

ION Management Modules (IONMM and IONMM-232)

User Guide

Part Number 33457
Revision K September 2022

Intellectual Property

© 2022 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

Tel: +1 (800) 526-8766, Tel: +1 (949) 453-3990, or <https://www.lantronix.com/technical-support/>

Sales Offices

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

Disclaimer

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

Revision History

Rev	Date	Description
J	10/31/18	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.
K	9/14/22	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.

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

Caution: Do not install the 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 [Appendix A](#) for [Electrical Safety Warnings](#) translated into multiple languages.

Contents

1	Introduction.....	9
	Document Overview	9
	Product Overview	10
	Model Descriptions	11
	Features.....	11
	Backup / Restore / Upgrade	11
	Management Access Methods.....	12
	IP Address Modes (IPv4 / IPv6, DHCP, Static, BootP).....	12
	Ethernet and USB Interfaces.....	12
	Single Slot Design	12
	Security Features	13
	System Logging (Syslog)	13
	SNMP Support.....	14
	Multiple Community Strings.....	14
	Physical Specifications	15
	Documentation Conventions.....	16
	Related Documents and Online Help	17
2	Installation.....	18
	General	18
	Installing the IONMM	18
	Connections and LEDs	19
	Accessing the IONMM	21
	Using a Local Serial Interface (USB).....	21
	Operating Systems Supported	21
	Installing the USB Driver - Windows XP.....	22
	Installing the USB Driver - Windows 7	23
	Installing the USB Driver - Windows 8.1	24
	Configuring Terminal Emulator.....	25
	Change COM Port for USB Serial Adapter (Windows 7, 8.1, and 10).....	25
	Starting a USB Session	26
	Terminating a USB Connection	26
	Access via an Ethernet Network.....	27
	Starting a Telnet Session	27
	Terminating a Telnet Session.....	27
	Web Browser Support	28
	Starting the Web Interface.....	28
	Terminating the Web Interface	30
	Setting Up the IP Configuration	31
	IPv4 Config Setup.....	31
	IPv6 Config Setup.....	32
	Menu System Description.....	34
	Reboot and Reset Functions	36
	System Reboot.....	36
	Reset to Factory Config.....	37
3	Configuration.....	38
	General	38
	Setting the IPv4 Configuration	38
	Configuring IPv4 Address Mode (Bootp, DHCP, or Static IP).....	39
	IPv4 Addressing Config – CLI Method	39
	IPv4 Addressing Config – Web Method	40
	Assigning an IPv4 DHCP Address	41
	IPv4 DHCP Config – CLI Method	41
	IPv4 Address Mode (DHCP / Static / BootP) Config – Web Method	43

BootP Addressing Configuration	43
Defining Domain Name System (DNS) Servers	44
DNS Lookups over IPv6 Transport.....	44
DNS '3 vs. 3' Rule ('Up to 3' Rule)	44
DHCPv6 DNS Server Configuration.....	44
Static DNS Server Configuration.....	45
DNS Config – CLI Method.....	45
DNS Config – Web Method	47
IPv6 Description.....	49
Differences between IPv4 and IPv6	50
IPv6 Features.....	50
ION IPv6 Function Descriptions.....	51
IPv6 Management Functions	52
IPv6 Address Formats.....	52
ICMP v6 (Internet Control Message Protocol for IPv6).....	53
IPv6 Neighbor Discovery Protocol.....	53
IPv6 DAD (Duplicate Address Detection).....	53
IPv6 Static Configuration.....	56
ION IPv6 Configuration Considerations	57
IPv4 and IPv6 Initialization Defaults	58
IP Address Mode Notes	58
Telnet IPv4 and IPv6 Connections	58
TFTP IPv4 and IPv6 Connections	58
IPv6 Address Config – CLI Method	59
IPv6 Address Config – Web Method	60
Changes to Existing ION Applications with IPv4 / IPv6	62
Dynamic Table Entry Limits.....	62
System Configuration	63
System Configuration – CLI Method	63
System Configuration – Web Method.....	64
Login Type Configuration (Local / RADIUS / TACACS+).....	65
Login Type Config – CLI Method.....	65
Login Type Config – Web Method.....	67
Ports Configuration	68
Port Configuration – CLI Method.....	68
Port Configuration – Web Method.....	70
Configuring System Login Users	71
Note Regarding SNMPv3 Users vs. Web/CLI Login Users	71
Configuring System Login Users - CLI Method.....	72
Configuring System / Login Users - Web Method.....	74
Configuring Security Features	75
Configuring an ACL	76
ACL Config (IPv4) – CLI Method.....	78
ACL Config (IPv4) – Web Method	81
ACL under IPv6	84
ACL Config (IPv6) – CLI Method.....	84
ACL Config (IPv6) – Web Method	86
Configuring HTTPs	89
HTTPS Config – CLI Method.....	90
HTTPS Config – Web Method.....	92
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	100

Configuring TACACS+	102
TACACS+ Config - Web Method	104
TACACS+ Config - CLI Method	105
Configuring SNMP	108
SNTP Config – CLI Method	109
SNTP Config – Web Method	114
Configuring SSH	115
SSH Config – CLI Method	116
SSH Config – Web Method	118
Configuring SSH and RADIUS	120
Configuring System Logging (Syslog)	121
Syslog Config – CLI Method	123
Syslog Config – Web Method	124
Configuring SNMP	126
SNMP Config – CLI Method	127
SNMP Config – Web Method	130
Change a SNMP User's Group - Web Method	138
SNMP v3 Commands	142
Web Interface-to-CLI Command Cross Reference	143
Example of ION SNMP Operation	146
4 Operation	147
General	147
Backup and Restore Operations (Provisioning)	147
Backing Up the Configuration	148
Backing Up Standalone Modules	151
Editing the Config File (Optional)	153
Restoring the Configuration	156
Backup / Restore (Provisioning) - CLI Method	159
Backup All and Restore All	161
Notes	161
CLI Commands	161
Overview of Backup/Restore via the CLI	162
Backup and Restore Procedure via CLI Commands	162
Backup and Restore CLI Command Descriptions	164
Other Helpful CLI Commands	175
Backup All and Restore All CLI Messages	177
WEB UI Method	183
Backup All via the Web GUI	183
Restore All via the Web GUI	186
Backup All and Restore All Web UI Messages	188
Disabling USB Console Access	192
Reset to Factory Defaults	193
Resetting Defaults – CLI Method	193
Resetting Defaults – Web Method	194
Resetting Uptime	195
Uptime Reset – CLI Method	195
Uptime Reset – Web Method	196
System Reboot	197
Rebooting the System – CLI Method	197
Rebooting the System – Web Method	198
Transfer Files via Serial Protocol (X/Y/Zmodem) - CLI Method	199
Upgrade the Firmware	200
Upgrading IONMM and/or NID Firmware – CLI Method	200
Upgrading the IONMM Firmware – Web Method	202
Upgrading NIDs – Web Method	204

db.idx File Example	205
Performing the Upgrade	206
Upgrade the IONMM and/or NID Firmware	208
Upgrading IONMM and/or NID Firmware – CLI Method	208
Upgrading IONMM and/or NID Firmware – Web Method	210
Management of Other Modules	216
Managing Using the CLI Commands	216
Managing via the Web Interface.....	218
Replacing the IONMM	219
5 Troubleshooting	220
General	220
Basic ION System Troubleshooting.....	220
Error Indications and Recovery Procedures.....	221
LED Fault and Activity Displays.....	222
Troubleshooting Auto-negotiation Mismatches	223
IPv6 Troubleshooting.....	223
Verify IPv6 Connectivity	224
For Additional Information	224
IPv6 Auto Config Troubleshooting.....	224
Problem Conditions	225
CLI Messages	241
Web Interface Messages	289
SNMP Messages	303
Basic Recovery Steps	303
Syslog Messages and Sys.log Output.....	314
Syslog Messages	314
Sample Sys.log Output.....	317
Windows Event Viewer Messages	320
The Config Error Log (config.err) File.....	321
config.err Messages	322
config.err Message Responses.....	322
Webpage Messages	326
Recording Model Information and System Information	336
Compliance Information	338
Declaration of Conformity	339
Electrical Safety Warnings.....	340
Electrical Safety.....	340
Elektrische Sicherheit.....	340
Elektrisk sikkerhed.....	340
Elektrische veiligheid.....	340
Sécurité électrique.....	340
Sähköturvallisuus	340
Sicurezza elettrica	340
Elektrisk sikkerhet.....	340
Segurança eléctrica.....	340
Seguridad eléctrica.....	340
Elsäkerhet.....	340
Appendix B Factory Default Settings	341
Appendix C Configuration Quick Reference – CLI.....	349
IPv4 Configuration	349
IPv6 Configuration	349
ACL Configuration (IPv4).....	350
ACL Configuration (IPv6).....	350
Backup / Restore Configuration.....	351

HTTPS Configuration.....	351
Management VLAN Configuration.....	352
RADIUS Configuration.....	352
TACACS+ Configuration.....	353
SNMP Configuration.....	354
SNTP Configuration.....	355
SSH Configuration.....	356
Syslog Configuration.....	356
System (Login) User Configuration.....	357
Transfer Files via Serial Protocol (X/Y/Zmodem).....	357
Appendix D ION System File Content and Location	358
File Status after Reset to Factory Defaults.....	358
Back Up and Restore File Content and Location	359
Reboot File Content and Location.....	361
Firmware Upgrade File Content and Location	362
Glossary	363
Index.....	416

List of Figures

Figure 1: Sample ION System Configuration.....	10
Figure 2: IONMM Installation	18
Figure 3: IONMM and IONMM-232 Connectors and LEDs	19
Figure 4: CLI Location Hierarchy	216

List of Tables

Table 1: Physical Specifications.....	15
Table 2: Documentation Conventions	16
Table 3: IONMM Connector and LED Descriptions.....	20
Table 4: IONMM System-Level Menu Description.....	34
Table 5: Port-Level Menu Description	36
Table 6: User Level Rights via Web / CLI.....	71
Table 7: Timezones	109
Table 8: Syslog Severity Levels.....	121
Table 9: SNMP v3 Initialization (Default) Values	139
Table 10: SNMP v3 Web Interface Default Values.....	140
Table 11: SNMP Command Categories	142
Table 12: Web Interface to CLI Command Cross Reference.....	143
Table 13: Device-Level Factory Defaults.....	341
Table 14: Port-Level Factory Defaults.....	348
Table 15. File Status after a Reset to Factory Defaults	358
Table 16. Back Up and Restore File Content and Location	359
Table 17: File Content and Location after a System Reboot.....	361
Table 18: File Content and Location after a Firmware Upgrade.....	362

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.
- Appendix A: Warranty and Compliance Information – This appendix describes the warranty and compliance information for the IONMM.
- Appendix B: Factory Default Settings – This appendix provides a table listing the default settings for the IONMM.
- Appendix C: Configuration Quick Reference – This appendix provides a quick reference for the CLI commands used to configure the IONMM.
- Appendix D: 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.

In addition to the above, this manual contains a glossary of terms used in the manual and an index to the information contained within the manual.

Product Overview

The ION Management Module (IONMM) is a single slot design slide-in module that lets you configure and manage all of 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 in order 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.

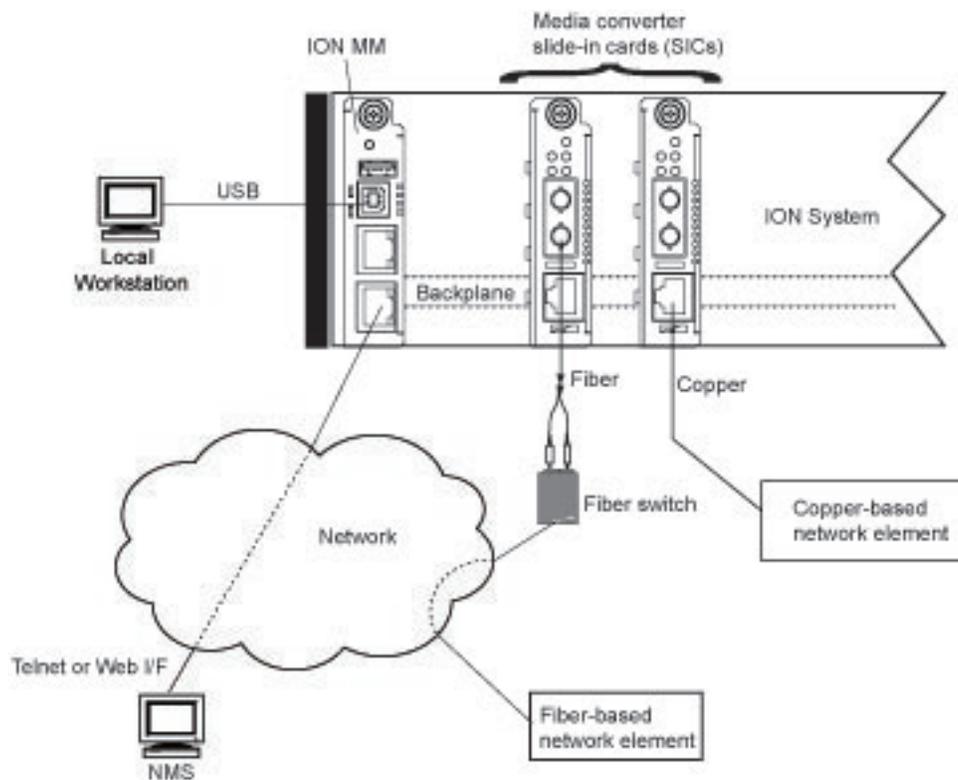


Figure 1: Sample ION System Configuration

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. Provides two 10/100 Mbps RJ-45, one USB 2.0 device port, and one USB 2.0 host port.
IONMM-232	Management Module for the ION Chassis. Provides an RJ-45 RS-232 CONSOLE connector for CLI commands.

Features

The following are features of the ION Management Module.

- Backup/restore/upgrade ION modules
- A variety of management access methods
- Two 10/100BaseT/TX Ethernet interfaces
- An RJ-45 RS-232 Console port (IONMM-232)
- Single slot design
- Several security features
- Enhanced user management
- Syslog (System Logging)
- Multiple IP addressing modes (IPv4 / IPv6, DHCP, Static, Bootp)
- SNMP v1, SNMP v2c, and SNMP v3 Support
- Multiple community strings
- Public and private MIB support

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) to upload its present configuration onto a TFTP server. The IONMM can also download the configuration from the TFTP server to update its settings. TFTP 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 [Downloads](#) 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.
- 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.

The Bootp protocol lets a network user be automatically configured (receive an IP address) and have an OS booted without user involvement. The BOOTP server automatically assigns the IP address from a pool of addresses for a certain duration of time.

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 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 / 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 are able to 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 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 similar to 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 actually change MIB variables on a network element.

Physical Specifications

The physical specifications for the IONMM are described in the table below.

Table 1: Physical Specifications

Item	Specification
Standards	IEEE Std. 802.3
Ports	Two 10/100 Mbps RJ-45 ports: one USB 2.0 <i>Device</i> port, and one USB 2.0 <i>Host</i> port (the USB-HOST port is not currently used)
Dimensions	Width: 0.86" (22 mm) Depth: 6.5" (165 mm) Height: 3.4" (86 mm)
Power Consumption	2 Watts under normal operation (the USB-HOST port is not currently used).
Environment	Operating Temp: 0°C (32 to 122°F) 5% - 95% humidity (non-condensing) 0 to 10,000 ft. altitude Storage Temp: 0 to 85°C (-40 to 185°F)
Shipping Weight	1 lb. [0.45 kg]
Compliance	EN55022 Class A, EN55024, CE Mark
Warranty	Lifetime

See the *IONMM-232 Install Guide* for IONMM-232 specifications.

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 Drivers, Firmware, etc. go to the [Product Support](#) webpage (logon required). For Lantronix Application Notes, Manuals, Brochures, Data Sheets, Specifications, etc. go to the [Support Library](#) (no logon required). Note that this manual provides links to third part web sites for which Lantronix is not responsible.

The ION system and related manuals are listed below.

1. IONMM Install Guide, 33420
2. IONMM-232 Install Guide, 33725
3. ION106-x Six Slot Chassis User Guide, 33658
4. ION Management Module (IONMM) User Guide, 33457 (this manual)
5. ION Systems CLI Reference Manual, 33461
6. ION219-x 19-Slot Chassis Installation Guide, 33412
7. ION219 Cxx1x NID Installation Guides, 33414 - 33417
8. ION Dry Contact Relay (DCR) Kit Install Guide, 33422
9. IONPS-A-R1 Power Supply User Guide, 33614
10. IONPS-D-R1 Power Supply User Guide, 33707
11. ION ADP Install Guide, 33413
12. SFP manuals (see Lantronix [SFP page](#))
13. ION System Release Notes (software version related)
14. Product Documentation 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 of the descriptions and procedures reflect the latest software/firmware version, noted in the [Revision History](#) on page 2.

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 (Telnet session or Web interface).

Installing the IONMM

The IONMM is to be installed only in a Lantronix ION chassis (e.g., ION001-x, ION002-AD, ION106-x, or ION219-x). A complete list of ION products is on our [website](#).

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.

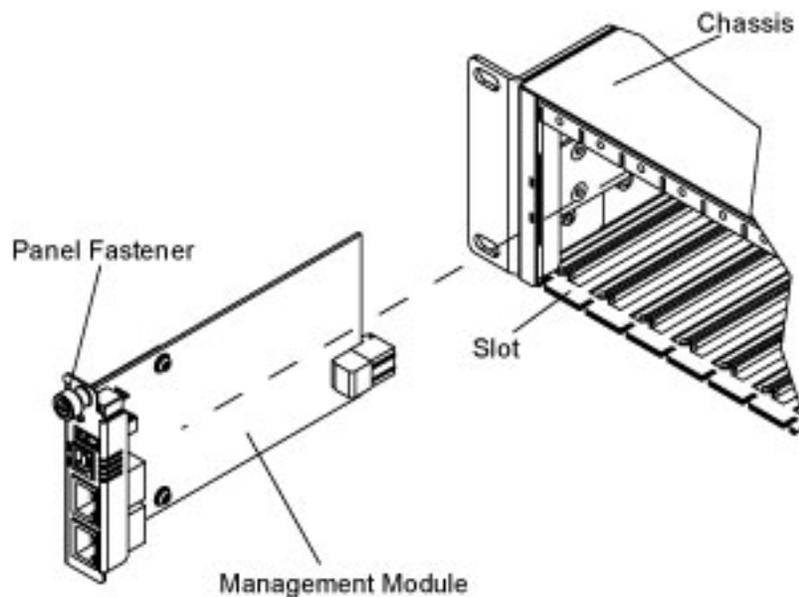


Figure 2: IONMM Installation

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.

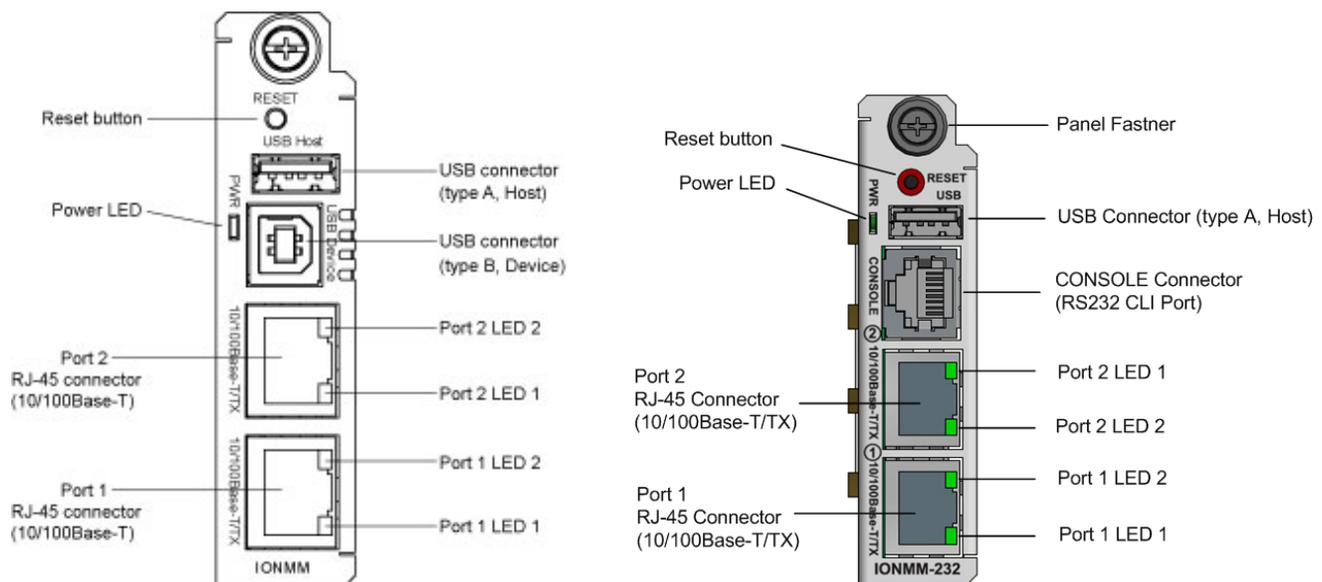


Figure 3: IONMM and IONMM-232 Connectors and LEDs

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 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: <ul style="list-style-type: none"> • 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 a 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 USB 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](#) or on the Lantronix website at <https://www.transition.com/products/media-converters/ionmm/>.

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

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.

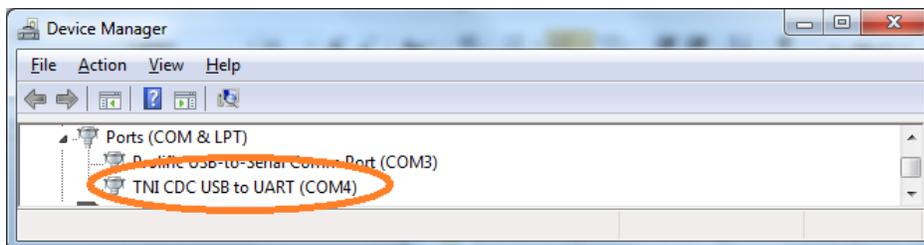
Installing the USB Driver - Windows 7

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

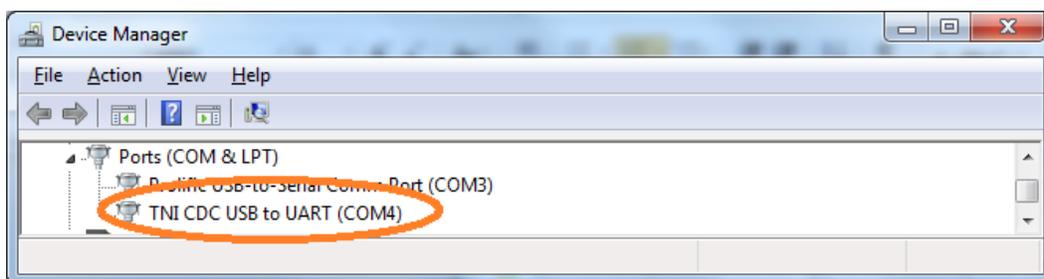
After the USB driver has been installed you must set up the terminal emulator software (e.g., Tera Term or HyperTerminal) to use the USB COM port.

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 (Windows 7, 8.1, and 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 Systems 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**.

Access via an Ethernet Network

The IONMM can be managed remotely through the Ethernet network via either a 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, in order 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 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. The following describes the procedure to connect to and access the IONMM via a Telnet session.

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

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

You can now enter commands to set up the various configurations for the IONMM.

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](#)”. For a description of all available CLI commands see the *ION Systems CLI Reference Manual, 33461*.

Terminating a Telnet Session

To terminate the Telnet session:

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

Web Browser Support

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

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).

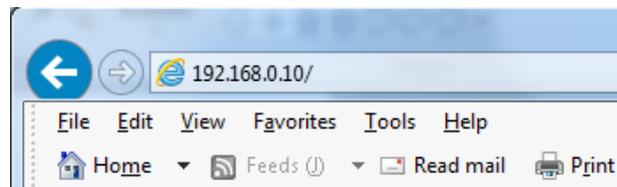
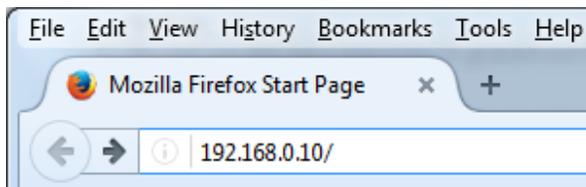
A Web session can be used to connect to and set up the IONMM.

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.



Sign in to ION System Web Interface

User Name: ION
 Password:

Sign in

Mon Sep 26 2016 11:03:43 GMT-0500 (Central Standard Time)

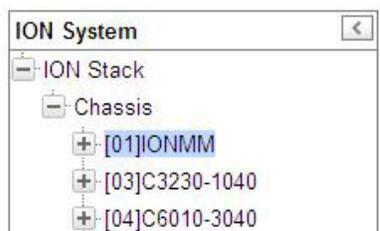
Note: If your system uses a security protocol (e.g., RADIUS, SSH, etc.), you must enter the login and password required by that protocol.

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).

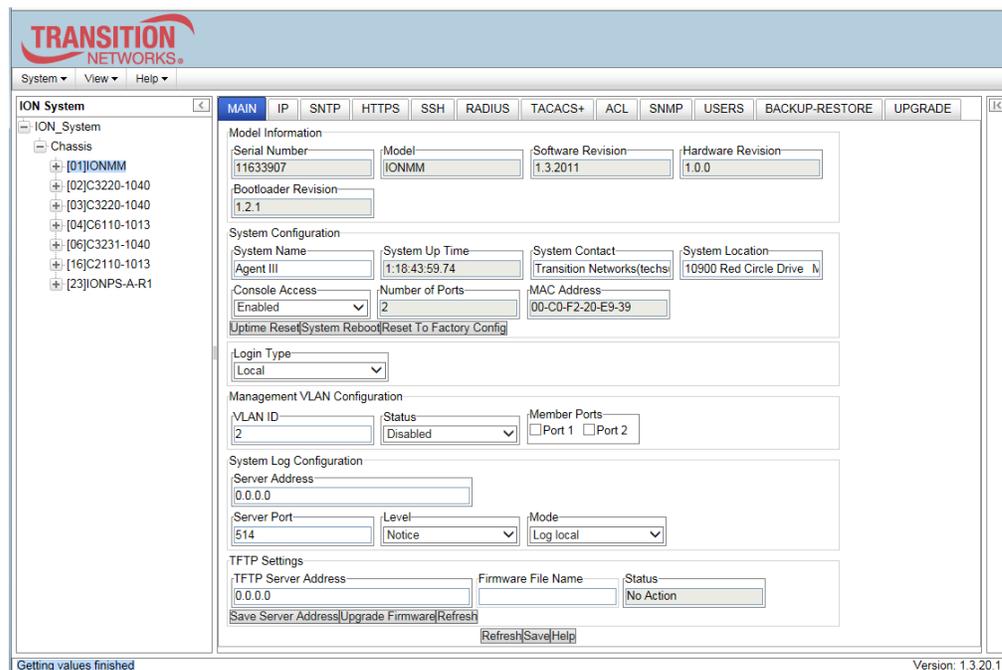
6. Click the **Sign in** button or press the **Enter** key. The opening screen displays.



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).

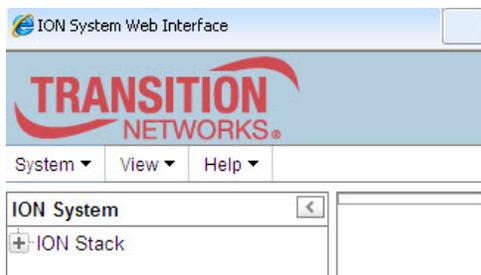
Note: At IONMM FW v 1.3.14 and before, the ION System does not automatically log out upon exit or after a timeout period, which could leave it vulnerable if left unattended. Follow your organizational policy on when to sign out.

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 a 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 a Telnet session or through the Web interface.

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

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

* 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: <i>Refresh</i> , <i>Save</i> , and <i>Help</i> .
MAIN tab (Port 2)	Sections: Sections: Port Configuration, Auto Negotiation Settings, and Capabilities Advertised. Buttons: <i>Refresh</i> , <i>Save</i> , and <i>Help</i> .

Reboot and Reset Functions

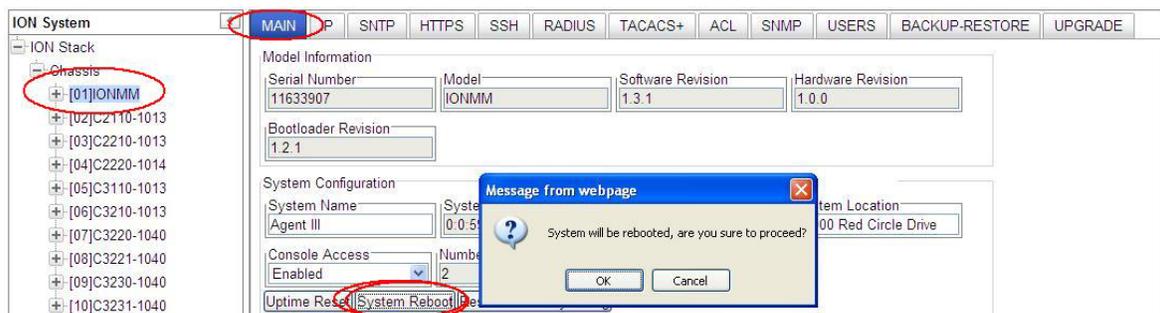
Certain functions such as a System Reboot, Reset to Factory Configuration, Reset Power to a Slot, and Power Off a Slot cause the system to delete its stored files. **Caution:** These stored files are lost unless you first perform a system Backup. See the “[Backup and Restore Operations](#)” section starting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

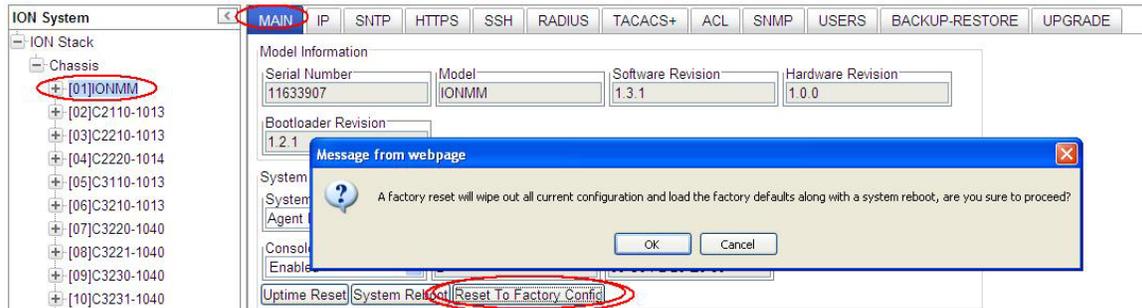
The message “*Loading, please wait...*” displays. A System Reboot can take several minutes.

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, in order 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 (Bootp, DHCP, or Static IP)

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 a 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 through the use of 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 a 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
-----
```

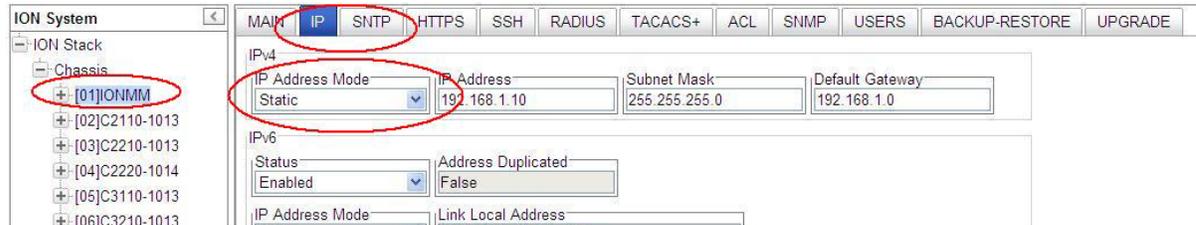
```
DNS server1   ipv4      0.0.0.0
DNS server2   ipv4      0.0.0.0
DNS server3   ipv4      0.0.0.0
```

```
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 of 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 actually works, ION consider it an available DNS address, and others are considered 'unavailable' addresses even if they are actually '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 a Telnet session (see “Starting a Telnet Session”).
2. At the command prompt: **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=dns 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.

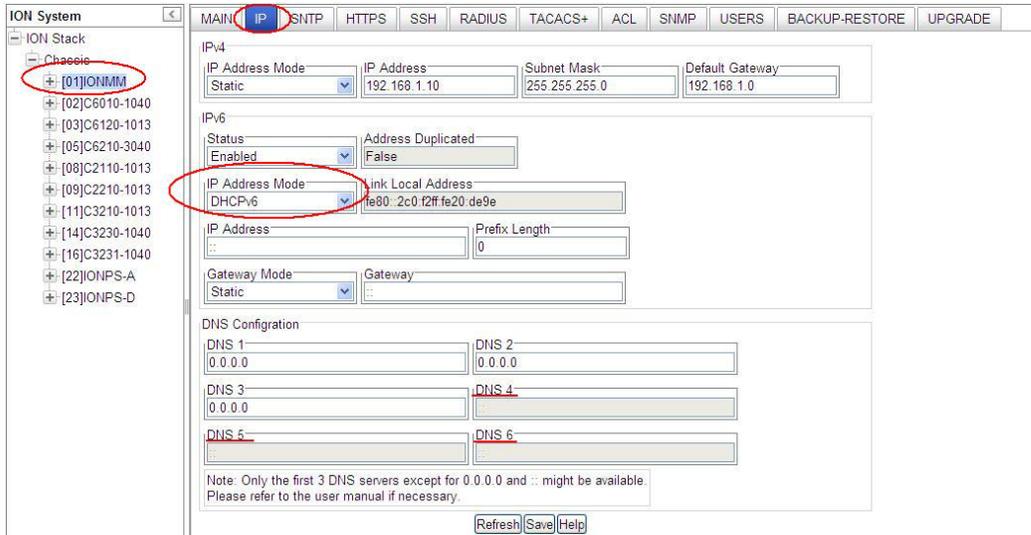
The screenshot shows the ION System web interface. The 'IP' tab is selected. The 'DNS Configuration' section is highlighted with a red box. It contains six input fields for DNS 1 through DNS 6. DNS 1, 2, and 3 are set to 0.0.0.0. DNS 4, 5, and 6 are set to ::. A note below the fields states: 'Note: Only the first 3 DNS servers except for 0.0.0.0 and :: might be available. Please refer to the user manual if necessary.' There are 'Refresh', 'Save', and 'Help' buttons at the bottom of the section.

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

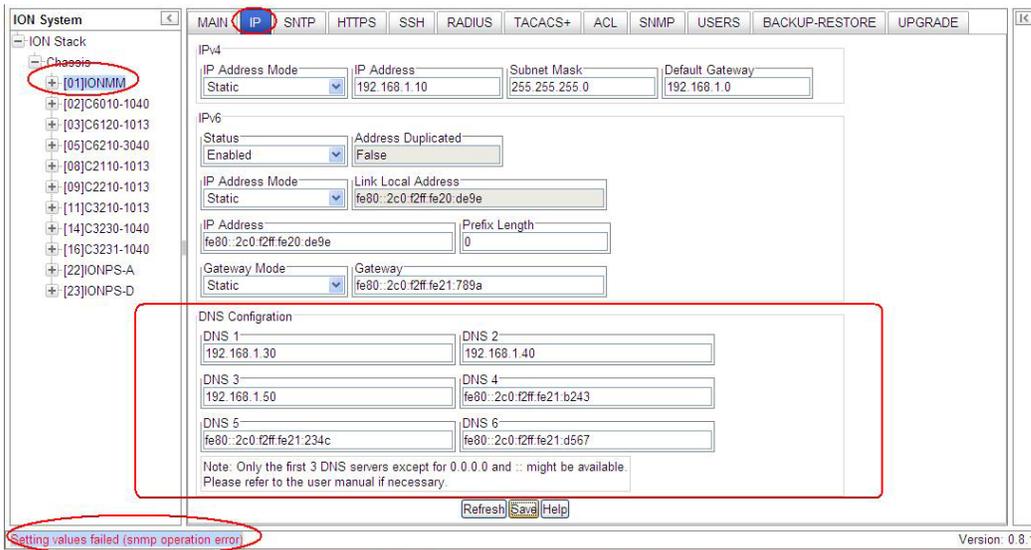
4. In the DNS 1- DNS 3 fields, enter a valid IPv4 IP address (not applicable if DHCP is selected for IPv4 Address Mode).
5. In the DNS 4- DNS 6 fields, enter a valid IPv6 IP address (not applicable if DHCP v6 is selected for IPv6 Address Mode).
6. Scroll down and click **Save** when done.

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 particular 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. In order 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 final 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	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$
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

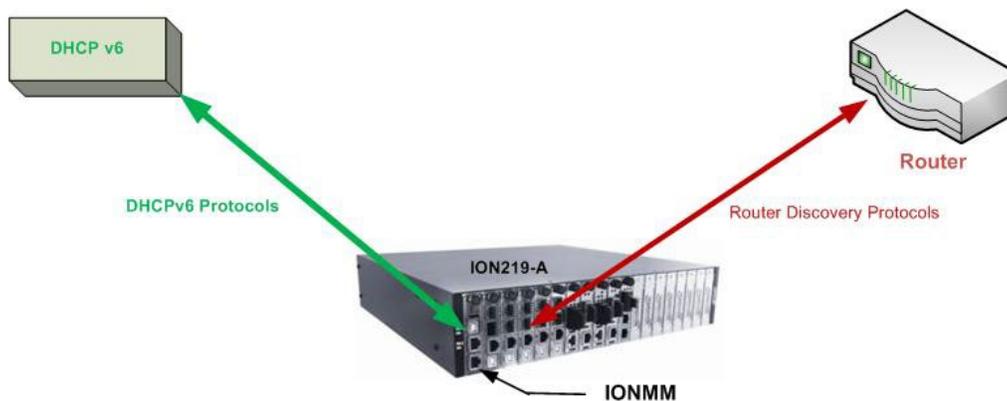


Figure x. Multiple Routers - One DHCPv6 server and One Router

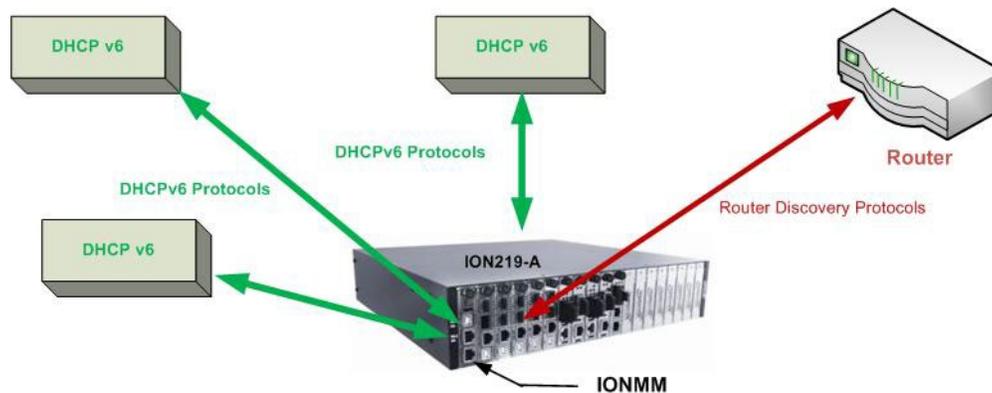


Figure x. Multiple DHCPv6 servers and One Router

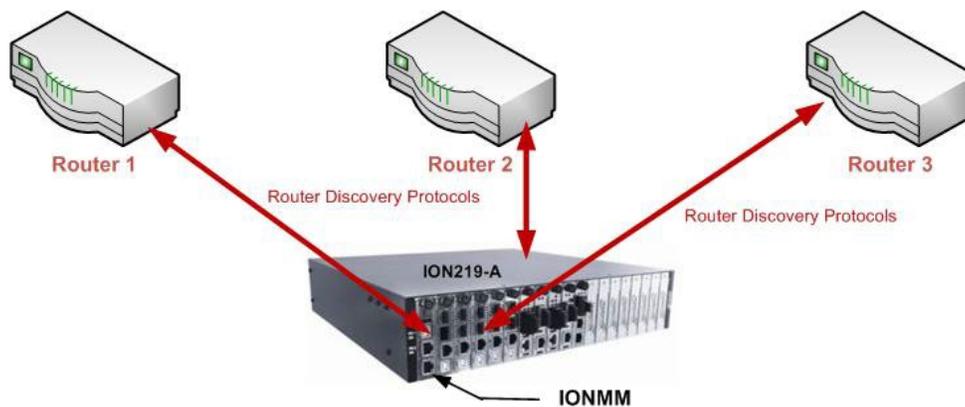


Figure x. Multiple Routers

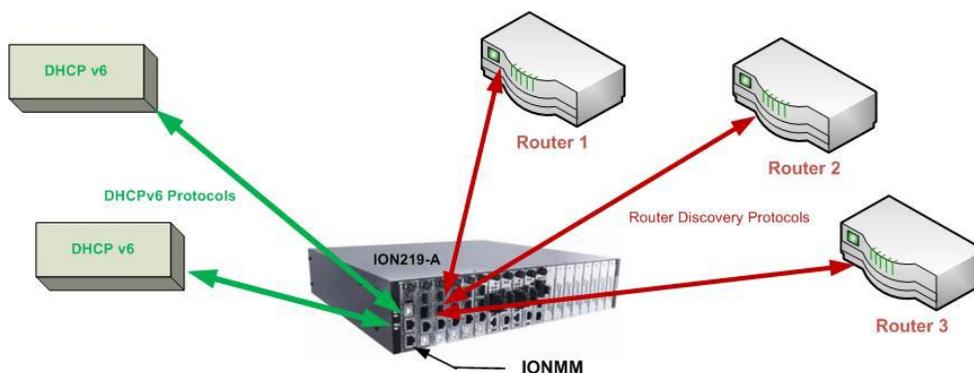


Figure x. Multiple DHCPv6 Servers and Routers

IPv6 Management Functions

IPv6 Address Formats

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: $x:x:x:x:x:x$. 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 ($FE80::/10 + \text{Intf}(64)$)
- Global address ($2000::/3 + \text{prefix}(45) + \text{Subnet}(16) + \text{Intf}(64)$)
- Unique Local IPv6 Unicast Addresses ($FC00::/7 + \text{Global ID}(40) + \text{Subnet}(16) + \text{Intf}(64)$)

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 (FF02:0:0:0:1: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 be 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 in 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 in order 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 particular 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 fwddbAfter 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 in order 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 a 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>
```

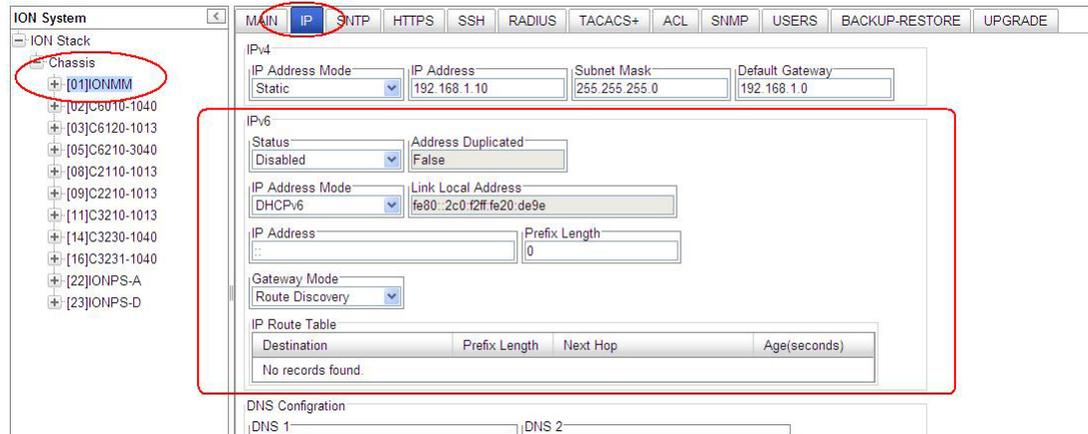
Note: the command "set dhcp state" is replaced by "set ip address mode" after ION v 1.2.0.

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
```

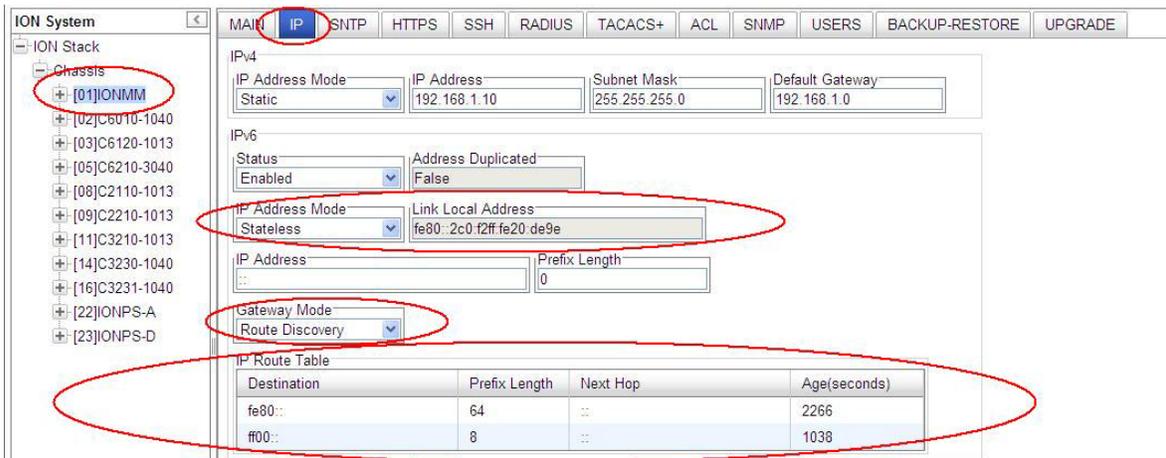
IPv6 Address Config – Web Method

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.

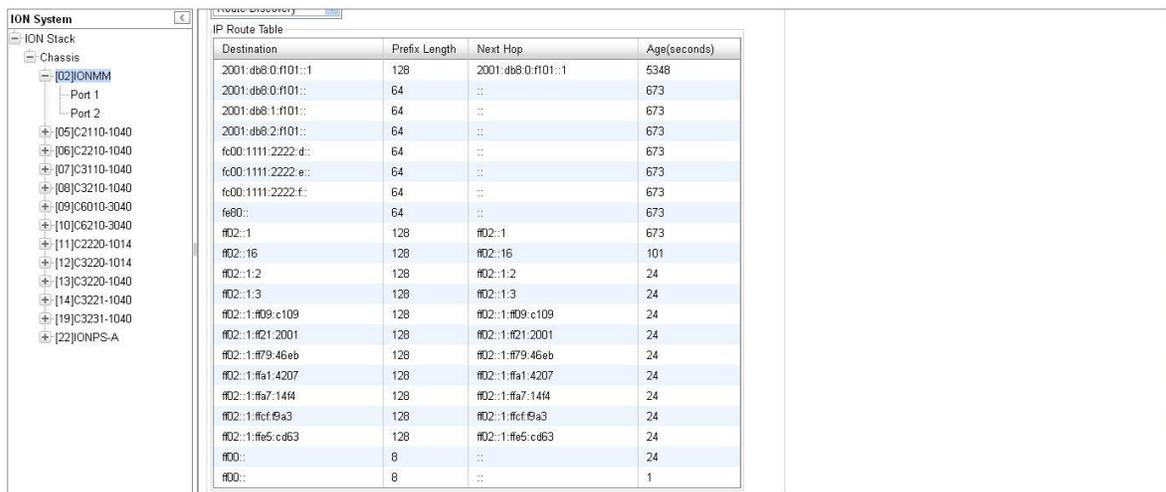
11. Verify the IP Route Table settings. For example:



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

These 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	IonDevSysUserTable	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.

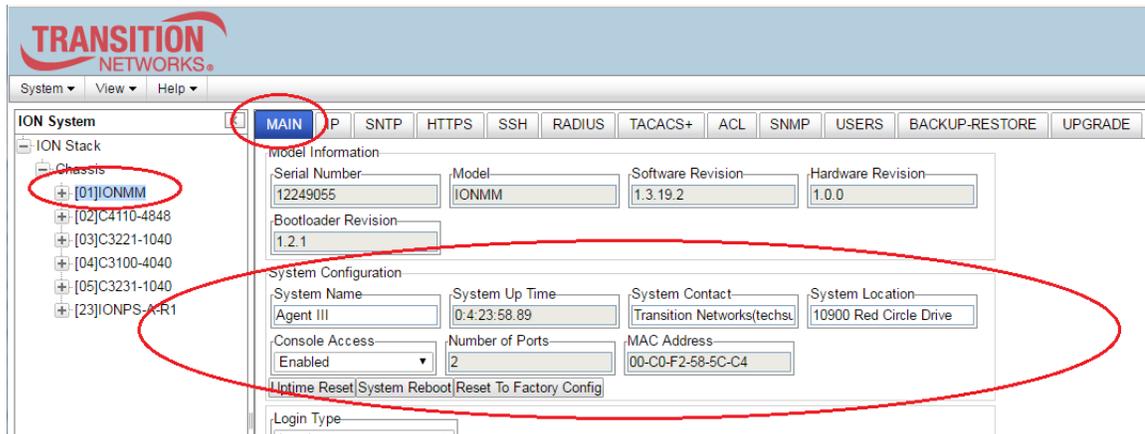
1. Access the NID through either a USB connection (see “[Starting a USB Session](#)”) or a Telnet session (see “[Starting a Telnet Session](#)”).
2. At the command prompt type **set system contact=CONTACT**, where CONTACT is the new contact (e.g., person, department name), and press **Enter**.
3. Type **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 a 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 a 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
```

```

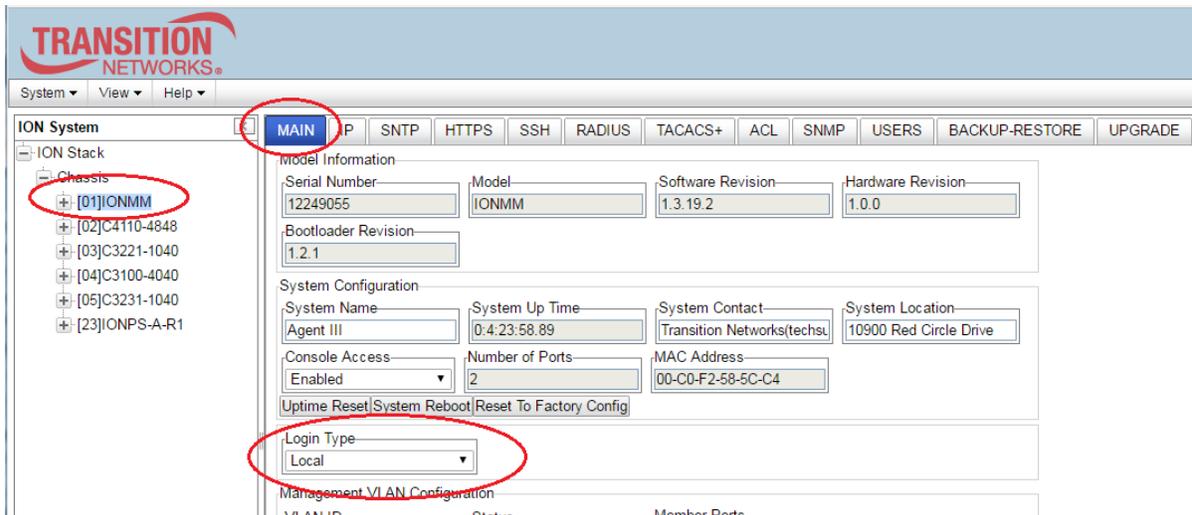
Agent III C1|S1|L1P1>set tacplus ?
  client
  svr
Agent III C1|S1|L1P1>set tacplus client state ?
  disable
  enable
Agent III C1|S1|L1P1>set tacplus svr 1 ?
  retry
  secret
  timeout
  type
Agent III C1|S1|L1D>set tacplus svr 1 retry 3
Agent III C1|S1|L1D>set tacplus svr 1 secret Buffrey1
Agent III 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 a 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).

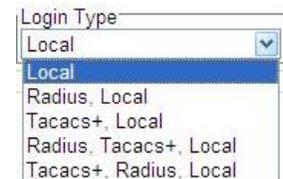
Radius, Local: the ION software will validate the RADIUS login and then the local login.

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 a 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**. This option displays on Port 1 only.
5. At the **Auto Negotiation** dropdown, select **Enable** or **Disable**.
If you select **Disabled** and click the **Save** button, the **Force Speed** and **Force Duplex** dropdowns display. (On Port 2, if AutoNegotiation is Disabled, the Forced Speed field does not display.
 - a. At **Force Speed**, select **10Mbps** or **100Mbps** as the forced rate for this IONMM port.
 - b. At **Force Duplex**, select **Half Duplex** or **Full Duplex** as this IONMM port’s forced duplex mode.
 If you selected Auto Negotiation **Disabled**, 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 a Telnet session (see “[Starting a Telnet Session](#)”).
2. Check the existing set of ION system users. At the device’s command prompt type **show sysuser** and press the **Enter** key. All of 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 = <**administrator**, **read-write**, 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 **administrator**, **read-write**, 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.

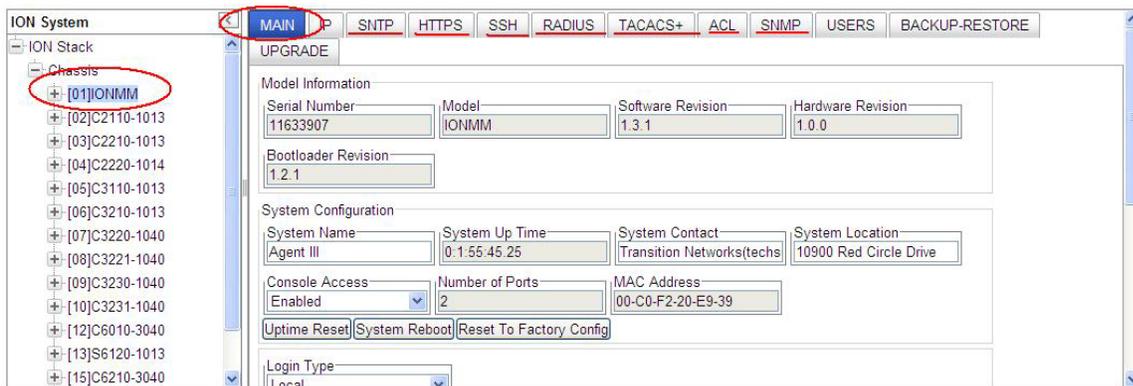
3. In the **User Name** field, enter this user’s name (1-64 alphanumeric characters with no spaces between characters).
4. In the **Password** field, enter this user’s password.
5. In the **Confirm Password** field, re-enter the password as entered in step 4. If the two password entries do not match, 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 outgoing 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 ipv4addrange 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 a 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
condlist=1
C1|S7|L1D>add acl rule position=tail table=filter chain=input policy=trap condition=2
condlist=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.

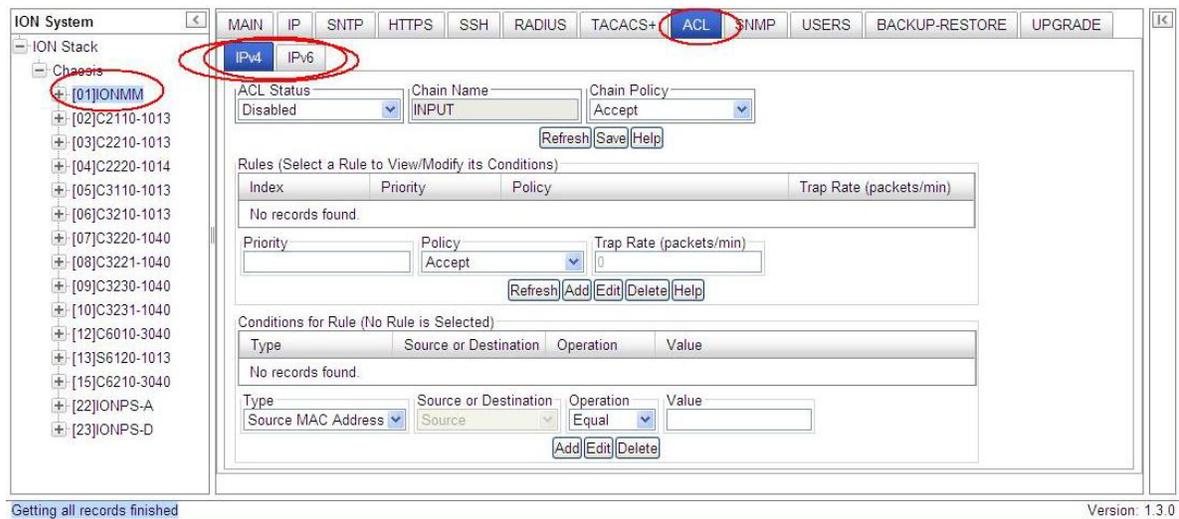
Example:

```
Agent III C1|S1|L1D>show acl rule index table-type chain-type priority policy traprate(pack-
ets/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** field, 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 **ICMP Type** values selectable: 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.

ION System

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

ACL Status: Enabled | Chain Name: INPUT | Chain Policy: Accept

Refresh Save Help

Rules (Select a Rule to View/Modify its Conditions)

Index	Priority	Policy	Trap Rate (packets/min)
1	1	Accept	0
2	6	Drop	0
3	9	Trap	1

Priority: 1 | Policy: Accept | Trap Rate (packets/min): 0

Refresh Add Edit Delete Help

Conditions for Rule 1

Type	Source or Destination	Operation	Value
IPv4 Address	Source	Equal	192.168.1.30
TCP Port	Source	Not Equal	6

Type: ICMP Type | Source or Destination: Source | Operation: Not Equal | Value: ICMP-ECHO-REPLY

Add Edit Delete

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 compare 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

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 a 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          0            ipv6addr     src          equal         ::
2          0            ipv6addr     src          equal         ::
3          0            ipv6addr     src          equal         ::
4          0            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 rate 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 IPv6 options 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).

One 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` (`entPhysicalIndex`, `ip6tablesGRuleIndex`)

A `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.

The screenshot shows the ION System configuration interface. The left sidebar displays the ION Stack hierarchy, including Chassis and various IONMM and IONPS components. The main configuration area is titled 'IPv6' and contains the following sections:

- ACL Status:** Enabled (dropdown), Chain Name: INPUT, Chain Policy: Accept (dropdown). Buttons: Refresh, Save, Help.
- Rules (Select a Rule to View/Modify its Conditions):**

Index	Priority	Policy	Trap Rate (packets/min)
1	1	Trap	330

Below the table, there are input fields for Priority (1), Policy (Trap), and Trap Rate (330). Buttons: Refresh, Add, Edit, Delete, Help.
- Conditions for Rule 1:**

Type	Source or Destination	Operation	Value
IPv6 Network	Source	Equal	fe80::2c0:f2ff:fe20:de9e/32

Below the table, there are dropdowns for Type (IPv6 Network), Source or Destination (Source), and Operation (Equal). The Value field contains 'fe80::2c0:f2ff:fe20:de9e' and a separate field contains '/ 32'. Buttons: Add, Edit, Delete.

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 through the Web interface.

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 a Telnet session.
- After configuring the NID for HTTPS, a re-login occurs immediately; you must enter the **https://** prefix in order 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 SSL, while HTTP sends it all as plain text

HTTPS utilizes the transport layer security (TLS) protocol for transmitting private documents via the Internet. SSL utilizes a cryptographic system that uses two keys to encrypt data; a public key known to everyone and a private or secret key known only to the recipient of the message. Anything encrypted with either key can only be decrypted with its corresponding key. Thus if a message or data stream were encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data only could have come from the server.

For the IONMM, HTTPS can be used for client authentication in order 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.

Because SSL utilizes public key cryptography to encrypt the data stream traveling over the Internet, a certificate is not really necessary as the data is secure and cannot easily be decrypted by a third party. However, certificates do serve a crucial role in the communication process. The certificate, signed by a trusted Certificate Authority, ensures that the certificate holder is really who they claim to be. Without a trusted signed certificate, your data may be encrypted; however, the party you are communicating with may not be whom you think. Without certificates, impersonation attacks would be much more common.

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

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

Note: enabling HTTPS has no effect on either the USB or Telnet interface. However, access through the Web interface must go through HTTPS authentication.
4. In the **HTTPS Port** field, enter the port number for HTTPS operations. The valid range is from 1-65535. The default is port 443.
4. In the **Certificate Type** field, select **Self Certified** or **Authorized**.
5. In the **TFTP Server IP Address** field, enter the IP address of your TFTP 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 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.

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 of the 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 a 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 through the use of 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 in the event that 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.

The RADIUS server is usually a background process running on a *UNIX* or *Windows NT* machine.

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 a 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 of 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 starting for specific error messages.

Configuring TACACS+

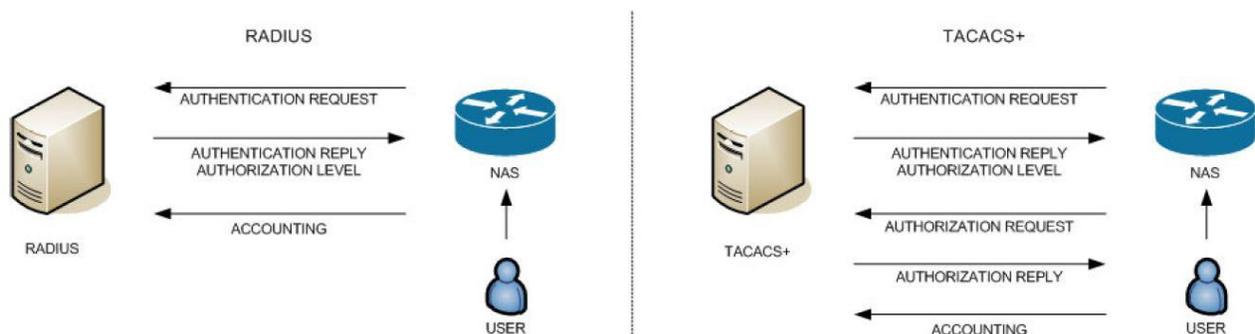
TACACS+ (Terminal Access Controller Access Control System) provides routers and access servers with authentication, authorization and accounting services. TACACS+ is used along with or as a replacement for RADIUS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram 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 in order 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 - Web Method

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

The screenshot shows the IONMM web interface for TACACS+ configuration. The left sidebar shows the ION Stack hierarchy with [01]IONMM selected. The main content area is titled 'TACACS+' and contains the following configuration options:

- TACACS+ Client:** A dropdown menu set to 'Enabled'.
- TACACS Server 1:**
 - Server Address: fe80::2c0:f2ff:fe21:b100
 - Server Secret: ••••••••
 - Retries (1-5): 4
 - Timeout (1-60s): 55
- TACACS Server 2:**
 - Server Address: fe80::2c0:f2ff:fe21:b24c
 - Server Secret: ••••••••
 - Retries (1-5): 1
 - Timeout (1-60s): 5
- TACACS Server 3:**
 - Server Address: 0.0.0.0
 - Server Secret: ••••••••
 - Retries (1-5): 3
 - Timeout (1-60s): 30
- TACACS Server 4:**
 - Server Address: 0.0.0.0
 - Server Secret: ••••••~
 - Retries (1-5): 3
 - Timeout (1-60s): 30
- TACACS Server 5:**
 - Server Address: 0.0.0.0
 - Server Secret: ••••••~
 - Retries (1-5): 3
 - Timeout (1-60s): 30
- TACACS Server 6:**
 - Server Address: 0.0.0.0
 - Server Secret: ••••~
 - Retries (1-5): 3
 - Timeout (1-60s): 30

At the bottom right of the configuration area, there are buttons for 'Refresh', 'Save', and 'Help'.

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.

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 a 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. See "[TACACS+ Commands](#)".
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. See "[TACACS+ Commands](#)".
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"
```

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 a Telnet session (see “Starting a Telnet Session”).
2. Enable SNTP. Type: **set sntp state=enable**
3. Press **Enter**.
4. Set the current time. Type: **set 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
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 sntp 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 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.

The screenshot shows the IONMM web interface. The top navigation bar includes tabs for MAIN, IP, **SNTP**, HTTPS, SSH, RADIUS, TACACS+, ACL, SNMP, USERS, BACKUP-RESTORE, and UPGRADE. The left sidebar shows the ION Stack with Chassis [01]IONMM selected. The main content area is titled 'SNTP Configuration' and contains the following fields:

- SNTP Client:** Disabled (dropdown)
- Device Time:** 1969 1231 21:12:57
- UTC Timezone:** (GMT-06:00)Central Time (US & Canada) (dropdown)
- Daylight Saving Time Configuration:**
 - Daylight Saving Time:** Disabled (dropdown)
 - Daylight Saving Period Start:** 1969 1231 18:00:00
 - Daylight Saving Period End:** 1969 1231 18:00:00
 - Daylight Saving Offset (mins):** 0
- SNTP Servers:** Six input fields for SNTP Server 1 through SNTP Server 6, all containing 0.0.0.0.

Buttons for Refresh, Save, and Help are located at the bottom of the form. The status bar at the bottom left says 'Getting values finished' and the bottom right says 'Version: 1.3.0'.

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. 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 in order 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 a 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.

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 time 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.

Key Settings
User

Public-Key Type: No Copy

TFTP Server IP Address

Source File Name

Copy Delete Refresh

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 Server Address** field, enter the IP address of your TFTP 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., <i>earthquake, tornado</i>) - 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., <i>loss of backup connection</i>).
Critical	2 - Critical error conditions. Should be corrected immediately, but indicates failure in a primary system - fix CRITICAL problems before ALERTs (e.g., <i>loss of primary connection</i>).
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., <i>file system 85% full</i>). 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 written down;

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 a 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:

```

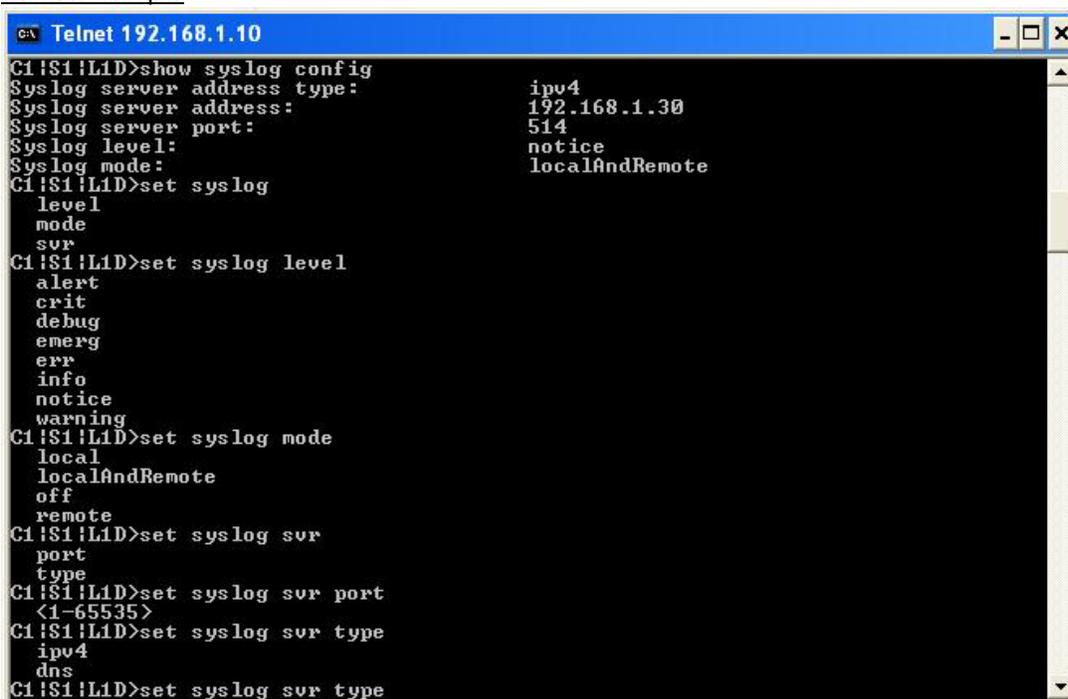
Agent III C1|S1|L1D>show syslog config
Syslog server address type:      ipv4
Syslog server address:          192.168.0.2
Syslog server port:             514
Syslog level:                   info
Syslog mode:                    local
Agent III C1|S1|L1D>

```

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:



```

C:\ Telnet 192.168.1.10
C1|S1|L1D>show syslog config
Syslog server address type:      ipv4
Syslog server address:          192.168.1.30
Syslog server port:             514
Syslog level:                   notice
Syslog mode:                    localAndRemote
C1|S1|L1D>set syslog
  level
  mode
  svr
C1|S1|L1D>set syslog level
  alert
  crit
  debug
  emerg
  err
  info
  notice
  warning
C1|S1|L1D>set syslog mode
  local
  localAndRemote
  off
  remote
C1|S1|L1D>set syslog svr
  port
  type
C1|S1|L1D>set syslog svr port
  <1-65535>
C1|S1|L1D>set syslog svr type
  ipv4
  dns
C1|S1|L1D>set syslog svr type

```

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.

The screenshot shows the IONMM web interface. The 'MAIN' tab is selected. The 'System Log Configuration' section is highlighted with a red oval. The configuration fields are as follows:

Model Information			
Serial Number	Model	Software Revision	Hardware Revision
11633907	IONMM	1.3.1	1.0.0
Bootloader Revision			
1.2.1			
System Configuration			
System Name	System Up Time	System Contact	System Location
Agent III	0:3:36:39:81	Transition Networks(techs)	10900 Red Circle Drive
Console Access	Number of Ports	MAC Address	
Enabled	2	00-C0-F2-20-E9-39	
Uptime Reset System Reboot Reset To Factory Config			
Login Type			
Local			
Management VLAN Configuration			
VLAN ID	Status	Member Ports	
2	Disabled	<input type="checkbox"/> Port 1 <input type="checkbox"/> Port 2	
System Log Configuration			
Server Address			
0.0.0.0			
Server Port	Level	Mode	
514	Notice	Log local	

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.

<i>Emergency</i>	Emergency; system is unusable (most critical)
<i>Alert</i>	Action must be taken immediately
<i>Critical</i>	A critical condition exists
<i>Error</i>	Error condition
<i>Warning</i>	Warning condition
<i>Notice</i>	Normal but significant condition (default setting)
<i>Info</i>	Informational message
<i>Debug</i>	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"}:

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

4. Verify the Syslog configuration.



System Log Configuration

Server Address
fe80::2c0:f2ff:fe20:de9e

Server Port
2

Level
Warning

Mode
Log local and remote

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 of 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 a 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>
```

```
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>

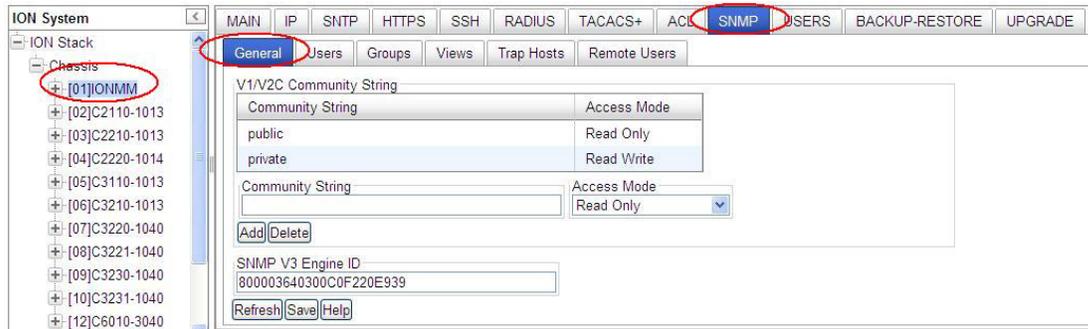
```

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 of 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:

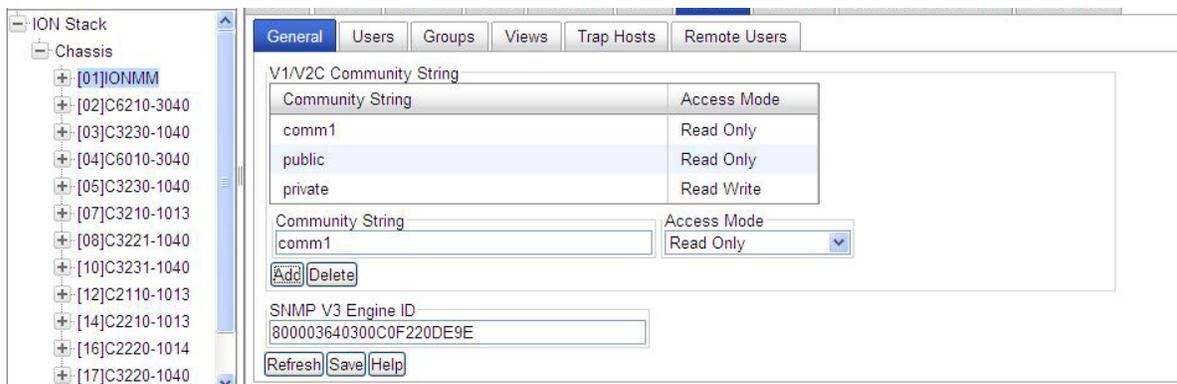
Community String: enter the string to be added (e.g., **comm_1**) from 1-32 alphanumeric characters (no space characters).

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

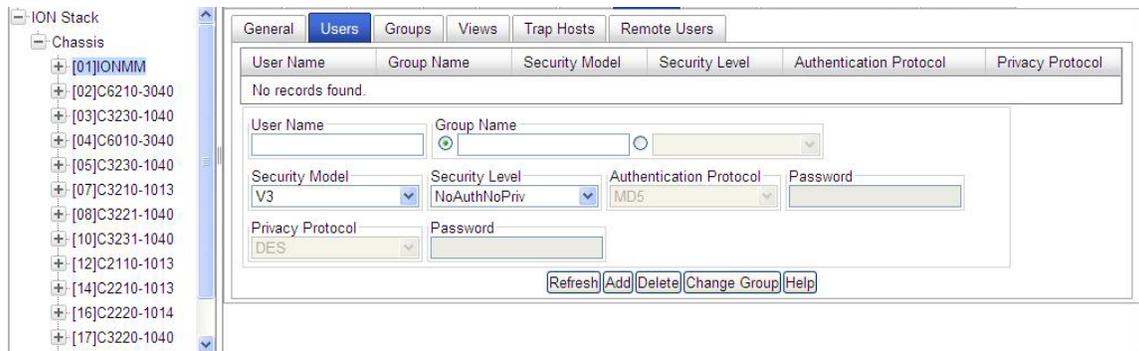
SNMP V3 Engine ID: enter the string to be added (e.g., **800003640300C0F220DE9E** above).

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.

User Name	Group Name	Security Model	Security Level	Authentication Protocol	Privacy Protocol
Adam	G1V3AuthPrivMD5	V3	AuthPriv	MD5	DES
JeffS	private2	V3	NoAuthNoPriv	None	None

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

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	

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.

The screenshot shows the IONMM configuration interface. On the left, a tree view shows the ION Stack structure under Chassis, listing components like [01]IONMM, [02]C6210-3040, [03]C3230-1040, [04]C6010-3040, [05]C3230-1040, [07]C3210-1013, [08]C3221-1040, [10]C3231-1040, [12]C2110-1013, [14]C2210-1013, and [16]C2220-1014. The main pane is titled 'Views' and contains a table with two columns: 'View Name' and 'OID Sub Tree List'. The first row shows 'defaultView' and 'Click To See Detail...'. Below the table, there is a 'View Name' input field, an 'OID Sub Tree' input field, and a 'Type' dropdown menu set to 'Included'. At the bottom, there are buttons for 'Refresh', 'Add', 'Edit', 'Delete', and 'Help'.

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

The screenshot shows the IONMM configuration interface with the 'Views' sub-tab selected. The left pane shows the ION Stack tree view, including components like [01]IONMM, [02]C6210-3040, [03]C3230-1040, [04]C6010-3040, [05]C3230-1040, [07]C3210-1013, [08]C3221-1040, [10]C3231-1040, [12]C2110-1013, [14]C2210-1013, [16]C2220-1014, [17]C3220-1040, and [22]IONPS-A. The main pane shows the 'Views' configuration with the 'defaultView' entry selected in the table. The details table below shows three rows of data:

OID Sub Tree	Type
0	Included
1	Included
2	Included

Below the table, there is an 'OID Sub Tree' input field and a 'Type' dropdown menu set to 'Included'. At the bottom, there are buttons for 'Refresh', 'Add', 'Edit', 'Delete', and 'Help'.

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.

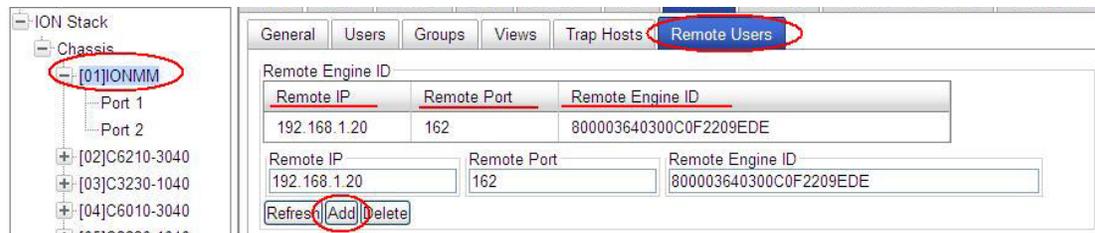
18. Select the **Remote Users** sub-tab.

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.

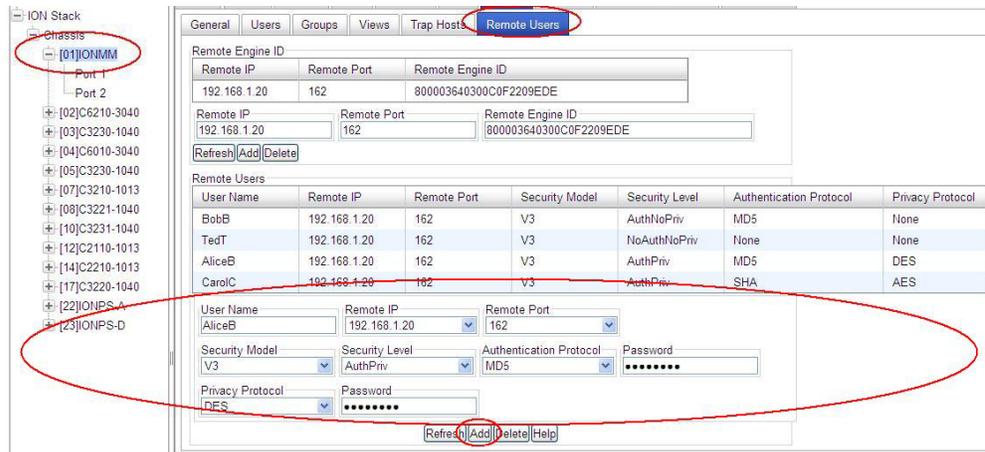
Remote Port: enter the UDP port number to be used by the trap manager (e.g., port number 162).

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.

The screenshot shows the IONMM web interface. On the left, the 'ION Stack' tree is visible, with '[01]IONMM' selected. The main area displays the 'Users' tab. A table lists users with columns: User Name, Group Name, Security Model, Security Level, Authentication Protocol, and Privacy Protocol. The user 'AndersonT' is highlighted in blue, with its Group Name 'comm_1' circled in red. Below the table, the 'User Name' field is 'AndersonT' and the 'Group Name' dropdown is set to 'private', also circled in red. The 'Change Group' button at the bottom right is circled in red.

User Name	Group Name	Security Model	Security Level	Authentication Protocol	Privacy Protocol
BobB	private	V3	AuthPriv	MD5	DES
TedT		V3	NoAuthNoPriv	None	None
JeffS	private	V3	AuthPriv	SHA	AES
CarolC		V3	AuthPriv	SHA	AES
GomesD		V3	AuthPriv	SHA	AES
AndersonT	comm_1	V3	AuthNoPriv	SHA	None

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

The screenshot shows the IONMM web interface after the user 'AndersonT' has been moved to the 'private' group. The 'Group Name' field is now 'private'. The 'Change Group' button is circled in red.

User Name	Group Name	Security Model	Security Level	Authentication Protocol	Privacy Protocol
BobB	private	V3	AuthPriv	MD5	DES
TedT		V3	NoAuthNoPriv	None	None
JeffS	private	V3	AuthPriv	SHA	AES
CarolC		V3	AuthPriv	SHA	AES
GomesD		V3	AuthPriv	SHA	AES
AndersonT	private	V3	AuthNoPriv	SHA	None

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	<p>“80 00 03 64 03 00 c0 f2 xx xx xx”.</p> <p>“03 64” is the enterprise number of Lantronix. “00 c0 f2 xx xx xx” is the MAC address of an ION device.</p> <p>For example: “800003640300C0F2209EDE”.</p>
SNMP Users sub-tab	
User Name	ION
Group Name	Default Group
Security Model	v1/v2c
Security Level	AuthNoPriv
Authentication Protocol	blank
Authentication Password	blank
Privacy Protocol	blank
Privacy Password	blank
SNMP Groups sub-tab	
Group Name	blank / Default Group / Test Group
Security Model	blank / V3 / V2
Security Level	NoAuthNoPriv
Read View	defaultView
Write View	defaultView
Notify View	defaultView
SNMP Views sub-tab	
View Name	defaultView
OID Subtree List	blank / “Click To See Detail ...”
Actions	blank
OID Subtree	blank
Type	Included

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

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.

Example of ION SNMP Operation

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

Entity	Physical Index
[0] ION219	134217728
[7] C4120	164626432
[9] C6210	173015040
[16] IONMM	202375168
[23] IONPS-AL	231735296

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.

4 Operation

General

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 of 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 to enter a “**show card info**” CLI command to view the SIC card’s current configuration before a backup/restore operation to verify the desired configuration settings. There are several CLI **show** commands that allow you to display (show) information about 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:** starting at ION v 1.3.10, Backup file name and TFTP upload/download file name are extended to a maximum of 128 characters.

For information on the status of important ION system files resulting from this operation, see “[Appendix D: 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 [Release Notes](#).

Backing Up the Configuration

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 actually 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.

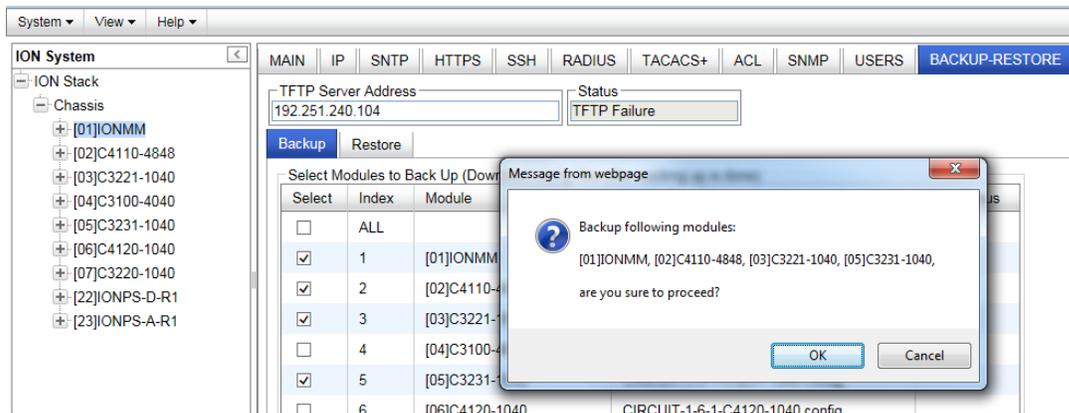
Select	Index	Module	Config File (Click to Modify)	Prov Status
<input type="checkbox"/>	ALL			
<input type="checkbox"/>	1	[01]IONMM	CIRCUIT-1-1-IONMM.config	
<input type="checkbox"/>	2	[02]C4110-4848	CIRCUIT-1-2-1-C4110-4848.config	
<input type="checkbox"/>	3	[03]C3221-1040	CIRCUIT-1-3-1-C3221-1040.config	
<input type="checkbox"/>	4	[04]C3100-4040	CIRCUIT-1-4-1-C3100-4040.config	
<input type="checkbox"/>	5	[05]C3231-1040	CIRCUIT-1-5-1-C3231-1040.config	
<input type="checkbox"/>	6	[06]C4120-1040	CIRCUIT-1-6-1-C4120-1040.config	
<input type="checkbox"/>	7	[07]C3220-1040	CIRCUIT-1-7-1-C3220-1040.config	
<input type="checkbox"/>	8	[22]ONPS-D-R1	CIRCUIT-1-22-1-ONPS-D-R1.config	
<input type="checkbox"/>	9	[23]ONPS-A-R1	CIRCUIT-1-23-1-ONPS-A-R1.config	

3. In the TFTP Server Address field, enter a valid IPv4 or IPv6 address (e.g., 192.168.1.30) or a valid IPv6 address (e.g., fe80::2c0:f2ff:fe20:de9e).
4. Verify that the TFTP Server address shown is correct, that the TFTP Server is running and configured, and that the file to be downloaded is located correctly (e.g., at `C:\TFTP-Root`).
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
<ol style="list-style-type: none"> a) In the Config File column, click the file name. b) Type a new name for the backup file. Note: the file name must be 1–63 characters long and must end with .config. c) Continue with step 8 below. 	Continue with step 8 below.

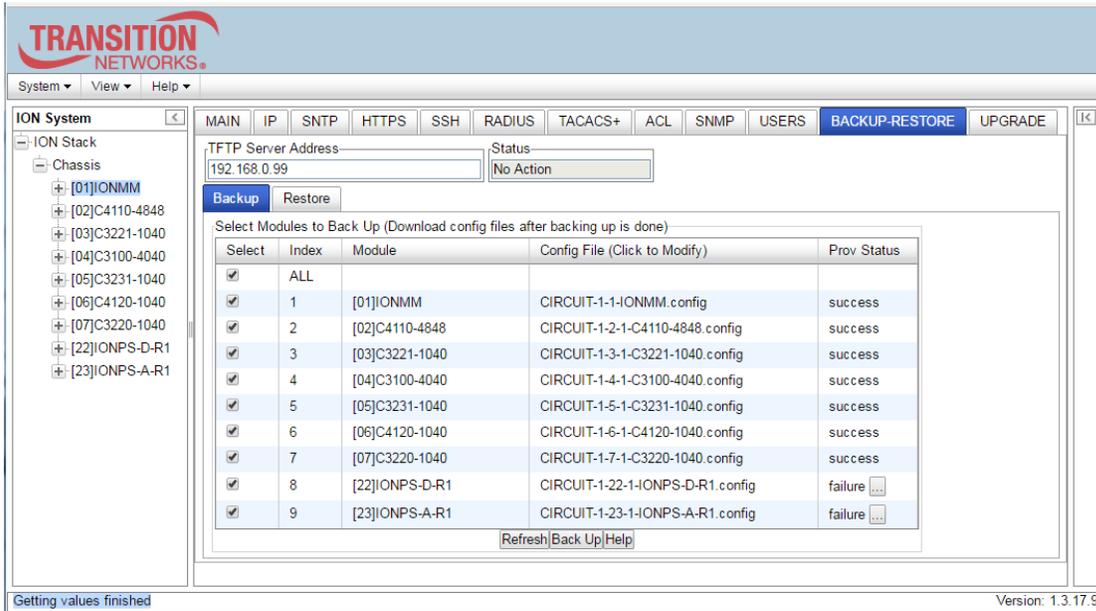
9. Click the **Back Up** button. The message “*Backup is being processed ...*” displays. The Back Up operation can take several minutes.
10. When the confirmation window displays, click **OK**. The backup file is saved in the IONMM.



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 Server:
 - a. Make sure the TFTP Server is running and configured.
 - b. In the **TFTP Server Address** field, enter the IP address of the server.
 - c. Click the **Download** button. The message “*File is being transferred*” displays.
 - d. When the successful completion message displays, click **OK**. The TFTP Server now contains an emergency backup file for the module specified.

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



The screenshot shows the 'Backup-Restore' tab in the ION System interface. The TFTP Server Address is set to 192.168.0.99. Below the table, there are buttons for 'Backup', 'Restore', 'Refresh', 'Back Up', and 'Help'.

Select	Index	Module	Config File (Click to Modify)	Prov Status
<input checked="" type="checkbox"/>	ALL			
<input checked="" type="checkbox"/>	1	[01]IONMM	CIRCUIT-1-1-IONMM.config	success
<input checked="" type="checkbox"/>	2	[02]C4110-4848	CIRCUIT-1-2-1-C4110-4848.config	success
<input checked="" type="checkbox"/>	3	[03]C3221-1040	CIRCUIT-1-3-1-C3221-1040.config	success
<input checked="" type="checkbox"/>	4	[04]C3100-4040	CIRCUIT-1-4-1-C3100-4040.config	success
<input checked="" type="checkbox"/>	5	[05]C3231-1040	CIRCUIT-1-5-1-C3231-1040.config	success
<input checked="" type="checkbox"/>	6	[06]C4120-1040	CIRCUIT-1-6-1-C4120-1040.config	success
<input checked="" type="checkbox"/>	7	[07]C3220-1040	CIRCUIT-1-7-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	8	[22]ONPS-D-R1	CIRCUIT-1-22-1-IONPS-D-R1.config	failure 
<input checked="" type="checkbox"/>	9	[23]ONPS-A-R1	CIRCUIT-1-23-1-IONPS-A-R1.config	failure 

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

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

- [Editing the Config File \(Optional\)](#) on page 153
- [Restoring the Configuration](#) on page 156

Backing Up 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.

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

3. In the **Select** column, check the checkbox of the module to be backed up.

4. Do you want to rename the backup file?

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

5. Click the **Back Up** button.6. When the confirmation window displays, click **OK**. The backup file is saved in the IONMM module.

7. To send a copy of the backup file to the TFTP server:

- a. Make sure the TFTP Server is running and configured.
- b. In the **TFTP Server Address** field, enter the IP address of the TFTP server.
- c. Click the **Download** button.
- d. When the successful completion message displays, click **OK**.

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

- [Editing the Config File \(Optional\)](#) on page 153
- [Restoring the Configuration](#) on page 156

Editing the Config File (Optional)

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

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

1. Complete the applicable Backup procedure from the previous section.
2. Open the Config file (in Notepad, WordPad, Word, OpenOffice Writer, etc.) from the TFTP server location (e.g., *C:\TFTP-Root\1-9-C3231-1040.config*).
3. Edit the Config file sections. Each Config file contains a DEVICE LEVEL CONFIG section and two PORT x CONFIG sections (three PORT x CONFIG sections for the model x3232 NIDs).
4. Save the edited Config file back to the TFTP 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 snmp-svr svr=1 type=dns addr=0.0.0.0
31 set snmp-svr svr=2 type=dns addr=0.0.0.0
32 set snmp-svr svr=3 type=dns addr=0.0.0.0
33 set snmp-svr svr=4 type=dns addr=0.0.0.0
34 set snmp-svr svr=5 type=dns addr=0.0.0.0
35 set snmp-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@transition.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
```

Restoring the Configuration

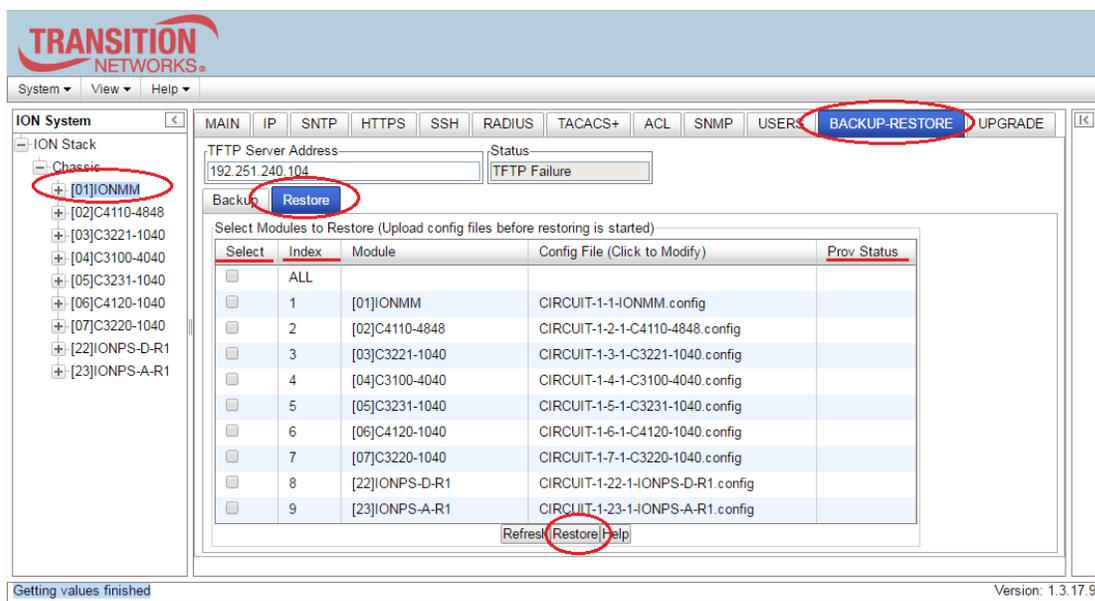
The following procedure describes how to restore the configuration of one or more modules in the ION system.

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

IMPORTANT

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

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.



The screenshot shows the IONMM web interface. The 'BACKUP-RESTORE' tab is selected in the top navigation bar. The 'Restore' sub-tab is also selected. The 'Modules to Restore' table is displayed, listing modules and their configuration files. The table has columns for Select, Index, Module, Config File (Click to Modify), and Prov Status. The first row is selected, and the 'Restore' button is circled in red.

Select	Index	Module	Config File (Click to Modify)	Prov Status
<input type="checkbox"/>	ALL			
<input type="checkbox"/>	1	[01]IONMM	CIRCUIT-1-1-IONMM.config	
<input type="checkbox"/>	2	[02]C4110-4848	CIRCUIT-1-2-1-C4110-4848.config	
<input type="checkbox"/>	3	[03]C3221-1040	CIRCUIT-1-3-1-C3221-1040.config	
<input type="checkbox"/>	4	[04]C3100-4040	CIRCUIT-1-4-1-C3100-4040.config	
<input type="checkbox"/>	5	[05]C3231-1040	CIRCUIT-1-5-1-C3231-1040.config	
<input type="checkbox"/>	6	[06]C4120-1040	CIRCUIT-1-6-1-C4120-1040.config	
<input type="checkbox"/>	7	[07]C3220-1040	CIRCUIT-1-7-1-C3220-1040.config	
<input type="checkbox"/>	8	[22]IONPS-D-R1	CIRCUIT-1-22-1-IONPS-D-R1.config	
<input type="checkbox"/>	9	[23]IONPS-A-R1	CIRCUIT-1-23-1-IONPS-A-R1.config	

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

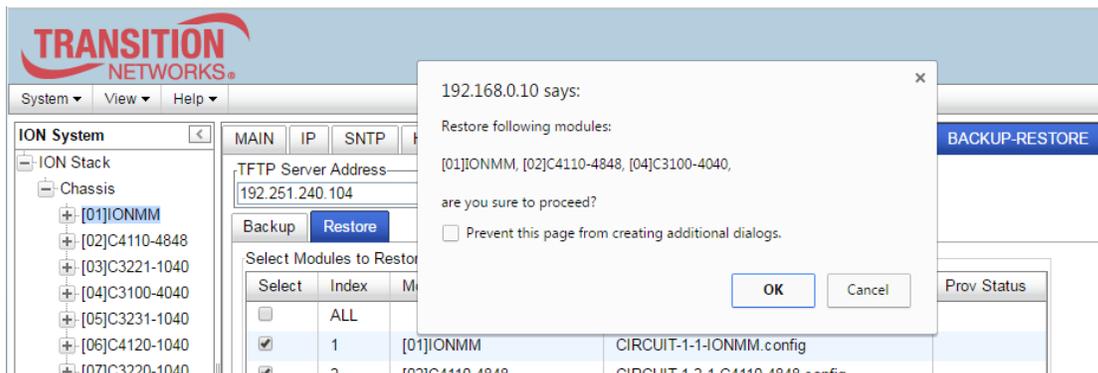
5. Is the configuration file to be restored different than the one shown in the Config File column?

Yes	No
a) In the Config File column, click the file name. b) Type the name of the backup file to be restored. Note: the file name must end with .config . c) Continue with Continue with step 6.	Continue with step 6 below.

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

Yes	No
a) In the TFTP Server Address field, enter the IP address of the server. b) Click Upload . c) When the successful transfer message displays, click OK . d) Continue with step 7.	Continue with step 7 below.

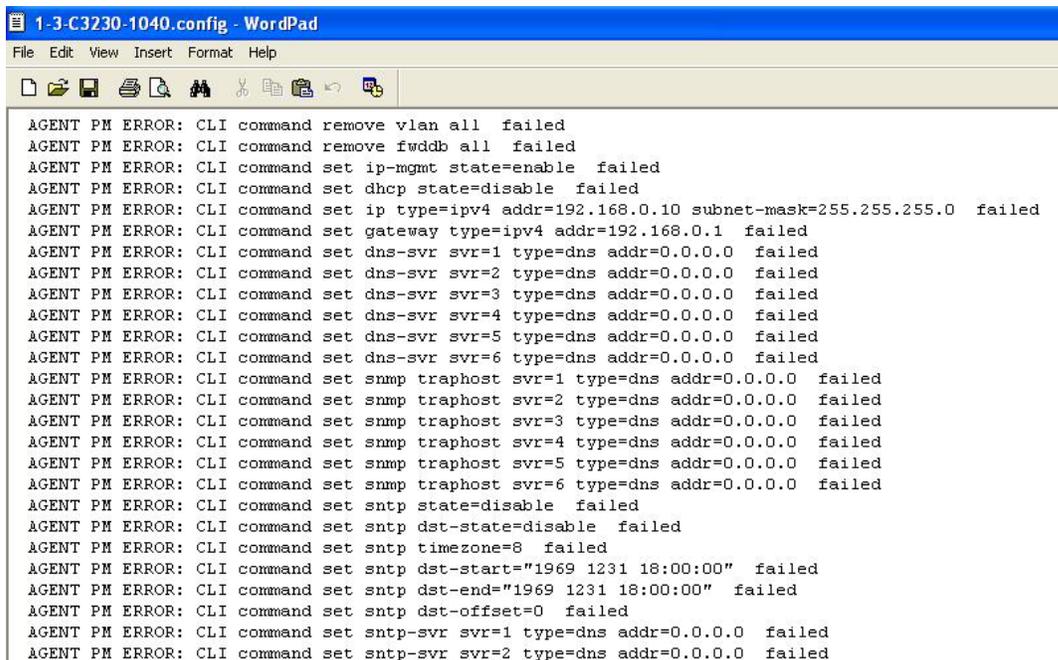
7. Click the **Upload** button. The config file is uploaded via the TFTP server. When done, the message “File has been successfully transferred via TFTP.”
8. Click the **OK** button to clear the Webpage confirmation message.



9. Click **Restore** button.
10. When the confirmation window displays, click **OK**. The configuration will be restored from the specified file. During the Restore operation the message “Restoring is being processed ...” displays, and the **Prov Status** column displays “ongoing”.
When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.
11. If the **Restore** operation fails, the **Prov Status** column displays  then click the box to download an error log from the device.

The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root, with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad or a text editor.

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



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

See “[The Config Error Log \(config.err\) File](#)” for error messages and possible recovery procedures.

Backup / Restore (Provisioning) - CLI Method

Access the NID through either a USB connection (see “Starting a USB Session”) or a 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                          success
2      [02]C6210-3040                          1-2-1-C6210-3040.config                    success
3      [02:L2]REM:S6210-3040                    1-2-2-S6210-3040.config                    success
4      [03]C3230-1040                          1-3-1-C3230-1040.config                    success
5      [04]C6010-3040                          1-4-1-C6010-3040.config                    success
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                    success
3      [02:L2]REM:S6210-3040                    1-2-2-S6210-3040.config                    success
4      [03]C3230-1040                          1-3-1-C3230-1040.config                    success
5      [04]C6010-3040                          1-4-1-C6010-3040.config                    success
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.

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 new Backup All and Restore All features can be configured via the ION System Web GUI or CLI commands. The new Backup/Restore feature provides Automatic TFTP 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 is 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.

CLI Commands

IONMM v 1.3.18 and above provides these commands for Backup and Restore:

- backup all
- backup module-list
- get restore module-list
- prov get tftp svr addr
- prov set tftp svr< type> <addr>
- restore <TFTP-FILENAME> all
- restore <TFTP-FILENAME> module-list <string>
- saveconf module-list
- show provision backup modules
- show provision restore modules

Backup and restore commands at IONMM 1.3.18 and above are described in the following sections.

Overview of Backup/Restore via the CLI

1. Set the TFTP address, enable SNTP, and set the SNTP server in the browser before beginning this BU/Restore.
2. Have the TFTP server running.
3. Enter the CLI command "**backup all**" to back up all modules in the chassis, create a time-stamped tarfile (*.tar), and transfer the tarfile file to your PC via TFTP.

Backup and Restore Procedure via CLI Commands

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>**".
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. See the related manual for details.
3. The "**backup all**" command finds all the cards in the chassis, backs up the configs in a time-stamped TAR file (*.tar), and TFTP's the file to the PC.

Note: When using the CLI to backup all or restore all, you must enter these commands first:

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 mod 2,4,5" or "backup mod 2,3,4,5". The selected cards will be backed up, time stamped, and transferred via TFTP to the PC.

5. The "**saveconf module-list <string>**" command will back up the configs to the *IONMM/tftpboot* directory only. No TFTP transfer occurs. This is exactly like the old command. See **Note 1** at the end of this procedure.

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.

```

Agent III C1|S19|L1D>backup module-list 4,8
::-> timeStamp = 20170201_09-35-12-AM
::-> tftpaddr = 192.168.0.61
Processing...
::-> rm /tftpboot/*.log
rm: cannot remove '/tftpboot/*.log': No such file or directory
::-> backup_20170201_09-35-12-AM.tar
::-> /bin/tar -cvf backup_20170201_09-35-12-AM.tar /tftpboot
tar: removing leading '/' from member names
tftpboot/
tftpboot/GP-1-7-1-C3230-1040.config      Index 8
tftpboot/GP-1-15-1-C3210-1040.config
tftpboot/GP-1-22-1-IONPS-A-R1.config.err
tftpboot/GP-1-9-1-C2220-1014.config
tftpboot/GP-1-1-1-C3220-1040.config.err
tftpboot/GP-1-1-1-C3220-1040.config
tftpboot/rlist.txt
tftpboot/GP-1-4-1-C3230-1040.config
tftpboot/GP-1-19-1-IONMM.config
tftpboot/GP-1-14-1-C4110-4848.config.err
tftpboot/GP-1-2-1-C3220-1040.config
tftpboot/GP-1-13-1-C3231-1040.config
tftpboot/GP-1-11-1-C6210-3040.config
tftpboot/GP-1-6-1-C3221-1040.config
tftpboot/GP-1-5-1-C3230-1040.config
tftpboot/GP-1-12-1-C6010-3040.config
tftpboot/GP-1-17-1-C3210-1013.config
tftpboot/GP-1-14-1-C4110-4848.config
tftpboot/GP-1-3-1-C3220-1040.config      Index 4
tftpboot/GP-1-16-1-C3220-1040.config
tftpboot/GP-1-22-1-IONPS-A-R1.config
tftpboot/GP-1-8-1-C3220-1014.config
tftpboot/GP-1-10-1-C3110-1040.config
tftpboot/moduleLength.bin
::-> tftp -l backup_20170201_09-35-12-AM.tar -p 192.168.0.61

Backup finished
Agent III C1|S19|L1D>_

```

Backup and Restore CLI Command Descriptions

Command: Backup All Chassis Cards

Syntax: **backup all**

Description: The "backup all" command finds all the cards in the chassis, backs up the configs in a time-stamped TAR file (*.tar), and sends the file to the PC via TFTP. **Note:** you must first set the TFTP server address using the command "**prov set tftp svr type ipv4 addr <TFTP IP>**".

Example: Set the TFTP server address using the command "**prov set tftp svr type ipv4 addr <TFTP IP>**". Then do a **backup all**.

```

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>

```

Example: A successful 24 module backup by the CLI and the related tarfile:

```

Agent III C1|S19|L1D>show prov bac mod
Index  Module                               Config File
-----
1      [00]                                     SHIVA-1-1-0-0-backplane.config
2      [01]                                     SHIVA-2-1-1-1-C3210-1040.config
3      [02]                                     SHIVA-3-1-2-1-C3220-1040.config
4      [03]                                     SHIVA-4-1-3-1-C3220-1014.config
5      [04]                                     SHIVA-5-1-4-1-C2110-1040.config
6      [05]                                     SHIVA-6-1-5-1-C3220-1040.config
7      [06]                                     SHIVA-7-1-6-1-C3221-1040.config
8      [07]                                     SHIVA-8-1-7-1-C3220-1014.config
9      [08]                                     SHIVA-9-1-8-1-C3231-1040.config
10     [09]                                     SHIVA-10-1-9-1-C3220-1040.config
11     [09:L2]REM:                             SHIVA-11-1-9-2-C3230-1040.config
12     [10]                                     SHIVA-12-1-10-1-C3230-1040.config
13     [10:L2]REM:                             SHIVA-13-1-10-2-C3220-1040.config
14     [11]                                     SHIVA-14-1-11-1-C3220-1014.config
15     [12]                                     SHIVA-15-1-12-1-C3220-1040.config
16     [12:L2]REM:                             SHIVA-16-1-12-2-C3220-1040.config
17     [13]                                     SHIVA-17-1-13-1-C6010-3040.config
18     [14]                                     SHIVA-18-1-14-1-C3220-1040.config
19     [15]                                     SHIVA-19-1-15-1-C4110-4848.config
20     [16]                                     SHIVA-20-1-16-1-C3230-1040.config
21     [17]                                     SHIVA-21-1-17-1-C3220-1040.config
22     [17:L2]REM:                             SHIVA-22-1-17-2-C3220-1040.config
23     [19]                                     SHIVA-23-1-19-1-IONMM.config
24     [23]                                     SHIVA-24-1-23-1-IONPS-A.config

Agent III C1|S19|L1D>backup all
::--> timeStamp = 20170405_07-15-31-AM
::--> tftpaddr = 192.168.0.61
::--> xm -f /tftpboot/*
==> Found all chassis cards <==

::--> backupname = SHIVA_backup_20170405_07-15-31-AM.tar
::--> backupModuleIndex = 24
::--> backupCommand = 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
Processing...
.....
Backup finished
Agent III C1|S19|L1D>_

```

Name	Size	Modified
SHIVA-9-1-8-1-C3231-1040.config	12,510	4/5/2017 8:17 AM
SHIVA-8-1-7-1-C3220-1014.config	10,354	4/5/2017 8:16 AM
SHIVA-7-1-6-1-C3221-1040.config	12,382	4/5/2017 8:16 AM
SHIVA-6-1-5-1-C3220-1040.config	10,372	4/5/2017 8:16 AM
SHIVA-5-1-4-1-C2110-1040.config	263	4/5/2017 8:16 AM
SHIVA-4-1-3-1-C3220-1014.config	10,342	4/5/2017 8:16 AM
SHIVA-3-1-2-1-C3220-1040.config	10,376	4/5/2017 8:16 AM
SHIVA-24-1-23-1-IONPS-A.config	2,793	4/5/2017 8:18 AM
SHIVA-23-1-19-1-IONMM.config	3,135	4/5/2017 8:18 AM
SHIVA-22-1-17-2-C3220-1040.config	10,412	4/5/2017 8:19 AM
SHIVA-2-1-1-1-C3210-1040.config	2,241	4/5/2017 8:15 AM
SHIVA-21-1-17-1-C3220-1040.config	10,368	4/5/2017 8:18 AM
SHIVA-20-1-16-1-C3230-1040.config	10,407	4/5/2017 8:18 AM
SHIVA-19-1-15-1-C4110-4848.config	256	4/5/2017 8:18 AM
SHIVA-18-1-14-1-C3220-1040.config	10,383	4/5/2017 8:18 AM
SHIVA-17-1-13-1-C6010-3040.config	237	4/5/2017 8:17 AM
SHIVA-16-1-12-2-C3220-1040.config	10,367	4/5/2017 8:18 AM
SHIVA-15-1-12-1-C3220-1040.config	10,414	4/5/2017 8:17 AM
SHIVA-14-1-11-1-C3220-1014.config	257	4/5/2017 8:17 AM
SHIVA-13-1-10-2-C3220-1040.config	10,397	4/5/2017 8:18 AM
SHIVA-12-1-10-1-C3230-1040.config	10,454	4/5/2017 8:17 AM
SHIVA-11-1-9-2-C3230-1040.config	10,440	4/5/2017 8:17 AM
SHIVA-1-1-0-0-backplane.config	53	4/5/2017 8:15 AM
SHIVA-10-1-9-1-C3220-1040.config	10,405	4/5/2017 8:17 AM
backup_rlist.bin	3,360	4/5/2017 8:18 AM

Command: Backup Module-list

Syntax: **backup module-list** <string>

Description: The "backup module-list <string>" command will back up a selected set of SICs, where the <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 backup.

Example 1: Back up specified set of modules successful:

```
Agent III C1|S1|L1D>backup ?
  all
  module-list
Agent III C1|S1|L1D>backup module-list ?
  STR_MODULE_LIST
Agent III C1|S1|L1D>backup module-list 1,2 ?
  <cr>
Agent III C1|S1|L1D>backup module-list 3-5
::-> timeStamp = 19700106_11-57-23-AM
::-> tftpaddr = 192.168.0.61
::-> rm -f /tftpboot/*
==> Found all chassis cards <==

::--> backupname = SN101829_backup_19700106_11-57-23-AM.tar
::--> backupModuleIndex = 18
Processing...
==> prov_info[2].prov_cfg[x].entryStatus = 1
==> prov_info.prov_cfg[2].ent_index = 8900000
==> prov_info.prov_cfg[2].backup_file = SN101829-3-1-2-1-C4110-4848.config

Processing...
::-> prov_info.prov_cfg[val_array[0]-1].ent_index = 8900000
.
Backup finished
Agent III C1|S1|L1D>
```

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.



Command: Get Restore module-list**Syntax: get restore module-list**

Description: Get restore specified provision modules.

You can enter a comma-separated list (e.g., 1,2,3,4 with no spaces between module numbers) or a range (e.g., 1-4) of module numbers.

Example:

```
Agent III C1|S1|L1D>get ?
  restore
Agent III C1|S1|L1D>get restore ?
  module-list
Agent III C1|S1|L1D>get restore module-list ?
  STR_MODULE_LIST
Agent III C1|S1|L1D>get restore module-list 1,2 ?
  <cr>
Agent III C1|S1|L1D>get restore module-list 1,2
::-> tftpaddr = 1,2
Processing...

Restore finished
Agent III C1|S1|L1D>get restore module-list 1-4
::-> tftpaddr = 1-4
Processing...

Restore finished
Agent III C1|S1|L1D>
Agent III C1|S1|L1D>get restore module-list 1, 2, 3, 4
% Unknown command.
Agent III C1|S1|L1D>get restore module-list 1,2,3,4
::-> tftpaddr = 1,2,3,4
Processing...

Restore finished
Agent III C1|S1|L1D>get restore module-list 1-4 ?
  <cr>
Agent III C1|S1|L1D>get restore module-list 1-4
::-> tftpaddr = 1-4
Processing...
Error: cannot get backplane stack name!
Agent III C1|S1|L1D>get restore module-list 3-5
::-> tftpaddr = 3-5
Processing...
Error: cannot get backplane stack name!
Agent III C1|S1|L1D>
```

Command: Provision Get TFTP Server AddressSyntax: **prov get tftp svr addr**

Description: Get the current TFTP server IP address.

Example: Get the current TFTP server IP address:

```
Agent III C1|S1|L1D>pr?
  prov  Get current TFTP server address.
Agent III C1|S1|L1D>pr ?
  get
  set
Agent III C1|S1|L1D>pr get ?
  get
Agent III C1|S1|L1D>pr get ?
  tftp
Agent III C1|S1|L1D>pr get tftp ?
  svr
Agent III C1|S1|L1D>pr get tftp svr ?
  addr
Agent III C1|S1|L1D>pr get tftp svr addr ?
  <cr>
Agent III C1|S1|L1D>pr get tftp svr addr
**-> In Get TFTP SVR
**-> File descriptor: 0
**-> vty connection 0=term, 1=file, 2=shell, 3=shell_serv: 2
**-> vty status 0=norm, 1=close, 2=more, 3=moreline, 4=start, 5=cont: 0
**-> vty node status: 1
**-> vty addr from: (null)
**-> vty in config mode: 0
**-> vty location-chassis: 1
**-> vty location-slot: 1
**-> vty location-l0ap: 0
**-> vty location-l1ap: 0
::-> get prov tftp svr addr: 192.168.0.61
Agent III C1|S1|L1D>
```

Command: Provision Set TFTP Server Type**Syntax:** `prov set tftp svr type x addr xx`**Description:** Set the TFTP server IP address.**Note:** If you log out of the CLI and log back on, you must set the TFTP server IP again with "prov set tftp svr type ipv4 addr <tftp ip>".**Example:** Get the current TFTP Server IP address, change it, and then get it again to verify that it was changed:

```
Agent III C1|S1|L1D>pr get tftp svr addr
**-> In Get TFTP SVR
**-> File descriptor: 0
**-> vty connection 0=term, 1=file, 2=shell, 3=shell_serv: 2
**-> vty status 0=norm, 1=close, 2=more, 3=moreline, 4=start, 5=cont: 0
**-> vty node status: 1
**-> vty addr from: (null)
**-> vty in config mode: 0
**-> vty location-chassis: 1
**-> vty location-slot: 1
**-> vty location-l0ap: 0
**-> vty location-l1ap: 0
::-> get prov tftp svr addr: 192.168.0.61
Agent III C1|S1|L1D>prov set tftp svr type ipv4 addr 192.251.240.104
Agent III C1|S1|L1D>pr get tftp svr addr
**-> In Get TFTP SVR
**-> File descriptor: 0
**-> vty connection 0=term, 1=file, 2=shell, 3=shell_serv: 2
**-> vty status 0=norm, 1=close, 2=more, 3=moreline, 4=start, 5=cont: 0
**-> vty node status: 1
**-> vty addr from: (null)
**-> vty in config mode: 0
**-> vty location-chassis: 1
**-> vty location-slot: 1
**-> vty location-l0ap: 0
**-> vty location-l1ap: 0
::-> get prov tftp svr addr: 192.251.240.104
Agent III C1|S1|L1D>
```

Command: Restore All

Syntax: **restore** <TFTP-FILENAME> **all**

Description: Restore all of the ION SIC modules. Send the named TAR file via TFTP to the IONMM and write the config files to the ION cards. This assumes that the cards' model numbers (e.g., C3220-1014) and slot numbers are the same as those in the TAR file.

Example:

```
Agent III C1|S1|L1D>restore all ?
  all
  module-list
Agent III C1|S1|L1D>restore all all
backupname = all
::-> tftpaddr = 192.251.240.104
::-> tftp -r all -g 192.251.240.104
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: last timeout
::-> tar -xvf all -C /tftpboot .
tar: all: No such file or directory
::-> restoreCommand = 2,3,4,5,6,7,8,9,10
Processing...
::-> Restore file name: CIRCUIT-1-1-1-IONMM.config
::-> Restore file name: CIRCUIT-1-2-1-C4110-4848.config
::-> Restore file name: CIRCUIT-1-3-1-C3221-1040.config
::-> Restore file name: CIRCUIT-1-4-1-C3100-4040.config
::-> Restore file name: CIRCUIT-1-5-1-C3231-1040.config
::-> Restore file name: CIRCUIT-1-6-1-C4120-1040.config
::-> Restore file name: CIRCUIT-1-7-1-C3220-1040.config
::-> Restore file name: CIRCUIT-1-22-1-IONPS-D-R1.config
::-> Restore file name: CIRCUIT-1-23-1-IONPS-A-R1.config
.....
Restore finished
Agent III C1|S1|L1D>
```

Message: *tar: all: No such file or directory* or *tar: Namestr: No such file or directory*

Meaning: The CLI indicates the Restore finished; however, the Restore was not successful.

Recovery: Make sure the TFTP server is up and running and that the file exists and is properly named.

Command: Restore <TFTP-FILENAME> module-list <string>

Syntax: restore <TFTP-FILENAME> module-list <string>

Description: Restore the specified provision modules. Note that you must first run the command '**show provision backup modules**' to see the list of modules to choose from. The parameters are:

TFTP-FILENAME = enter the file name of a backup file that resides on the TFTP server.

module-list = enter the Index number next to the cards (not the slot number or model number).

Example: Restore a set of specified modules successfully:

```
Agent III C1|S1|L1D>restore all module-list ?
STR_MODULE_LIST
Agent III C1|S1|L1D>restore all module-list 2,3,4,5
==> Found all chassis cards <==

::-> tftpaddr = 192.168.0.61
::-> tftp -r all -g 192.168.0.61
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: timeout
tftp: last timeout
::-> tar -xf all -C /tftpboot .
tar: all: No such file or directory
Read complete
==> prov_info[2].prov_cfg[x].entryStatus = 1
==> prov_info.prov_cfg[2].ent_index = 8900000
==> prov_info.prov_cfg[2].restore_file = SN101829-3-1-2-1-C4110-4848.config.conf
ig

Processing...
::-> prov_info.prov_cfg[1].restore_file =

::-> prov_info.prov_cfg[2].restore_file = SN101829-3-1-2-1-C4110-4848.config.conf
fig

.....
Restore finished
Agent III C1|S1|L1D>
```

Command: Saveconf Module-list

Syntax: **saveconf module-list** <string>

Description: Backup the specified provision modules to the IONMM. The "**saveconf module-list** <string>" command will back up the configs to the *IONMM/tftpboot* directory only (no TFTP transfer is performed).

Example:

```
Agent III C1|S1|L1D>save ?
  module-list
Agent III C1|S1|L1D>save module-list ?
  STR_MODULE_LIST
Agent III C1|S1|L1D>save module-list 1-17 ?
  <cr>
Agent III C1|S1|L1D>save module-list 1-17
==> Found all chassis cards <==

Processing...
...
Backup finished
Agent III C1|S1|L1D>
```

Command: Show Provision Backup Modules

Syntax: **show provision backup modules**

Description: Show all modules in the chassis that can be backed up. When using the command "backup module-list <string>", the <string> is the index of the cards separated by commas. To get the indexes, use the command "show prov backup modules", then select which index matches the cards you want to back up.

Example:

```
Agent III C1|S1|L1D>show provision backup modules
Index  Module                Prov Status          Config File
-----
-----
1      [00]                   CIRCUI-1-1-0-0-backplane.config
2      [01]                   CIRCUI-2-1-1-1-IONMM.config          success
3      [02]                   CIRCUI-3-1-2-1-C4110-4848.config    success
4      [03]                   CIRCUI-4-1-3-1-C3221-1040.config    success
5      [04]                   CIRCUI-5-1-4-1-C3100-4040.config
7      [07]                   CIRCUI-7-1-7-1-C3220-1040.config
8      [08]                   CIRCUI-8-1-8-1-C2210-1013.config
9      [09]                   CIRCUI-9-1-9-1-C2110-1013.config
10     [10]                   CIRCUI-10-1-10-1-S6120-1013.config
11     [12]                   CIRCUI-11-1-12-1-C3230-1040.config
12     [13]                   CIRCUI-12-1-13-1-C6010-3040.config
13     [14]                   CIRCUI-13-1-14-1-C6210-3040.config
14     [15]                   CIRCUI-14-1-15-1-C3220-1040.config
15     [16]                   CIRCUI-15-1-16-1-C2220-1014.config
16     [17]                   CIRCUI-16-1-17-1-C3220-1013.config
17     [23]                   CIRCUI-17-1-23-1-IONPS-A-R1.config
Agent III C1|S1|L1D>
```

Command: Show Provision Restore modulesSyntax: **show provision restore modules**

Description: Show all modules in the chassis that can be restored. When using the command "restore module-list <string>" the <string> is the index of the cards separated by commas. To get the indexes, use the command "show prov restore modules", and then select which index matches the cards you want to back up.

Example:

```
Agent III C1|S1|L1D>show prov restore modules
Index  Module                Prov Status                Config File
-----
1      [00]                    CIRCUI-1-1-0-0-backplane.config
2      [01]                    CIRCUI-2-1-1-1-IONMM.config
3      [02]                    CIRCUI-3-1-2-1-C4110-4848.config
4      [03]                    CIRCUI-4-1-3-1-C3221-1040.config
5      [04]                    CIRCUI-5-1-4-1-C3100-4040.config
6      [05]                    CIRCUI-6-1-5-1-C3231-1040.config
7      [07]                    CIRCUI-7-1-7-1-C3220-1040.config
8      [08]                    CIRCUI-8-1-8-1-C2210-1013.config
9      [09]                    CIRCUI-9-1-9-1-C2110-1013.config
10     [10]                    CIRCUI-10-1-10-1-S6120-1013.config
11     [12]                    CIRCUI-11-1-12-1-C3230-1040.config
12     [13]                    CIRCUI-12-1-13-1-C6010-3040.config
13     [14]                    CIRCUI-13-1-14-1-C6210-3040.config
14     [15]                    CIRCUI-14-1-15-1-C3220-1040.config
15     [16]                    CIRCUI-15-1-16-1-C2220-1014.config
16     [17]                    CIRCUI-16-1-17-1-C3220-1013.config
17     [23]                    CIRCUI-17-1-23-1-IONPS-A-R1.config
Agent III C1|S1|L1D>
```

Message: <Restore failed, but no message displayed>

Meaning: When a restore is attempted via CLI and fails, you can run 'show provision restore modules' to see which modules failed to properly restore, but there is no way for you to get the config.err files from the IONMM to see what part(s) of the restore failed.

Recovery: From the IONMM CLI, enter the command **ls -l /tftpboot**, then enter **cat /tftpboot/configfile.err** to read the contents of the error file.

Example:

```
Agent III C1|S1|L1D>ls -l /tftpboot
-rw-r--r--  1 root  root           0 Dec 31 19:13 1-1-0-0-backplane.config
-rw-r--r--  1 root  root        211 Dec 31 20:23 1-1-0-0-backplane.config.err
-rw-r--r--  1 root  root        249 Dec 31 19:16 10-1-9-1-C2110-1013.config
-rw-r--r--  1 root  root         65 Dec 31 19:57 10-1-9-1-C2110-1013.config.err
-rw-r--r--  1 root  root       1022 Dec 31 19:16 11-1-10-1-S6120-1013.config
-rw-r--r--  1 root  root      10626 Dec 31 19:16 12-1-12-1-C3230-1040.config
-rw-r--r--  1 root  root        213 Dec 31 19:58 12-1-12-1-C3230-1040.config.err
-rw-r--r--  1 root  root        185 Dec 31 19:17 13-1-13-1-C6010-3040.config
-rw-r--r--  1 root  root        179 Dec 31 19:17 14-1-14-1-C6210-3040.config
-rw-r--r--  1 root  root      10365 Dec 31 19:17 15-1-15-1-C3220-1040.config
-rw-r--r--  1 root  root        132 Dec 31 19:59 15-1-15-1-C3220-1040.config.err
-rw-r--r--  1 root  root       1013 Dec 31 19:17 16-1-16-1-C2220-1014.config
-rw-r--r--  1 root  root        213 Dec 31 20:00 16-1-16-1-C2220-1014.config.err
-rw-r--r--  1 root  root      10331 Dec 31 19:18 17-1-17-1-C3220-1013.config
-rw-r--r--  1 root  root        224 Dec 31 19:18 18-1-18-1-C4120-1048.config
-rw-r--r--  1 root  root       2245 Dec 31 19:18 19-1-23-1-IONPS-A-R1.config
-rw-r--r--  1 root  root        108 Dec 31 20:01 19-1-23-1-IONPS-A-R1.config.err
```

```
-rw-r--r-- 1 root root 3130 Dec 31 19:13 2-1-1-IONMM.config
-rw-r--r-- 1 root root 167 Dec 31 19:14 3-1-2-1-C4110-4848.config
-rw-r--r-- 1 root root 124 Dec 31 20:24 3-1-2-1-C4110-4848.config.err
-rw-r--r-- 1 root root 12583 Dec 31 19:14 4-1-3-1-C3221-1040.config
-rw-r--r-- 1 root root 149 Dec 31 19:14 5-1-4-1-C3100-4040.config
-rw-r--r-- 1 root root 12803 Dec 31 19:15 6-1-5-1-C3231-1040.config
-rw-r--r-- 1 root root 207 Dec 31 19:54 6-1-5-1-C3231-1040.config.err
-rw-r--r-- 1 root root 225 Dec 31 19:15 7-1-6-1-C3110-1040.config
-rw-r--r-- 1 root root 10394 Dec 31 19:15 8-1-7-1-C3220-1040.config
-rw-r--r-- 1 root root 257 Dec 31 19:15 9-1-8-1-C2210-1013.config
-rw-r--r-- 1 root root 384 Dec 31 19:56 9-1-8-1-C2210-1013.config.err
-rw-r--r-- 1 root root 107520 Dec 31 19:18 _backup_19691231_07-18-33-PM.tar
-rw-r--r-- 1 root root 2660 Dec 31 19:18 backup_rlist.bin
Agent III C1|S1|L1D>
Agent III C1|S1|L1D>cat /tftpboot/configfile.err
cat: /tftpboot/configfile.err: No such file or directory
/tftpboot/configfile.errAgent III C1|S1|L1D>
```

Other Helpful CLI Commands

Command: Show Card Information

Syntax: **show card info**

Example: Display the IONMM (or any other card) details:

```
Agent III C1|S1|L1D>show card info
System name:      Agent III
Uptime:           3 days, 20:14:45
CPU MAC:          00-c0-f2-20-e9-39
Number of ports:  2
Serial number:    11633907
Config mode:      software
Software:         1.3.2011
Bootloader:       1.2.1

Hardware:         1.0.0
Agent III C1|S1|L1D>go c=1 s=3 l1d
Agent III C1|S3|L1D>show card info
System name:      C3221-1040
Uptime:           6 days, 15:58:52
CPU MAC:          00-c0-f2-21-14-18
Port number:      3
Serial number:    11714306
Config mode:      software
Software:         1.3.18
Bootloader:       1.2.1

Hardware:         1.0.0
Agent III C1|S3|L1D>
```

Command: Show System Information

Syntax: **show system info**

Example: Display the IONMM (or any other card) details:

```
Agent III C1|S3|L1D>show system info
system descr:      The C3221-1040 of the Transition networks ION
(Chassis Generation III) platform products
system objectID:   1.3.6.1.4.1.868.2.5.1802661751
system uptime:     2 days, 21:42:31
system contact:    Lantronix(techsupport@transition.com)
system name:       C3221-1040
system location:   10900 Red Circle Drive  Minnetonka, MN 55343
USA
Agent III C1|S3|L1D>home
Agent III C1|S1|L1D>show system info
system descr:      The management module of the Transition
networks ION (Chassis Generation III) platform products
system objectID:   1.3.6.1.4.1.868.2.5.544108393
system uptime:     02:46:06
system contact:    Lantronix(techsupport@transition.com)
system name:       Agent III
system location:   10900 Red Circle Drive  Minnetonka, MN 55343
USA
```

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

Command: Show Firmware-db Update Result

Syntax: **show firmware-db update result**

Example:

```
Agent III C1|S1|L1D>show firmware-db update result
Database file name:
Database update result:      none
Agent III C1|S1|L1D>
```

Command: Show Firmware Upgrade Result

Syntax: **show firmware upgrade result**

Example:

```
Agent III C1|S1|L1D>show firmware upgrade result
index module      status      reason      time started      time completed
-----
1                00:00:00      00:00:00
2                00:00:00      00:00:00
3                00:00:00      00:00:00
4                00:00:00      00:00:00
5                00:00:00      00:00:00
6                00:00:00      00:00:00
7                00:00:00      00:00:00
8                00:00:00      00:00:00
Agent III C1|S1|L1D>
```

Command: Show Upgrade Firmware File

Syntax: **show upgrade firmware file**

Example:

```
Agent III C1|S1|L1D>show upgrade ?
firmware
Agent III C1|S1|L1D>show upgrade firmware ?
file
Agent III C1|S1|L1D>show upgrade firmware file ?
<cr>
Agent III C1|S1|L1D>show upgrade firmware file
No upgrade firmware files now!
Agent III C1|S1|L1D>
```

Backup All and Restore All CLI 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:

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; see "[Contact Us](#)" below.

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.conf
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.conf
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

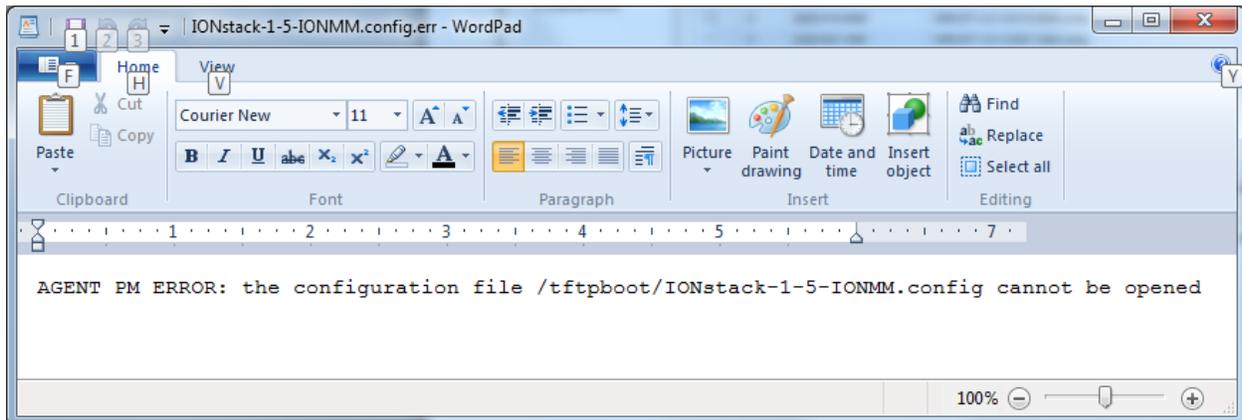
::-> array_len = 6
Processing...
::-> prov_cfg[val_array[0]-1].ent_index = 8500000
::-> Restore file name: CIRCUIT-1-1-1-1-IONMM.config
      Failed to set ION_PROV_TARFILE.2
::-> prov_cfg[val_array[1]-1].ent_index = 8D00000
::-> Restore file name: CIRCUIT-2-1-3-1-C3221-1040.config
::-> prov_cfg[val_array[2]-1].ent_index = 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>
```

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

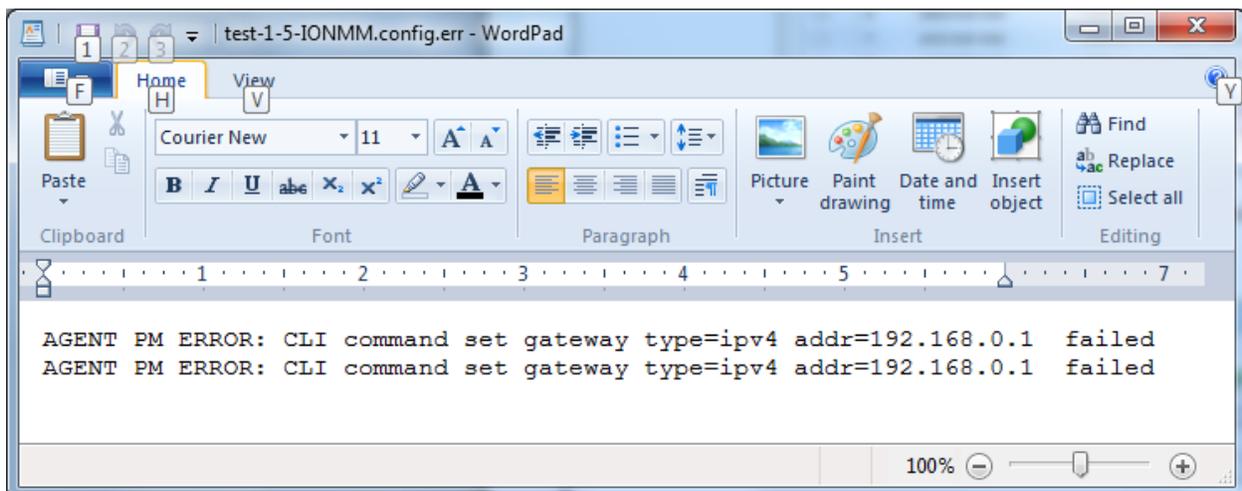


Meaning: The config file has a problem.

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; see "Contact Us" below.

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.

WEB UI 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:

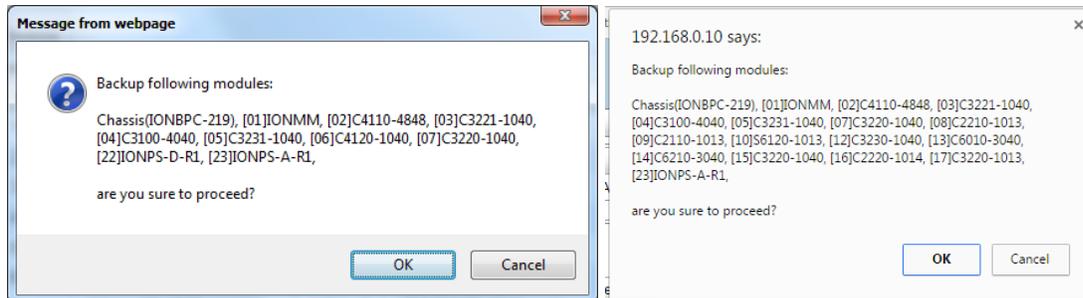
Backup All via the Web GUI

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**.

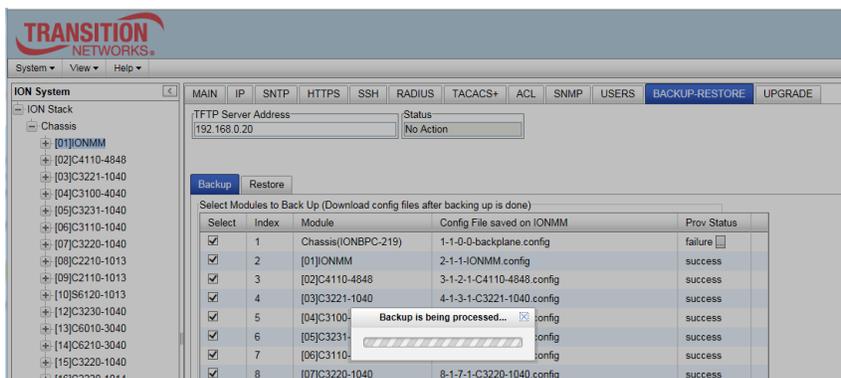
Select	Index	Module	Config File saved on IONMM	Prov Status
<input checked="" type="checkbox"/>	1	Chassis(ONBPC-219)	1-1-0-0-backplane.config	
<input checked="" type="checkbox"/>	2	[01]IONMM	2-1-1-IONMM.config	
<input checked="" type="checkbox"/>	3	[02]C4110-4848	3-1-2-1-C4110-4848.config	
<input checked="" type="checkbox"/>	4	[03]C3221-1040	4-1-3-1-C3221-1040.config	
<input checked="" type="checkbox"/>	5	[04]C3100-4040	5-1-4-1-C3100-4040.config	
<input checked="" type="checkbox"/>	6	[05]C3231-1040	6-1-5-1-C3231-1040.config	
<input checked="" type="checkbox"/>	7	[06]C3110-1040	7-1-6-1-C3110-1040.config	
<input checked="" type="checkbox"/>	8	[07]C3220-1040	8-1-7-1-C3220-1040.config	
<input checked="" type="checkbox"/>	9	[08]C2210-1013	9-1-8-1-C2210-1013.config	
<input checked="" type="checkbox"/>	10	[09]C2110-1013	10-1-9-1-C2110-1013.config	
<input checked="" type="checkbox"/>	11	[10]S6120-1013	11-1-10-1-S6120-1013.config	
<input checked="" type="checkbox"/>	12	[12]C3230-1040	12-1-12-1-C3230-1040.config	
<input checked="" type="checkbox"/>	13	[13]C6010-3040	13-1-13-1-C6010-3040.config	
<input checked="" type="checkbox"/>	14	[14]C6210-3040	14-1-14-1-C6210-3040.config	
<input checked="" type="checkbox"/>	15	[15]C3220-1040	15-1-15-1-C3220-1040.config	
<input checked="" type="checkbox"/>	16	[16]C2220-1014	16-1-16-1-C2220-1014.config	
<input checked="" type="checkbox"/>	17	[17]C3220-1013	17-1-17-1-C3220-1013.config	
<input checked="" type="checkbox"/>	18	[18]C4120-1048	18-1-18-1-C4120-1048.config	
<input checked="" type="checkbox"/>	19	[23]IONPS-A-R1	19-1-23-1-IONPS-A-R1.config	

2. Click the **Back Up** button. This will backup config files to IONMM and TFTP on TFTP server.

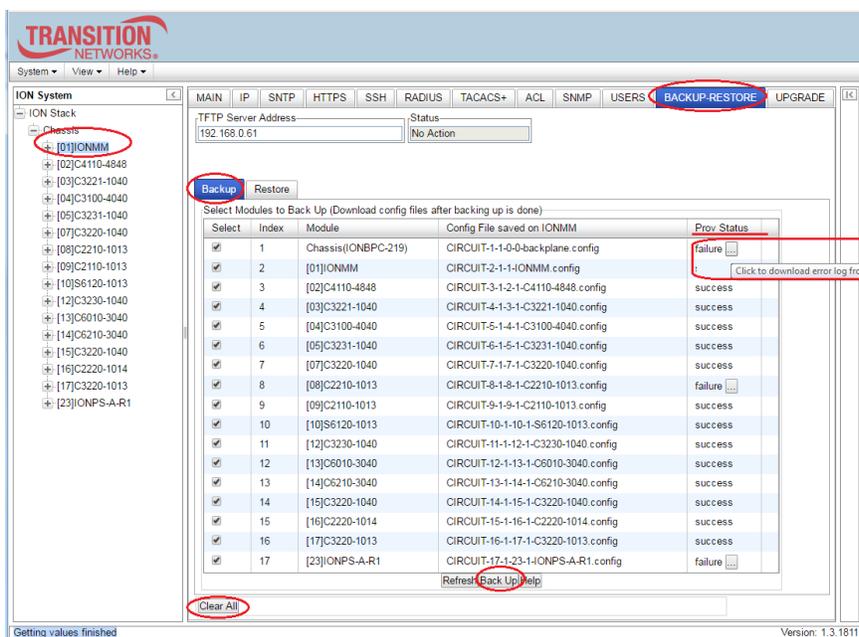
A webpage message displays listing the selected modules for backup and prompting you to verify that you want to proceed with the backup of these modules.



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.

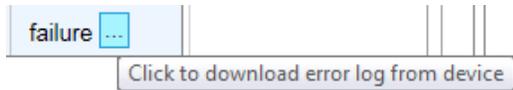


4. When the backup process completes, the Backup page displays again with the new status (*success* or *failure*) displayed in the "Prov Status" column. If Prov Status *ongoing* displays longer than momentarily, click **Refresh**.



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 server must be configured and running.



7. At the confirmation message, click the **OK** button to clear the webpage message. Make sure the TFTP 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:

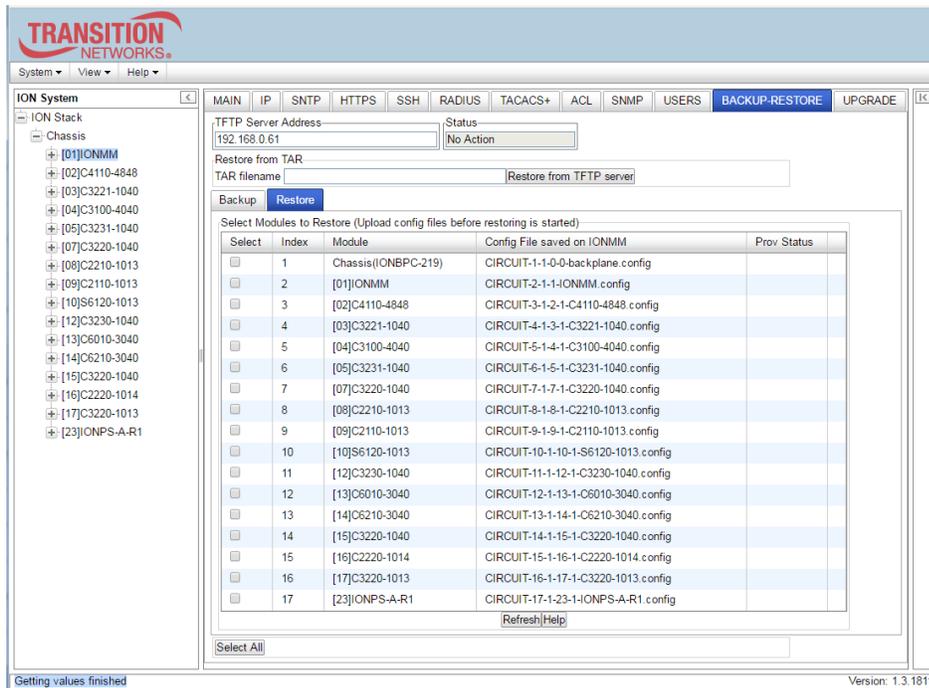
Select	Index	Module	Config File saved on IONMM	Prov Status
<input checked="" type="checkbox"/>	1	Chassis(ION219)	ODIN-1-1-0-0-backplane.config	success
<input checked="" type="checkbox"/>	2	[01]C3220-1040	ODIN-2-1-1-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	3	[02]C3220-1040	ODIN-3-1-2-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	4	[03]C6010-3040	ODIN-4-1-3-1-C6010-3040.config	success
<input checked="" type="checkbox"/>	5	[04]C3220-1014	ODIN-5-1-4-1-C3220-1014.config	success
<input checked="" type="checkbox"/>	6	[05]C3220-1040	ODIN-6-1-5-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	7	[06]C3221-1040	ODIN-7-1-6-1-C3221-1040.config	success
<input checked="" type="checkbox"/>	8	[07]C3220-1014	ODIN-8-1-7-1-C3220-1014.config	success
<input checked="" type="checkbox"/>	9	[08]C3231-1040	ODIN-9-1-8-1-C3231-1040.config	success
<input checked="" type="checkbox"/>	10	[09]C3220-1040	ODIN-10-1-9-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	11	[09-L2]REM C3230-1040	ODIN-11-1-9-2-C3230-1040.config	success
<input checked="" type="checkbox"/>	12	[10]C3230-1040	ODIN-12-1-10-1-C3230-1040.config	success
<input checked="" type="checkbox"/>	13	[11]C3220-1014	ODIN-13-1-11-1-C3220-1014.config	success
<input checked="" type="checkbox"/>	14	[12]C3220-1040	ODIN-14-1-12-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	15	[13]C3210-1040	ODIN-15-1-13-1-C3210-1040.config	success
<input checked="" type="checkbox"/>	16	[14]C3220-1040	ODIN-16-1-14-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	17	[15]C4110-4848	ODIN-17-1-15-1-C4110-4848.config	success
<input checked="" type="checkbox"/>	18	[16]C3230-1040	ODIN-18-1-16-1-C3230-1040.config	success
<input checked="" type="checkbox"/>	19	[17]C3220-1040	ODIN-19-1-17-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	20	[17-L2]REM C3220-1040	ODIN-20-1-17-2-C3220-1040.config	success
<input checked="" type="checkbox"/>	21	[18]C3220-1040	ODIN-21-1-18-1-C3220-1040.config	success
<input checked="" type="checkbox"/>	22	[19]IONMM	ODIN-22-1-19-IONMM.config	success
<input checked="" type="checkbox"/>	23	[23]IONPS-A	ODIN-23-1-23-1-IONPS-A.config	success

Refresh Back Up Help

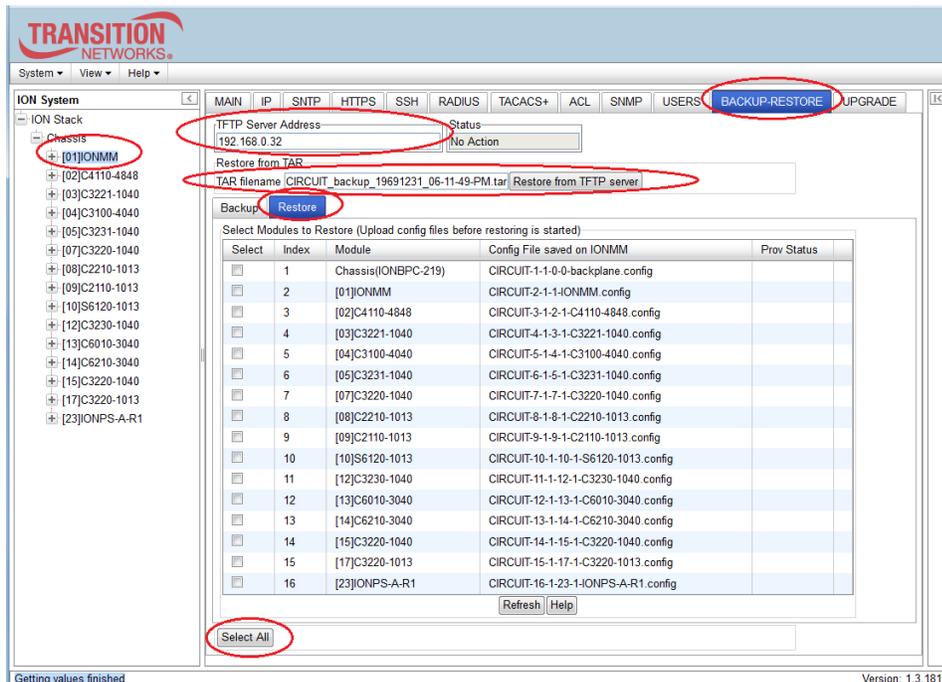
Clear All

Restore All via the Web GUI

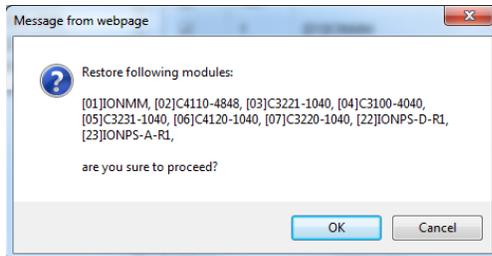
IONMM at v 1.3.18 lets you select and restore all of the discovered module via the Web GUI. The cards being backed up / restored must be in Software mode (Hardware/Software Jumper set to Software).



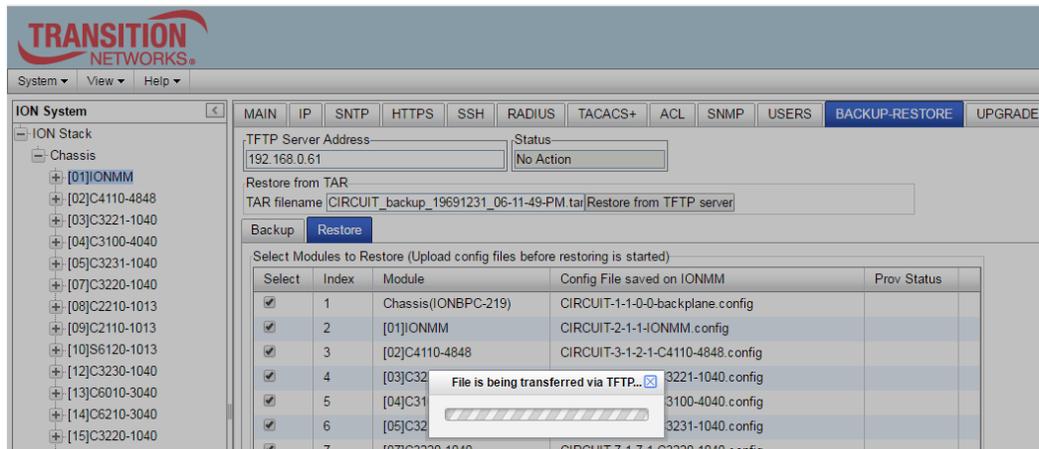
1. Navigate to the IONMM > BACKUP-RESTORE > Restore tab and click the **Select All** button. A check mark is placed in the Select column of each discovered module and the **Select All** button toggles to display **Clear All**.



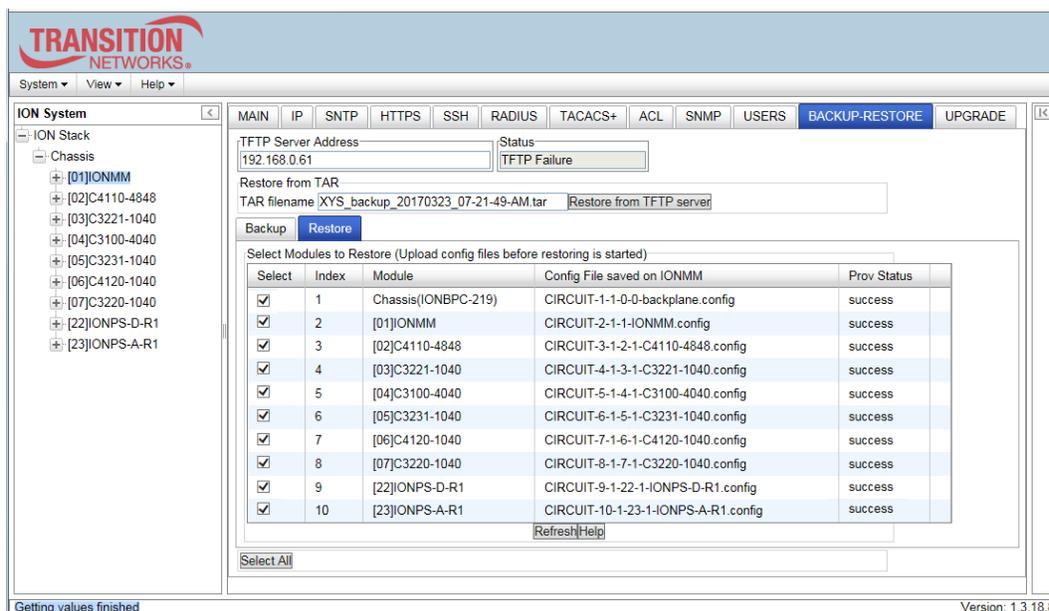
2. Enter the TFTP Server Address (e.g., 192.168.0.32 shown above).
3. Enter the TAR filename (e.g., CIRCUIT_backup_19691231_06-11-49-PM.tar shown above).
4. Click the **Restore from TFTP server** button. A webpage message displays listing the selected modules for restore and asking to verify that you want to proceed with restoring these modules.



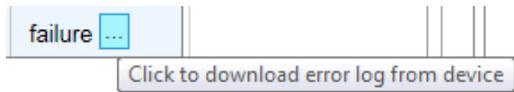
5. If you are not sure click **Cancel**. If you are sure click **OK**. The restore process begins. The screen is grayed out while the Restore is in process, and the message "File is being transferred via TFTP..." displays.



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 server must be configured and running.



8. At the confirmation message, click the **OK** button to clear the webpage message. Make sure the TFTP server is up and configured, verify the name and location of the file being transferred, and continue operation.

Backup All and Restore All 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

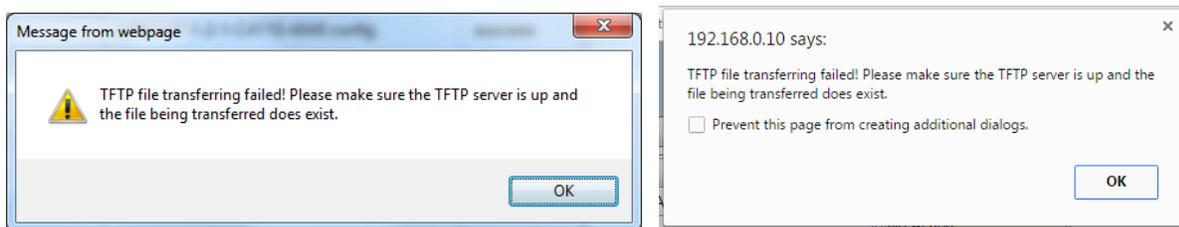
Sending restore commands succeeded

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

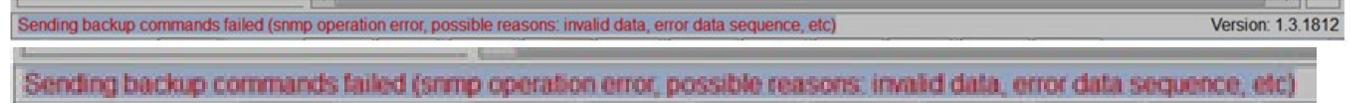
Failed to open backup_rlist.bin\n

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.

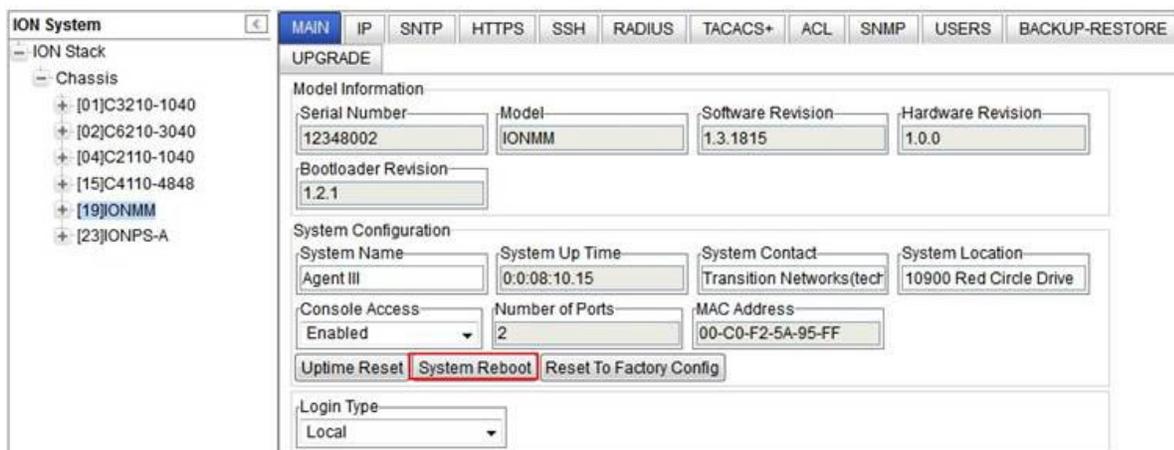
Message: *Sending backup commands failed (snmp operation error, possible reasons: invalid data, error data sequence, etc)*



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 its 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.

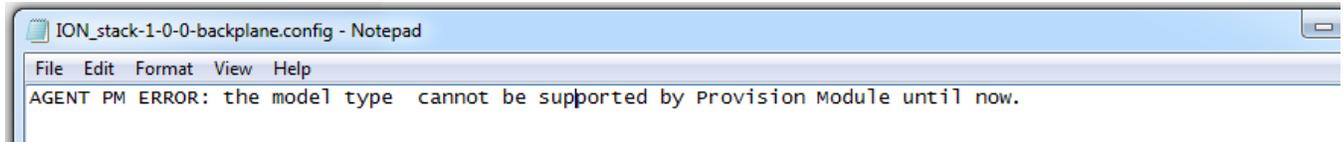
Recovery: **1.** Open the file *config.err* in the tftpboot directory in WordPad or similar package to see the failed function. **2.** Verify the Backup or Restore page parameters. **3.** Make sure the chassis name has 32 or less ASCII printable characters. **4.** Re-try the Backup or Restore operation. **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; see "[Contact Us](#)" below.

A screenshot of a Notepad window titled "ION_stack-1-0-0-backplane.config - Notepad". The window has a menu bar with "File", "Edit", "Format", "View", and "Help". The text inside the window reads: "AGENT PM ERROR: the model type cannot be supported by Provision Module until now."

```
ION_stack-1-0-0-backplane.config - Notepad
File Edit Format View Help
AGENT PM ERROR: the model type cannot be supported by Provision Module until now.
```

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.

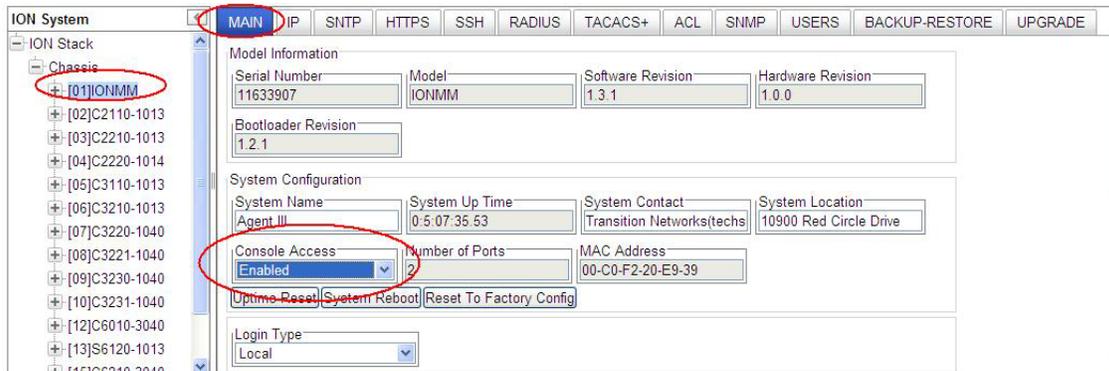
Disabling Console Access – CLI Method

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. Press **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 D: 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 a 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”](#)).

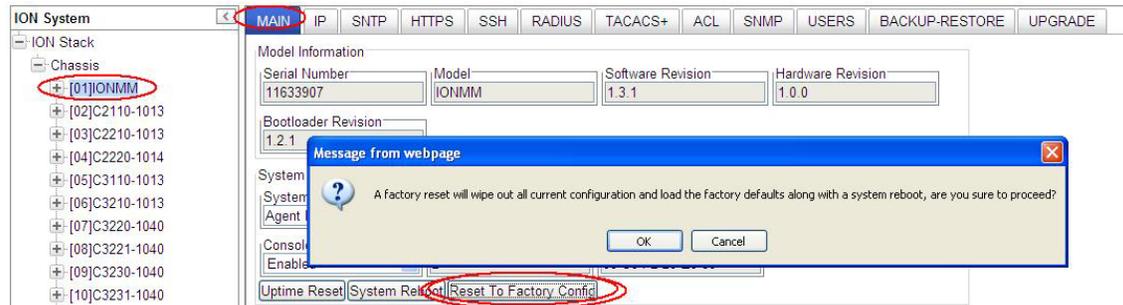
Note: Your USB and/or Telnet session will be disconnected.

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 set 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 a 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.

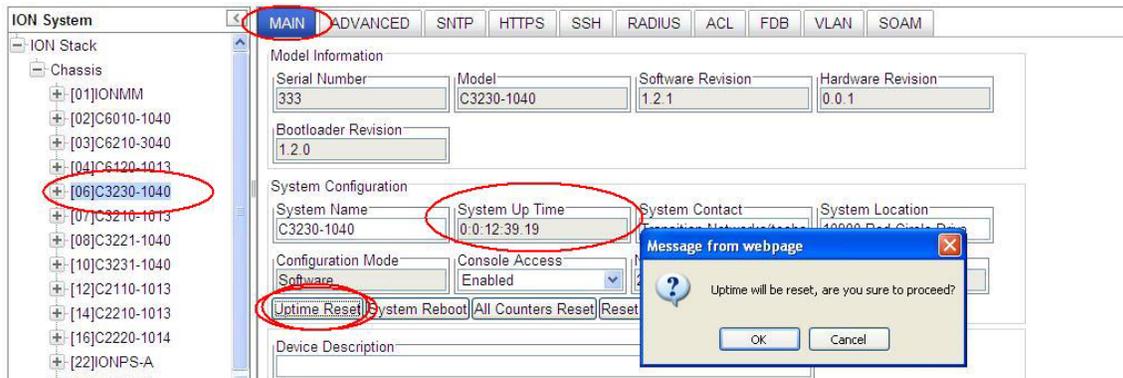
For example: C1|S1|L1D>**reset uptime**
C1|S1|L1D>

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 D: 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.

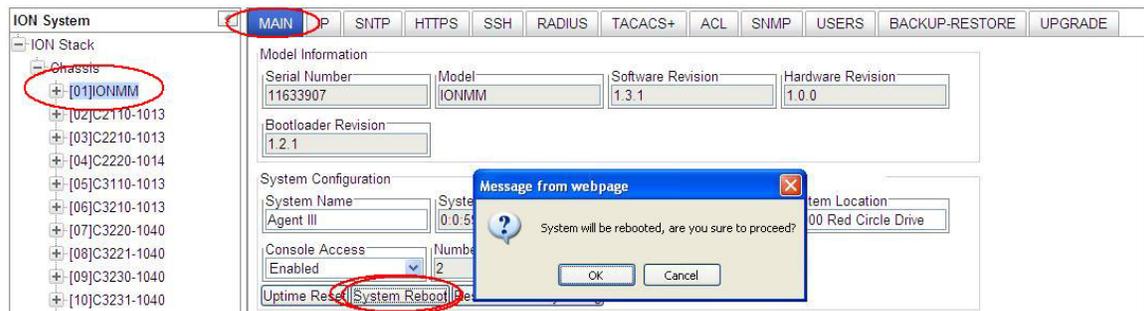
1. Access the IONMM through either a USB connection (see "[Starting a USB Session](#)") or a Telnet session (see "[Starting a Telnet Session](#)").
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please 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 a 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 similar to the TFTP 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%\$**

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 a 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 retrieve file!
now start to transfer the file ...
ŠCCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0BB0
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file ...
Šlsz: cannot open /tftpboot/xxxx: No such file or directory
BB0BB0BB0
BB0BB0
Can't open any requested files.
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial upgrade protocol zmodem file=xxxx
now start to transfer the file ...
**B000000063f694ceive.**B000000063f694
CCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0BB0
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 being added, [fixes](#), [enhancements](#), etc.

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).

For information on the status of important ION system files resulting from this operation, see “[Appendix D: 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

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 a 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
4. Go to the Lantronix Software Upgrades web page at <http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.
5. Locate the “**Agent Firmware**” section and click the link in the right hand column (e.g., “**Download IONMM.bin.1.0.5.bin**”).
6. Zip the downloaded file.
7. Retrieve the firmware database file using the **tftp get** command to get the file from the TFTP Server, and then press **Enter**. For example:
tftp get iptype=(ipv4 | dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
tftp put iptype=(ipv4|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
8. Unzip the file. Type **update firmware-db file=FILENAME** and press **Enter**.
9. Verify the Update results. Type **show firmware-db update result** and press **Enter**.

10. Upgrade the module. Type **upgrade module** and press **Enter**. 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 that the ION106-x chassis limits the size of the db.zip file to 50 Mb for bulk upgrades.

Note: The TFTP server must be configured and running, and the upgrade files must be resident in the default directory on the TFTP server (normally *C:/TFTP-Root*).

1. Access the IONMM through the Web interface (see “Starting the Web Interface”).
2. At the **MAIN** tab, locate the **TFTP Settings** section.

The screenshot shows the IONMM web interface. The 'MAIN' tab is selected. In the left sidebar, the 'IONMM' module is highlighted. The 'TFTP Settings' section is circled in red. It contains the following fields and buttons:

- TFTP Server Address:** 192.168.1.30
- Firmware File Name:** IONMM_1.1.0_AP.bin
- Status:** No Action
- Buttons: Save Server Address, Upgrade Firmware, Refresh
- Bottom buttons: Refresh, Save, Help

4. 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).
5. To save the 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.

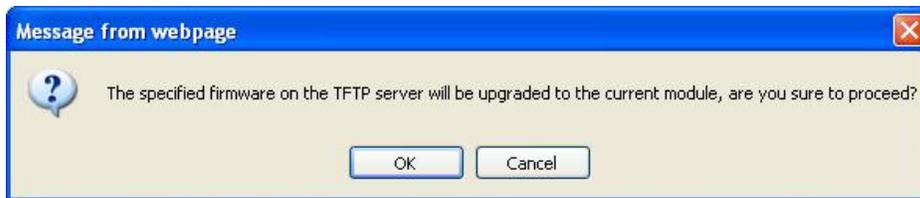
This is a close-up of the TFTP Settings section. The fields are filled with the following values:

- TFTP Server Address:** 192.168.1.30
- Firmware File Name:** IONMM_1.1.0_AP.bin
- Status:** No Action

Buttons: Save Server Address, Upgrade Firmware, Refresh

Bottom buttons: Refresh, Save, Help

7. Click the **Upgrade** button. A confirmation window displays.

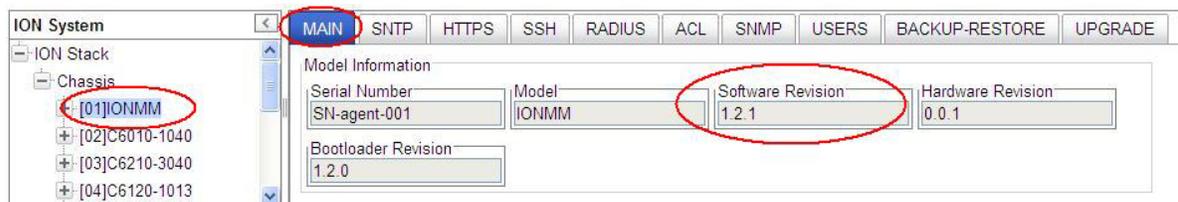


8. Click **OK**. The upgrade begins and the message “*the firmware is being upgraded*” displays. The Status field displays “*Success*” when the firmware upgrade successfully completes.

TFTP Settings		
TFTP Server Address	Firmware File Name	Status
192.168.1.30	IONMM_0.6.5_AP.bin	Success
Save Server Address	Upgrade Firmware	Refresh
Refresh Save Help		

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.)

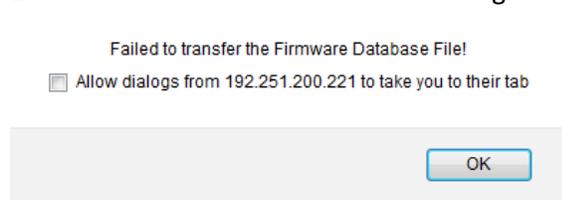
Recovery: Upgrade multiple devices in stages so that the size of the db.zip file is 50 Mb or less for bulk upgrades.

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](#)” 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 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**”.

The following procedure is for creating the firmware database index and archive files.

1. Launch the program that will be used to create the index file.

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

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

xx yy zz

where:

xx = name of the module as shown in the Web I/F (see the file example below)

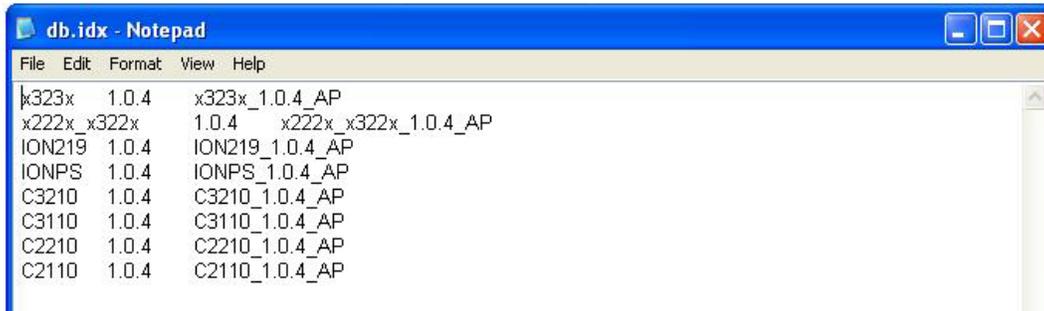
yy = revision level of the firmware upgrade file

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.



```
db.idx - Notepad
File Edit Format View Help
x323x 1.0.4 x323x_1.0.4_AP
x222x_x322x 1.0.4 x222x_x322x_1.0.4_AP
ION219 1.0.4 ION219_1.0.4_AP
IONPS 1.0.4 IONPS_1.0.4_AP
C3210 1.0.4 C3210_1.0.4_AP
C3110 1.0.4 C3110_1.0.4_AP
C2210 1.0.4 C2210_1.0.4_AP
C2110 1.0.4 C2110_1.0.4_AP
```

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

Note: if you used a program, such as Notepad, that does not allow you to save the file 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 **nine** .bin files:

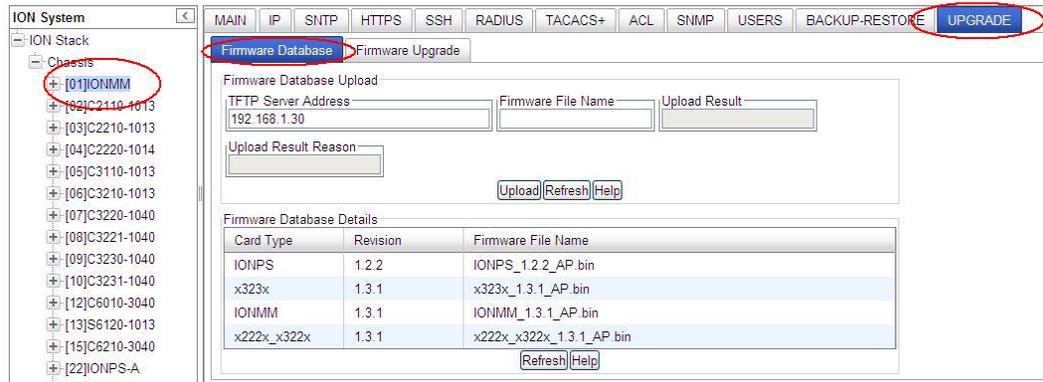
- db.idx
- x323x
- x222x/x32xx
- ION219
- IONPS
- C3210
- C3110
- C2210
- C2110

5. Do the upgrade (see “[Performing the Upgrade](#)” section below).

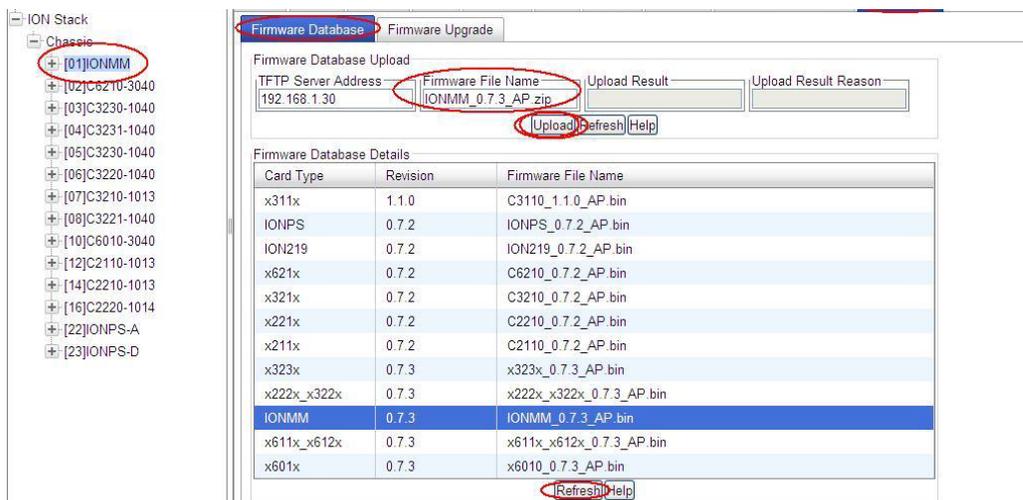
Performing the Upgrade

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.



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 zip file you created (max. 32 characters).



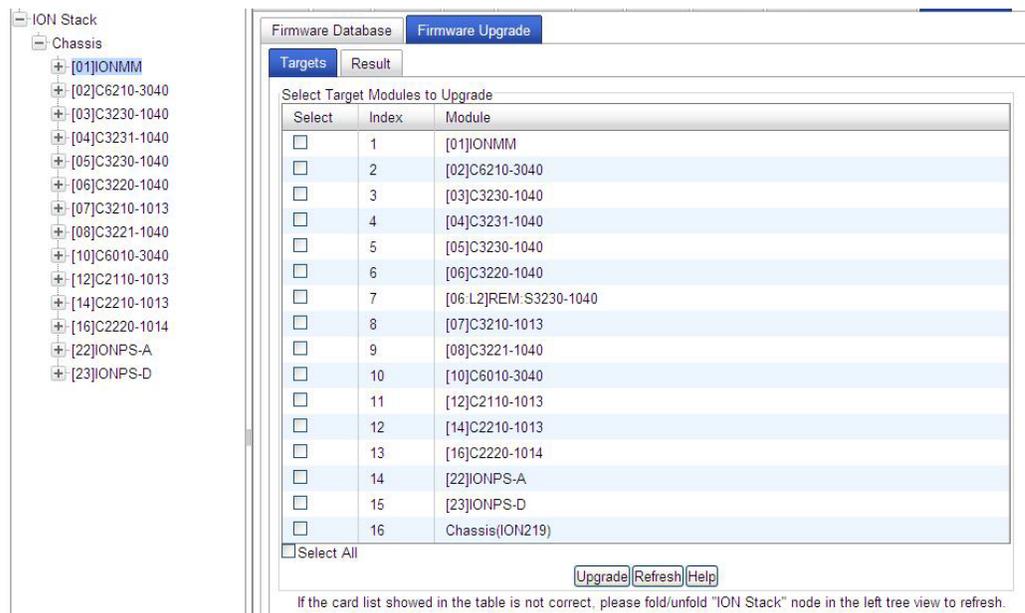
5. Click the **Upload** button.

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

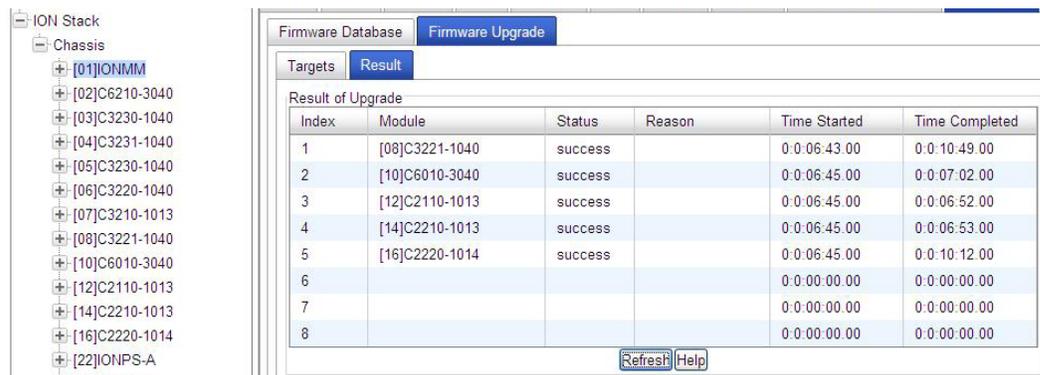
6. Wait for the file to successfully load. The message “Success” displays in the **Upload Result** field, and the modules listed in the *db.idx* file are listed in the **Firmware Database Details** section.

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.

Upgrade the IONMM and/or NID Firmware

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

Note: Lantronix recommends that before completing any steps on an install that you verify that the management module has the latest firmware version installed and running. The latest firmware version is at:

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

These procedures require that you have the TFTP server running and configured.

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

Upgrading IONMM and/or NID Firmware – CLI Method

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

1. Access the IONMM through either a USB connection (see “Starting a USB Session”) or a 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
```

4. Go to the Lantronix Software Upgrades web page at <http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.
5. Locate the “Agent Firmware” section and click the link in the right hand column (e.g., “Download IONMM.bin.1.0.5.bin”).
6. Zip the downloaded file.
7. Retrieve the firmware database file using the **tftp get** command to get the file from the TFTP Server, and then press **Enter**. For example:

```
tftp get iptype=(ipv4 |dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
tftp put iptype=(ipv4|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
```

8. Unzip the file. Type **update firmware-db file=FILENAME** and press **Enter**.
9. Verify the Update results. Type **show firmware-db update result** and press **Enter**. The related **Firmware file name** and **Database update result** display.
10. Upgrade the module. Type **upgrade module** and press **Enter**.

A table of available modules displays with upgrade instructions.

```
Agent III C1|S1|L1D>upgrade module
Available modules:
```

```
index      module                                     loc
-----
```

```

1      ION219      c=1 s=0 l1d
2      IONMM      c=1 s=1 l1d
3      C6010-1040 c=1 s=2 l1d
4      C6210-3040 c=1 s=3 l1d
5      C6120-1013 c=1 s=4 l1d
6      C3220-1040 c=1 s=6 l1d
7      C3210-1013 c=1 s=7 l1d
8      C3221-1040 c=1 s=8 l1d
9      C3230-1040 c=1 s=9 l1d
10     C3231-1040 c=1 s=10 l1d
11     C2110-1013 c=1 s=12 l1d
12     C2210-1013 c=1 s=14 l1d
13     C2220-1014 c=1 s=16 l1d
14     C3230-1040 c=1 s=18 l1d
15     IONPS-A    c=1 s=22 l1d
16     IONPS-D    c=1 s=23 l1d

```

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

- Choose the module(s) to upgrade (# 6- IONMM in the example above) and press **Enter**. (You can also quit the upgrade process; type q and press Enter.) This informational message displays:

```

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

```

- Verify the Upgrade results. Type **show firmware upgrade result** and press **Enter**. The firmware upgrade results display in a table.

```

Agent III C1|S1|L1D>show firmware upgrade result
index  module          status  reason  time started  time completed
-----
1      IONMMc=1 s=7 l1d  success  00:21:24  00:21:47
Agent III C1|S1|L1D>

```

If the firmware upgrade was successful, the time started and time completed display.

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

Upgrading IONMM and/or NID Firmware – Web Method

The following describes the procedure for upgrading the firmware in the IONMM through the Web Interface. If the IONMM is to be upgraded at the same time as other modules in the ION Chassis, see the related ION NID User Guide.

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

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

A. Verify the Current IONMM / NID Firmware Version

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

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

B. Locate the New IONMM / NID Firmware Version

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

1. Go to the Lantronix Software Upgrades web page at <http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.
2. Locate the “Agent Firmware” section and examine the link in the right hand column (e.g., “**Download IONMM.bin.1.0.5.bin**”).
3. Compare the IONMM / NID version displayed in the **MAIN** tab **Software Revision** area with the version number on the web site, and continue if the web site version is newer than the current (running) version.
4. Click the link located in step 2 above to download the new firmware file.

C. Run TFTP Server

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

1. Install, run and configure the TFTP Server.
2. Copy the file downloaded in step 4 above to the required TFTP Server location.
Note: the upgrade file must be resident in the default directory on the TFTP server (normally *TFTP-Root*).
3. Note the location of the downloaded file and its filename for use in steps 4 and 5 below.

D. Upgrade the IONMM / NID Firmware

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

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

D1. Upgrade IONMM / NID Firmware from the **MAIN** Tab

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

TFTP Settings

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

Save Server Address Upgrade Firmware Refresh

Refresh Save Help

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

TFTP Settings

TFTP Server Address 192.168.1.30	Firmware File Name IONMM_1.0.4_AP.bin	Status No Action
-------------------------------------	--	---------------------

Save Server Address Upgrade Firmware Refresh

Refresh Save Help

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

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

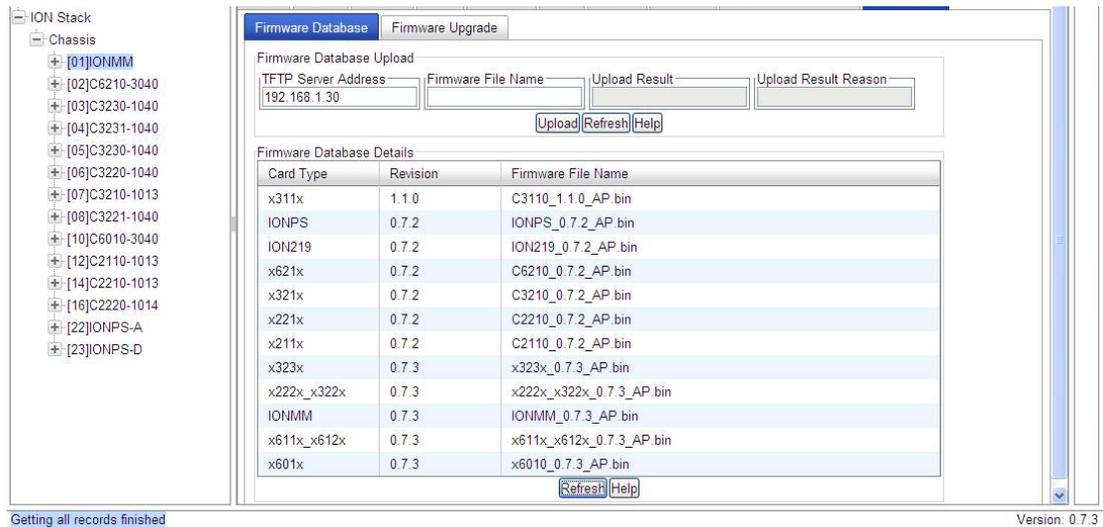
7. Click **OK**.

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

8. Click the **Refresh** button. The **Software Revision** area is updated from the old version number to the new version number (e.g., from 1.0.4 to 1.0.5).
9. If you will be using the same TFTP Server Address for future upgrades, click the **Save Server Address** button.

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

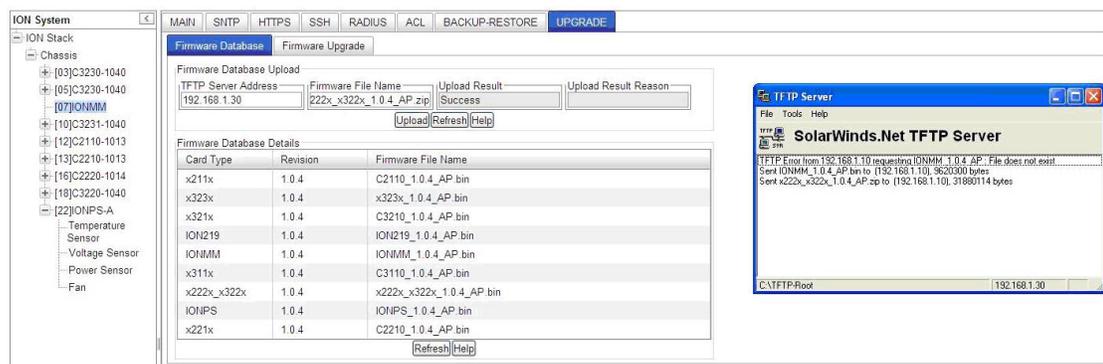
1. Access the IONMM card through the Web interface (see “Starting the Web Interface”).
2. Select the **UPGRADE** tab.
3. Select the **Firmware Database** sub-tab if not already selected.
4. Locate the **Firmware Database Upload** section.



5. Enter the **TFTP Server Address**. This is the IP address of the TFTP Server from step C (“Run TFTP Server”) above.
6. Enter the **Firmware File Name**. This is the name of the firmware file from step B2 above.
7. Click the **Upload** button.

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

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

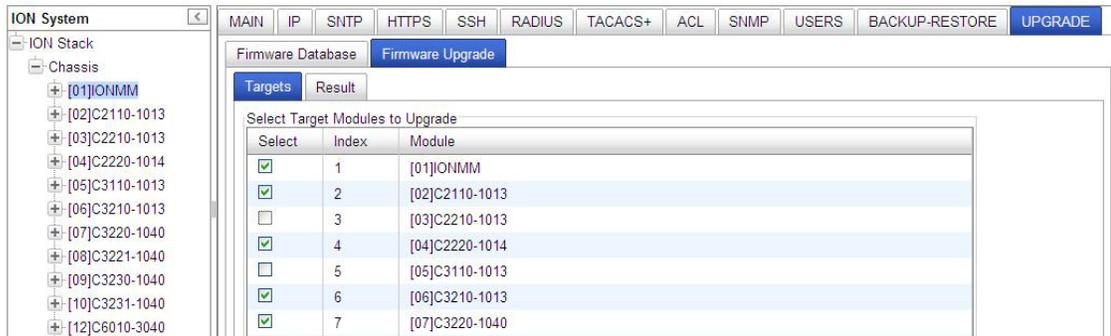


8. If the firmware upload operation failed, the **Upload Result** area displays either:

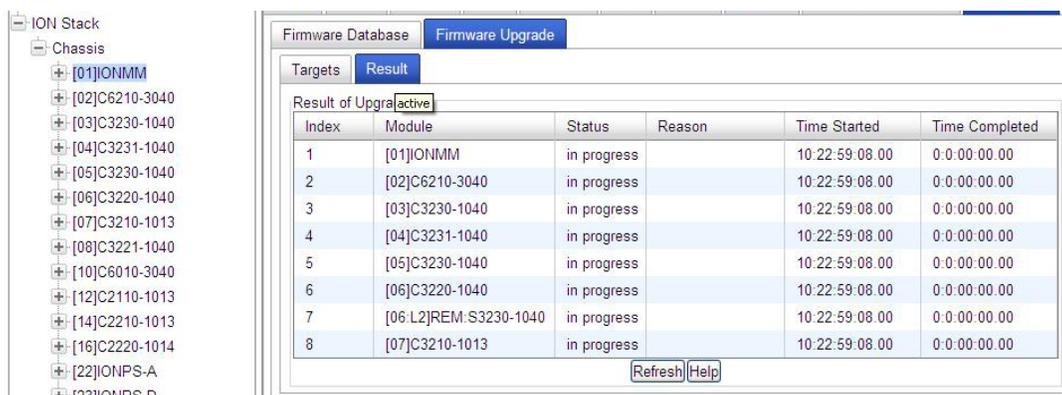
- **None:** no operation was performed, or
- **Failure:** the specified operation has failed.

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

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



- In the **Select** column, check the **IONMM** and/or one or more NIDs as the Target Module(s) to be upgraded.
- Click the **Upgrade** button. A confirmation message displays.
- Click the **OK** button to proceed.
During the upload, the message *"Getting records in progress..."* displays.
If the upload was successful, the message *"Getting all records finished"* displays.
If the upload was unsuccessful, *"Getting records failed (http server error)"* displays.
- Click the **Result** sub-tab. A table displays with upgrade status information.



- Click the **Refresh** button.

The screenshot shows the ION Stack tree on the left and the Firmware Upgrade window on the right. The Firmware Upgrade window has tabs for 'Targets' and 'Result'. The 'Result' tab is active, showing a table titled 'Result of Upgrade' with the following data:

Index	Module	Status	Reason	Time Started	Time Completed
1	[03]C3230-1040	success		0:3:30:05.00	0:3:33:16.00
2	[05]C3230-1040	success		0:3:30:05.00	0:3:33:07.00
3	[10]C3231-1040	success		0:3:30:05.00	0:3:47:35.00
4	[13]C2210-1013	success		0:3:30:05.00	0:3:30:12.00
5	[16]C2220-1014	success		0:3:30:05.00	0:3:34:45.00
6	[18]C3220-1040	success		0:3:30:05.00	0:3:33:06.00
7	[22]IONPS-A	success		0:3:30:05.00	0:3:30:12.00
8	Chassis(ION219)	success		0:3:30:05.00	0:3:30:12.00

Buttons for 'Refresh' and 'Help' are located at the bottom of the table.

16. Verify that the **Status** column displays “*success*” to indicate that the upgrade was successfully completed.

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

17. If more than eight devices are to be upgraded, repeat steps 9 - 16 above for the remaining devices.

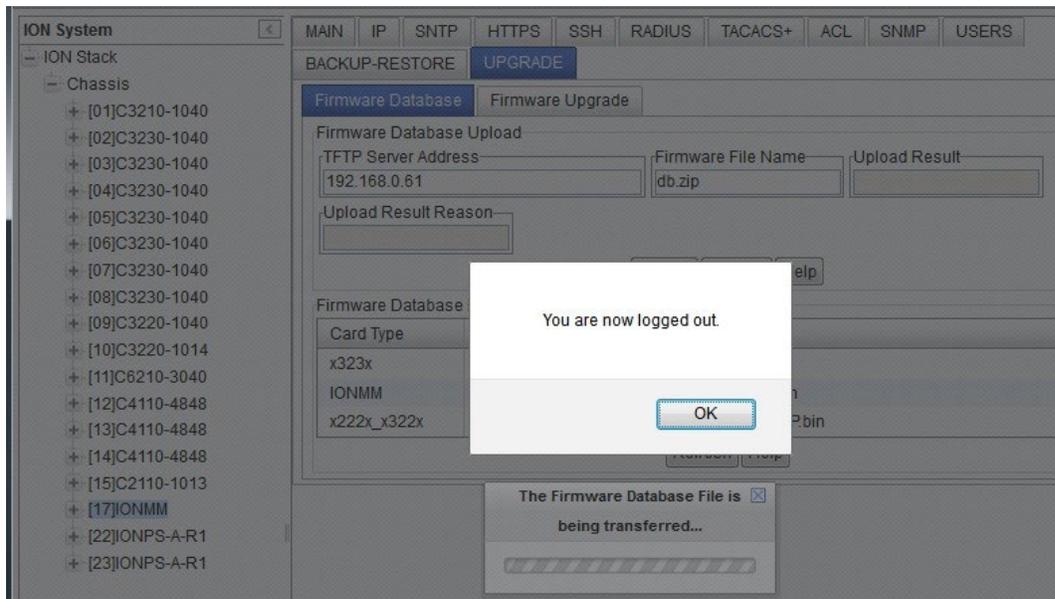
18. If the upgrade fails, the **Reason** column displays a failure code. See “[Section 5 – Troubleshooting](#)” for error messages and recovery procedures.

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

For information on the status of important ION system files resulting from this operation, see “[Appendix D: ION System File Content and Location](#)”.

Messages

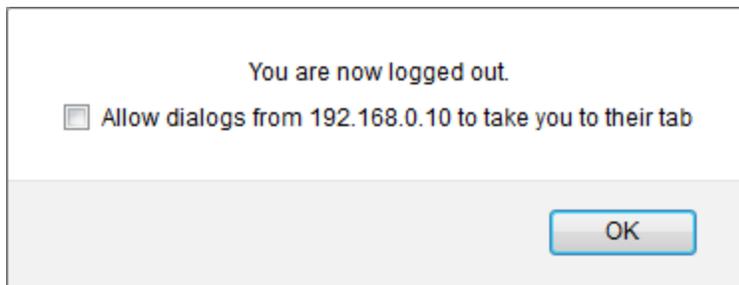
Message: *The firmware Database File is being transferred...* followed by *You are now logged out* displays during a firmware upgrade; or the file transfer completes but the files are not added.



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. In order to enter a command for a different device or port in the ION system, you must change the location of the command prompt. The **go** command 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.

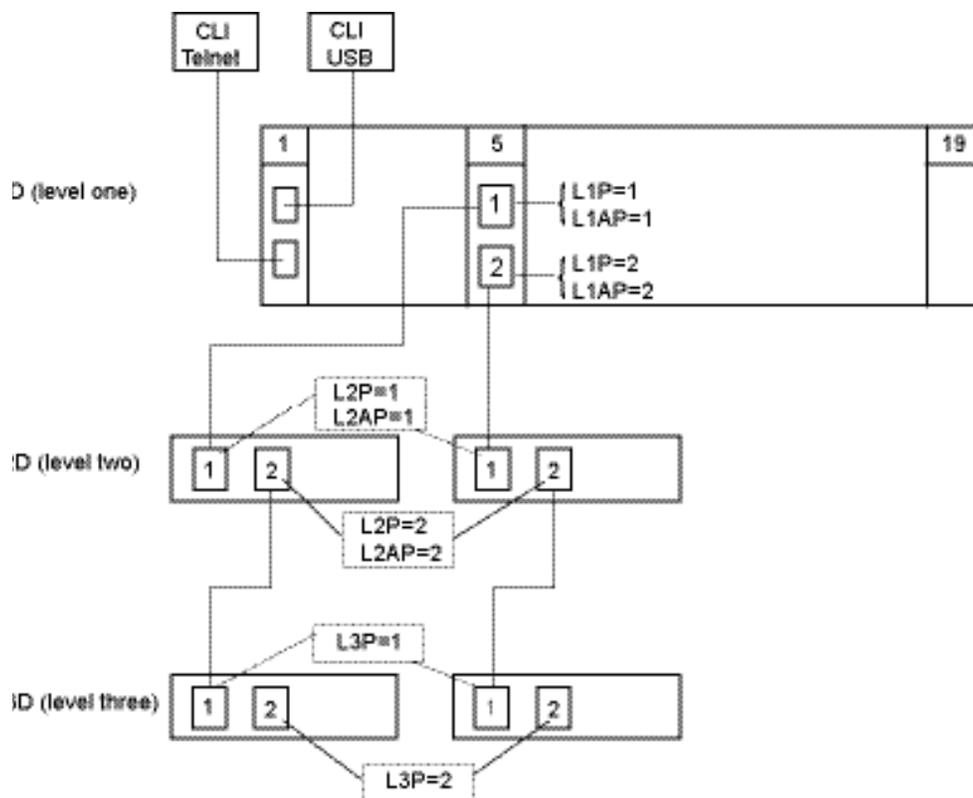


Figure 4: CLI Location Hierarchy

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 4: 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 4: 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.

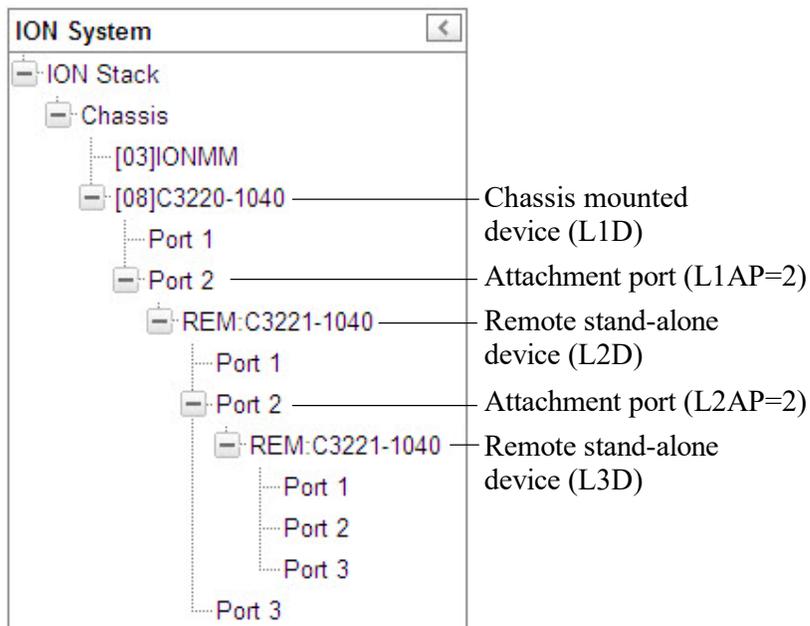
The following procedure is for using CLI commands to manage other SICs.

1. Access the IONMM through either a USB connection (see [“Starting a USB Session”](#)) or a 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”).

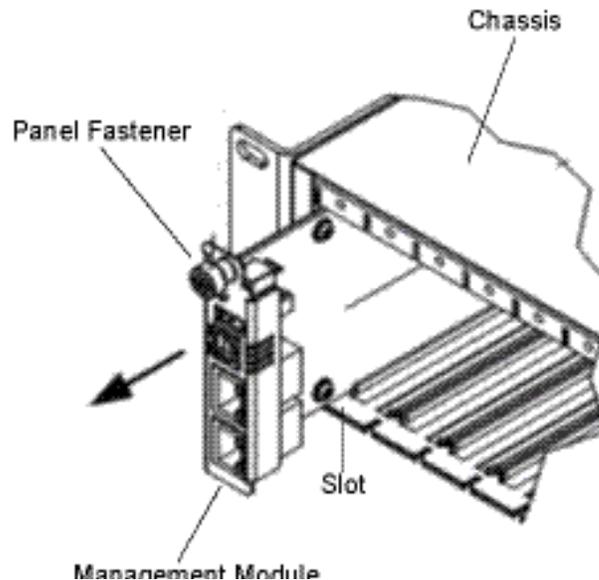


2. Click on the slide-in card / port to be managed.
3. The operations that can be performed depend on the slide-in card type. Refer to the specific product document for more information. See the “Related Documents” section.

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 [“Restoring 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 most simple and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the NIDs are seated properly, view the CLI **show** command output, 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 TN 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 fix for each.
12. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
13. Isolate on the 1-2 most likely root causes of what went wrong, and gain as much information as you can to prove the suspected cause(s).
14. If you find a sequence of actions that causes the problem to recur, 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 TN for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED fault and activity displays (page [191](#))
- Problem Conditions (page [194](#))
- CLI Messages (page [210](#))
- Web Interface Messages (page [258](#))
- Syslog Messages and Sys.log Output (page [284](#))
- Windows Event Viewer Messages (page [291](#))
- Config Error Log (config.err) File Messages (page [292](#))
- Webpage Messages (page [294](#))

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 with the exception of link-local (equivalent to IPv4 APIPA) addresses, which resolve automatically. DNS handles records for IPv6 host names similar to IPv4 and also 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** 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:fd0%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:fd0%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>
```

For 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](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 particular 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 Technical Support. See [Contact Us](#).

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? <ul style="list-style-type: none"> • 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? <ul style="list-style-type: none"> • Yes – end procedure. • No – continue with step 5. 	Continue with step 5 .

5. If the problem persists, contact Technical Support. See [Contact Us](#) below.**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 a 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

<p>Access the IONMM through HTTPS or disable HTTPS (see “Configuring HTTPS”).</p> <p>Is access restored?</p> <ul style="list-style-type: none"> • Yes – end procedure. • No – continue with step 7. 	<p>Continue with step 7.</p>
---	------------------------------

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
<p>a) Make sure that the management station/PC is part of the same VLAN as the IONMM.</p> <p>b) Make sure that the correct port is being used on the IONMM.</p> <p>c) Is access restored?</p> <ul style="list-style-type: none"> • Yes – end procedure. • No – continue with step 10. 	<p>Continue with step 10.</p>

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Cannot upgrade modules

See [Upgrade fails](#).

Cannot upload upgrade files

See [Upload fails](#).

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Upgrade fails

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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.

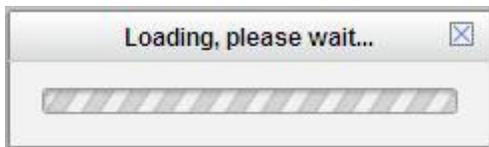
1. See the IONMM or chassis card install Guide for Jumper setting information.
2. Contact Lantronix for more information. Contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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.

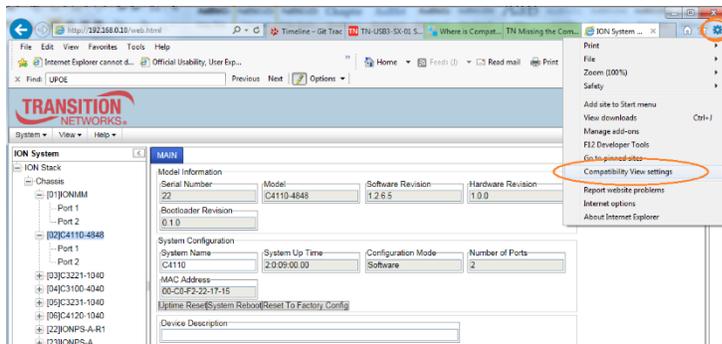
ION System web pages do not display or display incorrectly in Internet Explorer 11.

The ION System message *“loading, please wait ...”* displays continuously and IE11 freezes

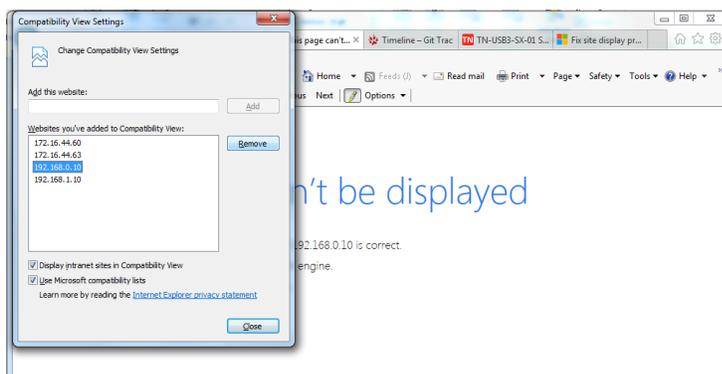
Cause: In earlier IE versions, the Compatibility View button would try to fix a broken standards-based website by getting the page to display like it did in Internet Explorer 7. Compatibility issues were largely resolved since IE 7, to the point where the Compatibility View button was removed for IE11.

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.



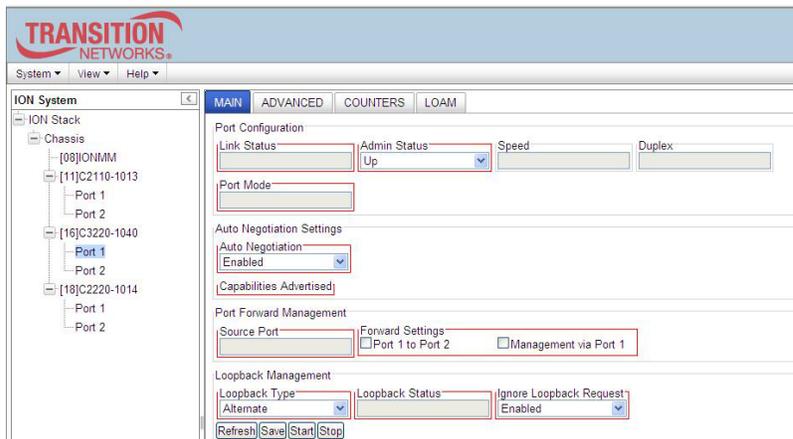
3. You also have the option to uncheck (disable) two other features:
 - Display intranet sites in Compatibility View
 - Use Microsoft compatibility lists
4. Click the Close button when done and log back in to the ION System.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Windows XP Forces a Reboot after Installing a Device

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

1. Select not to restart the computer and then unplug and re-plug the device. This may allow the device to function properly without restarting.
2. Restart the computer to allow the device to work correctly.
3. Contact Lantronix for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at + 1 952-358-3601.

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. See [Contact Us](#) below.

**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, SNMP 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. See [Contact Us](#) below.

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 Transition Network's LLDP packet (xxDP) the ION system handles it separately.

If it is not a Transition Network's 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](#)” section, or “[Backup and Restore Operations \(Provisioning\)](#)”).
3. Reboot the NID. See “[Reboot](#)”.
4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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 in order to use it. In v 0.5.14, the stored key was moved from the root file system to the application flash area (/agent3/conf).

Problem: 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. See [Contact Us](#) below.

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

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

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See the *ION System CLI Reference Manual, 33461*.
4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. U See [Contact Us](#) below.

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. See [Contact Us](#) below.

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

Cannot show port QoS configuration in this card!
Cannot show port QoS priority remapping in this card!
Cannot set tag type for priority in this card!
Cannot set default priority in this card!
Cannot set IEEE tag for priority in this card!

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

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

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

1. Verify if the card supports the desired function.
2. Verify the command entry.
4. Use the **go** command to switch to a different card port supporting loopback.

Cannot get VLAN database configuration on this card!

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

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

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

Command incomplete

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

1. Verify the command syntax. Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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

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

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

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Fail to get MAC address!

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

1. Verify that the correct hierarchy has been specified in the command (see [“Managing Slide-In and Remote Modules Using CLI Commands”](#)).
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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Failed to set DHCP client state!

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

1. Verify the operation in the “[Assigning a Dynamic IP Address](#)” section.
2. Retry the operation. See the related DHCP command in *the ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 of the location parameters:

```
go [c=<1-16>] [s=<1-32>] [l1p=<1-15>] [l2p=<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>] [l1p=<1-15>] [l2p=<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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Invalid condition value: xxxx

This message indicates that the input for the value= parameter on the **add acl condition** command is 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. See [Contact Us](#) below.

Invalid location parameters, cannot find the physical entity!

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

1. Verify that the correct hierarchy has been specified in the command (see [“Managing Slide-In and Remote Modules Using CLI Commands”](#)).
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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Unable to open xx. Please check your port settings.

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

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

Yes	No
Continue with step 4 .	Restart the management station.

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. See [Contact Us](#) below.

Error, you should first give full location parameters

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

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

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

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

```
g[c<16>][s<13>][l1p<15>][2p<15>][lp<15>][2p<15>][Bp<15>][ld|2d|Bd]
```

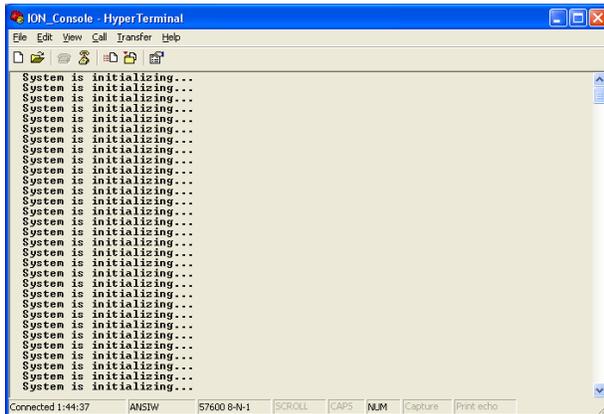
for a slide in card, or

```
g[c<016>][s<032>][l1p<15>][2p<15>][lp<15>][2p<15>][Bp<15>][ld|2d|Bd]
```

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. US/Canada: 1-800-260-1312, International: + 1 952-358-3601.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Error: this command should be executed on a port!

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

Unknown command!

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

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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:

g|c<1-16>|s<1-32>|l|ap<1-15>|2p<1-15>|lp<1-5>|2p<1-15>|bp<1-15>|lid|2d|Bd)
for a slide in card, or

g|c<0-16>|s<0-32>|l|ap<1-15>|2p<1-15>|lp<1-5>|2p<1-15>|bp<1-15>|lid|2d|Bd)
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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 “[Section 6: Command Line Interface \(CLI\) Reference](#)”.
6. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See “[TFTP Commands](#)”.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If 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. See [Contact Us](#) below.

Cannot set remote fault detect state on this card!

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

1. Verify that the card you entered the command on supports this function. See [Set RFD State](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

Fail to set aging time!

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

1. Verify the **dot1bridge aging-time** command syntax. See [Configure Forwarding Learning Aging Time](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

Get aging time failed!

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

1. Verify the **dot1bridge aging-time** command syntax. See [Configure Forwarding Learning Aging Time](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 config** 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 **show fwddb config fdbid=** command.
4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Please reboot the card for the changes to take effect!

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

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

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

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”](#).
4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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”](#).
2. Try entering the command again.

If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

The value of current 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. US/Canada: 1-800-260-1312, International: + 1 952-358-3601.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Problem: HT Overtyping Problem - You tried to edit a typo in a CLI command, the new data is stored, but the old data is appended to it.

Meaning: HyperTerminal (HT) is a terminal emulation program developed by Hillgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a text entry. Overtyping an entry should automatically replace the previous characters. This is a HyperTerminal problem that the ION CLI stack cannot resolve.

Response:

1. Upgrade to the latest version (a free download from www.hilgreave.com). The more current product seems to run more smoothly and has text editing features not found in earlier versions.
2. In HT, turn off local echo - refer to the HT helps and documentation for the command to use.
3. Make sure the keyboard Insert mode is turned off.
4. Download and use PuTTY or TeraTerm to use as a replacement for HT.
5. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

```

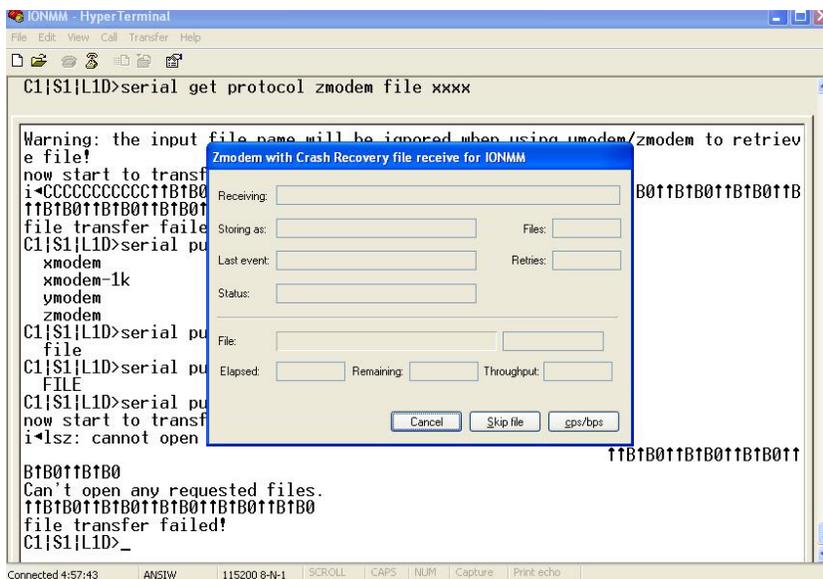
Can't open any requested files.
cannot open /tftpboot/xxxx: No such file or directory
now start to transfer the file ...
file transfer failed!
file transfer succeeded!
now start to upgrade the system ...
/usr/local/bin/flash_firmware /tftpboot/
upgrade failed!
upgrade failed due to wrong file %s!
upgrade 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

ERROR: There is already a same named user!

ERRPR: User name can not 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. See [Contact Us](#) below.

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 sysuser 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, See [Contact Us](#) below.

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.

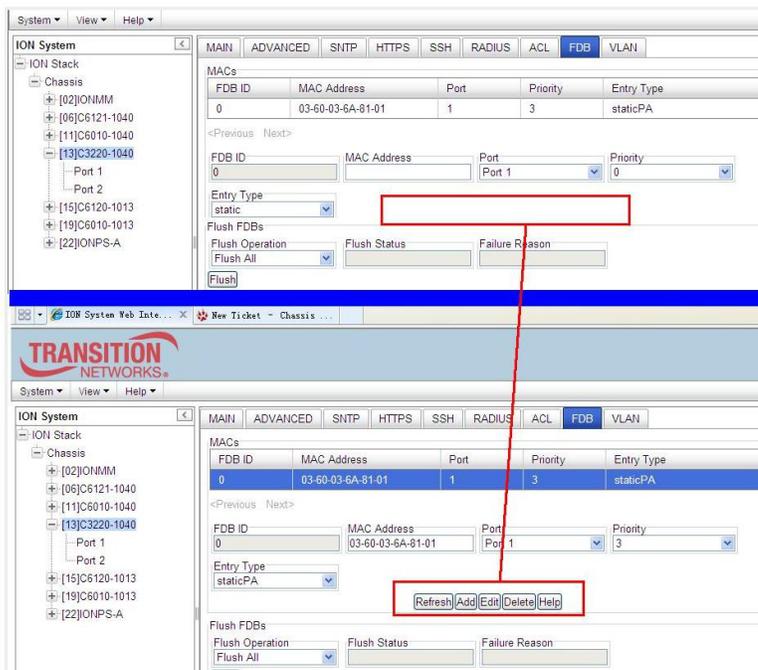
Set IP address type failed.

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. See [Contact Us](#) below.

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>.

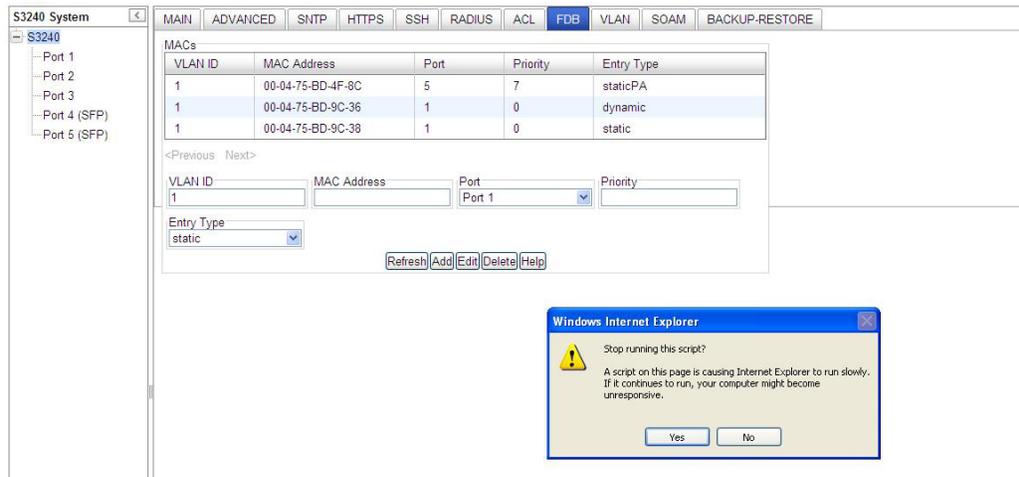
Script error message received.

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 occurred. Do you wish to Debug?

Done, but with errors on page.



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

Message:

*Getting DNS server%u address fail%
 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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](#)” on page 44.
3. Contact Tech Support if the problem persists. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Message:

Its value must be an integer or IPv6 address like 'ffff: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'.", {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'.", {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'.", {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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 ipv4addrange or ipv4network)!

One ACL rule can only has one layer4 ACL condition(tcpport or tcpportrange or udppport or udppportrange 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 udppport or udppportrange 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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)" on page 44.

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. See [Contact Us](#) below.

Cannot Ping IONMM Device

With the "Management VLAN" state set to "enabled", the PC can not ping the IONMM device. The reason is enabling the Management VLAN function gives management control to the Management VLAN that you enabled.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Failed to retrieve DMI info on current port.

You clicked the Device port's DMI tab, but the device does not support DMI. Not all NID models support DMI. The NIDs that support DMI have a "D" at the end of the model number.

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

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. See [Contact Us](#) below.

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

This is the current operational state of the interface.

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

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

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

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

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

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

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

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

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. See [Contact Us](#) below.

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

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

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

1. Verify that diagnostic tests were run properly and completed successfully.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

TFTP for Restore upload operation:

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

Message: *TFTP operation failed!*

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

1. Check:
 - The IP address of the TFTP server is correct.
 - The TFTP server is online and available.
 - The correct file name, db.zip, 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. See [Contact Us](#) below.

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

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

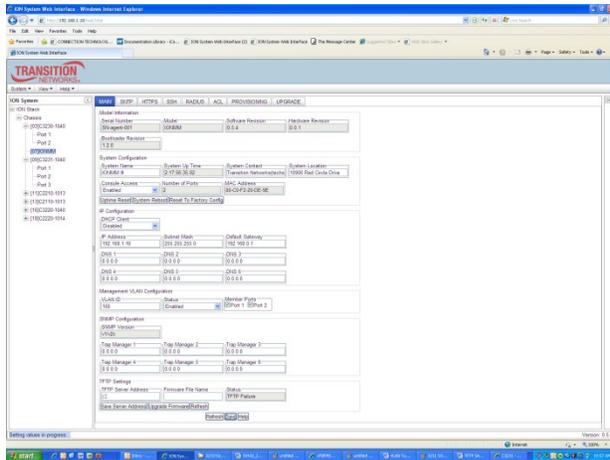
1. Click the [Continue to this website...](#) selection.
2. See the “[Configuring HTTPS](#)” section.

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. See [Contact Us](#) below.

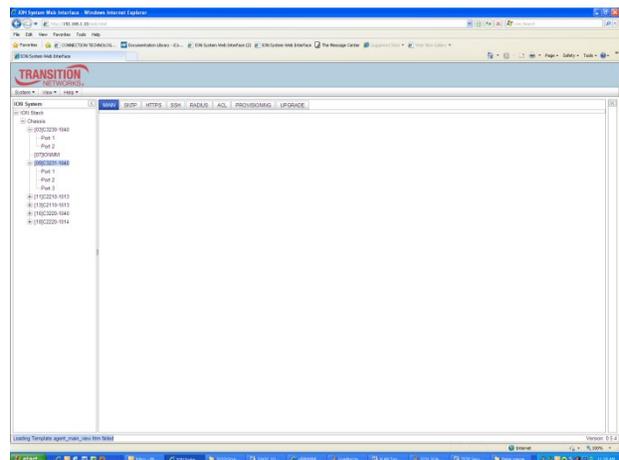
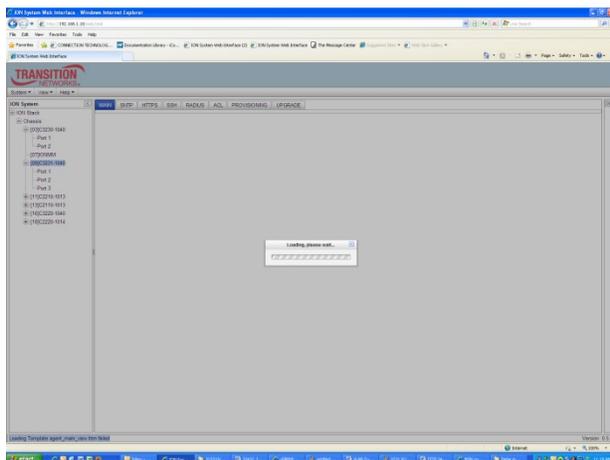
Message: “Setting values in progress ...” displays continuously

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.

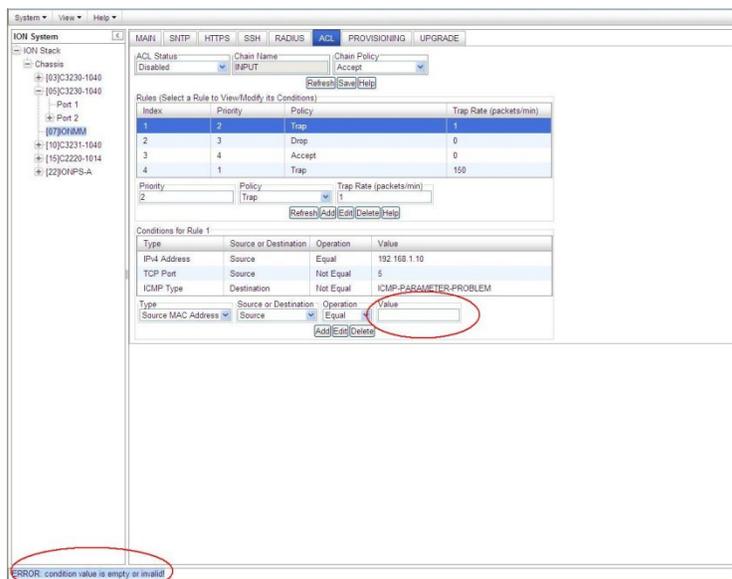
Message: *priority is empty or invalid*

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. See [Contact Us](#) below.

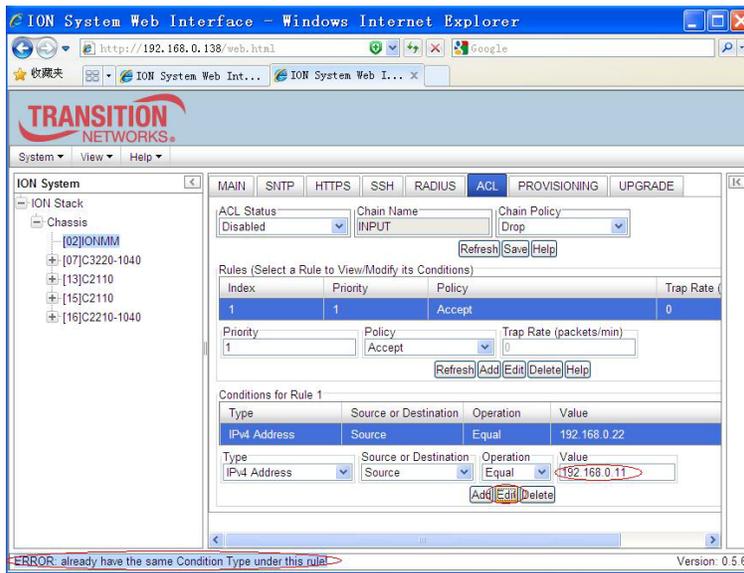
Message: *ERROR: condition value is empty or invalid!*



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. 3. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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.

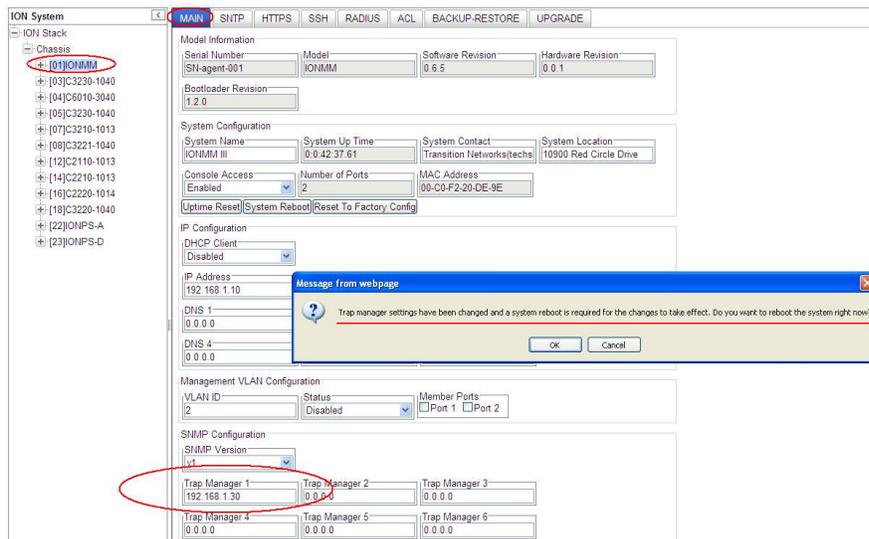
The screenshot shows the ION System web interface. The main content area is in the BACKUP-RESTORE tab. It features a table for selecting modules to restore. The table has columns for Select, Index, Module, Config File (Click to Modify), Prov Status, and TFTP Action. One row is selected, showing Index 1, Module S3231-1040, Config File 67.config, and Prov Status ongoing. A red box highlights the 'ongoing' status. Below the table are buttons for Refresh, Restore, and Help. At the bottom of the interface, a red box highlights the error message 'Getting values failed (http server error)'.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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

The screenshot shows the 'ION System' interface with the 'BACKUP-RESTORE' tab selected. The 'Backup' sub-tab is active. A table titled 'Select Modules to Back Up (Download config files after backing up is done)' is displayed. The table has columns for 'Select', 'Index', 'Module', 'Config File (Click to Modify)', 'Prov Status', and 'TFTP Action'. The 'Prov Status' column shows 'success' for most modules, but 'failure' for [03]C3230-1040. A message box is overlaid on the table, displaying a warning icon and the text 'File has been successfully transferred via TFTP.' The message box has an 'OK' button.

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

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. See [Contact Us](#) below.

Message: *No such user!*



The screenshot shows the login page for the ION System Web Interface. At the top left is the Transition Networks logo. The page title is "Sign in to ION System Web Interface". Below the title are two input fields: "User Name:" with the value "ION" and "Password:" with masked characters. A "Sign in" button is located below the password field. A red error message "No such user!" is displayed below the button.

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!*



The screenshot shows the login page for the ION System Web Interface. At the top left is the Transition Networks logo. The page title is "Sign in to ION System Web Interface". Below the title are two input fields: "User Name:" and "Password:". A "Sign in" button is located below the password field. A red error message "Wrong password!" is displayed below the button.

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 can not 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 can not 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below..

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 engineIDType, 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 same named group!*~~
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. See [Contact Us](#) below.

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" can not 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Message:

Resetting 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. US/Canada: 1-800-260-1312, International: + 1 952-358-3601.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Message: *Invalid input of timeout 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 12u**s**). For example:

```
C1|S1|L1D>addsnmptraphost 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>addsnmptraphost 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. See [Contact Us](#) below.

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 can not 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. See [Contact Us](#) below.

Message: *Invalid group parameter for user!*

No group name is specified!

Too many options follow \"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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.
- 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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|80|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[718]: 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.

175 Dec 31 18:05:45 (none) user.warn syslog: agentx_pkthandler_response: Response to un-

↑
 Line Number
 ↑
 Date (month day time)
 ↑
 (unused)
 ↑
 Level
 ↑
 General log message info. / Request line from the server
 ↑
 Specific log message info. / Response line to the Server

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Sys.log sample - A typical Syslog output is shown below (Telnet screen)

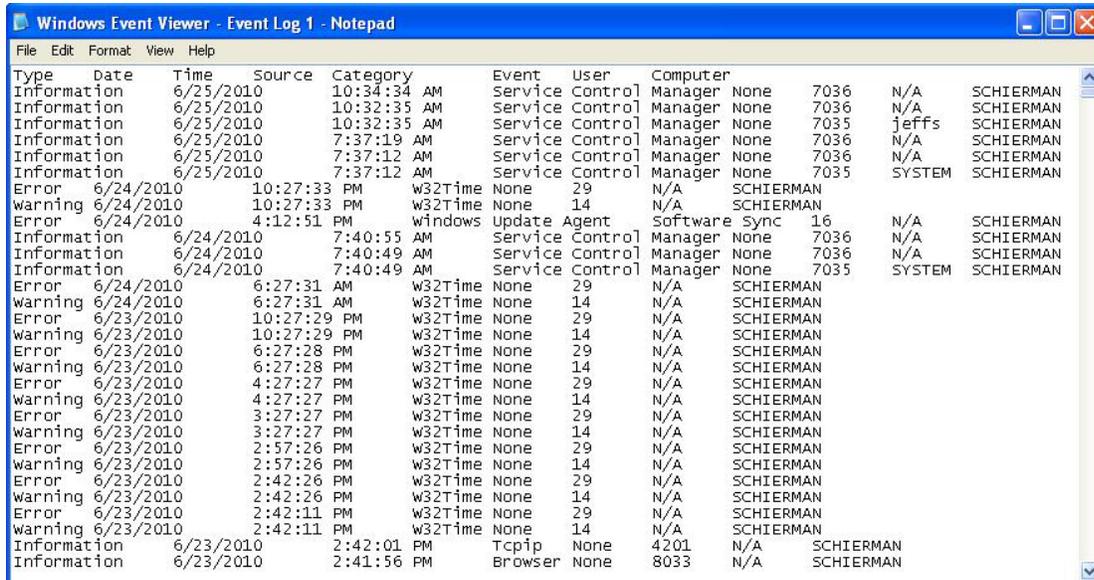
```
Telnet 192.168.0.60
BusyBox v1.4.1 (2011-03-01 14:39:04 CST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ cd /var/log
/var/log $ cat sys.log
Jan 1 08:00:18 (none) user.notice syslog: attach platform info in shared memory at 0x40006000
Jan 1 08:00:19 (none) user.err upgradeManager[719]: upgradeManager starts...
Jan 1 08:00:19 (none) user.err upgradeManager[720]: upgradeManager enters main loop...
Jan 1 08:00:21 (none) local5.notice bpd_linux[731]: BPD Started.
Jan 1 08:00:22 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 11 is released already.
Jan 1 08:00:23 (none) daemon.notice ION-EM[739]: attach platform info in shared memory at 0x40006000
Jan 1 08:00:23 (none) daemon.notice ION-EM[739]: Entity Manager running in Master Mode
Jan 1 08:00:26 (none) user.notice subagent[741]: subAgent Started.
Jan 1 08:00:27 (none) user.notice subagent[741]: attach platform info in shared memory at 0x40006000
Jan 1 08:00:27 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 7 is released already.
Jan 1 08:00:28 (none) daemon.notice ION-EM[739]: Discovered Chassis: 1
Jan 1 08:00:28 (none) user.err upgradeManager[720]: location = 134217228
Jan 1 08:00:28 (none) user.err upgradeManager[720]: just reply OK ...
Jan 1 08:00:28 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 15 is released already.
Jan 1 08:00:29 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[4], relpos-[1]
Jan 1 08:00:29 (none) user.err upgradeManager[720]: location = 152043520
Jan 1 08:00:29 (none) user.err upgradeManager[720]: just reply OK ...
Jan 1 08:00:29 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 13 is released already.
Jan 1 08:00:29 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 13 is released already.
Jan 1 08:00:29 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[22], relpos-[1]
Jan 1 08:00:29 (none) user.err upgradeManager[720]: location = 227540992
Jan 1 08:00:29 (none) user.err upgradeManager[720]: just reply OK ...
Jan 1 08:00:29 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 14 is released already.
Jan 1 08:00:30 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[14], relpos-[1]
Jan 1 08:00:30 (none) user.err upgradeManager[720]: location = 193986560
Jan 1 08:00:30 (none) user.err upgradeManager[720]: just reply OK ...
Jan 1 08:00:30 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 14 is released already.
Jan 1 08:00:30 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[6], relpos-[1]
Jan 1 08:00:30 (none) user.err upgradeManager[720]: location = 160432128
Jan 1 08:00:30 (none) user.err upgradeManager[720]: just reply OK ...
Jan 1 08:00:30 (none) user.err upgradeManager[720]: location = 139460608
Jan 1 08:00:31 (none) user.err upgradeManager[720]: It is AGENT card itself!
Jan 1 08:00:31 (none) user.err upgradeManager[720]: just reply OK ...
Jan 1 08:00:31 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 15 is released already.
Jan 1 08:00:33 (none) daemon.err snmpd[730]: ion-ns/logical: session from local subAgent2 end_point_name [/var/agentx/n
aster]
Jan 1 08:00:34 (none) daemon.err snmpd[730]: ion-ns/logical: session from local subAgent2 end_point_name [/var/agentx/n
aster]
Jan 1 08:00:34 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 13 is released already.
Jan 1 08:00:35 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 14 is released already.
Jan 1 08:00:36 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 15 is released already.
/var/log $
```

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:



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

Message: Information 6/25/2010 7:37:12AM ServiceControlManager None 7035 SYSTEM

Meaning: Information message regarding SCM.

Recovery: No action required.

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

Meaning: Error level message regarding W32Time.

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

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

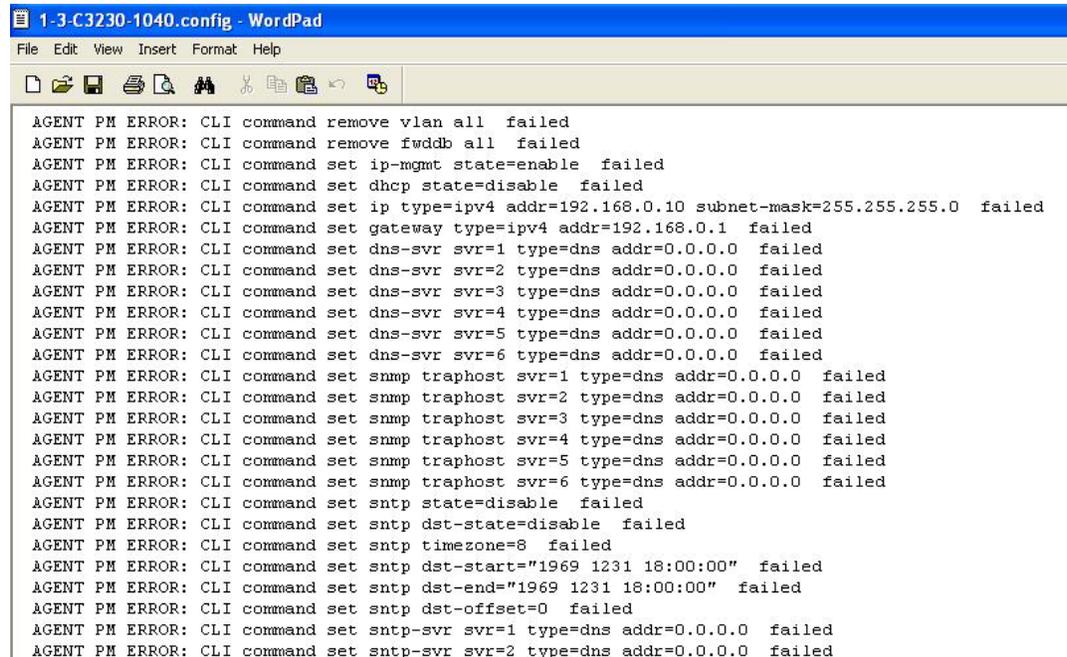
Meaning: Warning level message regarding W32Time.

Recovery: Check the other system logs for related messages. If the problem persists, contact Technical Support. See [Contact Us](#) below.

The Config Error Log (config.err) File

The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad or a text editor.

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



```

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

```

These messages show a translation of failed web interface functions that were attempted, translated into CLI commands.

The config.err files are saved in the TFTP server location specified (typically *C:\TFTP-Root*) with a file name something like: *1-2-2-C3220-1040_20100608.config.err*.

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

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

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

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

config.err Messages

Sample config.err file information is provided below.

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

Line

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

config.err Message Responses

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

Message: remove vlan all failed

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

Message: set snmp 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 SNTP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

Message: set snmp 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 SNTP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

Message: set snmp 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 SNTP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

Message: set snmp dst-start="1969 1231 18:00:00" 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. See [Contact Us](#) below.

Message: set snmp dst-end="1969 1231 18:00:00" 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. See [Contact Us](#) below.

Message: set snmp dst-offset=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. See [Contact Us](#) below.

Message: set snmp-svr 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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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 SNMP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

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. See [Contact Us](#) below.

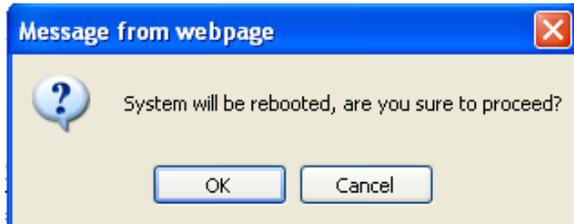
Message: set dot1dbridge ip-priority-index=0 remap-priority=0 failed

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. See [Contact Us](#) below.

Webpage Messages

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

See [Menu System Notes](#) for more information.



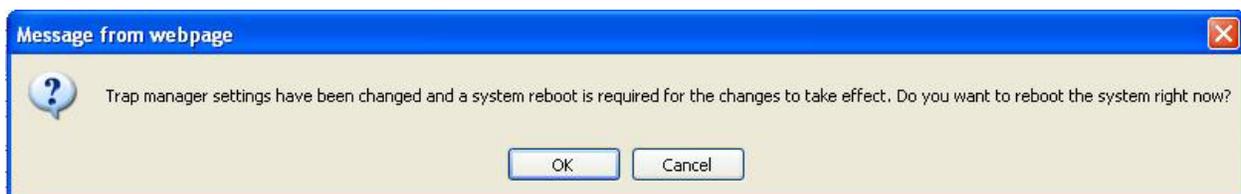
Message: *System will be rebooted, are you sure to proceed?*

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. See [Contact Us](#) below.

Message: Failed to Transfer the Firmware Database File!

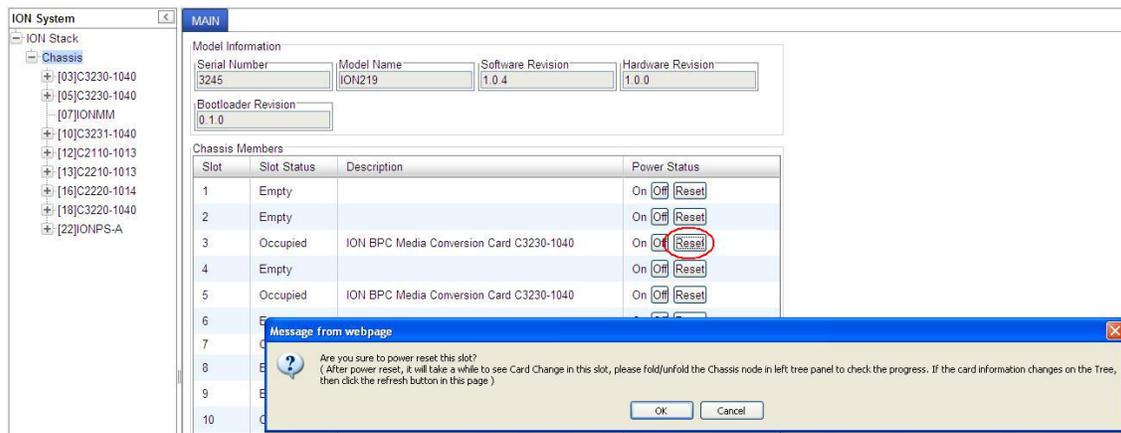


Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the [Upgrade the IONMM Firmware](#) section.

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. See [Contact Us](#) below.

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.)*

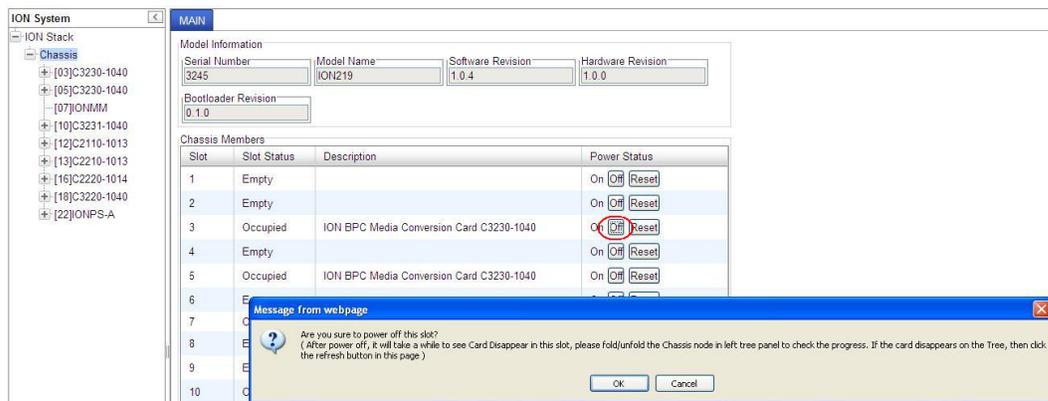


Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Reset** button for a particular slot.

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 Notes](#)” section.
6. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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.)*

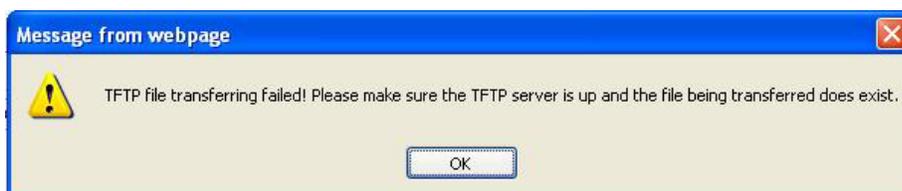


Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Off** button for a particular slot.

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 Notes](#)” section.
6. If the problem persists, contact Technical Support. See [Contact Us](#) below.

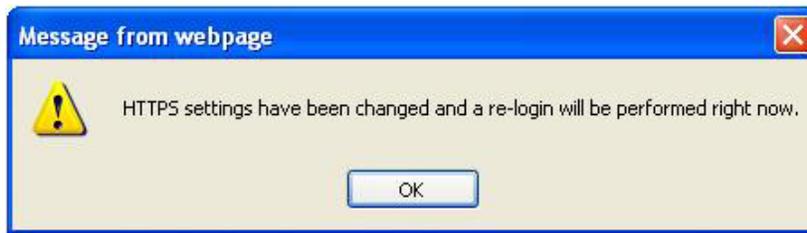
Message: *TFTP file transferring failed!*



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 the TN website at <http://transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.

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”.

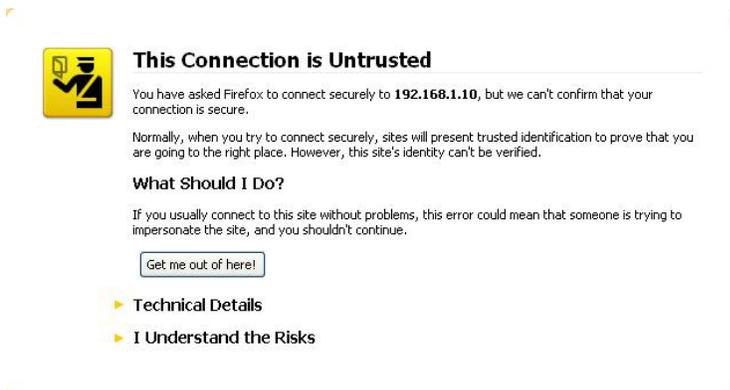
Message: *The Connection was Reset*

The screenshot shows a Firefox error dialog box with a yellow warning icon. The title is "The connection was reset". The main text says "The connection to the server was reset while the page was loading." Below this, there are three bullet points: "The site could be temporarily unavailable or too busy. Try again in a few moments.", "If you are unable to load any pages, check your computer's network connection.", and "If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web." At the bottom, there is a "Try Again" button.

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.

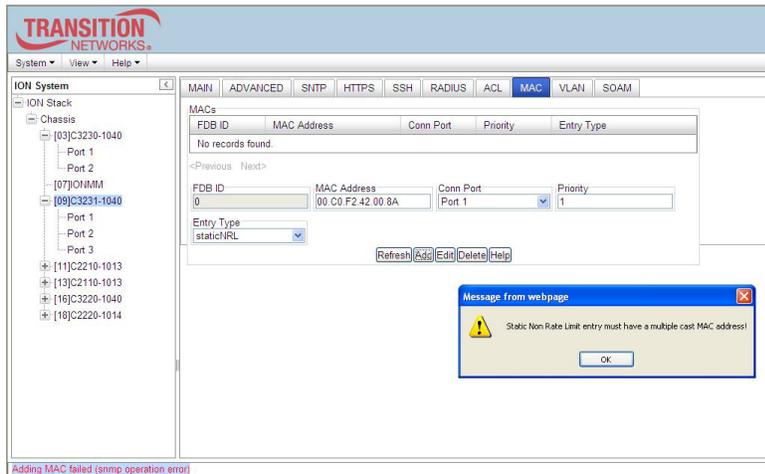
Message: *This Connection is Untrusted*

The screenshot shows a Firefox error dialog box with a yellow warning icon. The title is "This Connection is Untrusted". The main text says "You have asked Firefox to connect securely to 192.168.1.10, but we can't confirm that your connection is secure." Below this, there is a paragraph: "Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified." Then, there is a section titled "What Should I Do?" with the text: "If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue." At the bottom, there is a "Get me out of here!" button and two expandable sections: "Technical Details" and "I Understand the Risks".

Meaning: You tried to connect via FireFox to a URL, but the FireFox web browser did not find a trusted certificate for that site.

Recovery: Click **Technical Details** for details, or click **I Understand the Risks** to continue operation.

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



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

Recovery:

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

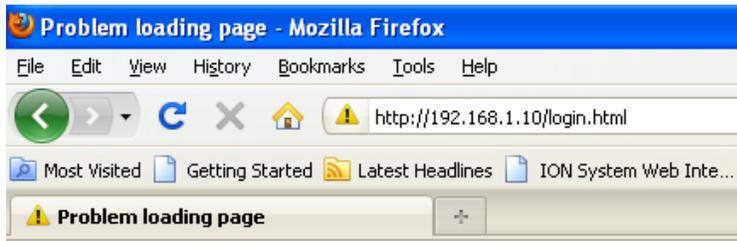
Message: *Local Area Connection x – A network cable is unplugged*



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

Recovery:

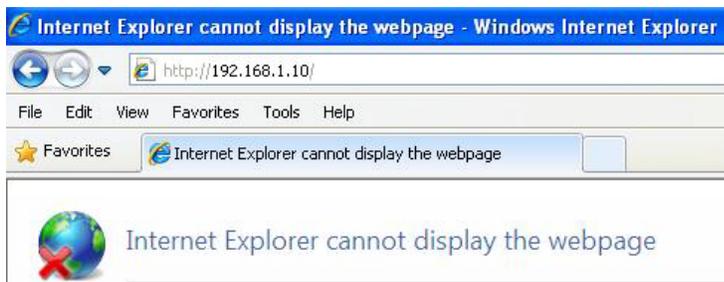
1. If you pressed the **RESET** button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM's **USB-DEVICE** connector, or plug the USB cable back into the NID's **USB** connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support. See [Contact Us](#) below.

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 Browsers Supported](#)".
2. Verify the URL entered. See "[Initial Setup with a Static IP Address via the CLI](#)".
3. Verify NID access. See "[Accessing the 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. See [Contact Us](#) below.

Message: *Internet Explorer cannot display webpage*

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

Recovery:

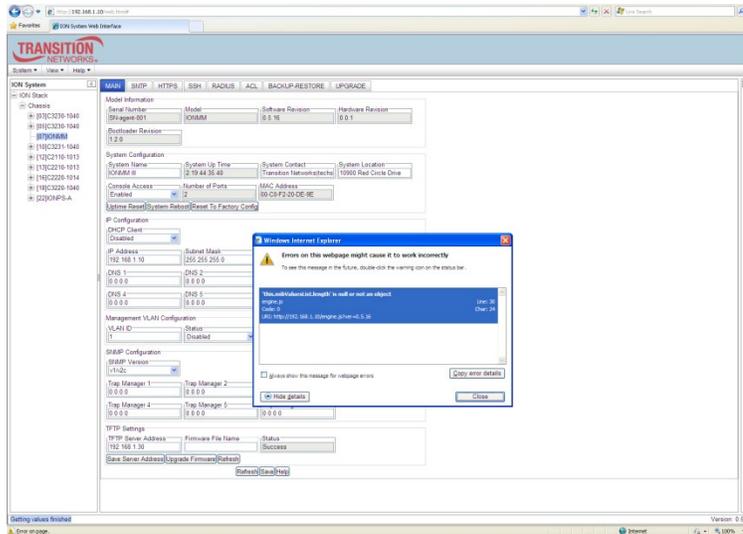
1. Make sure the web browser / version you are using is supported. See "[Web Browsers Supported](#)".
2. Verify the URL entered. See "[Initial Setup with a Static IP Address via the CLI](#)".
3. Verify NID access. See "[Accessing the NIDs](#)".
4. Verify the IP address setting. See "[Setting the IP Addressing](#)".
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. See [Contact Us](#) below.

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 **Ctrl-C** keyboard command)
4. Paste the error details text (use **Ctrl-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; Trident/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. See [Contact Us](#) below.

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.

The screenshot shows the IONMM web interface with the following configuration details:

- Model Information:** Serial Number: 11633907, Model: IONMM, Software Revision: 1.3.2011, Hardware Revision: 1.0.0, Bootloader Revision: 1.2.1
- System Configuration:** System Name: Agent III, System Up Time: 0:19:03:47:57, System Contact: Transition Networks(techs), System Location: 10900 Red Circle Drive, Console Access: Enabled, Number of Ports: 2, MAC Address: 00-C0-F2-20-E9-39
- Management VLAN Configuration:** VLAN ID: 2, Status: Disabled, Member Ports: Port 1, Port 2
- System Log Configuration:** Server Address: 0.0.0.0, Server Port: 514, Level: Notice, Mode: Log local
- TFTP Settings:** TFTP Server Address: 0.0.0.0, Firmware File Name: (empty), Status: No Action

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., changing switch mode, rebooting, 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: _____

Compliance 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 Fall ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention ! Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures 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 öffentliches Telekommunikationsnetz in den EG-Mitgliedstaaten verstößt gegen die jeweiligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Declaration of Conformity

Manufacture's Name: Lantronics, Inc.

Manufacture's Address: 48 Discovery, Suite 250, Irvine, California 92618 USA

Declares that the products: IONMM

Conforms to the following Product Regulations:

**EMC- EN 55022:2006 + A1:2007 (CISPR 22:2005/A1:2005) Class A; FCC Part 15 Subpart B Class A
EMC Directive 2004/108/EC; EB 55024:1988 + A1:2001 + A2:2003; EN61000-4-2:1995 + A1:1998 + A2:2001;
EN61000-4-3:2006; EN61000-4-4:2004 + Corrigendum 2006; EN61000-4-5:2006;
EN61000-4-6:2007; EN61000-4-8:1993 + A1:2001; EN61000-4-11 2nd Edition:2004**

With the technical construction on file at the above address, this product carries the CE Mark

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

Place: Irvine, California

Date: April 27, 2022

Signature: *Fathi Hakam*

Full Name: Fathi Hakam

Position: Vice President of Engineering

Manufacture's Name: Lantronics, Inc.

Manufacture's Address: 48 Discovery, Suite 250, Irvine, California 92618 USA

Declares that the products: IONMM-232

Conforms to the following Product Regulations:

**FCC Part 15 Class A, EN 55032:2012, EN 55024:2010
Directive 2014/30/EU
Low-Voltage Directive 2014/35/EU
IEC /EN 60950-1:2006+A2:2013
2011/65/EU EN 60581:2012**

With the technical construction on file at the above address, this product carries the CE Mark

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

Place: Irvine, California

Date: April 27, 2022

Signature: *Fathi Hakam*

Full Name: Fathi Hakam

Position: Vice President 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

VIGTIG: Dette udstyr skal installeres i overensstemmelse med sikkerhedsadvarselne.

Elektrische veiligheid

BELANGRIJK: Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

Sécurité électrique

IMPORTANT: Cet équipement doit être utilisé conformément aux instructions de sécurité.

Sähköturvallisuus

TÄRKEÄÄ: Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

IMPORTANTE: questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal installeres i samsvar med sikkerhetsregler.

Segurança eléctrica

IMPORTANTE: Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

Seguridad eléctrica

IMPORTANTE: La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

Elsäkerhet

OBS! Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.

Appendix B Factory 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@transition.com) System Location: 10900 Red Circle Drive 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
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
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 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 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
-------------------------	--

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 C 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.

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>

SNMP Configuration

1. Access the IONMM through either a USB connection or a 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.
set 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> addr=<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  
confirmpass=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
```

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 D 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 Re-store to Factory Default
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Lost
Net-SNMP configuration file	snmpd.conf	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 of the SNMP settings (the same as what can be set via the Web interface / CLI) for one SIC into a file containing a list of CLI commands. This file can be downloaded from IONMM. When restoring for one SIC, you can upload a provisioning backup file (this file must have been made via the Backup operation and must be for the same SIC type) to the IONMM and do a Restore. See the IONMM **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	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'	/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 in order to use it. In v 0.5.14, the stored key was moved from the root file system to the application flash area (/agent3/conf). This missing key problem will occur only if you upgrade from 0.5.14 to a later release. In ION versions after 0.5.14, the user-public key is saved after an upgrade.

Glossary

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

100BASE-FX

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

1000BASE-X

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

802.1

The IEEE standard for port-based Network Access Control.

802.1ad

IEEE 802.1ad (Provider Bridges) is an amendment to IEEE standard IEEE 802.1Q-1998 (aka QinQ or Stacked VLANs), intended to develop an architecture and bridge protocols to provide separate instances of the MAC services to multiple independent users of a Bridged LAN in a manner that does not require cooperation among the users, and requires a minimum of cooperation between the users and the provider of the MAC service.

802.1ag

The IEEE standard for Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management, 2007. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3-2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to LOAM.

802.1ah

IEEE 802.1ah-2008 is a set of architecture and protocols for routing of a customer network over a provider network, allowing interconnection of multiple Provider Bridge Networks without losing each customer's individually defined VLANs. The final standard was approved by the IEEE in June 2008.

802.1p

The IEEE standard for QoS packet classification.

802.1p Prioritization

The ability to send traffic to various prioritization queues based on the 802.1q VLAN Tag priority field. (AKA, CoS. Standard: IEEE 802.1p.)

802.1q

IEEE 802.1Q, or VLAN Tagging, is a networking standard allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks. IEEE 802.1Q (aka, dot1q) is commonly refers to the encapsulation protocol used to implement this mechanism over Ethernet networks. IEEE 802.1Q defines the meaning of a VLAN with respect to the specific conceptual model for bridging at the MAC layer and to the IEEE 802.1D spanning tree protocol.

802.1Q VLAN

802.1Q is a standardized way of segmenting and distributing VLAN information. Switches that support 802.1Q can recognize and forward, a tag packet upon egress. See also VID, dot1Q, IEEE 802.1Q. Contrast "PVLAN".)

802.3

The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to LOAM.

ACL

(Access Control List) A set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute.

Address

An IPv6-layer identifier for an interface or a set of interfaces.

Anycast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocol's measure of distance).

AES

(Advanced Encryption Standard) A privacy protocol; one of two encryption algorithms used for ION system data privacy. AES is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES ciphers were analyzed extensively and are now used worldwide (as was its predecessor, DES). AES was announced by NIST as U.S. FIPS PUB 197 (FIPS 197) in 2001 after a 5-year standardization process. AES was implemented as a Federal government standard in 2002 after approval

by the U.S. Secretary of Commerce. AES is available in many different encryption packages. See also "DES".

Alarm Terminology - RFC 3877

The IETF's definitions of Alarms and other terms related to alarm management:

Error: A deviation of a system from normal operation.

Fault: A lasting error or warning condition.

Event: Something that happens which may be of interest (e.g., fault, a change in status, crossing a threshold, or an external input to the system).

Notification: Unsolicited transmission of management information.

Alarm: Persistent indication of a fault.

Alarm State: A condition or stage in the existence of an alarm. At a minimum, alarms states are raise and clear. They could also include severity information such as defined by perceived severity in the ITU model M.3100 (cleared, indeterminate, critical, major, minor and warning).

Alarm Raise: The initial detection of the fault indicated by an alarm or any number of alarm states later entered, except clear.

Alarm Clear: The detection that the fault indicated by an alarm no longer exists.

Active Alarm: An alarm which has an alarm state that has been raised, but not cleared.

Alarm Detection Point: The entity that detected the alarm.

Perceived Severity: The severity of the alarm as determined by the alarm detection point using the information it has available.

ANSI

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

ARAP

(AppleTalk Remote Access Protocol) the protocol used for accessing AppleTalk networks remotely. ARAP was introduced in conjunction with AppleTalk Remote Access in 1991. ARAP is an open protocol, and specifications are available for third-party developers. In its latest versions of the Apple Remote Access product family, the AppleTalk Remote Access Protocol has been enhanced to provide superior performance and configuration flexibility. ARA slowly disappeared in the late 1990s when TCP/IP took over the vast majority of networking needs, notably remote access. In Mac OS X, ARAP is no longer required, as Apple has migrated their networking software to IP, and includes free remote access software.

AV pairs

(Attribute Value Pairs) AV-pairs are strings of text in the form attribute=value, sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

ARP

(Address Resolution Protocol) A protocol for mapping an IP address to a physical machine address that is recognized in the local network.

Auto-Negotiation

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

Auto MDI / MDIX

Auto MDI/MDIX automatically detects the MDI or MDIX setting on a connecting device in order to obtain a link. This means installers can use either a straight through or crossover cable and when connecting to any device, the feature is pretty self-explanatory.

Authentication

The process of ensuring message integrity and protection against message replays. Authentication includes both data integrity and data origin authentication.

Authoritative SNMP engine

SNMPv3 introduced the concept of an authoritative SNMP engine that lets you create authorized users for specific SNMPv3 agents. One of the SNMP copies involved in network communication designated as the allowed SNMP engine to protect against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (e.g., get exact, get next, set request), the receiver of these messages is authoritative. When an SNMP message does not expect a response, the sender is authoritative.

Bandwidth Profile Traffic Parameters

A Bandwidth profile associated with an Ethernet service consists of four traffic parameters: CIR, CBS, EIR, and EBS. A service frame is also associated with a Color Mode (CM); together, these five parameters specify the bandwidth profile for a particular service (i.e., Bandwidth Profile = CIR, CBS, EIR, EBS, CM).

Big Endian

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

BPC

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

BPDU

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

Bridge

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

CAT 1 – CAT 7 Cabling

ANSI/EIA Standard 568 is one of several standards that specify "categories" (each a "CAT") of twisted pair cabling systems. Assigned by the American National Standards Institute/Electronic Industries Association, these standards categories include CAT 1 – CAT 7, as shown below.

Category	Max Data Rate	Typical Application
CAT 1	Up to 1 Mbps (1 MHz)	Analog voice (POTS), ISDN BRI
CAT 2	4 Mbps	IBM Token Ring network cabling systems
CAT 3	16 Mbps	Voice (analog mainly); 10BASE-T Ethernet
CAT 4	20 Mbps	Used in 16 Mbps Token Ring, but not much else.
CAT 5	100 MHz	100 Mbps TPDDI. 155 Mbps ATM. No longer supported; replaced by 5E. 10/100BASE-T.
CAT 5E	100 MHz	100 Mbps TPDDI, 155 Mbps ATM, Gigabit Ethernet. Offers better near-end crosstalk than CAT 5.
CAT 6	Up to 250 MHz	Minimum cabling required for data centers in TIA-942. Quickly replacing CAT 5e.
CAT 6E	Up to 500 MHz	Field-tested to 500 MHz. Supports 10 Gigabit Ethernet (10GBASE-T). May be either shielded (STP, ScTP, S/FTP) or unshielded (UTP). Standard published in Feb. 2008. The minimum requirement for Data Centers in the ISO Data Center standard.
CAT 7 (ISO Class F)	600 MHz, 1.2 GHz in pairs with Siemon connector	Full-motion video, Teleradiology, Government and manufacturing environments. Fully Shielded (S/FTP) system using non-RJ45 connectors but backwards compatible with hybrid cords. Standard published in 2002. Until Feb. 2008, the only standard to support 10GBASE-T for a full 100m.

CAT 7A/Class FA and Category 6A/Class EA specifications were published in February, 2008.

CE

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

Certificate

A public key certificate - an electronic document which incorporates a digital signature to bind together a public key with an identity (information such as the name of a person or an organization, their address, etc.). The certificate can be used to verify that a public key belongs to an individual without exchanging secret keys. The signatures on a certificate are of a certificate authority (CA) and attest that the identity information and the public key belong together.

CHAP

(Point-to-Point Protocol authentication via Challenge/Handshake Authentication Protocol).

CHAP is used to periodically verify the identity of the peer using a 3-way handshake. CHAP provides protection against playback attack through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges. CHAP authentication depends on a "secret" known only to the authenticator and that peer. The secret is not sent over the link. This method is most likely used where the same secret is easily accessed from both ends of the link.

The CHAP process for connecting to a system includes:

1. After a link is made, the server sends a 'challenge' message to the connection requestor.
2. The requestor responds with a value obtained by using a one-way hash function.
3. The server checks the response by comparing it its own calculation of the expected hash value.
4. If the values match, the authentication is acknowledged; otherwise the connection is typically terminated.

At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP. Compared to PAP, CHAP has a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string). IETF RFC 1334 defines both CHAP and PAP.

CFM

The IEEE 802.1ag standard for Connectivity Fault Management (CFM) divides a network into maintenance domains in the form of hierarchy levels. The levels are allocated to users, service providers, and operators. CFM assigns Maintenance End Points (MEPs) to the edges of each domain, and Maintenance Intermediate Points (MIPs) to ports within domains. This helps define the relationships between all entities from a maintenance perspective, letting each entity monitor the layers under its responsibility and more easily localize problems.

CIR

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

Circuit ID

A company-specific identifier assigned to a data or voice network between two locations. This circuit is then leased to a customer by that ID. If a subscriber has a problem with the circuit, the subscriber contacts the telecommunications provider to provide this circuit id for action on the designated circuit.

Several Circuit ID formats exist (Telephone Number Format, Serial Number Format, Carrier Facility Format and Message Trunk Format). Telecom Circuit ID formats (LEC circuit IDs) provide service codes for DSL, HDSL, ADSL, Digital data, SST Network Trunk, Switched Access, E1, Switched Access, Basic Data

and Voice, LAN, SONET, Ethernet, Video, Voice, Digital Transmission, and others. [Contrast “Device Description”](#).

CLI

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

Communication

In IPv6, any packet exchange among nodes that requires that the address of each node used in the exchange remain the same for the duration of the packet exchange. Examples are a TCP connection or a UDP request- response.

Community

Two levels of ION system access privileges are password protected:

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

Community string

A text string used to authenticate messages between a management station and an SNMP v1/v2c engine.

A Community string is used as the name of the community; it acts as a password by controlling access to the SNMP community.

CoS

(Class of Service) a 3-bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value from 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic. While CoS operates only on Ethernet at the data link layer, other QoS mechanisms (such as DiffServ) operate at the network layer and higher. Others operate on other physical layer. See also ToS and QoS. In MEF terms, CoS is a set of Service Frames that have a commitment from the Service Provider to receive a particular level of performance. See also "QoS".

QoS provides a 'guaranteed' level of service, while CoS provides no explicit guarantee, just a higher level of service at each higher priority.

CoS Queues

Class of Service allows traffic to be directed into different priority levels or “internal queues” in the switch on a particular network transaction. When network traffic congestion occurs, the data assigned to a higher queue will get through first. (Standard: IEEE 802.1p.)

CSA

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

C-Tag

(Customer Tag) When the 0x8100 tag is added twice, the outer tag is called the Provider tag and the inner one is called the Customer IEEE 802.1Q tag. The inner VLAN tag is referred to as the customer VLAN tag (C-Tag) because the customer assigns it. Contrast S-Tag. Before the standardization, some vendors used 0x8100 and 0x9100 for outer Provider tagging. The 0x88A8 tag was adapted by the IEEE later.

The C-Tag is one of several ION system VLAN tagging options. The ION system can provide QinQ service where a frame may contain one or more tags by adding or stripping provider tags on a per-port basis. There are different cases for VLAN service translation options that are possible in the ION system for dealing with C-Tags and S-Tags. Contrast with S-Tag. See also Provider tag.

DAD

(Duplicate Address Detection) - part of the NDP protocol that lets nodes check if an address is already in use.

daemon

A program which services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.

dBm

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

DCE

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

Deprecated address

In IPv6, an address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection).

DES

(Data Encryption Standard) A privacy protocol; one of two encryption algorithms used for ION system data privacy. DES is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official FIPS standard for the US in 1976 and has since enjoyed widespread

use internationally. DES is based on a symmetric-key algorithm that uses a 56-bit key. Despite criticism, DES was approved as a federal standard in 1976, and published in 1977 as FIPS PUB 46, authorized for use on all unclassified data. DES was confirmed as the standard in 1983, 1988 (revised as FIPS-46-1), 1993 (FIPS-46-2), and in 1999 (FIPS-46-3, as "Triple DES"). See also "AES".

DHCP

(Dynamic Host Configuration Protocol) A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

DHCP lets a network administrator supervise and distribute IP addresses from a central point, and automatically sends a new address when a computer is plugged into a different place in the network. (Standard: RFC 2131.)

DiffDerv

In terms of traffic classification, DiffDerv lets a network perform differentiated service treatments.

Discovering / Discovery

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

Down MEP

A MEP residing in a Bridge that receives CFM PDUs from, and transmits them towards, the direction of the LAN. See also Up MEP.

DMI

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

DMM / DMR

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

DNS

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

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

DNS server

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

DoSAP

(Domain Service Access Point) A member of a set of SAPs at which a Maintenance Domain is capable of offering connectivity to systems outside the Maintenance Domain. Each DoSAP provides access to an instance either of the EISS or of the ISS.

Dr. Watson

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

DSCP

DiffServ (Differentiated Services) Prioritization provides the ability to prioritize traffic internally based on the DSCP field in the IP header of a packet. (AKA, DiffServ Modification DSCP / DiffServ. Standard: RFC 3290.)

DST

(Daylight Savings Time) Advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring (March) and are adjusted backward in autumn (November).

DTE

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

dual-stack name server

A name server that is configured to run both IPv4 and IPv6 protocols. IETF RFC 3901 describes a means to maintain name space continuity using administrative policies, for operating DNS where queries and responses are carried in a mixed environment of IPv4 and IPv6 networks.

Dynamic IP addressing

"Dynamic" means moving or changing. A dynamic IP address is an address that is used for the current session only; when the session is terminated, the IP address is returned to the list of available addresses.

If a network uses dynamic addressing, it means that when a network interface asks to join the network, it is randomly allocated an IP address from a pool of available addresses within that network. Thus, under dynamic addressing, a computer may possess over time (e.g. across reboots) a variety of different IP addresses. Dynamic addressing is often used in scenarios where end-user computers are intermittently connected to the network.

The DHCP protocol provides a means to dynamically allocate IP addresses to computers on a network. A system administrator assigns a range of IP addresses to a DHCP server, and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server, which can grant the request. The request and grant process uses a lease concept with a controllable time period.

EEA

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

Egress Frame

A service frame sent from the Service Provider network to the CE. Contrast Ingress Frame.

Egress rules

Egress rules determine which frames can be transmitted out of a port, based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether the frames will be transmitted as tagged or untagged frames.

EIR

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

ELMI Protocols

Enhanced Link Management Interface (ELMI or E-LMI) is the Ethernet Local Management Interface, based on MEF 16. In the ION system, ELMI Protocol disposition (pass or discard) is defined in the L2CP Disposition section of the device port's MAIN tab and at the CLI with the **set l2cp state** command.

ESD

(Electrostatic Discharge) A sudden and momentary electric current that flows between two objects.

EtherType

One of two types of protocol identifier parameters that can occur in Ethernet frames after the initial MAC-48 destination and source identifiers. Ethertypes are 16-bit identifiers appearing as the initial two octets after the MAC destination and source (or after a tag).

Implies use of the IEEE Assigned EtherType Field with IEEE Std 802.3, 1998 Edition Local and Metropolitan Area Networks. The EtherType Field provides a context for interpretation of the data field of the frame (protocol identification). Several well-known protocols already have an EtherType Field.

The IEEE 802.3, 1998 Length/EtherType Field, originally known as EtherType, is a two-octet field. When the value of this field is greater than or equal to 1536 decimal (0600 hexadecimal) the EtherType Field indicates the nature of the MAC client protocol (EtherType interpretation). The length and EtherType interpretations of this field are mutually exclusive.

The ION system **Ether Type** parameters are set at the ION device port's **ADVANCED** tab in the **VLAN Tag Management** section.

ETH-CC

(Ethernet Continuity Check) – the function used for proactive OAM. It detects loss of continuity (LOC) between any pair of MEPs in a MEG. ETH-CC also allows detection of unintended connectivity between two MEGs (Mismerge), unintended connectivity within the MEG with an unexpected MEP (Unexpected MEP), and other defect conditions (e.g., Unexpected MEG level, Unexpected period, etc.). ETH-CC is used for fault management, performance monitoring, or protection switching.

A MEP must always report reception of frames with unexpected ETH-CC information. ETH-CC transmission may be enabled or disabled in a MEG. When ETH-CC transmission is enabled in a MEG, all MEPs are enabled to periodically transmit frames with ETH-CC information to all other MEPs in the MEG. The ETH-CC transmission period is the same for all MEPs in the MEG. When a MEP is enabled to generate frames with ETH-CC information, it is also enabled to receive frames with ETH-CC information from its peer MEPs in the MEG.

When ETH-CC transmission is disabled in a MEG, all MEPs are unable to transmit frames with ETH-CC information. A MIP is transparent to the ETH-CC information and thus does not require any configuration information to support ETH-CC. When a MEP does not receive ETH-CC information from a peer MEP, in the list of peer MEPs, within an interval of 3.5 times the ETH-CC transmission period, it detects loss of continuity to that peer MEP. The interval is equivalent to a loss of 3 consecutive frames carrying ETH-CC information from the peer MEP. The OAM PDU used for ETH-CC information is CCM. Frames that carry the CCM PDU are called CCM frames.

ETH-LB

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

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

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

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

ETH-LT

(Ethernet Link Trace) - an on-demand OAM function that can be used 1) to retrieve adjacency relationship between a MEP and a remote MEP or MIP, and 2) for Fault localization – when a fault (e.g., a link and/or a device failure) occurs, the sequence of MIPs and/or MEP will likely differ from the expected sequence. These differences provide information about the fault location.

ETH-LT request information is initiated in a MEP on an on-demand basis. After transmitting a frame with ETH-LT request information, the MEP expects to receive frames with ETH-LT reply information within a specified period of time. Network elements containing MIPs or MEPs and receiving the frame with ETH-LT request information respond selectively with frames containing ETH-LT reply information.

EUI-64

The 64-bit Extended Unique Identifier (EUI-64) in IPv6.

Event log

Records events such as port link down, configuration changes, etc. in a database.

FCC

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

FDB

The Forwarding Database for an ION system VLAN, identified by a unique FDB ID and kept for a specified aging time.

FDX

(Full Duplex) Communication in both directions simultaneously.

FEF

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

FID

(Forwarding Information Database) The address database in the switch; may be the same as the V-LAN ID (VID) or different, depending on the device.

Filtering Database

When a bridge receives data, it determines to which VLAN the data belongs either by implicit or explicit tagging. In explicit tagging, a tag header is added to the data. The bridge also keeps track of VLAN members in a filtering database which it uses to determine where the data is to be sent. Membership information for a VLAN is stored in a filtering database. The filtering database consists of two types of entries:

- *Static Entries:* Static information is added, modified, and deleted by management only. Entries are not automatically removed after some time (ageing), but must be explicitly removed by management.
- *Dynamic Entries:* Dynamic entries are “learned” by the bridge and cannot be created or updated by management. The learning process observes the port from which a frame with a given source addresses and VLAN ID (VID) is received, and updates the filtering database. The entry is updated only if a) this port allows learning, b) the source address is a workstation address and not a group address, and c) there is space available in the database.

Entries are removed from the filtering database by the aging process where, after a certain amount of time specified by management, entries allow automatic reconfiguration of the filtering database if the topology of the network changes.

Firmware

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

Flow Control

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

FNG alarm

A Fault Notification Generation (FNG) alarm is generated whenever a CCM (Continuity Check Message) is lost.

FNG state

A MEP Fault Notification Generation (FNG) status, either **FNG Reset**, **FNG Defect**, **FNG Report Defect**, **FNG Defect Reported**, or **FNG Defect Clearing**.

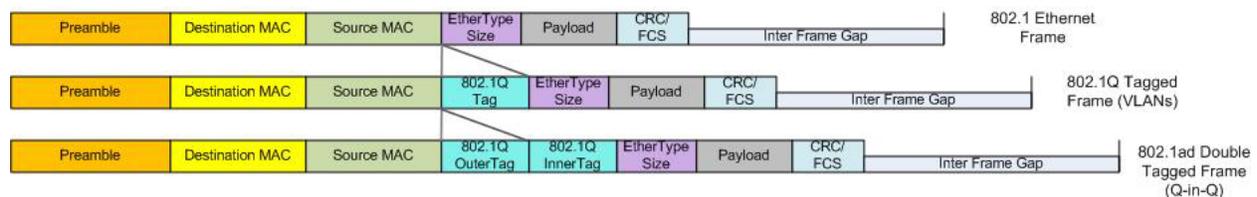
Frame

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

Frame Format

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

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



Frame Loss Ratio

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

Frame Delay

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

FTP

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

GBIC

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

Gbps

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

Global address

In IPv6, an address with unlimited scope.

Group

A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive.

Group Views

The ION system supports three SNMP v3 Views: notifview, readview, and writeview.

GUI

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

Host

In IPv6, any node that is not a router.

HSCP

(High-Security Console Password)

HTML

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

HTTPS

(Hypertext Transfer Protocol Secure) A combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server.

ICMP

(Internet Control Message Protocol) Part of the internet protocol suite that is used by networked computers to send error, control and informational messages indicating, for instance, that a requested service is not available or that a host or router could not be reached.

ICMPv6

(Internet Control Message Protocol version 6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6) defined in RFC 4443.[1] ICMPv6 is an integral part of IPv6 and performs error reporting, diagnostic functions (e.g., ping), and a framework for extensions to implement future changes. Several extensions are published to define new ICMPv6 message types and

options for existing ICMPv6 message types. The Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 that replaces and enhances functions of ARP. Secure Neighbor Discovery Protocol (SEND) is an extension of NDP with extra security. Multicast Router Discovery (MRD) allows discovery of multicast routers.

IEC

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

IEEE

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

IGMP

(Internet Group Management Protocol) A communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

IGMP snooping

Internet Group Multicast Protocol snooping allows a switch to "listen in" on the IGMP conversation between hosts and routers. Based on the query and reports being passed through the switch, a forwarding database for multicast is created.

Informs

One of two types of SNMP notifications that can be sent. See also "traps". An SNMP notification can be sent as a 'trap' or an 'inform'. Traps are less reliable since the trap receiver does not send acknowledgments when it receives traps. The trap sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, making informs more likely to reach their intended destination. However, informs use more agent and network resources. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received, otherwise the request times out. Also, a trap is sent only once, while an inform may be retried several times.

The ION SNMPv3 feature provides users SNMP v1/v2c/v3 access to manage the ION system through the IONMM. Any ION defined traps can be sent to the configured trap servers in v1 or v2c or v3 format through the IONMM. If the IONMM sends out v2c/v3 informs, the trap servers will send responses.

Ingress

The direction from the CE into the Service Provider network. Contrast Egress.

Ingress rules

A means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame.

Interface

In IPv6, a node's attachment to a link.

Interface identifier - in IPv6, a link-dependent identifier for an interface that is (at least) unique per link. Stateless address autoconfiguration combines an interface identifier with a prefix to form an address. In address autoconfiguration, an interface identifier is a bit string of known length. The exact length of an interface identifier and the way it is created is defined in a separate link-type specific document that covers issues related to the transmission of IP over a particular link type. In many cases, the identifier will be the same as the interface's link-layer address.

Invalid address

In IPv6, an address that is not assigned to any interface. A valid address becomes invalid when its valid lifetime expires. Invalid addresses should not appear as the destination or source address of a packet. In the former case, the internet routing system will be unable to deliver the packet, in the latter case the recipient of the packet will be unable to respond to it.

IP

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

IPv6

(Internet Protocol version 6) - The Version 6 IP protocol for Next Generation (IPng).

IPv6 Header

The IPv6 Header format is shown below - from RFC 2460 - IPv6 Specification (Dec. 1998):

The IPv6 header fields are:

- Version: The 4-bit Internet Protocol version number (6).
- Traffic Class: An 8-bit traffic class field.
- Flow Label: A 20-bit flow label.
- Payload Length: the 16-bit unsigned integer. The Length of the IPv6 payload (i.e., the rest of the packet following this IPv6 header, in octets. Note that any extension headers present are considered part of the payload (i.e., included in the length count).
- Next Header: An 8-bit selector that identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.

- **Hop Limit:** An 8-bit unsigned integer decremented by 1 by each node that forwards the packet. The packet is discarded if the Hop Limit is decremented to zero.
- **Source Address:** The 128-bit address of the originator of the packet.
- **Destination Address:** The 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

A full IPv6 implementation also includes these six extension headers: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, and Encapsulating Security Payload headers. Unlike IPv4, IPv6 nodes are not required to enforce a maximum packet lifetime, which is why the IPv4 "Time to Live" field was renamed "Hop Limit" in IPv6.

IPC

(Interprocess Communications) The exchange of data between one program and another either within the same computer or over a network. It implies a protocol that guarantees a response to a request.

IP Stacking

The capability to stack multiple switches together and manage them under one IP address.

IPToS

(IP Type of Service) Prioritization - The ability to prioritize traffic internally based on the IPToS field in the IP header of a packet.

IPv4

(Internet Protocol version 4) the primary Internet protocol used today. An IPv4 address has 32 bits.

ITU

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

ITU-T OAM Performance Monitoring

OAM functions for performance monitoring allow measurement of different performance parameters. The performance parameters are defined for point-to-point ETH connections. This covers Frame Loss Ratio and Frame Delay parameters. An additional performance parameter, Throughput, is identified per RFC 2544.

Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size, which is 1518 bytes (1522 if VLAN-tagged). Though this is not a standard, more vendors are adding support for jumbo frames. An initiative to increase the maximum size of the MAC Client Data field from 1500-bytes to 9000-bytes. The initiative was not adopted by the IEEE 802.3 Working Group, but it was endorsed by a number of other

companies. Larger frames would provide a more efficient use of the network bandwidth while reducing the number of frames that have to be processed. The Jumbo Frame proposal restricts the use of Jumbo Frames to full-duplex Ethernet links, and defines a "link negotiation" protocol that allows a station to determine if the station on the other end of the segment is capable of supporting Jumbo Frames.

Kbps

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

L2/L3/L4 Access Control List Port Based ACLs

ACLs allow administrators to create permit and deny lists based on various traffic characteristics such as Source MAC, Destination MAC, Source IP, Destination IP, and UDP/TCP ports.

L2CP

(Layer 2 Control Protocol) – a network control protocol standardized by the IETF, IEEE and MEF.

The IETF, in an Internet-Draft, defined a framework for a Layer 2 Control Protocol (L2CP) mechanism between a service-oriented layer 3 edge device and a layer 2 Access Node in a multi-service architecture. This mechanism allows QoS-related, service-related, and subscriber-related operations.

The MEF and IEEE 802.1 terms are related as follows:

<u>MEF Term</u>	<u>IEEE 802.1 Term</u>
Peer	Participate
Tunnel	Forward (relay)
Discard	Not forward, Not participate

LAN

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

L2CP Service Frame

A Service Frame that is used for Layer 2 control (e.g., Spanning Tree Protocol).

L2CP Service Frame Delivery

The process by which a Layer 2 Control Protocol Service Frame is passed through the Service Provider network switches without being processed by those switches and delivered to the proper UNI(s).

L2CP Tunneling

The process by which a Layer 2 Control protocol Service Frame is passed through the Service Provider network without being processed and delivered unchanged to the proper UNI(s).

LA

(Link Aggregation) Allows one or more links to be aggregated together to form a Link Aggregation Group, so a MAC Client can treat the Link Aggregation Group as if it were a single link. LA specifies the establishment of data terminal equipment (DTE) to DTE logical links, consisting of n parallel instances of full duplex, point-to-point links operating at the same data rate. The IEEE standard defines the MAC independent Link Aggregation capability, and general information relevant to specific MAC types that support Link Aggregation. Link Aggregation allows full duplex point-to-point links that have a higher aggregate bandwidth than the individual links that form the aggregation. This provides improved utilization of available links in a bridged LAN environment, plus improved resilience in handling individual link failures. Link aggregation, at times referred to as 'trunking', 'muxing' or 'bonding', increases the capacity and availability of a channel between devices using existing hardware.

LACP

(Link Aggregation Control Protocol) A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.

LACP lets you bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. (Standard: IEEE 802.3ad.)

LAN

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

Last Gasp

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

Layer 2 Switch

A network device that functions as multi-port switch.

Layer 3 Switch

A network device that functions as a router and a multi-port switch.

Layer 4 Switch

A switch that makes forwarding decisions taking Layer 4 protocol information into account.

LBM

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

LBR

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

LED

(Light Emitting Diode) An electronic light source.

Link

In IPv6, a communication facility or medium over which nodes can communicate at the link layer (i.e., the layer immediately below IPv6). Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.

Link MTU

The IPv6 Maximum Transmission Unit - the maximum packet size in octets that can be conveyed over a link.

Link-layer address

In IPv6, a link-layer identifier for an interface. Examples include IEEE 802 addresses for Ethernet links and E.164 addresses for ISDN links.

Link-local address

One of IPv6 addresses for local link usage. In IPv6, an address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address.

In IPv6, the two types of local-use unicast addresses defined are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Reference IETF RFC 2373. See also "Site-Local unicast address".

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present. Routers must not forward any packets with link-local source or destination addresses to other links. All interfaces are required to have at least one link-local unicast address.

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. Globally-connected sites typically use the same subnet IDs for site-local and global prefixes.

Routers must not forward any packets with site-local source or destination addresses outside of the site.

Little Endian

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

LLDP

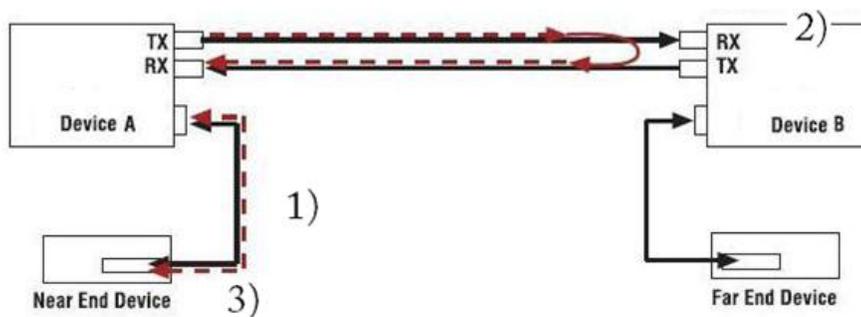
(Link Layer Discovery Protocol) A standard method for Ethernet Network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the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

LOAM

(Link OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.3ah OAM. The major features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, and Remote Loopback. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to SOAM.

Loopback (LB)

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



- 1) Test signal inserted by near end device.
- 2) Device B set to remote loopback on Fiber.
- 3) Returned test signal received by near end device.

LPT

(Link Pass Through) A troubleshooting feature that allows a device to monitor both the fiber and copper RX ports for loss of signal. In the event of a loss of RX signal on one media port, the device will automatically disable the TX signal of the other media port, thus “passing through” the link loss.

LTM

(Linktrace Message) A CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR.

LTR

(Linktrace Reply) A unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP.

MA

(Maintenance Association) A set of MEPs, each configured with the same MAID and MD Level, established to verify the integrity of a single service instance. An MA can also be thought of as a full mesh of Maintenance Entities among a set of MEPs so configured.

MAC

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

MAC-based Security

the ability to lock the learning mechanism down on a port. This means that no further MACs will be learned on those ports. (AKA, MAC Lockdown.)

MAC Table Size

the location where switches store learned addresses. The size of the MAC table determines how many unicast streams the switch can support without flooding. (AKA, FDB (Forwarding Data Base) table, CAM table, MAC.)

Mbps

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

MD

(Maintenance Domain) The network or the part of the network for which faults in connectivity can be managed. The boundary of a Maintenance Domain is defined by a set of DoSAPs, each of which can become a point of connectivity to a service instance.

MD5

(Message-Digest algorithm 5) An authentication protocol; one of two cryptography methods used for ION system user authentication. MD5 is a widely used cryptographic hash function with a 128-bit hash value. Specified in RFC 1321, MD5 is used in a wide range of security applications, and is also commonly used to check file integrity. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. MD5 was designed by Ron Rivest in 1991 to replace the earlier hash function MD4. See also "SHA".

MDI

(Medium Dependent Interface) A type of Ethernet port connection using twisted pair cabling. The MDI is the component of the media attachment unit (**Error! Reference source not found.**) that provides the physical and electrical connection to the cabling medium. MDI ports connect to MDIX ports via straight-

through twisted pair cabling; both MDI-to-MDI and MDIX-to-MDIX connections use crossover twisted pair cabling. See also MDIX.

The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX). The x323x device's *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection.

MDIX

(MDI Crossover) A version of MDI that enables connection between like devices. The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX).

The x323x device's *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection. See also MDI.

ME

(Maintenance Entity) An entity that requires management and is a relationship between two maintenance entity group (MEG) end points. MEs in Ethernet networks can nest but not overlap.

MEG

(Maintenance Entity Group) A ME Group (MEG) consists of the MEs that belong to the same service inside a common OAM domain.

MEG Level

The MEG Level is used to distinguish between OAM frames belonging to different nested MEs. MEs belonging to the same MEG share a common MEG Level. Eight MEG Levels have been identified for the purposes of Ethernet OAM.

When a Subscriber, Service Providers, and Network Operators share the MEG Levels space, allocation of MEG Levels can be negotiated between the various roles involved. A default allocation of MEG Levels is such that Service OAM frames for a Subscriber ME use MEG Level 7, 6 or 5; Service OAM frames for an EVC ME use MEG Level 3 or 4 as EVC ME belongs to a Service Provider OAM Domain; and Operator MEs use MEG Levels 2, 1, or 0. The MEG Levels used for UNI ME and NNI ME default to 0. Note that this default allocation of MEG Level space between Subscribers, Service Providers and Operators could change based on a mutual agreement between them.

MEP

(Maintenance end point) An inward-facing point at the edge of the domain that defines the boundary and confines CFM messages within these boundaries. Inward facing means that they communicate through the relay function side, not the wire side (connected to the port).

See also MIP, Down MEP, and Up MEP.

A MEG End Point (MEP) is a provisioned OAM reference point which can initiate and terminate proactive OAM frames. A MEP can also initiate and react to diagnostic OAM frames. A Point-to-Point EVC has two MEPs, one on each end point of the ME. A Multipoint-to-Multipoint EVC of n UNIs has n MEPs, one on each end point.

MHF

(MIP Half Function) A MIP consists of two MIP Half Functions (MHFs) on a single Bridge Port, an Up MHF and a Down MHF. An MHF may maintain a MIP CCM Database, separate from the MEP CCM Databases.

MIB

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

MIBs stem from the OSI/ISO Network management model and are a type of database used to manage the devices in a communications network. A MIB comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using a subset of Abstract Syntax Notation One (ASN.1) called "Structure of Management Information Version 2 (SMIV2)" RFC 2578. The database is hierarchical (tree-structured) and entries are addressed through object identifiers. IETF RFCs discuss MIBs, notably RFC 1155, "Structure and Identification of Management Information for TCP/IP based internets", RFC 1213, "Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, "A Simple Network Management Protocol".

MIB Module

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

MIB modules usually contain object definitions, may contain definitions of event notifications, and sometimes include compliance statements specified in terms of appropriate object and event notification groups. As such, MIB modules define the management information maintained by the instrumentation in managed nodes, made remotely accessible by management agents, conveyed by the management protocol, and manipulated by management applications. MIB modules are defined according to the rules defined in the documents which specify the data definition language, principally the SMI as supplemented by the related specifications.

MIB object identifier

See "OID".

MIB variable

See "OID".

MIP

(Maintenance intermediate point) – A point internal to a domain, not at the boundary, that responds to CFM only when triggered by trace route and loopback messages. MIPs forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level, and forward all CFM frames at a higher level, regardless of whether they are received from the relay or wire side.

A MEG Intermediate Point (MIP) is a provisioned OAM reference point that can react to diagnostic OAM frames initiated by MEPs. A MIP does not initiate proactive or diagnostic OAM frames. See also MEP.

MLD

(Multicast Listener Discovery) - a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link (much as IGMP is used in IPv4). MLD is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3. The MLD protocol is described in RFC 3810 which was updated by RFC 4604. Windows Vista and later support MLDv2. FreeBSD 8 includes support for MLDv2. The Linux kernel has supported MLDv2 since v 2.5.68.

MSA

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

MSDU

(MAC Service Data Unit) The service data unit that is received from the logical link control (LLC) sub-layer which lies above the medium access control (MAC) sub-layer in a protocol stack (communications stack).

MT-RJ

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

Multicast

One of the four forms of IP addressing, each with its own unique properties, a multicast address is associated with a group of interested receivers. Per RFC 3171, addresses 224.0.0.0 through 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4. The sender sends a single datagram (from the sender's unicast address) to the multicast address, and the intermediary routers take care of making copies and sending them to all receivers that have registered their interest in data from that sender. See also "Unicast".

Multicast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

Multicast destination

A multicast IP address indicating all hosts and routers that are members of the corresponding group. See also Unicast destination.

Multi-point MEG

A MEG with more than one peer MEP. Contrast Point-to-point MEG.

MVRP

(Multiple VLAN Registration Protocol) a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches. It was defined in the IEEE 802.1ak amendment to 802.1Q-2005 standard. MVRP provides a method to dynamically share VLAN information and configure the needed VLANs within a layer 2 network.

NAS

(Network Access Server), a TN, Cisco, or other device, or any other client which makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets. Servers using RADIUS or TACACS protocol are often called NAS (Network Access Server), not to be confused with NAS (Network Attached Storage).

Native VLAN

The initial VLAN to which a switch port belonged before becoming a trunking port. If the trunking port becomes an access port, in most of the cases, that port will go back to its native VLAN. Traffic coming from the initial VLAN is untagged. To avoid VLAN hopping, do not to use this VLAN for other purposes.

NDP

(Neighbor Discovery Protocol) - a protocol in the Internet Protocol Suite used with IPv6. NDP operates in the Link Layer and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and DNS servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes per IETF RFC 4861.

Neighbors

In IPv6, nodes attached to the same link.

NIC

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

NID

(Network Interface Device) A device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In telecommunications, a NID is a device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In fiber-to-the-premises systems, the signal is transmitted to the customer premises using fiber optic technologies.

In general terms, a NID may also be called a Network Interface Unit (NIU), Telephone Network Interface (TNI), Slide-in-card (SIC), or a slide-in-module.

NMS

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

Node

In IPv6, a device that implements IPv6.

Non Intrusive test

Ability to troubleshoot a circuit while it is in use.

Notification

An SNMP trap or inform message. See also "traps" and "informs". SNMP notifications can be sent as traps or informs. Traps are less reliable since the receiver does not send an acknowledgment when it receives a trap (the sender cannot tell if the traps were received). However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again (making informs more likely to reach their intended destination). On the other hand, informs use more agent and network resources. While a trap is discarded as soon as it is sent, an inform request is held in memory until a either response is received or the request times out. Note also that traps are sent only once, while an inform may be resent several times. These inform retries increase traffic and contribute to a higher overhead on the network.

Notification host

An SNMP entity to which notifications (traps and informs) are to be sent.

Notifview

An SNMP v3 string of up to 64 characters that is the name of the view that enables you to specify a notify, inform, or trap. The default notifview is 'nothing' (i.e., the null OID). If a view is specified, any notifications in that view that are generated are sent to all users associated with the group (provided an SNMP server host configuration has been created for the user).

Notify view

A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group.

NTP

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

OAM

(Operation, Administration and Maintenance) A group of network management functions that provide network fault indications, performance information, data, and diagnosis. Since Ethernet OAM functions are not designed to work completely over half-duplex interfaces, the value NonOperHalfDuplex is returned whenever Ethernet OAM is enabled ('Admin Status' is Enabled) but the interface is in half-duplex operation.

OAM Event

The following OAM event types are defined and logged in the ION system:

- Errored Symbol Event
- Errored Frame Period Event
- Errored Frame Event
- Errored Frame Seconds Event
- Link Fault
- Dying Gasp Event
- Critical Link Event

The first four are considered threshold crossing events, as they are generated when a metric exceeds a given value within a specified window. The other three are not threshold crossing events.

OAMPDU

(Ethernet OAM protocol data unit) The mechanism by which two directly connected Ethernet interfaces exchange OA information.

OID

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

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

OSI

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

OUI

(Organizationally Unique Identifier) the Ethernet Vendor Address component. Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the

station) and the last/right 6 digits, which specify the interface serial number for that interface vendor. These high-order 3 octets (6 hex digits) are called the Organizationally Unique Identifier or OUI.

Packet

An IPv6 header plus payload.

PAP

(Point-to-Point Protocol authentication via Password Authentication Protocol) provides a simple method for the peer to establish its identity using a 2-way handshake. This is done only after initial link establishment. After link establishment is done, an ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated. PAP is not a strong authentication method. Passwords are sent over the circuit "in the clear", and there is no protection from playback or repeated trial and error attacks. The peer is in control of the frequency and timing of the attempts. PAP works like a standard login procedure; the remote system authenticates itself to the using a static user name and password combination. The password can be encrypted for additional security, but PAP is subject to numerous attacks. In particular, since the information is static, it is subject to password guessing as well as snooping. IETF RFC 1334 defines both PAP and CHAP.

Path MTU

The minimum IPv6 link MTU of all the links in a path between a source node and a destination node.

Pause

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

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

PD

(Powered Device) Modules that are designed to extract power from a conventional twisted pair Category 5 Ethernet cable. All PD modules are IEEE802.3af compatible, with built-in signature chip, output voltage adjustment and class programming.

PDU

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

PID

(Priority ID) on the x323x NID, the PID is configured at the ADVANCED tab in the "IEEE Priority Class" section; the selections are Remap 0 to: (PID) 0123.

PID

(Process ID) in Netstat, the -o option displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).

Port-Based Rate Limiting

The ability to regulate throughput on a per-port basis. (AKA, metering, Rate Limiting.)

Port Labeling

The ability to assign names to ports through the management interface.

Preferred address

In IPv6, an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface.

Preferred lifetime

In IPv6, the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.

Primary VID

The VID, among a list of VIDs associated with a service instance, on which all CFM PDUs generated by MPs except for forwarded LTM are to be transmitted.

Priority-tagged frame

A tagged frame whose tag header carries priority information, but carries no VLAN identification information. Note: Priority tagged frames, which, by definition, carry no VLAN identification information, are treated the same as untagged frames for the purposes of VLAN identification. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. These frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).

Privacy

An encrypted state of the contents of an SNMP packet where they are prevented from being disclosed on a network. Encryption is performed with algorithms called DES or AES.

Protocol Endpoint

A communication point from which data may be sent or received. It represents communication points at various levels on an Open Systems Interconnection (OSI) structure.

Provider Tag

When the 0x8100 tag is added twice, the outer one is called the Provider tag and the inner one is called the Customer IEEE 802.1Q tag. Before the standardization, some vendors used 0x8100 and 0x9100 for outer Provider tagging. The 0x88A8 tag was adapted by the IEEE later. See also 'Customer tag'.

Provisioning

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

PSE

(Power Sourcing Equipment) In power over Ethernet (PoE), equipment that serves as power injectors to provide output of 48V DC power over the twisted-pair cable plant to terminal units with PoE compliant devices known as powered devices (PDs). For devices not PoE-compliant, splitters inserted into the Ethernet cabling provide 12V or 6V DC output.

PVID

(Port VID) A default VID that is assigned to an access port to designate the virtual LAN segment to which this port is connected. The PVID places the port into the set of ports that are connected under the designated VLAN ID. Also, if a trunk port has not been configured with any VLAN memberships, the virtual switch's PVID becomes the default VLAN ID for the ports connection.

PVLAN

(Private Virtual-LAN) a non-standardized way of segmenting ports into separate groups. (Contrast "802.1Q VLAN".)

Q-in-Q (or "QinQ" or "Q in Q")

(IEEE 802.1Q in 802.1Q) an Ethernet networking standard for Ethernet frame formats (actually, 802.1Q-in-Q is an amendment to IEEE 802.1Q, and not a separate specification). It is also known simply as "QinQ" or "Q in Q". The original 802.1Q specification allows a single VLAN header to be inserted into an Ethernet frame. Q-in-Q allows multiple VLAN headers to be inserted into a single frame. In the context of an Ethernet frame, a Q-in-Q frame has 2 VLAN 802.1Q headers (i.e., the Q-in-Q frame is 'double-tagged').

QoS

(Quality of Service) A mechanism to allow different classes of services to the customers. The QoS varies on a per customer basis, depending on their Service Level Agreement (SLA) they chose, and the kind of service they want. Customer traffic priorities are assigned based on their SLAs. QoS is standardized at both layer 2 and layer 3.

Service providers offering Layer 2 services can use the IEEE 802.1 Q/p standard for QoS.

It allows a service provider to attach special tags, called VLAN IDs, to all incoming frames from a customer. With this, the service provider can have multiple customers using the same circuit, but still maintain separation between them. Each customer's traffic is identified by a different VLAN tag. The method also allows for the addition of a priority value to be associated to the VLAN tag. By using the priority field, service providers can offer various classes of service.

The two current Layer 3 (IP) QoS standards are IETF RFC-791, which defines the ToS, and RFC-2475, which defines DSCP. Both standards use the same field in the IP packet header to identify the level of service for the packet.

The various QoS parameters (either for Layer 2 or 3) are stored as part of the overhead in the transmitted frames. See also CoS and ToS.

RADIUS

(Remote Authentication Dial In User Service) Is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service. The RADIUS protocol does not transmit passwords in cleartext between the NAS and RADIUS server (not even with PAP protocol). Rather, a shared secret is used along with the MD5 hashing algorithm to obfuscate passwords.

RADIUS has been officially assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting by the IANA. However, prior to IANA allocation of ports 1812 and 1813, ports 1645 (authentication) and 1646 (accounting) were unofficial default ports assigned by many RADIUS Client/Server implementations at the time. Ports 1645 and 1646 are still used for backwards compatibility.

Read view

An SNMP View name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the Group.

A Readview is a string of up to 64 characters that is the name of the view that enables you only to view the contents of the agent. The default readview is assumed to be every object belonging to the Internet (1.3.6.1) OID space, unless you use the read option to override this state.

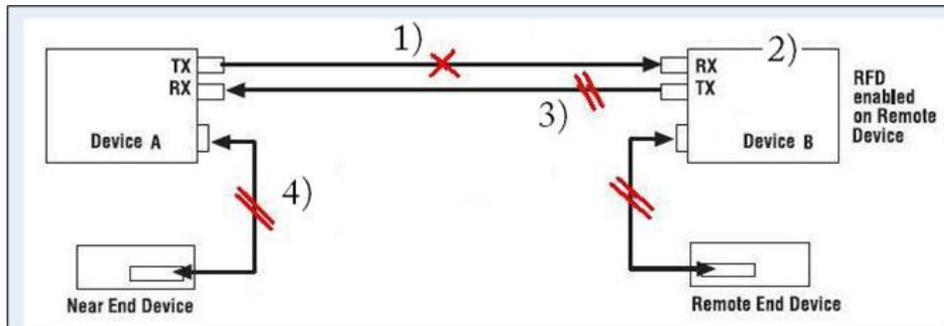
Redundancy

The Fiber Redundancy feature is designed to allow customer traffic and CPU-centric protocols to survive a fault on an uplink port by placing the traffic on a secondary backup port.

On the ION system, the Fiber Redundancy feature adds a form of automatic protection switching using a LOS mechanism that triggers the switch to the surviving line. The ION system uses 1:1 protection, with a modified form of bi-directional switching. TLPT and SLPT are operational with fiber redundancy enabled or disabled. The fault discovery method is LOS at the receiving interface for a set continuous period of time. Traffic rerouting occurs within a minimum period of time after the Primary Port is declared in the fault state. Traffic flow is restored within a minimum set period of time after a fault occurs.

RFD

(Remote Fault Detect) a troubleshooting feature found on Gigabit Ethernet copper-to-fiber media converters and NIDs. By enabling Remote Fault Detect on the remotely located device, the status of the fiber link will be monitored and any link failures will be reported back to the local converter. Should the remote converter lose its fiber RX signal, Remote Fault Detect will force the converter to shut down its fiber TX port. If Link Pass Through is enabled on both ends, then the copper ports will also be shut down to notify both end devices of the link failure. When you enable Remote Fault Detect on the remote device, the local end-device will be notified of remote fiber RX loss.



- 1) Device B loses Fiber link.
- 2) Device A disables its TX copper port via Link Pass Through (LPT) to alert the remote end device (Device A) of link loss.
- 3) Device B disables its Fiber TX port to alert Device A of link loss.
- 4) Device A disables its TX copper port via LPT to alert the Local end device of link loss.

RJ-45

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

RMON

(Remote Network Monitoring) Software that supports the monitoring and protocol analysis of LAN. A part of SNMP, RMON is a network management protocol that gathers remote network information. (Standard: RFC 1271.)

Router

In IPv6, a node that forwards IPv6 packets not explicitly addressed to itself.

RS-232

(Recommended Standard 232) A standard for serial binary data signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

SAP

(Service Access Point) The point at which an Ethernet service is offered.

Security model

The security strategy used by the SNMP agent. Currently, ION supports three security models: SNMPv1 and SNMPv2c.

Self-signed certificate

An identity certificate that is signed by its own creator. That is, the person that created the certificate also signed off on its legitimacy. Such certificates are also called 'root certificates'.

Sender ID

Defined in RFC 4406, Sender ID is a Microsoft protocol derived from SPF (hence the identical syntax), which validates one of a message's address header fields defined by RFC 2822. Which header field it validates is selected according to the PRA (Purported Responsible Address) algorithm per RFC 4407. The PRA algorithm selects the header field with the e-mail address responsible for sending the message. Sender ID can be compared to other RFC 2822 layer protocols like DomainKeys IM (DKIM). The purpose of Sender ID is to help fight spoofing, one of the major deceptive practices used by spammers. Sender ID works by verifying that each e-mail message did indeed originate from the Internet domain from which it was sent. See <http://www.ietf.org/rfc/rfc4406.txt> and <http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspix> for more information.

SFP

(Small Form-Factor Pluggable) A compact, hot-pluggable transceiver used in telecommunication and data communications applications. It interfaces a network device mother board (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. The SFP transceiver is specified by a multi-source agreement (MSA) between competing manufacturers. The SFP was designed after the GBIC interface, and allows greater port density (number of transceivers per inch along the edge of a mother board) than the GBIC, thus SFP is also known as "mini-GBIC". Optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature lets you monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. AKA, Digital Optical Monitoring (DOM), DMI (Diagnostic Monitoring Interface), or DMM (Diagnostic Maintenance Monitoring).

SFP+

SFP+ is an enhanced version of the SFP that supports data rates up to 10 Gbit/s. SFP+ supports 8 Gbit/s Fibre Channel, 10-gigabit Ethernet and Optical Transport Network standard OTU2. It is a popular industry format supported by many network component vendors. Initial standard applications focused on 8G Fibre Channel, 10G Ethernet and 10G Fibre Channel, where the electrical interface to the host board is a standardized serial interface called SFI. The applications have expanded to include SONET OC-192, SDH STM-64, OTN G.709, CPRI wireless, 16G Fibre Channel, and the emerging 32G Fibre Channel application.

SFP28

SFP28 is a 25 Gbit/s interface which has evolved from 100 Gigabit Ethernet, typically implemented with 4 × 25 Gbit/s data lanes. Identical in mechanical dimensions to SFP and SFP+, SFP28 implements one 28 Gbit/s lane (25 Gbit/s + error correction) for top-of-rack switch to server connectivity. SFP28 may also be used to "break out" a single 100GbE port in a top-of-rack switch into four 25 Gbit/s individual server connections. SFP28 functions with both optical and copper interconnects.

SGMII

(Serial Gigabit Media Independent Interface) A standard Gigabit Ethernet interface used to connect an Ethernet MAC-block to a PHY. To carry frame data and link rate information between a 10/100/1000 PHY and an Ethernet MAC, SGMII uses a different pair for data signals and for clocking signals, with both being present in each direction (i.e., TX and RX). The x323x NIDs have SGMII support for use with 10/100/1000BASE-T copper SFPs. The x323x uses the **set ether phymode=SGMII** CLI command to select SGMII mode.

SHA

(Secure Hash Algorithm) An authentication protocol; one of two cryptography methods used for ION system user authentication. SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. FIPS standard. SHA-1 is part of many widely accepted security applications and protocols (e.g., TLS, SSL, PGP, SSH, S/MIME, and IPSec). See also "MD5".

Site-Local address

An IPv6 address for a local site only. In IPv6, an address having scope that is limited to the local site. In IPv6, the two types of local-use unicast addresses defined are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Reference IETF RFC 2373. See also "Link-Local unicast address".

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present. Routers must not forward any packets with link-local source or destination addresses to other links. All interfaces are required to have at least one link-local unicast address.

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. Globally-connected sites typically use the same subnet IDs for site-local and global prefixes.

Routers must not forward any packets with site-local source or destination addresses outside of the site.

SLA

(Service Level Agreement) In general terms, a part of a service contract where the level of service is formally defined in terms of a contracted delivery time or performance. In Metro Ethernet, the contract between the Subscriber and Service Provider specifying the agreed to service level commitments and related business agreements.

SMAC

(Static MAC) A MAC address that is manually entered in the address table and must be manually removed. It can be a unicast or multicast address. It does not age and is retained when the switch restarts. You can add and remove static addresses and define the forwarding.

SMIv2

RFC 2580 ("Conformance Statements for SMIv2") defines the format for compliance statements which are used for describing requirements for agent implementations and capability statements which can be used to document the characteristics of particular implementations. The term "SMIv2" is somewhat ambiguous because users of the term intend it to have at least two different meanings. Sometimes the term is used to refer to the entire data definition language of RFCs 2578 - 2580 while other times it is used to refer to only the portion of the data definition language defined in RFC 2578. According to the IETF, this ambiguity is unfortunate but is rarely a significant problem in practice. The SMI is divided into three parts (module definitions, object definitions, and notification definitions).

SNMP

(Simple Network Management Protocol) A request-response protocol that defines network communication between a Managed Device and a Network Management Station (NMS). A set of protocols for managing complex IP networks. (Standard: RFC 1157.) A protocol for network management that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. Various SNMP versions exist.

SNMP engine

A copy of SNMP that can reside either on the local or remote device.

SNMP group

A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes defined by the group.

SNMP Message

A sequence representing the entire SNMP message, which consists of the SNMP version, Community String, and SNMP PDU.

SNMP SMI

(SNMP Structure of Management Information) a collection of managed objects, residing in a virtual information store. The SMI is divided into three parts: module definitions, object definitions, and, notification definitions. There are two types of SMI: SMIv1 and SMIv2. For additional information see IETF RFC 1155 v1 and RFC 2578 v2.

SNMP Version

An integer that identifies the version of SNMP (e.g., SNMPv1 = 0).

SNMP Community String

An Octet String that may contain a string used to add security to SNMP devices.

SNMP PDU

An SNMP PDU contains the body of an SNMP message. There are several types of PDUs (e.g., GetRequest, GetResponse, and SetRequest).

SNMP User

A person for which an SNMP management operation is performed. For informs, the user is the person on a remote SNMP engine who receives the informs.

SNMPv1

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

SNMPv2

(SNMP version 2) the SNMPv2 Framework as derived from the SNMPv1 Framework. It is described in STD 58, RFCs 2578, 2579, 2580, and RFCs 1905-1907. SNMPv2 has no message definition.

SNMPv2c

(Community-based SNMP version 2) an experimental SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to 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.

SNMPv2c (SNMPv2 with community-based security) SNMPv2c had the most support within the IETF but had no security and administration whereas both SNMPv2u and SNMPv2* had security but lacked IETF support consensus.

SNMPv3

(SNMP version 3) an extensible SNMP Framework which supplements the SNMPv2 Framework by supporting a new SNMP message format, Security for Messages, Access Control, and Remote configuration of SNMP parameters. The SNMPv3 protocol adds encryption and authentication mechanisms into the SNMP protocol for a secure management protocol where SNMP agents cannot be accessed by unauthorized parties.

SNMP View

A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

SNTP

(Simple Network Time Protocol) A less complicated version of Network Time Protocol, which is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled via the Internet. SNTP is used to synchronize times on IP devices over a network. (Standard: RFC 2030.)

SOAM

(Service OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.1AG.

Ethernet CFM comprises three protocols that work together to help administrators debug Ethernet networks: continuity check, link trace and loopback protocols. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to LOAM.

Solicited-node multicast address

In IPv6, a multicast address to which Neighbor Solicitation messages are sent. The algorithm for computing the address is given in Discovery.

SSH

(Secure Shell) A network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet. SSH is used to provide a secure Telnet session to the console/command line interface of a network device through an insecure environment. (AKA, Secured Telnet; Standard: SSH RFC 1034).

SSL

(Secure Socket Layer) A protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data; a public key known to everyone and a private or secret key known only to the recipient of the message. SSL is used to manage a network device via its web interface. (AKA, HTTPS, Standard: RFC 2818).

S-Tag

(Service VLAN Tag) The outer VLAN tag is referred to as the Service provider VLAN tag (S-Tag) and it uniquely identifies a given customer within the network of the service provider. It is possible for multiple customer VLANs to be tagged using the same outer or Service provider VLAN tag (S-Tag), thereby trunking multiple VLANs among customer sites.

The S-tag is one of several ION system VLAN tagging options. The ION system can provide QinQ service where a frame may contain one or more tags by adding or stripping provider tags on a per-port basis. There are different cases for VLAN service translation options that are possible in the ION system for dealing with C-Tags and S-Tags. Contrast with “C-Tag”.

Stateless auto-configuration

A process to get IPv6 addresses from IPv6 standards.

Static IP addressing

"Static" comes from the word stationary, meaning not moving. A static IP address means it never changes. A static IP address is an IP address permanently assigned to a workstation. If a network uses static addressing, it means that each network interface has an assigned IP address that it always uses whenever it is online. With static addressing, the computer has a well-defined IP address which it uses always and which no other computer ever uses.

Static MAC Entry

Static MAC entry support means that users can assign MAC addresses to ports manually that never age out.

STID

(Sensor Transaction Identifier) The STID is used for power supply / sensor / IONDCR configuration via the **set sensor stid** command to define notification, relation, severity, and value parameters. The **show power config** command displays the power supply sensors information. The STID is shown in the Web interface at the **Power Supply** tab > **Temp, Volt, Power, and Fan** sub-tabs.

STP

(Spanning-Tree Protocol) A link layer network protocol that ensures a loop-free topology for any bridged LAN. STP prevents loops from being formed when switches are interconnected via multiple paths. STP is a Data Link Layer protocol that was standardized as IEEE 802.1D. STP creates a spanning tree within a mesh network of connected layer-2 bridges (usually Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. With Spanning Tree, a device learns Ethernet (MAC) addresses by inspecting the Ethernet frame and recording the source MAC address in a dynamic table. The device also associates a learned MAC address with a port. The device can then make intelligent forwarding decisions based on the destination MAC address.

The collection of bridges in a LAN can be considered a graph whose nodes are the bridges and the LAN segments (or cables), and whose edges are the interfaces connecting the bridges to the segments. To break loops in the LAN while maintaining access to all LAN segments, the bridges collectively compute a spanning tree (which is not necessarily a minimum cost spanning tree).

The general STP rules describe a way of determining what spanning tree will be computed by the algorithm, but those rules require knowledge of the entire network. The bridges must determine the root bridge and compute the port roles (root, designated, or blocked) with only the information that they have. To ensure that each bridge has enough information, bridges use special data frames called Bridge Protocol Data Units (BPDUs) to exchange information about bridge IDs and root path costs. A bridge sends a BPDU frame using the unique MAC address of the port itself as a source address, and a destination address of the STP multicast address 01:80:C2:00:00:00. See also "BPDU". See also "xSTP".

STP

(Shielded Twisted Pair) A special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground.

S-VLAN

Service VLAN (also referred to as Provider VLAN).

Syslog

(System Logging) a service run mostly on Unix and Linux systems (but also available for other OSes) to track events that occur on the system. Analysis can be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

Can refer to a method of general system logging, a log format, and/or a network log transmission mechanism. The Syslog function is implemented in the ION system via the **set syslog** CLI commands and via the device **MAIN** tab > **System Log Configuration** section parameters.

tacplus

TACACS+ is a protocol for AAA services (Authentication, Authorization, Accounting), very similar to RADIUS. Tacplus is TACACS+ program that provides routers and access servers with authentication, authorization and accounting services. This version is a major rewrite of the original Cisco source code. Key features include NAS specific host keys/prompts/enable passwords, NAS- and ACL-dependent group memberships, Connection multiplexing (multiple concurrent NAS clients per process), Session multiplexing (multiple concurrent sessions per connection, single-connection), IPv4 and IPv6 support, and compliant to latest TACACS+ protocol specification (at the time of publication).

TACACS+ / Tacplus involves:

- A NAS (Network Access Server), such as. a TN, Cisco, or other device, or any other client which makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets. Servers using RADIUS or TACACS protocol are often called NAS (Network Access Server), not to be confused with NAS - (Network Attached Storage).
- A daemon - a program which services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.
- AV pairs - strings of text in the form attribute=value, sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

Note: Since a “NAS” is sometimes referred to as a server, and a “daemon” is also often referred to as a server, the term “server” is avoided here in favor of the less ambiguous terms “NAS” and “Daemon”.

The Tacplus software provides logs for Authentication (authentication log = log_destination), Authorization (authorization log = log_destination), and Accounting (accounting log = log_destination).

Tacplus supports three authentication methods: Clear text, Data Encryption Standard (DES - local and remote), and S/Key.

By default, Tacplus provides authentication services for: 1. VTY login, 2. Point-to-Point Protocol authentication via Password Authentication Protocol (PAP), 3. Point-to-Point Protocol authentication via Challenge/Handshake Authentication Protocol (CHAP), and 4. AppleTalk Remote Access (ARAP).

CHAP and ARAP can only utilize clear text, as required by their protocol definitions. Support for Microsoft CHAP (MSCHAP) is available. Tacplus statuses include: PASS, FAIL, GETDATA, GETUSER, GETPASS, RESTART, ERROR, and FOLLOW.

Tag (IEEE 802.1Q tag)

An IEEE 802.1Q tag, if present, is placed between the Source Address and the EtherType or Length fields. The first two bytes of the 802.1Q tag are the Tag Protocol Identifier (TPID) value of 0x8100. The TPID is located in the same place as the EtherType/Length field in untagged frames, so an EtherType value of 0x8100 means the frame is tagged, and the true EtherType/Length is located after the Q-tag. The TPID is followed by two bytes containing the Tag Control Information (TCI), the IEEE 802.1p priority (QoS) and the VLAN ID. The Q-tag is followed by the rest of the frame.

Tagged frame

A packet that contains a header that carries a VLAN identifier and a priority value. Also called a VLAN tagged packet. A Tagged frame contains a tag header immediately following the Source MAC Address field of the frame or, if the frame contains a Routing Information field, immediately following the Routing Information field. There are two types of tagged frames: VLAN-tagged frames and priority-tagged frames.

Tagging / Tag Header

Sending frames across the network requires a way to indicate to which VLAN the frame belongs, so that the bridge will forward the frames only to those ports that belong to that VLAN, instead of to all output ports. This indication is added to the frame in the form of a tag header. The tag header a) allows user priority information to be specified, b) allows source routing control information to be specified, and c) indicates the format of MAC addresses. Frames in which a tag header has been added are called “tagged” frames. These tagged frames convey the VLAN information throughout the network.

TCP

(Transmission Control Protocol) One of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP.

Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

TCP/IP

(Transmission Control Protocol/Internet Protocol) The basic communication language or protocol of the Internet and/or a private network (either an intranet or an extranet).

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol (TCP), manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol (IP), handles the address part of each packet so that it gets to the right destination.

TDM

(Time Division Multiplexing) A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing.

TDR

1. (Time Domain Reflectometry) A measurement technique used to determine the characteristics of electrical lines by observing reflected waveforms. **2.** (Time Domain Reflector) An electronic instrument used to characterize and locate faults in metallic cables (for example, twisted wire pairs, coaxial cables). It can also be used to locate discontinuities in a connector, printed circuit board, or any other electrical path.

Telnet

A user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. Telnet is a terminal emulation program for TCP/IP networks that runs on your computer and connects your PC to a switch management. (Standard: RFC 854.) Tentative address

In IPv6, an address whose uniqueness on a link is being verified, prior to its assignment to an interface.

A tentative address is not considered assigned to an interface in the usual sense. An interface discards received packets addressed to a tentative address, but accepts Neighbor Discovery packets related to Duplicate Address Detection for the tentative address.

TFTP

(Trivial File Transfer Protocol) A file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). Due to its simple design, TFTP can be implemented using a very small amount of memory. Because it uses UDP rather than TCP for transport, TFTP is typically used to transfer firmware upgrades to network equipment.

TFTP Download / Upload

The ability to load firmware, configuration files, etc. through a TFTP server. (AKA, TFTP. Standard: RFC 1350.)

TFTP Root Directory

The location on the console device (PC) where files are placed when received, and where files to be transmitted should be placed (e.g., *C:\TFTP-Root*).

TFTP Server

An application that uses the TFTP file transfer protocol to read and write files from/to a remote server. In TFTP, a transfer begins with a request to read or write a file, which also serves to request a connection. If the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and must be acknowledged by an acknowledgment packet before the next packet can be sent. Examples of available packages include

Open TFTP Server, Tftpd32, WinAgents TFTP Server for Windows, SolarWinds free TFTP Server, TFTP Server 1.6 for Linux, and TftpServer 3.3.1, a TFTP server enhancement to the standard Mac OSX distribution.

Threshold crossing event

See “OAM Event”.

Throughput

The maximum rate at which no frame is dropped. This is typically measured under test conditions.

TID

(Transaction Identifier) The TID is entered in the CLI command **show soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> tid=<0-4294967295>**. The TID is shown in the Web interface at the **SOAM** tab > **MEP** sub-tab > **Linktrace** sub-tab.

TLS

(Transport Layer Security) A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

TLV

Type, Length, Value format - LLDP frames are sent by each equipment on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type, length, value (TLV) structures. An LLDP frame should start with mandatory TLVs (e.g., Chassis ID, Port ID, and Time to live). These mandatory TLVs are followed by any number of optional TLVs. The frame should end with a special TLV named end of LLDPDU. The IEEE 802.1ab specification contains a description of all of the TLV types.

TNDP

(TN Topology Discovery Protocol) the Lantronix implementation of LLDP. When set to Enabled, the device entering this command will no longer be discovered by the IONMM if it is remotely managed through this port. See also “LLDP” and the “**set tndp**” and “**show tndp**” CLI commands.

TOS

(Type of Service) The ToS byte in the IPv4 header has had several purposes over time, and has been defined in various ways by IETF RFC 791, RFC 1122, RFC 1349, RFC 2474, and RFC 3168. Currently, the ToS byte is a six-bit Differentiated Services Code Point and a two-bit Explicit Congestion Notification field.

The ToS model described in RFC 2474 uses the Differentiated Services Field (DS field) in the IPv4 Header and IPv6 Header. See also CoS and QoS.

TPID

(Tag Protocol Identifier) a field in a VLAN Tag for which IEEE802.1Q specifies a value of 0x8100.

Trap

In SNMP, a trap is a type of PDU used to report an alert or other asynchronous event about a managed subsystem.

Also, a place in a program for handling unexpected or unallowable conditions - for example, by sending an error message to a log or to a program user. If a return code from another program was being checked by a calling program, a return code value that was unexpected and unplanned for could cause a branch to a trap that recorded the situation, and take other appropriate action.

An ION system trap is a one-way notification (e.g., from the IONMM to the NMS) that alerts the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the IONMM rather than the NMS. For a management system to understand a trap sent to it by the IONMM, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Traps

One of two types of SNMP notifications that can be sent. See also "informs".

A "trap" is a one-way notification from the NID to the NMS. Its purpose is to alert the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the Agent rather than the NMS. In order for a management system to understand a trap sent to it by the NID, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Each Trap is an asynchronous notification from agent to manager. Includes current sysUpTime value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.

TCP/UDP Port Prioritization

The ability to prioritize traffic internally based on a TCP or UDP port number. (AKA, Layer 4 Prioritization.)

TTL

(Time to live) an Ethernet counter that records the number of times a transmission is sent/received without errors. TTL specifies how long a datagram is allowed to "live" on the network, in terms of router hops. Each router decrements (reduces by one) the value of the TTL field prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

The default TTL for ION software is 64. This means that a test packet must be successfully sent and received 63 times before a TTL expired message is generated. You can change the TTL value (e.g., a value of 255 is a demanding test because the packet must be sent and received error free 254 times).

Tunnel

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one (as in L2TP and VPN).

Tunneling

Encapsulating one type of packet inside the data field of another packet. This allows transmitting data that is structured in one protocol within the protocol or format of a different protocol. Tunneling can involve most OSI or TCP/IP protocol layers.

UAC

(User Account Control) Technology and security infrastructure of some *Microsoft* operating systems that improve OS security by limiting application software to standard user privileges until an administrator authorizes an increase.

UDP

(User Datagram Protocol) A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

Unicast

One of the four forms of IP addressing, each with its own unique properties. The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient. See also "Multicast".

Unicast address

In IPv6, an identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

Unspecified Address

In IPv6, the address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.

The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing headers. An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router.

Unicast destination

A host or router that can be identified by a unique unicast IP address. See also "Multicast destination".

Untagged frame

A frame that does not contain a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or, through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).

Upper layer

In IPv6, a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.

USB

(Universal Serial Bus) A plug-and-play interface between a computer and add-on devices, such as media players, keyboards, telephones, digital cameras, scanners, flash drives, joysticks and printers.

USM

(User-Based Security Model) The SNMPv3 USM lets you implement authentication and privacy in SNMP communication between agents and managers. For example, IETF RFC 2574 defines the User-based Security Model (USM) for SNMPv3.

SNMPv3's security header implements the User Security Model (USM), which provides confidentiality and integrity for network management communications. Confidentiality is provided through the use of Data Encryption Standard (DES). Although this algorithm is notoriously weak (due to its use of a 40-bit encryption key), it provides a marked advantage over plaintext community strings. The SNMPv3 USM also allows for user-based authentication and access control. Rather than using just the two-level "read" and "write" community strings of prior SNMP implementations, administrators can create specific accounts for each SNMP user and grant privileges through those user accounts.

The USM utilizes MD5 and the SHA as keyed hashing algorithms for digest computation to provide data integrity to directly protect against data modification attacks, to indirectly provide data origin authentication, and to defend against masquerade attacks. Contrast with "VACM".

UTC

(Coordinated Universal Time) A time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich.

UTP

(Unshielded Twisted Pair) The most common form of twisted pair wiring, because it is less expensive and easier to work with than STP (Shielded Twisted Pair). UTP is used in Ethernet 10Base-T and 100Base-T networks, as well as in home and office telephone wiring. The twist in UTP helps to reduce crosstalk interference between wire pairs.

VAC

Volts AC (alternating current, as opposed to DC – direct current).

VACM

(View-Based Access Control Model) a new security feature defined by SNMPv3. Like User-based Security Model (USM) it authenticates, encrypts, and decrypts SNMPv3 packets, as specified in RFC 2575. An SNMP entity's Access Control subsystem checks if a specific type of access to a specific managed object is allowed. Access control occurs in the agent when processing SNMP retrieval or modification request messages from a manager, and when a notification message is sent to the manager. VACM concepts are based the problems with SNMPv1 and SNMPv2c community strings. A community string identifies the requesting entity, the location of the requesting entity, and determines access control information and MIB view information. A single community string variable provides low flexibility and functionality. VACM builds on the community string concept with a stricter, and more dynamic, more easily administered access control model. Contrast with "USM".

Valid address

In IPv6, 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.

Valid lifetime

In IPv6, the length of time an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

Varbind

In SNMP, a Sequence of two fields, an Object ID and the value for/from that Object ID. Varbinds is short for Variable bindings. It's the variable number of values that are included in an SNMP packet. Each varbind is made of an OID, type, and value.

VCP

(Virtual Com Port) A driver that allows a USB device to appear as an additional COM port. The USB device can be accessed by an application in the same manner as a regular COM port.

VDC

Volts DC (direct current, as opposed to AC – alternating current).

VID

(VLAN Identifier) The identification of the VLAN, which is defined by the standard IEEE 802.1Q. VID has 12 bits and allows the identification of 4096 VLANs.

VLAN

(Virtual LAN) Refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

VLAN Endstation Endpoint

A protocol endpoint representing an endstation network port and its VLAN-specific attributes.

VLAN Switch Endpoint

A protocol endpoint representing a switch port and its VLAN-specific attributes.

VLAN-tagged frame

A tagged frame whose tag header carries both VLAN identification and priority information. A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs (i.e., it carries a tag header that carries a non-null VID). A VLAN-tagged frame is classified as belonging to a particular VLAN based on the value of the VID that is included in the tag header. The presence of the tag header carrying a non-null VID means that some other device, either the originator of the frame or a VLAN-aware Bridge, has mapped this frame into a VLAN and has inserted the appropriate VID. Contrast “untagged frame”.

VLAN Tunneling

(Virtual LAN Tunneling) A mechanism that allows service providers to use a single VLAN to support multiple VLANs of customers, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. At the same time, it significantly reduces the number of VLANs required to support the VPNs. VLAN Tunneling encapsulates the VLANs of the enterprise customers into a VLAN of the service provider. Also called ‘802.1q Tunneling’.

VOIP

(Voice over Internet Protocol) A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks.

VTY

(Virtual Type Terminal) - A vty interface and password must be created in order to enable Telnet access to an IPv6 router. Also Virtual TTY (VTY) connections are for connecting from a remote location via Telnet or SSH. PuTTY is a vty connection device. A “line” on a router is a physical async serial port (such as a terminal or modem), a virtual network connection, or another type of serial line on the router. A router can have a console line (labeled CTY), an AUX port (labeled AUX), multiple VTY lines, and multiple TTY lines. A Virtual Teletype command line interface is created in a router for a Telnet session. The router is able to generate a VTY dynamically.

Web-based Management

Allows users to manage the switch through a web browser. (AKA, Web GUI, Web interface, Web IF.)

Well Known Ethernet Multicast Addresses

Some common Ethernet multicast MAC addresses are shown below with their related Field Type and typical usage.

Ethernet Multicast Address	Usage
01-00-0C-CC-CC-CC	CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)
01-00-0C-CC-CC-CD	Cisco Shared Spanning Tree Protocol Address
01-80-C2-00-00-00	Spanning Tree Protocol (for bridges) (IEEE 802.1D)
01-80-C2-00-00-01	Ethernet OAM Protocol (IEEE 802.3ah)
01-80-C2-00-00-02	IEEE Std 802.3 Slow Protocols multicast address
01-80-C2-00-00-03	IEEE Std 802.1X PAE address
01-80-C2-00-00-04	IEEE MAC-specific control protocols
01-80-C2-00-00-08	Spanning Tree Protocol (for provider bridges) (IEEE 802.1AD)
01-00-5E-xx-xx-xx	IPv4 Multicast (RFC 1112)
33-33-xx-xx-xx-xx	IPv6 Multicast (RFC 2464)

Well-known IPv6 Multicast Addresses

These well-known multicast addresses are pre-defined. The group IDs defined in this section are defined for explicit scope values. Use of these group IDs for any other scope values, with the T flag equal to 0, is not allowed. These multicast addresses are reserved and cannot be assigned to any multicast group.

Reserved Multicast Addresses:

FF00:0:0:0:0:0:0:0
 FF01:0:0:0:0:0:0:0
 FF02:0:0:0:0:0:0:0
 FF03:0:0:0:0:0:0:0
 FF04:0:0:0:0:0:0:0
 FF05:0:0:0:0:0:0:0
 FF06:0:0:0:0:0:0:0
 FF07:0:0:0:0:0:0:0
 FF08:0:0:0:0:0:0:0
 FF09:0:0:0:0:0:0:0
 FFOA:0:0:0:0:0:0:0
 FFOB:0:0:0:0:0:0:0
 FFOC:0:0:0:0:0:0:0
 FFOD:0:0:0:0:0:0:0
 FFOE:0:0:0:0:0:0:0
 FFOF:0:0:0:0:0:0:0

The following multicast addresses identify the group of all IPv6 nodes, within scope 1 (interface-local) or 2 (link-local).

All Nodes Addresses: FF01:0:0:0:0:0:0:1
 FF02:0:0:0:0:0:0:0:1

The following multicast addresses identify the group of all IPv6 routers, within scope 1 (interface-local), 2 (link-local), or 5 (site-local).

All Routers Addresses: FF01:0:0:0:0:0:2
 FF02:0:0:0:0:0:2
 FF05:0:0:0:0:0:2

Solicited-Node Address: FF02:0:0:0:0:1:FFXX:XXXX

Solicited-Node multicast addresses are computed as a function of a node's unicast and anycast addresses.

A Solicited-Node multicast address is formed by taking the low-order 24 bits of an address (unicast or anycast) and appending those bits to the prefix FF02:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range FF02:0:0:0:0:1:FF00:0000 to FF02:0:0:0:0:1:FFFF:FFFF.

For example, the Solicited-Node multicast address corresponding to the IPv6 address 4037::01:800:200E:8C6C is FF02::1:FF0E:8C6C. IPv6 addresses that differ only in the high-order bits (e.g., due to multiple high-order prefixes associated with different aggregations) will map to the same Solicited-Node address, thereby reducing the number of multicast addresses a node must join.

A node is required to compute and join (on the appropriate interface) the associated Solicited-Node multicast addresses for all unicast and anycast addresses that have been configured for the node's interfaces (manually or automatically).

Well Known Ports

The set of all available port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. The Well Known Ports are 0 - 1023. The Registered Ports are 1024 - 49151. The Dynamic and/or Private Ports are 49152 - 65535. Port 443 is reserved for the HTTPS, port 179 for the BGP Border Gateway Protocol, and port 161 for SNMP. To see all the used and listening ports on your computer, use the **netstat** (or similar) command line command. For more on port assignments, see IETF [RFC 1700](#). RFC 1700 is replaced by an [On-line Database](#). See also the IANA [Service Name and Transport Protocol Port Number Registry](#).

Port Number	Description
20	FTP
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
143	Interim Mail Access Protocol (IMAP)
161	SNMP/UDP
162	SNMPTRAP/UDP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
546	DHCP Client
547	DHCP Server

Write View

A view name (up to 64 characters) for each SNMP group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group. A "Writeview" is a string of up to 64 characters that is the name of the view that lets you enter data and configure the contents of the agent. The default writeview is 'nothing' (i.e., the null OID). You must configure write access.

xSTP

Spanning Tree Protocol (multiple variations) defined in MEF specification 17. See also "STP".

XMODEM

A simple file transfer protocol developed in 1977 as the MODEM.ASM terminal program. XMODEM, like most file transfer protocols, breaks up the original data into a series of "packets" that are sent to a receiver, along with information that allows the receiver to tell if the packet was correctly received. It provides single file transfer using 128-byte packets with CRC or checksum error detection.

XMODEM-1K

An expanded version of XMODEM. Like other backward-compatible XMODEM extensions, it was intended that a -1K transfer could be started with any implementation of XMODEM on the other end, backing off features as required.

It provides simple serial file transfer between a server and client across a point-to-point link using fixed-length packets. Each server packet contains 1024 bytes of file data and is individually acknowledged by the receiving client. One file can be sent per transmission, and the transmission must be restarted from the beginning if it fails.

YMODEM

A protocol for file transfers between modems. YMODEM was developed as the successor to XMODEM. The original YMODEM was much the same as XMODEM except that it sent the file name, size, and timestamp in a regular XMODEM block before actually transferring the file. It provides multiple file transfer using 1 Kbyte packets, and is similar to Xmodem in other aspects.

ZMODEM

A file transfer protocol developed in 1986 to improve file transfer performance on an X.25 network. ZMODEM also offers restartable transfers, auto-start by the sender, an expanded 32-bit CRC, control character quoting, and sliding window support. It provides multiple file transfer, sending packets without waiting for acknowledgement, and permits an interrupted transfer to restart.

Y.1731

The ITU-T OAM Recommendation. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). See also "SOAM" and 802.1AG.

Index

ACL	15, 78	DHCP	
Conditions	80, 84	Configuring	43
Configuring, CLI method	80, 86	Server definition	43
Configuring, Web method	83, 88	Disable	
Default chain policy	80, 83, 86	Serial interface	194
Rules	81, 83	USB access	194
Trap rate	81, 83	DNS	
Add Users	73	Configuring, CLI method	47
Archive file		Configuring, Web method	49
Creating	206	Defining a server	46
Uploading	208	Documentation conventions	18
Backing up the configuration	13, 150, 152	Duplex modes	22
BootP	41	Dynamic IP address	43
Certificate authority	91	Edit Users	73
CLI		Error messages	
Configuration quick reference	351	CLI commands	243
CLI error messages	243	Web interface	291
COM port		Ethernet connection	22
Configuring	27	Telnet CLI	29
Compliance information	340	Web interface	30
Config Error log	323	Features	
Configuration		Management interfaces	14
ACL	78	Management module	13
Backing up	13, 150, 153	Security	15
Backup	161	TFTP backup and restore	13
HTTPS	91	Firmware	
HyperTerminal	27	Archive file	206
IP address	40	Backing up	150, 153
IP address	33, 34	Database index file (db.idx)	206
Management VLAN	96	Upgrading	202, 210
RADIUS	99	FocalPoint	14
Restoring	158, 161	Full duplex operation	22
SNTP	110	Gateway address	33, 41, 42
SSH	117	GUI	14
System logging	123	Half-duplex operation	22
USB COM port	27	HTTPS	15, 91
Configuration quick reference	351, 360	Certificates	92, 94
Connecting by		Configuring, CLI method	92
Telnet	29	Configuring, Web method	94
USB	28	Port number	92, 94
Web	30	Private key	92, 94
Connectors		Public key	91
RJ-45	22	HyperTerminal, configuring	27
USB	22	Hypertext transfer protocol secure, see HTTPS	15
Conventions, documentation	18	Install	
Database index file	206	IONMM	20
Daylight savings time	113, 116	USB driver	23
db.idx file	206	IP address	40
db.zip file	206	Dynamic, CLI method	43
Defaults		Static configuration, Web method	42
Factory settings	343	Static, CLI method	33, 34, 41
Reset factory settings	195	IP Address modes	14, 33, 35
Delete Users	73		

LEDs	21	USB	23
Duplex indicator	22	Web interface	30
Operating mode	22	Signing in	30
Power	22	Signing out	32
Management VLAN	15, 96	Simple network management protocol, see	
Configuring, CLI method	97	SNMP	14
Configuring, Web method	98	Simple network time protocol, see SNTP	77
Network access	29	SNMP	14
Telnet session	29	Configuring, CLI method	129
Web interface	30	Configuring, Web method	132
Network management system (NMS)	14	SNMP v1	16
Operating mode		SNMP v2c	16
10 MBps	22	SNMP versions	16
100 MBps	22	SNTP	110
100Base-TX	22	Configuring, CLI method	111
10Base-T	22	Configuring, Web method	116
Full duplex	22	Server	114
Half-duplex	22	SSH	15, 117
Power		Configuring, CLI method	118
Consumption	17	Configuring, Web method	120
LED	22	Host key	118, 121
Private key		Public key	118, 121
HTTPS	92, 94	Retry limit	118, 120
SSH	117	Timeout value	118, 120
Provisioning tab	150, 153, 158	Static IP address	41
Public key		Subnet mask	33, 41, 42
HTTPS	91	Syslog	123, 316
Public key cryptography	91	Tech Support	337
RADIUS	15, 99	Telnet	
Configuring, CLI method	100	Default login	343
Configuring, Web method	102	Default password	343
Retry limit	100, 102	Ethernet connector	22
Secret	100, 102	Setup	29
Server	99, 100, 102	Terminate session	29
Timeout	100, 102	Terminate	
Reboot	199	Telnet session	29
CLI method	199	USB interface	28
Web method	200	TFTP	
Replacing the management module	221	Server address	94, 121, 204, 208
Reset		Upgrading firmware	206, 212
Button	22	Timezones	111, 116
Factory defaults	195	Troubleshooting	222
Uptime	197	Upgrade firmware	
Restart		IONMM	204
ION MM	199	USB	
Restoring the configuration	158	Configure COM port	27
RJ-45 connectors	22	Connectors	22
Secure shell, see SSH	15	Default login	343
Secure socket layer (SSL)	91	Default password	343
Security features	15	Disable access	194
Serial interface	22	Driver installation	23, 30
Disable	194	Login	28
Setup	23	Setup	23
Setup		Starting a session	28
Serial interface	23	Terminate connection	28
Telnet	29	User	

levels	73, 74, 76
login	73
Name	74, 76
Password	76
VLAN, see Management VLAN	13
Web interface	
Error messages	291
Ethernet connector	22
Signing in	30
Signing out	32
webpage messages	328

