

## ION System C3210 Series

10/100/1000BASE-T to 1000BASE-SX/LX

Media and Rate Converter Module

## User Guide

**Part Number 33496**  
**Revision E August 2023**

## Intellectual Property

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

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

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

## Warranty

For details on the Lantronix warranty policy, 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 the Lantronix web site at [www.lantronix.com/about/contact](http://www.lantronix.com/about/contact).

## Disclaimer

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

## Revision History

Date	Rev	Description
09/12/11	C	Revised for ION Rel. 1.2.0 with: 1) Increased Rate Limiting options. 2) SNMPv3. 3) BootP Address mode. 4) WRR or Strict Egress Queue Modes. 5) Serial File Transfer (X/Y/Zmodem) commands. 6) IONMM System Name displays in CLI prompt. 7) Password can be changed using the community write string, and any login or password that is not fixed.
6/1/17	D	Revised for ION C3210 v2.0.0 to fix chassis slot number reporting incorrectly. Update contact info and format.
8/28/23	E	Initial Lantronix rebrand. Remove Glossary and Appendix A.

## 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 lightening transients or power faults. They are **not** to be connected to inter-building (*outside plant*) link segments that are subject to lightening.

**Caution:** **Do not** install the C3210 in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor C3210 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 [Appendix A](#) for Electrical Safety Warnings translated into multiple languages.



## Contents

<b>1. Introduction .....</b>	<b>7</b>
Pause .....	9
DMI Optical Management.....	10
Backwards Compatibility / Point System Support .....	10
TFTP (Trivial File Transfer Protocol) .....	11
Link Pass Through.....	11
IEEE 802.1p QoS Packet Classification .....	12
Device Description / Circuit ID.....	12
RFC 2544 Benchmarking .....	12
Serial File Transfer (X/Y/Zmodem).....	13
Downloading, Compiling and Integrating MIBs .....	15
Related Manuals and Online Helps .....	19
<b>2. Installation and System Setup .....</b>	<b>20</b>
Access via an Ethernet Network .....	25
<b>3. Management Methods .....</b>	<b>30</b>
Menu System Descriptions.....	36
Reboot, Reset, and Power Off Function Notes .....	38
<b>4 Configuration .....</b>	<b>41</b>
System Configuration – CLI Method .....	42
System Configuration – Web Method.....	43
Link Pass Through (LPT) Config – CLI Method .....	48
Link Pass Through (LPT) Config – Web Method .....	48
Set Ethernet Port Speed / Duplex Mode – Web Method.....	57
Set Bandwidth Allocation / Rate Limiting – CLI Method .....	58
Set Bandwidth Allocation / Rate Limiting – Web Method .....	60
Security Features.....	61
Configuring MAC Address Blocking .....	61
Configuring Port Forward Management / IP Access Blocking .....	65
<b>5. Operation .....</b>	<b>74</b>
Backing Up Standalone Modules .....	77
Editing the Config File (Optional) .....	79
Reset System Uptime – CLI Method .....	88
Reset System Uptime – Web Method .....	89
Reset All Ports Counters – CLI Method .....	90
Reset Port Counters– Web Method .....	91
Clear All Ethernet Port Counters – CLI Method .....	92
All Counters Reset – Web Method .....	93
Rebooting – CLI Method .....	94
Upgrading IONMM and/or C3210 Firmware – CLI Method.....	97
Upgrading IONMM and/or C3210 Firmware – Web Method .....	99
<b>6. Troubleshooting.....</b>	<b>112</b>
Basic ION System Troubleshooting.....	112
Error Indications and Recovery Procedures .....	113
LED Fault and Activity Displays.....	114
ION System Tests.....	181
Virtual Cable Test (VCT) .....	181
PCB Identification .....	191
x3210 PCB .....	191
HyperTerminal Messages .....	208
Ping Command Messages .....	210
Telnet Messages .....	210

PuTTY Messages .....	213
Recording Model Information and System Information .....	214
<b>Appendix A. Compliance and Safety Information .....</b>	<b>216</b>
<b>Appendix B. Factory Defaults .....</b>	<b>216</b>
<b>Appendix C. SNMP Traps Supported .....</b>	<b>219</b>
Traps List .....	219
<b>Appendix D. ION C3210 to GFEB105 Feature Mapping.....</b>	<b>245</b>
<b>Index .....</b>	<b>249</b>

## List of Figures

Figure 1: Private MIB Objects .....	14
Figure 2: Chassis Installation .....	20
Figure 3: SFP Installation .....	21
Figure 4: Model C3210 Connectors and LEDs .....	22
Figure 5: CLI Location Hierarchy .....	31
Figure 6: VLAN Tunneling Example.....	72
Figure C-1: SNMP Message Sequence .....	220

## List of Tables

Table 1: Supported MIBs .....	13
Table 3: C3210 Model Specifications .....	17
Table 4: Documentation Conventions.....	18
Table 5: Model C3210-10xx Connectors and LED Descriptions .....	23
Table 6: System-Level Menu Description .....	36
Table 7: Port-Level Menu Description.....	37
Table 8: Back Up and Restore File Content and Location.....	83
Table 9: File Status after a Reset to Factory Defaults .....	87
Table 10: File Content and Location after a System Reboot.....	96
Table 11: File Content and Location after a Firmware Upgrade .....	109
Table 12: VCT Parameters .....	184
Table 13: DMI Parameters .....	186
Table 14: Connector Types.....	189
Table 15: Device-Level Factory Defaults .....	216
Table 16: Port-Level Factory Defaults .....	217
Table 17: MIB Traps Summary .....	220
Table 18: Trap Server Log File Description .....	244
Table 19: ION C3210-to-xGFEB105 Feature Mapping.....	247

# 1. Introduction

## Document Overview

The purpose of this manual is to provide the user with an understanding of the C3210 Ethernet media converter. This manual documents the following models:

- **C3210-1013** : 10/100/1000Base-T (RJ-45) [100 m] to 1000Base-SX 850nm multimode (SC) [62.5/125  $\mu$ m fiber: 220 m/722 ft.] [50/125  $\mu$ m fiber: 550 m/1804 ft.] Link Budget: 8.5 dB
- **C3210-1039**: 10/100/1000Base-T (RJ-45) [100 m/328 ft.] to 1000Base-SX 850nm multimode (LC) via SFP [62.5/125  $\mu$ m fiber: 220 m/722 ft [50/125  $\mu$ m fiber: 550 m/1804 ft.] Link Budget: 8.0 dB
- **C3210-1014**: 10/100/1000Base-T (RJ-45) [100 m] to 1000Base-LX 1310nm single mode (SC)[10 km/6.2 mi.] Link Budget: 10.5 dB
- **C3210-1040**: 10/100/1000Base-T (RJ-45) [100 m] to 1000Base-X SFP Slot (empty)

## Product Overview

The C3210 is a group of Ethernet media converters that are designed as slide-in modules that install in an ION system chassis. The C3210 can be managed when installed in a managed ION chassis. If the C3210 is linked over fiber to a stand-alone device, it will be the Point System SGFEB10xx-120 (the SGFEBs are un-managed devices).

The ION C3210 media converters are 2- port Ethernet devices capable of media conversion between copper and fiber ports. These are chassis managed devices designed as slide-in-cards (SICs) for installation in an ION system chassis. A stand-alone equivalent can be found in the Point System product family, SGFEB10xx-120.

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. Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

## C3210 Series Features

The C3210 supports the following features.

The ION C3210 device provides an interface between 10/100/1000Base-T ports and 1000Base-SX/LX ports allowing users to integrated fiber optic cabling into 10/100/1000Base-T copper environments.

The overall benefits include:

- Integrate fiber into copper based networking environments
- Can be used in any ION Platform Chassis
- Bridging legacy 10/100 devices into a Gigabit Backbone
- Secure Uni-directional transmission
- Standards based, will link with any standard 10/100/1000Base-T and any standard 1000Base-SX or LX ports

The following manageable features are available when used in an ION Platform chassis along with an ION Management Module (IONMM):

- 10K Jumbo Frame Support
- Copper and Fiber Auto-Negotiation
- Switch Selectable Speeds
- AutoCross™
- Link Pass Through
- Remote Fault Detect
- Pause
- Automatic Link Restoration
- MAC filtering for network access control (authentication and authorization)
- Backward compatibility / Point System support
- IEEE 802.1P QoS, IPv4 TOS/Diffserv, IPv6 traffic class
- IEEE 802.1q Port VLAN, tagging and doubling tagging (Q-in-Q)
- VLAN Forwarding and VLAN Tag Management
- Field Upgradeable Firmware
- Virtual Cable Test on UTP port
- Uni-directional data transmission
- Bandwidth Allocation
- DMI digital diagnostics per SFF-8472
- RMON counters for each port
- Circuit ID and Device Description
- Serial File Transfer (X/Y/Zmodem) commands

These features are discussed in the following sections.

### 10K Jumbo Frame Support

The C3210 devices support jumbo frames. The MTU (Maximum Transmission Unit) frames size can be 10240 bytes (not configurable). Note: If the C3210 is linked to a SGFEB, then the maximum supported frame size is limited to the capability of the SGFEB (1623 bytes).

### Auto-Negotiation (802.3u)

This feature allows two devices to configure to achieve the best possible mode of operation over a copper link, automatically. The C3210 broadcasts its speed and duplex (full or half) capabilities to the connected device and negotiates the best mode of operation. Auto-Negotiation allows quick connections because the optimal link between the devices is established automatically.

In a scenario where the C3210 links to a non-negotiating device, disable Auto-Negotiation. In this instance, the mode of operation will drop to the lowest common denominator between the two devices (e.g., 10 Mbps at half-duplex).

Disabling this feature allows forcing the connection to the desired speed and duplex mode of operation.

### Pause

Pause is used to suspend data transmission temporarily to relieve buffer congestion. If an Ethernet device needs some time to clear network congestion, it will send a pause signal to the Ethernet device at the other end, then that device will wait a predetermined amount of time before re-transmitting its data.

This feature reduces data bottlenecks and allows efficient use of network devices, preventing data losses.

The pause feature is set using the SNMP interface to one of four settings:

- Disable (no pause)
- Symmetrical pause
- Asymmetric Tx (transmit) pause
- Asymmetric Rx (receive) pause

Enable the Pause feature, if available, on all Ethernet network devices attached to the C3210, otherwise disable this feature. Note that all Ethernet devices support this in full duplex mode.

### AutoCross (10/100/1000Base-T)

When active, the *AutoCross*™ feature allows the use of a straight-through (MDI) or crossover (MDIX) copper cable when connecting to 10/100Base-T or 10/100/1000Base-T converters. AutoCross determines the characteristics of the connection and configures the copper port to link up automatically. This occurs regardless of the cable configuration (MDI or MDI-X).

**Note:** Lantronix recommends leaving *AutoCross* in default mode (Auto).

### Bandwidth Profiling

A Bandwidth Profile is a method of characterizing Service Frames for the purpose of rate enforcement or policing. The C3210 devices support bandwidth profiling at the per-port level. Each port has an ingress bandwidth profile used to control the ingress traffic and an egress bandwidth profile for regulating traffic leaving the port. This feature provides TX and RX rate limiting from a pre-defined list of values in order to accommodate bursty traffic.

## Configuration Backup and Restore

The firmware uses Trivial File Transfer Protocol (TFTP) to upload its present configuration onto a TFTP server, and can also download the configuration from the TFTP server and update its settings. This is useful when you want to program more than one unit to the same configuration. One unit can be programmed and that configuration can be used to populate the other units. Care should be taken on some settings such as IP address and virtual LAN (VLAN) settings.

**Note:** Lantronix recommends as a “best practice” to backup SIC card 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.

For more information see [“Backup and Restore Operations”](#) on page 82.

## DMI Optical Management

Devices with Diagnostic Monitoring Interface (DMI) support allow diagnosing problems within the network. DMI devices have four functions:

- Transmit power
- Receive power
- Transmit bias current
- Temperature

Within each function, the DMI device will send a trap whenever a high or low warning event or high or low alarm event occurs (for a total of 16 traps).

Optical SFP transceivers support digital diagnostics monitoring (DDM) functions per industry-standard SFF-8472.

## Backwards Compatibility / Point System Support

The ION Platform offers backwards compatibility with Lantronix’ Point System family of media converters. Not only can an ION module be linked to a Point System Module over fiber, but Point System modules can be installed in the ION chassis through the use of an ION system adapter card.

The backplane in the ION chassis will power the Point System modules, allowing the module to perform its copper-to-fiber media converter functions. Full read/write management of Point System modules is also available in the ION chassis. This requires the use of a Point System Management Module along with the ION system adapter card.

By supporting management modules from both the ION Platform and the Point System, users are able to re-deploy and fully manage their Point System devices, easing their migration to the ION Platform.

## Management Access Methods

Management of the C3210, and subsequently the other slide-in modules, is accomplished through one of the following methods.

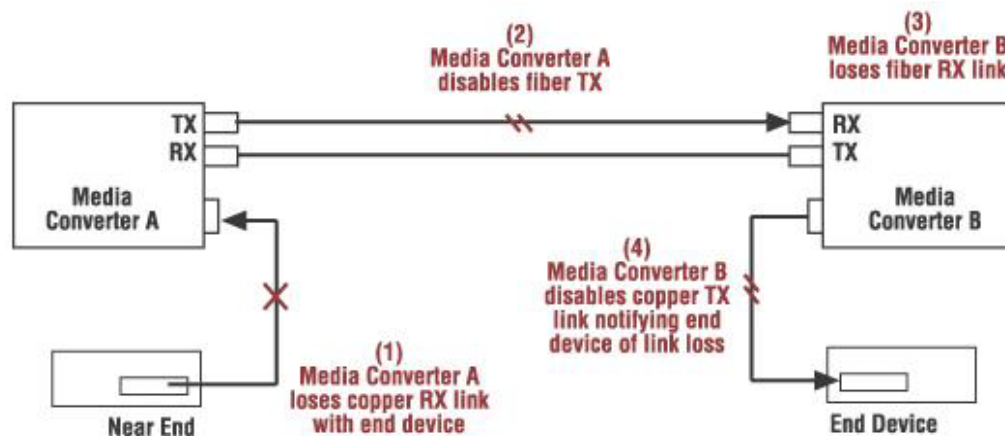
- Universal Serial Bus (USB) – uses a command line interface (CLI) to access and control the C3210 through a locally connected workstation.
- Telnet session – uses the CLI to access and control the C3210 through the network.
- Simple Network Management Protocol (SNMP) – both public and private Management Information Bases (MIBs) allowing for a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).

## TFTP (Trivial File Transfer Protocol)

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

## Link Pass Through

Link Pass Through is a troubleshooting feature that allows the media converter to monitor both the fiber and copper RX ports for loss of signal. In the event of a loss of RX signal on one media port, the converter will automatically disable the TX signal of the other media port, thus "passing through" the link loss. The end device is automatically notified of link loss which prevents loss of valuable data unknowingly transmitted over an invalid link.



## IP Access

Any management of the system via IP can be locked at the system level, or only on certain ports. For example, management can occur via web/SNMP only on Port 1, so that access via other ports can be blocked.

## MAC Filtering

When enabled on a port, stops learning all MAC addresses. To allow any frame with a MAC address not in the Static MAC database access, you must add the new address or it will be discarded. This allows filtering any unauthorized access to the network by unknown MAC addresses.

## MAC Addresses Blocking

The MAC address can be added to the static MAC address database with the 'connected port' as zero. This will cause any frames from that MAC address database to cause an ATU-member violation on that port, resulting in sending a trap. This could cause excessive traps (overload the Central Processing Unit (CPU) with interrupts) depending on the traffic generated by that MAC. You can disable MAC violations by setting the **Ignore SA Violation** on the port that is receiving the MAC address via the Web interface at **Port > Advanced > MAC Security > SA Lock**. The SA Lock enabled feature will detect if the device connected to this port has been changed, and when an unknown MAC address ingresses this port.

## Applicable Standards

- IEEE 802.1p QoS packet classification
- IEEE 802.1q VLAN and double VLAN tagging
- IEEE 802.1 Port-based Network Access Control

## IEEE 802.1p QoS Packet Classification

Quality of Service (QoS) is a mechanism that lets service providers offer different levels of services to customers. The QoS varies between customers based on the Service Level Agreement (SLA) they chose for the kind of service they want. The priorities of the customer traffic are assigned based on their SLAs.

The C3210 provides QoS at the Layer 2 level using CoS bits per IEEE 802.1p. The priority bits in the 802.3ac tag can be remapped as frames ingress the device based on Ingress port, Source MAC address, Destination MAC address, or VLAN ID in the 802.1q tag, or on the basis of remapping to a user-defined priority on a per port basis.

The C3210 also provides QoS based on DSCP/ToS bits in the IP header. The C3210 supports four output queues. Based on a frame's priority bits (layer 2 or layer 3), frames are assigned the egress output queues. The C3210 offers weighted round robin (WRR) 8-4-2-1 scheduling on the output queues to minimize frame latencies and starvation of lower priority queues.

## Device Description / Circuit ID

The x323x supports the Circuit ID, a company-specific identifier assigned by a provider to a data or voice network between two locations. This circuit is then leased to a customer by that ID. If a subscriber has a problem with the circuit, the subscriber contacts the telecom provider with this Circuit ID to initiate service action on the specified circuit. The ION Circuit ID port identifier is based on the agent-local identifier of the circuit (defined in RFC 3046), detected by the agent and associated with a particular port. The x323x supports the Circuit ID, a company-specific identifier assigned by the user to identify the converter and individual ports in any manner desired. At the device level, the x323x supports a 'Device Description' character string entry of up to 64 bytes.

## RFC 2544 Benchmarking

The C3210 supports IETF RFC 2544 (Benchmarking Methodology for Network Interconnect Devices). RFC 2544 defines several tests that can be used to describe the performance characteristics of a network interconnecting device, as well as specific formats for reporting the results of the tests (e.g., throughput, latency, frame loss rate, system recovery). The following RFC2544 testing reports are available for the C3210: Back-to-Back Test Report, Frame Loss Test Report, Latency Test Report, and Throughput Test Report.



## Serial File Transfer (X/Y/Zmodem)

The C3210 supports serial get, put, and upgrade CLI commands using the Xmodem, Xmodem-1k, Ymodem, and Zmodem protocols. These commands function similar to the TFTP download function; technical support can download configuration files and firmware files through the C3210 USB port by entering the corresponding CLI commands.

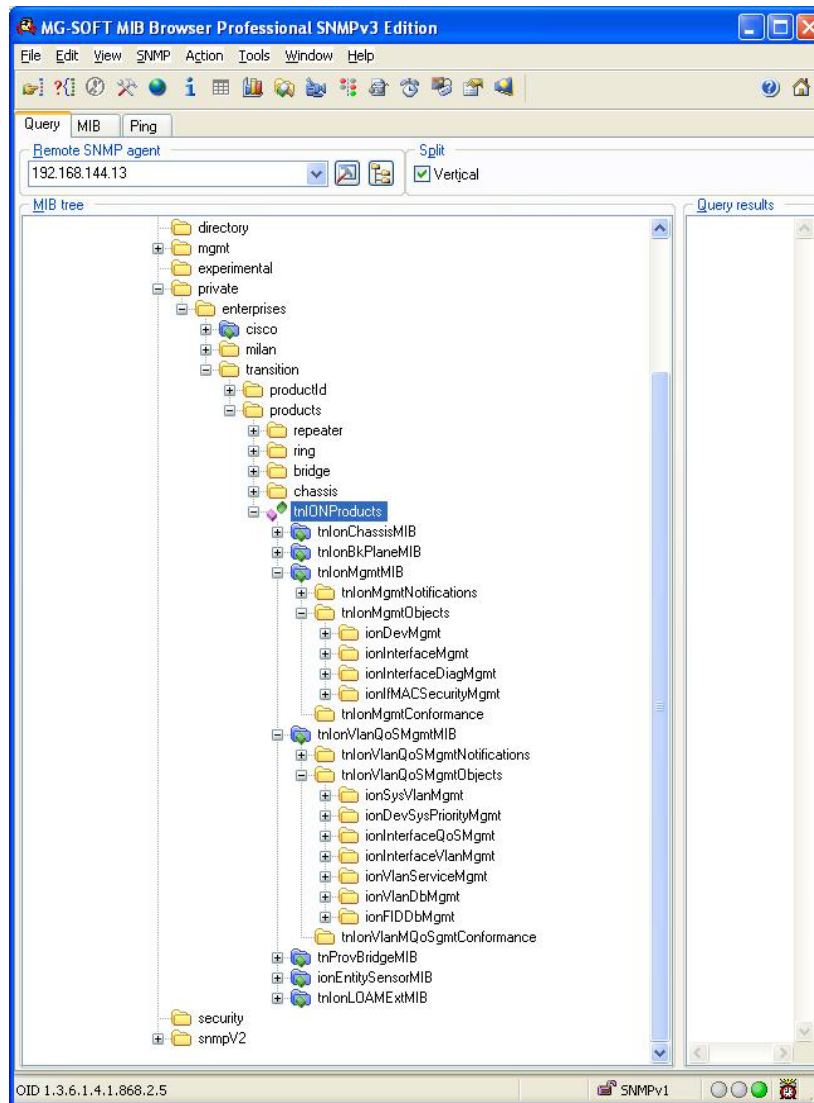
## Supported MIBs

The C3210 supports public (standard) and private Management Information Bases (MIBs). The C3210 provides complete management through the SNMP interface. It supports standard MIBs for management using SNMPv1/v2 as shown in the table below.

**Table 1: Supported MIBs**

#	MIB	RFC # or Private	Description
1	BRIDGE-MIB	RFC4188	Bridge MIB module for managing devices that support IEEE 802.1D
2	ENTITY-MIB	RFC 4133	MIB module for representing multiple logical entities supported by a single SNMP agent
3	ENTITY-SENSOR-MIB	RFC 3433	Defines Entity MIB extensions for physical sensors
4	EtherLike-MIB	RFC3635	Describe generic objects for Ethernet-like network interfaces
5	IANA-MAU-MIB	RFC 4836	Defines dot3MauType OBJECT-IDENTITIES and IANAifMauListBits, IANAifMauMediaAvailable, IANAifMauAutoNegCapBits, and IANAifJack-Type
6	IEEE8021-CFM-MIB	RFC ____	Connectivity Fault Management module for managing IEEE 802.1ag
7	IEEE8021-TC-MIB	RFC ____	Textual conventions used throughout the various IEEE 802.1 MIB modules
8	IF-MIB	RFC 2863	Describes generic objects for network interface sub-layers
9	MAU-MIB	RFC 4836	Management information for 802.3 MAUs
10	P-BRIDGE-MIB	RFC 4363	Module for managing Priority and Multicast Filtering
11	Q-BRIDGE-MIB	RFC 4363	Module for managing Virtual Bridged LANs
12	RFC1213-MIB (MIB-II)	RFC 1213	Defines the second version of the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets
13	RMON-MIB	RFC 1757	Defines objects for managing remote network monitoring devices (i.e., monitors or probes)
14	TRANSITION-SMI	Private	Lantronix Enterprise Structure of Management Information; assigns ION platform module identities
15	TRANSITION-TC	Private	Lantronix Inc MIB Textual Conventions module; defines textual conventions used in the Transition enterprise MIBs
16	TN-ION-BPC-MIB	Private	Lantronix, Inc. Enterprise MIB for Chassis Management.
17	TN-ION-CHASSIS-MIB	Private	Lantronix, Inc. Enterprise MIB for Chassis Management
18	TN-ION-MGMT-MIB	Private	Lantronix, Inc. Enterprise MIB for basic management of the ION Platform
19	TN-PROV-BRIDGE-MIB	Private	Lantronix, Inc. Enterprise MIB for IEEE Bridge provisioning, i.e., IEEE MAC/VLAN bridges
20	TN-ION-VLAN-MGMT-MIB	Private	Lantronix, Inc. Enterprise module for managing VLAN and QoS in ION platform products
21	TN-ION-ENTITY-SENSOR-MIB	Private	Lantronix, Inc. module for managing all ION power supply and fan modules)
22	ION-DEV-SYS-SNMPMGMT-MIB	Private	Lantronix Enterprise MIB for ION device SNMP management feature
23	ION-DEV-SYS-STATE-MIB	Private	Lantronix Enterprise MIB for ION device state
24	ION-DEV-SYS-TFTP-MIB	Private	Lantronix Enterprise MIB for ION device TFTP feature
25	ION-DEV-SYS-UPGRADER-MIB	Private	Lantronix Enterprise MIB for ION device upgrader feature

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



**Figure 1: 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 software downloads page at <https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/1844314274/Latest+firmware+for+the+C3210+Series> 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.

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 C3210 CLI Reference Manual, 33497.

## C3210 Models

The C3210 models are described below.

### Duplex Fiber Models and Simplex Fiber Models

C3210 products are available as chassis models. The models can include both standard and single-fiber models. Single fiber technology offers a 50% savings in fiber utilization. It is an attractive solution to maximize the usage of a limited number of fiber runs. In a traditional optical link, a fiber pair consists of two uni-directional strands. The single fiber technology multiplexes two optical wavelengths into a single strand fiber, so these devices are usually used in pairs. \*It is recommended these Single Fiber Models be used in pairs.

### Chassis Models (Cxxxx)

The ION Chassis models (also called slide-in-cards or SICs, or slide-in-modules) and managed devices have specific features and functions that are controlled via the ION Management Module. A network administrator can configure, monitor and troubleshoot ION slide-in-modules remotely via the ION Management Module.

An end-to-end fiber integration solution can be achieved by pairing the modules in a high density ION chassis with the modules in another ION chassis, or a Lantronix' Point System™ stand-alone media converter.

## Physical Specifications

The physical specifications for the chassis slide-in modules are described in the table below.

**Table 3: C3210 Model Specifications**

Dimensions	3.4" x 0.86" x 6.5" (86 mm x 22 mm x 165 mm)
MAC Filtering	1K MAC addresses
Power Input	Standalone: 12VDC @ 375mA SIC: Powered by the Chassis
Environment	0 to 50°C (32 to 122°F) operating; 5% - 95% humidity (non-condensing) 0 to 10,000 ft. altitude
Storage Temp	-40 to 85°C (-40 to 185°F)
Standards	IEEE 802.3, IEEE Std. 802.3ab, IEEE 802.3u, IEEE 802.3z, IEEE 802.3p, IEEE 802.3q
Data Rate	10/100/1000Mbps; Layer-2
Max Frame Size	10,240 Bytes (jumbo frame support)
DIP Switches	SW1: TP Auto-Negotiation.      SW2: TP Speed SW3: TP Duplex                      SW4: Link Pass Through SW5: Fiber Duplex                  SW6: Unused
HW/SW Jumpers	Hardware/Software mode, AutoCross™
Status LEDs	<b>PWR</b> (Power): ON = Connection to powered backplane <b>LACT</b> (Fiber Link): ON = Fiber link, Blinking = activity <b>UTP Duplex/Link</b> : Orange = half duplex link, Blinking = half duplex activity, Green = Full duplex link, Blinking = Full duplex activity. <b>Speed</b> : Off = 10Mbps operation (or no link), Orange = 100 Mbps operation, Green = 1000Mbps operation.
Power Consumption	3.6 Watts, 300mA @ 112VDC
Shipping Weight	1 lb. [.45 kg]
Regulatory Compliance	CISPR/EN55022 Class A, EN55024, EN61000, FCC Class A, CE Mark

## Documentation Conventions

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

**Table 4: Documentation Conventions**

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

## Related Manuals and Online Helps

A printed Documentation Postcard is shipped with each C3210. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface. For Lantronix Drivers, Firmware, Manuals, Product Notifications, Warranty Policy & Procedures, etc. go to the Lantronix [Technical Resource Center](#).

The ION system and related device manuals are listed below.

1. C3210 Systems CLI Reference Manual, 33497
2. ION Management Module (IONMM) User Guide, 33457
3. ION219-A 19-Slot Chassis Installation Guide, 33412
4. ION Dry Contact Relay (DCR) Kit Install Guide, 33422
5. IONPS-A AC Power Supply Install Guide, 33423
6. IONPS-D DC Power Supply Install Guide, 33424
7. IONADP Kit Install Guide (Point System Card Adapter for ION Chassis) 33413
8. E-MCR-05 Media Converter Rack User's Guide, 33392
9. ION NID Manuals (model specific)
10. SFP manuals (product specific)
11. Release Notes (software version specific)
12. Product Documentation Postcard, 33504

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.

## 2. Installation and System Setup

### General

This section describes how to install the C3210 and the procedures to access and initially set up the device through either a local serial interface (USB) or a remote Ethernet connection (Telnet session or Web interface).

### Installing the C3210 in the ION Chassis

The C3210 is a slide-in module that can only be installed in a Lantronix ION chassis (ION001, ION002, ION206, and ION219). For a complete list of ION platform products, go to the Lantronix [Technical Resource Center](#).

The following describes how to install the C3210 in the ION chassis.



**Caution:** Failure to wear a grounding device and observe electrostatic discharge precautions when installing the C3210 could result in damage or failure of the module.

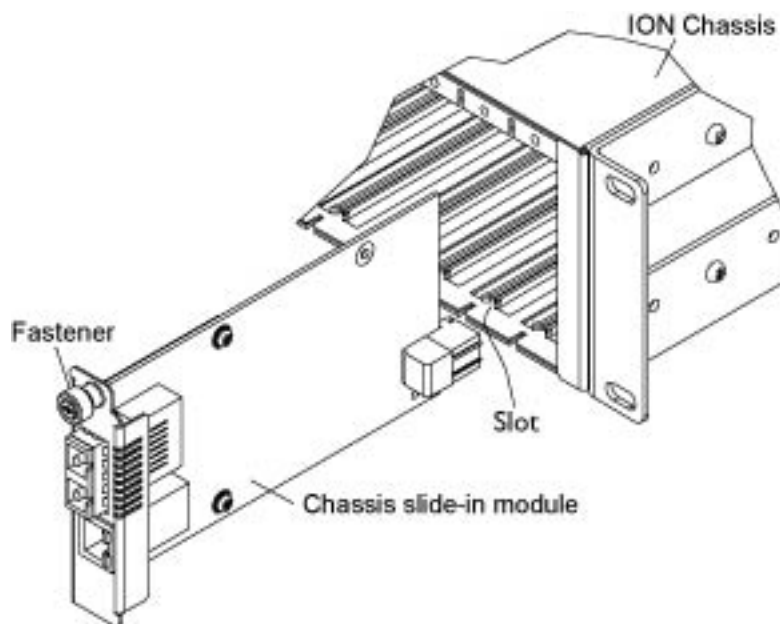


Figure 2: Chassis Installation



---

**IMPORTANT**

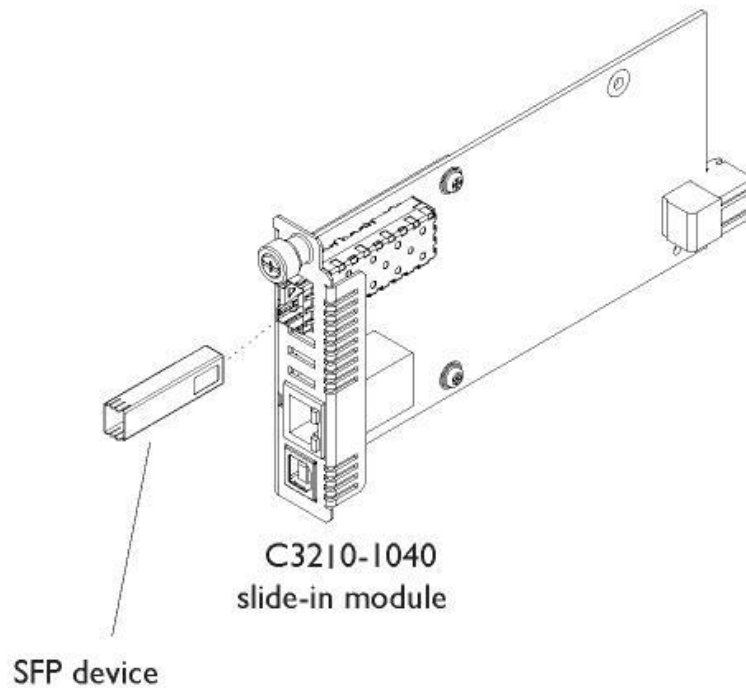
The C3210 slide-in cards are “hot swappable” devices, and can be installed with chassis power on.

---

1. Locate an empty slot in the ION System chassis.
2. Grasp the edges of the C3210 by its front panel.
3. Align the card with the upper and lower slot guides, and carefully insert the C3210 into the slot.
4. Firmly seat the C3210 against the chassis back panel.
5. Push in and rotate clockwise the panel fastener screw to secure the C3210 to the chassis (see [Figure 8: Chassis Installation](#) on the previous page).
6. Note that the card’s Power LED lights. See [Accessing the C3210](#).

## Installing SFPs

Some models allow you to install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection. The C3210-1040 has a single SFP port. See the SFP manual for important cautions and warnings. See Lantronix full line of SFP transceivers on Lantronix [SFP webpage](#).



**Figure 3: SFP Installation**

To install an SFP in the C3210:

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

## Connections and LEDs

The connections and LEDs resident on the various models are described below.

The C3210 connectors and LEDs are shown and described below.



**Figure 4: Model C3210 Connectors and LEDs**

The C3210-10xx connectors and LEDs are described in the table below.

**Table 5: Model C3210-10xx Connectors and LED Descriptions**

Connector/LED	Description
<b>1000Base-X</b> SFP port connector	Lets you install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection.  Used to connect the C3210 via fiber to another device (switch, router, media converter, etc.).
<b>10/100/1000</b> (Copper port) Network connectors	One connector for Ethernet 10/100Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either a remote Telnet session or the Web interface.
<b>PWR</b> (Power) LED	When lit, indicates that there is power to the C3210.
<b>LACT</b> (Link active) LED	Yellow – operation is 10 MBps, 10Base-T.  Green – operation is 100 MBps, 100Base-T.
<b>DUP</b> (Duplex) LED	When lit, indicates duplex mode: <ul style="list-style-type: none"><li>• Yellow – half-duplex</li><li>• Green – full duplex</li></ul> Blinking indicates link activity.

## Connecting the C3210 to the Standalone SGFEB10xx-120

Connect the C3210 to the unmanaged Point System SGFEB10xx-120 using fiber ports. If two fiber lines are supported, connect the local and remote device's primary lines together, and connect the secondary lines together. The C3210 can be managed when installed in a managed ION chassis.

## Accessing the C3210

The C3210 can be accessed through either a local serial interface via a USB connection or through an Ethernet network connection. The network connection can be done via a Telnet session or a Web graphical user interface (GUI).

### Access via Local Serial Interface (USB)

The C3210 can be connected to a local management station (PC) through a serial interface using a USB connection. The C3210 is controlled by entering command line interface (CLI) commands at the local management station. To use the serial interface (USB) the following is required:

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

---

### IMPORTANT

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

---

### Operating Systems Supported

The ION USB drivers are available at on the [Product Support](#) webpage (no logon required).

Windows® 7	Windows 7 x64	Windows XP® 32 bit
Windows 10	Windows 2003 32 bit	Windows Vista®
Windows Vista x64	Windows XP 64 bit	Windows 8

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

The x222x/x32xx provides a USB Type B connector that can be used as a virtual COM port for accessing the x222x/x32xx command line interface (CLI).

## ***Installing the USB Driver (Windows XP)***

---

### **IMPORTANT**

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

---

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

1. Extract the driver (from the provided CD or from the [website](#)) and place it in an accessible folder on the local drive of the PC.

2. Connect the C3210 to the USB port on the PC.

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

The *Welcome to the Found New Hardware Wizard* window displays.

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

The USB driver installation is complete. You must now configure access the C3210 via an Ethernet network.

### **Access via an Ethernet Network**

The C3210 can be managed remotely through the Ethernet network via either a Telnet session or the Web interface. Before this is possible, you must set up the IP configuration for the C3210.

---

### **IMPORTANT**

It is recommended that you initially set up the IP configuration through the serial interface (USB connection). See "[Performing Initial System Setup](#)" 6.

Otherwise, in order to communicate with the C3210 across the network for the first time, you must change the network settings (IP address, subnet mask and default gateway address) of your PC to coincide with the defaults of the C3210 (see "[Appendix B: Factory Defaults](#)"). Make note of the original settings for the PC as you will need to reset them after setting the IP configuration for the C3210.

---

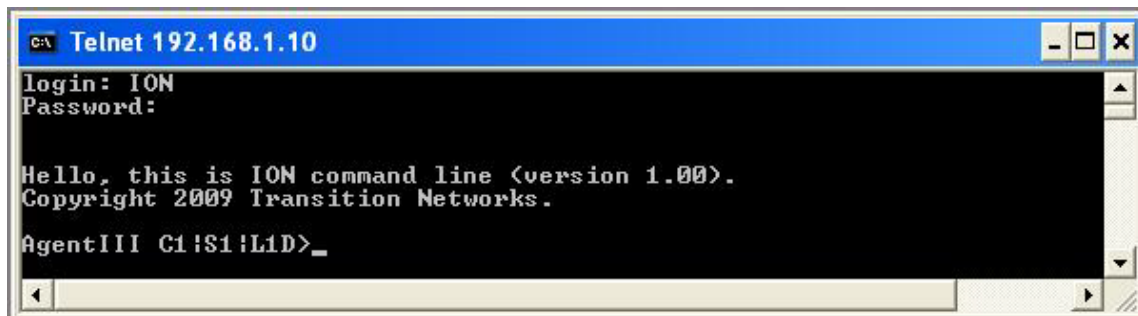
## Starting a Telnet Session

The C3210 can be controlled from a remote management station via a Telnet session over an Ethernet connection. The C3210 is controlled and configured through CLI commands. Use the following procedure to connect to and access the C3210 via a Telnet session.

1. Click **Start**.
2. Select **All Programs > Accessories**.
3. Click **Command Prompt**. The command prompt window displays.
4. At the command line type: **telnet <xx>** where:  
xx = IP address of the C3210
5. Press **Enter**. The login prompt displays.

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

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



10. Enter a **go** command to change the location for the command prompt. The **go** command format is:  
**go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] [l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d]**
11. Enter commands to set up the various configurations for the C3210. For configuration information, see [Section 4: Configuration](#). For a description of all available CLI commands see the *ION Systems CLI Reference Manual*, 33473.

**Note:** If required by your organization's security policies and procedures, use the CLI command **set community write=<xx>** to change the default password. See the *ION Systems CLI Reference Manual*, 33473.

## Terminating a Telnet Session

To terminate the Telnet session:

1. Type **q(uit)**.
2. Press the **Enter** key.

## Web Browsers Supported

The ION system supports the latest version of most popular web browsers. ~~including:-~~

- ~~• Firefox (Mozilla Firefox)~~
- ~~• Internet Explorer (IE)~~
- ~~• Google Chrome~~

## Starting the Web Interface

The C3210 can be controlled and configured from a remote management station via a Web graphical user interface (GUI) over an Ethernet connection. Information is entered into fields on the various screens of the interface. **Note:** fields that have a grey background cannot be modified.

A Web session can be used to connect to and set up the C3210.

---

## IMPORTANT

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

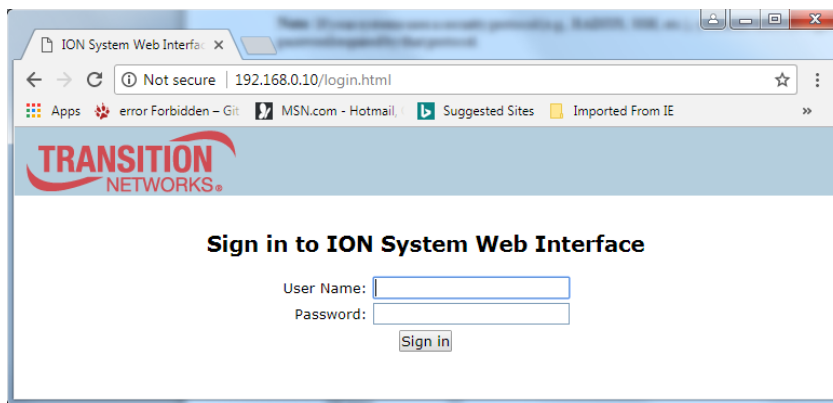
To sign in to the C3210 via the Web:

1. Open a web browser.



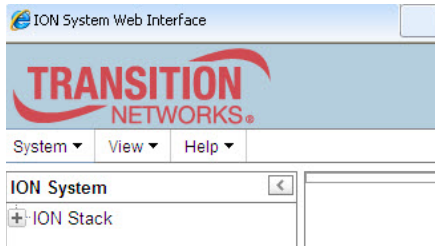
2. In the address (URL) block, type the IP address of the C3210 (the default address is 192.168.1.10).
3. Click **Go** or press **Enter**.

The ION System sign in screen displays.

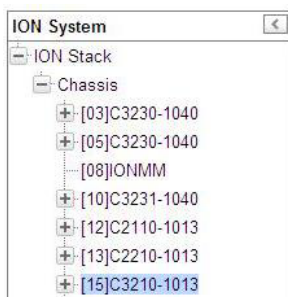


**Note:** If your system uses a security protocol (e.g., RADIUS, SSH, etc.), you must enter the login and password required by that protocol.

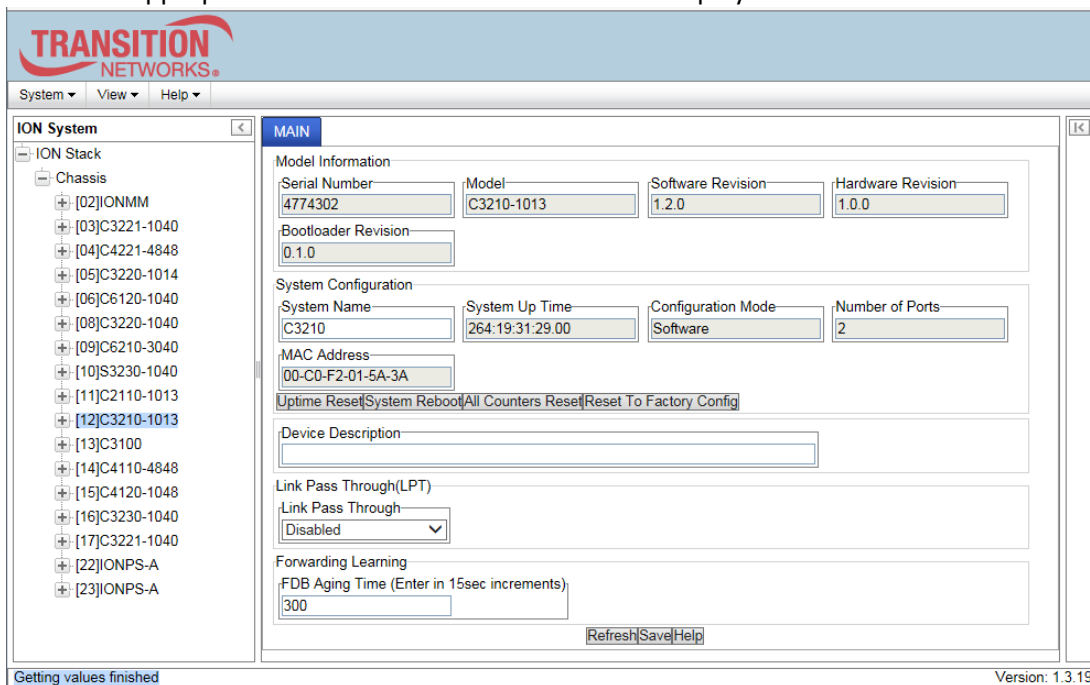
1. Type the System name (the default is **ION**). **Note:** the System name is case sensitive - all upper case.
2. Type the password (the default is **private**). **Note:** the password is case sensitive - all lower case.
3. Click **Sign in** or press **Enter**. The opening screen displays.



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



6. Select the appropriate model C3210. The **MAIN** screen displays for the selected C3210.



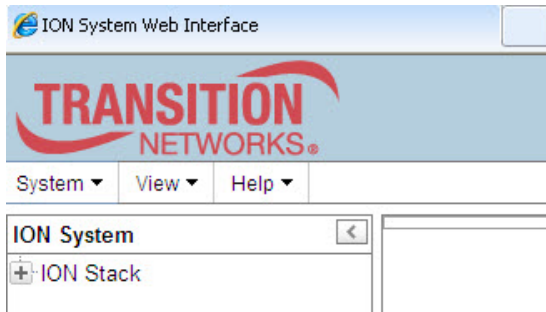
7. You can use the various tabs to configure the system, devices and ports. For configuration information, see "[Section 4: Configuration](#)".



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

### ***Terminating the Web Interface***

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



1. Click the **System** dropdown.
2. Click **Sign out**.



The ION sign in screen displays.

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

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

## 3. Management Methods

### General

The C3210s are managed either directly or through the IONMM. Whether the C3210 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 C3210 can be remotely managed directly (i.e., not through IONMM). This enables administrators to monitor and configure remote stand-alone C3210s 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 (C3210) 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:

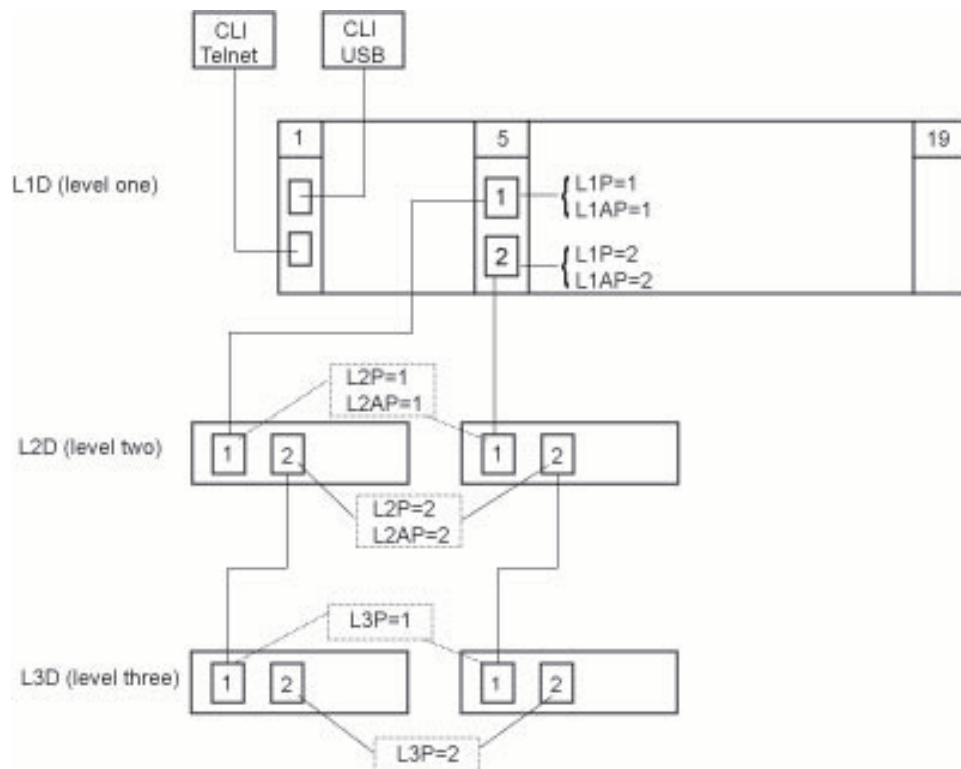
```
AgentIII C1|S7|L1D>
```

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 5: CLI Location Hierarchy**

In the figure above, 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 **can not** be managed by the IONMM.
- Attachment port – These are also ports on a specified device; they are labeled L1AP= and L2AP= and indicate an attachment point for another ION family device that **can** be managed by the IONMM.

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

### **Example 1**

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

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

The resulting command line prompt would be:

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

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

### **Example 2**

In the CLI location hierarchy, to go to device L2D in the network topology shown in Figure 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.

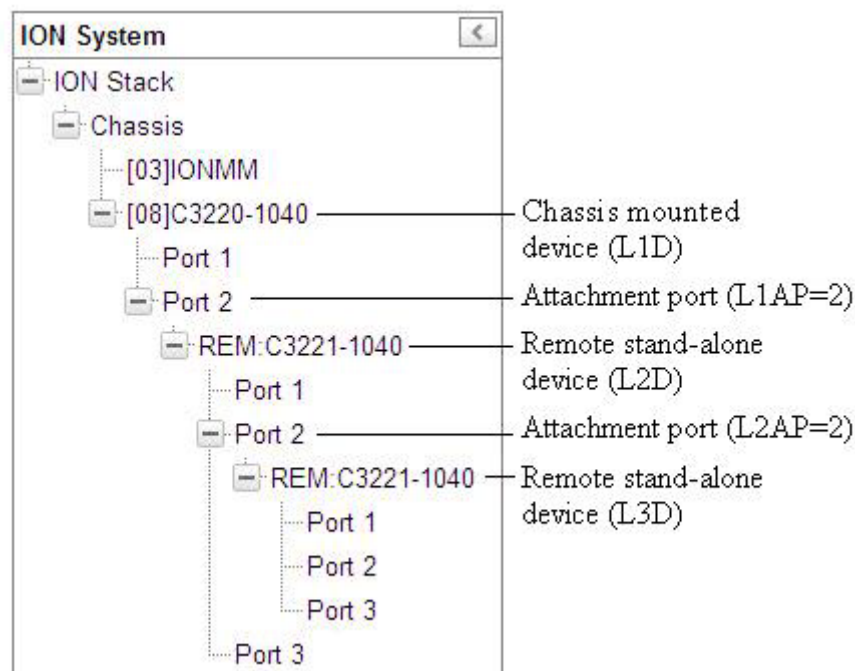
The following describes the procedure for using CLI commands to manage the C3210s.

1. Access the C3210 through either a USB connection.
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 C3210 using the appropriate commands. For a complete list of the available commands, see the *C3210 CLI Reference Manual, 33497*.
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 C3210 through the Web interface (see “[Starting the Web Interface](#)”).



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

## Direct Managed Devices

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

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

### 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 l1p=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 l1d
```

The resulting command line prompt would be:

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

## Managing Standalone Modules via the IONMM Web Interface

1. Access the C3210 through the Web interface (see “Starting the Web Interface”).
2. Click the plus sign **[+]** next to **ION Stack** to unfold the "ION Stack" node in the left tree view if not already done.
3. Click the plus sign **[+]** next to **Chassis** and click the plus sign **[+]** next to a module.

The screenshot displays the IONMM Web Interface. On the left, a tree view under 'ION System' shows 'ION Stack' expanded, with 'Chassis' and a list of modules. Module '[12]C3210-1013' is selected. The main area, titled 'MAIN', shows configuration fields for this module. The 'Model Information' section includes fields for Serial Number (4774302), Model (C3210-1013), Software Revision (1.2.0), and Hardware Revision (1.0.0). The 'System Configuration' section includes fields for System Name (C3210), System Up Time (264:19:31:29.00), Configuration Mode (Software), and Number of Ports (2). Below these are fields for MAC Address (00-C0-F2-01-5A-3A) and buttons for Uptime Reset, System Reboot, All Counters Reset, and Reset To Factory Config. The 'Link Pass Through (LPT)' section has a dropdown menu set to 'Disabled'. The 'Forwarding Learning' section has a field for FDB Aging Time (300). At the bottom right are buttons for Refresh, Save, and Help. The status bar at the bottom left says 'Getting values finished' and the bottom right says 'Version: 1.3.19'.

4. Click on the module or port to be managed (e.g., the C3210-1013 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 6: System-Level Menu Description**

Dropdown / Tab	Description
<b>ION System pane</b>	<p><b>ION Stack</b> - consists of one chassis or one standalone device. The Stack Members table lists the Stack's chassis and its type.</p> <p><b>Chassis</b> - 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"> <li>* Serial Number - The serial number of the chassis itself. Individual C3210s also have their own serial numbers.</li> <li>* Model Name - The exact model name of this device. When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number.</li> <li>* Software Revision, Hardware Revision, and Bootloader Revision.</li> <li>* Chassis Members table - lists local physical components in slots 1 to 19.</li> </ul> <p><b>Device</b> – provides tabs and sub-tabs for the IONMM and C3210s in the ION system.</p> <p><b>Port</b> - provides tabs and sub-tabs for a selected C3210 port.</p>
<b>System</b> Dropdown	Sign out.
<b>View</b> Dropdown	Refresh.
<b>Help</b> Dropdown	Online Help, ION Product Home Page, About ION System Web Interface.
<b>MAIN</b> Tab	<p><u>Sections</u>: Model Information, System Configuration, Device Description, Link Pass Through (LPT), and Forwarding Learning sections.</p> <p><u>Buttons</u>: Uptime Reset, System Reboot, All Counters Reset, and 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 7: Port-Level Menu Description**

Tab	Description
<b>MAIN</b> Tab	<p><u>Sections:</u> Circuit ID, Port Configuration, Auto Negotiation Settings, Capabilities Advertised, Port Forward Management Port Forward Management, and Virtual Cable Test (VCT).</p> <p><u>Buttons:</u> <i>Virtual Cable Test</i>, <i>Refresh</i>, <i>Save</i>, and <i>Help</i>.</p>
<b>ADVANCED</b> Tab	<p><u>Sections:</u> Bandwidth Allocation, MAC Security, VLAN Forwarding Rules, Priority Forwarding Rules, VLAN Tag Management, and User Priority.</p> <p><u>Buttons:</u> <i>Refresh</i>, <i>Save</i>, and <i>Help</i>.</p>
<b>COUNTERS</b> Tab	<p><u>Sections:</u> RMON Counters, Port Counter Received, Port Counters Sent, and Dot3 Statistics.</p> <p><u>Buttons:</u> <i>Reset Counters</i>, <i>Refresh</i>, and <i>Help</i>.</p>
<b>DMI</b> Tab (Port 2 only)	<p><u>Sections:</u> Interface Characteristics, Diagnostic Monitoring, Supported Media Length.</p> <p>The DMI (Diagnostic Maintenance Interface) function displays C3210 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See “<a href="#">DMI (Diagnostic Maintenance Interface) Parameters</a>” for more information.</p> <p><b>Note:</b> not all C3210 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 C3210 model that does not support DMI, the message “<i>The DMI feature is not supported on current port.</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 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:

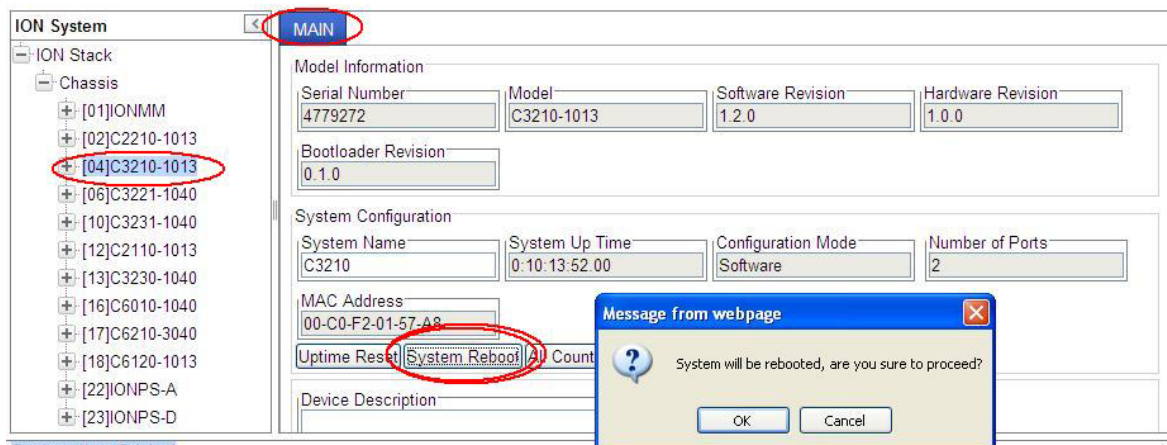
- Table 15: [Back Up and Restore File Content and Location](#)
- Table 16: [File Status after a Reset to Factory Defaults](#)
- Table 17: [File Content and Location after a System Reboot](#)
- Table 18: [File Content and Location after a Firmware Upgrade](#)



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

## System Reboot

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



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

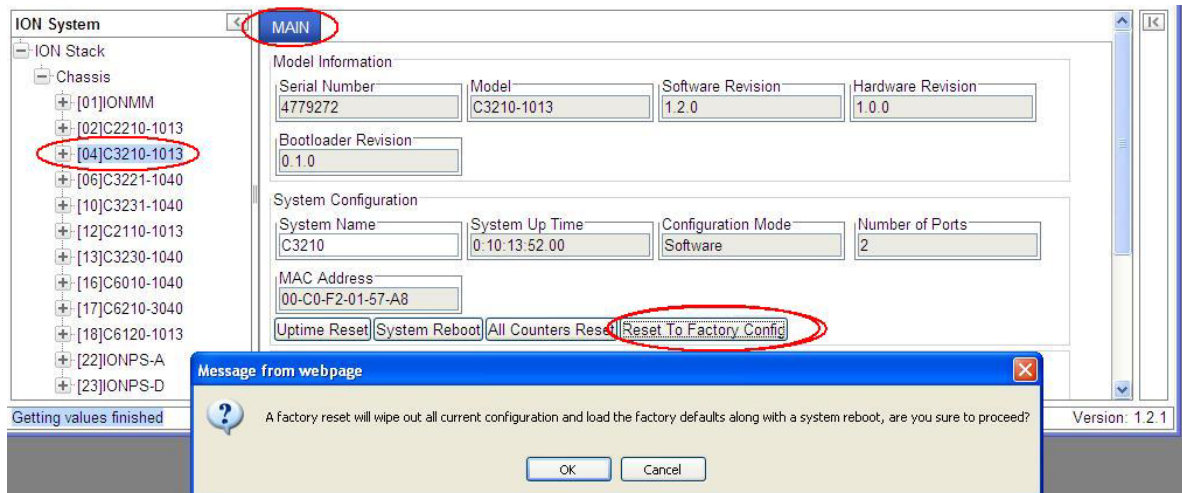
Press the **OK** button to clear the webpage message and begin the reboot process.

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

Note that a System Reboot can take several minutes.

## Reset To Factory Config

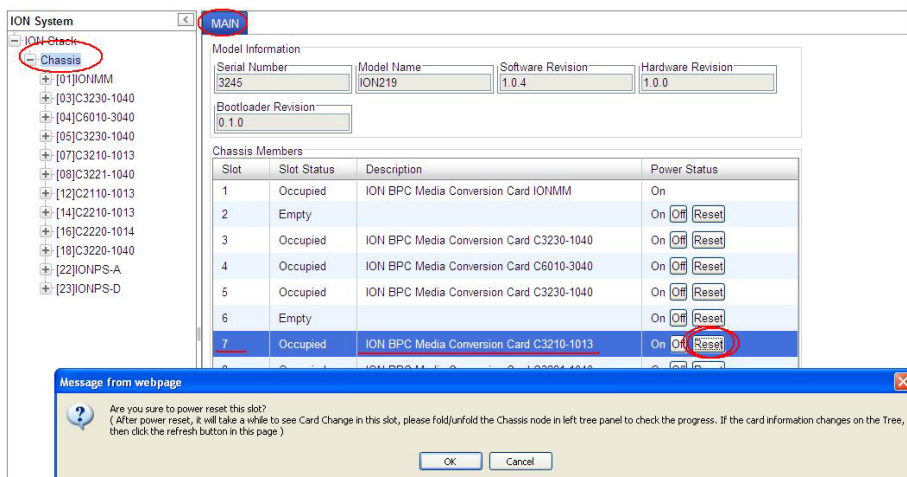
Clicking the **Reset To Factory Config** button resets the entire system configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the factory default settings. The message “A factory reset will wipe out all current configuration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

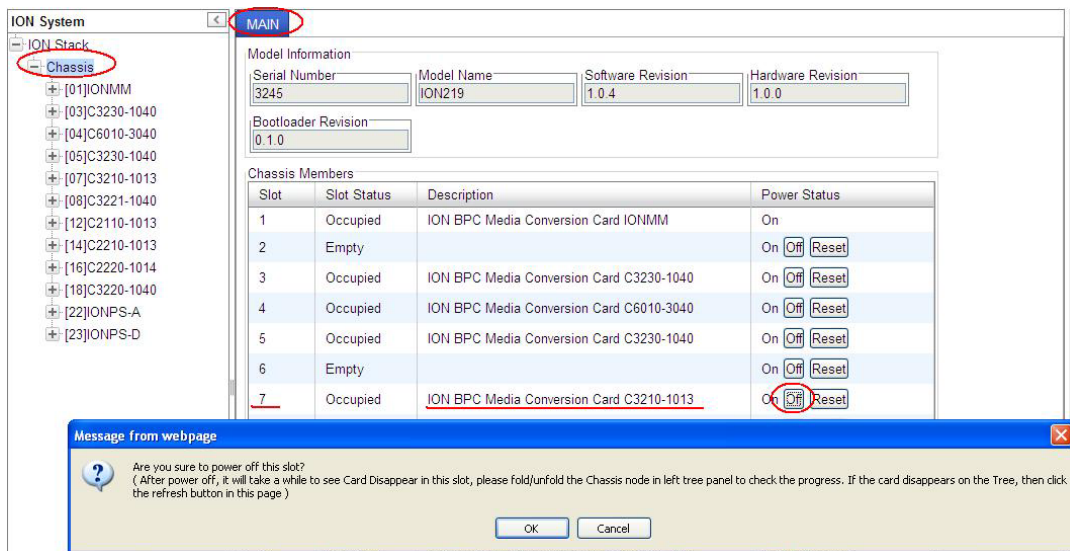


After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page.

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.

## 4 Configuration

### General

After the C3210 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 C3210.

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 *C3210 CLI Reference Manual, 33497*.

The operating characteristics that can be defined for the C3210 are:

- System setup
- Features
  - Ethernet Interface (*AutoCross*, Auto negotiation / Capabilities Advertised, Bandwidth allocation, Speed, Duplex mode)
  - Flow control (Pause frames/back pressure)
  - Forward Learning (FDB Aging)
  - Port Forward Management
  - IP/IEEE priority remapping
  - Link pass through (LPT)
  - Device ID / Circuit ID
  - Virtual Cable Test
- Security
  - Media access control (MAC) security
  - VLAN Forwarding and VLAN Tag 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 C3210
- 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 C3210 through either a USB connection.
2. Type **set system name=NAME**, where NAME is the new system name, and press **Enter**.

For example:

```
C1|S5|L1D>set system name=C3210-1013
```

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

```
Agent III C1|S6|L1D>show card info
System name:      C3210
Uptime:           5 days, 20:02:25
MAC:              00-c0-f2-01-57-a8
Port number:      2
Serial number:    4779272
Config mode:      software
Software:         1.2.0
Bootloader:       0.1.0
Hardware:         1.0.0
Agent III C1|S6|L1D>
```

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

## System Configuration – Web Method

1. Access the C3210 through the Web interface.
2. At the device's **MAIN** tab, locate the **System Configuration** section.

The screenshot displays the ION System web interface. On the left, a tree view under 'ION Stack' shows a list of components, with '[04]C3210-1013' highlighted by a red circle. The main panel is titled 'MAIN' and contains two sections: 'Model Information' and 'System Configuration'. The 'Model Information' section includes fields for 'Serial Number' (4779272), 'Model' (C3210-1013), 'Software Revision' (1.2.0), and 'Hardware Revision' (1.0.0). The 'System Configuration' section includes fields for 'System Name' (C3210), 'System Up Time' (0:10:13:52:00), 'Configuration Mode' (Software), and 'Number of Ports' (2). A red oval highlights the 'System Configuration' section. At the bottom of the 'System Configuration' section, there are four buttons: 'Uptime Reset', 'System Reboot', 'All Counters Reset', and 'Reset To Factory Config'.

3. In the **System Name** field, enter the name and for the C3210. The name can be alphabetic, numeric or a combination, but can not contain any spaces between the characters.
4. Scroll to the bottom and click **Save**.

## Device Description Configuration

The x222x/x32xx 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 x222x/x32xx using either the CLI or Web method.

### Device Description– CLI Method

1. Access the NID through either a USB connection.
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|S9|L1P1>set device description  zzzzzzz
Error: this command should be executed on a device!
Agent III C1|S9|L1P1>go l1d
Agent III C1|S9|L1D>set device description  zzzzzzz
Agent III C1|S9|L1D>show device description
Device description: zzzzzzz
Agent III C1|S9|L1D>
```



## Device Description Config – Web Method

1. Access the x222x/x32xx through the Web interface.
2. At the x222x/x32xx **MAIN** tab, locate the **Device Description** section.

ION System

MAIN

ION Stack

Chassis

- [01]IONMM
- [02]C3210-1013
- [04]C3210-1013
- [06]C3221-1040
- [10]C3231-1040
- [12]C2110-1013
- [13]C3230-1040
- [16]C6010-1040
- [17]C6210-3040
- [18]C6120-1013
- [22]IONPS-A
- [23]IONPS-D

Model Information

Serial Number	Model	Software Revision	Hardware Revision
4779272	C3210-1013	1.2.0	1.0.0

Bootloader Revision

0.1.0

System Configuration

System Name	System Up Time	Configuration Mode	Number of Ports
C3210	0:10:13:52:00	Software	2

MAC Address

00-C0-F2-01-57-A8

Uptime Reset System Reboot All Counters Reset Reset To Factory Config

Device Description

3. Enter the Device Description of up to 64 bytes for the device.

ION System

MAIN

ION Stack

Chassis

- [01]IONMM
- [02]C2210-1013
- [04]C3210-1013
- [06]C3221-1040
- [10]C3231-1040
- [12]C2110-1013
- [13]C3230-1040
- [16]C6010-1040
- [17]C6210-3040
- [18]C6120-1013
- [22]IONPS-A
- [23]IONPS-D

Model Information

Serial Number	Model	Software Revision	Hardware Revision
4779272	C3210-1013	1.2.0	1.0.0

Bootloader Revision

0.1.0

System Configuration

System Name	System Up Time	Configuration Mode	Number of Ports
C3210	0:10:13:52:00	Software	2

MAC Address

00-C0-F2-01-57-A8

Uptime Reset System Reboot All Counters Reset Reset To Factory Config

Device Description

XX/YYYY/000000/111/CC/SEG

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

If you enter more than 64 characters for the Circuit ID and then click **Save**, the characters entered display in red, and the message *"Invalid input found!"* displays in the lower left corner of the Web interface.

To recover:

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

## Circuit ID Configuration

The x222x/x32xx 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 x222x/x32xx using either the CLI or Web method.

### Circuit ID Config – CLI Method

1. Access the NID through either a USB connection.
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>
```

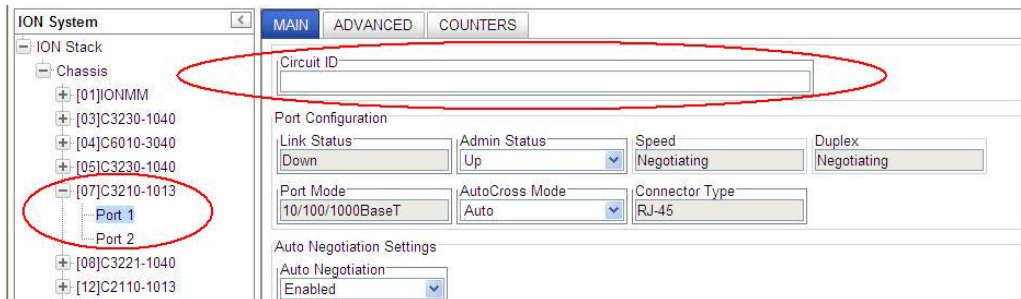
5. At the each of the device port's command prompts, enter the Circuit ID as in step 2 and 3.
6. At the each of the device port's command prompts, verify the Circuit ID setting as in step 4.  
For example:

```
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>
```

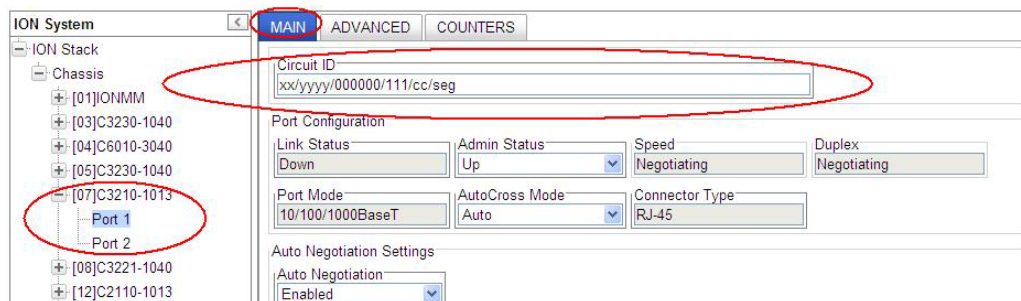
## Circuit ID Config – Web Method

1. Access the C3210 through the Web interface.
2. Select the appropriate port and locate the **Circuit ID** field.



The screenshot shows the ION System web interface. On the left, a tree view under 'ION Stack' shows 'Chassis' expanded, with '[07]C3210-1013' selected and 'Port 1' highlighted. On the right, the 'MAIN' tab is active, and the 'Circuit ID' field is highlighted with a red oval. Below it, the 'Port Configuration' section shows 'Link Status' as 'Down', 'Admin Status' as 'Up', 'Speed' as 'Negotiating', 'Duplex' as 'Negotiating', 'Port Mode' as '10/100/1000BaseT', 'AutoCross Mode' as 'Auto', and 'Connector Type' as 'RJ-45'. The 'Auto Negotiation Settings' section shows 'Auto Negotiation' as 'Enabled'.

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



The screenshot shows the ION System web interface with the 'Circuit ID' field populated with the sample text 'xx/yyyy/000000/111/cc/seg'. The 'MAIN' tab is active, and the 'Circuit ID' field is highlighted with a red oval. The 'Port Configuration' and 'Auto Negotiation Settings' sections are visible below it.

4. Click **Refresh** to update screen information.
5. Repeat steps 2 -4 for each port as required.
6. Click **Save** when done.

If you enter more than 64 characters for the Circuit ID and then click **Save**, the characters entered display in red, and the message *"Invalid input found!"* displays in the lower left corner of the Web interface.

To recover:

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

## Link Pass Through (LPT) Configuration

The C3210 supports LPT (Link Pass Through) at the device level.

The LPT feature can be configured in the C3210 using either the CLI or Web method.

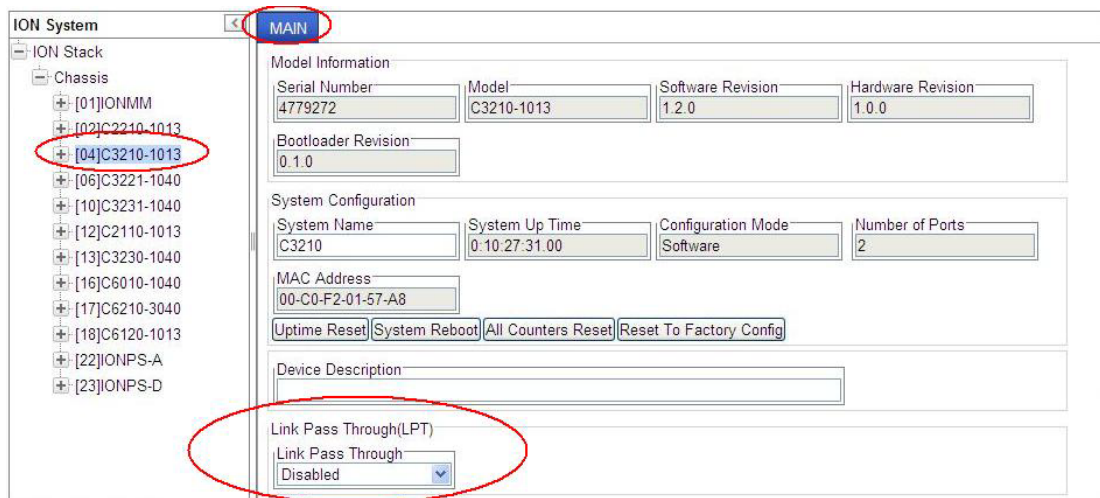
### Link Pass Through (LPT) Config – CLI Method

1. Access the C3210 through a USB connection.
2. At the device's command prompt type: **set lpt state** =xx, where xx= <enable or disable>.
3. Press the **Enter** key.
4. Type **set lpt monitor-port**=xx, where xx is the port that performs LPT monitoring.
5. Press the **Enter** key.
6. Verify the LPT setting. Type **show lpt config** and press **Enter**. For example:

```
C1|S8|L1D>show lpt config
Link pass through configuration:
-----
Link pass through state:                enable
Transparent link pass through state:    notSupported
Selective link pass through state:      notSupported
Link pass through monitor port:        3
Remote fault detect state:             notSupported
C1|S8|L1D>
```

### Link Pass Through (LPT) Config – Web Method

1. Access the C3210 through the Web interface.
2. At the **MAIN** tab, locate the **Link Pass Through (LPT)** section.



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

## Configuring 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 C3210 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:

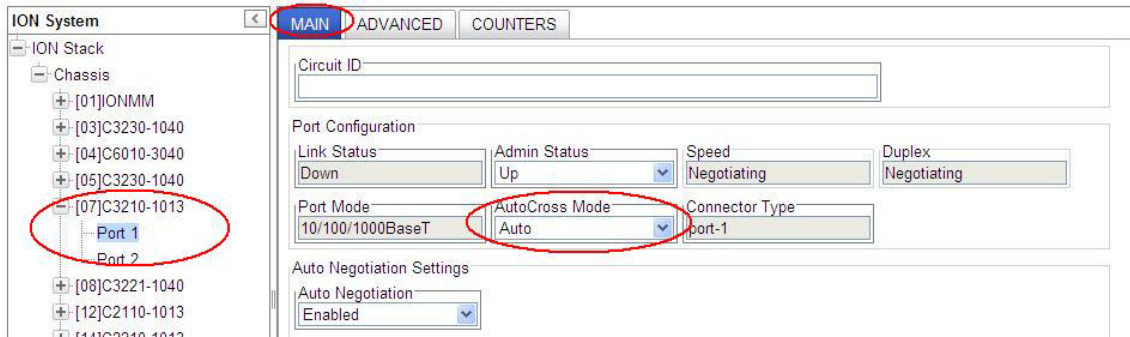
- This feature is defined on a port level; depending on the physical connector it is not applicable for all ports.
- Lantronix recommends leaving *AutoCross* in default mode, **Auto**.

### AutoCross Config – CLI Method

1. Access the C3210 through a USB connection.
2. At the device port's command line, type: **set ether autocross=xx** where:  
xx = cable type. Valid choices are:
  - **Auto** – hardware will automatically correct errors in cable selection.
  - **MDI** – transmit pair on one end of the cable is connected to the receive pair on the other end.
  - **MDIX** – cross over cable is used.
3. Press **Enter**.

## AutoCross Config – Web Method

1. Access the C3210 through the Web interface.
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).
  - **MDI** – the transmit pair on one end of the cable is connected to the receive pair on the other end.
  - **MDIX** – a cross over cable is used.

## Configuring 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
- duplex
- pause capability (whether Pause frames are supported)

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 can not 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. The pause default value for a copper port is “disabled”.

### 10/100/1000BaseT Port – CLI Method

1. Access the C3210 through a USB connection.
2. At the command line, type: **set ether autoneg state=xx** where:  
**xx** = **enable** or **disable**
3. Press **Enter**.
4. If Auto negotiation is enabled, go to step 5.  
If Auto negotiation is disabled, go to step 9
5. Set the advertised speed/duplex capabilities; type: **set ether adv-cap** where:  
**xx** = advertised speed capability; valid choices are:
  - **10TFD** (TP port 10 Mbps full duplex)
  - **10THD** (TP port 10 Mbps half-duplex)
  - **100TFD** (TP port 100 Mbps full duplex)
  - **100THD** (TP port 100 Mbps half-duplex)
  - **1000TFD** (TP port 1000 Mbps full duplex)
  - **1000THD** (TP port 1000 Mbps half-duplex)
  - **1000XFD** (fiber port 1000 Mbps full duplex)
  - **1000XHD** (fiber port 1000 Mbps half-duplex)

To specify more than one capability use a plus sign (+) between entries (e.g., adv-cap=10TFD+100TFDI+1000THD)

6. Press **Enter**.

7. Set the advertised pause frame capability; type: **set ether pause=xx** where:

**xx** = advertised pause capability; valid choices are:

- **nopause** (the port will advertise that it has no pause capabilities)
- **apause** (asymmetric; the port will advertise that it can only transmit pause frames)
- **bpause** (asym/sym; the port will advertise that it supports both asymmetric and symmetric capabilities (not supported on all models))
- **pause** (the port will advertise it has pause capability)
- **spause** (symmetric; the port will advertise that it can transmit and receive pause frames) (not supported on all models)

8. Press **Enter**.

9. Set the speed of this port; type: **set ether speed=xx** where:

**xx** = speed setting; valid choices are:

- **10M**
- **100M**
- **1000M**

10. Press **Enter**.

11. Set the duplex of this port; type: **set ether duplex=xx** where:

**xx** = duplex setting; valid choices are:

- **full**
- **half**

12. Press **Enter**.



13. Verify the configuration has been set. Type: **show ether config** and press **Enter**. The current Ethernet configuration displays. For example:

```
Agent III C1|S6|L1P1>show ether config
Port-11013
TP port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 RJ-45
PHY operation mode:        phy10-100-1000BaseT
Speed:                     Negotiating
Duplex:                    Negotiating
Autocross:                 auto
PHY mode change cap:       false

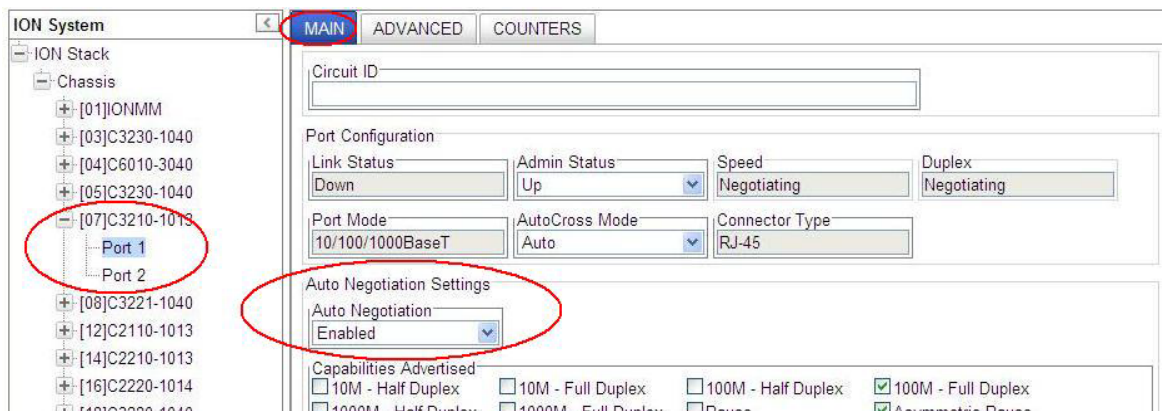
AutoNeg admin state:       enable
Advertisement:
Capability:                 10THD+10TFD+100THD+100TFD+1000THD+1000TFD
Pause:                      nopause
Agent III C1|S6|L1P1>

Agent III C1|S6|L1P1>go l1p=2
Agent III C1|S6|L1P2>show ether config
Port-21013
FIBER port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 SC Multimode Fiber
PHY operation mode:        phy1000BaseX
Speed:                     Negotiating
Duplex:                    Negotiating
PHY mode change cap:       false

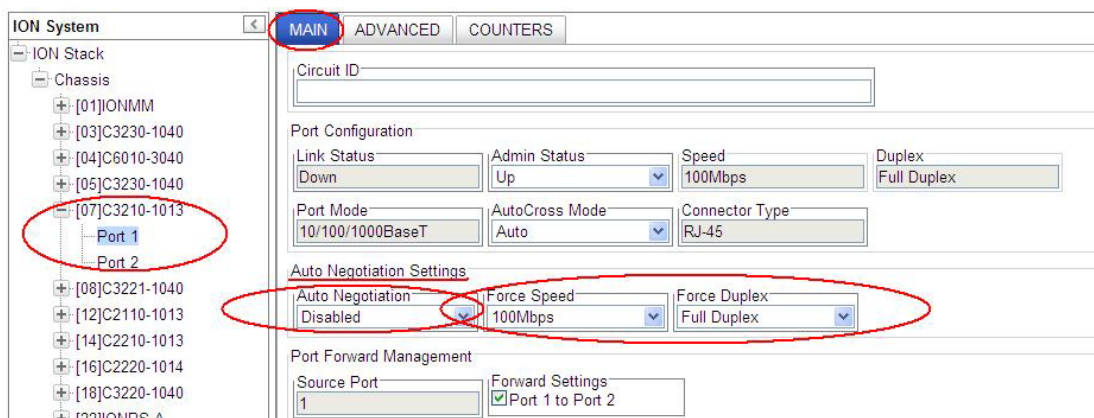
AutoNeg admin state:       enable
Advertisement:
Capability:                 1000XHD+1000XFD
Pause:                      nopause
Agent III C1|S6|L1P2>
```

## 10/100/1000BaseT Port – Web Method

1. Access the C3210 through the Web interface.
2. Select the appropriate port.
3. Locate the **Auto Negotiation Settings** section on the **MAIN** tab.



4. In the **Auto Negotiation** field, select whether this feature is enabled or disabled.
5. If **Auto Negotiation** is set to **Enabled**, in the **Capabilities Advertised** field, select:
  - the speed and duplex settings to be advertised to other devices
  - the type of pause frames supported on this port (**Pause** and/or **Asymmetric Pause**)
6. If you want to manually force speed and duplex settings, set **Auto Negotiation** to **Disabled**, click **Save**, and then select:
  - the port's operating speed,
  - the port's duplex mode of operation.



7. Click **Save** when done.

## Set Ethernet Port Speed / Duplex Mode (Force Speed / Duplex Mode)

Disabling the auto negotiate feature lets you 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.

A port's Ethernet port speed and Duplex mode can be configured in the C3210 using either the CLI or Web method.

### Set Ethernet Port Speed / Duplex Mode – 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 C3210 through either a USB connection or a Telnet session.
2. At the command line, type: **set ether autoneg state disable** and press **Enter**.
3. Set the speed of this port; type: **set ether speed=xx** where:  
    **xx** = speed setting; valid choices are:
  - **10M**
  - **100M**
  - **1000M**
4. Press **Enter**.
5. Set the Duplex mode for this port; type: **set ether duplex=xx** where:  
    **xx** = duplex setting; valid choices are:
  - **full**
  - **half**
6. Press **Enter**.

7. Verify the configuration has been set. Type: **show ether config** and press **Enter**.  
The Ethernet configuration displays. The first example below show a TP port, the second example shows a Fiber Port:

```
Agent III C1|S6|L1P1>show ether config
Port-11013
TP port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 RJ-45
PHY operation mode:        phy10-100-1000BaseT
Speed:                    Negotiating
Duplex:                   Negotiating
Autocross:                auto
PHY mode change cap:      false

AutoNeg admin state:      enable
Advertisement:
Capability:                10THD+10TFD+100THD+100TFD+1000THD+1000TFD
Pause:                    nopause
Agent III C1|S6|L1P1>go l1p=2
Agent III C1|S6|L1P2>show ether config
Port-21013
FIBER port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 SC Multimode Fiber
PHY operation mode:        phy1000BaseX
Speed:                    Negotiating
Duplex:                   Negotiating
PHY mode change cap:      false

AutoNeg admin state:      enable
Advertisement:
Capability:                1000XHD+1000XFD
Pause:                    nopause
Agent III C1|S6|L1P2>
```

## Set Ethernet Port Speed / Duplex Mode – 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 C3210 through the Web interface.
2. Select the appropriate port.
3. Locate the **Auto Negotiation Settings** section on the port's **MAIN** tab.

The screenshot shows the ION System web interface. The 'MAIN' tab is selected. In the left sidebar, the tree structure shows 'ION Stack' > 'Chassis' > '[07]C3210-1013' > 'Port 1'. The 'Port 1' item is highlighted. The main content area shows the configuration for Port 1. The 'Auto Negotiation Settings' section is circled in red, showing 'Auto Negotiation' set to 'Disabled', 'Force Speed' set to '100Mbps', and 'Force Duplex' set to 'Full Duplex'. Other sections like 'Port Configuration' and 'Port Forward Management' are also visible.

8. Set **Auto Negotiation** to **Disabled**.
9. In the **Force Speed** field, select the copper port's Ethernet operating speed (10M | 100M). The default is 10 Mbps.
10. In the **Force Duplex** field, select the port's Duplex mode of operation (Half Duplex | Full Duplex). The default is Full Duplex.
11. Click **Save**.

## Bandwidth Allocation / Rate Limiting

The C3210's Bandwidth Allocation (Rate Limiting) can be configured to limit both Ingress bandwidth and Egress bandwidth. If so configured, traffic at rates over this CIR (Committed Information Rate) is discarded. Note that these limits cannot be set faster than the port speed.

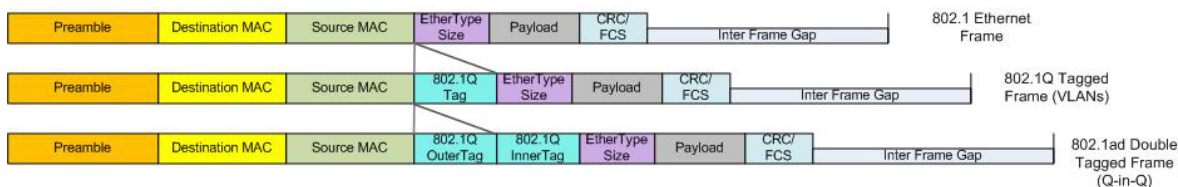
Bandwidth Allocation / Rate Limiting can be configured in the C3210 using either the CLI or Web method.

### Set Bandwidth Allocation / Rate Limiting – CLI Method

1. Access the C3210 through either a USB connection or a Telnet session.
2. At the command line, define which transmission layer is to be counted when determining the rate limit. Type **set bw alloc-type={countAllLayer1 | countAllLayer2 | countAllLayer3}**. The default is Count all Layer 1 bytes.

- **Counts All Layer 1:** (the default): in determining the rate limit, this selection counts the following bytes in a frame: Preamble (8 Bytes) + DA to CRC + Inter Frame Gap (12 bytes).
- **Counts All Layer 2:** in determining the rate limit, this selection counts the bytes in a frame from the DA to the CRC in determining the rate limit.
- **Counts All Layer 3:** in determining the rate limit, this selection counts these bytes in a frame:
  - from the DA (Destination MAC Address) to the CRC (18 bytes if untagged)
  - from the DA (Destination MAC Address) to the CRC (22 bytes if tagged)

**Note:** The Counts All Layer 3 selection will skip the Ethernet header, the CRC, and Tags (if any tags exist).



3. Press **Enter**.
4. Define the ingress and egress rate limits of the port. Type **set irate=<xx> erate=<yy>** where:
  - xx** = In-rate: Ingress rate in kbps
  - yy** = Egress-rate: Egress rate in kbps

The valid selections for irate (ingress) and egress-rate (erate) are:

**On 1000M port:** Unlimited, 1M, 2M, 3M, 4M, 6M, 8M, 10M, 20M, 30M, 40M, 50M, 60M, 70M, 80M, 100M, 200M, 300M, 400M, 500M, 600M, 700M, 800M, and 900M bps.

**On 100M port:** Unlimited, 1M, 2M, 3M, 4M, 6M, 8M, 10M, 20M, 30M, 40M, 50M, 60M, 70M, and 80M bps.

The default Egress and Ingress Rate Limit are "Unlimited" for both copper ports and fiber ports.

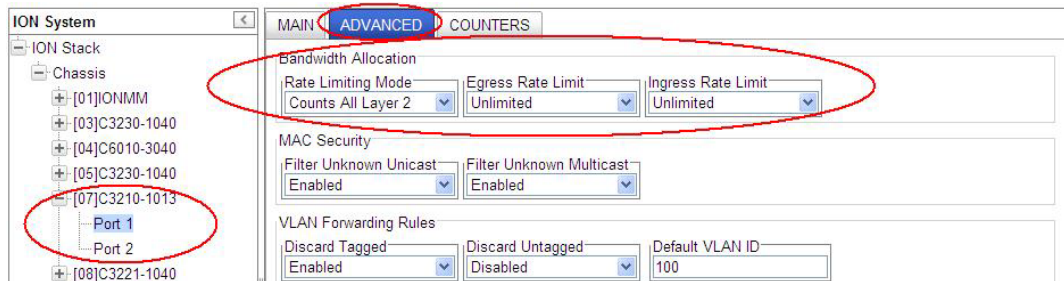
5. Press **Enter**.
6. Verify the bandwidth allocation for the port. Type **show bandwidth allocation** and press **Enter**.

Example:

```
C1|S15|L1P2>set bw alloc-type countAllLayer3
C1|S15|L1P2>set irate=rate1M erate=rate1M
C1|S15|L1P2>show bandwidth allocation
Bandwidth allocation type:    countAllLayer3
Ingress rate:                rate1M
Egress rate:                 rate1M
C1|S15|L1P2>
```

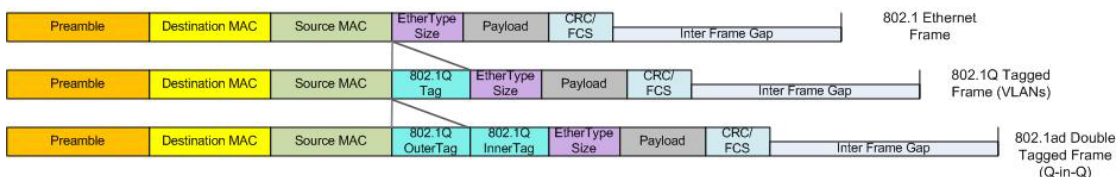
## Set Bandwidth Allocation / Rate Limiting – Web Method

1. Access the C3210 through the Web interface.
2. Select the appropriate port's **ADVANCED** tab.
3. Locate the **Bandwidth Allocation** section.



4. In the **Rate Limiting Mode** field, select which bytes in a frame are to be counted in determining the rate limit:
  - **Counts All Layer 1:** (the default): in determining the rate limit, this selection counts the following bytes in a frame: Preamble (8 Bytes) + DA to CRC + Inter Frame Gap (12 bytes).
  - **Counts All Layer 2:** in determining the rate limit, this selection counts the bytes in a frame from the DA to the CRC in determining the rate limit.
  - **Counts All Layer 3:** in determining the rate limit, this selection counts the following bytes in a frame:
    - from the DA (Destination MAC) to the CRC (18 bytes if untagged)
    - from the DA (Destination MAC) to the CRC (22 bytes if tagged)

**Note:** The Counts All Layer 3 selection will skip the Ethernet header, the CRC, and Tags (if any tags exist).



5. In the Egress Rate Limit field, select the Egress bandwidth limit in bits per second. Traffic which goes over this rate is discarded. See below for the rate limit selections and default.

In the Ingress Rate Limit field, select the Ingress bandwidth limit in bits per second. This is the Committed Information Rate (CIR) on this interface for Ingress. Traffic above this rate is discarded. See below for the rate limit selections and default. The valid selections for irate (ingress) and egress-rate (erate) are:

**On 1000M port:** Unlimited, 1M, 2M, 3M, 4M, 6M, 8M, 10M, 20M, 30M, 40M, 50M, 60M, 70M, 80M, 100M, 200M, 300M, 400M, 500M, 600M, 700M, 800M, and 900M bps.

**On 100M port:** Unlimited, 1M, 2M, 3M, 4M, 6M, 8M, 10M, 20M, 30M, 40M, 50M, 60M, 70M, and 80M bps.

The default Egress and Ingress Rate Limit are "Unlimited" for both copper ports and fiber ports.

6. Click **Save** when done.



## Security Features

The following can be defined for the C3210:

- Media Access Control (MAC) addressing
- Virtual LANs (VLANs)

### Configuring MAC Address Blocking

The MAC address can be added to the static MAC address database with the 'connected port' as port zero. This will cause any frames from that MAC address database to cause an ATU-member violation on that port, resulting in sending a trap. This could cause excessive traps (overload the Central Processing Unit (CPU) with interrupts) depending on the traffic generated by that MAC.

This feature remembers the Ethernet MAC address connected to the switch port and allows only that MAC address to communicate on the port. If any other MAC address tries to communicate through the port, port security will take the action specified by the Set Ethernet Port Source MAC Address Lock Action command.

The 'SA lock' (Source Address Lock) function is used to detect if the device connected to this port is changed. After the 'SA lock' is enabled, any new MAC is received will trigger the 'SA lock action'. If the MAC address is already learned by the device, 'SA lock action' won't be triggered. Note that this feature only blocks data traffic, not management traffic.

MAC Address Blocking can be configured for the C3210 port using either the CLI or Web method.

#### ***MAC Address Blocking – CLI Method***

1. Access the C3210 through either a USB connection or a Telnet session.
2. Access the desired port.
3. Enable the Ethernet Source Address Lock. Type: **set ether src-addr-lock true** and press **Enter**.
4. Select the Ethernet Source Address Lock Action. Type: **set ether src-addr-lock action=x**  
where: x = the SA lock action to perform = {all | discard | discardandnotify | shutdown }

The SA Lock Actions performed when encountering an unknown MAC address are:

**discard:** frames with unknown MAC addresses are discarded. This is the default value.

**discard and notify:** A trap is sent to notify the intrusion/SA change and the frame is discarded.

**shutdown:** This will shut down the interface on receiving the frame.

**all:** All of the above actions take place. The frame is discarded, a trap is sent and the port is shutdown to prevent intrusion attack.

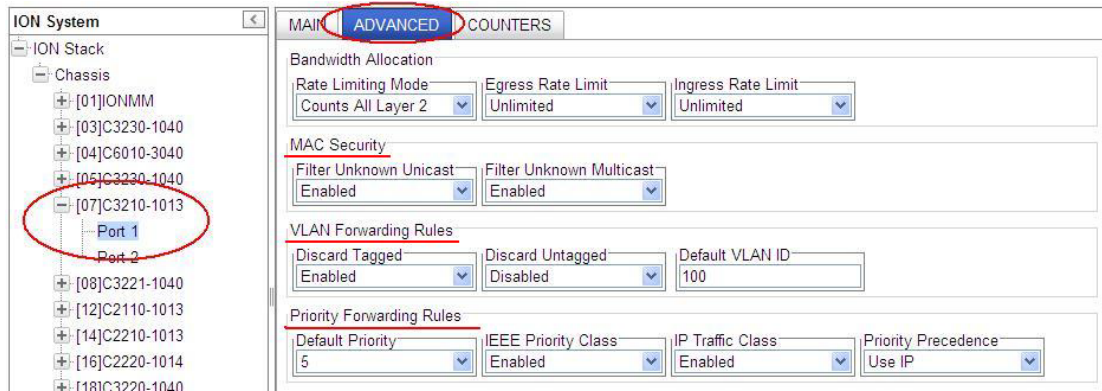
5. Press **Enter**.

6. Verify the security configuration. Type **show ether security config** and press **Enter**.  
The Ethernet Port Security configuration table displays. For example:

```
Agent III C1|S13|L1P1>set ether src-addr-lock true
Agent III C1|S13|L1P1>set ether src-addr-lock action discardandnotify
Agent III C1|S4|L1P1>show ether security config
Ethernet port security configuration:
-----
Source MAC address lock:          disable
Source MAC address lock action:   discard
Filter unknown dest unicast:     disable
Filter unknown dest multicast:    enable
Agent III C1|S4|L1P1>go l1p=2
Agent III C1|S4|L1P2>show ether security config
Ethernet port security configuration:
-----
Source MAC address lock:          disable
Source MAC address lock action:   discard
Filter unknown dest unicast:     disable
Filter unknown dest multicast:    disable
Agent III C1|S4|L1P2>
```

## MAC Address Blocking – Web Method

1. Access the C3210 through the Web interface.
2. Select the desired port.
3. Select the **ADVANCED** tab.



4. Locate the **MAC Security** section.
5. In the **SA Lock** field, select **Enabled**. The **SA Lock** (Source Address Lock) when set to **Enabled** monitors for any source MAC address change on this port. This feature is used to detect if the device connected to this port has been changed, and is also useful for detecting intrusion when an unknown MAC address ingress this port.
6. In the **SA Lock Action** (Source Address Lock Action) field, select **Enabled**. When SA Lock is set to Enabled to monitor for any source MAC address change on this port, '**SA Lock Action**' sets the action to be taken when such an event is detected. This feature is useful to detect if the device connected to this port has been changed and also for intrusion when unknown MAC address ingress this port.

The SA Lock Actions performed on encountering an unknown MAC address are:

**Discard:** frames with unknown MAC addresses are discarded. This is the default value.

**Discard and Notify:** A trap is sent to notify the intrusion/SA change and the frame is discarded.

**Shutdown:** This will shut down the interface on receiving the frame.

**All:** All the above actions take place. The frame is discarded, a trap is sent and the port is shutdown to prevent intrusion attack.

7. In the **Filter Unknown Unicast** field, select **Enabled** to filter all unicast frames with an unknown destination address from egressing this Port.
8. In the **Filter Unknown Multicast** field, select **Enabled** to filter all multicast frames with unknown destination address from egressing this Port.
9. Locate the **VLAN Forwarding Rules** section.
10. At the **Discard Tagged** field, select Enabled or Disabled. At **Discard Untagged** select Enabled or Disabled. At **Force Default VLAN** select Enabled or Disabled
11. Enter a **Default VLAN ID** in the range of 2-4093.

12. Locate the **Priority Forwarding Rules** section.
13. In the **Default Priority** field, select the default priority (**0-7**, where 0 is the lowest priority) for frames ingressing this port, if it doesn't have any IEEE 802.3ac tag or any IP TOS/Diffserv traffic class fields.
14. In the **IEEE Priority Class** field, select **Enabled** so that if the frame is IEEE tagged, and this mib variable is set to 'true', the 802.1p bits are used as the frame's priority.
15. In the **IP Traffic Class** field, select **Enabled** so that if the frame has IP TOS/Diffserv traffic class fields, and this mib variable is set to 'true', the traffic class fields will be used as the frame's priority.
16. In the **Priority Precedence** field, select **Enabled** so that if the frame has IP TOS/Diffserv traffic class fields, and IEEE 802.3ac tagged, then 'Priority Precedence' decides which one is to be considered as the frame's priority.
17. In the **SA Priority Override** field, select **Enabled** to let a frame's Source MAC address decide the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.
18. In the **DA Priority Override** field, select **Enabled** to let a frame's Destination MAC address decide the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.
19. In the **VID Priority Override** field, select **Enabled** to let a frame's VLAN ID (VID) decide the priority of the frame. The new priority value is assigned based on the priority assigned to that VLAN ID in the VLAN database.
20. Click the **Save** button at the bottom of the screen.

## Configuring Port Forward Management / IP Access Blocking

Any management of the system via IP can be locked at the system level, or only on certain ports. For example, management can occur via web/SNMP only on Port 1, so that access via other ports can be blocked. For each port, define the set of ports that frames ingressing this Source port can be forwarded to, and define the port that will perform its management functions.

Port Forward Management / IP Access Blocking can be configured in the C3210 using either the CLI or Web method.

### ***Port Forward Management / IP Access Blocking – CLI Method***

1. Access the C3210 through either a USB connection or a Telnet session.
2. Access the desired port.
3. Set the forwarding port list. Type: **set fwd portlist=y**  
where: y = the port number{1 or 2} to be forwarded to
4. Press **Enter**.
5. Enable port management access. Type **set port mgmtaccess=z**  
where: z=enable or disable
6. Press **Enter**.
7. View the port list. Type **show fwd portlist** and press **Enter**. The FWD Portlist table displays.  
For example:

```
C1|S1|L1D>go s=13 l1p=1
C1|S13|L1P1>set fwd portlist 2
C1|S13|L1P1>show fwd portlist
```

port-id	fwd portlist	mgmt access
1	2	disable

```
C1|S13|L1P1>set port mgmtaccess enable
C1|S13|L1P1>show fwd portlist
```

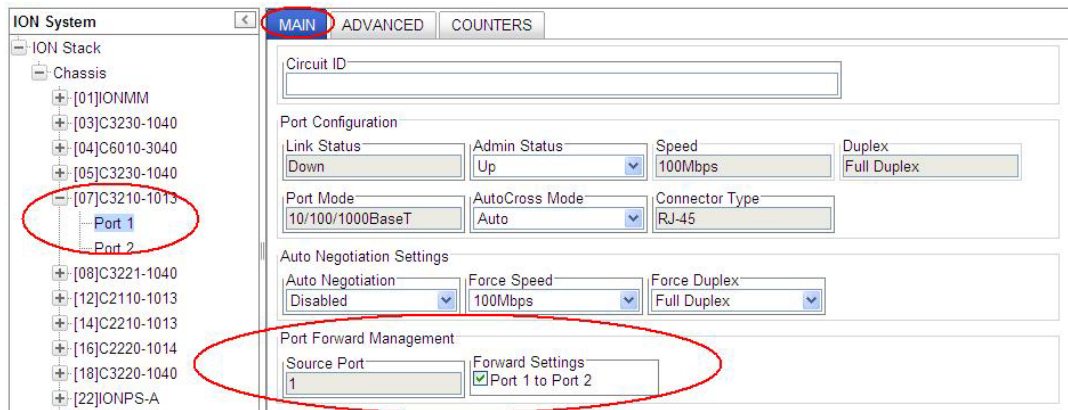
port-id	fwd portlist	mgmt access
1	2	enable

```
C1|S13|L1P1>set fwd portlist 2,3
C1|S13|L1P1>show fwd portlist
```

port-id	fwd portlist	mgmt access
1	2,3	enable

## Port Forward Management / IP Access Blocking – Web Method

1. Access the C3210 through the Web interface.
2. Select the appropriate port.
3. On the port's **MAIN** tab, locate the **Port Forward Management** section.



4. In the **Forward Settings** fields, check the checkbox for the set of ports that frames ingressing this Source port can be forwarded to.
5. Check the checkbox for the **Management via Port x** as required for this port.
6. Click **Save**.

## Configuring VLAN Features

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Ports on a switch can be grouped into VLANs in order to limit traffic flooding since it is limited to ports belonging to that VLAN and its trunk ports. Any switch port can belong to a VLAN. Packets are forwarded and flooded only to stations in the same VLAN. Each VLAN is a logical network, and packets destined for stations that do not belong to the same VLAN must be forwarded through a routing device. Each VLAN can also run a separate instance of the spanning-tree protocol (STP).

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

Virtual LANs are essentially Layer 2 constructs, whereas IP subnets are Layer 3 constructs. In a campus LAN employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs. Virtual LANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to one another and this correspondence is useful during the network design process.

A virtual LAN (VLAN) is a collection of network nodes that share the same broadcast domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers. This allows users to share information and resources as though located on the same LAN. VLANs also allow a single physical LAN to be divided into multiple logical LANs.

This section covers Port VLAN and VLAN tunneling configuration including:

[Port VLAN Config – CLI Method](#) on page [72](#) (Port VLAN Forwarding Rules and Tag Management)

[Port VLAN Config – Web Method](#) on page [73](#) (Port VLAN Forwarding Rules and Tag Management)

[VLAN Tunneling Config](#) on page [75](#)

## Configuring Port VLAN Forwarding Rules and VLAN Tag Management

You can configure the C3210 copper port for VLAN Forwarding and VLAN Tag Management using either the CLI or Web method.

### **Port VLAN Config –CLI Method**

1. Access the NID through either a USB connection or a Telnet session.
2. Define the interface's VID. Type **set port default-vid**<1-4094> and press **Enter**. This VLAN ID is given to untagged frames on ingress into the device.
3. Define discard tagged frame handling for this port. Type **set port discard-tagged**<false|true> and press **Enter**. If you enter **set port discard-tagged=true**, then all tagged non-management frames ingressing this port are filtered. All untagged and priority tagged frames are processed as normal frames.
4. Define discard untagged frame handling for this port. Type **set port discard-untagged**<false|true> and press **Enter**. If you enter **set port discard-untagged=true**, then - all untagged and priority tagged non-management frames ingressing this port are filtered. All 802.1Q tagged frames are processed as normal frames.
5. Select whether this port is to be forced to use the default VID. Type **set port force-default-vid**<false|true> and press **Enter**. This forces all untagged and (802.1Q) tagged frames to take up the interface's Default VLAN ID.
6. Define the port's VLAN tagging/port type.  
Type **set port vlan tag mode**<customer|network|provider> and press **Enter**.

This is the interface's tagging mode. The interface can be set as:

**Network:** This is the normal network mode. It can take untagged and 802.3ac tagged frames. In this mode, 802.1q can be enabled on the interface. Frames with an Ethertype of 0x8100 are considered as tagged.

**Provider:** In provider mode, frames are considered provider tagged if it matches the 'Provider Ether Type'. Frames which are ingress with a provider tag are stripped of their provider tag on egressing this interface. If the frame's ethertype doesn't match the 'Provider Ether Type' it is as untagged.

**Customer:** The customer mode is a normal access port which is not 802.1Q-aware.

7. If you selected **Provider** in step 6 above, select the port's VLAN tagging Provider EtherType.  
Type **set port vlan tag provider ethtype**<x8100|x88a8|x9100> and press **Enter**.  
Skip this step if you selected **Customer** or **Network** in step 5 above.
8. Verify the VLAN configuration. Type **show vlan config** and press **Enter**.

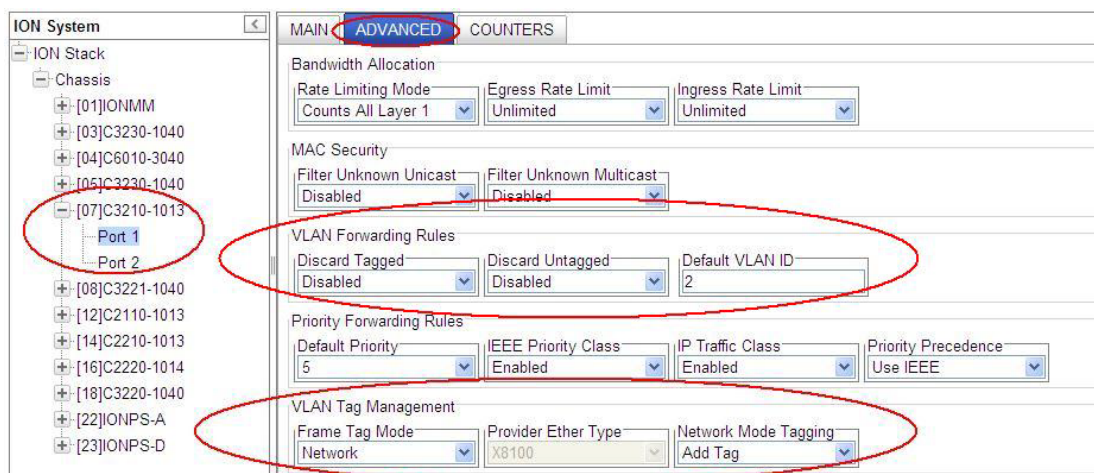


9. For example:

```
C1|S8|L1P1>set port default-vid<2-4094>
C1|S8|L1P1>set port discard-tagged<false|true>
C1|S8|L1P1>set port discard-untagged<false|true>
C1|S8|L1P1>set port force-default-vid<false|true>
C1|S8|L1P1>set port vlan tag mode<customer|network|provider>
C1|S8|L1P1>set port vlan tag provider ethtype<x8100|x88a8|x9100>
C1|S3|L1D>show vlan config
vlan id      vlan state      vlan portlist
-----
2            enable          none
C1|S3|L1D>
```

### Port VLAN Config –Web Method

1. Access the NID through the Web interface.
2. Select the appropriate port.
3. At the port's **ADVANCED** tab, locate the **VLAN Forwarding Rules** section.



4. In the **Discard Tagged** field, select **Enabled** if tagged frames are to be discarded. The default is Disabled (tagged frames are not discarded).
5. In the **Discard Untagged** field, select **Enabled** if untagged frames are to be discarded. The default is Disabled (untagged frames are not discarded).
6. In the **Default VLAN ID** field, enter the associated **VLAN ID** number. The valid range is from 2–4094. This sets the VLAN ID which is to be used for all management traffic to and from the device. The management station that belongs to this VLAN is the only one able to manage the C3210. When the value is not 0 or 1, the Management traffic is expected to be tagged with the Management VLAN ID configured when 802.1Q is enabled.

7. Locate the **VLAN Tag Management** section.
8. In the **Frame Tag Mode** field, select **Network**, **Provider**, or **Customer** as the frame tag mode for this port. The default Status is **Network**. If you select **Provider**, the **Provider Ether Type** field activates. If you select **Network**, the **Network Mode Tagging** field activates. If you select **Customer**, neither field is active.
9. If you selected **Provider** in step 8 above, the **Provider Ether Type** field becomes active. Select either **X8100**, **X9100**, or **X88A8** as the **Provider Ether Type** for this port.
10. If you selected **Network** in step 8 above, the **Network Mode Tagging** field becomes active. Select either **Unmodified**, **Remove Tag**, or **Add Tag** for **Network Mode Tagging** for this port. The default is **Add Tag**.
11. Click the **Save** button when done.

## Configuring VLAN Tunneling (802.1q Tunneling)

Sending multiple VLANs across the service provider's Metro Ethernet network can be accomplished with VLAN Tunneling, also known as 802.1q Tunneling. The original 802.1Q specification allows a single VLAN header to be inserted into an Ethernet frame. Q-in-Q allows multiple VLAN headers to be inserted into a single frame.

VLAN Tunneling is a mechanism that service providers can use to provide secure Ethernet VPN services to their customers. Ethernet VPNs using VLAN Tunneling are possible because of the two-level VLAN tag scheme used. The outer VLAN tag is referred to as the service provider VLAN tag (S-Tag) and uniquely identifies a given customer within the network of the service provider. The inner VLAN tag is referred to as the customer VLAN tag (C-Tag) because the customer assigns it. It is possible for multiple customer VLANs to be tagged using the same outer or service provider VLAN tag, thereby trunking multiple VLANs among customer sites.

VLAN Tunneling lets service providers use a single VLAN to support multiple VLANs of customers, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. At the same time, it significantly reduces the number of VLANs required to support the VPNs. VLAN Tunneling encapsulates enterprise customers' VLANs into a VLAN of the service provider.

VLAN Tunneling accomplishes the following:

- Enterprise customers receive transparent Layer 2 links between sites within a metro area, such as a link from a branch office to a main campus.
- Service providers can separate or group traffic on a per-customer basis using outer VLAN tags as it traverses the common infrastructure so that the same infrastructure can provide service to multiple customers.
- The VLAN ID of the enterprise and the VLAN ID of the service provider do not have to match.
- Customers can treat the switching infrastructure in a remote site as if it were part of the local site. They can use the same VLAN space and run protocols such as STP across the provider infrastructure through 802.1q.

The VLAN Tunneling model allows the customer edge switch on each side of the tunnel to view the service provider infrastructure as nothing more than a transparent bridge.

### How VLAN Tunneling Works

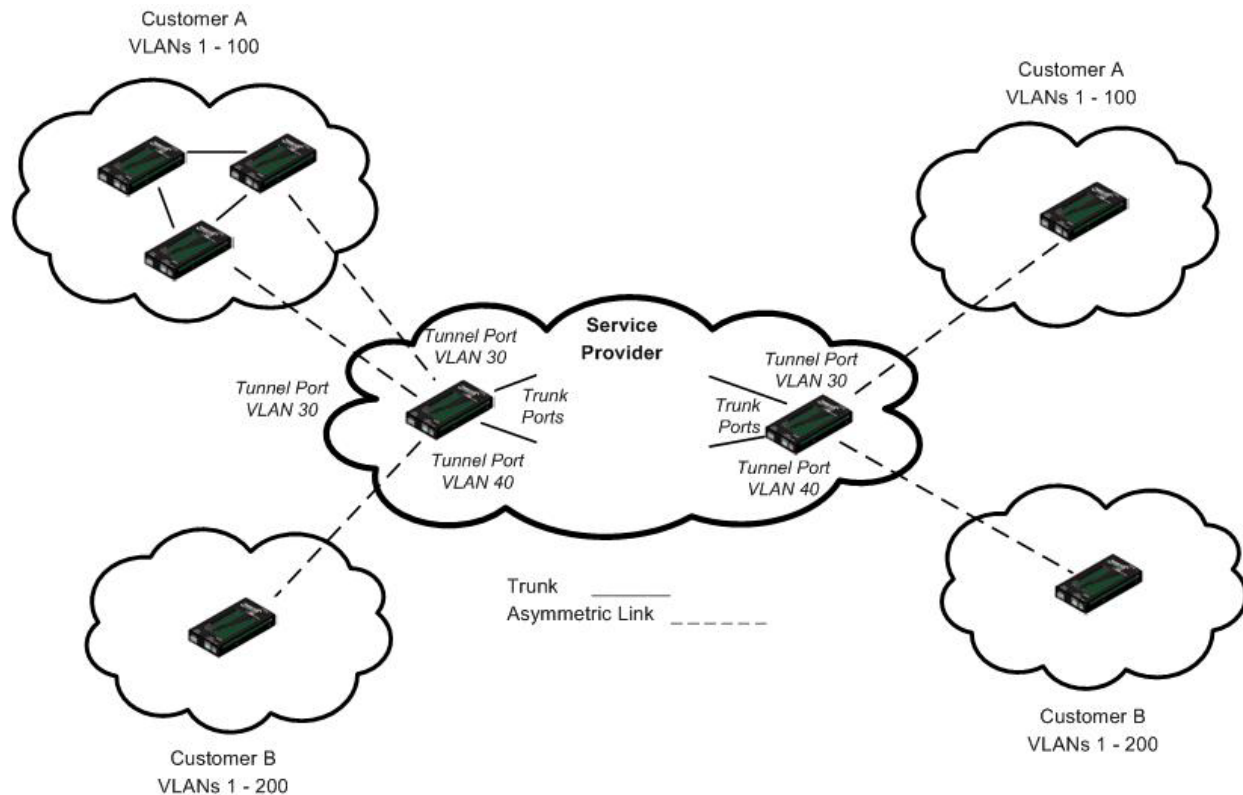
A tunnel port is a port that is configured to support 802.1q (VLAN) tunneling. Each customer comes in on a dedicated customer-facing port on the service provider switch where a VLAN that is dedicated to tunneling is assigned. The service provider assigns each customer an outer VLAN tag or a service provider VLAN tag that uniquely identifies him within the network. The service provider VLAN also keeps the customer traffic isolated from other customer traffic that is traversing the same service provider network. That service provider VLAN supports all the VLANs of the customer.

VLAN Tunneling refers to multiple tagging of dot1Q frames as they enter a service provider switch from a client switch. VLAN Tunneling can tag or untag any frames that it receives from the customer tag. VLAN Tunneling also has native VLAN frames that are untagged. The service provider switch adds the outer VLAN tag.

Tagged and untagged customer traffic comes from a port on a customer device and enters the service-provider edge switch through a tunnel port. Each customer edge port that is connected to a VLAN tunnel

port is typically configured as a trunk port. The customer trunk port is unaware of the provider VLAN tunnel and can communicate with all of its other trunk ports that are connected to the metro network of the provider as if they were directly connected. This makes the process transparent to the enterprise's switching network.

A hub customer edge might have connectivity to two remote spoke sites and have only half of the VLANs from the hub site go to one site, and the remaining VLANs go to the second remote site. This is possible using two service provider VLANs for this enterprise customer when certain sites need to see only some and not all of the VLAN traffic from the hub site.



**Figure 6: VLAN Tunneling Example**

The link between the 802.1q trunk port on a customer device and the tunnel port is an “asymmetrical” link. One end is designated an 802.1q trunk port, and the other end is configured as a tunnel port. The tunnel port is configured with an access VLAN ID that is unique to a customer.

Using the VLAN tunneling feature, a service provider uses a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from various customers is segregated within the service-provider infrastructure even when they appear to be on the same VLAN.

Thus VLAN tunneling expands VLAN space by using a ‘VLAN-in a-VLAN’ hierarchy, and by tagging the already-tagged packets. The port configured to support VLAN tunneling is called a tunnel port. When configuring tunneling, a tunnel port is assigned to a VLAN that is dedicated to tunneling. Each customer requires a separate VLAN, but that VLAN supports all of the customer's VLANs.

## Summary

The original 802.1Q specification allows a single VLAN header to be inserted into an Ethernet frame. Q-in-Q allows multiple VLAN headers to be inserted into a single frame, an essential capability for implementing Metro Ethernet network topologies.

IEEE 802.1Q-in-Q is an Ethernet networking standard for Ethernet frame formats. 802.1Q-in-Q is an amendment to IEEE 802.1Q, and not an independent specification of its own; but the amendment, a non-trivial extension, acquired this alias. It is also known simply as "QinQ" or "Q-in-Q".

In a multiple VLAN header context, the term "VLAN tag" or just "tag" for short is often used in place of "802.1Q VLAN header". Q-in-Q allows multiple VLAN tags in an Ethernet frame.

When used in the context of an Ethernet frame, a Q-in-Q frame is a frame that has two VLAN 802.1Q headers (double-tagged).

## Prerequisites for VLAN Tunneling Functions

1. Network topology and network administration have been reviewed.
2. Business and service policies have been established.

## Restrictions for Configuring VLAN Tunneling Functions

The ION system supports static VLAN configuration. While VLAN Tunneling works well for Layer 2 packet switching, there are incompatibilities with some Layer 2 features and with Layer 3 switching.

1. A tunnel port cannot be a routed port.
2. IP routing is not supported on a VLAN that includes 802.1Q ports.
3. Fallback bridging is not supported on tunnel ports.
4. Tunnel ports do not support IP access control lists (ACLs).
5. Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports.
6. Cisco's Dynamic Trunking Protocol (DTP) is not compatible with 802.1Q tunneling.
7. Loopback detection is supported on 802.1Q tunnel ports.
8. If management is required over a provider port, it must use Management VLAN.
9. You can set up a VLAN without Management VLAN enabled. You can not set up a VLAN without setting up VLAN Forwarding Rules, because then it would not validate any frames with no filtering rules in the VLAN filtering database.

For specific procedures on configuring VLAN Tunneling via the CLI or Web method, see "[VLAN Tunneling Configuration Examples](#)".

## 5. Operation

### General

This section describes the non-configuration operations that can be performed for the C3210.

### Backup and Restore Operations (Provisioning)

Through the Web interface you can back up and restore the configuration information for the IONMM and any or all of the C3210s 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 *C3210 CLI Reference Manual*, 33497.

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

---

### IMPORTANT



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

---

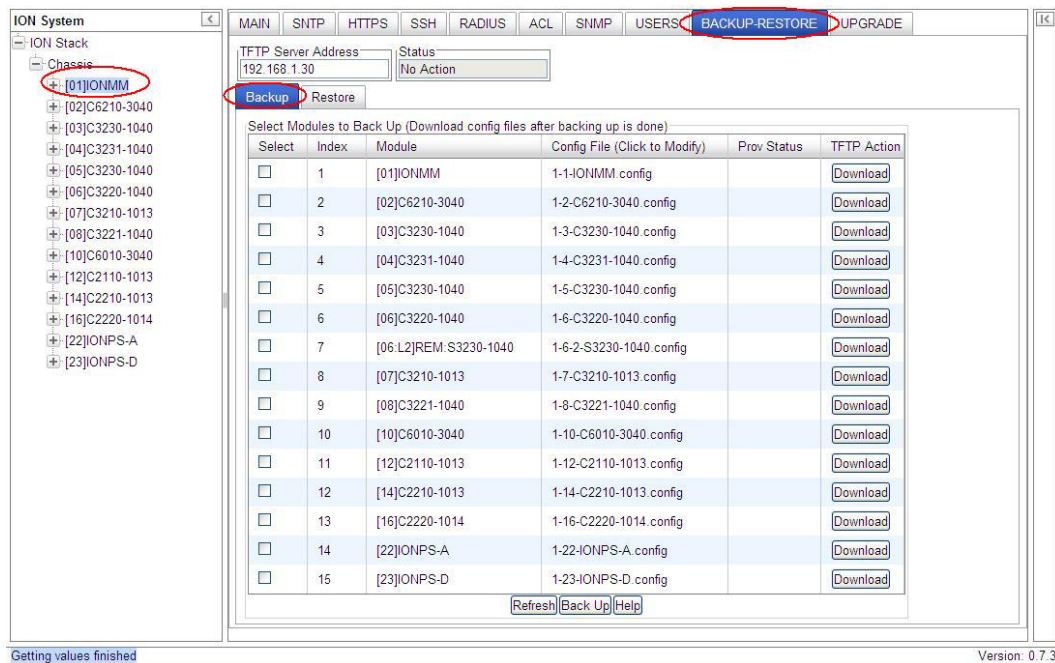
For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- Table 15: [Back Up and Restore File Content and Location](#)
- Table 16: [File Status after a Reset to Factory Defaults](#)
- Table 17: [File Content and Location after a System Reboot](#)
- Table 18: [File Content and Location after a Firmware Upgrade](#)

## Backing Up Slide-In and Remote Modules

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

1. Access the IONMM through the Web interface.
2. Select the **BACKUP-RESTORE** tab. Select the **Backup** sub-tab if not already displayed.



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

Yes	No
a) In the <b>Config File</b> column, click the file name. b) Type a new name for the backup file. <b>Note:</b> the file name must be 1–63 characters long and must end with <b>.config</b> . c) Continue with <a href="#">step 8</a> below.	Continue with <a href="#">step 9</a> below.




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


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

The screenshot shows the 'BACKUP-RESTORE' tab in the Lantronix web interface. The 'TFTP Server Address' is set to 192.168.1.30 and the 'Status' is 'No Action'. The 'Backup' button is highlighted. Below, a table titled 'Select Modules to Back Up (Download config files after backing up is done)' shows two modules selected for backup:

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input checked="" type="checkbox"/>	1	[03]C3230-1040	1-3-C3230-1040.config	success	<a href="#">Download</a>
<input checked="" type="checkbox"/>	2	[08]IONMM	1-8-IONMM.config	success	<a href="#">Download</a>

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

The screenshot shows the 'BACKUP-RESTORE' tab. The 'TFTP Server Address' is 192.168.1.30 and 'Status' is 'No Action'. The 'Backup' button is highlighted. The table below shows a failed backup for module [11]C2210-1013:

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[03]C3230-1040	1-3-C3230-1040.config		<a href="#">Download</a>
<input type="checkbox"/>	2	[08]IONMM	1-8-IONMM.config	success	<a href="#">Download</a>
<input checked="" type="checkbox"/>	3	[11]C2210-1013	1-11-C2210-1013.config	failure 	<a href="#">Download</a>
<input type="checkbox"/>	4	[13]C2110-1013	1-13-C2110-1013.config		<a href="#">Download</a>
<input type="checkbox"/>	5	[16]C3220-1040	1-16-C3220-1040.config		<a href="#">Download</a>
<input type="checkbox"/>	6	[18]C2220-1014	1-18-C2220-1014.config		<a href="#">Download</a>

Buttons at the bottom: Refresh, Back Up, Help.

If the card list showed in the table is not correct, please fold/unfold "ION Stack" node in the left tree view to refresh.

The error (.ERR) log file is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad. See ["The Config Error Log \(config.err\) File"](#) section for error messages and possible recovery procedures.



## Backing Up Standalone Modules

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

### IMPORTANT



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

1. Access the IONMM module through the Web interface.
2. Select the **BACKUP-RESTORE** tab.

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		<a href="#">Download</a>
<input type="checkbox"/>	2	[03]C3230-1040	1-3-C3230-1040.config		<a href="#">Download</a>
<input type="checkbox"/>	3	[04]C6010-3040	1-4-C6010-3040.config		<a href="#">Download</a>
<input type="checkbox"/>	4	[05]C3230-1040	1-5-C3230-1040.config		<a href="#">Download</a>
<input type="checkbox"/>	5	[07]C3210-1013	1-7-C3210-1013.config		<a href="#">Download</a>
<input type="checkbox"/>	6	[08]C3221-1040	1-8-C3221-1040.config		<a href="#">Download</a>
<input type="checkbox"/>	7	[12]C2110-1013	1-12-C2110-1013.config		<a href="#">Download</a>
<input type="checkbox"/>	8	[14]C2210-1013	1-14-C2210-1013.config		<a href="#">Download</a>
<input type="checkbox"/>	9	[16]C2220-1014	1-16-C2220-1014.config		<a href="#">Download</a>
<input type="checkbox"/>	10	[18]C3220-1040	1-18-C3220-1040.config		<a href="#">Download</a>
<input type="checkbox"/>	11	[22]IONPS-A	1-22-IONPS-A.config		<a href="#">Download</a>
<input type="checkbox"/>	12	[23]IONPS-D	1-23-IONPS-D.config		<a href="#">Download</a>

3. In the **Select** column, check the checkbox of the module to be backed up.
4. Do you want to rename the backup file?

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

5. Click the **Download** button. When completed, the message *"File has successfully transferred via TFTP"* displays.
6. Click the **OK** button to clear the web page message.

7. Click the **Back Up** button.
8. At the confirmation message, click OK. The message *"Backup is being processed ..."* displays. The Back Up operation can take several minutes.
9. To send a copy of the backup file to the TFTP server:
  - a. Make sure the TFTP Server is running and configured.
  - b. In the **TFTP Server Address** field, enter the IP address of the TFTP server.
  - c. Click the **Download** button.
  - d. When the successful completion message displays, click **OK**.

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

- [Editing the Config File \(Optional\)](#)
- [Restoring Slide-In and Remote Modules](#)

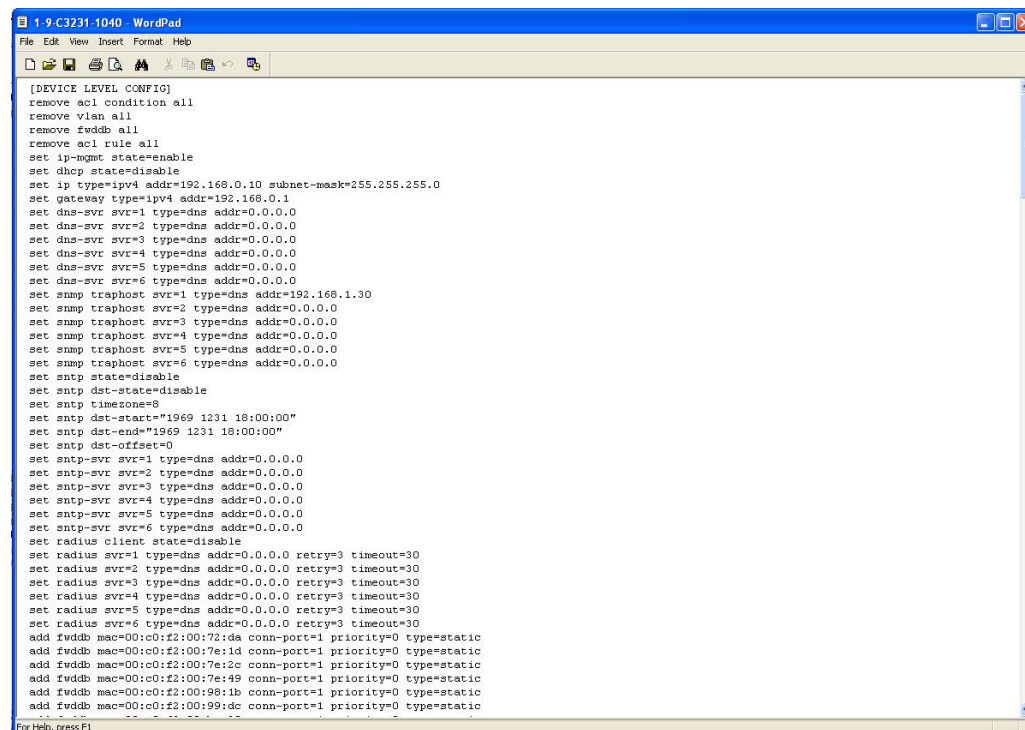
## Editing the Config File (Optional)

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

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

1. Complete the applicable Backup procedure from the previous section.
2. Open the Config file (in Notepad, WordPad, Word, OpenOffice Writer, etc.) from the TFTP server location (e.g., C:\TFTP-Root\1-9-C3231-1040.config).
3. Edit the Config file sections. Each Config file contains a DEVICE LEVEL CONFIG section and two PORT x CONFIG sections.
4. Save the edited Config file back to the TFTP server location (e.g., C:\TFTP-Root\1-9-C3210-1040.config).
5. Continue with the applicable Restore procedure from the following section using the edited Config file.

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



```
[DEVICE LEVEL CONFIG]
remove acl condition all
remove vlan all
remove fwddb all
remove acl rule all
set ip-mgmt state=enable
set dhcp state=disable
set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0
set gateway type=ipv4 addr=192.168.0.1
set dns-svr svr=1 type=dns addr=0.0.0.0
set dns-svr svr=2 type=dns addr=0.0.0.0
set dns-svr svr=3 type=dns addr=0.0.0.0
set dns-svr svr=4 type=dns addr=0.0.0.0
set dns-svr svr=5 type=dns addr=0.0.0.0
set dns-svr svr=6 type=dns addr=0.0.0.0
set snmp traphost svr=1 type=dns addr=192.168.1.30
set snmp traphost svr=2 type=dns addr=0.0.0.0
set snmp traphost svr=3 type=dns addr=0.0.0.0
set snmp traphost svr=4 type=dns addr=0.0.0.0
set snmp traphost svr=5 type=dns addr=0.0.0.0
set snmp traphost svr=6 type=dns addr=0.0.0.0
set snmp state=disable
set snmp dst-state=disable
set snmp timezone=8
set snmp dst-start="1969 1231 18:00:00"
set snmp dst-end="1969 1231 18:00:00"
set snmp dst-offset=0
set snmp-svr svr=1 type=dns addr=0.0.0.0
set snmp-svr svr=2 type=dns addr=0.0.0.0
set snmp-svr svr=3 type=dns addr=0.0.0.0
set snmp-svr svr=4 type=dns addr=0.0.0.0
set snmp-svr svr=5 type=dns addr=0.0.0.0
set snmp-svr svr=6 type=dns addr=0.0.0.0
set radius client state=disable
set radius svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30
set radius svr=2 type=dns addr=0.0.0.0 retry=3 timeout=30
set radius svr=3 type=dns addr=0.0.0.0 retry=3 timeout=30
set radius svr=4 type=dns addr=0.0.0.0 retry=3 timeout=30
set radius svr=5 type=dns addr=0.0.0.0 retry=3 timeout=30
set radius svr=6 type=dns addr=0.0.0.0 retry=3 timeout=30
add fwddb mac=00:c0:f2:00:72:1d conn-port=1 priority=0 type=static
add fwddb mac=00:c0:f2:00:7e:1c conn-port=1 priority=0 type=static
add fwddb mac=00:c0:f2:00:7e:49 conn-port=1 priority=0 type=static
add fwddb mac=00:c0:f2:00:98:1b conn-port=1 priority=0 type=static
add fwddb mac=00:c0:f2:00:99:dc conn-port=1 priority=0 type=static
```

## Restoring Slide-In and Remote Modules

The following procedure describes how to restore the configuration of one or more slide-in or remote modules in the ION system. **Note:** these Restore procedures require that the TFTP server be running and properly configured, and that the backup configuration file is named and located properly.

### IMPORTANT

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

1. Access the IONMM through the Web interface.
2. Select the **BACKUP-RESTORE** tab and select the **Restore** sub-tab. The “Modules to Restore” table displays.

The screenshot shows the ION System Web interface. On the left, the 'ION Stack' tree view is expanded, showing the 'IONMM' module selected. The main content area has tabs for MAIN, SNTP, HTTPS, SSH, RADIUS, ACL, **BACKUP-RESTORE**, and UPGRADE. The 'BACKUP-RESTORE' tab is active, and the 'Restore' sub-tab is selected. Below the sub-tabs, there is a 'TFTP Server Address' field (192.168.1.30) and a 'Status' field (No Action). The 'Backup' and 'Restore' buttons are visible, with 'Restore' being the active one. Below these buttons is a table titled 'Select Modules to Restore (Upload config files before restoring is started)'. The table has columns: Select, Index, Module, Config File (Click to Modify), Prov Status, and TFTP Action. The table lists 13 modules, each with an 'Upload' button in the TFTP Action column. At the bottom of the table, there are buttons for 'Refresh', 'Restore', and 'Help'.

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[01]IONMM	1-1-IONMM.config		Upload
<input type="checkbox"/>	2	[03]C3230-1040	1-3-C3230-1040.config		Upload
<input type="checkbox"/>	3	[04]C6010-3040	1-4-C6010-3040.config		Upload
<input type="checkbox"/>	4	[05]C3230-1040	1-5-C3230-1040.config		Upload
<input type="checkbox"/>	5	[05 L2]REM-S3230-1040	1-5-2-S3230-1040.config		Upload
<input type="checkbox"/>	6	[07]C3210-1013	1-7-C3210-1013.config		Upload
<input type="checkbox"/>	7	[08]C3221-1040	1-8-C3221-1040.config		Upload
<input type="checkbox"/>	8	[12]C2110-1013	1-12-C2110-1013.config		Upload
<input type="checkbox"/>	9	[14]C2210-1013	1-14-C2210-1013.config		Upload
<input type="checkbox"/>	10	[16]C2220-1014	1-16-C2220-1014.config		Upload
<input type="checkbox"/>	11	[18]C3220-1040	1-18-C3220-1040.config		Upload
<input type="checkbox"/>	12	[22]IONPS-A	1-22-IONPS-A.config		Upload
<input type="checkbox"/>	13	[23]IONPS-D	1-23-IONPS-D.config		Upload

3. If the list of modules shown in the table is not correct, unfold the ION Stack in the left tree view, and then refold it to refresh the table information.
4. In the **Select** column, check the checkbox of each module to be restored.

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

Yes	No
a) In the <b>Config File</b> column, click the file name. b) Type the name of the backup file to be restored. <b>Note:</b> the file name must end with <b>.config</b> . c) Continue with <a href="#">step 5</a> .	Continue with <a href="#">step 5</a> .


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

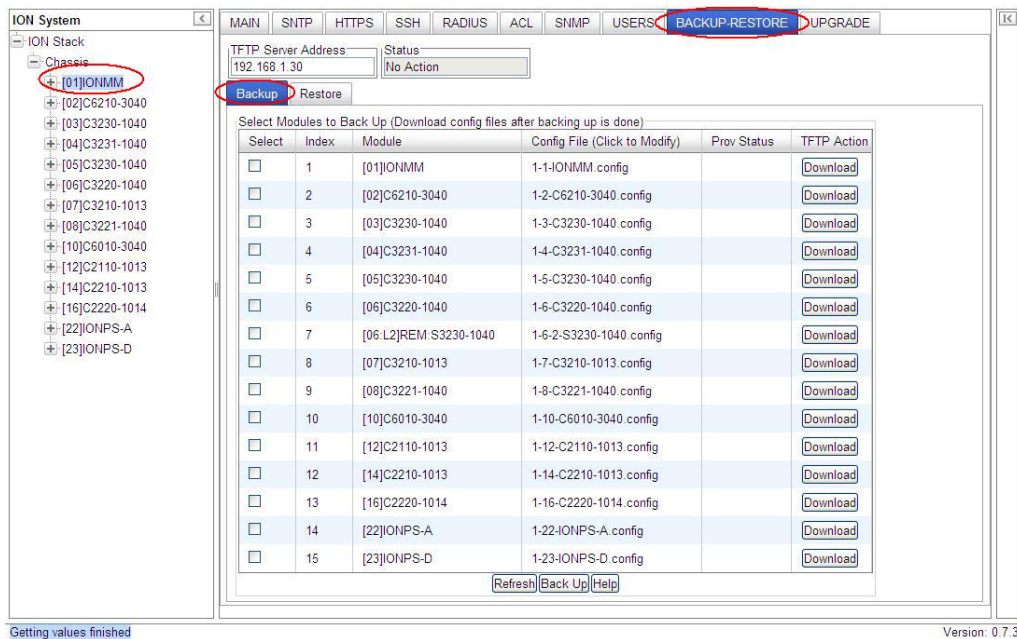
Yes	No
a) In the <b>TFTP Server Address</b> field, enter the IP address of the server. b) Click <b>Upload</b> . c) When the successful transfer message displays, click <b>OK</b> . d) Continue with <a href="#">step 6</a> .	Continue with <a href="#">step 6</a> .

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

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

When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.

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



The error log file (.ERR file) is downloaded to the TFTP server address specified, at *C:\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
[Icons]
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

```

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

## Back Up and Restore File Content and Location

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

**Note:** Doing a reboot, restart, an upgrade or a reset to factory settings may cause some configuration backup files, HTTPS certification file, SSH key file, and Syslog files to be lost.

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

**Table 8: Back Up and Restore File Content and Location**

File Type	Filename	File Description	Stored Directory	Backed up? (Y/N)	Changed after Re-store? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Re-store	/tftpboot	Yes - these files are created during Backup operation	No
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	No - not needed; the configurations included in this file are backed up by SNMP set operations.	Yes
HTTPS configuration file*	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No - not needed; the configurations included in this file are backed up by SNMP set operations	Yes
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No	No
SSH host key**	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No (see Note 1)	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 (see Note 2)	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No	Always changes
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No - not needed; the configurations included in this file will be backed up by SNMP set operations	Yes



**Back Up and Restore Notes:**

1. The HTTPS certificate is stored in '/agent3/conf/lighttpd', and is retained over power cycle and upgrades. For SSH, the host keys (RSA and DSA) are stored in '/agent3/conf/dropbear', and are also retained over power cycle and upgrades.
2. For the SSH user key, there is a 'root' user and the user key for 'root' is stored in '/root/.ssh'. This key is retained for power cycle but not upgrades. The Dropbear SSH2 server uses the Linux users as the users and it maintains the user keys with the Linux users.



## Displaying Information

There are several CLI commands that allow you to display (show) information about the C3210 configuration. For a complete description of these and other CLI commands see the *C3210 CLI Reference Manual*, 33497.

## 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 C3210 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”](#).

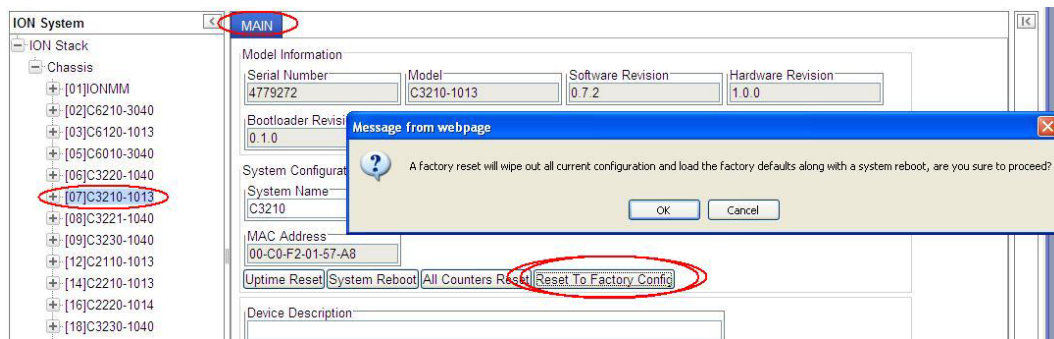
**Note:** Your USB and/or Telnet session will be disconnected.

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

## Resetting Defaults – Web Method

**Caution:** This operation deletes all configuration information that was saved in the C3210, including the IP address you assigned to the C3210.

1. Access the C3210 through the Web interface (see “Starting the Web Interface”).
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



4. Click the **Reset to Factory Config** button. The message “A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?” displays.
5. Click **Cancel** if you are sure you want to proceed with the Reboot. Click **OK** only if you wish to reboot.

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

**Note:** Your Web session will be discontinued.

6. Set the IP configuration (see “Doing the Initial System Setup”).

## File Status after Reset to Factory Defaults

The table below shows the status of C3210 files after a system re-boot.

**Table 9: 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 C3210 system uptime field displays the amount of time that the C3210 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 C3210 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: C1|S7|L1P2>**reset uptime**

Error: this command should be executed on a device!

C1|S7|L1P2>**go l1d**

C1|S7|L1D>**reset uptime**

C1|S7|L1D>

Use the **show system information** command to display the current system uptime.

**Note:** The **reset uptime** command is not available for the Power Supply modules.

## Reset System Uptime – Web Method

1. Access the C3210 through the Web interface.
2. At the **MAIN** tab, locate the **System Configuration** section.

The screenshot shows the ION System web interface. On the left is a tree view under 'ION Stack' with 'Chassis' expanded, listing various components. Component '[07]C3210-1013' is circled in red. The main panel is titled 'MAIN' and contains 'Model Information' and 'System Configuration' sections. In the 'System Configuration' section, the 'System Up Time' field is circled in red and shows '4:5:41:28.00'. Below this, the 'Uptime Reset' button is also circled in red. Other buttons like 'System Reboot', 'All Counters Reset', and 'Reset To Factory Config' are visible.

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

This screenshot is similar to the previous one, but with a confirmation dialog box overlaid on the bottom right. The dialog box is titled 'Message from webpage' and contains the text 'Uptime will be reset, are you sure to proceed?'. It has 'OK' and 'Cancel' buttons. The 'Uptime Reset' button in the background is still circled in red.

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.

## Resetting Counters

Before running certain diagnostics / tests, you may want to reset (zero out) all or some C3210 device and/or port counters.

The C3210 counters can be reset via the CLI method or Web method.

### Reset All Ports Counters – CLI Method

This is a device-level command to reset all of the C3210 ports counters.

1. Access the C3210 through either a USB connection or a Telnet session.
2. At the command prompt type: **reset all ports counters** and press **Enter**. For example:

```
AgentIII C1|S7|L1D>show cardtype
Card type:                C3220-1013
AgentIII C1|S7|L1D>reset ?
    all
    factory
    uptime
AgentIII C1|S7|L1D>reset all ports counters
AgentIII C1|S7|L1D>
```

Use the **show ether statistics** command to display Port Counters Received, Port Counters Sent, and related information.

The counters that are reset include all Port Counters, Port LOAM Counters, Port LOAM Event Configuration, Port LOAM Event Log, and Port DMI.

## Reset Port Counters– Web Method

This is a port-level function used to reset all of a C3210 port's counters.

1. Access the C3210 through the Web interface.
2. Select the desired C3210 port.
3. Select the **COUNTERS** tab.

The screenshot shows the ION System web interface. On the left is a sidebar with a tree view of the ION Stack. The 'Chassis' section is expanded, showing a list of ports. Port 1 (C3210-1013) is selected and circled in red. The main content area has three tabs: MAIN, ADVANCED, and COUNTERS. The COUNTERS tab is active and circled in red. It displays several sections of counters, all with values of 0:

- RMON Counters:** Total Octets, Packets Received, Broadcast Packets, Multicast Packets, CRC Align Errors, Undersize Packets, Oversize Packets, Fragments, Jabbers, Collisions, Drop Events, 64 Octets, 65 to 127 Octets, 128 to 255 Octets, 256 to 511 Octets, 512 to 1023 Octets, 1024 to Max Octets.
- Port Counters Received:** Total Octets, Unicast Packets, Broadcast Packets, Multicast Packets, Rx Discards, Rx Errors.
- Port Counters Sent:** Total Octets, Unicast Packets, Broadcast Packets, Multicast Packets, Tx Discards, Tx Errors.
- Dot3 Statistics:** Alignment Errors, FCS Errors, SQE Test Errors, Deferred Frames, Internal MAC Tx Errors, Internal MAC Rx Errors, Carrier Sense Errors, Symbol Errors, Single Collisions, Multiple Collisions, Late Collisions, Excessive Collisions, Oversized Frames, Duplex Status (Unknown), Rate Control Ability (True), Rate Control Status (Off).

At the bottom of the main content area, there are three buttons: 'Reset Counters' (circled in red), 'Refresh', and 'Help'.

4. If desired, click the **Refresh** button and observe and record the various counter field counts for later comparison.
5. Click the **Reset Counters** button. The C3210 port-level counters are reset to zero and begin incrementing immediately. The counters that are reset include:
  - RMON Counters
  - Port Counters Received
  - Port Counters Sent
  - Dot3 Statistics

## Clear All Ethernet Port Counters – CLI Method

This is a port-level command to reset all of a C3210 port's Ethernet counters.

1. Access the C3210 via either a USB connection or a Telnet session.
2. Select the desired C3210 port.
3. At the command prompt type **clear ether all counters** and press **Enter**. For example:

```
C1|S3|L1D>clear ether all counters
Error: this command should be executed on a port!
C1|S3|L1D>go lp=1
C1|S3|L1P1>clear ether all counters
C1|S3|L1P1>
```

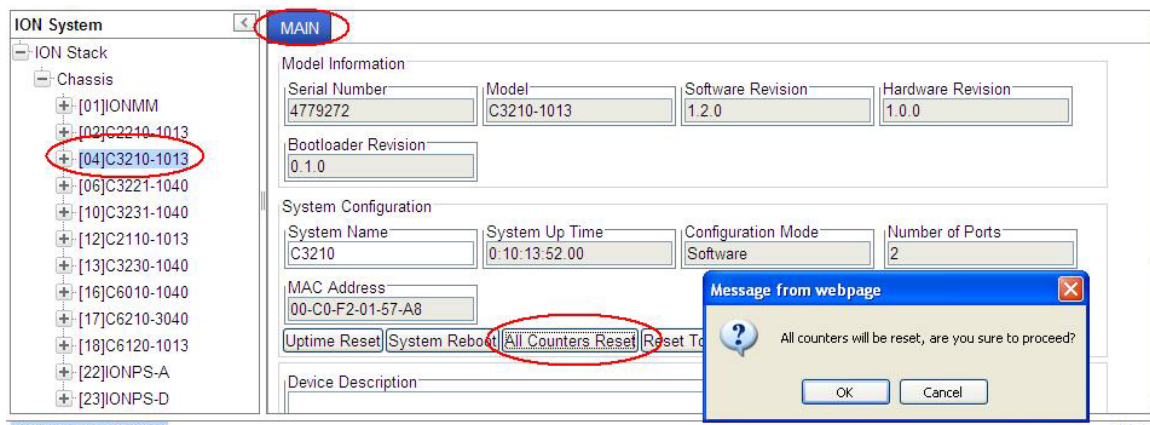
The counters that are reset include all Port Counters, Port LOAM Counters, Port LOAM Event Configuration, Port LOAM Event Log, and Port DMI.



## All Counters Reset – Web Method

This is a device-level function to reset all of the C3210 counters.

1. Access the C3210 through the Web interface.
2. At the **MAIN** tab, locate the **System Configuration** section.
3. If desired, observe and record the various counter field counts for later comparison.
4. Click the **All Counters Reset** button. The message “All counters will be reset, are you sure to proceed?” displays.



5. Click the **OK** button to proceed. The C3210 device counters are reset to zero and begin incrementing immediately. These counters are reset:
  - Port > COUNTERS
  - Port > LOAM > Counters
  - Port > LOAM > Event Configuration
  - Port > LOAM > Event Log
  - Port > DMI

## 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 C3210 reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.

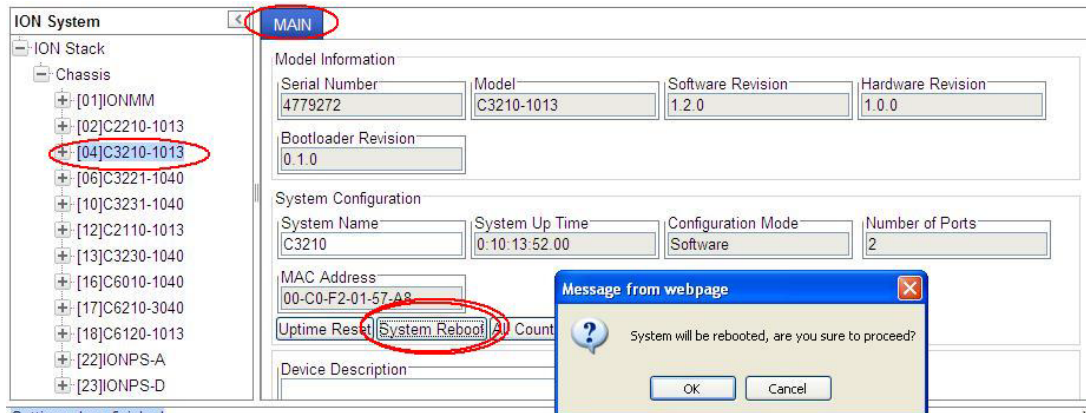
1. Access the C3210 through either a USB connection or a Telnet session.
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login again!* The ION system reboots the C3210. If this operation is performed 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.
  - For a Telnet session
    - a) Press **Enter**.
    - b) Start 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 C3210 through the Web interface.
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



4. Click the **System Reboot** button. The confirmation message "System will be rebooted, are you sure to proceed?" displays.
5. At the confirmation window, click the **OK** button to start the reboot, or click **Cancel** to quit the reboot.

The C3210 will restart and will be available for operations after about one minute.

## Reboot File Content and Location

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

**Table 10: File Content and Location after a System Reboot**

File Type	Filename	File Description	Stored Directory	Lost after Reboot? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Re-store	/tftpboot	Yes
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	No
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

## Upgrade the IONMM and/or C3210 Firmware

Occasionally changes must be made to the firmware version that is currently stored in IONMM or C3210 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 at the Lantronix Firmware Downloads [webpage](#). Ideally, all the cards in a chassis will be upgraded to the latest versions at the same time; running devices with a mix of old and new firmware can cause a “red box” condition. See “[Section 5: Troubleshooting](#)”.

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



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

You can upgrade the IONMM or C3210 Firmware from the Command Line Interface (CLI) or via the Web interface.

### Upgrading IONMM and/or C3210 Firmware – CLI Method

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

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

```
prov get tftp svr addr
prov set tftp svr type=(ipv4|dns) addr=ADDR
```
4. Go to the Lantronix Firmware Downloads [webpage](#).
5. Locate the “**Agent Firmware**” section and click the link in the right hand column (e.g., “**Download IONMM.bin.0.5.bin**”).
6. Zip the downloaded file.
7. Retrieve the firmware database file using the **tftp get** command to get the file from the TFTP Server, and then press **Enter**. For example:  
  

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

A table of available modules displays with upgrade instructions.

```
C1|S8|L1D>upgrade module
Available modules:
```

index	module	loc

```

-----
1      ION219                      c=1 s=0 l1d
2      C3230-1040                  c=1 s=3 l1d
3      C3230-1040                  c=1 s=5 l1d
4      IONMM                       c=1 s=8 l1d
5      C3231-1040                  c=1 s=10 l1d
6      C2110-1013                  c=1 s=12 l1d
7      C2210-1013                  c=1 s=13 l1d
8      C3210-1013                  c=1 s=15 l1d
9      C2220-1014                  c=1 s=16 l1d
10     C3220-1040                  c=1 s=18 l1d
11     IONPS-A                     c=1 s=22 l1d

```

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

8

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

11. Choose the module(s) to upgrade (# 8 in the example above) and press **Enter**.

12. Verify the Upgrade results. Type **show firmware upgrade result** and press **Enter**.

The firmware upgrade results are displayed in a table. If the firmware upgrade was successful, the *time started* and *time completed* display. For example:

```

C1|S8|L1D>show firmware upgrade result
index  module                      status  reason  time started  time completed
-----
1      C3210-1013 c=1 s=15 l1d  success                05:24:37      05:24:45
2                                     00:00:00      00:00:00
3                                     00:00:00      00:00:00
4                                     00:00:00      00:00:00
5                                     00:00:00      00:00:00
6                                     00:00:00      00:00:00
7                                     00:00:00      00:00:00
8                                     00:00:00      00:00:00
C1|S8|L1D>

```

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

## Upgrading IONMM and/or C3210 Firmware – Web Method

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

**Note:** Doing an IONMM / C3210 firmware upgrade will cause all configuration backup files to be lost.

The steps involved include **A.** Verify the current IONMM / C3210 Firmware version, **B.** Locate the current IONMM / C3210 Firmware version, **C.** Run the TFTP Server, and **D.** either 1. Upgrade IONMM / C3210 Firmware from the **MAIN** tab, or 2. Upgrade IONMM / C3210 Firmware from the **UPGRADE** tab.

### A. Verify the Current IONMM / C3210 Firmware Version

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

1. Access the IONMM via the Web interface.
2. Select the **MAIN** tab and locate the **Software Revision** area in the **Model Information** section. (You can also use the **Help** dropdown and select **About ION System Web Interface** to determine the current firmware version.)
3. Note the current version of the C3210 or IONMM firmware for use in steps D1 and D2 below.

### B. Locate the New IONMM / C3210 Firmware Version

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

1. Go to the Lantronix Firmware Downloads [webpage](#).
2. Locate the “**Agent Firmware**” section and examine the link in the right hand column (e.g., “**Download x222x / x32xx\_1.0.3\_AP.bin**”).
3. Compare the IONMM / C3210 version displayed in the **MAIN** tab **Software Revision** area with the version number on the web site, and continue if the web site version is newer than the current (running) version.
4. Click the link located in step 1 above to download the new firmware file.

### C. Run TFTP Server

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

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

## D. Upgrade the IONMM / C3210 Firmware

Perform this procedure to upgrade the IONMM / C3210 Firmware from either

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

### D1. Upgrade IONMM / C3210 Firmware from the **MAIN** Tab.

1. Access the IONMM card through the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select the **MAIN** tab.
3. Locate the **TFTP Settings** section at the bottom of the screen.

TFTP Settings

TFTP Server Address 192.168.1.30	Firmware File Name 	Status No Action
-------------------------------------	------------------------	---------------------

Save Server Address Upgrade Firmware Refresh

Refresh Save Help

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

TFTP Settings

TFTP Server Address 192.168.1.30	Firmware File Name x323x_1.0.3_AP	Status No Action
-------------------------------------	--------------------------------------	---------------------

Save Server Address Upgrade Firmware Refresh

Refresh Save Help

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

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

7. Click **OK**.

The file is downloaded and the C3210 and/or IONMM reboots. When the reboot is complete, the message “[xx]IONMM rebooting finished” displays.

8. Click the **Refresh** button. The **Software Revision** area is updated from the old version number to the new version number (e.g., from 1.0.1 to 1.0.3).
9. If you will be using the same TFTP Server Address for future upgrades, click the **Save Server Address** button.



## D2. Upgrade IONMM / C3210 Firmware from the **UPGRADE** Tab

1. Access the IONMM card through the Web interface.
2. Select the **UPGRADE** tab.
3. Select the **Firmware Database** sub-tab if not already selected.
4. Locate the **Firmware Database Upload** section.

The screenshot shows the ION System web interface. On the left is a tree view of the ION Stack, with the Chassis expanded to show various ION cards. The main panel has tabs for MAIN, SNTP, HTTPS, SSH, RADIUS, ACL, SNMP, USERS, BACKUP-RESTORE, and UPGRADE. The UPGRADE tab is active, and the Firmware Database sub-tab is selected. The Firmware Database Upload section contains fields for TFTP Server Address (192.168.1.30), Firmware File Name (s210\_0.7.4\_FPGA\_AP.bin), Upload Result, and Upload Result Reason. Below these are buttons for Upload, Refresh, and Help. The Firmware Database Details section contains a table with columns Card Type, Revision, and Firmware File Name.

Card Type	Revision	Firmware File Name
x311x	1.1.0	C3110_1.1.0_AP.bin
IONPS	0.7.2	IONPS_0.7.2_AP.bin
ION219	0.7.2	ION219_0.7.2_AP.bin
x621x	0.7.2	C6210_0.7.2_AP.bin
x321x	0.7.2	C3210_0.7.2_AP.bin
x221x	0.7.2	C2210_0.7.2_AP.bin
x211x	0.7.2	C2110_0.7.2_AP.bin
x323x	0.7.3	x323x_0.7.3_AP.bin
x222x_x322x	0.7.3	x222x_x322x_0.7.3_AP.bin
IONMM	0.7.3	IONMM_0.7.3_AP.bin
x611x_x612x	0.7.3	x611x_x612x_0.7.3_AP.bin
x601x	0.7.3	x6010_0.7.3_AP.bin

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

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

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

MAIN | SNMP | HTTPS | SSH | RADIUS | ACL | BACKUP-RESTORE | **UPGRADE**

Firmware Database | **Firmware Upgrade**

Firmware Database Upload

TFTP Server Address: 192.168.1.30 | Firmware File Name: x222x\_x322x.zip | Upload Result: Success | Upload Result Reason:

Upload Refresh Help

Firmware Database Details

Card Type	Revision	Firmware File Name
x323x	0.5.10	x323x.bin.0.5.10
x222x_x322x	0.5.10	x222x_x322x.bin.0.5.10
IONMM	0.5.10	IONMM.bin.0.5.10

Refresh Help

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

- **None:** no operation was performed, or
- **Failure:** the specified operation has failed.

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

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

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

ION System

ION Stack

- Chassis
  - [01]IONMM
  - [02]C6210-3040
  - [03]C3230-1040
  - [04]C3231-1040
  - [05]C3230-1040
  - [06]C3220-1040
  - [07]C3210-1013
  - [08]C3221-1040
  - [10]C6010-3040
  - [12]C2110-1013
  - [14]C2210-1013
  - [16]C2220-1014
  - [22]IONPS-A
  - [23]IONPS-D

MAIN | SNMP | HTTPS | SSH | RADIUS | ACL | SNMP | USERS | BACKUP-RESTORE | **UPGRADE**

Firmware Database | **Firmware Upgrade**

Targets | Result

Select Target Modules to Upgrade

Select	Index	Module
<input type="checkbox"/>	1	[01]IONMM
<input type="checkbox"/>	2	[02]C6210-3040
<input type="checkbox"/>	3	[03]C3230-1040
<input type="checkbox"/>	4	[04]C3231-1040
<input type="checkbox"/>	5	[05]C3230-1040
<input type="checkbox"/>	6	[06]C3220-1040
<input type="checkbox"/>	7	[06.L2]REM.S3230-1040
<input type="checkbox"/>	8	[07]C3210-1013
<input type="checkbox"/>	9	[08]C3221-1040
<input type="checkbox"/>	10	[10]C6010-3040
<input type="checkbox"/>	11	[12]C2110-1013
<input type="checkbox"/>	12	[14]C2210-1013
<input type="checkbox"/>	13	[16]C2220-1014
<input type="checkbox"/>	14	[22]IONPS-A
<input type="checkbox"/>	15	[23]IONPS-D
<input type="checkbox"/>	16	Chassis(ION219)

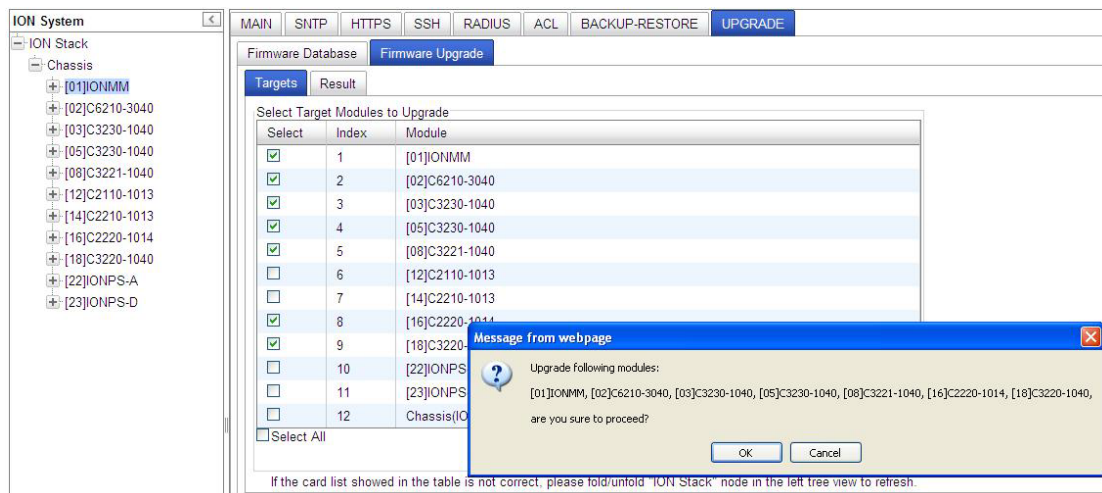
Select All

Upgrade Refresh Help

If the card list showed in the table is not correct, please fold/unfold "ION Stack" node in the left tree view to refresh.

11. In the **Select** column, check the **IONMM** and/or one or more C3210s as the Target Module(s) to be upgraded.

12. Click the **Upgrade** button. A confirmation message displays:



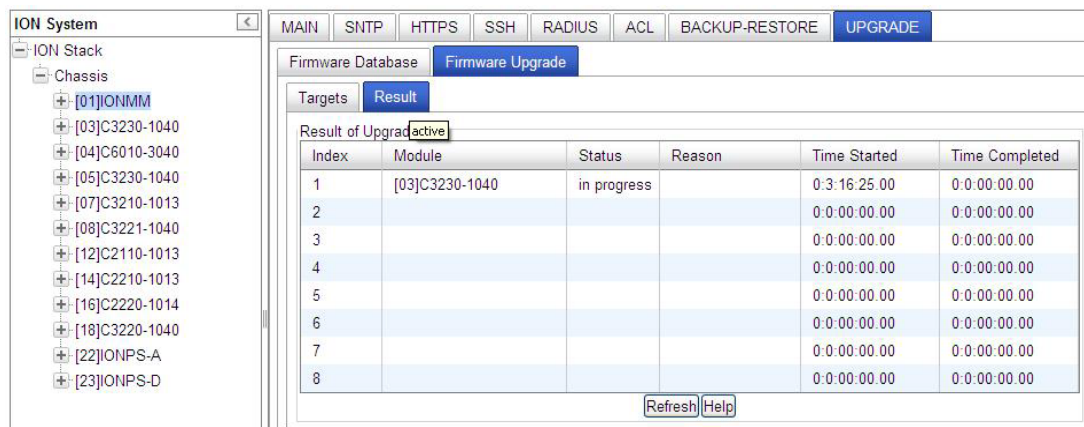
13. Click the **OK** button to proceed.

During the upload, the message "Getting records in progress..." displays.

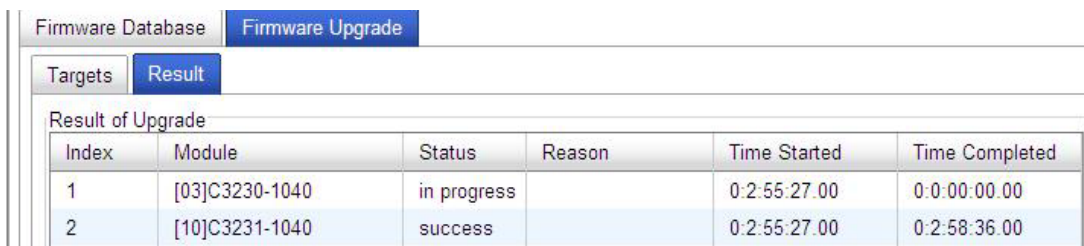
If the upload was successful, the message "Getting all records finished" displays.

If the upload was unsuccessful, "Getting records failed (http server error)" displays.

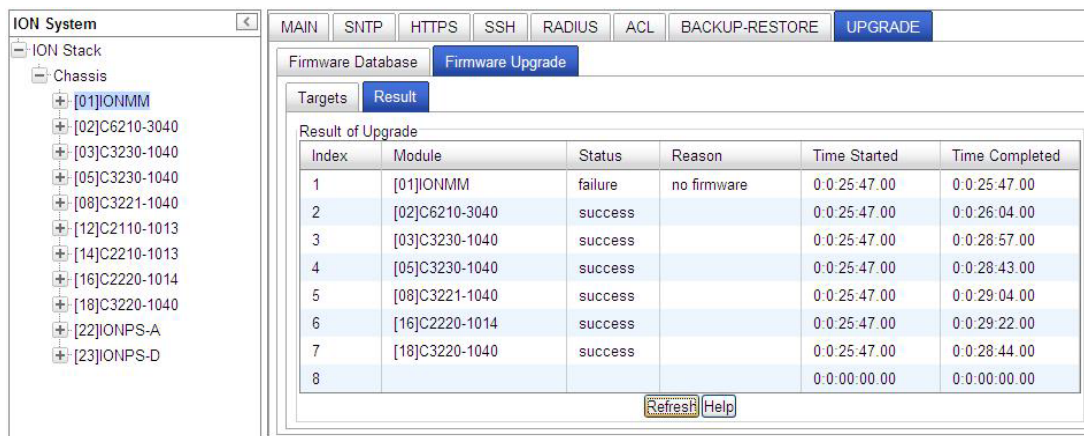
14. Click the **Result** sub-tab. A table displays with upgrade status information.



15. Click the **Refresh** button.

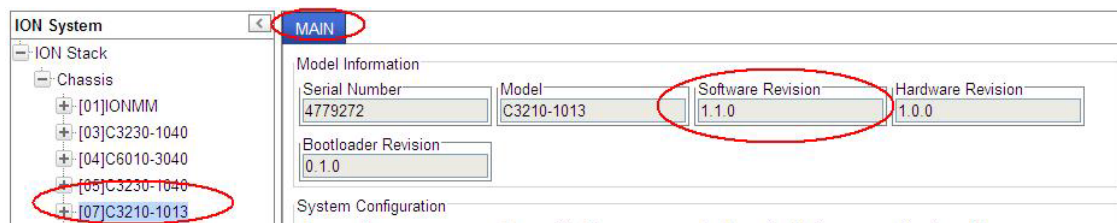


16. If upgrading more than one device, you may have to click **Refresh** again.



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

17. After the upgrade has successfully completed, “*success*” displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See “[Section 6 – Troubleshooting](#)” for error messages and recovery procedures.
18. Check the **MAIN** tab for each upgraded module to ensure that the correct revision level is displayed in the **Software Revision** field.



The sample screen above shows the C3210 **MAIN** tab with the **Software Revision** field indicating a successful firmware upgrade to version **1.1.0**.

## Upgrading Slide-In and Remote Modules Firmware via TFTP

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

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

- Have the upgrade files resident in the default directory on the TFTP Server (normally *C:/TFTP-Root*).
- Create the Database Index and Archive Files (below).
- Perform the Module Firmware Upgrade.

### Creating the Database Index and Archive Files

The database index file is a listing of the modules that can be upgraded and the firmware file that will be used to upgrade each module. The index file must be named **db.idx**. The archive file is a zip file containing the index file and the firmware upgrade files. The archive file must be named **db.zip** in Windows XP, or just “**db**” in Windows 7. The following describes the procedure for creating the firmware database index and archive files.

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

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

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

model rev file

Where:

model = name of the module

rev = revision level of the firmware upgrade file

file = name of the firmware upgrade file

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

**Example:** the example below shows a **db.idx** file for a system that has two modules (IONMM and C3210), and no second level remotes.

```
IONMM 1.0.5 IONMM_1.0.5_AP
C3210 1.1.0 C3210_1.1.0_AP
```

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

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

4. Create a zip file that contains each of the upgrade files and the index file. Save the .zip file to the TFTP Server root directory (e.g., filename of **C3210\_1.1.0\_AP.zip**). For example, using the files listed in the example above, the db.zip file would contain the following files:

- db.idx
- C3210\_1.1.0\_AP
- IONMM\_1.0.5\_AP

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



## Performing the Module Firmware Upgrade

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

1. Access the IONMM through the Web interface.
2. Select the **Upgrade** tab. The **Firmware Database** sub-tab displays.

The screenshot shows the ION System web interface. On the left is a tree view of the ION Stack, including Chassis and various modules like [01]IONMM, [03]C3230-1040, [04]C6010-3040, [05]C3230-1040, [07]C3210-1013, [08]C3221-1040, [12]C2110-1013, [14]C2210-1013, [16]C2220-1014, [18]C3220-1040, [22]IONPS-A, and [23]IONPS-D. The main area has tabs for MAIN, SNTP, HTTPS, SSH, RADIUS, ACL, BACKUP-RESTORE, and UPGRADE. The UPGRADE tab is active, showing sub-tabs for Firmware Database and Firmware Upgrade. The Firmware Database sub-tab is selected, displaying a 'Firmware Database Upload' section with fields for TFTP Server Address (192.168.1.30), Firmware File Name, Upload Result, and Upload Result Reason. Below these are buttons for Upload, Refresh, and Help. A 'Firmware Database Details' section contains a table with columns Card Type, Revision, and Firmware File Name.

Card Type	Revision	Firmware File Name
x222x_x322x	0.6.5	x222x_x322x_0.6.5_AP.bin
x323x	0.6.5	x323x_0.6.5_AP.bin
x621x	0.6.5	C6210_0.6.5_AP.bin
IONPS	0.6.6	IONPS_0.6.6_AP.bin
x601x	0.6.6	C6010_0.6.6_FPGA_AP.bin

3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP Server where the upgrade (zip) file is located.
4. In the **Firmware File Name** field, enter the name of the zip file you created (e.g., **x222x / x32xx.bin.10.5.zip**). **Note:** Be sure to include the .zip extension in the filename.
5. Click the **Upload** button.

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

6. Wait for the file to successfully upload. The messages *"The Firmware Database File is being transferred...."* and *"Getting all records finished"* display during the upload process.

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

**Firmware Database Upload**

TFTP Server Address: 192.168.1.30    Firmware File Name: x222x\_x322x.zip    Upload Result: Success    Upload Result Reason:

Upload Refresh Help

**Firmware Database Details**

Card Type	Revision	Firmware File Name
x323x	0.5.10	x323x.bin.0.5.10
x222x_x322x	0.5.10	x222x_x322x.bin.0.5.10
IONMM	0.5.10	IONMM.bin.0.5.10

Refresh Help

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

**ION System**

- ION Stack
  - Chassis
    - [01]IONMM
    - [02]C6210-3040
    - [03]C3230-1040
    - [05]C3230-1040
    - [08]C3221-1040
    - [12]C2110-1013
    - [14]C2210-1013
    - [16]C2220-1014
    - [18]C3220-1040
    - [22]IONPS-A
    - [23]IONPS-D

**Firmware Upgrade**

Targets Result

Select Target Modules to Upgrade

Select	Index	Module
<input checked="" type="checkbox"/>	1	[01]IONMM
<input checked="" type="checkbox"/>	2	[02]C6210-3040
<input checked="" type="checkbox"/>	3	[03]C3230-1040
<input checked="" type="checkbox"/>	4	[05]C3230-1040
<input checked="" type="checkbox"/>	5	[08]C3221-1040
<input type="checkbox"/>	6	[12]C2110-1013
<input type="checkbox"/>	7	[14]C2210-1013
<input checked="" type="checkbox"/>	8	[16]C2220-1014
<input checked="" type="checkbox"/>	9	[18]C3220-1040
<input type="checkbox"/>	10	[22]IONPS-A
<input type="checkbox"/>	11	[23]IONPS-D
<input type="checkbox"/>	12	Chassis(ION219)

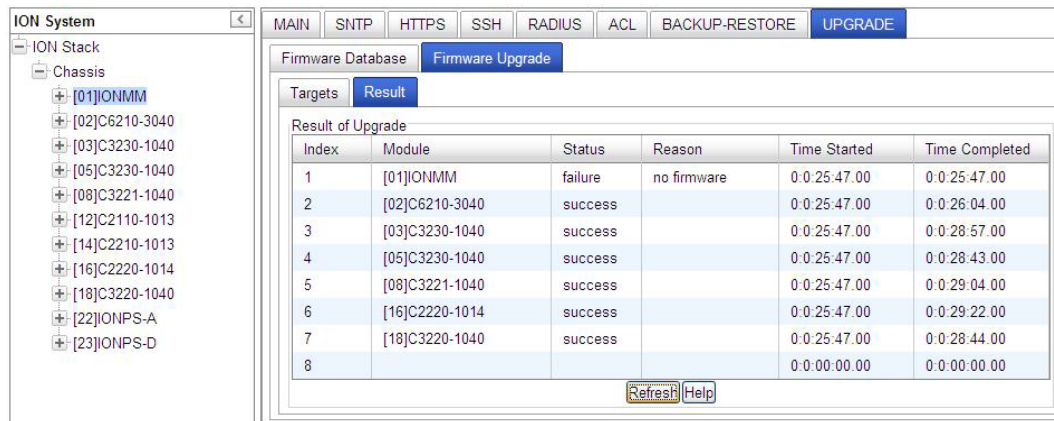
Select All Upgrade Refresh Help

If the card list showed in the table is not correct, please fold/unfold "ION Stack" node in the left tree view to refresh.

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

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

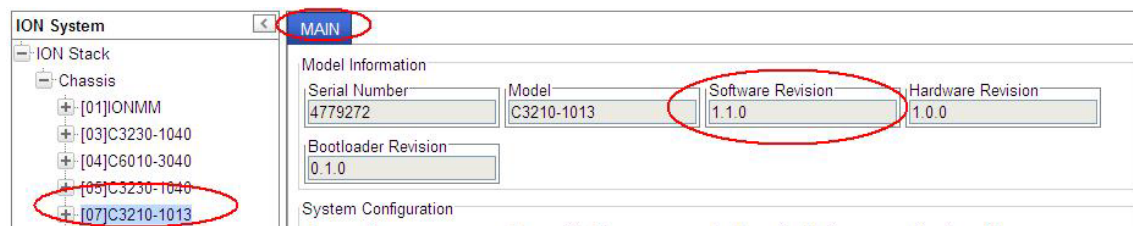
9. Click the **Upgrade** button.
10. When the confirmation window displays, click **OK**.
11. To monitor the progress, select the **Result** sub-tab and click **Refresh**.



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

After the upgrade has successfully completed, “*success*” displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See “[Section 6 – Troubleshooting](#)” for error messages and recovery procedures.

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





## Firmware Upgrade File Content and Location

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

**Table 11: File Content and Location after a Firmware Upgrade**

File Type	Filename	File Description	Stored Directory	Lost after Firmware Upgrade? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	No
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	Yes
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	Yes (1)
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

(1) Exception: after an upgrade from v1.0.3 to v0.5.12, the User Public-Key is not saved. 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. 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). 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.

## 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 similar to the TFTP download function; technical support can download configuration files and firmware files through the C3210 USB port by entering the corresponding CLI commands.

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

Perform this procedure to upgrade the C3210 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:

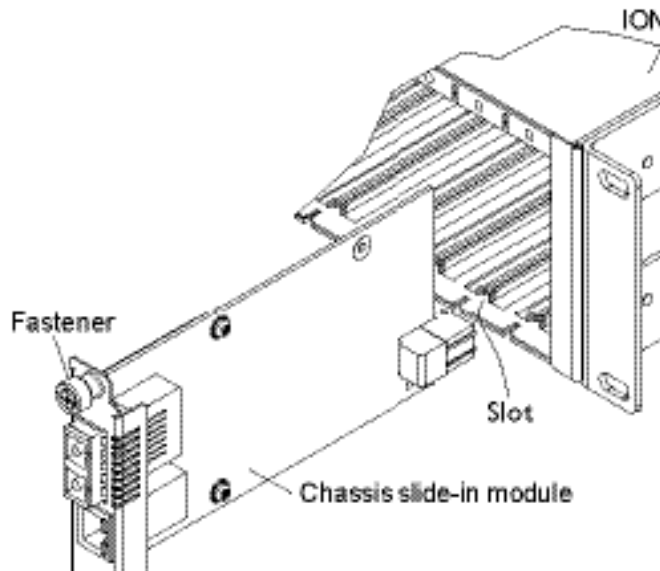
```
C1|S1|L1D>serial ?
  get
  put
  upgrade
C1|S1|L1D>serial get protocol zmodem file=xxxx
Warning: the input file name will be ignored when using ymodem/zmodem to retrieve
file!
now start to transfer the file ...
$CCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file ...
$lsz: 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 ...
**B000000063f694ceive.**B000000063f694
CCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>
```

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.

## Replacing a Chassis Resident C3210

The C3210 is a “hot swappable” device (it can be removed and installed while the chassis is powered on). To replace a chassis resident C3210, do the following.

1. Backup the configuration (see “[Backing Up Slide-In and Remote Modules](#)”).
2. Disconnect any cables attached to the C3210.



3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the C3210 from the ION Chassis.
5. Carefully slide the new C3210 fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the C3210 to the ION chassis.
7. Connect the appropriate cables to the C3210.
8. Load the configuration into the new C3210 (see “[Restoring Slide-In and Remote Modules](#)”).

## 6. 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 C3210 jumpers, and describes where and how to get technical support.

---

#### IMPORTANT

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

---

### Basic ION System Troubleshooting

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

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

- ION Chassis
- ION C3210s (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, 3<sup>rd</sup> party client or server software – RADIUS or TFTP, etc.)

When troubleshooting an ION system / network problem on site:

1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the most simple and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the C3210s 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 product supports the function you are attempting to perform. Your particular product or firmware version may not support all the features documented for this module. For

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

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

## Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED Fault and Activity Displays
- Problem Conditions
- CLI Messages
- Web Interface Messages)
- Windows Event Viewer Messages
- Config Error Log (config.err) File
- Webpage Messages
- Third Party Troubleshooting Messages

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.

### LACT (Link Activity) 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”](#)). Download the latest firmware version and upgrade as necessary.

### Fault LED is lit:

1. Check for a problem with the IONMM, software, or configuration.
2. Make sure all circuit protection and connection equipment and devices are working.
3. Verify that the ION system power supply is within operating range.
4. Remove the card from the chassis and re-insert it.
5. Make sure the USB cable is properly connected.
6. Reset the IONMM.

### TX or RX LED off (not flashing):

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

## Problem Conditions

**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 C3210 via the Web Interface**

1. Can you access the IONMM?

Yes	No
Continue with Step 2.	See “ <a href="#">Cannot access the IONMM via the Web</a> ”.

2. Power cycle the C3210.
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.

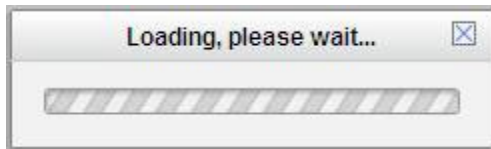
The device may have a jumper or switch that disables software management of the device. When Configuration Mode is **hardware**, the devices take some of the configurations from DIP switches or jumpers on the device. In **software** mode, configuration is controlled by management.

1. Refer to the "[Jumper Settings](#)" section 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](#)".

### *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. Refresh the IONMM or C3210 by clicking the **Refresh** key.
3. Collapse and then expand the ION System tree (i.e., fold and then unfold the "ION Stack" node in the left tree view) to refresh.
4. Cycle power for the module in question.
5. Upgrade the devices to the latest software version.
6. Reboot the device by clicking the **Reboot** key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
7. 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 C3210 is at an older version and shows the newer functions as 'red boxed'. Since the older version of C3210 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as 'red boxed'. Upgrade the devices to the latest software version.
3. Reboot the system. See the "[Reboot](#)" section for more information.
4. Contact Lantronix for more information. Contact Technical Support.

**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.

**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** can not 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 *C3210 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 *C3210 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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)**
2. Retry the operation. For a complete list of the available commands, see the *C3210 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 C3210 does not support this function. Use another command or switch to a C3210 that supports OAM.
2. For a complete list of the available commands, see the *C3210 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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)**
2. Retry the operation. For a complete list of the available commands, see the *C3210 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 *C3210 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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)**
2. Retry the operation. For a complete list of the available commands, see the *C3210 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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)**
2. Retry the operation. For a complete list of the available commands, see the *C3210 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 can not be established.

1. Verify that the correct hierarchy has been specified in the command (see [“Managing Slide-In and Remote Modules Using CLI Commands”](#)).
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 *C3210 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 *C3210 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.
2. Retry the operation. See the related DHCP command in *the C3210 CLI Reference Manual*, 33497.
3. If the problem persists, contact Technical Support.

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

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

1. Make sure this is the command / function you want.
2. See the commands in *the C3210 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 can not detect the presence of the device or port specified in the **go** command.

1. Verify that the correct hierarchy has been specified in the command (see ["Managing Slide-In and Remote Modules Using CLI Commands"](#)).
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 C3210s 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 <a href="#">step 4</a> .	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.

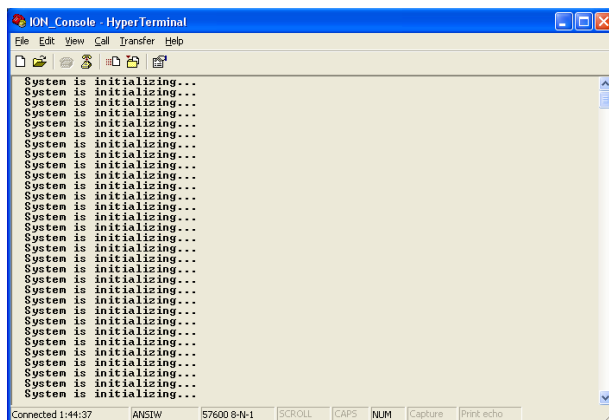
Enter the **go** command and be sure to include all of the location parameters.

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

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 *C3210 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 *C3210 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] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

**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 *C3210 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 *C3210 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](#)” 7.
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](#)”.
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.

**Cannot set remote fault detect state on this card!**

The attempted **set rfd state** command was rejected: C1|S7|L1D>set rfd state enable

1. Verify that the card you entered the command on supports this function. See [Set RFD State](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *C3210 CLI Reference Manual*, 33497..
3. If the problem persists, contact Technical Support.

**Fail to set aging time!**

The attempted **set dot1bridge aging-time** command was not able to complete.

1. Verify the **dot1bridge aging-time** command syntax. See [Configure Forwarding Learning Aging Time](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *C3210 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support.

**Get aging time failed!**

The attempted show dot1bridge aging-time command failed to complete.

1. Verify the **dot1bridge aging-time** command syntax. See [Configure Forwarding Learning Aging Time](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *C3210 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support.

**CLI command remove fwddb all failed**

The attempted C3220-1040 Backup/Restore failed during the restore; the restore displays "ongoing" status, and will not succeed.

The dynamic MAC address should not be backed up or restored - only static entries should be backed-up and restored.

1. Retry the operation. See "[Backup/Restore Operations](#)".
2. See the *C3210 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support.

**The format of Ethtype value should like 0x8810, 0x88a8 etc.**

The attempted CLI command entry failed (e.g., set dot1bridge).

1. Retry the operation with the correct parameter entry.
2. See the *C3210 CLI Reference Manual, 33497* for the full set of available command parameters.
3. If the problem persists, contact Technical Support.

**Redundancy is not supported on this card!**

The attempt to set or show fiber redundancy failed. For example, you entered the command: **show redundancy info**, but the device does not support fiber redundancy.

1. Verify that the card you entered the command on supports this function.
2. Retry the operation on a card that supports this function. See the "[Fiber Redundancy Commands](#)" section of the related manual.
3. 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](#)”.
2. If the problem persists, contact Technical Support.

**Fail to set SSH server state!**

You entered the command **set ssh server state=enable**, but have not generated an ssh host key.

1. This command / function is not supported on the C3210. Try a different command or switch to another device that supports this command / function.
2. If the problem persists, contact Technical Support.

**Fail to set management VLAN id!****Fail to set management VLAN state!**

You entered the command **set mgmt vlan state** or **set mgmt vlan port** or **set mgmt vlan vid** to enable or configure Management VLAN, but the operation failed.

1. Verify the VLAN Management configuration using the **show vlan** command and the **show vlan service** command.
2. Review the set mgmt vlan command syntax for the port / state / vid. See the “[VLAN Commands](#)”.
3. If the problem persists, contact Technical Support.



**Upgrade is only supported on IONMM card!**

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

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

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

**Cannot set bandwidth alloc type on this card!**

You entered the command **set bw alloc-type countAllLayerx** on a card that does not support it.  
For example:

```
C1|S7|L1P1>set bw alloc-type countAllLayer2
Cannot set bandwidth alloc type on this card!
```

1. Verify if the card supports bandwidth allocation.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See “[Bandwidth Commands](#)”.
4. If the problem persists, contact Technical Support.

**Cannot set ingress and egress rate on this card!**

You entered the command **set irate=xx erate=xx** on a card that does not support it. For example:

```
C1|S7|L1P1>set irate noLimit erate noLimit
Cannot set ingress and egress rate on this card!
```

1. Verify if the card supports rate limiting.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See “[Bandwidth Commands](#)”.
4. If the problem persists, contact Technical Support.

**DMI is only supported on FIBER port!**

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

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

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

**Link OAM is not supported on this card!**

You entered the command **show oam rx loopback control** on a card that does not support it. For example:

```
C1|S7|L1P1>show oam rx loopback control
Link OAM is not supported on this card!
```

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

Cannot clear loopback counters on this card!  
Cannot set administrate state on this port!  
Cannot set advertisement capability on this port!  
Cannot set autocross on this card!  
Cannot set auto negotiation state on this port!  
Cannot set Ethernet port speed for this card!  
Cannot set Ether port duplex mode on this card!  
Cannot set far end fault on this card!  
Cannot set filter unknown dest multicast frames on this port!  
Cannot set filter unknown dest unicast frames on this port!  
Cannot set pause on this port!  
Cannot set source address lock action on this port!  
No Time-domain reflectometer support on this card!  
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!

You entered a command (e.g., **clear ether all counters**) for a function not supported on the card.  
For example:

```
C1|S7|L1P1>clear ether all counters
Cannot clear loopback counters on this card!
```

1. Verify if the card supports the desired function. See Table 3 in the section “[Ethernet Port Commands](#)”.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. The command functions include 1) admin, 2) adv-cap, 3) autocross, 4) autoneg, 5) duplex, 6) fef, 7) filter-unknown-multicast, 8) filter-unknown-unicast, 9) loopback, 10) pause, 11) speed, and 12) src-addr-lock, 13) tdr, 14) ether security config, 15) fwddb, etc.

**Cannot show port QoS configuration in this card!**

**Cannot show port QoS priority remapping 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!**

You entered a QoS command for a function not supported on the card. For example:

```
C1|S7|L1P1>show qos config
Cannot show port QoS configuration in this card!

C1|S7|L1P1>show qos priority remapping
Cannot show port QoS priority remapping in this card!
```

1. Verify if the card supports the desired function.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. See “[QoS Commands](#)”.

**Cannot get VLAN database configuration on this card!**

You entered a VLAN command for a function not supported on the card. For example:

```
C1|S7|L1D>show vlan
Cannot get VLAN database configuration on this card!
C1|S7|L1D>show vlan service
Cannot show VLAN service configuration on this card!
```

1. Verify if the card supports the desired function.
2. Use the **go** command to switch to a different card port supporting VLAN.
3. Verify the command entry. See “[VLAN Commands](#)”.

**Fail to get system name!**

You entered a command for system information, but the information on the card was not available. For example:

```
C1|S10|L1D>show card info
Fail to get system name!
```

1. Try entering the **show cardtype** command.
2. Select the **MAIN** tab > **System Configuration** section > **System Name** field, and verify the name and for the device.
3. Use the **set system name** command to enter the **System Name** information (e.g., **set system name=NAME**). Make sure no spaces are included in the name text.
4. Remove and reset the card.
5. Try the operation again.

6. If the problem persists, contact Technical Support.

**Set system name timeout.**

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

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

1. Use the set system name command to enter the System Name information (e.g., **set system name=NAME**) without any special characters (e.g., without the ! or # or % or & characters).
2. Remove and reseat the card.
3. Try the operation again.
4. Select the **MAIN** tab > **System Configuration** section > **System Name** field, and verify the name for the device (e.g., no spaces between characters).
5. If the problem persists, contact Technical Support.

**System is busy, please retry this command later!**

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

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

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

**Get HTTPS state no such object.**

**Get management VLAN state no such object.**

**IP management state no such object.**

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

```
C1|S10|L1D>show https config
HTTPS configuration:
-----
Get HTTPS state no such object.
C1|S10|L1D>show mgmt vlan config
vlan id    vlan state          vlan portlist
-----
Get management VLAN state no such object.
C1|S10|L1D>show ip-mgmt config
IP management configuration:
-----
IP management state no such object.
```

1. Wait 1-2 minutes and then retry the command.
2. Verify if the card supports the desired function.
3. Use the **go** command to switch to a different card / port supporting the desired feature.
4. Verify the command entry. Reboot the system and then retry the command.
5. 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 fe 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.

**Can not set 1000M speed for this card!**

You tried to use the **set ether speed** command to set the device's speed to 1000 Mbps (1 Gbps), but the card you entered the command on does not support this speed. For example:

```
C1|S16|L1P1>set ether speed=1000M
Can not set 1000M speed for this card!
C1|S16|L1P1>
```

1. Use the **set ether speed ?** command to determine the card's speed capabilities.
2. Re-enter the **set ether speed= command** with a speed supported by the card.
3. If the problem persists, contact Technical Support.

**Fail to set Ethernet port speed!**

You tried to use the **set ether speed** command to set the device's speed, but the command was not accepted. For example:

```
C1|S16|L1P1>set ether speed 1000
Fail to set Ethernet port speed!
C1|S16|L1P1>
```

1. Verify the command syntax; for example make sure you entered "10M" or "100M", etc.
2. Use the **set ether speed ?** command to display the card's speed capabilities.
3. Re-enter the **set ether speed= command** with a speed supported by the card.
5. If the problem persists, contact Technical Support.

**Invalid pause value!**

You tried to use the **set ether pause** command to set the device's pause mode / value, but the value was not accepted. For example:

```
C1|S16|L1P1>set ether pause=bpause
Invalid pause value!
```

1. Use the **set ether pause ?** command to display the card's pause capabilities.
2. Configure the device for full duplex mode; only stations configured for full duplex operation can send pause frames.
3. Select another pause type – nopause, apause (asymmetric), bpause (asym/sym), pause (the port will advertise it has pause capability), or spause (symmetric).
4. If the problem persists, contact Technical Support.

**Current VLAN tagging mode is not 'provider'!**

You tried to set the port VLAN tag type, but the current tag mode doesn't match. For example:

```
C1|S16|L1P2>set port vlan tag provider ethtype=x8100
Current VLAN tagging mode is not 'provider'!
```

1. Set the VLAN tag mode to the desired mode using the **set port vlan tag mode** command.
2. Verify if the card supports the desired function.
3. Use the **go** command to switch to a different card / port supporting the desired feature.
4. If the problem persists, contact Technical Support.

**Cannot set VLAN network tagging on this port!**

You tried to set the port's VLAN tag type, but the device does not support it. For example:

```
C1|S16|L1P2>set port vlan tag network tagging addTag
Cannot set VLAN network tagging on this port!
```

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports VLAN tagging.
3. Try entering the **set port vlan tag** command again.
4. If the problem persists, contact Technical Support.

**Cannot show system information on this card!**

You entered the **show system information** command from an unsupported device. For example:

```
C1|S22|L1D>show system information
Cannot show system information on this card!
```

1. Use the **go** command to switch to a different device (e.g., from the Power Supply to the IONMM or an x323x card).
2. Try entering the **show system information g** command again.
3. If the problem persists, contact Technical Support.

**Fail to set management VLAN id!**

You tried to set the Management VLAN ID, but the VLAN ID was not accepted. For example:

```
C1|S18|L1D>set mgmt vlan port=2
Fail to set management VLAN id!
```

1. Verify the Management VLAN state setting (**set mgmt vlan state** command).
2. Verify the Management VLAN port setting (**set mgmt vlan port** command).
3. Try setting the Management VLAN ID again.
4. If the problem persists, contact Technical Support.

**Invalid forward port list!**

You entered an invalid parameter in response to a prompt (e.g., for a module number for firmware upgrade). For example:

```
C1|S7|L1D>upgrade module
Available modules:
index      module                                loc
-----
1          ION219                                c=1 s=0 l1d
2          C3230-1040                            c=1 s=3 l1d
3          C3230-1040                            c=1 s=5 l1d
4          S3230-1040                            c=1 s=5 l1ap=2 l2d
5          IONMM                                 c=1 s=7 l1d
6          C3231-1040                            c=1 s=10 l1d
7          C2220-1014                            c=1 s=16 l1d
8          C3220-1040                            c=1 s=18 l1d
9          IONPS-A                               c=1 s=22 l1d

Choose the module you want to upgrade: (eg. 1,3,16; at most 8 modules to up-
grade, press 'q' to exit upgrade)
show card info

Invalid forward port list!
```

1. Re-enter the command, wait for the prompt, and then enter a response in the correct syntax.
2. See the related command / function section of this manual.
3. For a complete list of the available commands, see the *C3210 CLI Reference Manual*, 33497.



4. If the problem persists, contact Technical Support.

**L2CP is not supported on this card!**

You tried to perform an L2CP function but the device does not support L2CP.

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports L2CP.
3. Try entering the command again. See “[Configuring L2CP](#)”.
4. If the problem persists, contact Technical Support.

**Please reboot the card for the changes to take effect!**

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

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

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

**Get DMI identifier no such object.**

You entered the CLI command to display DMI information, but it was not available. For example:

```
C1|S3|L1P2>show dmi info
Get DMI identifier no such object.
C1|S3|L1P2>
```

1. Make sure this is the command / function that you wanted.
2. Try entering the command again. See “[DMI \(Diagnostic Maintenance Interface\) Parameters](#)”.
3. If a problem persists, contact Technical Support.

**Get SNMP version no such object.**

You entered the CLI command to display SNMP configuration information, but it was not available. For example:

```
C1|S3|L1D>show snmp config
SNMP configuration:
-----
Get SNMP version no such object.
C1|S3|L1D>
```

1. Make sure this is the command / function that you wanted.
2. Verify the command syntax. See “[Configuring SNMP](#)” on page 245.
3. For complete command descriptions, see the *C3210 CLI Reference Manual*, 33497.
4. Try entering the command again. See “[DMI \(Diagnostic Maintenance Interface\) Parameters](#)”.
5. If a problem persists, contact Technical Support.

**Fail to get cable length**

You entered a VCT test / show cable length command but the Time Domain Reflector (TDR) test failed. For example, you entered **start ether tdr test** and pressed **Enter**.

1. Make sure the device supports the VCT Test (TDR Test) or the **show cable length** command (available for x2110).
2. Make sure you enter the Time Domain Reflector (TDR) test on an Ethernet copper port.
3. Verify the command syntax. See “[Virtual Cable Test \(VCT\)](#)”.
4. Type **show ether tdr config** to show the Ethernet port TDR Test configuration.
5. If the problem persists, contact Technical Support.

**Can not set speed on this port!**

You entered the CLI command to define the C3210 port’s operating speed, but the command failed. For example:

```
C1|S5|L1P2>set ether speed 100M
Can not set speed on this port!
C1|S5|L1P2>
```

1. Verify the C3210 supports this speed.
2. Verify the command syntax.
3. Re-enter the **set ether speed=** command with a speed supported by the card.
4. If the problem persists, contact Technical Support.

**Fail to set port advertisement capability!**

This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability (set ether adv-cap) command are not valid choices. For example:

```
C1|S5|L1P2>set ether adv-cap 1000XFD
C1|S5|L1P2>set ether adv-cap 1000XHD
Fail to set port advertisement capability!
C1|S5|L1P2>
```

1. Verify the C3210 supports this capability.
2. Verify the command syntax.
3. Retry the operation. For a complete list of the available commands, see “Appendix A: CLI Command Summary”.
4. If the problem persists, contact Technical Support.

### Long Command Causes Cursor Wrap to Same Line

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

```

C:\Telnet 192.168.0.101
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>show acl condition
index      type      src/dst  operation value      state      rule idx
-----
1          macaddr  src      equal    00:ee:ee:02:da:1a    active     1
2          ipv4addr  src      equal    172.16.6.123        notInService 0
123S16:|L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.1
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>
C1:S16:|L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.1
C1:S16:|L1D>

```

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

### 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. Contact Technical Support.

### Auto-negotiation is enabled, you can not set port speed now!

You entered a command to set the port speed, with the Auto-negotiation feature enabled; the Auto-negotiation function takes precedence.

1. Make sure of the port speed that you want.
2. Use the **set ether autoneg state** command and/or the set ether speed command as required.
3. If the problem persists, contact Technical Support.

**Cannot create VLAN database on this card!**

This model of NID does not support the VLAN database. For example:

```
C1|S7|L1D>add vlan-db vid 2 priority=5 pri-override=enable
Cannot create VLAN database on this card!
C1|S7|L1D>
```

1. Make sure this is the function that you want.
2. Use the **go** command to switch to a NID that supports the VLAN database.
3. Re-enter the **add vlan-db** command.
4. If the problem persists, contact Technical Support.

**Cannot remove vlan on this card!**

You entered a command to delete one or all VLANs from the NID, but the action cannot be performed. For example:

```
C1|S7|L1D>remove vlan all
Cannot remove vlan on this card!
C1|S7|L1D>remove vlan vid=3
Cannot remove vlan on this card!
C1|S7|L1D>
```

1. Make sure this is the function that you want.
2. Use the **go** command to switch to a NID that supports the VLAN database.
3. Use the **add vlan-db** command to add a VLAN VID if needed.
4. If the problem persists, contact Technical Support.

**Cannot remove forward database rows on this card!**

You entered a command to delete a VLAN forward database VID (forward database row) from the NID, but the action cannot be performed. For example:

```
C1|S7|L1D>remove vlan-db vid 3
Cannot remove forward database rows on this card!
C1|S7|L1D>
```

1. Make sure this is the function that you want.
2. Use the **go** command to switch to a NID that supports the VLAN FDB.
3. If the problem persists, contact Technical Support.

**The specified conn-port does not exist!**

You specified a connection port (conn-port) number outside the valid range.

1. Make sure this is the function that you want.
2. See “[Configuring MAC Address Filtering](#)” for more information.
3. If the problem persists, contact Technical Support.

**The specified monitor-port does not exist!**

You specified a monitoring port (monitor-port) number outside the valid range.

1. Make sure this is the function that you want.
2. See the related section (e.g., “Redundancy” or “Link Pass Through”) for more information.
3. If the problem persists, contact Technical Support.

**Cannot show cable length for fiber port!**

You entered the command to display the length of the copper cable for a port that does not support it.

1. Make sure the NID supports the **show cable length** command (only for x2110).
2. Verify the command syntax. See the related *User Guide* manual.
3. Type **show ether config** to show the Ethernet port’s configuration.
4. If the problem persists, contact Technical Support.

**Auto-negotiation is enabled, you can not set port duplex now!**

You entered the command to assign a duplex mode, but the command is not functional if Auto-negotiation is currently enabled.

1. Either leave the Auto-negotiation setting and use the current duplex setting, or disable AutoNegotiation and set the Duplex mode as required.
2. See the “[Set Ethernet Port Speed / Duplex Mode](#)” section for more information.
3. Use the **show ether config** command to display the current Auto-negotiation and Duplex settings.
4. If the problem persists, contact Technical Support.

**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 C3210. 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 C3210.
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!**

You entered the command to set or show a port mgmt. access function, but the C3210 does not support it. For example:

```
C1|S15|L1P1>set port mgmtaccess enable
Cannot set if this port can be managed by CPU on this card!
C1|S15|L1P1>
```

1. Review the related command section of this manual.
2. Verify that this NID supports the function attempted.
3. Try a related function on this NID.
4. Switch to another NID and try this function again.
5. If the problem persists, contact Technical Support.

**Cannot set USB port state on this card!**

You entered the command to set or show the current USB port state, but the C3210 does not support it. For example:

```
C1|S15|L1D>set usb state enable
Cannot set USB port state on this card!
C1|S15|L1D>
```

1. Review the related command section of this manual.
2. Verify that this NID supports the function attempted.
3. Try a related function on this NID.
4. Switch to another NID and try this function again.
5. If the problem persists, contact Technical Support.

**tftp get: set address type failed.**

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

```
C1|S15|L1D>tftp get ip type ipv4 ipaddr 192.168.1.30 remotefile C3210_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.
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!**

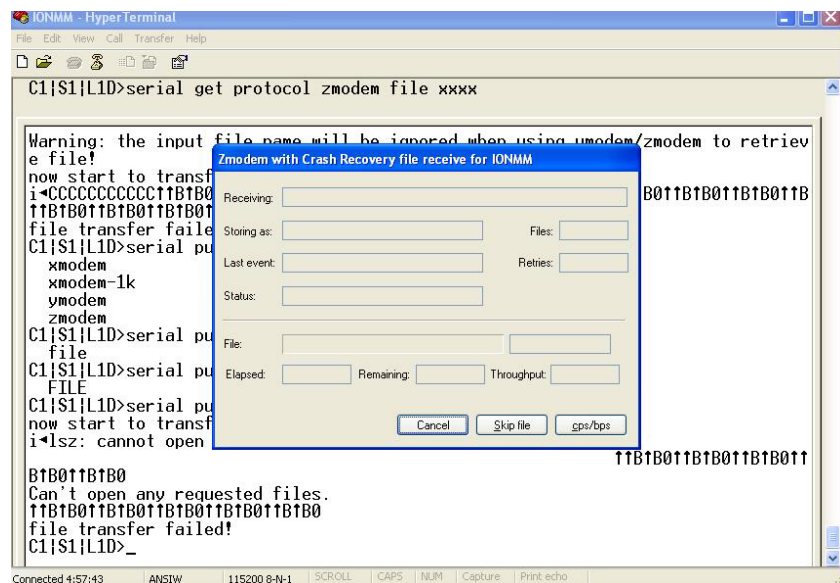
**Warning: xmodem/xmodem-1k protocol might append some garbage at the end of the file!**

**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.
3. If the problem persists, contact Technical Support.

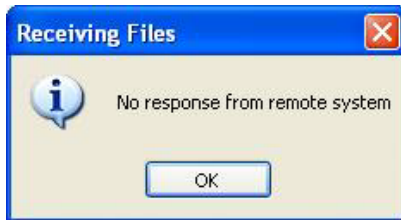
***File Transfer Failed*** - ZModem Crash Recovery dialog box:



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<sup>3</sup>.
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.
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 C3210 Firmware](#)”.
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 C3210 Firmware](#)”.
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.

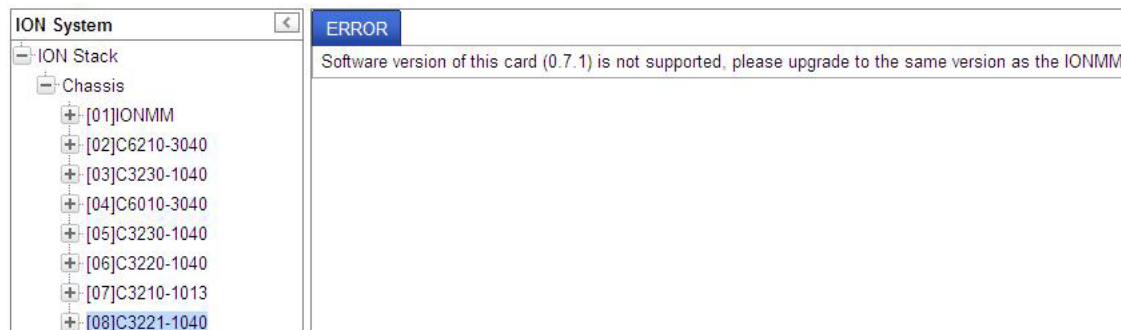
1. Enter another (supported) function at this card's firmware version, or use the "**go**" command to switch to another card.
2. Upgrade to a newer firmware version. See "[TFTP Transfer / Upgrade Commands](#)" or "[Upgrade / Update Firmware Commands](#)".
3. Retry the operation.
4. If the problem persists, 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.
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" can not be added to Member Ports for Management VLAN.
2. If a 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 can not 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](#)” 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.

1. Verify that the C3210 supports DMI.
2. See [“DMI \(Diagnostic Maintenance Interface\) Parameters”](#) for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

**Admin Status: Down (or Testing)**

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

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

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

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

This is the current operational state of the interface.

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

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

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

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

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

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

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

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see “[Section 2: Installation and System Setup](#)”.
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization to take place.
5. If the problem persists, contact Technical Support.

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

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

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

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



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

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

**Message: *Setting values failed (http server error)***

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

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

**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](#)”.
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.

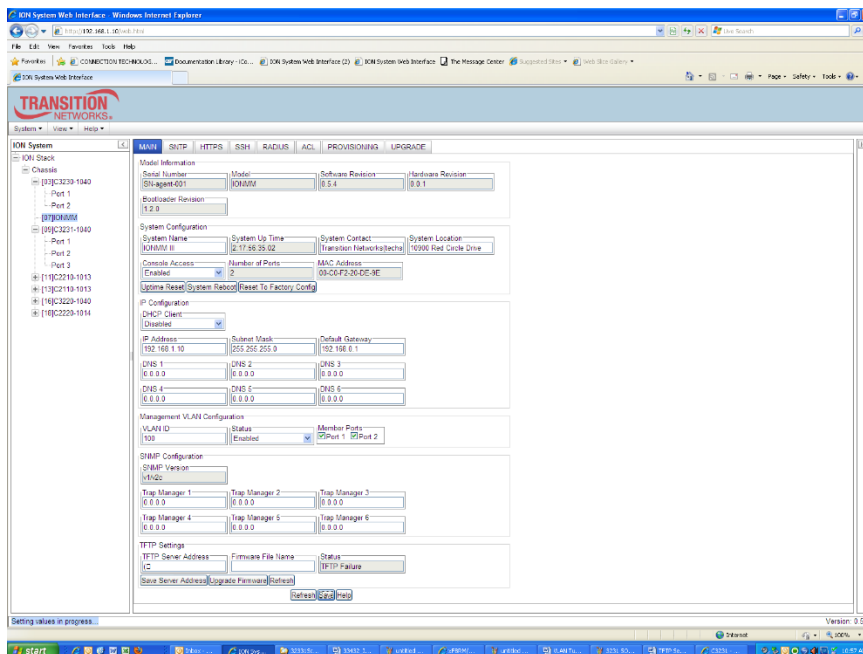
1. Click the [Continue to this website...](#) selection.
2. See the [“Configuring HTTPS”](#) section.

**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.

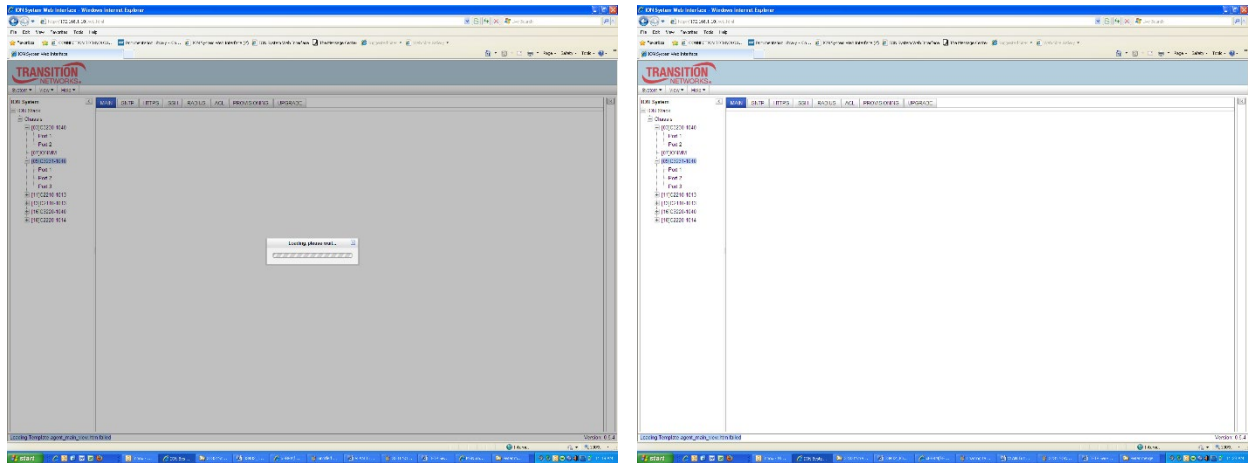
**Message: "Setting values in progress ..."** displays continuously

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 C3210 models support DMI. Lantronix C3210s that support DMI have a “D” at the end of the model number. If you click the DMI tab on a C3210 model that does not support DMI, the message “The DMI feature is not supported on current port.”

The DMI (Diagnostic Maintenance Interface) function displays C3210 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.

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

**Message:** *Loading Template agent\_main\_view.htm failed*

**Message:** *Loading htm files failed*

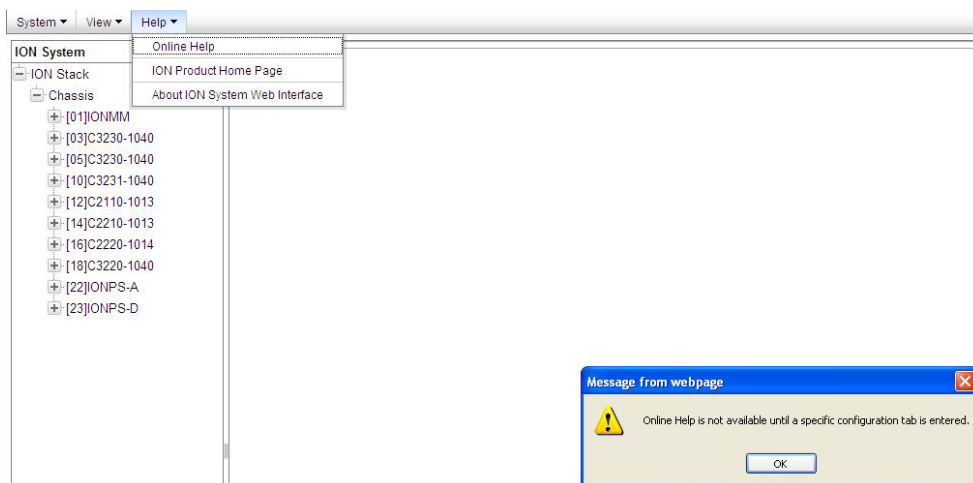
**Meaning:** The status displays at the lower left corner during Port 1 page loading.

**Recovery:** 1. Wait for the *Loading, please wait...* message to clear. This may take 1 minute or more. 2. See the *Loading, please wait...* message for details. 2. If the problem persists, contact Technical Support.

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



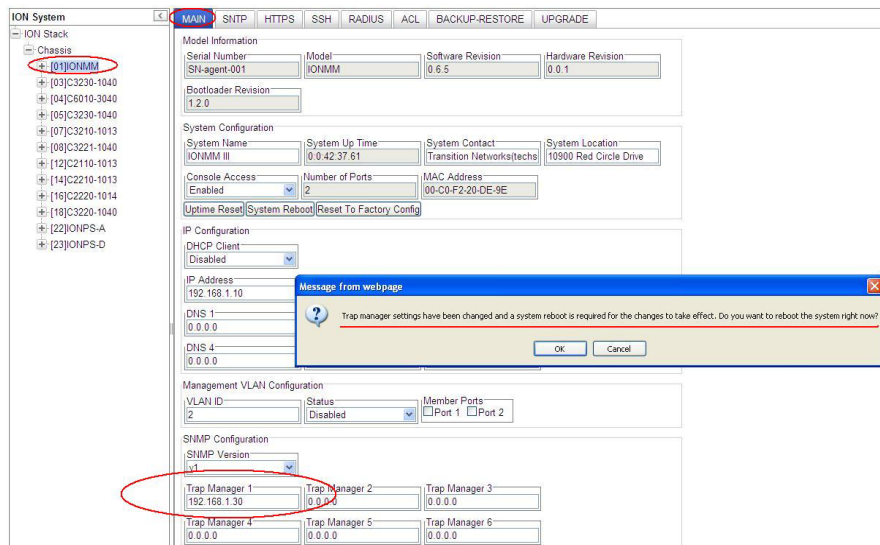
**Meaning:** You clicked on **Online Help** from the **Help** dropdown without first selecting a device.



**Recovery:**

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

**Message:** *Trap manager settings changed and a system reboot is required for the changes to take effect.*  
– Do you want to reboot the system right now?

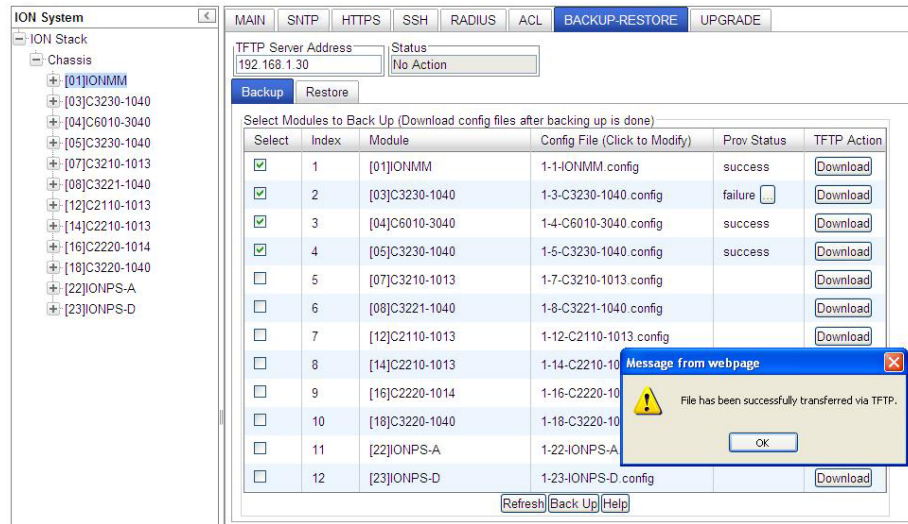


**Meaning:** Information only. At IONMM > MAIN > SNMP Configuration > Trap Manager x you entered an IP address for a trap server.

**Recovery:**

1. Click the **OK** button to clear the webpage message.
2. Verify the Trap Manager setting and continue operation.
3. If a problem persists, contact Technical Support.

**Message:** *File has been successfully transferred via TFTP."* but the Prov. status column displays failure [...].

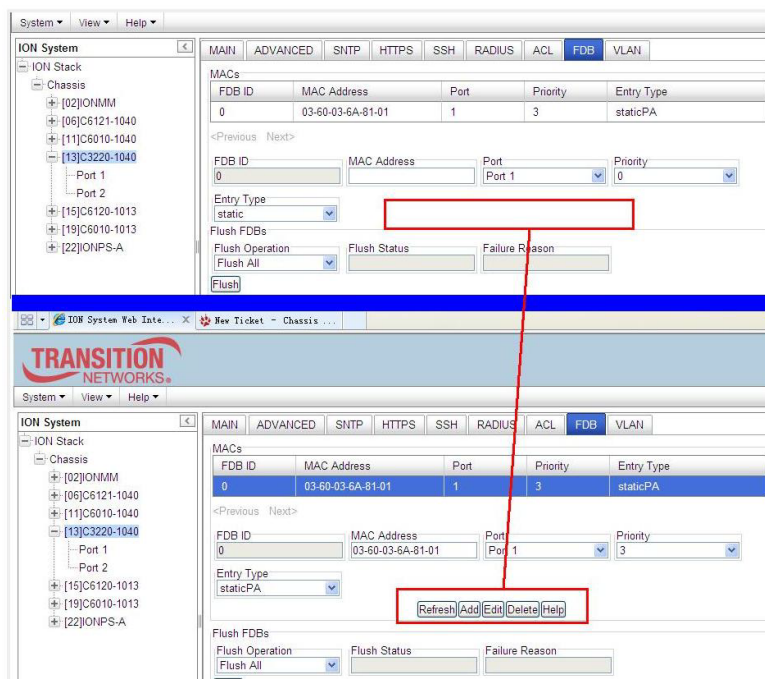


**Meaning:** At IONMM > BACKUP-RESTORE > Backup you selected a module to back up, the “successful transfer” message displays, but the Prov. Status column displays failure [...].

**Recovery:**

1. Click the **OK** button to clear the webpage message.
2. Click the [...] box after the word “failure” in the Prov Status column.
3. Open the config.ERR file at C:\TFTP-Root.
4. Fix any config commands and then retry the operation.
5. Verify the Backup and continue operation.
6. If a problem persists, contact Technical Support.

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.



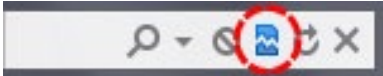
2. Log in to the ION system again.
3. Select the **FDB** tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
4. Click one existing MAC address in the MAC address list.



### 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.

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>.

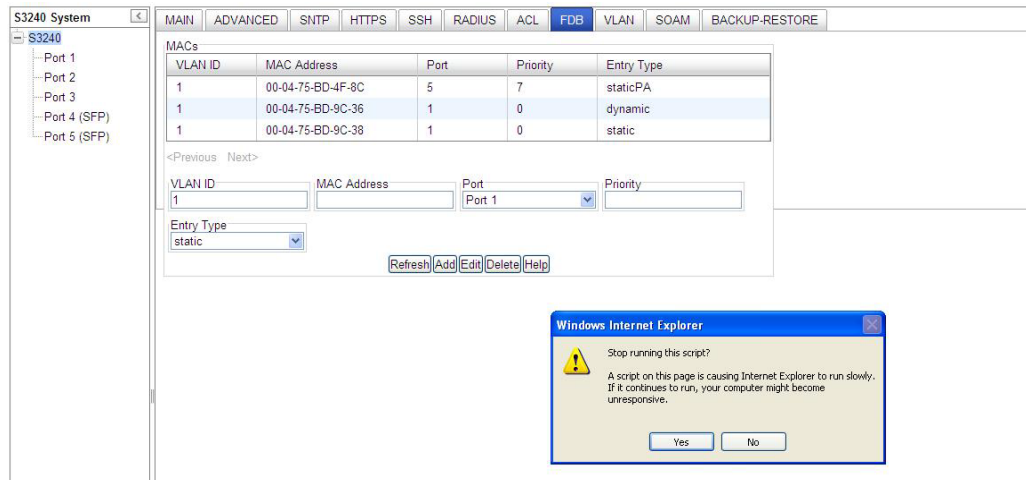
**Script error message received.**

**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.**



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 7:37:12 AM 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

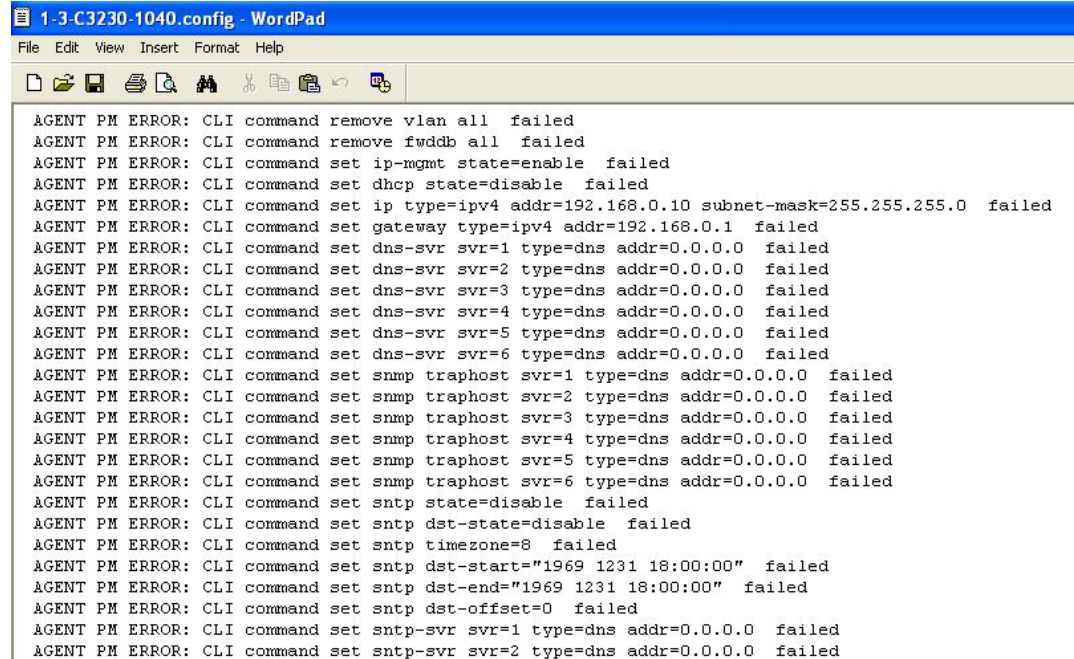
**Meaning:** Warning level message regarding W32Time.

**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-C3220-1040\_20100608.config.err*.

The first word in the message (e.g., add, set, remove) shows the type of action attempted.

The second word or phrase in the message (e.g., dhcp state, fwddb, gateway type, vlan-db vid, etc.) lists the general function attempted. This is the part of the message immediately preceding the = sign.

The next word or phrase in the message is the specific function attempted that immediately follows the = sign or the second word of the message (e.g., all, =enable, =disable, =8, =dns addr=0.0.0.0, etc.). This part of the error message may include several segments with = signs (e.g., =0.0.0.0 retry=3 timeout=30

The final word in the message line is the word "failed".

## config.err Messages

Sample config.err file information is provided below.

1-2-2-C3220-1040\_20100608.config.err

Line

```
1 AGENT PM ERROR: CLI command remove vlan all failed
2 AGENT PM ERROR: CLI command remove fwddb all failed
3 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:10 conn-port=1 priority=1 type=staticNRL failed
4 AGENT PM ERROR: CLI command remove vlan all failed
5 AGENT PM ERROR: CLI command remove fwddb all failed
6 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:02 conn-port=1 priority=1 type=staticNRL failed
7 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:03 conn-port=1 priority=1 type=staticNRL failed
8 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:04 conn-port=1 priority=1 type=staticNRL failed
9 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:05 conn-port=1 priority=1 type=staticNRL failed
10 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:06 conn-port=1 priority=1 type=staticNRL failed
11 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:07 conn-port=1 priority=1 type=staticNRL failed
12 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:08 conn-port=1 priority=1 type=staticNRL failed
13 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:09 conn-port=1 priority=1 type=staticNRL failed
14 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:10 conn-port=1 priority=1 type=staticNRL failed
15 AGENT PM ERROR: CLI command remove vlan all failed
16 AGENT PM ERROR: CLI command remove fwddb all failed
17 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:02 conn-port=1 priority=1 type=staticNRL failed
18 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:03 conn-port=1 priority=1 type=staticNRL failed
19 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:04 conn-port=1 priority=1 type=staticNRL failed
20 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:05 conn-port=1 priority=1 type=staticNRL failed
21 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:06 conn-port=1 priority=1 type=staticNRL failed
22 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:07 conn-port=1 priority=1 type=staticNRL failed
23 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:08 conn-port=1 priority=1 type=staticNRL failed
24 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:09 conn-port=1 priority=1 type=staticNRL failed
25 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:10 conn-port=1 priority=1 type=staticNRL failed
26 AGENT PM ERROR: CLI command remove vlan all failed
27 AGENT PM ERROR: CLI command remove fwddb all failed
28 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:00:10 conn-port=1 priority=1 type=staticNRL failed
```

## config.err Message Responses

Some typical error log file messages and the recommended responses are provided below (without the prefix of "AGENT PM ERROR: CLI command").

**Message:** remove vlan all failed

**Response:** 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *C3210 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 *C3210 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 *C3210 CLI Reference Manual*, 33497. 4. If the problem persists, contact Technical Support.

**Message:** set dns-svr svr=1 type=dns addr=0.0.0.0 failed

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

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

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

**Message:** set 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.

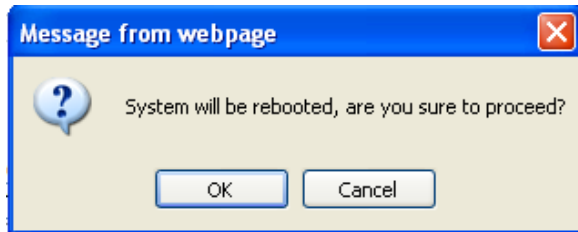


## Webpage Messages

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.

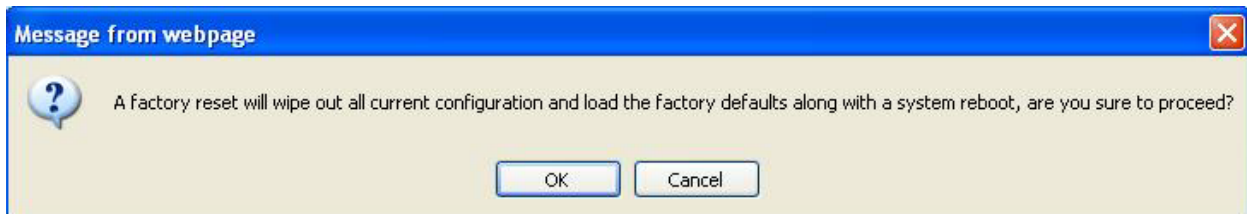
See “[Menu System Descriptions](#)”.

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



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

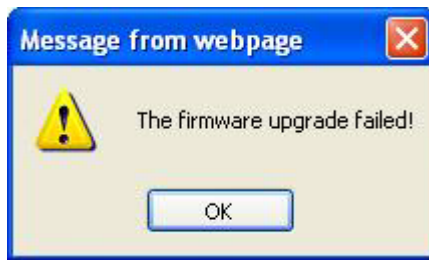
**Message:** *A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*



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



**Message:** *The firmware upgrade failed!*



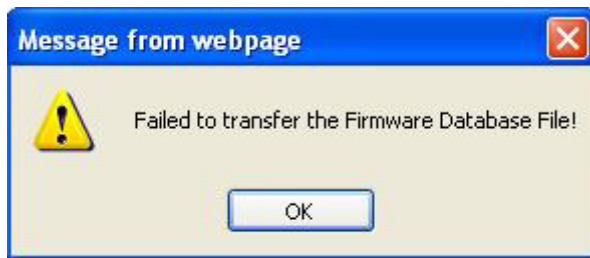
The **MAIN** tab > **TFTP Settings** section **Status** area displays *"TFTP Failure"*.

**Meaning:** While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the ["Upgrade the IONMM and/or C3210 Firmware"](#) section.

**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!*

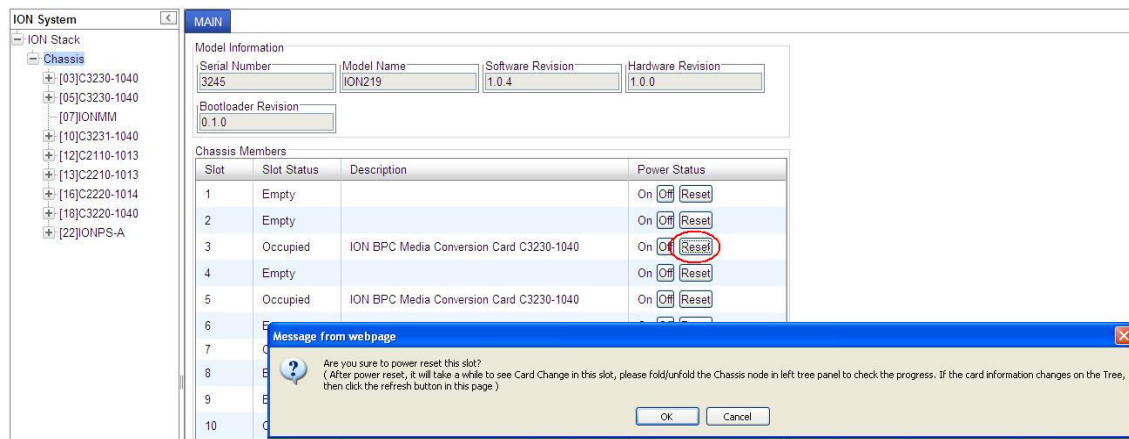


**Meaning:** A problem was detected while performing a Firmware Upgrade from the C3210 **MAIN** tab > **TFTP Settings** section or from the IONMM **UPGRADE** tab. See [“Upgrade the IONMM and/or C3210 Firmware”](#).

**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.)

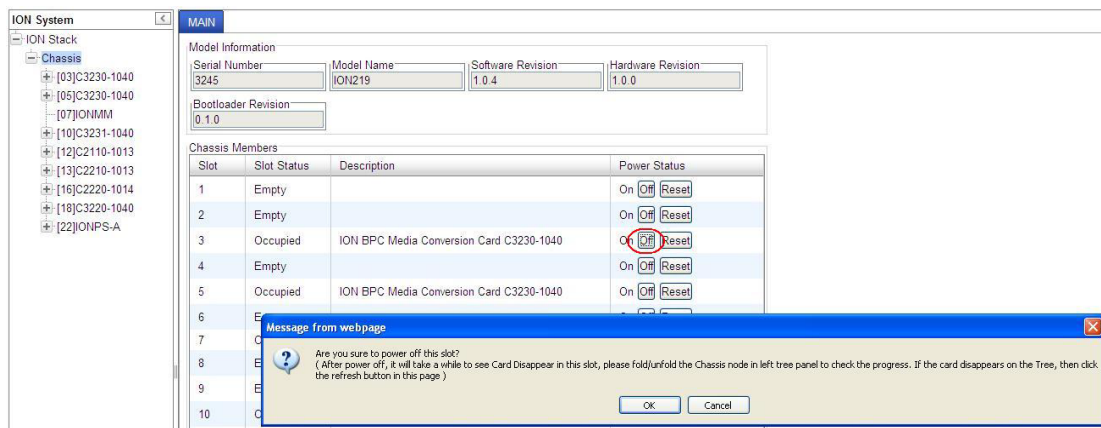


**Meaning:** A caution message generated at the **Chassis > MAIN** tab. You clicked the **Reset** button for a particular slot.

#### 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](#)”.
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.

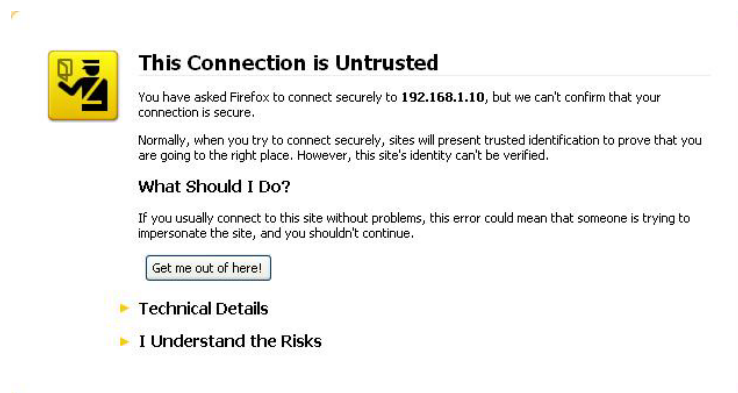
1. **Recovery:** If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to power off this slot, click the **OK** button to clear the message and remove 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](#)”.
6. If the problem persists, contact Technical Support.

**Message:** *The Connection was Reset*

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

**Recovery:**

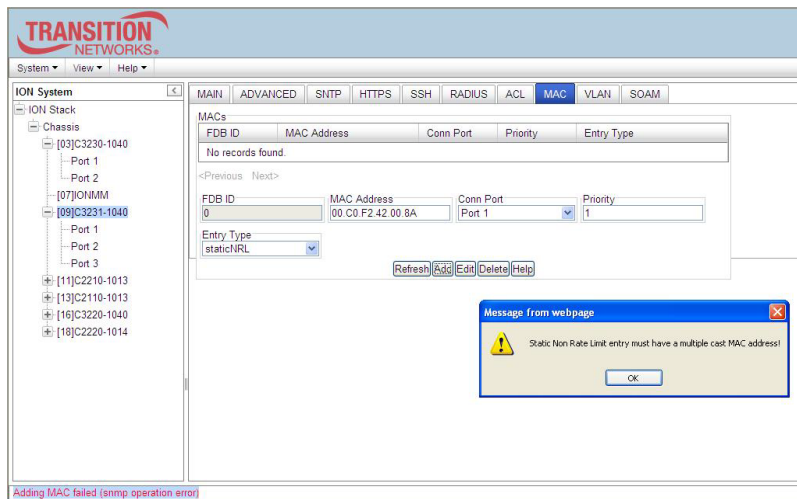
1. Verify the URL (e.g., *http://* versus *https://*).
2. Check if the applicable server is running (TFTP, Syslog, HTTPS server) in the expected location.
3. Click the **Try again** button to retry the operation.

**Message:** *This Connection is Untrusted*

**Meaning:** You tried to connect via FireFox to a URL, but the FireFox web browser did not find a trusted certificate for that site.

**Recovery:** Click **Technical Details** for details, or click **I Understand the Risks** to continue operation.

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

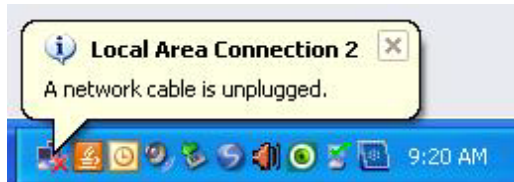


**Meaning:** When setting up MAC filtering, you entered a unicast MAC address and selected a Static NRL (Non Rate Limit) Entry Type.

**Recovery:**

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

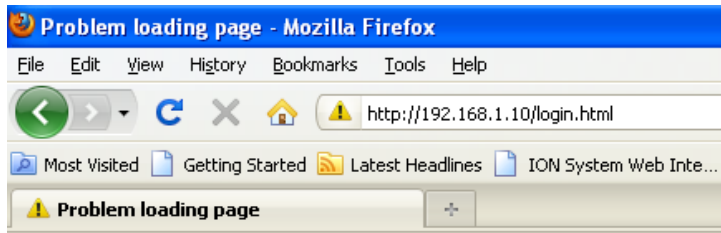
**Message:** *Local Area Connection x – A network cable is unplugged*



**Meaning:** You unplugged the USB cable at the C3210 or IONMM, or the C3210 or IONMM was unplugged from the ION chassis, or you pressed the Reset button on the IONMM.

**Recovery:**

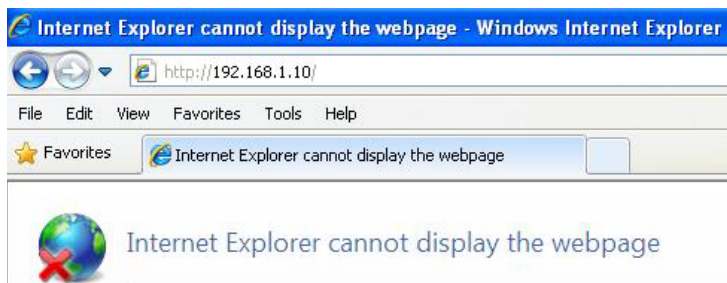
1. If you pressed the Reset button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM's USB-DEVICE connector, or plug the USB cable back into the C3210's USB connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support.

**Message:** *Problem loading page – Mozilla Firefox*

**Meaning:** You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

**Recovery:**

1. Make sure the web browser you are using is supported. See “[Web Browsers Supported](#)”.
2. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)”.
3. Verify C3210 access. See “[Accessing the C3210](#)”.
4. Verify the IP address setting. See “[Setting the IP Addressing](#)”.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

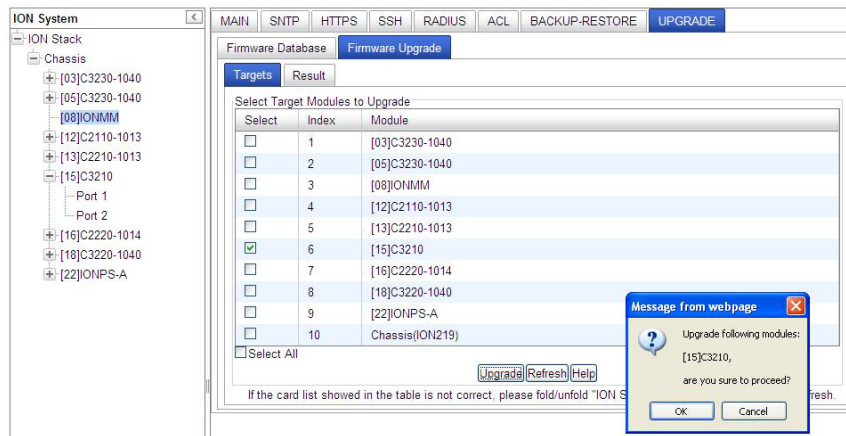
**Message:** *Internet Explorer cannot display webpage*

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

**Recovery:**

1. Make sure the web browser you are using is supported. See “[Web Browsers Supported](#)”.
2. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)”.
3. Verify NID access. See “[Accessing the C3210](#)”.
4. Verify the IP address setting. See “[Setting the IP Addressing](#)”.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

**Message:** *Upgrade following modules: [15]C3210, are you sure to proceed?*



**Meaning:** Verification message that you indeed want to upgrade the C3210 firmware.

**Recovery:**

1. If you are not sure you want to upgrade the C3210 firmware, click **Cancel** and continue operation.
2. If you are sure you want to upgrade the C3210 firmware, click **OK**. The upgrade process will continue.

See “Upgrade the IONMM and/or C3210 Firmware” for more information.



## ION System Tests

This section describes the C3210 system level tests, DMI functions, related test functions, and the xC3210 DIP switches and jumpers.

### Virtual Cable Test (VCT)

The VCT feature uses TDR (Time Domain Reflectometry) to determine the quality of cables, connectors, and terminations. Problems that can be determined include opens, shorts, cable impedance mismatches, failed connectors, and termination mismatches.

The VCT runs the cable diagnostic by transmitting a signal of known amplitude sequentially along each of the TX and RX pairs of an attached cable. The transmitted signal continues along the cable until it is reflected from a cable imperfection, and that distance is displayed. If the test status returned is Normal, the distance displayed is the actual cable length. The VCT test is intrusive, as the tested port's link is brought down during the test.

When the VCT is activated, a pre-defined amount of time elapses before a VCT test pulse is transmitted. This ensures that the link partner loses link, so that it stops sending 100BASE-TX idles or 10 Mbps data packets. The VCT can be performed either when there is no link partner, or when the link partner is Auto-Negotiating or sending 10 Mbps idle link pulses.

Use the VCT test to determine if cabling is at fault when you cannot establish a link. Problems can include opens, shorts, cable impedance mismatches, failed connectors, and termination mismatches, bad magnetics.

Do not change the port configuration while the TDR test is running.

Due to cable characteristics, run the TDR test several times to get accurate results.

Do not change port status (e.g., remove the cable at the near or far end) as the results may be inaccurate.

The VCT test can be configured via the CLI method or the Web method.

## VCT Test – CLI Method

Use the VCT test to determine if cabling is at fault when you cannot establish a link for a C3210 copper port.

1. Access the C3210 through either a USB connection.
2. Start the VCT Test. Type **start ether tdr test** and press **Enter**. The Time Domain Reflector (TDR) test starts on the specified Ethernet copper port.
3. Show the Ethernet port TDR Test configuration. Type **show ether tdr config** and press **Enter**. The Time Domain Reflectometry (TDR) test configuration displays for the Ethernet copper port. For example:

```
C1|S16|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----
TDR test state:                success
TDR test init time:           22:39:18
TDR test result valid:        true
C1|S16|L1P1>
```

4. Show the Ethernet port TDR Test results. Type **show ether tdr test result** and press **Enter**. The results of an Ethernet port TDR test display for the copper port. For example:

```
C1|S5|L1P1>show ether tdr test result
Cable pair :
index          distance to fault(unit)    status
-----
pair1 and 2    0(meter)                        open
pair3 and 6    0(meter)                        open
pair4 and 5    0(meter)                        open
pair7 and 8    1(meter)                        open
C1|S5|L1P1>
```

5. Run the TDR test several times to ensure accurate results. Do not change port status (e.g., remove the cable at the near or far end) as this may cause inaccurate results.

## VCT Test – Web Method

1. Access the C3210 through the Web interface.
2. Select the desired port.
3. At the port-level **MAIN** tab, check the information displayed in the **Link Status** and **Virtual Cable Test** areas.

ION System

MAIN ADVANCED COUNTERS

ION Stack

- Chassis
  - [03]C3230-1040
  - [05]C3230-1040
  - [08]IONMM
  - [10]C3231-1040
  - [12]C2110-1013
  - [13]C2210-1013
  - [15]C3210-1013
    - Port 1
    - Port 2
  - [16]C2220-1014
  - [18]C3220-1040
  - [22]IONPS-A

Circuit ID

Port Configuration

Link Status: Down Admin Status: Up Speed: Negotiating Duplex: Negotiating

Port Mode: 10/100/1000BaseT AutoCross Mode: Auto

Auto Negotiation Settings

Auto Negotiation: Enabled

Capabilities Advised

<input checked="" type="checkbox"/> 10M - Half Duplex	<input checked="" type="checkbox"/> 10M - Full Duplex	<input checked="" type="checkbox"/> 100M - Half Duplex	<input checked="" type="checkbox"/> 100M - Full Duplex
<input checked="" type="checkbox"/> 1000M - Half Duplex	<input checked="" type="checkbox"/> 1000M - Full Duplex	<input type="checkbox"/> Pause	<input type="checkbox"/> Asymmetric Pause

Port Forward Management

Source Port: 1 Forward Settings: ☒ Port 1 to Port 2

Virtual Cable Test

Index	Status	Distance To Fault
Pair 1 and 2	Unknown	
Pair 3 and 6	Unknown	
Pair 4 and 5	Unknown	
Pair 7 and 8	Unknown	

Virtual Cable Test

Refresh Save Help

4. Click the **Virtual Cable Test** button. The VCT test runs and test information displays.

Virtual Cable Test

Index	Status	Distance To Fault
Pair 1 and 2	Unknown	
Pair 3 and 6	Unknown	
Pair 4 and 5	Unknown	
Pair 7 and 8	Unknown	

Virtual Cable Test

Refresh Save Help

5. Check the information displayed in the **Link Status** (*Up or Down*) and **Virtual Cable Test** sections.

Virtual Cable Test		
Index	Status	Distance To Fault
Pair 1 and 2	Open	0 Meter
Pair 3 and 6	Open	0 Meter
Pair 4 and 5	Open	0 Meter
Pair 7 and 8	Open	0 Meter
Virtual Cable Test		
<input type="button" value="Refresh"/> <input type="button" value="Save"/> <input type="button" value="Help"/>		

The possible VCT Test parameters and states are shown in the table below.

**Table 12: VCT Parameters**

Parameter	Fault State	Meaning
Link Status Down		VCT Test failed due to lost link.
Link Status Up		VCT Test passed; link is up. No action needed.
Index - Pair x to y		There are four pairs of standard category 5 cable. Each pair displays one of these states: Open, Broken, Shorted, Terminated, Impedance Mismatch, or Unknown.
Status – Normal		The pair is properly terminated at the remote end (not a fault state). The 'Distance To Fault' is blank.
Status – Open	X	Open (not connected) connection failure status. Cable impedance is <u>greater</u> than 333 ohms.
Status – Broken	X	Broken connection failure status.
Status – Shorted	X	Shorted connection failure status. Cable impedance is <u>less</u> than 333 ohms.
Status – Terminated		Connection terminated status (non-fault state).
Status – Impedance Mismatch	X	The impedance of the pair is mismatched.
Status – Unknown	X	None of the above (i.e., not Normal, Open, Shorted, Terminated, Impedance Mismatch, or Unknown).
Distance To Fault - 0 Meter		The overall distance to the fault in Meters (Open or no fault found).
Distance To Fault > 0 Meter		The overall distance to the fault in Meters.

## DMI (Diagnostic Maintenance Interface)

The DMI (Diagnostic Maintenance Interface) function displays C3210 diagnostic / maintenance information such as [fiber](#) interface characteristics, diagnostic monitoring parameters, and supported [fiber](#) media lengths.

**Note:** Lantronix C3210s that support DMI have a “-D” at the end of the model number.

DMI can be configured in the C3210 using either the CLI or Web method.

### DMI Config – CLI Method

1. Access the C3210 through either a USB connection.
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:

```
C1|S13|L0AP1|L1P2/>set dmi preset-power-level=10
C1|S13|L0AP1|L1P2/>show dmi info
Diagnostic monitoring interface information:
-----
DMI connect type:                LC
DMI bit rate:                    13*100Mbps
DMI link length(single mode fiber, 100m): 100*100m
DMI link length(50 micron multi-mode fiber, 10m): 50*10m
DMI link length(62.5 micron multi-mode fiber, 10m): 50*10m
DMI link length(copper cable, m): N/A
DMI identifier:                  SFP
DMI laser wavelength:            1310*nm
DMI temperature:                 47.3*C
DMI temperature alarm setting:   normal
DMI bias current:                20912*uA
DMI bias current alarm setting:  normal
DMI Tx power:                    249*uW
DMI Tx power:                    normal
DMI Rx power:                    0*uW
DMI Rx power:                    normal
DMI Rx power preset level:       0*uW
```

## DMI Config – Web Method

1. Access the C3210 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, the 'ION Stack' tree is expanded to show 'Chassis' and a list of devices. Device '[18]C3220-1040' is selected, and its 'Port 2' is highlighted with a red circle. The main panel shows the 'DMI' tab selected, which is also circled in red. The DMI tab contains three sections: 'Interface Characteristics', 'Diagnostic Monitoring', and 'Supported Media Length'. Each section has several input fields for configuration and monitoring data. At the bottom right of the main panel are 'Refresh', 'Save', and 'Help' buttons.

Interface Characteristics		
DMI ID	Connector Type	Nominal Bit Rate (Mbps)
SFP	LC	1300
Fiber Interface Wavelength (nm)		
850		

Diagnostic Monitoring		
Receive Power (μW)	Receive Power (dBm)	Receive Power Alarm
0		Normal
Rx Power Intrusion Threshold (μW)		
0		
Temperature (°C)	Temperature (°F)	Temperature Alarm
37.5	99.5	Normal
Transmit Bias Current (μA)	Transmit Bias Alarm	
4656	Normal	
Transmit Power (μW)	Transmit Power (dBm)	Transmit Power Alarm
255	-5.935	Normal

Supported Media Length		
9/125u Singlemode Fiber (m)	50/125u Multimode Fiber (m)	62.5/125u Multimode Fiber (m)
N/A	500	300
Copper (m)		
N/A		

Buttons: Refresh, Save, 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 13: 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 " <a href="#">Connector Types</a> " 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. An <i>ionDMITemperatureEvt</i> event is sent when there is a warning or alarm on DMI temperature
Transmit Bias Current (uA)	(measured current)	Transmit bias current on local fiber interface, in uA (microamperes). The sample screen above shows 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 Singlemode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). The sample screen above shows N/A, indicating the media is not applicable.
Supported Media Length	50/125u Multimode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 500 meters as the supported media length.
Supported Media Length	62.5/125u MM Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 300 meters as the supported media length.
Supported Media Length	Copper (m)	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters. The sample screen above shows N/A, indicating the media is not applicable.



## Connector Types

The DMI connector type indicates the external optical or electrical cable connector provided as the interface. The information below is from SFF 8472 Rev 9.5.

**Table 14: Connector Types**

Value	Description of connector
00h	Unknown or unspecified
01h	SC
02h	Fibre Channel Style 1 copper connector
03h	Fibre Channel Style 2 copper connector
04h	BNC/TNC
05h	Fibre Channel coaxial headers
06h	FiberJack
07h	LC
08h	MT-RJ
09h	MU
0Ah	SG
0Bh	Optical pigtail
0C-1Fh	Reserved
20h	HSSDC II
21h	Copper Pigtail
22h-7Fh	Reserved
80-FFh	Vendor specific

The LC, MT-RJ LC, SC, ST, or VF-45 connector types (jacks) are shown below.



**ST**



**SC**



**LC**



**MT-RJ**



**VF-45**

## Set Debug Level

You can use the CLI method to define the system debug level.

1. Access the C3210 through either a USB connection.
2. Set the desired debug level. Type:

**set dbg level=<0-2>**

where:

**0**=debug Severity level 0 (Emergency: system is unusable - e.g., serious hardware failure or imminent power failure).

**1**=debug Severity level 1 (Alert: action must be taken immediately).

**2**=debug Severity level 2 (Critical condition).

3. Press **Enter**.

```
For example: C1|S5|L1D>set dbg level 0
              C1|S5|L1D>set dbg level 1
              C1|S5|L1D>set dbg level 2
              C1|S5|L1D>
```

## DIP Switches and Jumper Settings

The C3210 has on-board components that can be used to configure device operation, typically at the direction of a technical support specialist. In most cases, the factory default settings provide optimal configuration settings; however, DIP Switch and Jumper setting changes may be required for operating mode changes or troubleshooting purposes.

### PCB Identification

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

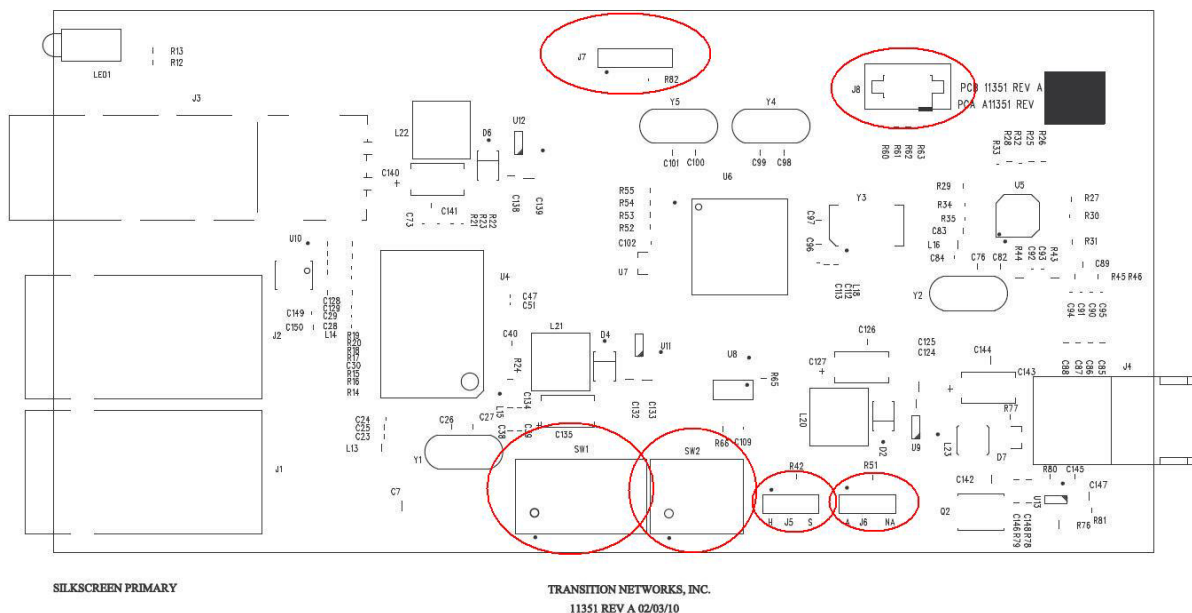
- **x3210** PCB: 11325 Rev. A, B and C (this information is silkscreened on the top of the PCB).
- **x3210** PCB: 11351 Rev. A (this information is silkscreened on the bottom of the PCB).

Each PCB has jumpers and / or DIP switches. Not all of these jumpers / DIP switches are intended for use in the field.

**Note:** Do not change these configurable items except at the direction of a technical support specialist.

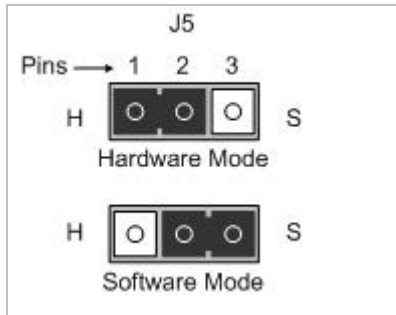
#### x3210 PCB

x3210 PCB: All PCBs (this information is silkscreened on the bottom of the PCB). This PCB has four jumpers and two DIP switches. **Note:** not all of these are used in the field.



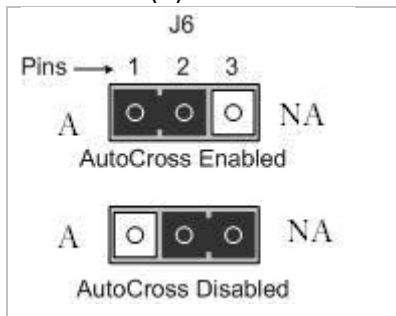
### J5 - Hardware / Software Mode Jumper

Jumper J5 enables x3210 Hardware Mode or Software Mode. The default setting is Software mode.

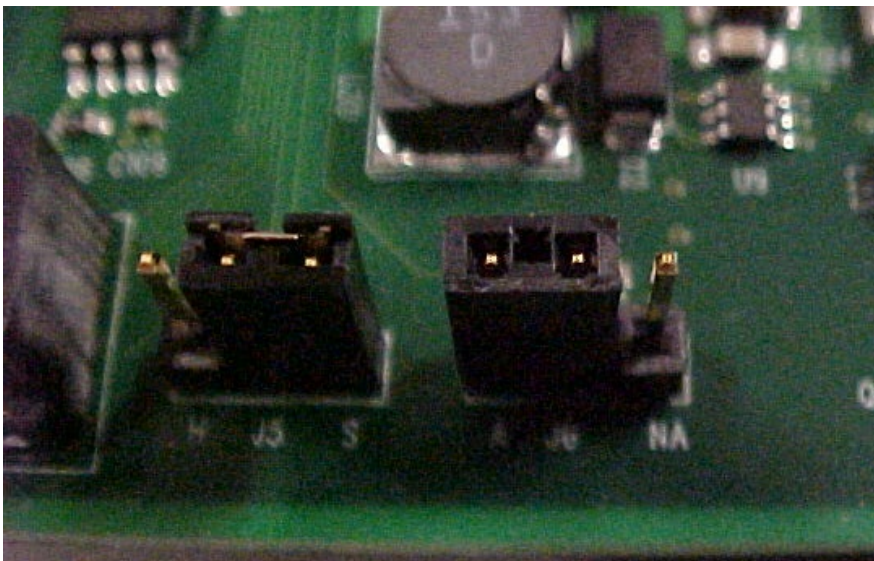
		<table><tr><th colspan="2">J5</th></tr><tr><th>Jumper Pin #s</th><th>Function</th></tr><tr><td>1-2</td><td>Hardware Mode (H).</td></tr><tr><td>2-3</td><td>Software Mode (S).</td></tr></table>		J5		Jumper Pin #s	Function	1-2	Hardware Mode (H).	2-3	Software Mode (S).
J5											
Jumper Pin #s	Function										
1-2	Hardware Mode (H).										
2-3	Software Mode (S).										

### J6 - Autocross Enable / Disable Jumper

Jumper J6 can be used in the field to enable or disable the x3210 Autocross feature. The default setting is Autocross Enabled (A).

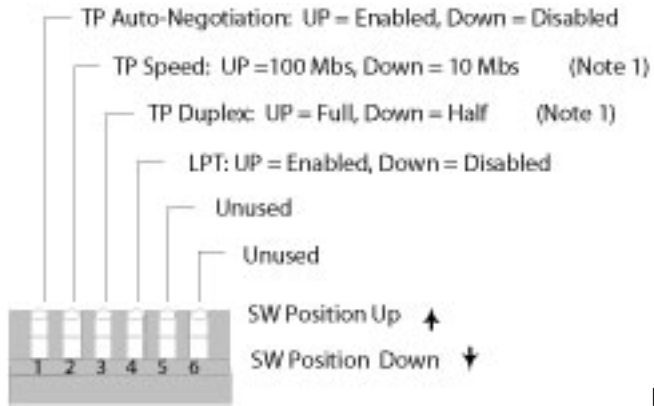
		<table><tr><th colspan="2">J6</th></tr><tr><th>Jumper Pin #s</th><th>Function</th></tr><tr><td>1-2</td><td>Autocross Enabled (<b>A</b>).</td></tr><tr><td>2-3</td><td>Autocross Disabled (<b>NA</b>).</td></tr></table>		J6		Jumper Pin #s	Function	1-2	Autocross Enabled ( <b>A</b> ).	2-3	Autocross Disabled ( <b>NA</b> ).
J6											
Jumper Pin #s	Function										
1-2	Autocross Enabled ( <b>A</b> ).										
2-3	Autocross Disabled ( <b>NA</b> ).										

Jumpers J5 and J6 are shown below.



### ***DIP Switch SW1 (Autoneg, Speed, Duplex, LPT, and Fiber Duplex)***

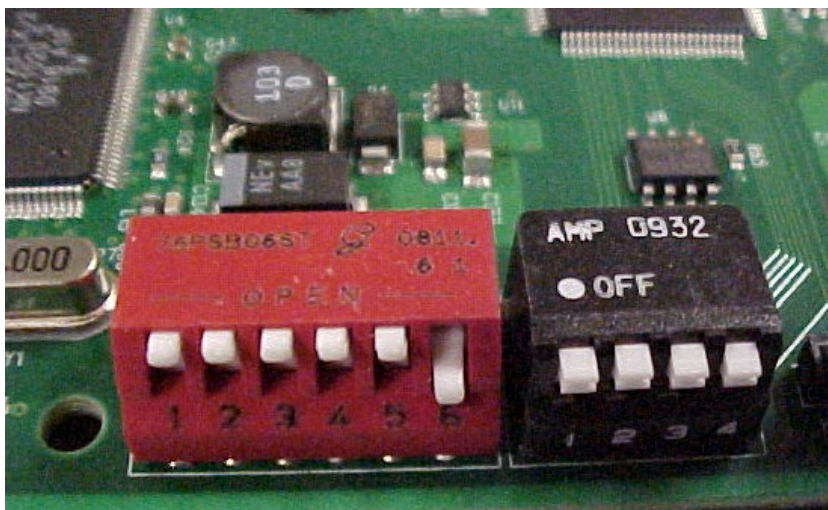
The 6-position DIP Switch SW1 can be used in the field to configure the x3210 TP1 AutoNegotiation, Speed, Duplex, LPT, and Fiber Duplex settings.



**Note 1:** Only use when Auto-Negotiation is disabled.

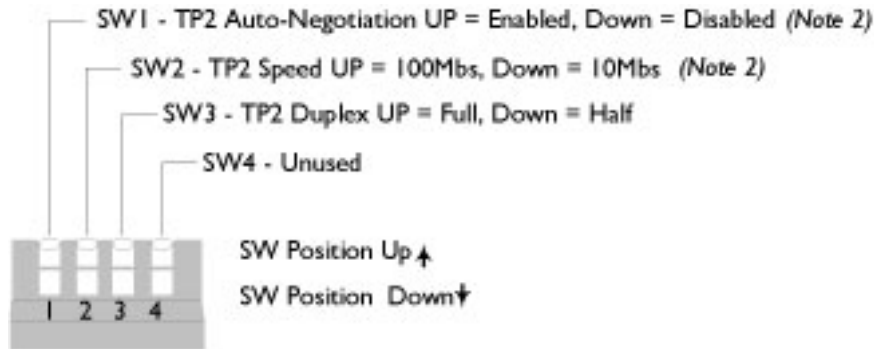
<b>Switch #</b>	<b>High position (Up - Default)</b>	<b>Low position (Down)</b>
1	TP1 AutoNegotiation Enabled	TP1 AutoNegotiation Disabled
2	TP1 100 Mbps Speed	TP1 10 Mbps Speed (only with AutoNegotiation disabled)
3	TP1 Full Duplex mode	TP1 Half Duplex mode (only with AutoNegotiation disabled)
4	LPT Enabled	LPT (Link Pass Through) Disabled (for TX to FX only)
5	Full duplex fiber	Half duplex fiber (valid only for 100FX)
6	Not used.	Not used.

DIP switches SW1 (left) and SW2 (right) are shown below.



### ***DIP Switch SW2 (TP2 Autoneg, Speed, Duplex)***

The 4-position DIP Switch SW2 can be used in the field to configure the x3210 TP2 AutoNegotiation, Speed, and Duplex settings.



<b><u>Switch #</u></b>	<b><u>High position (Up)</u></b>	<b><u>Low position (Down)</u></b>
1	TP2 AutoNegotiation Enabled	TP2 AutoNegotiation Disabled
2	TP2 100 Mbps Speed	TP2 10 Mbps Speed (only with AutoNegotiation disabled)
3	TP2 Full Duplex mode	TP2 Half Duplex mode (only with AutoNegotiation disabled)
4	Reserved – do not use.	Reserved – do not use.

**Note 2:** Only use when Auto-Negotiation is disabled.

### ***J78 (Not Used)***

Do not use. Jumper J7 is used for manufacturing / debug purposes only.

### ***J8 (Not Used)***

Do not use. Jumper J8 is used for manufacturing / debug purposes only.

## 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.

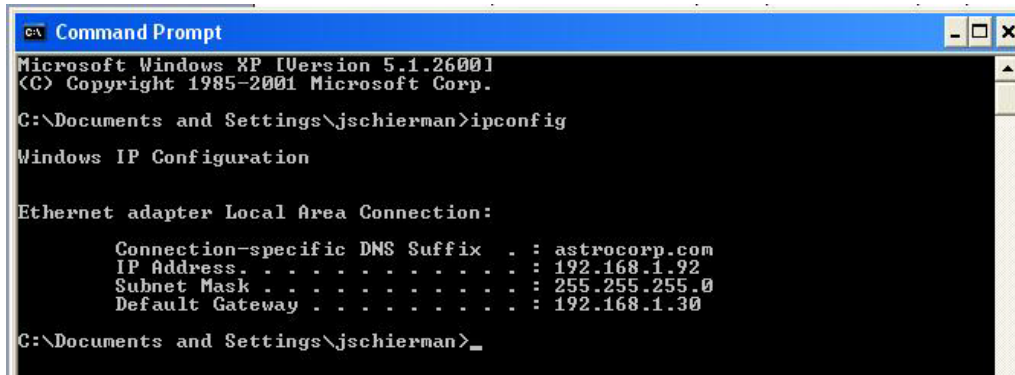
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway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



```
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

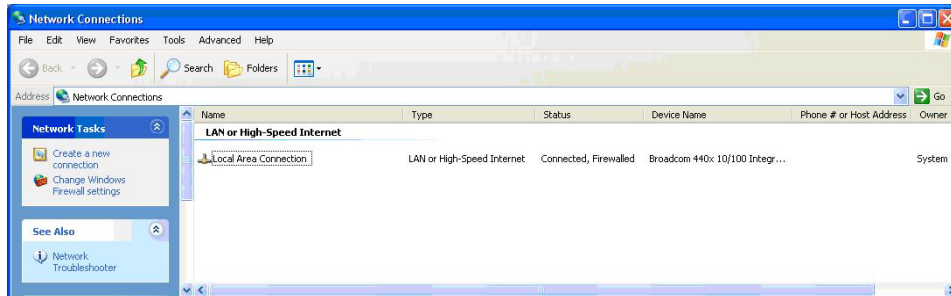
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
 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

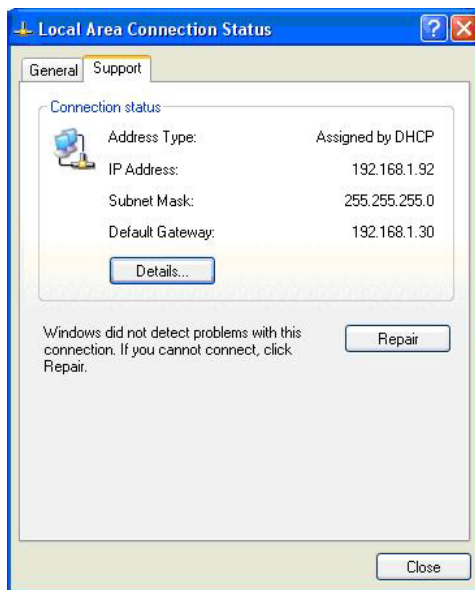
## Windows Network Connections

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.

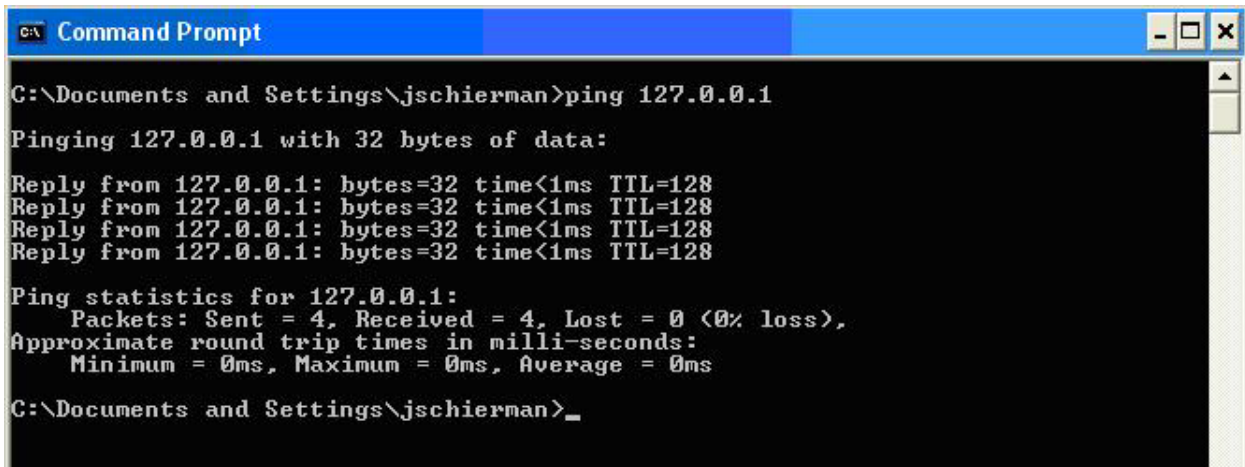


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

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

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

## PuTTY

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

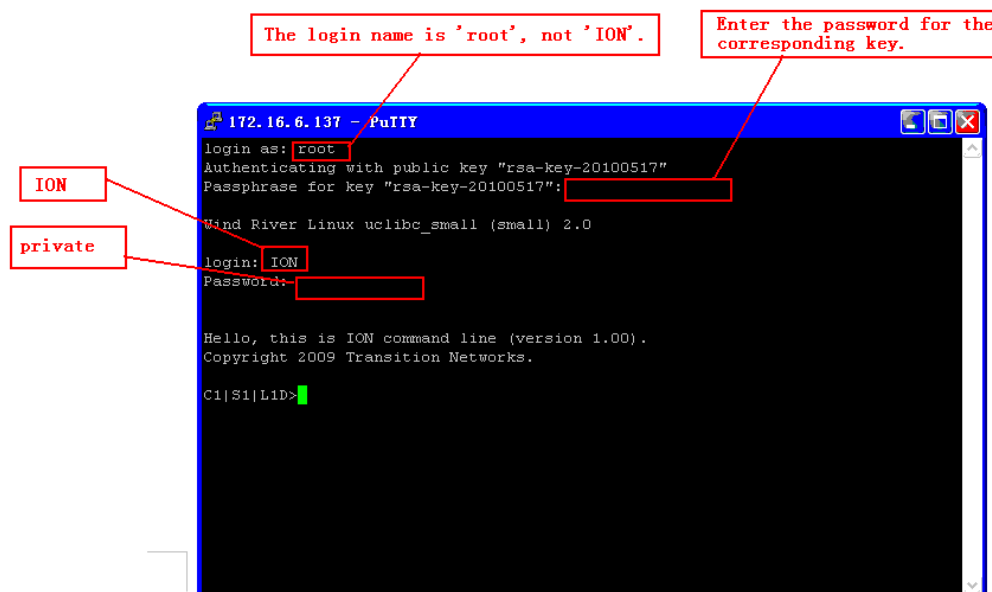
The PuTTY SSH and telnet client was developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is developed and supported by a group of volunteers. PuTTY has been ported to various other operating systems. Official versions exist for some Unix-like platforms, with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

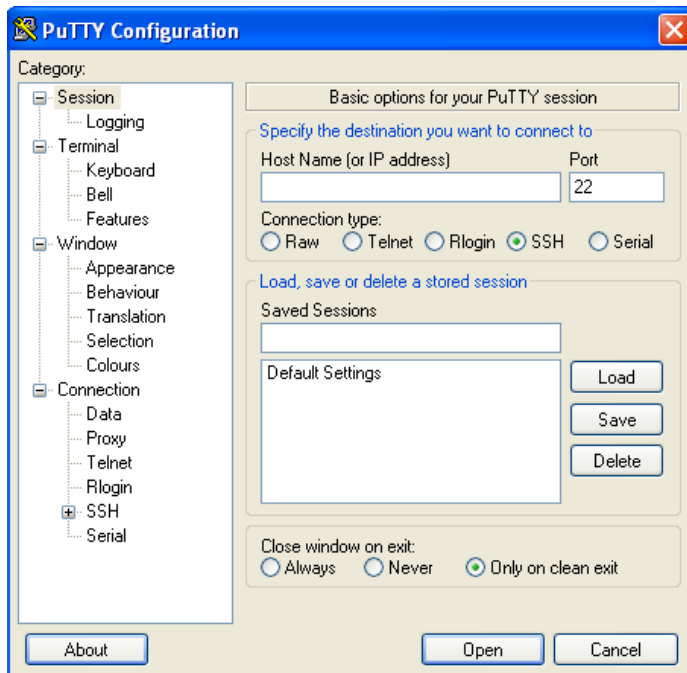
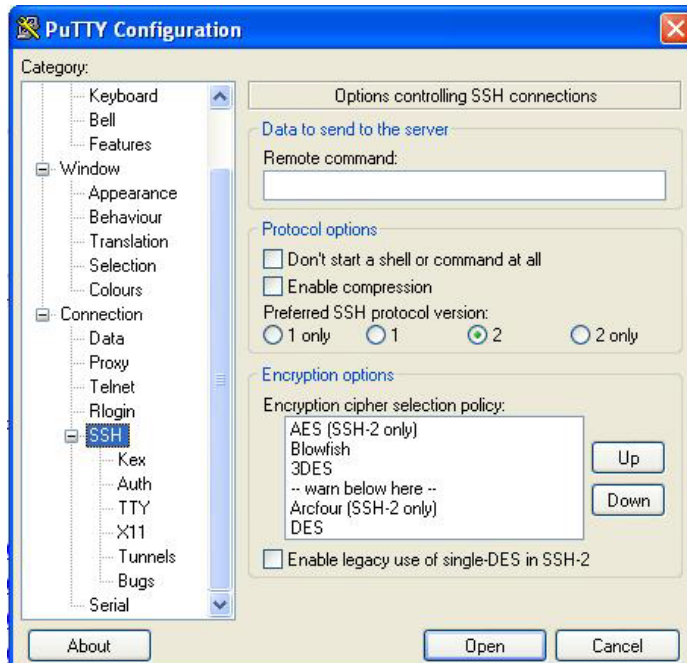
The PuTTY terminal emulator application also works as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols.

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](http://www.microsoft.com); the first query will go out as [www.microsoft.com.att.com](http://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:

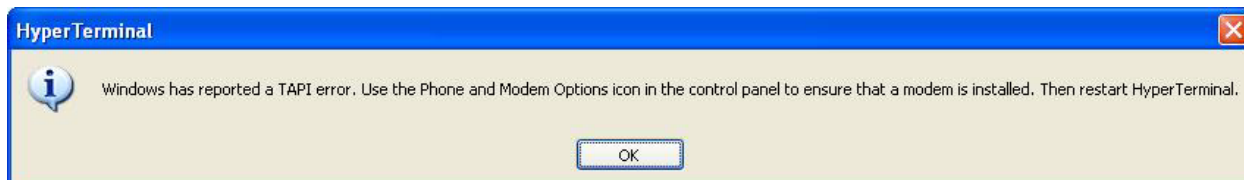
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

## Third Party Tool Messages

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

### HyperTerminal Messages

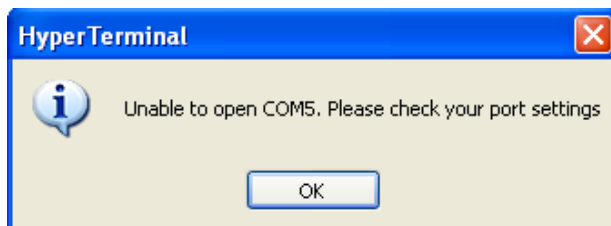
**Message:** *Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal.*



**Response:**

1. Verify your **computer's Ports (COM & LPT)** setting. See "[Configuring HyperTerminal](#)".
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.
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.

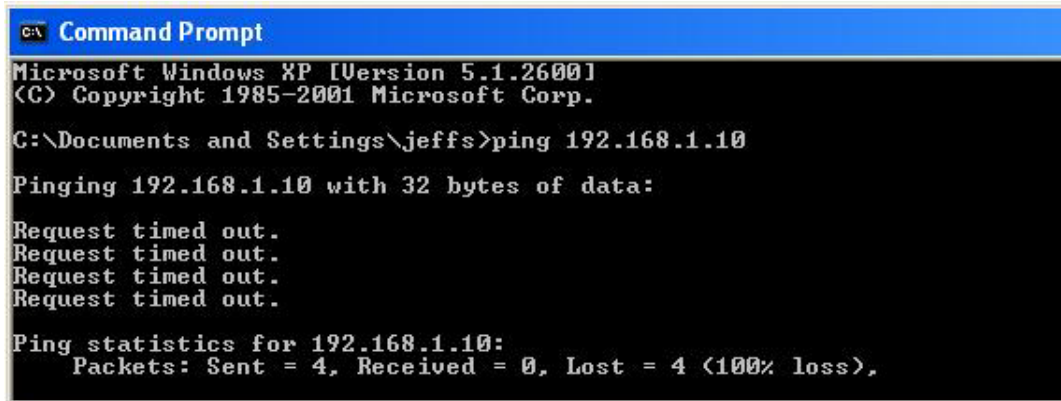
**Meaning:** HyperTerminal (HT) is a terminal emulation program developed by Hillgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a 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](http://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),
```

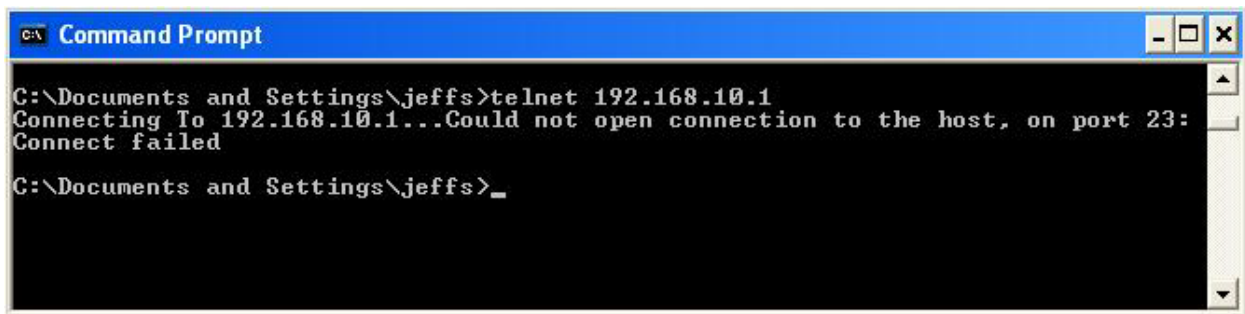
**Meaning:** The Ping command failed.

**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.

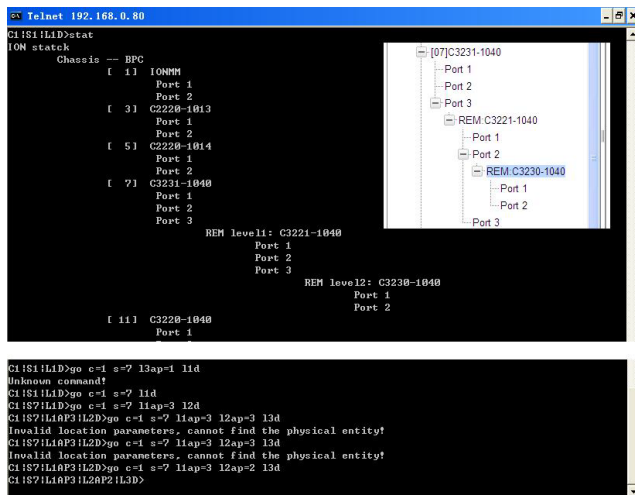
**Message:** *Invalid location parameters, cannot find the physical entity!*

```
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.

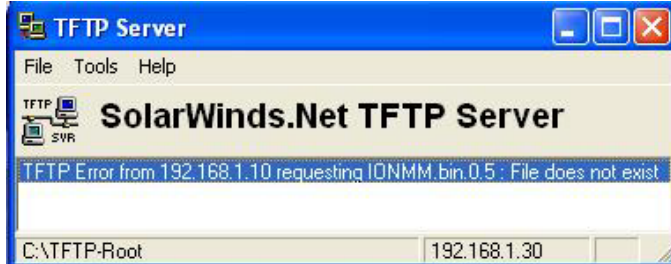
**Recovery:**

1. Verify the CLI command syntax.
2. For a complete list of the available commands, see the *C3210 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.

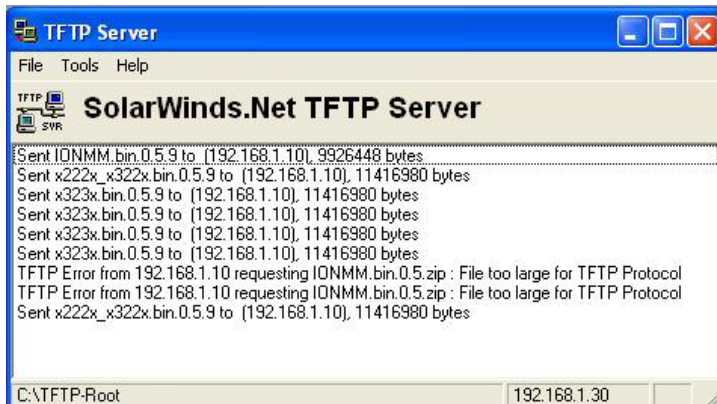
**Message:** *File does not exist*



**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.

## Recording Model Information and System Information

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

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 Technical Support Specialist.

**TRANSITION NETWORKS**

System View Help

**ION System** MAIN

**Model Information**

Serial Number: 4774302 Model: C3210-1013 Software Revision: 1.2.0 Hardware Revision: 1.0.0

Bootloader Revision: 0.1.0

**System Configuration**

System Name: C3210 System Up Time: 264:19:31:29.00 Configuration Mode: Software Number of Ports: 2

MAC Address: 00-C0-F2-01-5A-3A

Uptime Reset System Reboot All Counters Reset Reset To Factory Config

Device Description:

Link Pass Through (LPT): Link Pass Through: Disabled

Forwarding Learning: FDB Aging Time (Enter in 15sec increments): 300

Refresh Save Help

Getting values finished Version: 1.3.19

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](#)”.

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. Compliance and Safety Information

See the Install Guide for compliance and safety information.

## Appendix B. Factory Defaults

The C3210 *Device* Level Factory Defaults are shown in Table 15 below.

The C3210 *Port* Level Factory Defaults are shown in Table 16.

### Device-Level Factory Defaults

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

**Table 15: Device-Level Factory Defaults**

Item/Field	Default Setting
Web Access Password	private
Telnet/USB Login	ION
Telnet/USB Password	private
<b>Main tab</b>	
System Configuration	System Name: e.g., C3210-1040
Configuration Mode	Software
Device Description	blank or (none)
Link Pass Through(LPT)	Enabled
Forwarding Learning	FDB Aging Time: 300

## Port-Level Factory Defaults

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

The C3210 *Device* Level Factory Defaults are shown in the table above.

The C3210 *Port* Level Factory Defaults are shown in the table below.

**Table 16: Port-Level Factory Defaults**

Item/Field	Default Setting
<b>Main tab</b>	
Circuit ID	blank
Link Status	Up
Admin Status	Up
Speed	Negotiating
Duplex	Negotiating
Port Mode	1000BaseX
AutoCross Mode	Auto
Connector Type	RJ-45 (Port 1) SC Multimode Fiber (Port 2)
Auto Negotiation	Enabled
Force Speed Force Duplex	100Mbps Full Duplex
Capabilities Advertised	<ul style="list-style-type: none"> <li>• All speed/duplex boxes checked</li> <li>• Pause and Asymmetric Pause boxes unchecked</li> </ul>
Pause Admin Mode	Disabled (copper port)
Forward Settings	All boxes checked
Virtual Cable Test	No records found
<b>Advanced tab</b>	
Rate Limiting Mode	Counts All Layer 2
Egress Rate Limit	Unlimited
Ingress Rate Limit	Unlimited
Filter Unknown Multicast	Disabled

Filter Unknown Unicast	Disabled																		
Discard Tagged	Disabled																		
Discard Untagged	Disabled																		
Default VLAN ID	1																		
Default Priority	0																		
IEEE Priority Class	Enabled																		
IP Traffic Class	Enabled																		
Priority Precedence	Use IEEE																		
Frame Tag Mode	Network																		
Provider Ether Type	X8100																		
Network Mode Tagging	Unmodified																		
User Priority	<table> <tr> <th>Remap</th><th>To</th></tr> <tr><td>0</td><td>0</td></tr> <tr><td>1</td><td>1</td></tr> <tr><td>2</td><td>2</td></tr> <tr><td>3</td><td>3</td></tr> <tr><td>4</td><td>4</td></tr> <tr><td>5</td><td>5</td></tr> <tr><td>6</td><td>6</td></tr> <tr><td>7</td><td>7</td></tr> </table>	Remap	To	0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7
Remap	To																		
0	0																		
1	1																		
2	2																		
3	3																		
4	4																		
5	5																		
6	6																		
7	7																		
<b>DMI</b> tab (Port 2 only)	The DMI feature is not supported on current port.																		

## Appendix C. SNMP Traps Supported

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.

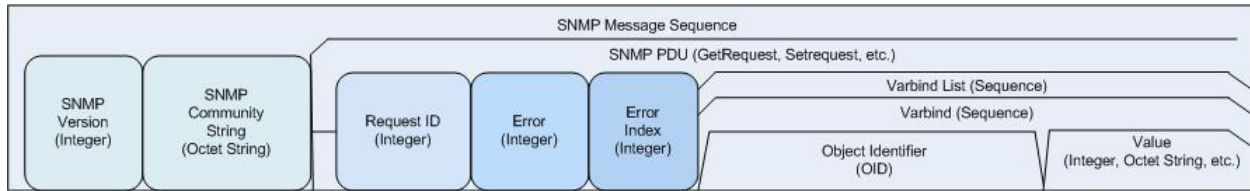
### Traps List

1. ionSlotStatusChangeEvt
2. ionChassisDiscoveredEvt
3. ionChassisRemovedEvt
4. entSensorThresholdNotification
5. ionDMIRxIntrusionEvt
6. ionDMIRxPowerEvt
7. ionDMITxPowerEvt
8. ionDMITxBiasEvt
9. ionDMITemperatureEvt
10. newroot
11. topologyChange
12. linkDown
13. linkUp
14. risingAlarm
15. fallingAlarm
16. ionIfSourceAddrChangeEvt
17. ionDevSysAcIldsEvt

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

See the “[Supported MIBs](#)” section for information on the C3210s support for public (standard) and private MIBs. Also see “[Configuring SNMP](#)”. 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 C-1: SNMP Message Sequence**

## MIB Traps Summary

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

**Table 17: MIB Traps Summary**

<b>MIB</b> (linked to section)	<b>TRAP</b> (linked to section)	<b>VARBINDS</b>
<b>TN-ION-BPC-MIB</b>	ionSlotStatusChangeEvt	entPhysicalIndex, ionChassisSlotNumber ionChassisSlotStatus
<b>TN-ION-Chassis-MIB</b>	ionChassisDiscoveredEvt	entPhysicalIndex ionChassisStackSerialNo
	ionChassisRemovedEvt	entPhysicalIndex ionChassisStackSerialNo
<b>TN-ION-ENTITY-SEN-SOR-MIB</b>	entSensorThresholdNotification	entSensorThresholdValue entSensorValue
<b>TN-ION-MGMT-MIB</b>	ionDMIRxIntrusionEvt	ifIndex ionDMIRxPwrLvIPreset ionDMIRxPowerLevel
	ionDMIRxPowerEvt	ifIndex ionDMIRxPowerAlarm ionDMIRxPowerLevel
	ionDMITxPowerEvt	ifIndex ionDMITxPowerAlarm ionDMITxPowerLevel
	ionDMITxBiasEvt	ifIndex, ionDMITxBiasAlarm, ionDMITxBiasCurrent
	ionDMITemperatureEvt	ifIndex ionDMITempAlarm ionDMITemperature



<b>MIB</b> (linked to section)	<b>TRAP</b> (linked to section)	<b>VARBINDS</b>
	<a href="#">rxPwrThreshold</a>	
<b>BRIDGE-MIB</b>	newroot	
	topologyChange	
<b>IF-MIB</b>	linkDown	ifIndex, ifAdminStatus, ifOperStatus
	linkUp	ifIndex, ifAdminStatus, ifOperStatus
<b>RMON</b>	risingAlarm	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmFallingThreshold
	fallingAlarm	alarmIndex, alarmVariable, alarmSample- Type, alarmValue, alarmFallingThreshold
<b>TN-ION-VLAN-MGMT-MIB</b>	ionIfSourceAddrChangeEvt	
<b>ION-DEV-SYS-ACL-MIB</b>	ionDevSysAcldsEvt	

### ***TN-ION-MGMT-MIB.smi***

```

ionDevSysMgmt      OBJECT IDENTIFIER ::= { ionDevMgmt 1 }
ionDevSysLPT       OBJECT IDENTIFIER ::= { ionDevMgmt 2 }

```

```
--
```

```
--ION Ethernet Interface management
```

```
... ..
```

```
 ::= { tnIonMgmtNotifications 6 }
```

## Agent\_III\_Private MIBS

### **ION-DEV-SYS-ACL-MIB**

The **ionDevSysAclIdsEvt** event is included in 'ION-DEV-SYS-ACL-MIB.my'. This event is related to 'iptableRulesTable' which is also defined in 'ION-DEV-SYS-ACL-MIB.my'.

```
ionDevSysAclIdsEvt  NOTIFICATION-TYPE
    OBJECTS {
        entPhysicalIndex, gRuleIndex
    }
```

STATUS current

DESCRIPTION

"An ionDevSysAclIdsEvt event is sent if an IDS (Intrusion Detection Systems) is detected.

The entPhysicalIndex event indicates in which SIC the IDS is detected.

The entPhysicalIndex/gRuleIndex indicates which ACL rule is matched for this IDS."

::= { tnIonMgmtNotifications 16 }

### **ION-DEV-SYS-HTTPS-MIB**

None

### **ION-DEV-SYS-IPMGMT-MIB**

None

### **ION-DEV-SYS-RADIUS-MIB**

None

### **ION-DEV-SYS-SNMPMGMT-MIB**

None

### **ION-DEV-SYS-SNTP-MIB**

None

### **ION-DEV-SYS-SSH-MIB**

None

### **ION-DEV-SYS-TFTP-MIB**

None

***TN-ION-VLAN-MGMT-MIB.mib***

The **ionIfSourceAddrChangeEvt** event is included 'TN-ION-VLAN-MGMT-MIB.mib'.  
The 'ionIfSourceAddrChangeEvt' event is related to 'ionIfMACSecurityTable' which is defined in 'TN-ION-MGMT-MIB.smi'.

```
ionIfSourceAddrChangeEvt  NOTIFICATION-TYPE
    OBJECTS {
        ionFIDDbMacAddress, ionFIDDbConnPort
    }
STATUS    current
DESCRIPTION
    "An ionIfSourceAddrChangeEvt event is sent when the ionIfSourceAddrLock is set to 'true',
    the ionIfSourceAddrLockAction is set to 'discardAndNotify' or 'all' and there is an intrusion/SA change
    on this port."
::= { tnIonVlanQoS MgmtNotifications 1 }
```

## TN\_ION Private MIBS

### TN-ION-BPC-MIB

#### *ionSlotStatusChangeEvt*

An ionSlotStatusChangeEvt event is sent when a new module is inserted in this slot or when it is removed. The chassis is identified by its entPhysicalIndex.

#### Varbinds

##### *entPhysicalIndex*

SYNTAX INTEGER

DESCRIPTION

"The entPhysicalIndex in this chassis."

##### *ionChassisSlotNumber*,

SYNTAX INTEGER

DESCRIPTION

"The slot number in this chassis."

##### *ionChassisSlotStatus*

SYNTAX INTEGER { empty(1), occupied(2) }

DESCRIPTION

"The status of the slot, whether occupied or empty."

#### OID

#### MIB Description

ionSlotStatusChangeEvt NOTIFICATION-TYPE

OBJECTS {

entPhysicalIndex,  
ionChassisSlotNumber,  
ionChassisSlotStatus  
}

STATUS current

DESCRIPTION

"An ionSlotStatusChangeEvt event is sent when a new module is inserted in this slot or when it is removed. The chassis is identified by its entPhysicalIndex."

::= { tnIonBkPlaneNotifications 1 }

## TN-IONCHASSIS-MIB

### *ionChassisDiscoveredEvt*

An ionChassisDiscoveredEvt event is sent when a new chassis is discovered.

### Varbinds

#### *entPhysicalIndex*

SYNTAX INTEGER

DESCRIPTION

"The entPhysicalIndex in this chassis."

#### *ionChassisStackSerialNo*

SYNTAX OCTET STRING

DESCRIPTION

"The chassis serial number, this is unique to each chassis."

### OID

#### MIB Definition

ionChassisDiscoveredEvt NOTIFICATION-TYPE

```
OBJECTS {  
    entPhysicalIndex,  
    ionChassisStackSerialNo  
}
```

STATUS current

DESCRIPTION

"An ionChassisDiscoveredEvt event is sent when a new chassis is discovered."

```
::= { tnIonChassisNotifications 1 }
```

***ionChassisRemovedEvt***

An ionChassisRemovedEvt event is sent when a managed chassis is removed.

**Varbinds*****entPhysicalIndex***

SYNTAX INTEGER

DESCRIPTION

"The entPhysicalIndex in this chassis."

***ionChassisStackSerialNo***

SYNTAX OCTET STRING

DESCRIPTION

"The chassis serial number, this is unique to each chassis."

**OID****MIB Description**

ionChassisRemovedEvt NOTIFICATION-TYPE

```
OBJECTS {  
    entPhysicalIndex,  
    ionChassisStackSerialNo  
}
```

STATUS current

DESCRIPTION

"An ionChassisRemovedEvt event is sent when a managed chassis is removed."

::= { tnIonChassisNotifications 2 }

## TN-ION-ENTITY-SENSOR-MIB

### ***entSensorThresholdNotification***

The sensor value crossed the threshold listed in entSensorThresholdTable.

This notification is generated once each time the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification.

### ***Varbinds***

#### **entSensorThresholdValue**

SYNTAX            SensorValue

DESCRIPTION

"This variable indicates the value of the threshold.

To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision.

However, you can directly compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."

#### **entSensorValue**

SYNTAX            SensorValue

DESCRIPTION

"This variable reports the most recent measurement seen by the sensor.

To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision.

However, you can compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."

### **SensorValue TEXTUAL-CONVENTION**

SensorValue ::= TEXTUAL-CONVENTION

STATUS            current

DESCRIPTION

"For sensors that measure volts AC, volts DC, amperes, watts, hertz, Celsius, or cmm, this item is a fixed point number ranging from -999,999,999 to +999,999,999. Use the value -1000000000 to indicate underflow. Use the value +1000000000 to indicate overflow. Use SensorPrecision to indicate how many fractional digits the SensorValue has.

For sensors that measure percentRH, this item is a number ranging from 0 to 100.

For sensors that measure rpm, this item can take only nonnegative values, 0..999999999.

For sensors of type truthvalue, this item can take only two values: true(1), false(2).

For sensors of type specialEnum, this item can take any value in the range (-1000000000..1000000000),

but the meaning of each value is specific to the sensor.

For sensors of type other and unknown, this item can take any value in the range (-10000000000..10000000000), but the meaning of the values are specific to the sensor.

Use Entity-MIB entPhysicalTable.entPhysicalVendorType to learn about the sensor type."

SYNTAX INTEGER (-10000000000..10000000000)

## **OID**

### **MIB Description**

```
entSensorThresholdNotification NOTIFICATION-TYPE
OBJECTS { entSensorThresholdValue, entSensorValue }
STATUS current
DESCRIPTION
```

"The sensor value crossed the threshold listed in entSensorThresholdTable.

This notification is generated once each time the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification."

```
::= { entitySensorMIBNotifications 1 }
```



## TN-ION-MGMT-MIB

### *ionDMIRxIntrusionEvt*

An ionDMIRxIntrusionEvt event is sent if the ionDMIRxPowerLevel falls below the ionDMIRxPwrLvlPreset indicating an intrusion on the fiber.

### Varbinds

#### *ifIndex*

SYNTAX INTEGER32 ()

DESCRIPTION

"IF-MIB Index of the port this was relevant to."

#### *ionDMIRxPwrLvlPreset*

SYNTAX INTEGER (0..65535)

DESCRIPTION

"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."

#### *ionDMIRxPowerLevel*

SYNTAX INTEGER

DESCRIPTION

"DMI: Diagnostic Monitoring Interface for fiber transceivers. Receive power on local fiber measured in microwatts."

## OID

### MIB Description

ionDMIRxIntrusionEvt NOTIFICATION-TYPE

```
OBJECTS {
    ifIndex, ionDMIRxPwrLvlPreset, ionDMIRxPowerLevel
}
```

STATUS current

DESCRIPTION

"An ionDMIRxIntrusionEvt event is sent if the ionDMIRxPowerLevel falls below the ionDMIRxPwrLvlPreset indicating an intrusion on the fiber."

```
::= { tnIonMgmtNotifications 1 }
```

***ionDMIRxPowerEvt***

An ionDMIRxPowerEvt event is sent when there is a warning or alarm on Rx Power.

**Varbinds*****ifIndex******ionDMIRxPowerAlarm***

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),  
lowAlarm(6), highAlarm(7) }  
DESCRIPTION "."
```

***ionDMIRxPowerLevel***

```
SYNTAX      INTEGER  
DESCRIPTION
```

"DMI: Diagnostic Monitoring Interface for fiber transceivers. Receive power on local fiber, measured in microwatts."

**OID****MIB Description**

```
ionDMIRxPowerEvt  NOTIFICATION-TYPE  
OBJECTS {  
    ifIndex, ionDMIRxPowerAlarm, ionDMIRxPowerLevel  
}  
STATUS current  
DESCRIPTION  
"An ionDMIRxPowerEvt event is sent when there is a warning or alarm on Rx Power."  
::= { tnIonMgmtNotifications 2 }
```

***ionDMITxPowerEvt***

An ionDMITxPowerEvt event is sent when there is a warning or alarm on Tx Power.

**Varbinds*****ifIndex******ionDMITxPowerAlarm***

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),  
lowAlarm(6), highAlarm(7) }  
DESCRIPTION "."
```

***ionDMITxPowerLevel***

```
SYNTAX          INTEGER  
DESCRIPTION "DMI: Diagnostic Monitoring Interface for fiber transceiv-  
ers. Transmit power on local fiber measured in microwatts."
```

**OID****MIB Definition**

```
ionDMITxPowerEvt  NOTIFICATION-TYPE  
OBJECTS {  
    ifIndex, ionDMITxPowerAlarm, ionDMITxPowerLevel  
}  
STATUS current  
DESCRIPTION  
"An ionDMITxPowerEvt event is sent when there is a warning or alarm on Tx Power."  
::= { tnIonMgmtNotifications 3 }
```

**ionDMITxBiasEvt**

An ionDMITxBiasEvt event is sent when there is a warning or alarm on Tx Bias current,

**Varbinds*****ifIndex******ionDMITxBiasAlarm***

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),  
lowAlarm(6), highAlarm(7) }  
DESCRIPTION ". "
```

***ionDMITxBiasCurrent***

```
SYNTAX INTEGER  
DESCRIPTION  
"Transmit bias current on local fiber interface, in microamperes."
```

**OID****MIB Description**

```
ionDMITxBiasEvt  NOTIFICATION-TYPE  
OBJECTS {  
    ifIndex, ionDMITxBiasAlarm, ionDMITxBiasCurrent  
}  
STATUS current  
DESCRIPTION  
"An ionDMITxBiasEvt event is sent when there is a warning or alarm on Tx Bias current."  
::= { tnIonMgmtNotifications 4 }
```

***ionDMITemperatureEvt*****Varbinds*****ifIndex******ionDMITempAlarm***

SYNTAX INTEGER

DESCRIPTION "."

***ionDMITemperature***

SYNTAX INTEGER

STATUS current

DESCRIPTION

"Temperature of fiber transceiver in tenths of degrees C."

**OID****MIB Description**

ionDMITemperatureEvt NOTIFICATION-TYPE

```
OBJECTS {  
    ifIndex, ionDMITempAlarm, ionDMITemperature  
}
```

STATUS current

DESCRIPTION

"An ionDMITemperatureEvt event is sent when there is a warning or alarm on DMI temperature."

::= { tnIonMgmtNotifications 5 }

**TN-PROVBRIDGE-MIB**

None

## ION Public MIBS

### BRIDGE-MIB

#### ***newRoot***

The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.

#### **Varbinds**

None

#### **OID**

#### **MIB Description**

```
newRoot NOTIFICATION-TYPE
```

```
-- OBJECTS      { }
```

```
STATUS          current
```

```
DESCRIPTION
```

"The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional."

```
::= { dot1dNotifications 1 }
```

#### ***topologyChange***

A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newroot trap is sent for the same transition. Implementation of this trap is optional.

#### **Varbinds**

None

#### **OID**

#### **MIB Description**

```
topologyChange NOTIFICATION-TYPE
```

```
-- OBJECTS      { }
```

```
STATUS          current
```

```
DESCRIPTION
```

"A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newroot trap is sent for the same transition. Implementation of this trap is optional."

```
::= { dot1dNotifications 2 }
```

## ENTITY-MIB

entConfigChange NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.

An agent should not generate more than one entConfigChange 'notification-event' in a given time interval (five seconds is the suggested default). A 'notification-event' is the transmission of a single trap or informs PDU to a list of notification destinations.

If additional configuration changes occur within the throttling period, then notification-events for these changes should be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event should be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started right away.

An NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events, e.g., due to throttling or transmission loss."

::= { entityMIBTrapPrefix 1 }

## EtherLike-MIB

None

## IANA-MAU-MIB

None

## IEEE8021-CFM-V2-MIB

None

## IEEE8021-TC-MIB

None

## IF-MIB

***linkDown***

**varbinds**

***ifIndex***

SYNTAX InterfaceIndex

DESCRIPTION

"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

***ifAdminStatus***

```
SYNTAX  INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3)      -- in some test mode
}
```

## DESCRIPTION

"The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state)."

***ifOperStatus***

```
SYNTAX  INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3),      -- in some test mode
    unknown(4),      -- status can not be determined
                    -- for some reason.
    dormant(5),
    notPresent(6),    -- some component is missing
    lowerLayerDown(7) -- down due to state of
                    -- lower-layer interface(s)
}
```

## DESCRIPTION

"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

***InterfaceIndex ::= TEXTUAL-CONVENTION***

DISPLAY-HINT "d"

## DESCRIPTION

"A unique value, greater than zero, for each interface or interface sub-layer in the managed system. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

```
SYNTAX  Integer32 (1..2147483647)
```



## OID

### MIB Description

```
linkDown NOTIFICATION-TYPE
OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
STATUS current
DESCRIPTION
```

"A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."

```
::= { snmpTraps 3 }
```

### *linkUp*

#### varbinds

### *ifIndex*

```
SYNTAX      InterfaceIndex
DESCRIPTION
```

"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

### *ifAdminStatus*

```
SYNTAX  INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3)      -- in some test mode
}
```

DESCRIPTION

"The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state)."

### *ifOperStatus*

```
SYNTAX  INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3),     -- in some test mode
    unknown(4),     -- status can not be determined -- for some reason.
    dormant(5),
    notPresent(6),  -- some component is missing
    lowerLayerDown(7) -- down due to state of -- lower-layer interface(s)
}
```

DESCRIPTION

"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

### ***InterfaceIndex ::= TEXTUAL-CONVENTION***

DISPLAY-HINT "d"

DESCRIPTION

"A unique value, greater than zero, for each interface or interface sub-layer in the managed system. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

SYNTAX Integer32 (1..2147483647)

## **OID**

### **MIB Description**

linkUp NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }

STATUS current

DESCRIPTION

"A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 4 }

## **LLDP-MIB**

None

## **NOTIFICATION-LOG-MIB**

None

## **P-BRIDGE-MIB**

None

## **Q-BRIDGE-MIB**

None

## **RFC1213-MIB**

None

## RMON-MIB (RFC 2819)

### *risingAlarm*

SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP.

### **Varbinds**

### *alarmIndex*

SYNTAX Integer32 (1..65535)

#### DESCRIPTION

"An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device."

### *alarmVariable*

SYNTAX OBJECT IDENTIFIER

#### DESCRIPTION

"The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.

Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

### *alarmSampleType*

SYNTAX INTEGER {  
    absoluteValue(1),  
    deltaValue(2)  
}

#### DESCRIPTION

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

This object may not be modified if the associated alarmStatus object is equal to valid(1).

***alarmValue***

SYNTAX Integer32

## DESCRIPTION

"The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds.

The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes."

***alarmRisingThreshold***

SYNTAX Integer32

## DESCRIPTION

"A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.

A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3).

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

**OID****MIB Description**

risingAlarm NOTIFICATION-TYPE

OBJECTS { alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmRisingThreshold }

STATUS current

## DESCRIPTION

"The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps."

::= { rmonEventsV2 1 }

### ***fallingAlarm***

The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

## **Varbinds**

### ***alarmIndex***

SYNTAX Integer32 (1..65535)

DESCRIPTION

"An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device."

### ***alarmVariable***

SYNTAX OBJECT IDENTIFIER

DESCRIPTION

"The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.

Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

### ***alarmSampleType***

SYNTAX INTEGER {  
    absoluteValue(1),  
    deltaValue(2)  
}

DESCRIPTION

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

This object may not be modified if the associated alarmStatus object is equal to valid(1).

***alarmValue***

SYNTAX Integer32

## DESCRIPTION

"The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds.

The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes."

***alarmRisingThreshold***

SYNTAX Integer32

## DESCRIPTION

"A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3).

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

**MIB Description**

fallingAlarm NOTIFICATION-TYPE

OBJECTS { alarmIndex, alarmVariable, alarmSampleType,  
alarmValue, alarmFallingThreshold }

STATUS current

## DESCRIPTION

"The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps."

```
::= { rmonEventsV2 2 }
```

**RMON2-MIB**

None

**SNMP-COMMUNITY-MIB**

None

**SNMP-NOTIFICATION-MIB**

None

**SNMP-TARGET-MIB**

None

## 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 18: Trap Server Log File Description**

Category	Example	Meaning
E=		Endian
Ebig=		bugEndian
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 IETF RFC 2573, available from the IETF web site at <http://www.ietf.org/rfc/rfc2573.txt>.



## Appendix D. ION C3210 to GFEB105 Feature Mapping

The C3210 is intended to be linked over fiber to a stand-alone CGFEB10xx-120. This appendix describes how these two converters work together, particularly in the area of Max frame size limitations in this configuration.

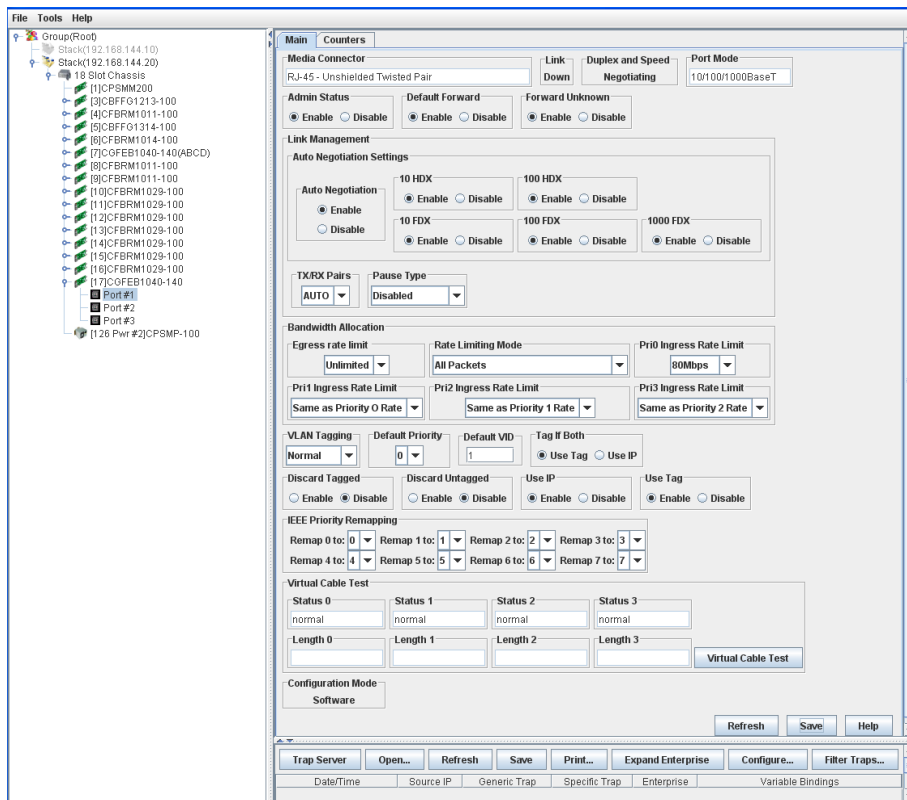
This appendix outlines the similarities and differences in the terminology used in the management of each product (see figures and table below) for concurrent C3210 and CGFEB10xx-120 users.

The SGFEB10xx-12x is a 10/100/1000 Ethernet Media Converter that can integrate 1000Base-SX/LX Fiber into 10/100/1000 Copper environments, extend network distance, and bridge legacy 10/100 devices to a Gigabit backbone. SGFEB10xx-12x features include Auto-Negotiation (copper and fiber ports), Switch-selectable speeds (UTP) when Auto Negotiation is off, AutoCross, Link Pass Through, Remote Fault Detect, and Pause.

Device Level configuration is very similar, so the focus here is on the port level configuration comparisons. At port level, some fields like Auto Negotiation are not addressed here since they are the same between the devices. Fields which are very different are highlighted in the table below in red. These are distinguishable feature differences between the products.

### PS GFEB Port 1 (Copper) Main Tab

The Main tab of Port # 1 of the Point System CGFEB1040-140 is shown below.



**ION 3210 Port level MAIN Tab**

The screenshot shows the 'MAIN' tab of the ION 3210 Port level configuration. The left sidebar lists the ION Stack components, including Chassis and various ports. The main area contains the following sections:

- Circuit ID:** A text input field.
- Port Configuration:**
  - Link Status: Down
  - Admin Status: Up
  - Speed: 100Mbps
  - Duplex: Full Duplex
  - Port Mode: 10/100/1000BaseT
  - AutoCross Mode: MDI
  - Connector Type: RJ-45
- Auto Negotiation Settings:**
  - Auto Negotiation: Disabled
  - Force Speed: 100Mbps
  - Force Duplex: Full Duplex
- Port Forward Management:**
  - Source Port: 1
  - Forward Settings: Port 1 to Port 2
- Virtual Cable Test:**

Index	Status	Distance To Fault
Pair 1 and 2	Unknown	
Pair 3 and 6	Unknown	
Pair 4 and 5	Unknown	
Pair 7 and 8	Unknown	

Buttons at the bottom: Refresh, Save, Help. Status bar: Getting values finished, Version: 0.7.6

**ION 3210 Port level ADVANCED Tab**

The screenshot shows the 'ADVANCED' tab of the ION 3210 Port level configuration. The left sidebar is the same as the MAIN tab. The main area contains the following sections:

- Bandwidth Allocation:**
  - Rate Limiting Mode: Counts All Layer 2
  - Egress Rate Limit: Unlimited
  - Ingress Rate Limit: Unlimited
- MAC Security:**
  - Filter Unknown Unicast: Disabled
  - Filter Unknown Multicast: Disabled
- VLAN Forwarding Rules:**
  - Discard Tagged: Disabled
  - Discard Untagged: Disabled
  - Default VLAN ID: 1
- Priority Forwarding Rules:**
  - Default Priority: 0
  - IEEE Priority Class: Enabled
  - IP Traffic Class: Enabled
  - Priority Precedence: Use IP
- VLAN Tag Management:**
  - Frame Tag Mode: Customer
  - Provider Ether Type: x88A8
  - Network Mode Tagging: Unmodified
- User Priority:**

Remap 0 to:	1	Remap 2 to:	3
Remap 4 to:	5	Remap 6 to:	7

Buttons at the bottom: Refresh, Save, Help. Status bar: Getting values finished, Version: 0.7.6

Fields (features) which are very different are shown with an asterisk in **red\*** in the table below.

**Table 19: ION C3210-to-xGFEB105 Feature Mapping**

PS GFEB	ION C3210	Description
Tx/Rx Pairs	Autocross	Autocross options of MDI, MDI-X, Auto.
Default Forward	Filter Unknown Multicast	To forward or discard unknown Multicast frames.
Forward unknown	Filter unknown Unicast	To forward or discard unknown Unicast frames.
Default priority	Default priority	Default priority of this port; frames that ingress this port untagged are assigned this priority
Default VID	Default VLAN ID	Default VLAN ID of this port; frames that ingress this port untagged are assigned this VLAN ID.
Rate Limiting Mode*	Rate Limiting Mode*	<p>Controls how to count the rate for the purpose of rate limiting.</p> <p>CGFEB: the options are the types of frames (Broadcast, Multicast, Unknown, Unicast, or All Packets).</p> <p>C3210: the options are different. The Rate Limiting Mode field controls which bytes in a frame will be counted in determining the rate limit:</p> <ul style="list-style-type: none"> <li>• Counts All Layer 1: (the default): in determining the rate limit, this selection counts the following bytes in a frame: Preamble (8 Bytes) + DA to CRC + Inter Frame Gap (12 bytes).</li> <li>• Counts All Layer 2: in determining the rate limit, this selection counts the bytes in a frame from the DA to the CRC in determining the rate limit.</li> <li>• Counts All Layer 3: in determining the rate limit, this selection counts the following bytes in a frame; either 1) from the DA (Destination MAC) to the CRC (18 bytes if untagged), or 2) from the DA (Destination MAC) to the CRC (22 bytes if tagged).</li> </ul> <p>Note: The Counts All Layer 3 selection will skip the Ethernet header, the CRC, and Tags (if any tags exist).</p>
Egress rate limit	Egress rate limit	Egress rate control, the actual list of values differs between the products.
Prio0 Ingress rate limit*	Ingress rate limit*	<p>Ingress rate limiting. CGFEB: this is only for frames that are in the prio0 queue. ION C3110: the rate limits apply to all kinds of traffic.</p>
Prio1 Ingress rate limit*	Not Applicable*	Ingress rate limiting. On CGFEB, this is only for frames that are in the prio1 queue.
Prio2 Ingress rate limit*	Not Applicable*	Ingress rate limiting. On CGFEB, this is only for frames that are in the prio2 queue.
Prio3 Ingress rate limit*	Not Applicable*	Ingress rate limiting. On CGFEB, this is only for frames that are in the prio3 queue.

PS GFEB	ION C3210	Description
Discard Tagged	Discard Tagged	To discard or forward tagged frames
Discard untagged	Discard untagged	To discard or forward untagged frames
VLAN Tagging*  1) Normal 2) Double Tag 3) Tag 4) Untag	VLAN Tag Management*: Frame Tag Mode & Network Mode tagging  1) Customer 2) Provider 3) Network (Add tag in network mode tagging) 4) Network (Remove tag in network mode tagging)	The devices do the same kind of VLAN tag/untagging options but the terminology options differ as highlighted.
Ether type default to 0x8100 not user configurable*	Provider Ether type *	The ION C3210 lets you choose one of the 3 Ether types (0x8100, 0x9100, 0x88a8) when Provider mode (double tagging) is enabled.
Use IP	IP traffic class	To enable or disable using the IP traffic class or DiffServ priority if present in the frame for switching decisions.
Use IEEE	IEEE priority class	To enable or disable using the IEEE priority if present in the frame for switching decisions.
Tag if Both	Priority precedence	If both the options of using IP and IEEE priority are enabled and if a frame happens to have both then which one should be used for switching decision is decided by this field. The options are 'use IP' or 'use IEEE' priority for this frame.
IEEE priority remapping	User priority	Gives a table of remapping options 0-7.

Counters which are very different are shown with an asterisk in red \* in the table below.

PS GFEB	ION C3210	Description
Only RMON mib counters*	RMON, IF-MIB stats and Ether-like MIB statistics *	The ION C3210 provides more MIB counters.

Other notable differences are shown with an asterisk in red \* in the table below.

PS GFEB	ION C3210	Description
Max frame size is 1632*	Max frame size is 10k*	The ION C3210 supports Jumbo frames.
'Port x-y Block forwarding' [3-port version] and 'Port VLAN' [2-port version] available at device level	It is available on each port as 'Port Forward Management' → Forward settings checkbox *	To allow frames to be forwarded between Port 1 and Port 2 or not. Typically used for spoofing in one direction.
No uptime information	Uptime available*	The ION C3210 reports System Uptime.
No unique string for device or port level	Unique string "Circuit ID" can be assigned to the device and on each port. *	The ION C3210 supports Circuit ID assignment and display.
No MAC address given to the unit	Has a unique MAC address used for all backplane communication. Not really used for any user communication. *	The ION C3210 supports MAC addressing.

## Index

- Archive file
  - Creating, 105
  - Uploading, 106
- Auto negotiate, 51
- AutoCross, 9, 49
- Auto-negotiation, 9
- Backing up the configuration, 75, 77
- browser support, 27
- CGFEB10xx-120, 245
- Chassis installation, 20
- Circuit ID, 44, 46
- CLI error messages, 120
- Config File, 79
- Configuration
  - Backing up, 10, 75, 77
  - Restoring, 80
- Connecting by
  - Telnet, 26
  - Web, 27
- Conventions, documentation, 18
- Database index file, 105
- db.idx.file, 105
- db.zip file, 105
- Defaults
  - Reset factory settings, 85
- Device Description field, 12
- Documentation conventions, 18
- Duplex LED
  - Model x3230-10xx, 23
- Duplex modes, 23
- Duplex setting, 52, 55
- Error messages
  - CLI commands, 120
  - Web interface, 153
- Ethernet connection
  - Telnet CLI, 26
  - Web interface, 27
- Ethernet connector
  - Model x3230-10xx, 23
- Features
  - Management module, 8
- Firmware
  - Archive file, 105
  - Backing up, 75, 77
  - Database index file (db.idx), 105
  - Upgrading, 97
- FocalPoint, 9
- Full duplex operation, 23
- GFEB105, 245
- GUI, 30
- Half-duplex operation, 23
- Install
  - Chassis model, 20
  - IONMM, 20
  - SFPs, 21
  - USB driver, 24
- LEDs, 22
- Link active LED
  - Model x3230-10xx, 23
- MAC address
  - Blocking, 12, 61
  - Filtering, 11
- Management VLAN, 68
  - Configuring, CLI method, 68
- MDI, 9, 49
- MDIX, 9, 49
- Network access, 25
  - Telnet session, 26
  - Web interface, 27
- Network management system (NMS), 11
- Operating mode
  - 10 MBps, 23
  - 100 MBps, 23
  - 100Base-TX, 23
  - 10Base-T, 23
  - Full duplex, 23
  - Half-duplex, 23
- Pause, 9
- Pause frames, 52
- Point System, 7, 10, 16, 19, 245
- Port
  - Advertised capabilities, 51
  - Duplex setting, 52, 55
  - Pause capability, 52
  - Speed setting, 52, 55
- Power LED
  - Model x3230-10xx, 23
- Problem conditions, 115
- Provisioning tab, 75, 77, 80
- RADIUS
  - Configuring, CLI method, 61, 63
  - Configuring, Web method, 186
- Reboot, 94
  - Web method, 95
- Reset
  - Factory defaults, 85
  - Uptime, 88
- Reset to Factory Config, 86
- Resetting Defaults, 86
- Restart
  - ION MM, 94
- Restoring the configuration, 80, 83
- RFC 2544 Benchmarking, 13
- Security
  - MAC address blocking, 12, 61
- Serial interface

- Setup, 24
- Setup
  - Serial interface, 24
  - Telnet, 26
  - USB, 24
  - Web interface, 27
- SFP installation, 21
- SGFEB, 7, 8, 245, 247
- Signing in, 27
- Signing out, 29
- Simple network management protocol, see SNMP, 11
- SNMP, 11
- SOAM
  - Configuring, CLI method, 185
- Speed setting, 52, 55
- SSH
  - Configuring, CLI method, 69
- System Restart, 94
- Tech Support, 214
- Telnet
  - Default login, 216
  - Default password, 216
  - Ethernet connector, 23
  - Setup, 26
  - Terminate session, 26
- Terminate
  - Telnet session, 26
- TFTP, 10
  - Server address**, 106
  - Upgrading firmware, 99, 105
- Troubleshooting, 112
- Upgrade firmware
  - IONMM, 109
  - Other modules, 105
- USB
  - Default login, 216
  - Default password, 216
  - Driver installation, 24, 27
  - Setup, 24
- VLAN, 10
- VLAN Configuration, 67
- VLANs
  - Configuring, 67
- Web interface
  - Error messages, 153
  - Ethernet connector, 23
  - Signing in, 27
  - Signing out, 29

**Lantronix Corporate Headquarters**

48 Discovery  
Suite250  
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](http://www.lantronix.com/about/contact).