OC48. The fiber length and type is defined by the SFP+ module inserted.

The OC (Optical Carrier) specifies the speed of fiber optic networks conforming to the SONET standard.

The speeds for common OC levels include OC-1 = 51.85 Mbps, OC-3 = 155.52 Mbps, OC-12 = 622.08 Mbps, OC-24 = 1.244 Gbps, OC-48 = 2.488 Gbps, OC-192 = 9.952 Gbps, and OC-255 = 13.21 Gbps.

**Device Description Config – Web Method**

1. Access the x4110 via the Web interface.
2. At the x4110 MAIN tab, locate the Device Description section.
3. At the dropdown, select the Data Rate Retiming value.




4. Scroll to the bottom and click the **Save** button.

The Data Rate Retiming values are described below.

**Table 4: Data Rate Retiming Values**

| Data Rate | Description |
|---|---|
| 10GE | 10 gigabit Ethernet (10GbE or 10 GigE) (factory default). |
| 10GFCFEC | 10GFC + FEC = 10GbE Fibre Channel with Forward Error Correction. |
| 10GFC | 10GbE Fibre Channel. |
| OC192FEC | WAN/OC-192+FEC = OC-192 network line with transmission speeds up to 9953.28 Mbit/s with Forward Error Correction. |
| OC192 | WAN/OC-192 = OC-192 network line with transmission speeds up to 9953.28 Mbit/s. |
| 8GFC | 8G Fiber Channel with 8.5 gigabaud Line rate and 1,600 MBps throughput (at full duplex). |
| 4GFC | 4G Fiber Channel with 4.25 gigabaud Line rate and 800 MBps throughput (at full duplex). |
| 2GFC | 2G Fiber Channel with 2.125 gigabaud Line rate and 400 MBps throughput (at full duplex). |
| 1GFC | 1GbE Fibre Channel |
| 25GE | 2.5 gigabit Ethernet |
| 1GE | 1 gigabit Ethernet. |
| OC48 | Sonet OC-48 network line with transmission speeds to 2488.32 Mbit/s. |

## Circuit ID Configuration

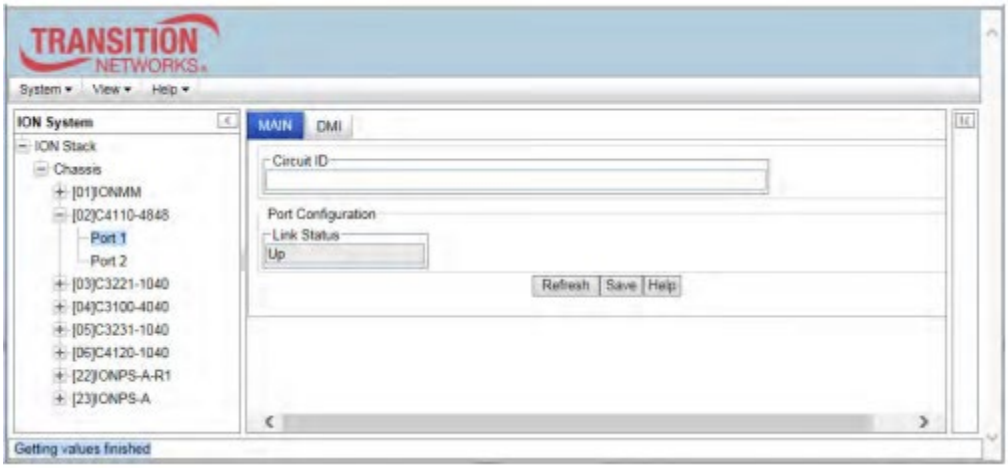
The x4110 supports a Device Description at the device level and a Circuit ID at the port level. The Circuit ID provides the option to configure an ASCII text string up to 64 bytes and override the default information, which is vlan-module-port in binary format. The Circuit ID can be configured in the x4110 via the Web as follows.

**Circuit ID Config – Web Method**

1. Access the x4110 via the Web interface (see “Starting the Web Interface”).

2. Select the appropriate port and locate the Circuit ID field.

3. Enter the Circuit ID of up to 64 bytes for the port. The default is blank.




4. Click Save to update screen information.

5. Repeat steps 2 -4 for each port as required.

6. Click Save when done. If you enter more than 64 characters for the Circuit ID and then click Save, the characters entered display in red, and the message “Invalid input found!” displays in the lower left corner of the Web interface. To recover: a) Click Refresh, and re-enter a Circuit ID of 64 or fewer characters and click Save. b) The message “Setting values succeeded” displays in the lower left corner of the Web interface.

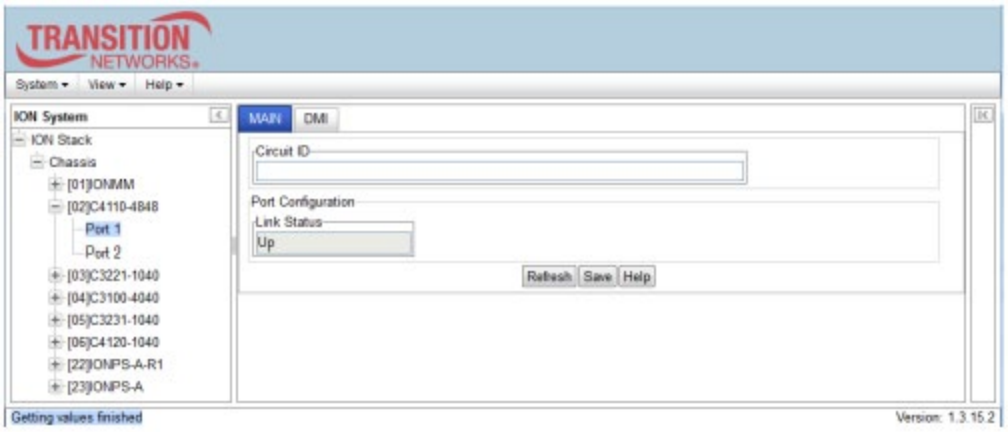
## Ethernet Port Configuration

A port's Ethernet port speed and link status can be verified in the x4110 via the Web GUI as follows.

**Ethernet Port Config – Web Method**

Use this procedure to set the Circuit ID for the Ethernet port and to check the port's link status.

1. Access the x4110 via the Web interface.
2. Select the appropriate port.
3. Locate the Port Configuration section on the port's MAIN tab.




4. Check the Link Status parameter value (read only) for the current port's link status (Up or Down).
5. Click the Refresh button if necessary.

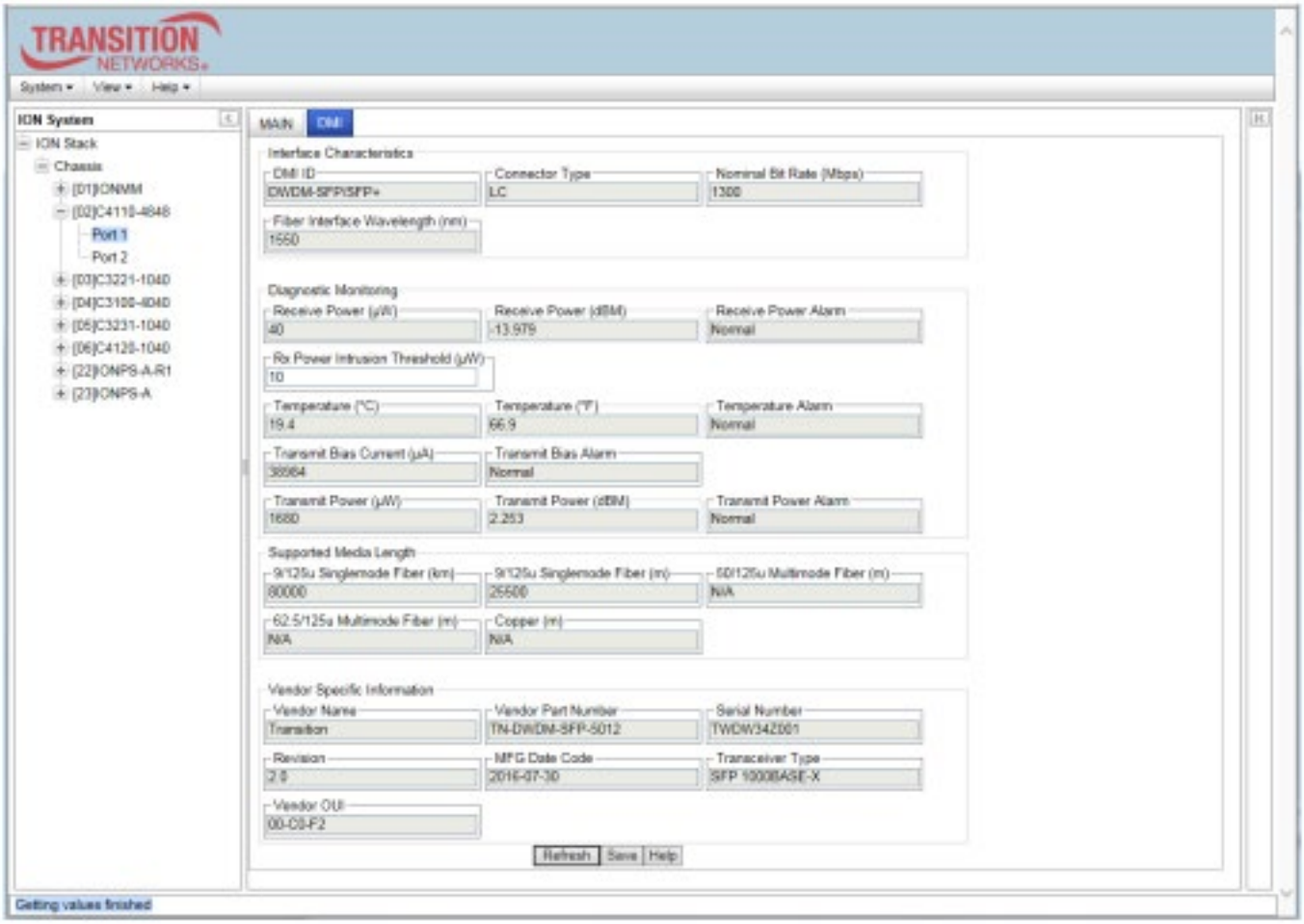
## DMI (Diagnostic Maintenance Interface)

The DMI (Diagnostic Maintenance Interface) function displays x4110 SFP/SFP+ diagnostic and maintenance data such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. For more SFP/XFP information see the Lantronix SFP webpage.

DMI can be configured in the x4110 via the Web GUI as follows.

**DMI Config – Web Method**

1. Access the x4110 via the Web UI.
2. Select the desired device and port.
3. Select the DMI tab.




4. The Interface Characteristics, Diagnostic Monitoring, Supported Media Length, and Vendor Specific Information sections display. See the table below for parameter descriptions.
5. You can click the Refresh button to update the information displayed. You can click the Save button to save the updated information.

The DMI tab parameters are described in the table below.

**Table 5: DMI Parameters**

| Parameter | Possible Parameters | Description |
|---|---|---|
| DMI ID | Unknown, GBIC, soldered to motherboard, SFP, Reserved, vendor-specific | Specifies the physical device from SFF-8472 Rev 9.5 Standard:<br>00h Unknown or unspecified<br>01h GBIC<br>02h Module/connector soldered to motherboard<br>03h SFP<br>04-7Fh Reserved<br>80-FFh Vendor specific |
| Connector Type | LC, MT-RJ LC, SC, ST, RJ-45, VF-45, or unknown | The external optical or electrical cable connector provided as the interface.<br>* MT-RJ: Media Termination - Recommended Jack for Duplex multimode connections.<br>* LC: Lucent Connector or Local Connector for High-density connections, SFP transceivers.<br>* SC: Subscriber Connector for Datacomm and Telecomm.<br>* ST: BFOC Straight Tip / Bayonet Fiber Optic Connector for Multimode - rarely Singlemode (APC not possible).<br>* VF-45: Snap connector for Datacom uses.<br>See the “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 11 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 -19.586 dBM. |
| Receive Power Alarm | Normal -1,<br>Not Supported - 2,<br>Low Warn - 3,<br>High Warn - 4,<br>Low Alarm - 6<br>High Alarm - 7 | Alarm status for receive power on local fiber. |
| Rx Power Intrusion Threshold (uW) | 0-10 | 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. |
| Temperature (˚C) | (measured temp.) | Temperature of fiber transceiver in tenths of degrees C (Celsius). The sample screen above shows 40.1˚C. |
| Temperature (˚F) | (measured temp.) | Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). The sample screen above shows 104.2 ˚F. |

| | | |
|---|---|---|
| Temperature Alarm | Normal -1,<br>Not Supported - 2,<br>Low Warn - 3,<br>High Warn - 4,<br>Low Alarm - 6<br>High Alarm - 7 | Alarm status for temperature of fiber transceiver.<br>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 14768 uA (microamps). |
| Transmit Bias Alarm | Normal -1,<br>Not Supported - 2,<br>Low Warn - 3,<br>High Warn - 4,<br>Low Alarm - 6<br>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.<br>The sample screen above shows 240 uW (microwatts). |
| Transmit Power (dBM) | (measured power) | Transmit power on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength.<br>The sample screen above shows -6.126 dBM. |
| Transmit Power Alarm | Normal -1,<br>Not Supported - 2,<br>Low Warn - 3,<br>High Warn - 4,<br>Low Alarm - 6<br>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)<br>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<br>meters. The sample screen above shows N/A, indicating the media is not applicable. |

### DMI Messages

**Message**: The DMI feature is not supported on current port.

Meaning: C4110 port 2 DMI is not shown if there is no SFP in port 1. Without an SFP in port 1, the port 2 DMI will display "The DMI feature is not supported on the current port.”. When an SFP is inserted into port 1, port 2 DMI data displays as expected.

Recovery: Insert an SFP in Port 1 and click the Refresh button.

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

Meaning: The setting for Rx Power Intrusion Threshold (µW) was exceeded. This is a configured 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.

Recovery: Check for an intrusion or change the Rx Power Intrusion Threshold setting to a differrent value. Click the Save button and click the Refresh button.

**Message**: Invalid input found!

Meaning: You entered a parameter value outside of the valid range.

Recovery: Enter a valid parameter and continue operation.

**Message**: No changes to be saved

Meaning: You clicked the Save button without changing any parameter values.

Recovery: Enter a valid parameter, click Save, and continue operation.

For More Information on topics such as Fiber Optics Power Measurements, Fiber and Cable Loss, OTDRs, Bandwidth, Reflectance/Optical Return Loss, and Fiber Optic Cleaning Procedures see The Fiber Optic Association - Tech Topic in the FOA Guide to Optics and Premises Cabling on the FOA website at http://www.thefoa.org/tech/FAQS/FAQ-TEST.HTM#bw

# 4: Operation

## General

This section describes the non-configuration operations that can be performed for the x4110.

## Backup and Restore Operations (Provisioning)

Using the Web interface you can back up and restore the configuration information for the IONMM and any or all of the x4110s in the ION system. See the IONMM User Guide manual for more information.

## Displaying Information

There are several CLI commands that allow you to display (show) information about the x4110 configuration. For a complete description of these and other CLI commands see the x4110 CLI Reference manual.

## Reset to Factory Defaults

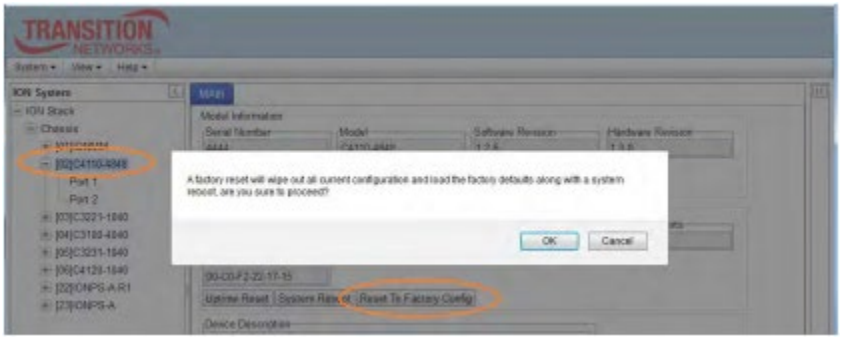
If need be, you can reset all configurations in the IONMM back to their original factory defaults. This operation can be accomplished via the Web GUI as described below.

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

**Resetting Defaults – Web Method**

**Caution**: This operation deletes all configuration information that was saved in the x4110, including the IP address you assigned to the x4110.

1. Access the x4110 via the Web interface.
2. Select the MAIN tab.
3. Locate the System Configuration section.




4. Click the Reset to Factory Config button. The message "*A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*" displays.
5. Click Cancel if you are sure you want to proceed with the Reboot. Click OK only if you wish to reboot.
   All configuration parameters will be reset to their factory values. For a list of all factory defaults, see "Appendix B: Factory Defaults").
   **Note**: Your Web session will be discontinued.
6. Set the IP configuration (see "Doing the Initial System Setup").

## File Status after Reset to Factory Defaults

The table below shows the status of x4110 files after a system re-boot.

**Table 6: File Status after a Reset to Factory Defaults**

| File Type | Filename | File Description | Stored Directory | Status after Restore to Factory Default |
|---|---|---|---|---|
| Provisioning backup files | e.g., '1-1-IONMM.config' | These files are only used by provisioning Restore | /tftpboot | Lost |
| Net-SNMP configuration file | snmpd.conf | This file is a configuration file for Net-SNMP | /agent3/conf/snmp | Restored to factory configuration |
| HTTPS configuration file | lighttpd-ssl.conf | This file is a configuration file for HTTPS | /agent3/conf/lighttpd | Restored to factory configuration |
| HTTPS certification file | server.pem | HTTPS certificate | /agent3/conf/lighttpd | Restored to factory configuration |
| SSH host key | dropbear_rsa_host_key dropbear_dss_host_key | SSH host key files | /agent3/conf/lighttpd | Restored to factory configuration |
| SSH user key file | authorized_keys | Currently we have one 'root' user; this file is the user key file for 'root' | /root/.ssh | Restored to factory configuration (lost) |
| Syslog file | sys.log | The syslog file for IONMM | /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) |

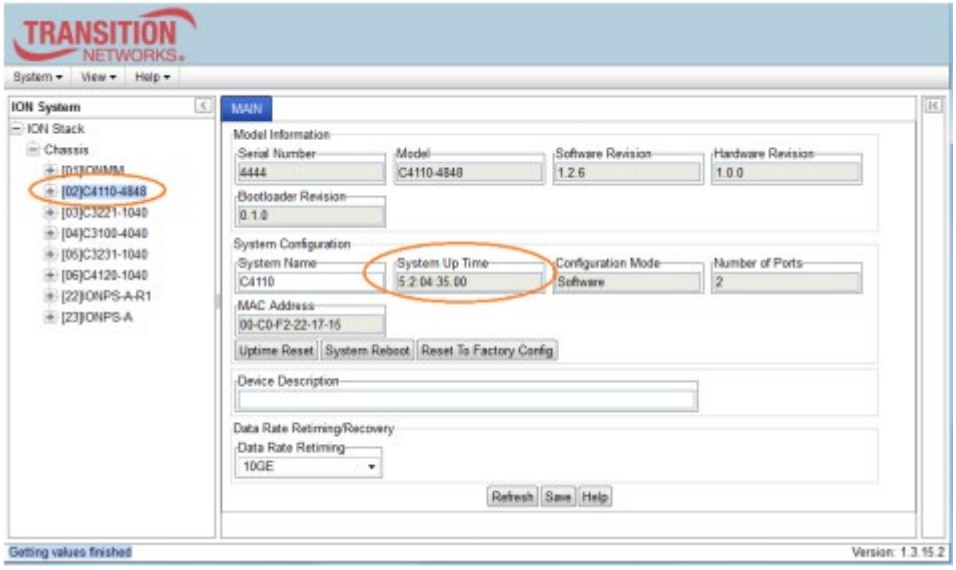
## Resetting Uptime

The x4110 system uptime field displays the amount of time that the x4110 has been in operation. The System Up Time is displayed in the format days:hours:minutes:seconds.milliseconds. For example, a System Up Time field display of 9:8:15:18.26 indicates the ION system has been running for 9 days, 8 hours, 15 minutes, 18 seconds, and 26 milliseconds.

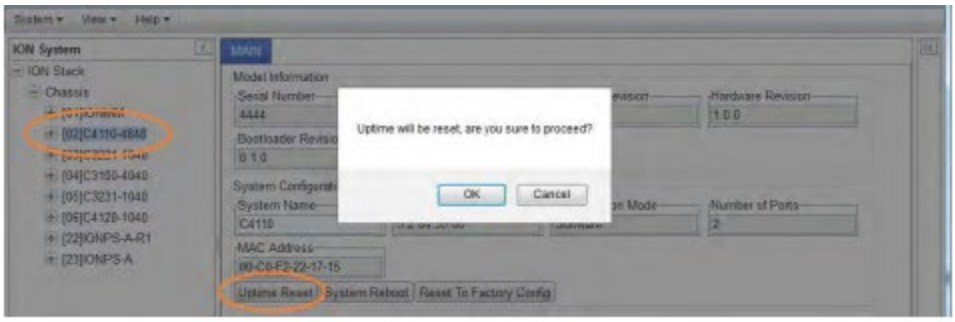
The ION System Up Time counter can be reset via the Web GUI as described below.

**Reset System Uptime – Web Method**

1. Access the x4110 via the Web interface.
2. At the MAIN tab, locate the System Configuration section.




3. If desired, observe and record the System Up Time field count. 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 device has been running for 9 days, 8 hours, 15 minutes, 18 seconds, and 26 milliseconds.
4. Click the Uptime Reset button to reset the counter to zero.




5. At the "*Uptime will be reset, are you sure to proceed*" message, click OK to reset the system up time.
6. The message "Setting values succeeded" displays at the bottom left of the screen when the up time reset is done.
7. Click the Refresh button at the bottom of the screen. The System Up Time field resets to zero, and immediately begins to increment.

## 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 11 in this section for file content and location after a System Reboot.

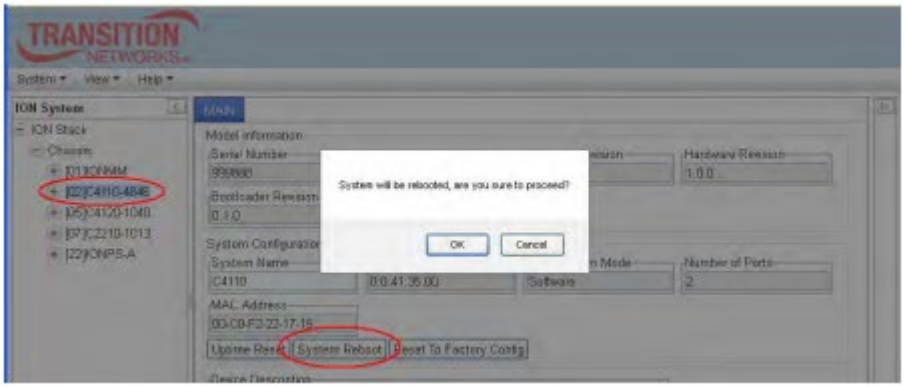
**Warning**: Doing a system reboot, restart, upgrade, or a reset to factory settings will cause all configuration backup files, HTTPS certification file, SSH key file, and Syslog file to be deleted.

**Rebooting – Web Method**

**Caution**: Doing a system reboot will cause all configuration backup files, HTTPS certification file, SSH key 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 x4110 via the Web interface.
2. Select the device's MAIN tab.
3. Locate the System Configuration section.




4. Click the System Reboot button. The confirmation message "System will be rebooted, are you sure to proceed?" displays.
5. At the confirmation window, click the OK button to start the reboot, or click Cancel to quit the reboot. The x4110 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 7: 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 |
| Net-SNMP configuration file | snmpd.conf | This file is a configuration file for Net-SNMP | /agent3/conf/snmp | No |
| HTTPS configuration file | lighttpd-ssl.conf | This file is a configuration file for HTTPS | /agent3/conf/lighttpd | No |
| HTTPS certification file | server.pem | HTTPS certificate | /agent3/conf/lighttpd | No |
| SSH host key | dropbear_rsa_host_key dropbear_dss_host_key | SSH host key files | /agent3/conf/lighttpd | No |
| SSH user key file | authorized_keys | Currently we have one 'root' user; this file is the user key file for 'root' | /root/.ssh | No |
| Syslog file | sys.log | The syslog file for IONMM | /tftpboot | No |
| MIB configuration files | e.g., 'agent3.conf' 'ifMib.conf' | The MIB configuration files for SNMP setting | /agent3/conf | No |

## Upgrade the IONMM and/or x4110 Firmware

Occasionally changes must be made to the firmware version that is currently stored in IONMM or x4110 memory. This could occur because of features, fixes or enhancements being added.

**Note**: Lantronix recommends that before completing any steps on an install that you verify that the IONMM has the latest firmware version installed and running. Keep your products up to date by downloading the latest firmware. You must log in or create an account to download firmware.

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 the IONMM User Guide for details.

# 5: 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 and x4110 and 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 x4110 (SICs, or slide-in-cards)
- IONMM (ION Management Module)
- 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 – RADIUS or TFTP, etc.)

When troubleshooting an ION system / network problem on site:

1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the 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 x4110s are seated properly, view the CLI show command output, verify IP addresses and Gateway IP address, check Windows Event Viewer, ping the interface, run the various tests if functional, etc.).
6. Write down your initial 2-3 guesses as to the cause of the problem.
7. Verify that the Lantronix product supports the function you are attempting to perform. Your particular product or firmware version may not support all the features documented for this module. For the latest feature information and caveats, see the release notes for your particular device/system and firmware release.
8. Use the Web interface or command line interface (CLI) to obtain all possible operating status information (log files, test results, show command outputs, counters, etc.)
9. Use the ION system manual procedure to retry the failed function or operation.

10. For the failed function or operation, verify that you entered valid parameters using the cursor over-help (COH) and/or the ION system manual.
11. Based on the symptoms recorded, work back through each step in the process or operation to recall a point at which the problem occurred, and examine for a possible failure point and fix for each.
12. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
13. Isolate on 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 102 before calling Tech Support.

## Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED Fault and Activity Displays (page 36)
- Problem Conditions (page 37)
- CLI Messages (page 38)
- Web Interface Messages (page 43)
- Windows Event Viewer Messages (page 53)
- Config Error Log (config.err) File (page 54)
- Webpage Messages (page 58)
- Third Party Troubleshooting Messages (page 61)

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:

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

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

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

**L/A SFP+ LED off (not lit):**

1. Check the data cables for obvious problems, incorrect type, incorrect wiring, etc.
2. See if the administrator has manually disabled the console device (PC) via the Web interface.
3. Check if other network devices are working properly.
4. Remove the suspect card from the chassis and re-insert it.
5. Check Auto-Negotiation setting.
6. See if the port transmission mode / speed (full or half-duplex, etc.) match those of the attached device.
7. Verify that the ION system devices have the latest firmware versions (see “Upgrade the Firmware” in the IONMM User Guide).
8. Download the latest firmware version and upgrade as necessary.

**Problem Conditions**

Cannot access the IONMM via Telnet
Cannot access the IONMM via the Web
Cannot access the IONMM via USB port
Management Module does not power on
Telnet connection is lost after a CLI command is executed
Upgrade fails
Upload fails
USB connection resets after a CLI command is executed

1. Verify that the default password has not been changed.
2. Check with your IT department that the network is up and running.
3. Refer to the IONMM User Guide for details.

**Cannot access the x4110 via the Web Interface**

1. Can you access the IONMM?
Yes : Continue with Step 2.
No : See “Cannot access the IONMM via the Web”.
2. Power cycle the x4110.
3. If the problem persists, contact Technical Support. See “Contact Us”.

**Configuration Mode Mismatch**

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

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

1. Refer to the “Jumper Settings” section of the Install Guide manual for details on hardware mode configuration.
2. Contact Lantronix for more information. See “Contact Us”

***loading, please wait* ... Displays continuously**

1. Wait for one or more minutes for the operation 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. See “Contact Us”.

**Parameter Boxes Outlined in Red / Cannot Enter Parameters**

1. Check if the device is physically connected and powered on.
2. Verify the x4110 DIP swtch settings and HW/SW Jumper setting.
3. Refresh the IONMM or x4110 by clicking the Refresh button.
4. 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.
5. Cycle power for the module in question.
6. Upgrade the devices to the latest software version.
7. Reboot the device by clicking the Reboot key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
8. If the problem persists, contact Technical Support. See “Contact Us”.

**Red box Condition after Reboot**

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. 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 C4110 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 x4110 is at an older version and shows the newer functions as ‘red boxed’. Since the older version of x4110 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as ‘red boxed’. Upgrade the devices to the latest software version.

3. Reboot the system. See the “Reboot” section for more information.

4. Contact Tech Support for more information. See “Contact Us”.

**Windows XP Cannot Find Drivers For My Device**

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

1. Contact Lantronix for more information.

**Windows XP Forces a Reboot after Installing a Device**

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

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

**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 Tech Support for more information. See “Contact Us”.

**Windows XP Displays an Error and then Terminates Installation**

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

To successfully install the device, you must change the driver signing options to either warn or ignore in order 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.

**Little indication of an IONPS-D Power Supply failure in Web interface**

Meaning: If a power supply is powered down or loses input power, the only indication on the web interface is a Power reading of 0.0. The "Power Status OK" means that the Power Sensor is operating normally, not that the input power is OK.

Recovery: To check the loss of power, check at IONPS-A > MAIN tab > Sensor and Fan(s) section > Power value field.

**User Public-Key Missing after Upgrade from v1.0.3 to v0.5.12**

Meaning: In ION v1.0.3, the user-public key is binding with the Linux root user and is stored in the root file system (/root/.ssh/). This file system will be replaced after this version upgrade, so this key will be lost.

Recovery: This missing key problem will occur only if you upgrade from 0.5.14 to a later release. In ION versions after 0.5.14, the user-public key is saved after an upgrade. You can still log in through SSH, but you must upload the public key again in order to use it. In v 0.5.14, the stored key was moved from the root file system to the application flash area (/agent3/conf).

**Problem**: "Unknown command." message displays when entering system name/contact/location.
Problem: The System Name cannot be restored when the system name contains special character "space" in the middle.

Meaning: The "Unknown command." message displays when the system name/contact/location contains a "space" character within the text using the CLI command "set system name" or "set system contact" or "set system location" is entered. The entry for the system contact, system location, and system name must be a text string with no spaces between characters. Note that numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed.

Recovery: From the Web interface, at the device's MAIN tab in the System Configuration section, reenter the "System Name" or "System Contact" or "System Location", making sure there are no spaces between the text characters. From the CLI, re-enter the "set system name" or "set system contact" or "set system location" CLI command, making sure there are no spaces between the text characters.

**Problem**: Bandwidth Ingress fault

Meaning: With rate set at 100Mbps with Full Duplex and Frame Size = 9216 a bandwidth Ingress fault occurs. When Ingress rate limiting is set at or below 512Kbps, the S322x will pass approximately 1 Mbps of traffic. At 768kbps and above rate limiting is working. This problem only happens on Ingress (not Egress) and only happens when connected at 100Mbps Full Duplex. Packets of 1518k or less work fine. This is a known hardware component limitation that only occurs when using very large Jumbo Frame (>5k) and very low bandwidth (≤512k).

Recovery: Change the rate, duplex mode, frame size, packet size, or Ingress Rate Limit. See the related section of this manual for details.

## 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. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails. The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for
1. user management traffic. The PC can then ping to the S2220-1013 again, and the WEB UI can be
2. managed again.
3. If the problem persists, contact Technical Support.

**Cannot Ping IONMM Device**

1. With the "Management VLAN" state set to "enabled", the PC cannot ping the IONMM device.
1. The reason is enabling the Management VLAN function gives management control to the
2. Management VLAN that you enabled.
3. Enter the CLI command `set mgmt vlan state disable` and press Enter. The PC can ping to S2220-1013 success again, and the Web interface can be managed again.
4. If the problem persists, contact Technical Support.

**Getting values failed (snmp operation timeout)**

This message indicates that you entered an invalid parameter value.

1. Click the Refresh button to clear the message.
2. Verify the recent parameter entries. Refer to the related CoH (cursor-over-help) and revise parameter entries as needed.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

**Failed to start Virtual Cable Test.**

This message indicates that the VCT test could not be started.

1. Check the following:
    - Module has power.
    - Cable is properly connected to the port.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

**Firmware DB operation failed, unzip failed.**

This message indicates that the upload of the upgrade file failed.

1. Check that the db.zip file (Windows XP) or db file (Windows 7) file was specified in the Database File Name field.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

**invalid input file**

This message displays in the "Upload Result Reason" field at IONMM > Upgrade tab> Firmware database sub-tab if the "Firmware File Name" entered had an incorrect filename format.

1. Verify the parameter value entered; see "Upgrading IONMM Firmware – Web Method" for valid
2. input information.
3. Retry the operation with a valid firmware file name (e.g., IONMM.bin.0.5.4, or x222x / x32xx.bin.0.5.4).
4. If the problem persists, contact Technical Support.

**Invalid input found!**
This message indicates that you entered a parameter outside the valid range (e.g., VLAN ID = 0).
1. Verify the parameter value to be entered; check the online Help for valid input information.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

**Invalid password!**
This message indicates that the password entered during sign on is not valid.
1. Sign in using the correct password. The default password is private.
1. Note: the password is case sensitive.
2. If the problem persists, contact Technical Support.

**Failed to retrieve DMI info on current port.**
You clicked the Device port's DMI tab, but the device does not support DMI. Not all NID models support DMI. The NIDs that support DMI have a "D" at the end of the model number.
1. Verify that the x4110 supports DMI.
2. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

**Admin Status: Down (or Testing)**
In the device's port, at the MAIN tab in the Port Configuration section, the Admin Status field displays "Down". Typically, if 'Admin Status' is Down, then 'Link Status' is also Down.
The status here is the desired state of the interface. The "Testing" status indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with 'Admin Status' in the Down state. As a result of either explicit management action or per configuration information retained by the managed system, 'Admin Status' is then changed to either the Up or Testing states, or remains in the Down state.
1. Verify the initialization process; see "Section 2: Installation and System Setup".
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization to take place.
4. If the problem persists, contact Technical Support.

**Link Status: Down (or Testing or Dormant, or NotPresent)**
This is the current operational state of the interface.
The 'Link Status' Testing state indicates that no operational packets can be passed.
If 'Admin Status' is Down then 'Link Status' likely will be Down.
If 'Admin Status' is changed to Up, then 'Link Status' should change to Up if the interface is ready to transmit and receive network traffic.
'Link Status' should change to Dormant if the interface is waiting for external actions (such as a serial line waiting for an incoming connection);
'Link Status' should remain in the Down state if and only if there is a fault that prevents it from going to the Up state;
'Link Status' should remain in the NotPresent state if the interface has missing (typically, hardware) components.

**Link Status: Down**: The ION system interface is not ready to transmit and receive network traffic due a fault.
1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see "Section 2: Installation and System Setup".
3. Verify the attempted operation procedure in the related section of this manual.

4. Retry the operation. Wait several minutes for initialization to take place.
5. If the problem persists, contact Technical Support.

**Link Status: Dormant: The ION system interface is waiting for external actions (such as a serial line** waiting for an incoming connection).

1. Wait several minutes for initialization to take place, and then retry the operation.
2. If the problem persists, contact Technical Support.

**Link Status: NotPresent: the interface has missing components (typically hardware).**

1. Verify the ION system installation; see “Section 2: Installation and System Setup“.
2. Wait several minutes for initialization to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

**Link Status: Testing: The ION system interface can not pass operational packets.**

1. Verify that diagnostic tests were run properly and completed successfully.
2. Wait several minutes for initialization to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

**Message**: Setting values failed (snmp operation error)
This message indicates that the SNMP Configuration entered had an invalid SNMP entry (e.g., an unrecognized Trap Manager address entry).

1. Enter a valid value. Refer to the Help screen for more information.
2. Try another operation.
3. If the problem persists, contact Technical Support.

**Message**: Web UI Management connection Lost

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails.
1. The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
2. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic.
3. The PC can ping to S2220-1013 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support.

**Message**: “Setting values in progress ...” displays continuously
The message “Setting values in progress ...” displays for over 10 minutes after you set up a VLAN 100, then set Management VLAN to Enabled and clicked Save.

Getting values failed (http server error) then displays.
Loading Template agent_main_view.htm failed displays:
MAIN tab displayed is blank after you close the Loading ... dialog box.
Meaning: These messages display after you turn on the Management VLAN function either via the ION Web interface or the CLI. (The CLI command is set mgmt vlan state=enable, and the Web interface is from the IONMM MAIN screen in the Management VLAN Configuration section, where the Status field is set to Enabled. In both cases, management control is given to the Management VLAN that you enabled.
The recovery (re-gaining control from the CLI or Web interface) is to turn off Management VLAN via the CLI (set mgmt vlan state=enable) or via the Web interface (IONMM MAIN > Management VLAN Configuration > Status > Enabled).

**Message**: Loading Template agent_main_view.htm failed
Loading htm files failed
Loading htm file succeeded
Loading JavaScript file failed
Loading Template Config file failed
Meaning: The status displays at the lower left corner during Port 1 page loading.
Recovery: 1.Wait for the Loading, please wait... message to clear. This may take 1 minute or more. 2. See the Loading, please wait... message for details. 2. If the problem persists, contact Technical Support.

**Message**: The DMI feature is not supported on current port
Meaning: Not all x4110 models support DMI. Lantronix x4110s that support DMI have a “D” at the end of the model number. If you click the DMI tab on a x4110 model that does not support DMI, the message “The DMI feature is not supported on current port.”
The DMI (Diagnostic Maintenance Interface) function displays x4110 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.
Recovery: 1. Verify that the device and port support DMI. See “DMI (Diagnostic Maintenance Interface) Parameters” for more information.

**Message**: Loading Template agent_main_view.htm failed
**Message**: Loading htm files failed
Meaning: The status displays at the lower left corner during Port 1 page loading.
Recovery: 1.Wait for the Loading, please wait... message to clear. This may take 1 minute or more.
2. See the Loading, please wait... message for details. 3. If the problem persists, contact Technical Support.

**Message**: Online Help is not available until a specific configuration is entered.
Meaning: You clicked on Online Help from the Help dropdown without first selecting a device.
Recovery:
1. Click the OK button to close the webpage message.
2. Select an ION device.
3. Click on Help > Online Help again.

**Message**: Trap manager settings changed and a system reboot is required for the changes to take effect. – Do you want to reboot the system right now?
Meaning: Information only. At IONMM > MAIN > SNMP Configuration > Trap Manager x you entered an IP address for a trap server.
Recovery:
1. Click the OK button to clear the webpage message.
2. Verify the Trap Manager setting and continue operation.
3. If a problem persists, contact Technical Support.

**Message**: File has been successfully transferred via TFTP.” but the Prov. status column displays failure [...].
Meaning: At IONMM > BACKUP-RESTORE > Backup you selected a module to back up, the “successful transfer” message displays, but the Prov. Status column displays failure [...].
Recovery:
1. Click the OK button to clear the webpage message.
2. Click the [...] box after the word “failure” in the Prov Status column.
3. Open the config.ERR file at C:\TFTP-Root.
4. Fix any config commands and then retry the operation.
5. Verify the Backup and continue operation.

6. If a problem persists, contact Technical Support.

**Problem**: In IE8 or IE9, at C3220 > FDB, the 'Refresh', 'Add', 'Edit', 'Delete', 'Help' buttons of FDB do not display.

1. Select IE8 Tools > Compatibility Mode to use the IE8 'Compatibility View'. The message "Compatibility View - 192.168.1.10 is now running in Compatibility View.' displays.
2. Log in to the ION system again.
3. Select the FDB tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
5. 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.
5. Check the Microsoft Support Online website http://support.microsoft.com/ph/807/en-us/#tab0 for more
1. information.
6. See also: http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx
2. http://support.microsoft.com/kb/960321
3. 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
4. http://support.microsoft.com/kb/956197.

**Script error message received.** Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No

Error: Object doesn't support this property or method.

A Runtime Error has occurred. Do you wish to Debug?

Done, but with errors on page.

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
5. http://support.microsoft.com/kb/308260.

**Message**: Getting card hardware mode failed
Meaning: The x4110 is in Hardware mode and you tried to perform a Software operation.
Recovery:
1. Change the mode to Software mode.
2. See the “Field-configurable DIP Switch (SW1) and Jumper (J9)” section of the C4110 Install Guide manual.
3. Contact LantronixTechnical Support. See “Contact Us”.

**Windows Event Viewer Messages**
Windows Event Viewer - Event Log 1:

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.

**The Config Error Log (config.err) File**
The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as 1-11-C2210-1013.config. You can open the file in WordPad or a text editor.
These messages show a translation of failed web interface functions that were attempted, translated into CLI commands.
The config.err files are saved in the TFTP server location specified (typically C:\TFTP-Root) with a file name something like: 1-2-2-C3220-1040_20100608.config.err.
The first word in the message (e.g., add, set, remove) shows the type of action attempted.
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.
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
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**: remove vlan all failed
Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the x4110 CLI Reference Manual, 33497. 4. If the problem persists, contact Technical Support.

**Message**: remove fwddb all failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set ip-mgmt state=enable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set dhcp state=disable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed
Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in the x4110 CLI Reference Manual, 33497. 4. If the problem persists, contact Technical Support.

**Message**: set gateway type=ipv4 addr=192.168.0.1 failed
Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in the x4110 CLI Reference Manual, 33497. 4. If the problem persists, contact Technical Support.

**Message**: set dns-svr svr=1 type=dns addr=0.0.0.0 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set snmp traphost svr=1 type=dns addr=0.0.0.0 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set sntp state=disable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set sntp dst-state=disable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set sntp timezone=8 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set sntp dst-end="1969 1231 18:00:00" failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set sntp dst-offset=0 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set sntp-svr svr=1 type=dns addr=0.0.0.0 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set radius client state=disable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set radius svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: add vlan-db vid=100 priority=0 pri-override=disable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: add vlan-db vid=200 priority=0 pri-override=disable failed

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.
**Message**: set acl state=disable failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set acl table=filter chain=input policy=accept failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: set dot1dbridge ip-priority-index=0 remap-priority=0 failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

**Message**: AGENT PM ERROR: CLI command show dot1dbridge ip-tc priority remapping failed
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

### Webpage Messages

Certain menu operations will display a webpage verification message to verify that you want to proceed. These messages also provide information on the effect that the operation will have if you continue. These messages display for operations such as Reset to Factory Config, Reboot the System, or other operational confirmation messages. See “Menu System Descriptions”.

**Message**: System will be rebooted, are you sure to proceed?
Response: Click OK only if you wish to reboot. Otherwise click Cancel.

**Message**: A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?
Response: Click OK only if you wish to reboot. Otherwise click Cancel.

**Message**: Are you sure to power reset this slot? (After power reset, it will take a while to see card change in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page.)
Meaning: A caution message generated at the Chassis > MAIN tab. You clicked the Reset button for a particular slot.

Recovery:
1. If you are not sure that you want to reset this slot, click the Cancel button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to reset this chassis, click the OK button to clear the message and reset power to the slot.
3. At the Chassis > MAIN tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the Refresh button on this page.
5. See “Menu System Descriptions”.
6. If the problem persists, contact Technical Support.

**Message**: Are you sure you want to power off this slot? (After power off, it will take a while to see Card Disappear in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page.)
Meaning: A caution message generated at the Chassis > MAIN tab. You clicked the Off button for a particular slot.
Recovery:
1. If you are not sure that you want to power off this slot, click the Cancel button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to power off this slot, click the OK button to clear the message and remove power to the slot.
3. At the Chassis > MAIN tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the Refresh button on this page.
5. See “Menu System Descriptions”.
6. If the problem persists, contact Technical Support.

**Message**: The Connection was Reset
Meaning: The FireFox web browser connection failed to load the page.
Recovery:
1. Verify the URL (e.g., http:// versus https://).
2. Check if the applicable server is running in the expected location.
3. Click the Try again button to retry the operation.

**Message**: This Connection is Untrusted
Meaning: You tried to connect via Firefox to a URL, but the Firefox web browser did not find a trusted certificate for that site.
Recovery: Click Technical Details for details, or click I Understand the Risks to continue operation.

**Message**: Local Area Connection x – A network cable is unplugged
Meaning: You unplugged the USB cable at the x4110 or IONMM, or the x4110 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 x4110’s USB connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support.

**Message**: Problem loading page – Mozilla Firefox
Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.
Recovery:
1. Make sure the web browser you are using is supported. See “Web Browsers Supported”.

2. Verify the URL entered. See “Initial Setup with a Static IP Address via the CLI”.
3. Verify x4110 access. See “Accessing the x4110”.
4. Verify the IP address setting. See “Setting the IP Addressing”.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

**Message**: Internet Explorer cannot display webpage
Meaning: You tried to log in to the ION system from IE, but the login failed.
Recovery:
1. Make sure the web browser you are using is supported. See “Web Browsers Supported”.
2. Verify the URL entered. See “Initial Setup with a Static IP Address via the CLI”.
3. Verify NID access. See “Accessing the x4110”.
4. Verify the IP address setting. See “Setting the IP Addressing”.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

## Third Party Troubleshooting Tools

This section provides information on third party troubleshooting tools for Windows, Linux, etc. Note that this section may provide links to third party web sites. Lantronix is not responsible for any third party web site content or application. The web site information was accurate at the time of publication, but may have changed in the interim.

- Ipconfig and ifconfig
- Windows Network Connections
- Ping
- Telnet
- PuTTY
- Tracert (Traceroute)
- Netstat
- Winipcfg
- Nslookup
- Dr. Watson

**Note**: IETF RFC 2151 is a good source for information on Internet and TCP/IP tools at ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt.

**Ipconfig** (Windows Vista): Use the procedure below to find your IP address, MAC (hardware) address, DHCP server, DNS server and other useful information under Windows Vista.
1. Go to the start menu and type command in the box.
2. Right-click on Command Prompt and click Run as administrator. If a User Account Control window pops up, click Continue.
3. At the C:\> prompt type ipconfig and press Enter. Your IP address, subnet mask and default gateway display. If your IP address is 192.168.x.x, 10.x.x.x, or 172.16.x.x, then you are receiving an internal IP address from a router or other device.
4. For more detailed information, type ipconfig /all at the prompt. Here you can get the same information as ipconfig plus your MAC (hardware) address, DNS and DHCP server addresses, IP lease information, etc.

**Note**: If you are receiving a 169.254.x.x address, this is a Windows address that generally means your network connection is not working properly.

**ipconfig** (Windows XP): ipconfig (Internet Protocol Configuration) in Windows is a console application that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.
Use the ipconfig command to quickly obtain the TCP/IP configuration of a computer.

1. Open a Command Prompt. Click Start, point to Programs, point to Accessories, and then click Command Prompt.
2. Type ipconfig and press Enter. The Windows IP Configuration displays:
3. Make sure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
4. For more information, use the /all parameter (type ipconfig /all and press Enter).

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

**ifconfig**

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

```
[root@sleipnir root]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:6E:0A:3D:26
        inet addr:192.168.168.11 Bcast:192.168.168.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:13647 errors:0 dropped:0 overruns:0 frame:0
        TX packets:12020 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:7513605 (7.1 Mb) TX bytes:1535512 (1.4 Mb)
        Interrupt:10
lo Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:892258 (871.3 Kb) TX bytes:892258 (871.3 Kb)
```

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

**Windows Network Connections**

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

1. Open Network Connections from Start → Settings → Network Connections.
2. Right-click a network connection.
3. Click Status.
4. Click the Support tab. Your connection status information displays.
5. Click the Details button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

**Ping**

Use the ping command to test a TCP/IP configuration by using the ping command (in Windows XP Professional in this example). Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

1. Open a Command Prompt. To open a command prompt, click Start, point to Programs, point to Accessories, and then click Command Prompt.
2. At the command prompt, ping the loopback address by typing ping 127.0.0.1.
3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host on a different subnet). If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server. If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

   If the ping command is not found or the command fails, you can use Event Viewer to check the System Log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.

The ping command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

**Telnet**

Telnet is a simple, text-based program that lets you connect to another computer via the Internet. If you've been granted the right to connect to that computer by that computer's owner or administrator, Telnet will let you enter commands used to access programs and services that are on the remote computer, as if you were sitting right in front of it.

The Telnet command prompt tool is included with the Windows Server 2003 and Windows XP operating systems. See the related OS documentation and helps for more information. Note that if you are only using computers running Windows, it may be easier to use the Windows Remote Desktop feature. For more information about Remote Desktop, see the related OS documentation and helps.

**Telnet Client**

By default, Telnet is not installed with Windows Vista or Windows 7, but you can install it by following the steps below.

To install Telnet Client:

1. Click the Start button, click Control Panel, click Programs, and then select Turn Windows
1. features on or off. If prompted for an administrator password or confirmation, type the password or
2. provide confirmation.
3. In the Windows Features dialog box, check the Telnet Client checkbox.
4. Click OK. The installation might take several minutes.

After Telnet Client is installed, open it by following the steps below.
To open the Telnet Client:
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/enus/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.

**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 allows you to help 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 practically all Unix-like operating systems. Variants with similar functionality are also available, such as tracepath on modern Linux installations and tracert on Microsoft Windows operating systems. Windows NT-based operating systems also provide pathping, which provides similar functionality.

The tracert TCP/IP utility allows you to determine the route packets take through a network to reach a particular host that you specify. Tracert works by increasing the "time to live" (TTL) value of each successive packet sent. When a packet passes through a host, the host decrements the TTL value by one and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded. Tracert, if used properly, can help you find points in your network that are either routed incorrectly or are not existent at all.

The Tracert Windows based command-line tool lets you trace the path that an IP packet takes to its destination from a source. Tracert determines the path taken to a destination by sending ICMP (Internet Control Message Protocol) Echo Request messages to the destination. When sending traffic to the destination, it incrementally increases the TTL (Time to Live) field values to help find the path taken to that destination address.

Tracert options include:
-? which displays help at the command prompt.
-d which prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names (this speeds up the display of tracert results). Using the –d option helps when you want to remove DNS resolution. Name servers are helpful, but if not available, incorrectly set, or if you just want the IP address of the host, use the –d option.

**Netstat**

Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on UNIX, Unix-like, and Windows NT-based operating systems.

The netstat tool is used for finding network problems and determining the amount of traffic on the network as a performance measurement. It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protcols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, netstat displays active TCP connections.

Note: parameters used with this command must be prefixed with a hyphen (-) and NOT a slash (/):
-a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-b Displays the binary (executable) program's name involved in creating each connection or listening port. (Windows XP, 2003 Server only - not Microsoft Windows 2000 or other non-Windows operating systems).
-e Displays Ethernet statistics, such as the number of bytes and packets sent and received.
-f Displays fully qualified domain names (FQDN) for foreign addresses.(not available under Windows)
-i Displays network interfaces and their statistics (not available under Windows).
-o Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).
-p (Windows): Protocol : Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
-p (Linux) Process : Show which processes are using which sockets (you must be root to do this).

**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.

**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.

## Third Party Tool Messages

This section discusses messages generated by HyperTerminal, Ping, and Telnet during ION system

**installation, operation and configuration.**

**HyperTerminal Messages**

**Message**: Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal.
Response:
1. Verify your computer's Ports (COM) setting. See "Configuring HyperTerminal".
2. Use the Computer Management > Device Manager > Troubleshooter button located on the General tab in Properties.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support.

**Message**: Unable to open COM x. Please check your port settings.
Response:
1. Verify your computer's Ports (COM) setting. See "Configuring HyperTerminal".
2. Use the Computer Management > Device Manager > Troubleshooter button located on the General tab in Properties.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support.

**Problem**: HT Overtyping Problem - You tried to edit a typo in a CLI command, the new data is stored, but the old data is appended to it.
Meaning: HyperTerminal (HT) is a terminal emulation program developed by Hillgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a text entry. Overtyping an entry should automatically replace the previous characters. This is a HyperTerminal problem that the ION CLI stack cannot resolve.
Response:
1. Upgrade to the latest version (a free download from www.hilgreave.com). The more current product seems to run more smoothly and has text editing features not found in earlier versions.
2. In HT, turn off local echo - refer to the HT helps and documentation for the command to use.
3. Make sure the keyboard Insert mode is turned off.
4. Download and use PuTTY or TeraTerm to use as a replacement for HT.

**Ping Command Messages**

**Message**: Request timed out.
Meaning: The Ping command failed.
Recovery:
1. Verify the connection, verify correct IP address entry, and retry the operation.
2. Verify if the default IP address has changed using the Ipconfig (or similar) command.

**Telnet Messages**
Message: Could not open connection to the host, on port 23: Connect failed.
Meaning: The attempted Telnet connection failed.
Recovery:
1. Verify the physical connection, verify correct IP address entry, and retry the operation.
2. Check if the default IP address has changed using the Ipconfig (or similar) command.

**Message**: Invalid location parameters, cannot find the physical entity!
Meaning: The go command you entered includes a location that does not exist or that you entered incorrectly.
Recovery:
1. Run the stat command to verify your configuration.
2. Click the plus sign [+] next to ION Stack to unfold the "ION Stack" node in the left tree view to refresh device status.
3. Click the plus sign [+] next to Chassis to unfold the chassis devices.
4. Compare the stat command results to the Web interface tree view configuration information.
5. Re-run the stat command with the correct location parameters.
6. Ping the device in question.
7. Unplug and re-plug the USB connector on the IONMM card.
8. If the problem persists, contact Technical Support.

**Message**: Unknown command!
Meaning: The command you entered is not supported, or you entered the wrong command format / syntax.
Recovery:
1. Verify the CLI command syntax.
2. For a complete list of the available commands, see the x4110 CLI Reference Manual, 33497.

**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.

## 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 Technical Support Specialist.

1. Select the ION system 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 slot info, show system information, show ether config, show ip-mgmt config, or others as request by the Support Specialist.

2. Record the Model Information for your system.

Serial Number: _____ Model: _____

Software Revision: _____ Hardware Revision: _____

Bootloader Revision: _____

3. Record the System Configuration information for your system.

System Up Time: _____ Configuration Mode: _____

Number of Ports: _____ MAC Address: _____

Data Rate Retiming: _____

LED Status: _____

4. Provide additional Model and System information to your Technical Support Specialist. See “Basic ION System Troubleshooting”.

Your service contract number: _____

A description of the failure: _____

_____

_____

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

_____

_____

_____

The serial and revision numbers of all involved Lantronix products in the network:

_____

_____

A description of your network environment (layout, cable type, etc.): _____

_____

_____

Network load and frame size at the time of trouble (if known): _____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

_____

_____

Any previous Return Material Authorization (RMA) numbers: _____

# Appendix A: Warranty and Compliance Information

For Warranty, Returns, Electrical Safety Warnings, and Compliance Information see the related Install Guide manual.

# Appendix B: SNMP MIBs and Traps Support

See the IONMM SNMP User Guide for information on SNMP traps supported, supported MIBs, private MIB objects tree example, Downloading, Compiling and Integrating MIBs, Trap service and functions, the Trap Server Log, and an example of ION SNMP operation.

**For Additional SNMP MIB Trap Information**

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

The notification MIB is described in section 4.2 and section 7.2 of RFC 2573, available from the IETF web site at http://www.ietf.org/rfc/rfc2573.txt.

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

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

**Sales Offices**
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.