LANTRONIX®

ION Management Modules

IONMM and IONMM-232

User Guide

Part Number 33457
Revision N August 2026

Intellectual Property

© 2022-2026 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

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

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

Warranty

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

Contacts

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

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

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

Disclaimer

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

Revision History

Date	Rev	Description
10/31/18	J	FW v 1.3.16 added support for the IONPS-D-R1 48VDC power supply for the 19-slot ION chassis. FW v 1.3.18 updated the Backup All / Restore All feature and added IONMM-232 support. FW v 1.3.19 added C4221 support and updated the left column of the ION Web UI. FW v 1.4.2 added RMPS support and fixed red-boxing, CLI display of remote power supplies, and Restore.
9/14/22	K	FW v 1.5.0: Fixed issues with Daylight Savings Time (DST) enablement. Added management support for enhancements to C4221-4848. Added support for x6310 ION POTS Adapter, enhanced backup and restore operation, and added support for x4221 L2CP configuration. Initial Lantronix rebrand.
11/6/24	L	IONMM and IONMM-232 FW v 1.5.12: • Updated ssh server to v2022.82. • Updated DMI to show Vendor Specific Information. • Updated certificate and noted that after upgrading from version earlier than 1.5.0, new backups should be made. • Removed Glossary and Index. • Re-branded IONMM and IONMM-232 FW. • Updated online Help files. • Fixed expired IONMM Certificate. Added note that to see the new certificate, do a “Factory Reset” on the IONMM and then turn on HTTPs. • Added Note that Telnet is not secure. • Noted TAA and NDAA Compliant. • Updated features and specifications. • Allow IONMM CLI to view remote Ports from attached Local card C6120-1040. • Update DoCs. See the Release Notes for more information.
September 2025	M	IONMM 1.5.17: • Added SFTP support • Moved Backup All / Restore All command reference to *ION System CLI Reference, 33461*. • See the Release Notes for more information.
August 2026	N	IONMM 1.5.23: • Disable TLS 1.0/1.1

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

Caution: Do not ship or store devices near strong electrostatic, electromagnetic, magnetic, or radioactive fields.
Caution: When handling chassis Network Interface Devices (NIDs) observe electrostatic discharge precautions. This requires proper grounding; i.e., wear a wrist strap.
Caution: Copper based media ports, e.g., Twisted Pair (TP) Ethernet, USB, RS232, RS422, RS485, DS1, DS3, Video Coax, etc., are intended to be connected to intra-building (inside plant) link segments that are not subject to lightening transients or power faults. They are not to be connected to inter-building (outside plant) link segments that are subject to lightening.
Caution: Do not install the NIDs in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor NID performance.
Caution: Read the installation instructions before connecting the chassis to a power source. Failure to observe this caution could result in poor performance or damage to the equipment.
Caution: Only trained and qualified personnel should install or perform maintenance on the ION210-A chassis. Failure to observe this caution could result in poor performance or damage to the equipment.

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.

Warning: These products are not intended for use in life support products where failure of a product could reasonably be expected to result in death or personal injury. Anyone using this product in such an application without express written consent of an officer of Lantronix does so at their own risk, and agrees to fully indemnify Lantronix for any damages that may result from such use or sale.

See Chapter 6, for Electrical Safety Warnings translated into multiple languages.

Contents

1. Introduction 12

Document Overview 12
Product Overview 13
Model Descriptions 14
Features 14
Backup / Restore / Upgrade 14
Management Access Methods 15
IP Address Modes (IPv4 / IPv6, DHCP, Static, BootP) 15
Ethernet and USB Interfaces 15
Single Slot Design 15
Security Features 16
System Logging (Syslog) 16
SNMP Support 17
Multiple Community Strings 17
Physical Specifications 18
Documentation Conventions 19
Related Documents and Online Help 20

2. Installation 21

General 21
Installing the IONMM 21
Connections and LEDs 22
Accessing the IONMM 24
Using a Local Serial Interface (USB) 24
Operating Systems Supported 24
Installing the USB Driver - Windows XP 25
Installing the USB Driver - Windows 7 26
Installing the USB Driver - Windows 8.1 27
Configuring Terminal Emulator 28
Change COM Port for USB Serial Adapter 28
Starting a USB Session 29
Terminating a USB Connection 29
Cable-CCC-06 29
Access via an Ethernet Network 30
Starting a Telnet Session 30
Terminating a Telnet Session 30
Using SSH 31
Web Browser Support 31
Terminating the Web Interface 33
Setting up the IP Configuration 34
IPv4 Config Setup 34
IPv6 Config Setup 35

Menu System Description 37
Reboot and Reset Functions 39
System Reboot 39
Reset to Factory Config 40

3. Configuration 41

General 41
Setting the IPv4 Configuration 41
Configuring IPv4 Address Mode 42
IPv4 Addressing Config – CLI Method 42
IPv4 Addressing Config – Web Method 43
Assigning an IPv4 DHCP Address 44
IPv4 DHCP Config – CLI Method 44
IPv4 Address Mode (DHCP / Static / BootP) Config – Web Method 46
BootP Addressing Configuration 46
Defining Domain Name System (DNS) Servers 47
DNS Lookups over IPv6 Transport 47
DNS '3 vs. 3' Rule ('Up to 3' Rule) 47
DHCPv6 DNS Server Configuration 47
Static DNS Server Configuration 48
DNS Config – CLI Method 48
DNS Config – Web Method 50
IPv6 Description 52
Differences between IPv4 and IPv6 53
IPv6 Features 53
ION IPv6 Function Descriptions 54
IPv6 Management Functions 55
IPv6 Address Formats 55
ICMP v6 (Internet Control Message Protocol for IPv6) 56
IPv6 Neighbor Discovery Protocol 56
IPv6 DAD (Duplicate Address Detection) 56
IPv6 Static Configuration 59
ION IPv6 Configuration Considerations 60
IPv4 and IPv6 Initialization Defaults 61
IP Address Mode Notes 61
Telnet IPv4 and IPv6 Connections 61
TFTP IPv4 and IPv6 Connections 61
IPv6 Address Config – CLI Method 62
IPv6 Address Config – Web Method 63
Changes to Existing ION Applications with IPv4 / IPv6 65
Dynamic Table Entry Limits 65
System Configuration 66
System Configuration – CLI Method 66
System Configuration – Web Method 67
Login Type Configuration (Local / RADIUS / TACACS+) 68

Login Type Config – CLI Method 68
Login Type Config – Web Method 70
Ports Configuration 71
Port Configuration – CLI Method 71
Port Configuration – Web Method 72
Configuring System Login Users 73
Configuring System Login Users - CLI Method 74
Configuring System / Login Users - Web Method 75
Configuring Security Features 76
Configuring an ACL 77
ACL Config (IPv4) – CLI Method 79
ACL Config (IPv4) – Web Method 82
ACL under IPv6 85
ACL Config (IPv6) – CLI Method 85
ACL Config (IPv6) – Web Method 86
Configuring HTTPs 89
HTTPS Config – CLI Method 90
HTTPS Config – Web Method 91
Configuring Management VLAN 94
Management VLAN Config – CLI Method 95
Management VLAN Config – Web Method 96
Configuring RADIUS 97
RADIUS Config – CLI Method 98
RADIUS Config – Web Method 99
Configuring TACACS+ 101
TACACS+ Config - CLI Method 102
TACACS+ Config - Web Method 105
Configuring SNTP 106
SNTP Config – CLI Method 107
SNTP Config – Web Method 111
Configuring SSH 112
SSH Config – CLI Method 113
SSH Config – Web Method 115
Configuring SSH and RADIUS 118
Configuring System Logging (Syslog) 119
Syslog Config – CLI Method 121
Syslog Config – Web Method 122
Configuring SNMP 124
SNMP Config – CLI Method 125
SNMP Config – Web Method 128
Change a SNMP User's Group - Web Method 135
SNMP v3 Default Values 136
SNMP v3 Commands 138
Web Interface-to-CLI Command Cross Reference for SNMP 140

SNMP CLI Messages 141
ION SNMP Operation Example 142
Configuring SFTP 144
SFTP CLI Commands 144
SFTP Configuration – CLI Method 144
SFTP Configuration – Web Method 148

4. Operation 149

Backup and Restore Operations (Provisioning) 149
Backup the Configuration – Web Method 150
Backup Standalone Modules 153
Editing the Config File (Optional) 155
Restore the Configuration – Web Method 158
Backup and Restore - CLI Method 161
Backup All and Restore All 164
Backup All and Restore All – CLI Method 164
CLI Commands 164
Backup and Restore via the CLI 165
Troubleshooting - CLI Messages 168
Troubleshooting - config.err File Messages 172
Backup All and Restore All – Web Method 174
Backup All via the Web UI 174
Restore All via the Web UI 177
Troubleshooting – Web UI Messages 180
Disabling USB Console Access 184
Disabling Console Access – CLI Method 184
Reset to Factory Defaults 185
Resetting Defaults – CLI Method 185
Resetting Defaults – Web Method 185
Resetting Uptime 187
Uptime Reset – CLI Method 187
Uptime Reset – Web Method 187
System Reboot 189
Rebooting the System – CLI Method 189
Rebooting the System – Web Method 190
Transfer Files via Serial Protocol (X/Y/Zmodem) - CLI Method 191
Upgrade the Firmware 192
Upgrading IONMM and/or NID Firmware – CLI Method 192
Upgrading the IONMM Firmware – Web Method 195
Upgrading NIDs – Web Method 198
Performing the Upgrade 200
Management of Other Modules 204
Managing Using the CLI Commands 204
Managing via the Web Interface 206
Replacing the IONMM 207

5. Troubleshooting 208

General 208
Basic ION System Troubleshooting 208
Error Indications and Recovery Procedures 209
LED Fault and Activity Displays 210
Troubleshooting Auto-negotiation Mismatches 211
IPv6 Troubleshooting 211
Address Resolution in Windows 7 211
Verify IPv6 Configuration in Windows 7 211
Verify IPv6 Connectivity 212
Additional Information 212
IPv6 Auto Config Troubleshooting 212
Problem Conditions 213
CLI Messages 228
Web Interface Messages 275
SNMP Messages 289
Syslog Messages and Sys.log Output 300
Syslog Messages 300
Sample Sys.log Output 303
Windows Event Viewer Messages 306
Config Error Log (config.err) File 307
config.err Messages 308
config.err Message Responses 308
Webpage Messages 312
Recording Model Information and System Information 322

6. Compliance and Safety Information 324

NDAA, RoHS, REACH and WEEE Compliance 325
Trade Agreement Act (TAA) Compliant Products 325
Accessibility Statement 325
EU Declaration of Conformity 326
UK Declaration of Conformity 327
Electrical Safety Warnings 328

Appendix A. Factory Default Settings 329

Appendix B. Configuration Quick Reference – CLI 335

IPv4 Configuration 335
IPv6 Configuration 335
ACL Configuration (IPv4) 335
ACL Configuration (IPv6) 336
Backup / Restore Configuration 336
HTTPS Configuration 337
Management VLAN Configuration 337
RADIUS Configuration 337

Create a User with RADIUS and SSH Enabled 338
Create a User with SSH Enabled (RADIUS Disabled) 338
SFTP Configuration 338
SNMP Configuration 339
SNTP Configuration 340
SSH Configuration 340
Syslog Configuration 341
System (Login) User Configuration 341
TACACS+ Configuration 341
Transfer Files via Serial Protocol (X/Y/Zmodem) 342

Appendix C. ION System File Content and Location 343

File Status after Reset to Factory Defaults 343
Back Up and Restore File Content and Location 344
Reboot File Content and Location 345
Firmware Upgrade File Content and Location 346

List of Figures

Figure 1: Sample ION System Configuration 13
Figure 2: IONMM Installation 21
Figure 3: IONMM and IONMM-232 Connectors and LEDs 22
Figure 4 Multiple Routers - One DHCPv6 Router and One Router 54
Figure 5 Multiple DHCPv6 Servers and One Router 54
Figure 6 Multiple Routers 55
Figure 7 Multiple DHCPv6 Servers and Routers 55
Figure 8: CLI Location Hierarchy 204

List of Tables

Table 1: Physical Specifications 18
Table 2: Documentation Conventions 19
Table 3: IONMM Connector and LED Descriptions 23
Table 4: IONMM System-Level Menu Description 37
Table 5: Port-Level Menu Description 39
Table 6: User Level Rights via Web / CLI 73
Table 7: Timezones 107
Table 8: Syslog Severity Levels 119
Table 9: SNMP v3 Initialization (Default) Values 136
Table 10: SNMP v3 Web Interface Default Values 137
Table 11: SNMP Command Categories 138
Table 12: Web Interface to CLI Command Cross Reference 140
Table 13: Device-Level Factory Defaults 329
Table 14: Port-Level Factory Defaults 334
Table 15. File Status after a Reset to Factory Defaults 343
Table 16. Back Up and Restore File Content and Location 344
Table 17: File Content and Location after a System Reboot 345
Table 18: File Content and Location after a Firmware Upgrade 346

1. Introduction

Document Overview

The purpose of this manual is to provide you with information necessary to install, configure and use the ION Management Module (IONMM) from Lantronix.

This manual is set up as follows:

- 1: Introduction – This section provides an overview of the ION Management Module (IONMM) and briefly describes its features and functions.
- 2: Installing and Accessing the IONMM – This section describes how to install the IONMM in a chassis and connect to it through either a USB or SNMP interface. It also describes the connectors and LEDs that are on the IONMM.
- 3: Configuration – This section describes how to set up and configure the IONMM device and ports for various operations (HTTPS, SNMP, VLAN, etc.). Configuration guidelines are given for both serial interface and Web connections.
- 4: Operation – This section describes the various operations that can be performed via the IONMM.
- 5: Troubleshooting – This section describes any error messages, codes, or conditions that could occur during IONMM operations.
- 6: Compliance and Safety Information – This section provides compliance and safety information.
- Appendix A: Factory Default Settings – This appendix provides a table listing the default settings for the IONMM.
- Appendix B. Configuration Quick Reference –CLI - This appendix provides an overview of several main functions configurable via the CLI.
- Appendix C: ION System File Content and Location – This appendix provides information on the status of standard ION system files following Reset, Back Up, Reboot, and Firmware Upgrade operations.

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

Product Overview

The ION Management Module (IONMM) is a single slot design slide-in module that lets you configure and manage all the other ION family slide-in modules installed in an ION Chassis and remotely connected standalone modules. The IONMM can also manage standalone ION family media converters that are configured as remote devices (connected to a slide-in module in the ION chassis).

The IONMM connects directly to the chassis backplane and communicates with the individual ION slide-in modules installed within that ION Chassis. Only management traffic is sent across the ION Chassis backplane to maintain security of management access and information. No customer data traffic is shared on the backplane. The purpose of all other ION slide-in modules is to provide a network interface to various devices.

A simple ION System configuration is shown below.

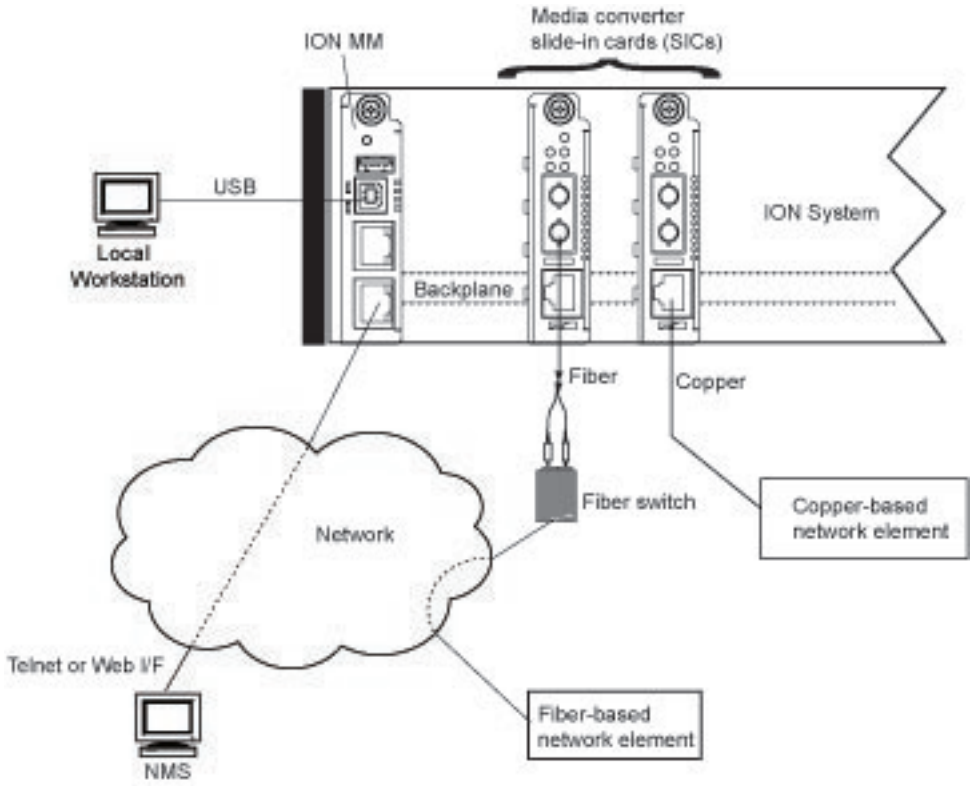


Figure 1: Sample ION System Configuration

Each slide-in module for the ION Chassis has specific features and functions that can be controlled via the IONMM. A network administrator can configure, monitor and troubleshoot ION modules remotely via the IONMM. Remote access to management information helps reduce operating expenses by reducing technician dispatches and lowering the mean-time-to-repair by proactively looking for potential issues and receiving detailed SNMP traps if a problem occurs.

For more information on managing other slide-in modules, see “Management of Other Modules”.

Model Descriptions

Model	Description
IONMM	Management Module for the ION Chassis with a USB Type B CLI port. Provides two 10/100 Mbps RJ-45 ports, one USB 2.0 device port, and one USB 2.0 host port.
IONMM-232	Management Module for the ION Chassis with a RS232 RJ-45 CLI port. Provides two 10/100 Mbps RJ-45 ports, one USB 2.0 device port, and one RS232 RJ-45 host port.
Cable-CCC-06	Cisco DB9 to RJ-45 console cable, 6 ft.; option, order separately. TAA Compliant.

Features

The following are features of the ION Management Module. Backup/restore/upgrade ION modules

- Various management access methods
- Two 10/100BaseT/TX Ethernet interfaces
- Single slot design
- Several security features
- Enhanced user management
- Syslog (System Logging)
- Multiple IP addressing modes (IPv4 / IPv6, DHCP, Static, Bootp)
- SNMP v1, v2c, and v3 Support
- Multiple community strings
- Public and private MIB support
- Management VLAN
- TLS
- SSH
- IEEE 802.1X/RADIUS
- ACL Rules
- SNTP

Backup / Restore / Upgrade

Through the IONMM you can backup and/or restore configurations for each of the modules in the ION system. You can also upgrade the firmware for all modules.

The IONMM can use TFTP (Trivial File Transfer Protocol) or SFTP (Secure File Transfer Protocol) to upload its present configuration onto a TFTP or SFTP server. The IONMM can also download the configuration from the TFTP or SFTP server to update its settings. TFTP or SFTP is useful when a user wants to program more than one unit to the same or similar configurations. One unit can be programmed and saved, 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.

For more information see “Backup/Restore Operations” and “Upgrade the Firmware”.

To find the latest version of the firmware, go to the Tech Support webpage.

Management Access Methods

Management of the IONMM, 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 IONMM through a locally-connected workstation running a terminal emulation program such as HyperTerminal.
- SSH/Telnet session – uses the CLI to access and control the IONMM through the network.
- Web-browser – access and control the IONMM using a standard web browser and a graphical user interface (GUI).
- Simple Network Management Protocol (SNMP) – ION management uses both public and private Management Information Bases (MIBs) allowing a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).

IP Address Modes (IPv4 / IPv6, DHCP, Static, BootP)

The ION software supports IPv4/IPv6 dual protocol stacks, which allows IPv4 and IPv6 to co-exist in the same devices, in the same physical interface, and in the same networks. IPv4 is a basic feature that is always enabled, but the IPv6 is an enhanced feature that you can disable and enable. When IPv6 is disabled, the configurations related to IPv6 will exist but will not function. These configurations can be changed or removed by the user. The ION software supports multiple DHCP or DHCPv6 or Stateless (Router) servers.

The IONMM supports DHCP, Static IP, and BootP addressing modes.

BOOTP (Bootstrap Protocol) is a network protocol used by a network client to obtain an IP address from a configuration server. BOOTP is usually used during the bootstrap process when a computer is starting up. A BOOTP configuration server assigns an IP address to each client from a pool of addresses. BOOTP uses the User Datagram Protocol (UDP) as a transport on IPv4 networks only.

BOOTP uses two well-known port numbers: UDP port number 67 for the server and UDP port number 68 for the BOOTP client. BOOTP and its extensions became the basis for the Dynamic Host Configuration Protocol (DHCP). If configured for BOOTP mode, the IP address will be assigned by IETF RFC951.

Ethernet and USB Interfaces

The IONMM has two Ethernet 10/100 BaseT RJ-45 connectors that allow the network administrator to manage the ION chassis through a remote computer using either a remote Telnet connection or a Web interface. The IONMM has a Universal Serial Bus (USB) connector; a serial port for configuring and controlling the IONMM and other slide-in cards through a command line interface (CLI). The IONMM-232 has an RJ-45 RS-232 CONSOLE connector for CLI commands.

Single Slot Design

The single slot design of the IONMM optimizes the number of slide-in modules that can be installed in the ION chassis.

Security Features

The security features allow you to control access to the ION Chassis via the IONMM to ensure that only authorized personnel can view and change the settings of the slide-in modules.

- Log user out if idle (inactive) for 15 minutes and display "*You are now logged out.*".
- Access Control Lists (ACLs) – ACLs can be configured in the IONMM to allow access to authorized users and to deny access to all others. For more information see "Configuring an ACL".
- Hypertext Transfer Protocol Secure (HTTPS) – the IONMM supports the use of HTTPS, which utilizes the secure socket layer (SSL) protocol for transmitting private documents via the Internet. For more information see "Configuring HTTPS".
- Management VLAN – In a VLAN enabled network, the administrator can assign a VLAN as a management VLAN. This VLAN ID will be used in all management frames. This separates the management traffic from the data. For more information see "Configuring Management VLAN".
- RADIUS authentication – The IONMM supports authentication using the Remote Authentication Dial In User Service (RADIUS) protocol. When enabled, RADIUS is used to authenticate and authorize users trying to access the IONMM through either the Web login, serial port (USB), or SSH/Telnet session. The RADIUS server must be configured before RADIUS authentication is enabled. For more information see "Configuring RADIUS".
- TACACS+ (Terminal Access Controller Access Control System) provides routers and access servers with authentication, authorization and accounting services. TACACS+ is used along with or as a replacement for RADIUS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Some administrators recommend using TACACS+ because TCP is seen as a more reliable protocol. While RADIUS combines authentication and authorization in a user profile, TACACS+ separates the authentication and authorization operations. By default, Tacplus listens on TCP port 49 and provides network devices with authentication, authorization and accounting services (AAA). For more information see "Configuring TACACS+".
- Secure Shell (SSH) authentication – the IONMM supports both the Rivest-Shamir-Adleman (RSA) and Digital Signature Algorithm (DSA) for public key cryptography for both connection and authentication. For more information see "Configuring SSH".
- USB access – The USB port can be turned off to prevent unauthorized access to the system through the serial interface. For more information see "Disabling the Serial Interface (USB)".

System Logging (Syslog)

The IONMM supports system logging via the Syslog function. Syslog can be used for system management and security auditing, as well as generalized information, analysis, and message debugging. Since Syslog is supported by a wide variety of devices and receivers across multiple platforms, it is used to integrate log data from many different types of devices into a central repository. The syslog protocol conveys event notification messages using a layered architecture, allowing a variety of transport protocols, and providing a message format of vendor-specific extensions to be provided in a structured way.

The IONMM System Log lets you configure the Syslog Server Address, Server Port, Level (one of eight levels of reporting), and logging Mode (local, remote, local and remote, or no logging). A recommended practice is to use the Notice or Informational level for normal messages.

SNMP Support

Simple Network Management Protocol (SNMP) is a network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The IONMM supports three security models: SNMPv1, SNMPv2c, and SNMPv3.

SNMPv1 (SNMP version 1) is the original Internet-standard Network Management Framework, as described in IETF RFCs 1155, 1157, and 1212.

SNMPv2c (Community-based SNMP version 2) is a SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is like the SNMPv1 message format. The second version of SNMP, it supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security. Both versions (SNMPv1 and SNMPv2) of the Internet Standard Management SNMP Framework share the same basic structure and components, and all versions follow the same architecture. The SNMP framework consists of 1) a data definition language, 2) definitions of management information (the Management Information Base, or MIB), 3) a protocol definition, and 4) security and administration.

SNMPv3 (Simple Network Management Protocol Version 3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.
SNMPv3 provides important security features: 1) Confidentiality - Encryption of packets to prevent snooping by an unauthorized source. 2) Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism. 3) Authentication - to verify that the message is from a valid source.

Multiple Community Strings

The IONMM supports the use of multiple SNMP community strings. SNMP community strings are like passwords for network elements. Most often, there is one community string which is used for read-only access to a network element. The default value for this community string is often “public”. Using this community string like a password, the NMS can retrieve data from network elements.

Less often, there is also a read-write community string. The default value for this is often “private”. Using this community string, the NMS can change MIB variables on a network element.

Physical Specifications

The physical specifications for the IONMM are described in the table below. See the *IONMM-232 Install Guide* for IONMM-232 specifications.

Table 1: Physical Specifications

Item	Specification
Standards	IEEE 802.3, IEEE 802.1x
Ports	IONMM: two 10/100 Mbps RJ-45 ports, one USB 2.0 device port, one USB 2.0 host port. IONMM-232: two 10/100 Mbps RJ-45 ports, one USB 2.0 device port, one RS232 RJ-45 host port.
Dimensions	Width: 0.86” (22 mm) x Depth: 6.5” (165 mm) x Height: 3.4” (86 mm)
Power Consumption	2 Watts under normal operation. 4.8 Watts with full 2.5 Watts used by USB host port (e.g., with a Flash Drive connected requiring 2.5 Watts).
Environment	Environment specs are dependent on the chassis chosen. Operating Temp: 0°C to +50°C (+32 to +122°F) Storage Temp: 0 to 85°C (-40 to 185°F) Humidity: 5% - 95% (non-condensing) Altitude: 0 to 10,000 ft.
Shipping Weight	1 lb. [0.45 kg]
Compliance	EN55022 Class A, EN55024, CE Mark, TAA and NDAA Compliance
Warranty	Lifetime

Documentation Conventions

The following conventions are used in this manual for commands/input entries.

Table 2: Documentation Conventions

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

Related Documents and Online Help

A printed Documentation Postcard is shipped with each IONMM. Context-sensitive Help screens and cursor-over-help (COH) facilities are built into the Web interface.

For Lantronix Documentation, Firmware, Application notes, etc. see the Lantronix Technical Resource Center.

The ION system and related manuals are listed below.

1. IONMM-232 Install Guide, 33725
2. ION System CLI Reference, 33461
3. ION106-x Six Slot Chassis User Guide, 33658
4. ION219-x 19-Slot Chassis Installation Guide, 33412
5. ION219 Cxx1x NID Installation Guides, 33414 - 33417
6. ION Dry Contact Relay (DCR) Kit Install Guide, 33422
7. ION ADP Install Guide, 33413
8. SFP manuals (see the Lantronix SFP page)
9. ION System Release Notes (software version related)
10. Product Support Postcard, 33504

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

Note that this manual provides links to third part web sites for which Lantronix is not responsible.

2. Installation

General

This section describes how to install the ION Management Module (IONMM) in an ION Chassis, and the procedures to access and initially set up the IONMM through either a local serial interface (USB) or a remote Ethernet connection (SSH/Telnet session or Web interface).

Installing the IONMM

The IONMM is to be installed only in a Lantronix ION chassis (e.g., ION106-x or ION219-x). A complete list of ION products is on our IONMM webpage.

Note: While the IONMM can be hot swapped in any slot in the chassis system, Lantronix recommends that an organization use the same slot in every chassis, thereby normalizing any maintenance procedures and techniques. Typically, this has the IONMM installed in slot 1 of the chassis as shown in the figure below.

Use the procedure below to install the IONMM in the ION chassis.

Wear a grounding device and observe electrostatic discharge precautions when installing the IONMM into the chassis. Failure to observe this caution could result in damage to or failure of the module.

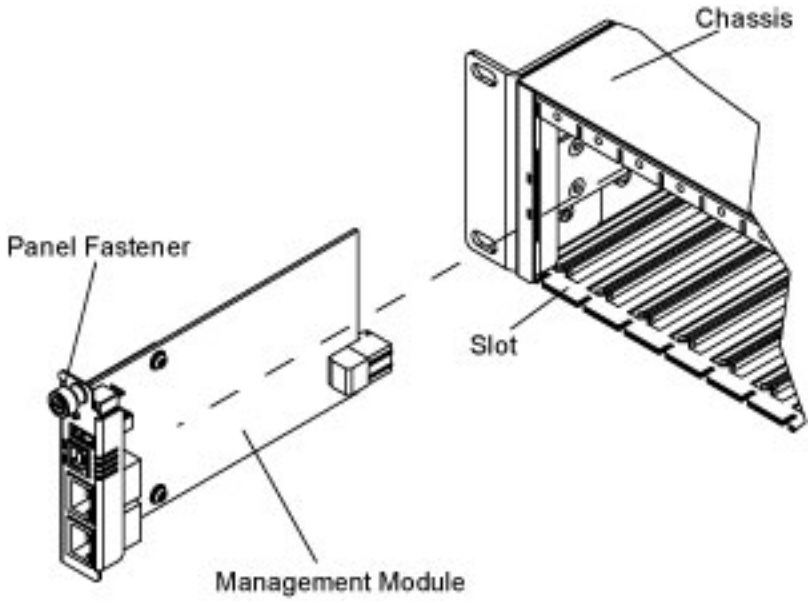


Figure 2: IONMM Installation

Note: The IONMM is a “hot swappable” device and can be installed with power on in the chassis.

1. Locate an empty slot in the ION System chassis.
2. Grasp the edges of the card by its front panel.
3. Align the module with the upper and lower slot guides, and carefully insert the card into the installation slot.
4. Firmly seat the card against the chassis back panel.
5. Push in and rotate clockwise the panel fastener screw to secure the card (see Installing the IONMM on the previous page).
6. Connect the management module to the network via the USB Device and Port 1 or Port 2.
7. See “Accessing the IONMM”.

Connections and LEDs

The IONMM connections and LEDs are shown in the figure below.

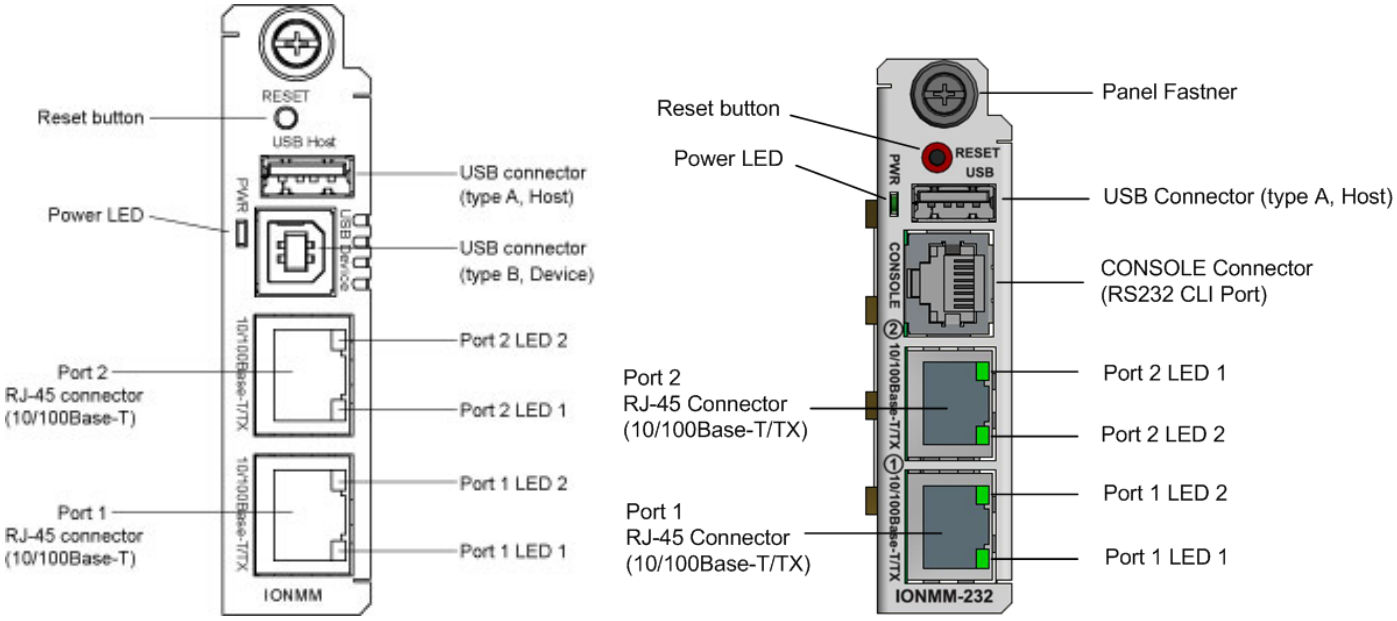


Figure 3: IONMM and IONMM-232 Connectors and LEDs

The IONMM connections and LEDs shown in Figure 3 above are described in the table below.

Table 3: IONMM Connector and LED Descriptions

Connector/LED	Description
RESET button	Pressing this button reinitializes the IONMM.
USB connectors (IONMM)	Two universal serial bus (USB) connectors. **USB-HOST** – not used (for future use). **USB-DEVICE** – used to connect the IONMM to a PC for a direct serial interface. A system administrator can access and control the IONMM using CLI commands through this connection.
USB connector (IONMM-232)	One USB Connector (type A, Host)
CONSOLE Connector (IONMM-232)	One RJ-45 RS-232 connector for CLI commands)
10/100BASE-T/TX RJ-45 connectors (Port 1 and Port 2)	Two connectors 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 SSH/Telnet session or the Web interface. **Note:** Port1 is the lower port and Port 2 is the upper port.
PWR (Power) LED	When lit, the PWR led indicates that there is power to the Management Module.
LED 1 (Ports 1 and 2)	Yellow – operation is 10 Mbps, 10Base-T. Green – operation is 100 Mbps, 100Base-T.
LED 2 (Ports 1 and 2)	On (lit) indicates duplex mode: • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Accessing the IONMM

The IONMM (or IONMM-232, hereafter "IONMM") can be accessed by using either a local serial interface via a USB connection or through an Ethernet network connection. The network connection can be done via an SSH or Telnet session or a Web graphical user interface (GUI).

Using a Local Serial Interface (USB)

The IONMM can be connected to a local management station (PC) through a serial interface using a connection. The IONMM 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 end)
- Terminal emulator program (e.g., HyperTerminal) on the PC
- USB driver installed on the PC
- Configured COM port

Operating Systems Supported

USB drivers for the following Operating Systems are available on the ION System web page.

Windows® 7	Windows 8 (32 bit)	Windows 10 (32 bit/64 bit)
Windows 7 x64	Windows 8 (64-bit)	Windows 11

The Virtual COM port (VCP) drivers make the USB device appear as an additional COM port available to the PC. Application software can access the USB device in the same way as it would access a standard COM port. The drivers are not required with the IONMM-232.

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 this procedure. The drivers are not required with the IONMM-232.

To install the USB driver on a computer with the *Windows XP* operating system, do the following.

1. Extract the driver from the website and place it in an accessible folder on the local drive of the PC.
2. Connect the IONMM to the USB port on the PC. 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.
9. Click **Next**. Installation of the driver begins.
10. When the finished installing screen displays, click **Finish**.

The USB driver installation is complete. You must now configure the COM port to be used by the terminal emulator.

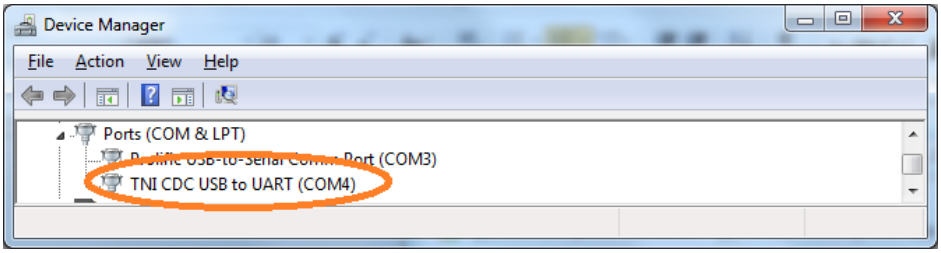
Installing the USB Driver - Windows 7

IMPORTANT

The following driver installation instructions are for the *Windows 7 (64-bit)* operating system only. Installing the USB driver using another operating system is similar, but not necessarily identical to this procedure. The drivers are not required with the IONMM-232.

To manually install the USB driver on a computer with the *Windows 7 64-bit* operating system, do the following.

1. Extract the driver from the website and place it in an accessible folder on the local drive of the PC.
2. Connect the IONMM to the USB port on the PC.
3. Open Windows Control Panel.
4. Select System > Hardware > Device Manager. The Device Manager window displays. **Note**: You must be logged on as an administrator or have administrative privileges to access the Device Manager.
5. Right-click USB-Serial Controller in the Other devices tab, and then select Install from the drop down menu. A dialog box displays.
6. Select Browse my computer for driver software. You will be asked to install the driver.
7. Select Install. When updating the driver software is complete a dialog box appears saying, “Windows has successfully updated your driver software...”.
8. The USB driver installation is complete. You must now configure the COM port to be used by the terminal emulator.
9. If the successfully updated message does not display, check your computer’s user documentation for help.



Installing the USB Driver - Windows 8.1

IMPORTANT

The following driver installation instructions are for the *Windows 8* operating system only. Installing the USB driver using another operating system is similar, but not necessarily identical to this procedure. The drivers are not required with the IONMM-232.

To install the USB driver on a computer with the *Windows 8* operating system:

1. Press the Windows key and type “startup”. Choose “Change advanced startup options”.
2. On the right side click on the “Restart now” button under Advanced startup.
3. Your PC will reboot and display the “Choose an Option” screen; choose “Troubleshoot”.
4. At the Troubleshoot screen choose “Advanced options”.
5. In the Advanced options screen choose “Startup Settings”.
6. A list of Windows Startup Settings displays; click the “Restart” button. Your PC will reboot.
7. Your PC will boot into a Startup Settings screen. Select “7) Disable driver signature enforcement”.
8. Your PC will reboot one more time and will not load normally.
9. Plug the USB into the PC and IONMM card and have the USB driver saved locally to the PC.
10. The install will fail again; right click on “My computer” and click “Manage” to get to “Device Manager”.
11. In Device Manager, expand “Ports (COM& LPT)” to view your connection with an error on the driver.
12. Right click on the driver and choose “Update driver software”.
13. You will get a pop up with two options; choose “Browse my PC for driver”.
14. Point to the folder location where you have the driver installed and click “install”.
15. You will receive another Windows Security pop up; choose “Install this driver software anyway”.
16. The driver will install correctly, and you will no longer see the error on the connection in Device Manager.
17. You will now be able to connect via USB to the device and log in. On a stand-alone device, be sure to set it to “Remote” so you can remotely manage the device.

Configuring Terminal Emulator

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

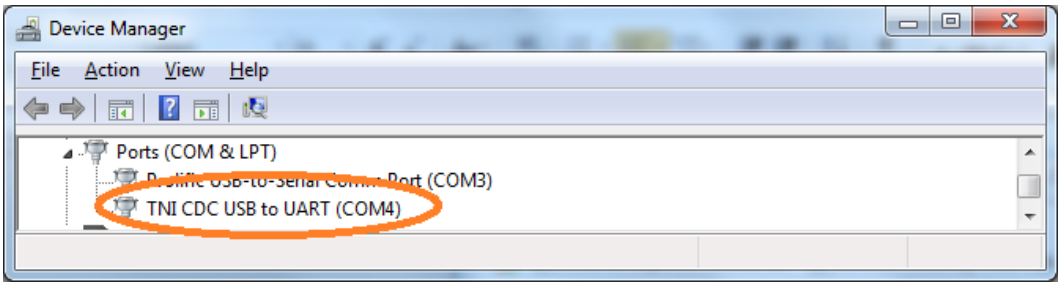
1. Download and install a terminal emulator program such as HyperTerminal or Tera Term.
2. Select the appropriate COM port in the terminal emulator program.
3. Set the console terminal interface to: 115200-8-N-1-N (bps=115200, data bits=8, parity=None, stop bits=1, flow control=None).
4. At the Log In screen, use the keyboard to enter Username root and Password root and hit the Enter key.
5. Login (see "Starting a USB Session" below).

Change COM Port for USB Serial Adapter

This section applies for workstations running Windows 7, 8.1, or 10.

1. Go to the Device Manager.
2. Expand the Ports '(COM& LPT)'
3. If Windows has set the port to something like COM10 you will want to change it. Many legacy applications expect the port to be 1-4.
4. Right click on the device and click on 'Properties'.
5. Click on 'Port Settings'. Then click on 'Advanced…'.
6. Once you're in 'Advanced Settings for COM10' on the bottom you can see the 'COM Port Number: COM10'. Click on that to change it to the lowest possible number (1-4).
7. Click 'OK' on all open Property Windows.

The Device Manager > Ports '(COM& LPT)' should look like this:



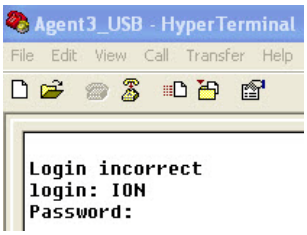
Starting a USB Session

The following procedure describes how to access the IONMM via a USB connection in HyperTerminal.

1. Start the terminal emulator program (e.g., HyperTerminal).
2. After the emulator screen displays, press **Enter**. The login prompt displays. **Note:** if a "Login incorrect" message displays, ignore it.

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

3. Type your login (the default is **ION**). Note that the login is case sensitive (all capital letters).
4. Press **Enter**. The HyperTerminal password prompt displays.
5. Type your password (the default is **private**). Note that the password is case sensitive (all lower case letters).



6. Press **Enter**. The command line prompt displays.

You can now enter commands to set up the various configurations for the IONMM (see "Section 3: Configuration"). For a description of all available CLI commands see the *ION System CLI Reference Manual, 33461*.

Terminating a USB Connection

To terminate the USB, connection, do the following.

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

Cable-CCC-06

Cable-CCC-06 is a blue 6 foot Cisco DB9 to RJ-45 console cable. It is an optional accessory (sold separately).

Access via an Ethernet Network

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

IMPORTANT

It is recommended that you initially set up the IP configuration through the serial interface connection. See Setting Up the IP Configuration section.

Otherwise, to communicate with the IONMM 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 IONMM (see "Appendix A: Factory Default Settings").

Make note of the original settings for the PC as you must reset them after setting the IP configuration for the IONMM.

Starting a Telnet Session

The IONMM can be controlled from a remote management station via a Telnet session over an Ethernet connection. The IONMM is controlled and configured through CLI commands.

Note that Telnet is not secure and can expose data to potential eavesdroppers. Consider using SSH for more secure communications. See "Using SSH" below.

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

For configuration information, see "Section 3: Configuration".

Terminating a Telnet Session

To terminate the Telnet session:

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

Using SSH

Use a terminal emulator (such as TeraTerm) with SSH client functionality to establish an SSH connection with the IONMM system. After opening the SSH connection, use the CLI commands to interact with and configure the device.

Web Browser Support

The ION system supports current versions of most current web browsers (e.g., Mozilla Firefox, Google Chrome, Opera, Safari, Microsoft Edge).

Starting the Web Interface

The IONMM 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 (edited).

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

IMPORTANT

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

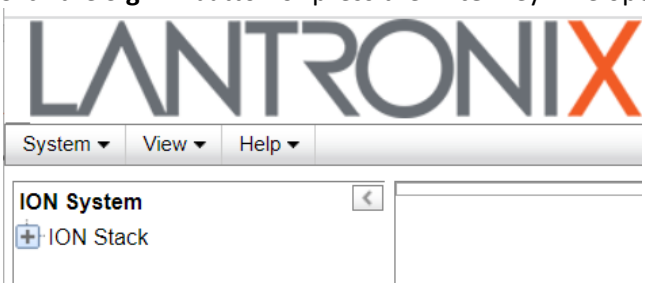
To sign in to the IONMM via the Web:

1. Open a web browser.
2. In the address (URL) block, type the IP address of the NID (the default address is **192.168.0.10**).
3. Click **Go** or press **Enter**. The ION System Sign in screen displays.

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

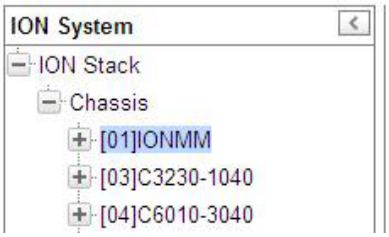
4. Type a User Name of up to 64 characters (the default is **ION**). Note that the User Name is case sensitive (all capital letters).
5. Type the Password (the default is **private**). Note that the Password is case sensitive (all lower case letters).

6. Click the **Sign in** button or press the **Enter** key. The opening screen displays.

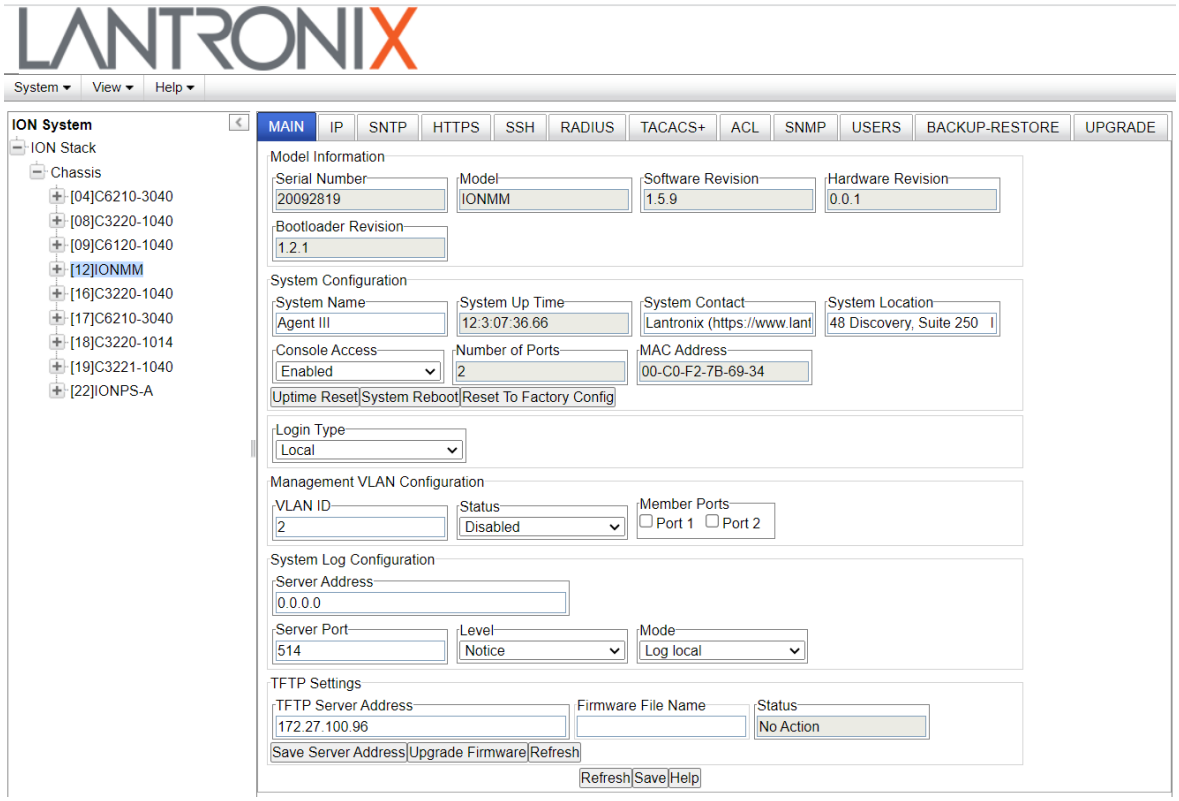


7. Click the plus sign **[+]** next to **ION Stack**. This unfolds "ION Stack" node in the left tree view and will refresh device status.

8. Click the plus sign **[+]** next to **Chassis** to unfold the chassis devices.



9. Click **IONMM**. The IONMM **MAIN** screen displays.



10. You can use the various tabs to configure the IONMM device and ports. For configuration information, see "Section 3: Configuration".

Note that the IONMM **MAIN** screen tabs that display will depend on the user level assigned. Users with read/write privileges do not view the IONMM **UPGRADE** tab or the **BACKUP-RESTORE** tab.

11. Click the plus sign **[+]** next to **IONMM** to unfold the IONMM ports.

Note that the ION system supports up to three levels of device discovery (two remote and one local).

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 is shown while the page loads.

Note: At IONMM v 1.3.19 the left column of the ION Web UI is changed so that if a "stack" has been given a name, that name will be displayed at the top of the tree in the left column, once the stack is selected in the left column. If the "stack" hasn't been given a name, then the default name "ION Stack" will be displayed.

Terminating the Web Interface

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

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

The ION sign in screen displays.

3. Continue with the "Setting Up the IP Configuration" section below.

Setting up the IP Configuration

IPv4 Config Setup

This section describes the procedure for setting a static IPv4 address for the IONMM. When this procedure is completed, you can communicate with the IONMM across the network via either a Telnet session or through the Web interface.

When manually setting the IONMM's IP address, it can only be given a Class A, Class B or Class C address; it cannot be given a multicast or reserved IP address. The multicast addresses, loopback addresses, and link local addresses that can be used in a local network include 10.0.0.0~10.255.255.255, 172.16.0.0~172.31.255.255, and 192.168.0.0~192.168.255.255).

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **set ip type=ipv4 addr**=<xx> **subnet–mask =**<yy> where:

   xx = the IP address of the IONMM

   yy = subnet mask
3. Press **Enter**.
4. Type: **set gateway type=ipv4 addr**=<xx> where:

   xx = default gateway address
5. Press **Enter**.
6. Set the IP Address Mode. Type **set ip address mode**={bootp}dhcp|static} and press **Enter**. The default is **static**.
7. Verify the IP configuration is set. Type: **show ip–mgmt config** and press **Enter**.
8. View the displayed IP configuration and verify that it is set properly. For example:

```
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
------------------------------------------------------------------------
Management State:             disable
Link Local Address:           fe80::2c0:f2ff:fe20:e939
Global Address Mode:          static
Global Address:               ::
Management Prefix:            0
Duplicate Address Detect:     false
Gateway Mode:                 static
Gateway Address:              ::

server index    addr_type    address
```

```
------------------------------------------------------------------------
DNS server1    ipv4        0.0.0.0
DNS server2    ipv4        0.0.0.0
DNS server3    ipv4        0.0.0.0
DNS server4    ipv6        ::
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S1|L1D>
```

IPv6 Config Setup

This section describes the procedure for setting an IPv6 address for the IONMM. When this procedure is completed, you can communicate with the IONMM across the network via either an SSH/ Telnet session or via the Web UI.

1. Set the IPv6 Mode to either static, dhcpv6, or stateless. The default is static.
   If 'Stateless Auto configuration' is selected, then Route Discovery must first be enabled.
   Type **set ipv6 address mode**=<static|dhcpv6|stateless> and press **Enter**.
2. Enable IPv6 Management state. Type **set ipv6-mgmt state=enable** and press **Enter**.
3. Configure the IPv6 gateway method to use. Type **set ipv6 gateway mode**=<static|routerdisc>, where ***static*** = the static method is to be used (the default) and ***routerdisc*** = the dynamic method (Route Discovery) is to be used.
4. Configures the IPv6 method to be used on this device. The default is static.
   If 'Stateless Auto configuration' is selected, then Route Discovery must first be enabled.
   Type **set ipv6 address mode**=<static|dhcpv6|stateless> and press **Enter**.

   For example:

```
Agent III C1|S1|L1D>set ipv6-mgmt state=enable
Agent III C1|S1|L1D>set ip type=ipv6 addr=2001:1234::1 prefix=64
Agent III C1|S1|L1D>set ipv6 gateway mode routerDisc
Agent III C1|S1|L1D>set ipv6 address mode static
```

5. Use the **show ip-mgmt config** command to verify the settings. For example:

```
Agent III C1|S1|L1D>set ipv6-mgmt state=enable
Agent III C1|S1|L1D>set ip type=ipv6 addr=2001:1234::1 prefix=64
Agent III C1|S1|L1D>set ipv6 gateway mode routerDisc
Agent III C1|S1|L1D>set ipv6 address mode static
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
------------------------------------------------------------------------
Management State:             enable
Link Local Address:           fe80::2c0:f2ff:fe20:e939
Global Address Mode:          static
```

```
Global Address:               2001:1234::1
Management Prefix:            64
Duplicate Address Detect:     false
Gateway Mode:                 routerDisc

Dynamic Router Table:
Table1__Destination:          2001:1234::
Table1__PfxLen:               64
Table1__NextHop:              ::
Table1__Age:                  15

Table2__Destination:          fe80::
Table2__PfxLen:               64
Table2__NextHop:              ::
Table2__Age:                  15

Table3__Destination:          ff00::
Table3__PfxLen:               8
Table3__NextHop:              ::
Table3__Age:                  15


server index   addr_type   address
-------------------------------------------------------------------------
DNS server1    ipv4        0.0.0.0
DNS server2    ipv4        0.0.0.0
DNS server3    ipv4        0.0.0.0
DNS server4    ipv6        ::
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S1|L1D>
```

Menu System Description

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

Table 4: IONMM System-Level Menu Description

Tab	Description
MAIN Tab	Sections: Model Information, System Configuration, Login Type, Management VLAN Configuration, System Log Configuration, and TFTP Settings. Buttons: *Uptime Reset* - resets the device's system uptime. *System Reboot* - resets all system states and reinitializes the system. Configuration settings are NOT saved during a System Reboot. *All Counters Reset* - resets all system counters including port counters. *Reset To Factory Config* - resets all system configurations to factory defaults. Wipes out all current configuration details and loads the factory defaults. *Save Server Address* –saves the current TFTP Server Address. *Upgrade Firmware* – starts the firmware upgrade process with the Firmware File Name specified. *Refresh* – restores the previous settings. *Save* – stores the current settings in memory. *Help* – displays context-sensitive online Help information.
IP Tab	Sections: IPv4, IPv6, and DNS Configuration. Buttons: Refresh, Save Help.
SNTP Tab	Sections: SNTP Configuration, Daylight Saving Time (DST) Configuration, and SNTP Servers. Buttons: Refresh, Save Help.
HTTPS Tab	Sections: HTTPS Status, HTTPS Port, and Copy HTTPS Certification functions. Buttons: Copy Certificate, Refresh, Save Help.
SSH Tab	Sections: SSH Server Status, Host Public-Key Settings, and User Public-Key Settings. Buttons: Refresh / Save / Help. Generate / Delete / Refresh. Copy Public Key / Delete / Refresh.
RADIUS Tab	Sections: RADIUS Client and RADIUS Server 1-6 Config. Buttons: Refresh, Save, Help.
TACACS+ Tab	Sections: TACACS+ Client and TACACS Server 1 - TACACS Server 6 sections. Buttons: Refresh, Save, Help.

ACL Tab	Sections: ACL Status, Chain Name / Chain Policy. Rules / Conditions for Rules. Buttons: Refresh / Save / Help. Refresh / Add / Edit / Delete / Help. Add / Edit / Delete.
SNMP Tab*	Sub-tabs: General, Users, Groups, Views, Trap Hosts, Remote Users. Fields: Community String, Access Mode, SNMP V3 Engine ID. Buttons: Add, Delete, Refresh, Save, Help buttons.
USERS Tab*	Fields: User Name, Password, Confirm Password, Level fields. Buttons: Refresh, Add, Edit, Delete, and Help buttons.
SFTP Tab*	Fields: SFTP Status, SFTP Server Address, SFTP Server Port, SFTP User Name, Remote File Location, SFTP Password, Confirm Password Buttons: Refresh, Save, Help, Save Password
BACKUP - RESTORE Tab*	Sub-tabs: Backup and Restore. Fields: TFTP/SFTP Server Address and Status fields. *Backup* - lets you select modules from a list to Back Up (you must download config files after backing up is done). Buttons: Download, Refresh, Back Up, Help. *Restore* - lets you select modules to Restore (you must upload config files before restoring is started). Buttons: Upload, Refresh, Restore, and Help.
UPGRADE Tab*	Sub-tabs: Firmware Database and Firmware Upgrade. *Firmware Database* lets you specify a Firmware File Name to upload, the target TFTP/SFTP Server Address, the upload results, and resulting Firmware Database details. Fields: TFTP/SFTP Server Address, Firmware File Name, Upload Result, and Upload Result Reason fields. Buttons: Upload, Refresh, Help. *Firmware Upgrade* provides two sub-tabs that let you select Target Modules to upgrade and to view upgrade results. Two sub tabs: Targets and Results. Buttons: Upgrade, Refresh, Help.

***** Note that not all tabs are viewable by all user levels. For example, the BACKUP-RESTORE tab and the USERS tab are only available to admin users.

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

Table 5: Port-Level Menu Description

Tab	Description
MAIN tab (Port 1)	Sections: Port Configuration, Auto Negotiation Settings, and Capabilities Advertised. Buttons: *Refresh, Save,* and *Help.*
MAIN tab (Port 2)	Sections: Sections: Port Configuration, Auto Negotiation Settings, and Capabilities Advertised. Buttons: *Refresh, Save,* and *Help.*

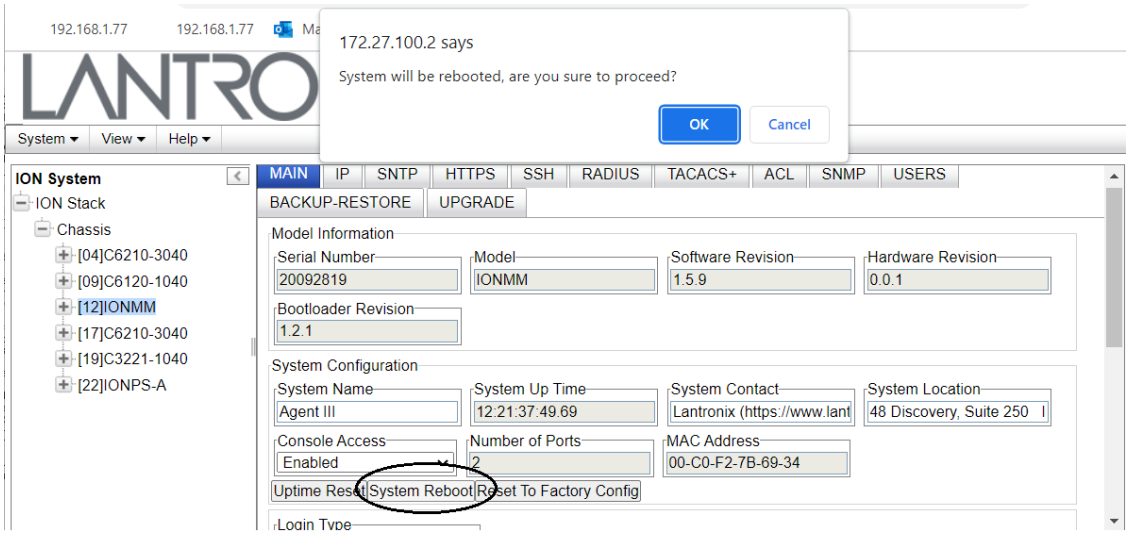
Reboot and Reset Functions

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 its stored files. ***Caution***: These stored files are lost unless you first perform a system Backup. See the "Backup and Restore Operations" section starting 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 " Appendix C: ION System File Content and Location".

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. From the IONMM MAIN tab, click the **System Reboot** button. A confirmation message displays.



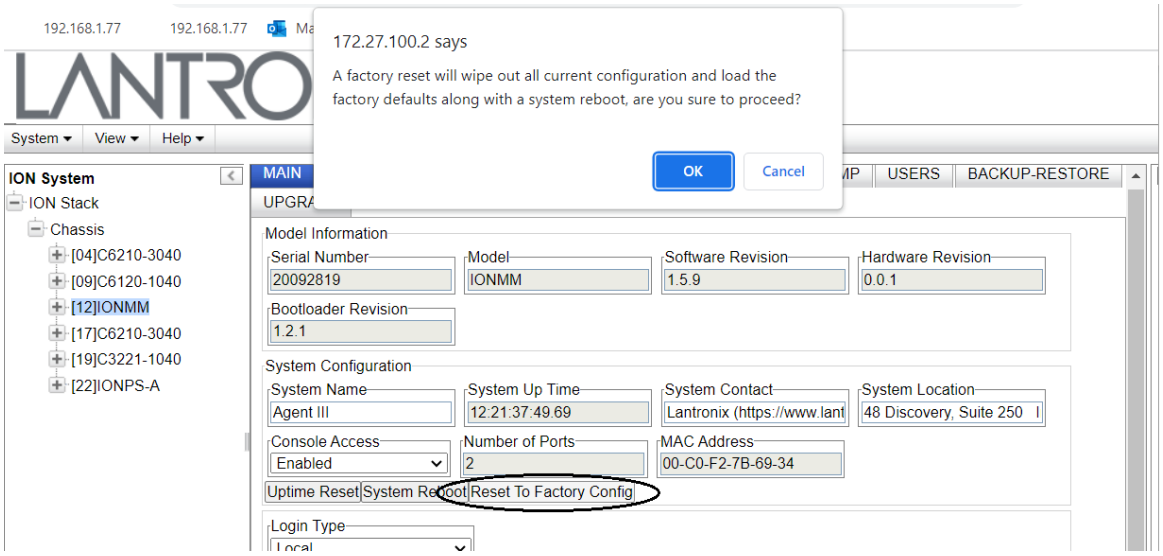
Press the **Cancel** button if you are not sure you want a system reboot to occur.
Press the **OK** button to clear the webpage message and begin the reboot process.

The message "*Loading, please wait...* displays. A System Reboot can take several minutes.
Note: A System Reboot will reset all the system states and reinitialize the system. All existing configuration data is saved during a restart.

Reset to Factory Config

Clicking the **Reset To Factory Config** button resets the entire system configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the system configuration with the factory default settings.

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



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

3. Configuration

General

This section describes how to configure the IONMM.

After the IONMM has been installed and access has been established, it must be configured to operate within your network. Besides the initial system configuration which establishes the IP addressing, the IONMM can also be configured to operate with various security protocols.

Configurations can be done either by entering CLI commands (USB and Telnet) or through a Web interface. For a complete description of all CLI commands, see the related *ION System CLI Reference Manual*.

Setting the IPv4 Configuration

The IP configuration allows the IONMM to communicate across the network with other devices in the network, most notably, a management station. It is this configuration that defines the IP address, IP type, IP mode, default gateway address and subnet mask of the IONMM. Additionally, Domain Name System (DNS) servers can be set up as part of the IP configuration.

The IP address assigned to the IONMM can either be a static (permanent) address entered by you, or a dynamic (temporary) address assigned by a DHCP server.

The IP Address Mode can be BootP, DHCP, or Static IP addressing.

IMPORTANT

It is recommended that you initially set up the IP configuration through the serial interface (USB connection). See "Setting up the IP Configuration".

Otherwise, to communicate with the IONMM 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 IONMM (see "Appendix B: Factory Default Settings").

Make note of the original settings for the PC as you will need to reset them after setting the IP configuration for the IONMM.

The factory default settings are:

IP Address = 192.168.0.10

Subnet Mask =255.255.255.0

Default Gateway addr = 192.168.0.1

IP Type = IPv4

IP Addr = 192.168.0.10

Subnet–mask = 255.255.255.0

IP Address mode = Static

Configuring IPv4 Address Mode

A static IP address is one that is permanently assigned to the IONMM. The static IP address, type, and mode, subnet mask, and default gateway address can be configured in the IONMM using either the CLI or Web method.

IPv4 Addressing Config – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Define the IP address and subnet mask for the IONMM. Type:

   set ip type=ipv4 addr=<xx> **subnet–mask =**<yy>

   where:

   xx = IP address of the IONMM

   yy = subnet mask
3. Press **Enter**.
4. Define the IP address mode (select either **bootp**, **dhcp**, or **static**) and press **Enter**. (If you select **bootp**, the IP address will be assigned per RFC951.)
5. Define the default gateway address. Type: **set gateway type=ipv4 addr=<**xx>

   where:

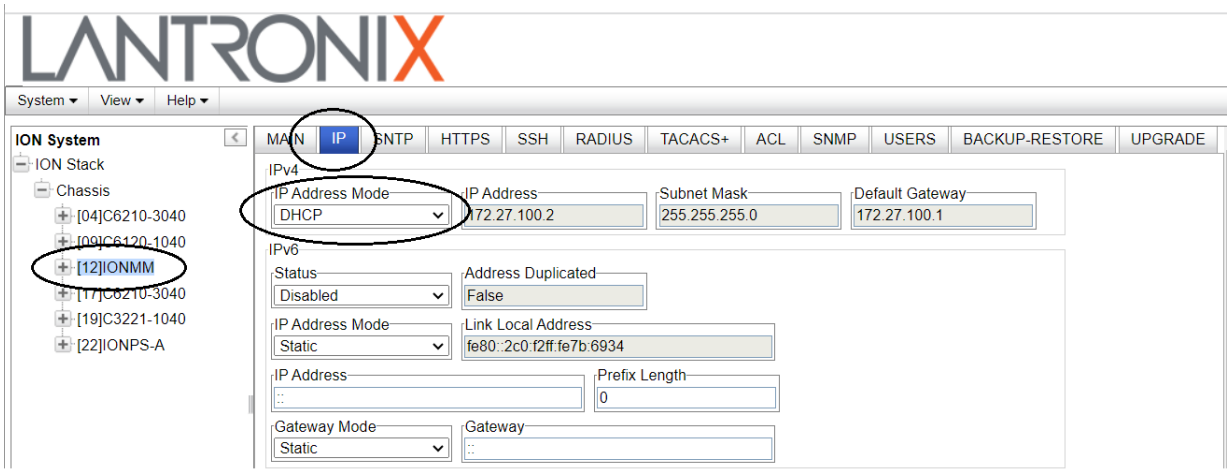
   xx = default gateway address
6. Press **Enter**.
7. Verify the configuration has been set. Type **show ip–mgmt config** and press **Enter**. For example:

```
Agent III C1|S1|L1D>set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0
Agent III C1|S1|L1D>set gateway type=ipv4 addr=192.168.0.1
Agent III C1|S1|L1D>set ip address mode ?
  bootp
  dhcp
  static
Agent III C1|S1|L1D>set ip address mode=static
Agent III C1|S1|L1D>show ip-mgmt config
IP management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

server index             addr_type      address
------------------------------------------------------------------------
DNS server1              ipv4           0.0.0.0
DNS server2              ipv4           0.0.0.0
DNS server3              ipv4           0.0.0.0
DNS server4              ipv4           0.0.0.0
```

```
DNS server5                ipv4            0.0.0.0
DNS server6                ipv4            0.0.0.0
Agent III C1|S1|L1D>set ip
  address
  type
Agent III C1|S1|L1D>set ip address mode
  bootp
  dhcp
  static
Agent III C1|S1|L1D>
```

IPv4 Addressing Config – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **IP** tab if not already displayed.
3. Locate the **IPv4** configuration section.



4. At the **IP Address Mode** dropdown, select **DHCP**, **Static**, or **BootP**. The default is **Static**.
5. Enter the **IP Address**, **Subnet Mask**, and **Default Gateway** address into the appropriate fields.
6. Scroll down and click **Save** when done.

Assigning an IPv4 DHCP Address

A dynamic or temporary IP address can be assigned using a DHCP server. The DHCP server contains a list of IP address that can be used and assigns one when a requesting device wants to communicate. The address is assigned to the device for that session only.

Note:

- A DHCP server must be on the network, configured, and accessible for dynamic IP address assignment via DHCP.
- A Configuration backup does not back up the leased IP address; only the DHCP state is backed up.
- If the DHCP server can't be reached, the DHCP client will try to reach the DHCP server every 30 seconds until it gets a correct response from the DHCP server. Before getting the IP address, an ION device is not manageable via the Web interface. You must log in through CLI and set the DHCP function to 'disable', set an IP address, and then login via the Web interface again.
- If any port changes from link down to link up, the DHCP client will try to renew the IP settings by resending the DHCP request to the DHCP server.

A dynamic IP address can be configured in the IONMM using either the CLI or Web method.

IPv4 DHCP Config – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Set the IP Address mode. Type **set ip address mode**={bootp|dhcp|static} and press **Enter**.
3. Use the **show ip config** command to verify the DHCP configuration. For example:

```
Agent III C1|S1|L1D>set ip type dhcp addr=192.168.30.30 subnet-mask=255.255.255.0
Agent III C1|S1|L1D>set ip address mode=dhcp
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
------------------------------------------------------------------------
Management State:             enable
Link Local Address:           fe80::2c0:f2ff:fe20:e939
Global Address Mode:          static
Global Address:               2001:1234::1
Management Prefix:            64
Duplicate Address Detect:     false
Gateway Mode:                 routerDisc

Dynamic Router Table:
Table1__Destination:          2001:1234::
Table1__PfxLen:               64
Table1__NextHop:              ::
Table1__Age:                  116269
```

```
Table2__Destination:          fe80::
Table2__PfxLen:               64
Table2__NextHop:              ::
Table2__Age:                  30713

Table3__Destination:          ff00::
Table3__PfxLen:               8
Table3__NextHop:              ::
Table3__Age:                  30713


server index   addr_type   address
------------------------------------------------------------------------------
DNS server1    ipv4        0.0.0.0
DNS server2    ipv4        0.0.0.0
DNS server3    ipv4        0.0.0.0
DNS server4    ipv6        ::
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S1|L1D>
```

IPv4 Address Mode (DHCP / Static / BootP) Config – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. At the device's **IP** tab, locate the **IPv4** configuration section.

3. In the **IP Address Mode** field, select **DHCP**. The default is **Static**.
4. Scroll down and click **Save**.

BootP Addressing Configuration

1. Configure IPv4 address mode to "bootp".
2. Connect ION to the BootP server.
3. The BootP options display:
   Option: (t=55,l=9) Parameter Request List
   1=Subnet Mask
   3=Router
   6=Domain Name server
   12=Host Name
   15=Domain Name
   28=Broadcast Address
   40=Network Information Service Domain
   41=Network Information Service Servers
   42=Network Time Protocol Servers
4. For more definition, refer to IETF RFC 951, RFC 2132, etc.

Note that ION does not support some of the displayed BootP options, such as Network Information Service Domain (40), Network Information Service Servers (41), Network Time Protocol Servers (42) or others.

The BootP function is restricted from supporting dynamic getting DNS. Unlike DHCP, the BOOTP protocol does not provide a protocol for recovering dynamically assigned addresses once they are no longer needed. It is still possible to dynamically assign addresses to BOOTP clients, but some administrative process for reclaiming addresses is required.

Defining Domain Name System (DNS) Servers

A Domain Name System (DNS) is a database that correlates names of devices and domains on the network to IP addresses. Every device and domain in a network is assigned an IP address. It is the responsibility of the DNS server to translate the name assigned to a device to the actual IP address of the device. Every domain has a DNS server that handles its requests for translating names to IP addresses.
Up to six DNS servers can be defined using either the CLI or Web method.

DNS Lookups over IPv6 Transport

ION supports two approaches of recursive DNS server address configuration for an IPv6 host: 1) DHCPv6, and 2) static configuration.

The total max number of DNS Server addresses is six; when IPv6 is enabled, the max number is three for each IP style (IPv4 or IPv6). All the network applications will try only three server addresses (e.g., if IPv4 has two or more valid DNS server address (not 0.0.0.0) and IPv6 has one or more DNS server valid address (not ::), the network application will try the first IPv4 DNS server, then the first IPv6 DNS server, and then the second IPv4 DNS server. If IPv4 has only one or less, then the application will try more IPv6.

DNS '3 vs. 3' Rule ('Up to 3' Rule)

Up to six DNS IPv6 services are supported. The ION DNS '3 vs. 3' rule (or "up to 3" rule) is based on two concepts:

1. If the DNS server is 0.0.0.0 or **::**, ION considers it an invalid DNS address; others are considered valid DNS addresses.
2. If the DNS server works, ION consider it an available DNS address, and others are considered 'unavailable' addresses even if they are 'valid' addresses.

ION supports six DNS servers; however, because of some system constraints (e.g., timeout issues) ION utilizes up to three valid DNS addresses to determine if they are available. So there may be at most three valid DNS addresses which cannot be used, though one of them might be valid and available. ION DNS Servers 1, 2, and 3 are reserved for IPv4 only, and DNS Servers 4, 5, and 6 are just for IPv6.

To balance the IPv4 and IPv6, the sequence of DNS Server validity checking is 1, 4, 2, 5, 3, 6 with supporting logic that determines:

1. If the DNS address is invalid, it will be skipped.
2. ION will check up to three valid DNS addresses in the sequence above to find the first available DNS address. When an available DNS address is found, the validity checking process will stop.

DHCPv6 DNS Server Configuration

DHCPv6 includes the "DNS Recursive Name Server" option, through which a host can obtain a list of IP addresses of recursive DNS servers. The DNS Recursive Name Server option carries a list of IPv6 addresses of RDNSes to which the host may send DNS queries. The DNS servers are listed in the order of preference for use by the DNS resolver on the host. The DNS Recursive Name Server option can be carried in any DHCPv6 Reply message, in response to either a Request or an Information request message.

If the IPv6 IP address mode is changed to DHCPv6, the old three IPv6 DNS server addresses will be cleared to the unspecified address (::). When the DHCPv6 reply message comes, the ION system will get

the first three DNS server addresses to be the candidates for up layer application to use. The Save behavior occurs for IPv4 DHCP and Bootp.

Static DNS Server Configuration

You can enter a DNS Server address manually. For IPv4, if IP address mode is static, you must enter the DNS server addresses manually. For IPv6, if IP address mode is static or stateless, you must enter the DNS server address manually.

DNS Config – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **set dns–svr svr=**<xx> **type=**ipv4 or ipv6 **addr=**<zz> where:

   xx = the number (1–6) of the DNS server being defined. Up to six DNS servers can be defined.
   yy = format of the DNS server IP address; select **dns** (domain name address format).
   zz = IP address of the DNS server.
3. Press **Enter**.
4. Repeat Steps 2 and 3 for each server to be defined. For example:

```
Agent III C1|S1|L1D>set dns-svr svr=1 type ipv4 addr=192.168.1.30
Agent III C1|S1|L1D>set dns-svr svr=2 type=type addr=192.168.2.30
Agent III C1|S1|L1D>set dns-svr svr=3 type ipv4 addr=192.168.3.30
```

5. Use the **show ip config** command to verify the DNS configuration. For example:

```
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
------------------------------------------------------------------------
Management State:             enable
Link Local Address:           fe80::2c0:f2ff:fe20:e939
Global Address Mode:          static
Global Address:               2001:1234::1
Management Prefix:            64
Duplicate Address Detect:     false
Gateway Mode:                 routerDisc

Dynamic Router Table:
Table1__Destination:          2001:1234::
Table1__PfxLen:               64
Table1__NextHop:              ::
Table1__Age:                  13539

Table2__Destination:          fe80::
Table2__PfxLen:               64
```

```
Table2__NextHop:              ::
Table2__Age:                  13539

Table3__Destination:          ff00::
Table3__PfxLen:               8
Table3__NextHop:              ::
Table3__Age:                  13539

server index   addr_type   address
------------------------------------------------------------------------
DNS server1    ipv4        0.0.0.0
DNS server2    ipv4        0.0.0.0
DNS server3    ipv4        0.0.0.0
DNS server4    ipv6        ::
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S1|L1D>
```

Example:

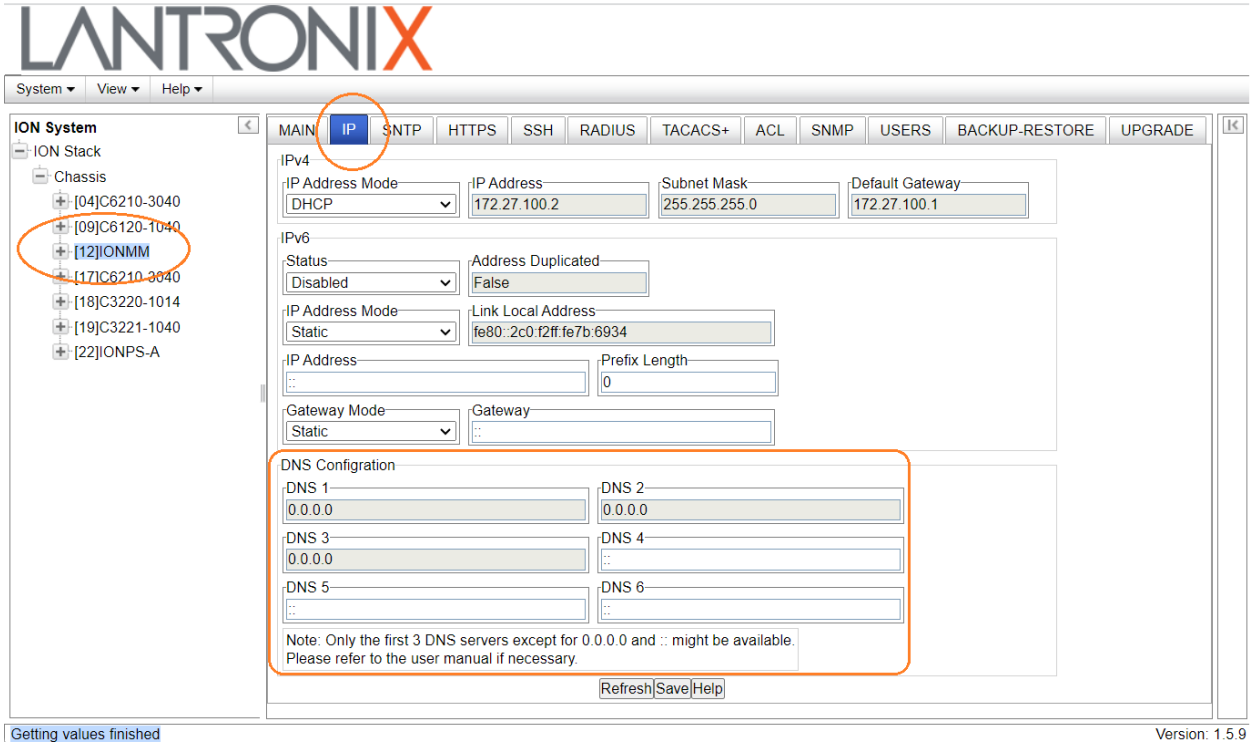
```
Agent III C1|S1|L1D>set dns-svr svr 1 type ipv4 addr 192.168.1.30
Caution: only the first three valid DNS server can be available, please refer to user
menu for the details
Agent III C1|S1|L1D>set dns-svr svr 1 type ipv6 addr 192.168.1.30
server1 to server3 is just used for ipv4!
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
------------------------------------------------------------------
Management State:             enable
Link Local Address:           fe80::2c0:f2ff:fe20:de9e
Global Address Mode:          static
Global Address:               ::
Management Prefix:            64
Duplicate Address Detect:     false
Gateway Mode:                 static
Gateway Address:              fe80::2c0:f2ff:fe21:789a

server index   addr_type   address
------------------------------------------------------------------
DNS server1    ipv4        192.168.1.30
DNS server2    ipv4        192.168.1.40
DNS server3    ipv4        192.168.1.50
DNS server4    ipv6        ::
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S1|L1D>
```

Messages:
warning: server1 to server3 is just used for ipv4!
warning: server4 to server6 is just used for ipv6!

DNS Config – Web Method

The DNS 1 through DNS 6 entries can be in IPv4 or IPv6 format, or both (a combination of up to 3 of each). DNS servers 1-3 are for IPv4; DNS servers 4-6 are for IPv6. See "DNS '3 vs. 3' Rule ('Up to 3' Rule)'.

1. Access the NID via the Web interface (see "Starting the Web Interface").
2. Select the **IP** tab.
3. Locate the **DNS Configuration** section.

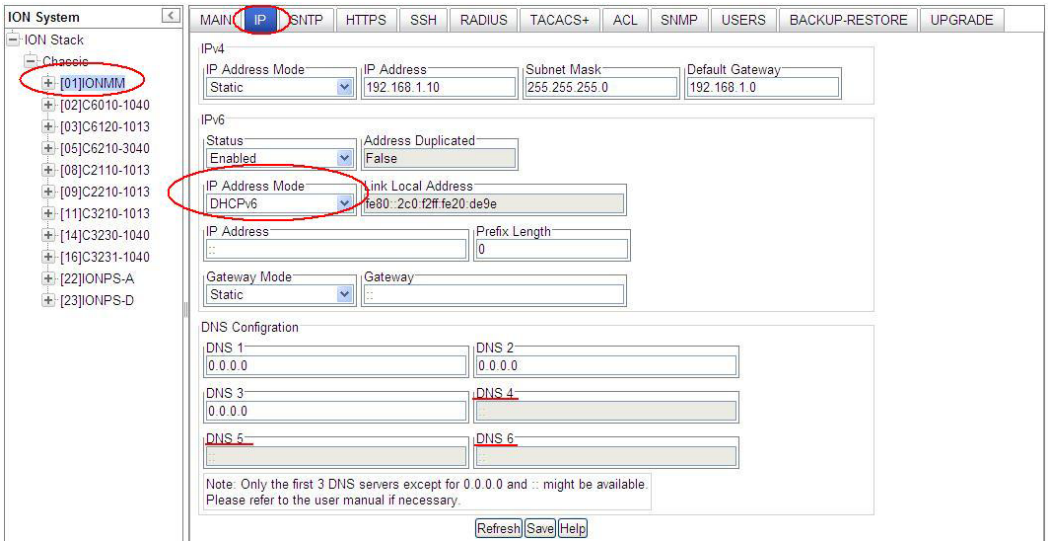


Note: Only the first 3 DNS servers except for 0.0.0.0 and :: might be available.

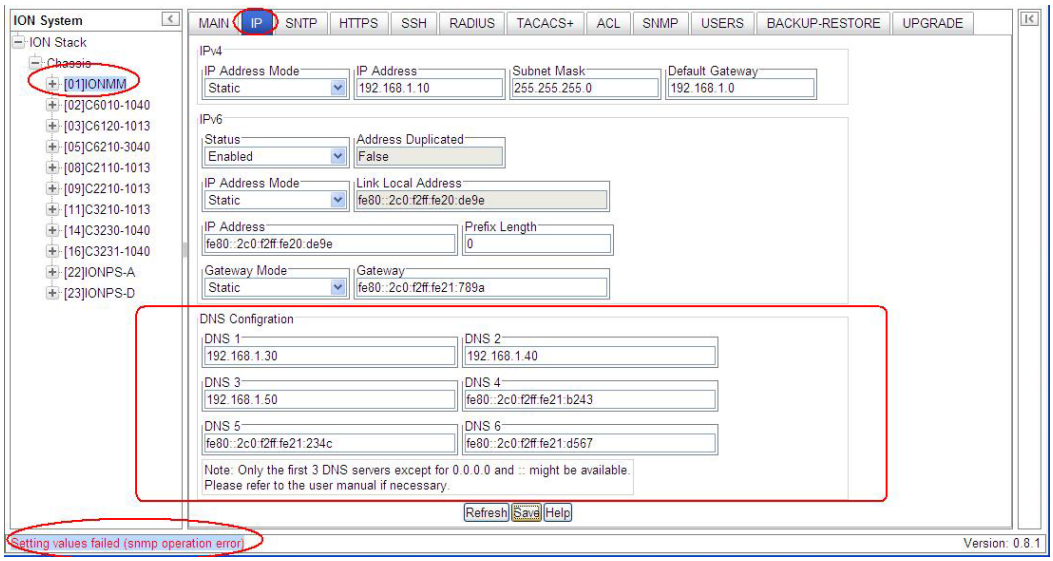
4. In the DNS 1- DNS 3 fields, enter a valid IPv4 IP address (not applicable if DHCP is selected for IPv4 Address Mode).
5. In the DNS 4- DNS 6 fields, enter a valid IPv6 IP address (not applicable if DHCP v6 is selected for IPv6 Address Mode).
6. Scroll down and click **Save** when done.

The **DNS Configuration** with **Static** or **Stateless** selected as the IPv6 Address Mode has DNS 1 - DNS 6 enabled is shown above.

The **DNS Configuration** with **DHCPv6** selected as the IPv6 Address Mode has DNS 4, DNS 5, and DNS 6 disabled (grayed out) is shown below.



The figure below shows an invalid configuration:



See the "DNS '3 vs. 3' Rule ('Up to 3' Rule)" above for more information.

IPv6 Description

IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4). The changes from IPv4 to IPv6 include:

- **Expanded Addressing Capabilities**: IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. A new type of address called an "anycast address" is defined, which is used to send a packet to any one of a group of nodes.
- **Header Format Simplification**: Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.
- **Improved Support for Extensions and Options**: Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- **Flow Labeling Capability**: A new capability is added to enable the labeling of packets belonging to traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.
- **Authentication and Privacy Capabilities**: Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

  Note: The IPv6 version of ICMP is required by all IPv6 implementations.
- **Maximum Packet Lifetime**: Unlike IPv4, IPv6 nodes are not required to enforce maximum packet lifetime. That is the reason the IPv4 "Time to Live" field was renamed "Hop Limit" in IPv6.
- **Fragmenting**: The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination. Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path. To send a packet that is too large to fit in the MTU of the path to its destination, a source node may divide the packet into fragments and send each fragment as a separate packet, to be reassembled at the receiver. For every packet that is to be fragmented, the source node generates an Identification value. The identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address. If a Routing header is present, the Destination Address of concern is that of the destination.

Differences between IPv4 and IPv6

One major difference between IPv4 and IPv6 is the number of available IP addresses. Other differences are shown below.

	IPv4	IPv6
Address size	32-bit number	128-bit number
Address format	Dotted Decimal Notation (e.g., 192.149.252.76)	Hexadecimal Notation (e.g., 2001:0DB8:0004:0015:BE30: 5BFF:FEA2:0B59 192.149.0.0/24 2001:0DB8:0004::/32)
Prefix notation	192.149.0.0/24	2001:0DB8:0004::/32
No. of avail. addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456
Payload	IPv4 limits packets to 64 KB of payload	optional support for “jumbogram” packets - up to 4 GB
TTL / Hop limit	Time-to-Live field	Hop-Limit field
Multicast	Optional, but usually implemented	Part of the base specification in IPv6
QoS support	No standard support	IPv6 has standardized support for QoS

IPv6 Features

The ION system provides the following IPv6 features.

- IPv4/IPv6 Dual Protocol Stack
- IPv6 Routing Protocols
- IPv6 Management
    - IPv6 Address Types, Unicast/Multicast
    - ICMPv6
    - IPv6 Neighbor Discovery protocol
    - IPv6 DAD
    - IPv6 Stateful Auto-configuration with support of DHCPv6
    - IPv6 MTU Path Discovery
    - SNMP over IPv6 Transport
    - DNS Lookups over IPv6 Transport
    - IPv6 ACL
    - IPv6 Mode Applications
        - Telnet, HTTP, Https,
        - TFTP, SNMP, SNTP
        - RADIUS, TACACS+

These features are described in the following sections.

ION IPv6 Function Descriptions

IPv6 Dual Protocol Stacks and Multiple Server Support
The ION software supports IPv4/IPv6 dual protocol stacks, which allows IPv4 and IPv6 to co-exist in the same devices, in the same physical interface, and in the same networks. IPv4 is a basic feature that is always enabled, but the IPv6 is an enhanced feature that you can disable and enable. When IPv6 is disabled, the configurations related to IPv6 will exist but will not function. These configurations can be changed or removed by the user.

The ION software supports multiple DHCP or DHCPv6 or Stateless (Router) servers. In the scenarios below, ION will get one IP addresses (the first one to arrive to ION) and all router information

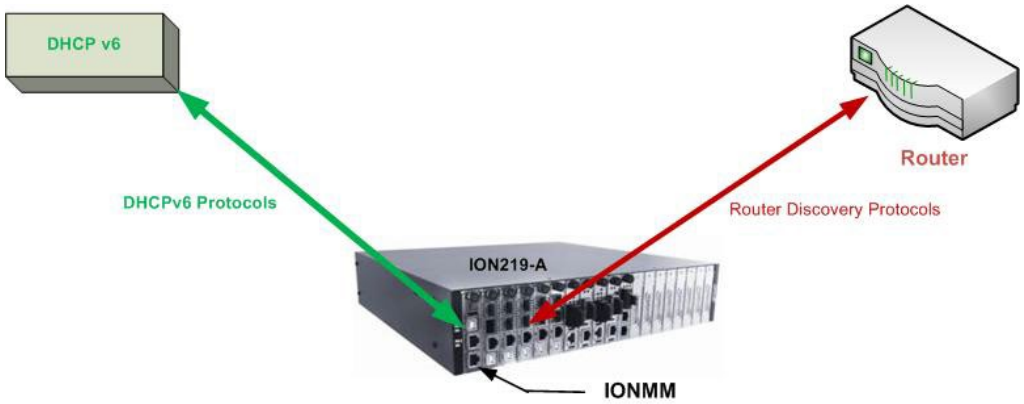


Figure 4 Multiple Routers - One DHCPv6 Router and One Router

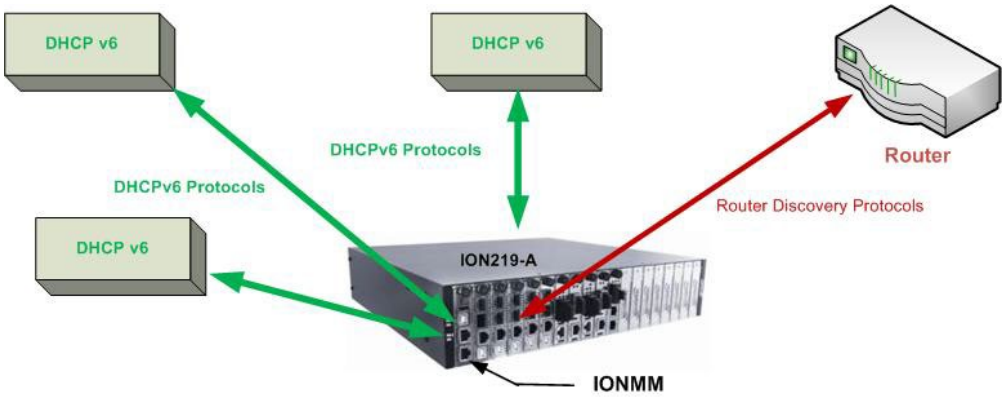


Figure 5 Multiple DHCPv6 Servers and One Router

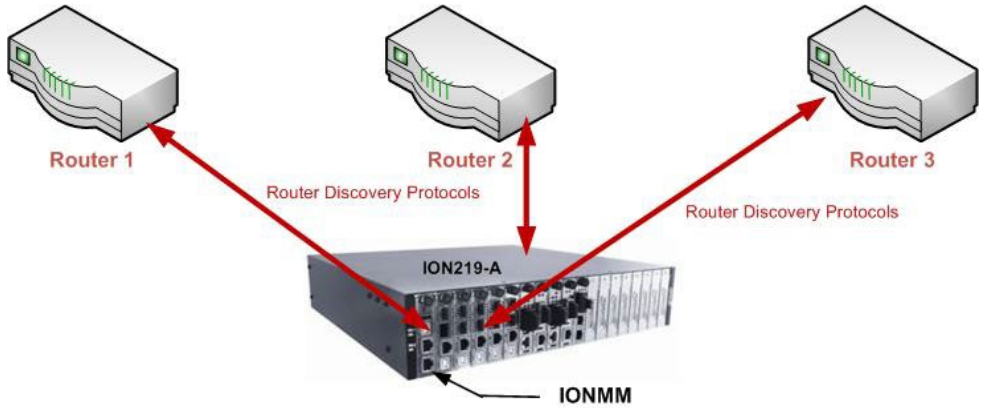


Figure 6 Multiple Routers

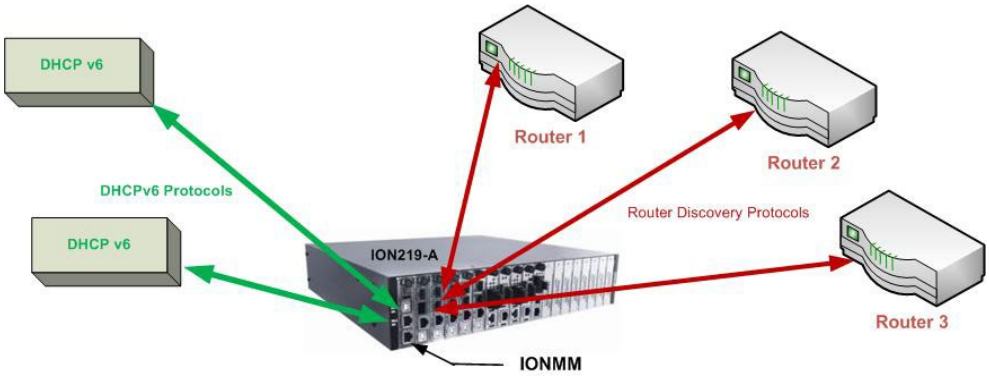


Figure 7 Multiple DHCPv6 Servers and Routers

IPv6 Management Functions

IPv6 Address Formats

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: *x:x:x:x:x:x:x:x*. It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less cumbersome, two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The compressed IPv6 address formats (Unicast and Multicast) are explained below.

IPv6 Unicast Addresses

ION IPv6 Unicast Address support includes:

- Link-local IPv6 address (FE80::/10 + Intf(64))
- Global address (2000::/3 + prefix(45) + Subnet(16) + Intf(64))
- Unique Local IPv6 Unicast Addresses (FC00::/7 + Global ID(40) + Subnet(16) + Intf(64))

Note: ION supports one Link-local IPv6 address which is read-only and one Global Address or Unique Local address. The Link-local address is configured on ION device using the link-local prefix FE80:: /10

(1111 1110 10) and the interface identifier in the modified EUI-64 format. The Global Address or Unique Local address can be configured via the static method, DHCPv6, and stateless auto-configuration. Other IP v6 addresses can be set in ION system by Web/CLI/FP, but only to test in certain situations. ION does not allow Loopback [::1/128] in any address field user can input. Unspecified address [::/128] is used for user to clear current address.)

IPv6 Multicast Addresses

ION IPv6 multicast support includes:

- Solicited-node multicast group (FF02:0:0:0:0:1:FF00::/104)
- All nodes link-local multicast group (FF02::1)
- All routers link-local multicast group (FF02::2)

ION does not support any Multicast Address in any user-editable address field.

ICMP v6 (Internet Control Message Protocol for IPv6)

ICMPv6 provides the same functionality as ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6.

IPv6 Neighbor Discovery Protocol

The Neighbor Discovery protocol is used by nodes on the same link to handle following functions:

- To determine each other's link-local addresses
- To maintain reach-ability information of the paths to active neighbors
- Host Discovery
- Router Discovery
- Prefix Discovery
- Parameter Discovery
- Address Auto-configuration
- Address Resolution
- Duplicate Address Detection

The Neighbor Discovery protocol uses the following messages:

- Neighbor solicitation and advertisement messages
- Router advertisement and solicitation messages

IPv6 DAD (Duplicate Address Detection)

IPv6 DAD is an IPv6 component to check the duplicated address. The function is always enabled on ION. When a new IPv6 address is configured on ION, this device will first check duplicated address on the link. If the S3280 finds the new address has existed on the link, this new address cannot been used. If the IP address is duplicated with another node, the ION Web/CLI will show the DAD attribute if the duplicated address is detected.

IPv6 Auto Configuration per IETF RFC 2462

One important goal for IPv6 is to support node Plug and Play. That is, it should be possible to plug a node into an IPv6 network and have it automatically configured without any human intervention. IETF RFC 2462 defines both a stateful and stateless address autoconfiguration mechanism for IPv6.

IPv6 supports the following types of auto-configuration:

- Stateless auto-configuration
- Stateful auto-configuration

Stateless and stateful autoconfiguration complement each other. For example, a host can use stateless autoconfiguration to configure its own addresses but use stateful autoconfiguration to obtain other information. The site administrator specifies which type of autoconfiguration to use through the setting of appropriate fields in Router Advertisement messages (Discovery). Stateful autoconfiguration for IPv6 is the subject of DHCPv6.

IPv6 addresses are leased to an interface for a fixed (possibly infinite) length of time. Each address has an associated lifetime that indicates how long the address is bound to an interface. When a lifetime expires, the binding (and address) become invalid, and the address may be reassigned to another interface elsewhere on the Internet. To handle the expiration of address bindings gracefully, an address goes through two distinct phases while assigned to an interface. Initially, an address is "preferred", meaning that its use in arbitrary communication is unrestricted. Later, an address becomes "deprecated" in anticipation that its current interface binding will become invalid. While in a deprecated state, the use of an address is discouraged, but not strictly forbidden. New communication (e.g., the opening of a new TCP connection) should use a preferred address when possible. A deprecated address should be used only by applications that have been using it and would have difficulty switching to another address without a service disruption.

To ensure that all configured addresses are likely to be unique on a given link, nodes run a "duplicate address detection" algorithm on addresses before assigning them to an interface. The Duplicate Address Detection algorithm is performed on all addresses, independent of whether they are obtained via stateless or stateful autoconfiguration.

In IPv6, a valid address can be a preferred or deprecated address. A valid address may appear as the source or destination address of a packet, and the internet routing system is expected to deliver packets sent to a valid address to their intended recipients.

The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. The '::' symbol can also represent a valid IPv4 address (e.g., '::192.1.2.34').

In IPv6, routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. In the absence of routers, a host can only generate link-local addresses. However, link-local addresses are sufficient for allowing communication among nodes attached to the same link.

Routers generate periodic Router Advertisements that include options listing the set of active prefixes on a link. A ‘Lease lifetime’ provides the mechanism through which a site phases out old prefixes. The system administrator must set appropriate prefix lifetimes to minimize the impact of failed communication when renumbering takes place. The deprecation period should be long enough that most, if not all, communications are using the new address at the time an address becomes invalid.

IPv6 Stateless Auto-configuration

The ION software implements the stateless auto-configuration feature of IPv6 which is used to automatically configure ION device. The new and globally assigned unique IPv6 addresses are associated with the ION device. A router on a local link periodically sends router advertisement messages with 64-bit prefix

of the link and the default route to all hosts on the link. When an ION device on the link receives the message, it takes the link prefix from the message and appends a 64-bit interface ID (link-layer address from MAC address in EUI-64 format) to automatically compose its IPv6 local-link address. The Duplicate Address Detection (DAD) logic of IPv6 stateless auto-configuration verifies the uniqueness of the assigned unicast address. It uses neighbor solicitation messages to verify the uniqueness of a unicast IPv6 address. A station might fail the IPv6 stateless auto-configuration process when the router is not presented on the same link, or its DAD cycle is failed. The Stateless Auto-configuration feature is enabled by default. DNS server address list is not supported in Stateless Auto-configuration.

Stateless autoconfiguration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. In the absence of routers, a host can only generate link-local addresses. However, link-local addresses are sufficient for allowing communication among nodes attached to the same link.
Stateless auto-configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address.
The stateless approach is used when a site is not particularly concerned with the exact addresses hosts use, so long as they are unique and properly routable. Stateless auto-configuration is suitable for small organizations and individuals. In this case, each host determines its addresses from the contents of received router advertisements. Using the IEEE EUI-64 standard to define the network ID portion of the address, it is reasonable to assume the uniqueness of the host address on the link.

IPv6 Stateful Auto-configuration with DHCPv6 Support

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. ION only supports IPv6 address, prefix, and DNS address allocation in DHCPv6.

Stateful autoconfiguration has hosts obtain interface addresses and/or configuration information and parameters from a server. Servers maintain a database that keeps track of which addresses have been assigned to which hosts. The stateful autoconfiguration protocol allows hosts to obtain addresses, other configuration information or both from a server. Stateful auto-configuration requires a certain level of human intervention because it needs a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server for the installation and administration of the nodes. The DHCPv6 server keeps a list of nodes to which it supplies configuration information. It also maintains state information so the server knows how long each address is in use, and when it might be available for reassignment.
The stateful approach is used when a site requires tighter control over exact address assignments. Both stateful and stateless address autoconfiguration may be used simultaneously.
Stateful auto-configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator.

IPv6 Static Configuration

As in IPv4, the host address can be statically defined in the case where the IPv6 address, mask, and the gateway address are all manually defined on the host. Using static configuration causes all of the Auto-configuration features provided by IPv6 to be lost.
When IPv6 mode is switched from DHCPv6 and Stateless to static, all IPv6 address and prefix and IPv6 DNS values will be set back to the default value of all zero. When IPv4 mode is switched from DHCP/BootP to static, IP address and Mask and Gateway and DNS values will be set back to default values (192.168.0.10 and 255.255.255.0 and 192.168.0.1 and all zeros).
When IPv6 mode is switched from DHCP to Static, the IPv6 address and DNS will be set to "::" by the web interface, and IPv4 will be set to the default of 192.168.0.10 and DNS will be set to 0.0.0.0.

The ION system behavior when switching IP modes is summarized below:

1. When you switch IPv6 address mode from DHCPv6 to Static, this configuration will be set to default:
   a. IPv6 address (::)
   b. IPv6 prefix (0)
   c. IPv6 DNS (::)
2. When switch IPv6 address mode from Stateless to static, this configuration will be set to default:
   a. IPv6 address (::)
   b. IPv6 prefix (0)
3. When switch IP address mode from DHCP to static or from static to DHCP, this configuration will be set to default:
   a. IP address (192.168.0.10)
   b. Network Mask (255.255.255.0)
   c. Gateway (192.168.0.1)
   d. DNS (0.0.0.0)

IPv6 MTU (Maximum Transmission Unit) Path Discovery

Per RFC 1981 - Path MTU Discovery for IPv6, Path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, however, fragmentation is handled by the source of a packet when the path MTU of one link along a given data path is not large enough to accommodate the size of the packets. Having IPv6 hosts handle packet fragmentation saves IPv6 router processing resources and helps IPv6 networks run more efficiently. ION does not allow changes to the default MTU value of 1500.

IPv6 Route

ION forwards packets using route information that is either manually configured or dynamically learned using a routing protocol. But the manual configuration and dynamical protocol can’t work together. The IPv6 route options are:

- Default gateway (manually configured), or
- A simple routing protocol (Stateless auto-configuration).

ION IPv6 Configuration Considerations

This section provides IPv6 configuration prerequisites and restrictions. For the latest feature information and caveats, see the release notes for your device and software release. The prerequisites and restrictions below apply to all ION models unless otherwise noted.

1. An ION NID is a L2 device, which is deployed at access edge. The IP stack only provides Management for the NID cards. As such, the following features are not implemented in ION: IPv6 Anycast, MLD v1/v2, MLD v1/v2 snooping.
2. ION supports one Link-local IPv6 address which is read-only, and one global address. The Link-local address is configured on an ION device using the link-local prefix FE80:: /10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. The aggregatable global address can be configured using the static method, DHCPv6, and stateless auto-configuration.
3. DNS address cannot be saved when you change mode from DHCPv6 to Static (i.e., when changing from DHCPv6 to Static, only the IPv6 address can be saved).
4. Windows XP has very limited IPv6 support which has been found to be unstable when interoperating with an ION IPv6 system. Windows Vista or above and the latest Linux are recommend for customer use with ION IPv6 systems.
5. The ION Web/CLI/FP interfaces use common MIB operation to get/set configurations, while the IONMM uses the AgentX protocol to communication with the SIC cards. This mechanism can cause the specific failure reason of set operation in device can't get back to the UI. The TDM card port loopback setting displays as failed, because either the other port is already in loopback mode or an internal error occurred.
6. In ION products, only these input string fields can support internal space character entry:
    a. System Contact
    b. System Location
    c. Circuit ID
    d. the filename used for backup-restore.
7. The ION Web/CLI/ supports these characters:
    a. Web/FP/CLI only supports ASCII printable characters. Specifically, characters combination which can pass the test of this Regex is supported: /^[a-zA-Z\d`~!@#$%^&*(){}[\];:'",.<>\-_=+\\|\/?]*$/. This Regex allows "space". (Where "Regex" is a regular expression - a sequence of characters with specific meanings, e.g., in Perl, other flavors vary).
    b. Some MIBs do not support the "space" character as a valid entry.
8. When you try to run CLI commands by executing a script or pasting strings, some commands need a 'sleep' period between them; otherwise, these commands cannot be executed successfully:
    a. Add vlan-db.
    b. Add fwddb

    After adding a VLAN or FWDDB by script, add a 3 second sleep in the script before adding another VLAN or FWDDB.
9. The SOAM MD name cannot be modified once created.
10. The maximum number of ION System Users is 64.

IPv4 and IPv6 Initialization Defaults

The IPv4/IPv6 factory default configuration settings are:

- IPv4: Enable
- IP address: 192.168.0.10
- Default Gateway: 192.168.0.1

The IPv6 default configuration includes:

- Link-Local IP address: FE80::/10 (1111 1110 10)
- IPv6: Disabled

IPv6 can be configured in the ION system using either the CLI or Web method.

IP Address Mode Notes

1. When you switch IPv6 address mode from DHCPv6 to Static, the defaults become:
    a. IPv6 address (::)
    b. IPv6 prefix (0)
    c. IPv6 DNS (::)
2. When you switch IPv6 address mode from Stateless to static, the defaults become:
    a. IPv6 address (::)
    b. IPv6 prefix (0)
3. When you switch IP address mode from DHCP to static or from static to DHCP, the defaults become:
    a. IP address (192.168.0.10)
    b. Network Mask (255.255.255.0)
    c. Gateway (192.168.0.1)
    d. DNS (0.0.0.0)
4. ION will check link up / link down every 3 seconds, so a link down and then a very quick link up (less than three seconds) will not trigger a DHCPv6 confirm message.

Telnet IPv4 and IPv6 Connections

The ION Telnet server supports both IPv4 connections and IPv6 connections at the same time. A user can establish a Telnet session directly to the ION device using an IPv6 Telnet client. A VTY (Virtual Type Terminal) interface and password must be created to enable Telnet access to an IPv6 device.
The ION system supports up to 16 Telnet sessions.

TFTP IPv4 and IPv6 Connections

TFTP is a simple protocol used to transfer files. A TFTP client needs the IP address entered in one action. The TFTP server can be an IPv4 address, an IPv6 address or a DNS name, but only the latest TFTP IP address or DNS name can be saved. If IPv6 is disabled and the TFTP server address is an IPv6 address, the server cannot be used. In this case you must change the TFTP server either to an IPv4 address or a DNS name.

IPv6 Address Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Check the current IP addressing configuration. Type **show ipv6 interface** and press **Enter**.
3. Define the IPv6 Gateway Mode. Type **set ipv6 gateway mode**=<routerDisc|static> and press **Enter**.
4. Define the IPv6 Address. Type **set ip type**=TYPE **addr**=ipaddr-type (subnet-mask|prefix)=A and press **Enter**.
5. Verify the IP configuration. Type **show ip-mgmt config** and press **Enter**. For example:

```
Agent III C1|S1|L1D>set ipv6 address mode ?
  dhcpv6
  stateless
  static
Agent III C1|S1|L1D>set ipv6 address mode=static
Agent III C1|S1|L1D>set ipv6 gateway mode=<routerDisc|static>
Agent III C1|S1|L1D>set ip type=TYPE addr=ipaddr-type (subnet-mask|prefix)=A
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
------------------------------------------------------------------------
Management State:             disable
Link Local Address:           fe80::2c0:f2ff:fe20:de9e
Global Address Mode:          dhcpv6
Global Address:               ::
Management Prefix:            0
Duplicate Address Detect:     false
Gateway Mode:                 routerDisc

Dynamic Router Table:

server index   addr_type   address
------------------------------------------------------------------------
DNS server1    ipv4        0.0.0.0
DNS server2    ipv4        0.0.0.0
DNS server3    ipv4        0.0.0.0
DNS server4    ipv6        ::
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S1|L1D>
```

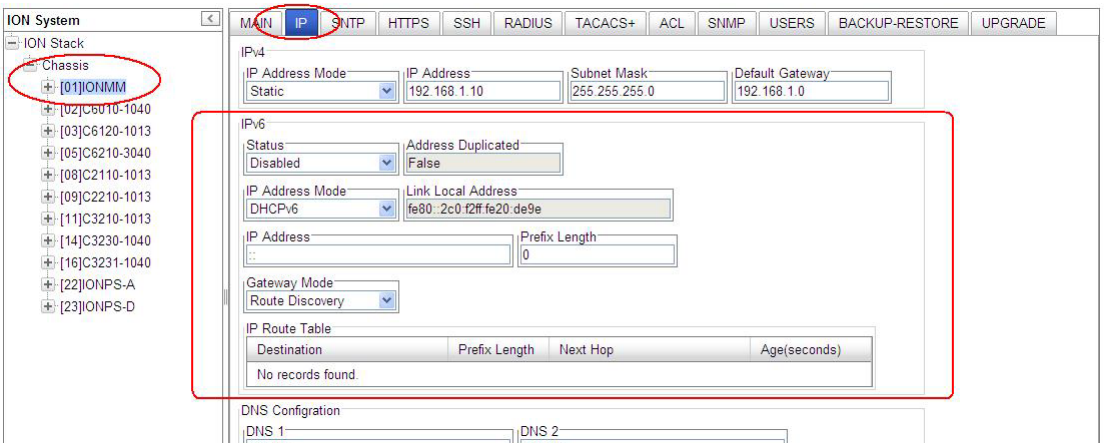
Note: the command "set dhcp state" is replaced by "set ip address mode" after ION v 1.2.0.

Example:

```
C1|S13|L0D/>set ip type=ipv4 addr=192.168.0.3 subnet-mask=255.255.255.0
C1|S13|L0D/>set ip type=ipv6 addr=2001:1234::1 prefix=64
```

IPv6 Address Config – Web Method

1. Access the NID via the Web interface (see "Starting the Web Interface").
2. Select the **IP** tab.
3. Locate the **IPv6** section.



4. At the IPv6 **Status** dropdown, select **Enabled**. The default is **Disabled**. When enabled, the IP Route Table populates after a **Save**.
5. In the **Address Duplicated** field, verify False or True is displayed. The default is False (read-only field). Note that it will take up to three seconds for the **Address Duplicated** field to display TRUE when a new address is being verified. This field displays the status of IPv6 address for the device, where:

   True: duplicate address detected.

   False: no duplicate address detected.
6. At the **IP Address Mode** dropdown, select **Static**, **DHCPv6**, or **Stateless**, where:

   Static: selects static IPv6 addressing.

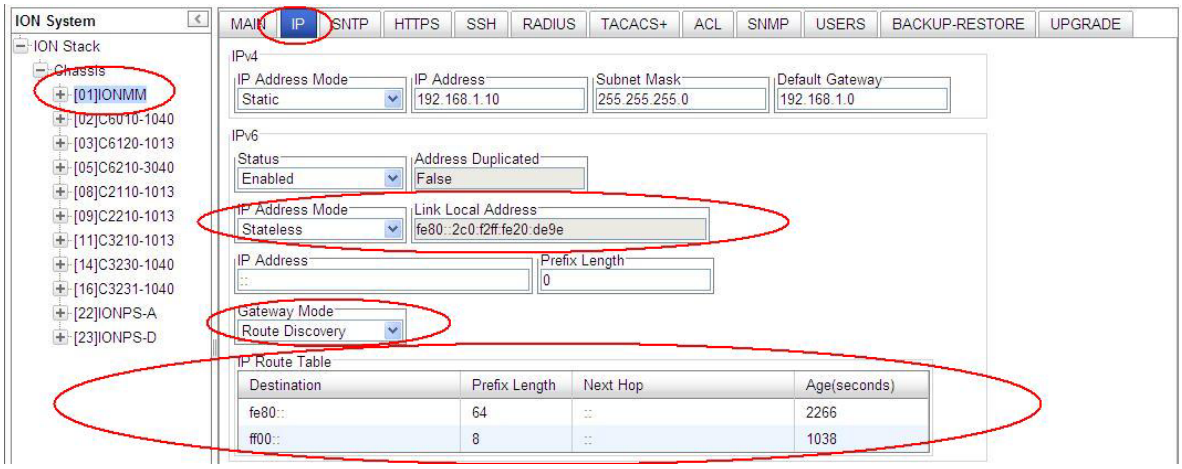
   DHCPv6: selects DHCP v6 addressing and disables (grays out) the DNS 4 -DNS 6 fields.

   Stateless: selects IPv6 stateless addressing.
7. In the **Link Local Address** field, verify the displayed address (e.g., fe80::2c0:f2ff:fe20:de9e).
8. In the **IP Address** field, enter a valid IPv6 address to be used (e.g., fe80::2c0:f2ff:fe21:b243).
9. In the **Prefix Length** field enter a value of 0-127 as the IPv6 prefix length.
10. At the **Gateway Mode** dropdown, select **Static** or **Route Discovery**, where:

    Static: selects Static gateway operation, displays the **Gateway** entry field, and hides the IP Route Table. In the **Gateway** field, enter a valid IPv6 address.

    Route Discovery: selects route discovery operation, displays the **IP Route Table** entry field, and hides the **Gateway** field. Verify the **IP Route Table** in terms of Destination, Prefix Length, Next Hop, and Age time. The IPv6 Address and Gateway should be on the same sub-net.

11. Verify the **IP Route Table** settings. For example:

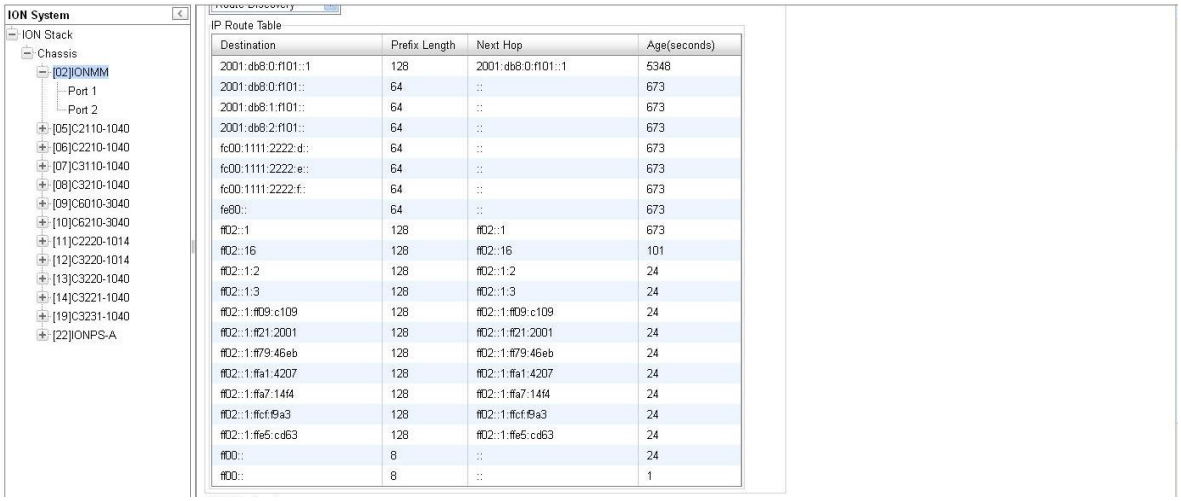


The screen above shows an **IONMM** > **IP** tab with **IP Addr Mode** = **Stateless** and **Gateway Mode** = **Route Discovery**. The IP Route table holds a maximum of 16 entries.

IP Route Table Parameters

The table contains an entity's IPv6 dynamic routing information. Each entry is a particular route to a particular destination. This table is specifically for the result of route discovery which is needed for stateless auto-configuration feature. The Destination column is for the routing target network, and the Next Hop column is for the router (gateway). The Static gateway address is one specific default entry of the routing table. The Static gateway address must be in the same sub-network of current IPv6 address, otherwise, an error will return when this static gateway address is assigned.

For “Route Discovery”, ION will ignore the routing information from a different sub-network. If the current IPv6 address was changed by the static assignment or DHCPv6, etc. to a different sub-network of current routing/gateway address, the current routing/gateway becomes invalid.



The IP Route Table displays each IP route's Destination, Prefix Length, Next Hop, and Age time, where:

Destination: The destination IP address of this route (i.e., a valid IPv6 address).
Prefix Length: The number of leading one bits that form the mask to be logical-ANDed with the destination address before being compared to the value in the ipv6DynRouteDest field (e.g., 8, or 64, etc.) The valid range is 0 - 127.
Next Hop: On remote routes, the address of the next system en route. For non-remote routes, a zero length string.
Age: The number of seconds since this route was last updated or otherwise determined to be correct.
Note that no semantics of 'too old' can be implied, except through knowledge of the routing protocol by which the route was learned.

Changes to Existing ION Applications with IPv4 / IPv6

The existing ION management applications below support both IPv4 and IPv6 environments at the same time. These applications support IPv6 and follow the new socket interface extension described in IETF RFC 2553, 3493, and 3542.

- Telnet, Telnets
- HTTP, HTTPs
- SSHv2
- TFTP
- SNMP
- SNTP
- DNS
- RADIUS
- TACACS+

Dynamic Table Entry Limits

Theses IPv6 changes bring the entry limitations for several dynamic tables shown below.

No.	Module Name	Table Name	Maximum Entries
1	ACL	iptableRulesTable	64
2		iptableConditionsTable	128
3	ACL for IPv6 tables	ip6tablesRulesTable	64
4		ip6tablesConditionsTable	128
5	FDB	ionFIDDbTable	255 static and 255 dynamic
6	VLAN	ionVLANDbTable	255
7	SNMPv3 local / remote users	usmUserTable	64
8	SNMP Groups	vacmAccessTable	64
9	SNMP views	vacmViewTreeFamilyTable	64
10	SNMP communities	snmpCommunityTable	16
11	SNMP trap host		6
12	System user	lonDevSysUserTable	64

System Configuration

The system configuration defines:

- a name for the IONMM, contact and location information, and
- whether the Console (serial interface / USB connection) is enabled.

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.

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.

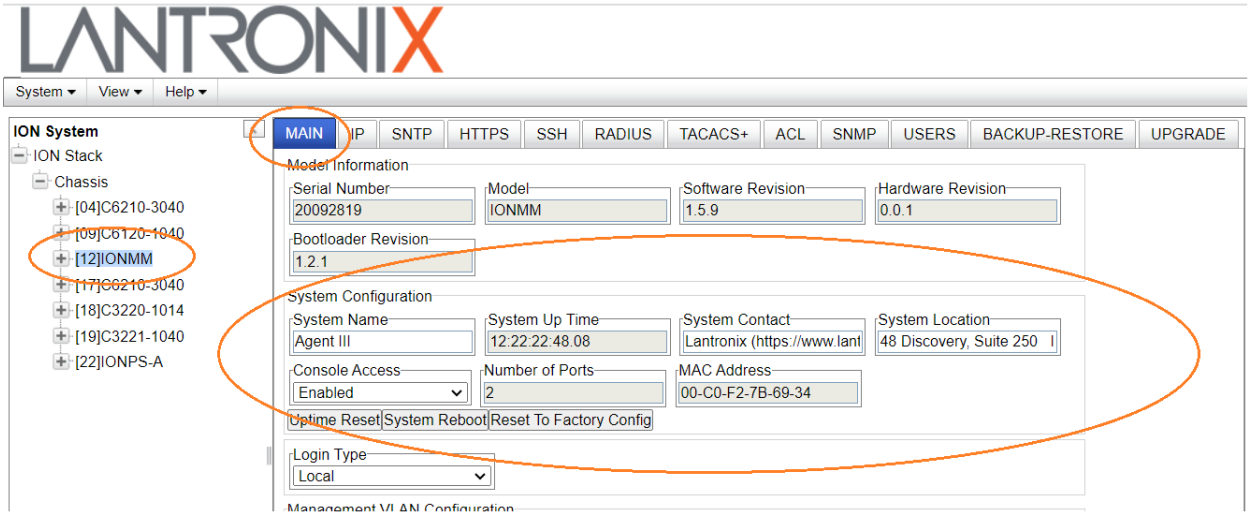
1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the command prompt type **set system contact=**CONTACT, where CONTACT is the new contact (e.g., person, department name), and press **Enter**.
3. Type **set system location=**LOC, where LOC is the new location description (e.g., division, address, etc.) and press **Enter**.
4. Type **set system name**=NAME, where NAME is the new system name, and press **Enter**.
5. Verify the new system Configuration. Type **show system info** and press **Enter**. For example:

```
Agent III C1|S1|L1D>set system ?
  contact
  location
  name
Agent III C1|S1|L1D>set system contact=support
Agent III C1|S1|L1D>set system name=mgmt_module2
mgmt_module2 C1|S1|L1D>set system location=headquarters
mgmt_module2 C1|S1|L1D>show system info
system descr:                 The management module of the Lantronix ION
                 (Chassis Generation III) platform products
system objectID:       1.3.6.1.4.1.868.2.5.544108393
system uptime:                06:22:07
system contact:        support
system name:                  mgmt_module2
system location:       headquarters
mgmt_module2 C1|S1|L1D>
```

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

System Configuration – Web Method

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



4. In the **System Name** field, enter the name for the IONMM device. The name can be alphabetic, numeric or a combination.
5. In the **System Contact** field, enter the name and information of the person to contact if there is a problem with the system. The name and information can be alphabetic, numeric or a combination.
6. In the **System Location** field, enter the information describing the physical location of where the system is located (e.g., room 110, IT, lab, etc.). The information can be alphabetic, numeric or a combination.
7. In the **Console Access** field, select:
   - **Enabled** – allows communications through the USB serial interface (usually to a PC for entering CLI commands).
   - **Disabled** – communications through the USB serial interface is not allowed (CLI commands can only be entered through an SSH or Telnet session).
8. Scroll to the bottom and click **Save**.

Login Type Configuration (Local / RADIUS / TACACS+)

The MAIN tab and/or CLI commands let you define the ION user login method in terms of local, RADIUS, and/or TACACS+ capability.

You can configure the ION user login method via either the CLI or Web method. See the "ION IPv6 Configuration Considerations" section.

Login Type Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Check the current Login Type configuration. Type **show tacplus config** and press **Enter**.
3. Set the desired login method. If more than just "local" login is required, sets the login sequence (order of login validation). Type **set login method**=type, where:
   type = (local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal), and:

   local = the ION software will validate the local login only.

   radiuslocal = the ION software will validate the RADIUS login and then the local login.

   radiustacpluslocal = the ION software will validate the RADIUS login, then the TACACS+ login, and then the local login.

   tacpluslocal = the ION software will validate the TACACS+ login and then the local login.

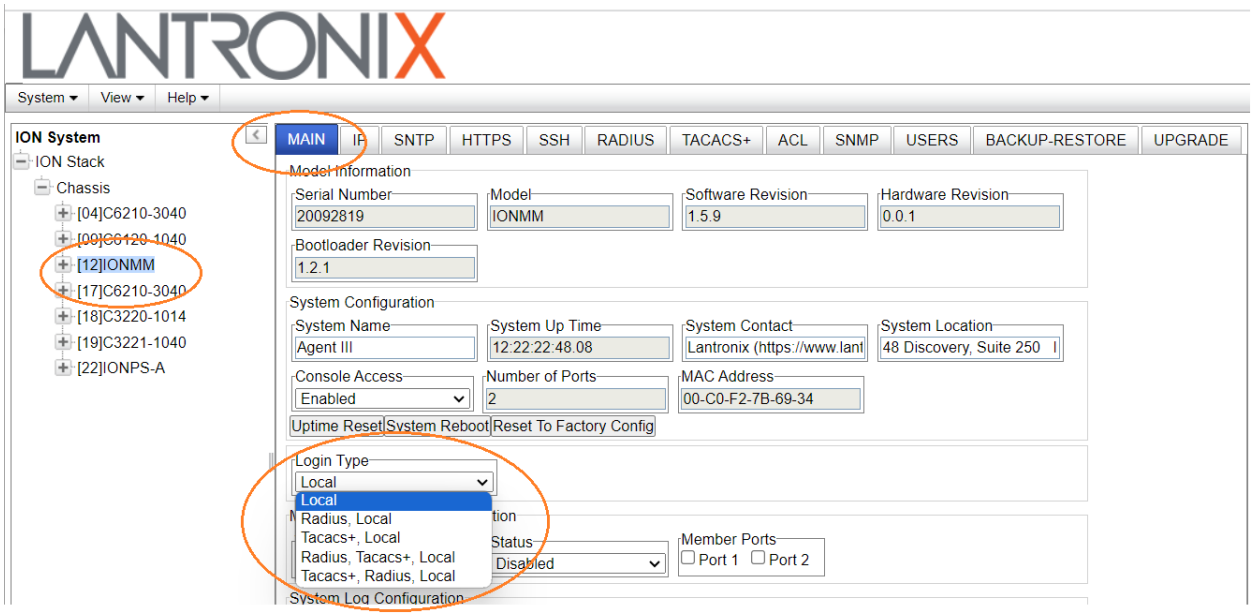
   tacplusradiuslocal = the ION software will validate the TACACS+ login, then the RADIUS login, and then the local login.
4. Verify the TACACS+ and/or RADIUS configuration. For example:

```
Agent III C1|S1|L1D>set login method ?
  local
  radiuslocal
  radiustacpluslocal
  tacpluslocal
  tacplusradiuslocal
Agent III C1|S1|L1D>show tacplus config
TACPLUS client state:         enable

 TACPLUS authentication server:
index   type    addr                                                retry  timeout
-------------------------------------------------------------------------------
1       ipv4    192.168.1.30                                        2      25
2       ipv6    fe80::2c0:f2ff:fe21:b24c                            3      10
3       dns     0.0.0.0                                             3      30
4       dns     0.0.0.0                                             3      30
5       dns     0.0.0.0                                             3      30
6       dns     0.0.0.0                                             3      30
```

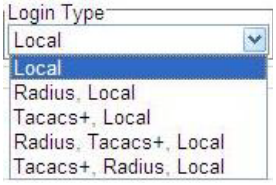
```
Agent III C1|S1|L1P1>set tacplus ?
  client
  svr
Agent III C1|S1|L1P1>set tacplus client state ?
  disable
  enable
Agent III C1|S1|L1P1>set tacplus svr 1 ?
  retry
  secret
  timeout
  type
Agent III C1|S1|L1D>set tacplus svr 1 retry 3
Agent III C1|S1|L1D>set tacplus svr 1 secret Buffrey1
Agent III C1|S1|L1D>set tacplus svr 1 timeout 20
Agent III C1|S1|L1D>set tacplus svr 1 type ?
  ipv4
  ipv6
  dns
Agent III C1|S1|L1D>set tacplus svr 1 type ipv6 addr fe80::2c0:f2ff:fe20:de9e
Agent III C1|S1|L1D>show tacplus config
TACPLUS client state:         enable

 TACPLUS authentication server:
index   type    addr                                                    retry  timeout
-------------------------------------------------------------------------------------
1       ipv6    fe80::2c0:f2ff:fe20:de9e                                3      20
2       ipv6    fe80::2c0:f2ff:fe21:b24c                                3      10
3       dns     0.0.0.0                                                 3      30
4       dns     0.0.0.0                                                 3      30
5       dns     0.0.0.0                                                 3      30
6       dns     0.0.0.0                                                 3      30
Agent III C1|S1|L1D>
```

Login Type Config – Web Method

1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").



2. At the **Login Type** dropdown, select the required level of login; the selections are:
Local: only local logins supported (the default - no RADIUS or TACACS+ configured).
Radius, Local: the ION software will validate the RADIUS login and then the local login.
Tacacs+, Local: the ION software will validate the TACACS+ login and then the local login.
Radius, Tacacs+, Local: the ION software will validate the RADIUS login, then the TACACS+ login, and then the local login.
Tacacs+, Radius, Local: the ION software will validate the TACACS+ login, then the RADIUS login, and then the local login.



   If more than just "local" login is required, select the login sequence (order of login validation).

3. Verify your selection and continue configuration.

Ports Configuration

The two IONMM 10/100Base-T/TX Ethernet ports can be configured for AutoCross Mode, Auto Negotiation, and Capabilities Advertised. The read-only information displayed at the port-level **MAIN** tab includes Link Status, Speed, Duplex, Port Admin Mode, Port Mode, and Connector Type.

The IONMM ports can be configured via the CLI or the Web interface.

Port Configuration – CLI Method

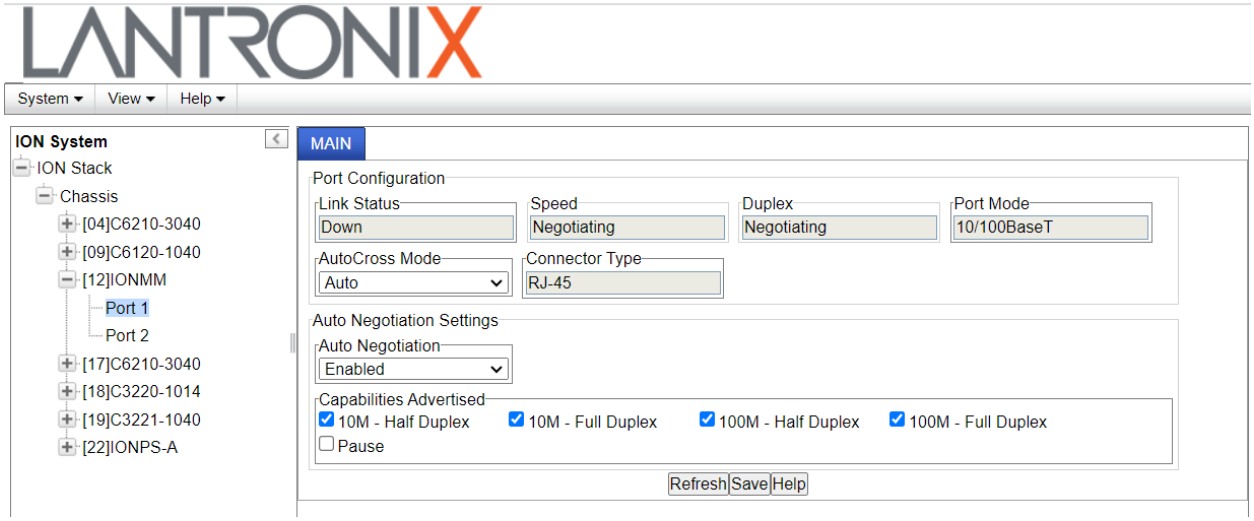
1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Use the go command to select port 1. Type **go l1p=1** and press **Enter**.
3. Enable or disable AutoCross Mode. At the command prompt type **set ether autocross=x** and press **Enter**.
4. Enable or disable Auto Negotiation. At the command prompt type **set ether autoneg state=x** and press **Enter**.
5. Define the set of capabilities to be advertised for this copper IONMM port. At the command prompt type **set ether adv-cap=x** and press **Enter**.
6. Use the **go** command to switch to port 2. Type **go l1p=2** and press **Enter**.
7. Repeat steps 3-5 above for Port 2.
8. Verify the port configuration settings. Type **show ether config** and press **Enter**. For example:

```
AgentIII C1|S1|L1P1>set ether autoneg state=disable
AgentIII C1|S1|L1P1>set ether speed=100M
AgentIII C1|S1|L1P1>set ether adv-cap ?
  STR_ETHER_ADV_CAPABILITY  A combination of 10THD,10TFD,100TFD, 100THD,1000THD
and 1000TFD for copper port, like 10TFD+100TFD+100THD+1000TFD; and N/A for none
capability; Cannot set this attribute for fiber port
AgentIII C1|S1|L1P1>set ether adv-cap=10TFD+100TFD+100THD+1000TFD
Agent III C1|S1|L1P1>show ether config
Port-1
TP port:
------------------------------------------------------------------------------
Link operation status:        up
Admin status:                 up
Port mode:                    RJ-45
PHY operation mode:           phy10-100BaseT
Speed:                        100M
Duplex:                       full
Autocross:                    auto
PHY mode change cap:          false

AutoNeg admin state:
Agent III C1|S1|L1P1>
Agent III C1|S1|L1P1>go l1p=2
Agent III C1|S1|L1P2>show ether config
Port-2
TP port:
------------------------------------------------------------------------------
Link operation status:        down
```

```
Admin status:                  up
Port mode:                     RJ-45
PHY operation mode:            phy10-100BaseT
Speed:                         10M
Duplex:                        half
Autocross:                     auto
PHY mode change cap:           false

AutoNeg admin state:
Agent III C1|S1|L1P2>
```

Port Configuration – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Click the plus sign [+] next to IONMM to unfold the IONMM ports.
3. Select Port 1.



4. At the **AutoCross Mode** dropdown, select **MDI**, **MDIX**, or **Auto**.
5. At the **Auto Negotiation** dropdown, select **Enable** or **Disable**.
   If you select **Disabled** and click the **Save** button, the Capabilities Advertised section displays.

   If you selected Auto Negotiation **Disabled** and click Save, the Capabilities Advertised section does not display.
6. In the **Capabilities Advertised** section, check the checkboxes for the capabilities to be advertised for this port. The capabilities that can be advertised are **10M - Half Duplex**, 10M - Full Duplex, **100M - Half Duplex**, **100M - Full Duplex**, and **Pause**.
7. Click the **Save** button when done.
8. Perform steps 4-7 for Port 2.

Configuring System Login Users

This section explains how to add, define, configure and delete ION system users via the Web interface and the CLI. This function works on an IONMM or a standalone SIC. The three levels of ION system login user rights are described in the table below.

Table 6: User Level Rights via Web / CLI

Level	Change own password?	Read configs?	Write configs though Web/CLI (1)	Upgrade / Backup / Restore ?	Create new users, Delete users (not itself and ION)?
Admin	Yes	Yes	Yes	Yes	Yes
Read-Write	Yes	Yes	Yes	No	No
Read-only	Yes	Yes	No	No	No

Note (1): (except for upgrade and backup/restore)

- There is one default **Admin** user named “ION”. Its default password is “private”. This user cannot be deleted.
- An **Admin** user has full rights to read/write all configurations through Web/CLI. An admin user can create new users and delete any users other than itself and ION.
- A **Read-Write** user can read/write all configurations except for Upgrade and Backup/Restore though Web/CLI. A read-write user can also change its own login password. When a read-write user logs in via the Web, the “UPGRADE” tab and the “BACKUP/RESTORE” tab are disabled. When a read-write user logs in via the CLI, all **set** commands except for upgrade and backup/restore can be executed.
- A **Read-Only** user can read all configurations except for Upgrade and Backup/Restore via the Web/CLI. When a read-only user logs into the Web interface, the Web will be disabled (like hardware mode) and only its own login password can be changed. When a read-only user logs in CLI, all **set** commands will be invisible and only its own password can be changed.
- This user management does not apply to Focal Point.
- Doing an SNMP **get** operation on the password object will return “********” (eight ‘asterisks).

Note Regarding SNMPv3 Users vs. Web/CLI Login Users
Note: do not confuse SNMPv3 users with the Web/CLI login users. SNMPv3 user configuration has nothing to do with the WEB/CLI login users. These two type users are different and have different functionalities. The SNMPv3 users are used for SNMPv3 access (for example MGSoft). The Web/CLI login users are used for Web/CLI login when users try to use the ION Web interface or CLI to access the ION system. SNMPv3 users cannot use their SNMP login credentials to log in to the ION Web/CLI (and vice-versa). See “Configuring SNMP Users” for information on configuring Web/CLI login users.

You can add, edit and delete ION system users via the CLI method or via the Web interface.

Configuring System Login Users - CLI Method

The User Level assignment defines the set of CLI commands that are accessible to a user. An Admin level user can access 251 commands; a Read-write user can access 248 commands; a Read-only user can access 52 commands (**show** commands only).

1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").

2. Check the existing set of ION system users. At the device's command prompt type **show sysuse**r and press the **Enter** key. All the existing ION system users and related information displays. This command only works on an IONMM or a standalone SIC.

3. Create a new system user. Type: **add sysuser name**=NAMESTR **level**=<admin|read-write|read-only> **pass**=PASSSTR **confirmpass**=PASSSTR

where:

name = NAMESTR = the new user's login username (1-63 characters, beginning with an alphanumeric character; no spaces).

level = <**admin**istrator, **read-writ**e, or **read-only**>

pass = PASSSTR = the new user's password string. The user password cannot contain any space characters.

confirmpass = PASSSTR = reentry of the new user password; must match the "pass" entry exactly.

4. Press the **Enter** key.

5. To edit an existing user's access level, type **set sysuser name**=NAMESTR **level**=(admin|read-write|read-only) and press **Enter**.

where:

name = NAMESTR = the existing user's current username.

level = the user's new access level; either **admin**istrator, **read-writ**e, or **read-only**.

6. To set a new password for an existing ION system user, type **set sysuser name**=NAMESTR **pass**=PASSSTR **confirmpass**=PASSSTR and press **Enter**.

where:

name = NAMESTR = the new user's login username (1-63 characters; no spaces).

pass = PASSSTR = the new user's password string. The user password must begin with an alphanumeric character and cannot contain any space characters.

confirmpass = PASSSTR = the new user's password string; type the same as for **pass** above.

7. To remove an existing system user, type **remove sysuser name**=NAMESTR and press **Enter**.

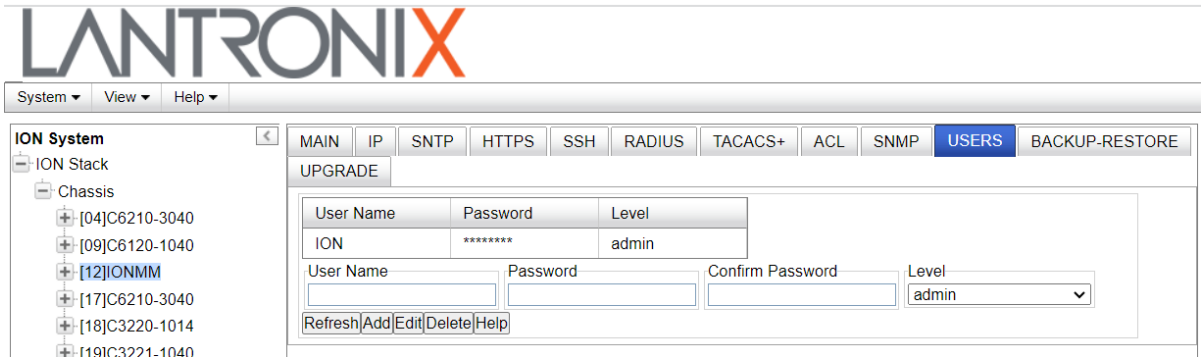
For example:

```
Agent III C1|S1|L1D>show sysuser
name                    level           password
ION                     admin           ********
Agent III C1|S1|L1D>add sysuser name AndersonT level read-only pass ******** confirmpass
********
Agent III C1|S1|L1D>add sysuser name BensonJ level read-only pass ******** confirmpass
********
Agent III C1|S1|L1D>add sysuser name CarlsonAnn level read-only pass ******** confirmpass
********
Agent III C1|S1|L1D>add sysuser name CarlsonAndy level read-only pass ******** confirmpass
********
Agent III C1|S1|L1D>add sysuser name Fitz level read-only pass ********** confirmpass
**********

Agent III C1|S1|L1D>show sysuser
name                    level           password
ION                     admin           ********
ion                     admin           ********
AndersonT               read-only       ********
BensonJ                 read-only       ********
CarlsonAnn              read-only       ********
CarlsonAndy             read-only       ********
Fitz                    read-only       ********
Agent III C1|S1|L1D>
```

8. Backup the configuration. See "Backup and Restore Operations (Provisioning)".

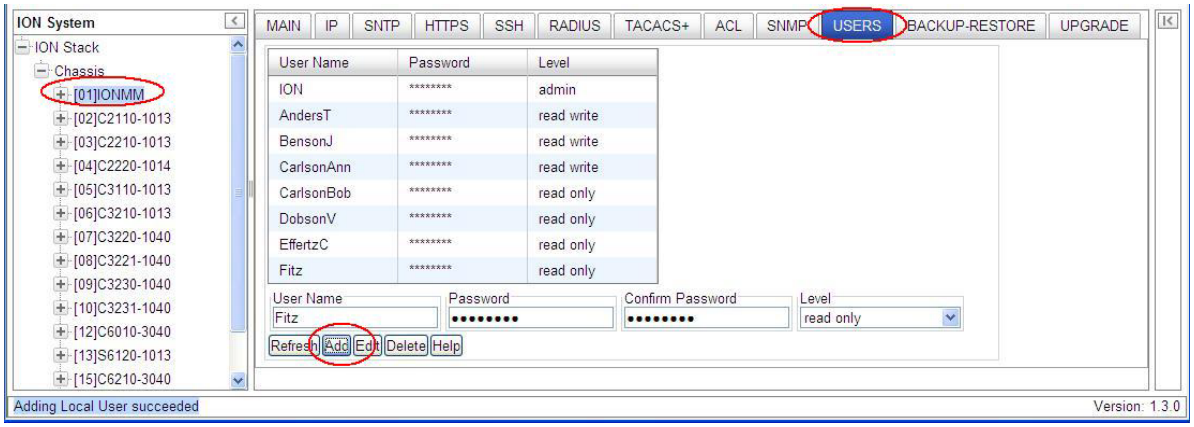
Configuring System / Login Users - Web Method

1. Access the IONMM or NID through the Web interface (see "Starting the Web Interface").
2. At the IONMM **USERS** tab, locate the Users table.



3. In the **User Name** field, enter this user's name (1-64 alphanumeric characters with no spaces between characters).
4. In the **Password** field, enter this user's password.
5. In the **Confirm Password** field, re-enter the password as entered in step 4. If the two password entries do not match, the message "*ERROR: The two passwords are not the same, please check!*" displays and you must enter matching passwords.

6. At the **Level** dropdown, select this user's access level (**admin**, **read write**, or **read only**).
7. Click the **Add** button. The new user is added to the User s table.

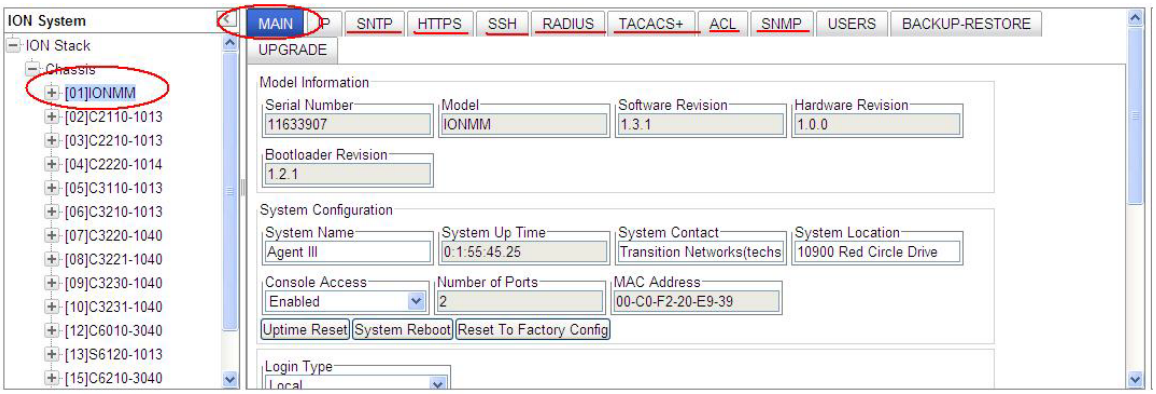


8. Perform steps 3-7 above for each new user to be added.
9. Click the **Refresh** button to update the screen information.
10. To edit an existing user, select (highlight) the entry in the table, edit the **User Name**, **Password**, and/or **Level** fields, and click the **Edit** button. The message "*Modifying Local User succeeded*" displays.
11. To delete an existing user, select (highlight) the entry in the table and click the **Delete** button. The selected user is deleted from the table and the message "*Deleting Local User succeeded*" displays.

Configuring Security Features

The IONMM can be configured to work with:

- Access Control List (ACL) from the **ACL** tab.
- Hyper Text Transfer Protocol Secure (HTTPS) from the **HTTPS** tab.
- Management VLAN from the IONMM **MAIN** tab.
- Remote Authentication Dial In User Service (RADIUS) from the **RADIUS** tab.
- Terminal Access Controller Access Control System (TACACS+) authentication, authorization and accounting services from the **TACACS+** tab.
- Simple Network Time Protocol (SNTP) from the **SNTP** tab.
- Secure Shell (SSH) from the **SSH** tab.
- Simple Network Management Protocol (SNMP) from the IONMM **SNMP** tab.



Configuring these features is discussed in the following sections.

Configuring an ACL

An Access Control List (ACL) is a collection of permit and deny rules and conditions that provide security across an Ethernet connection internet or intranet) by blocking unauthorized users and allowing authorized users to access specific resources.

IMPORTANT

An ACL does not control access to the IONMM through a serial interface (USB connection).

- If the NID is managed by the IONMM, configuring ACL should be done at the IONMM and not at the NID.
- The ION system supports the configuration of the INPUT chain of the filter table of Linux iptables; all rules being added belong to the INPUT chain of the filter table.
- At least one condition is needed for a rule before the rule can work. After you create a rule, you also need to create at least one condition for it.
- Multiple conditions can be assigned to one rule; only when all conditions of the rule are matched for an input packet, the policy of the rule can be applied to it.
- If multiple rules are matched to an input packet, the rule with the highest priority will be applied.
- You can add/modify/delete a rule or a condition whether the ACL is enabled or disabled.
- Since only the configuration for INPUT chain of the filter table is supported, there is no option to select the table-type and chain-type. They are fixed values: table is filter and chain is INPUT. This table and chain meets most, if not all, ACL functionality requirements.
- The IONMM does not support two ACL conditions with the same condition type. The ACL only blocks access from outside of the IONMM. The ACL does not apply any restriction to the out-going packets from the IONMM.
- Configure both a rule and a condition; even if a rule is configured without a condition, the top ACL condition applies to all packets.

In a very basic sense, ACLs consist of chains, rules, and conditions.

A chain is a table that contains a set of rules, usually for a particular function, such as input or output. The chain also defines a default policy that will be used if a policy is not determined by the end of processing for all rules. The only chain that can be specified for the IONMM is INPUT. This chain contains the rules and conditions for accessing the IONMM through an Ethernet connection (Telnet session or Web interface).

The rules of an ACL define the policy to be followed for certain defined conditions. There are three different policies (rules) that can be defined for the IONMM:

- **Accept** – allow communication from the device
- **Drop** – disallow communication from the device
- **Trap** – initiate an SNMP trap message

The conditions of an ACL define the objects the policies apply to (e.g., MAC or IP addresses, ports, etc.).

ACLs are read from top to bottom. When a packet comes to the IONMM, it is matched against the first line in the ACL; if it does not meet the criteria there, then it drops to the next line, and so on until it reaches a permit or deny that fits it. For all ACLs there is an implied deny beneath the last line of the ACL. When applying an ACL to an interface it is recommended that there be at least one permit statement.

The Access Control List (ACL) can be configured for IPv6 traffic flows in the IP stack. An ACL ensures that only permitted traffic flows working in the IP stack for security reasons.

The ION system supports a maximum of 64 ACL rules and 128 ACL conditions. If the maximum is exceeded, the message "Setting values failed (snmp operation error, possible reasons: invalid data, error data sequence, dynamic table capability limit, etc)" displays. Note that when displaying ACL rules, the CLI must check multiple dynamic tables and find the relationship between ACL rules and ACL conditions. It will take much more time than other simple commands. The more ACL rules and conditions added, the slower the display command will be.

ION uses an 'index' to identify an ACL instead of using a name. For ION ACLs, IPv4 and IPv6 are totally separate functions.

When IPv6 is enabled, you can have up to three of an IP style (IPv4 or IPv6).

For IPv6:

1. One ip6tables ACL rule can only have one layer 2 ACL condition (macaddr).
2. One ip6tables ACL rule can only have one layer 3 ACL condition (ipv6addr or ipv6network).
3. One ip6tables ACL rule can only have one layer 4 ACL condition (tcpport or tcpportrange or udpport or udpportrange or icmp).

For IPv4:

1. One ACL rule can only have one layer 2 ACL condition (macaddr).
2. One ACL rule can only have one layer 3 ACL condition (ipv4addr or ipv4addrrange or ipv4network).
3. One ACL rule can only have one layer 4 ACL condition (tcpport or tcpportrange or udpport or udpportrange or icmp).

An ACL can be configured in the IONMM using either the CLI or Web method.

ACL Config (IPv4) – CLI Method

For a complete list of all CLI commands for ACL operations see the *ION System CLI Reference Manual, 33461*.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Enable ACL. Type: **set acl state=enable** and press **Enter**.
3. Define the default chain policy. **Note:** the defaults are set to **table**=**filter** and **chain**=**input** and cannot be changed. Type:

   set acl table=filter chain=input policy=<xx>

   where:

   xx = default policy if a policy is not determined by the end of the table; valid choices are:

   - **accept** (allows communication – the factory default setting)
   - **drop** (disallows communication)

4. Press **Enter**.
5. Define a condition that will be associated with a rule. Type:

   add acl condition type=<ww> **srcdst=**<xx> **oper=**<yy> **value=**<zz> **index=**<aa>

   where:

   ww = what the condition applies to; the valid choices are:

   - **macaddr**
   - **ipv4network**
   - **udpport**
   - **ipv4addr**
   - **ipv4addrrange**
   - **udpportrange**
   - **tcpport**
   - **tcpportrange**
   - **icmp**

   xx = restriction stream; valid choices are:

   - **src** (the condition applies to the source address)
   - **dst** (the condition applies to the destination address)

   yy = operation type; valid choices are:

   - **equal** (the condition applies if the packet equals the condition type)
   - **notequal** (the condition applies if the packet does not equal the condition type)

   zz = address, port number or type associated with the value specified for operation **type=**

   Note: if a range is specified for **type=**, then the two values for num must be separated by a hyphen (i.e., 1–4).

6. Press **Enter**.
7. Repeat steps 5 and 6 for each condition to be defined.
8. Define a rule to be associated with the chain. Type:

add acl rule position=<ww> **table=filter chain=input policy=**<xx> **traprate=**<yy> **condition=**<zz>

where:

ww = whether the new rule is put to the top or end of rule list; valid choices are:

- **head**
- **tail**

xx = ACL policy type; valid choices are:

- **accept** (if the rule is met, packets are to be accepted)
- **drop** (if the rule is met, packets are to be dropped)
- **trap** (if the rule is met, a trap is to be sent)

yy = number (1 – 65535) of times the trap can be sent in a minute. This value is only valid if:

- **policy=trap** is specified.
- A trap server is defined on the **MAIN** tab.
- A trap server is in the network and available.

Zz = index numbers of the conditions that will be assigned to the rule.

If more than one condition is specified, each must be separated by a comma with no spaces (e.g., 2,3,6).

9. Press **Enter** when done. The Condition List index information displays (e.g. *cond_list=1*).
10. Repeat steps 8 and 9 to define a rule for each condition to be associated with the chain.
11. Verify that ACL has been enabled. Type: **show acl state** and press **Enter**. The current ACL management state information displays:

```
C1|S7|L1D>show acl state
ACL management state:          disable
```

12. Verify the ACL rules have been defined and associated. Type: **show acl rule** and press **Enter**. The current ACL Rule information table displays. For example:

```
C1|S7|L1D>set acl state=enable
C1|S7|L1D>set acl table=filter chain=input policy=accept
C1|S7|L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=192.168.1.30
C1|S7|L1D>add acl condition type=ipv4addr srcdst=src oper=notequal value=192.168.1.30
C1|S7|L1D>add acl rule position=head table=filter chain=input policy=accept condition=1 con-
dlist=1
C1|S7|L1D>add acl rule position=tail table=filter chain=input policy=trap condition=2 con-
dlist=2
C1|S7|L1D>show acl rule
index    table-type     chain-type     priority  policy    traprate(packets/min)   condition
-------------------------------------------------------------------------------------------
1        filter         input          1         trap      1500                    2
```

If no ACL rules are yet defined, the message "*No ACL rule now!*" displays.

13. To verify the ACL condition configuration, type **show acl condition** and press **Enter**. The current ACL conditions display. For example:

```
C1|S7|L1D>show acl condition
index type            src/dst   operation  value          rule idx
-------------------------------------------------------------------------------
1        ipv4addr     src       equal      172.11.1.1      0
2        ipv4addr     src       equal      192.168.1.30    1
```

14. To verify the ACL chain configuration, type **show acl chain** and press **Enter**. The current ACL chain displays. For example:

```
C1|S7|L1D>show acl chain
table-type     contain-type   chain-name                default-policy
-------------------------------------------------------------------
filter         input          INPUT                      accept
```

If no ACL rules are yet defined, the message "*No ACL rule now!*" displays.

Problem: Setting ACL drop rule to enable causes loss of management.

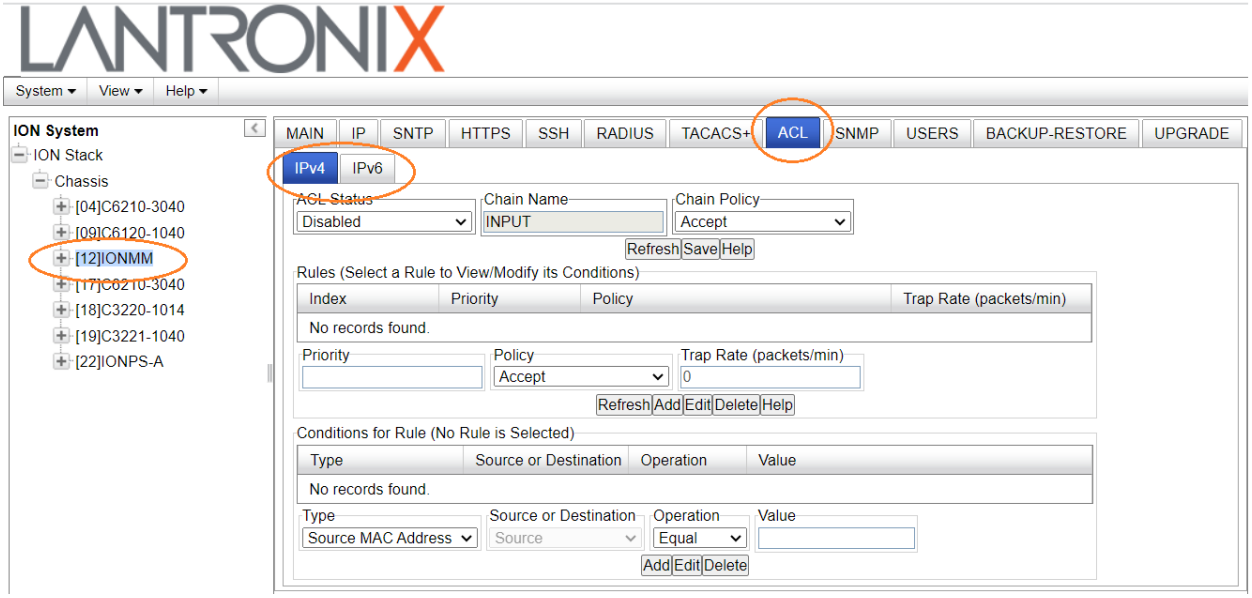
Description: Configuring an ACL rule with priority of 1 and policy of drop and enabling ACL Status in Web UI or CLI causes loss of IP management. No conditions for rule have been set yet.
Example:

```
Agent III C1|S1|L1D>show acl rule index table-type chain-type priority policy traprate(packets/min) condition
1 filter input 1 drop 0 no Agent III C1|S1|L1D>
```

Recovery: 1. Disable ACL status via USB to restore management. 2. Configure both a rule and a condition. 3. Note that even if a rule is configured without a condition, the top ACL condition applies to all packets.

ACL Config (IPv4) – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. At the **ACL** tab, select the IPv4 tab if not already selected.



3. In the **ACL Status** field, select **Enabled**.
4. In the **Chain Name** field, **INPUT** is the default and the only valid entry.
5. In the **Chain Policy** field, select the default policy if a policy is not determined by the end of the table:
   - **Accept** (allows communication, default value)
   - **Drop** (disallows communication)
6. Define a Rule.
   a) In the **Priority** field, enter a number indicating the relative position of the rule to other rules in the table. (This is the index of the corresponding iptables rule within the chain within the table.) The valid range is 1 – 65,535.
   b) In the **Policy** field, select the policy to be associated with this rule (**Accept**, **Drop**, or **Trap**).
   c) In the **Trap Rate** field, enter a value indicating the number of traps that will be sent per minute. The valid range is 1- 655,525 traps sent per minute.

      The **Trap Rate** field is only valid if:
      - The policy selected is **Trap**.
      - A trap server is defined on the **SNMP** tab.
      - A trap server is on the network, configured and available.

   d) Click **Add**.
7. Define additional rules as needed following step 6.

8. Define a condition:

   a) Select a rule by clicking its index number. The selected rule line is highlighted.

   b) In the **Type** field, select the condition type. The options are ***Source MAC Address*** (1), ***IPv4 Address*** (2***), IPv4 Address Range*** (3***), IPv4 Network*** (4), ***TCP Port*** (5), ***TCP Port Range*** (6), ***UDP Port*** (7), ***UDP Port Range*** (8), or ***ICMP Type*** (9).

   c) In the **Source or Destination** field, select whether the type is a source or a destination.

   d) In the **Operation** filed, select whether the match for this condition is "equal to" type or "not equal to" type.

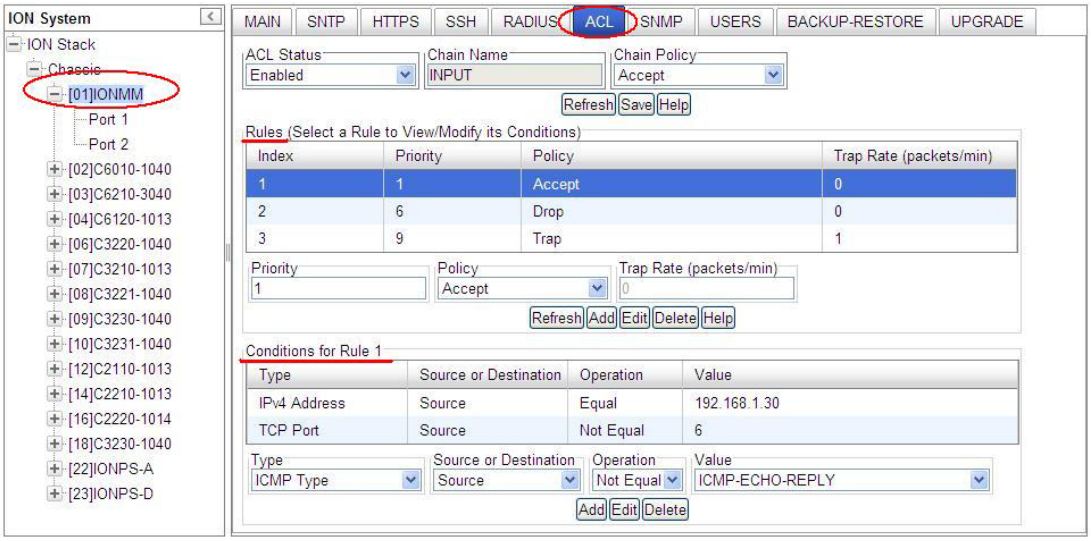
   d) If the **Type** field selection was *ICMP Type*, then in the **Value** field, specify the address, port number or type associated with the selection in the **Type** field.
   There are 36 selectable **ICMP Type** values: 1. ICMP-ECHO-REPLY, 2. ICMP-DESTINATION-UNREACHABLE, 3. ICMP-NETWORK-UNREACHABLE, 4. ICMP-HOST-UNREACHABLE, 5. ICMP-PROTOCOL-UNREACHABLE, 6. ICMP-PORT-UNREACHABLE, 7. ICMP-FRAGMENTATION-NEEDED, 8. ICMP-SOURCE-ROUTE-FAILED, 9. ICMP-NETWORK-UNKNOWN, 10. ICMP-HOST-UNKNOWN, 11. ICMP-NETWORK-PROHIBITED, 12. ICMP-HOST-PROHIBITED, 13. ICMP-TOS-NETWORK-UNREACHABLE, 14. ICMP-TOS-HOST-UNREACHABLE, 15. ICMP-COMMUNICATION-PROHIBITED, 16. ICMP-HOST-PRECEDENCE-VIOLATION, 17. ICMP-PRECEDENCE-CUTOFF, 18. ICMP-SOURCE-QUENCH, 19. ICMP-REDIRECT, 20. ICMP-NETWORK-REDIRECT, 21. ICMP-HOST-REDIRECT, 22. ICMP-TOS-NETWORK-REDIRECT, 23. ICMP-TOS-HOST-REDIRECT, 24. ICMP-ECHO-REQUEST, 25. ICMP-ROUTER-ADVERTISEMENT, 26.ICMP-ROUTER-SOLICITATION, 27. ICMP-TIME-EXCEEDED, 28. ICMP-TTL-ZERO-DURING-TRANSIT, 29. ICMP-TTL-ZERO-DURING-REASSEMBLY, 30. ICMP-PARAMETER-PROBLEM, 31. ICMP-IP-HEADER-BAD, 32. ICMP-REQUIRED-OPTION-MISSING, 33. ICMP-TIMESTAMP-REQUEST, 34. ICMP-TIMESTAMP-REPLY, 35. ICMP-ADDRESS-MASK-REQUEST, and 36. ICMP-ADDRESS-MASK-REPLY.

   f) Click **Add**. The message "*Setting values succeeded*" displays.

9. Define additional Conditions as needed following step 8.

10. To change an existing Rule, select the Rule in the table, click the **Edit** button, and make changes per steps 5-6 above.

11. Verify the displayed ACL information.



12. After all rules and conditions have been defined, click the **Save** button near the top of the screen.

ACL under IPv6

You can set up to 255 ACL Rules and up to 255 ACL Conditions. Note that since ACL rules and conditions must process dynamic tables and check the relationship between multiple tables, the **ACL show** commands need more time to display the content compared to other tables. These commands can only be executed on IONMM or a standalone SIC.

For a complete list of all CLI commands for ACL operations see the *ION System CLI Reference Manual, 33461*.

ACL Config (IPv6) – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Enable ACL. Type: **set ip6tables acl state** and press **Enter**.
3. Define the default chain policy. Type: **set ip6tables acl table=filter chain=input policy=accept** and press **Enter**.
4. Define a condition that will be associated with a rule. Type: **set ip6tables acl condition=1 rule_index=1** and press **Enter**.
5. Repeat step 4 for each condition to be defined.
6. Define a rule to be associated with the chain. Type: **add ip6tables acl rule position=head table=filter chain=input policy=1 trap=444** and press **Enter**.
7. Repeat step 6 to define a rule for each condition to be associated with the chain.
8. Verify that ACL has been enabled. Type: **show ip6tables acl state** and press **Enter**. The current ACL management state information displays:

```
Agent III C1|S9|L1D>show ip6tables acl state
ACL of IPv6 tables management state:    enable
Agent III C1|S9|L1D>
```

9. Verify the ACL rules have been defined and associated. Type: **show ip6tables acl rule** and press **Enter**. The current ACL Rule information table displays. For example:

```
Agent III C1|S9|L1D>set ip6tables acl state=enable
Agent III C1|S9|L1D>set ip6tables acl table=filter chain=input policy=accept
Agent III C1|S1|L1D>add ip6tables acl rule position=head table=filter chain=input
policy=1 trap=444
Agent III C1|S1|L1D>add ip6tables acl rule index=2 table=filter chain=input
prio=2 policy=trap traprate=100
Agent III C1|S1|L1D>set ip6tables acl condition=1 rule_index=1
Agent III C1|S1|L1D>add ip6tables acl condition type= ipv6addr srcdst=src
oper=equal value=VAL
Agent III C1|S1|L1D>show ip6tables acl rule
index     table-type    chain-type    priority  policy  traprate(pkts/min)    condi-
tion
-------------------------------------------------------------------------------
----
2         filter         input          1      trap      0                 no
1         filter         input          2      trap      0                 no
```

```
Agent III C1|S1|L1D>
```

If no ACL rules are yet defined, the message "*No ACL rule now!*" displays.

10. To verify the ACL condition configuration, type **show ip6tables acl condition** and press **Enter**. The current ACL conditions display. For example:

```
Agent III C1|S1|L1D>show ip6tables acl condition
index     type           src/dst   operation    value                rule idx
-------------------------------------------------------------------------------
1         ipv6addr       src       equal        ::
   0
2         ipv6addr       src       equal        ::
   0
3         ipv6addr       src       equal        ::
   0
4         ipv6addr       src       equal     fe80::2c0:f2ff:fe20:de9e      0
Agent III C1|S1|L1D>
```

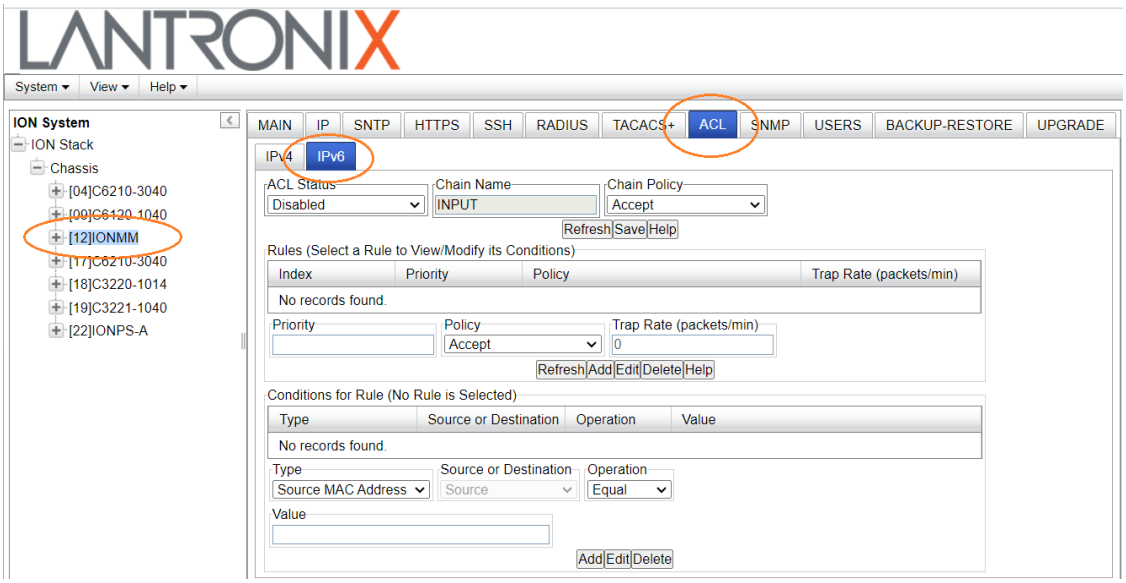
11. To verify the ACL chain configuration, type **show ip6tables acl chain** and press **Enter**. The current ACL chain displays. For example:

```
Agent III C1|S1|L1D>show ip6tables acl chain
table-type     contain-type   chain-name                  default-policy
-------------------------------------------------------------------------
filter         input          INPUT                       accept
C1|S3|L1D>
```

If no ACL rules are yet defined, the message "*No ACL rule now!*" displays.

ACL Config (IPv6) – Web Method

1. Navigate to the **ACL** tab. The **IPv4** sub-tab displays by default.
2. Select the **IPv6** sub-tab.



3. At the **ACL Status** dropdown, select **Enabled**.

4. At the **Chain Policy** dropdown, select **Accept** or **Drop**.
5. In the **Rules** - **Priority** field, enter a priority of 1-65,535.
6. At the **Policy** dropdown, select **Accept** or **Drop** or **Trap**.
7. In the **Trap Rate** (packets/min) field, enter the desired rat for trapping (if selected). The valid range is 1-65,535. The trap sent rate is 2 packet/sec (two packets/second (2 pps). The matched packets number in one minute. If over this rate matched, a trap will be sent.
8. Click the **Add** button to add this Rule.
9. At the **Conditions** - **Type** dropdown, select the basis for conditions for this rule. The IPv6options are:
   Source MAC Address (default)
   IPv6 Address
   IPv6 Network
   TCP Port
   TCP Port Range
   UDP Port
   UDP Port Range
   ICMP Type

4. Enter a "**Value**" (a valid IPv6 address / a number from 0-128 or an IP address such as ffff:00:00:00:00:00:00:00).

A rule can at most have three conditions and each condition must belong to a different protocol layer.

1. Layer 2 condition type: Source-MAC-address.
2. Layer 3 condition type: IPv6-address, IPv6-network.
3. Layer 4 condition type: TCP-port, TCP-port-range, UDP-port, UDP-port-range, ICMP-type.

IPv6 Condition Type Values

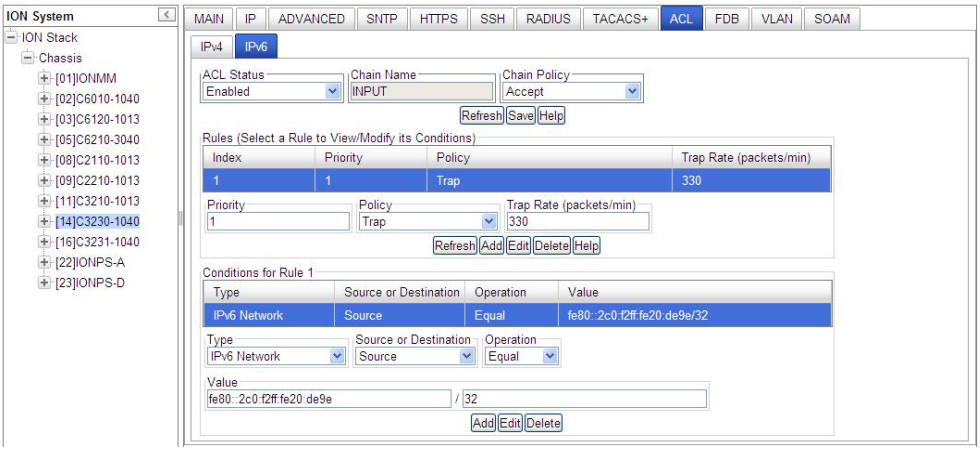
Source MAC address: first 6 bytes for mac address.
IPv6 address: the first 16 bytes for IPv6 address.
)IPv6 network: address[/mask], the first 16 bytes for IPv6 address, the followed bytes can be either of two cases.
Case 1: the 17th byte is a plain number, specifying the number of 1's at the left side of the network mask.
Case 2: bytes 17-32 are the value for network mask.
TCP port: the first two bytes for TCP port number.
TCP port range: the first 4 bytes(0-1 byte for the start TCP port number, 2-3 byte for the end TCP port number).
UDP port: the first two bytes for UDP port number.
UDP port range: the first 4 bytes(0-1 byte for the start UDP port number, 2-3 byte for the end UDP port number).
ICMP type: the first two bytes for ICMP type. For ICMP type, the following values are supported:

ICMP_DESTINATION-UNREACHABLE = 0x3ff,
ICMP_NO-ROUTE = 0x0301,
ICMP_COMMUNICATION-PROHIBITED = 0x0302,
ICMP_ADDRESS-UNREACHABLE = 0x0303,
ICMP_PORT-UNREACHABLE = 0x0304,
ICMP_PACKET-TOO-BIG = 0x04ff,
ICMP_TIME-EXCEEDED = 0x05ff,
ICMP_TTL-ZERO-DURING-TRANSIT = 0x0501,
ICMP_TTL-ZERO-DURING-REASSEMBLY = 0x0502,
ICMP_PARAMETER-PROBLEM = 0x06ff,
ICMP_BAD-HEADER = 0x0601,
ICMP_UNKNOWN-HEADER-TYPE = 0x0602,
ICMP_UNKNOWN-OPTION = 0x0603,
ICMP_ECHO-REQUEST = 0x07ff,

ICMP_ECHO-REPLY = 0x08ff,
ICMP_ROUTER-SOLICITATION = 0x09ff,
ICMP_ROUTER-ADVERTISEMENT = 0x0aff,
ICMP_NEIGHBOUR-SOLICITATION = 0x0bff,
ICMP_NEIGHBOUR-ADVERTISEMENT = 0x0cff,
ICMP_REDIRECT = 0x0dff, Use this OID to set the value of the corresponding condition type.

Notifications: ionDevSysIPv6AclIdsEvt , ip6tablesGRuleIndex)

An ionDevSysIPv6AclIdsEvt event is sent if an ip6tables IDS (Intrusion Detection Systems) is detected. *entPhysicalIndex* indicates in which SIC the IDS is detected. *entPhysicalIndex/ip6tablesGRuleIndex* indicates which ip6tables ACL rule is matched for this IDS. For example, shown below is a C3230 NID with IPv6 ACL configured with one Rule and one Condition.



In the example above, the **Rule** index 1 has a Priority of 1, a Policy of Trap, and a Trap Rate of 330. The **Conditions** for Rule 1 has Type set to IPv6 Network, Source or Destination set to Source, Operation set to Equal, and Value set to fe80::2c0:f2ff:fe20:de9e / 32.

Messages: *Error: when condition type is srcmaddr, srcdst can only be src.*

Configuring HTTPs

HTTPs is a secure version of the Hyper Text Transfer Protocol (HTTP) and is used as a security option when accessing the IONMM via the Web UI.

IMPORTANT

- If the NID is managed by the ION Management Module (IONMM), configuring HTTPS should be done at the IONMM and not at the NID.
- HTTPS has no affect when accessing the IONMM through either the USB or an SSH or Telnet session.
- After configuring the NID for HTTPS, a re-login occurs immediately; you must enter the **https://** prefix to re-connect to the ION system.

There are two primary differences between an HTTPS and an HTTP connection:

- HTTPS connects on port 443, while HTTP is on port 80
- HTTPS encrypts the data sent and received with TLS, while HTTP sends it all as plain text

TTPS uses the Transport Layer Security (TLS) protocol to protect communications over the network. TLS employs two types of cryptography. During the initial handshake, it uses asymmetric (public-key) cryptography: the server has a public key available to anyone and a corresponding private key known only to that server. This key pair is used to authenticate the server's identity and to securely establish shared, symmetric session keys. Once the handshake is complete, TLS uses symmetric encryption for the actual data stream—both parties use the same secret session key to encrypt and decrypt messages. The server may use its private key to generate a digital signature during the handshake, which the client verifies with the server's public key, ensuring the communication is authentic and has not been tampered with.

For the IONMM, HTTPS can be used for client authentication to limit access to the IONMM to authorized users. To do this, the site administrator typically creates a certificate for each user, a certificate that is loaded into their browser. Normally, that contains the name and e-mail address of the authorized user and is automatically checked by the server on each reconnect to verify the user's identity, potentially without even entering a password.

The trust inherent in HTTPS is based on major certificate authorities. Organizations may also run their own certificate authority, particularly if they are responsible for setting up browsers to access their own sites (for example, sites on a company intranet, etc.). They can easily add copies of their own signing certificate to the trusted certificates distributed with their browser.

TLS encrypts the data stream traveling over the network so that passive eavesdroppers cannot easily read it. However, encryption alone is not enough to keep the connection secure. Before any application data is sent, the server presents a certificate - ideally digitally signed by a trusted Certificate Authority. Your client verifies this certificate to confirm that the public key used to establish the encrypted session truly belongs to the intended server. Without a trusted signed certificate, an attacker could impersonate the server and insert themselves into the connection—terminating your encrypted channel, reading or altering your data, and then re-encrypting it to forward to the real server. In that situation, your data would indeed be encrypted, yet the party on the other end would not be whom you think. Certificates

are therefore essential: without them, man-in-the-middle and impersonation attacks would be far more common.

Note: the authentication certificate and private key file must be resident in the default directory on the TFTP/SFTP Server (e.g., C:/TFTP-Root), and the TFTP/SFTP server must be configured properly and running.

The ION HTTP server provides authentication for client connections, but not encryption. The data that the client and server transmit to each other is not encrypted. This leaves communication between clients and servers vulnerable to interception and attack. The Secure HTTP (HTTPS) feature lets you connect to the ION HTTPS server securely. It uses Secure Sockets Layer (SSL) to provide device authentication and data encryption. The HTTP server can support both IPv4 and IPv6 at the same time. The ION system supports up to 16 HTTP/HTTPS clients.

HTTPS can be configured in the IONMM using either the CLI or Web method.

HTTPS Config – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Enable HTTPS. Type: **set https state=enable**

   Note: enabling HTTPS has no effect on either the USB or Telnet interface. However, access through the Web interface must go through HTTPS authentication.
3. Press **Enter**.
4. Set the port number to be used. The factory default is 443. Type: **set https port=**<xx> and press **Enter**.
5. Define whether the certificate is from a certificate authority or is self-generated. Type:

   set https certificate–type=<xx>

   where:

   xx = certificate authority; valid choices are:
   - **authorized**
   - **self–certificate**
6. Press **Enter**.
7. Specify the name of the certificate file. Type: **set https certificate–file=**<xx> where:

   xx = name of the file
8. Press **Enter**.
9. Specify the name of the private key file. Type: **set https private–key file=**<xx> where:

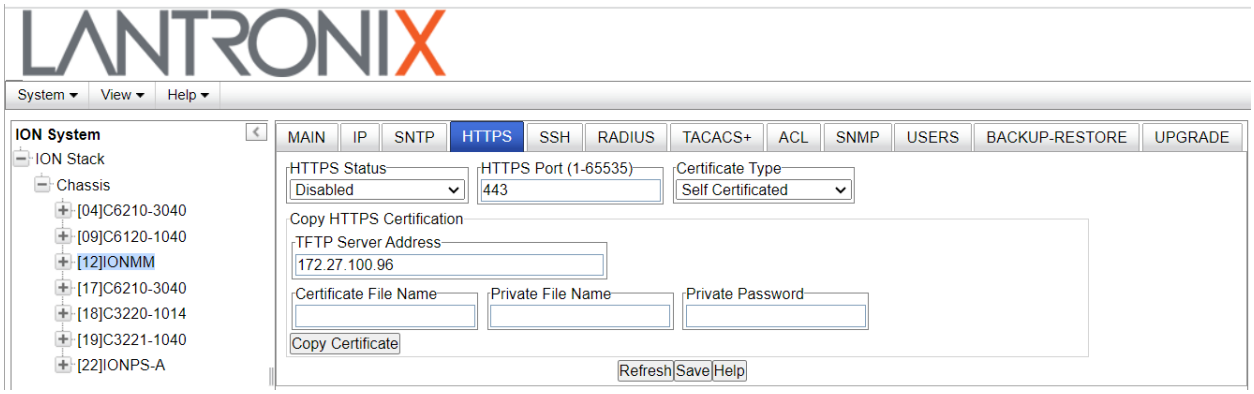
   xx = name of the file
10. Press **Enter**.
11. Define the password to be used for the private key file. Type: **set https private–key password**
12. Press **Enter**. The message "*Please input password:*" displays.
13. Type the password then press **Enter**. The message "*Please input password again:*" displays.

14. Type the password again then press **Enter**.
15. Verify the configuration has been set. Type: **show https config** and press Enter.
16. Press **Enter**. The current HTTPS configuration table displays. For example:

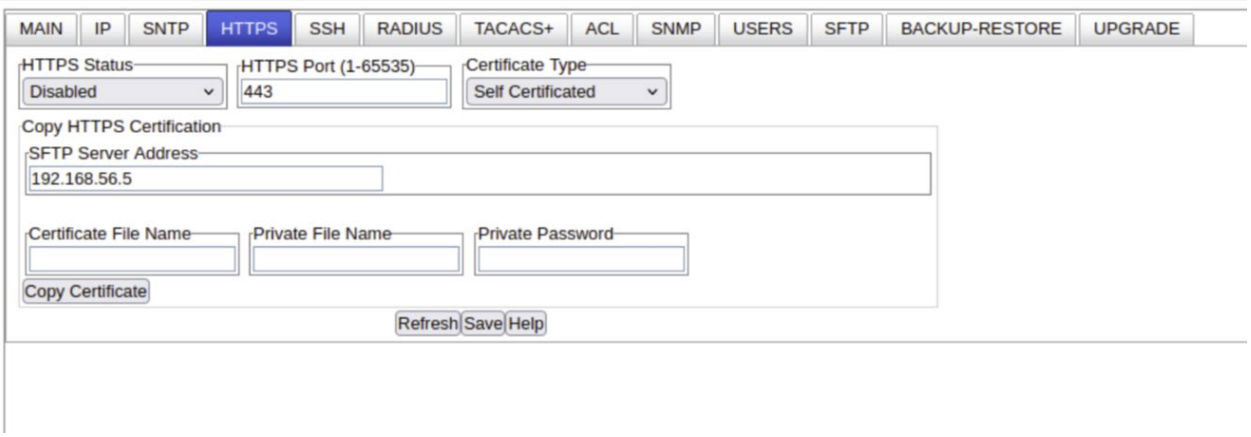
```
Agent III C1|S1|L1D>set https state=enable
Agent III C1|S1|L1D>set https port=443
Agent III C1|S1|L1D>set https certificate-type=authorized
Agent III C1|S1|L1D>set https certificate-file=name.cer
Agent III C1|S1|L1D>set https private-key file=name.key
Agent III C1|S1|L1D>set https private-key password
Please input password:

Please input password again:

Agent III C1|S1|L1D>show https config
HTTPS configuration:
------------------------------------------------------------------------
HTTPS state:                    enable
HTTPS port:                     443
HTTPS certificate file:         name.cer
HTTPS private key file:         name.key
Agent III C1|S1|L1D>
```

HTTPS Config – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **HTTPS** tab.



If SFTP is enabled, the HTTPS page will display the SFTP Server Address field.



3. In the **HTTPS Status** field, select **Enabled**.

   Note: enabling HTTPS has no effect on either the USB or Telnet interface. However, access via the Web UI must go through HTTPS authentication.

4. In the **HTTPS Port** field, enter the port number for HTTPS operations. The valid range is 1-65535. The default is port 443.

4. In the **Certificate Type** field, select **Self Certificated** or **Authorized**.

5. In the **TFTP/SFTP Server IP Address** field, enter the IP address of your TFTP/SFTP server. This entry must be an IP address or a domain name.

6. In the **Certificate File Name** field, enter the name of the file with the authentication certificate.

   Note: the authentication certificate and private key file must be resident in the default directory on the TFTP/SFTP Server (e.g., *C:/TFTP-Root*).

7. In the **Private File Name** field, enter the name of the private key file.

8. In the **Private Password** field, enter the private key password. This is the password to access the private key file.

9. Click the **Copy Certificate** button.

10. Click the **Save** button. A re-login occurs immediately, and the ION login prompt displays.

11. The ION System Web Interface is now an HTTPS (secure) address. In your web browser, click **Tools**, click *Internet Options*, click **Advanced**, and make sure the **SSL** and **TLS** protocols are enabled under the security section.

12. For subsequent logins, use **https** instead of **http** as the URL prefix (e.g., https://192.168.0.10/web.html).

13. Enter the ION system *User Name* and *Password*.

14. Click the **Sign In** button. The **MAIN** tab displays.

    If the message *Invalid user name or password!* displays, see the Troubleshooting section of this document.

Note: enabling HTTPS has no effect on either the USB or Telnet interface. However, access through the Web interface must go through HTTPS authentication.

Note: FW v 1.5.12 fixed expired IONMM Certificate. To see the new certificate, do a “Factory Reset” on the IONMM and then turn on HTTPs. The new certificate isn’t loaded until you do the “Factory Reset”.

Configuring Management VLAN

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.

The Management VLAN is used to separate management traffic from other network traffic to and from the IONMM. The Management VLAN is designed to help ensure the security of management control by making sure that equipment not belonging to the Management VLAN does not have access to the management traffic.

When configuring Management VLAN for the IONMM you can specify whether one or both ports on the IONMM are part of the Management VLAN.

IMPORTANT

1) If a NID is managed by the IONMM, configuring SNTP should be done at the IONMM and not at the NID.
2) When you specify a Management VLAN, your Web and Telnet interfaces to the IONMM are lost, unless the management station is on the same VLAN. Only stations in the same VLAN will be allowed to communicate with the IONMM through the network.
3) Enabling a Management VLAN does not disable a USB serial interface to the IONMM.
4) The VLAN Identifier (VID) provides identification of the VLAN, which is defined by the standard IEEE 802.1Q. Each VID has 12 bits to allow the identification of up to 4094 VLANs on each switched path.
5) See Appendix B for Management VLAN default settings.

The following configuration restrictions apply to the Management VLAN feature for the IONMM:

1) Management VLAN Status cannot be changed to “Enabled” with VLAN “1” and valid VLAN ID allowed is “2 to 4094”. However, VLAN “1” can be selected when Management VLAN status is set to “Disabled”. (Also applies to IONMM.) Thus:
    - a VLAN ID of 2-4094 is valid with Management VLAN enabled.
    - a VLAN ID of 1-4094 is valid with Management VLAN disabled.
2) Management VLAN status cannot be changed to “Enabled” when no port members are selected.
3) Management VLAN Status “Disabled” means that Management access is allowed on all the ports; the values in Management VLAN ID and port members are ignored (at **Device** > **Port** > **ADVANCED** tab > **VLAN Forwarding Rules** section > **VLAN Status** field).

Note: If the Management VLAN ID is entered in the VLAN table, the Management VLAN associated with the VLAN ID cannot be enabled. ION versions 1.3.1 and 1.2.1 both have same result. In ION V1.2.1 and above, the Management VLAN cannot be viewed or changed in the VLAN table. In this case remove the Management VLAN ID in the VLAN table and continue operation.

Management VLAN can be configured in the IONMM using either the CLI or Web method.

Management VLAN Config – CLI Method

Note before performing this configuration: When you specify a Management VLAN, your Web and Telnet interfaces to the IONMM are lost, unless the management station (PC) is on the same VLAN. Only management stations in the same VLAN can communicate with the IONMM through the network. Enabling a Management VLAN does not disable a USB serial interface to the IONMM.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Type: **set mgmt vlan vid=<**xx> where:

   xx = VLAN ID number (2–4094). **Note:** VID 1 is reserved for internal use.
3. Press **Enter**.
4. Type: **set mgmt vlan port=<**xx> where:

   xx = port(s) on the IONMM to be associated with the VID. If both ports are specified, they must be separated by a comma with no spaces (i.e., port=1,2). **Note:** IONMM port 1 is the lower port (farthest from the USB connector) and port 2 is the upper port (closest to the USB connector).
5. Press **Enter**.
6. Enable Management VLAN. Type set mgmt vlan state=enable and press Enter.
7. Verify the configuration has been set. Type **show mgmt vlan config** and press **Enter**.
   The Management VLAN configuration table displays. For example:

```
Agent III C1|S1|L1D>set mgmt vlan vid 10
Agent III C1|S1|L1D>set mgmt vlan port=1,2
Agent III C1|S1|L1D>set mgmt vlan state enable
Agent III C1|S1|L1D>show mgmt vlan config
vlan id   vlan state          vlan portlist
--------------------------------------------------------------------------
10        enable              1,2
Agent III C1|S1|L1D>
```

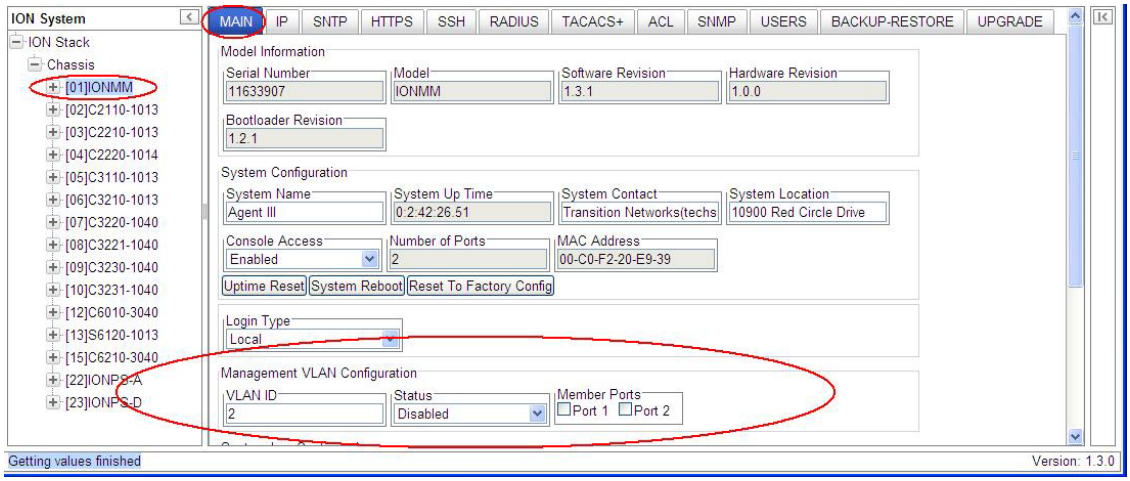
The example above places the IONMM in VLAN 10, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

Message:
Error: Cannot create VLAN database on this card!
Error: Cannot flush vlandb on this card!
Meaning: Displays if the function is not supported on the device or at this device's firmware version.
Recovery: Try another command, try the command on another device, or change firmware versions.

Management VLAN Config – Web Method

Note before performing this configuration: When you specify a Management VLAN, your Web and Telnet interfaces to the IONMM are lost, unless the management station (PC) is on the same VLAN. Only management stations in the same VLAN can communicate with the IONMM through the network. Enabling a Management VLAN does not disable a USB serial interface to the IONMM.

1. Access the IONMM through the Web interface (see" Starting the Web Interface").
2. Select the **MAIN** tab.
3. Locate the **Management VLAN Configuration** section.



4. In the **VLAN ID** field, enter the VLAN ID number (2–4094).
5. In the **Status** field, select **Enabled**.
6. In the **Member Ports** field, select the port(s) that will be associated with the VID.
7. Click the **Save** button when done.

This places the NID in the VLAN specified, allowing the member ports (Ethernet connections) selected in step 6 to receive management traffic only from devices that are also in the specified VLAN.

When configuring a VLAN on the C4221 through the IONMM, set the membership of each port to either ***noMod*** (traffic with the configured VLAN tag # can ingress and egress that port) or ***notMember*** (traffic with the configured VLAN tag will not be allowed to ingress or egress that port).

Message: "*Setting values failed (snmp operation error, possible reasons: invalid data, error data sequence, etc)*" displays if Status is Enabled but no ports are selected when a save is made.

Configuring RADIUS

Remote Authentication Dial In User Service (RADIUS) is a client/server protocol that runs in the application layer. Using the User Datagram Protocol (UDP) as transport, RADIUS enables remote access servers (referred to as clients) to communicate with a central server to authenticate users and authorize their access to the requested system or service.

Transactions between the client (IONMM) and RADIUS server are authenticated using a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the IONMM and RADIUS server.

From the user's perspective, the entire authentication process takes place seamlessly and transparently. When the user seeks access to the IONMM, the management module, acting as the RADIUS client, notifies the RADIUS server. The RADIUS server then:

- Looks up the user's security information.
- Passes authentication and authorization information between the appropriate authentication server(s) and the IONMM.
- Logs, by means of the RADIUS accounting feature, such information as when, how often, and for how long the user logged on.

The IONMM submits an access-request to the RADIUS server via the network. If no response is returned within a specified length of time (timeout value), the request is re-sent a specified number of times (retry limit).

The IONMM can also forward requests to an alternate server or servers if the primary server is down or unreachable. Up to six RADIUS servers can be configured. The additional servers are only contacted if communication with the first server is lost, then the request is routed to the second server, and so on.

RADIUS can be configured in the IONMM using either the CLI or Web method.

IMPORTANT

After configuring the IONMM for RADIUS, you will be required to enter the RADIUS defined username and password to connect to the IONMM.

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on ION and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format that can be modified to work with any security system currently available on the market. RADIUS can be configured with or without TACACS+ configuration.

The RADIUS server can be an IPv4 address, an IPv6 address, or a DNS name. The RADIUS server has strict priorities. If IPv6 is enabled, the device will try to authenticate to the RADIUS servers one by one, based on their priorities, until it gets a response, whether it is an IPv4 address, an IPv6 address or a DNS name. But if IPv6 is disabled, the IPv6 address RADIUS servers will be ignored. Up to six RADIUS servers are supported on one device.

The provided **RADIUS Client** works on both IPv4 and IPv6. The selected RADIUS **Server Address** entry can be IPv4, IPv6, or a combination of both.

RADIUS Config – CLI Method

Note: This procedure will end your current session, and you must then log in using your RADIUS log in and password. After configuring the IONMM for RADIUS, you will be required to enter the RADIUS defined username and password when connecting to the IONMM.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Define a single RADIUS server. Type:

   set radius svr=<vv> **type=**<ww> **addr=**<xx> [**retry=**<yy>] [**timeout=**<zz>]

   where:

   vv = server number (1–6)

   ww = IP address format; valid choices are:
   - **ipv4** (32-bit address format)
   - **dns** (domain name address format)
   - **ipv6** (ipv6 addressing format)

   xx = RADIUS server IP address

   yy = optional; number of times the access request will be resent to the server before being discarded or re-directed to another server. The factory default is 5.

   Zz = optional; number of seconds to wait for a response from the RADIUS server before re-sending the request. The factory default is 60.
3. Define a secret. Type: **set radius svr=<**xx> **secret=<**yy>

   where:

   xx = server number (enter the same as entered in step 2).

   Yy = the secret that you set up in the RADIUS server. The secret is used to validate communications. Maximum length of the secret is 128 characters.
4. Press **Enter**.
5. Repeat Steps 3–4 for each server to be defined. Up to six servers can be defined in the system.
6. Verify the configuration has been set. Type: **show radius config**
7. Press **Enter**. The RADIUS Configuration table information displays:

```
Agent III C1|S1|L1D>set radius svr=1 type=ipv4 addr=192.168.1.30 retry=2 timeout=15
Agent III C1|S1|L1D>set radius svr=1 secret=private
Agent III C1|S1|L1D>set radius client state=enable
Agent III C1|S1|L1D>show radius config
RADIUS client state:          disable

RADIUS authentication server:
index     addr-type      addr           retry     timeout
-------------------------------------------------------------------------
1         dns            0.0.0.0        3         30
2         dns            0.0.0.0        3         30
3         dns            0.0.0.0        3         30
```

```
4          dns              0.0.0.0         3          30
5          dns              0.0.0.0         3          30
6          dns              0.0.0.0         3          30
Agent III C1|S1|L1D>
```

8. Enable RADIUS. Type:

   set radius client state=enable

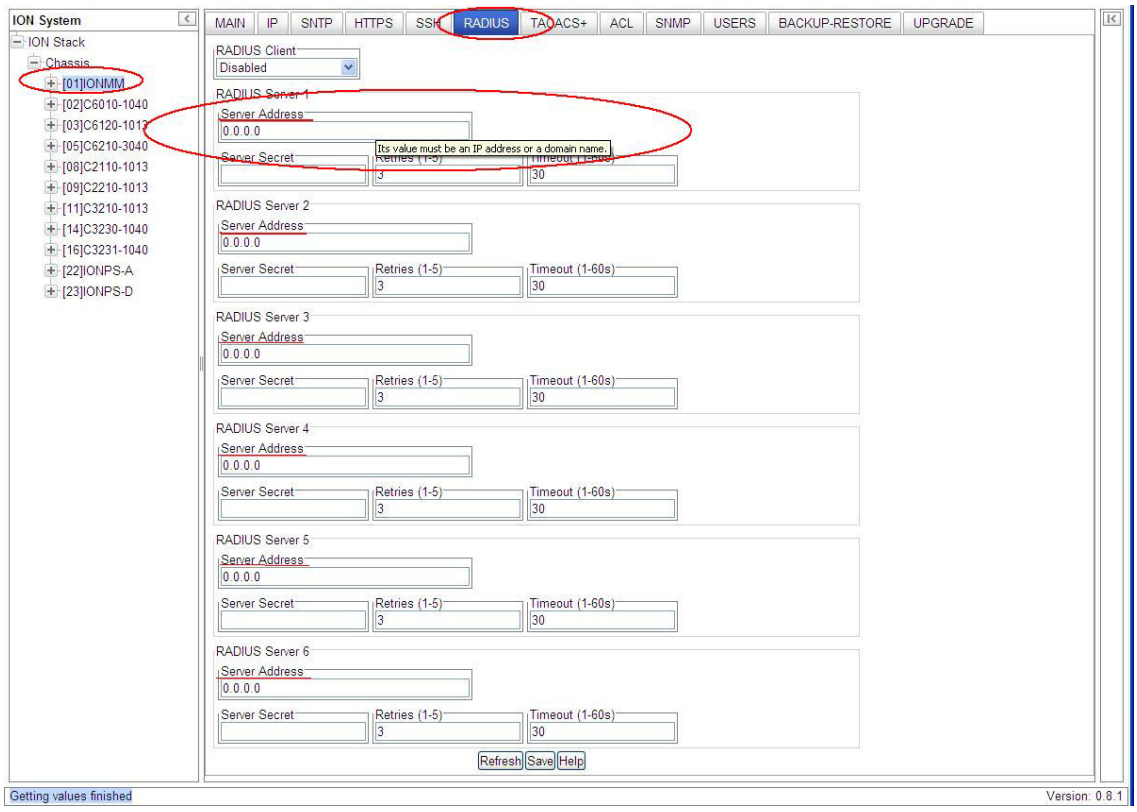
9. Press **Enter**.

   Your current session will be lost, and you must log in using your RADIUS log in and password.

RADIUS Config – Web Method

Note: This procedure will end your current session, and you must then log in using your RADIUS log in and password.

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **RADIUS** tab.



3. In the **Radius Client** field, select **Enabled**. The default is **Disabled**.
4. Configure the RADIUS server.
   - In the **Radius Server** field, enter the IP address of the RADIUS server.
   - In the **Server Secret** field enter the secret that you set up in the RADIUS server. The secret is used to validate communications. The maximum length of the secret is 128 characters.

- In the **Retries** field enter the number of times the access request will be re-sent to the server before being discarded or re-directed to another server. The factory default is 5. The valid range of entries is from 1-5 retries.
- In the **Timeout** field enter the number of seconds to wait for a response from the server before re-sending the request. The factory default is 60. The valid range of entries is from 1-60 seconds.

5. Repeat step 4 for each RADIUS server to be defined.
6. When all the RADIUS Servers have been defined, click **Save**.
   The message "*The RADIUS settings have been changed and a re-login will be performed right now.*" displays.
7. Click the **OK** button.
8. The new sign in message displays: "*Sign in to ION System Web Interface (RADIUS)*".
9. Enter the new User Name and Password and then click the **Sign in** button.
10. If your web browser displays a Certificate Error, follow the on-screen instructions. See the Troubleshooting section for specific error messages.

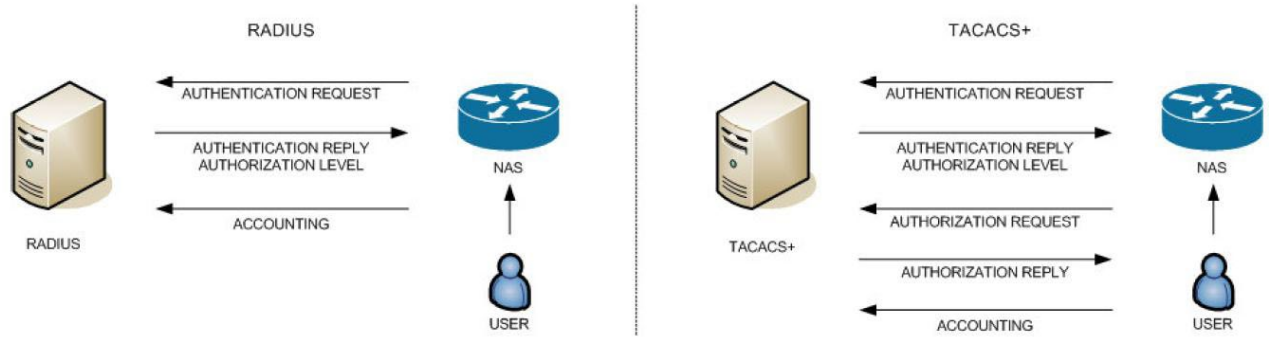
Configuring TACACS+

TACACS+ (Terminal Access Controller Access Control System) provides routers and access servers with authentication, authorization and accounting services. TACACS+ is used along with or as a replacement for RADIUS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Some administrators recommend using TACACS+ because TCP is seen as a more reliable protocol. While RADIUS combines authentication and authorization in a user profile, TACACS+ separates the authentication and authorization operations.

By default, TACACS+ (also referred to as “Tacplus”) listens on TCP port 49 and provides network devices with authentication, authorization and accounting services (AAA). TACACS+ can be configured with or without RADIUS configuration.

Note that when refreshing the TACACS+ page, all shared secrets display as "********". This is by design for all types of passwords. This is typically caused by adding letters after the "*" and then refreshing the page. After a refresh, just '********' displays instead of the password which was previously set. Thus after refresh, if you add some letters following the previous password (actually is '********' now), the'********' and added letters will be saved. This is the standard mechanism for all passwords in the ION web interface.

TACACS+ (Terminal Access Controller Access Control System) provides routers and access servers with authentication, authorization and accounting services. TACACS+ is used along with or as a replacement for RADIUS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Some administrators recommend using TACACS+ because TCP is seen as a more reliable protocol. While RADIUS combines authentication and authorization in a user profile, TACACS+ separates the authentication and authorization operations.
By default, Tacplus listens on TCP port 49 and provides network devices with authentication, authorization and accounting services (AAA).



A TACACS+ session is a single authentication sequence, a single authorization exchange, or a single accounting exchange.

Authentication is the action of determining who a user (or entity) is.

Authorization is the action of determining what a user is allowed to do. Authentication typically precedes authorization but is not required to.

Accounting involves recording what a user is doing, and/or has done. Accounting in TACACS+ can be used to account for services used, such as in a billing environment, and as an auditing tool for security services.

A TACACS+ session is maintained between the TACACS+ client and 'daemon'; however, it does not necessarily correspond to a given user or user action.

The privilege level (priv_lvl) indicates what the user is authenticating as. Privilege levels are values from 0 to 15 with each level representing a privilege level that is a superset of the next lower value.
The type of authentication (authen_type) indicates what is being performed. Values can include ASCII, PAP, CHAP, ARAP, and MSCHAP.

The current authentication status values can include PASS, FAIL, GETDATA, GETUSER, GETPASS, RESTART, ERROR, and FOLLOW.

The authen_method indicates the authentication method used by the client to acquire the user information. These methods can include NOT_SET, NONE, KRB5, LINE, ENABLE, LOCAL, TACACSPLUS, GUEST, RADIUS, KRB4, and RCMD.

- KRB5 and KRB4 are Kerberos version 5 and 4.
- LINE refers to a fixed password associated with the line used to gain access.
- LOCAL is a NAS local user database.
- ENABLE is a command that authenticates to grant new privileges.
- TACACSPLUS is TACACS+.
- GUEST is an unqualified guest authentication, such as an ARAP guest login.
- RADIUS is the Radius authentication protocol.
- RCMD refers to authentication provided by R-command protocols from Berkeley Unix. (Note the security limitations with R-command authentication.)

TACACS+ can be configured via the CLI or Web interface.

TACACS+ Config - CLI Method

These commands are used by the IONMM or a standalone SIC for TACACS+ configuration.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Enable TACACS+. Type **set tacplus client state=enable** and press **Enter**.
3. Set the TACACS+ server type. Type **set tacplus svr 1 type= *ipv4*|*ipv6*|*dns*** and press **Enter**.
4. Set the number of retry attempts to be made before quitting. Type: **set tacplus svr 1 retry**=<1-5> and press **Enter**.
5. Define the TACACS+ secret (password) to be used. Type **set tacplus svr 1 secret**= SECRET and press **Enter**.
6. Set the number of timeouts to be included. Type: **set tacplus svr 1 timeout**=<1-60> and press **Enter**.
7. Verify the TACACS+ settings. Type **show tacplus config** and press **Enter**.
8. Set the user login levels. Type:
   set login method=(local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal) and press **Enter**. This is the order in which the user attempts logins.
9. Verify the settings. Type **show tacplus config** and press Enter. For example:

```
Agent III C1|S1|L1D>set tacplus svr 1 ?
  retry
```

```
  secret
  timeout
  type
Agent III C1|S1|L1D>set tacplus svr 1 retry 2
Agent III C1|S1|L1D>set tacplus svr 1 secret ********
Agent III C1|S1|L1D>set tacplus svr 1 timeout 25
Agent III C1|S1|L1D>set tacplus svr 1 type ?
  ipv4
  ipv6
  dns
Agent III C1|S1|L1D>set tacplus svr 1 type ipv6 addr fe80::2c0:f2ff:fe21:b100
Agent III C1|S1|L1D>show tacplus config
TACPLUS client state:         enable

 TACPLUS authentication server:
index   type    addr                                retry  timeout
-------------------------------------------------------------------
1       ipv6    fe80::2c0:f2ff:fe21:b100            2      25
2       dns     0.0.0.0                             3      30
3       dns     0.0.0.0                             3      30
4       dns     0.0.0.0                             3      30
5       dns     0.0.0.0                             3      30
6       dns     0.0.0.0                             3      30
Agent III C1|S1|L1D>
```

TACACS+ Messages

Message:
Error: The parameter is wrong!
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!"
Fail to get system user name!
Fail to set TACPLUS client state!
Fail to set Tacplus server address type!
Fail to set TACPLUS server address!
Fail to set TACPLUS server retry
Fail to set TACPLUS server time out!
Fail to set TACPLUS server row status!
Fail to set TACPLUS server time out!
Getting TACPLUS server fail
Invalid TACPLUS server address!
Please input a digital number to specify radius server index!
Please input a digital number to specify RADIUS server retry!
Please input a digital number to specify tacplus server time out!
Please input a digital number to specify TACPLUS server retry!
Please input a digital number to specify TACPLUS server time out!
Please input a digital number to specify tacplus server index!
Please input a digital number to specify TACPLUS server index!
Please input a number to specify the TACPLUS server index!
Set TACPLUS server secret
TACPLUS authentication server index is out of range!

TACPLUS server retry is out of range!
TACPLUS server time out is out of range!
The ipv6 address is multicast address
The TACPLUS authentication server specified does not exist!
Wrong parameter number!
Meaning: You entered a TACACS+ (Tacplus) command, but the command was unsuccessful.
Recovery:
1. Make sure you enter the TACACS+ command on an IONMM or a standalone SIC at the device level.
2. Make sure the TACACS+ client is enabled and that the TACACS+ server is correctly configured and running.
3. Make sure you enter the command parameters within the valid ranges and in the proper syntax.
4. Check the RADIUS configuration.
5. Retry the command. See the related manual or section.
6. Check your third party TACACS+ server documentation and helps (e.g., ClearBox Server, etc.).
7. If the problem persists, contact Technical Support.

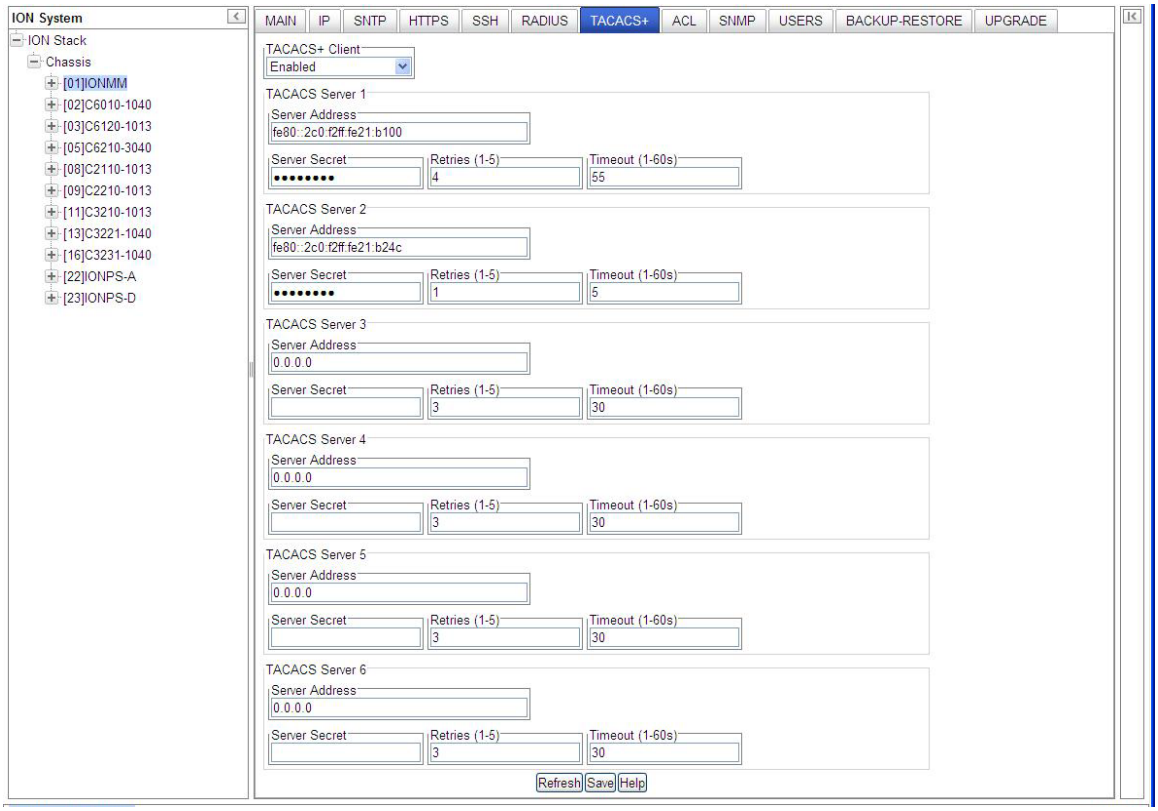
Message: *The TACACS+ settings have been changed and a re-login will be performed right now.*
Meaning: When you hit **Save** after any TACACS+ re-config a re-login is required.
Recovery:
1. Log back in to the system.
2. Enter the **show tacplus config** command and verify the TACACS+ configuration settings.

TACACS+ Syslog Messages
Tacplus logs error messages to syslog, and informational messages to facility LOG_LOCAL6. Debug messages are not sent to syslog. Note that that syslogd provides little in the way of diagnostics when it encounters errors in the *syslog.conf* file.

syslog (LOG_ERR, "error sending auth req to TACACS+ server")
syslog(LOG_ERR, "error sending continue req to TACACS+ server")
syslog (LOG_ERR, "auth failed: %d", msg)
syslog (LOG_ERR, "auth failed: %d", msg)
syslog (LOG_INFO, "Tacplus daemon fail to get message from messageQ.")
"STATUS_INVALID, should be session reset, Reregister from begining\n"
"Fail for sending ionDevSysUserLoginMethodObjects,ignored...\n"
"Number of subid is not correct when ionDevSysUserLoginMethodObjects_com, expect %d, get %d \n"
"agentx_mapset Error"
"agentx_ot_add Error"

TACACS+ Config - Web Method

1. From the IONMM, navigate to the **TACACS+** tab.



2. At the **TACACS+ Client** dropdown, select **Enabled**. The default is **Disabled**.
3. At the **TACACS Server 1** Server Address, enter a valid IPv4 or IPv6 address. For this TACACS+ server, enter:

   Server Secret: enter a server secret (password); the entry displays as a series of •••• characters. This is a string well known to both client and server and is used to validate and/or encrypt data, transmitted between them.

   Retries (1-5): enter the number of connection attempts before quitting further attempts.

   Timeout (1-60s): The number of seconds to wait for a response from the TACACS+ server before re-sending the request. After a timeout, the TACACS+ client may retry to the same TACACS+ server, send to a different server, or give up. The default is 30 seconds. The valid range of entries is from 1-60 seconds.
4. At the **TACACS Server 2-6** Server Address, enter valid IPv4 or IPv6 address(es). For each TACACS+ server, enter **Server Secret**, **Retries (1-5)**, and **Timeout (1-60s)** values. Configure up to six TACACS Servers per steps 1-2 above.
5. Click the **Save** button when done.

Configuring SNTP

Simple Network Time Protocol (SNTP) is derived directly from the Network Time Protocol (NTP). SNTP synchronizes the system time on a network element with that of a server that has been synchronized by a reference source such as a radio, satellite receiver, or modem. SNTP is used in scenarios that do not require or justify the high performance and accuracy of NTP.

SNTP can operate in unicast, multicast, and anycast modes. A unicast client sends a request to a designated server at the server unicast address and expects a reply from which it can determine the time and, optionally, the round trip delay, and the local clock offset relative to the server. A multicast server periodically sends an unsolicited message to a designated local broadcast address, or to a multicast group address. A multicast client listens on this address and sets its time accordingly. The client generally sends no requests on to a multicast service because a request could get disrupted by untrusted SNTP or NTP multicast servers. You can prevent disruption by an untrusted server by using an access control mechanism to choose only the designated server known to, and trusted by, the client.

The IONMM supports only client implementations of SNTP. You can use the client implementation of SNTP to synchronize the clock on the IONMM to up to six SNTP servers.

SNTP is a simplified, client-only version of NTP used on ION. SNTP can only receive the time from an NTP server; it cannot be used to provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP.

The SNTP server can be an IPv4 address, an IPv6 address, or a DNS name. The SNTP server has strict priorities. If IPv6 is enabled, the device will try to sync time from the servers one by one, based on their priorities, until it gets a response, whether it is an IPv4 address, an IPv6 address, or a DNS name. The ION SNTP client will try once for each SNTP server address and wait 10 seconds for response. If the SNTP server is a DNS name and this name can be mapped to multiple IPv4 or IPv6 addresses, the ION SNTP client will try each address for 10 seconds. If no response is received, the ION SNTP client will try another server address. If IPv6 is disabled, the IPv6 address SNTP servers will be ignored. Up to six SNTP servers are supported on one device.

SNTP servers can be IPv6 type and IPv4 type. The two types can co-exist at one time. The priority is ordered by the service index.

SNTP can be configured in the IONMM using either the CLI or Web method.

SNTP Config – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Enable SNTP. Type: **set sntp state=enable**
3. Press **Enter**.
4. Set the current time. Type: s**et curr–time=<"**xx**"**> where:

   xx = the current date and time in the format "yyyy mmdd hh:mm:ss". **Note:** the entire string must be enclosed in quotes.
5. Press **Enter**.
6. Set your timezone and press **Enter**. Type: **set sntp timezone=<**xx> where:

   xx = a number (1-63) indicating the time zone from the table below.

Table 7: Timezones

Zone	Description
1	(GMT –12:00) Eniwetok, Kwajalein
2	(GMT –11:00) Midway, Island, Samoa
3	(GMT –10:00) Hawaii
4	(GMT –09:00) Alaska
5	(GMT –08:00) Pacific, Time, US, and, Canada, Tijuana
6	(GMT –07:00) Arizona
7	(GMT –07:00) Mountain, Time, US, and Canada
8	(GMT –06:00) Central, Time, US, and Canada
9	(GMT –06:00) Mexico, City, Tegucigalpa
10	(GMT –06:00) Saskatchewan
11	(GMT –05:00) Bogota, Lima, Quito
12	(GMT –05:00) Eastern, Time, US, and, Canada
13	(GMT –05:00) Indiana, East
14	(GMT –04:00) Atlantic, Time, Canada
15	(GMT –04:00) Caracas, La, Paz
16	(GMT –04:00) Santiago
17	(GMT –03:30) Newfoundland
18	(GMT –03:00) Brasilia
19	(GMT –03:00) Buenos, Aires, Georgetown
20	(GMT –02:00) Mid-Atlantic
21	(GMT –01:00) Azores, Cape, Verde, Is
22	(GMT) Casablanca, Monrovia
23	(GMT) Greenwich, Mean, Time, Dublin, Edinburgh, Lisbon, London
24	(GMT +01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
25	(GMT +01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
26	(GMT +01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius
27	(GMT +01:00) Sarajevo, Skopje, Sofija, Warsaw, Zagreb
28	(GMT +02:00) Athens, Istanbul, Minsk
29	(GMT +02:00) Bucharest
30	(GMT +02:00) Cairo

Zone	Description
31	(GMT +02:00) Harare, Pretoria
32	(GMT +02:00) Helsinki, Riga, Tallinn
33	(GMT +02:00) Jerusalem
34	(GMT +03:00) Baghdad, Kuwait, Riyadh
35	(GMT +03:00) Moscow, St, Petersburg, Volgograd
36	(GMT +03:00) Nairobi
37	(GMT +03:30) Tehran
38	(GMT +04:00) Abu, Dhabi, Muscat
39	(GMT +04:00) Baku, Tbilisi
40	(GMT +04:30) Kabul
41	(GMT +05:00) Ekaterinburg
42	(GMT +05:00) Islamabad, Karachi, Tashkent
43	(GMT +05:30) Bombay, Calcutta, Madras, New, Delhi
44	(GMT +06:00) Astana, Almaty, Dhaka
45	(GMT +06:00) Colombo
46	(GMT +07:00) Bangkok, Hanoi, Jakarta
47	(GMT +08:00) Beijing, Chongqing, Hong, Kong, Urumqi
48	(GMT +08:00) Perth
49	(GMT +08:00) Singapore
50	(GMT +08:00) Taipei
51	(GMT +09:00) Osaka, Sapporo, Tokyo
52	(GMT +09:00) Seoul
53	(GMT +09:00) Yakutsk
54	(GMT +09:30) Adelaide
55	(GMT +09:30) Darwin
56	(GMT +10:00) Brisbane
57	(GMT +10:00) Canberra, Melbourne, Sydney
58	(GMT +10:00) Guam, Port, Moresby
59	(GMT +10:00) Hobart
60	(GMT +10:00) Vladivostok
61	(GMT +11:00) Magadan, Solomon, Is, New, Caledonia
62	(GMT +12:00) Auckland, Wllington
63	(GMT +12:00) Fiji, Kamchatka, Marshall, Islands

7. Do you want to set daylight savings time (DST)?

Yes	**No**
Continue with step 8.	Go to step 16.

8. Enable DST. Type: **set sntp dst–state=enable**
9. Press **Enter**.
10. Set the date and time that DST is to start. Type: **set sntp dst–start=<“**xx**”>**

where:

xx = the date and time DST is to begin in the format “yyyy mmdd hh:mm”. **Note:** the entire string must be enclosed in quotes.

11. Press **Enter**.
12. Set the date and time that DST is to end. Type: **set sntp dst–end=<“**xx**”>**

    where:

    xx = the date and time DST is to end in the format “yyyy mmdd hh:mm”. **Note:** the entire string must be enclosed in quotes.

13. Press **Enter**.
14. Set the amount of time that clocks are to shift because of daylight savings. Type:

    set sntp dst–offset=<xx>

    where:

    xx = number of minutes (1–720) indicating the time shift. **Note:** the usual time shift is one hour (60 minutes).

15. Press **Enter**.
16. Define the IP address of the SNTP server.
    Type: **set sntp–svr svr=<**xx> **type=<**yy> **addr=<**zz> **retry** = ww

    where:

    xx = number (1–6) of the SNTP server being defined

    yy = IP address format; valid choices are:

    - **ipv4** (32-bit address format)
    - **dns** (domain name address format)
    - **ipv6** (extended ipv6 address format)

    zz = IP address of the SNTP server

    ww = optional number of retry attempts.

17. Press **Enter**.
18. Verify the configuration has been set. Type: **show sntp config**
19. Press **Enter**. The SNTP Configuration displays. For example:

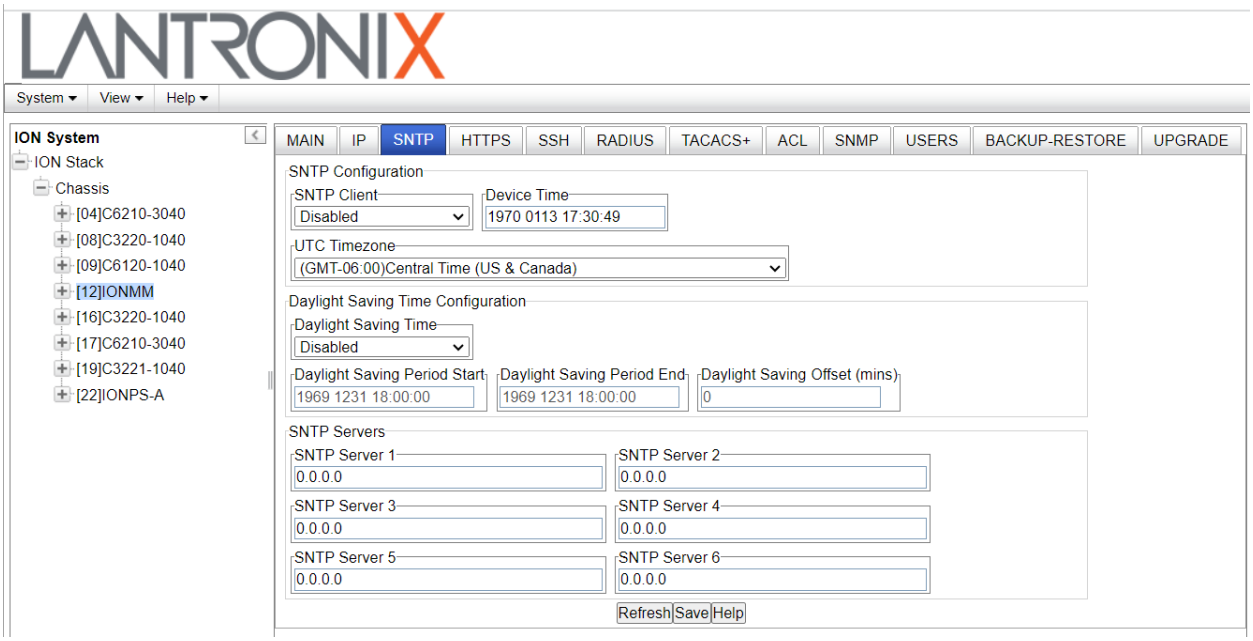
```
C1|S3|L1D>set sntp state=enable
C1|S3|L1D>set curr-time=”20100106 13:15:30”
C1|S3|L1D>set sntp timezone=8
C1|S3|L1D>set sntp dst-state=enable
C1|S3|L1D>set sntp dst-start=”20100307 02:00:00”
C1|S3|L1D>set sntp dst-end=”20101107 02:00:00”
C1|S3|L1D>set sntp dst-offset=60
C1|S3|L1D>set sntp-svr svr=1 type=ipv4 addr=192.168.1.20
C1|S3|L1D>show sntp config
SNTP configuration:
```

```
------------------------------------------------------------------------
SNTP state:                             enable
SNTP daylight saving time state:        enable
Sntp timezone:                          (GMT-6:00) Central Time US and Canada
Current time:                           2010 0106 13:15:30
Sntp daylight saving start time:        2010 0307 02:00:00
Sntp daylight saving end time:          2010 1107 02:00:00
sntp daylight saving offset:            60

Sntp server:
index               addr-type           address
------------------------------------------------------------------------
1                   ipv4                192.168.1.20
2                   dns                 0.0.0.0
3                   dns                 0.0.0.0
4                   dns                 0.0.0.0
5                   dns                 0.0.0.0
6                   dns                 0.0.0.0
C1|S1|L1D>set curr-time ?
  STR_CURR_TIME  The value of current time should time should follow this format,
  "YYYY MMDD HH:MM:SS", such as "1999 1211 13:22:34".
C1|S1|L1D>
```

Messages: *When SNTP state is enabled, you cannot set current time!*

SNTP Config – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **SNTP** tab.



3. In the **SNTP Client** field select **Enabled**.
4. In the **Device Time** field, enter the current time in the format **yyyy mmdd hh:mm:ss**.
5. In the **UTC Timezone** field, select your timezone (e.g., zone 12 (GMT –05:00) Eastern, Time, US, and Canada).
6. If you want to set daylight savings time (DST), continue with step 7 below.
   If you do not want to set daylight savings time (DST), continue with step 11 below.
7. In the **Daylight Saving Time** field select **Enabled**.
8. In the **Daylight Saving Period Start** field, enter the DST start date and time in the format yyyy mmdd hh:mm:ss.
9. In the **Daylight Saving Period End** field, enter the DST end date and time in the format yyyy mmdd hh:mm:ss.
10. In the **Daylight Saving Offset (mins)** field, enter the DST offset in minutes (1–720); usually 60 minutes.
11. Enter the IPv4 or IPv6 address or domain name of each SNTP server (e.g., 192.168.1.30). Up to six SNTP servers can be configured.
12. 12. Click **Save** when done.
13. If the SNTP Server configuration is modified, for example changing Daylight Saving offset, it must be disabled and re-enabled for the new configuration to take effect.

Configuring SSH

Secure Shell (SSH), sometimes known as Secure Socket Shell or Secure Telnet, is a Unix-based command interface and protocol used for securely getting access to a remote device. SSH can be used as a security option when accessing the IONMM through a Telnet session.

The Secure Shell (SSH) application / protocol provides a secure replacement for the Berkeley r-tools. The SSH protocol secures the sessions using standard cryptographic mechanisms, and SSHv2 can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. The SSH server can support both IPv4 and IPv6 at the same time. The ION system supports up to 16 SSH sessions.

IMPORTANT

- You must install an SSH client on the management station to access the IONMM for management via the SSH protocol.
- SSH has no affect when accessing the IONMM through either the USB or the Web interface.
- 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 is 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 to use it.
  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.

For ION Systems, SSH can be configured for either Login/Password authentication or Public/Private key and Certificate authentication.

For Login/Password, you must establish the SSH login and password in the SSH client. When logging in to the IONMM you will be required to first enter the SSH login and password then the ION System password.

For Public/Private key and Certificate, SSH commands are encrypted and secured in several ways. Both ends of the client/server connection are authenticated using a digital certificate provided by the administrator and passwords are encrypted to prevent interception. Once a password is given and verified a session will be created and SSH will issue a unique digital signature (or private key) associated with that session. To make a secure connection, SSH must be installed, activated, and certificates must be given to both the source machine and the IONMM. For SSH implementation, the IONMM can support and will generate both the Rivest-Shamir-Adleman (RSA) and Digital Signature Algorithm (DSA) for public key cryptography for both connection and authentication.

When using the SSH client to login to ION, both the userid and password are not fixed.

Note: The ION system provides a temporary certificate and key, but they must be updated with a permanent version for production use (e.g., from Verisign, DigiCert, Thawte, etc.).

SSH can be configured in the IONMM using either the CLI or Web method.

SSH Config – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Enable SSH. Type: **set ssh server state=enable**
3. Is SSH being configured for Login/Password authentication or Public/Private key and Certificate?

Login/Password	Public/Private key and Certificate
End of procedure.	Continue with step 4.

4. Press **Enter**.
5. Set the timeout value. Type: **set ssh client timeout=**<xx> where:

   xx = number, 1–120, of seconds to wait for a response before timing out
6. Press **Enter**.
7. Set the retry limit. Type: **set ssh auth–retry=**<xx> where:

   xx = number, 1–5, of retries that will be attempted before dropping the connection.
8. Generate the host public key. Type: **generate ssh host–key=**<xx> where:

   xx = type of key to be generated; valid choices are:
   - **rsa**
   - **dsa**
   - **both**
9. Obtain the public key file. This file should be obtained by doing a TFTP **get** command.
10. Associate the public key with a user. Type: **set ssh public–key user=**<xx> **type=**<yy> **file=**<zz>

    where:

    xx = name of a user to be associated with the key.

    yy = type of key to be associated with the user; valid choices are:
    - **rsa**
    - **dsa**

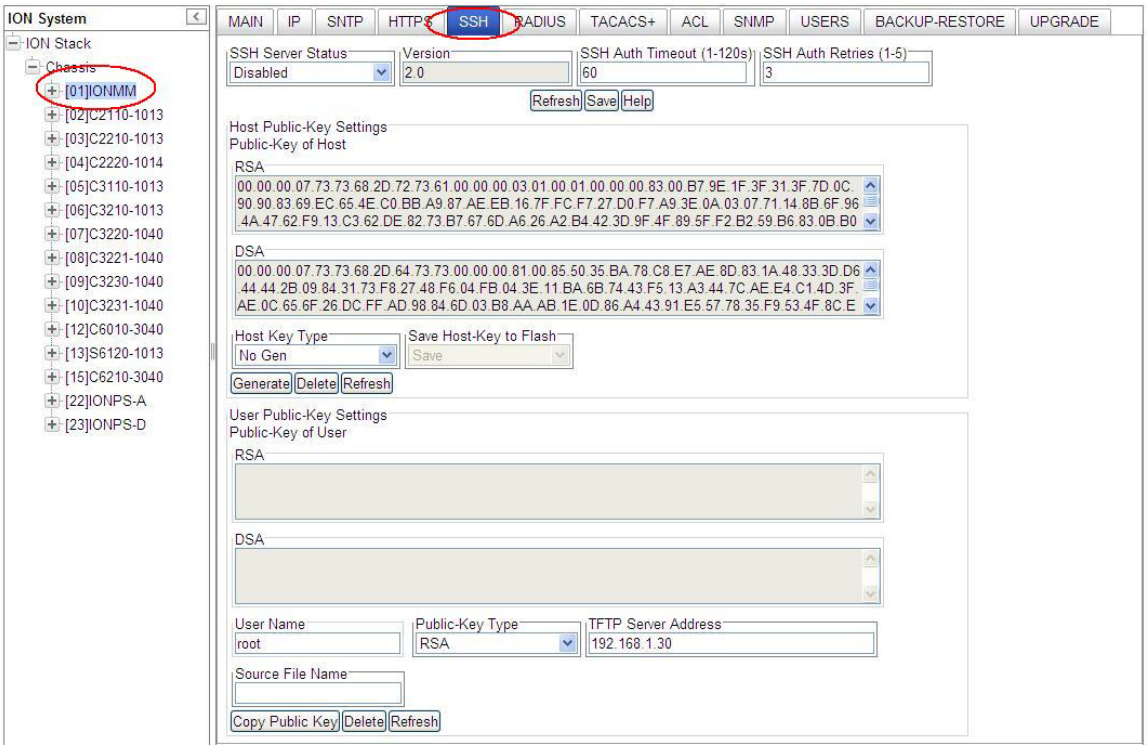
    zz = name of the file that contains the public key
11. Press **Enter**.
12. Verify the configuration has been set. Type: **show ssh config**.

13. Press **Enter**. The SSH configuration displays:

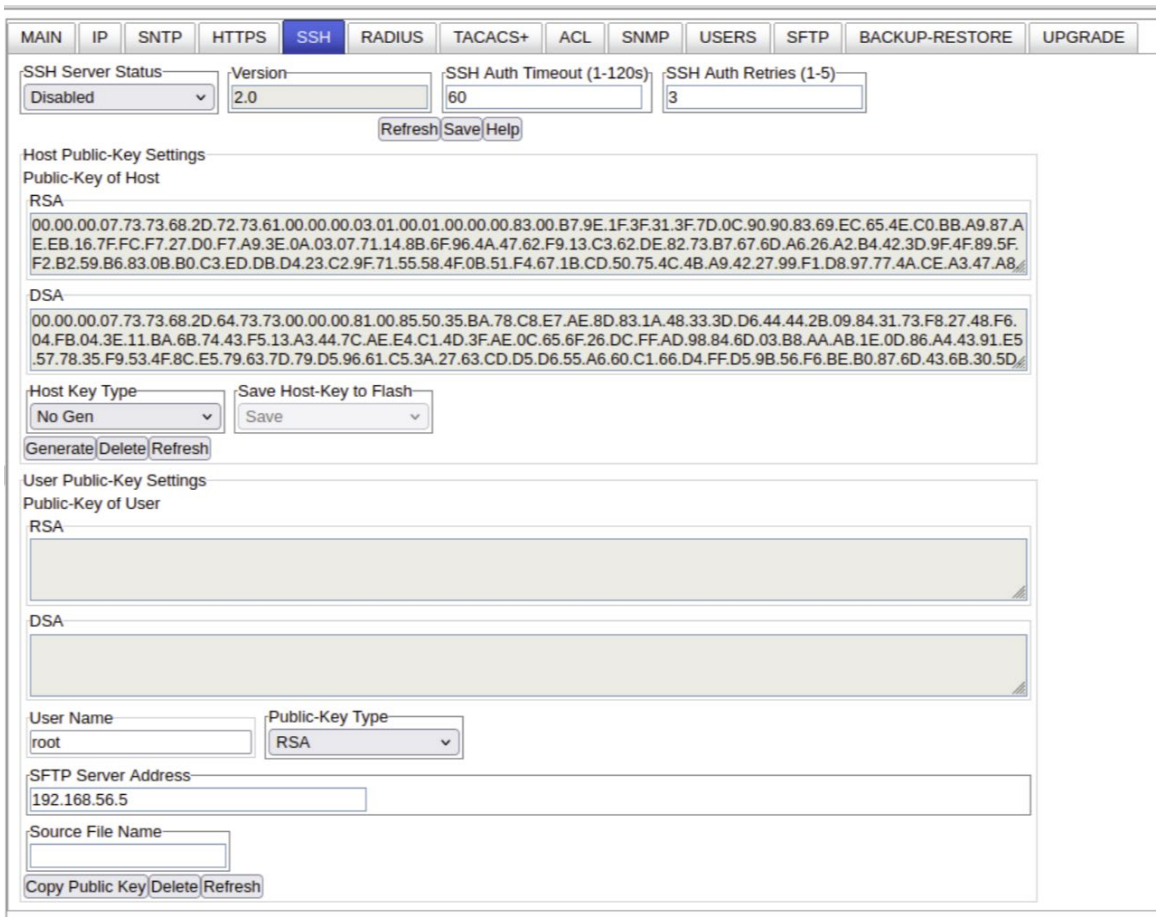
```
Agent III C1|S1|L1D>set ssh server state=enable
Agent III C1|S1|L1D>set ssh client timeout=15
Agent III C1|S1|L1D>set ssh auth-retry=3
Agent III C1|S1|L1D>generate ssh host-key=both
Processing...
Processing...
Host-key generated!
C1|S3|L1D>set ssh public-key user=agent type=dsa file=id_dsa.pub
Agent III C1|S1|L1D>show ssh config
Secure Shell configuration:
------------------------------------------------------------------------
Secure shell server state:                                  disable
Secure shell version:                                       2.0
Secure shell time out:                                      60
Secure shell authentication retries:                        3
Agent III C1|S1|L1D>
```

SSH Config – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **SSH** tab.



If SFTP is enabled, the SSH configuration page will display SFTP Server address.

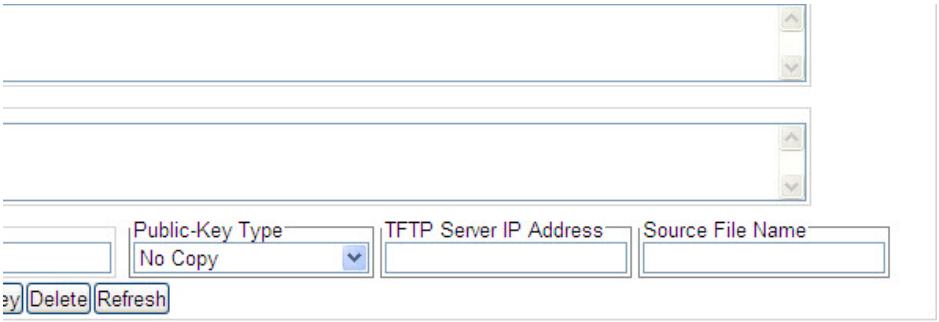


3. In the **SSH Server Status** field, select **Enabled**.
4. Is SSH being configured for Login/Password authentication or Public/Private key and Certificate?

Login/Password	**Public/Private key and Certificate**
Go to step 17.	Continue with step 5.

5. In the **Version** field, enter the version number of SSH being used.
6. In the **SSH Auth Timeout** field, enter the number of seconds that the IONMM will wait for a response before dropping the connection. This is the period, in seconds, that the router waits for the SSH client to respond. The valid range is 1-120 seconds. The default is 60 seconds.
7. In the **SSH AUTH Retries** field, enter the number of times that communication will be attempted before the connection is dropped. This is the number of attempts after which the interface is reset. The valid range is 1-5 retries. The default is 3 retries.

8. In the **Host Key Type** field, select the type of host key to be generated; valid choices are:
   - **No Gen** – no key will be generated (disables the function of SSH).
   - **RSA** – generate an RSA key (the generated key will display in the RSA block).
   - **DSA** – generate a DSA key (the generated key will display in the DSA block).
   - **Both** – generate both an RSA key and a DSA key.
9. In the **Save Host-Key to Flash** field, leave the field at **Not Save**; this is for future use.
10. Click **Generate**. The host key(s) is generated.
11. Scroll down to the **User Public-Key Settings** section.



12. In the **User Name** field, enter the name of the user to be associated with the user public key.
13. In the **Public-Key Type** field, select one of the following:
    - **No Copy**
    - **RSA**
    - **DSA**
14. In the **TFTP/SFTP Server Address** field, enter the IP address of your TFTP/SFTP server.
15. In the **Source File Name** field, enter the name of the file.
16. Click **Copy Public Key**.
17. At the top of the screen, click **Save** to set the configuration when done.
    You can click the **Delete** button to delete the selected host key.
    You can click the **Refresh** button to refresh the displayed RSA / DSA host key information.

Configuring SSH and RADIUS

Certain requirements exist for using the ION Default Username/Password with SSH and RADIUS. Below are two typical application examples using RADIUS and/or SSH.

Example 1 Create a user with SSH via the ION CLI (SSH and RADIUS enabled):

1. Launch the SSH client.
2. Enter 'ION' – 'private' to log in to SSH (the first time).
3. Enter the RADIUS user and password to log in to RADIUS.
4. Add the 'TEST' (user name) – 'TEST111' (password) user (see Note below).
5. Close the SSH client.
6. Launch the SSH client again
7. Enter 'TEST' – 'TEST111' to log in to SSH.
8. Enter the RADIUS user and password to log in to RADIUS.

Example 2 Create a user with SSH via the ION CLI (SSH enabled but RADIUS disabled):

1. Launch the SSH client.
2. Enter 'ION' – 'private' to login to SSH (the first time).
3. Add 'TEST' (user name) – 'TEST111' (password) user (see Note below).
4. Close the SSH client.
5. Launch the SSH client again.
6. Enter 'TEST' – 'TEST111' to login via SSH.

Note: in the examples above, when adding a new user (step 3 or step 4 - add 'TEST' – 'TEST111' user), you can also modify the password of the user 'ION' and then use the user 'ION' and the new password to log in again.

Configuring System Logging (Syslog)

The IONMM and x323x devices support system logging via the Syslog function.

Syslog can be used for system management and security auditing, as well as generalized information, analysis, and message debugging. It is supported by a wide variety of devices and receivers across multiple platforms. Because of this, Syslog is used to integrate log data from many different types of devices into a central repository. The syslog protocol conveys event notification messages using a layered architecture, allowing a variety of transport protocols, and providing a message format of vendor-specific extensions to be provided in a structured way.

Note: Take care when updating the configuration; omitting or misdirecting message facility.level can cause important messages to be ignored by syslog or overlooked by the administrator.

Severity relates to the importance of a message. There are eight defined severity levels (0-7), listed in descending order from highest priority (0) to lowest priority (7).

Table 8: Syslog Severity Levels

Syslog Level (highest to lowest severity)	**Description**
Emergency	**0** - Emergency message or system failure. A "panic" condition - notify all tech staff on call (e.g., *earthquake, tornado*) - affects multiple apps/servers/sites.
Alert	**1** - Urgent problem, requiring immediate action. Should be corrected immediately - notify staff who can fix the problem (e.g., *loss of backup connection*).
Critical	**2** - Critical error conditions. Should be corrected immediately but indicates failure in a primary system - fix CRITICAL problems before ALERTs (e.g., *loss of primary connection*).
Error	**3** - Standard errors. Non-urgent failures - these should be relayed to developers or admins; each item must be resolved within a pre-set amount of time.
Warning	**4** - Warning conditions; system operation status events. Warning messages are not errors, but indications that an error will occur if action is not taken (e.g., *file system 85% full*). Each item must be resolved within a pre-set amount of time.
Notice	**5** - Standard operational events; events that should be looked at. Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required
Info	**6** - Status messages, notification of conditional program events. Informational: Normal operational messages; may be logged for reporting, measuring throughput, etc. - no action is required.
Debug	**7** - Debugging events and trace output. Info useful to developers for debugging the application, but not usually useful during operation.

Messages used to enable debugging or software testing are assigned Severity 7. Severity 0 is reserved for messages of very high importance (e.g., serious hardware failures or imminent power failure). Refer to your organizations policy administrator for this level of severity. Note that the syslog protocol does not provide for acknowledgment of message delivery. See “Syslog Messages and Sys.log Output” for more information.

ION uses the syslog protocol to manage system logs and alerts. ION lacks large internal storage space for storing these logs. To overcome this limitation, ION offers the following two options:

- **Internal buffer**— the device's operating system allocates a small part of memory buffers to log the most recent messages. The buffer size is limited to 2M. When the buffer is full, the new log will overwrite the old one. However, when the device reboots, these syslog messages are lost.
- **Syslog**— Use a UNIX-style SYSLOG protocol to send messages to an external device for storing. The storage size does not depend on the router's resources and is limited only by the available disk space on the external syslog server.

The Syslog server address is the only remote IP address entry that IPv4, IPv6, and DNS share in the ION system. When syslog mode is set to logRemote or logLocalAndRemote, this field is used.

The range of port is from 1 to 65535, and the available value of syslog mode can be:

- **logLocal**: syslog messages will only be recorded in local file system.
- **logRemote**: syslog messages will only be sent to remote syslog server.
- **logLocalAndRemote**: syslog messages will be recorded on local file system and remote syslog server.
- **off**: no syslog messages will be recorded.

When Syslog Level is set to a certain value such as err(4), only the syslog messages with higher priority will be recorded - in this example, emerg(1), alert(2), crit(3) and err(4) will be recorded.

When the log file's size is larger than 200k, new logs will rotate to overwrite the oldest logs.

System Logging (Syslog) can be configured via the CLI or the Web interface.

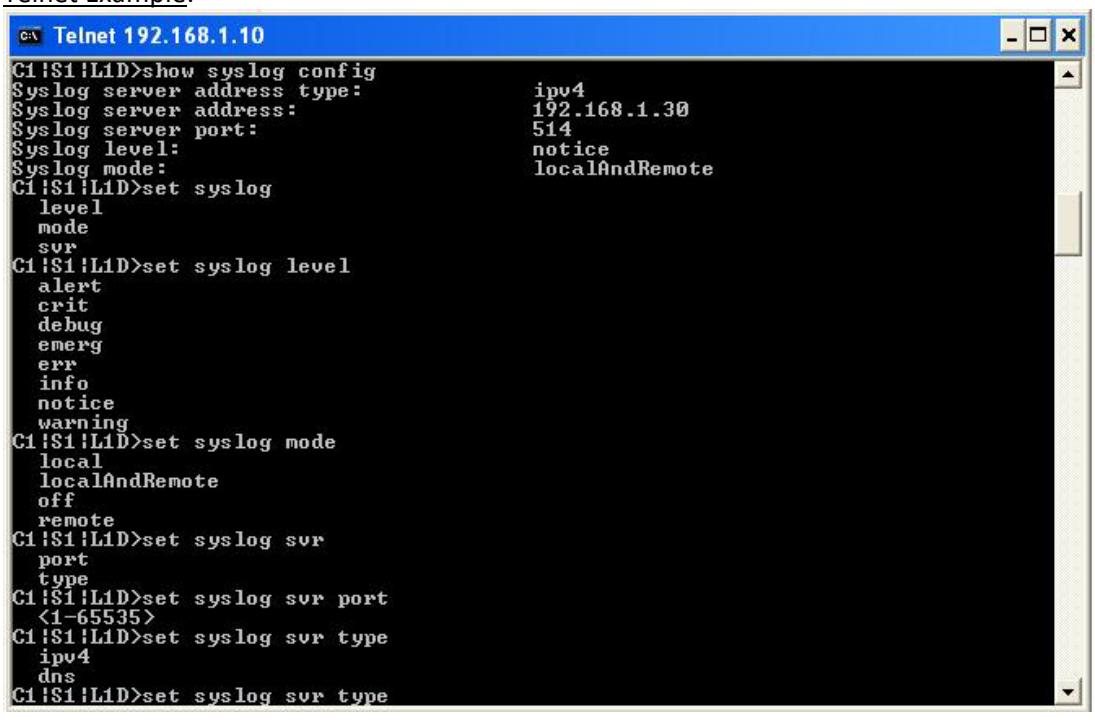
Syslog Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the device's command prompt type the following set of four CLI commands to define Syslog operations (the Syslog server address and port, and Syslog level and mode). Press the **Enter** key after each command.
   set syslog mode=(local/localAndRemote/off/remote)
   set syslog level=(alert/crit/debug/emerg/err/info/notice/warning)
   set syslog svr type=(ipv4|ipv6|dns) **addr**=SYSLOG_SVR_ADDR
   set syslog svr port=<1-65535>
3. Verify the Syslog configuration using the **show syslog config** command. For example:

```
Agent III C1|S1|L1D>show syslog config
Syslog server address type:             ipv4
Syslog server address:                  192.168.0.2
Syslog server port:                     514
Syslog level:                           info
Syslog mode:                            local
Agent III C1|S1|L1D>
```

   See Table 9 above for complete descriptions of the Syslog severity levels.
   You can use the clear syslog command to erase all existing records on the configured Syslog server.

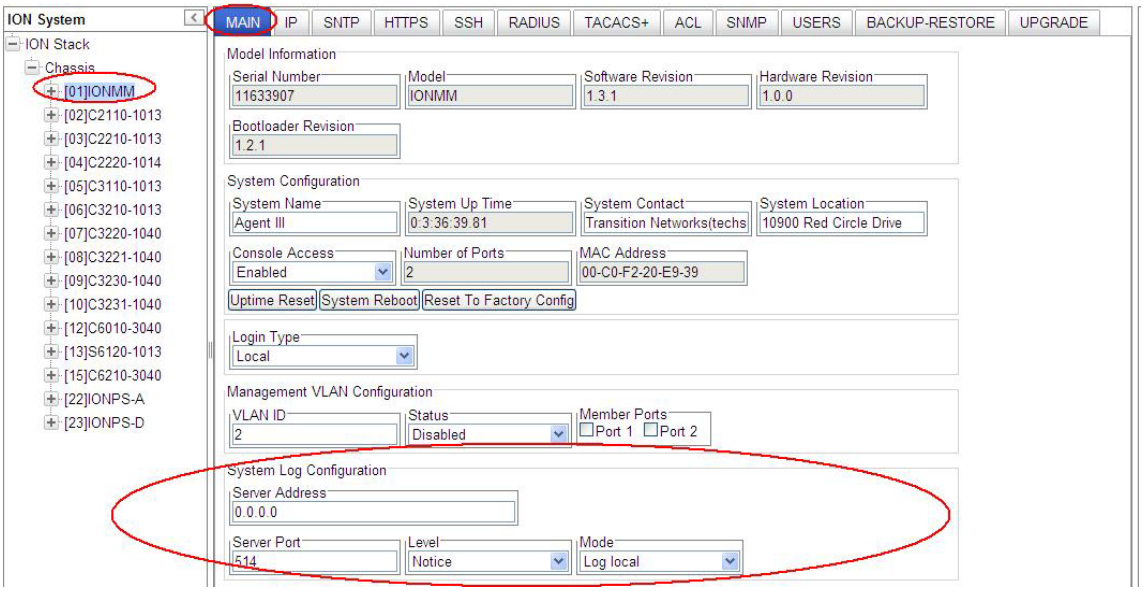
Telnet Example:



Syslog Config – Web Method

1. Access the IONMM or NID through the Web interface (see "Starting the Web Interface").

2. At the IONMM **MAIN** tab, locate the **System Log Configuration** section.



3. At the **System Log Configuration** section, define the IONMM Syslog configuration.

   Server Address - The address of the Remote Syslog server. enter a valid IPv4 or IPv6 address (e.g., 192.168.1.30 or fe80::2c0:f2ff:fe21:b243).
   Server Port – The remote syslog server listening port. The default is port 514. The valid range is port numbers 1-65535.
   Level – One of eight Syslog message severity levels. The enumeration values are equal to the values that syslog uses + 1; a messages with a severity level lower than or equal to this level will be logged.

Emergency	Emergency: system is unusable (most critical)
Alert	Action must be taken immediately
Critical	A critical condition exists
Error	Error condition
Warning	Warning condition
Notice	Normal but significant condition (default setting)
Info	Informational message
Debug	Debug-level messages (least critical)

   See Table 9 above for full Syslog severity level descriptions.

Mode – The current Syslog operating mode {"*Log local*", "*Log Remote*", "*Log Local and Remote*", and "*Off*"}:

Log local	Syslog messages are only saved to the local device;
Log Remote	Syslog messages are only sent to a remote server;
Log Local and Remote	Syslog messages are saved to a local device and sent to the Syslog remote server defined above;
Off	Do not save syslog messages. The Syslog function is disabled.

4. Verify the Syslog configuration.

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

See "Syslog Messages and Sys.log Output" for more Syslog information.

Configuring SNMP

The IONMM can act as an agent in an SNMP environment, enabling the IONMM to notify the management station of significant events within the network. Notification is done with traps, which are unsolicited messages sent to the management station in response to certain events that have taken place (e.g., warm start, etc.).

A full SNMP configuration can include:

1. **General** configuration (Community String, Access Mode, SNMP V3 Engine ID).
2. **Local Users** configuration (User Name, Group Name, Security Model, Security Level, Auth Protocol, Privacy Protocol, etc.).
3. **Groups** configuration (Group Name, Security Model, Security Level, Read/Write/Notify View).
4. **Views** configuration (View Name, OID Sub Tree / Type).
5. **Trap Hosts** configuration (Trap Version, Trap Manager, Port, Community String, Security Level, Trap/Inform, etc.).
6. **Remote Engines** configuration (optional - Address type, IP address, Port, and Engine ID).
7. **Remote Users** configuration (optional - Remote IP, Remote Engine ID, User Name, Group Name, Remote IP address, Security Model / Level, etc.).

Note:

1) Configure the local SNMPv3 Engine ID (in General tab) before you configure the Local Users. Otherwise, when you modify the SNMPv3 Local Engine ID, all SNMPv3 Local Users will be deleted.

2) Configure the SNMPv3 Remote Engine ID before you configure the Remote Users for this engine. Otherwise, when you modify the SNMPv3 Remote Engine ID, all SNMPv3 Remote Users will be deleted.

SNMP can be configured in the IONMM using either the CLI or Web method.

SNMP Config – CLI Method

This procedure is for a full SNMP configuration via CLI commands. Not all user applications will require all the steps below. For a full description of the individual commands see "SNMP v3 Commands".

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Define the General configuration. For example, type:

```
add snmp community name xxxxxxx access_mode={read_only|read_write}
add snmp remote engine addrtype=ipv4 addr=xx port=xx engine_id=xx
set snmp local engine=xx
```

3. Define one or more Local Users. For example, type:

```
add snmp local user name=STR_USR_NAME security-level=(noAuthNoPriv|authNoPriv|authPriv)
    [auth-protocol=(md5|sha) password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]
    [group=STR_GRP_NAME]

set snmp local user name=xxxx group=xxxx
```

4. Define one or more Groups. Type **set snmp group name**=STR_SNMP_GRP and press **Enter**.

```
set snmp local user group=xxx
```

5. Define one or more Views. Type **set snmp view name**= STR_SNMP_VIEW and press **Enter**. (You can later delete an existing OID Sub Tree with the **remove snmp view name** command.)
6. Define one or more Trap Hosts.
   Type **add snmp traphost version**=v3 **type**=ipv4 **addr**=STR_SVR_ADDR and press **Enter**.
7. Define one or more Remote Engines. Type **add snmp remote engine addrtype**=ipv4 **addr**=192.168.1.30 **port**=xx **engine_ id**=xxxxx and press **Enter**.
8. Define one or more Remote Users by address type. For example, type:

```
add snmp remote user name=STR_USR_NAME addrtype=ipv4 addr=192.168.1.30 port=55 security-
level={noAuthNoPriv|authNoPriv|authPriv} auth-protocol={md5|sha} password=xxxxxxx priv-
protocol={des|aes} password=STR_PRIV_PASS
```

9. Press **Enter**.
10. Define one or more Remote Users by the remote engine. For example, type:

```
add snmp remote user name=STR_USR_NAME engine=STR_ENGINES security-level=authPriv
auth-protocol=md5 password=STR_AUTH_PASS priv-protocol=des password=STR_PRIV_PASS
```

11. Press **Enter**.
12. Verify the configuration has been set. Use the **show snmp commands** to display the current (existing) SNMP configuration elements (community, group, view, etc.). For example:

```
C1|S1|L1D>show snmp ?
  community
  group
  local
  remote
  traphost
```

```
  view
```

```
C1|S1|L1D>show snmp community
Community string                    Access mode
-------------------------------------------------------------------------------
comm1                               read_write
public                              read_write
private                             read_only
xxxxxxx                             read_only
C1|S1|L1D>
```

```
C1|S1|L1D>show snmp group
Name      Security Model  Security Level   Read View   Write View      Notify View
-------------------------------------------------------------------------------
public    v1              noAuthNoPriv    defaultView
public    v2c             noAuthNoPriv    defaultView
private   v1              noAuthNoPriv    defaultView   defaultView
private   v2c             noAuthNoPriv    defaultView   defaultView
```

```
C1|S1|L1D>show snmp local engine
Local engine ID:    80.00.03.64.03.00.c0.f2.20.de.9e (hex)
C1|S1|L1D>
```

```
Agent III C1|S1|L1D>show snmp local user
User Name    Group Name   Security Model   Security Level         Auth Protocol   Privacy Protocol
-------------------------------------------------------------------------------
BobB         private     v3              authPriv         MD5            DES
TedT                    v3              noAuthNoPriv
JeffS        private     v3              authPriv         SHA            AES
CarolC                  v3              authPriv         SHA            AES
GomesD                  v3              authPriv         SHA            AES
AndersonT    private     v3              authNoPriv       SHA
Agent III C1|S1|L1D>
```

```
AgentIII C1|S1|L1D>show snmp remote engine
Remote Address                  Remote port     Remote Engine ID
192.168.1.20                    162             800003640300c0f2209ede
AgentIII C1|S1|L1D>
```

```
C1|S1|L1D>show snmp remote user
User Name  Engine ID  Security Model Security Level Auth Protocol  Privacy Protocol
-------------------------------------------------------------------------------
C1|S1|L1D>
```

```
AgentIII C1|S1|L1D>show snmp traphost
Trap version   IP          Port Community/Security name  Security level  Trap/inform Timeout  Retry
    times
-------------------------------------------------------------------------------------------------
    ---
v3          192.168.1.30    162  TrpHstA6                    authPriv       trap
v3          192.168.1.40    162  private                 authNoPriv    trap
v3          192.168.1.50    162  public                  authPriv      trap
v2c         192.168.0.10    162  public                  noAuthNoPriv          inform      1500
    3
v1          192.168.1.20    162  public                  noAuthNoPriv          trap
AgentIII C1|S1|L1D>
```

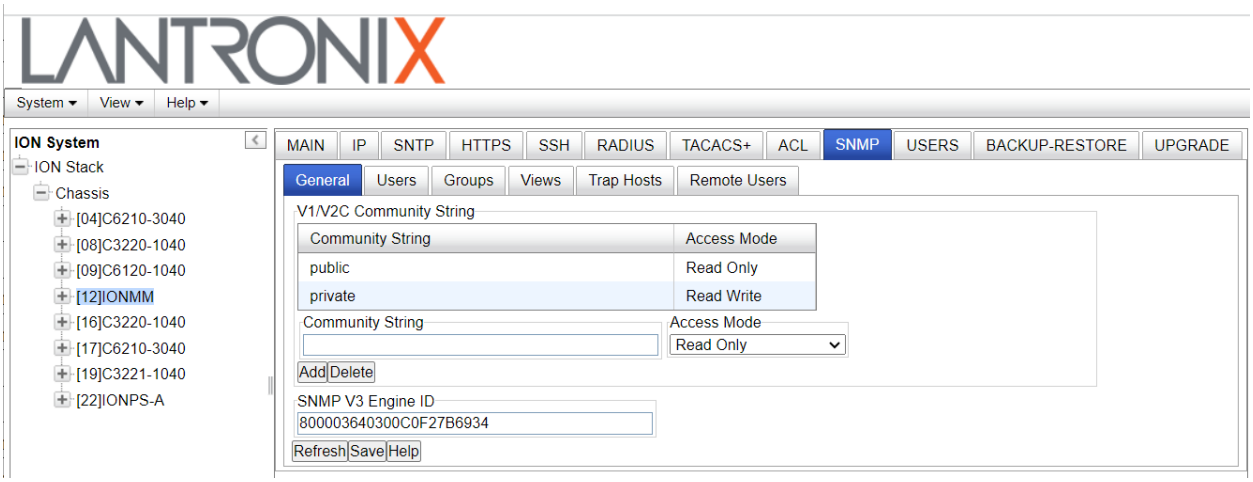
```
C1|S1|L1D>show snmp view
name             OID Sub Tree        type
-------------------------------------------------------------------------------
defaultView      0                   include
defaultView      1                   include
defaultView      2                   include
C1|S1|L1D>
```

8. Backup the configuration. See “Backup and Restore Operations (Provisioning)”.

SNMP Config – Web Method

This procedure is for a full SNMP configuration via the Web interface. Not all user applications will require all the steps below. For the full set of the individual default values see Table 17 later in this section.

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **SNMP** tab.
3. Select the **General** sub-tab if not already displayed.



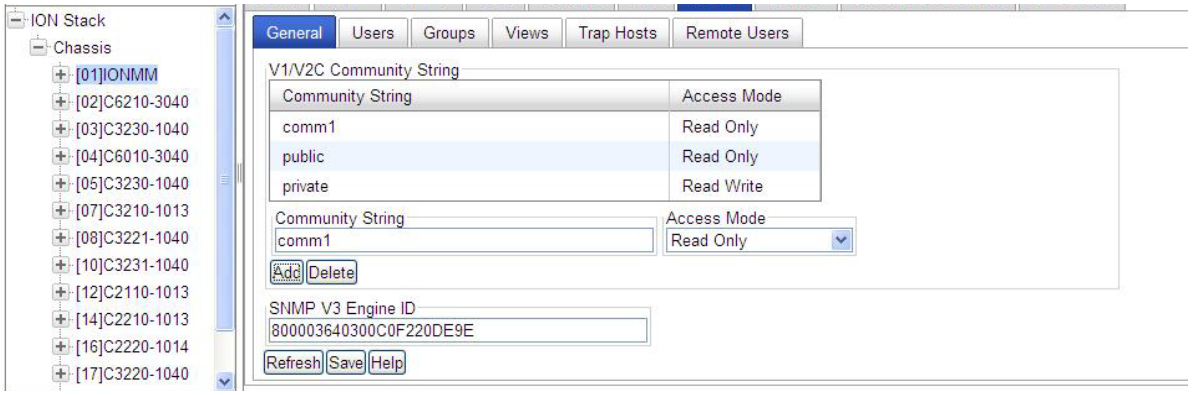
4. Add a new community string as required:

   Community String: enter the string to be added (e.g., **comm_1**) from 1-32 alphanumeric characters (no space characters).

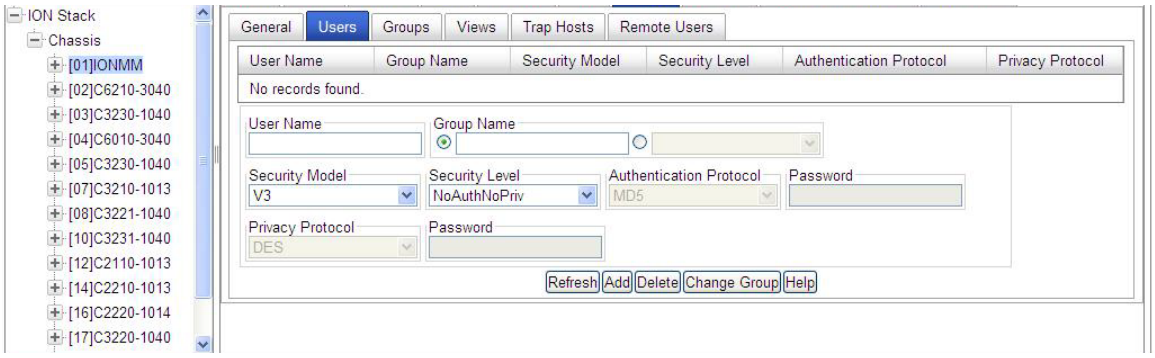
   Access Mode: select **Read Only** or **Read Write.**

   SNMP V3 Engine ID: enter the string to be added (e.g., **800003640300C0F220DE9E** above). Enter 18-128 characters using the characters a-f, 0-9, and A-F. The total length must be a dual from 18-128.

5. Click the **Add** button. The new entry is added to the table.



6. Click the **Save** button when done.
7. Select the **Users** sub-tab.



8. Enter the fields as required:

   User Name: The name of the user connecting to the SNMP agent. The valid range is 1-32 characters, and cannot include spaces.

   Group Name: The name of the SNMP group to which the user is assigned. The valid range is 1-32 characters (no space characters). When a local SNMPv3 user is added, a group name must be specified (but specifying a group name does not mean that this group already exists in the group table). A Group Name can be selected from the Default Group dropdown instead of entering one here.

   Security Model: The user security model; only SNMP V3.

   Security Level: The security level used for the user:

   - ***noAuthNoPriv*** – There is no authentication or encryption used in SNMP communications. (This is the default for SNMP V3.)
   - ***AuthNoPriv*** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMP V3 security model).
   - ***AuthPriv*** – SNMP communications use both authentication and encryption (only available for the SNMP V3 security model).

   Authentication Protocol: The method used for user authentication. The options are **MD5** or **SHA**. The default is **MD5**.

   Authentication Password: A minimum of eight plain text characters is required. The valid range is 8-64 characters (no space characters).

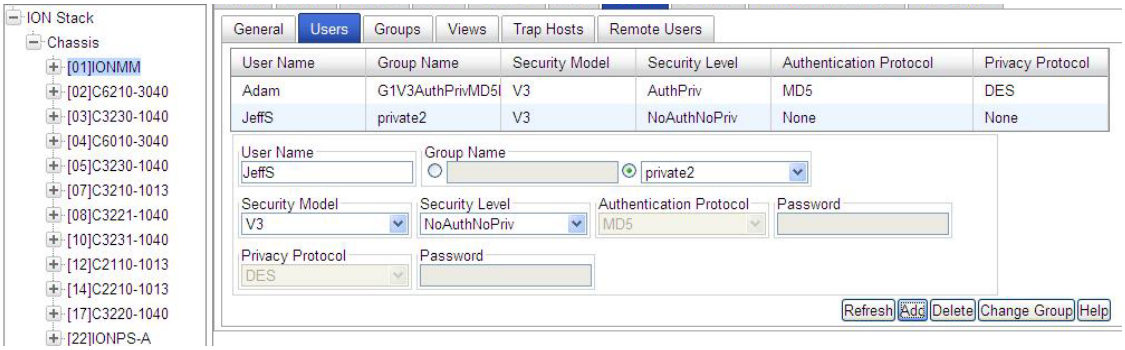
   Privacy Protocol: The encryption algorithm used for data privacy. (Options: **DES** or **AES**; Default: **DES**.)

   Privacy Password: A minimum of eight plain text characters is required. (Range: 8-64 characters.)

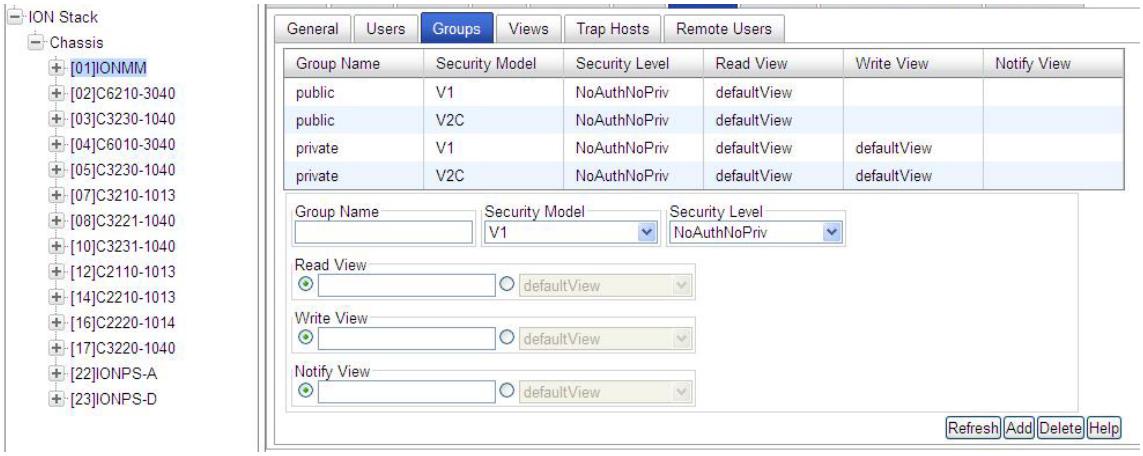
   securityName (implied): A human-readable string representing the user in a format that is Security Model independent. There is a one-to-one relationship between *userName* and *securityName*. In ION system, the security name is the same as user name.

   EngineID (implied for local USM user): The engineID of the SNMP engine the USM user belongs to. For a local USM user, the engineID must be the local engineID. For a remote USM user, this engineID must be specified. Note that Remote engine ID cannot be the same as the local engine ID.

9. Click the **Add** button. The new user is added to the table.



10. Select the **Groups** sub-tab.



11. Add and Edit the fields as required:

    Group Name: The name of the SNMP group. Enter one or more unique Group Names of 1-32 characters (no space characters).

    Security Model: The group security model; SNMP **V1**, **V2C** or **V3**.

    Security Level: The security level used for the group:

    - ***NoAuthNoPriv***: There is no authentication or encryption used in SNMP communications.
    - ***AuthNoPriv***: SNMP communications use authentication, but the data is not encrypted (only available for the SNMP V3 security model).
    - ***AuthPriv***: SNMP communications use both authentication and encryption (only available for the SNMP V3 security model).

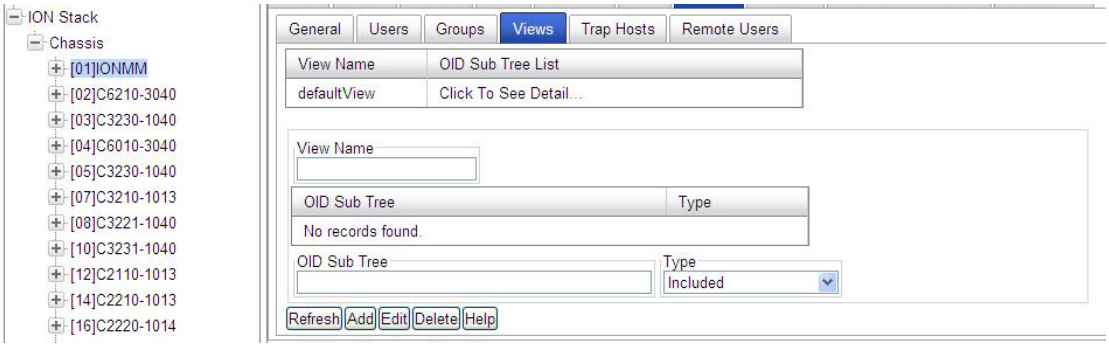
      The Group Security Level is the minimum level of security required in order to gain the access rights to the views (read/write/notify). If the User Security Level is less than the Group Security Level, this user will have no access rights to the views. A Security Level of ***noAuthNoPriv*** is less than ***authNoPriv*** which in turn is less than ***authPriv***. SNMPv1/v2c users (community string) are assigned ***noAuthNoPriv***.

    Read View: The configured view for read access. You can leave this view blank (none), or enter a specific view name (1-64 characters, no space characters), or select the **defaultView** radio button. **Note** that an entry here does not mean this view already exists in the view table.

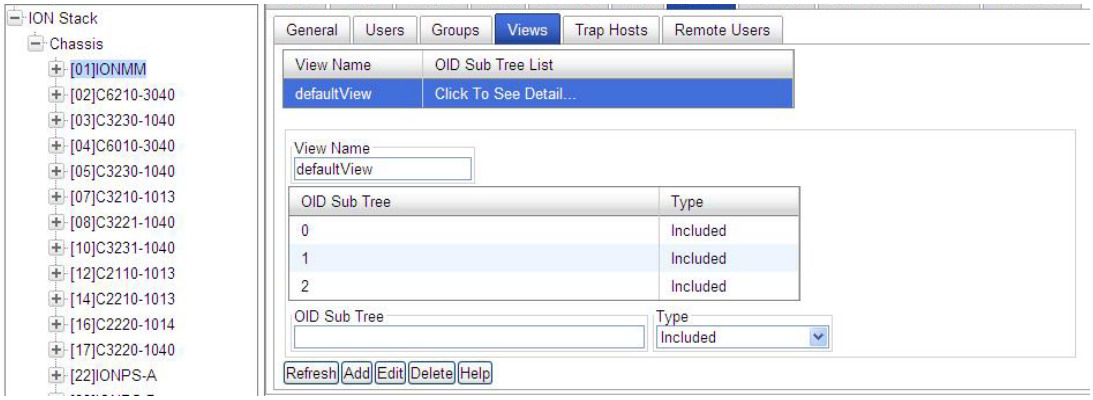
Write View: The configured view for write access. You can leave this view blank (none), or enter a specific view name (1-64 characters, no space characters), or select the **defaultView** radio button. **Note** that an entry here does not mean this view already exists in the view table.

Notify View: The configured view for notifications. You can leave this view blank (none), or enter a specific view name (1-64 characters, no space characters), or select the **defaultView** radio button. **Note** that an entry here does not mean this view already exists in the view table.

12. Select the **Views** sub-tab.



13. Click on "***Click To See Detail ...***" in the table. The details display:



14. Add / Edit the fields as required:

View Name: enter a name (1-64 characters) for this SNMP view (e.g., ***Default View***, ***Test View*** above).

OID Sub Tree: The object identifier (OID) of a branch within the MIB tree. Enter an OID sub-tree for this view (e.g., 1.3.6.1.2.1.47.1.1.1 above).

Type: Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view. At the dropdown select **Included** or **Excluded** and click the **Add** button when done.

Verify that the OID Sub Trees table shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view and click the **Add** button.

15. Select the **Trap Hosts** sub-tab.

16. Add / Edit the fields as required.

Trap Version: select the trap version (*v1*, *v2c* or *v3*) that the trap manager wants to receive. The default is SNMP *v2c*.

IP: the trap host IP address of a new management station to receive notification messages. At **IONMM** > **SNMP** > **Trap Hosts** you can enter IPv4 or IPv6 Trap Host IP addresses. The Trap hosts' IP address can be IPv6 type and IPv4 type. The two types can co-exist at the same time.

Port: enter the UDP port number to be used by the trap manager. The default is port number 162.

Community/Security Name: specify a valid SNMPv1/v2c trap community string or an SNMPv3 user name for a trap manager entry. (Range: 1-32 characters, case sensitive, no spaces) If the "Trap Version" is v1 or v2c, this field is used to specify the trap community of the trap host. If the "Trap Version" is v3, this field is used to specify a local or remote SNMPv3 User Name. Based on the selection of "Trap/Inform":

- For an SNMPv3 Trap, this field specifies a local SNMPv3 user name. If this user name doesn't exist in the local SNMPv3 user table, then traps cannot be sent out.
- For an SNMPv3 Inform, this field specifies a remote SNMPv3 user name. If this user name for the specific trap host does not exist in the remote SNMPv3 user table, then the informs cannot be sent out.

Security Level: When Trap Version ***v3*** is selected, specify one of the following security levels.

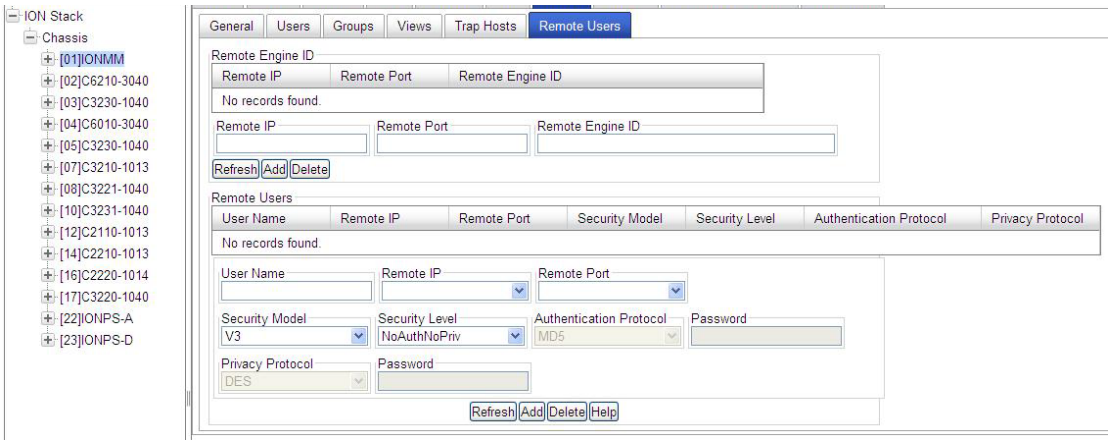
- ***NoAuthNoPriv*** – There is no authentication or encryption used in SNMP communications (the default setting).
- ***AuthNoPriv*** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
- ***AuthPriv*** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

Trap/Inform: When the "Trap Version" of a trap host is "v2c" or "v3", this field can be used to specify whether notifications are sent either by Trap or by Inform messages.

Timeout: The number of centiseconds (hundredths of a second) to wait for an acknowledgment before resending an inform message. The unit of this field is centiseconds. The valid range is 0-2147483647 centiseconds; the default is 1500 centiseconds. This selection is only available for version v2c and v3 Informs.

Retry Times: The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. The valid range is 0-255 retries; the default is 3 retries. This selection is only available for version v2c and v3 Informs.

17. Verify the table selections and click the **Add** button when done.
18. Select the **Remote User**s sub-tab.

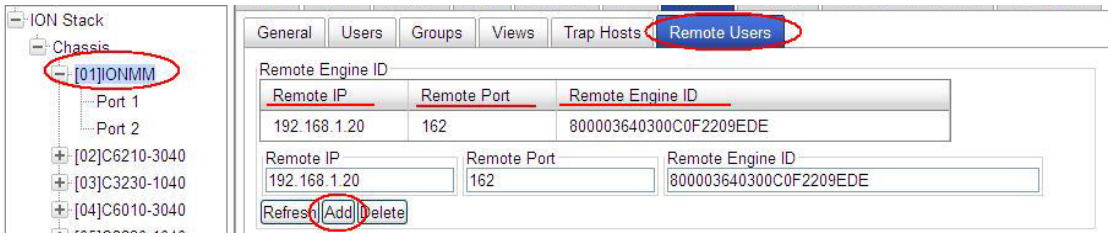


19. Add / Edit the **Remote Engine ID** section fields as required.

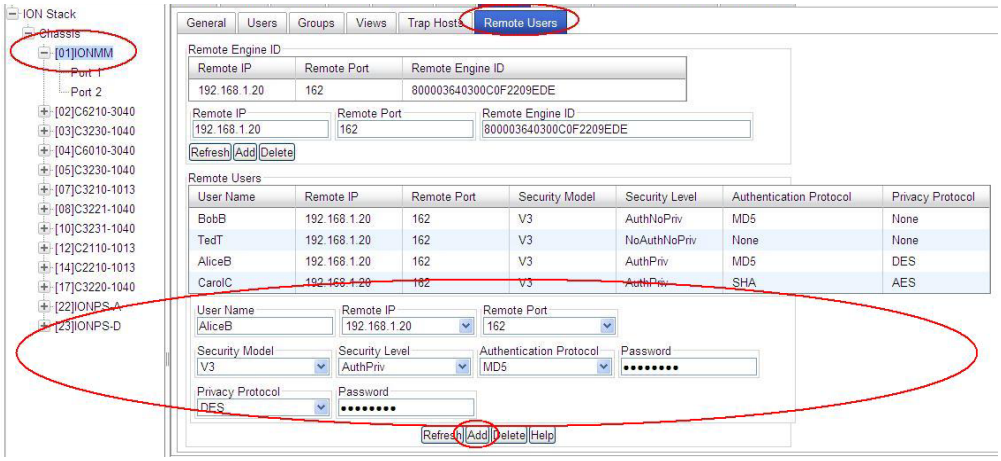
    Remote IP: enter the trap host IP address of a remote management station to receive notification messages. Trap Remote IP addressing can be IPv6 type and IPv4 type. The IPv4 and IPv6 types can co-exist at the same time.

    Remote Port: enter the UDP port number to be used by the trap manager (e.g., port number 162).

    Remote Engine ID: specify the engineID of the SNMP engine the remote user belongs to. For a remote USM (User-Based Security Model) user, this engineID must be specified. Note that the Remote engine ID cannot be the same as the local engine ID.



20. Click the **Add** button when done.
21. Add / Edit the **Remote Users** section fields as required.



User Name: Enter the name of the remote user connecting to the SNMP agent. The valid range is 1-32 characters (no space characters).

Remote Port: select an existing remote IP address from the dropdown.

Remote IP: from the dropdown, select an existing trap host IP address of a remote management station to receive notification messages (e.g., 192.168.1.123).

Security Model: The user security model; only SNMP ***V3***.

Security Level: The security level to be used for this remote user:

- ***NoAuthNoPriv*** – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
- ***AuthNoPriv*** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
- ***AuthPriv*** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

Authentication Protocol: The method to be used for user authentication. The options are **MD5** or **SHA**. The default is **MD5**.

Authentication Password: A minimum of eight plain text characters is required. The valid range is 8-64 characters).

Privacy Protocol: The encryption algorithm used for data privacy. The selections are **DES** or **AES**. The default is **DES**.

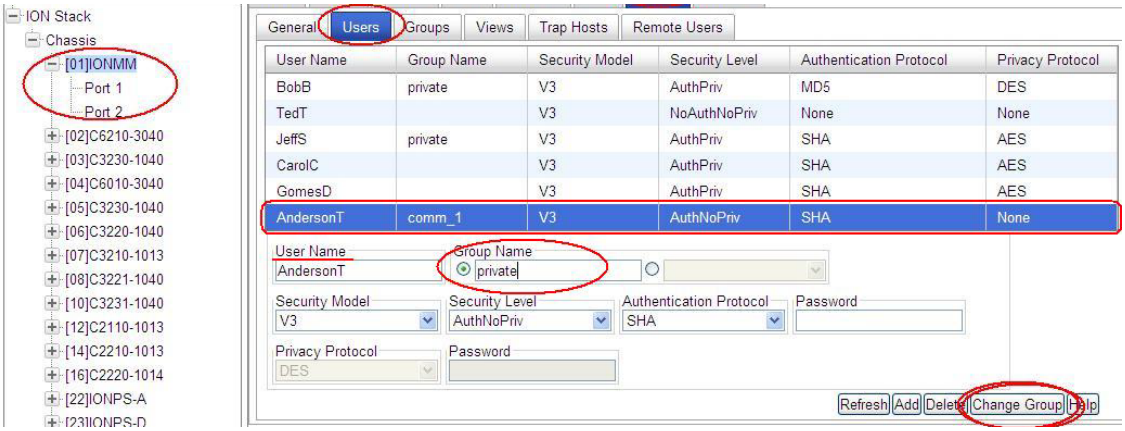
Privacy Password: Enter at least eight plain text characters. The valid range is 8-64 characters.

22. Verify the Remote Users table selections and click the **Add** button when done.
23. Backup the configuration. See “Backup and Restore Operations (Provisioning)”.

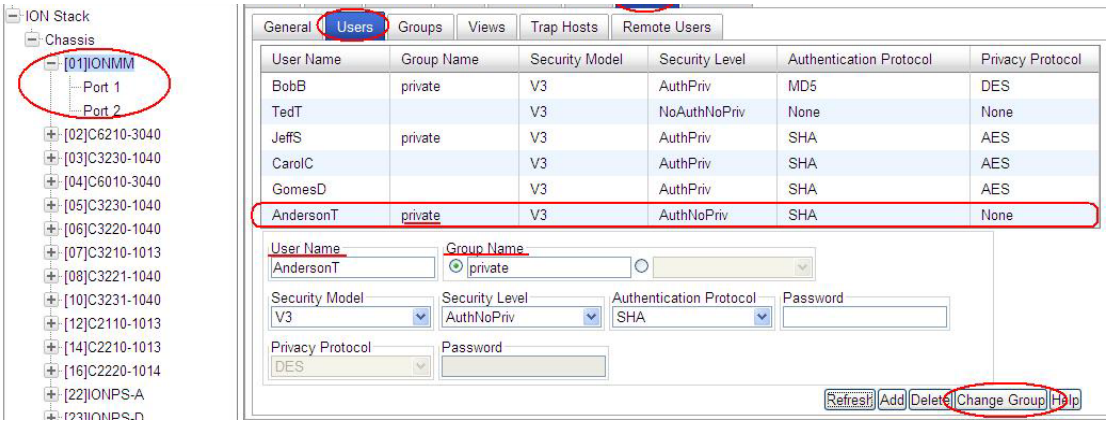
Change a SNMP User's Group - Web Method

You can change an existing User from one group to another group via the Web interface.

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **SNMP** tab.
3. In the **Users** sub-tab, select (highlight) an existing user in the table.
4. Enter the new Group name in the **Group Name** field.
5. Click the **Change Group** button.



6. Click the **Refresh** button if required. The user's new Group Name displays in the table.



In this example, user "AndersonT" is moved from the Group "comm._1" to the Group "private".

7. If the message "*ERROR: Invalid Input*" displays, click **Refresh** to clear the message, and make sure a user is selected (highlighted) and that an existing Group Name is entered in the **Group Name** field.

SNMP v3 Default Values

SNMPv3 initializes with the following default values.

Table 9: SNMP v3 Initialization (Default) Values

Item or Table	Default Value
SNMP version	V1/v2c
V1/v2c Write community string	private
V1/v2c Read only community string	public
SNMPv3 engine ID	"*80 00 03 64 03 00 c0 f2 xx xx xx*", where: "*03 64*" is the enterprise number of Lantronix. "*00 c0 f2 xx xx xx*" is the MAC address of an ION device.
Trap hosts	None configured.
Users	None configured.
Groups	Four default group entries, the "public" group and the "private" group are used for SNMPv1/v2 community string. These group entries are read-only. **Public v1**: this entry has SNMPv1 read access to the default view. **Public v2c**: this entry has SNMPv2c read access to the default view. **Private v1**: this entry has SNMPv1 read and write access to the default view. **Private v2c**: this entry has SNMPv1 read and write access to the default view.
Views	One default read-only view: ***DefaultView***. This view includes access to the entire MIB tree.

Notes for SNMPv1 and SNMPv2c Users

- At default there are two community strings and these two default community strings can be deleted by the user: 1) "public": a read-only community string, and 2) "private": a read-write community string.
- The **Read only** community string has full SNMPv1/v2c read access to the default view. It will be automatically added into the "public" group.
- The **Read write** community string has full SNMPv1/v2c read and write access default view. It will be automatically added into the "private" group.

Table 10: SNMP v3 Web Interface Default Values

SNMP tab	
SNMP General sub-tab	
V1/v2c Write community string	private
V1/v2c Read only community string	public
SNMPv3 engine ID	"*80 00 03 64 03 00 c0 f2 xx xx xx*". "*03 64*" is the enterprise number of Lantronix. "*00 c0 f2 xx xx xx*" is the MAC address of an ION device. For example: "*800003640300C0F2209EDE*".
SNMP Users sub-tab	
User Name Group Name Security Model Security Level Authentication Protocol Authentication Password Privacy Protocol Privacy Password	ION Default Group v1/v2c AuthNoPriv blank blank blank blank
SNMP Groups sub-tab	
Group Name Security Model Security Level Read View Write View Notify View	blank / Default Group / Test Group blank / V3 / V2 NoAuthNoPriv defaultView defaultView defaultView
SNMP Views sub-tab	
View Name OID Subtree List Actions OID Subtree Type	defaultView blank / "Click To See Detail ..." blank blank Included

SNMP Trap Hosts sub-tab	
Trap Version IP Port Community / Security Name Security Level Trap/Inform Timeout (centisecond) Retry Times	V3 172.16.6.9 162 private NoAuthNoPriv Trap 1500 3
SNMP Remote Users sub-tab	
Remote IP Remote Port Remote Engine ID User Name Group Name Remote IP Security Model Security Level Authentication Protocol Authentication Password Privacy Protocol Privacy Password	blank 162 blank blank blank blank V3 NoAuthNoPriv blank blank blank blank

SNMP v3 Commands

Command Categories

Table 11: SNMP Command Categories

Group Commands add snmp group remove snmp group show snmp group	***Local User Commands** * add snmp local user remove snmp local user set snmp local engine show snmp local engine show snmp local user	***Remote User Commands** * add snmp remote user remove snmp remote user show snmp rmt user
***View Commands** * add snmp view remove snmp view set snmp view show snmp view	***Trap Host commands*** add snmp traphost show all SNMP trap hosts show snmp traphost	*** SNMP Remote Engine Commands** * add snmp remote engine remove snmp rmt engine show snmp rmt engine
***Community Commands** * add snmp community remove snmp community show snmp community		

Web IF Sub-tabs: SNMP **General**, SNMP **Users** (Local + Remote), SNMP **Groups**, SNMP **Views**, SNMP **Trap Hosts**, SNMP **Remote Users** sub-tabs.

SNMP v3 Commands - Alphabetical List

1. Add SNMP Community Name / Access Mode
2. Add SNMP Group
3. Add SNMP Local User
4. Add SNMP Remote Engine
5. Add SNMP Remote User Name / Address Type
6. Add SNMP Remote User Name / Engine
7. Add SNMP Traphost
8. Add SNMP View Name
9. Remove SNMP Community Name
10. Remove SNMP Group
11. Remove SNMP Local User
12. Remove SNMP Remote Engine
13. Remove SNMP Remote User Name / Address Type
14. Remove SNMP Remote User Name / Engine ID
15. Remove SNMP Traphost
16. Remove SNMP View
17. Set SNMP Local Engine
18. Set SNMP Local User Name
19. Set SNMP View
20. Show SNMP Community
21. Show SNMP Group
22. Show SNMP Local Engine
23. Show SNMP Local User
24. Show SNMP Remote Engine
25. Show SNMP Remote User
26. Show SNMP Traphost
27. Show SNMP View

Web Interface-to-CLI Command Cross Reference for SNMP

The table below provides a cross-reference of configurable parameters via the Web interface versus CLI commands.

Table 12: Web Interface to CLI Command Cross Reference

Web Field	CLI Command
SNMP General sub-tab	
Community String Access Mode	Add SNMP Community Name / Access Mode
SNMP v3 Engine ID	Add SNMP Remote Engine Add SNMP Remote User Name / Engine Remove SNMP Remote Engine
SNMP Users sub-tab	
User Name Group Name Security Model Security Level Authentication Protocol Authentication Password Privacy Protocol Privacy Password	Add SNMP Local User Remove SNMP Local User Set SNMP Local User Name Show SNMP Local User Add SNMP Group Remove SNMP Group Set SNMP Local User Group Show SNMP Group
SNMP Groups sub-tab	
Group Name Security Model Security Level Read View Write View Notify View	Add SNMP Group Remove SNMP Group Set SNMP Local User Group Show SNMP Group
SNMP Views sub-tab	
View Name OID Subtrees Actions OID Subtree Type	Add SNMP View Name Remove SNMP View Set SNMP View Show SNMP View

SNMP Trap Hosts sub-tab	
Trap Version IP Port Community / Security Name Security Level Authentication Protocol Authentication Password Privacy Protocol Privacy Password Engine ID	Add SNMP Traphost Remove SNMP Traphost Show SNMP Traphost
SNMP Remote Users sub-tab	
Remote IP Remote Engine ID User Name Group Name Remote IP Security Model Security Level Authentication Protocol Authentication Password Privacy Protocol Privacy Password	Add SNMP Remote User Name / Address Type Add SNMP Remote User Name / Engine Remove SNMP Remote User Name / Address Type Remove SNMP Remote User Name / Engine ID Show SNMP Remote User

SNMP CLI Messages

Message:
At most 255 SNMP views can be created!
At most 255 SNMP communities can be created!
At most 255 SNMP groups can be created!
Fail to create SNMP community!
Fail to create SNMP group!
Fail to create SNMP view!
Meaning: You exceeded the SNMP configuration maximum of 255 Communities, Groups, or Views.
Recovery:
1. Verify the limit of 255 SNMP Users, Groups, and Views entries has not been reached.
2. Verify the SNMP Trap hosts and Remote Users tabs parameter settings.
3. See the "SNMP Web Interface" section for more information.

Syslog Messages

Message: LOG_WARNING, A defined IDS is detected.
Meaning: This is an IDS. Generate a trap message to SNMP. ION / Syslog monitors for malicious activities / policy violations and reports them to the Management Station.
Recovery: Follow your organization's procedure or process for detection of a defined IDS.

SNMP Engine ID Length

The **Engine ID** value must be (a-f) or (A-F) or 0-9 and the total length must be a dual from 18 to 64.

Message:

Its value must be consist of a-f or A-F or 0-9 and the total length must be a dual from 18 to 64.

Save the Engine ID failed!

SNMP Web Interface Messages

Message:

community name too long

Couldn't allocate enough memory

example config COMMUNITY not properly configured

example config NETWORK not properly configured

getnameinfo failed

missing CONTEXT_NAME parameter

missing NAME parameter

missing SOURCE parameter

missing COMMUNITY parameter

no IPv6 source address in PDU?

security name too long

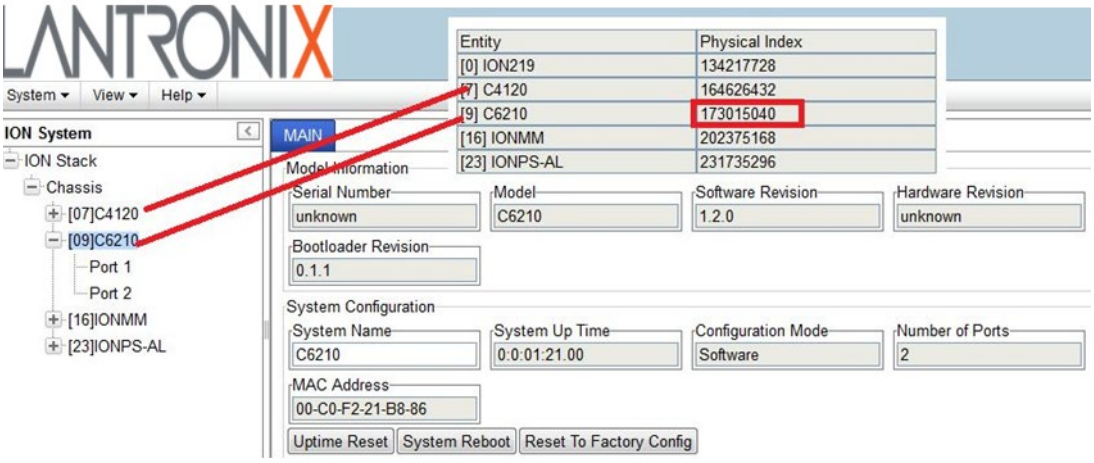
Meaning: A problem occurred during SNMP configuration.

Recovery:

1. Verify the SNMP Users, Groups, and Views tabs parameter settings.
2. Verify the SNMP Trap hosts and Remote Users tabs parameter settings.
3. See the "SNMP Web Interface" section for more information.

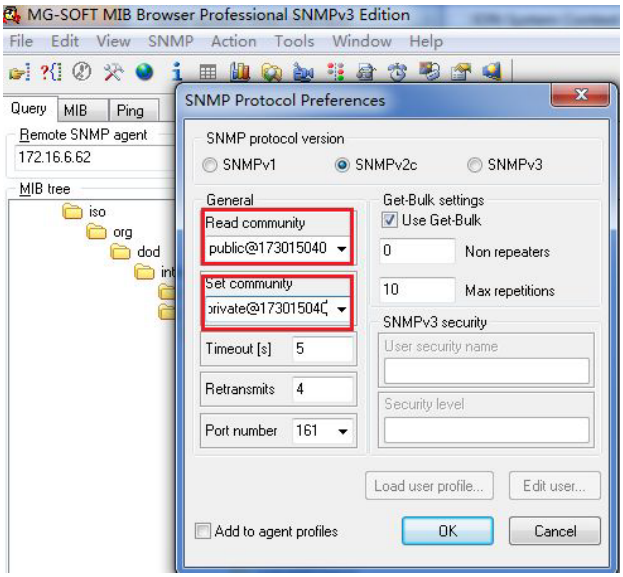
ION SNMP Operation Example

As shown in the screen below, every card has its physical index (automatically produced and stored in entityMIB when initializing).



MOST mibs are registered individually based on the physical index for the sake of better performance.

To read MIBs on C6210 (slot 9), most of the time (normally for private mibs) we must use this community string: "public@173015040" OR "public::173015040" instead of "public" (see below).



However, some public mibs can only be accessed by using "public" or "private". The entityMIB is an example.

In other words, MIBs need their own community string which should be automatically provided by a fixed rule during runtime, based on the MIBs themselves as well as the entity they are serving.

Configuring SFTP

SFTP support was added in IONMM version 1.5.17. The SFTP (Secure File Transfer Protocol) feature enables secure file transfers between your IONMM device and remote servers. This includes firmware upgrades and configuration backups/restores. SFTP provides encrypted file transfers, making it more secure than traditional TFTP.

SFTP CLI Commands

The following CLI commands were added in IONMM version 1.5.17 to support SFTP in the IONMM:

prov get sftp server addr	: Display current SFTP server address
prov set sftp server type=(ipv4|ipv6|dns) addr=ADDR	: Set SFTP server address
show sftp config	: Display SFTP configuration
set sftp username=USERNAME	: Set SFTP username
set sftp password	: Set SFTP password (interactive)
set sftp state=(enable|disable)	: Enable or disable SFTP
set sftp port=<1-65535>	: Set custom SFTP port (default: 22)
set sftp serverpath=SERVERPATH	: Set remote server directory path
sftp get remotefile=RFILE	: Download file from SFTP server
sftp upgrade remotefile=RFILE	: Download and install IONMM firmware via SFTP

Operations like Backup/Restore, HTTPS, SSH, and firmware upgrade will use SFTP or TFTP based on whether SFTP is enabled or disabled.

SFTP Configuration – CLI Method

1. After a factory reset to the IONMM, default values for sftp management look like this:

```
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                   Disabled
Server port:                  22
SFTP User :
Server Path :
SFTP password:                Not set
```

2. Specify sftp server user name

```
Agent III C1|S3|L1D>set sftp username sftpuser1
SFTP username has been set to sftpuser1.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                   Disabled
Server port:                  22
SFTP User :                   sftpuser1
Server Path :
SFTP password:                Not set
```

3. Set sftp user's password.
Enter the password twice to help prevent typos and ensure accuracy.

Important Notes:

- Set the password before doing any sftp related operations like backup, restore, firmware upgrade. Operation will fail if the password is not set or set incorrectly.
- To improve security, the password is temporarily stored in the IONMM's storage. This password is excluded from configuration backup. The password will be lost when IONMM is upgraded/downgraded with a new firmware and also when factory reset is done. The password needs to be set again before doing sftp transfer.
- The "show sftp config" command will display "Not Set" if the password is not configured yet and shows "*****" if password is already set.

```
Agent III C1|S3|L1D>set sftp password
Please input password:

Please input password again:

SFTP password has been set.
Agent III C1|S3|L1D>
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                   Disabled
Server port:                  22
SFTP User :                   sftpuser1
Server Path :
SFTP password:                ******
```

4. Specify the path/directory on the sftp server (where files come from or go to)

Note: Make sure that the configured directory/folder has required permissions (read & write) on the server.

If no path/directory is configured, user's home directory will be used as target for the sftp transfers.

```
Agent III C1|S3|L1D>set sftp serverpath ""
SFTP server path has been set to .
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                   Disabled
Server port:                  22
SFTP User :                   sftpuser1
Server Path :
SFTP password:                ******
```

If the SFTP server is a Linux machine and you want to specify an absolute path on the server, it should start with a "/" (forward slash).

```
Agent III C1|S3|L1D>set sftp serverpath /home/ionbackup
SFTP server path has been set to /home/ionbackup.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
```

```
SFTP state:                    Disabled
Server port:                   22
SFTP User :                    sftpuser1
Server Path :                  /home/ionbackup
SFTP password:                 ******
```

If the SFTP server is a Windows machine and you want to specify an absolute path including a drive name (like C: or D:) on the server, it also should start with a "/" (forward slash). For example, if the path on the Windows machine "C:\user\ionbackup", it should be configured in the ION like "/C:/user/ionbackup"

```
Agent III C1|S3|L1D>set sftp serverpath /C:/user/ionbackup
SFTP server path has been set to /C:/user/ionbackup.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                    Disabled
Server port:                   22
SFTP User :                    sftpuser1
Server Path :                  /C:/user/ionbackup
SFTP password:                 ******
```

If a relative path (i.e. a path under user's home directory) to be used, just specify it without a leading "/" (forward slash). It applies to both Linux and Windows machines.

```
Agent III C1|S3|L1D>set sftp serverpath ion/backup
SFTP server path has been set to ion/backup.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                    Disabled
Server port:                   22
SFTP User :                    sftpuser1
Server Path :                  ion/backup
SFTP password:                 ******
```

Set/reset the path to user's home directory.

```
Agent III C1|S3|L1D>set sftp serverpath ""
SFTP server path has been set to .
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                    Disabled
Server port:                   22
SFTP User :                    sftpuser1
Server Path :
SFTP password:                 ******
```

5. Set sftp server port. By default port 22 is used for sftp transfers. If you would like to use a custom port number, use this command. Also make sure that the server is configured accordingly.

```
Agent III C1|S3|L1D>set sftp port 4000
SFTP port has been set to 4000.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
```

```
------------------------------------------------------------------------
SFTP state:                    Enabled
Server port:                   4000
SFTP User :                    sftpuser1
Server Path :
SFTP password:                 ******
```

6. Enable or disable the sftp admin state. If disabled, tftp transfer will be used instead of sftp.

```
Agent III C1|S3|L1D>set sftp state enable
SFTP has been enabled.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                    Enabled
Server port:                   22
SFTP User :                    sftpuser1
Server Path :
SFTP password:                 ******
```

7. Upload a new firmware to the firmware-db

```
Agent III C1|S3|L1D>show upgrade firmware file
Card type                          Revision                          Firmware file name
-------------------------------------------------------------------------------------------
IONPS                         1.2.5                             IONPS_1.2.5_AP.bin
x222x_x322x                   1.3.18                            x222x_x322x_1.3.18_AP.bin
x323x                         1.3.18                            x323x_1.3.18_AP.bin
x411x                         3.0.5                             x4110_3.0.5_AP.bin
x631x                         3.0.0                             x6310_3.0.0_AP.bin
x611x_x612x                   2.0.11                            x611x_x612x_2.0.11_AP.bin
x621x                         2.0.0                             x6210_2.0.0_AP.bin
x311x                         2.0.3                             x3110_2.0.3_AP.bin
x211x                         2.0.0                             x2110_2.0.0_AP.bin
IONMM                         1.5.15                            IONMM-1.5.15_AP.bin

Agent III C1|S3|L1D>sftp get remotefile IONMM-1.5.17_AP.bin
SFTP transferring...

File transferred successfully!
Agent III C1|S3|L1D>

Agent III C1|S3|L1D>update firmware-db file IONMM-1.5.17_AP.bin
Updating is in progress...

Update succeeded!

Agent III C1|S3|L1D>show upgrade firmware file
Card type                          Revision                          Firmware file name
-------------------------------------------------------------------------------------------
IONPS                         1.2.5                             IONPS_1.2.5_AP.bin
x222x_x322x                   1.3.18                            x222x_x322x_1.3.18_AP.bin
x323x                         1.3.18                            x323x_1.3.18_AP.bin
x411x                         3.0.5                             x4110_3.0.5_AP.bin
x631x                         3.0.0                             x6310_3.0.0_AP.bin
x611x_x612x                   2.0.11                            x611x_x612x_2.0.11_AP.bin
x621x                         2.0.0                             x6210_2.0.0_AP.bin
```

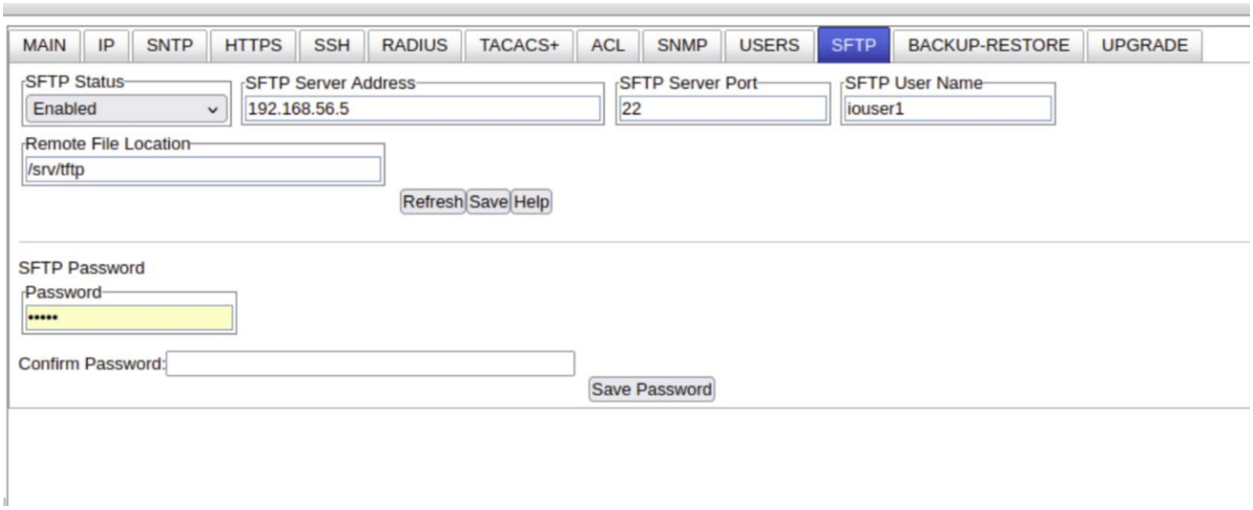
```
x311x                    2.0.3                    x3110_2.0.3_AP.bin
x211x                    2.0.0                    x2110_2.0.0_AP.bin
IONMM                    1.5.15                   IONMM-1.5.15_AP.bin
```

8. Upgrade the IONMM with a new firmware image

```
Agent III C1|S3|L1D>sftp upgrade remotefile IONMM-1.5.15_AP.bin

Processing...

SFTP upgrade succeeded!
```

SFTP Configuration – Web Method

1. Access the IONMM through the Web interface.
2. Select the **SFTP** tab.



3. In the **SFTP Status** field, select **Enabled**.
4. Type the SFTP server IP address and port. By default port 22 is used.
5. Type the SFTP user name.
6. Type the directory for the remote file location.
7. Click **Save** and continue to the password field.
8. Type the SFTP password and retype it to confirm.
9. Click **Save Password**.

Operations like Backup/Restore, HTTPS, SSH, and firmware upgrade will use SFTP or TFTP based on whether SFTP is enabled or disabled.

4. Operation

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

Backup and Restore Operations (Provisioning)

You can back up and restore the configuration information for the IONMM and any or all the NIDs in the ION system via the Web interface.

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 view the SIC card's current configuration before a backup/restore operation to verify the desired configuration settings. Use the command "**show card info**" for this. There are several CLI **show** commands that allow you to display (show) information about the NID configuration. For a complete description of these and other CLI commands see the *ION System CLI Reference Manual, 33461*.

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

Note: The maximum length for the file name of the backup file or TFTP/SFTP upload or download file is 128 characters (added at ION v1.3.10).

For information on the status of important ION system files resulting from this operation, see "Appendix C: ION System File Content and Location".

Note: IONMM and IONMM-232 Firmware version 1.5.0 enhanced the backup and restore operations. After upgrading to v1.5.0, new backups should be made. See the ION Release Notes.

Backup the Configuration – Web Method

The following procedure describes how to back up the configuration of one or more modules in the ION system. The backup file is stored in IONMM memory. Note that a backup/restore operation of a NID with full configuration (maximum entries for all dynamic tables) may take a long time (approximately 50 minutes).

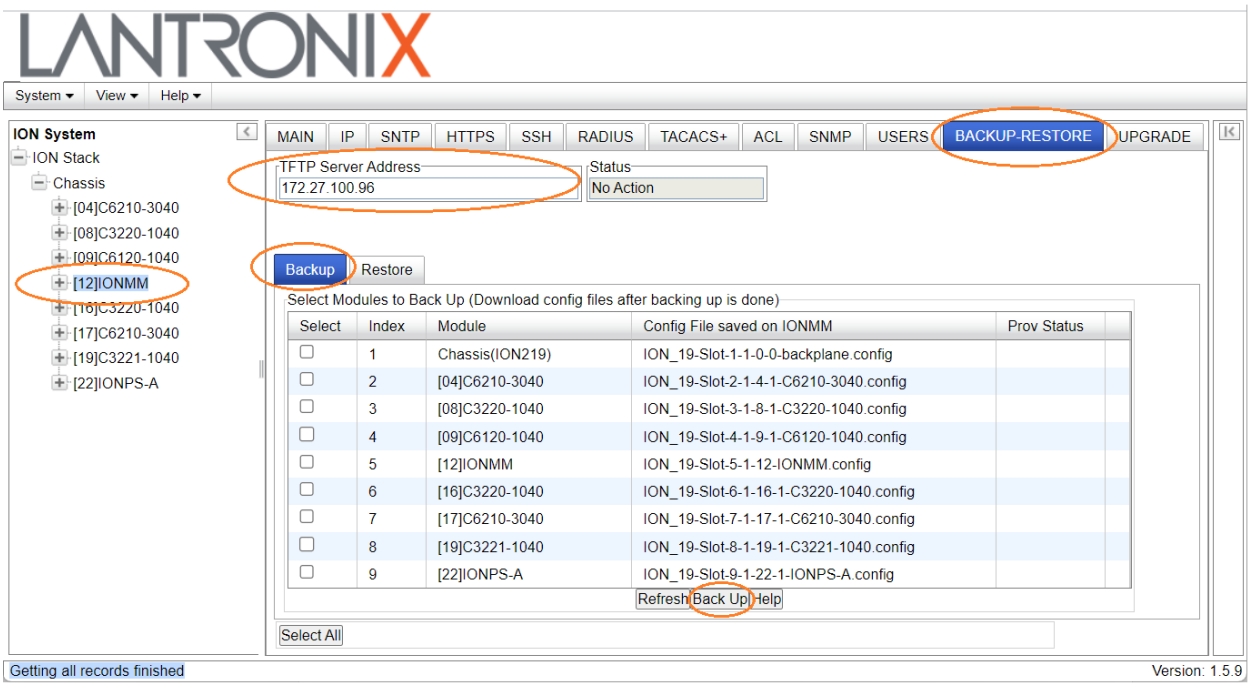
When you execute a backup/restore, the status will change to 'Success' approximately one second after you start the backup/restore, but it is still ongoing in the background. A message displays saying that action is ongoing; after the action is finished, then the status will change to 'Success'.

If you add 255 VLAN entries via script, then perform a backup and restore, the backed up config file list totals 255 VLAN entries (less the default VLAN). When you perform the restore, it fails, due to adding the 255th VLAN entry. See "Dynamic Table Entry Limits".

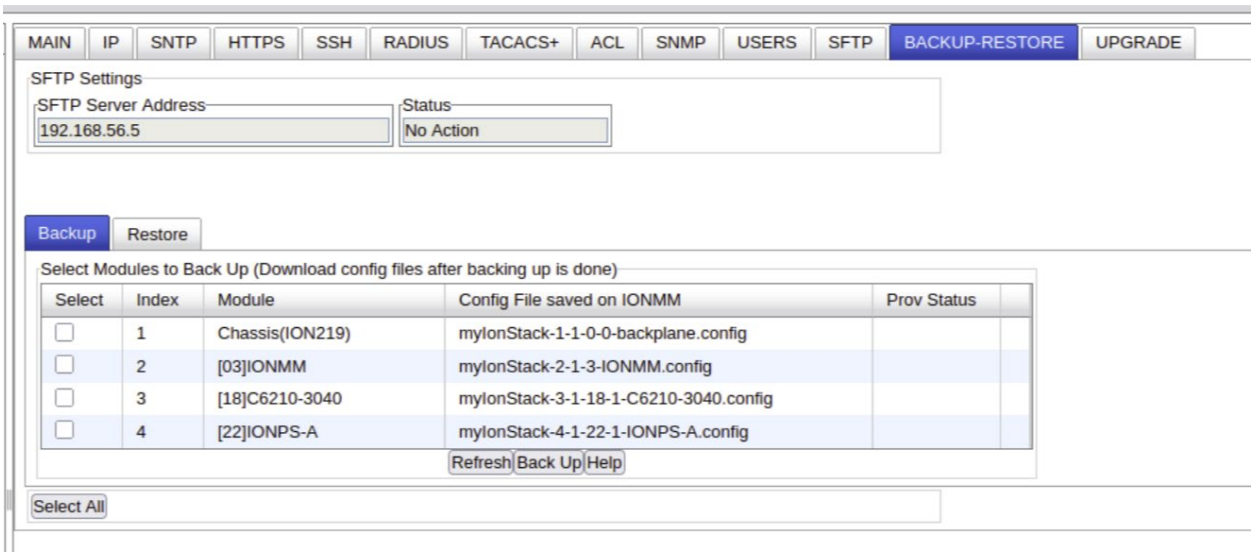
IMPORTANT

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).

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



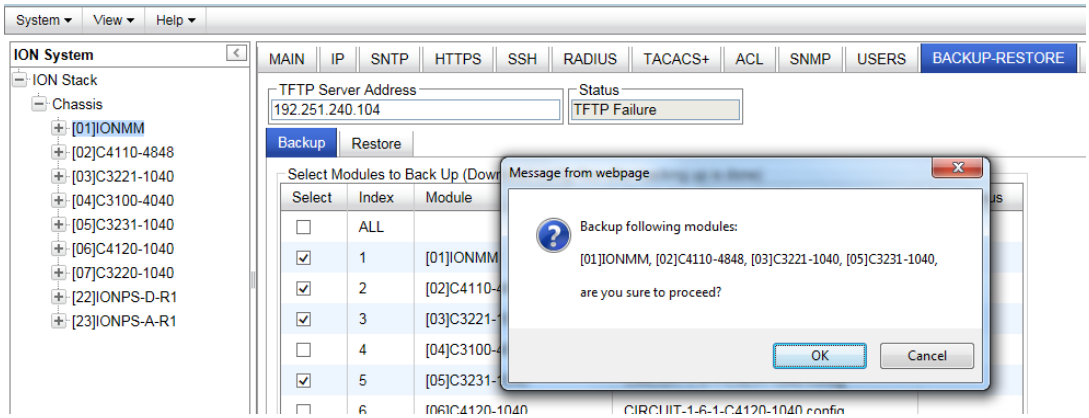
If SFTP is enabled, the Backup-Restore page will display the SFTP Server Address.



3. In the TFTP Server Address field, enter a valid IPv4 or IPv6 address (e.g., 192.168.1.30 or fe80::2c0:f2ff:fe20:de9e).
4. Verify that the TFTP/SFTP Server is running and configured, and that the file to be downloaded is located correctly (e.g., at *C:\TFTP-Root*).
5. 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.
6. Note the **Status** field message (*Wrong Firmware*, *No Action*, etc.).
7. In the **Select** column, check the checkbox of each module to be backed up.
8. Do you want to rename the backup file?

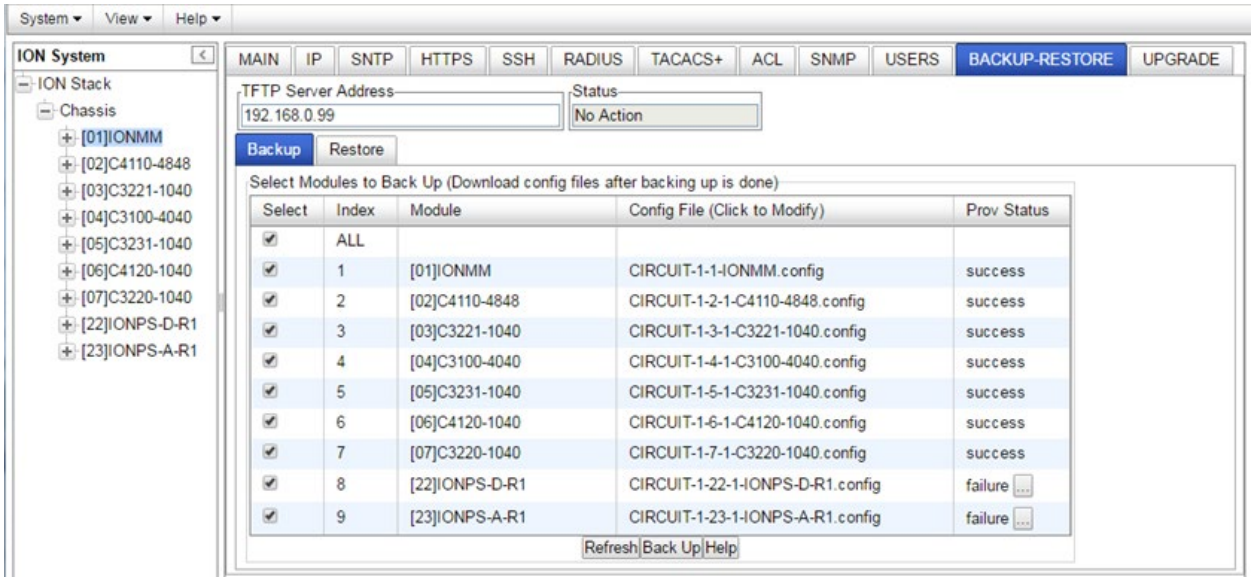
Yes	**No**
a) In the **Config File** column, click the file name. b) Type a new name for the backup file. **Note:** the file name must be 1–63 characters long and must end with **.config**. c) Continue with step 9 below.	Continue with step 9 below.

9. Click the **Back Up** button. The message "*Backup is being processed ...*" displays. The Back Up operation can take several minutes.
10. 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*).

11. Click the **Download** button. When completed, the message "*File has successfully transferred via TFTP*" displays.
12. Click the **OK** button to clear the web page message.
13. If the Back Up operation fails, go to step 15 below.
14. To send a copy of the backup file to the TFTP/SFTP Server:
    a. Make sure the TFTP/SFTP 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/SFTP 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 error (.ERR) log file is downloaded to the TFTP/SFTP server address specified, in TFTP-Root with a filename such as *1-11-C2210-1013.config*. You can open the file in a text editor. See "The Config Error Log (config.err) File" section for error messages and possible recovery procedures.

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

- Editing the Config File (Optional)
- Restoring the Configuration

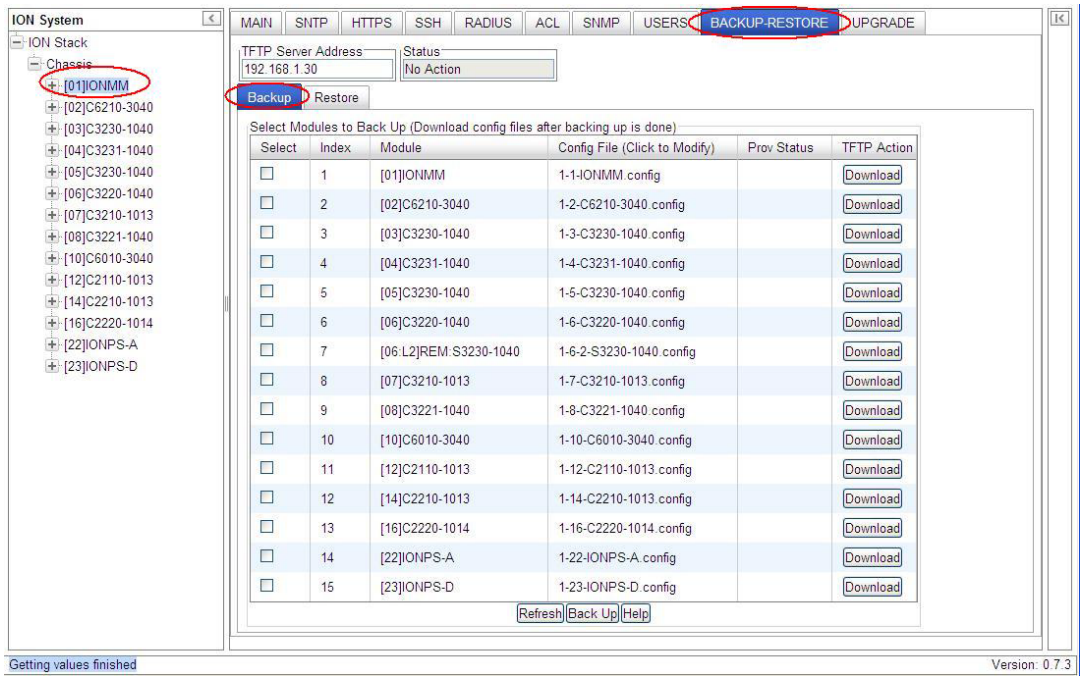
Backup Standalone Modules

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

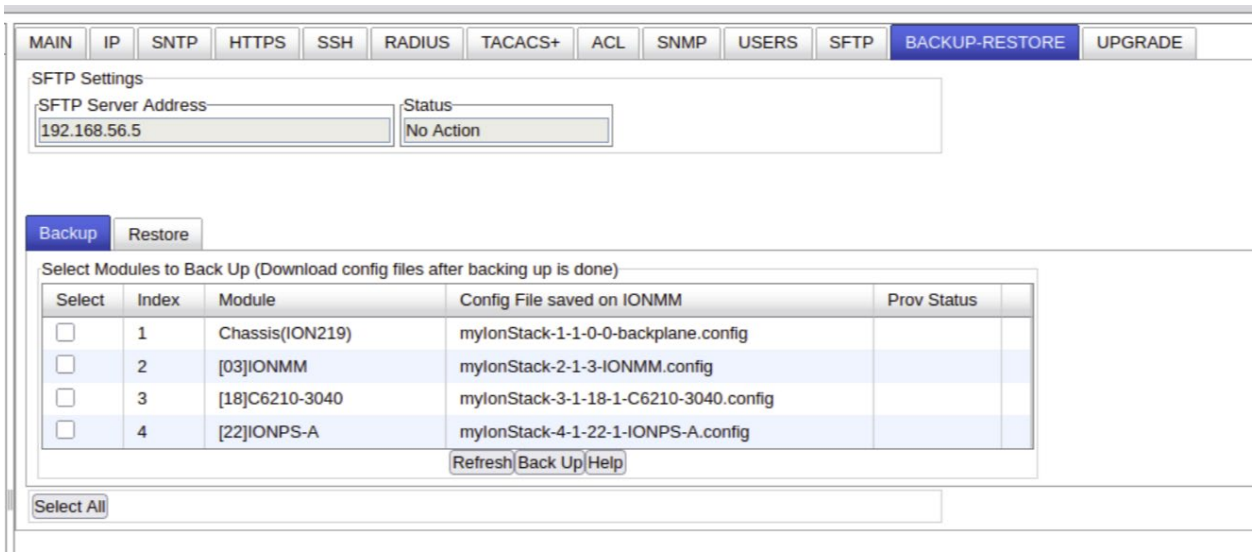
IMPORTANT

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.

1. Access the IONMM module through the Web interface (see "Starting the Web Interface").
2. Select the **BACKUP-RESTORE** tab.



If SFTP is enabled, the web page displays the SFTP Server Address.



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

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

5. Click the **Back Up** button.
6. When the confirmation window displays, click **OK**. The backup file is saved in the IONMM module.
7. To send a copy of the backup file to the TFTP/SFTP server:
    a. Make sure the TFTP/SFTP Server is running and configured.
    b. In the **TFTP/SFTP Server Address** field, enter the IP address of the TFTP/SFTP 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 the Configuration

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 a plain text editor from the TFTP/SFTP 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 (three PORT x CONFIG sections for the model x3232 NIDs).
4. Save the edited Config file back to the TFTP/SFTP server location (e.g., *C:\TFTP-Root\1-9-C3231-1040.config*).
5. Continue with the applicable Restore procedure from the following section using the edited Configuration file.

A sample IONMM Config file is shown below.

```
1 [DEVICE LEVEL CONFIG]
2 set acl state=disable
3 set ip6tables acl state=disable
4 remove acl condition all
5 remove ip6tables acl condition all
6 remove sysuser all
7 prov remove snmp all
8 remove acl rule all
9 remove ip6tables acl rule all
10 set ip address mode =static
11 set ip type=ipv4 addr=192.251.220.197 subnet-mask=255.255.255.0
12 set gateway type=ipv4 addr=192.251.220.2
13 set ipv6-mgmt state=disable
14 set ipv6 address mode =static
15 set ip type=ipv6 addr=:: prefix=0
16 set ipv6 gateway mode=static
17 set gateway type=ipv6 addr=::
18 set dns-svr svr=1 type=ipv4 addr=0.0.0.0
19 set dns-svr svr=2 type=ipv4 addr=0.0.0.0
20 set dns-svr svr=3 type=ipv4 addr=0.0.0.0
21 set dns-svr svr=4 type=ipv6 addr=::
22 set dns-svr svr=5 type=ipv6 addr=::
23 set dns-svr svr=6 type=ipv6 addr=::
24 set sntp state=disable
25 set sntp dst-state=disable
26 set sntp timezone=8
27 set sntp dst-start="1969 1231 18:00:00"
28 set sntp dst-end="1969 1231 18:00:00"
29 set sntp dst-offset=0
30 set sntp-svr svr=1 type=dns addr=0.0.0.0
```

```
31 set sntp-svr svr=2 type=dns addr=0.0.0.0
32 set sntp-svr svr=3 type=dns addr=0.0.0.0
33 set sntp-svr svr=4 type=dns addr=0.0.0.0
34 set sntp-svr svr=5 type=dns addr=0.0.0.0
35 set sntp-svr svr=6 type=dns addr=0.0.0.0
36 set radius client state=disable
37 set radius svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30
38 set radius svr=2 type=dns addr=0.0.0.0 retry=3 timeout=30
39 set radius svr=3 type=dns addr=0.0.0.0 retry=3 timeout=30
40 set radius svr=4 type=dns addr=0.0.0.0 retry=3 timeout=30
41 set radius svr=5 type=dns addr=0.0.0.0 retry=3 timeout=30
42 set radius svr=6 type=dns addr=0.0.0.0 retry=3 timeout=30
43 set tacplus client state=disable
44 set tacplus svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30
45 set tacplus svr=2 type=dns addr=0.0.0.0 retry=3 timeout=30
46 set tacplus svr=3 type=dns addr=0.0.0.0 retry=3 timeout=30
47 set tacplus svr=4 type=dns addr=0.0.0.0 retry=3 timeout=30
48 set tacplus svr=5 type=dns addr=0.0.0.0 retry=3 timeout=30
49 set tacplus svr=6 type=dns addr=0.0.0.0 retry=3 timeout=30
51 set acl table=filter chain=input policy=drop
52 set acl state=disable
53 set ip6tables acl table=filter chain=input policy=accept
54 set ip6tables acl state=disable
55 set mgmt vlan state=disable
56 set mgmt vlan port=none
57 set mgmt vlan vid=2
58 prov set tftp svr type=ipv4 addr=192.251.220.100
59 set system name="Agent III"
60 set system contact="Lantronix(techsupport@lantronix.com)"
61 set system location="10900 Red Circle Drive     Minnetonka, MN 55343 USA"
62 set https state=disable
63 set https port=443
64 set usb-port state=enable
65 set ssh server state=enable
66 set ssh client timeout=60
67 set ssh auth-retry=3
68 set syslog svr port=514
69 set syslog mode=localAndRemote
70 set syslog level=alert
71 set syslog svr type=ipv4 addr=192.251.220.100
72 add snmp community name public access_mode read_only
73 add snmp community name private access_mode read_write
74 set login method= local
75 set sysuser name ION pass private confirmpass private
76 [PORT 1 CONFIG]
77 set ether autoneg state=enable
```

```
78 set ether autocross=auto
79 set ether adv-cap=10THD+10TFD+100THD+100TFD
80 set ether pause=nopause
81 set ether admin state=up
82 [PORT 2 CONFIG]
83 set ether autoneg state=enable
84 set ether autocross=auto
85 set ether adv-cap=10THD+10TFD+100THD+100TFD
86 set ether pause=nopause
87 set ether admin state=up
```

Restore the Configuration – Web Method

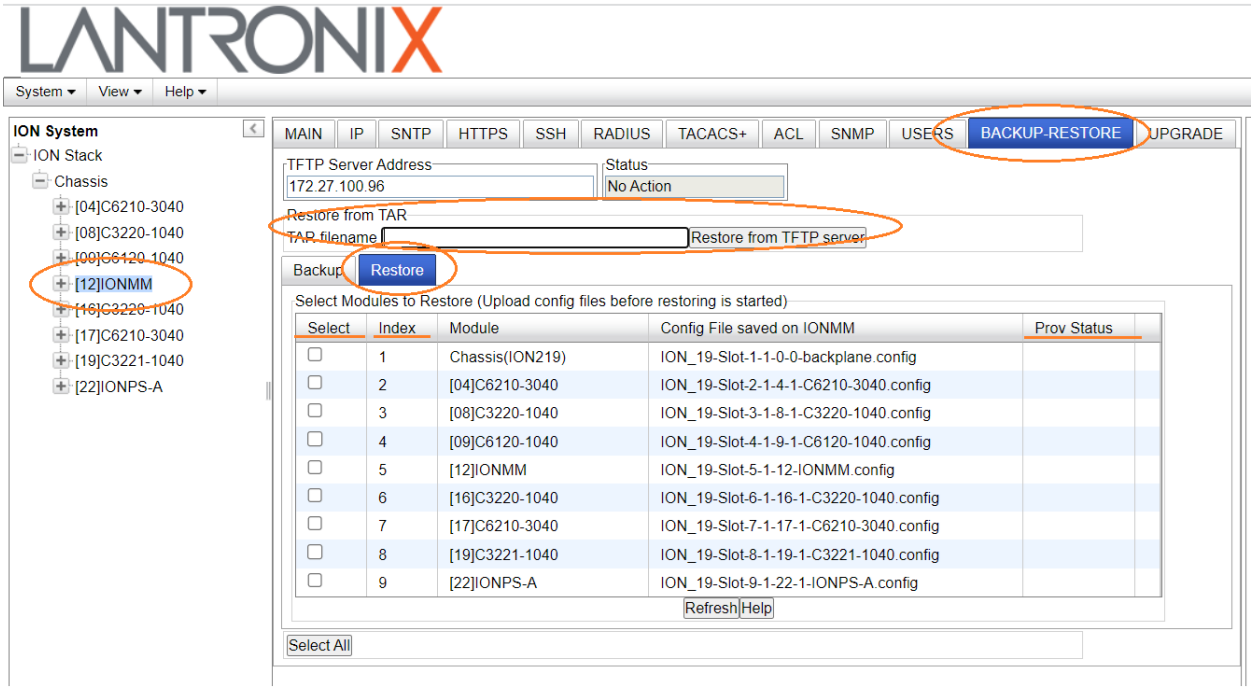
The following procedure describes how to restore the configuration of one or more modules in the ION system.

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

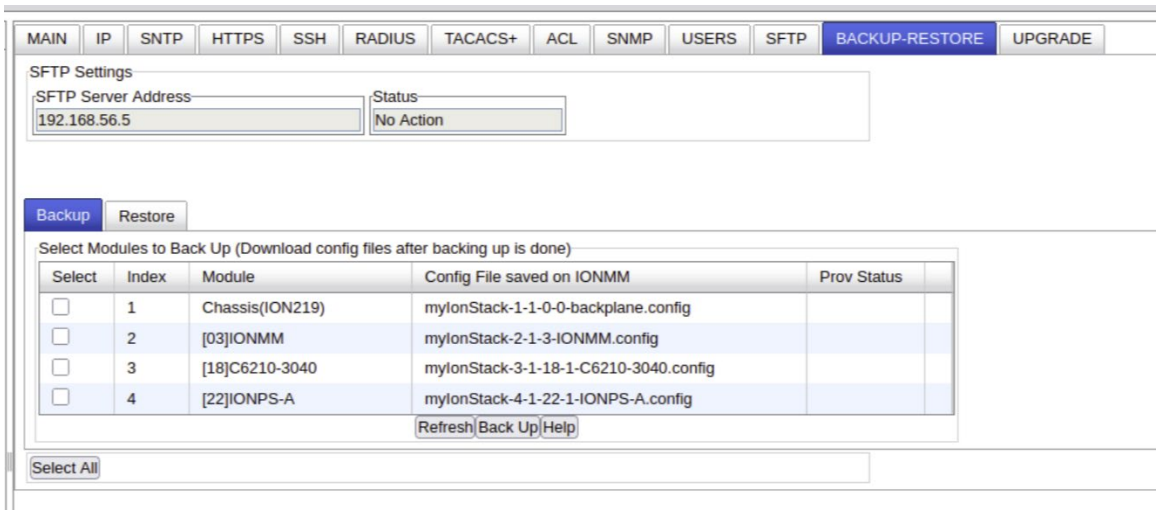
IMPORTANT

A restore operation requires a backup configuration file.

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. At the **BACKUP-RESTORE** tab, select the **Restore** sub-tab. The "Modules to Restore" table displays.



If SFTP is enabled, the Backup-Restore page will display the SFTP Server Address.



3. Enter a TFTP Server Address, or in the Restore from TAR section, enter a TAR filename (e.g., IONMM_1.5.5_AP.zip) and click the **Restore from TFTP server** button as required.
4. If the card list shown in the table is not correct, unfold the ION Stack in the left tree view, and then refold it to refresh the table information.
5. In the **Select** column, check the checkbox of each module to be restored. Note that you must Upload config files before restoring is started.
6. Is the configuration file to be restored different than the one shown in the Config File column?

Yes	**No**
a) In the **Config File** column, click the file name. b) Type the name of the backup file to be restored. **Note:** the file name must end with **.config**. c) Continue with Continue with step 6.	Continue with step 7 below.

7. Does the configuration file need to be retrieved from the TFTP/SFTP server?

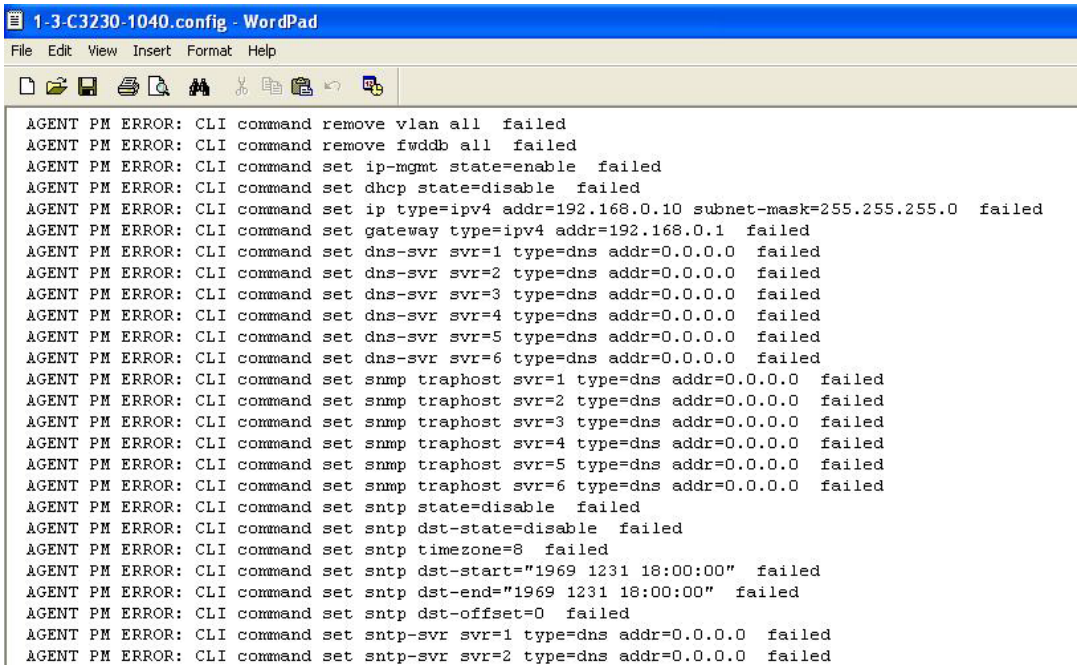
Yes	**No**
a) In the **TFTP Server Address** field, enter the IP address of the server. b) Click **Upload**. c) When the successful transfer message displays, click **OK**. d) Continue with step 8.	Continue with step 8 below.

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

9. Click the **OK** button to clear the Webpage confirmation message "*are you sure to proceed?*".
10. Click **Restore** button.
11. 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.
12. If the **Restore** operation fails, the **Prov Status** column displays "failure", then click the box to download an error log from the device.

The error log file (.ERR file) is downloaded to the TFTP/SFTP server address specified, in TFTP-Root, with a filename such as *1-11-C2210-1013.config*. You can open the file in a text editor.

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



See "The Config Error Log (config.err) File" for error messages and possible recovery procedures.

Backup and Restore - CLI Method

For more information about the CLI commands for backup and restore and all other CLI commands, refer to the *ION System CLI Reference, 33461*.

Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").

1. At the command prompt, check the current provisioning status. Type **show provision modules** and press **Enter**.

2. Specify a backup index item number and a config file name.
Type **set backup module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.

3. Specify a restore index item number and a config file name.
Type **set restore module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.

4. Specify 1-10 provision modules to be backed up. Type **backup prov module-list=xx** and press **Enter**.

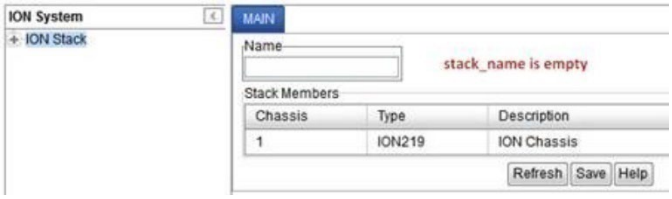
5. Specify 1-10 provision modules to be restored. Type **restore prov module-list =xx** and press **Enter**.

6. Verify the configuration. Type **show prov modules** and press **Enter**. For example:

```
C1|S1|L1D>show prov modules
Index   Module                          Config File               Prov Status
-------------------------------------------------------------------------------
1       [01]IONMM                       1-1-IONMM.config
2       [02]C6210-3040                  1-2-1-C6210-3040.config
3       [02:L2]REM:S6210-3040           1-2-2-S6210-3040.config
4       [03]C3230-1040                  1-3-1-C3230-1040.config
5       [04]C6010-3040                  1-4-1-C6010-3040.config
C1|S1|L1D>set backup module-index 1 config-file xxxxx
C1|S1|L1D>set restore module-index 1 config-file 1
C1|S1|L1D>backup module-list 1
Processing...
Processing...
Backup finished
C1|S1|L1D>restore module-list 1
Processing...
Restore finished
C1|S1|L1D> C1|S1|L1D>show prov modules
Index   Module                          Config File               Prov Status
-------------------------------------------------------------------------------
1       [01]IONMM                       1-1-IONMM.config          success
2       [02]C6210-3040                  1-2-1-C6210-3040.config
3       [02:L2]REM:S6210-3040           1-2-2-S6210-3040.config
4       [03]C3230-1040                  1-3-1-C3230-1040.config
5       [04]C6010-3040                  1-4-1-C6010-3040.config
C1|S1|L1D>
```

You can change the name of the "Config File" that displays when using the '**show provision modules**' command. Use the **refresh provision configure filename** command to change the name of the "Config File" displayed. **Note**: at IONMM FW v 1.4.2 the **set backup module-index**, **set restore module-index**, and **refresh provision configure filename** commands are no longer supported.

Note: When doing a backup all chassis cards or just backing up some cards in a chassis, if the "stack_name" field is empty, then the chassis serial number is added to the front of the tarfile.



Backup/Restore Status:
No backup/restore operations are processed.
This card is a remote remote x2x2x/x3x2x/x3x3x SIC and now is doing backup.
This card is a remote remote x2x2x/x3x2x/x3x3x SIC and now is doing restore.
This card is an IONMM or standalone x2x2x/x3x2x/x3x3x SIC and now is doing backup.
This card is an IONMM or standalone x2x2x/x3x2x/x3x3x SIC and now is doing restore.

Messages:
Error: this command should be executed on a remote mode x2x2x/x3x2x/x3x3x SIC!
Fail to set backup/restore operation!
Fail to set physical index!
Fail to set provisioning status!

Message: *The specified module does not exist!*
Invalid backup module-list, please give the parameter like module-list=1,4,13
Meaning: You entered an invalid Backup module list parameter.
Example:

```
Agent III C1|S1|L1D>backup module-list dddd
Invalid backup module-list, please give the parameter like module-list=1,4,13
Agent III C1|S1|L1D>backup module-list 3333
(The session will be forced to quit after you input "3333" similar characters.)
Agent III C1|S1|L1D>backup module-list 1
The specified module does not exist!
Agent III C1|S1|L1D>backup module-list 1
Processing...

Backup finished
Agent III C1|S1|L1D>
```

Recovery:
1. Enter a valid backup module-list input parameter
2. Retry the Backup operation. See the related section of the manual.
3. Contact Tech Support if the problem persists.

***Error**: Fail to transfer the file!*
Problem: ION 6 slots - CLI - perform backup configuring modules as a range fails.
Meaning: If all modules are configured to be backed up as range does not work correctly and has no validation.
Example:

```
backup module-list 1-10
```

```
Processing...
Backup finished (less than 15 seconds)
tftp put iptype ipv4 ipaddr 192.251.200.52 localfile 6-slots-1-1-1-IONMM.config
Tftp transferring...
Error: Fail to transfer the file!
```

Recovery: Configure as a series of modules (e.g., 2,3,4,5) and NOT including a range of modules (do not include e.g., 2-5) then all modules are backed up correctly.

Backup All and Restore All

IONMM v 1.3.18 adds Backup All and Restore All capabilities.
The Backup All and Restore All features can be configured via the ION System Web GUI or CLI commands. The Backup/Restore feature provides Automatic TFTP or SFTP transfer, backup, and restore of up to 41 modules at one time, time-stamped filenames that include the stackname and index number, and time-stamped tarfile containing all the config files. The cards being backed up / restored must be in Software mode (Hardware/Software Jumper set to Software mode).

Notes

1. TAR files are timestamped; individual files are not.
2. The default ION Stack name is changed from “ION Stack” (with a space) to “ION_Stack” (with an underscore in place of the space character). IONMM v1.3.18 adds the chassis Stack Name to the start of the tarfile and config files. If the stack name is empty, IONMM adds the chassis serial number Name to the start of the tarfile and config files. **Note**: at IONMM v 1.3.19, when doing a backup with no stack name the CLI prepends the serial number of the chassis to the TARFILE, but the Web UI does not; the Web just prepends an underscore, "_" (_backup.....).
3. Up to 41 cards can be backed up at one time. Up to 41 cards can be restored at one time.
4. The tarball contents are zipped under the directory 'tftpboot'.
5. When extracted, the directory 'tftpboot' is created holding the individual config files.
6. For current timestamping, SNTP must be enabled and running.
7. Before doing a Backup or Restore, disable the DHCP client for each device you want to backup/restore.
8. When a Backup is performed, the first action is to delete all files in the IONMM tftpboot directory (/tftpboot). This allows the new tarfile to contain the selected config files and nothing else.
   The second action is to delete all tarfiles in the root directory (/). This prevents the tarfiles from potentially filling up all the memory if a user backs up on a daily as is. The backup tarfile compresses all config files in the /tftpboot directory but doesn't include the directory itself.
9. After a Backup or Restore a file named *config.err* is created in the tftpboot directory that you can view in WordPad or similar package for troubleshooting purposes.
10. An Admin user has full rights to read/write all configurations via the Web and CLI. A Read-Write user can read/write all configurations except for Upgrade and Backup/Restore via the Web and CLI.
11. When a Backup or Restore starts, the session timer resets to 2 hours. When finished, it resets to 15 minutes.

Backup All and Restore All – CLI Method

CLI Commands

The following CLI commands are available for backup and restore operations:

- backup all
- backup module-list
- get restore module-list
- restore <tar filename> all
- restore <tar filename> module-list <string>
- saveconf module-list
- show provision backup modules
- show provision restore modules
- prov get tftp svr addr=ADDR

- prov set tftp svr type=(ipv4|ipv6}dns) addr=ADDR
- prov get sftp server addr=ADDR
- prov set sftp server type=(ipv4|ipv6|dns) addr=ADDR

Backup and Restore via the CLI

Note: For current timestamping, SNTP must be enabled and running. Use the **set sntp** and **show sntp** commands.

1. Set the TFTP server address using the command "**prov set tftp svr type ipv4 addr <TFTP IP>**".

If SFTP is enabled, use the command: "**prov set sftp server type=ipv4 addr=ADDR**".

Make sure that the TFTP or SFTP server is running.

2. Make sure that the ION cards are in Software mode. The ION cards will have config errors if the card is in Hardware mode. For a successful backup the cards must be in Software mode.

3. The "**backup all**" command finds all the cards in the chassis, backs up the configs in a time-stamped TAR file (*.tar), and transfers the file to the PC using TFTP or SFTP.

Note: When using the CLI to backup all or restore all, you must enter the **prov set tftp** or **prov set sftp** command first. See the following example:

```
Agent III C1|S1|L1D>prov set tftp svr type ipv4 addr 192.168.0.61
Agent III C1|S1|L1D>backup all
::-> timeStamp = 19700106_11-45-25-AM
::-> tftpaddr = 192.168.0.10
::-> rm -f /tftpboot/*
==> Found all chassis cards <==

::--> backupname = SN101829_backup_19700106_11-45-25-AM.tar
::--> backupModuleIndex = 18
::--> backupCommand = 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Processing...
.......................
Backup finished
Agent III C1|S1|L1D>
```

4. Enter the command "**backup module-list <*string*>**" where ***string*** is the index of the cards separated by commas. To get the indexes, use the command "**show prov back mod**", then select which index matches the cards you want to back up. For example:

```
Agent III C1/S19/L1D>show prov back mod
Index    Module                                    Config File
-------------------------------------------------------------------------
1        [00]backplane                             GP-1-0-0-backplane.config
2        [03]C3220-1040                            GP-1-3-1-C3220-1040.config
3        [06]C3220-1040                            GP-1-6-1-C3220-1040.config
4        [09]C3230-1040                            GP-1-9-1-C3230-1040.config
5        [12]C3230-1040                            GP-1-12-1-C3230-1040.config
6        [19]IONMM                                 GP-1-19-1-IONMM.config
7        [22]IONPS-A-R1                            GP-1-22-1-IONPS-A-R1.config
Agent III C1/S19/L1D>
```

Then you can form the command "**backup module-list 2,4,5**" or "**backup module-list 2,3,4,5**". This command backs up the configs of the selected cards in a time-stamped TAR file (*.tar) and transfers the file to the PC using TFTP or SFTP.

6. Enter the command **"restore <tarfile name> module-list <string>**".
For example: "***restore backup_20170131_04-12-04-PM.tar module-list 4,5***".

```
Agent III C1/S19/L1D>restore backup_20170131_04-12-04-PM.tar module-list 4,5
::-> tftpaddr = 192.168.0.61
::-> tftp -r backup_20170131_04-12-04-PM.tar -g 192.168.0.61
::-> mv /tftpboot /tftpboot_old
::-> tar -xvf backup_20170131_04-12-04-PM.tar
numberOfRestoreModules = 19  (Total number of modules in the tarfile)
Processing...
::-> entity_index = 147849216 slot = 3 level = 1
::-> entity_index = 152043520 slot = 4 level = 1

Restore finished
```

7. The "**restore all <tarfile name>**" command will TFTP the named TAR file to the IONMM and write the config files to the cards. This assumes that the cards' model numbers (e.g., C3220-1014) and slot numbers are the same as those in the TAR file.

```
Agent III C1/S19/L1D>restore all backup_20170131_04-12-04-PM.tar
::-> backupname = backup_20170131_04-12-04-PM.tar
::-> tftpaddr = 192.168.0.61
::-> tftp -r backup_20170131_04-12-04-PM.tar -g 192.168.0.61
::-> mv /tftpboot / tftpboot_old
::-> tar -xvf backup_20170131_04-12-04-PM.tar
::-> restoreCommand = 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Processing...
::-> Restore file name: GP-1-1-1-C3220-1040.config
::-> Restore file name: GP-1-2-1-C3220-1040.config
::-> Restore file name: GP-1-3-1-C3220-1040.config
::-> Restore file name: GP-1-4-1-C3230-1040.config
::-> Restore file name: GP-1-5-1-C3230-1040.config
::-> Restore file name: GP-1-6-1-C3221-1040.config
::-> Restore file name: GP-1-7-1-C3230-1040.config
::-> Restore file name: GP-1-8-1-C3220-1014.config
::-> Restore file name: GP-1-9-1-C2220-1014.config
::-> Restore file name: GP-1-10-1-C3110-1040.config
::-> Restore file name: GP-1-11-1-C6210-3040.config
::-> Restore file name: GP-1-12-1-C6010-3040.config
::-> Restore file name: GP-1-13-1-C3231-1040.config
::-> Restore file name: GP-1-14-1-C4110-4848.config
::-> Restore file name: GP-1-15-1-C3210-1040.config
::-> Restore file name: GP-1-16-1-C3220-1040.config
::-> Restore file name: GP-1-17-1-C3210-1013.config
::-> Restore file name: GP-1-19-1-IONMM.config
::-> Restore file name: GP-1-22-1-IONPS-A-R1.config

Restore finished
Agent III C1/S19/L1D>
```

When the restore is successfully finished the message *Restore finished* displays.

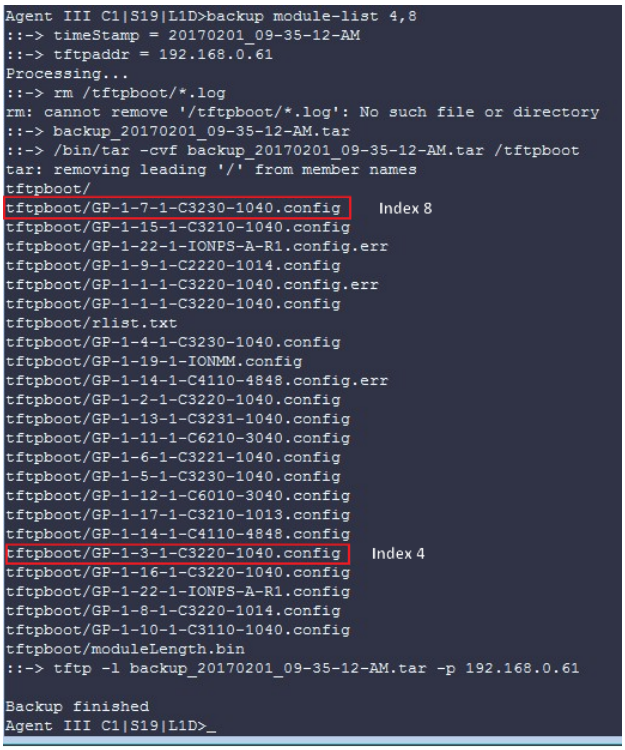
8. An SNTP server must be running on your PC for the time stamp to be accurate, and you must enable it on the IONMM:

```
Agent III C1|S1|L1D>set sntp ?
  dst-end     Set SNTP daylight saving end time.
  dst-offset
  dst-start   Set SNTP daylight saving start time.
  dst-state
  state
  timezone    Coordinated Universal Time timezone
Agent III C1|S1|L1D>set sntp state ?
  disable
  enable
```

```
Agent III C1|S1|L1D>
```

Note 1: Regarding the results of Step 5 above ("backup module-list <string>") used to save selected config files to tftpboot and transfer to PC with TFTP:

Only indexes 4 and 8 were backed up by the command, but the tftpboot directory has other config files which are also added to the tarfile. If Index 4 and Index 8 existed before, they will also be updated.



Troubleshooting - CLI Messages

After a Backup or Restore a file named *config.err* is created in the tftpboot directory that you can view in a text editor for troubleshooting purposes, as it shows the failed function.

Message:
Backup finished
Restore finished
Read backup_rlist.bin complete
Meaning: Successful Backup and Restore Messages (no action required).

Message:

Error: Wrong parameter number!
Error: this command should be executed on a device!
Error: Another user is using TFTP, please try it later!
Error: Fail to transfer the file!
error: Fail to set card entity index!
Error: Software version of this card is too old, please upgrade it!
Error: this command should be executed on IONMM or a standalone SIC!
Error: this command should be executed on a device!
Error: The specified module does not exist!
Error: backup all Invalid module: x
Error: backup module Invalid module: x
Error: Failed to set card entity index!
Error: Invalid backup module-list, please give the parameter like module-list=1,4,13
Error: Invalid restore module-list, please give the parameter like module-list=1,4,13
Error: At one time we can only backup at most 10 cards!
Error: Only 42 cards can be restored at one time.
Error: cannot get backplane stack name!
Error: cannot get card name!
Error: Restore backup has an invalid module: x
Failed to run command: x

Meaning: Failed backup and restore messages (action required).

Recovery:

1. Review the failed command parameters. **2.** Open the file *config.err* is in the tftpboot directory in WordPad or similar package to see the failed function. **3.** Verify the Backup or Restore command parameters. **4.** Re-try the Backup or Restore operation.

Message*:*
CLI command x failed.
The model type in unknown.
AGENT PM ERROR: failed to generate go port command!
AGENT PM ERROR:CLI command %s (tail) failed.
AGENT PM ERROR: CLI failed to send the quit command

Recovery: **1.** Review the failed command parameters. **2.** Open the file *config.err* is in the tftpboot directory in WordPad or similar package to see the failed function. **3.** Verify the Backup or Restore command parameters. **4.** Re-try the Backup or Restore operation.
Message: *tftp: timeout*

tftp: last timeout
Meaning: The tftp operation did not successfully complete. For example:

```
tftpboot/CIRCUIT-1-23-1-IONPS-A-R1.config.err
::-> tftp -l backup_19691231_09-09-37-PM.tar -p 192.251.240.104
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: last timeout

Backup finished
```

Recovery: **1.** Make sure the TFTP server is running and configured. **2.** Verify the IP address entered for the TFTP server is correct. **3.** Re-try the command. **Note** that the ION system will not let the ION login session timeout during tftp transmission. When Backup/Restore starts the session timer resets to 2 hours. When finished, the session timer resets to 15 minutes.

Message:
backup in use by CLI
Failed to open /inUse.txt
Creating /inUse.txt in root directory
Meaning: The flag "inUse.txt" indicates the CLI is currently performing the backup or restore function.
Recovery: **1.** Wait for the function in process to complete. **2.** Re-try the operation.

Message: *Failed to open /tftpboot/stackname.txt*
Meaning: Could not read and attach the stack name or chassis serial number to the config file name.
Recovery: **1**. Try changing the Stack name to exclude any space characters. 2. The Stack name must be less than 32 characters long and this pattern = /[a-zA-Z\d`~!@#$%&*(){}[\];:'",.<>\-_=+\\|\/?]{0,32}$/;

Message: <no warning message> when TFTP transfer fails
Meaning: IONMM CLI backup reports no error or warning when TFTP transfer fails. Backing up to a PC when the TFTP server isn't running fails to create the file on the TFTP server (expected), but there is no warning message on the IONMM to tell you that the TFTP transfer failed.
Recovery: 1. Verify success/failure by checking the tftp server's log.

Message: *AGENT PM ERROR: the configuration file /tftpboot/test-x-x-xxxx.config cannot be opened*
Meaning: The first web Restore All after a IONMM reset fails. This occurs after either a software system reboot or a card/chassis power cycle. All modules fail with the error message.
Recovery: Perform a Backup All, and then re-try the Restore All.

Issue: Legacy web backup also creates a TAR file
Meaning: A backup of an individual module via the web (legacy backup, meaning ALL not selected), a TAR file containing backups of all modules is downloaded to the TFTP server. A download of the backup of the individual module must still be performed.
Recovery: None; normal / unexpected behavior.

Problem: IONMM CLI subsequent backups fail if any original cards are removed from chassis after initial backup.
Meaning: 1. Install some cards in a chassis. 2. Do a backup all. 3. Remove a card from the chassis. 4. Do a Backup All. 5. Notice the second backup all fails, with a message about an "invalid module".
Recovery: Power cycle the IONMM.

Problem: During IONMM CLI backup, additional cards added to chassis after initial backup are not backed up during subsequent backups.
Meaning: 1. Install some cards in chassis. 2. Do a Backup All. 3. Add additional cards to the chassis. 4. Do a Backup All. 5. Compare the backup files; the additional cards are not in the second backup.
Recovery: 1. Verify the Backup All parameter entries. 2. Retry the operation. 3. Make sure you are running the latest IONMM firmware; upgrade if possible. 4. Retry the operation. 5. Contact Lantronix Technical Support.

Problem: Backup fails / IONMM hangs when running a "backup all" from the CLI (e.g., on a C3230 or a C6120).
Meaning: The card itself is causing the Backup failure.
Recovery: 1. Do a <ctrl>z to stop the process. 2. Remove/replace the failed card. 3. Try the Backup again.
Example:

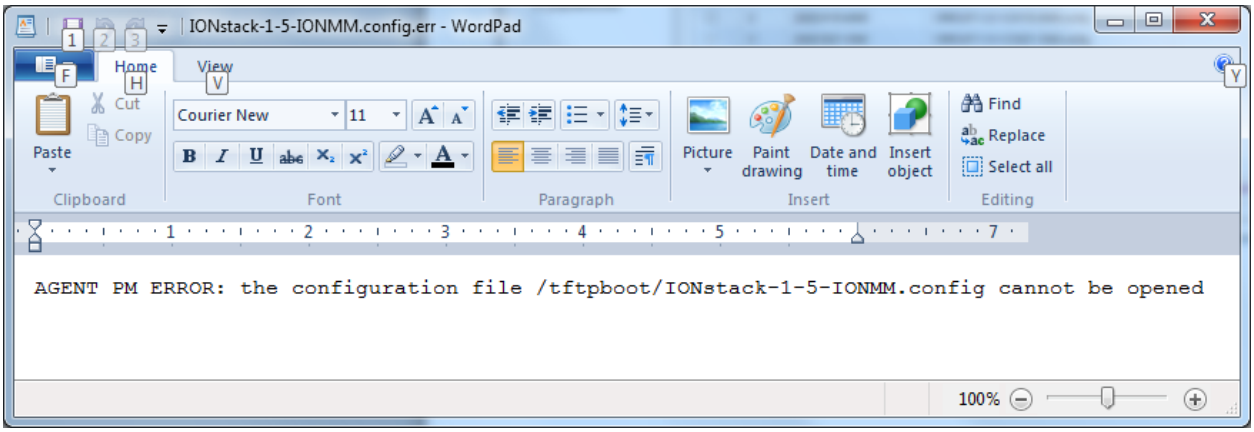
```
Agent III C1|S1|L1D>restore t all
==> BACKPLANE, Entity index = 8000000
==> AGENT, Slot = 1, Entity index = 8500000
Slot = 2, Entity index = 8900000
Slot = 3, Entity index = 8D00000
Slot = 4, Entity index = 9100000
Slot = 5, Entity index = 9500000
Slot = 7, Entity index = 9D00000
Slot = 8, Entity index = A100000
Slot = 9, Entity index = A500000
Slot = 10, Entity index = A900000
Slot = 12, Entity index = B100000
Slot = 13, Entity index = B500000
Slot = 14, Entity index = B900000
Slot = 15, Entity index = BD00000
Slot = 23, Entity index = DD00000
==> Found all chassis cards <==

backupname = t
::-> tftpaddr = 0.0.0.0
::-> tftp -r t -g 0.0.0.0
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: last timeout
::-> tar -xf t -C /tftpboot .
tar: t: No such file or directory
Read backup_rlist.bin complete

::-> Restore stack_name =
::-> val_array[0] = 1
::-> prov_info.prov_cfg[val_array[0]-1].ent_index = 8500000
```

```
::-> prov_info.prov_cfg[val_array[0]-1].restore_file = CIRCUIT-1-1-1-1-IONMM.con
fig


::-> Restore stack_name =
::-> val_array[1] = 2
::-> prov_info.prov_cfg[val_array[1]-1].ent_index = 8D00000
::-> prov_info.prov_cfg[val_array[1]-1].restore_file = CIRCUIT-2-1-3-1-C3221-104
0.config


::-> Restore stack_name =
::-> val_array[2] = 3
::-> prov_info.prov_cfg[val_array[2]-1].ent_index = 9100000
::-> prov_info.prov_cfg[val_array[2]-1].restore_file = CIRCUIT-3-1-4-1-C3100-404
0.config


::-> Restore stack_name =
::-> val_array[3] = 1
::-> prov_info.prov_cfg[val_array[3]-1].ent_index = 8500000
::-> prov_info.prov_cfg[val_array[3]-1].restore_file = CIRCUIT-1-1-1-1-IONMM.con
fig


::-> Restore stack_name =
::-> val_array[4] = 2
::-> prov_info.prov_cfg[val_array[4]-1].ent_index = 8D00000
::-> prov_info.prov_cfg[val_array[4]-1].restore_file = CIRCUIT-2-1-3-1-C3221-104
0.config


::-> Restore stack_name =
::-> val_array[5] = 3
::-> prov_info.prov_cfg[val_array[5]-1].ent_index = 9100000
::-> prov_info.prov_cfg[val_array[5]-1].restore_file = CIRCUIT-3-1-4-1-C3100-404
0.config

::-> array_len = 6
Processing...
::--> prov_cfg[val_array[0]-1].ent_index = 8500000
::-> Restore file name: CIRCUIT-1-1-1-1-IONMM.config
        Failed to set ION_PROV_TARFILE.2
::--> prov_cfg[val_array[1]-1].ent_index = 8D00000
::-> Restore file name: CIRCUIT-2-1-3-1-C3221-1040.config
::--> prov_cfg[val_array[2]-1].ent_index = 9100000
::-> Restore file name: CIRCUIT-3-1-4-1-C3100-4040.config
::--> prov_cfg[val_array[3]-1].ent_index = 8500000
::-> Restore file name: CIRCUIT-1-1-1-1-IONMM.config
::--> prov_cfg[val_array[4]-1].ent_index = 8D00000
::-> Restore file name: CIRCUIT-2-1-3-1-C3221-1040.config
::--> prov_cfg[val_array[5]-1].ent_index = 9100000
::-> Restore file name: CIRCUIT-3-1-4-1-C3100-4040.config
<ctrl-z> <remove/replace failed card>
.....................................................................% Unknown command.

Agent III C1|S1|L1D>
```

Troubleshooting - config.err File Messages

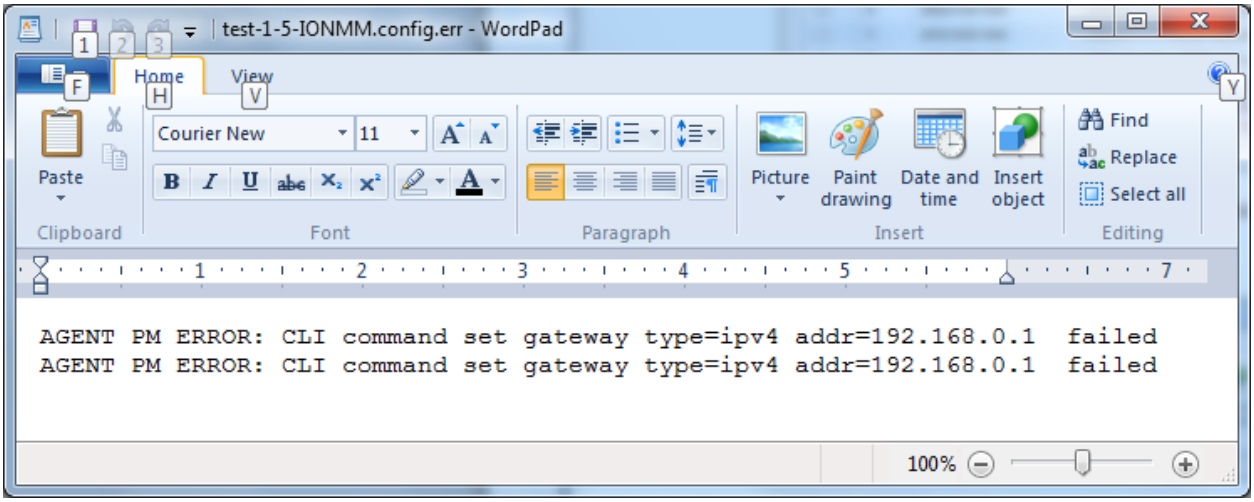
After a Backup or Restore a file named *config.err* is created in the tftpboot directory that you can view in WordPad or similar package for troubleshooting purposes, as it shows the failed function.

Message: `AGENT PM ERROR: the configuration file /tftpboot/IONstack-1-5-IONMM.config cannot be opened`



Meaning: The config file has a problem.
Recovery: 1. Make sure the TFTP server is running and its IP address is correct. . 2. Verify the filename is correct. 3. View the config.err file. 4. Retry the operation.

Message: `AGENT PM ERROR: CLI command set gateway type=ipv4 addr=192.168.0.1 failed`



Meaning: Trying to set the IP address was unsuccessful.
Recovery: 1. Verify the gateway type is IPv4. 2, Verify the IP address you entered. 3. View the config.err file. 4. Retry the operation.

Message: *AGENT PM ERROR: the configuration file /tftpboot/test-x-x-xxxx.config cannot be opened*
Meaning: The first web Restore All after a IONMM reset fails.
This occurs after either a software system reboot or a card/chassis power cycle. All modules fail with the error: "*AGENT PM ERROR: the configuration file /tftpboot/test-x-x-xxxx.config cannot be opened*".

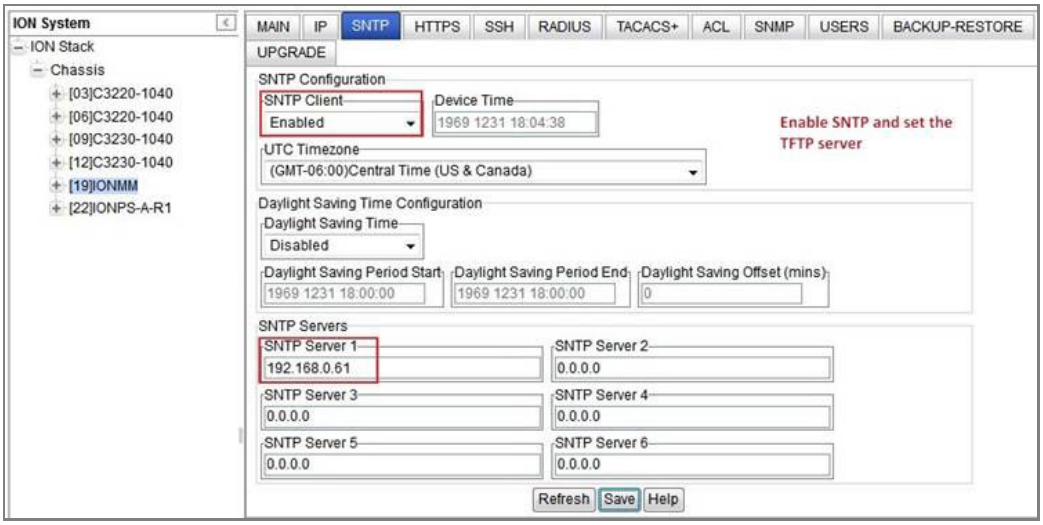
Recovery: Perform a Backup All, and then re-try the Restore All.
Message: *AGENT PM ERROR: the model type cannot be supported by Provision Module until now.*
Meaning: After performing a Backup All, the backup tar file contains an ION_stack-1-0-0-backplane.config file with the message.
Recovery:
1. Verify the Backup All parameter entries.
2. Retry the operation.
3. Make sure you are running the latest IONMM firmware; upgrade if possible.
4. Retry the operation.
5. Contact Lantronix Technical Support.
Example:

```
IONMM-12157809 C1|S19|L1D>cat /tftpboot/IONstackName-1-0-0-backplane.config.err
AGENT PM ERROR: the model type  cannot be supported by Provision Module until now.
AGENT PM ERROR: the model type  cannot be supported by Provision Module until now.
AGENT PM ERROR: the model type  cannot be supported by Provision Module until now.
AGENT PM ERROR: the model type  cannot be supported by Provision Module until now.
IONMM-12157809 C1|S19|L1D>backup module-list 1,2,3,4,5,6,7,8
Processing...

Backup finished
```

Message: Backup status *ongoing* displays continuously.
Meaning: When a Backup All fails, it can become a run-away process. After a Backup All failure, entering the **`show prov back mod`** command will indicate that the backup status is *ongoing*. The status remains that way until the IONMM is rebooted. Another backup all cannot be successfully completed while a backup is ongoing.
Recovery: Reboot the IONMM and try the Backup All function again.

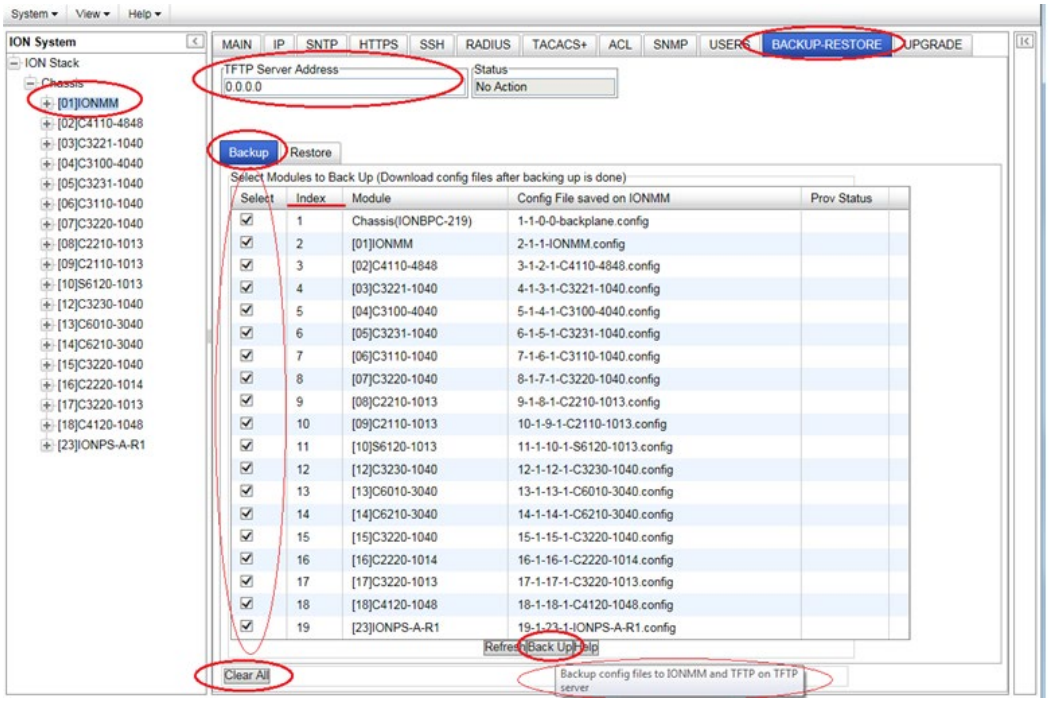
Backup All and Restore All – Web Method

The Backup All and Restore All at IONMM v1.3.18 and above lets you backup and restore up to 41 modules via the Web GUI. An SNTP server must be running on your PC for the time stamp to be accurate, and you must enable it on the IONMM Web UI as shown below:

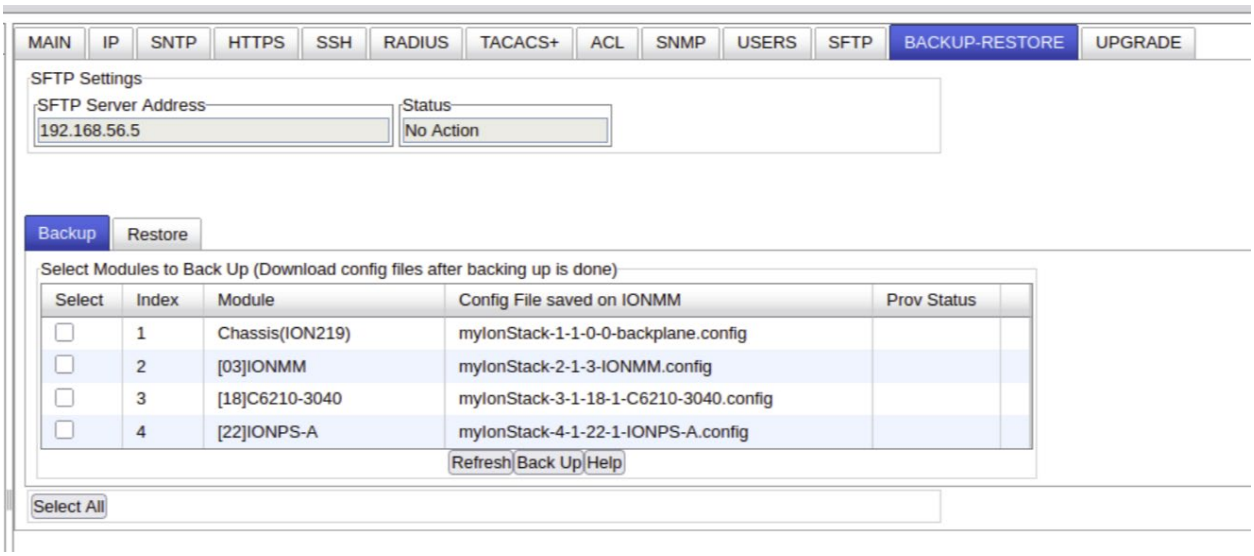


Backup All via the Web UI

1. Navigate to the IONMM > BACKUP-RESTORE > Backup tab and click the **Select ALL** button.
A checkmark is placed in the Select column for all modules, and the **Select All** button toggles to display **Clear All**.

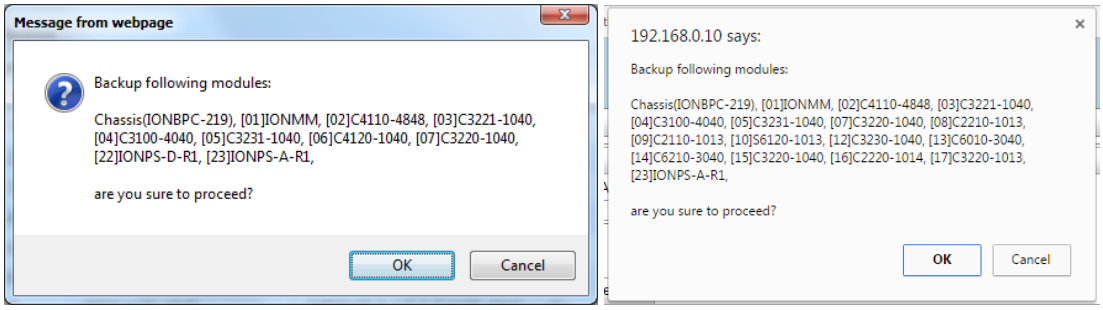


If SFTP is enabled, the Backup-Restore webpage will display SFTP Server address.

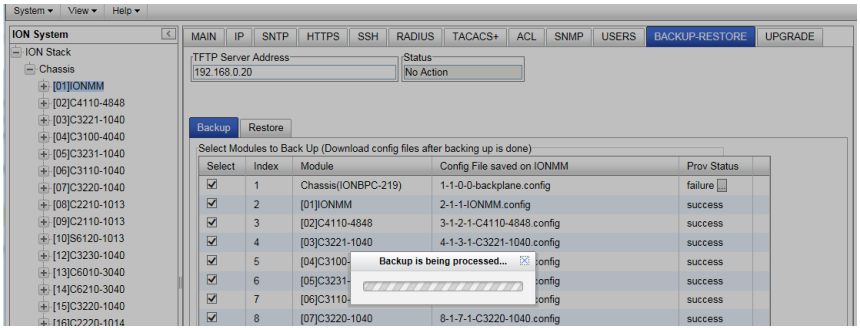


2. Click the **Back Up** button. This will backup config files to IONMM and TFTP/SFTP on the TFTP/SFTP server.

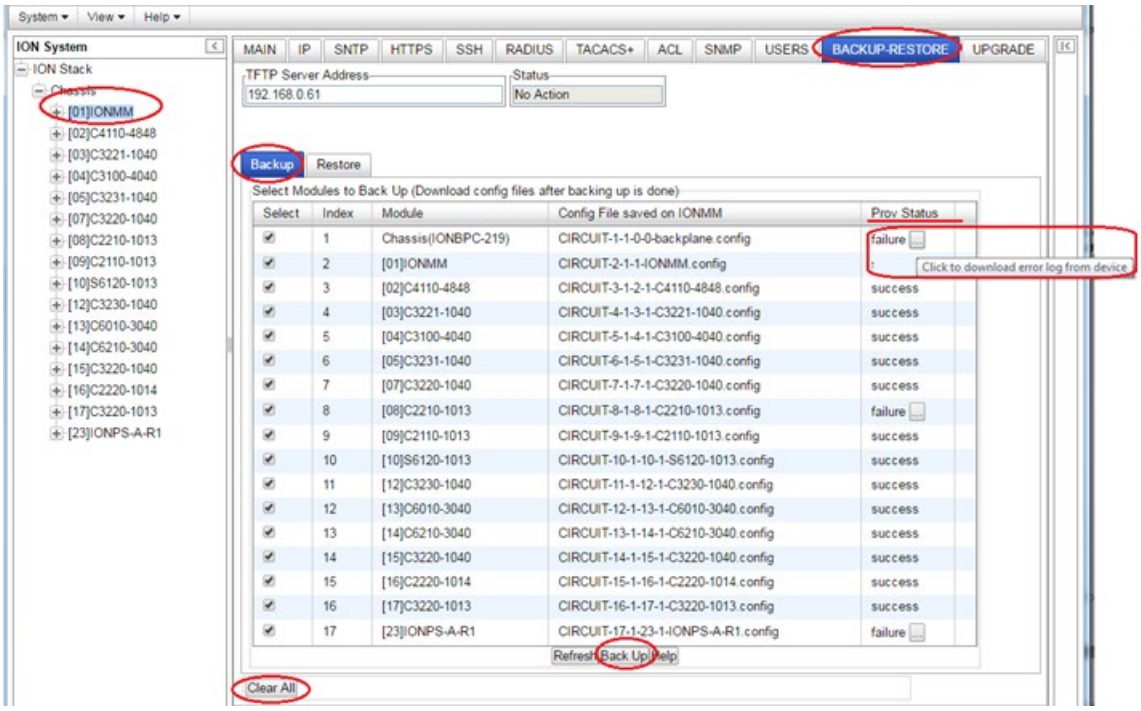
A webpage message displays listing the selected modules for backup and prompting you to verify that you want to proceed with the backup of these modules.



3. If you are not sure click **Cancel**. If you are sure click **OK**. The backup process begins. The screen is grayed out while the Backup is in progress.



4. When the backup process completes, the Backup page displays again with the new status (*success* or *failure*) displayed in the “Prov Status” column. If Prov Status *ongoing* displays longer than momentarily, click **Refresh**.



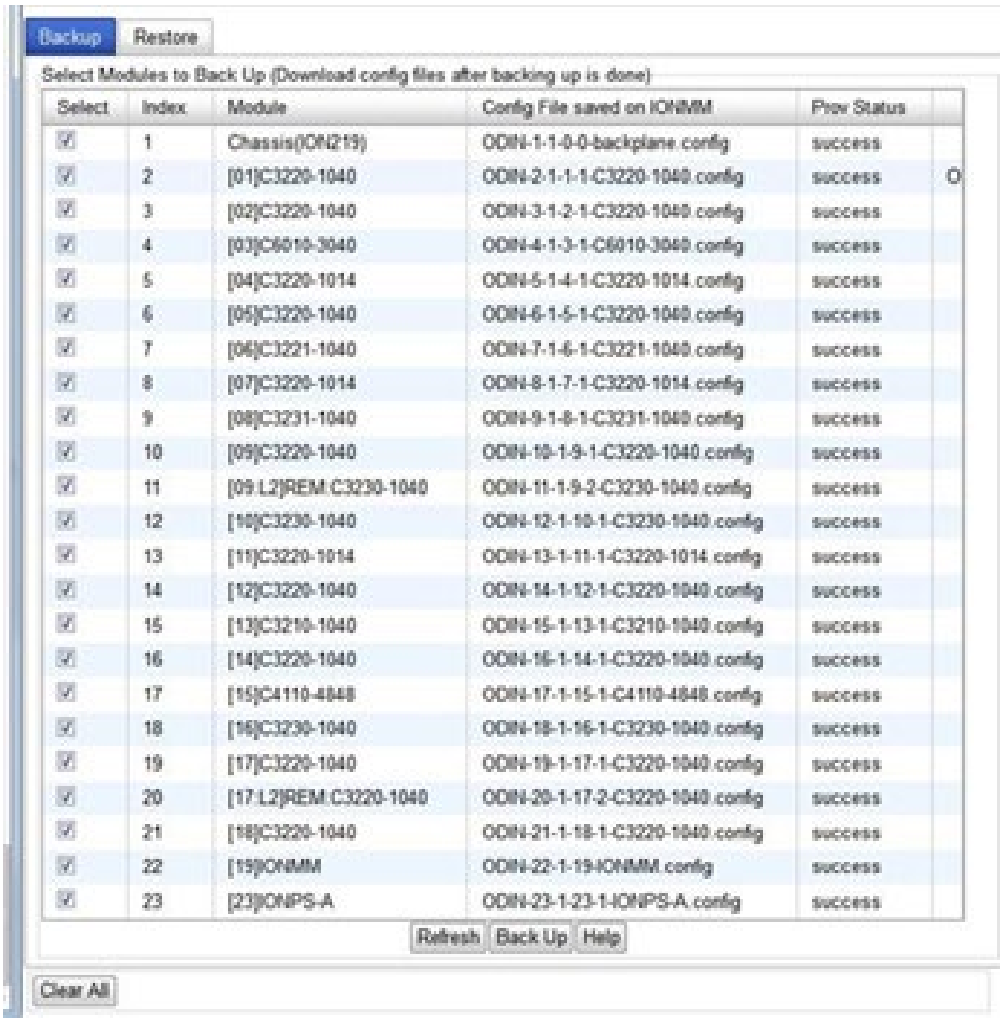
5. Verify the status shows *success* in the Prov. Status column.

6. If the status shows *failure*, click the failure ... icon to download an error log from the failed device. Note that the TFTP/SFTP server must be configured and running.

7. At the confirmation message, click the **OK** button to clear the webpage message. Make sure the TFTP/SFTP server is up and configured, verify the name and location of the file being transferred, and continue operation.

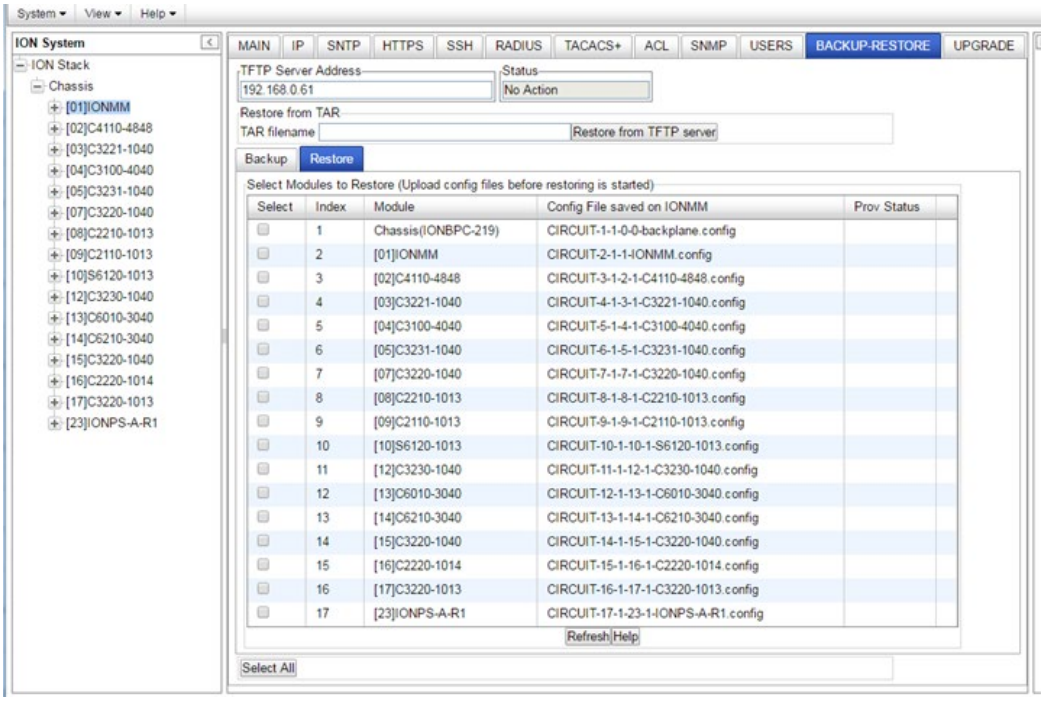
8. Hover the cursor over the failure ... icon in the "Prov Status" column of a row; you can click the icon to download the error log from the device. The file *config.err* is created in the tftpboot directory that you can view in WordPad or similar package to see the failed function.

Example: The web successfully backed up 23 cards:

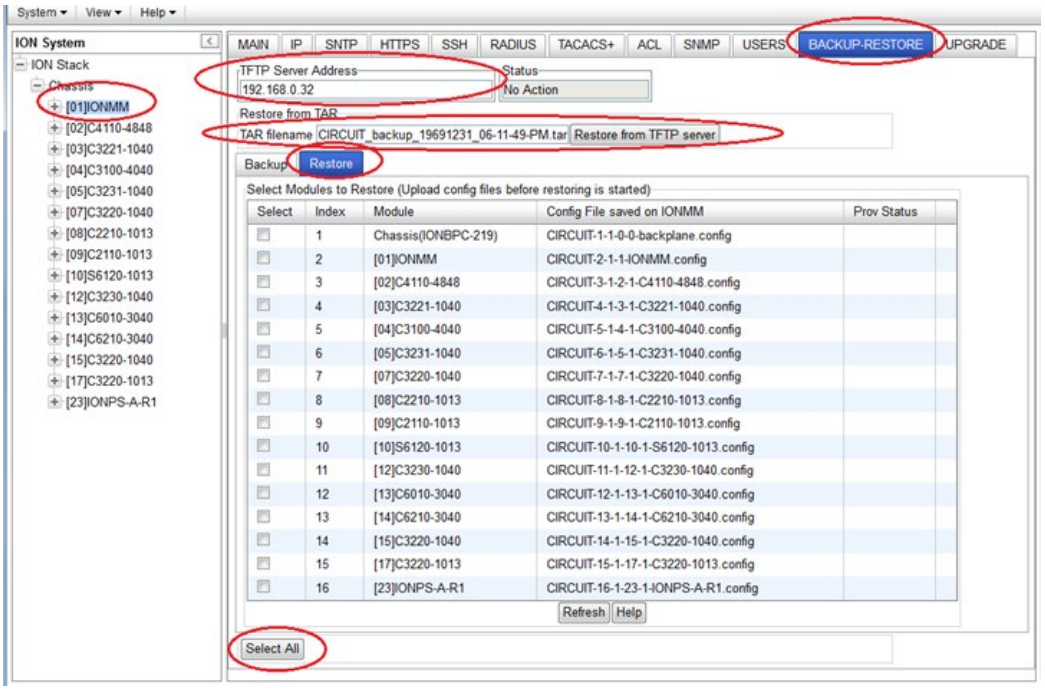


Restore All via the Web UI

IONMM at v 1.3.18 lets you select and restore all the discovered module via the Web GUI. The cards being backed up / restored must be in Software mode (Hardware/Software Jumper set to Software).



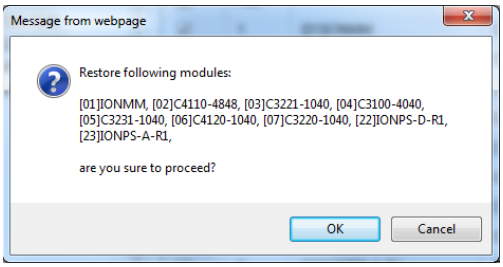
1. Navigate to the IONMM > BACKUP-RESTORE > Restore tab and click the **Select All** button. A check mark is placed in the Select column of each discovered module and the **Select All** button toggles to display **Clear All**.



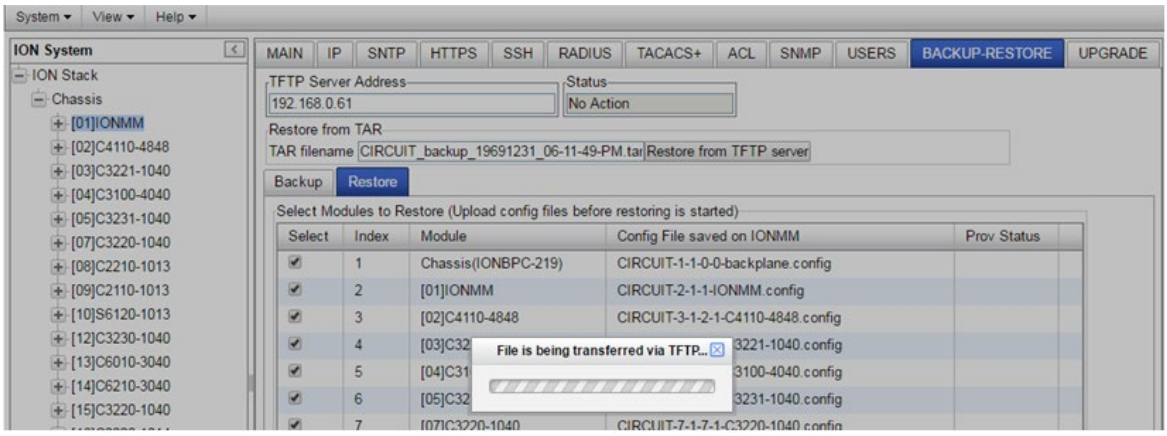
If SFTP is enabled, the web page will display the SFTP Server Address.

2. Enter the TFTP Server Address (e.g., 192.168.0.32 shown above).
3. Enter the TAR filename (e.g., CIRCUIT_backup_19691231_06-11-49-PM.tar shown above).

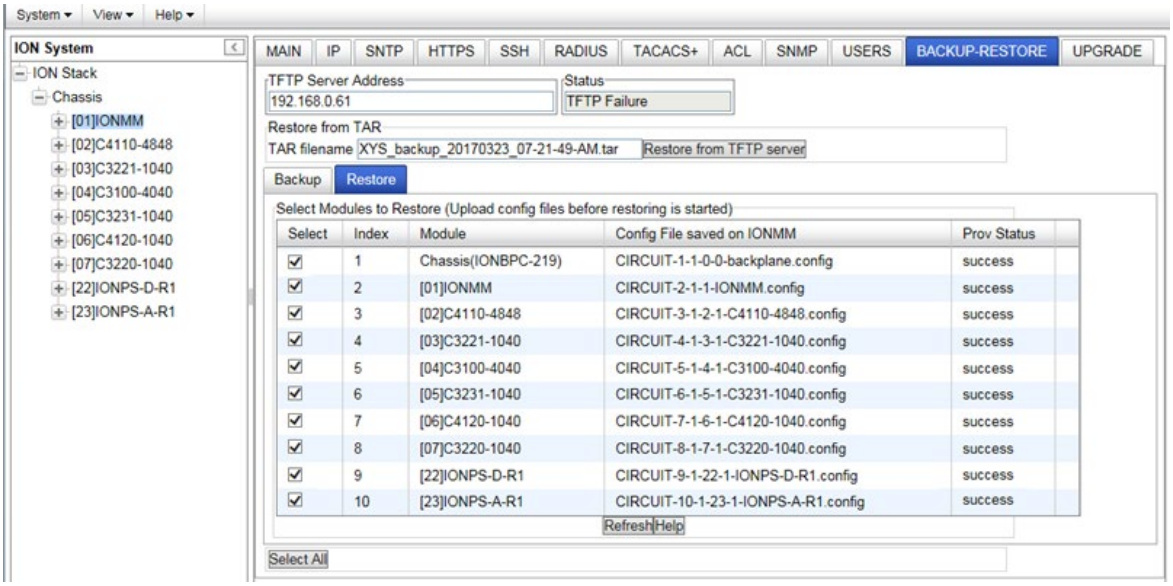
4. Click the **Restore from TFTP/SFTP server** button. A webpage message displays listing the selected modules for restore and asking to verify that you want to proceed with restoring these modules.



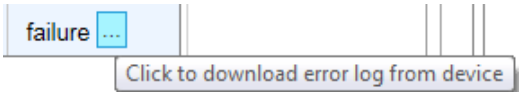
5. If you are not sure click **Cancel**. If you are sure click **OK**. The restore process begins. The screen is grayed out while the Restore is in process, and the message "*File is being transferred via TFTP...*" displays.



6. When the restore process completes, the Restore page displays again with the new status (*success* or *failure*).



7. In the Prov. Status column, verify the status shows *success*. If the status shows *failure*, click the icon to download an error log from the failed device. Note that the TFTP/SFTP server must be configured and running.



8. At the confirmation message, click the **OK** button to clear the webpage message. Make sure the TFTP/SFTP server is up and configured, verify the name and location of the file being transferred, and continue operation.

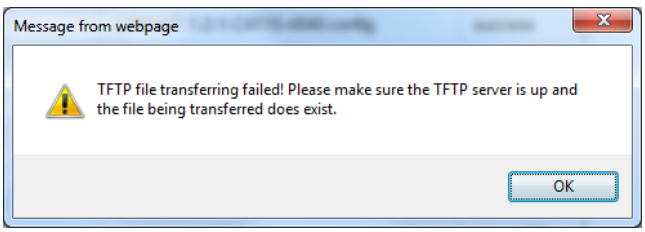
Troubleshooting – Web UI Messages

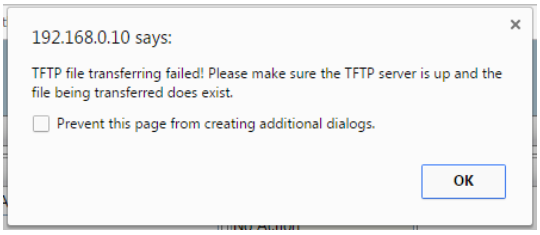
After a Backup or Restore a file named *config.err* is created in the tftpboot directory that you can view in WordPad or similar package for troubleshooting purposes, as it shows the failed function.

Message:
Must enter Tar filename
Please select at least one module.
Backup following modules:
Restore following modules:
Recovery: 1. Follow the message directions.

Message:
Backup is being processed...
Restoring is being processed...
Sending backup commands succeeded
Sending restore commands succeeded
Recovery: 1. No recovery required.

Message: *TFTP Server Address is empty or invalid!*
Message: *Message from webpage. TFTP file transferring failed! Please make sure the TFTP server is up and the file being transferred does exist.*
Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Make sure the TFTP server is up and configured. **3.** Verify the name and location of the file being transferred. **4.** Continue operation.





Message: *Setting values failed (snmp operation error, possible reasons: invalid data, error data sequence, etc)*
Meaning: May display on Backup from Web UI for no apparent reason.
Recovery: Click the Refresh button at the bottom of the web page and continue operation.

Message: *You are now logged out.*
Meaning: Displays after the "TFTP file transferring failed" or after the 15 minute inactivity time is reached.
Recovery: Click the **OK** button and log back in to the ION system.

Message: *Cannot proceed because some other TFTP operation is currently in progress!*
Meaning: You tried to start a second tftp transfer operation when one is already in process.
Recovery: **1.** Wait for the current tftp transfer operation to complete. **2.** Re-try the command.
Note that the ION system will not let the ION login session timeout during tftp transmission. When a Backup/Restore starts, the session timer resets to 2 hours. When finished, the session timer resets to 15 minutes.

Message: *File is being transferred via TFTP...*
Meaning: A transfer of files is currently in progress between the TFTP server and the device *tftpboot* directory.
Recovery: 1. Wait for the tftp transfer to complete. 2. Continue operation.

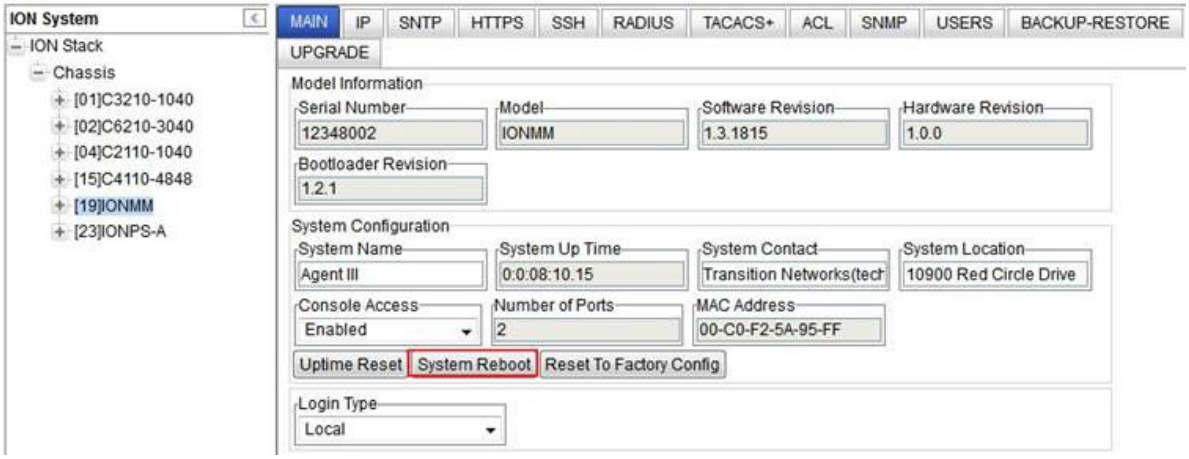
Message: *File has been successfully transferred via TFTP.*
Meaning: The ftp transfer was successfully completed.
Recovery: None; continue operation.

Message: *Restore complete* (but the related tftp transfer failed)
Meaning: IONMM CLI restore from an invalid tftp filename causes IONMM to restore from internal memory.
The message "*Restore complete*" displays, but the tftp transfer failed. For example, typing '**restore 123 all**' (where **123** is an invalid tftp filename) causes the IONMM to restore from its last backup, which apparently still resided on the IONMM's internal memory. The restore should have aborted after the tftp transfer failure, but instead the transfer was completed to IONMM memory.
Recovery: 1. Check the *config.err* file in the tftpboot directory to see the failed function. 2. Re-try the tftp transfer operation with a valid tftp server address and filename.

Message:
Failed to open file /tftpboot/backup_rlist.bin
Failed to read backup_rlist.bin\n
Failed to open /stackname.txt\n
Failed to open backup_rlist.bin\n
Failed to write backup_rlist.bin\n
Meaning: The backup failed.
Recovery: **1.** Open the file *config.err* is in the tftpboot directory in WordPad or similar package to see the failed function. **2.** Verify the Backup command parameters. **3.** Make sure the chassis name has less than 32 ASCII printable characters. **4.** Re-try the Backup or Restore operation. **5.** Reset the IONMM card.

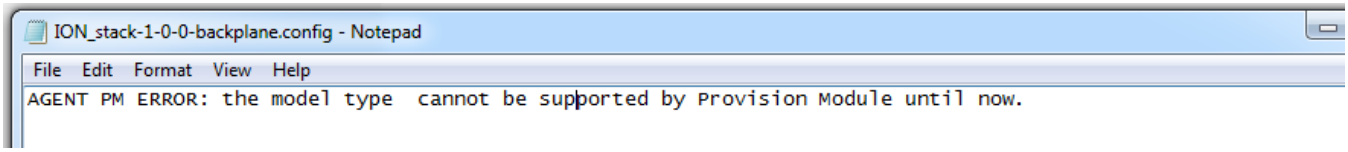
Message: *Sending backup commands failed (snmp operation error, possible reasons: invalid data, error data sequence, etc)*

Meaning: The message displays momentarily on the web at the start of backups and restores. It doesn't cause any issues; it is related to doing multiple operations in a row – not present the first time or just a flash and then longer the next operation(s).
If you cancel a web Backup operation by clicking the upper right X in the progress window, subsequent backups will fail until a Restore is performed or the IONMM is reset. The subsequent backup looks like it's running but it never completes.
Recovery: **1.** Click the **Refresh** button to clear the message. **2.** Continue operation. **3.** Click the **System Reboot** button when ongoing status doesn't change to success or failure. **4.** Continue operation.



Message:
Sending backup commands failed
Sending restore commands failed
Setting values failed
Backup is being processed… displays continually and Backup/Restore All hangs
Meaning: Displays when a backup or restore fails. Backup of 6120 fails with "*Sending backup commands failed (snmp operation error, possible reasons: invalid data, error data sequence, etc)*" in the lower left corner in red in
the Web UI.
Meaning: The operation gives no failure indication; it just never completes. After canceling it with the x in the progress pop-up, subsequent backup or restore attempts show the above failure in the lower left status area.
Recovery: **1.** Open the file *config.err* is in the tftpboot directory in WordPad or similar package to see the failed function. **2.** Verify the Backup or Restore page parameters. **3.** Make sure the chassis name has 32 or less ASCII printable characters. **4.** Re-try the Backup or Restore operation. **5.** Reset the IONMM card.

Message: *AGENT PM ERROR: the model type cannot be supported by Provision Module until now.*
Meaning: After performing a Backup All in the Web UI, the backup tar file contains an ION_stack-1-0-0-backplane.config file with the message.
Recovery:
1. Verify the Backup All parameter entries.
2. Retry the operation.
3. Make sure you are running the latest IONMM firmware; upgrade if possible.
4. Retry the operation.
5. Contact Lantronix Technical Support.



Message: *restore failed*

Meaning: Currently, when the IONMM restores a config to a card that is in hardware mode, the restore fails because the card is in hardware mode, and config changes can only be written to the card while it's in software mode. The IONMM reports the restore as "failed" but does not explain why the restore failed. When you try to restore a config and the restore fails, the card that the restore was attempted on may be left in an undefined state of part old config and part new config.

Recovery: The cards being backed up / restored must be in Software mode (Hardware/Software Jumper is set to Software mode). Verify that the cards' Web GUI MAIN tab Configuration Mode displays "Software".

Disabling USB Console Access

Access to the IONMM through the USB serial interface can be disabled as a security precaution. When disabled, the IONMM will not respond to CLI commands entered by a local management station across the USB serial interface. The only access to the IONMM will be through either a Telnet session or the Web interface.

Note: Access via the USB serial Console interface can be disabled using either the CLI or Web method.

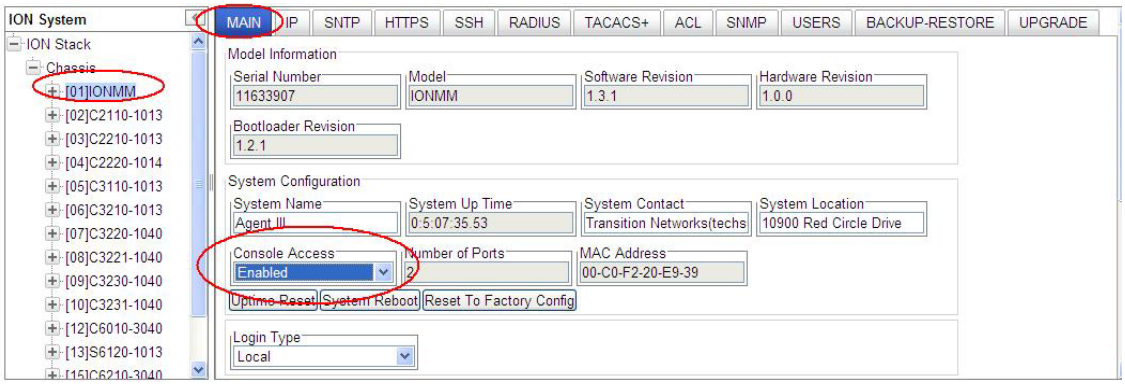
Disabling Console Access – CLI Method

1. Set the status of the device's USB connection to disabled. Type **set usb state=disable**.
2. Press **Enter**.
3. Verify the status of the device's USB connection is disabled. Type **show usb state**.
4. Pres **Enter**. The USB state displays:

```
C1|S7|L1D>show usb state
USB port state:                disable
```

Disabling Console Access – Web Method

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



4. In the **Console Access** field, select **Disabled**. The default is **Enabled**.
5. Scroll to the bottom and click **Save**. With the IONMM's USB connection disabled, it will no longer respond to CLI commands entered by a local console via the USB serial interface. The only access will now be through either a Telnet session or the Web interface.

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. For information on the status of important ION system files resulting from this operation, see " Appendix C: ION System File Content and Location".

IMPORTANT

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

Resetting Defaults – CLI Method

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **reset factory**.
3. Press **Enter**. The message "*Warning: this command will restart the specified card, connection will be lost!*" displays.

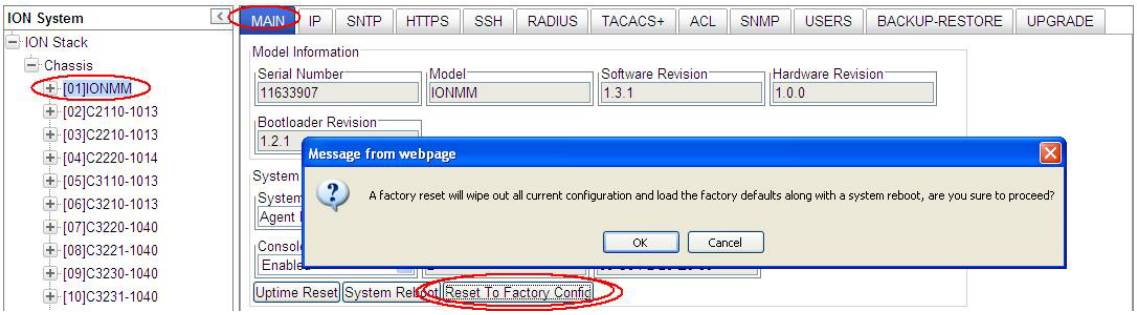
   All configuration parameters are reset to their factory values. For a list of all factory defaults, see Appendix B: "Factory Default Settings").

   Note: Your USB and/or Telnet session will be disconnected.
4. Set the IP configuration (see "Setting Up the IP Configuration").

Resetting Defaults – Web Method

Note: This operation deletes all configuration information that was saved in the IONMM, including the IP and gateway addresses you assigned to the IONMM.

1. Access the IONMM 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 Default Settings".

   Note: Your Web session will be discontinued.

6. Set the IP configuration (see "Setting Up the IP Configuration").

Resetting Uptime

The IONMM uptime field displays the amount of time that the IONMM 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.

A System Reboot or a Reset to Factory Configuration resets the uptime counter automatically.

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

Uptime Reset – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the device level command prompt type: **reset uptime** and press **Enter**. The System Up Time field resets to zero, and immediately begins to increment.

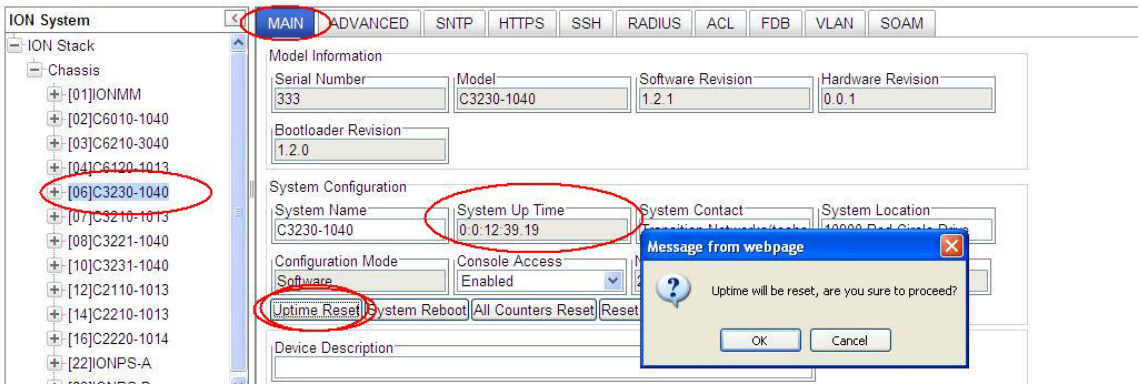
   For example:
   ```
   C1|S1|L1D>reset uptime
   C1|S1|L1D>
   ```

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

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

Uptime Reset – Web Method

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. At the **MAIN** tab, locate the **System Configuration** section.



3. If desired, observe and record the **System Up Time** field count.
4. Click the **Uptime Reset** button.
5. When the "*Uptime reset, are you sure*" window displays, click **OK**.

   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 is reset to zero, and immediately begins to increment.

System 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.

For information on the status of important ION system files resulting from this operation, see "Appendix C: ION System File Content and Location".

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

Rebooting the System – CLI Method

After an x323x reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.

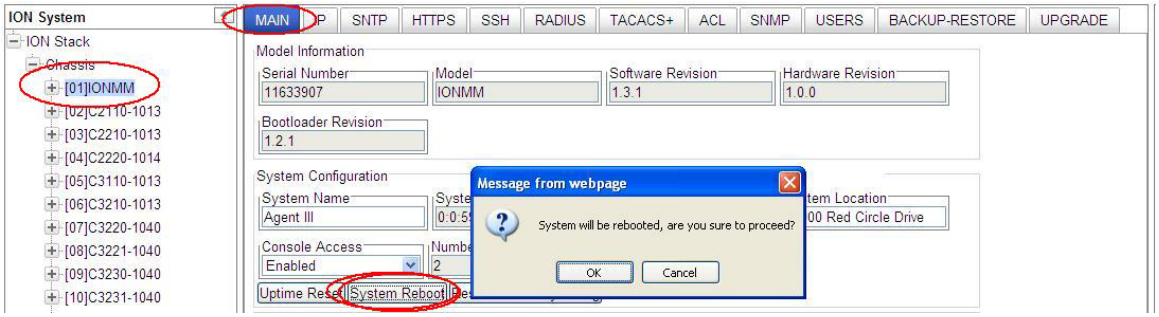
1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login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

Rebooting the System – Web Method

Note: 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).

Note: if you have a USB or Telnet session established, terminate the session before doing the reboot.

1. Access the IONMM through the Web interface (see "Starting 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 **OK** to proceed or click **Cancel** to quit the reboot.

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

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

Use the **serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem)** commands to transfer a file over a serial line. These commands can only be entered at the device level (e.g., when the command line prompt is C1|S8|L1P1> or similar). These commands function like the TFTP/SFTP download function; technical support can download configuration files and firmware files through the IONMM USB port by entering the corresponding CLI commands.

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

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

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting 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 re-
trieve file!
now start to transfer the file  ...
ŠCCCCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file  ...
Šlsz: cannot open /tftpboot/xxxx: No such file or directory
BB0BB0BB0
BB0BB0
Can't open any requested files.
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial upgrade protocol zmodem file=xxxx
now start to transfer the file  ...
**B000000063f694ceive.**B000000063f694
CCCCCCCCCCBB0BBBB0BBBB0BBBB0BB0BB0BB0BB0
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.

Upgrade the Firmware

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

Lantronix recommends that before completing any steps on an install that a user verify that the IONMM has the latest firmware version installed and running. Find the latest firmware version on the IONMM webpage (login required). These procedures require that you have the TFTP or SFTP server running and configure. Note that after upgrading from a version earlier than 1.5.0, new backups should be made.

For information on the status of important ION system files resulting from this operation, see "Appendix C: ION System File Content and Location".

IMPORTANT

Upgrading modules via the IONMM may cause some configuration backup files to be lost.

Note: You cannot upgrade a module with multiple BIN files. Do not upgrade an ION SIC and its attached remote standalone device at the same time.

You can upgrade the IONMM or NID Firmware from the Command Line Interface (CLI) or via the Web interface. Note that the ION106-x chassis limit the size of the db.zip file to 50 Mb for bulk upgrades. Note that the upgrade firmware filename is limited to 32 characters in length.

Upgrading IONMM and/or NID Firmware – CLI Method

To upgrade the IONMM Firmware from the CLI.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting 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
   For an SFTP server, use:
   prov get sftp server addr
   prov set sftp server type=(ipv4|ipv6|dns) addr=ADDR
4. Locate the latest firmware files from the IONMM product webpage. Go to https://www.lantronix.com/products/ionmm-series-2/.
5. Locate the "**Agent Firmware**" section and click the link in the right hand column (e.g., "Download IONMM.bin.1.0.5.bin").
6. Zip the downloaded file.
7. Retrieve the firmware database file using the **tftp get or sftp get** command to get the file from the TFTP/SFTP 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]

For SFTP, use:

sftp get 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|S7|L1D>upgrade module
Available modules:

index     module                                    loc
-------------------------------------------------------------------------
1         ION219                                    c=1 s=0 l1d
2         C3230-1040                                c=1 s=3 l1d
3         C3230-1040                                c=1 s=5 l1d
4         S3230-1040                                c=1 s=5 l1ap=2 l2d
5         IONMM                                     c=1 s=7 l1d
6         C3231-1040                                c=1 s=10 l1d
7         C2110-1013                                c=1 s=12 l1d
8         C2210-1013                                c=1 s=13 l1d
9         C2220-1014                                c=1 s=16 l1d
10        C3220-1040                                c=1 s=18 l1d
11        IONPS-A                                   c=1 s=22 l1d

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

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

11. Choose 1-8 modules to upgrade (# **1-6,10,11** 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|S7|L1D>show firmware upgrade result
index     module                          status      reason  time started     time completed
-------------------------------------------------------------------------------------------
1         card registering...             success                 00:21:23          00:21:32
2         C3230-1040 c=1 s=3 l1d          inProgress              00:21:23          00:00:00
3         C3230-1040 c=1 s=5 l1d          inProgress              00:21:24          00:00:00
4         S3230-1040 c=1 s=5 l1ap=2 l2d   inProgress              00:21:24          00:00:00
5         IONMMc=1 s=7 l1d                success             00:21:24          00:21:47
6         C3231-1040 c=1 s=10 l1d         inProgress          00:21:26          00:00:00
7         C3220-1040 c=1 s=18 l1d         inProgress              00:21:26          00:00:00
8         IONPS-A c=1 s=22 l1d            success                 00:21:29          00:21:40
C1|S7|L1D>
```

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

Upgrading the IONMM Firmware – Web Method

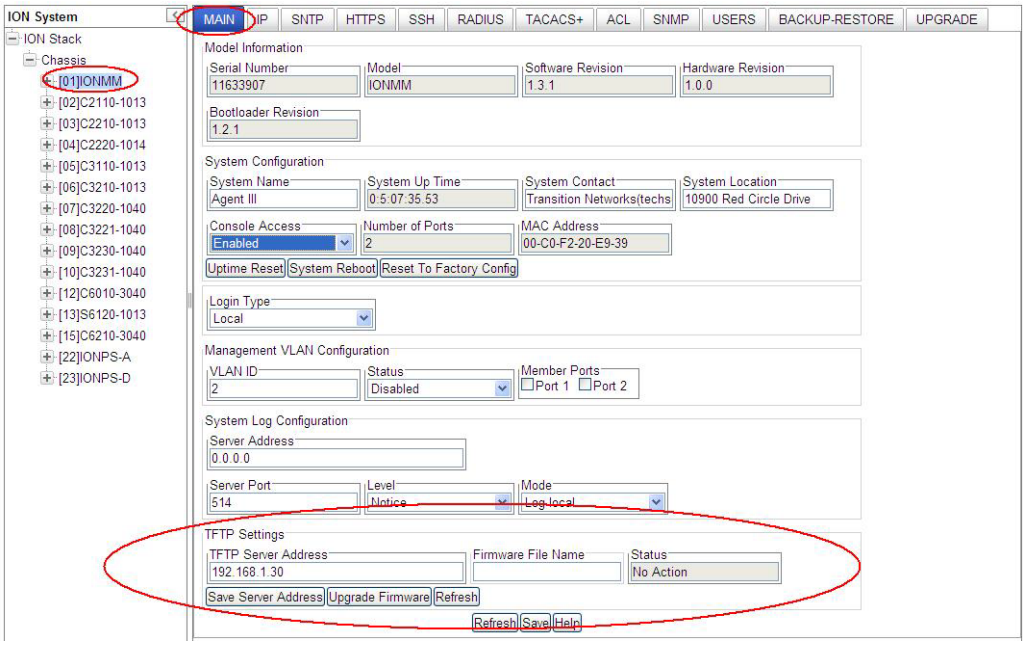
The following procedure is for upgrading the firmware in the IONMM through the Web Interface. If other modules in the ION Chassis are to be upgraded at the same time as the IONMM, see the related *ION NID User Guide*.

Note: The ION106-x chassis limits the size of the db.zip file to 50 Mb for bulk upgrades. Note that after upgrading from a version earlier than 1.5.0, new backups should be made.

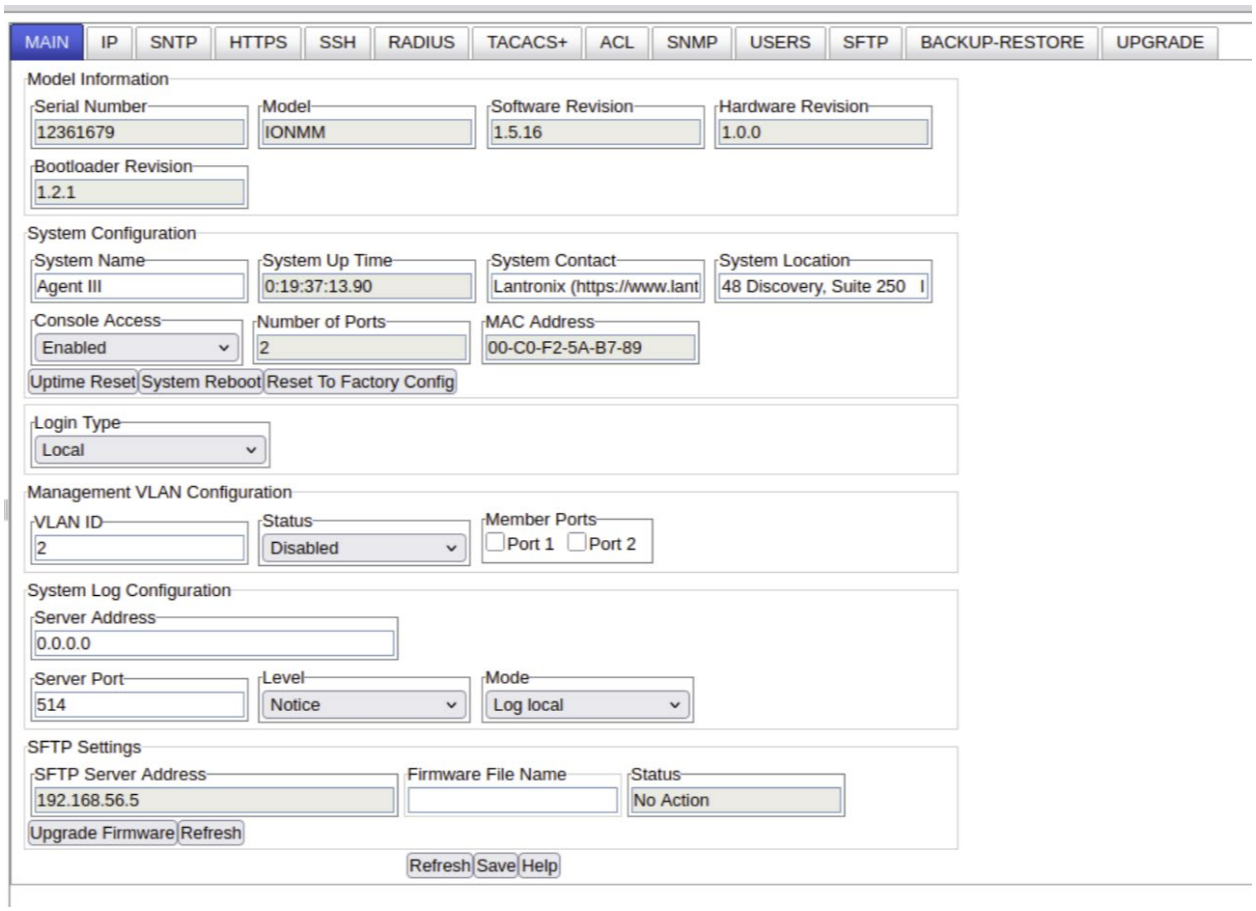
Note: The TFTP or SFTP server must be configured and running, and the upgrade files must be resident in the default directory on the TFTP or SFTP server (normally *C:/TFTP-Root*).

The following procedure describes the upgrade method if you are using a TFTP server. To perform a firmware upgrade using SFTP, configure and enable the SFTP server using the SFTP tab. See "Configuring SFTP".

1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. At the **MAIN** tab, locate the **TFTP Settings** section.



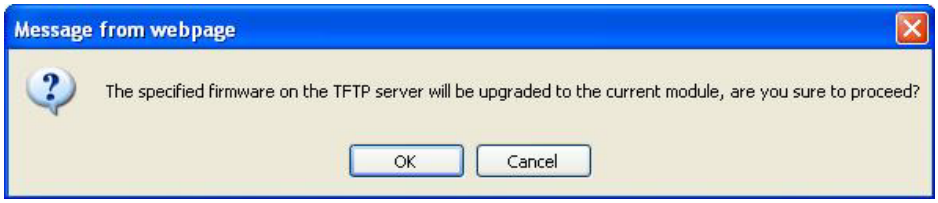
If SFTP is enabled, the web page displays the SFTP Server Address.



5. In the **TFTP Server Address** field, enter the IP address of the TFTP server where the upgrade file is located (e.g., 192.168.1.30 in the screen above). To save the TFTP server address for future use, click **Save Server Address** (optional).

6. In the **Firmware File Name** field, enter the name of the upgrade file (e.g., *IONMM_1.1.0_AP.bin*). The file extension ***.bin*** must be included.

7. Click the **Upgrade Firmware** button. A confirmation window displays.

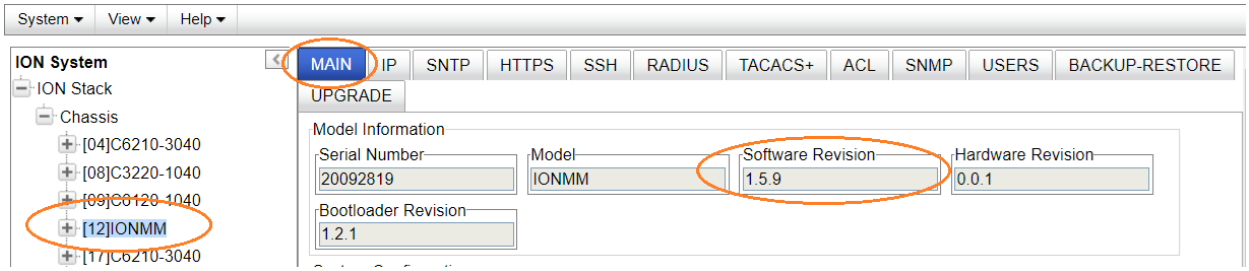


8. Click **OK**. The upgrade begins and the message "*the firmware is being upgraded*" displays.

   The Status field displays "*Success*" when the firmware upgrade successfully completes.

If the upgrade fails, the message "*The firmware upgrade failed!*" displays. Click the web page **OK** button to clear the message. (If the **Status** field displays the reason "*TFTP Failure*", make sure the TFTP server is running and properly configured.)

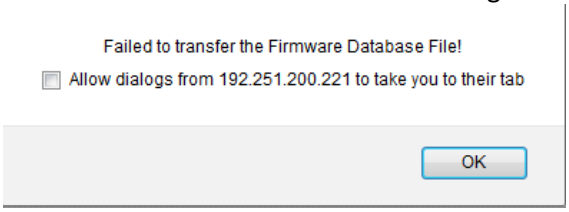
9. Check the **Software Revision** field to ensure that the valid revision level displays (e.g., 1.2.1 in the example below).



You may need to click the **Refresh** button at the bottom of the page to update the **Software Revision** field.

Message: IONMM result displays "*Error: TFTP transfer failed*"
TFTP server result displays "*Dropped because peer didn't respond*"
Meaning: You tried to upgrade with too large of a file. The ION106-x chassis limits the size of the db.zip file to 50 Mb for bulk upgrades. (ION 6 slots - CLI -Uploading bulk firmwares failed using db.zip.)
Recovery: Upgrade multiple devices in stages so that the size of the db.zip file is 50 Mb or less for bulk upgrades.

Message: *Failed to transfer the Firmware Database File!*
Meaning:
Recovery: 1. Check the checkbox to "Allow dialogs from 192.251.200.221 to take you to their tab".
2. Click the OK button to clear the message dialog. 3. Reduce the file size and re-try the operation.



Upgrading NIDs – Web Method

This procedure is used to upgrade one or more of the NIDs installed in the ION Chassis.

Note: Do not use this procedure for upgrading just the IONMM; instead use the procedure in the section "Upgrading the IONMM Firmware – Web Method" to upgrade just the IONMM firmware.

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

- Have the upgrade files resident in the default directory on the TFTP or SFTP server (normally *C:\TFTP-Root*).
- Create the firmware database index and archive files.
- Perform the 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. If using Windows 7, name the index file just "**db**".

To create the firmware database index and archive files.

1. Launch a plain text editor to create the index file.
2. Make an entry for each firmware file to be used for the upgrade in the following format:

   xx yy zz

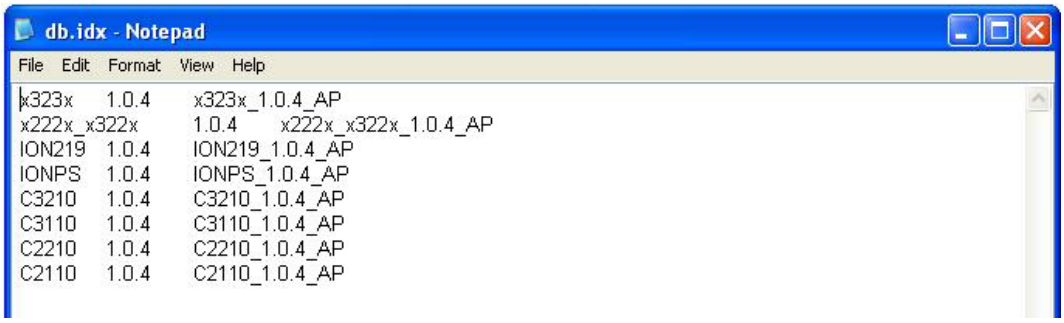
   where:

   xx = name of the module as shown in the Web interface (see the file example below)
   yy = revision level of the firmware upgrade file
   zz = name of the firmware upgrade file

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

db.idx File Example

The example below shows a ***db.idx*** file for an ION system with eight chassis-resident modules (x323x, x222x/x32xx, ION219, IONPS, C3210, C3110, C2210, and C2110). Note that more than one device can be updated by a db.idx file.



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 with a .idx extension, then save it as a text file and rename it (i.e., change *db.txt* to *db.idx*) in Windows Explorer.

4. Create a zip file that contains each of the upgrade files and the index file.

   For example, using the files listed in the example above, the **db.zip** file (or "**db**" file in Windows 7) would contain the following .bin files:

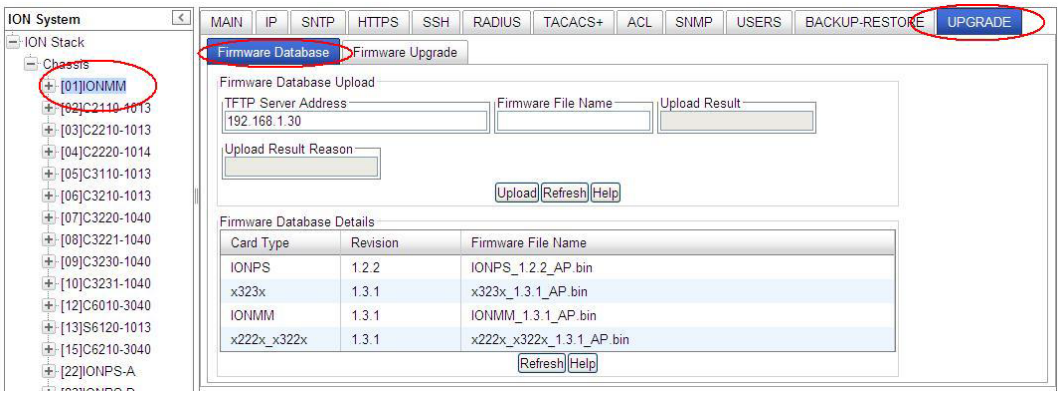
   - db.idx
   - x323x
   - x222x/x32xx
   - ION219
   - IONPS
   - C3210
   - C3110
   - C2210
   - C2110

5. Do the upgrade (see "Performing the Upgrade" section below).

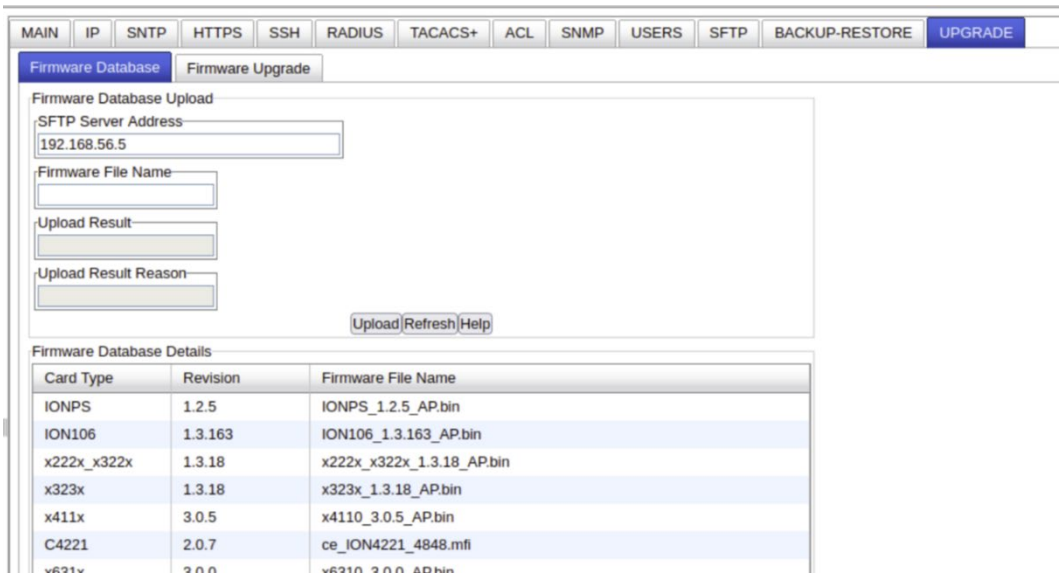
Performing the Upgrade

The upgrade consists of two parts: uploading the archive file to the IONMM and loading the upgrade file into the appropriate modules. The following describes the procedure for upgrading ION family modules' firmware from the IONMM.

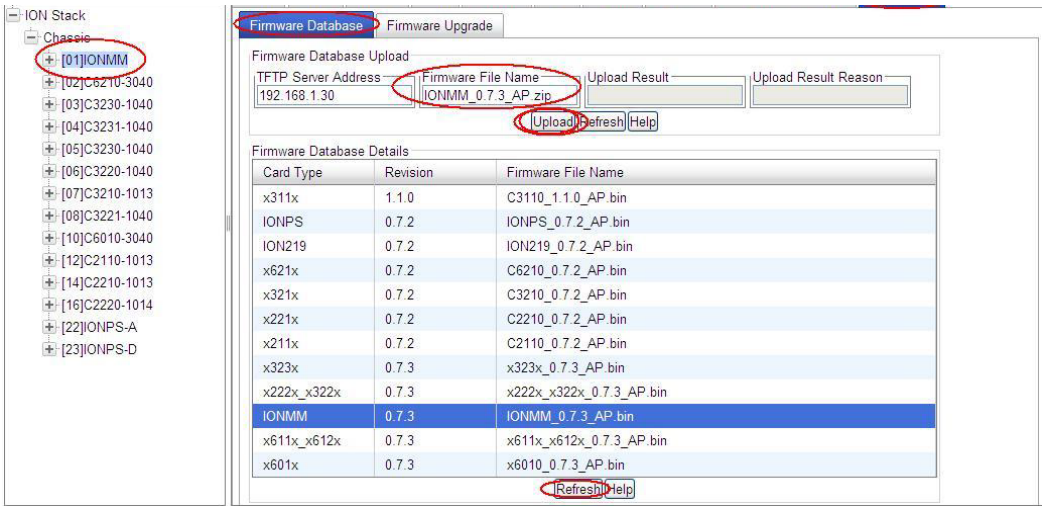
1. Access the IONMM through the Web interface (see "Starting the Web Interface").
2. Select the **UPGRADE** tab. The **Firmware Database** sub-tab displays.



If SFTP is enabled, the Upgrade page displays the SFTP Server Address.



3. In the **TFTP Server Address** field, enter the IP address of the TFTP server where the upgrade file is located.
4. In the **Firmware File Name** field, enter the name of the archive file you created (max. 32 characters).



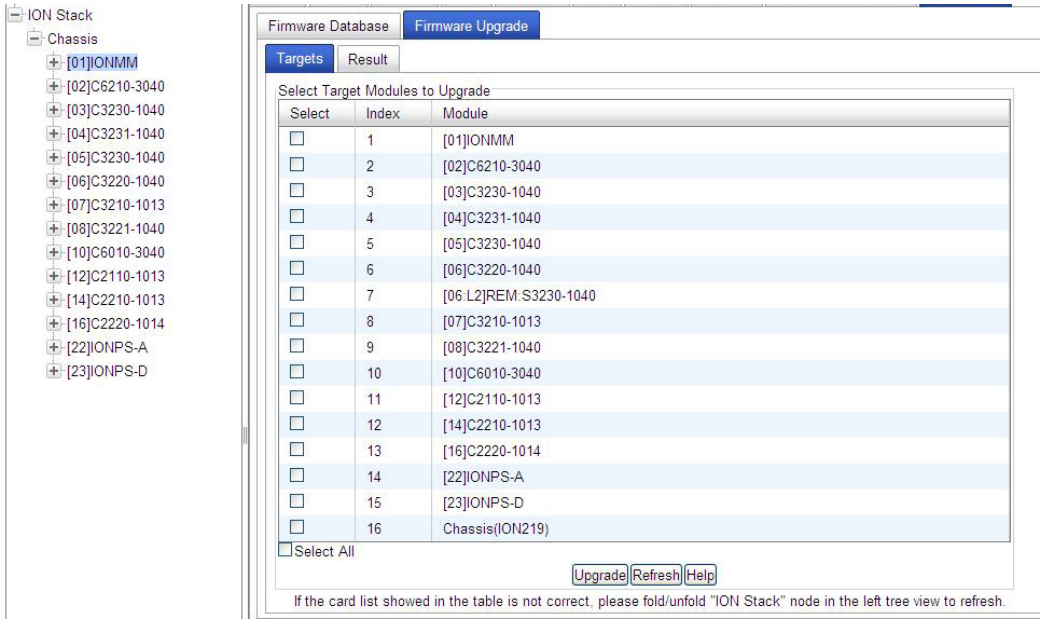
5. Click the **Upload** button.

   The archive file is uploaded from the TFTP or SFTP 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 load. The message "*Success*" displays in the **Upload Result** field, and the modules listed in the *db.idx* file are listed in the **Firmware Database Details** section.

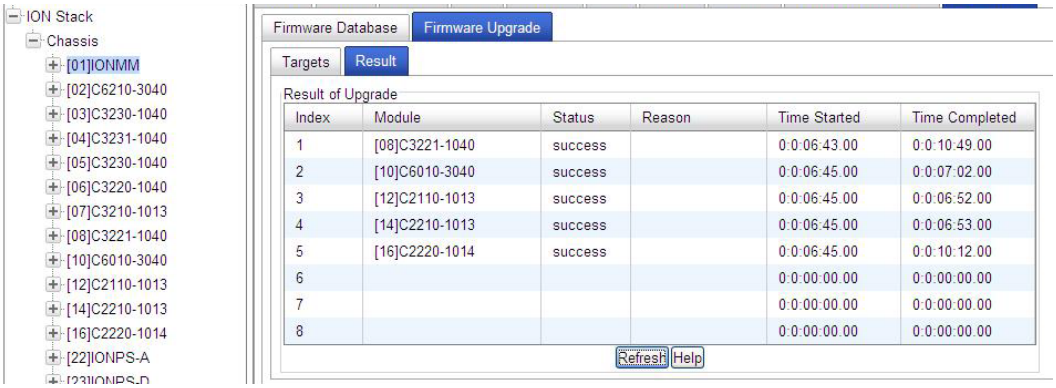
   If the upgrade fails, the **Upload Result Reason** box displays a failure code. See "Section 5 – Troubleshooting" for error messages and recovery procedures.

7. Select the **Firmware Upgrade** sub-tab.



8. In the **Select** column, check the checkbox of each module to be upgraded (up to 8 modules can be upgraded at a time).

9. Click the **Upgrade** button. A confirmation window displays: "*Upgrade following modules: xxxx, xxxx, xxxx-xxxx, are you sure to proceed?*".
10. At the confirmation window, click **OK**.
11. To monitor the progress, select the **Result** sub-tab and click **Refresh**.



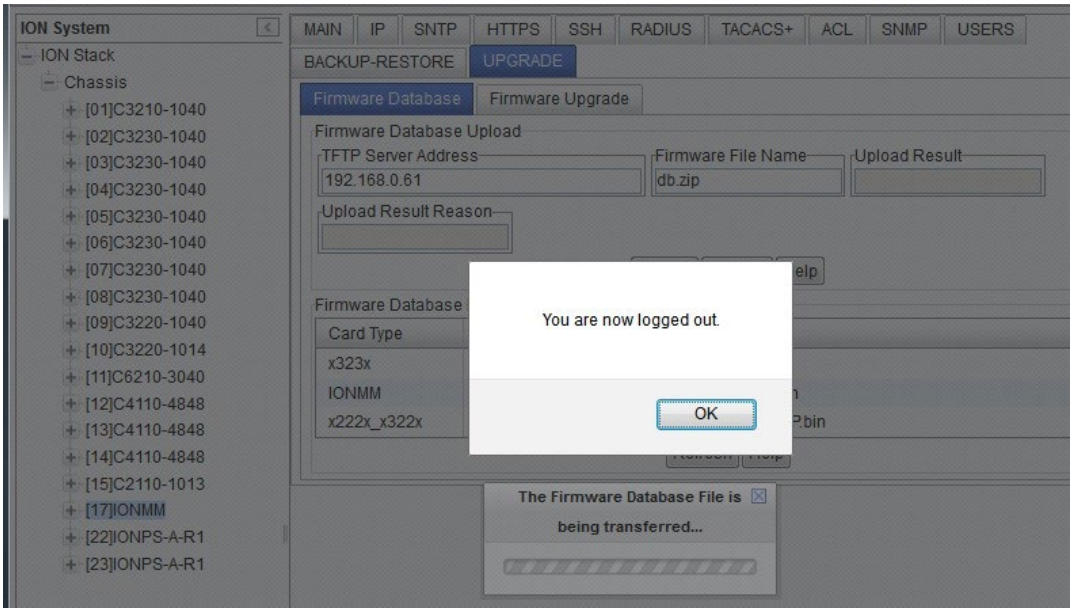
Note: the upgrade will take five or more minutes to complete. The exact amount of time for the upgrade depends on the number and types of modules being upgraded.

After the upgrade has completed, "*success*" displays in the **Status** column of the **Result** tab. Check the **MAIN** tab for each module to ensure that the correct revision level displays in the **Software Revision** field.

For information on the status of important ION system files resulting from this operation, see "Appendix C: ION System File Content and Location".

Messages

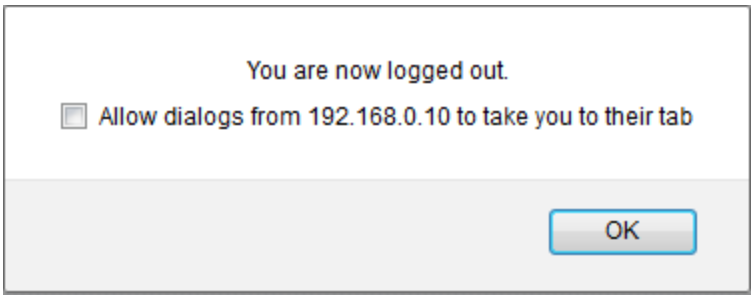
Message: *The firmware Database File is being transferred*... followed by *You are now logged out* displays during a firmware upgrade; or the file transfer completes but the files are not added.



Meaning: An Inactivity Timer was added at IONMM FW v 1._._. If the timeout occurs during a TFTP transfer when loading firmware, the transfer completes but the files are not added to the firmware database.

Recovery:

1. Click the **OK** button to clear the message.
2. Log back in to the ION System.
3. Retry the operation, but before the 15 minute timeout period elapses, wiggle the mouse or press any key to reset the timer.
4. Try zipping up the firmware files. A .Zip file with IONMM, x322x, and x323x firmware creates a file of 38.7M, which takes ~14 minutes to load on a Windows 7 PC. That takes just under 15 minutes, so you won't get logged out. The transfer completes and the files are added. If you add the S3240 (11.6M) making the zip file 49.9M, the session times out. The transfer completes but the files are not added.



Management of Other Modules

The IONMM allows management of slide-in cards (SICs) installed in the ION Chassis through either the CLI or the Web interfaces on the IONMM. The CLI can be accessed through either the USB or Telnet facilities. Communications between the IONMM and the SICs is through the ION Chassis backplane.

Managing Using the 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:

`Agent III C1|S1|L1D>` (or just `C1|S1|L1D>`)

This prompt indicates that any subsequent commands entered are for the module located in chassis 1/slot1. 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 allows you to 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.

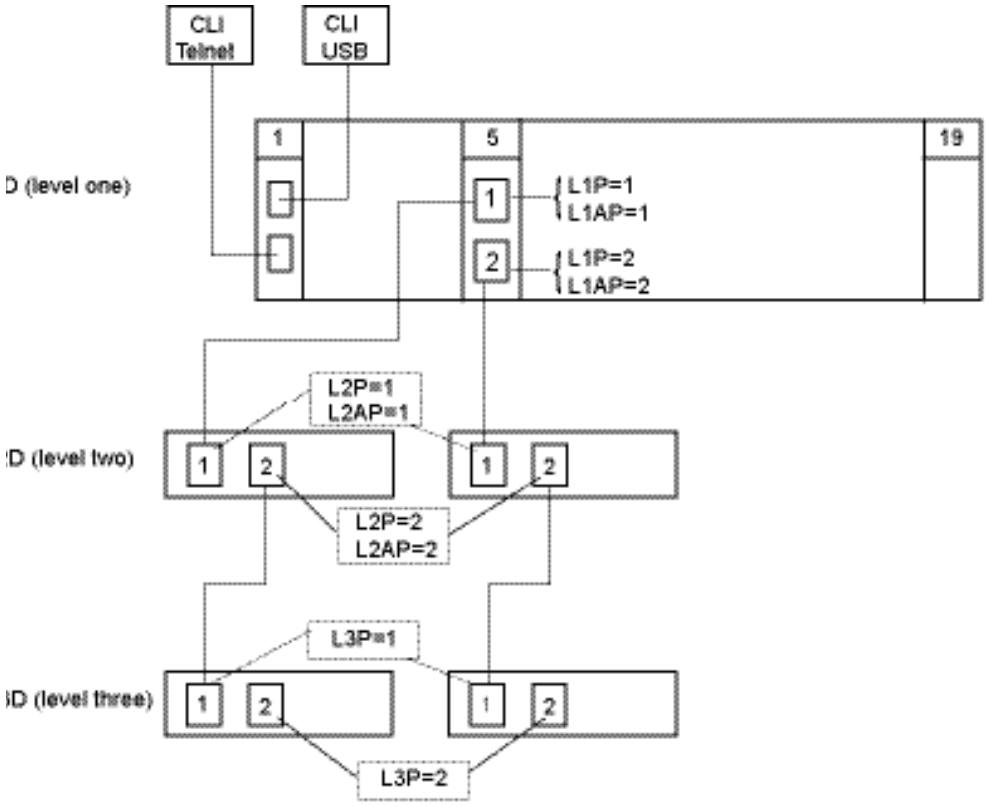


Figure 8: CLI Location Hierarchy

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

- L1D, or level one device, refers to cards (IONMM and other SICs) that are installed in the chassis.

- L2D, or level two device, refers to a device that is directly connected to a port in a card 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 two device.

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

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

Physically these are the same port. That is, L1P1 and L1AP1 are both port one on a level one device. However, it is how they are used that determines their syntax. For example, L1P1 indicates that the port is used to connect to a service device that is not managed by the IONMM. L1AP1 indicates that the port is used to connect to a level 2 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 8: CLI Location Hierarchy, 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 8: CLI Location Hierarchy, 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>
```

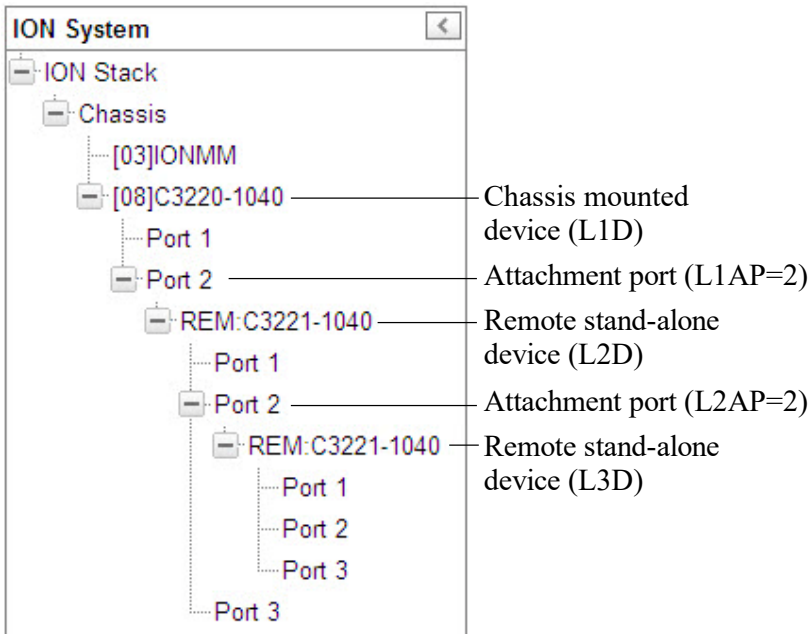
Any CLI command appropriate for the device can now be entered.

The following procedure is for using CLI commands to manage other SICs.

1. Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").
2. Use the **go** command to change the operational location to the device/port to be managed.
3. Configure the SIC using the appropriate commands. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
4. To return the location to the IONMM, type **home** then press **Enter**.

Managing via the Web Interface

1. Access the IONMM through the Web interface (see "Starting the Web Interface").

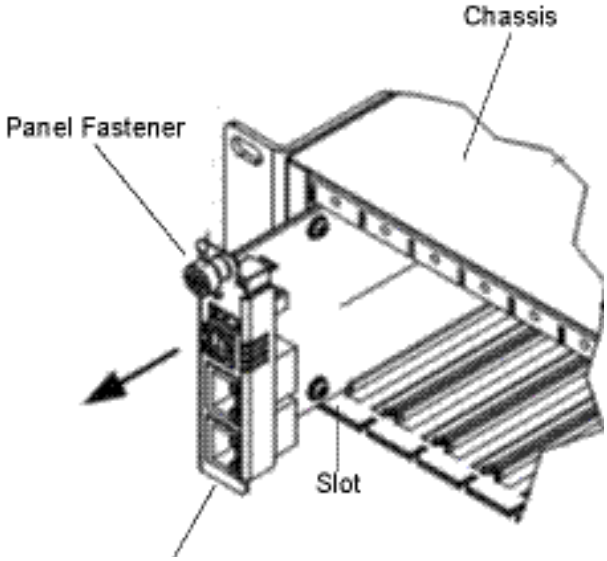


2. Click on the slide-in card / port to be managed.
3. The operations that can be performed depend on the slide-in card type. Refer to the specific product document for more information. See the "Related Documents" section.

Replacing the IONMM

The IONMM is a “hot swappable” device (it can be removed and installed while the chassis is powered on). Use this procedure to replace the IONMM.

1. Backup the configuration (see Backing Up the Configuration).
2. Disconnect any cables attached to the Management Module.



3. Loosen the IONMM panel fastener by turning it counterclockwise.
4. Pull the existing IONMM from the Chassis.
5. Carefully slide the new IONMM fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the IONMM to the chassis.
7. Connect the network and/or USB cables to the IONMM.
8. Load the configuration into the new IONMM (see “ the Configuration”).

5. Troubleshooting

General

This section provides basic and specific problem determination processes, and a description of problem conditions that may occur or messages that may be displayed. This section also documents ION system tests and describes where and how to get technical support.

IMPORTANT

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

Basic ION System Troubleshooting

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

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

- ION Chassis
- ION NIDs (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web Interface or ION command line interface - CLI).
- ION power supply
- ION Options (IONADP, ION LG Kit, SFPs, etc.)
- Data cables, electrical cables, and electrical outlets
- Third party network equipment (circuit protection equipment, battery backup, 3rd party client or server software – RADIUS or TFTP, etc.)

When troubleshooting an ION system / network problem on site:

1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the simpler problem causes and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the NIDs are seated properly, view the CLI **show** command output, check the Syslog file, verify IP addresses and Gateway IP address, check Windows Event Viewer, ping the interface, run the various SOAM tests if functional, etc.).
6. Write down your initial 2-3 guesses as to the cause of the problem.
7. Verify that the Lantronix product supports the function you are attempting to perform.

8. Use the Web interface or command line interface (CLI) to obtain all possible operating status information (log files, test results, **show** command outputs, counters, etc.)
9. Use the ION system manual procedure to retry the failed function or operation.
10. For the failed function or operation, verify that you entered valid parameters using the cursor over help (COH) and/or the ION system manual.
11. Based on the symptoms recorded, work back through each step in the process or operation to recall a point at which the problem occurred, and examine for a possible failure point and fixe for each.
12. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
13. Isolate 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, document the full sequence several times 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.

Review the "Recording Model Information and System Information" section before calling Technical 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
- SNMP Messages
- Syslog Messages and Sys.log Output
- Windows Event Viewer Messages
- The Config Error Log (config.err) File
- Webpage 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.
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 the related document).
5. Verify that the ION system devices have the latest firmware versions (see "Upgrade the Firmware").
6. Download the latest firmware version and upgrade as necessary.
7. Check if other network devices are working properly.

Power (PWR) LED off (not lit):

1. Check for a loose power cord.
2. Remove the card from the chassis and re-insert it. Replace if failed.
3. Check for a power supply failure. Replace power supply if failed.
4. Make sure all circuit protection and connection equipment and devices are working.
5. Verify that the ION system power supply is within operating range (see the related document).

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 card from the chassis and re-insert it.
5. Verify that the ION system devices have the latest firmware versions (see "Upgrade the Firmware").
6. Download the latest firmware version and upgrade as necessary.

DUP (Duplex) LED lit:

1. Remove the suspect card from the chassis and re-insert it.
2. Make sure the USB cable is properly connected.
3. Check for an IONMM configuration problem (see "Section 3: Configuration").
4. Make sure all circuit protection and connection equipment and devices are working.
5. Verify that the ION system power supply is within operating range (see the related document).
6. Reset the ION system (see "Reset to Factory Defaults").

TX or RX LED off (not flashing):

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

Troubleshooting Auto-negotiation Mismatches

The IEEE 802.3ab Auto-negotiation protocol manages the switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, causing a mismatch and reducing performance. A mismatch can occur when:

1. A manually set speed or duplex parameter is different than the manually set speed or duplex parameter on the connected port.
2. A port is set to auto-negotiate, and the connected port is set to full duplex with no AutoNegotiation.

To maximize performance and ensure a link, follow one of these two guidelines when changing the settings for duplex and speed:

1. Set both ports to auto-negotiate both speed and duplex, or
2. Manually set the speed and duplex parameters for the ports on both ends of the connection.

IPv6 Troubleshooting

Start by using these third party resources when performing general IPv6 problem solving:

- The standard Windows 7 command-line tools with full IPv6 functionality (Ping, Ipconfig, Pathping, Tracert, Netstat, and Route all support IPv6).
- The IPv6-specific tools in the Netsh command.

Address Resolution in Windows 7

In unicast global IPv6 (equal to IPv4 Public) addresses, the 64-bit host portion of the address is derived from the MAC address of the network adapter. The Neighbor Discovery (ND) protocol resolves IPv6 addresses to MAC addresses. The resolution of host names to IPv6 addresses is done by DNS except for link-local (equivalent to IPv4 APIPA) addresses, which resolve automatically. DNS handles records for IPv6 host names like IPv4 and uses pointer (PTR) records to perform reverse lookups. Where DNS is not implemented (e.g., peer-to-peer environments) the Peer Name Resolution Protocol (PNRP) provides dynamic name registration and name resolution.

Verify IPv6 Configuration in Windows 7

The main tool is Ipconfig. The command **ipconfig /all** displays both IPv4 and IPv6 configuration. To display the configuration of only the IPv6 interfaces use netsh. The **netsh interface ipv6 show address**s command displays each interface IPv6 address including the interface ID after the % character (the configuration can be accessed via the GUI).

Verify IPv6 Connectivity

Try to **ping** the local address. Note that if pinging link-local addresses from one host to another, you must include the destination adapter interface ID (e.g., ping fe80::38e7:3df1:f5ff:fdf0%13). When pinging site-local (equal to IPv4 Private) addresses you can add the interface ID to ensure that the address is configured on the desired interface. You must add an 'allow' rule for ICMPv6 traffic to pass through each computer's firewall.

Command examples - third party CLI commands for IPv6:

```
ipconfig /all
netsh interface ipv6 show address
ping fe80::38e7:3df1:f5ff:fdf0%13)
netsh interface ipv6 delete neighbors
netsh interface ipv6 show neighbors
netsh interface ipv6 delete destinationcache
netsh interface ipv6 show destinationcache
netsh interface ipv6 show route
route print
tracert -d <destination IPv6 address>
pathping -d <destination IPv6 address>
```

Additional Information

IPv6 Forum at http://www.ipv6forum.com/

ARIN (American Registry for Internet Numbers) at https://www.arin.net/knowledge/ipv6_info_center.html or ARIN wiki at http://www.getipv6.info/index.php/Main_Page

Cisco: http://www.ciscopress.com/articles/article.asp?p=777892&seqNum=7

Troubleshooting IPv6 on Windows 7: http://itexpertvoice.com/home/troubleshooting-ipv6-on-windows-7-and-why-its-worth-the-bother/

Troubleshooting IPv6 on Windows Servers (Microsoft TechNet): http://technet.microsoft.com/en-us/library/cc780623(WS.10).aspx

Test IPv6 Connectivity Using the ping6 Command (Windows XP)
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_pro_diag_ping6_conn.mspx?mfr=true

IPv6 Auto Config Troubleshooting

Determine whether your computer will require reconfiguration. For example, for Microsoft .NET Framework version 2.0 and later, IPv6 is enabled by default. For .NET Framework version 1.1 and earlier, IPv6 is disabled by default. For more information see the MSDN article at http://msdn.microsoft.com/en-us/library/8db2058t.aspx. Windows Server 2008 provides complete support for IPv6 and all of its features and does not need additional installation or configuration.
For Windows 7 see http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx.
For Windows XP see http://support.microsoft.com/kb/2478747.
For Windows Vista see http://ipv6.com/articles/general/IPv6-Microsoft-Vista.htm.
For Linux / BSD, see http://ipv6.com/articles/applications/Linux-and-BSD.htm or http://tldp.org/HOWTO/html_single/Linux+IPv6-HOWTO/ or your distribution documentation and/or website.

Problem Conditions

Cannot access the IONMM via USB port

1. Check that the USB cable is connected to the IONMM and to the PC/workstation.
2. Unplug and replug the USB cable at the IONMM USB-DEVICE port.
3. Check that the USB driver is installed on the PC/workstation. See "Installing the USB Driver".
4. Check that the terminal emulator software is configured properly for the USB port and launched. See "Configuring HyperTerm".
5. Make sure that serial access (console access) is enabled.
   a) Access the IONMM through the Web interface (see "Starting the Web Interface").
   b) Select the **MAIN** tab.
   c) Locate the **System Configuration** section.
   d) If **Enabled** is not showing in the **Console Access** field, select it and click **Save**.
6. Restart the local management station (PC).
7. Press the IONMM **RESET** button at the top of the IONMM card.
8. Power cycle the IONMM. Make sure the IONMM **PWR** LED is lit.
9. If the problem persists, contact Lantronix Technical Support.

Cannot access the IONMM via Telnet

1. Check whether SSH is enabled.
   a) Access the IONMM through either a USB connection (see "Starting a USB Session") or the Web interface (see "Starting the Web Interface").

   Note: if you are unable to access the IONMM through the Web interface, go to step 3.

   b) From the CLI, type: **show ssh config** and press **Enter**.
   c) From the Web interface, select the **SSH** tab and check the **SSH Server Status field**.
2. Is SSH enabled?

Yes	**No**
Access the IONMM using SSH security or disable SSH (see "Configuring SSH"). Is access restored? • Yes – end of procedure. • No – continue with step 3.	Continue with step 3.

3. Check whether Management VLAN is enabled.

   a) At the USB command prompt, type: **show mgmt vlan config**

   b) Press **Enter**.

4. Is Management VLAN enabled?

Yes	No
a) Make sure that the management station/PC is part of the same VLAN as the IONMM. b) Make sure that the correct port is being used on the IONMM. c) Is access restored? • Yes – end procedure. • No – continue with step 5.	Continue with step 5.

5. If the problem persists, contact Technical Support.

Cannot access the IONMM via the Web

1. Does the sign in screen appear?

Yes	No
Sign in using the default password; **private**. **Note:** the password is case sensitive.	Continue with step 2.

2. Verify that the default password has not been changed.
3. Check with your IT department that the network is up and running.
4. Check that the network cable is connected to the IONMM and the network port.
5. Check the IP addressing. At the command prompt, type **show ip-mgmt config** and press **Enter**. Verify the assigned IP address, Gateway IP address, and sub-net mask.
6. Check if HTTPS is enabled.

   a) Access the IONMM through either a USB connection (see "Starting a USB Session") or an SSH or Telnet session (see "Starting a Telnet Session").

   Note: if you are unable to access the IONMM through the Telnet interface, go to step 7.

b) At the command prompt, type: **show https config** and press **Enter**.

7. Is HTTPS enabled?

Yes	**No**
Access the IONMM through HTTPS or disable HTTPS (see "Configuring HTTPS"). Is access restored? • Yes – end procedure. • No – continue with step 8.	Continue with step 8.

8. Check if Management VLAN is enabled. At the USB command prompt, type **show mgmt vlan config** and press **Enter**.
9. Is Management VLAN enabled?

Yes	**No**
a) Make sure that the management station/PC is part of the same VLAN as the IONMM. b) Make sure that the correct port is being used on the IONMM. c) Is access restored? • Yes – end procedure. • No – continue with step 10.	Continue with step 10.

10. Disable the Management VLAN function. At the USB command prompt, type **set mgmt vlan state=disable** and press **Enter**.
11. If the problem persists, contact Technical Support.

Cannot activate IP-based management

1. Verify that the IP, gateway, and subnet mask are configured correctly.
2. With DHCP enabled, DHCP could have failed leaving the system with the old static IP configuration. Check the configuration via the USB port.
   a) Access the IONMM through a USB connection (see "Starting a USB Session").
   b) At the command prompt, type: **show ip–mgmt config**.
   c) Press **Enter**.
3. If the problem persists, contact Technical Support.

IONMM does not power on

1. Does the chassis have power?

Yes	**No**
Check that the IONMM is seated properly in the chassis.	a) Check that the power cord is plugged into the unit and the wall socket. b) Plug the IONMM into a different outlet.

2. If the problem persists, contact Technical Support.

Telnet connection is lost after a CLI command is executed

1. Can you connect to the IONMM through the Web interface?

Yes	**No**
Go to step 3.	Continue with step 2.

2. Check the following:
   - the IONMM is seated properly in the chassis
   - the IONMM is powered up
   - the network cable is seated
   - the network is operational
3. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
4. Cycle power for the module in question. **Note**: for slide-in cards, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. If the problem persists, contact Technical Support.

Trap Server does not record traps

1. Ensure the Trap Server application is running.
2. SNMP traps may be blocked by a router or firewall. Consult your Network administrator to determine if this is the case.
3. Check that the correct SNMP trap manager IP address has been defined for the module.
   - For Web Interface – go to the **SNMP Configuration** section on the **MAIN** tab.
   - For CLI – at the device level, type: **show snmp config** and press Enter.
4. If the problem persists, contact Technical Support.

Upgrade fails

Cannot upgrade modules

Cannot upload upgrade files

1. Make sure that:
   - The correct module(s) has been selected and is powered on.
   - The module selected is listed in the **Card Type** column on the **Firmware Database** sub-tab.
   - A hierarchy conflict does not exist (i.e., trying to upgrade a level 2 module and its level 1 module at the same time).
   - The NIDs are upgraded to the same version as the IONMM.
2. Wait two minutes, and then retry the operation. If the operation still fails, continue with step 3 below.
3. Reboot the IONMM and all modules in the upgrade stream.
4. Retry the operation. **Note:** you will have to do another upload of the upgrade files.
5. If the problem persists, contact Technical Support.

Upload fails

1. Check the following:
   - The IONMM is powered on.
   - The IP address of the TFTP server is correct.
   - The TFTP server is online and available.
   - The correct file name, **db.zip**, is specified (including the .zip extension) for Windows XP (do not include the extension in Windows 7).
   - The **db.zip** file (or **db** file) is in the default directory on the TFTP server.
   - The **db.zip** file (or **db** file) contains the db.idx file and the upgrade files.
   - The **db.idx** file (or **db** file) is formatted correctly ("Creating the Database Index and Archive Files").
2. Wait three minutes then retry the operation. If the operation still fails, continue with step 3.
3. Reboot the IONMM.
4. Retry the upload operation.
5. If the problem persists, contact Technical Support.

USB connection resets after a CLI command is executed

1. Can you connect to the IONMM through the Web interface?

Yes	No
Go to step 4 of "Telnet connection is lost after a CLI command is executed".	Continue with step 2.

2. Check the following:
   - the IONMM is seated properly in the chassis
   - the IONMM is powered up
   - the network cable is seated
   - the network is operational
3. For all modules (slide-in and remote) check the following:
   - the module is properly seated/connected
   - the module is powered up
4. Cycle power for the module in question.
5. If the problem persists, contact Technical Support.

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 has a Jumper that disables software management of the device. When Configuration Mode is **hardware**, the devices take some of the configurations from Jumper J9 on the PCB. In **software** mode, configuration is controlled by management.

1. See the IONMM or chassis card install Guide for Jumper setting information.
2. Contact Lantronix for more information. Contact Technical Support.

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 discovery to complete. Note that the ION system supports up to three levels of device discovery (two remote and one local).

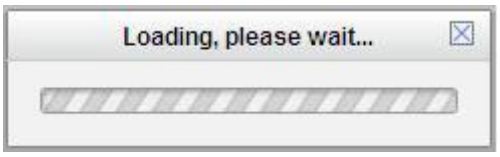
2. Click the ☒ icon to close the message.

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.

***loading, please wait ...* displays continuously and IE9 Freezes**



You clicked on the IONMM in the ION system Web interface, but the message displays. This occurs only with IE9 (Internet Explorer 9, which requires Windows 7 or Windows Vista).

1. Wait several moments for the message to clear.
2. Click the ☒ icon to close the message.
3. Use the IE9 **Compatibility View** button in the address bar to resolve this issue (see Note 1 below). See the Microsoft IE9 release notes at http://msdn.microsoft.com/en-us/ie/ff959805 for known IE9 issues.
4. Try going back to IE8, as this function works with IE8.
5. Try another web browser (Firefox, Chrome, etc.).
6. If the problem persists, contact Technical Support.

Note 1: See the IE9 Compatibility View (http://support.microsoft.com/kb/956197) for three methods.

Method 1: Enable Compatibility View for your whole website or for specific website directories.

Method 2: Enable Compatibility View for specific web pages.

Method 3: Enable Compatibility View for multiple computers by using Group Policy settings.

Windows 7 editions: Home Premium, Windows 7 Professional, and Windows 7 Ultimate.

No ACL condition now!

1. You entered the command **show acl condition**, but you have not yet defined any ACL conditions.
2. Use the **set acl condition command** to define a related ACL condition. (Use the **IONMM** > **ACL** tab via the Web interface.)
3. If the problem persists, contact Technical Support.

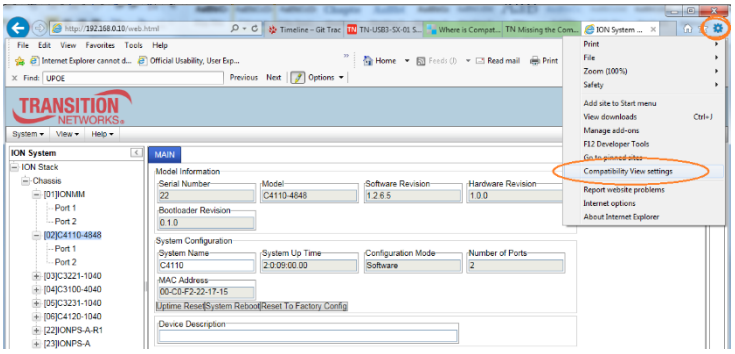
Problem/Message:

Internet Explorer 11 message indicates "*This page can't be displayed.*"
"*Invalid username or password* message displays at the ION System Login page in IE 11.
ION System web pages do not display or display incorrectly in Internet Explorer 11.
The ION System message "loading, please wait ..." displays continuously and IE11 freezes

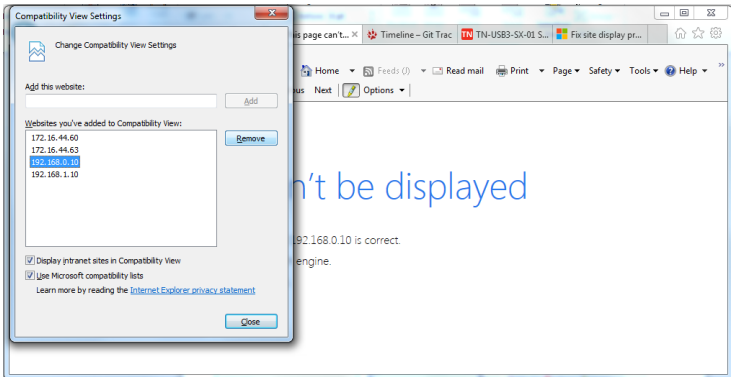
Cause: In earlier IE versions, the Compatibility View button would try to fix a broken standards-based website by getting the page to display like it did in Internet Explorer 7. Compatibility issues were largely resolved since IE 7, to the point where the Compatibility View button was removed for IE11.

Recovery: Remove the ION URL from Compatibility View:

1. With ION up, click on the Gear icon at the top right corner of your IE window and choose Compatibility View settings.



2. Select the ION URL in "Websites you've added to Compatibility View:" and click the Remove button.



3. You also have the option to uncheck (disable) two other features:
   - □ Display intranet sites in Compatibility View
   - □ Use Microsoft compatibility lists
4. Click the Close button when done and log back in to the ION System.

No ACL rule now!

When doing a backup of the IONMM and several other modules, an error was detected when the IONMM was initially backed up (*AGENT PM ERROR: CLI command show acl rule failed*).

1. Execute a System reboot on the IONMM.
2. Execute a backup on the IONMM alone.
3. 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 NID 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. Reboot the device by clicking the **Reboot** key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
6. Upgrade the device(s) to the latest software version.
7. Reboot the ION System using the **Reboot System** button.
8. If the problem persists, contact Technical Support.

Red box Condition after Reboot

When the reboot is finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The ‘red box’ condition occurs while the devices are resetting; this condition can continue several minutes after the reboot. Until the system is ready to be fully managed, certain fields may display within "red boxes". The "red boxes" will disappear when the system is ready to be fully managed.

1. Wait a couple of minutes for the current operation to complete, and then continue operation.
2. Check the devices’ firmware versions. For example, a C2220 has only certain items ‘red boxed’. The IONMM in this case is at latest version and shows certain new functions on the GUI, while the C2220 is at an older version and shows the newer functions as ‘red boxed’. Since the older version of C2220 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.

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 Displays an Error and then Terminates Installation

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

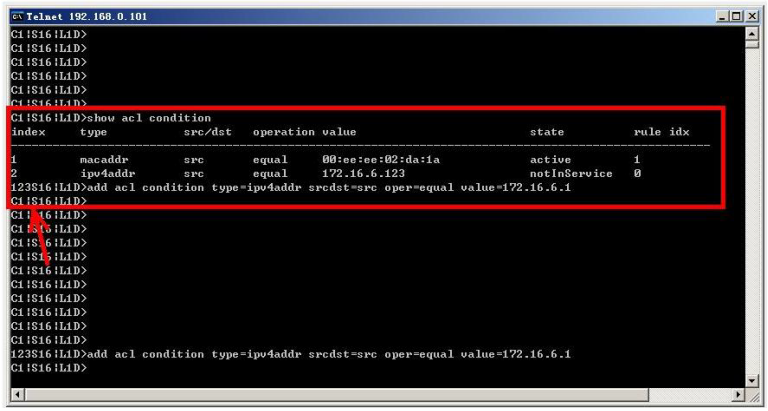
To successfully install the device, you must change the driver signing options to either warn or ignore to allow the installation to complete.

1. To change the current driver signing setting, in Windows XP, go to "Control Panel\System", click on the "Hardware" tab and then click "Driver Signing".
2. Select the desired signing option.

For other USB Driver / OS Messages (Win2K, Vista, Windows 7, Linux, Mac) refer to the separate document with Driver / OS install, uninstall and troubleshooting information.

Long Command Causes Cursor Wrap to Same Line

When the input command reached the input max length, the cursor did not return to the next line but went back to the begin of the same line covered the original data



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.

Cannot find new IP address

DHCP issued address is not being displayed
IP Address Wrong

If the DHCP client is enabled on the IONMM **Main** page, there is no easy way to determine the new IP address. If DHCP client status set to "enable", the value of "ip address" shows the last IP, not the current dynamic allocation IP.
When a **show ip-mgmt config** command is entered on the CLI, the previous "fixed" IP address is still returned.
If a Fully Qualified Domain Name is used on any of the IONMM pages to access other devices (TFTP, SNTP or Radius), or to ping another PC, they will fail because of an internal sync problem when getting the IP settings from the ION system when the DHCP client is enabled.

1. Disable the DHCP client and set the DNS server; the problem resolves. (If you enable the DHCP client and then set the DNS servers via the Web interface, this issue may occur due to the internal sync problem noted above).
2. Contact Lantronix for more information. Contact Technical Support.

L2CP: LLDP packets will not forward when the "LLDP protocol" set to "Pass"

All the LLDP packets received are forwarded internally, as the ION system uses it to do topology discovery. The ION system checks the LLDP packets to find out whether it is an ION system LLDP packet.

If it is a Lantronix LLDP packet (xxDP) the ION system handles it separately.
If it is not a Lantronix LLDP packet, it may be handled in one of two ways, based on the packet verification result: if it is a valid LLDP message, the ION system will forward it to the specific port based on the port's L2CP configuration; if the packet is invalid, it is immediately discarded.

The L2CP MIB definition for xxDP forwarding states that "LLDP protocol frames with a destination address of 01-80-C2-00-00-0E which are not TN discovery LLDP frames are either discarded or passed at this port".

Message: *Getting Records failed (snmp operation timeout)*
Getting records failed (http server error)
Meaning: The NID could not find the records associated with the operation attempted.
Recovery:

1.Verify the attempted operation was performed correctly (e.g., Policy/ Rule type drop down on the ACL page).

2. Retry the operation. See the applicable section ("Upgrade the Firmware" section, or "Backup and Restore Operations (Provisioning)".

3. Reboot the NID.

4. If the problem persists, contact Technical Support.

Problem: 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 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: ION upgrade unsuccessful.
Clicking on a chassis card causes "snmp time-out" error.
Communication with the IONMM locks up after IONMM upgrade.
Meaning: You upgraded the IONMM to ION Release 1.2.1 but did not upgrade any of the ION Chassis cards. The upgrade was unsuccessful since the chassis cards were not upgraded with the IONMM card upgrade. This is due to the MIB changes that were implemented after ION Rel. 1.1.0.
Recovery:

1. Perform a hard reset (IONMM card removal) to re-initialize the ION Chassis.
2. Log in to the IONMM again.
3. Upgrade the ION NID cards to match the IONMM upgrade version.

Problem: "*Unknown command.*" message displays when entering system name/contact/location.

Problem: The **System Name** cannot be restored when the system name contains special character "space" in the middle.

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

Recovery: From the Web interface, at the device's **MAIN** tab in the **System Configuration** section, re-enter the "**System Name**" or "**System Contact**" or "**System Location**", making sure there are no spaces between the text characters.

From the CLI, re-enter the "**set system name**" or "**set system contact**" or "**set system location**" CLI command, making sure there are no spaces between the text characters. For example:

```
C1|S1|L1D>set system ?
  contact
  location
  name
C1|S1|L1D>set system name=123abcABC ~!@#$%^&*()_+"
% Unknown command.
C1|S1|L1D>set system name=123abcABC ~!@#$%^&*(
% Unknown command.
C1|S1|L1D>set system name=123abcABC ~!@#$%
% Unknown command.
C1|S1|L1D>set system name=123abcABC
C1|S1|L1D>set system name=123abcABC
C1|S1|L1D>set system name=123abcABC!@#$%
C1|S1|L1D>set system name=aa bb
% Unknown command.
C1|S1|L1D>set system name=$%^^&*
C1|S1|L1D>set system contact=Rob Roy
% Unknown command.
C1|S1|L1D>set system contact=RobRoy
C1|S1|L1D>set system location=12345 West 6th
% Unknown command.
C1|S1|L1D>set system location=12345West6th
C1|S1|L1D>set system name=123abcABC
C1|S1|L1D>
```

CLI Messages

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

Add ACL rule failed.

This message indicates that the rule could not be added.

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

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

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

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See the *ION System CLI Reference Manual, 33461*.
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 *ION System CLI Reference Manual, 33461*.
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.

1. Use the **go** command to change from the IONMM to the specific slide-in module. The **go** command format is:

   ```
   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.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support.

Cannot get LOAM 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. Use the **go** command to change location of where the command operates. The **go** command format is:

   ```
   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.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
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=<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.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support.

Cannot clear loopback counters on this card!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set autocross on this card!
Cannot set auto negotiation state on this port!
Cannot set Ethernet port speed for this card!
Cannot set Ether port duplex mode on this card!
Cannot set far end fault on this card!
Cannot set filter unknown dest multicast frames on this port!
Cannot set filter unknown dest unicast frames on this port!
Cannot set pause on this port!
Cannot set source address lock action on this port!
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!

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.
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.
4. Use the **go** command to switch to a different card port supporting loopback.
2. Verify the command entry.

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.

Command incomplete

This message indicates that not all 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 *ION System CLI Reference Manual,* 33461.
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 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=<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.

2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
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=<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.

2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.

3. If the problem persists, contact Technical Support.

Fail to get MAC address!

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

1. Verify that the correct hierarchy has been specified in the command.
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds and 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 *ION System CLI Reference Manual*, 33461.
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 *ION System CLI Reference Manual*, 33461.
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 an IPv4 DHCP Address" section.
2. Retry the operation. See the related DHCP command in *the ION System CLI Reference Manual*, 33461.
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. Verify the operation in the applicable section of this manual.
2. Retry the operation. See the related command in *the ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support.

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 no 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 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, 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 ACL condition index!

This message indicates that you tried to associate an ACL condition with an ACL rule but the condition does not exist.

1. Check what conditions exist, type:

   show acl condition

2. Associate the correct condition with the correct rule or create the condition if it does not exist.
3. If the problem persists, contact Technical Support.

Invalid ACL rule index!
Error: The specified ACL rule index does not exist!

This message indicates that you tried to associate an ACL condition with an ACL rule that does not exist.

1. Check what rules exist, type:

   show acl rule

2. Associate the correct condition with the correct rule or create the rule if it does not exist.
3. If the problem persists, contact Technical Support.

Invalid condition value: xxxx

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

1. Verify the value being input; it must match with the value input for type=.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid location parameters, cannot find the physical entity!

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

1. Verify that the correct hierarchy has been specified in the command.
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 ACL condition now!

1. You entered the CLI command **show acl condition**, but no ACL conditions have yet been defined.
2. Use the **set acl condition** command to define a related ACL condition.
3. If the problem persists, contact Technical Support.

No DMI support on this port!

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

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

Now the value of table can only be "filter"!

You entered an unsupported ACL table or chain parameter value. For example:

```
C1|S7|L1D>set acl table {raw|nat|mangle}
C1|S7|L1D>set acl table raw chain {prerouting|input|forward|output|postrouting}
C1|S7|L1D>set acl table nat chain {prerouting|input|forward|output|postrouting}
C1|S7|L1D>set acl table mangle chain {prerouting|forward|output|postrouting}
```

1. Enter the parameters table=filter and chain=input. See “Configuring an ACL”.
2. Retry the operation. See the *ION System CLI Reference Manual*, *33461*.
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.
   - On the desktop, right-click on My Computer.
   - Select Manage.
   - Click Device Manager.
   - In the right panel, expand the list for COM & LPT.
3. Is the COM port in the list?

Yes	**No**
Continue with step 4.	Restart the management station.

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 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)
```

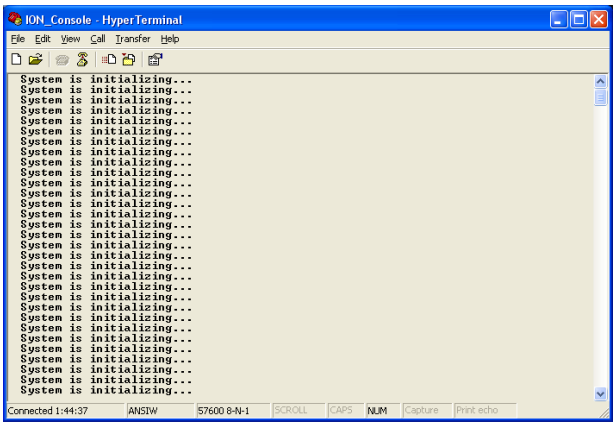
for a slide in card, or

```
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.

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.

Start HTTPS certificate failed.

1. Verify the HTTPS parameters (HTTPS is enabled, the certificate type is defined, certificate file defined, private key file defined, password defined).
2. Verify that the HTTPS server is operational.
3. Retry the operation (i.e., type **start https certificate** and press **Enter**).
4. If the problem persists, contact Technical Support.

This command is only available on <x323x> card!

1. Verify the command entered is the one you want.
2. Verify that the device for the command entered can support the function of the command (e.g., SOAM functions / commands are supported by NID models S323x / C323x NIDs).
3. Retry the operation (i.e., type **show soam port** and press **Enter**).
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 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 *ION System CLI Reference Manual*, *33461*.
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 *ION System CLI Reference Manual*, *33461*.
4. If the problem persists, contact Technical Support.

Error location parameter number!
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!

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=<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.

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 *ION System CLI Reference Manual*, *33461*.
6. If the problem persists, contact Technical Support.

Invalid erate!
Invalid irate!

You tried to set the Ingress or Egress rate to an unacceptable limit. For example, you typed:

```
C1|S3|L1D> C1|S7|L1D>set irate=100m erate=100m
```

and then pressed **Enter**.

1. Verify the CLI command syntax.
2. Retry the operation. See the **Set Bandwidth Rate Limit** command in the *ION System CLI Reference Manual*, *33461*.
3. If the problem persists, contact Technical Support.

TFTP transfer failed!

The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.

1. Verify the CLI command syntax.
2. Verify the firmware version.
3. Be sure the TFTP server is configured and running.
4. Check that the remotefile is in the proper location (e.g., the file *x323x.bin.1.0.5* is at *C:\TFTP-Root*).
5. Retry the operation. See the **tftp upgrade** command in the *ION System CLI Reference Manual, 33461*.
6. If the problem persists, contact Technical Support.

Error: Fail to transfer the file!
tftp get: set address type failed.
tftp put failed.

Performing a backup configuring all modules as a range does not backup correctly. 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.
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 all modules are entered for backup as a range (e.g., 1-10), enter as a series (e.g., 1,2,3,4,5,6,7,8,9,10) and all the modules will be backed up correctly.
5. 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.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
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.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
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.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
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 *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support.

Cannot get port VLAN configuration on this card!

Cannot get VLAN tag management configuration on this port!

You tried to enter a **show port vlan confi**g command on a device that does not support or is not configured for VLAN. For example:

```
C1|S7|L1P2>show port vlan config
Cannot get port VLAN configuration on this card!
```

1. Verify the CLI command is the one you want.
2. Use the **go** command to switch to a device/port that supports VLAN.

3. Try entering the command again.
4. If the problem persists, contact Technical Support.

Cannot show bandwidth allocation configuration on this card!

You tried to enter the **show bandwidth allocation** command on a device that does not support or is not configured for BW allocation. For example:

```
C1|S7|L1P2>show bandwidth allocation
Cannot show bandwidth allocation configuration on this card!
```

1. Verify the CLI command is the one you want.
2. Use the **go** command to switch to a device/port that supports BW allocation.
3. Try entering the command again.
4. If the problem persists, contact Technical Support.

DMI is only supported on FIBER port!

You tried to enter the **show dmi info** command on a port that does not support or is not configured for DMI. For example:

```
C1|S7|L1P2>show dmi info
DMI is only supported on FIBER port!
```

1. Verify the CLI command is the one you want.
2. Verify that the port supports DMI. For Lantronix NIDs and SFPs, the model number will have a “D” at the end.
3. Use the **go** command to switch to a fiber port that supports DMI.
4. Try entering the command again.
5. If the problem persists, contact Technical Support.

Link OAM is not supported on this card!

You tried to enter a **show oam** command on a device that does not support or is not configured for Link OAM. For example:

```
C1|S7|L1P2>show oam rx loopback control
Link OAM is not supported on this card!
```

1. Verify the CLI command is the one you want.
2. Use the **go** command to switch to a device/port that supports VLAN.
3. Try entering the command again.
4. If the problem persists, contact Technical Support.

Cannot get link pass through information on this card!

You tried to enter a **show lpt config** command on a device that does not support or is not configured for Link Pass Through. For example:

```
C1|S7|L1P2>show lpt config
Cannot get link pass through information on this card!
```

1. Verify the CLI command is the one you want.
2. Use the **go** command to switch to a device/port that supports VLAN.
3. Try entering the command again.
4. If the problem persists, contact Technical Support.

Cannot get forward database configuration on this card

You tried to enter a **show fwddb** command on a device that does not support or is not configured for forward database (e.g., from the IONMM). For example:

```
C1|S7|L1D>show fwddb config fdbid 0
Cannot get forward database configuration on this card
```

1. Verify the CLI command is the one you want.
2. Use the **go** command to switch to a device/ that supports the Forwarding Database function.
3. Try entering the s**how fwddb config fdbid=** command.
4. If the problem persists, contact Technical Support.

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

You entered a **show power config** command from a device other than a power supply. For example, you entered the following command from the IONMM:

```
C1|S7|L1D>show power config
Please change to power supply slot first before showing its configure!
```

1. Verify the CLI command is the one you want.
2. Use the **go** command to switch to a power supply.
3. Try entering the command again.
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 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.

Cannot show circuit-ID on this card!

You tried to display the Circuit ID information, but the function is not supported.

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports Circuit ID display.
3. Try entering the command again. See "Circuit ID" in the applicable NID User Guide manual.
4. If the problem persists, contact Technical Support.

Cannot set circuit-ID on this card!

You tried to display the Circuit ID information, but the function is not supported.

1. Verify the Circuit ID parameters. See "Circuit ID" in the applicable NID User Guide manual.
2. Try entering the command again.

If the problem persists, contact Technical Support.

Cannot get port VLAN configuration on this card!

You tried to display the VLAN configuration settings, but the function is not supported. For example:

```
C1|S1|L1P1>show port vlan config
Cannot get port VLAN configuration on this card!
C1|S1|L1P1>
```

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports VLAN configuration.
3. Try entering the command again. See "Circuit ID" in the applicable NID User Guide manual.
4. If the problem persists, contact Technical Support.

Cannot get VLAN tag management configuration on this port!

You tried to display the VLAN configuration settings, but the function is not supported. For example:

```
C1|S1|L1P1>show port vlan tag config
Cannot get VLAN tag management configuration on this port!
C1|S1|L1P1>
```

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports VLAN configuration.
3. Try entering the command again. See “Circuit ID” in the applicable NID User Guide manual.
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 IONMM. 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 this device.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support.

set sntp timezone=<1-63>
Set operation\n"
Simple Network Time Protocol\n"
Coordinated Universal Time timezone\n"
please use \"show timezone\" to see detailed value of each timezone\n"

You made an error entering the set / show SNTP timezone command.

1. Verify the command syntax. See the related section of this manual.
2. Retry the command entry.
3. If the problem persists, contact Technical Support.

The value of current time should time should follow this format, \"YYYY MMDD HH:MM:SS\", such as \"1999 1211 13:22:34

There was an error entering the SNTP timezone command to set / show the current local time of a device.

1. Verify the command syntax. See the related section of this manual.
2. Retry the command entry.
3. If the problem persists, contact Technical Support.

Fail to get port redundancy state!

Redundancy is enabled, so cannot set the administration state of fiber ports!

There was an error entering the **set** / **show redundancy** commands.

1. Verify the command syntax. See the related section of this manual.
2. Retry the command entry.
3. If the problem persists, contact Technical Support.

Pause capability advertised by local auto-negotiation entity

If no pause capability, setting nopause; otherwise, for copper port , use a combination of pause and apause, like pause+apause or pause or apause; for fiber port, use a combination of apause and spause, like apause+spause or spause or apause

There was an error entering the set ether pause command.

1. Verify the command syntax. See the related section of this manual.
2. Retry the command entry.
3. If the problem persists, contact Technical Support.

Speed and duplex capability advertised by local auto-negotiation entity

There was an error entering the set ether adv cap command.

1. Verify the command syntax. See the related section of this manual.
2. Retry the command entry.
3. If the problem persists, contact Technical Support.

A combination of 10THD,10TFD,100TFD, 100THD,1000THD and 1000TFD for copper port, like 10TFD+100TFD+100THD+1000TFD; and N/A for none capability; Cannot set this attribute for fiber port
There was an error entering the **set ether adv cap** command.

There was an error entering the **set ether adv cap** command.

1. Verify the command syntax. See the related section of this manual.
2. Retry the command entry.
3. If the problem persists, contact Technical Support.

Fail to get auto-negotiation state!
Fail to set dot3 pause
Cannot remove VLAN from the database!

There was an error entering the related command.

1. Try another command on this device.
2. Try this command on another card that supports the attempted function.
3. 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 Hilgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a text entry. Overtyping an entry should automatically replace the previous characters. This is a HyperTerminal problem that the ION CLI stack cannot resolve.

Response:

1. Upgrade to the latest version (a free download from www.hilgreave.com). The more current product seems to run more smoothly and has text editing features not found in earlier versions.
2. In HT, turn off local echo - refer to the HT helps and documentation for the command to use.
3. Make sure the keyboard Insert mode is turned off.
4. Download and use PuTTY or Tera Term to use as a replacement for HT.
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 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.

The two passwords do not match!

You tried to generate a private key, but the operation failed. For example:

```
C1|S3|L1D>set https private-key password
Please input password:
xxxxxx
Please input password again:
yyyyyyy
The two passwords do not match!
C1|S3|L1D>
```

1. Verify that this is the operation you want.
2. Retry the operation; be sure to type the password the same both times.
3. If the problem persists, contact Technical Support.

VID already exist!

You tried to add a VLAN-DB, but the operation failed. For example:

```
C1|S3|L1D>add vlan-db vid=20 priority=3 pri-override=enable
VID already exist!
C1|S3|L1D>
```

1. Verify that this is the operation you want.
2. Retry the operation; be sure to type a unique VLAN-DB VID.
3. If the problem persists, contact Technical Support.

Sys.log file lost on reboot

The device will dump all syslog files from RAM to flash on re-boot or if a system crash occurs.
The last (most recent) syslog is stored as last_sys.log which can be retrieved using the tftp command.
The filename sys.log is the current syslog file. The filename last_sys.log is the old syslog file.

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!
Invalid backup module-list, please give the parameter like module-list=1,4,13
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.

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.

Adding Local User failed
Cannot add an system user on this card!
Default ION user is forbidden to be deleted!
Deleting Local User failed
ERROR: Can not delete current logined user!
ERROR: Current user is not authorized to do this operation!
ERROR: The two passwords are not the same, please check!
Error: this command should be executed on IONMM or a standalone SIC!
ERROR: This user could not be deleted!
Fail to activate the user!
Fail to create a system user!
Fail to create user!
Fail to get system user level!
Fail to get system user name!
Fail to get system user password!
Fail to remove the system user!
Fail to set system user level!
Fail to set system user name!
Fail to set system user password!
Modifying Local User failed
Password is too long!
The confirm password is not identical with the password!
There is no such user!
The user name must begin with an alphanumeric char!
The user password must begin with an alphanumeric char!
This user already exists!
To modify default ION user's level is not allowed!
User name is too long!

You tried to add (create), modify, or delete an ION user, 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 "Configuring System / Login Users" section.

3. 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!

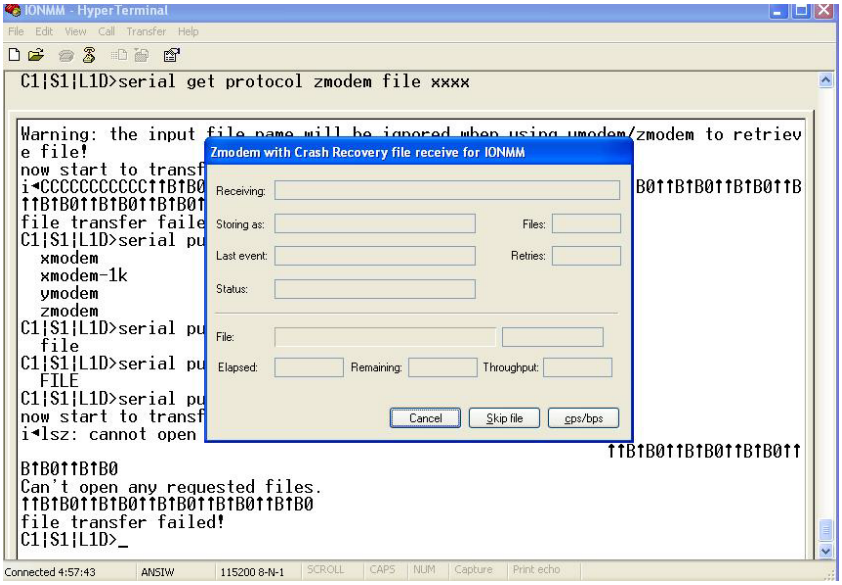
You entered a Serial File Transfer command, but the operation failed.

1. Verify that this is the operation you want (e.g., serial get/put/upgrade command).

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.

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 Microsoft or Hilgraeve Technical Support:

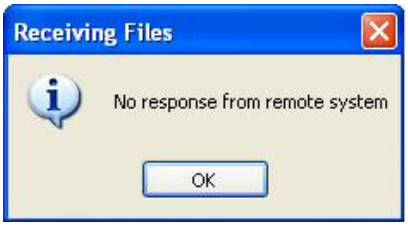
HyperTerminal Support

HyperTerminal is part of certain Microsoft Windows versions and is supported by Microsoft with 24-hour worldwide responsibility for Windows communications components. Contact Microsoft Windows Support at (425) 635-7000, or contact your computer manufacturer. See the Microsoft Support knowledge base for articles regarding your topic: http://support.microsoft.com/directory/ and do a key word search using your issue keywords.

HyperACCESS Support

Certain other Microsoft Windows versions do not include HyperTerminal support. HyperACCESS is the official, full powered Hilgraeve version of HyperTerminal Private Edition. If you need a more powerful HyperTerminal alternative, HyperACCESS is available. For questions call (734)-243-0576 ext. 1# or see http://www.hilgraeve.com/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.

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.

The specified module does not exist!

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

1. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section.

2. 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.

3. 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 cannot be run on this card at this firmware version.

1. Check the card's current firmware version using the "**show card info**" command.
2. Upgrade the card firmware. See "Upgrade the 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 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.

The confirm password is not identical with the password!
The user name length must be in range [1..64]!
The user name must begin with an alphanumeric char!
You can only change your own password, not others!

You entered a command to create a new system user, but the command failed.

1. Verify the command syntax ("add sysuser name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR").
2. Retry the operation, making sure the "pass" and "confirmpass" entries match.
3. If the problem persists, contact Technical Support.

ERROR: There is already a same named user!
ERRPR: User name cannot be modified!

You tried to add or change a user's User Name via the Web or the CLI, but the action was rejected.

1. Verify the command syntax (e.g., "**add sysuser name**=NAMESTR).
2. Retry the operation, making sure the user name entry is unique.
3. Retry the operation, making sure you are not trying to change the user name of the default user.
4. If the problem persists, contact Technical Support.

ERROR: Current user is not authorized to do this operation!

You tried an operation (e.g., login password entry, set user name) to which you are not authorized (only the super user level can perform this function).

1. Check with your system administrator.
2. Make sure this is the user you want - check the Users table entry.
3. Verify the user's access level (admin, read write, or read only). Verify the command syntax ("add sys-user name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR").
4. See the "Configuring System / Login Users" section.

This card is in hardware mode and no setting allowed!

You tried to make a configuration change via the Web interface or the CLI, but the action was rejected. For example:

```
AgentIII C1|S3|L1D>set tdm inband enable
This card is in hardware mode and no setting allowed!
AgentIII C1|S3|L1D>
```

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. Make the required changes via DIP switch configuration. See the related section of the manual.
2. Change the Hardware/Software Jumper setting to Software mode.
3. Retry the configuration change via the Web interface or the CLI.
4. Contact Lantronix for more information. Contact Technical Support,

It must be a valid oid.

When you add a view/group/local user/remote user and the name contains "&" character, it can be added successfully, but the rest characters after "&" cannot be seen from web table list, CLI shows correctly.

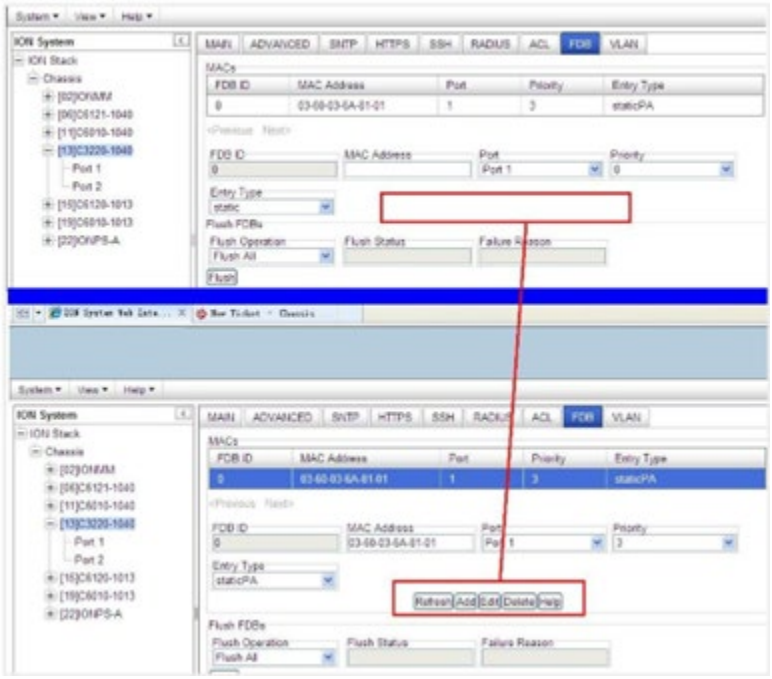
Set IP address type failed.

You tried to change the IP address type (mode), but the operation failed. For example:

```
C1|S5|L1D>set ip type=bootp addr=192.168.1.30 subnet-mask=255.255.255.0
Set IP address type failed.
```

1. Enter another (supported) command on this card, or use the "**go**" command to switch to the IONMM.
2. Make sure the DHCP or BootP server is correctly configured and running.
3. Retry the operation. See “Setting Up the IP Configuration” for the “set ip mode” command.
4. If the problem persists, contact Technical Support.

In IE8, 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*** *- 192.168.0.10 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

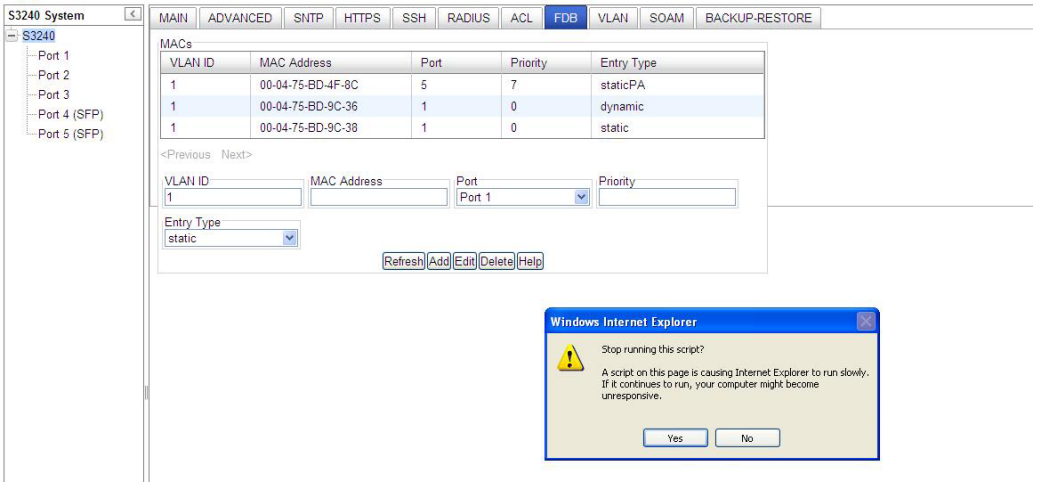
Websites that were designed for earlier versions of Internet Explorer might not display correctly in the current version. However, you can often improve how a website will look in Internet Explorer by using the new 'Compatibility View' feature. When you turn on Compatibility View, the webpage displayed (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 occured. 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.

Message:
Getting DNS server%u address fail%s
Invalid Ipv6 Gateway address!
Invalid Ipv6 Global address!
Invalid SNTP server address!
Invalid TFTP server address!
Please input a number to specify the DNS server index!"
prefix is out of range!
Meaning: An error was detected in IPv6 configuration information (e.g., you set a SNTP server address incorrectly).
Recovery:
1. CLI: Make sure the **set sntp-svr** format follows "set sntp-svr svr=<1-6> type=(ipv4|dns|ipv6) addr=ADDR". See the "IPv6 CLI Commands" section.
2. Web: Verify the IPv6 Management Status, Method, Prefix, and Gateway Method selections and the IPv6 Management Link Local Address, Management Address and Management Gateway settings.
3. Contact Tech Support if the problem persists.

Message:
Fail to set DNS server address!
Fail to set gateway address!
Failed to set ip address mode state!
Fail to set Ipv6 address prefix!
Fail to set IPv6 management state!
Fail to set RADIUS server address!
Fail to set RADIUS server address type!
Meaning: An IPv6 configuration change attempt failed (e.g., you entered an incorrect RADIUS, TACACS+, DNS server, or IPv6 address). For example, the RADIUS server configuration entry was invalid; only the first three valid DNS servers are available.
Recovery:
1. Enter only up to three RADIUS server addresses / types.
2. See the "set radius svr" command
Recovery:
1. Check the ION IPv6 Configuration Considerations. For example, enter only up to three RADIUS server addresses / types.
2. Verify the "ION IPv6 CLI Commands' and IPv6 Address Config – Web Method', and Changes to Existing ION Applications with IPv4 / IPv6'. For example, see the "**set radius svr**" command.

Message: *IP management is not supported on this card!*
Meaning: Try another function on this device, or switch to another device and try this function again.
Recovery:
1. Try another function on this device, or switch to another device and try this function again.
2. Upgrade the device(s) to the latest firmware version.
3. Contact Tech Support if the problem persists.

Message:
Fail to set Ipv6 Global address!
Fail to set gateway address!
Fail to set DNS server address!
Invalid address!
Invalid IP address!
Please input a digital number to port number!
Please input a valid ip address!
This trap address already exists!
Meaning: You made an invalid IP address entry.
Recovery:
1. For IPv4, enter a unique, valid fixed address length of 6. For IPv6, enter a fixed address length of 18.
2. See the related section of this manual and retry the operation.
3. Contact Tech Support if the problem persists.

Message:
Fail to analyse remote engine address!
Fail to get addr domain addr!
Invalid engineID!
No engine ID is specified for this address!
Remote engine address or port is not valid!
Example:

```
C1|S1|L1D>remove snmp remote user name=AliceB addrtype=ipv4
addr=192.168.1.30 port=162
No engine ID is specified for this address!
C1|S1|L1D>
```

Meaning: You tried to change an SNMP element but the engine ID was not recognized.
Recovery:
1. Check the **add snmp rmt engine** command parameters. See "IPv6 CLI Commands" in this manual.
3. Contact Tech Support if the problem persists.

Message:
Caution: only the first three valid DNS server can be available, please refer to user menu for the details
DNS server index is out of range!
Fail to set DNS server address type!
Invalid OID for this view
It must be a valid oid.
Now ipv4 mode is BOOTP, so you can not configurate dns server1 to server3.
Now ipv4 mode is DHCP, so you can not configurate dns server1 to server3.
Now ipv6 mode is dhcpv6, so you can not configurate dns server4 to server6.
Example:

```
C1|S1|L1D>remove snmp view name=defaultView oid=1
Invalid OID for this view
```

Meaning: A problem exists in DNS server configuration. You can set the DNS server when IPv4 address mode is not DHCP and IPv6 address mode is not DHCPv6. Only the first three valid DNS servers are available. Do not configure unselected mode parameters when another mode is enabled.
Recovery:
1. See "DNS Lookups over IPv6 Transport"
3. Contact Tech Support if the problem persists.

Message:
Error IP V6 Gateway Address
Multicast IPv6 address can not be set.
Local host IPv6 address can not be set.
Meaning: You entered an IPv4 value for the IPv6 address, or an IPv6 value for the IPv4 address.
Recovery:
1. Verify the IPv4 and/or IPv6 DNS address settings.
2. Enter a valid IPv6 address and retry the operation. See the related section of this manual and retry the operation.
3. Contact Tech Support if the problem persists.

Message:
Error IPv6 Address!
Error IPv6 Network Address
Its value must be an IPv4 address like '192.168.0.1'.
Its value must be an IPv6 address.
Its value must be an IP address or a domain name.
Its value must be an IPv4 address or IPv6 address.
Its value must be a valid subnet mask IP
Meaning: You entered an incorrect value for the IPv6 address, or there was an error with the IPv6 Condition value conversion.
Recovery:
1. Enter a valid IPv6 address and retry the operation. See the related section of this manual and retry the operation.
3. Contact Tech Support if the problem persists.

Message:
Its value must be an integer or IPv6 address like 'ffff:0:0:0:0:0:0:0'.
Its value must be an integer ranging from {from} to {to} or IPv6 address like 'ffff:0:0:0:0:0:0:0'.", {from: from, to: to}
Its value must be an integer greater than or equal to {from} or IPv6 address like 'ffff:0:0:0:0:0:0:0'.", {from: from}
Its value must be an integer less than or equal to {to} or IPv6 address like 'ffff:0:0:0:0:0:0:0'.", {to: to}
Meaning: You entered an incorrect value for the IPv6 address, or there was an error with the IPv6 Condition value conversion.
Recovery:
1. Enter a valid IPv6 address and retry the operation. See the related section of this manual and retry the operation.
3. Contact Tech Support if the problem persists.

Message:
It can be set to any characters combination except the space character.
Its value must be a character string less than 64 bytes
Its value must be a MAC address like 'XX-XX-XX-XX-XX-XX' (separated by '-').
Its value must be consist of a-f or A-F or 0-9 and the total length must be a dual from 18 to 128
Meaning: Information on the entry field.
Recovery:
1. Follow the entry field instructions.
2. Retry the operation. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
Fail to get syslog server address type!
Fail to set syslog server address!
Example:

```
Agent III C1|S1|L1D>set syslog svr type dns addr www.tndvt.com
Fail to set syslog server address!
C1|S1|L1D>show syslog config
C1|S1|L1D>set syslog svr type ipv4 addr 192.168.0.33
Fail to get SIC configure mode!
C1|S1|L1D>
```

Meaning: You tried to add a new syslog server, but the server IP address entry was not valid.
Recovery:
1. Enter a valid syslog server IP address and retry the operation. See the related section of this manual.
2. Contact Tech Support if the problem persists.

Message:
Fail to set group of the user!
Invalid group parameter for user!
Meaning: You tried to add a new SNMP local user, but the group entry was not valid.
Recovery:
1. Enter a valid SNMP group and retry the operation. See the "add snmp local user' command.
2. Contact Tech Support if the problem persists.

Message:
Invalid ipv6 input found!
IPv6 Address and Gateway should be at the same sub-net!
IPv4 Address and Gateway should be at the same sub-net!
the subnet mask of gateway is different from the one of global address
Meaning: You set up the IP address and gateway on different sub-nets. The subnet mask of the gateway is different from the subnet mask of the global address.
Recovery:
1. Change either the IP address or the subnet mask for the NID.
2. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
Error: need set subnet-mask when ipv4 address is set!
Error: need subnet-mask when ipv4 address is set!
Fail to set IPv4 address! (need set subnet-mask when ipv4 address is set!)
Fail to set Ipv6 Global address!
Fail to set Ipv6 address prefix!
Fail to set subnet mask! (need set subnet-mask when ipv4 address is set!)
Meaning: An error was detected in the attempted IP Address setup.
Recovery:
1. Verify the IP address, gateway address, DNS server or other related IP address setting.

2. See the "**Set IP address and subnet mask**" command.
3. Contact Tech Support if the problem persists.

Invalid address!
Invalid DNS server address!
Invalid gateway address!
Invalid IP address! (need set subnet-mask when ipv4 address is set!)
Invalid ipv6 address! (need set prefix when ipv6 address is set!)
Invalid RADIUS server address!
Invalid SNTP server address!
Invalid subnet mask!
Invalid TFTP server address:x
Please input a number to specify the DNS server index!
prefix is out of range!
Set ipv4 gateway address type

Meaning: An error was detected in the attempted IP Address setup.

Recovery:

1. Verify the IP address, gateway address, DNS server or other related IP address setting.
2. See the "**Set IP address and subnet mask**" command.
3. Contact Tech Support if the problem persists.

Message:

Inavlid network mask value, correct format like 2001:ef:201:3213::2000/ffff:ffff:: or 2001::1002/96\n
invalid ACL condition value, correct format like 2001:ef:201:3213::2000/ffff:ffff:: or 2001::1002/96\n
This is ipv6 multicast address which can not be set
This is ipv6 Unspecified address which can not be set
This is ipv6 loopback address which can not be set

Meaning: An error was detected in the attempted IP Address setup.

Recovery:

1. Verify the IPv6 address setting.
2. See the "Set IP address and subnet mask" command.
3. Contact Tech Support if the problem persists.

Message: *ERROR: The current mib table can only have a maximum of " + maximum + " records!*
Get Dynamic Table Length Failed1!
Get dynamic table capability failed!

Meaning: The dynamic table length limitation reached; the dynamic table is full and not available for adding records. The maximum of dynamic table that ION supports is 1024.

Recovery:

1. Limit the number of table entries to 1024.
2. Contact Tech Support if the problem persists.

Message:
ERROR: already have a ipv6Condition Type under the same level!
ERROR: already have a Condition Type under the same level!
ERROR: already have the same Condition Type under this rule!
ERROR: already have the same Condition Type under this rule!
ERROR: already have the same layer Condition under this rule!
Invalid ip6tables ACL condition index!
One ACL rule can only has one layer2 ACL condition(macaddr)!
One ACL rule can only has one layer3 ACL condition(ipv4addr or ipv4addrrange or ipv4network)!
One ACL rule can only has one layer4 ACL condition(tcpport or tcpportrange or udpport or udpportrange or icmp)!
One ip6tables ACL rule can only has one layer2 ACL condition(macaddr)!
One ip6tables ACL rule can only has one layer3 ACL condition(ipv6addr or ipv6network)!
One ip6tables ACL rule can only has one layer4 ACL condition(tcpport or tcpportrange or udpport or udpportrange or icmp)!
Meaning: An ACL Rule configuration problem exists. When IPv6 is enabled, you can have up to three of an IP style (IPv4 or IPv6).
Recovery:
1. Check the ACL Rule configuration settings.
2. See "DNS Lookups over IPv6 Transport".
3. Contact Tech Support if the problem persists.

Message:
Get Ipv6 Management Address
Get Ipv6 Management Prefix
IP address
IP subnet mask
Meaning: You entered a gateway IP address or IP subnet mask outside of the valid range.
Recovery:
1. Enter a valid gateway IP address and IP subnet mask.
2. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
VID already exist!
ERROR: already have the same layer Condition under this rule!
Fail to add ACL addition!
There is already a same named view!
Fail to create SNMP view!
We can create at most 6 trap hosts!
Meaning: There was a problem with an ip6tables ACL command.
Recovery:
1. Verify the IPv6 ACL command parameters. See the related section of this manual.
2. Retry the operation.
3. Contact Tech Support if the problem persists.

Message:
Fail to create parameter entry!
Fail to security name!
Notification type can only be trap or inform!
Meaning: An SNMP v3 operation failed.
Recovery:
1. Verify the SNMP v3 notify, security model, and security level parameter values.
2. Verify the "**add snmp traphost**" command. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
Notification type can only be trap or inform!
When notify type is not \"inform\", you can not set the value of \"timeout!
When notify type is not \"inform\", you can not set the value of \"retry!
When traphost version is v1, the setting for notify, timeout and retry will be ignored!
Meaning: You entered an SNMP parameter that does not apply to the current SNMP configuration settings.
(You tried setting 'timeout' or 'retry' value when 'notify' type is set to trap').
Recovery:
1. Verify the SNMP 'notify' parameter value.
2. See the "SNMP Configuration" section of this manual.
3. Contact Tech Support if the problem persists.

Message:
The specified SNMP group does not exist!
The specified SNMP view does not exist!
Meaning: You tried to remove an SNMP v3 group or view that does not exist.
Recovery:
1. Confirm the group or view that you want to delete.
2. Retry the operation. See the "SNMP Configuration" section of this manual.
3. Contact Tech Support if the problem persists.

Message: *the value of dupAddr detect beyond the scope.*
Meaning: The IPv6 Duplicate Address Detect mechanism detected a duplicate address or invalid address.
A station may have failed the IPv6 stateless auto-configuration process because the router is not presented on the same link or its DAD cycle is failed.
Recovery:
1. Check the attached device's IPv6 address.
2. Verify the attempted operation; refer to the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
Adding VLAN failed
Deleting VLAN failed
Modifying VLAN failed
The default VLAN 1 cannot be modified or removed!
Meaning: The VLAN operation is very slow when adding multiple VLANs to the system, or modifying or deleting a VLAN fails.
Recovery:
1. Upgrade to the latest firmware version if not currently at the latest version.
2. Retry the operation. Make sure you are not creating more VLANs that are supported. See the 'VLAN Configuration" section.
3. Contact Tech Support if the problem persists.

Message:
All-zero MAC address is not valid for ACL condition!
invalid ACL condition value, correct format like 2001:ef:201:3213::2000/ffff:ffff:: or 2001::1002/96\n
Meaning: You entered an invalid IPv6 MAC address in the ACL Condition field.
Recovery:
1. Verify the IPv6 MAC address entered in the ACL Condition field is valid.
2. See "ION IPv6 Function Descriptions" and "ACL" section.
3. Contact Tech Support if the problem persists.

Message: *This vlan has already been used as the management vlan, please modify.*
Meaning: You tried to add a VLAN whose VID is the same as the existing Management VLAN ID.
Recovery:
1. Enter a valid, unique VLAN ID.
2. See "VLAN Configuration".
3. Contact Tech Support if the problem persists.

Message: *RADIUS authentication server: index addr-type addr retry timeout*
Meaning: An invalid user and password to login ION was attempted.
Recovery:
1. Verify the user name and password entries.
2. Verify the RADIUS configuration setting, e.g.:

```
Agent III C1|S1|L1D>show radius config RADIUS client state: enable
```

3. Contact Tech Support if the problem persists.

Message: *The certificate file(s) is being copied. Please wait...*
Meaning: Information only.
Recovery:
1. Wait for the process to complete.
2. Contact Tech Support if a problem occurs.

Message: *Invalid syslog server address!*
Meaning: You entered a server address for the Syslog server.
Recovery:
1. Re-enter the command using a valid Syslog server address.
2. See the related section of this manual for more information.
3. Contact Tech Support if the problem persists.

Message:
All-zero MAC address is not valid for ACL condition!
Invalid condition valule: %
Meaning: You entered a command with an invalid MAC address.
For example:

```
Agent III C1|S1|L1D>add acl condition type macaddr srcdst src oper equal value 00-00-00-00-00-00
All-zero MAC address is not valid for ACL condition!
```

Recovery:
1. Re-enter the command using a valid MAC address.
2. See the related section of this manual for more information.
3. Contact Tech Support if the problem persists.

Message: *snmp operation error, possible reasons: invalid data, error data sequence, dynamic table capability limit, etc.*
Meaning: You exceeded the limitation of 255 ACL/ACLv6 rules or conditions. When you try to add more than 255 ACL /ACLv6 rules, or try to add more than 255 ACL/ACLv6 conditions, this warning displays.
Recovery:
1. Make sure you remain within the limit for ACL/ACLv6 rules or conditions.
2. See the related section of this manual for more information.
3. Contact Tech Support if the problem persists.

Message:
The maxium length of system contact is 255!
The maxium length of system name is 255!")
The maxium length of system location is 255!
The maxium string length of circuit ID is 64
The maxium string length of device description is 255
Meaning: You entered too many characters in an entry field.
Recovery:
1. Re-enter the text in the entry field using fewer characters.
2. Verify the new entry is accepted without any errors.
3. Contact Tech Support if the problem persists.

Message: *Failed to transfer the certificate file(s)!*
Meaning: The HTTPS certificate file transfer failed.
Recovery:
1. At the message "*Please input Private File Name!*" enter a valid name. See "Configuring HTTPS".
2. Verify the name of the certificate file to be copied and/or the private key file to be copied.
3. Only tftp supported in web and should be set at the end. See the "TFTP (Trivial File Transfer Protocol)" section of this manual. Try uploading the Private File using the CLI method.
4. Contact Tech Support if the problem persists.

Message: **Connection closed by foreign host.**
Meaning 1: An SSH operation caused the connection to close. For example:

```
Agent III C1|S1|L1D>set ssh server state disable
Agent III C1|S1|L1D>Connection closed by foreign host.
```

Meaning 2: A SOAM operation caused the connection to close. For example:

```
Agent III C1|S8|L1D>show soam md 1
Connection closed by foreign host.
```

Recovery:
1. Restart the operation.
2a. Verify the SSH configuration. See the related section of this manual.
2b. Verify the SOAM configuration. See the "SOAM' of this manual.
3. Contact Tech Support if the problem persists.

Message:
Please input a digital number to specify radius server index!
RADIUS authentication server index is out of range!
Set RADIUS server secret Failed
The RADIUS authentication server specified does not exist!
This card can not set RADIUS secret!
Meaning: You entered a RADIUS CLI command incorrectly, or the RADIUS server was not configured, or the card does not support RADIUS.
Recovery:
1. Check the CLI command syntax and re-enter the command. See the related section of this manual.
2. Make sure the RADIUS server is up and running.
3. Contact Tech Support if the problem persists.

Message: *Error: Set egress/ingress rate failed!*
Meaning: You used the CLI command to select 5M/7M/9M/90M in "Egress Rate Limit" or "Ingress Rate Limit" drop-down list and clicked **Save**. ION cannot accept the configuration that you entered.
Recovery:
1. Check the CLI command syntax and re-enter the command.
2. Contact Tech Support if the problem persists.

Message:
fdbid must equal to 0 now!
No data in VLAN forward database table now!
Please input a number to specify the fdbid!
The specified conn-port does not exist!
Meaning:

```
Agent III C1|S3|L1D>show fwddb config fdbid 0
No data in VLAN forward database table now!
Agent III C1|S3|L1D>add fwddb mac 00-00-00-00-00-01 conn-port 1 priority 2 type
static
Agent III C1|S3|L1D>add fwddb mac 00-00-00-00-00-02 conn-port 1 priority 2 type
static
```

Recovery:
1. Check the CLI command syntax and re-enter the command. See the related section of this manual.
2. Verify the FDB configuration. See the related section of this manual.
3. Verify that the card on which the command was entered can support the function attempted (e.g., the case where an ION FBRM BFFG card entered a command that only an ION_NID supports, such as a **fwddb config** command).
4. Contact Tech Support if the problem persists.

Message:
Invalid priority override value!
The range of priority is 0 .. 7!
Meaning: You entered the command "**add fwddb mac**" with a priority outside of the valid range.
Recovery:
1. Check the CLI command syntax and re-enter the command. See the related section of this manual.
2. Verify the VLAN configuration. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
Fail to find first row of acl rules!
Fail to get ACL rule!
Fail to get ip6tables ACL rule chain type!
Fail to get ip6tables ACL rule priority!
Fail to get ip6tables ACL rule policy!
Fail to get ip6tables ACL rule table type!
Fail to get ip6tables ACL rule traprate!
No ACL rule now!
Meaning: You entered a command (**show ip6tables acl rule**) to display the current ACL table, chain, and/or policy, but the command failed.
Recovery:
1. Note that the value of table can only be "filter" and the value of chain can only be "input".
2. Verify the ACL configuration. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message: *Fail to get SIC configure mode!*
Meaning: The 'reset to factory configuration' failed. For example:

```
C1|S1|L1D>reset factory
Fail to get SIC configure mode!
```

Recovery:
1. Verify the card configuration.
2. Verify the card firmware version.
3. Contact Tech Support if the problem persists.

Message: *Setting values failed (snmp operation error, possible reasons: invalid data, error data sequence, dynamic table capability limit, etc)*
Meaning: Possible reasons include 1) You exceeded the ION system support maximum of 64 ACL rules and/or 128 ACL conditions. 2) You entered an invalid or unrecognized IP address setting.
Recovery:
1. Reduce the number of ACL entries. See the related section of this manual.
2. Verify the IP address, IP Gateway address, IPv6 Prefix length, etc. See the related section of this manual.
3. See "IPv6 Troubleshooting".
4. Contact Tech Support if the problem persists.

Message:
An error occurred during a connection to 2001:db8:2:f101:14a:9732:7d4d:aef5:443.
Peer's Certificate issuer is not recognized.
(Error code: sec_error_unknown_issuer)
Meaning: FireFox cannot support IPv6 mode to login to the ION system. The ION system cannot support the FireFox browser to login in SSL mode in IPv6.
Recovery:
1. Temporarily switch to IPv4 or to another browser.
2. Complete the login and switch back per step 1 as needed.
3. Contact Tech Support if the problem persists.

Message: *No DMI support on this port!*
Meaning: You tried to set DMI on a port that does not support DMI.
Recovery:
1. Choose another port that supports DMI.
2. Contact Tech Support if the problem persists.

Message:
SNMP community name length can not be 0!
SNMP community name length should be shorter than 32!
Meaning: You entered an invalid community name for SNMP operation.
Recovery:
1. Enter an SNMP community name with 1-31 characters.
2. See the related section of this manual.
3. Contact Tech Support if the problem persists.

Message:
DB is full. Max of MAs and MEGs per system reached
MEG with this index already exists. MA and MEG have shared index space
Parent of MA is MD. Try to find MD with given index. It must be configured.
Meaning: The SOAM MD/MA/MEG configuration can not be supported.
Recovery:
1. Verify the SOAM configuration. See the "SOAM' section of this manual.
2. Remove any unused MA or MEGs and restart the operation.
3. Contact Tech Support if the problem persists.

Message:
Error - Send the command failed: Ambiguous input: group MAC address provided while isMulticastLb flag not set.
Invalid input: Destination MAC address is invalid.
Invalid MAC address.
Storage failed!
This MA is in used.
Unknown error!
Meaning: A SOAM MIB error was logged during SOAM operation / configuration.
Recovery:
1. Verify the SOAM configuration. See the "SOAM' section of this manual.
2. Remove any unused MA or MEGs and retry the operation.
3. Contact Tech Support if the problem persists.
Message: *Please select the MEP from the table!*
Meaning: You tried to perform part of a SOAM function and clicked the **Refresh** button before completing the SOAM function.
Recovery:
1. Complete the SOAM function and click the **Refresh**" button when completed.
2. See the "SOAM' section of this manual.
3. Contact Tech Support if the problem persists.

Message:
4_T1 port display name enhanced/Remote card version checking with stand alone card.
Cannot find software version of this card!
Error: Set egress/ingress rate failed!
IONMM card version is 1.3, and ARM-based card is 1.2, the SIC needs upgrade
Software version of this card (" + cardVersion + ") is not supported, please upgrade to the same version as the Standalone Card
Software version of this card (" + cardVersion + ") is not supported, please upgrade to the same version as the IONMM
Various FP and ION web interface and CLI compatibility messages.
Meaning: An ION NID compatibility issue occurred. There is a mismatch between a NID and the IONMM firmware versions. For example, you selected 5M/7M/9M/90M at the "Egress Rate Limit" or "Ingress Rate Limit" dropdown, clicked **Save**, and the message displayed.
Recovery:
1. Verify your configuration using the information below.
   - ION version 1.2.2 is released for these AVR-based SIC cards with some bug fixes: C3110, C3210, C2110, C2210, C611x, C612x, C6210, BPC and Power Supply.

- ION version 1.3.0 is released for these ARM-based SIC cards with fixes and powerful new features: IONMM, C/S222x, C/S322x, and C/S323x.
- IONMM v1.3 supports the v1.2 AVR-based SIC cards. IONMM v1.3 does not support the v1.2 ARM-base SIC cards.

ARM-based SIC; IONMM revision	1.1	1.2	1.3
1.1	Y	N	N
1.2	N*	Y	N
1.3	N*	N*	Y

Note 1: ARM-base SIC cards include IONMM, C/S222x, C/S322x, and C/S323x.
Note 2: N* means an error interface will display to remind you to upgrade the SIC firmware to the same revision of IONMM.

AVR-based SIC; IONMM revision	1.1	1.2	
1.1	Y	N	
1.2	N*	Y	
1.3	N*	Y	

Note 1: AVR-base SIC cards include C3110, C3210, C2110, C2210, C611x, C612x, C6210, BPC, and Power Supply.

1. Check the firmware versions of the NID and IONMM and upgrade as needed.
2. Check the Release Notes for possible installation scenarios.
3. Re-try the operation.
4. Contact Tech Support if the problem persists.

Problem: S3231 port 1 link is down and the S3231 can't be managed anymore.
Meaning: The S3231 port 1 and attached switch ports should all have link up and S3231 should be able to be managed. If the Management VLAN config has not changed, the S3231 should be manageable all the time.
For example, after the S3231 has run for about two days under Management VLAN, you performed some get and set operations on this card during this time, but made no changes to the Management VLAN configuration. You reboot S3231 to try to recover the Management but it doesn't work.
Recovery: Verify if MAC security is enabled; if so, the port is closed when more than one MAC address arrives at this port (normal operation)

Message:
warning: server1 to server3 is just used for ipv4!
warning: server4 to server6 is just used for ipv6!
Meaning: The DNS 1 through DNS 6 entries can be in IPv4 or IPv6 format, or both (a combination of up to three of each). DNS servers 1-3 are for IPv4; DNS servers 4-6 are for IPv6.
Recovery:
1. Change the DNS server settings to make them valid.
2. See “DNS ‘3 vs. 3’ Rule (‘Up to 3’ Rule)”.

Web Interface Messages

IMPORTANT

For each procedure described below, do each step sequentially as indicated. If the result of a step corrects the problem, **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., on an 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 S2220-1013 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support.

Cannot Ping IONMM Device

With the "Management VLAN" state set to "enabled", the PC cannot ping the IONMM device.
The reason is enabling the Management VLAN function gives management control to the Management VLAN that you enabled.

1. 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.
2. 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 was specified in the **Firmware File Name** field in Windows XP (just "**db**" with no extension in Windows 7).
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.1.0.5*, or *x323x.bin.1.0.5*).
3. If the problem persists, contact Technical Support.

Invalid input found!

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

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

Invalid password!

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

1. Sign in using the correct password. The default password is **private**. Note that the password is case sensitive. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. If the problem persists, contact Technical Support.

Failed to retrieve DMI info on current port.

You clicked the Device port's DMI tab, but the device does not support DMI. Not all NID models support DMI.

1. Verify that the NID 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 and discovery to take place.
4. If the problem persists, contact Technical Support.

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

This is the current operational state of the interface.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 in online and available.
   - The correct file name, db.zip, is specified (in Windows XP); just "**db**" in Windows 7.
   - The db.zip 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.

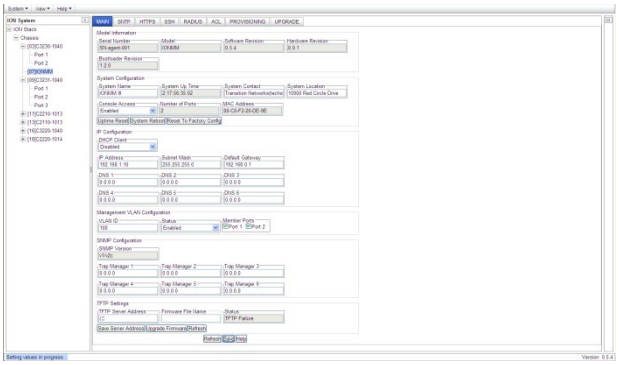
1. Click the Continue to this website... selection.
2. See the "Configuring HTTPS" section.

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.

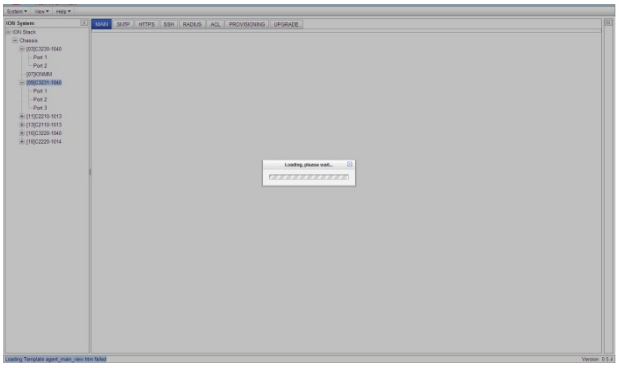
Message: "*Setting values in progress ...*" displays continuously

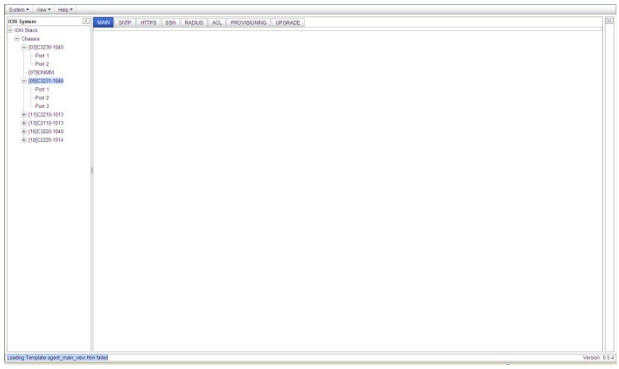
The message "Setting values in progress ..." displays for over 10 minutes after you set up a VLAN 100, then set Management VLAN to Enabled and clicked Save.



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

Meaning: Not all NID models support DMI. Lantronix NIDs that support DMI have a "D" at the end of the model number. If you click the DMI tab on a NID model that does not support DMI, the message "*The DMI feature is not supported on current port*" displays.

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

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

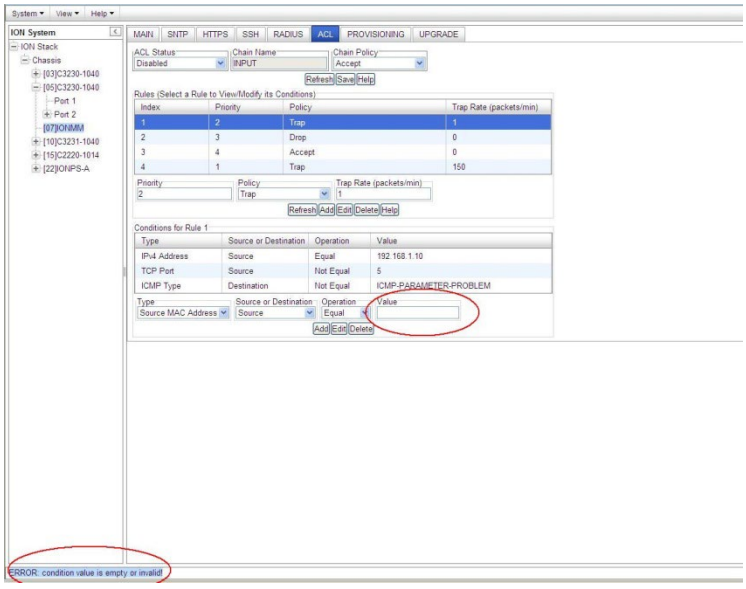
Message: *priority is empty or invalid*

Meaning: Can't change ACL status to enable, message box show "priority is empty or invalid"

Recovery: 1. Review the ACL entries. See “Configuring an ACL”.

2. If the problem persists, contact Technical Support.

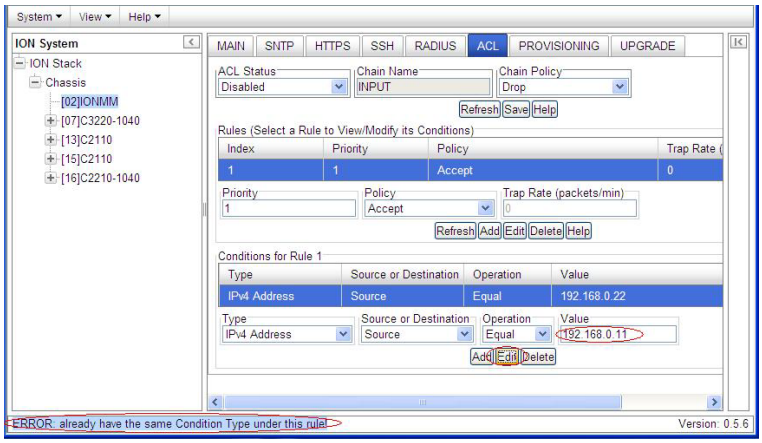
Message: *ERROR: condition value is empty or invalid!*



Meaning: At **IONMM** > **ACL** tab, you tried to add a Condition to a Rule, but you did not enter a Value.

Recovery: 1. Select the Rule. 2. Select the **Type**, **Source or Destination**, and **Operation** field parameters, and then enter a Value field parameter (e.g., a MAC address, IP Address, TCP Port, etc.), depending on the **Type** field parameter that you selected. 3. Click the **Add** button. See “Configuring an ACL”.

Message: *Error - already have the same Condition Type under this rule*



Meaning: At the **IONMM** > **ACL** tab, when you try to edit or add a Condition to an IP address, the error message displays.

Recovery: 1. Select a different **Condition Type**, and then change back the original type condition. The Type selections are Source, MAC Address, IPv4 Address, IPv4 Address Range, IPv4 Network, TCP Port, TCP Port Range, UDP Port, UDP Port Range, and ICMP Type.

2. See "Configuring an ACL".

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

Meaning: The system password was accepted, but the system

Recovery: Sign in using the correct password. The default password is private. Note that the password is case sensitive.

1. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. Verify the SNMP configuration.
4. If the problem persists, contact Technical Support.

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

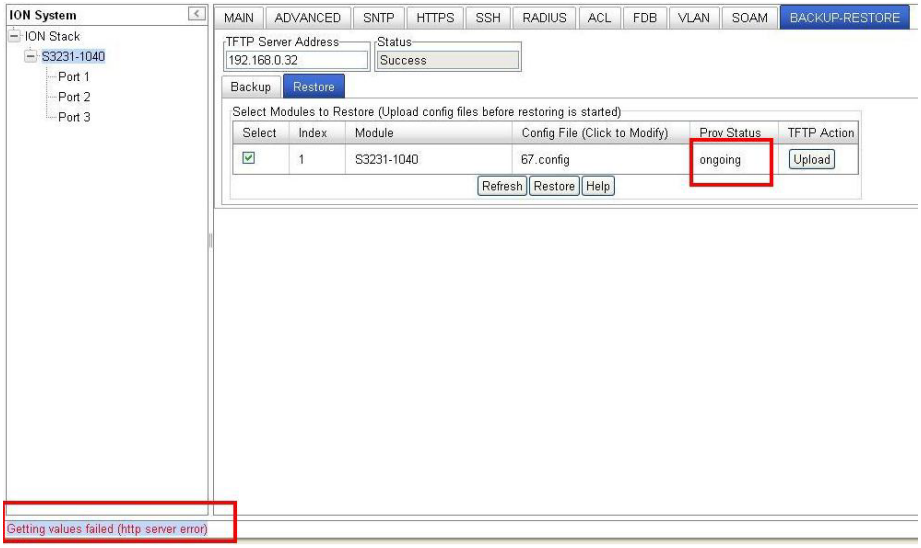
Meaning: You clicked on **Online Help** from the **Help** dropdown without first selecting a device.

Recovery:

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

Message: *Getting values failed (http server error)* and *"ongoing" Prov Status*

Meaning: When performing a Restore operation (BACKUP-RESTORE tab) with SOAM configured, the message "*Getting values failed (http server error)*" displays and the Prov Status column displays "*ongoing*" after wait message box disappears.

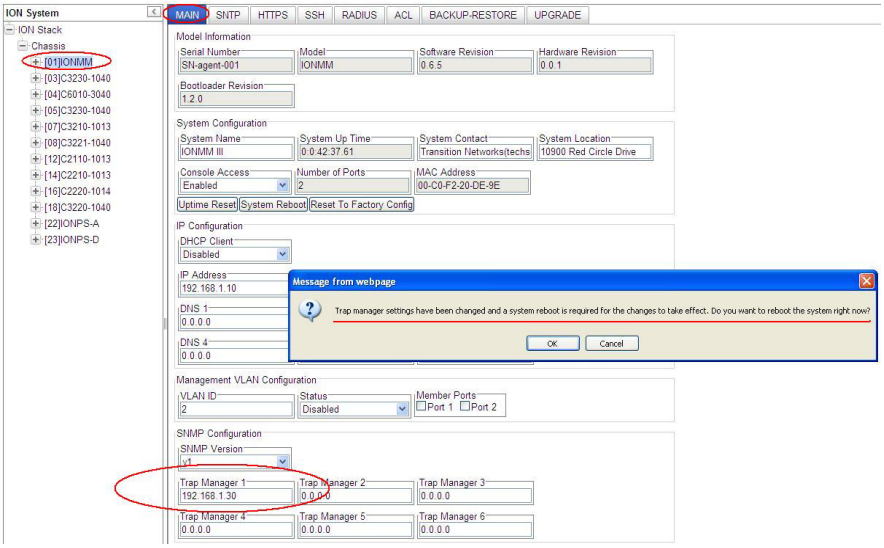


During the card Restore operation, the HTTP/HTTPS server must restart in order to activate the new configuration. At that time, the Web interface momentarily loses connection with the Web server, but when you click the **Refresh** button, the status display and other web operations work normally.

Recovery:

1. Click the **Refresh** button.
2. Verify the Restore configuration and continue operation.
3. If the problem persists, contact Technical Support.

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?*

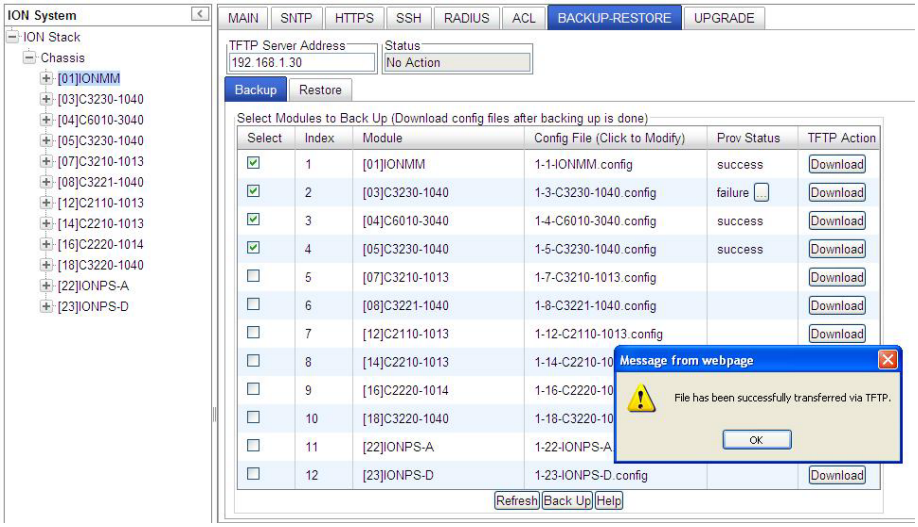


Meaning: Information only. At **IONMM > MAIN** > **SNMP Configuration** > **Trap Manager x** you entered an IP address for a trap server.

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.

Message: *No such user!*

Meaning: The User Name entered is not valid. The entry must match that of a valid existing user.

Recovery:
1. Verify the User Name and Password at **IONMM** > **USERS** tab.
2. Make sure the parameters are entered correctly (no spaces between characters in the User Name) and retry the Sign in.
3. Make sure the Num Lock and Caps Lock keyboard keys are turned off.
4. See the "Configuring System / Login Users - Web Method" section.

Message: *Wrong password!*

Meaning: The Password entered is not valid. The entry must match that of a valid existing user.

Recovery:
1. Verify the User Name and Password at **IONMM** > **USERS** tab.
2. Make sure the parameters are entered correctly (at least 8 characters containing letters and numbers in the Password) and retry the Sign in.
3. Make sure the Num Lock and Caps Lock keyboard keys are turned off.
4. See the "Configuring System / Login Users - Web Method" section.

Problem: If the Management VLAN ID is entered in the VLAN table, the Management VLAN associated with the VLAN ID cannot be enabled. ION versions 1.3.1 and 1.2.1 both have the same result.
Meaning: In ION V1.2.1 and above, the Management VLAN cannot be viewed or changed in the VLAN table.
Recovery:
1. Remove the Management VLAN ID in the VLAN table.

SNMP Messages

For any problem that persists, contact Tech Support.

Basic Recovery Steps

You entered a command, but the operation failed or is still in process.

1. Wait for a few moments for the operation to complete.
2. Use the **Help** or **?** command to get assistance (help) on a group of commands or on a specific command.
3. Make sure this is the command you want and that the device/port/configuration supports this command.
4. Make sure this device/port supports the function attempted. Use the **go** command to switch locations.
5. Verify the command syntax and re-enter the command. See the related section of the manual for specifics.
6. Try using the Web interface to perform the function.
7. If the "continue **y**(es) **n**(o)" prompt displays, type **y** and press **Enter** to continue.
8. If the problem persists, contact Tech Support.

Message:
Bad engine ID value after -3E flag.\n
Bad key value after -3m flag.\n
bad mask
bad mask length
bad source address
cannot resolve source hostname
Can't set up engineID of type text from an empty string.\n
community name too long
could not generate localized authentication key (Kul) from the master key (Ku).
could not generate localized privacy key (Kul) from the master key (Ku).
could not generate the authentication key from the supplied pass phrase.
could not generate the privacy key from the supplied pass phrase.
Could not get proper authentication protocol key length
could not get proper key length to use for the privacy algorithm.
example config COMMUNITY not properly configured
example config NETWORK not properly configured
Meaning: You entered an SNMP v3 command, but the command failed due to an invalid or misinterpreted entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
improper key length to -l
Invalid authentication protocol specified after -3a flag: %s\n
invalid EngineID argument to -e
invalid key value argument to -l
invalid key value argument to -m
Invalid privacy protocol specified after -3x flag: %s\n
Invalid security level specified after -3l flag: %s\n
Meaning: You entered an SNMP v3 command, but the command failed due to an invalid or improper parameter entry.
Recovery: 1) Make sure this is the command you want. Use the Help **(?)** command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support. .

Message:
malloc failure processing -3e flag.\n
malloc failure processing -e flag
Missing argument after SNMPv3 '-3%c' option.\n
missing COMMUNITY parameter\n
missing CONTEXT_NAME parameter
missing NAME parameter
missing SOURCE parameter
Need engine boots value after -3Z flag.\n
Need engine time after \"-3Z engineBoot,\".\n
no authentication pass phrase
no IP address for source hostname
security name too long
Unknown authentication protocol
Unknown authentication type
Unknown EngineID type requested for setup (%d). Using IPv4.\n
Unknown privacy protocol
Unknown privacy type
Unknown SNMPv3 option passed to -3: %c.\n
Unknown version specification
Unsupported enginedIDType, forcing IPv4
Meaning: You entered an SNMP v3 command, but the command failed due to an unrecognized entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
Are you sure to delete all the views with the name xx? (confirm)
Are you sure to delete this view ? (confirm)
Adding Community String failed!
Adding group failed!
Adding View failed!
Add Security group failed!
Add user failed!
bad security model, should be: v1, v2c or usm or a registered security plugin name
bad security level (noauthnopriv, authnopriv, authpriv)
bad prefix match parameter \"0\", should be: exact or prefix - installing anyway
bad prefix match parameter, should be: exact or prefix
Delete community string failed!
Delete user failed!
Delete vacm security group failed!
Delete view failed!
Edit view failed!
Failed to change group!
failed to create group entry
Illegal configuration line: missing fields
Illegal view name
Meaning: You entered an SNMP v3 command, but the command failed due to an unrecognized entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the

command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
missing GROUP parameter
missing SECURITY parameter
missing NAME parameter
missing CONTEXT parameter
missing MODEL parameter
missing LEVEL parameter
missing PREFIX parameter
Nothing changed!

Meaning: You entered an SNMP v3 command, but the command failed due to a missing parameter entry.

Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
Adding Remote Engine ID failed!
Add remote user failed!
Adding Target Address failed!
Delete Remote Engine ID failed!
Delete remote user failed!
** Delete remote user successfully! Trying to delete group... (status message only - displays momentarily)*
ERRPR: There is already a same host with the input IP and Port!
ERROR: There is already a same named community string!
ERROR: There is already a group with the same group name and security model!
ERROR: There is already a same named user!
ERROR: There is already a same named view!
ERROR: There is already a same remote engine ID!
If SNMP Engine ID is modified, all the users will be erased, are you sure?

Meaning: You entered an SNMP v3 command, but the command failed.

Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) Make sure you enter a unique host, community, group, user, view, or engine ID. 6) If the problem persists, contact Tech Support.

Message:
Cannot create SNMP group on this card!
Cannot remove SNMP view on this card!
Cannot remove this group!
Cannot remove this view!
Cannot set filter type of a SNMP view on this card!
Cannot set SNMP local engine ID on this card!
Cannot set notify view of a SNMP group on this card!
Cannot set read view of a SNMP group on this card!
Cannot set write view of a SNMP group on this card!
Cannot show SNMP group on this card!
Cannot show SNMP local engine ID on this card!
Cannot show SNMP view on this card!
Fail to create SNMP group!
Fail to get SNMP group!
Fail to get SNMP local engine ID!
Fail to get SNMP local user!
Fail to get SNMP remote user!
Fail to get SNMP user!
Fail to remove SNMP group!
Fail to set SNMP local engine ID!
Fail to set SNMP notify view!
Fail to set SNMP read view!
Fail to set SNMP view status!
Fail to set SNMP write view!
Invalid OID for this view!
Local Engine ID length range is <5 - 32>!
No SNMP group created now!
No SNMP local user created now!
No SNMP user created now!
No such SNMP group name!
SNMP view name length should be shorter than 32!
The specified user does not exist!
Meaning: You entered an SNMP v3 command, but the command failed. For example, when the security model is v1 or v2c, the groups "public" and "private" cannot be removed; but when the security model is v3 the groups "public" and "private" can be removed.
Recovery: 1) Make sure this is the command you want. 2) Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) Make sure the group, engine or user to be edited exists. 7) If the problem persists, contact Tech Support.

Message:
ERROR: Remote engine ID could not be the same as local engine ID!
ERROR: There is already a same remote engine ID!
ERROR: There is already a same remote engine ID with the input ip and port!
Meaning: You entered an SNMP v3 command, but the command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
Reseting local Engine ID will delete all exist local users, continue?(y: yes, n: no)
Meaning: You entered an SNMP v3 command, but a confirmation message displayed.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Enter **n** if you are not sure you want to reset the local Engine ID, or enter y to continue to reset the local Engine ID and delete all existing local users.

Message:
ERROR: Adding sub oid tree to defaultView is prohibited!
ERROR: defaultView can not be deleted!
ERROR: Modifying defaultView is prohibited!
ERROR: Please do not modify the View Name or the OID Sub Tree!
ERROR: Sub oid tree in defaultView can not be deleted!
ERROR: This group can not be deleted!
Meaning: You entered an SNMP v3 command, but the add/delete/modify command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
EngineID length must be in range [9..64]!
Invalid engineID!
Password is too long!
The password name length must be in range [1..64]!
The authentication password length must be in range [8..64]!
The privacy password length must be in range [8..64]!
Meaning: You entered an SNMP v3 command, but the command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
Cannot add SNMP view on this card!
Cannot show SNMP view on this card!
Cannot show SNMP trap hosts on this card!
Fail to get SNMP target address!
Fail to get SNMP view!
No SNMP view created now!
No SNMP trap host is created now!
Trap version is out of range!
Meaning: You entered a "**show snmp traphost**" or "**show all SNMP trap hosts**" or "**show snmp view**" command that failed to complete.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
Cannot add SNMP trap hosts on this card!
Fail to create notif table!
Fail to create parameter entry!
Fail to create trap host!"
Fail to set domain!
Fail to set traphost address!
Fail to set traphost parameters!
Fail to set traphost tag list!
Fail to security model! <set?>
Fail to security message process model! <set?>
Fail to security name! <set?>
Fail to security level! <set?>
Fail to set notif tag!
Fail to set notif type!
Invalid address!
SNMP community/security name length should be shorter than 32!
We can create at most 6 trap hosts!
Meaning: You entered a "**add snmp traphost**" command that failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
Fail to get SNMP target address!
The specified trap host does not exist!
Meaning: You entered a "**remove snmp traphost**" command that failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
Cannot show SNMP trap hosts on this card!
Fail to get SNMP target address!
Cannot remove SNMP community on this card!
SNMP community name length should be shorter than 32!
Fail to get SNMP target address!
The specified community has existed!
Cannot find the specified community!
Fail to get remote engine!
Fail to get user_to_group entry!
Fail to remove snmp user!
Fail to remove snmp view!
Fail to remove snmp group!
Fail to remove snmp user-group mapping!
Fail to remove snmp community!
Fail to remove snmp traphost!
Meaning: You entered an SNMP community command (get/set/show/add/remove), but the command failed to complete.

Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
When security level is v1 or v2c, security model can only be noAuthNoPriv
Fail to get community name! (*the device will search all rows of the SNMP Community Table, and if the community name can not be found, will add it*)
Fail to create community!
Meaning: You entered an SNMP Traphost or SNMP Trap Manager CLI command, but the command failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
Cannot add SNMP trap hosts on this card!
The specified trap host has existed!
Meaning: You tried to enter an "**add snmp community name**" command, but the command failed to complete.
Recovery:
1) Verify the "**access mode**" and "**community name**" parameter syntax. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If required, at the command prompt, enter the ION login and Password information. 5) If the problem persists, contact Tech Support.

Message:
Fail to get SNMP view!
Cannot show SNMP view on this card!
No such SNMP view name!
No SNMP view created now!
Meaning: You entered a "**show snmp view**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP Group Name of 8-32 characters. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If required, at the command prompt, enter the ION login and Password information. 5) If the problem persists, contact Tech Support.

Message:
authentication protocol is invalid!
Fail to create SNMPv3 usmuser!
Fail to get response from snmpd!
Fail to get response from snmpd!
Fail to send message to snmpd!
Fail to set group of the user!
Privacy protocol is invalid!
Meaning: You entered a "**add snmp local user**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP user. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message: *SNMP group name length should be shorter than 32!*
Meaning: You entered a "**set snmp local user name**" command but the operation failed.

Recovery: 1) Verify that you entered a unique SNMP group name of 8-32 characters. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
Fail to create SNMPv3 usmuser!
Remote engine address is not valid!
Meaning: You entered a "**add snmp remote user**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP user name and engine ID. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
Fail to analyse remote engine address!
Fail to create SNMPv3 usmuser!
Meaning: You entered a "**add snmp remote user name**" command but the operation failed.
Recovery:

Message: *Cannot show SNMP remote engine on this card!*
Meaning: You entered a "**show snmp remote engine**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP remote engine ID. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
Fail to get SNMP remote engine!
Please input a digital number to specify trap rate!
The specified remote engine has existed!
Meaning: (e.g., you entered an "**add snmp remote engine**" command but the operation failed.
Recovery: 1) Verify that you want this operation performed. If you are not sure, enter **n** and press **Enter**. 2) To continue, type **y** and press **Enter**. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message: *If you remove this remote engine, all remote users related to this engine will also be removed, continue?(y: yes, n: no)*
Meaning: You entered a "**remove snmp remote engine**" command but the confirmation message displayed.
Recovery: 1) Verify that you want this operation performed. If you are not sure, type **n** and press **Enter**. 2) To continue, type **y** and press **Enter**. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message: *Notification type can only be trap or inform!*
Meaning: You entered a "**get prov tftp svr**" or "**set prov tftp svr**" command but the operation failed.
Recovery: 1) Re-enter the command with "Trap" or "Inform" as the parameter. 2) Make sure the SNMP user's security model is v3. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message: *ERROR: There is already a remote user with the same name, ip and port!*
Meaning: You entered a duplicate record using the "add snmp rmt user" command.
Recovery: 1) Re-enter the command with a unique user name, IP address, and Port number. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
SNMP user name length should be shorter than 32!
This user already exists!
Meaning: The user already exists or you entered too many characters (32 characters maximum) for the SNMP User Name.
(The SNMP user's security model can only be v3.)
Recovery: 1) Re-enter the command with a unique user name, IP address, and Port number. 2) Make sure the user name entered has less than 32 characters in it. 3) Make sure the SNMP user's security model is **v3**. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
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.
Meaning: You attempted a function that is not supported by this version of firmware.
Recovery: 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.

Message:
The confirm password is not identical with the password!
The user name length must be in range [1..64]!
The user name must begin with an alphanumeric char!
You can only change your own password, not others!
Meaning: You entered a command to create a new system user, but the command failed.
Recovery: 1) Verify the command syntax ("**add sysuser name**=NAMESTR **level**=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR"). 2) Retry the operation, making sure the "pass" and "confirmpass" entries match. See the related command section.
3) If the problem persists, contact Technical Support.

Message: *Invalid input of timout value!*
Meaning: You set an unsupported SNMP trap timeout boundary value.
Recovery: 1) In the "**add snmp traphost**" command, specify a valid timeout (-15s%-16s%-5u%-30s%-16s%-12s%-12u%-12u%s (change from 8u to 12us). For example:

C1|S1|L1D>**add snmp traphost** version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6 security_level authPriv notify trap timeout=<0-2147483647>]
C1|S1|L1D>**add snmp traphost** version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6 security_level authPriv notify trap timeout 1000 retry 25

Problem: An SNMP user cannot access the IONMM.
Meaning: The User security level is not compatible with the Group level. For example, you added an SNMPv3 User to a SNMP v1 Group, or added a User to a non-existing Group, so this user can not access the IONMM.
Recovery: 1) Make sure the Group exists. Verify the User's security level. See the "Configure SNMP" section for specific details.

Problem: Can't assign a SNMPv3 User to multiple Groups.
Meaning: The SNMPv3 standards do not allow you to assign a SNMPv3 user to multiple groups.
Recovery: 1) Create an additional, unique user. 2) Assign the new user to a different group. 3) Make sure that each user belongs to just one group.

Problem: Can't configure SNMPv3 for chassis ION NIDs.
Meaning: The SNMPv3 features currently only apply to the IONMM and standalone S323x/S322x/S222x devices.
Recovery: 1) Contact Tech Support.

Message: *Its value must be a-f or A-F or 0-9 and the total length must be a dual from 18 to 128*
Meaning: The engine ID is specified by hexadecimal characters. Each two input characters correspond to one octet character. For engine ID "80 00 03 64 03 00 c0 f2 00 01 02", the first two characters '80' correspond to the first octet character '\128' with ASCII value of 128 (8*16 + 0 = 128). The second two characters "00" correspond to the second octet character '\0' with ASCII value of 0 (0*16 + 0 = 0).
Recovery: 1) This applies only for SNMP v3 Engine ID converting. Enter this.pattern = /^[A-F\d]{18,128}$/.

Message: *It must be a valid oid.*
Meaning: You entered an invalid OID.
Recovery: 1) Enter this pattern = /^[1-9]+(\.\d{1,5})*$/.

Message: *It must be a string which consists of letters and numbers.*
Meaning: You entered an invalid string.
Recovery: 1) Enter this pattern = /^[\w]{1,256}$/;
2) Enter this min = lengthMin;
3) Enter this max = lengthMax;

Message: *It can be set to any characters combination except the character tab and space.*
Meaning: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "tab" and "space" characters.
If you enter a "tab" and/or "space" character in these fields (via CLI or Web interface) the message "It can be set to any characters combination except the character tab and space." and "this.pattern is required: /^[\S]*{1,256}$/." display.
Recovery: 1) Re-enter the command or field without the "tab" or "space" characters.

Problem: Entries display in red in SNMP v3 fields (e.g., at **IONMM** > **SNMP** > **Users** sub-tab, the **User Name** / **Group Name** / **Password** entry displays in red)
Meaning: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "tab" and "space" characters.
If you enter a "tab" and/or "space" character in these fields (via the Web interface) the characters display in red and the message "Getting records failed (http server error)" displays in the lower-left corner of the page.
Recovery: 1) Re-enter the command or field without the "tab" or "space" characters.

Message:
The default group whose name is \"public\" or \"private\" and security-model is v1 or v2c cannot be removed!
While the group whose name is \"public\" or \"private\" and security-model is v3 can be removed!
Meaning: The default group cannot be removed (deleted) from the ION system configuration.
Recovery: 1) Make sure this is the command you want. 2) Delete another existing Group. 3) See the related section of the manual for specifics. 4) If the problem persists, contact Tech Support.

Message: *Invalid group parameter for user!*
No group name is specified!
Too many options folllow \"group name\"!
Meaning: You entered the CLI command for adding a local snmpv3 user, but the entry failed.
Recovery: 1) Verify the "**add snmp local user name**" syntax. 2) Check if the ION firmware is the latest and upgrade if possible. 3) If the problem persists, contact Tech Support.

Message:
Following \"authentication password\" should be either \"group\" option or no option!
Following \"noAuthNoPriv\" should be either \"group\" option or no option!
Following \"privacy password\" should be \"group\" option or no option!
Meaning: You entered an invalid group parameter while creating an SNMP v3 user
Recovery: 1) Verify the "add snmp local user" syntax. 2) Check if the ION firmware is the latest and upgrade if possible. 3) If the problem persists, contact Tech Support.

Message: *AGENT PM ERROR: CLI command prov show snmp user failed*
Meaning: The IONMM backup failed after no group SNMP local user added to the system.
Recovery: 1) Check if the ION firmware is the latest and upgrade if possible. 2) Try the IONMM backup procedure again. 3) If the problem persists, contact Tech Support.

Problem: SNMP Local or Remote Users are deleted when you modify the SNMPv3 Local or Remote Engine ID. If you enter a "show snmp group name" command without entering a specific group name, the session is ended and the ION login prompt displays.
Meaning: You configured the SNMPv3 Local or Remote Engine ID before you configure the Local or Remote Users for this engine. For example:

```
AgentIII C1|S1|L1D>show snmp group name
Name         Security Model     Security Level    Read View   Write View   Notify View
-------------------------------------------------------------------------------------
login: ION
Password:
```

Recovery: 1. Log in to the ION system again. 2. Configure the SNMPv3 Local or Remote Engine ID before you configure the Local or Remote Users for this engine. See "Configuring SNMP". Retry the operation.

Syslog Messages and Sys.log Output

This section documents Syslog messages and related Sys.log output.

Syslog Messages

The set of messages displayable while using the Syslog function are provided below with possible meanings and suggested recovery procedures.

agentx_mapset Error
agentx_ot_add Error

Meaning: possible internal error
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Fail for sending ionSyslogMgmtTable ,ignored...
Meaning: possible internal error.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Fail to get syslog server address type!
Fail to get syslog server address type!
Fail to get syslog server port!
Fail to get syslog level!
Fail to get syslog level!
Fail to get syslog server address!
Meaning: the **show syslog config** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Fail to set syslog server port!
Fail to set syslog mode!
Fail to set syslog level!
Fail to set syslog server address!
Fail to set syslog server address type!
Meaning: the **set syslog level / mode / svr** attempt failed.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid syslog server address!
Meaning: the **set syslog svr** attempt failed (e.g., **set syslog svr type**=ipv4 addr=192.168.01).
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Number of subid is not correct when ionSyslogMgmtTable_get, expect %d, get %d \n
Meaning: possible internal error
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Please input a digital number to specify syslog server port!
Meaning: the **set syslog svr port** attempt failed.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation with a valid, unused UDP port number.
3. If the problem persists, contact Technical Support.

Session reset, Reregister from begging\n
STATUS_INVALID, should be session reset, Reregister from beginning\n
Meaning: possible internal error.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Syslog is not supported on this card!
Meaning: You tried to configure a Syslog parameter, but this device does not support the Syslog feature.
Recovery:
1. Verify that this is the command / function you wanted.
2. Switch to a device that supports Syslog.
3. Retry the operation.
4. If the problem persists, contact Technical Support.
5.

System initializing or SNMP service busy, please wait..." : "Invalid password!
Meaning: possible internal error.
Recovery:
1. Wait for several seconds for the message to clear.
2. Verify the Syslog configuration. See “Configuring System Logging (Syslog)”.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

unknown column in ionSyslogMgmtTable_get\n
Meaning: possible internal error.
Recovery:
1. Verify the Syslog configuration. See “Configuring System Logging (Syslog)”.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Syslog Warning: A defined IDS is detected.
Meaning: The Upgrade file failed, the Web interface reports an error, the system can't login and keeps initializing. For example:

```
Line  1 Jan  1 19:33:01 (none) user.warn subagent[818]: A defined IDS is detected.
```

At the ACL tab, you selected rule 1 and edited policy to "Trap", Trap Rate to "4", selected Condition 1, and then edited the Condition 1 value to the local host's IP address. Then uploaded upgrade file by TFTP server tried to upgrade the system. The upgrade file failed, the Web interface reported an error, and the system can't login and keeps initializing. After enabling the ACL trap for the same source IP as the TFTP server and doing tftp operation to the TFTP server, a large amount of packets with the source TFTP server IP are received by the IONMM and each packet is looked at as an IDS packet which caused the subagent and snmpd to become overburdened.
Recovery: None; this issue appears as something like a manual IDS attack to the ION system, which may not be an issue for most users.

Sample Sys.log Output

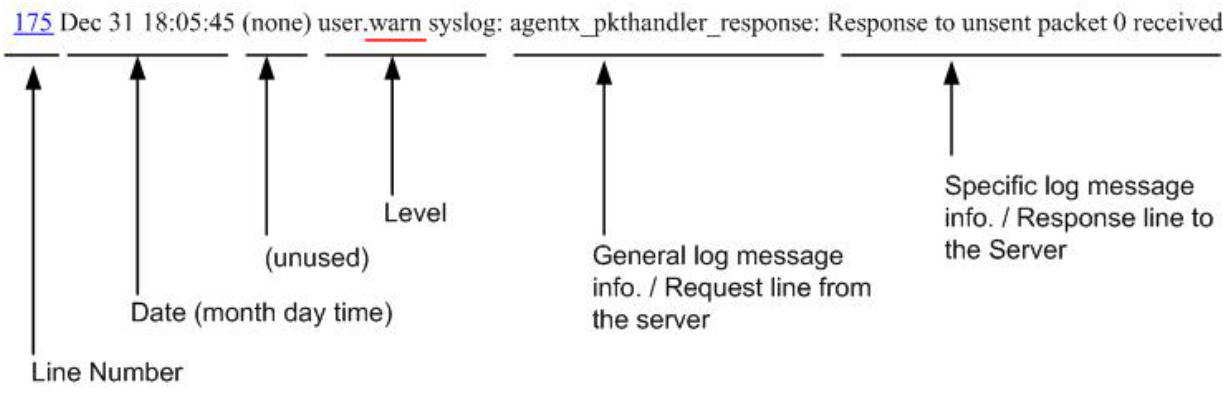
A typical Syslog output is shown below.

```
Line
   1 C0|S0|L1D>cat sys.log
   2 Dec 31 18:00:07 (none) local5.notice bpd_linux[716]: BPD Started.
   3 Dec 31 18:00:08 (none) local5.notice loam[715]: LOAM started
   4 Dec 31 18:00:12 (none) user.notice subAgent2[726]: subAgent Started.
   5 Dec 31 18:00:16 (none) daemon.notice ION-EM[742]: Entity Manager running in Mast
   6 er Mode
   7 Dec 31 18:00:17 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[0],
   8  relpos-[1]
   9 Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=1
  10 Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=2
  11 Dec 31 18:00:19 (none) user.notice subAgent2[726]: subAgent session connected.
  12 Dec 31 18:00:19 (none) user.notice subAgent2[726]: Standalone mode, Send the col
  13 dStart trap.
  14 Dec 31 18:00:21 (none) daemon.err snmpd[719]: ion-ns/logical: session from local
  15  subAgent2 end_point_name [/var/agentx/master]
  16 Dec 31 18:28:58 (none) local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a
  17 ppPduFrameLen == 0 when recvMsgFromAppSAP
  18 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  19 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  20 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  21 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  22 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  23 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  24 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  25 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  26 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  27 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  28 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  29 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  30 Dec 31 18:29:08 (none) daemon.warn ION-EM[742]: AgentX master agent failed to re
  31 spond to ping.  Attempting to re-register.
```

A typical syslog message is shown below.

```
175 Dec 31 18:05:45 (none) user.warn syslog: agentx_pkthandler_response: Response to un-
    sent packet 0 received
```

The Syslog format is shown below.



Syslog messages, their meanings, and suggested responses are provided below.

Message: local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a ppPduFrameLen == 0 when recvMsgFromAppSAP

Meaning: Level 3 Error (err) severity; received a frame with a frame length of 0.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Retry the operation. 3. If the problem persists, contact Technical Support.

Message: daemon.warn ION-EM[742]: AgentX master agent failed to respond to ping. Attempting to re-register.

Meaning: Level 4 Error (warn) severity; the IONMM did not respond to a ping.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Retry the operation. 3. If the problem persists, contact Technical Support.

Message: Dec 31 18:31:39 (none) user.crit subAgent2[822]: agentx_protocol_disconnect: Subagent disconnected from master.

Meaning: Level 2 - Critical condition.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

Message: 61Dec 31 18:31:39 (none) user.crit subAgent2[822]: agentx_protocol_disconnect: Subagent disconnected from master.

Meaning: Level 2 - Critical condition.

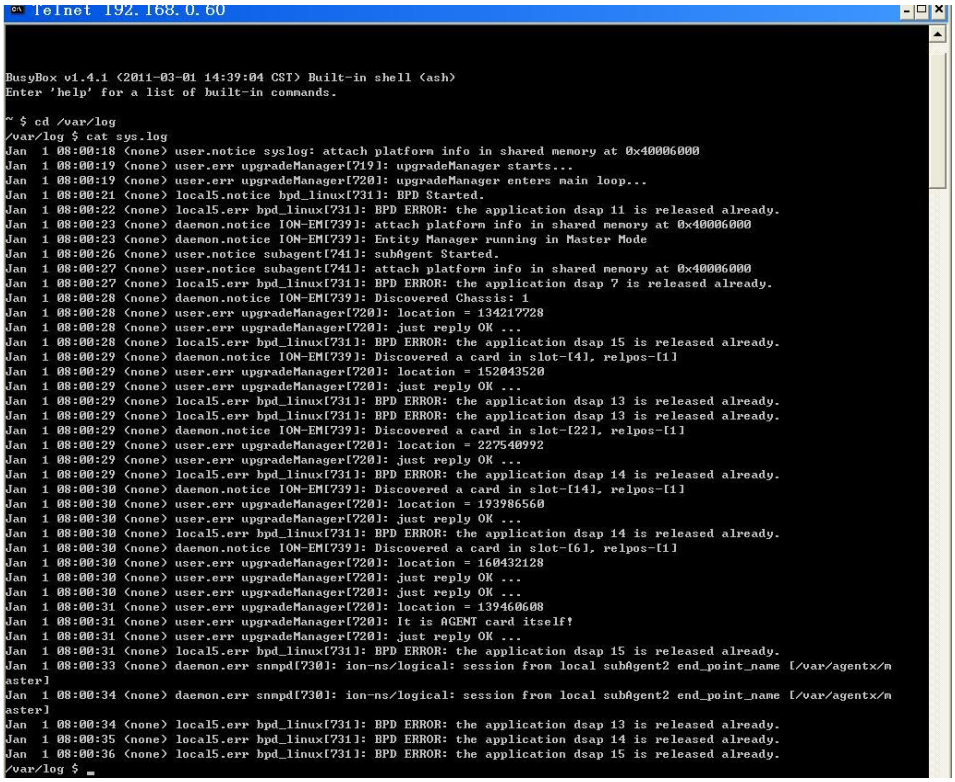
Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

Message: user.err upgradeManager

Meaning: you unplugged the SIC card, system will send a syslog which descript as "user.err upgradeManager", that not match the event.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

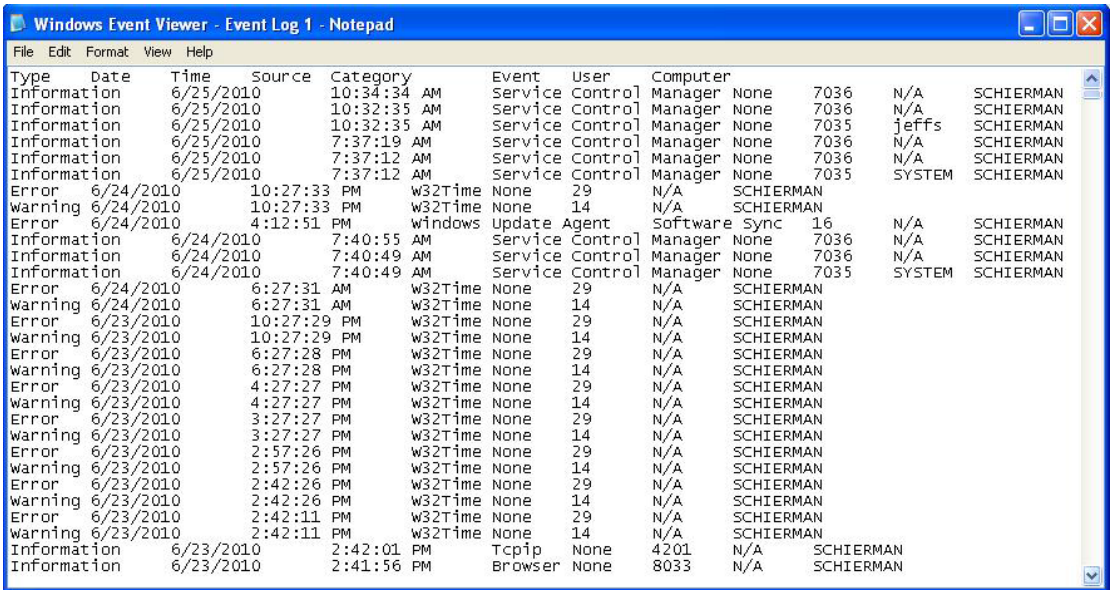
Sys.log sample - A typical Syslog output is shown below (Telnet screen)



Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:



Windows Event Viewer - Event Log 1 - Notepad

File Edit Format View Help

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

Message: Information 6/25/2010 7:37:12 AM Service Control Manager None 7035 SYSTEM
Meaning: Information message regarding SCM.

Recovery: No action required.

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

Meaning: Error level message regarding W32Time.

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

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

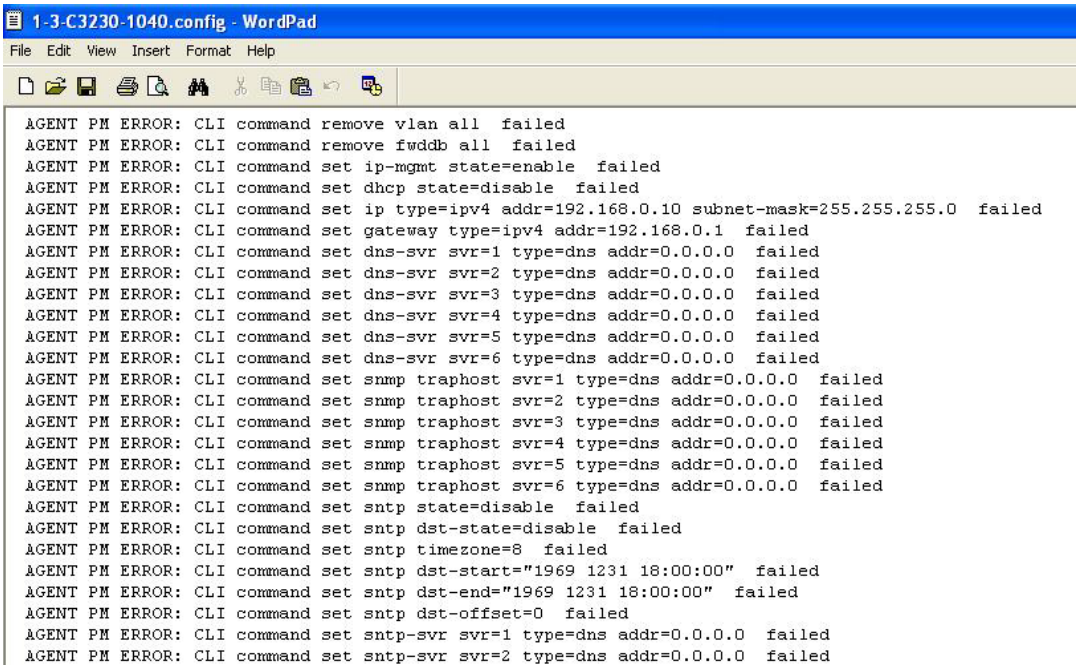
Meaning: Warning level message regarding W32Time.

Recovery: Check the other system logs for related messages. If the problem persists, contact Technical Support.

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.



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 *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Message: remove fwddb all failed

Response: 1. Check if this is a recurring problem. 2. Verify the Forwarding Database (FWDB) operation in the related section of this manual. Retry the FWDB operation. 3. See the related FWDB command in *the ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Message: set dhcp state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the DHCP operation in the related section of this manual. Retry the DHCP operation. 3. See the related DHCP command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Message: set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in the *ION System CLI Reference Manual, 33461*. 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 ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the DNS Server operation in the related section of this manual. Retry the operation. 3. See the related DNS server command in the *ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in the *ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

Message: set sntp state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

Message: set sntp dst-state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

Message: set sntp timezone=8 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

Message: set sntp dst-offset=0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

Message: set radius client state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the RADIUS operation in the related section of this manual. Retry the RADIUS operation. 3. See the related RADIUS command in *the ION System CLI Reference Manual, 33461*. 4. 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 the RADIUS server setup, configuration and documentation. 2. Verify the RADIUS operation in the related section of this manual. Retry the RADIUS operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support.

Message: add vlan-db vid=100 priority=0 pri-override=disable 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 *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Message: add vlan-db vid=200 priority=0 pri-override=disable 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 *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Message: set acl state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Message: set acl table=filter chain=input policy=accept failed

Response: 1. Check if this is a recurring problem. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

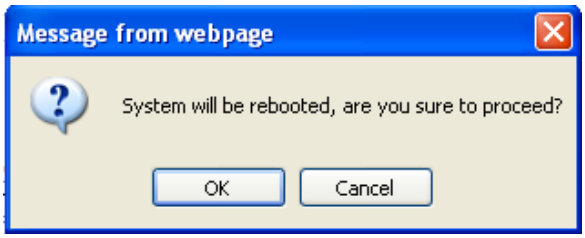
Message: set dot1dbridge ip-priority-index=0 remap-priority=0 failed

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 dot1dbridge command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support.

Webpage Messages

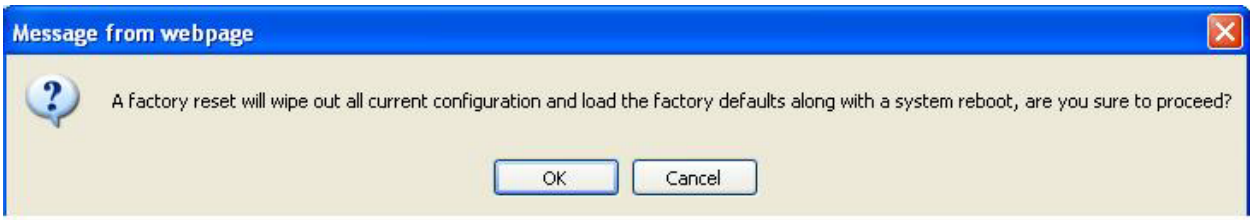
Certain menu operations will display a webpage verification message to verify that you want to proceed. These messages also provide information on the effect that the operation will have if you continue. These messages display for operations such as **Reset to Factory Config**, **Reboot the System,**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

See Menu System Description for more information.



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

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



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

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

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

Meaning: At the device's **MAIN** > **SNMP Configuration** tab you clicked Save to create a new SNMP trap server location.

Response: Click **OK** only if you wish to reboot the system right now. Otherwise click **Cancel**. See SNMP Configuration.

Message*: The firmware upgrade failed*!

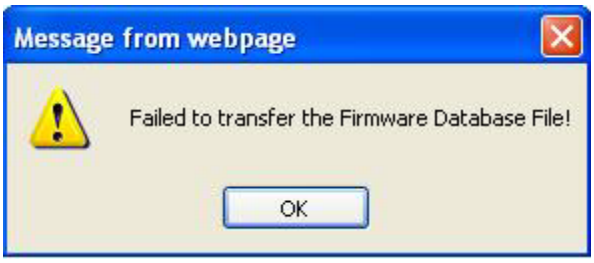
The **MAIN** tab **> TFTP Settings** section **Status** area displays "*TFTP Failure*".

Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the Upgrade the IONMM Firmware section.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Lantronix web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.1.0.5**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.1.0.5 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Make sure that the Management VLAN function is disabled.
8. Reset the 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*!

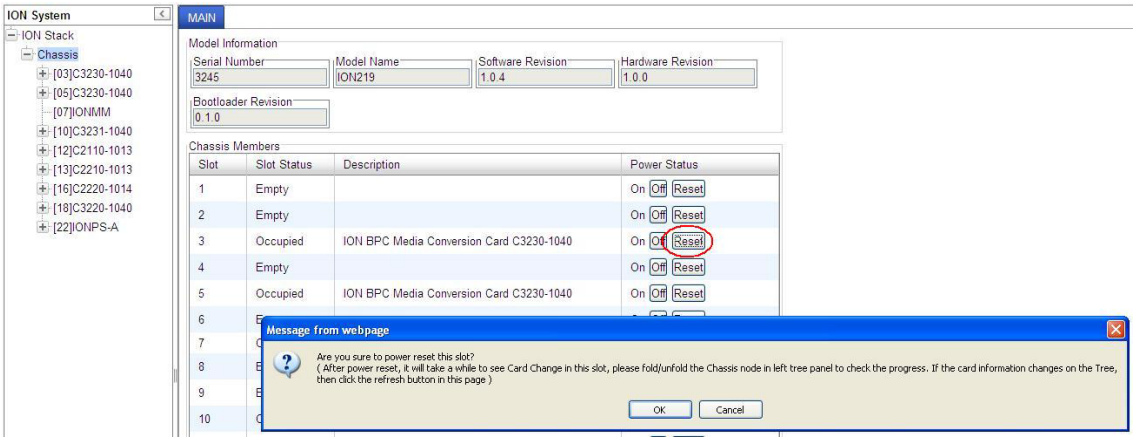


Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the Upgrade the IONMM Firmware section.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Lantronix web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.1.0.5**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.1.0.5 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Reset the IONMM card. The **TFTP Settings** section **Status** area should display "*Success*" when done.
8. If the problem persists, contact Technical Support.

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

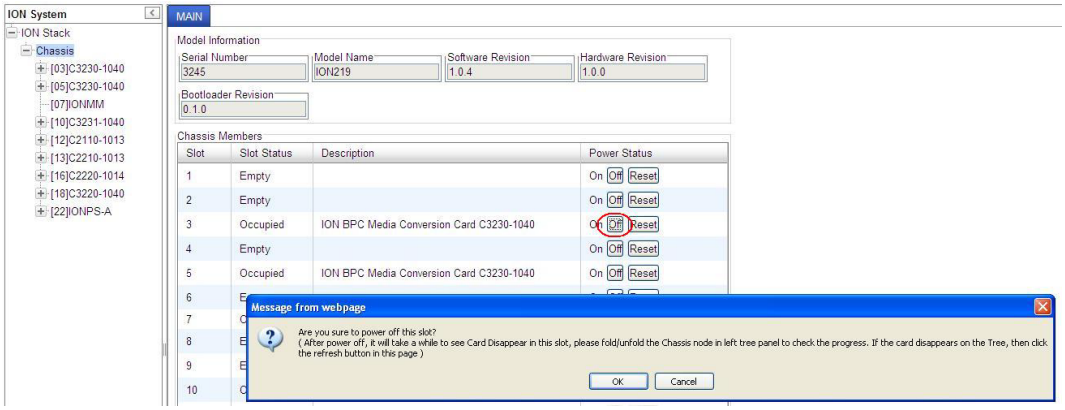


Meaning: A caution message generated at the **Chassis** > **MAIN** tab. You clicked the **Reset** button for a particular slot.

Recovery:

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

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



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

Recovery:

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

Message: *TFTP file transferring failed!*

Meaning: Either the TFTP Server is not running, or the filename entered was incorrect or not found. See the "Backup/Restore Operations" section.

Recovery: Start the TFTP Server and verify the name and location of the file to be transferred.
If the file does not exist (e.g., at *C:\TFTP-Root*), then download the file from https://www.lantronix.com/products/ionmm-series-2/#product-resources.

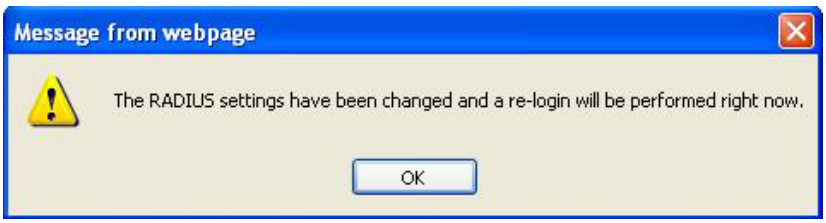
Message: *HTTPS settings have been changed and a re-login will be performed right now.*

Meaning: You performed a Copy Certificate function for the IONMM in the HTTPS tab.

Recovery:

1. Click **OK** to clear the message.
2. See "Configuring HTTPS".
3. If a message displays regarding a problem with the website's security certificate, select "Continue to this website".

Message*: The RADIUS settings have been changed and a re-login will be performed right now.*

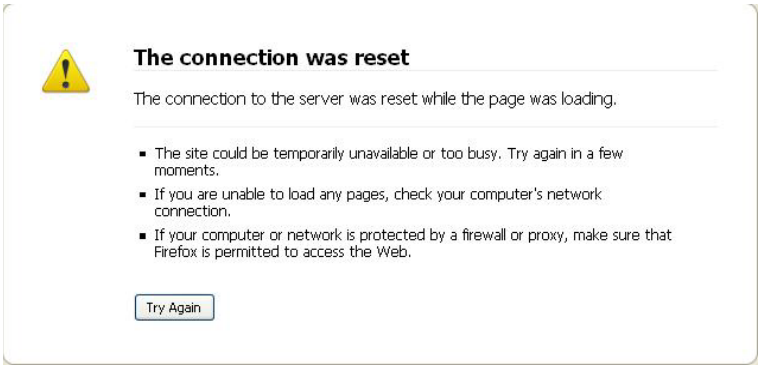


Meaning: You performed a Copy Certificate function for the IONMM in the RADIUS tab.

Recovery:

1. Click **OK** to clear the message.
2. Sign in to ION System Web Interface (RADIUS). See "Configuring RADIUS".
3. If a message displays regarding a problem with the website's security certificate, select "Continue to this website".

Message: *The Connection was Reset*



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

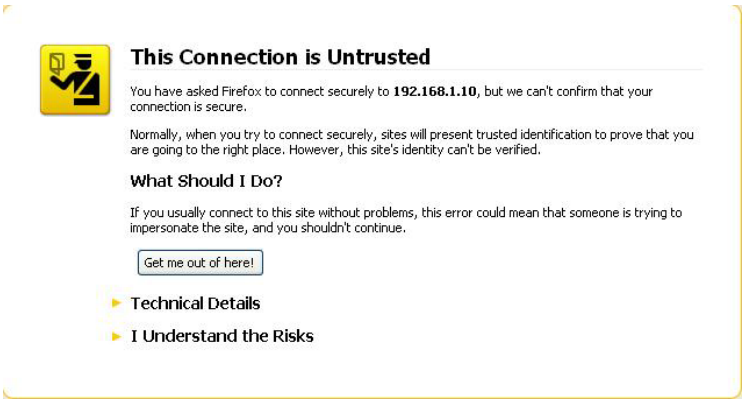
Recovery:

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.

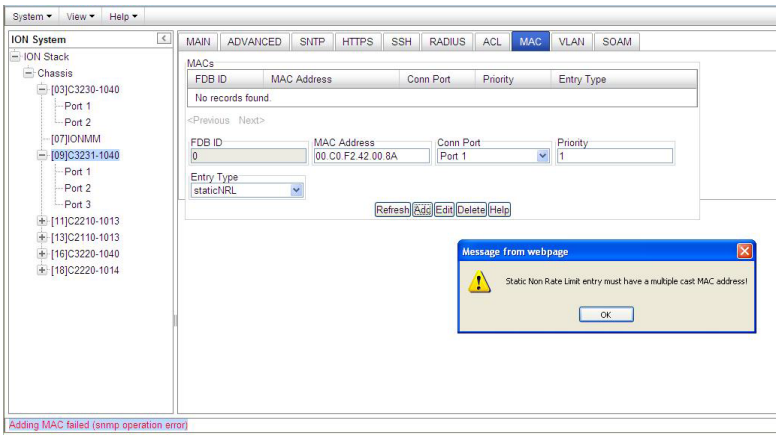
Message: *This Connection is Untrusted*



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!*

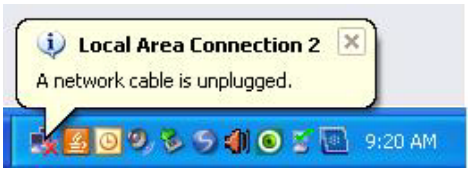


Meaning: When setting up MAC filtering, you entered a unicast MAC address and selected a Static NRL (Non Rate Limit) Entry Type.

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*

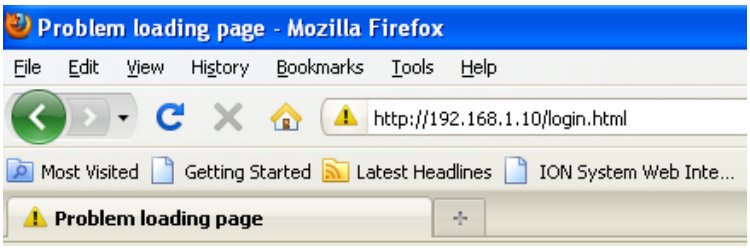


Meaning: You unplugged the USB cable at the NID or IONMM, or the NID or IONMM was unplugged from the ION chassis, or you pressed the **RESET** button on the IONMM.

Recovery:

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

Message: *Problem loading page – Mozilla Firefox*

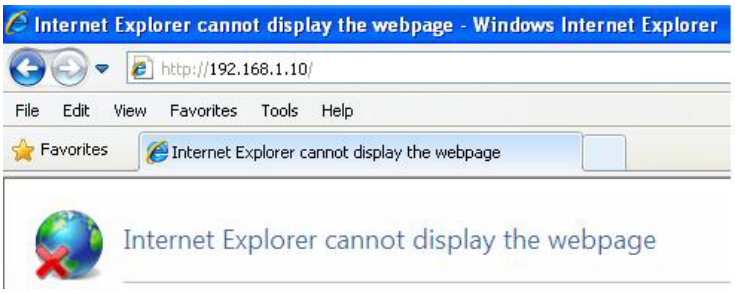


Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See "Web Browser Support".
2. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI".
3. Verify NID access. See "Accessing the NIDs".
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*



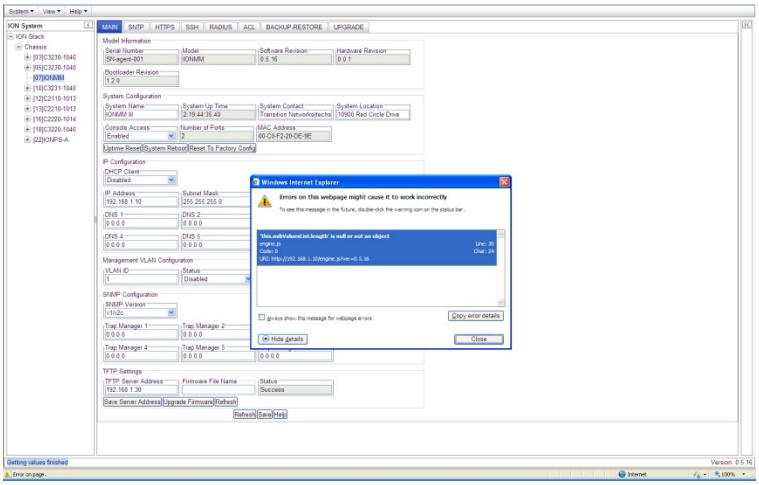
Meaning: You tried to log in to the ION system from IE, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See "Web Browser Support".
2. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI".
3. Verify NID access. See "Accessing the NIDs".
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: Error on page.
Message: Errors on this webpage might cause it to work incorrectly.
Message: 'this.mibValuesList.length' is null or not an object

Meaning: In Windows IE, the message displays after some amount of inactivity.



Recovery:

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

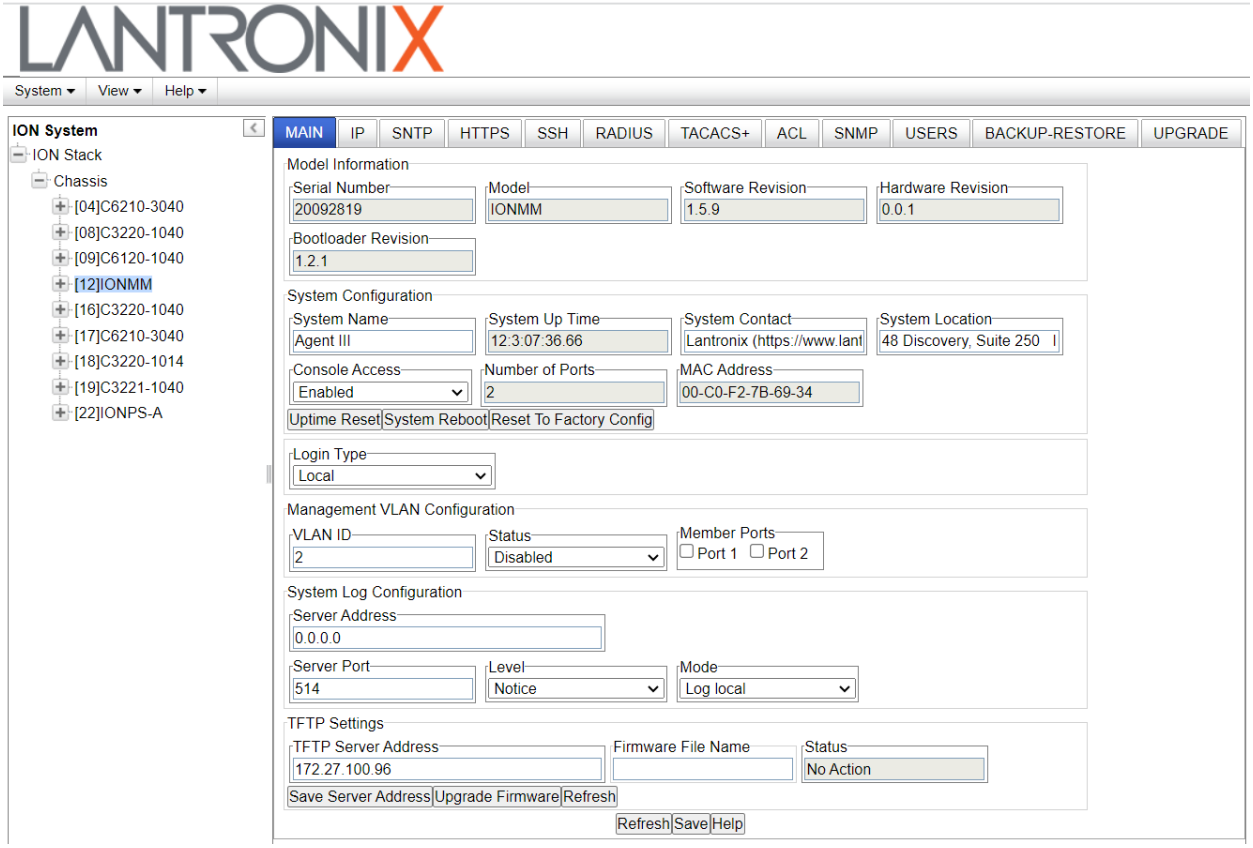
```
User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Tri-
dent/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152;
.NET CLR 3.5.30729)
Timestamp: Mon, 6 Dec 2010 14:20:17 UTC

Message: 'this.mibValuesList.length' is null or not an object
Line: 30
Char: 24
Code: 0
URI: http://192.168.0.10/engine.js?ver=0.5.16
```

5. Click the **Close** button to close the Windows IE error dialog.
6. Click the ION system **Refresh** button.
7. Retry the operation.
8. If the problem persists, contact Technical Support.

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 to help the Technical Support Specialist.

1. Select the ION system **MAIN** tab. (From the CLI, use the commands needed to gather the information requested below, such as **show card info**, **show slot info**, **show system info**, **show ether config**, **show ip-mgmt config**, **show snmp config**, or others as request by the Support Specialist.



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

   Serial Number: _____ Model: _____

   Software Revision: _____ Hardware Revision: _____

   Bootloader Revision: _____

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

   System Up Time: _____ Console Access: _____

   Number of Ports: _____ MAC Address: _____

   IP Address Mode: _____ _ Login Type: _____

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., changed switch mode, rebooted, etc.): _____

_____

_____

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

_____

_____

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

_____

_____

_____

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

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

_____

_____

Any previous Return Material Authorization (RMA) numbers: _____

6. Compliance and Safety Information

Standards CISPR22/EN55022 Class A, CE Mark
IEEE Standards and RFC compliance: IEEE 802.3™-2000
Regulatory Compliance for Immunity: EN55024

FCC Regulations: This equipment has been tested and found to comply with the limits for class A devices, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and radiates radio frequency energy; therefore, if not installed and used in accordance with the instructions in this document, the device could cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference; all customers will be required to correct the interference problem at their expense.

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

UL Recognized: Tested and recognized by the Underwriters Laboratories, Inc.

Canadian Regulations: This digital apparatus does not exceed the Class A limits for radio noise from digital apparatus set out on the radio interference regulations of the Canadian Department of Communications.
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la Class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

European Regulations

WARNING: This is a Class A product. In a domestic environment, this product could cause radio interference in which case the user may be required to take adequate measures.
Achtung ! Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fäll ist der Benutzer für Gegenmaßnahmen verantwortlich.
Attention ! Ceci est un produit de Classe A. Dans un environment domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilsateur de prende les measures spécifiques appropriées.

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

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

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

NDAA, RoHS, REACH and WEEE Compliance

See the compliance webpage at https://www.lantronix.com/legal/rohs/.

Trade Agreement Act (TAA) Compliant Products

See the TAA webpage at https://www.lantronix.com/legal/rohs/taa-compliant-products/

Accessibility Statement

In our effort to help provide a fully accessible and optimized experience for our website visitors, lantronix.com has taken careful measures to help ensure an enhanced user experience, whether the website visitor is using assistive technologies such as a screen reader, magnifier or other assistive technology to access the website.

For more information see https://www.lantronix.com/accessibility-statement/.

EU Declaration of Conformity

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Model Number: IONMM, IONMM-232

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)

- **IEC /EN 60950-1:2006+A2:2013**

EMC Directive (2014/30/EU)

- **EN 55032:2012**
- **EN 55024:2010**

EU Directive 2011/65/EU for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and XX*
***XX - different products may have different exemptions, confirm with RoHS team.**

- **EN IEC 63000:2018**

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: Eric Bass Date: 15 October 2024

Name: Eric Bass Title: VP of Engineering

UK Declaration of Conformity

LANTRONIX®

UK CA

UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Model Number: IONMM, IONMM-232

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Electrical Equipment Regulations

- **IEC /EN 60950-1:2006+A2:2013**

Electromagnetic Compatibility Regulations 2016

- **EN 55032:2012**
- **EN 55024:2010**

UK SI 2012 No. 3032 for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and 6(c).
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU[7(c)-I] and 2018/741/EU[6(c)]
BS EN IEC 63000 : 2018

Statement of Conformity: The product specified above meets the test requirements of the relevant legislation of United Kingdom, including the application of sound engineering practice.

Signature: Eric Bass Date: 15 October 2024

Name: Eric Bass Title: VP of Engineering

Electrical Safety Warnings

Electrical Safety

IMPORTANT: This equipment must be installed in accordance with safety precautions.

Elektrische Sicherheit

WICHTIG: Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

Elektrisk sikkerhed

VIGTIGT: Dette udstyr skal installeres i overensstemmelse med sikkerhedsadvarslerne.

Elektrische veiligheid

BELANGRIJK: Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

Sécurité électrique

IMPORTANT: Cet équipement doit être utilisé conformément aux instructions de sécurité.

Sähköturvallisuus

TÄRKEÄÄ: Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

IMPORTANTE: questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal installeres i samsvar med sikkerhetsregler.

Segurança eléctrica

IMPORTANTE: Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

Seguridad eléctrica

IMPORTANTE: La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

Elsäkerhet

OBS! Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.

Appendix A. Factory Default Settings

The factory default settings for the IONMM are shown in the tables below. The default settings shown are as seen in the tabs/fields of the Web interface.

Table 13: Device-Level Factory Defaults

Item/Field	Default Setting
Web Access Password	private
Telnet/USB Login	ION
Telnet/USB Password	private
MAIN tab	
Model Information	Serial Number: device dependent (e.g., 1234567) Model: device dependent (e.g., IONMM) Software Revision: FW vs. dependent (e.g., 1.3.19) Hardware Revision: HW vs. dependent (e.g., 0.0.1) Bootloader Revision: BL vs. dependent (e.g., 1.2.0)
System Configuration	System Name: IONMM III System Contact: Lantronix (techsupport@lantronix.com) System Location: 48 Discovery Number of Ports: 2 MAC Address: 00-C0-F2-20-DE-9E
Console Access	Enabled
MAC Address	00-00-00-00-00-00
Login Type	Local
Management VLAN Configuration	VLAN ID: 1 Status: Disabled Member Ports: Port 1 and Port 2 unchecked
System Log Configuration	Server Address: 192.168.0.2 Server Port: 514 Level: Notice Mode: Log local
TFTP Server Address	0.0.0.0
Firmware File Name	blank

Item/Field	Default Setting
Status	blank
IP tab	
IPv4	IP Address Mode: Static IP Address: 192.168.0.10 Subnet Mask: 192.168.1. 0 Default Gateway: 192.168.0.1
IPv6	Status: Enabled IP Address Mode: Static IP Address: 2001:1234::1 Prefix Length: 64 Gateway Mode: Route Discovery
DNS Configuration	DNS 1-6: 0.0.0.0
SNTP tab	
SNTP Client	Disabled
Device Time	1970 0105 12:57:25
UTC Timezone	(GMT-06:00)Central Time (US & Canada)
Daylight Saving Time	Disabled
Daylight Saving Period Start	1969 1231 18:00:00
Daylight Saving Period End	1969 1231 18:00:00
Daylight Saving Offset	0
SNTP Server x	0.0.0.0
HTTPS tab	
HTTPS Status	Disabled
HTTPS Port	443
Certificate Type	Self Certificated
TFTP Server Address	0.0.0.0

Item/Field	Default Setting
Certificate File Name	blank
Private File Name	blank
Private Password	blank
SSH tab	
SSH Server Status	Disabled
Version	2.0
SSH Auth Timeout	60
SSH Auth Retries	3
Host Key Type	No Gen
Save Host-Key to Flash	(N/A)
User Name	blank
Public-Key Type	No Copy
TFTP Server Address	0.0.0.0
Source File Name	blank
RADIUS tab	
RADIUS Client	Disabled
Server Address x	0.0.0.0
Server Secret x	blank
Retries x	3
Timeout x	30
TACACS+ tab	
TACACS+ Client	Enabled
TACACS Server 1-6	Server Address: 0.0.0.0 Server Secret: blank

Item/Field	Default Setting
	Retries (1-5): 3 Timeout (1-60s): 30
ACL tab	
ACL Status	Disabled
Chain Name	INPUT
Chain Policy	Accept
Rules table	No records found.
Priority	blank
Policy	Accept
Trap Rate	0
Conditions for Rule table	No records found.
Type	Source MAC Address
Source or Destination	Source
Operation	Equal
Value	blank
SNMP tab	
General sub-tab	**Community String:** blank Access Mode: Read Only SNMP V3 Engine ID: 800003640300C0F2209EDE
Users sub-tab	User Name: blank Group Name: blank Security Model: V3 Security Level: NoAuthNoPriv Authentication Protocol: grayed out Password: grayed out Privacy Protocol: grayed out Password: grayed out
Groups sub-tab	Group Name: blank Security Model: V1

Item/Field	Default Setting
	Security Level: NoAuthNoPriv Read View: blank Write View: blank Notify View: blank
Views sub-tab	View Name: blank OID Sub Tree: blank Type: Included
Trap Hosts sub-tab	Trap Version: V1 IP: blank Port: 162 Community/Security Name: blank Security Level: NoAuthNoPriv Trap/Inform: Trap Timeout (centisecond): grayed out Retry Times: grayed out
Remote Users sub-tab	Remote IP: blank Remote Port: blank Remote Engine ID: blank User Name: blank Security Model: V3 Security Level: NoAuthNoPriv Authentication Protocol: grayed out Password: grayed out Privacy Protocol: grayed out Password: grayed out
USERS tab	
User table	User Name: ION Password: ******** Level: admin
User entry field	**User Name: blank** **Password: blank** **Confirm Password: blank** **Level: admin**
SFTP Tab	
SFTP state	**Disabled**

Item/Field	Default Setting
Server port	**22**
SFTP password	**Not set**

Note: The IONMM **BACKUP-RESTORE** and **UPGRADE** tabs have no default settings.

Table 14: Port-Level Factory Defaults

Item/Field	Default Setting
Port Configuration (Port 1)	Link Status: Up Speed: 100Mbps Duplex: Full Duplex Port Admin Mode: 10/100BaseT Port Mode: 10/100BaseT AutoCross Mode: Auto Connector Type: RJ-45 Auto Negotiation: Enabled Capabilities Advertised: 10M - Half Duplex, 10M - Full Duplex, 100M - Half Duplex,100M - Full Duplex all checked Pause: Unchecked
Port Configuration (Port 2)	Link Status: Down Speed: Negotiating Duplex: Negotiating Port Mode: 10/100BaseT AutoCross Mode: Auto Far End Fault Mode: Enabled Connector Type: RJ-45 With Auto Negotiation Enabled: Capabilities Advertised: 10M - Half Duplex, 10M - Full Duplex, 100M - Half Duplex,100M - Full Duplex all checked Pause: Unchecked With Auto Negotiation Disabled: Force Speed:10Mbps Force Duplex: Half Duplex

Appendix B. Configuration Quick Reference – CLI

IPv4 Configuration

1. Define IP address and subnet mask.

   set ip type={ipv4 } **addr=**<ipaddr> **subnet–mask =**<subnet>

2. Define default gateway.

   set gateway type={ipv4} **addr=<**gway>

3. Set the IP Address Mode.

   set ip address mode={bootp|dhcp|static}

3. Define DNS servers.

   set dns–server svr=<index> **type=<**format> **addr=**<ipaddr>

IPv6 Configuration

1. Set the IPv6 Mode.

   set ipv6 address mode=<static|dhcpv6|stateless>

2. If 'Stateless Auto configuration' is selected, then enable Route Discovery (step 4).

3. Enable IPv6 Management state.

   set ipv6-mgmt state=enable

4. Configure the IPv6 gateway method.

   set ipv6 gateway mode=<static|routerdisc>

ACL Configuration (IPv4)

1. Enable ACL.

   set acl state=enable

2. Define default chain policy.

   set acl table=filter **chain**=input **policy=**<ptype>

3. Define one or more conditions.

   add acl condition type=<xx> **srcdst**={src | dst} **oper**={equal | notequal} **value=**<yy>

4. Define one or more rules.

   add acl rule position={head | tail} **table**=filter **chain**=input **policy**={accept | drop | trap} **traprate=**<rate> **condition=**<list>

ACL Configuration (IPv6)

1. Enable ACL.

   set ip6tables acl state

2. Define the default chain policy.

   set ip6tables acl table=filter chain=input policy=accept

3. Define condition(s) to be associated with a rule.

   set ip6tables acl condition=1 rule_index=1

4. Define rule(s) to be associated with the chain.

   add ip6tables acl rule position=head table=filter chain=input policy=1 trap=444

5. Verify that ACL has been enabled.

   show ip6tables acl state

6. Verify the ACL rules have been defined and associated.

   show ip6tables acl rule

Backup / Restore Configuration

1. Check the current provisioning status.

   show provision modules

2. Specify a backup index item number and a config file name.

   set backup module-index=<1-256> config-file=STR_CFG_FILE

3. Specify a restore index item number and a config file name.
   set restore module-index=<1-256> config-file=STR_CFG_FILE

4. Specify 1-10 provision modules to be backed up.

   backup prov module-list=xx

5. Specify 1-10 provision modules to be restored.

   restore prov module-list =xx

6. Verify the configuration.

   show prov modules

Note: at IONMM FW v 1.4.2 the set backup module-index, set restore module-index, and refresh provision configure filename commands are no longer supported.

HTTPS Configuration

1. Enable HTTPS.

   set https state=enable

2. Define the certificate type.

   set https certificate–type={authorized | self-certificate}

3. Define the certificate file.

   set https certificate–file=<name>

4. Define the private key file.

   set https private–key file=<name>

5. Define the password.

   set https private–key password

Management VLAN Configuration

1. Enable management VLAN.

   set mgmt vlan state=enable

2. Define the VLAN ID for the IONMM.

   set mgmt vlan vid=<xx>

3. Define which ports will be used for management VLAN traffic.

   set mgmt vlan port=<xx>

RADIUS Configuration

1. Define the RADIUS server.

   set radius svr=<index> **type**={ipv4 |ipv6|dns} **addr=**<ipaddr> [**retry=**<limit>] [**timeout=**<secs>]

2. Define the RADIUS server secret.

   set radius svr=<index> **secret=<**secret>

3. Enable RADIUS.

   set radius client state=enable

Create a User with RADIUS and SSH Enabled

1. Launch the SSH client.
2. Enter 'ION' – 'private' to log in to SSH (the first time).
3. Enter the RADIUS user and password to log in to RADIUS.
4. Add the 'TEST' (user name) – 'TEST111' (password) user.
5. Close the SSH client.
6. Launch the SSH client again
7. Enter 'TEST' – 'TEST111' to log in to SSH.
8. Enter the RADIUS user and password to log in to RADIUS.

Create a User with SSH Enabled (RADIUS Disabled)

1. Launch the SSH client.
2. Enter 'ION' – 'private' to login to SSH (the first time).
3. Add 'TEST' (user name) – 'TEST111' (password) user (see Note below).
4. Close the SSH client.
5. Launch the SSH client again.
6. Enter 'TEST' – 'TEST111' to login via SSH.

SFTP Configuration

1. Enable SFTP admin state.

   set sftp state enable
2. Set SFTP server address and custom port.

   prov set sftp server type=(ipv4|ipv6|dns) addr=ADDR

   set sftp port=<1-65535>
3. Set SFTP user name and password.

   set sftp username=USERNAME

   set sftp password
4. Specify the remote server directory path.

   set sftp serverpath=SERVERPATH
5. Download file from SFTP server.

   sftp get remotefile=RFILE
6. Download and install IONMM firmware.

   sftp upgrade remotefile=RFILE

SNMP Configuration

1. Access the IONMM through either a USB connection or an SSH or Telnet session.
2. Define the General configuration. Type:

   add snmp community name=xxxxxxx **access_mode**={read_only|read_write}
   add snmp remote engine addrtype=ipv4 **addr**=xx **port**=xx **engine_id**=xx
   set snmp local engine=xx
3. Define one or more Local Users. Type:

   add snmp local user name=STR_USR_NAME **group**=STR_GRP_NAME **security-level**=(no-AuthNoPriv|authNoPriv|authPriv) [auth-protocol=(md5|sha) password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]

   set snmp local user name=xxxx **group**=xxxx
4. Define one or more Groups. Type:
   set snmp group name=STR_SNMP_GRP
   set snmp local user group=xxx
5. Define one or more Views. Type **set snmp view name**= STR_SNMP_VIEW.
6. Define one or more Trap Hosts.
   Type **add snmp traphost version**=v3 **type**=ipv4 **addr**=STR_SVR_ADDR.
7. Define one or more Remote Engines. Type
   add snmp remote engine addrtype=ipv4 **addr**=192.168.1.30 **port**=xx **engine_ id**=xxxxx.
8. Define one or more Remote Users by address type. Type:
   add snmp remote user name=STR_USR_NAME **addrtype**=ipv4 **addr**=192.168.1.30 **port**=55 **security-level**={noAuthNoPriv|authNoPriv|authPriv}**auth-protocol**={md5|sha} **password**=xxxxxxx priv-protocol={des|aes} password=STR_PRIV_PASS
9. Define one or more Remote Users by the remote engine. Type:
   add snmp remote user name=STR_USR_NAME **engine**=STR_ENGINES **security-level**=authPriv auth-protocol=md5 **password**=STR_AUTH_PASS **priv-protocol**=des **password**=STR_PRIV_PASS
10. Verify the configuration has been set. Type **show snmp config**.

SNTP Configuration

1. Enable SNTP.

   set sntp state=enable

2. Set the current time.

   s**et curr–time=<“**time**”>**

3. Define your timezone.

   set sntp timezone=<zone>

4. Enable daylight savings time (DST).

   set sntp dst–state=enable

5. Define DST start time.

   set sntp dst–start=<“time**”>**

6. Define DST end time.

   set sntp dst–end=<“time**”>**

7. Define DST offset.

   set sntp dst–offset=<value>

8. Define SNTP server.

   set sntp–svr svr=<index> **type**={ipv4 | dns} **addr=<**ipaddr>

SSH Configuration

1. Enable SSH.

   set ssh server state=enable

2. Define the timeout value.

   set ssh client timeout=<seconds>

3. Define the retry limit.

   set ssh auth–retry=<limit>

4. Generate the host key.

   generate ssh host–key={rsa | dsa | both}

5. Define the public key user.

   set ssh public–key user=<name> **type**={rsa | dsa} **file=**<file>

Syslog Configuration

1. Set the level of Syslog operation.

   set syslog level=<alert/crit/debug/emerg/err/info/notice/warning>

2. Set the Syslog operating mode.

   set syslog mode=<local/localAndRemote/off/remote>

3. Set the Syslog server type and address.

   set syslog svr type=<ipv4|dns> **add**r=<ipaddr>

4. Define the Syslog server port.

   set syslog svr port=<1-65535>

System (Login) User Configuration

1. Create a new system user.

   add sysuser name=NAMESTR **level**=<admin|read-write|read-only> **pass**=PASSSTR confirm**pass**=PASSSTR

2. Edit an existing user's access level.

   set sysuser name=NAMESTR **level**=<admin|read-write|read-only)>

3. Set a new password for an existing ION system user.

   set sysuser name=NAMESTR **pass**=PASSSTR **confirmpass**=PASSSTR

4. Remove an existing system user.

   remove sysuser name=NAMESTR

TACACS+ Configuration

1. Enable the TACACS+ client.

   set tacplus client state=enable

2. Configure the TACACS + server retry attempts.

   set tacplus svr 1 retry=<1-5>

3. Configure the TACACS + server (password).

   set tacplus svr 1secret=SECRET

4. Configure the TACACS + server timeout period.

   set tacplus svr 1 timeout=<1-60>

5. Configure the TACACS + server type.

   set tacplus svr 1 type=<ipv4 / ipv6 / dns>

Transfer Files via Serial Protocol (X/Y/Zmodem)

1. Send a request to servers / local file system to download content for a subsequent put command.

   serial get protocol={xmodem|xmodem-1k|ymodem|zmodem}

2. Send a request to servers / local file system to upload content.

   serial put protocol=zmodem **file**=xxxx

3. Perform a firmware upgrade over the selected serial line.

   serial upgrade protocol=<xmodem|xmodem-1k|ymodem|zmodem **file**=xxxx

Appendix C. ION System File Content and Location

This appendix provides information on the status of standard ION system files following these operations:

- Reset to Factory Defaults (Table 15)
- Back Up and Restore (Table 16)
- System Reboot (Table 17)
- Firmware Upgrade (Table 18)

File Status after Reset to Factory Defaults

The table below shows the status of system files after a Reset to Factory Defaults.

Table 15. File Status after a Reset to Factory Defaults

File Type	Filename	File Description	Stored Directory	Status after Restore to Factory Default
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Lost
Net-SNMP configuration file	snmpd.conf	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
SOAM files	_____	SOAM Configuration file	_____	Restored to factory configuration
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	Restored to factory configuration (lost)

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 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).
A Back Up operation backs up all 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 **MAIN** tab description. Currently, the Backup content includes configuration files, HTTPS certification file, SSH key file, the Syslog file, and certain other files, as outlined in the table below.

Table 16. Back Up and Restore File Content and Location

File Type	Filename	File Description	Stored Directory	Backed up? (Y/N)	Changed after Restore? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes - these files are created during Backup operation	No
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	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	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No	Always changes
SOAM files	_____	SOAM Configuration file	_____	Restored to factory configuration	SOAM files
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:

- 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.
- 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.

Reboot File Content and Location

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

Table 17: File Content and Location after a System Reboot

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

Firmware Upgrade File Content and Location

The table below shows the content and location of files resulting from a firmware upgrade.

Table 18: 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	drop-bear_rsa_host_key drop-bear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/agent3/conf/root/.ssh	No (1)
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	Yes
SOAM files	_____	SOAM Configuration file	_____	Restored to factory configuration
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

(1) Exception: after Upgrade from v1.0.3 to v0.5.12, the User Public-Key is missing. 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 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.

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