

ION System x4120 Series

10 Gbps Copper-to-Fiber Converter

Slide-in-Card and NID

User Guide

Part Number 33551

Revision D March 2024

Intellectual Property

© 2023-2024 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

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

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

Warranty

For details on the Lantronix warranty policy, 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 of Changes
A	06/13/13	Initial release for v 1.2.3.
B	6/6/18	Update for FW v 1.2.6 with support for management and FW upgrade of a C4120 when installed in an unmanaged ION chassis and contact info. Update for FW v 2.0.1 and Bootloader v 0.1.5 with Slot ID and TLPT fixes.
C	8/21/23	Initial Lantronix re-brand. Remove Glossary and Index.
D	3/29/24	Correct the Model # from x4120-1040 to x4120-1048.

Cautions and Warnings

Definitions

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

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

Cautions



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



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



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



Caution: **Do not** install the x4120 in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor x4120 performance.



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



Caution: Only trained and qualified personnel should install or perform maintenance on the ION219-A chassis. Failure to observe this caution could result in poor performance or damage to the equipment.



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



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

Warnings



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



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



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



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



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

See the Install Guide for Electrical Safety Warnings translated into multiple languages.

Table of Contents

1: Introduction	6
Document Overview	6
Related Manuals and Online Helps	8
2: Management Methods	9
3: Configuration	20
Device Description Configuration	23
Agent III C1 S17 L1D>set device description thenewone	23
Agent III C1 S17 L1D>show dev descr	23
Device description: thenewone	23
Agent III C1 S17 L1D>.....	23
Transparent Link Pass Through (TLPT) Configuration	27
Auto Negotiation – Web Method.....	33
Check Ethernet Port Config – Web Method	35
Loopback Management	36
4: Operation	38
Reboot	44
Rebooting – CLI Method	44
Transfer Files via Serial Protocol (X/Y/Zmodem) – CLI Method	48
5: Troubleshooting	50
General	50
Basic ION System Troubleshooting.....	50
Error Indications and Recovery Procedures.....	51
LED Fault and Activity Displays.....	52
The Config Error Log (config.err) File.....	96
Third Party Troubleshooting Tools.....	113
Recording Model Information and System Information	132
Appendix A: Warranty, Compliance and Electrical Safety	134
Appendix B: SNMP MIBs and Traps Support	135

List of Figures

Figure 1: CLI Location Hierarchy	10
Figure 2: Private MIB Objects	136
Figure 3: SNMP Message Sequence.....	138

List of Tables

Table 1: Documentation Conventions.....	7
Table 2: System-Level Menu Description	15
Table 3: Port-Level Menu Description.....	16
Table 4: File Status after a Reset to Factory Defaults	41
Table 5: File Content and Location after a System Reboot	46
Table 6: DMI Parameters	110
Table 7: Trap Server Log File Description	141

1: Introduction

Product Overview

The x4120-1048 is a 10 Gigabit Ethernet copper to fiber media converter. It offers conversion technology by providing one 10GBase-T RJ-45 port and one pluggable 10GBase-X fiber SFP+ port. The open SFP+ port supports a wide variety of Lantronix 10GE SFP+ fiber modules, as well as third party MSA compatible SFP+ modules.

The x4120 provides several 10G Ethernet enterprise and data center connectivity solutions. Since most 10G Ethernet switches support a combination of copper RJ-45 and open SFP+ ports, the x4120 allows users to convert either of these ports to the media type of their preference to match their network requirements, including direct attached copper SFP+ cables.

The C4120 slide-in-card is a managed device when installed in a managed ION Chassis. The stand-alone S4120 is an unmanaged device, until it is linked to C4120 installed in a managed ION chassis, and then remote in-band management of the S4120 is available.

These devices can be managed via Command Line Interface (CLI), Web interface, or Telnet. Access is through the IONMM (ION Management Module), also installed in the ION chassis. See the related *Installation Guide* on the web at <https://www.lantronix.com/products-class/chassis/>.

Document Overview

The purpose of this manual is to provide the user with an understanding of the Lantronix x4120 Ethernet media converter. This manual documents the following models:

- **C4120-1048** : 10GBase-T Copper to Fiber Media Converter
- **S4120-1048** : 10GBase-T Copper to Fiber Media Converter

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

Related Manuals and Online Helps

A printed Documentation Postcard is shipped with each x4120. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface. A substantial set of technical documents, white papers, case studies, etc. are available on the Lantronix web site at <https://www.lantronix.com/technical-support/>.

The ION system and related device manuals are listed below.

1. Product Documentation Postcard, 33504
2. C4120 Install Guide, 33549
3. S4120 Install Guide, 33550
4. x4120 User Guide, 33551 (this manual)
5. x4120 CLI Reference Manual, 33552
6. ION Management Module (IONMM) User Guide, 33457
7. SFP manuals (product specific)
8. Release Notes (software version specific)

This manual may provide links to third part web sites for which Lantronix is not responsible. Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version. While all screen examples may not display the latest version number, all of the descriptions and procedures reflect the latest software/firmware version, noted in the [Revision History](#) on page 2. Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

2: Management Methods

General

The x4120s are managed either directly or through the IONMM. Whether the x4120 is 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 x4120 can be remotely managed directly (i.e., not through IONMM). This enables administrators to monitor and configure remote stand-alone x4120s 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 (x4120) 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 Using CLI Commands

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

For example:

```
AgentIII C1|S7|L1D>
```

or just:

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

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

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

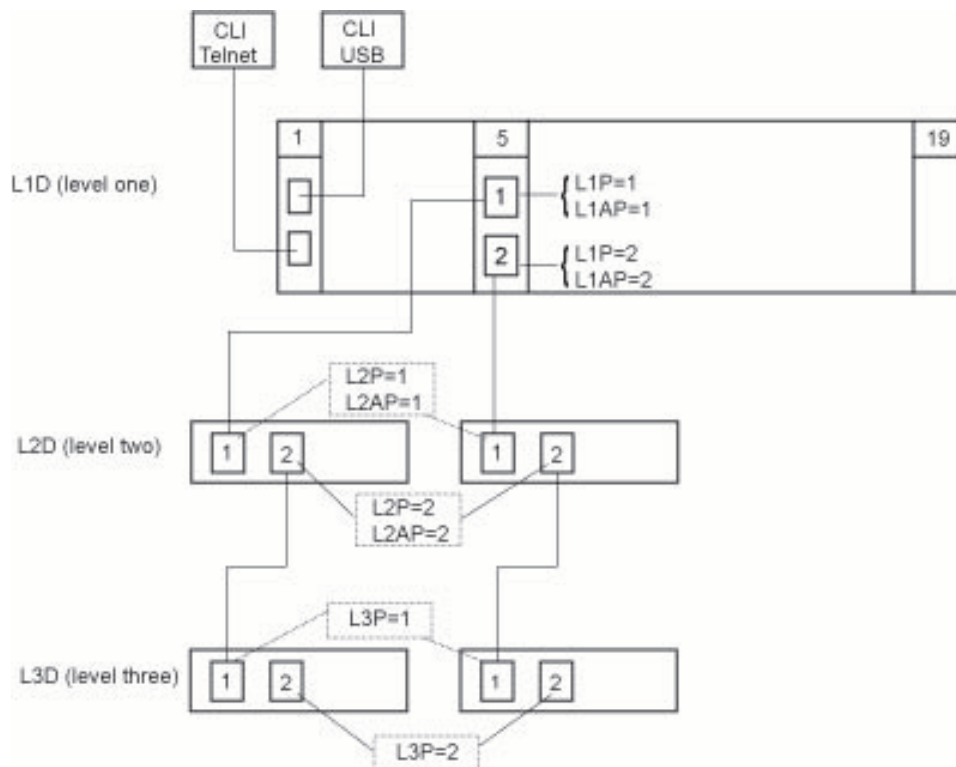


Figure 1: CLI Location Hierarchy

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

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

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

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

Physically these are the same port. That is, L1P1 and L1AP1 are both port one on a level one device. However, it is how they are used that determines their syntax. For example, L1P1 indicates that the port

is used to connect to a service device that is not managed by the IONMM. L1AP1 indicates that the port is used to connect to a level two device that can be managed by the IONMM.

Example 1

In the CLI location hierarchy, to go to the first port (L3P1) on device L3D in the network topology shown in Figure 19, you would enter the following command from the base prompt.

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

The resulting command line prompt would be:

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

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

Example 2

In the CLI location hierarchy, to go to device L2D in the network topology shown in Figure 5, you would enter the following command from the base prompt.

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

The resulting command line prompt would be:

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

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

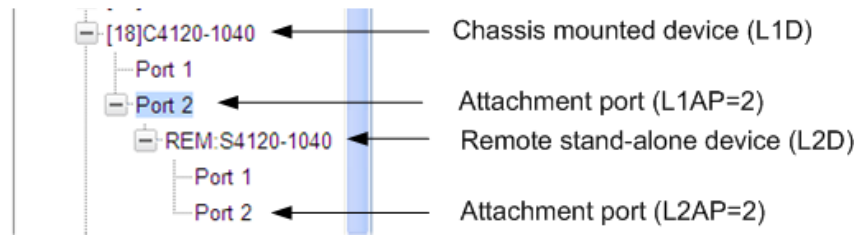
The following describes the procedure for using CLI commands to manage the x4120s.

1. Access the x4120 through either a USB connection or a Telnet session.
2. Use the **go** command to change the operational location to the device/port to be managed. The **go** command format is:

```
go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```
3. Configure the x4120 using the appropriate commands. For a complete list of the available commands, see the *x4120 CLI Reference Manual*.
4. To return the location to the IONMM, type **home** and press **Enter**.

Managing Slide-In and Remote Modules via the Web Interface

1. Access the x4120 through the Web interface (see “[Starting the Web Interface](#)” on page 45).



2. Click on the slide-in module or port to be managed.
3. The operations that can be performed depend on the type of slide-in module. Refer to the product documentation for the information. See the “[Related Manuals](#)” section on page 8.

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 Using CLI Commands

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

For example:

```
AgentIII C1|S7|L1D>
```

or just:

```
C1|S7|L1D>
```

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

The **go** command format is:

```
go [c=CHASSIS] [s=SLOT] [11ap=PORT] [12ap=PORT] (11p=PORT|12p=PORT|13p=PORT|11d|12d|13d)
```

EXAMPLE

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

```
C1|S7|L1D>go 11p=1
```

The resulting command line prompt would be:

```
C1|S7|L1P1>
```

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

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

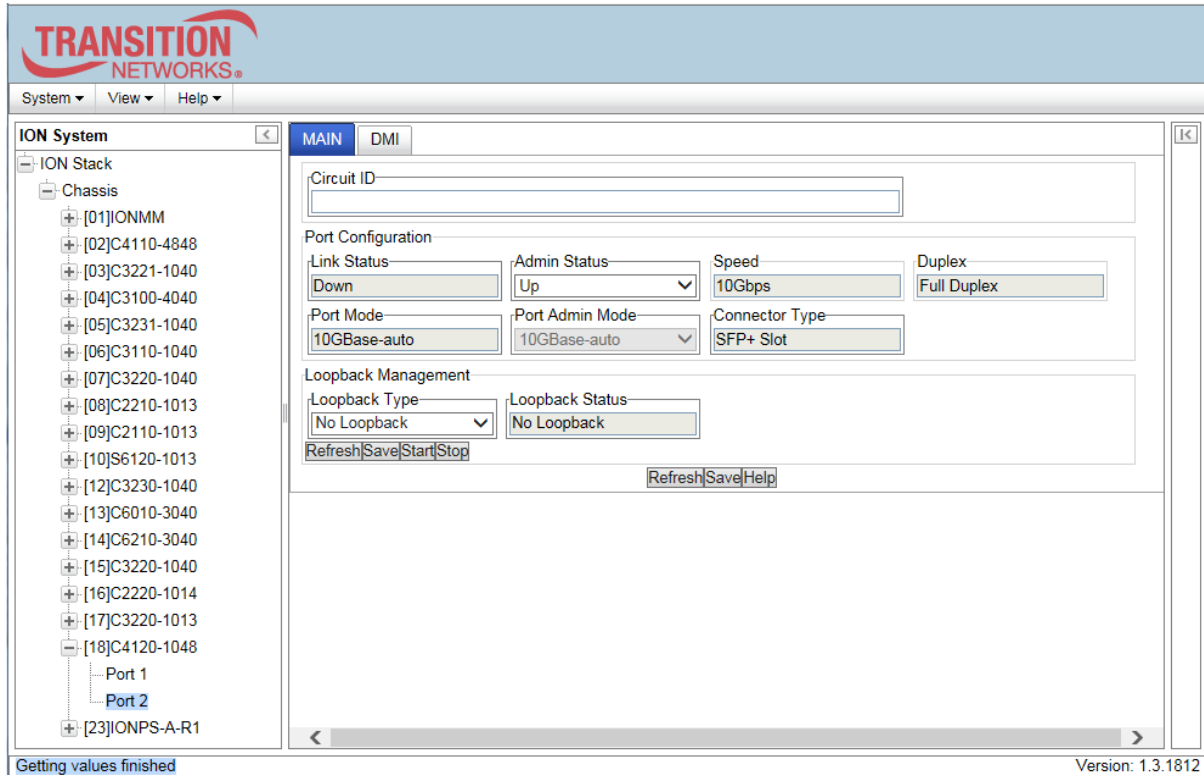
```
C1|S7|L1P1>go 11d
```

The resulting command line prompt would be:

```
C1|S7|L1D>
```

Managing Standalone Modules via the IONMM Web Interface

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Click the plus sign **[+]** next to **ION Stack** to unfold the "ION Stack" node in the left tree view if not already done.
3. Click the plus sign **[+]** next to **Chassis** and click the plus sign **[+]** next to a module.



4. Click on the module or port to be managed (e.g., the C4120 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	<p>ION Stack - consists of one chassis or one standalone device. The Stack Members table lists the Stack's chassis and its type.</p> <p>Chassis - the ION System family of products; the Chassis View shows a summary view of one such chassis. Model Information includes:</p> <ul style="list-style-type: none"> * Serial Number - The serial number of the chassis itself. Each x4120 also have its own serial number. * 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. * Software Revision, Hardware Revision, and Bootloader Revision. * Chassis Members table - lists local physical components in slots 1 to 19. <p>Device – provides tabs and sub-tabs for the IONMM and x4120s in the ION system.</p> <p>Port - provides tabs and sub-tabs for a selected x4120 port.</p>
System Dropdown	Sign out.
View Dropdown	Refresh.
Help Dropdown	Online Help, ION Product Home Page, About ION System Web Interface.
MAIN Tab	<p><u>Sections</u>: Model Information, System Configuration, Device Description, and Transparent Link Pass Through (TLPT) sections.</p> <p><u>Buttons</u>: Uptime Reset, System Reboot, Reset To Factory Config buttons. Refresh, Save, and Help buttons.</p>

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	<p><u>Sections:</u> Circuit ID, Port Configuration, and Loopback Management.</p> <p><u>Buttons:</u> <i>Refresh, Save, Start, Stop</i> and <i>Help</i>.</p>
DMI Tab (Port 2 only)	<p><u>Sections:</u> Interface Characteristics, Diagnostic Monitoring, Supported Media Length.</p> <p>The DMI (Diagnostic Maintenance Interface) function displays x4120 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See “DMI (Diagnostic Maintenance Interface) Parameters” on page 248 for more information.</p> <p>Note: not all x4120 and SFP models support DMI. Lantronix models that support DMI have a “D” at the end of the model number. If you click the DMI tab on a x4120 model that does not support DMI, the message “<i>The DMI feature is not supported on current port.</i>”</p> <p><u>Buttons:</u> <i>Refresh, Save, and Help</i>.</p>

Reboot, Reset, and Power Off Function Notes

Certain functions such as a System Reboot, Reset to Factory Configuration, Reset Power to a Slot, and Power Off a Slot) cause the system to delete certain stored files. **Caution:** In some circumstances, these stored files are lost unless you first perform a System Backup. See the “[Backup and Restore Operations](#)” section starting on page 199 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:

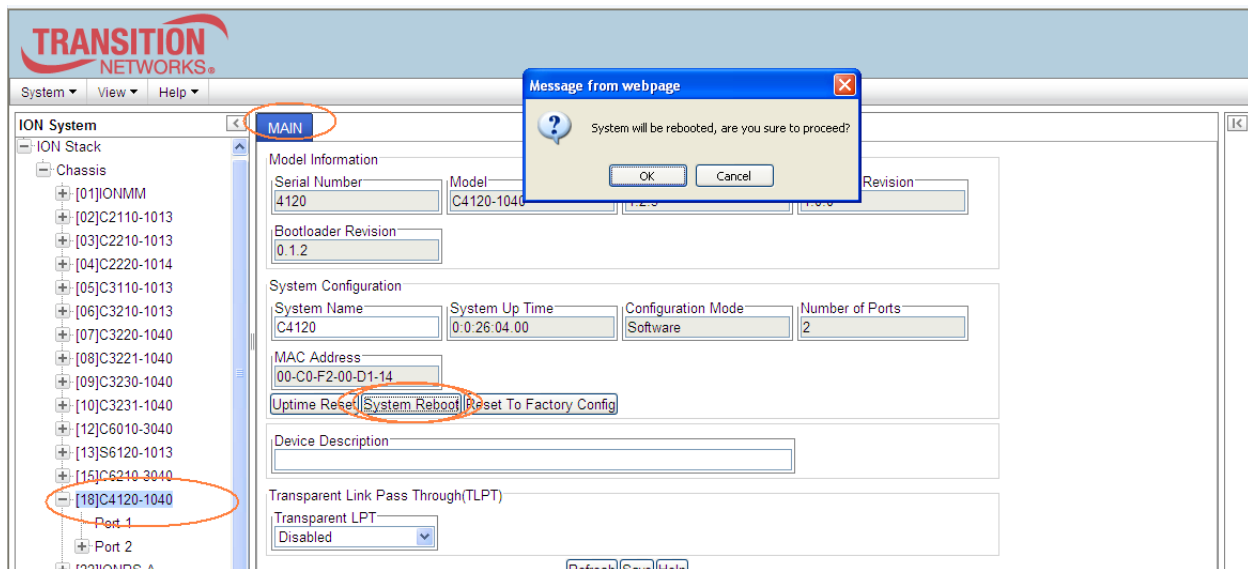
- Table 3: Port-Level Menu Description on page 18
- Table 4: File Status after a Reset to Factory Defaults on page 43
- Table 5: File Content and Location after a System Reboot on page 48



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

System Reboot

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



Press the **Cancel** button if you are not sure you want a system reboot to occur.

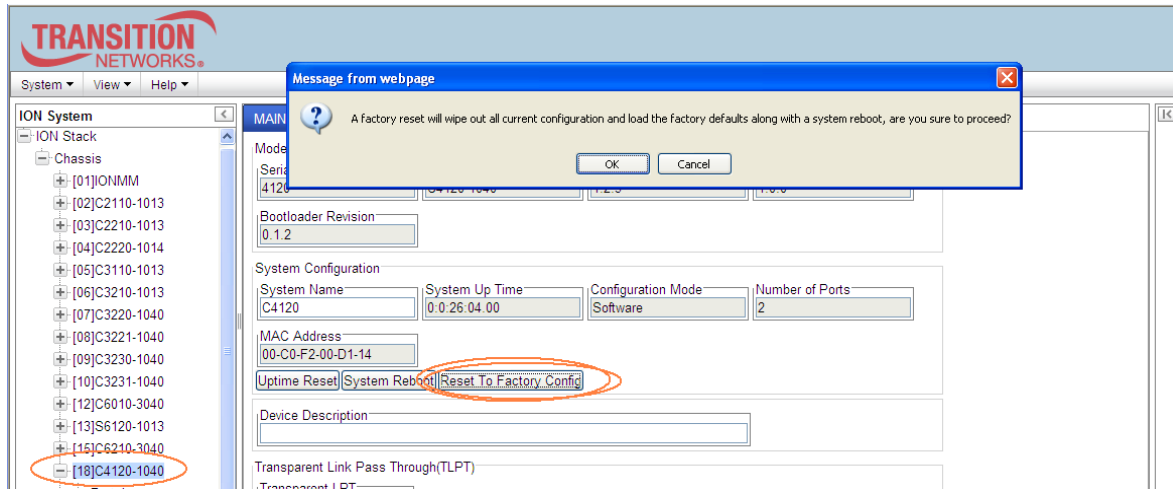
Press the **OK** button to clear the webpage message and begin the reboot process.

The message “*Loading, please wait...*” displays.

Note that a System Reboot can take several minutes.

Reset To Factory Config

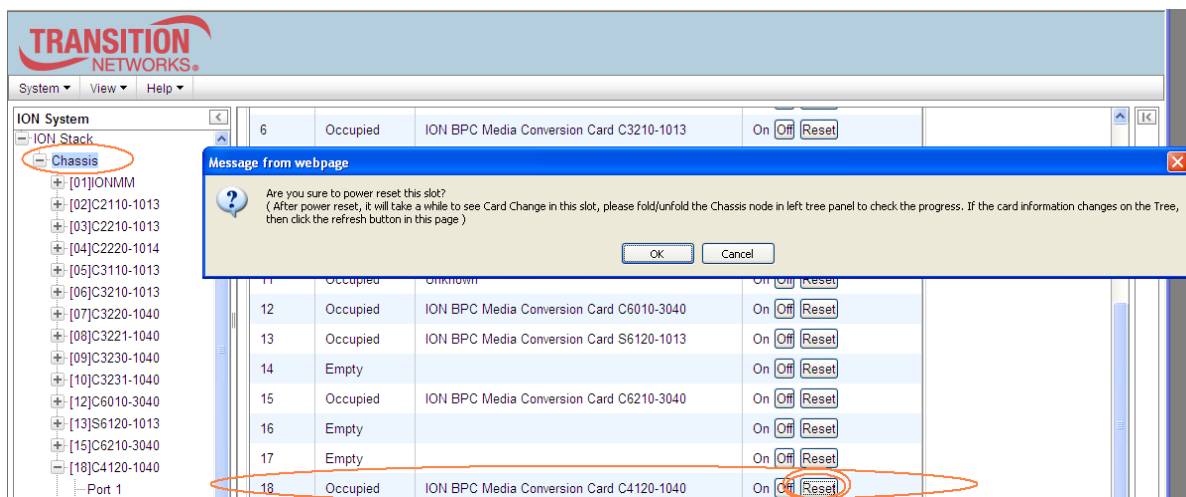
Clicking the **Reset To Factory Config** button resets the entire system configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the factory default settings. The message “A factory reset will wipe out all current configuration 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.

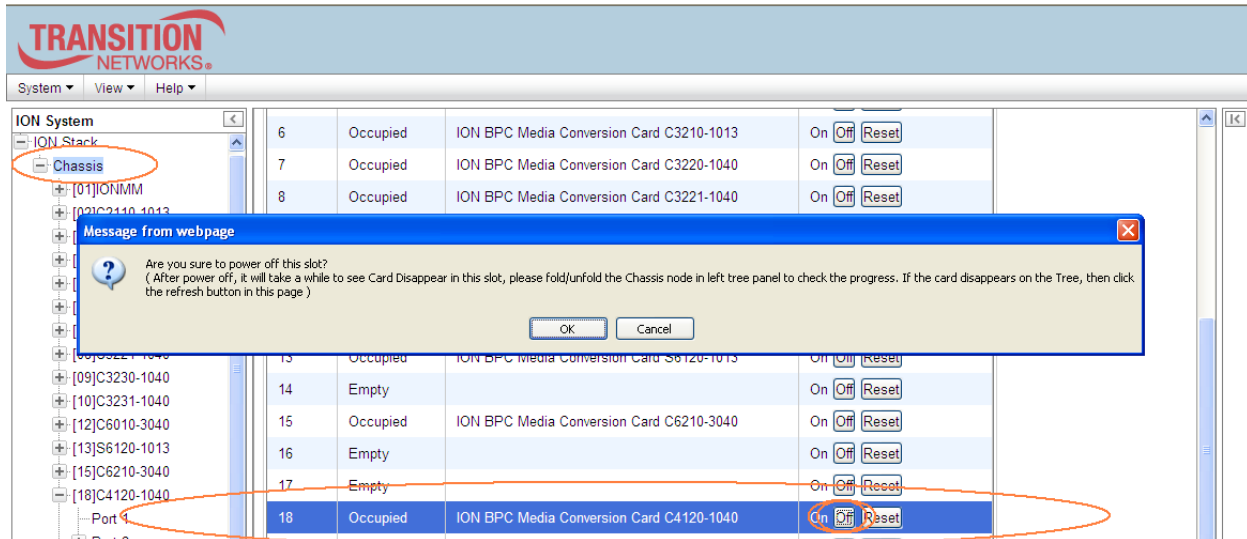


After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page.

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 x4120 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 x4120.

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 *x4120CLI Reference Manual*.

The operating characteristics that can be defined for the x4120 are:

- System setup
- Features
 - Transparent Link pass through (TLPT)
 - Device Description
- Port setup
 - Circuit ID
 - Admin Status
 - Loopback Management

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 C4120
- 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 CLI or the Web interface.

System Configuration – CLI Method

The system information can be alphabetic, numeric or a combination.

1. Access the x4120 through either a USB connection or a Telnet session.
2. Type **set system name=NAME**, where NAME is the new system name, and press **Enter**.

For example:

```
C1|S5|L1D>set system name=x4120-1013
```

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

```
Agent III C1|S18|L1D>show card info
System name:      C4120
Uptime:          00:02:19
MAC:             00-c0-f2-00-d1-38
Port number:     2
Serial number:   789568
Config mode:     software
Software:        2.0.0
Bootloader:      0.1.5
Hardware:        1.0.0
Agent III C1|S18|L1D>
```

Note: the **show card info** command does not work on a Power Supply module.

System Configuration – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. At the device’s **MAIN** tab, locate the **System Configuration** section.

The screenshot displays the web interface for the x4120 device. The top navigation bar includes the 'TRANSITION NETWORKS' logo and a menu with 'System', 'View', and 'Help'. The left sidebar shows the 'ION System' tree with a 'MAIN' tab selected. The main content area is divided into sections: 'Model Information' (Serial Number: 789568, Model: C4120-1048, Software Revision: 2.0.0, Hardware Revision: 1.0.0, Bootloader Revision: 0.1.5), 'System Configuration' (System Name: C4120, System Up Time: 0:0:04:54.00, Configuration Mode: Software, Number of Ports: 2, MAC Address: 00-C0-F2-00-D1-38), and 'Transparent Link Pass Through (TLPT)' (Transparent LPT: Disabled). At the bottom, there are buttons for 'Uptime Reset', 'System Reboot', and 'Reset To Factory Config', along with 'Refresh', 'Save', and 'Help' buttons. The status bar at the bottom indicates 'Getting values finished' and 'Version: 1.3.1812'.

3. In the **System Name** field, enter the name and for the x4120. 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 x4120 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 x4120 using either the CLI or Web method.

Device Description– CLI Method

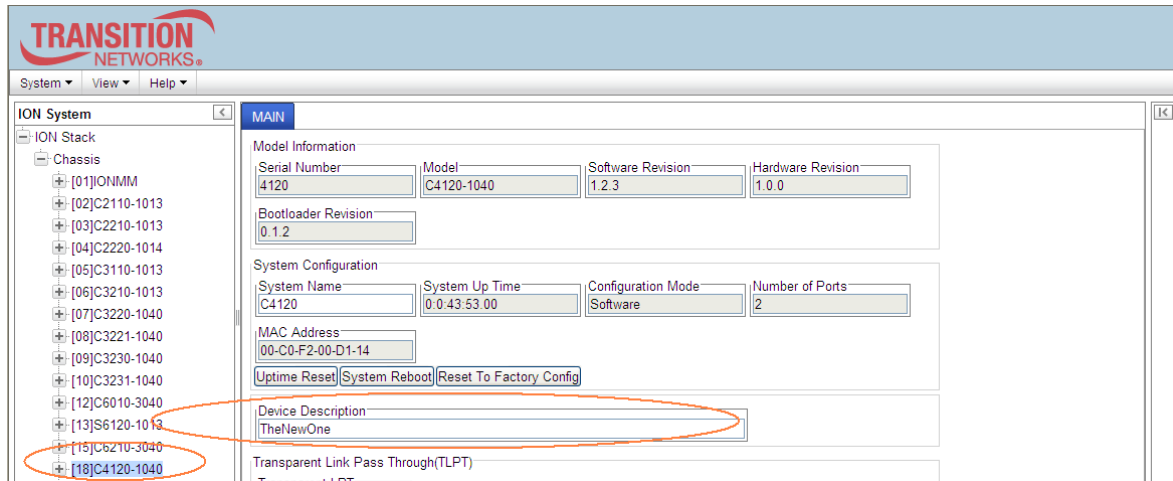
1. Access the NID through either a USB connection or a Telnet session.
2. At the device's command prompt type: **set device description=<xx>** where:

xx = the Device Description to be used for this device or port.
3. Press **Enter**.
4. Verify the Device Description setting. Type **show device description** and press **Enter**. Note that the dash ("-") is required, and the letters "ID" must be upper-case. The Device Description information displays. For example:

```
Agent III C1|S17|L1D>set device description thenewone
Agent III C1|S17|L1D>show dev descr
Device description: thenewone
Agent III C1|S17|L1D>
```

Device Description Config – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. At the x4120 **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.

Circuit ID Configuration

The x4120 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 63 bytes and override the default information, which is vlan-module-port in binary format.

The Circuit ID can be configured in the x4120 using either the CLI or Web method.

Circuit ID Config – CLI Method

1. Access the NID through either a USB connection or a Telnet session.

2. At the device's command prompt type: **set circuit-ID=<xx>** where:

xx = the Circuit ID to be used for this device or port.

3. Press **Enter**.

4. Verify the Circuit ID setting. Type **show circuit-ID** and press **Enter**. Note that the dash ("-") is required, and the letters "ID" must be upper-case. The Circuit ID information displays. For example:

```
C1|S16|L1D>set circuit XX/YYYY/000000/111/CC/SEG
C1|S16|L1D>show circuit-ID
Circuit-ID:      XX/YYYY/000000/111/CC/SEG
C1|S16|L1D>
```

5. At the each of the device port's command prompts, enter the Circuit ID as in step 2 and 3.

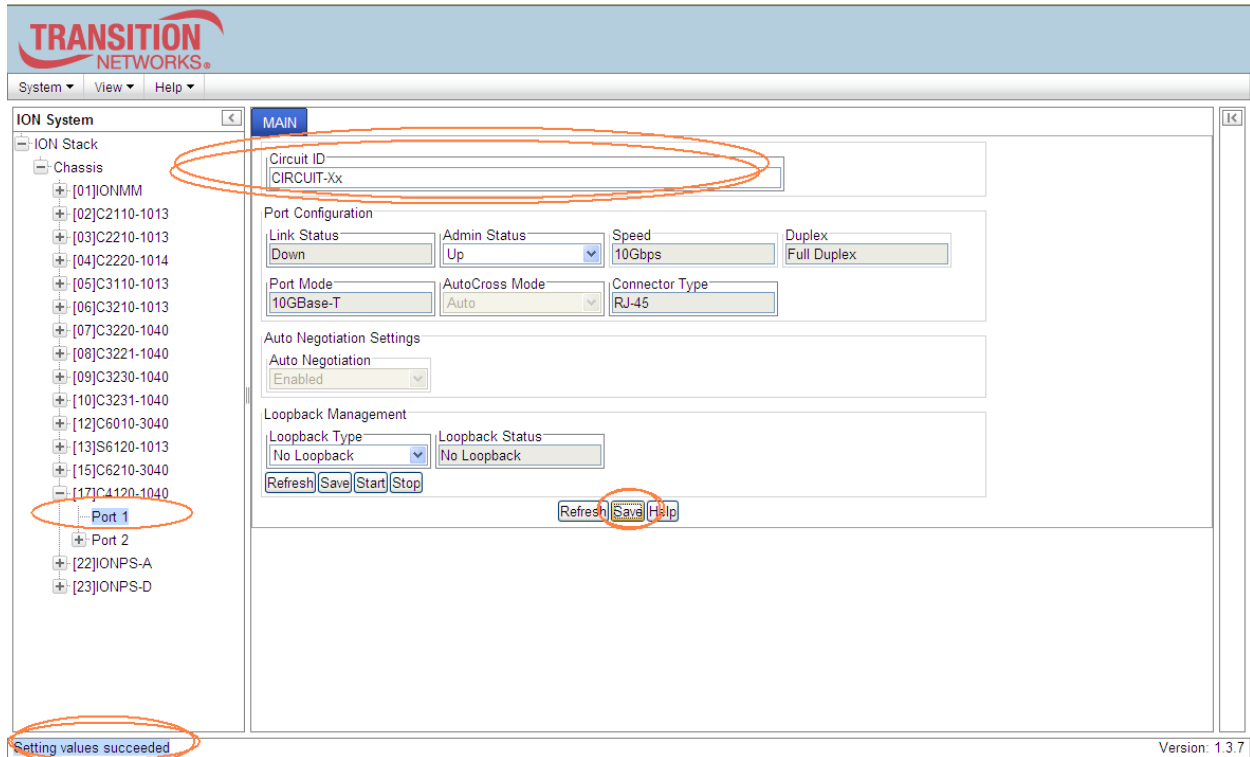
6. At the each of the device port's command prompts, verify the Circuit ID setting as in step 4. For example:

```
C1|S16|L1D>go l1p=1
C1|S16|L1P1>set circuit-ID=xx/yyyy/000000/111/cc/seg
C1|S16|L1P1>show circuit-ID
Circuit-ID:      xx/yyyy/000000/111/cc/seg
C1|S16|L1P1>

C1|S16|L1P1>go l1p=2
C1|S16|L1P2>set circuit XX/YYYY/000000/111/CC/SEG
C1|S16|L1P2>show circuit-ID
Circuit-ID:      XX/YYYY/000000/111/CC/SEG
C1|S16|L1P2>
```

Circuit ID Config – Web Method

1. Access the x4120 via the Web interface (see “Starting the Web Interface” on page 45).
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:

- c) Click Refresh, and re-enter a Circuit ID of 64 or fewer characters and click **Save**.
- d) The message “*Setting values succeeded*” displays in the lower left corner of the Web interface.

Transparent Link Pass Through (TLPT) Configuration

The x4120 supports Transparent Link Pass Through (TLPT) at the device level. The TLPT feature can be configured in the x4120 using either the CLI or Web method. **Note** that x4120 FW v2.0.1 upgraded TLPT to operate correctly.

Transparent Link Pass Through (LPT) Config – CLI Method

1. Access the x4120 through either a USB connection or a Telnet session.
2. At the device's command prompt type: **set transparent lpt state =xx**, where xx= <enable or disable>.
3. Press the **Enter** key.
4. Verify the TLPT setting. Type **show lpt config** and press **Enter**. For example:

```
Agent III C1|S17|L1D>set transparent lpt state ?
  disable
  enable
Agent III C1|S17|L1D>set transparent lpt state enable
Agent III C1|S17|L1D>set transparent lpt state disable
Agent III C1|S17|L1D>set transparent lpt state enable
Agent III C1|S17|L1D>show lpt config
Link pass through configuration:
-----
Link pass through state:          notSupported
Transparent link pass through state:  enable
Selective link pass through state:  notSupported
Link pass through monitor port:    0
Remote fault detect state:        notSupported
Agent III C1|S17|L1D>
```

Use the **show lpt config** command to display the current link pass through configuration.

Transparent Link Pass Through (TLPT) Config – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. At the **MAIN** tab, locate the **Transparent Link Pass Through (TLPT)** section.

The screenshot displays the Transition Networks web interface. The left sidebar shows a tree view of the ION System configuration, with the [18]C4120-1048 node selected. The main content area is titled "MAIN" and contains the following sections:

- Model Information:** Serial Number (789568), Model (C4120-1048), Software Revision (2.0.0), Hardware Revision (1.0.0), and Bootloader Revision (0.1.5).
- System Configuration:** System Name (C4120), System Up Time (0:0:04:54.00), Configuration Mode (Software), and Number of Ports (2).
- MAC Address:** 00-C0-F2-00-D1-38.
- Device Description:** A text input field.
- Transparent Link Pass Through (TLPT):** A section with a dropdown menu for "Transparent LPT" currently set to "Disabled".

Buttons for "Refresh", "Save", and "Help" are located at the bottom right of the configuration area. The status bar at the bottom left shows "Getting values finished" and the bottom right shows "Version: 1.3.1812".

3. Select **Enabled** or **Disabled**. The default is Disabled. Click **Save** when done.

Displaying AutoCross

Normally, twisted pair (copper) ports must be connected so that the Transmit pair on one end is connected to the Receive pair on the other end, and vice versa. If the cabling is done so that Transmit on one end is wired to Transmit on the other, and Receive is wired to Receive, the link will not come up.

Hubs and switches are deliberately wired opposite of the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used and the pairs will match up properly. When two hubs/switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to make sure that the correct pairs are connected.

The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX).

On x4120 devices the *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection, making the distinction between a straight through cable and a crossover cable unimportant.

Note:

- This feature is defined on a port level; depending on the physical connector it is not applicable for all ports.
- Lantronix recommends leaving *AutoCross* in default mode, **Auto**.

AutoCross Config – CLI Method

1. Access the x4120 through either a USB connection or a Telnet session.

2. At the device port's command line, type **show ether autocross=xx** where:

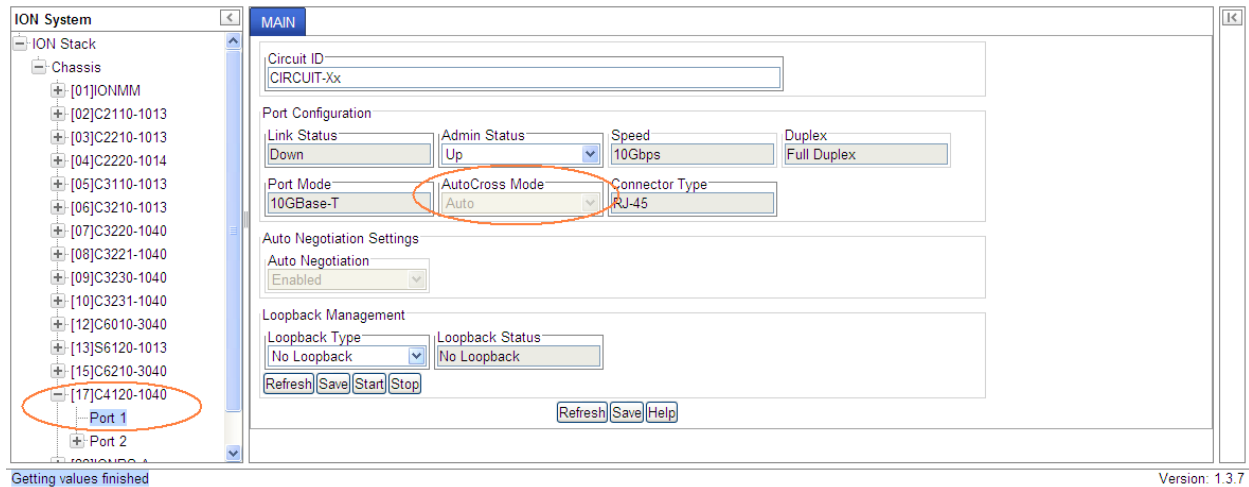
xx = cable type. Valid choices are:

- **Auto** – hardware will automatically correct errors in cable selection.

3. Press **Enter**.

AutoCross Config – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port’s **MAIN** tab.
3. Locate the **Port Configuration** section.



4. In the **AutoCross Mode** field, select the mode to be used.
 - **Auto** – ION System hardware will automatically correct errors in cable selection (default mode - recommended).

Displaying Auto Negotiation

The auto negotiate feature is defined on a port basis, letting you set the capabilities that will be advertised for a device over a specific port.

Auto negotiation is a feature that can be used by devices that are capable of different transmission rates (such as 10 Mbit/sec and 100 Mbit/sec), different duplex modes (half-duplex and full duplex), and/or different standards at the same speed. Every device declares its possible modes of operation when attempting to connect to another device. The two devices then choose the best possible modes of operation that are shared by the two devices. These modes of operation include speed and duplex.

When one device supports auto negotiation and the other does not, the device that has auto negotiation abilities can determine the speed of the other device, and then select the same speed for itself. However, this procedure cannot determine the duplex setting of the other device, so half-duplex is always assumed. If one device is using full duplex while the other one is using half-duplex, a duplex mismatch occurs. The usual effect of this mismatch is that the connection works but at a very low speed. Disabling the auto negotiate feature allows you to force the connection to the desired speed and duplex mode of operation as long as both devices can support the operation.

Note: The auto negotiate feature is always enabled for gigabit devices/ports.

Auto Negotiation – CLI Method

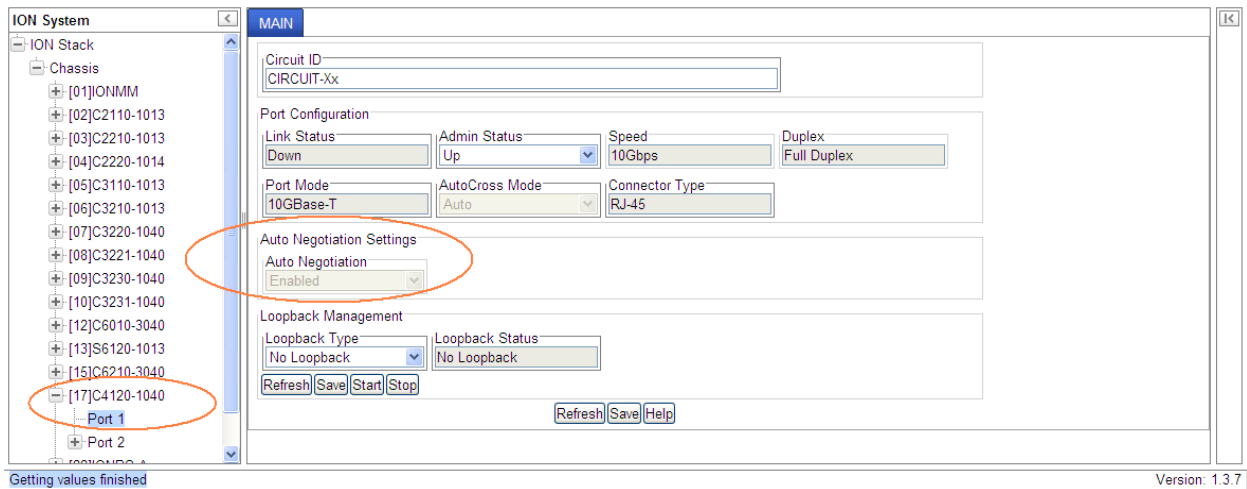
1. Access the x4120 through either a USB connection or a Telnet session.
2. Verify the configuration settings Type: **show ether config** and press **Enter**. The current Ethernet configuration displays. For example:

```
Agent III C1|S17|L1P1>show ether config
Port-11040
TP port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 RJ-45
PHY operation mode:        phy10GBaseT
Speed:                    10G
Duplex:                   full
Autocross:                auto

AutoNeg admin state:      enable
Agent III C1|S17|L1P1>
```


Auto Negotiation – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port.
3. Locate the **Auto Negotiation Settings** section on the **MAIN** tab.



4. In the **Auto Negotiation** field, observe whether this feature is enabled or disabled.

Check Ethernet Port Configuration

With auto negotiate disabled, the connection is forced to the desired speed and duplex mode of operation as long as both devices can support the operation. **Note:** The Auto Negotiate feature is always enabled for gigabit devices/ports.

A port's Ethernet port speed and mode can be verified in the x4120 using either the CLI or Web method.

Check Ethernet Port Config– CLI Method

Use this procedure to define the port's Ethernet transmission speed and Duplex mode to be used on the Ethernet port. The defaults are 10 Mbps and Full Duplex.

Note: This command is only applicable on a copper port.

1. Access the x4120 through either a USB connection or a Telnet session).
2. Check the configuration settings. Type: **show ether config** and press **Enter**.
The Ethernet configuration displays. The example below show a TP port, the second example shows a Fiber Port:

```
Agent III C1|S17|L1P1>show ether config
Port-11040
TP port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 RJ-45
PHY operation mode:        phy10GBaseT
Speed:                     10G
Duplex:                    full
Autocross:                 auto

AutoNeg admin state:      enable
Agent III C1|S17|L1P1>
```

Check Ethernet Port Config – Web Method

Use this procedure to define the transmission speed and Duplex mode to be used on the Ethernet port. The defaults are 10 Mbps and Full Duplex. **Note:** This command is only applicable on a copper port.

1. Access the x4120 through the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select the appropriate port.
3. Locate the **Auto Negotiation Settings** section on the port's **MAIN** tab.

The screenshot displays the web interface for configuring an Ethernet port on the x4120 device. The left sidebar shows a tree view of the ION System hierarchy, with the following items listed: ION Stack, Chassis, [01]IONMM, [02]C2110-1013, [03]C2210-1013, [04]C2220-1014, [05]C3110-1013, [06]C3210-1013, [07]C3220-1040, [08]C3221-1040, [09]C3230-1040, [10]C3231-1040, [12]C6010-3040, [13]S6120-1013, [15]C6210-3040, [17]C4120-1040 (selected), Port 1 (selected), and Port 2. The main configuration area is titled 'MAIN' and contains the following sections:

- Circuit ID:** CIRCUI-Xx
- Port Configuration:**
 - Link Status: Down
 - Admin Status: Up
 - Speed: 10Gbps
 - Duplex: Full Duplex
 - Port Mode: 10GBase-T
 - AutoCross Mode: Auto
 - Connector Type: RJ-45
- Auto Negotiation Settings:** Auto Negotiation is set to Enabled.
- Loopback Management:**
 - Loopback Type: No Loopback
 - Loopback Status: No Loopback

Buttons for 'Refresh', 'Save', 'Start', and 'Stop' are located at the bottom of the configuration area. The status bar at the bottom left indicates 'Getting values finished' and the bottom right shows 'Version: 1.3.7'.

Loopback Management

The x4120 provides a PHY Layer loopback test from the CLI and Web interface.

Loopback Management – CLI Method

Use this procedure to set the type of loopback test and to start and stop the selected loopback test.

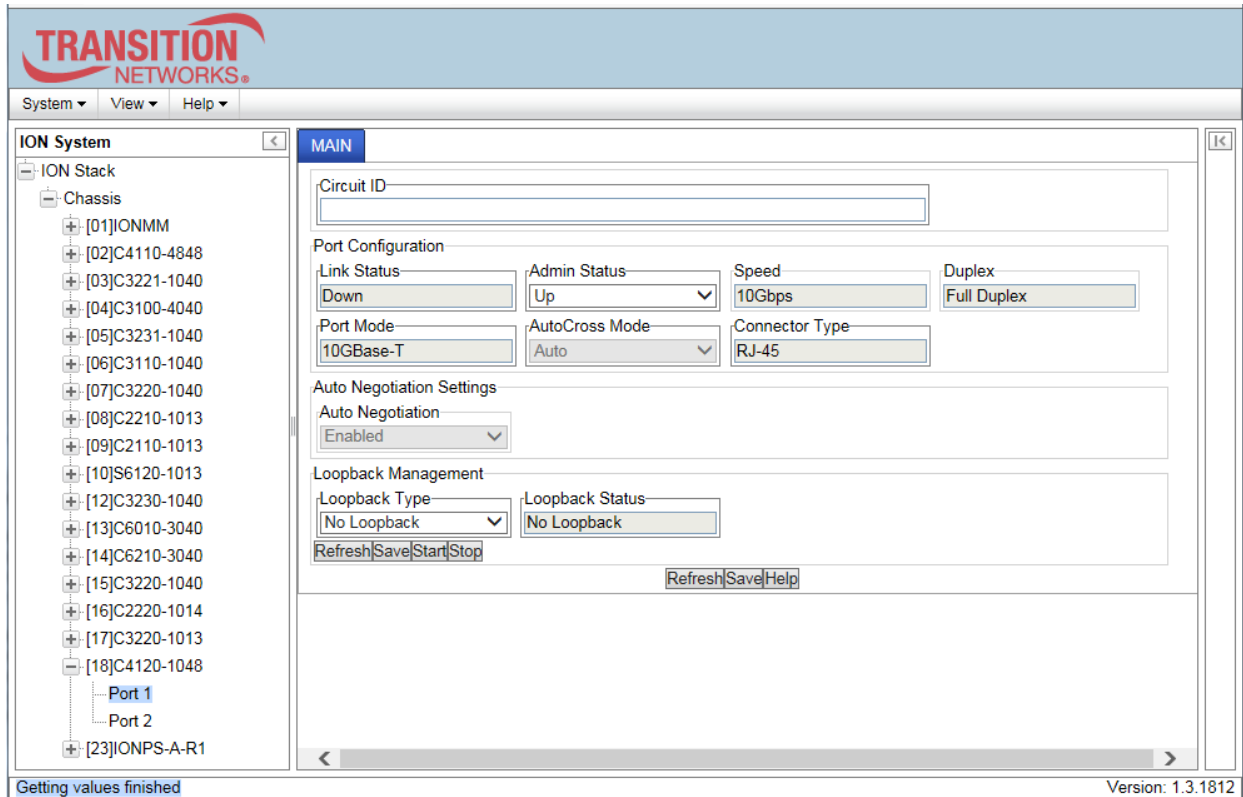
1. Access the x4120 through either a USB connection or a Telnet session.
2. Set the Ethernet Loopback Type. At the command line, type: **set ether loopback type= xx**, where:
xx = noloopback|phylayer.
3. Start the x4120 PHY Layer loopback test. At the command line, type: **set ether loopback oper=init** and press **Enter**.
4. Stop the x4120 PHY Layer loopback test. At the command line, type: **set ether loopback oper=stop** and press **Enter**.
5. For example:

```
Agent III C1|S17|L1P1>set ether loop type no
Agent III C1|S17|L1P1>set ether loop type phy
Agent III C1|S17|L1P1>set ether loop type remote
Error: Set Ethernet port loopback type failed.
Agent III C1|S17|L1P1>set ether loop oper init
Agent III C1|S17|L1P1>set ether loop oper stop
```

Loopback Management – Web Method

Use this procedure to perform a PHY Layer loopback test from the x4120 Web interface.

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port.
3. Locate the **Loopback Management** section on the port's **MAIN** tab.



4. At the Loopback type dropdown, select **PHY Layer**.
5. Click the **Start** button to begin the Loopback test.
6. Click the **Stop** button to end the Loopback test. The Loopback Status field displays “Local In Loopback” during loopback test operation.
7. Click the **Stop** button. The loopback test ends, Loopback Status reverts to “No Loopback”, and the Loopback Type field reverts to “No Loopback”.

4: Operation

General

This section describes the non-configuration operations that can be performed for the x4120.

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 x4120s in the ION system.

A Backup is used to get the SIC card running configuration, convert it to CLI commands, and save those CLI commands into the backup file. The backup file is stored in the IONMM.

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

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

Lantronix recommends that you to enter a “**show card info**” CLI command to view the SIC card’s current configuration before a backup/restore operation to verify the desired configuration settings. There are several CLI **show** commands that allow you to display (show) information about a SIC card’s configuration. For a complete description of these and other CLI commands see the *x4120 CLI Reference Manual*, 33497.

Displaying Information

There are several CLI commands that allow you to display (show) information about the x4120 configuration. For a complete description of these and other CLI commands see the *x4120 CLI Reference Manual*, 33552.

Reset to Factory Defaults

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

IMPORTANT



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

Resetting Defaults – CLI Method

1. Access the x4120 through either a USB connection or a Telnet session.
2. At the command prompt type: **reset factory**.
3. Press **Enter**. The following displays:

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

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

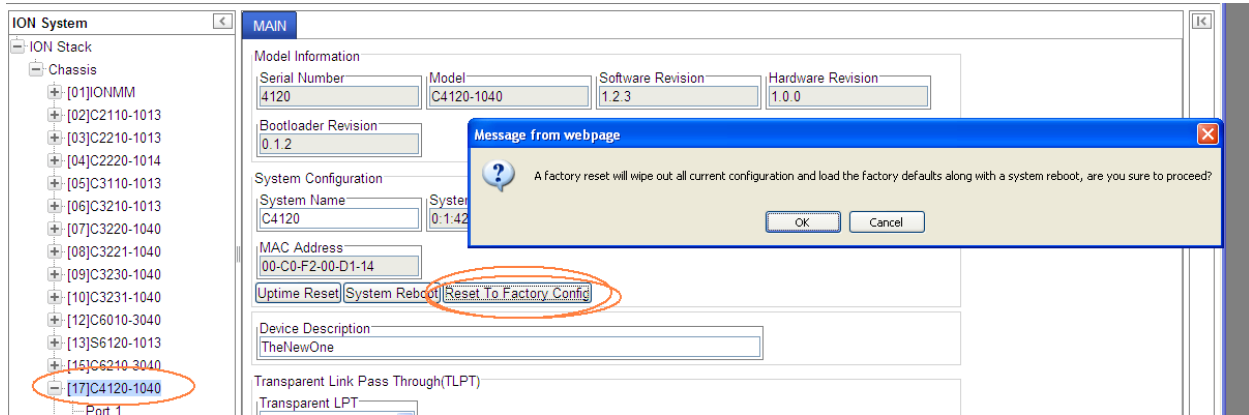
Note: Your USB and/or Telnet session will be disconnected.

4. Set the IP configuration (see “[Doing the Initial System Setup](#)” on page 48).

Resetting Defaults – Web Method

Caution: This operation deletes all configuration information that was saved in the x4120, including the IP address you assigned to the x4120.

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



4. Click the **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” on page 48).

File Status after Reset to Factory Defaults

The table below shows the status of x4120 files after a system re-boot.

Table 4: File Status after a Reset to Factory Defaults

File Type	Filename	File Description	Stored Directory	Status after Re-store 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 x4120 system uptime field displays the amount of time that the x4120 has been in operation.

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

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

Reset System Uptime – CLI Method

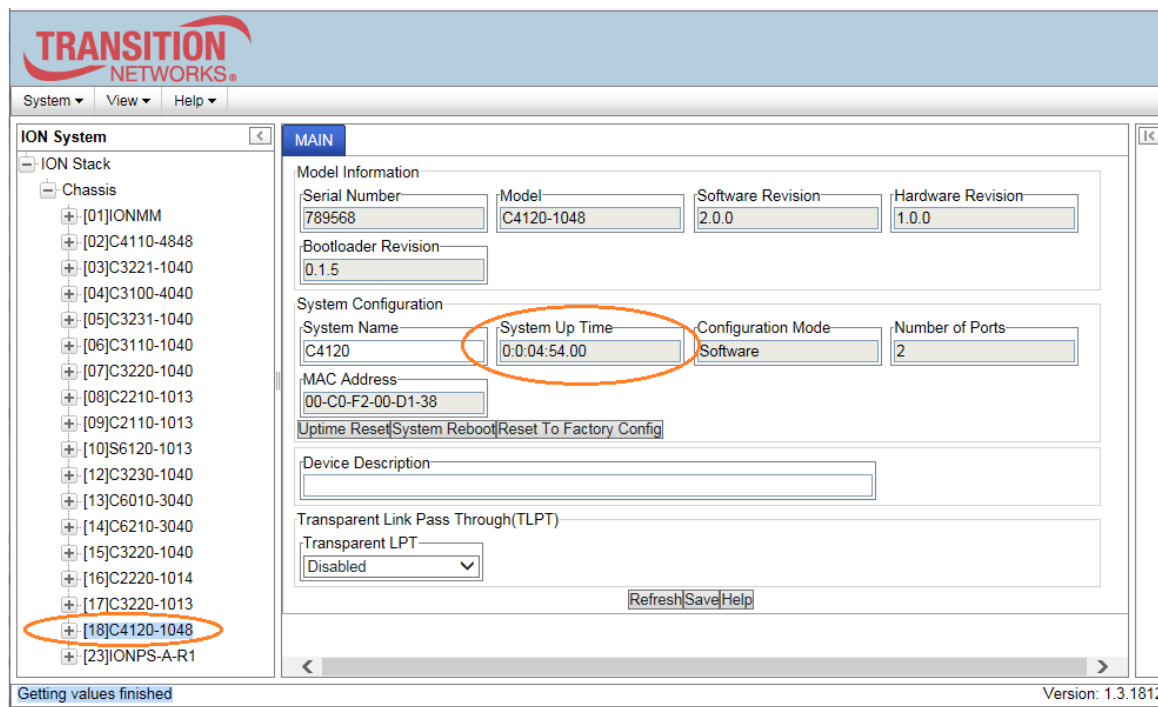
1. Access the x4120 through either a USB connection or a Telnet session.
2. At the command prompt type: **reset uptime** and press **Enter**. The System Up Time field resets to zero, and immediately begins to increment.

For example:

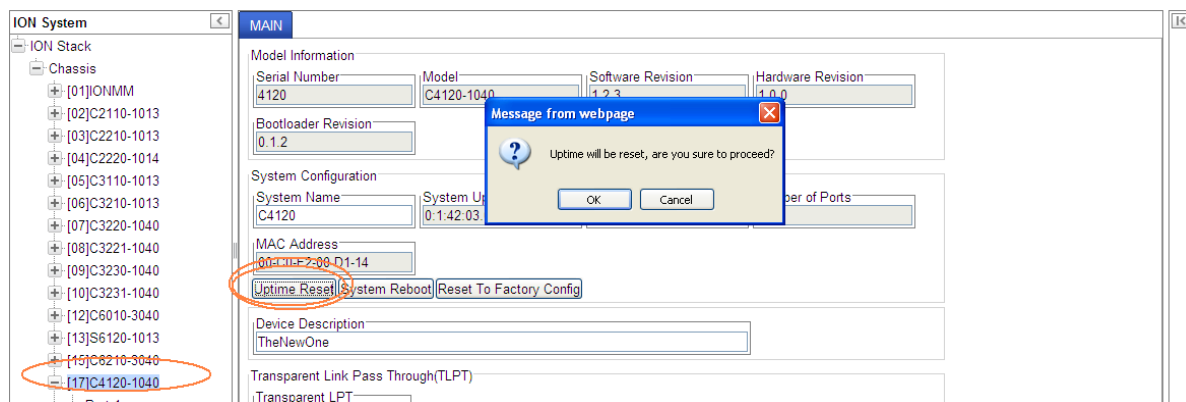
```
Agent III C1|S17|L1D>reset uptime  
Agent III C1|S17|L1D>
```

Reset System Uptime – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 26).
2. At the **MAIN** tab, locate the **System Configuration** section.



3. If desired, observe and record the **System Up Time** field count.
4. Click the **Uptime Reset** button.



5. At the “Uptime reset, are you sure” window, click **OK** to reset the system up time.

The message “Setting values succeeded” displays at the bottom left of the screen when the up time reset is done.

6. Click the **Refresh** button at the bottom of the screen. The **System Up Time** field resets to zero, and immediately begins to increment.

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.



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 – CLI Method

After a x4120 reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.

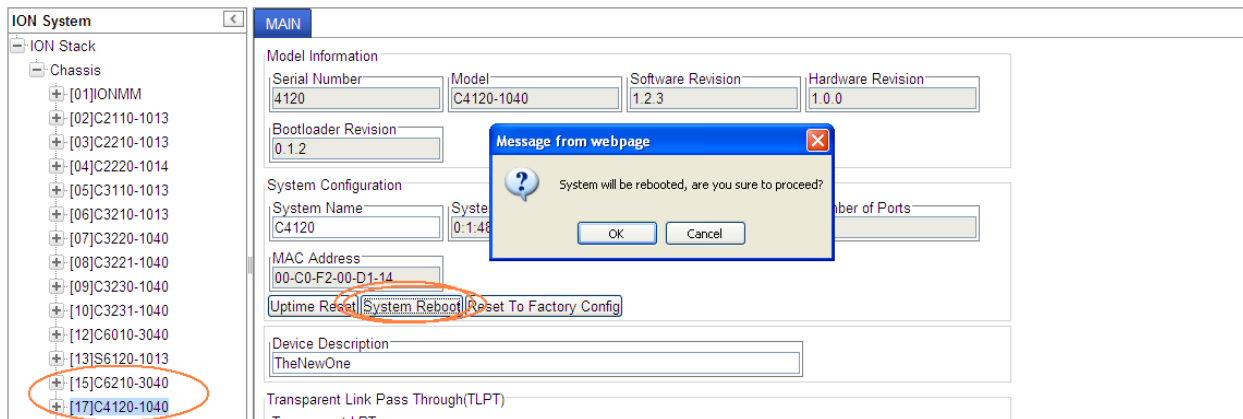
1. Access the x4120 through either a USB connection or a Telnet session.
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login again!* The ION system reboots the x4120. If this operation is performed on a standalone module, the connection / session is terminated.
3. To reestablish the connection / session, wait about one minute, and then:
 - For a USB connection
 - a) Select **Call>Disconnect**.
 - b) Select **File>Exit**.
 - c) Disconnect then reconnect one end of the USB cable.
 - d) Start a USB session (see "[Starting a USB Session](#)").
 - For a Telnet session
 - a) Press **Enter**.
 - b) Start a Telnet session (see "[Starting a Telnet Session](#)").

Rebooting – Web Method

Caution: Doing a system reboot 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 x4120 through 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 x4120 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 5: 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	drop-bear_rsa_host_key drop-bear_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 x4120 Firmware

Occasionally changes must be made to the firmware version that is currently stored in IONMM or x4120 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 management module has the latest firmware version installed and running. The latest firmware version is on the [C4120 Product Resources](#) page.

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.

Note: You cannot upgrade a module with multiple BIN files.

Remote Management in an Unmanaged Chassis

ION x4120 Version 1.2.6 was released August 12, 2016. This release added:

- Support for the management of a C4120 when installed in an unmanaged ION chassis. Management is supported by another C4120 installed in a managed chassis when the two are linked together via a fiber cable. On initial power up, additional time, approximately 1min & 10sec, is now required for the cards to be displayed in the management interface. This time is needed for the cards to determine if they are installed in a managed or an unmanaged chassis.
- Support for remote firmware upgrades of a C4120 in an unmanaged chassis. Remote firmware upgrades in an unmanaged chassis is supported only after a factory bootloader upgrade is performed. Remote firmware upgrades in an unmanaged chassis can take up to 3 minutes to transfer the file, reboot, search for management module, and display card in management interface.

For more information see “*Local Management of Cards in a Remote Un-managed Chassis*”.

Transfer Files via Serial Protocol (X/Y/Zmodem) – CLI Method

Use the **serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem)** commands to transfer a file over a serial line. These commands can only be entered at the device level (e.g., when the command line prompt is C1|S8|L1P1> or similar). These commands function like the TFTP download function; technical support can download configuration files and firmware files through the x4120 USB port by entering the corresponding CLI commands. If the serial file transfer causes HyperTerminal (HT) to have problems recognizing ION CLI commands, type q and press Enter, and then log back in to HT.

General Usage:

serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem) file=FILE%s

Perform this procedure to upgrade the x4120 firmware from the CLI.

1. Access the IONMM through either a USB connection or a Telnet session.
2. Sends a request to the server / local file system to download content for a subsequent **put** command. Type **serial get protocol zmodem file=xxxx** and press **Enter**.
3. Send a request to the server / local file system to upload content. Type **serial put protocol zmodem file=xxxx** and press **Enter**.
4. Perform a firmware upgrade over the selected serial line. Type **serial upgrade protocol zmodem file=xxxx** and press **Enter**.

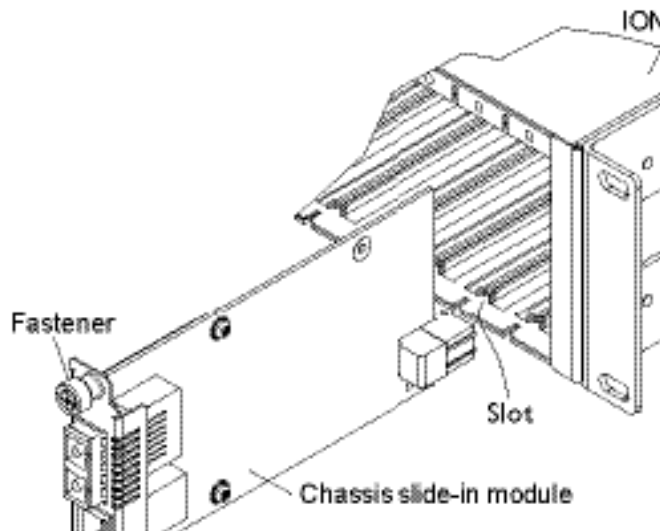
For example:

```
C1|S1|L1D>serial ?
  get
  put
  upgrade
C1|S1|L1D>serial get protocol zmodem file=xxxx
Warning: the input file name will be ignored when using ymodem/zmodem to retrieve
file!
now start to transfer the file ...
ŠCCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0BB0
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file ...
Šlsz: cannot open /tftpboot/xxxx: No such file or directory
BB0BB0BB0
BB0BB0
Can't open any requested files.
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial upgrade protocol zmodem file=xxxx
now start to transfer the file ...
**B00000063f694ceive.**B00000063f694
CCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>
```


Replacing a Chassis Resident C4120

The C4120 is a “hot swappable” device (it can be removed and installed while the chassis is powered on). To replace a chassis resident C4120, do the following.

1. Backup the configuration (see “[Backing Up Slide-In and Remote Modules](#)” on page 150).
2. Disconnect any cables attached to the x4120.



3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the x4120 from the ION Chassis.
5. Carefully slide the new x4120 fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the x4120 to the ION chassis.
7. Connect the appropriate cables to the x4120.
8. Load the configuration into the new x4120 (see “[Restoring Slide-In and Remote Modules](#)”).

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 x4120 and jumpers, and describes where and how to get technical support.

Note: 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 x4120s (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web Interface or ION command line interface - CLI).
- ION power supply
- ION options (ION SFPs, ION LG Kit, etc.)
- Data cables, electrical cables, and electrical outlets
- Third party network equipment (circuit protection equipment, battery backup, 3rd party client or server software – 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 simplest and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the x4120s 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 Lantronix product or firmware version may not support all the features documented for this module. For the latest feature information and caveats, see the release notes for your particular device/system and firmware release.
8. 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 before calling Lantronix for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED Fault and Activity Displays (page [54](#))
- Problem Conditions (page [55](#))
- CLI Messages (page [57](#))
- Web Interface Messages (page [62](#))
- Windows Event Viewer Messages (page [82](#))
- Config Error Log (config.err) File (page [113](#))
- Webpage Messages (page [117](#))
- Third Party Troubleshooting Messages (page [120](#))

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 x4120 via the Web Interface

1. Can you access the IONMM?

Yes	No
Continue with Step 2.	See “Cannot access the IONMM via the Web” .

2. Power cycle the x4120.
3. If the problem persists, contact Technical Support.

Cannot upgrade modules

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

Cannot upload upgrade files

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

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.

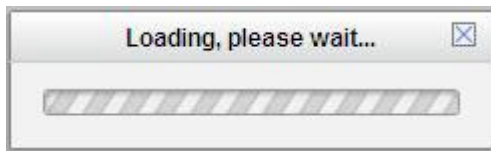
The device may have a jumper or switch that disables software management of the device. When Configuration Mode is **hardware**, the devices take some of the configurations from DIP switches or jumpers on the device. In **software** mode, configuration is controlled by management.

1. Refer to the “[Jumper Settings](#)” section on page [312](#) for details on hardware mode configuration.
2. Contact Lantronix for more information.

Ethernet connection works, but at a very low speed

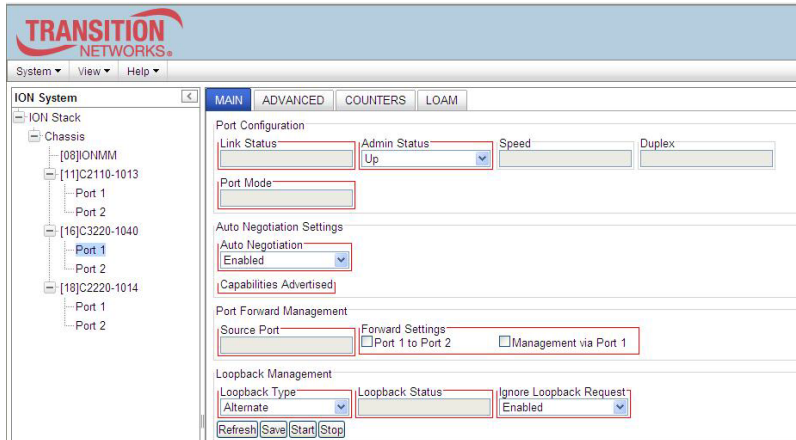
1. Check if the **Auto Negotiate** feature is enabled.
2. If **Auto Negotiate** is enabled, check if one device is using full duplex while the other one is using half-duplex (a duplex mismatch condition). The usual effect of this mismatch is that the connection works but at a very low speed.
3. Change Ethernet connection settings; see "[Configuring Auto Negotiation](#)" on page [77](#).

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.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



1. Check if the device is physically connected and powered on.
2. Verify the x4120 DIP switch settings and HW/SW Jumper setting.
3. Refresh the IONMM or x4120 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.

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 C2220 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 x4120 is at an older version and shows the newer functions as 'red boxed'. Since the older version of x4120 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as 'red boxed'. Upgrade the devices to the latest software version.
3. Reboot the system. See the "[Reboot](#)" section on page [115](#) for more information.
4. Contact Lantronix for more information.

TFTP Server Address is empty or invalid!

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

Windows XP Cannot Find Drivers For My Device

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

1. Contact Lantronix for more information. Contact Technical Support.

Windows XP Forces a Reboot after Installing a Device

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

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

Driver Installation Fails and Windows XP Gives Error Code 10

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

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

Windows XP Displays an Error and then Terminates Installation

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



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, re-enter 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.

CLI Messages

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

Ambiguous command

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

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

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

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

and then press the **Enter** key, the message “% *Ambiguous command.*” displays.

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

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

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See the *x4120 CLI Reference Manual*, 33497.
4. If the problem persists, contact Technical Support.

Bad advertisement capability!

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

1. Verify the command syntax.
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Cannot get link pass through information on this card

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

```
C1|S7|L1D>show lpt config
Cannot get link pass through information on this card!
C1|S7|L1D>
```

1. Use the **go** command to change from the IONMM to the specific slide-in module. The **go** command format is:
**go [c=CHASSIS] [s=SLOT] [I1ap=PORT] [I2ap=PORT]
[I1p=PORT|I2p=PORT|I3p=PORT|I1d|I2d|I3d]**
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Cannot get OAM configuration on this port!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. The x4120 does not support this function. Use another command or use the go command to switch to a device that supports OAM.
2. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Cannot get port security on this port!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
**go [c=CHASSIS] [s=SLOT] [I1ap=PORT] [I2ap=PORT]
(I1p=PORT|I2p=PORT|I3p=PORT|I1d|I2d|I3d)**
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Command incomplete

This message indicates that not all of the required fields were entered for the CLI command.

1. Verify the command syntax. Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Could not open connection to the host on port 23. Connection failed.

This message indicates that the Telnet server and client are configured for different ports. For Telnet operations the default port is 23.

1. Ensure that the Telnet port is set to 23 for both the server and the client. This will require someone with administrative rights in order to make a change.
2. Add the port number to the Telnet command. Example:
Telnet <ipaddr> <port#>
3. If the problem persists, contact Technical Support.

Error: this command should be executed on a device

This message indicates that the CLI command was entered for a port and it is only applicable for a device.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
**go [c=CHASSIS] [s=SLOT] [I1ap=PORT] [I2ap=PORT]
(I1p=PORT|I2p=PORT|I3p=PORT|I1d|I2d|I3d)**
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support.

Error: this command should be executed on a port

This message indicates that the CLI command was entered for a card and it is only applicable for a port.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
**go [c=CHASSIS] [s=SLOT] [I1ap=PORT] [I2ap=PORT]
(I1p=PORT|I2p=PORT|I3p=PORT|I1d|I2d|I3d)**
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support.

Fail to get MAC address!

This message indicates that communications to the module cannot be established.

1. Verify that the correct hierarchy has been specified in the command (see [“Managing Slide-In and Remote Modules Using CLI Commands”](#) on page 49).
2. For all modules (slide-in and remote) check the following:
 - module is properly seated/connected
 - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.

6. If the problem persists, contact Technical Support.

Fail to get port type!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the **go** command to change location of where the command operates.
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Failed to set DHCP client state!

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

1. Verify the operation in the “[Assigning a Dynamic IP Address](#)” section on page 41.
2. Retry the operation. See the related DHCP command in *the x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Failed to set current time**Failed to set SNTP state!****Failed to set SNTP daylight savings time state!****Failed to set timezone!****Failed to set SNTP server****Failed to set SNTP server!****Failed to set system contact****Failed to set system name****Failed to set system location!**

These messages indicate a problem in the SNTP setup / configuration.

1. Make sure this is the command / function you want.
2. See the commands in *the x4120 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

Error location parameter number!**Error: parameter out of range, chassis-id range is (0 .. 15)!****Error: parameter out of range, slot-id range is (1 .. 32)****Error: parameter out of range, slot-id range is (0 .. 32)****Incomplete location command!**

This message indicates that one or more parameters for the **go** command are missing. The go command was entered to set location parameters, but the module, slot and/or port value(s) were not included in the command string.

The go command can operate on a local or remote card/port, and you must give the last parameter to specify the target is a port or device. For example, the input go c=1 s=14 does not include the port parameter, so the CLI module displays "Incomplete location parameters".

1. Verify the command syntax.
2. Re-enter the go command and be sure to include all of the location parameters (chassis / slot / port) in the format:

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

for a slide in card, or

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

for a standalone card.

3. If the problem persists, contact Technical Support.

Invalid location parameters, cannot find the physical entity!

This message indicates that the system cannot detect the presence of the device or port specified in the **go** command.

1. Verify that the correct hierarchy has been specified in the command (see "[Managing Slide-In and Remote Modules Using CLI Commands](#)" on page 29).
2. For all modules (slide-in and remote) check the following:
 - module is properly seated/connected
 - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation.
6. If the problem persists, contact Technical Support.

Invalid user!

This message indicates that the specified user is not valid.

1. Verify the user.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Login incorrect

This message indicates that either the login or password entered while trying to establish a USB or Telnet connection is incorrect.

1. Verify the login/password.

Note: the login and password are case sensitive. The default login is **ION** and the default password is **private**.

2. Retry the operation.
3. If the problem persists, contact Technical Support.

No DMI support on this port!

This message indicates that you entered a DMI command for a port that does not support DMI.

1. Verify that the port supports DMI. For Lantronix x4120s and SFPs, the model number will have a “D” at the end.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

There is no matched command

This message indicates that there is no such command available on this system.

1. Verify the command syntax.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Unable to open xx. Please check your port settings.

This message indicates that HyperTerminal no longer recognizes which COM port to use for its connection.

1. Check that the USB cable is connected to the management station and the IONMM.
2. Check that the COM port is listed for the device manager on the management station.
 - a) On the desktop, right-click on **My Computer**.
 - b) Select **Manage**.
 - c) Click **Device Manager**.
 - d) In the right panel, expand the list for **COM & LPT**.

3. Is the COM port in the list?

Yes	No
Continue with step 4 .	Restart the management station (PC).

4. In the HyperTerminal window, select **File>Properties**.
5. Check that the correct port is listed in the **Connect using** field.
6. Restart the management station.
7. Reboot the IONMM.
8. If the problem persists, contact Technical Support.

Error, you should first give full location parameters

The location value is incomplete; it is missing the module, slot and/or port value(s). This message can display when a device-level command is entered (e.g., **show lpt config**).

When you change a bigger container, the value of smaller object is cleared. For example, originally the operated object is Chassis=1, slot=4, L1AP=1 L2AP=2 L3D, and then when the command chassis 3 is entered. This automatically sets the value of module, slot and port to 0.

If the value of module, slot and port are not set in later commands, and then you run a device-level command (e.g., **show lpt config**), this error message displays.

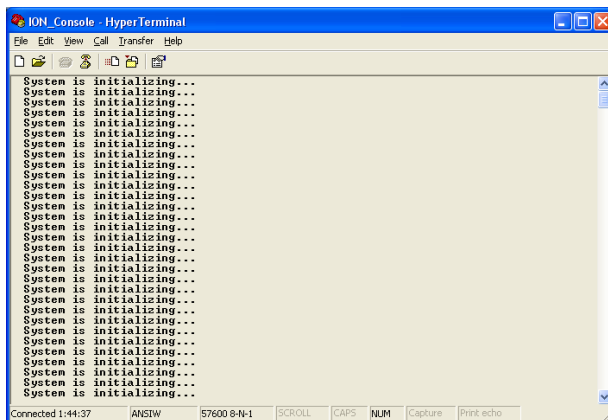
Enter the **go** command and be sure to include all of the location parameters.

```
go [c=<1-16>][s=<1-32>][l1p=<1-15>][l2p=<1-15>][l3p=<1-5>][l4p=<1-15>][l3d=<1-15>][l2d=<1-30>][l1d=<1-30>]
```

for a slide in card.

System is initializing...

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



1. Wait for a few minutes for the message to clear.
2. Cycle power to the IONMM.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

This command is only available on <x222x / x32xx> card!

1. Verify the command entered is the one you want.
2. Verify that the device for the command entered can support the function of the command.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Error: this command should be executed on a port!

1. Verify the command entered is the one you want.
2. Change to the desired port; enter the **go** command with all of the location parameters (chassis / slot / port).
3. Retry the operation from the port (i.e., type **show fwd portlist** and press **Enter**).

Unknown command!

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

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
4. If the problem persists, contact Technical Support. There is no matched command.

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

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the *x4120 CLI Reference Manual*, 33497.
4. If the problem persists, contact Technical Support.

Error location parameter number!

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

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

```
go [c=CHASSIS] [s=SLOT] [1ap=PORT] [2ap=PORT] (1p=PORT|2p=PORT|3p=PORT|1d|2d|3d)
```

Fail to set link pass through state!

You tried to set the LPT state to an unacceptable state. For example, you typed:

```
C1|S3|L1D>set lpt state=enable
```

and then pressed **Enter**.

1. Verify the CLI command syntax.
2. Check the **set lpt monitor-port** and **set selective lpt state** command settings.
3. Enter the **show lpt config** command and in the Link Pass Through configuration, check if the Link pass through state is set to **notSupported** or if the **Remote fault detect state** is set to **notSupported**.

If either is set to **notSupported**, change the setting to enable (e.g., type **set rfd state enable** and press **Enter**).

4. Retry the operation.
5. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.
6. If the problem persists, contact Technical Support.

TFTP transfer failed!

1. The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.
2. Verify the CLI command syntax.
3. Verify the firmware version.
4. Be sure the TFTP server is configured and running.
5. Check that the remotefile is in the proper location (e.g., the file *x222x / x32xx.bin.0.5.4* is at *C:\TFTP-Root*).
6. Retry the operation. See the **tftp upgrade** command in the *x4120 CLI Reference Manual, 33497*.
7. If the problem persists, contact Technical Support.

Fail to transfer the file!

The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., **tftp get** or **tftp put** or **tftp transfer**).

1. Check the command syntax. See “[TFTP Commands](#)” page on page 117.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support.

Fail to transfer the file!

tftp get: set address type failed.

tftp put failed.

The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., **tftp get** or **tftp put** or **tftp transfer**). For example:

```
C1|S4|L1D>tftp get iptype ipv4 ipaddr 192.168.1.30 remotefile xxxx
tftp get: set address type failed.
C1|S4|L1D>tftp put iptype ipv4 ipaddr 192.168.1.30 localfile xxxx
tftp put failed.
C1|S4|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remotefile xxxx
tftp get: set address type failed.
```

1. Check the command syntax. See “[TFTP Commands](#)” page on page 157.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support.

Invalid user!

You entered the command **show ssh public-key user admin**, but specified the wrong user (e.g., you typed **admin** instead of **root**).

1. Retry the operation using the correct user information. See “[Show SSH Public Key of a User](#)” on page 116.
2. If the problem persists, contact Technical Support.

Upgrade is only supported on IONMM card!

You entered a firmware *upgrade* or firmware *update* command from a device other than the IONMM. For example:

```
C1|S3|L1D>show firmware upgrade result
C1|S3|L1D>show firmware-db update result
C1|S3|L1D>show upgrade firmware file
C1|S3|L1D>update firmware-db file cert
C1|S3|L1D>upgrade module
```

1. Make sure of the command you want to enter. See “[Firmware Upgrade Commands](#)” on page 167.
2. Use the **home** command to go to the IONMM device.
3. Re-enter the firmware upgrade command from the IONMM.
4. If the problem persists, contact Technical Support.

DMI is only supported on FIBER port!

You entered the command **show dmi info** on a card that does not support it. For example:

```
C1|S7|L1P1>show dmi info
DMI is only supported on FIBER port!
```

1. Verify if the card supports DMI.
2. Use the **go** command to switch to a different card port supporting Fiber.
3. Verify the command entry. See “[DMI Commands](#)” on page 55.
4. If the problem persists, contact Technical Support.

System is busy, please retry this command later!

You entered a **show** or **set** command, but the command was not accepted by the system. For example:

```
C1|S10|L1D>show https config
System is busy, please retry this command later!
C1|S10|L1D>
```

1. Wait 1-2 minutes and then retry the command.
2. Reboot the system and then retry the command.
3. If the problem persists, contact Technical Support.

Warning: this command will restart system, connection will be lost and please login again!
Warm start failed.

You entered a **reboot** command, but the reboot was unsuccessful.

1. Wait 1-2 minutes and then retry the command.
2. If the problem persists, contact Technical Support.

4 packets transmitted, 0 packets received, 100% packet loss

The attempted ping command failed. For example:

```
PING 192.168.1.10 (192.168.1.10): 56 data bytes
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

1. Verify the IP address.
2. Check the cable connection.
3. Refer to the **Ping** command section.
4. Retry the command.
5. If the problem persists, contact Technical Support.

Ping command can only be used on management card!

The attempted ping command was not accepted by the system. For example:

```
C1|S5|L1D>ping 192.168.1.30
Ping command can only be used on management card!
```

1. Use the **go** command to switch to the IONMM card.
2. Refer to the **Ping** command section.
3. Retry the command.
4. If the problem persists, contact Technical Support.

Only 100M fiber port can set far end fault!

The attempted far end fault command was not accepted by the system. For example:

```
C1|S16|L1P1>set ether fef enable
Only 100M fiber port can set far end fault!
```

1. Use the **go** command to switch to the 100M fiber port.
2. Re-enter the **fef** command.
3. Use an alternate Ethernet test command in place of the **fef** command.
4. If the problem persists, contact Technical Support.

Please reboot the card for the changes to take effect!

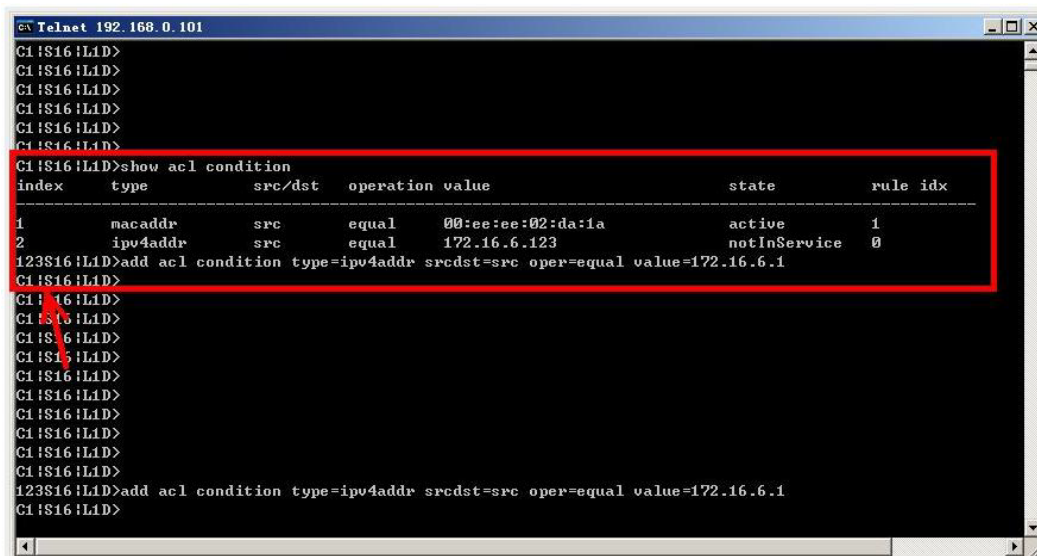
You made a change that requires a system reboot in order for the change to take effect. For example:

```
C1|S5|L1D>set snmp traphost svr 1 type ipv4 addr 192.168.1.30
Please reboot the card for the changes to take effect!
C1|S5|L1D>
```

1. Reboot the card. See the [“Reboot”](#) section.
2. Continue the operation.
3. If a problem persists, contact Technical Support.

Long Command Causes Cursor Wrap to Same Line

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

The screenshot shows a Telnet window titled 'Telnet 192.168.0.101'. The terminal output shows a series of 'C1!S16!L1D>' prompts. A red box highlights the following sequence: 'C1!S16!L1D>show acl condition' followed by a table of ACL conditions. Below the table, the command '123\$16!L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.1' is entered. This command is then repeated, but the second time it wraps back to the beginning of the line, overwriting the previous command text. The table shown in the screenshot is as follows:

index	type	src/dst	operation	value	state	rule idx
1	macaddr	src	equal	00:ee:ee:02:da:1a	active	1
2	ipv4addr	src	equal	172.16.6.123	notInService	0

1. Press the Enter key towards the end of the command string and continue entering command text.
2. Try using HyperTerminal or the Web interface, at least temporarily.
3. Contact Lantronix for more information.

Please change to power supply slot first before showing its configure!

You entered the show power config command from a device other than the power supply. For example:

```
C1|S16|L1D>show power config  
Please change to power supply slot first before showing its configure!  
C1|S16|L1D>
```

1. Make sure this is the command you want.
2. Verify the command syntax.
3. Use the go command to switch to the slot containing the power supply (typically slot 22 and/or 23).
4. Contact Lantronix for more information.

IP management is not supported on this card!**No tdm loopback supported on this card!****Syslog is not supported on this card!****TAOS status setting is not supported on this card!****TNDP is not supported on this card!**

You entered a command for a function that is not supported on the x4120. For example:

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

1. Try another command on the x4120.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support.

Cannot set if this port can be managed by CPU on this card!**Cannot set USB port state on this card!****tftp get: set address type failed.**

You entered a tftp command, but the address entered was not accepted.

```
C1|S15|L1D>tftp get iptype ipv4 ipaddr 192.168.1.30 remotefile x4120_1.0.4_AP  
tftp get: set address type failed.  
C1|S15|L1D>
```

1. Make sure the tftp server address is valid.
2. Verify that the TFTP Server is running and properly configured.
3. Try entering the tftp command again.
4. If the problem persists, contact Technical Support.

At one time we can only backup at most 10 cards!

At one time we can only restore at most 10 cards!

Backup finished

Error: this command should be executed on a device!

Error: this command should be executed on IONMM or a standalone SIC!

Fail to set card entity index!

Processing...

The MAX provision configure file name is 64!

The specified module does not exist!

You entered a “**backup**” or “**restore**” command to do a backup or restore function, but a problem was encountered or the process is not yet finished. You entered a “**prov**” command to do a backup or restore function, but a problem was encountered or the process is not yet finished.

1. Wait a few moments for the command to complete and the *Restore finished* or *Backup finished* message to display.
2. Retry the backup or restore operation with 10 or fewer devices listed.
3. Use the **go** command to switch to a device that supports this feature (IONMM or a standalone SIC).
4. Enter a config filename with less than 64 characters. See the “[Configuring Backup / Restore](#)” section on page [103](#).
5. If the problem persists, contact Technical Support.

Cannot proceed because some other TFTP operation is currently in progress!

Please input config file name!

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

TFTP Server Address is empty or invalid!

The firmware has been successfully upgraded and the system will be rebooted soon

The specified firmware on the TFTP server will be upgraded to the current module, operation is currently in progress!

The sys.log file will be transferred to the TFTP server, are you sure to proceed?

You tried a TFTP transfer operation, but the operation failed or is still in process.

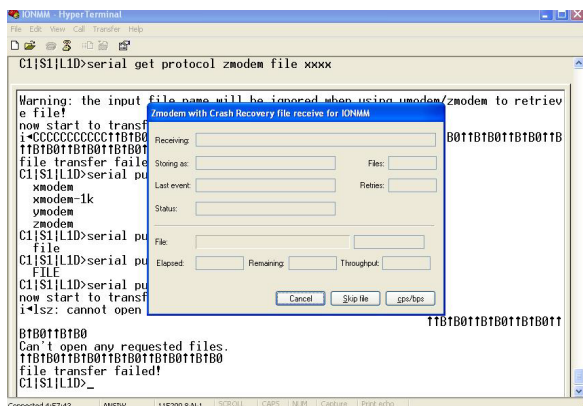
1. Wait for the “*operation is currently in progress!*” message to clear.
2. If an entry was requested in the message, enter the required information (e.g., valid TFTP Server address, or config file name).
3. Verify that this is the operation you want (e.g., click **OK** at the “*are you sure to proceed?*” message).
4. Verify the related command syntax in the applicable section of this manual (e.g., Syslog, or TFTP Upgrade section).
5. Retry the operation.
6. If the problem persists, contact Technical Support. .

Can't open any requested files.
cannot open /tftpboot/xxxx: No such file or directory
now start to transfer the file ...
file transfer failed!
file transfer succeeded!
now start to upgrade the system ...
/usr/local/bin/flash_firmware /tftpboot/
upgrade failed!
upgrade failed due to wrong file %s!
upgrade failed when programming the flash!
upgrade succeeded, system will be rebooted ...
Usage: serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem) file=FILE
Warning: the input file name will be ignored when using ymodem/zmodem to retrieve file!
Warning: xmodem/xmodem-1k protocol might append some garbage at the end of the file!
Wrong parameter number!

You entered a Serial File Transfer command, but the operation failed.

1. Verify that this is the operation you want.
2. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
3. If the problem persists, contact Technical Support.

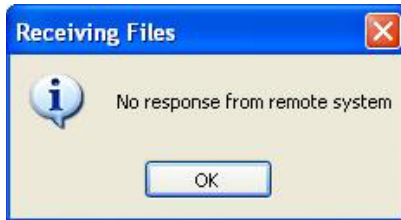
File Transfer Failed - ZModem Crash Recovery dialog box:



You entered a Serial File Transfer command, but the operation failed.

1. Either enter the requested information and click **cps/bps**, or click **Skip file**, or click **Cancel**.
2. See the HyperTerminal Helps or the [Hilgraeve web site](#) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Technical Support.

Receiving Files - No response from remote system



You entered a Serial File Transfer command, but the ZModem file transfer failed.

1. Click the **OK** button to clear the message dialog box.
2. See the HyperTerminal Helps or the [Hilgraeve web site](#) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Technical Support.

Cannot find software version of this card!

The ION card's firmware version must be newer than a specified version, otherwise this message is returned. You used the go command to switch to another card, but the system checked its version and decided that the new CLI can not be run on this card at this firmware version.

1. Check the card's current firmware version.
2. Upgrade the card firmware. See "[Upgrade the IONMM and/or x4120 Firmware](#)" on page 107.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Software version of this card is too old, please upgrade it!

The ION card's firmware version was checked and found to be too old to support this newer CLI command.

1. Upgrade the card firmware. See "[Upgrade the IONMM and/or x4120 Firmware](#)" on page 107.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

**This command is only valid on an IONMM!
Cannot show slot info on this card!**

You entered a "**show slot info**" command on an ION card other than an IONMM card.

1. Enter another (supported) show command on this card, or use the "**go**" command to switch to the IONMM.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

**ERROR Software version of this card ("cardVersion") is not supported, please upgrade to the same version as the IONMM
Getting card version failed
The failure get template config handler was called.**

You attempted a function that is not supported by this version of firmware.

1. Enter another (supported) function at this card's firmware version, or use the "**go**" command to switch to another card.
2. Upgrade to a newer firmware version. See "[TFTP Transfer / Upgrade Commands](#)" on page 204 or "[Upgrade / Update Firmware Commands](#)" on page 207.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

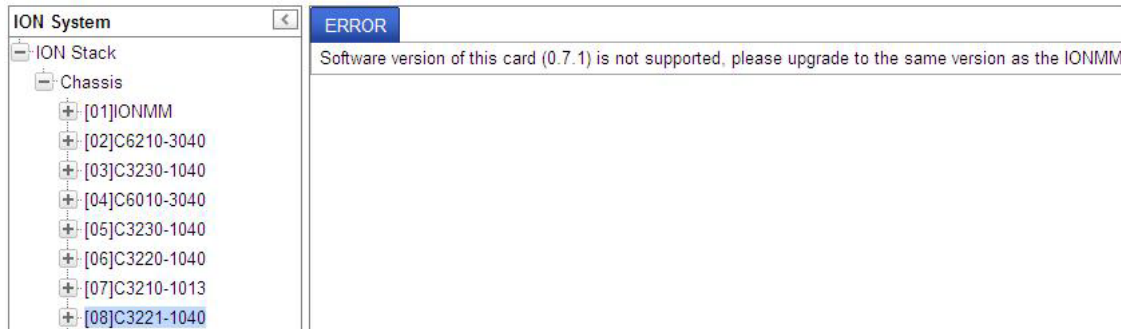
Online Help is not available until a specific configuration is entered.



You clicked on **Online Help** from the **Help** dropdown without first selecting a device.

1. Click the **OK** button to close the webpage message.
2. Select an ION device.
3. Click on **Help > Online Help** again.

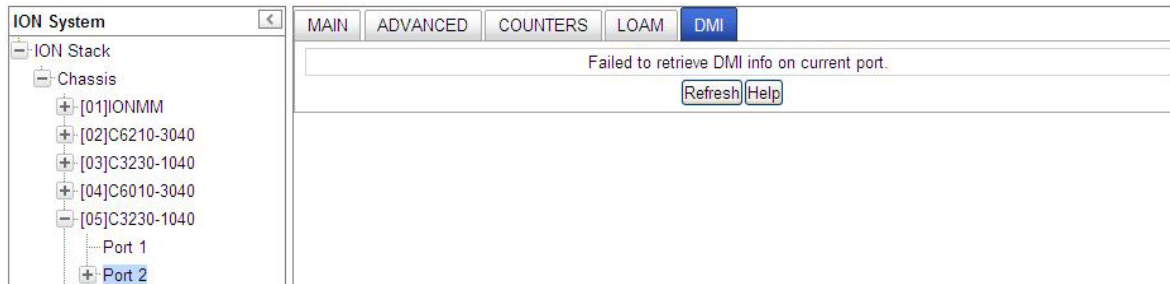
ERROR: Software version of this card (0.7.1) is not supported, please upgrade to the same version as the IONMM



You selected a device in the tree, but its firmware version is not compatible with the IONMM.

1. Select the IONMM device.
2. Select the UPGRADE tab.
3. Perform a firmware upgrade to this card (and others that may have outdated firmware). See the [Upgrade](#) section on page 347.
4. If a problem persists, contact Technical Support.

Failed to retrieve DMI info on current port



You selected **C3230 > Port 2 > DMI** but the DMI information does not display.

1. Click **Refresh**.
2. Expand and contract the tree.
3. If a problem persists, contact Technical Support.

Current power status of this slot is off, please turn it on before you reset it!

The reset function only works when the slot power is in the On position for the unit to reboot/reset.

1. At **Chassis > MAIN > Chassis Members** click the "On" button in the **Power Status** column of the device before you click the "Reset" button.
2. If a problem persists, contact Technical Support.

Setting the VLANID failed with an SNMP operation error message:

Setting values failed (snmp operation error) or
Adding VLAN failed (snmp operation error)

You tried to add or edit a VLAN ID but the effort failed.

1. The card must be in "Network" mode (at Port 1 > Advanced > Frame Tag Mode) to set the VLAN ID. If it is not set to "Network", an SNMP error will occur. Before adding the ports for Management VLAN, set the Frame Tag Mode of that port to "Network". When Provider tagging is required for that port, then set the Frame Tag Mode to "Provider". A port with the Frame Tag Mode set to the default setting "Customer" cannot be added to Member Ports for Management VLAN.
2. If a problem persists, contact Technical Support.

Cannot clear loopback counters on this card!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set autocross on this card!
Cannot set auto negotiation state on this port!
Cannot set Ethernet port speed for this card!
Cannot set Ether port duplex mode on this card!
Cannot set far end fault on this card!
Cannot set filter unknown dest multicast frames on this port!
Cannot set filter unknown dest unicast frames on this port!
Cannot set pause on this port!
Cannot set source address lock action on this port!
Cannot get port security configuration on this port!
Fail to get MAC control frames statistics!
Cannot show forwarding port list on this card!
Cannot show slot info on this card!
Cannot show USB port state on this card!
Cannot show USB port configure on this card!
Cannot show TP port cable length on this card!
Cannot set management VLAN on this card!
Cannot set PHY mode on this port!
Cannot clear counters on this port!
Cannot reset all ports' counters on this cards!
Cannot set remote fault detect state on this card!

You entered a command for a function not supported on the card.

1. Verify the command entry.
2. Verify if the card supports the desired function.
3. Use the **go** command to switch to a different card port supporting VLAN.
4. Verify the command entry.
5. If the problem persists, contact Technical Support.

Fail to set aging time!
Get aging time failed!
CLI command remove fwddb all failed
Redundancy is not supported on this card!
Fail to set SSH server state!
Fail to set management VLAN id!
Fail to set management VLAN state!
Cannot show port QoS configuration in this card!
Cannot set tag type for priority in this card!
Cannot set default priority in this card!
Cannot set IEEE tag for priority in this card!
Cannot set VLAN network tagging on this port!
Cannot show system information on this card!
Cannot create VLAN database on this card!
Cannot remove vlan on this card!
Cannot remove forward database rows on this card!
Cannot set bandwidth alloc type on this card!
Cannot set ingress and egress rate on this card!
The specified conn-port does not exist!
The specified monitor-port does not exist!
Cannot show cable length for fiber port!
Get DMI identifier no such object.
Get SNMP version no such object.
Fail to get cable length
Can not set speed on this port!
Fail to set port advertisement capability!
Fail to get system name!
Set system name timeout.
Get HTTPS state no such object.
Get management VLAN state no such object.
IP management state no such object.
L2CP is not supported on this card!
Link OAM is not supported on this card!
No Time-domain reflectometer support on this card!

You entered a command for a function not supported on the card.

6. Verify the command entry.
7. Verify if the card supports the desired function.
8. Use the **go** command to switch to a different card port supporting VLAN.
9. Verify the command entry.
10. If the problem persists, contact Technical Support.

Web Interface Messages

IMPORTANT

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

Cannot Ping IONMM Device

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails. The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic. The PC can then ping to the S2220-1013 again, and the WEB UI can be managed again.
4. 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. The reason is enabling the Management VLAN function gives management control to the Management VLAN that you enabled.
2. 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.
3. 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](#)” on page 120 for valid input information.
2. Retry the operation with a valid firmware file name (e.g., *IONMM.bin.0.5.4*, or *x222x / x32xx.bin.0.5.4*).
3. If the problem persists, contact Technical Support.

Invalid input found!

This message indicates that you entered a parameter outside the valid range (e.g., VLAN ID = 0).

1. Verify the parameter value to be entered; check the online Help for valid input information.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid password!

This message indicates that the password entered during sign on is not valid.

1. Sign in using the correct password. The default password is **private**.

Note: the password is case sensitive.

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 x4120 supports DMI.
2. See "[DMI \(Diagnostic Maintenance Interface\) Parameters](#)" on page 118 for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support. Admin Status: Down (or Testing)

In the device's port, at the MAIN tab in the Port Configuration section, the Admin Status field displays "Down". Typically, if 'Admin Status' is Down, then 'Link Status' is also Down.

The status here is the desired state of the interface. The "Testing" status indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with 'Admin Status' in the Down state. As a result of either explicit management action or per configuration information retained by the managed system, 'Admin Status' is then changed to either the Up or Testing states, or remains in the Down state.

1. Verify the initialization process; see "[Section 2: Installation and System Setup](#)" on page 40.
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization to take place.
4. If the problem persists, contact Technical Support.

Link Status: Down (or Testing or Dormant, or NotPresent)

This is the current operational state of the interface.

The 'Link Status' Testing state indicates that no operational packets can be passed.

If 'Admin Status' is Down then 'Link Status' likely will be Down.

If 'Admin Status' is changed to Up, then 'Link Status' should change to Up if the interface is ready to transmit and receive network traffic.

'Link Status' should change to Dormant if the interface is waiting for external actions (such as a serial line waiting for an incoming connection);

'Link Status' should remain in the Down state if and only if there is a fault that prevents it from going to the Up state;

'Link Status' should remain in the NotPresent state if the interface has missing (typically, hardware) components.

Link Status: Down: The ION system interface is not ready to transmit and receive network traffic due a fault.

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see “[Section 2: Installation and System Setup](#)” on page 40.
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization 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](#)” on page 40.
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 (http server error)*

This message indicates a configuration entry error (e.g., https).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See “[Configuring HTTPS](#)” on page 208.
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. Retry the operation. See “[Configuring SNMP](#)” on page 226.
3. If the problem persists, contact Technical Support.

Message: *TFTP file transferring failed!*

This message indicates that a TFTP operation could not be completed.

TFTP for Backup download operation:

1. Verify that:
 - a. The correct module(s) has been selected.
 - b. The IP address of the TFTP server is correct.
 - c. The TFTP server is online and available.
2. Perform a backup of the module(s) for which the download operation was intended. Make sure that the status of the backup operation for each module is “*Success*”.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

TFTP for Restore upload operation:

1. Check:
 - The IP address of the TFTP server is correct.
 - The TFTP server is online and available.
 - The file to be uploaded is in the default directory on the server.
 - The correct module(s) has been selected.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message: *TFTP operation failed!*

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

1. Check:
 - The IP address of the TFTP server is correct.
 - The TFTP server is online and available.
 - The correct file name (**db.zip** in Windows XP or just “**db**” in Windows 7) is specified.
 - The **db.zip** (or **db**) file is in the default directory on the TFTP server.
2. If the problem persists, contact Technical Support.

Message: *There is a problem with this website's security certificate.*

This message indicates that the security certificate presented by this website was changed.

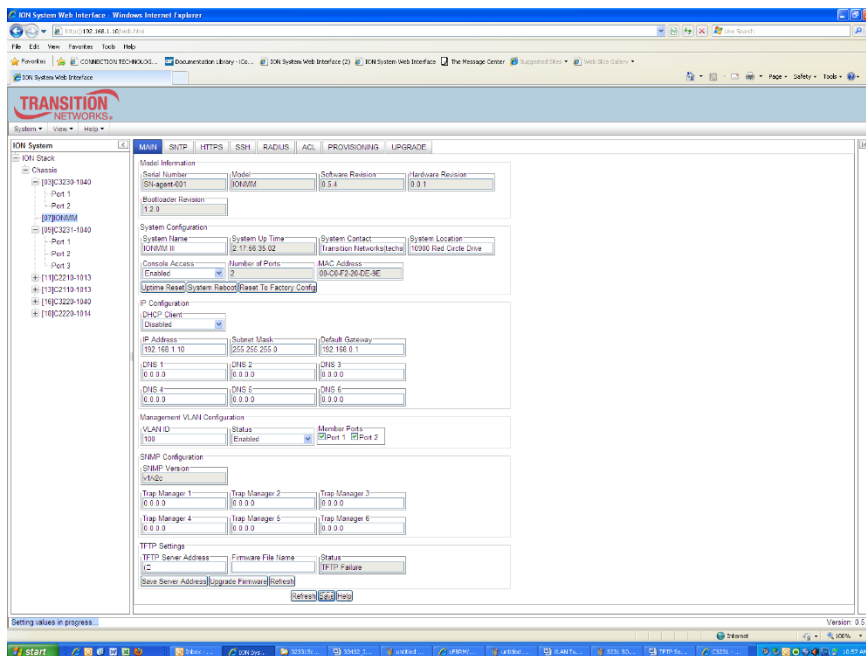
1. Click the [Continue to this website...](#) selection.
2. See the “[Configuring HTTPS](#)” section on page [192](#).

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

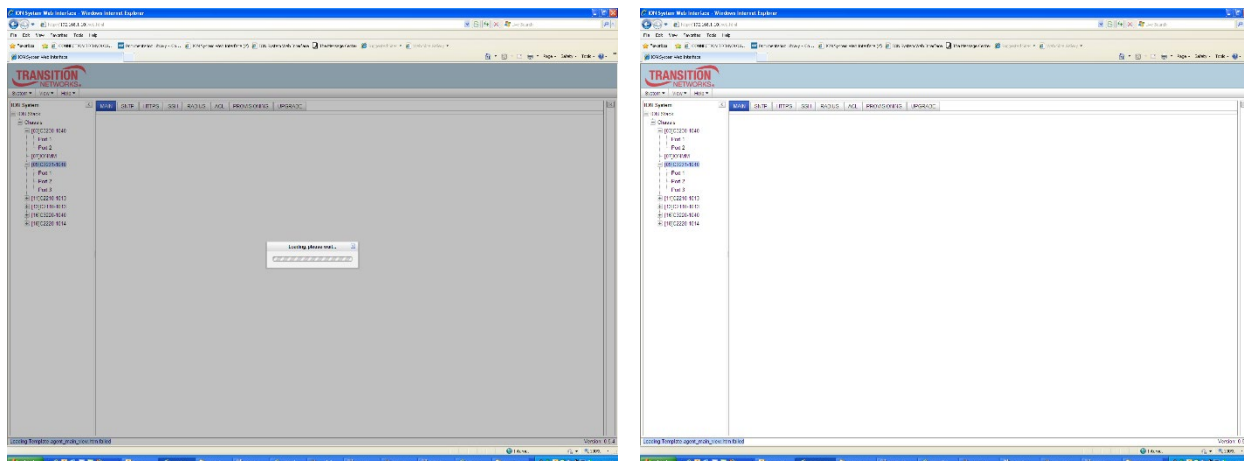
Message: "Setting values in progress ..." displays continuously

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 x4120 models support DMI. Lantronix x4120s that support DMI have a “D” at the end of the model number. If you click the DMI tab on a x4120 model that does not support DMI, the message “The DMI feature is not supported on current port.”

The DMI (Diagnostic Maintenance Interface) function displays x4120 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.

Recovery: 1. Verify that the device and port support DMI. See “[DMI \(Diagnostic Maintenance Interface\) Parameters](#)” on page 248 for more information.

Message: *Loading Template agent_main_view.htm failed*

Message: *Loading htm files failed*

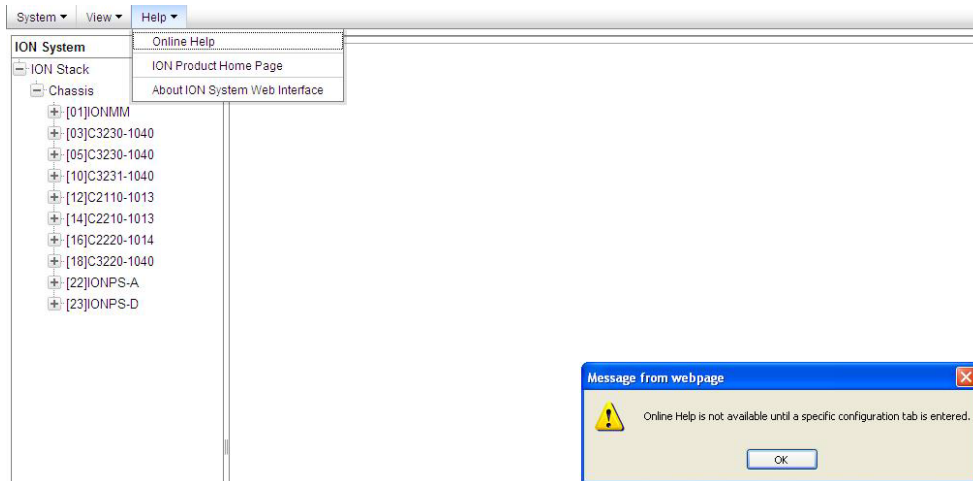
Meaning: The status displays at the lower left corner during Port 1 page loading.

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. 2. If the problem persists, contact Technical Support.

Message: *Online Help is not available until a specific configuration tab is entered.*



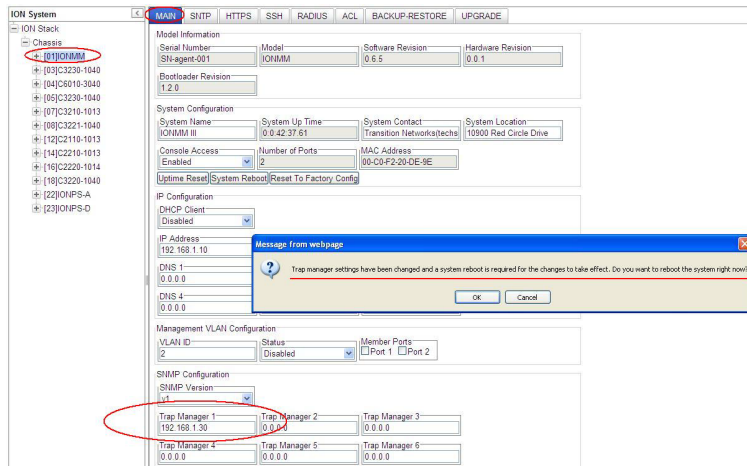
Meaning: You clicked on **Online Help** from the **Help** dropdown without first selecting a device.



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?*

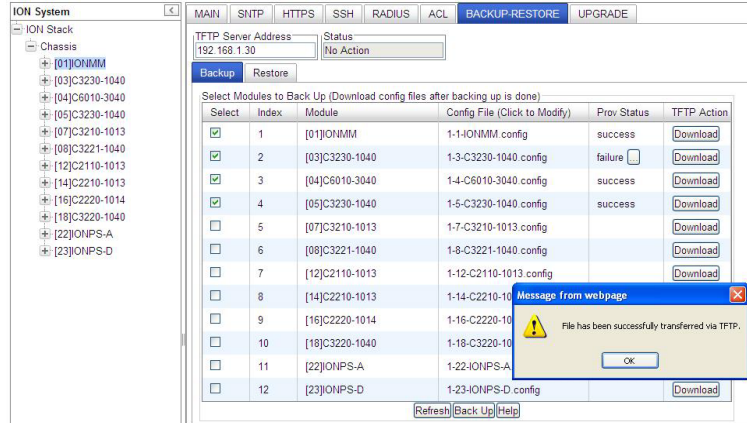


Meaning: Information only. At **IONMM > MAIN > SNMP Configuration > Trap Manager x** you entered an IP address for a trap server.

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 [...].

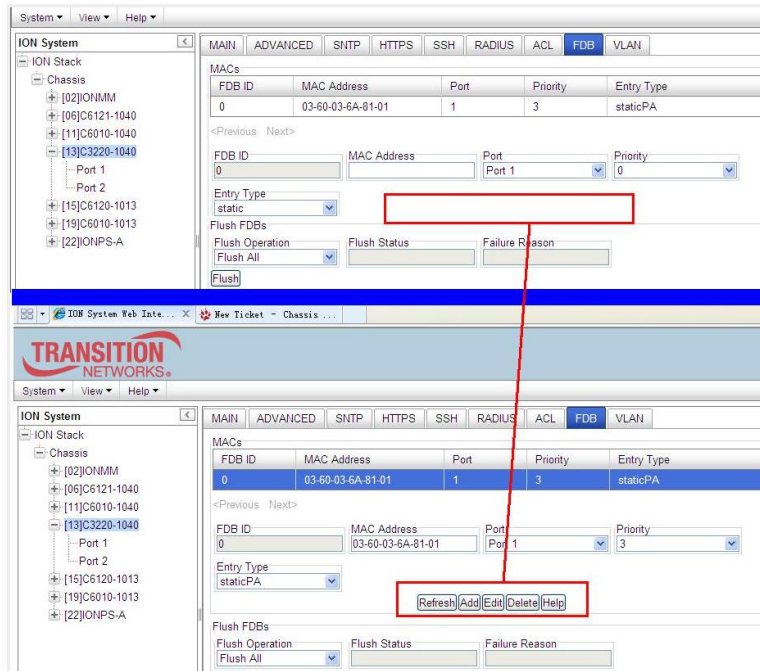


Meaning: At **IONMM > BACKUP-RESTORE > Backup** you selected a module to back up, the “successful transfer” message displays, but the Prov. Status column displays failure [...].

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.

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.
4. Click one existing MAC address in the MAC address list.

Website displays incorrectly in Internet Explorer 8 or 9

Websites that were designed for earlier versions of Internet Explorer might not display correctly in the current version. However, you can often improve how a website will look in Internet Explorer by using the new 'Compatibility View' feature. When you turn on Compatibility View, the webpage displayed (and any other webpages within the website's domain) will display as if you were using an earlier version of Internet Explorer.

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



If Internet Explorer recognizes a webpage that is not compatible, the **Compatibility View** button displays on the Address bar. To turn Compatibility View on, click the **Compatibility View** button. From now on, whenever you visit this website, it will be displayed in Compatibility View. However, if the website receives updates to display correctly in the current version of Internet Explorer, Compatibility View will automatically turn off. Note that not all website display problems are caused by browser incompatibility. Interrupted Internet connections, heavy traffic, or website bugs can also affect how a webpage is displayed. To go back to browsing with Internet Explorer 8 on that site, click the **Compatibility View** button again.

4. Check your ION firmware version and upgrade to the latest if outdated. See the "Upgrade" section on page 266.
5. Check the Microsoft Support Online website <http://support.microsoft.com/ph/807/en-us/#tab0> for more information.
6. See also: <http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx>
<http://support.microsoft.com/kb/960321>
<http://blogs.msdn.com/b/ie/archive/2008/08/27/introducing-compatibility-view.aspx>
7. In IE9, click the **Compatibility View** toolbar button on the Address bar to display the website as if you were using an earlier version of Internet Explorer. See the Microsoft Support website Article ID: 956197 at <http://support.microsoft.com/kb/956197>.

Script error message received.

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

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

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

Done, but with errors on page.

The screenshot shows a network management interface for 'S3240 System'. The 'FDB' tab is selected, displaying a table of MACs. Below the table are input fields for VLAN ID, MAC Address, Port, and Priority, along with an 'Entry Type' dropdown menu. A Windows Internet Explorer error dialog box is overlaid on the interface, displaying a warning icon and the text: 'Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer might become unresponsive.' The dialog box has 'Yes' and 'No' buttons.

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

1. Click the **Yes** button to stop the script.
2. Click **Show Details** to display error details.
3. Disable script debugging.
4. Test a Web page from another user account, another browser, and another computer.
5. Verify that Active Scripting, ActiveX, and Java are not being blocked by Internet Explorer.
6. Remove all the temporary Internet-related files.
7. Install the latest Internet Explorer service pack and software updates.
8. For more advanced troubleshooting, see the Microsoft Support Article ID 308260 at <http://support.microsoft.com/kb/308260>.

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:

Type	Date	Time	Source	Category	Event	User	Computer	
Information	6/25/2010	10:34:34 AM	Service Control Manager	None	7036	N/A	SCHIERMAN	
Information	6/25/2010	10:32:35 AM	Service Control Manager	None	7036	N/A	SCHIERMAN	
Information	6/25/2010	10:32:35 AM	Service Control Manager	None	7035	jeffs	SCHIERMAN	
Information	6/25/2010	7:37:19 AM	Service Control Manager	None	7036	N/A	SCHIERMAN	
Information	6/25/2010	7:37:12 AM	Service Control Manager	None	7036	N/A	SCHIERMAN	
Information	6/25/2010	7:37:12 AM	Service Control Manager	None	7035	SYSTEM	SCHIERMAN	
Error	6/24/2010	10:27:33 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/24/2010	10:27:33 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/24/2010	4:12:51 PM	windows	Update Agent	Software Sync	16	N/A	SCHIERMAN
Information	6/24/2010	7:40:55 AM	Service Control Manager	None	7036	N/A	SCHIERMAN	
Information	6/24/2010	7:40:49 AM	Service Control Manager	None	7036	N/A	SCHIERMAN	
Information	6/24/2010	7:40:49 AM	Service Control Manager	None	7035	SYSTEM	SCHIERMAN	
Error	6/24/2010	6:27:31 AM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/24/2010	6:27:31 AM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	10:27:29 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	10:27:29 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	6:27:28 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	6:27:28 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	4:27:27 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	4:27:27 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	3:27:27 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	3:27:27 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	2:57:26 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	2:57:26 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	2:42:26 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	2:42:26 PM	w32time	None	14	N/A	SCHIERMAN	
Error	6/23/2010	2:42:11 PM	w32time	None	29	N/A	SCHIERMAN	
Warning	6/23/2010	2:42:11 PM	w32time	None	14	N/A	SCHIERMAN	
Information	6/23/2010	2:42:01 PM	Tcpip	None	4201	N/A	SCHIERMAN	
Information	6/23/2010	2:41:56 PM	Browser	None	8033	N/A	SCHIERMAN	

Message: Information 6/25/2010 7:37:12AM ServiceControlManager 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

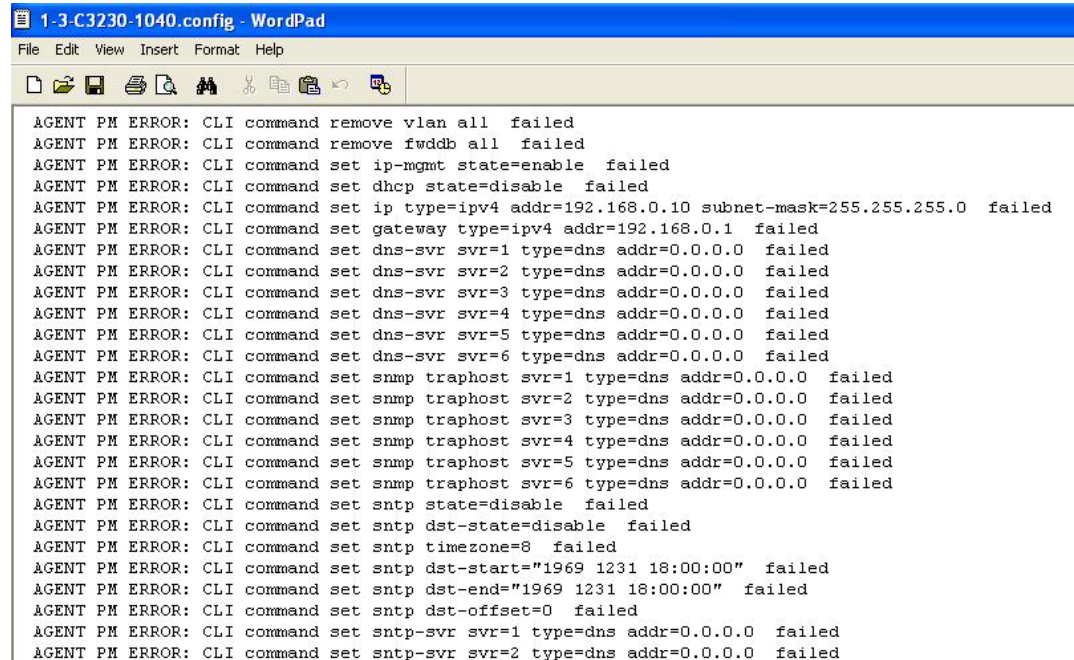
Meaning: Warning level message regarding W32Time.

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.

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



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

These messages show a translation of failed web interface functions that were attempted, translated into 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-C3220-1048_20180608.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-C3220-1048_20160608.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 *x4120 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 *x4120 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 *x4120 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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set snmp traphost svr=1 type=dns addr=0.0.0.0 failed

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

Message: set snmp state=disable failed

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

Message: set snmp dst-state=disable failed

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

Message: set snmp 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 snmp 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 snmp dst-offset=0 failed

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

Message: set snmp-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

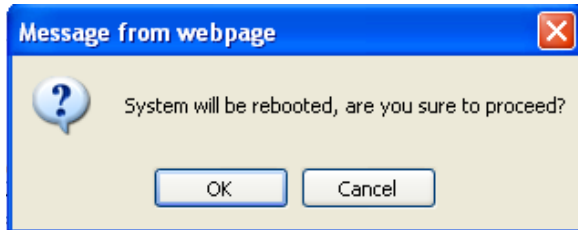
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support.

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.

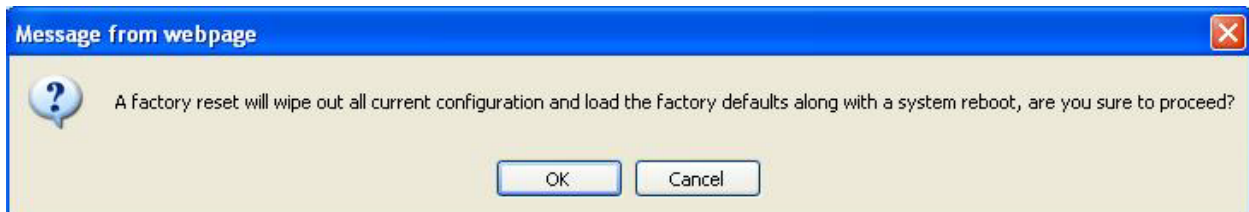
See “[Menu System Descriptions](#)” on page 15.

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



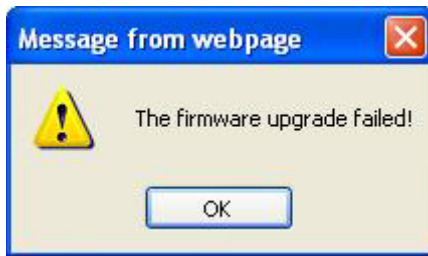
Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

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



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

Message: *The firmware upgrade failed!*



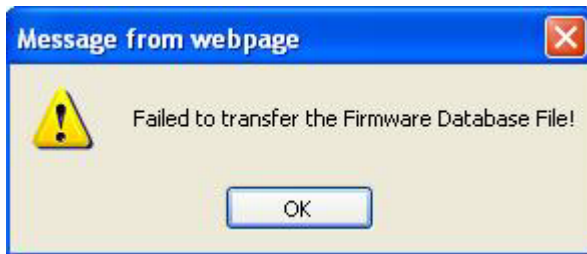
The **MAIN** tab > **TFTP Settings** section **Status** area displays "*TFTP Failure*".

Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the "[Upgrade the IONMM and/or x4120 Firmware](#)" section on page 109.

Recovery:

1. Click **OK** to clear the webpage message.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Lantronix web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.0.5.3**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.0.5.3 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Make sure that the Management VLAN function is disabled.
8. Reset the IONMM card. The **TFTP Settings** section **Status** area should display "*Success*" when done.
9. If the problem persists, contact Technical Support.

Message: Failed to Transfer the Firmware Database File!

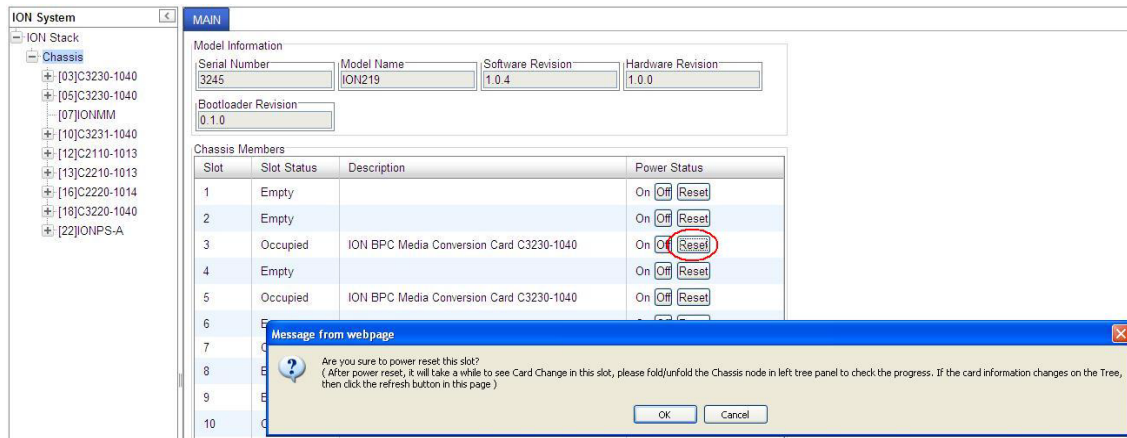


Meaning: A problem was detected while performing a Firmware Upgrade from the x4120 **MAIN** tab > **TFTP Settings** section or from the IONMM **UPGRADE** tab. See [“Upgrade the IONMM and/or x4120 Firmware”](#) on page 109.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Lantronix web site.
4. [Make sure the TFTP server is running and correctly configured.](#)
5. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
6. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.0.5.3**). [Include the filename extension if you have not done so.](#)
7. Check the log status in the TFTP Server package; when successful, it should show something like *“Sent IONMM.bin.0.5.3 to (192.168.1.30), 9876543 bytes”*. The **TFTP Settings** section **Status** area should display *“Success”* when done.
8. Reset the IONMM card. The **TFTP Settings** section **Status** area should display *“Success”* when done.
9. If the problem persists, contact Technical Support.

Message: *Are you sure to power reset this slot? (After power reset, it will take a while to see card change in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page.)*

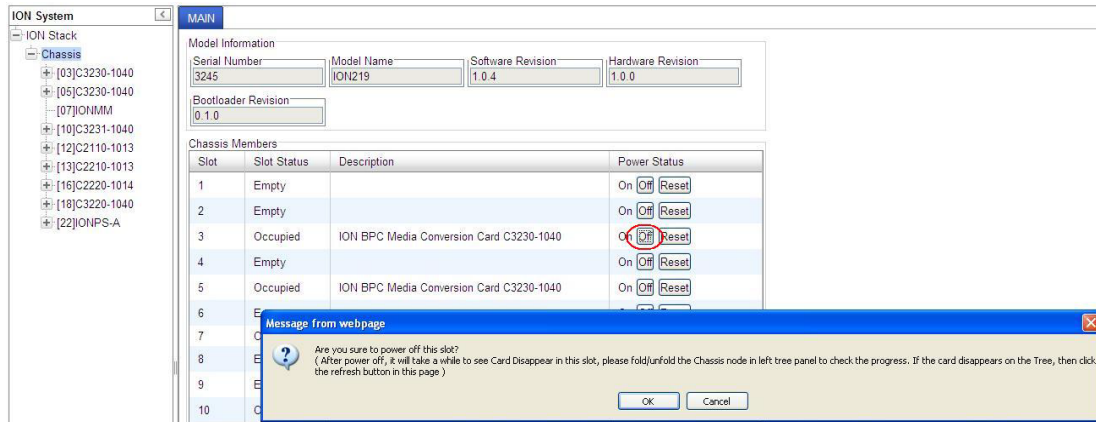


Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Reset** button for a particular slot.

Recovery:

1. If you are not sure that you want to reset this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to reset this chassis, click the **OK** button to clear the message and reset power to the slot.
3. At the **Chassis > MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See “[Menu System Descriptions](#)” on page 15.
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.

1. **Recovery:** 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](#)” on page 415.
6. If the problem persists, contact Technical Support.

Message: *The Connection was Reset*

The connection was reset

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


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

[Try Again](#)

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

Recovery:

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

Message: *This Connection is Untrusted*

This Connection is Untrusted

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

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

What Should I Do?

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

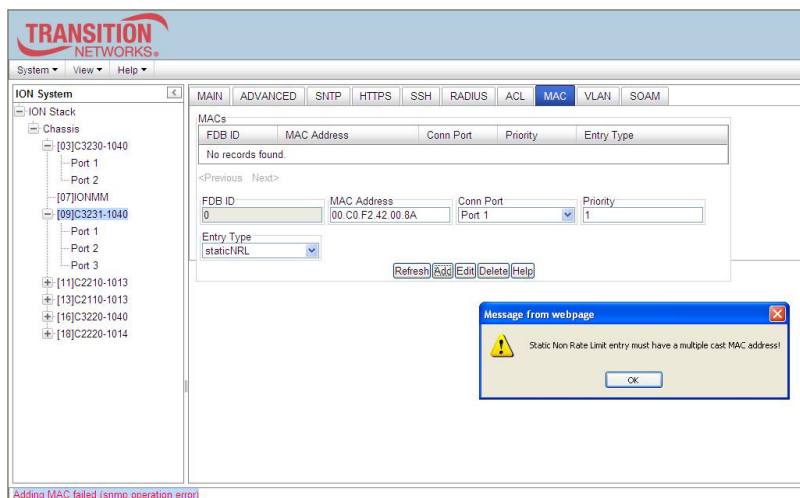
[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

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: *Static Non Rate Limit entry must have a multiple cast MAC address!*

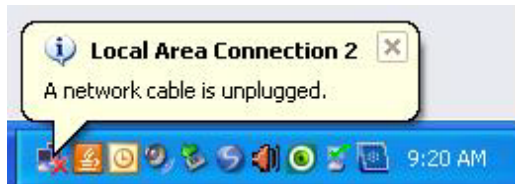


Meaning: When setting up MAC filtering, you entered a unicast MAC address and selected a Static NRL (Non Rate Limit) Entry Type.

Recovery:

1. Click **OK** to clear the message.
2. Either enter a multicast MAC Address, or select another Entry Type.

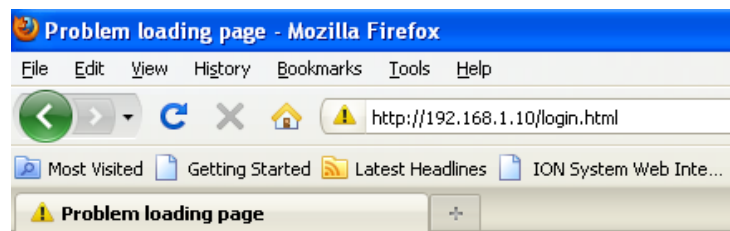
Message: *Local Area Connection x – A network cable is unplugged*



Meaning: You unplugged the USB cable at the x4120 or IONMM, or the x4120 or IONMM was unplugged from the ION chassis, or you pressed the Reset button on the IONMM.

Recovery:

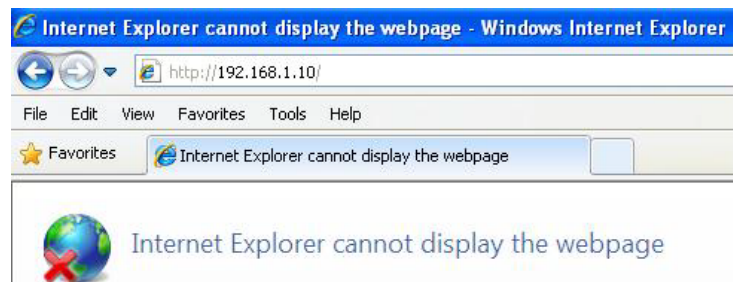
1. If you pressed the Reset button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM's USB-DEVICE connector, or plug the USB cable back into the x4120's USB connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support.

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](#)” on page 72.
2. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)” on page 59.
3. Verify x4120 access. See “[Accessing the x4120](#)” on page 60.
4. Verify the IP address setting. See “[Setting the IP Addressing](#)” on page 89.
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.

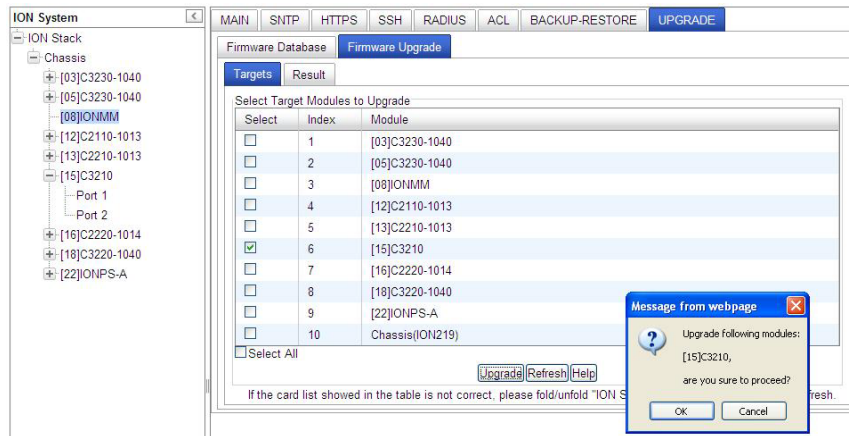
Message: *Internet Explorer cannot display webpage*

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](#)” on page 42.
2. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)” on page 49.
3. Verify NID access. See “[Accessing the x4120](#)” on page 50.
4. Verify the IP address setting. See “[Setting the IP Addressing](#)” on page 69.
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: Upgrade following modules: [15]x4120, are you sure to proceed?



Meaning: Verification message that you indeed want to upgrade the x4120 firmware.

Recovery:

1. If you are not sure you want to upgrade the x4120 firmware, click **Cancel** and continue operation.
2. If you are sure you want to upgrade the x4120 firmware, click **OK**. The upgrade process will continue.

See “[Upgrade the IONMM and/or x4120 Firmware](#)” in the IONMM User Guide.

DMI (Diagnostic Maintenance Interface)

The DMI (Diagnostic Maintenance Interface) function displays x4120 diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths.

DMI Config – CLI Method

1. Access the x4120 through either a USB connection or a Telnet session.
2. Set the Diagnostic Monitoring Interface receive preset power level. Type: **set dmi rx-power-preset-level=xx** where xx is a preset level for Rx Power on the Fiber port, in the range of 1 to 10.
3. Press **Enter**. For example: **set dmi preset-power-level=10**.
4. Display the DMI information. Type: **show dmi info** and press **Enter**. For example:

```
Agent III C1|S17|L1P2>set dmi preset-power-level=10
Agent III C1|S17|L1P2>show dmi info
Diagnostic monitoring interface information:
-----
DMI connector type:                LC
DMI indentifier:                   SFP
DMI Nominal bit rate:              10500*Mbps
DMI 9/125u Singlemode Fiber (m):   N/A
DMI 50/125u Multimode Fiber (m):   80*m
DMI 62.5/125u Multimode Fiber (m): 3*10m
Copper(m):                         N/A
DMI fiber interface wavelength:    850*nm
DMI temperature:                   42.0*C
DMI temperature:                   107.6*F
DMI temperature alarm:             normal
DMI transmit bias current:         6240*uA
DMI transmit bais alarm:          normal
DMI Transmit power:               589*uW
DMI Transmit power:               -2.299*dBM
DMI Transmit power alarm:         normal
DMI Receive power:                573*uW
DMI Receive power:                -2.418*dBM
DMI Receive power alarm:          normal
DMI Receive power intrusion threshold: 0*uW
Agent III C1|S17|L1P2>
```

The DMI tab parameters are described in the table below.

DMI Config – Web Method

1. Access the x4120 through the Web interface.
2. Select the desired device and port.
3. Select the **DMI** tab.

The screenshot shows the ION System web interface. On the left is a tree view of the ION Stack, including Chassis, IONMM, and various ports. The main area has two tabs: MAIN and DMI. The DMI tab is selected and displays the following configuration fields:

Interface Characteristics		
DMI ID	Connector Type	Nominal Bit Rate (Mbps)
SFP	LC	10500
Fiber Interface Wavelength (nm)		
850		
Diagnostic Monitoring		
Receive Power (µW)	Receive Power (dBm)	Receive Power Alarm
568	-2.457	Normal
Rx Power Intrusion Threshold (µW)		
0		
Temperature (°C)	Temperature (°F)	Temperature Alarm
41.2	106.2	Normal
Transmit Bias Current (µA)	Transmit Bias Alarm	
6288	Normal	
Transmit Power (µW)	Transmit Power (dBm)	Transmit Power Alarm
587	-2.314	Normal
Supported Media Length		
9/125u Singlemode Fiber (m)	50/125u Multimode Fiber (m)	62.5/125u Multimode Fiber (m)
N/A	80	30
Copper (m)		
N/A		

At the bottom of the DMI tab are buttons for Refresh, Save, and Help.

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

4. 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 6: 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: 00h Unknown or unspecified 01h GBIC 02h Module/connector soldered to motherboard 03h SFP 04-7Fh Reserved 80-FFh Vendor specific
Connector Type	LC, MT-RJ LC, SC, ST, RJ-45, VF-45, or unknown	The external optical or electrical cable connector provided as the interface. * MT-RJ: Media Termination - Recommended Jack for Duplex multimode connections. * LC: Lucent Connector or Local Connector for High-density connections, SFP transceivers. * SC: Subscriber Connector for Datacomm and Telecomm. * ST: BFOC Straight Tip / Bayonet Fiber Optic Connector for Multimode - rarely Singlemode (APC not possible). * VF-45: Snap connector for Datacom uses. See 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, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for receive power on local fiber.
Rx Power Intrusion Threshold (uW)	0-10	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, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for temperature of fiber transceiver. <i>An ionDMITemperatureEvt</i> event is sent when there is a warning or alarm on DMI temperature
Transmit Bias Current (uA)	(measured current)	Transmit bias current on local fiber interface, in uA (microamperes). The sample screen above shows 14768 uA (microamps).
Transmit Bias Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for transmit bias current on local fiber interface.
Transmit Power (uW)	(measured power)	Transmit power on local fiber measured in microwatts. The sample screen above shows 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. The sample screen above shows -6.126 dBm.
Transmit Power Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for transmit power on local fiber.
Supported Media Length	9/125u Single-mode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). The sample screen above shows N/A, indicating the media is not applicable.
Supported Media Length	50/125u Multimode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 500 meters as the supported media length.
Supported Media Length	62.5/125u MM Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 300 meters as the supported media length.
Supported Media Length	Copper (m)	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters. The sample screen above shows N/A, indicating the media is not applicable.

Third Party Troubleshooting Tools

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

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

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

Ipconfig

Ipconfig (Windows Vista): Use the procedure below to find your IP address, MAC (hardware) address, DHCP server, DNS server and other useful information under Windows Vista.

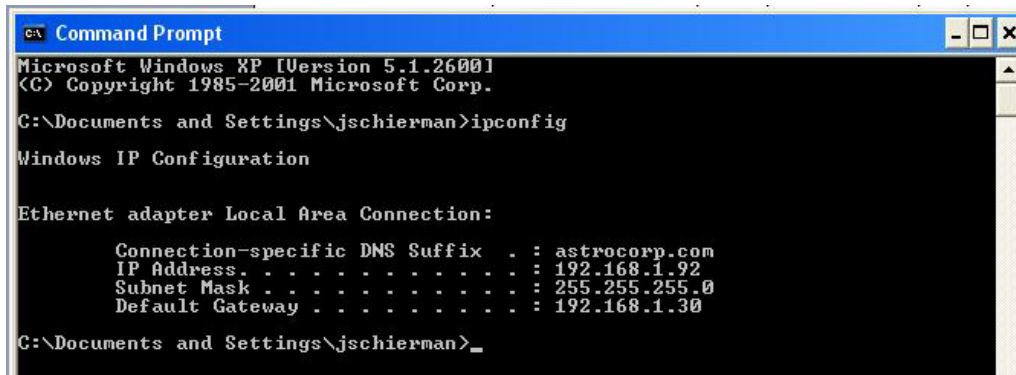
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway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

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

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

Use the **ipconfig** command to quickly obtain the TCP/IP configuration of a computer.

1. Open a Command Prompt. Click Start, point to Programs, point to Accessories, and then click Command Prompt.
2. Type **ipconfig** and press Enter. The Windows IP Configuration displays:



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

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

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

3. Make sure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
4. For more information, use the /all parameter (type **ipconfig /all** and press **Enter**).

The **ipconfig** command is the command-line equivalent to the **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

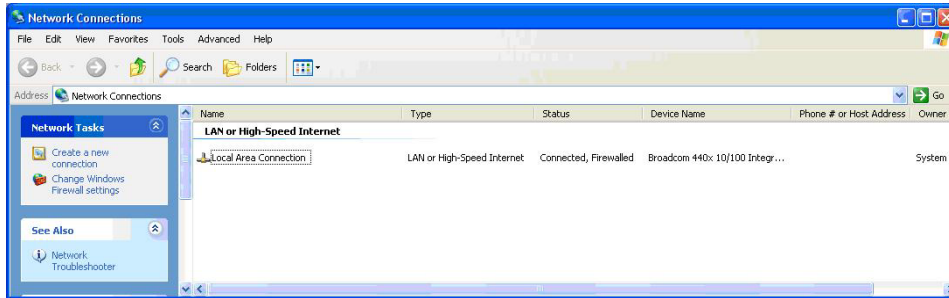
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
      TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:892258 (871.3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

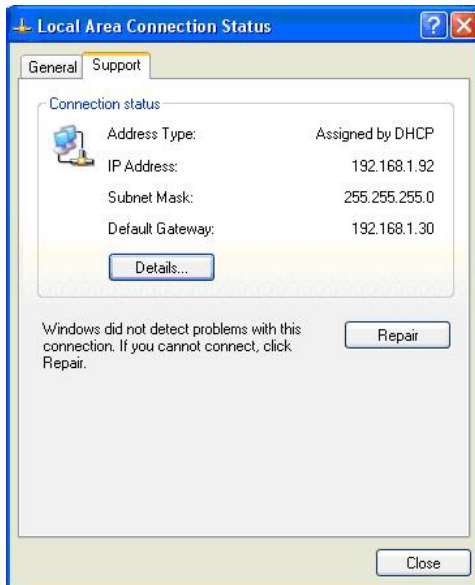
Windows Network Connections

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.

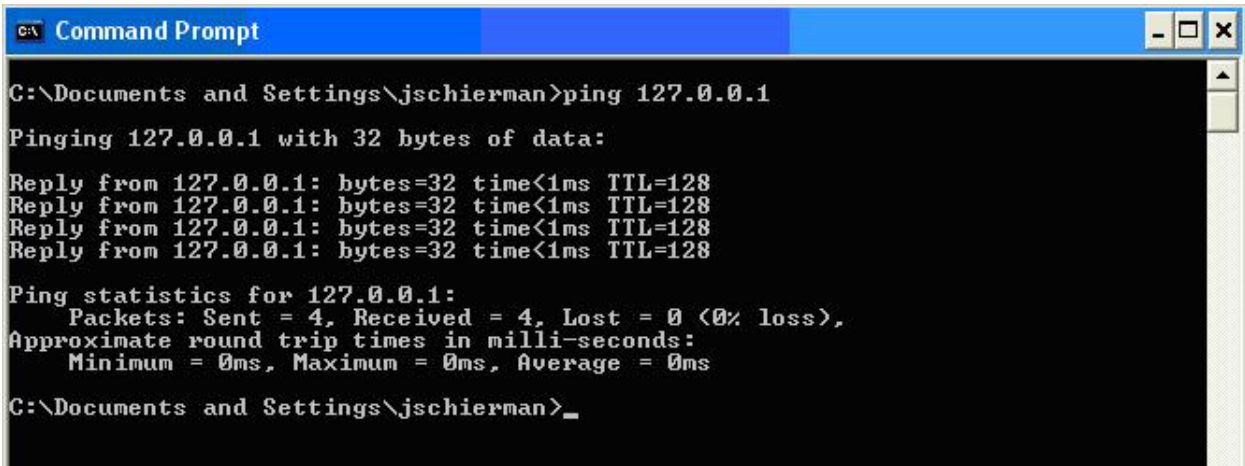


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

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**.



```
C:\Documents and Settings\jschierman>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

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

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the **ping** command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host on a different subnet). If the **ping** command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server. If the **ping** command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

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

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

Telnet

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

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

Telnet Client

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

To install Telnet Client:

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

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

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/en-us/library/cc787407\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc787407(W.S.10).aspx).

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

PuTTY

PuTTY is a simple, free, but excellent SSH and Telnet replacement for Windows 95/98/NT.

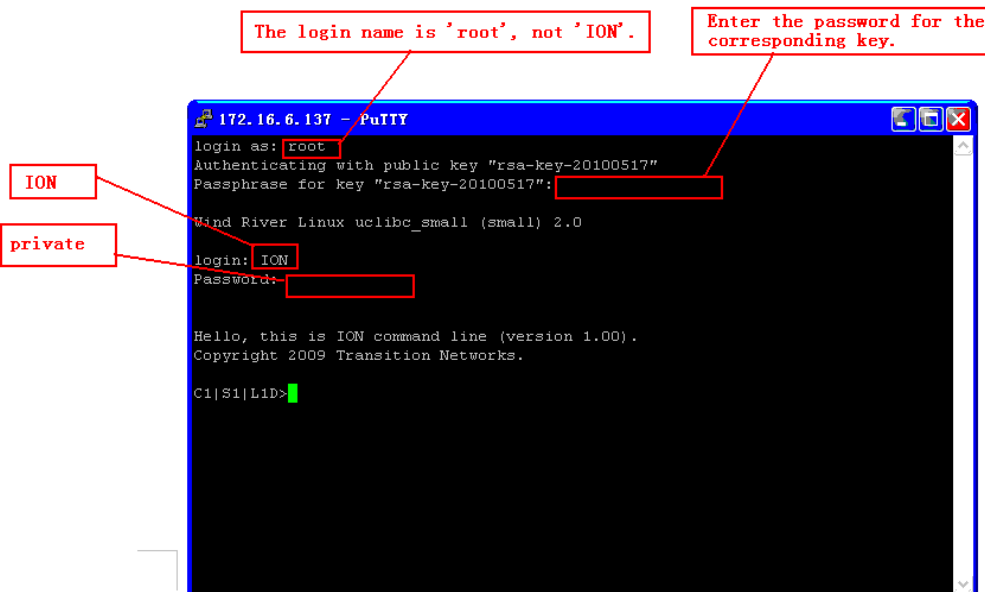
The PuTTY SSH and telnet client was developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is developed and supported by a group of volunteers. PuTTY has been ported to various other operating systems. Official versions exist for some Unix-like platforms, with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

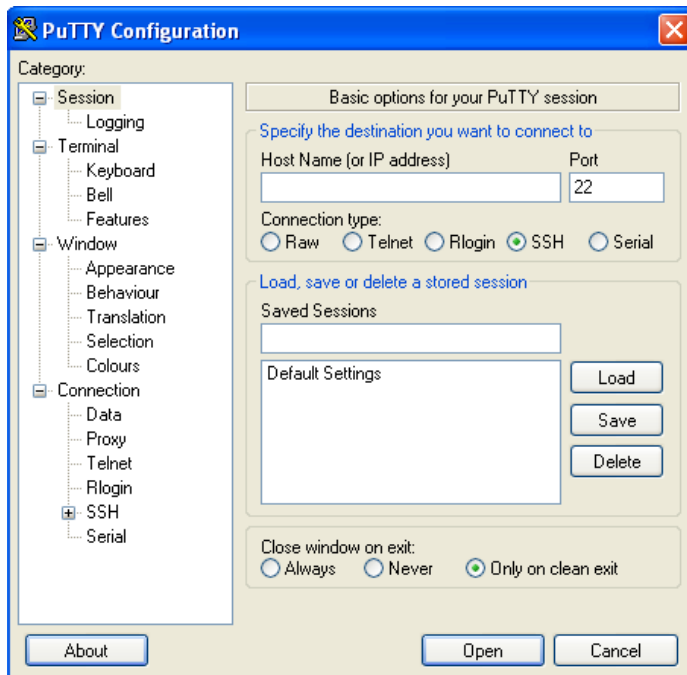
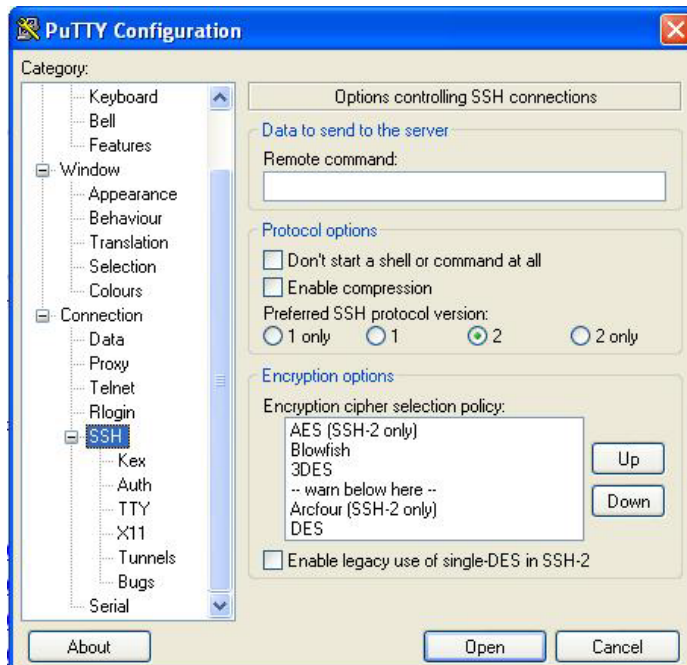
The PuTTY terminal emulator application also works as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols.

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

Note:

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



PuTTY Basic Options:**PuTTY SSH Options:**

Tracert (Traceroute)

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

Tracert is a Windows based tool that 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 protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, **netstat** displays active TCP connections.

Note: parameters used with this command must be prefixed with a hyphen (-) and NOT a slash (/):

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

Winipcfg

The **winipcfg** command is available in Windows ME, Windows 98, and Windows 95 to review your current TCP/IP network protocol settings. Follow these steps to view your current TCP/IP settings using **winipcfg**:

1. Click the Start button and then click Run.
2. Type **winipcfg** in the Open box, and then click OK. Your current TCP/IP settings are displayed.
3. To view additional information, click **More Info**.

Note: The Winipcfg display is not updated dynamically. To view changes, quit **winipcfg** and then run it again. If your IP address was dynamically allocated by a DHCP server, you can use the Release and Renew buttons to release and renew the IP address.

The following information is displayed by the **winipcfg** tool.

Adapter Address: This string of hexadecimal numbers represents the hard-coded identification number assigned to the network adapter when it was manufactured. When you are viewing the IP configuration for a PPP connection using Dial-Up Networking, the number is set to a default, meaningless value (because modems are not hard-coded with this type of address).

IP Address: This is the actual IP networking address that the computer is set to. It is either dynamically assigned to the computer upon connection to the network, or a static value that is manually entered in TCP/IP properties.

Subnet Mask: The subnet mask is used to "mask" a portion of an IP address so that TCP/IP can determine whether any given IP address is on a local or remote network. Each computer configured with TCP/IP must have a subnet mask defined.

Default Gateway: This specifies the IP address of the host on the local subnet that provides the physical connection to remote networks, and is used by default when TCP/IP needs to communicate with computers on other subnets.

Click **More Info** to display the following settings:

DHCP Server: This specifies the IP address of the DHCP server. The DHCP server provides the computer with a dynamically assigned IP address upon connection to the network. Clicking the Release and Renew buttons releases the IP address to the DHCP server and requests a new IP address from the DHCP server.

Primary and Secondary WINS Server: These settings specify the IP address of the Primary and Secondary WINS servers (if available on the network). WINS servers provide a service translating NetBIOS names (the alphanumeric computer names seen in the user interface) to their corresponding IP address.

Lease Obtained and Lease Expires: These values show when the current IP address was obtained, and when the current IP address is due to expire. You can use the Release and Renew buttons to release and renew the current IP address, but this is not necessary because the DHCP client automatically attempts to renew the lease when 50 % of the lease time has expired.

Nslookup

nslookup is a computer program used in Windows and Unix to query DNS (Domain Name System) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The name nslookup means "name server lookup". A common version of the program is included as part of the BIND package.

Microsoft Windows 2000 Server, Windows 2000 Advanced Server, and Windows NT Server 4.0 Standard Edition provide the **nslookup** tool.

Windows' nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through the Control Panel.

Nslookup.exe can be run in two modes: interactive and noninteractive. Noninteractive mode is used when just a single piece of data is needed.

1. The syntax for noninteractive mode is:

```
nslookup [-option] [hostname] [server]
```

2. To start Nslookup.exe in interactive mode, simply type "**nslookup**" at the command prompt:

```
C:\> nslookup
```

```
Default Server: nameserver1.domain.com
```

```
Address: 10.0.0.1
```

```
>
```

3. Type "**help**" or "?" at the command prompt to generate a list of available commands.

Notes

- The TCP/IP protocol must be installed on the computer running Nslookup.exe.
- At least one DNS server must be specified when you run the IPCONFIG /ALL command from a command prompt.
- Nslookup will always devolve the name from the current context. If you fail to fully qualify a name query (i.e., use a trailing dot), the query will be appended to the current context. For example, if the current DNS settings are att.com and a query is performed on www.microsoft.com; the first query will go out as www.microsoft.com.att.com because of the query being unqualified. This behavior may be inconsistent with other vendor's versions of Nslookup.

Dr. Watson

Dr. Watson detects information about Windows system and program failures and records the information in a log file. Dr. Watson starts automatically at the event of a program error. To start Dr. Watson, click **Start**, click **Run**, and then type **drwtsn32**. To start Dr. Watson from a command prompt, change to the root directory, and then type **drwtsn32**.

When a program error occurs, Dr. Watson creates a log file (Drwtsn32.log) which contains:

- The line *Application exception occurred:*.
- Program error information.
- System information about the user and the computer on which the program error occurred.
- The list of tasks that were running on the system at the time that the program error occurred.
- The list of modules that the program loaded.
- The state dump for the thread ID that is listed.
- The state dump's register dump.
- The state dump's instruction disassembly.
- The state dump's stack back trace.
- The state dump's raw stack dump.
- The symbol table.

The default log file path is:

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

The default Crash Dump path is:

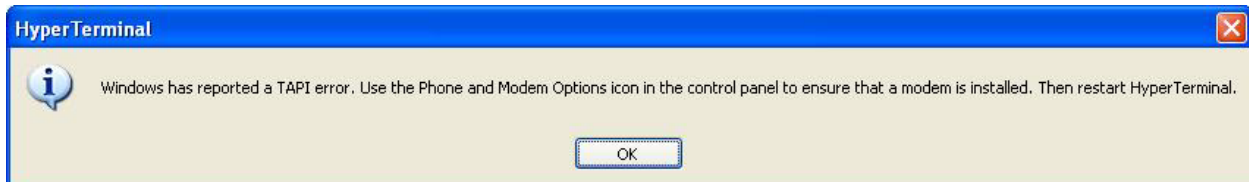
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

Third Party Tool Messages

This section discusses messages generated by HyperTerminal, Ping, and Telnet during ION system installation, operation and configuration.

HyperTerminal Messages

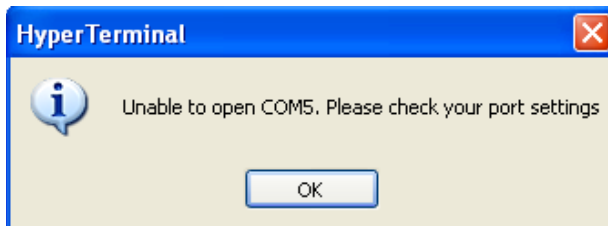
Message: *Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal.*



Response:

1. Verify your **computer's Ports (COM & LPT)** setting. See "[Configuring HyperTerminal](#)" on page 53.
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support.

Message: *Unable to open COM x. Please check your port settings.*



Response:

1. Verify your **computer's Ports (COM & LPT)** setting. See "[Configuring HyperTerminal](#)" on page 53.
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support.

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

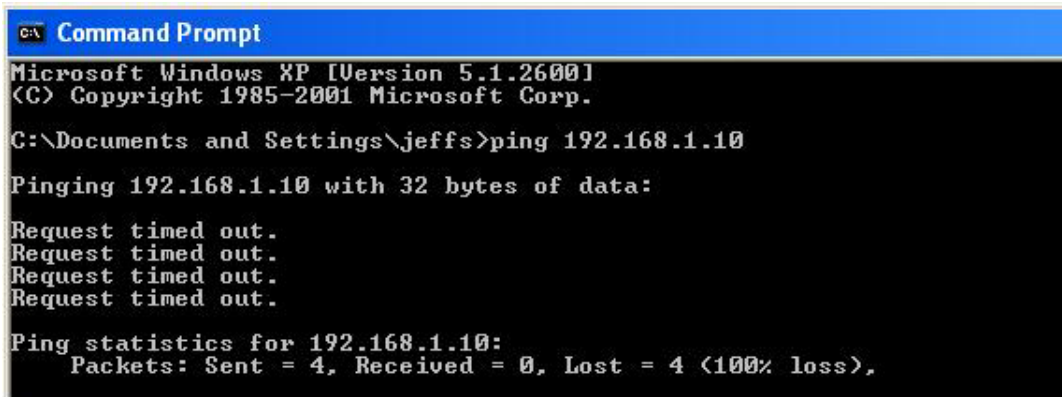
line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a text entry. Overtyping an entry should automatically replace the previous characters. This is a HyperTerminal problem that the ION CLI stack cannot resolve.

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.*



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\jeffs>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

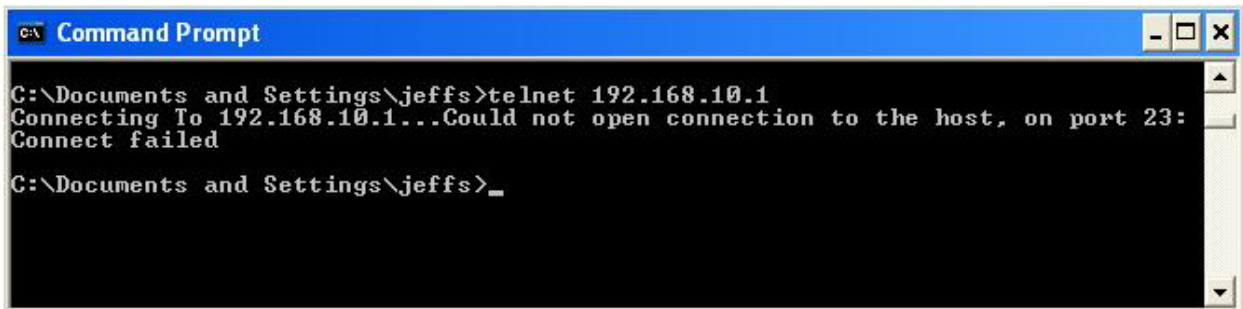
Meaning: The Ping command failed.

Recovery:

1. Verify the connection, verify correct IP address entry, and retry the operation.
2. Verify if the default IP address has changed using the Ipconfig (or similar) command.

Telnet Messages

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



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

Meaning: The attempted Telnet connection failed.

Recovery:

1. Verify the physical connection, verify correct IP address entry, and retry the operation.
2. Check if the default IP address has changed using the Ipconfig (or similar) command.

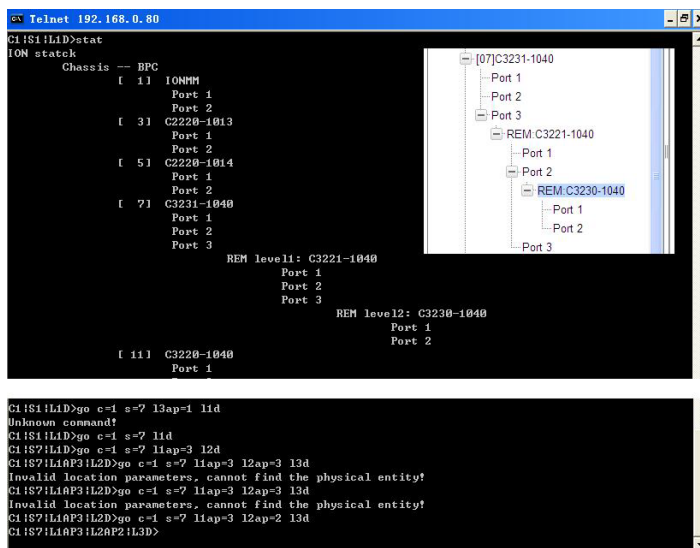
Message: *Invalid location parameters, cannot find the physical entity!*

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

Meaning: 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!*

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

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

Recovery:

1. Verify the CLI command syntax.
2. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.

TFTP Server Messages

Messages like the ones below may display during TFTP Server operation, depending on the TFTP Server package that you selected.

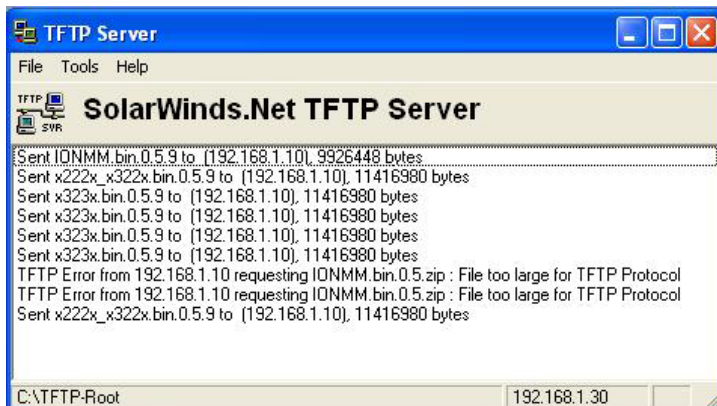
Message: *File does not exist*



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

Recovery: 1) Verify the TFTP server's correct file location (e.g., local disk at *C:\TFTP-Root*). 2) Make sure of the filename / extension. 3) Check the TFTP Server's online helps for suggestions.

Message: *File too large for TFTP Protocol*



Meaning: A TFTP Server error - you tried to upload a file e.g., (IONMM.bin.0.5 – 50Mb) but the TFTP server failed. The file you tried to upload via the TFTP server exceeded the file size capability.

Recovery: 1) Check if some extra files ended up in the zip folder – some repeated – 6 FW files total. 2) Remove some of the files from the zip folder and try the upload again. 3) Send the remaining files in a separate file. 4) Check the TFTP Server's online helps for suggestions.

PuTTY Messages

Messages like the ones below may display during PuTTY (or similar package) operation, depending on the package that you selected.

Message: *Server refused key*

Meaning: You can connect to a secure telnet session using password authentication, but when you try to connect using public key authentication, you receive a "*Server refused our key*" message on the client (PuTTY) session. For example, you generated a public/private key (using Puttygen) and saved them, loaded the client public key into the IONMM via TFTP, and enabled SSH. The PuTTY SSH Authentication pointed to the saved private key. You set the auto-log on user name to root as suggested, but when you activated PuTTY, after 20-30 seconds, the refusal message displayed and PuTTY reverted back to password authentication (the default).

Recovery:

1. When generating using puttyGen.exe, select the SSH2 keys - do not select the SSH1 keys.
2. Log in to PuTTY as 'root' with the public key authentication.
3. Use the online helps and documentation to set up Putty as suggested.
4. See the "[PuTTY](#)" section notes on page [408](#).

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.

The screenshot shows the 'MAIN' configuration page for an ION system. The left sidebar shows a tree view of the 'ION Stack' with 'Chassis' expanded, listing slots [01] through [23]. The main content area is divided into sections: 'Model Information' with fields for Serial Number (789568), Model (C4120-1048), Software Revision (2.0.0), Hardware Revision (1.0.0), and Bootloader Revision (0.1.5); 'System Configuration' with fields for System Name (C4120), System Up Time (0:0:04:54:00), Configuration Mode (Software), and Number of Ports (2); a MAC Address field (00-C0-F2-00-D1-38); a Device Description field; and a Transparent Link Pass Through (TLPT) section with a dropdown menu set to 'Disabled'. At the bottom of the configuration area are buttons for 'Uptime Reset', 'System Reboot', and 'Reset To Factory Config'. The footer of the page includes 'Refresh', 'Save', and 'Help' buttons, and the version number 'Version: 1.3.1812'.

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: _____

Device Description: _____

4. Provide additional Model and System information to your Technical Support Specialist. See “[Basic ION System Troubleshooting](#)” on page 151.

Your Lantronix service contract number: _____

A description of the failure: _____

A description of any action(s) already taken to resolve the problem (e.g., changing 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, Compliance and Electrical Safety

Please refer to the x4120 Install Guide for warranty and compliance information, and Electrical Safety Warnings.

Appendix B: SNMP MIBs and Traps Support

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

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

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

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

Supported MIBs

The x4120 implements the following Management Information Bases (MIBs).

- ionDevSysCfgTable
- ifTable
- ifXTable
- ionDMIIInfoTable
- ionIfLoopbackTable
- ionEthInterfaceTable
- ionDevSysLPTTable
- ifMauAutoNegTable

The C4120 will expand three options of TNethPhyMode structure for new PHY mode:

```
TNethPhyMode ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION
    "The different Ethernet PHY interfaces supported."
  SYNTAX INTEGER {
                                unknown(0)
                                phy10-100BaseT(1)
                                phy100BaseFX(2)
                                phy1000BaseX(3)
                                phy10-100-1000BaseT(4)
                                phySGMII(5)
                                phy10GBase-LRM(6)
                                phy10GBase-SR(7)
                                phy10GBase-LR(8)
                                phy10GBase-ER(9)
                                phy10GBase-ZR(10)
                                phy10GBase-T(11)
                                phy10GBase-auto(12)
  }
```

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

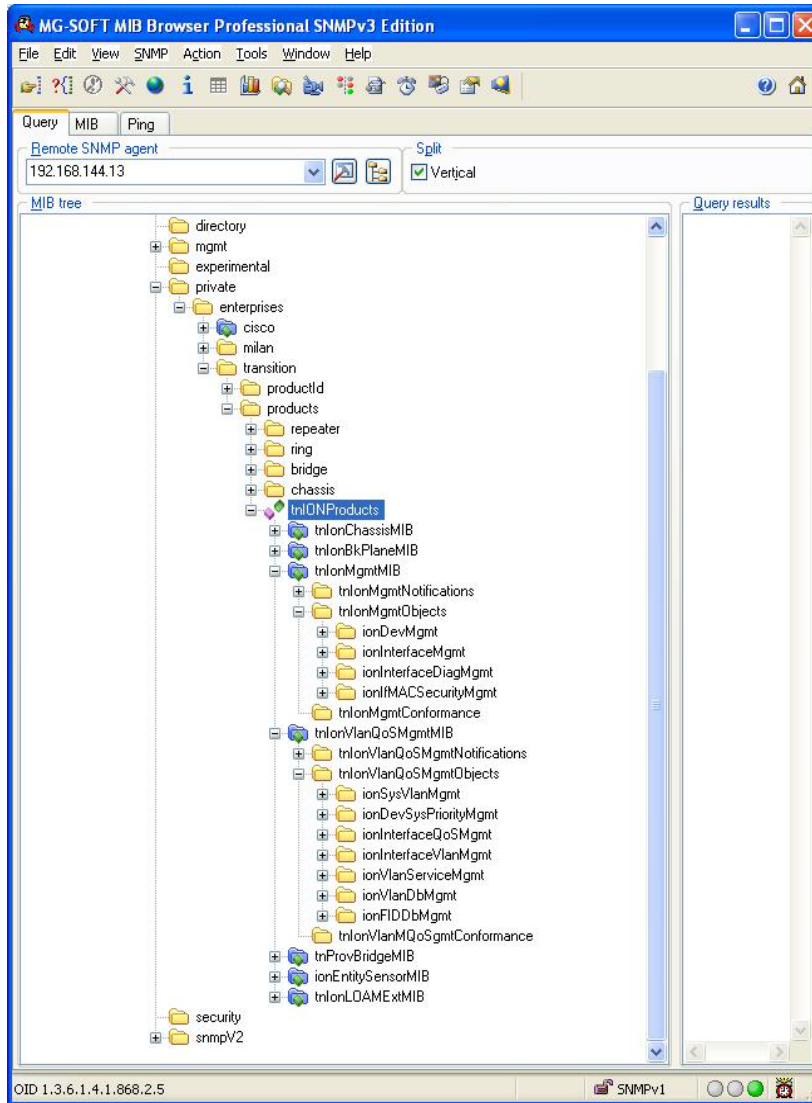


Figure 2: Private MIB Objects

Downloading, Compiling and Integrating MIBs

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

To download ION system private MIBs:

1. Go to the ION software [downloads page](#) and locate the **Management MIB** section.
2. Click the link in the far right column (e.g., **Download mcc16.zip**).
3. At the **File Download** window, click **Save**.
4. At the **Save As** dialog box, verify the filename and **Save in** location (e.g., C:\TFTP-Root) and click **Save**.
5. At the **Download complete** dialog click **Close**. The downloaded file is saved to the specified folder location.
6. If you plan to integrate the ION system with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView, you must compile the ION system MIBs with the HP OpenView NMS (Network Management System). See the NMS documentation for compiler instructions.
7. While working with MIBs, be aware that:
 - a. Mismatches on datatype definitions can cause compiler errors or warning messages.
 - b. The MIB datatype definitions are not mismatched; however, some standard RFC MIBs do mismatch.
 - c. If your MIB compiler treats a mismatch as an error, or if you want to delete the warning message, refer to the “[Technical Support](#)” section on page 405.

Set up your ION system SNMP configuration via the command line interface (CLI). Refer to “[Configuring SNMP](#)”. For a complete list of the available commands, see the x4120 CLI Reference, 33497.

Trap Service and Functions

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

See the “Supported MIBs” section on page 32 for information on the x4120s support for public (standard) and private MIBs. For information on “Configuring SNMP” see page 104. See the *ION Management Module (IONMM) User Guide* manual for SNMP traps supported on the IONMM.

A sample SNMP Message sequence is shown below.

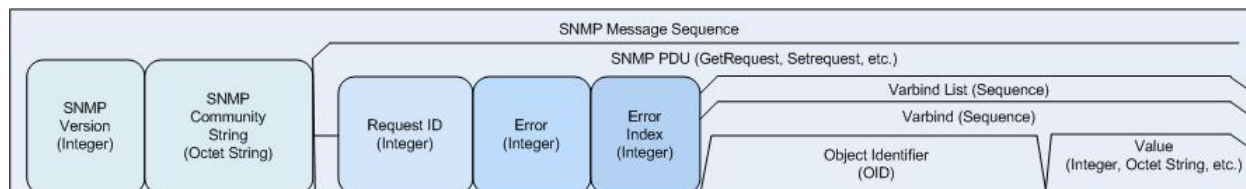


Figure 3: SNMP Message Sequence

The ION x4120 supports a Trap function to report the status as follow:

- 1) Ports link status change:
 - C4120 will send link up trap only once if port link status changes from link down to up;
 - C4120 will send link down trap only once if port link status changes from link up to down.
- 2) DMI trap:
 - An *ionDMIRxIntrusionEvt* event is sent if the *ionDMIRxPowerLevel* falls below the *ionDMIRxPwrLvIPreset* indicating an intrusion on the fiber
 - *ionDMIRxPowerEvt* event is sent when there is a warning or alarm on Rx Power
 - *ionDMITxPowerEvt* event is sent when there is a warning or alarm on Tx Power
 - *ionDMITxBiasEvt* event is sent when there is a warning or alarm on Tx Bias current
 - *ionDMITemperatureEvt* event is sent when there is a warning or alarm on DMI temperature.
 - C4120 will keep sending DMI traps until it becomes normal. Like the other ION SICS, the C4120 will periodically send out the specific trap every 3 seconds until the trap event condition doesn't meet.

Only the IONMM SNMP management tool integrates the trap service function. You can launch the Trap function when needed.

The Trap message includes the following content:

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

The display format in FP will be as following (example):

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

Trap MIBs are listed below:

IF-MIB:

linkDown
linkup

TN-ION-MGMT-MIB.smi :

ionDMIRxIntrusionEvt
ionDMIRxPowerEvt
ionDMITxPowerEvt
ionDMITxBiasEvt
ionDMITemperatureEvt

Trap Server Log

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

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

```
Line
1
2
3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
12
13 E=
14 Ebig=
15 IP=192.251.144.220
16 com=trap
17 GT=Notification
18 ST=
19 TS=Thu May 13 10:06:42 2010
20 VB-Count=3
21 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266790) 326 days, 15:37:47.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
22
23 E=
24 Ebig=
25 IP=192.251.144.220
26 com=trap
27 GT=Notification
28 ST=
29 TS=Thu May 13 10:10:17 2010
30 VB-Count=3
31 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288348) 326 days, 15:41:23.48 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
32
33 E=
34 Ebig=
35 IP=192.251.144.220
36 com=trap
37 GT=Notification
38 ST=
39 TS=Thu May 13 10:10:18 2010
40 VB-Count=5
41 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288428) 326 days, 15:41:24.28 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.4.1.868.2.5.2.0.1 |
iso.3.6.1.2.1.47.1.1.1.1.1.134217728 = 134217728 | iso.3.6.1.4.1.868.2.5.2.1.1.1.134217728.6 = 6 | iso.3.6.1.4.1.868.2.5.2.1.1.2.134217728.6
= 1
```

The trap server log file lines are described below.

```

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

```

Table 7: Trap Server Log File Description

Category	Example	Meaning
E=		Endian
Ebig=		bigEndian
IP=	192.251.144.220	IP address
com=	trap	
GT=	Notification	
ST=		
TS=	Thu May 13 10:06:37 2010	Timestamp – the log date that the file was recorded
VB-Count=	3	
Vars=	iso.3.6.1.2.1.1.3.0 =	Varbinds (Variable bindings) - the variable number of values that are included in an SNMP packet. Each varbind has an OID, type, and value (the value for/from that Object ID).
Timeticks:	(2822266290) 326 days, 15:37:42.90	
iso.3.6.1.6.3.1.1.4.1.0 =	iso.3.6.1.2.1.47.2.0.1	
iso.3.6.1.6.3.1.1.4.3.0 =	iso.3.6.1.2.1.47.2	

For Additional SNMP MIB Trap Information

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

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



Lantronix Corporate Headquarters

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

Technical Support

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

Sales Offices

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