ION System
x222x / x32xx Remotely Managed Network Interface Device (NID)

User Guide

Part Number 33472
Revision K August 2023

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.
Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries. All other trademarks and trade names are the property of their respective holders.

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

Warranty

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

Contacts

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

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

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

Disclaimer

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

Revision History

Date	Rev	Description
10/31/18	J	Revised for v 1.3.17. Add the RMPS (Remote Manage Power Supply) feature, Local Management of Cards in a Remote Un-managed Chassis, and DMI Vendor Specific Information. V 1.3.16 fixed calculations for ingress bandwidth limiting rates and fixed the backup and restore issue when the device is set to Local Management mode via a unique IP address. ION x222x / x32xx v 1.3.17 requires IONMM v 1.4.2.
8/28/23	K	Initial Lantronix rebrand. Update contact information, remove Converge EMS, Glossary, and Index. FW v1.3.26: update ssh server, link state now reflects admin state, improve Local and Remote backup in stand-alone modules. Clarify Appendix G information. See the Release Notes for more information.

Cautions and Warnings

Definitions

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

Cautions

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

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

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

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

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

Warnings

Warning: Use of controls, adjustments or the performance of procedures other than those specified herein may result in hazardous radiation exposure.
Warning: Visible and invisible laser radiation when open. **Do not** stare into the beam or view the beam directly with optical instruments. Failure to observe this warning could result in an eye injury or blindness.
Warning: DO NOT connect the power supply module to external power before installing it into the chassis. Failure to observe this warning could result in an electrical shock or death.
Warning: Select mounting bracket locations on the chassis that will keep the chassis balanced when mounted in the rack. Failure to observe this warning could allow the chassis to fall, resulting in equipment damage and/or possible injury to persons.
Warning: Do not work on the chassis, connect, or disconnect cables during a storm with lightning. Failure to observe this warning could result in an electrical shock or death.
See Appendix A on page 526 for Electrical Safety Warnings translated into multiple languages.

Contents

1. Introduction 11
Auto-Negotiation (802.3u) 13
Pause 13
AutoCross (10/100/1000Base-T) 13
Configuration Backup and Restore 14
DMI Optical Management 14
Backwards Compatibility / Point System Support 14
DHCP Client 15
DNS Client 15
Far End Fault (FEF) 15
Management Access Methods 16
TFTP (Trivial File Transfer Protocol) 16
SLPT (Selective Link Pass Through) 16
TLPT (Transparent Link Pass Through) 17
TLPT and Auto Link Restoration 18
Fiber Port Redundancy 18
IP-Based Remote Management Mode 18
Security Features 19
IP Address Modes (IPv4 / IPv6, DHCP, Static, BootP) 20
IEEE 802.1p QoS Packet Classification 21
IEEE 802.3ah Clause 57 LOAM Recommendation 21
VLAN Tunneling (802.1q Tunneling) 22
L2CP (Layer 2 Control Protocol) 25
Device Description / Circuit ID 25
MAC Address Learning 25
System Logging (Syslog) 26
TN Topology Discovery Protocol TX 26
RFC 2544 Benchmarking 26
SNMP Support 26
WRR or Strict Priority Queuing 27
Serial File Transfer (X/Y/Zmodem) 27
Public MIBs 28
Private MIBs 28
Downloading, Compiling and Integrating MIBs 32
Standard Models and Single Fiber Models 33
Chassis Models (*Cxxxx*) and Standalone Models (*Sxxxx*) 33
ION System Model Number Key 34
All Model x222x / x32xx 35
C2220 Series 35
C322x Series 35
S322x Series 35
MEF Certification 36
Related Manuals and Online Helps 37

2. Installation and System Setup 38
Rack Mount Installation 39
Tabletop Installation 40
Wall Mount Installation 41
Connecting to AC Power 42
Model x2220-1040 44
Model x3221-1040 46
Model x32x0-10xx 48
Operating Systems Supported 49
Installing the USB Driver (Windows XP) 50

Installing the USB Driver (Windows 8) 51
Access via an Ethernet Network 55
Initial Setup with a Static IP Address via the CLI 57
Access via Local Serial Interface (USB) 59
Changing Switch Mode (Local / Remote) 64

3. Management Methods 65
Managing Slide-In and Remote Modules Using CLI Commands 65
Managing Slide-In and Remote Modules via the Web Interface 68
Managing Standalone Modules Using CLI Commands 69
Managing a Standalone Module via the IONMM Web Interface 70
Managing a Standalone Module via the Web Interface 71
Menu System Descriptions 72
Reboot, Reset, and Power Off Function Notes 76

4. Configuration 79
Setting the IPv4 Addressing 80
DNS Lookups over IPv6 Transport 85
Assigning a Dynamic IP Address via DHCP 86
Defining DNS Servers 87
IPv6 Dual Protocol Stacks and Multiple Server Support 93
Telnet IPv4 and IPv6 Connections 100
TFTP IPv4 and IPv6 Connections 100
System Configuration – CLI Method 105
System Configuration – Web Method 106
Device Description Configuration 107
Device Description– CLI Method 107
Device Description Config – Web Method 108
Circuit ID Config – CLI Method 109
Circuit ID Config – Web Method 110
Login Type Config – CLI Method 111
Ports Configuration 114
AutoCross Config – CLI Method 114
AutoCross Config – Web Method 115
10/100/1000BaseT Port – CLI Method 116
10/100/1000BaseT Port – Web Method 119
Set Ethernet Port Speed / Duplex Mode – CLI Method 120
Set Ethernet Port Speed / Duplex Mode – Web Method 122
Set Port Admin Mode (Ethernet PHY Mode) 123
Set Port Admin Mode (Ethernet PHY Mode) – CLI Method 123
Port Admin Mode Config – Web Method 124
Far End Fault Mode Configuration 126
Far End Fault Mode Config – CLI Method 126
Set Bandwidth Allocation / Rate Limiting – CLI Method 127
Set Bandwidth Allocation / Rate Limiting – Web Method 129
Configuring Priority Queuing 132
Priority Queuing Config – CLI Method 132
Priority Queuing Config – Web Method 133
LOAM Configuration Prerequisites and Restrictions 134
Copper Port Loopback Procedure 149
Configuring Selective and Transparent Link Pass Through 152
Link Pass Through Config – CLI Method 154
Link Pass Through Config – Web Method 156
Forwarding Learning (FDB) Aging Time Config – CLI Method 158
FDB Aging Time Config – Web Method 159
SNTP Config – CLI Method 161
SNTP Config – Web Method 165

Configuring System Login Users 165
Note Regarding SNMPv3 Users vs. Web/CLI Login Users 166
Configuring System Login Users - CLI Method 167
Configuring System / Login Users - Web Method 169
Dynamic Table Entry Limits 170
Configuring an ACL 172
ACL Config (IPv6) – Web Method 182
Configuring HTTPS 185
Configuring MAC Address Filtering 190
Configuring MAC Address Blocking 193
Configure VLAN Mode (Secure/Disable/Fallback/Check) via Web GUI 197
Configuring Port Forward Management / IP Access Blocking 199
Configuring RADIUS 201
Configuring TACACS+ 206
Configuring SSH 212
Configuring SSH and RADIUS 217

Configuring SNMP 218
Note Regarding SNMPv3 Users vs. Web/CLI Login Users 218
SNMP Definition and Description 219
Management Information Base (MIB) 220
A MIB Example - ionDevSysCfgTable 221
SNMP PDUs 221
SNMP Version v1, v2c, v3 Considerations 223
SNMPv1 224
SNMPv2 224
SNMPv3 224
SNMPv3 USM MIB 233
SNMPv3 VACM – Groups 234
SNMPv3 VACM – Views 235
SNMPv3 Traps and Informs 235
ION System SNMP Support 237
SNMP Command Line Interface (CLI) Support 237
SNMP v3 Users, Groups, and Views Configuration 237
Configuring SNMP 241
SNMP Config – CLI Method 242
SNMP Config – Web Method 245
Change a SNMP User's Group - Web Method 253
SNMP v3 Default Values 253
SNMP v3 Commands 256
Web Interface-to-CLI Command Cross Reference 258
Configuring Management VLAN 262
Configuring VLANs – Network / Provider / Customer Mode 267
Flush VLAN Databases Config 279
Configuring VLAN Tunneling (802.1q Tunneling) 283
Configuring Fiber Port Redundancy 295
L2CP Protocol Descriptions 298
L2CP Config – CLI Method 300
L2CP Config – Web Method 302
TNDP Config – CLI Method 303
TNDP Config – Web Method 304
Configuring Loopback 305
Loopback Config – CLI Method 305
Loopback Config – Web Method 306
Configuring System Logging (Syslog) 307
Syslog Config – CLI Method 308

Syslog Config – Web Method 309
Configuring MAC Address Learning 311
MAC Address Learning Portlist Config – CLI Method 311
MAC Address Learning Portlist Config – Web Method 312

5. Operation 313
Backing Up Slide-In and Remote Modules 314
Backing Up Standalone Modules 317
Editing the Config File (Optional) 319
Restoring Slide-In and Remote Modules 320
Restoring Standalone Modules 323
Back Up and Restore File Content and Location 326
Backup / Restore (Provisioning) - CLI Method 328
Resetting Defaults – CLI Method 332
Resetting Defaults – Web Method 333
File Status after Reset to Factory Defaults 334
Reset System Uptime – CLI Method 335
Reset System Uptime – Web Method 336
Resetting Counters 337
Reset All Ports Counters – CLI Method 337
Reset Port Counters– Web Method 338
Clear All Ethernet Port Counters – CLI Method 339
All Counters Reset – Web Method 340
Rebooting – CLI Method 341
Rebooting – Web Method 342
Reboot File Content and Location 343
Upgrading IONMM and/or NID Firmware – CLI Method 344
Upgrading IONMM and/or NID Firmware – Web Method 346
Upgrading Slide-In and Remote Modules Firmware via TFTP 352
Upgrading Standalone Module Firmware via TFTP Server 356
Firmware Upgrade File Content and Location 358
Additional Upgrade Procedures 358
Transfer Files via Serial Protocol (X/Y/Zmodem) – CLI Method 359

6. Troubleshooting 361
Basic ION System Troubleshooting 361
Error Indications and Recovery Procedures 362
LED Fault and Activity Displays 363
IPv6 Troubleshooting 364
SNMP Messages 441
Basic Recovery Steps 441
Windows Event Viewer Messages 452
The Config Error Log (config.err) File 453
config.err Messages 454
config.err Message Responses 454
Syslog Messages and Sys.log Output 458
Syslog Messages 458
Sample Sys.log Output 461
ION System Tests 475
Virtual Cable Test (VCT) 475
DMI (Diagnostic Maintenance Interface) Parameters 479
Set Debug Level 486
Ethernet Statistics Counter Descriptions 487
PCB Identification 490
x2220 NID 491
x3220 NID 492
Ipconfig 493

ifconfig 495
Windows Network Connections 496
Ping 497
Telnet 498
PuTTY 499
Tracert (Traceroute) 501
Netstat 502
Winipcfg 503
Nslookup 504
DHCP 505
Dr. Watson 506
SNMPc 506
HPOV (HP OpenView) 507
US-CERT 507
HyperTerminal Messages 508
Ping Command Messages 509
Telnet Messages 510
TFTP Server Messages 512
PuTTY Messages 513
Recording Model Information and System Information 514

Appendix A. Compliance and Safety Information 516
MEF Certifications 517
Electrical Safety Warnings 518
Electrical Safety 518
Elektrische Sicherheit 518
Elektrisk sikkerhed 518
Elektrische veiligheid 518
Sécurité électrique 518
Sähköturvallisuus 518
Sicurezza elettrica 518
Elektrisk sikkerhet 518
Segurança eléctrica 518
Seguridad eléctrica 518
Elsäkerhet 518

Appendix B. Factory Defaults 519

Appendix C. Configuration Quick Reference – CLI 532
IPv6 Configuration 532
ACL Configuration (IPv6) 533
TACACS+ Configuration 536
System (Login) User Configuration 538
Transfer Files via Serial Protocol (X/Y/Zmodem) 539
SNMP Configuration 540

Appendix D. VLAN Tunneling Configuration Examples 541
Configuring VLAN 100 with Provider S-Tag 546
Configuring a VLAN with C-Tags and S-Tags 551
Q-in-Q Config – CLI Method 555
Q-in-Q Config – Web Method 559

Appendix E. SNMP Traps Supported 562
Traps List 562
SNMP v3 Traps 563
TN-ION-MGMT-MIB.smi 566
TN-ION-BPC-MIB 570
TN-IONCHASSIS-MIB 571

TN-ION-ENTITY-SENSOR-MIB 573
TN-ION-LOAM-EXT-MIB 575
TN-ION-MGMT-MIB 575
ionDMIRxPowerEvt 576
ionDMITxPowerEvt 577
ionDMITxBiasEvt 578
ionDMITemperatureEvt 579
newRoot 581
topologyChange 581
dot3OamThresholdEvent 582
linkDown 587
linkUp 588
risingAlarm 591
fallingAlarm 593
Trap Server Log 595

Appendix F Remote Manage Power Supply (RMPS) Feature 597

Appendix G: Local Management of Cards in a Remote Un-Managed Chassis 609

List of Figures

Figure 1: Far End Fault (FEF) 15
Figure 2: Selective Link Pass Through (SLPT) 17
Figure 3: Transparent Link Pass Through (TLPT) 17
Figure 4: TLPT and Auto Link Restoration 18
Figure 5: VLAN Tunneling Example 23
Figure 6: Private MIB Objects 31
Figure 7: Chassis Installation 38
Figure 8: Tabletop Installation 40
Figure 9: Wall Mount Installation 41
Figure 10: AC Power Connection 42
Figure 11: SFP Installation 43
Figure 12: Model C2220-1040 Connectors and LEDs 44
Figure 13: Model S2220-1040 Connectors and LEDs 44
Figure 14: Model C3221-1040 Connectors and LEDs 46
Figure 15: Model S3221-1040 Connectors and LEDs 46
Figure 16: Model C32x0-10xx Connectors and LEDs 48
Figure 17: Model S32x0-10xx Connectors and LEDs 48
Figure 18: CLI Location Hierarchy 66
Figure 20: Sample Loopback Configuration 150
Figure 21: Sample Loopback Counters Information 151
Figure 19: Selective Link Pass Through (SLPT) 152
Figure 20: Transparent Link Pass Through (TLPT) 153
Figure 21. MIB Example 221
Figure 22. SNMP PDU Format 221
Figure 23. SNMP v3 MIBs 230
Figure 24. SNMP v3 Trap-Inform MIBs 230
Figure 25. SNMP v3 Entity / Engine / Applications 231
Figure 26: ION System Managed via SNMP 237
Figure 27 .SNMP v3 Users, Groups, and Views 238
Figure 28: VLAN Tunneling Example 284
Figure D-1: VLAN Tagging Example 541
Figure D-2: Q-in-Q (Provider Tagging) 554
Figure E-1: SNMP Message Sequence 563

List of Tables

Table 1: Supported MIBs 28
Table 7: Documentation Conventions 36
Table 8: Model x2220-1040 Connectors and LED Descriptions 45
Table 9: Model x3221-1040 Connectors and LED Descriptions 47
Table 10: Model x32x0-10xx Connectors and LED Descriptions 49
Table 11: System-Level Menu Description 72
Table 12: Port-Level Menu Description 75
Table 13: LOAM Events 136
Table 14: Timezones 161
Table 15: User Level Rights via Web / CLI 166
Table 16. SNMPv3 Private MIB Levels / Auth / Encryption 225
Table 17: SNMPv3 Services 226
Table 18. SNMPv3 Private MIBs 227
Table 19. SNMPv3 Private MIBs 228
Table 20: SNMP v3 Default Values 234
Table 21: SNMP v3 Trap and Inform MIBs 235
Table 22: Web Interface Tabs to MIB Tables Mapping 236
Table 23: SNMP v3 Initialization (Default) Values 253
Table 24: SNMP v3 Web Interface Default Values 255
Table 28: Web Interface to CLI Command Cross Reference 258
Table 25: Syslog Severity Levels 307
Table 26: Back Up and Restore File Content and Location 326
Table 27: File Status after a Reset to Factory Defaults 334
Table 28: File Content and Location after a System Reboot 343
Table 29: File Content and Location after a Firmware Upgrade 358
Table 30: VCT Parameters 478
Table 31: DMI Parameters 482
Table 32: Device-Level Factory Defaults 519
Table 33: Port-Level Factory Defaults 527
Table 34: MIB Traps Summary 564
Table 35: Trap Server Log File Description 596

1. Introduction

Document Overview

The purpose of this manual is to provide the user with an understanding of the Lantronix x222x / x32xx network interface devices (NIDs). This manual documents the following models:

- **C2220** LOAM/IP-Based Remotely-Managed NID
- **C3220** LOAM/IP-Based Remotely-Managed NID
- **C3221** LOAM/IP-Based Remotely-Managed NID (2 open SFP slots)
- **S2220** LOAM/IP-Based Remotely-Managed NID
- **S3220** LOAM/IP-Based Remotely-Managed NID
- **S3221** LOAM/IP-Based Remotely-Managed NID (2 open SFP slots)
- **S3221-1040-T** LOAM/IP-Based Remotely-Managed Hardened NID

Product Overview

The x222x / x32xx are a group of Ethernet Network Interface Devices (NIDs) that are designed as either a standalone module (S222x / S32xx) or a slide-in module (C222x / S32xx) that installs in an ION system chassis. In either configuration, these devices are designed to manage devices remotely through the copper and fiber ports.

The ION x222x / x32xx Network Interface Devices (NIDs) are 2- or 3-port Ethernet Demarcation Devices capable of media conversion—one port connects to the network of the provider and the other port connects to the subscriber. These NIDs are chassis/IP-based managed devices that are designed as slide-in cards (SICs) for installation in an ION system chassis or as stand-alone modules.

These devices can be managed via Command Line Interface (CLI), Web Interface, or Telnet. See the *x222x & x32xx Installation Guide #33433* on our website.

The x222x / x32xx NIDs support Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57). LOAM is a group of network management functions that provide network fault indications, performance information, data, and diagnosis. These devices implement remote management via LOAM per the IEEE 802.3ah standard.

Features

The x222x / x32xx NIDs support the following features.

- 10K Jumbo Frame Support
- Auto-Negotiation
- Pause
- *AutoCross™*
- Bandwidth profiling
- Cable diagnostic function for TP ports
- Multiple IP addressing modes (IPv4 / IPv6, DHCP, Static, Bootp)
- DHCP client
- DMI Optical Management
- Backwards Compatibility / Point System Support
- Far-End-Fault (FEF)
- MAC filtering for network access control (authentication and authorization)
- Ipv4 IP TOS, DiffDerv and IPv6 traffic class QoS classification
- Multiple management methods
- Remote Firmware Upgrade
- Remote Loopback
- RMON Counters for each port
- SNTP
- TFTP
- Selective Link Pass Through (SLPT)
- Transparent Link Pass Through (TLPT) and Auto Link Restoration
- IP-Based Remote Management
- Link layer OAM (LOAM) per IEEE 802.3ah
- IEEE 802.1p QoS packet classification
- IEEE 802.1q VLAN and double VLAN tagging with 4096 VIDs
- VLAN Tunneling and Management VLAN
- Fiber Port Redundancy
- L2CP (Layer 2 Control Protocols)
- Circuit ID and Device Description
- TNDP (TN Topology Discovery Protocol) Disable
- System Logging (Syslog)
- MAC Learning Disable
- SNMP v1, v2c, and v3 support
- DHCP, Static, and BootP Address Modes
- WRR or Strict Priority Queuing
- Serial File Transfer (X/Y/Zmodem) commands
- RMPS (Remote Manage Power Supply) feature
- Local Management of Cards in a Remote Un-managed Chassis

10K Jumbo Frame Support

The x222x / x32xx NID devices support jumbo frames. The MTU (Maximum Transmission Unit) frames size can be 1522, 2048 or 10240 bytes (not configurable).

Auto-Negotiation (802.3u)

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

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

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

Pause

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

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

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

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

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

AutoCross (10/100/1000Base-T)

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

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

Bandwidth Profiling

A Bandwidth Profile is a method of characterizing Service Frames for the purpose of rate enforcement or policing. The x222x / x32xx NID devices support bandwidth profiling at the per-port level. Each port has an ingress bandwidth profile used to control the ingress traffic and an egress bandwidth profile for regulating traffic leaving the port. This feature provides TX and RX rate limiting from a pre-defined list of values in order to accommodate bursty traffic.

Configuration Backup and Restore

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

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

For more information see "Backup and Restore Operations" on page 267.

DMI Optical Management

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

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

Within each function, the DMI device will send a trap whenever a high or low warning event or high or low alarm event occurs (for a total of 16 traps). If both the local and remote NIDs are DMI models, the DMI device will indicate whether the trap event is from a local or remote device.

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

Backwards Compatibility / Point System Support

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

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

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

DHCP Client

Dynamic Host Configuration Protocol (DHCP) automates the assigning of IP addresses to devices within an IP network. DHCP is useful because it can make it easy to add new machines to the network.

When a DHCP-configured client (X222X/X32XX) connects to a network, it sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the DNS servers, other servers such as time servers, etc. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters (e.g., subnet mask, default gateway). The query is typically initiated right after a re-boot, and must complete before the client can initiate IP-based communication with other hosts.

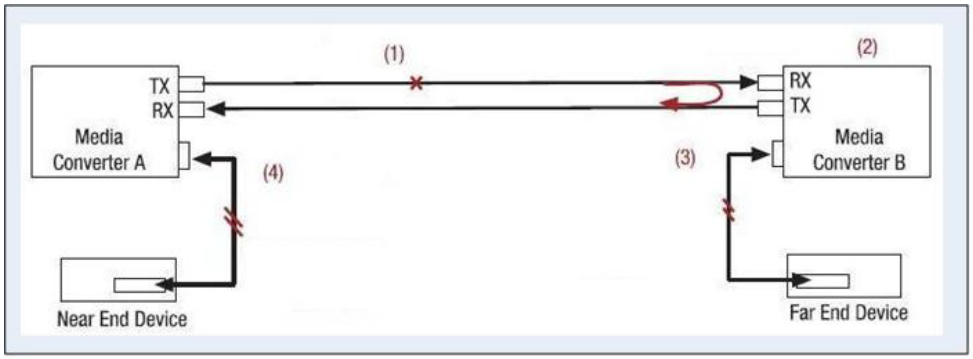
The x222x/x32xx provides DHCP client support (no DHCP server features). DHCP provides for dynamic IP address assignment to the x222x/x32xx. An x222x/x32xx CLI command is available to find out the DHCP assigned IP address.

DNS Client

The Sx222x/x32xx provides DNS client support (no DNS server features). DNS will allow use of a name instead of an IP address when using features like TFTP server, Trap Manager, SNTP server, etc. DHCP client and DNS server usage are independent; however, depending on the network setup, DHCP could automatically configure a DNS server as part of DHCP IP address assignment.

Far End Fault (FEF)

This troubleshooting feature is used with Link Pass Through to notify both end devices of a link loss. If the fiber RX signal is lost on the far end device, the 100FX device will automatically generate a far-end fault signal and send it on its TX fiber port to notify the near end device of the fiber link loss. Link Pass Through will then disable the copper links on both ends, alerting both end devices of network trouble.



1) Device B loses fiber RX link.

2) Device B disables copper TX via Link Pass Through (LPT) to alert far end device of link loss.

3) Device B sends FEF signal back on fiber TX to alert Device A of link loss.

4) Device A disables copper TX via LPT to alert near end device of link loss.

Figure 1: Far End Fault (FEF)

On 100BaseFx Ports, optical link integrity can be identified by FEF. This is very useful to detect network faults since fiber links can be long. FEF occurs when the device detects that it cannot sense any more IDLE symbols on the link. This indicates a fault on the receiving end, and the device sends FEF signals on its transmit circuit, notifying its link partner of the fault. Advantages include:

- Both end devices are notified automatically of the link loss.
- Prevents loss of valuable data transmitted unknowingly over an invalid link.
- Allows quick diagnosis and resolution of network problem.

Lantronix media converters that include the FEF feature will work with other network devices that support Far End Fault per IEEE standards.

Management Access Methods

Management of the x222x / x32xx, and subsequently the other slide-in modules, is accomplished through one of the following methods.

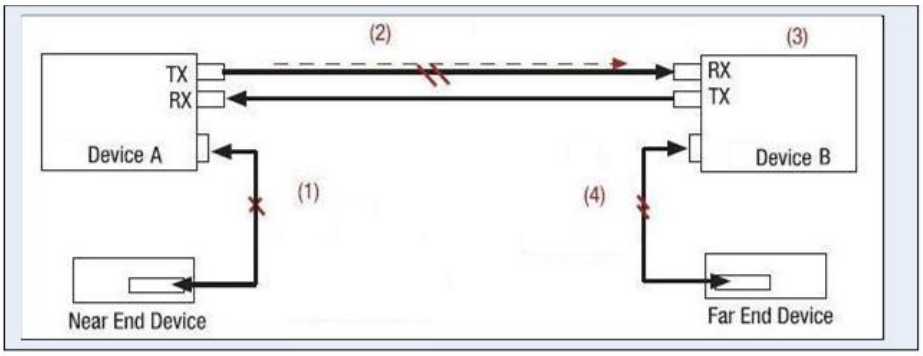
- Universal Serial Bus (USB) – uses a command line interface (CLI) to access and control the x222x / x32xx through a locally connected workstation.
- Telnet session – uses the CLI to access and control the x222x / x32xx through the network.
- Secure Shell (SSH) – uses the CLI to access and control the x222x / x32xx through the network. Web browser – access and control the x222x / x32xx using a standard web browser and a graphical user interface (GUI).
- Simple Network Management Protocol (SNMP) – both public and private Management Information Bases (MIBs) allowing for a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).

TFTP (Trivial File Transfer Protocol)

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

SLPT (Selective Link Pass Through)

This feature monitors the fiber Rx port for signal loss. If the fiber Rx goes down, the copper port stops transmitting. SLPT monitors the link status of one port on Device A, and any change in its operational state is passed on to the device's other port to bring down its link, and vice-versa. SLPT is similar to LPT, except SLPT only works in one direction - from Port 1 to Port 2, or from Port 2 to Port 1, but not in both directions. Selective LPT is typically supported by devices which support 'Transparent LPT'.



1) Device A loses copper RX link with end device.

2) Device A sends a link loss signal over the fiber.

3) Device B receives link loss signal and disables the copper TX port.

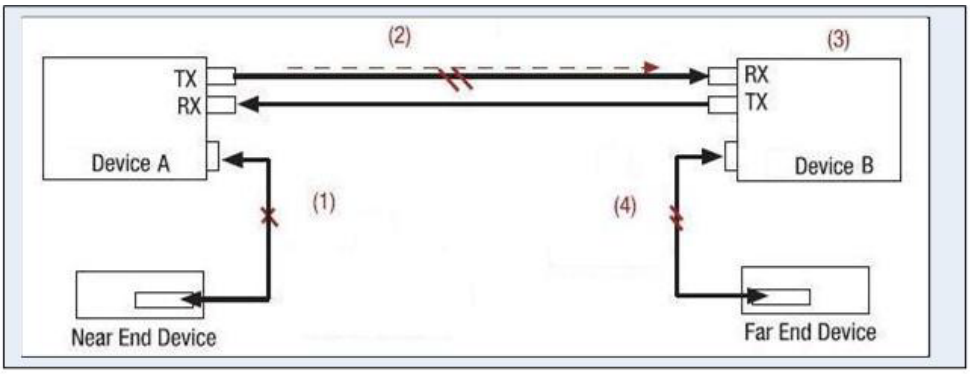
4) End device is notified of link failure.

Figure 2: Selective Link Pass Through (SLPT)

TLPT (Transparent Link Pass Through)

Transparent LPT requires a back-to-back setup of the same type of device. TLPT monitors the link status of one port on device A, and any change in its operational state is passed on to the peer device B port to bring down its far end port, and vice-versa.

For example, if the devices are connected by Port 2 on each, and if Device A - Port 1 becomes operationally down, then Device B - Port 1 is brought down. The devices can communicate with each other, but the link condition is passed on so a network administrator can know of the fault condition. Port 2 is the port that is monitored.



1) Device A loses copper RX link with end device.

2) Device A sends a link loss signal over the fiber.

3) Device B receives link loss signal and disables the copper TX port.

4) End device is notified of link failure.

Figure 3: Transparent Link Pass Through (TLPT)

TLPT and Auto Link Restoration

With LOAM enabled, Transparent Link Pass Through (TLPT) with automatic link restoration is available for the copper ports on the local and remote peer NIDs. When a copper port goes down, the information is passed to the other NID and the copper port on that NID will go down. When the link is restored, the link on the other port is also restored - the fiber ports remain UP. When TLPT is disabled, if the copper port link drops it does not affect its peer's copper port links.

Auto Link Restoration will restore the broken link automatically upon correcting the fault condition.

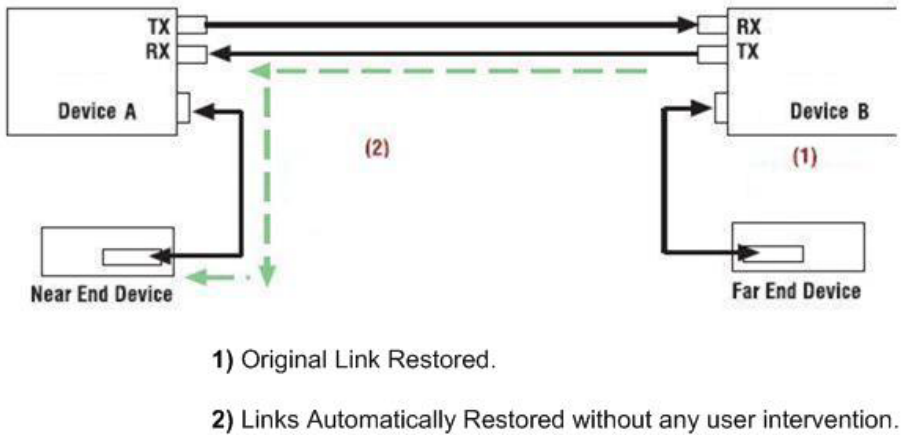


Figure 4: TLPT and Auto Link Restoration

Fiber Port Redundancy

The redundancy feature is designed to allow customer traffic and CPU-centric protocols to survive a fault on an uplink fiber port by placing the traffic on a secondary backup port.

Fiber redundancy is supported in 3-port models that have two fiber ports. One of the fiber ports is set as the Active port for the services and the other port is the Secondary port which will take over if the Active primary port loses its link. The Active primary port is monitored in software and when a failure is detected, switches over the data services to the secondary port.

The 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.

The fault discovery method is LOS at the receiving interface for a continuous period of 10ms. Traffic rerouting occurs after the Primary Port is declared in the fault state and traffic flow is restored.

The Redundancy (*aka*, automatic protection switching) mode ports are defined as follows: Customer Port is Port 1, Primary Port is Port 2, Secondary Port is Port 3, and the 'Active Port' is the Port that on which the Redundancy function is active.

IP-Based Remote Management Mode

The x222x / x32xx NIDs can be managed through SNMP. Select stand-alone products can also be managed through SNMP. Some remotely managed converters are IP addressable, while others must be used in conjunction with a managed chassis-based device. While chassis based products are generally

placed in the telecommunications room, stand-alone converters are generally placed in remote locations away from network administrators. Remote in-band management over fiber allows administrators access to the remote device to check status and enable/disable features or the device itself.

Security Features

The security features allow you to control access to the ION Chassis via the x222x / x32xx NID to ensure that only authorized personnel are able to view and change the settings of the slide-in modules.

- Access Control Lists (ACLs) – ACLs can be configured in the x222x / x32xx NID to allow access to authorized users and to deny access to all others. See "Configuring an ACL" on page 181.
- Hypertext Transfer Protocol Secure (HTTPS) – the x222x / x32xx NID supports the use of HTTPS, which utilizes the secure socket layer (SSL) protocol for transmitting private documents via the Internet. See "Configuring HTTPS" on page 194.
- 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. See "Configuring Management VLAN" on page 271.
- RADIUS authentication – The x222x / x32xx NID 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 x222x / x32xx NID through either the Web login, serial port (USB), or Telnet session. The RADIUS server must be configured before RADIUS authentication is enabled. See "Configuring RADIUS" on page 210.
- Secure Shell (SSH) authentication – the x222x / x32xx NID 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" on page 221.
- Simple Network Management Protocol (SNMP) access – If desired the administrator can stop all SNMP access to the x222x / x32xx NID. This will prevent unauthorized access to the system configuration through SNMP, but the desired/configured SNMP traps will still be sent. For more information see "Configuring SNMP" on page 228.
- USB access – The USB port can be turned off to prevent unauthorized access to the system through the serial interface. See "Disabling USB Access to the IONMM" on page 233.

IP Access

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

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.

MAC Filtering

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

MAC Addresses Blocking

The MAC address can be added to the static MAC address database with the ‘connected port’ as zero. This will cause any frames from that MAC address database to cause an ATU-member violation on that port, resulting in sending a trap. This could cause excessive traps (overload the Central Processing Unit (CPU) with interrupts) depending on the traffic generated by that MAC. You can disable MAC violations by setting the **Ignore SA Violation** on the port that is receiving the MAC address under **Port** > **Advanced** > **MAC Security** > **SA Lock** in the web interface.

The SA Lock enabled feature will detect if the device connected to this port has been changed, and when an unknown MAC address ingresses this port.

Applicable Standards

- IEEE 802.1p QoS packet classification
- IEEE 802.3ah Clause 57 Link OAM (LOAM)
- IEEE 802.1q VLAN and double VLAN tagging
- IEEE 802.1 Port-based Network Access Control

IEEE 802.1p QoS Packet Classification

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

The C2x2x/C3x2x NIDs provide QoS at the Layer 2 level using CoS bits as per IEEE 802.1p. The priority bits in the 802.3ac tag can be remapped as frames ingress the device based on Ingress port, Source MAC address, Destination MAC address, or VLAN ID in the 802.1q tag, or on the basis of remapping to a user-defined priority on a per port basis.

The C2x2x/C3x2x NIDs also provide QoS based on DSCP/ToS bits in the IP header.

The devices support four output queues. Based on a frame's priority bits (layer 2 or layer 3), frames are assigned the egress output queues. The device offers weighted round robin (WRR) 8-4-2-1 scheduling on the output queues to minimize frame latencies and starvation of lower priority queues.

IEEE 802.3ah Clause 57 LOAM Recommendation

Model x3x3x and x2x2x NIDs implement the IEEE LOAM 802.3ah standard for Link Monitoring on both the fiber and twisted pair interfaces with the following LOAM features:

- Critical Event
- Discovery
- Event notification with logs
- Last gasp/Dying gasp
- Remote Loop Back

Model x3x3x and x2x2x NIDs implement IETF RFC 4878 for LOAM functionality that includes discovery, error signaling, loopback, and link monitoring.

Critical Event

When the link on the other port fails, the NID sends a LOAM critical event signal to its peer, indicating the fault condition.

Discovery

An active-state NID initiates LOAM communications by sending PDUs across the link connected to an OAM enabled port. The NID at the other end (if LOAM capable) responds to the request from the active NID by establishing a LOAM communications channel.

Event Notification with Logs

A LOAM link event notifies its LOAM peer of any symbol or frame errors that occurred on its link. The window used for error monitoring, along with the threshold value, are configurable.

At the end of the window, if the errors are greater than or equal to the threshold value, a LOAM event notification is sent to its peer. If the threshold is set to zero, then at the end of each window an event notification is sent. This acts much like an asynchronous update of the link statistics.

Last Gasp/Dying Gasp

All NIDs come equipped with a Last Gasp/LOAM Dying Gasp feature. This feature enables the NID to store a small amount of power to enable sending an SNMP trap to alert the management console of a power failure. Feature benefits include:

- Notification of an impending power loss before it happens
- Allows for quicker resolution of the power loss

Remote Loop Back

LOAM remote loop back can be used to test link health by sending a loop back request from the active peer NID to the remote passive peer NID. Once the remote passive peer enters loop back mode, all frames coming into that port are looped back, but not forwarded to other ports.

The LOAM frames are still exchanged between the local and remote peer NIDs, but only LOAM frames get through. The active peer NID discards the frames coming out of its remote peer NID to prevent flooding the network. The remote loop back function requires a test head to generate traffic.

VLAN Tunneling (802.1q Tunneling)

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

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

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

VLAN Tunneling accomplishes the following:

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

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

How VLAN Tunneling Works

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

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

Tagged and untagged customer traffic comes from a port on a customer device and enters the service-provider edge switch through a tunnel port. Each customer edge port that is connected to a VLAN tunnel port is typically configured as a trunk port. The customer trunk port is unaware of the provider VLAN tunnel and can communicate with all of its other trunk ports that are connected to the metro network of the provider as if they were directly connected. This makes the process transparent to the enterprise's switching network.

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

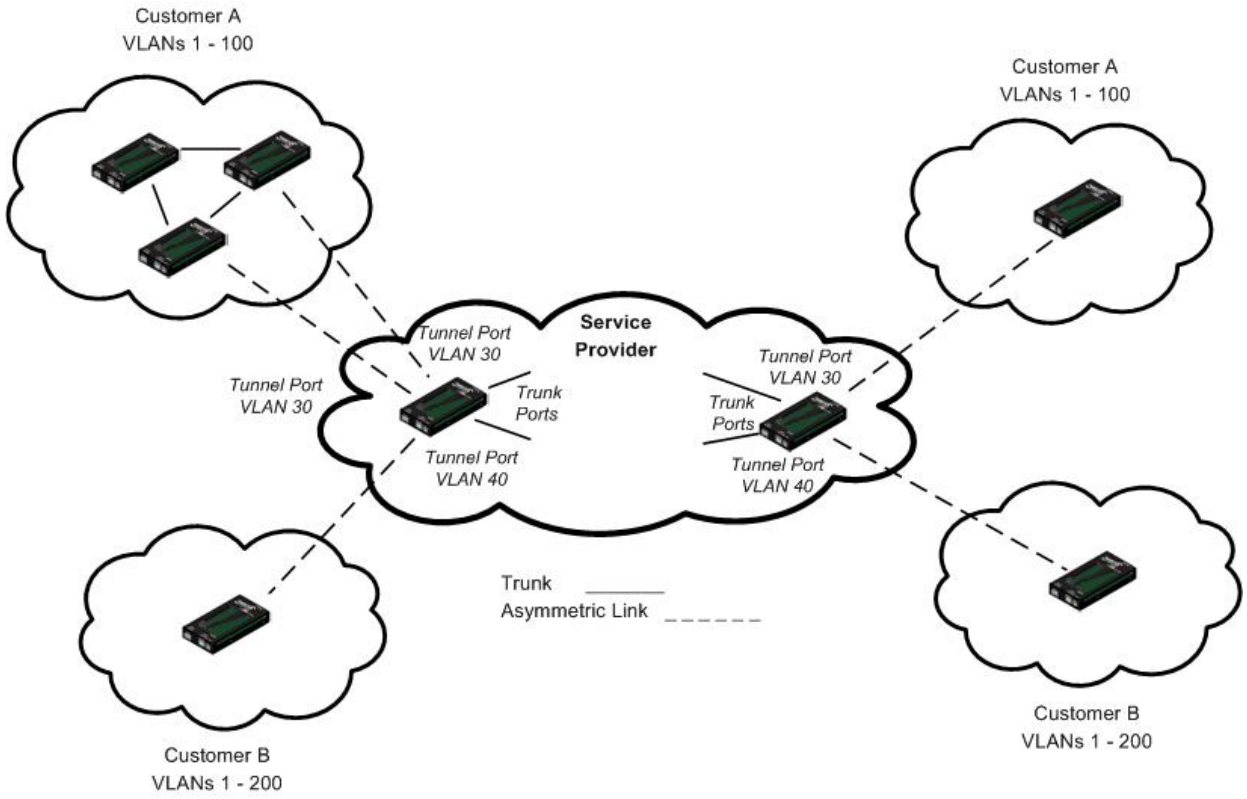


Figure 5: VLAN Tunneling Example

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

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

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

Summary

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

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

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

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

Prerequisites for VLAN Tunneling Functions

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

Restrictions for Configuring VLAN Tunneling Functions

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

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

See Appendix F of this manual for VLAN tunnel configuration examples.

L2CP (Layer 2 Control Protocol)

The x222x / x32xx NIDs support the Layer 2 Control Protocol (L2CP), a network control protocol standardized by the IETF, IEEE and MEF.

MEF 6 provides requirements for the processing of a Subscriber's Layer 2 Control Protocol (L2CP) frames on a given UNI for the services defined. The MEF 6 documents a Layer 2 Control Protocol identified by one of the following ranges of MAC Destination Addresses:

MAC DAs	Layer 2 Control Protocol
01-80-C2-00-00-00 through 01-80-C2-00-00-0F	Bridge Block of protocols
01-80-C2-00-00-20 through 01-80-C2-00-00-2F	GARP Block of protocols

Per MEF 6, for each service, protocols are configured to 'tunnel', 'peer', or 'discard' at the UNI. MEF allows for three L2CP processing options for each L2CP:

- **Peer** - the MEN will participate in the protocol.
- **Tunnel** - an ingress L2CP frame at a given UNI gets delivered unchanged to each of the destination UNIs. This requires all UNIs in the EVC to tunnel the same protocols. (Using 802.1 terms, the L2CP is 'forwarded' through the bridge relay.
- **Discard** - the MEN will ignore the L2CP frame (it will not participate in the protocol and it will not forward the frame).

Device Description / Circuit ID

The x222x / x32xx NIDs supports the Circuit ID, a company-specific identifier assigned by a provider to a data or voice network between two locations. This circuit is then leased to a customer by that ID. If a subscriber has a problem with the circuit, the subscriber contacts the telecom provider with this Circuit ID to initiate service action on the specified circuit.

The ION Circuit ID port identifier is based on the agent-local identifier of the circuit (defined in RFC 3046), detected by the agent and associated with a particular port. The x222x / x32xx supports the Circuit ID, a company-specific identifier assigned by the user to identify the converter and individual ports in any manner desired. At the device level, the x222x / x32xx supports a 'Device Description' character string entry of up to 64 bytes.

MAC Address Learning

This feature lets you disable MAC address learning on one or more ports for security purposes. If MAC address learning is disabled, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port. If you set MAC address learning to Enabled (Learning) on one or more ports, the other port states (Flooding, Filtering and Forwarding) are disabled.

System Logging (Syslog)

The x222x / x32xx 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 x222x / x32xx 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.

TN Topology Discovery Protocol TX

On the x222x and x322x converters, the TNDP feature can be Enabled, or Disabled, on a per-port basis. By default, it's Enabled on all ports.

When Enabled on a given port of an x22x or x322x converter, that converter may continually send LLDP frames in attempt to be discovered by an IONMM, through the given port. An LLDP frame is sent once every 1-2 seconds, while both of the following conditions exist:

1. The converter's "switch mode" is set to "remote" (this is Remote Management, the default setting).
2. The converter is not installed in a managed chassis.

When Disabled on a given port of an x222x or x322x converter, that converter cannot be discovered by an IONMM through the given port. Disabling TNTDP TX on a port does not prevent remote converters connected by that port from communicating with an IONMM through that port; it only prevents the configured converter from generating/sending its own LLDP Discovery frames through the given port.

Best Practices – The traffic related to remote management on these converters is transmitted in-band and is unnecessary on customer facing ports, therefore the TN Topology Discovery Protocol TX should be disabled on these ports. The TN Topology Discovery Protocol TX should only be enabled on the port that is the uplink port, back to another x222x or x322x card in an ION chassis that is utilizing the IONMM management module.

RFC 2544 Benchmarking

The x222x / x32xx supports IETF RFC 2544 (Benchmarking Methodology for Network Interconnect Devices). RFC 2544 defines several tests that can be used to describe the performance characteristics of a network interconnecting device, as well as specific formats for reporting the results of the tests (e.g., throughput, latency, frame loss rate, system recovery).

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 SBNMv3.

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.

WRR or Strict Priority Queuing

The x222x / x32xx supports WRR (Weighted Round Robin) or “Strict Priority” Egress Queue modes.

WRR scheduling allows each packet flow or connection to have its own packet queue. It is a simple approximation of GPS (generalized processor sharing). While GPS serves a near infinite amounts of data from each nonempty queue, WRR serves a number of packets for each nonempty queue (number = normalized (weight / meanpacketsize).

With the Strict Priority Queuing function enabled, only high priority packages will be passed and all low priority packages will be dropped during a network jam condition. SP queuing assumes that types of traffic can be differentiated and treated preferentially. Separate FIFO queues are created for each defined priority level and the arriving traffic is sorted into its proper queue as it arrives. So the first task of configuring strict priority queuing is to determine traffic classifications. Usually 2-5 priority levels are defined (e.g., high, medium, normal, low), although more levels can be defined. Having more queues means more complexity in running the algorithm. At the service side of the queue, the processing rule is simple: higher priority FIFO queues always get completely processed before lower priority queues get processed.

Serial File Transfer (X/Y/Zmodem)

The x222x / x32xx supports serial get, put, and upgrade commands using the Xmodem, Xmodem-1k, Ymodem, and Zmodem protocols. These commands function similar to the TFTP download function; technical support can download configuration files and firmware files through the x222x/x32xx USB port by entering the corresponding CLI commands.

Supported MIBs

The x222x / x32xx NIDs support public (standard) and private Management Information Bases (MIBs).

Public MIBs

The x222x / x32xx NID provides complete management through the SNMP interface. It supports the following standard MIBs for management using SNMPv1/v2c.

Private MIBs

The Lantronix private MIBs for SNMP IP-based management feature extensive management options, including:

Table 1: Supported MIBs

#	MIB	RFC # or Private	Description
1	BRIDGE-MIB	RFC4188	Bridge MIB module for managing devices that support IEEE 802.1D
2	DOT3-LOAM-MIB	RFC4878	MIB module for managing the new Ethernet LOAM features introduced by the Ethernet in the First Mile taskforce (IEEE 802.3ah)
3	ENTITY-MIB	RFC 4133	MIB module for representing multiple logical entities supported by a single SNMP agent
4	ENTITY-SENSOR-MIB	RFC 3433	Defines Entity MIB extensions for physical sensors
5	EtherLike-MIB	RFC3635	Describe generic objects for Ethernet-like network interfaces
6	IANA-MAU-MIB	RFC 4836	Defines dot3MauType OBJECT-IDENTITIES and IANAifMauListBits, IANAifMauMediaAvailable, IANAifMauAutoNegCapBits, and IANAifJackType
7	IEEE8021-CFM-MIB	RFC ____	Connectivity Fault Management module for managing IEEE 802.1ag
8	IEEE8021-TC-MIB	RFC ____	Textual conventions used throughout the various IEEE 802.1 MIB modules
9	IF-MIB	RFC 2863	Describes generic objects for network interface sub-layers
10	MAU-MIB	RFC 4836	Management information for 802.3 MAUs
11	P-BRIDGE-MIB	RFC 4363	Module for managing Priority and Multicast Filtering
12	Q-BRIDGE-MIB	RFC 4363	Module for managing Virtual Bridged LANs
13	RFC1213-MIB (MIB-II)	RFC 1213	Defines the second version of the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets
14	RMON-MIB	RFC 1757	Defines objects for managing remote network monitoring devices (i.e., monitors or probes)
15	TRANSITION-SMI	Private	Lantronix Enterprise Structure of Management Information; assigns ION platform module identities
16	TRANSITION-TC	Private	Lantronix Inc MIB Textual Conventions module; defines textual conventions used in the Lantronix enterprise MIBs
17	TN-ION-BPC-MIB	Private	Lantronix, Inc. Enterprise MIB for Chassis Management).
18	TN-ION-CHASSIS-MIB	Private	Lantronix, Inc. Enterprise MIB for Chassis Management
19	TN-ION-MGMT-MIB	Private	Lantronix, Inc. Enterprise MIB for basic management of the ION Platform
20	TN-PROV-BRIDGE-MIB	Private	Lantronix, Inc. Enterprise MIB for IEEE Bridge provisioning, i.e., IEEE MAC/VLAN bridges
21	TN-ION-VLAN-MGMT-MIB	Private	Lantronix, Inc. Enterprise module for managing VLAN and QoS in ION platform products
22	TN-ION-LOAM-EXT-MIB	Private	Lantronix, Inc. module for managing Link OAM (IEEE 802.3ah Clause 57) enterprise extensions in ION platform products
23	TN-ION-ENTITY-SENSOR-MIB	Private	Lantronix, Inc. module for managing all ION power supply and fan modules)

24	ION-DEV-SYS-ACL-MIB	Private	Lantronix Enterprise MIB for ION device ACL feature
25	ION-DEV-SYS-HTTPS-MIB	Private	Lantronix Enterprise MIB for ION device HTTPS feature
26	ION-DEV-SYS-IPMGMT-MIB	Private	Lantronix Enterprise MIB for ION device IP management feature
27	ION-DEV-SYS-PROV-MIB	Private	Lantronix Enterprise MIB for ION device Provision feature
28	ION-DEV-SYS-RADIUS-MIB	Private	Lantronix Enterprise MIB for ION device RADIUS management feature
29	ION-DEV-SYS-SNMPMGMT-MIB	Private	Lantronix Enterprise MIB for ION device SNMP management feature
30	ION-DEV-SYS-SNTP-MIB	Private	Lantronix Enterprise MIB for ION device SNTP management feature
31	ION-DEV-SYS-SSH-MIB	Private	Lantronix Enterprise MIB for ION device SSH feature
32	ION-DEV-SYS-STATE-MIB	Private	Lantronix Enterprise MIB for ION device state
33	ION-DEV-SYS-TFTP-MIB	Private	Lantronix Enterprise MIB for ION device TFTP feature
34	ION-DEV-SYS-UPGRADER-MIB	Private	Lantronix Enterprise MIB for ION device upgrader feature

The remote NID can be managed completely through LOAM. An example of a private MIB objects tree is shown in the figure below.

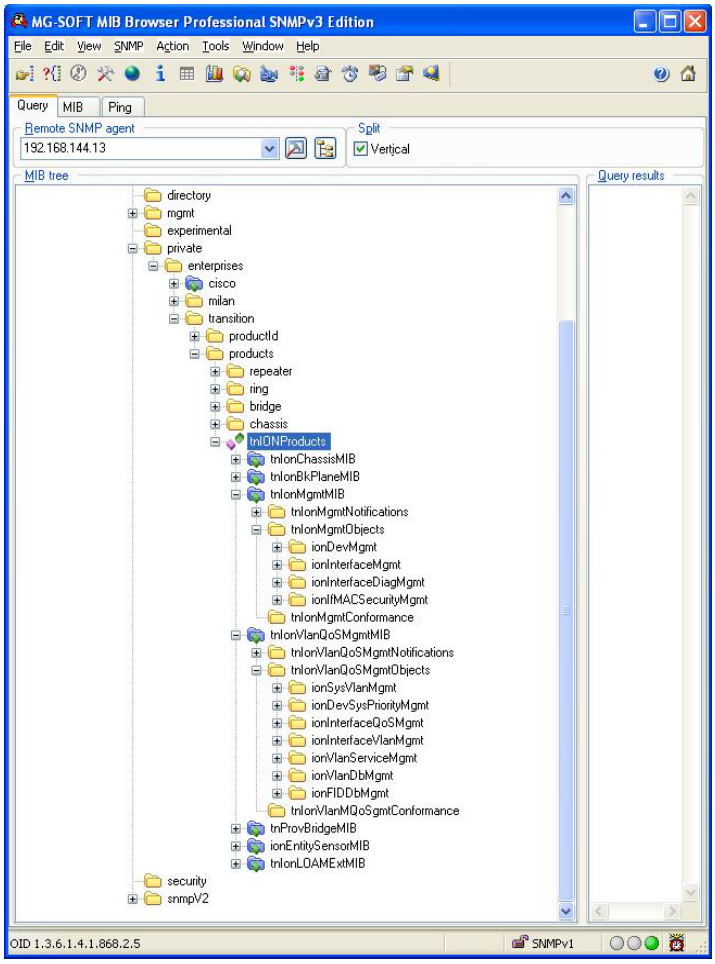


Figure 6: Private MIB Objects

Downloading, Compiling and Integrating MIBs

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

To download ION system private MIBs:

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

Set up your ION system SNMP configuration via the command line interface (CLI). Refer to "Configuring SNMP" on page 228. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.

For Additional MIB Information

For information on traps that the IONMM supports, see "Appendix G: SNMP Traps Supported" on page 543.

NID Models

The various models of the x222x / x32xx NIDs (Standard / Single Fiber Models and Chassis / Standalone Models) are described below.

Standard Models and Single Fiber Models

ION products are available in chassis and standalone models. The models can include both standard and single-fiber models, as well as specific models that support the DMI option. **Note:** the -D after the model number indicates DMI option support. The **-T** after the model number indicates extended temperature support.

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

Chassis Models (*Cxxxx*) and Standalone Models (*Sxxxx*)

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

ION Standalone models include remotely-managed NIDs (Network Interface Devices). An end-to-end fiber integration solution can be achieve by pairing the modules in a high density ION chassis with the modules in another ION chassis, an ION stand-alone, or a Lantronix' Point System™ stand-alone device.

ION System Model Number Key

Sample Model Number: C2220 – 1011 – D
Model Character #: 12345 – 6789 - xx

Character #	Meaning
1	**C** (Chassis) or **S** (Standalone)
2 and 3	**21** (100Base Ethernet); **22** (10/100 Ethernet); **31** (1000BASE Ethernet); **32** (10/100/1000 Ethernet); **41** (10GBASE Ethernet); **42** (10/100/100/1000/10G Ethernet); **60** (T1 / E1); 61 (4xT1); **62** (DS3 – T3 / E3).
4 and 5	**10** (Standard Conversion); **20** (Advanced Management); **xx** (Unique Identifier)
6, 7, 8, 9	**10** (RJ-45); **11** (Multimode ST); **13** (Multimode SC); **14** (Single Mode SC); **15** (Single Mode SC Long Haul); **16** (Single Mode SC Extra Long Haul); **17** (Single Mode SC Long Wave 1550); **19** (Single Mode LC); **24** (Extended Multimode SC); **29** (Single Fiber SC); **30** (Dual BNC); **33** (RJ-11); **35** (Single Mode SC Long Wave 1550 Extended); **39** (Multimode LC); **40** (SFP Slot).
xx	New features or capabilities: **-D** (DMI support); **-T** (extended temperature support)

Thus the sample model number C2220-1011-D above is a Chassis-based 10/100 Ethernet device with Advanced Management, Standard Conversion, RJ-45 / Multimode ST and optional DMI support.

Similarly, model number S3220-1035 is a Standalone, 10/100/1000 Ethernet device with Advanced Management, RJ-45 / Single Mode SC Long Wave 1550 Extended connection.

Physical Specifications

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

All Model x222x / x32xx

Dimensions	SIC: 3.4” x 0.86” x 6.5” (86 mm x 22 mm x 165 mm) Standalone: 3.25” x 1.0” x 6.5” (82 mm x 25 mm x 165 mm)
MAC Filtering	8K MAC addresses
Power Input	Standalone: 12VDC @ 375mA SIC: Powered by the Chassis
Environment	0 to 50°C (32 to 122°F) operating; 5% - 95% humidity (non-condensing) 0 to 10,000 ft. altitude
Storage Temp	-40 to 85°C (-40 to 185°F)

C2220 Series

Standards	IEEE Std. 802.3, IEE std. 802.3ah, IEE Std. 802.1P, IEEE std. 802.1Q
Data Rate	Copper: 10/100/1000Mbps Fiber: 100Mbps
Filtering Address	8K MAC Addresses
Power Consumption	4.5 Watts
Shipping Weight	1 lb. [.45 kg]
Regulatory Compliance	EN55022 Class A, EN55024, CE Mark

C322x Series

Standards	IEEE Std. 802.3, IEEE Std. 802.3ah, IEEE Std 802.1P, IEEE Std 802.1Q
Data Rate	Copper: 10/100/1000Mbps Fiber: 1000Mbps
Max Frame Size	10,240 bytes
Power Consumption	4.5 Watts
Shipping Weight	1 lb. [.45 kg]
Regulatory Compliance	EN55022 class A, EN55024, CE Mark

S322x Series

Standards	IEEE Std. 802.3, IEEE Std. 802.3ah, IEEE Std 802.1P, IEEE Std. 802.1Q
Data Rate	Copper: 10/100/1000Mbps Fiber: 1000Mbps
Max Frame Size	10,240 bytes
Dimensions	Width: 3.25” [82 mm] Depth: 6.5” [165 mm] Height:1.0” [25 mm]
Power Input:	100-240VAC,1A
Output:	12VDC, 1.25A
Shipping Weight	2.0 lbs. [0.90 kg]
Regulatory Compliance	EN55022 Class A, EN55024, UL60950, CE Mark

MEF Certification

The Lantronix ION system S3220, S2220, S3230, S3240, C2220, C3220, and C3230 have MEF 9, MEF 14, and MEF 21Certification. MEF Certificates are available at the Lantronix product resources page.

Documentation Conventions

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

Table 7: Documentation Conventions

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

Related Manuals and Online Helps

A printed documentation card is shipped with each x222x / x32xx device. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface.

A substantial set of technical documents, white papers, case studies, etc. are available on the Lantronix Support web page. Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

The ION system and related device manuals are listed below.

1. ION Management Module (IONMM) User Guide, 33457
2. ION Systems CLI Reference Manual, 33473
3. ION219-A 19-Slot Chassis Installation Guide, 33412
4. ION106-x Six Slot Chassis User Guide, 33658
5. IONPS-A-R1 Power Supply User Guide, 33614
6. IONPS-A AC Power Supply Install Guide, 33423
7. IONPS-D DC Power Supply Install Guide, 33424
8. SFP manuals (product specific)
9. Release Notes (software version specific)
10. Product Documentation Postcard, 33504

This manual may provide links to third part web sites for which Lantronix is not responsible. Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version. While all screen examples may not display the latest version number, all of the descriptions and procedures reflect the latest software/firmware version, noted in the Revision History on page 2.

2. Installation and System Setup

General

This section describes how to install the x222x / x32xx NID and the procedures to access and initially set up the NID through either a local serial interface (USB) or a remote Ethernet connection (Telnet session or Web interface).

Installing the Chassis Model (C222x / C32xx)

The Cx2xx NID is a slide-in module that can only be installed in a Lantronix ION chassis (ION001-x and ION219-x). For a complete list of ION platform products, go to the Lantronix webpage.

The following describes how to install the Cx2xx in the ION chassis.

Caution: Failure to wear a grounding device and observe electrostatic discharge precautions when installing the C222x / C32xx could result in damage or failure of the module.

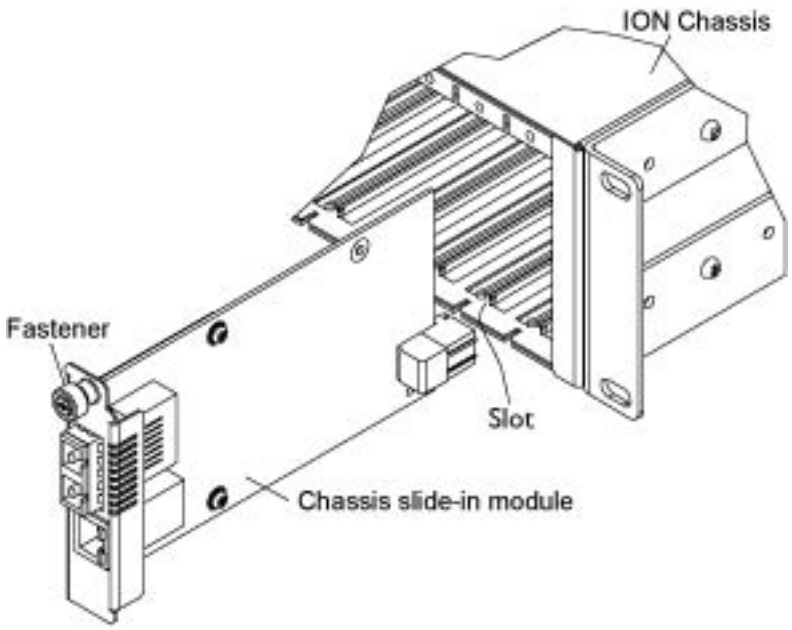


Figure 7: Chassis Installation

IMPORTANT

The Cx2xx slide-in cards are “hot swappable” devices, and can be installed with chassis power on.

1. Locate an empty slot in the ION System chassis.
2. Grasp the edges of the card by its front panel.
3. Align the card 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 to the chassis (see “Figure 9: Chassis Installation” on the previous page).
6. Note that the card’s Power LED lights. See “Accessing the NIDs” on page 65.

Installing the Standalone Model (S222x / S32xx)

The standalone model can be installed in any of these ways:

- Rack mounted
- Table top
- Wall mounted

Rack Mount Installation

The S222x / S32xx standalone module can be mounted into a Lantronix E-MCR-05 media converter rack, which can be installed on a tabletop or in a standard site rack. For installation details, see the E-MCR-05 Media Converter Rack product page.

Tabletop Installation

The S222x / S32xx ships with four rubber feet for optional installation on a table or other flat, stable surface in a well-ventilated area.

1. Remove the rubber feet from the card.
2. On the bottom of the NID, place one foot in each corner of the device.

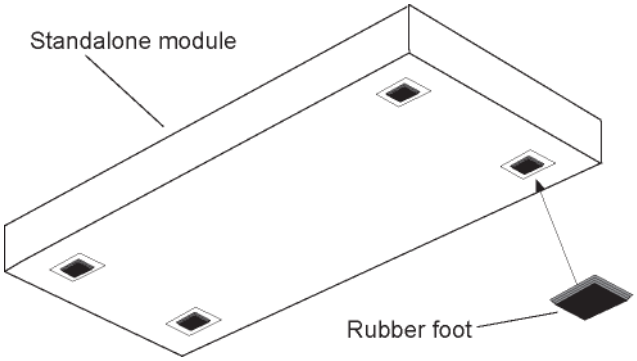


Figure 8: Tabletop Installation

3. Set the NID in place and connect the AC power adapter (see "Connecting to AC Power" on page 45).

Wall Mount Installation

1. Remove the four #4 Philips head screws securing the cover to the device and orient the device as shown in the figure below.

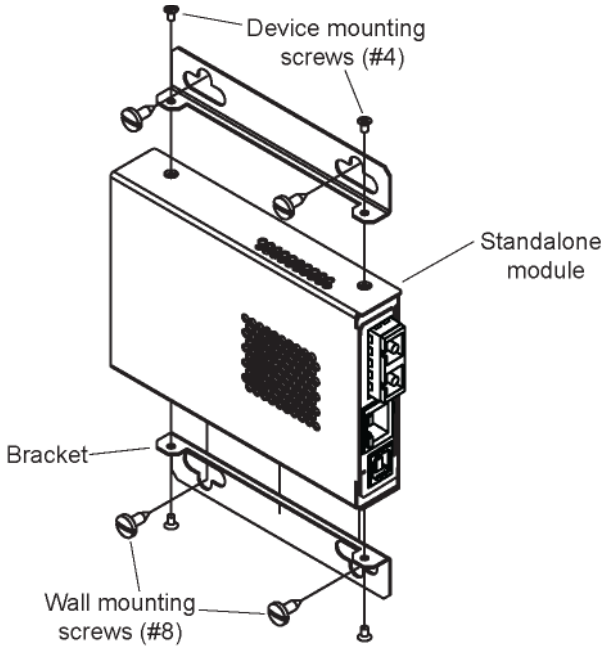


Figure 9: Wall Mount Installation

2. Mount one of the bracket assemblies to the device using two of the #4 Philips head screws.
3. Mount the other bracket assembly to the other side of the device using the other two #4 Philips head screws.
4. Position the device on the mounting surface.
5. Use the four #8 screws to mount the bracket to the mounting surface.
6. Connect the AC power adapter (see Connecting to AC Power on page 49).

Connecting to AC Power

After the standalone NID has been installed, connect it to the AC-DC power adapter. Use the AC power adapter shipped with the NID (TNPN 25025).

Warning: Risk of electrical shock.

1. Insert the barrel connector of the AC power adapter to the power inlet on the back of the standalone NID.

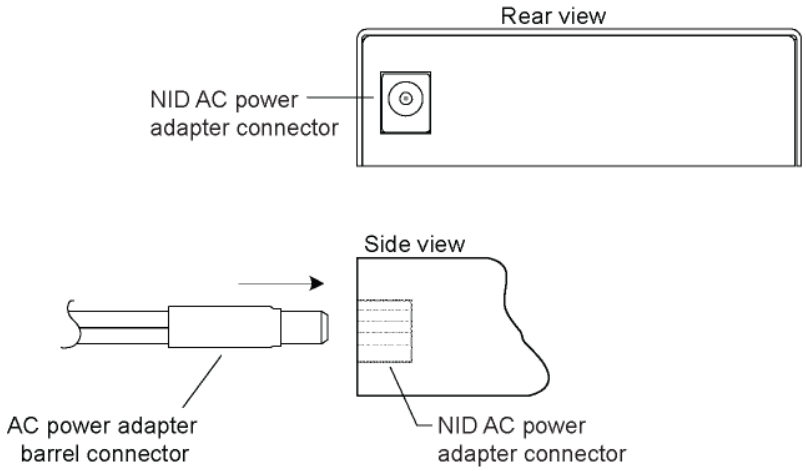


Figure 10: AC Power Connection

2. Plug the Power adapter plug into AC power at an appropriate AC outlet. Note that the standalone NID's front Power (PWR) LED lights.

Installing SFPs

Some models allow you to install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection. The C32x1-1040 and S32x0-1040 have a single SFP port. The C32x1-1040 and S32x1-1040 have two SFP ports. See the related SFP User Guide for cautions and warnings.

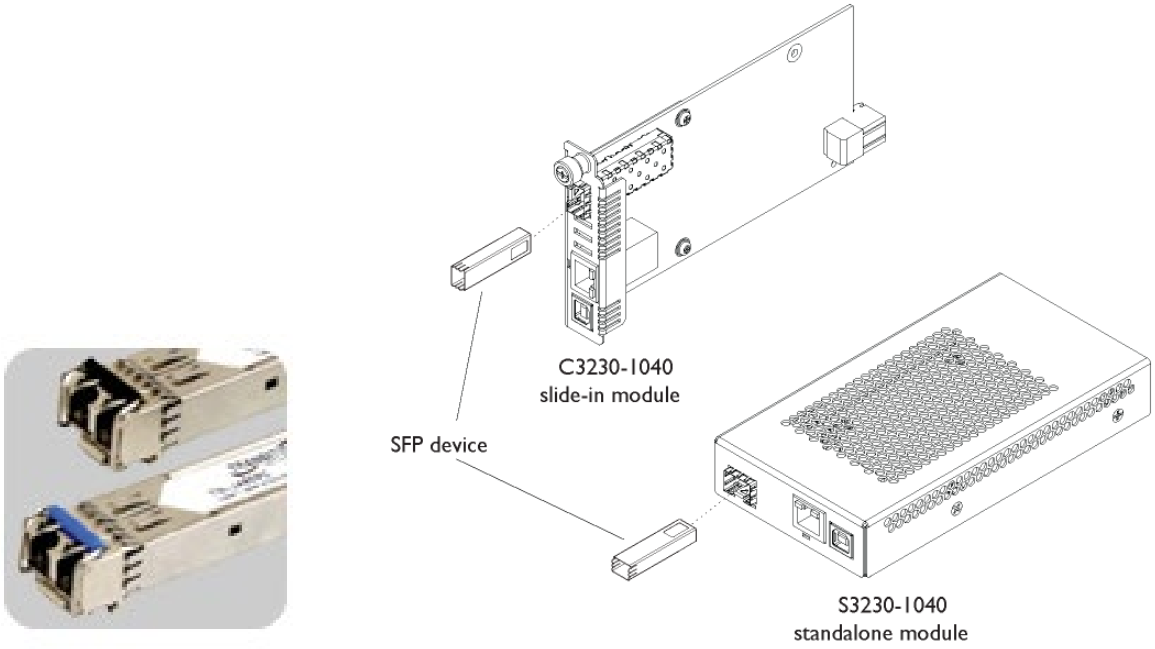


Figure 11: SFP Installation

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

Connectors and LEDs

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

Model x2220-1040

The x2220-1040 connectors and LEDs are shown in the two figures below and described in Table 8.

Figure 12: Model C2220-1040 Connectors and LEDs

Figure 13: Model S2220-1040 Connectors and LEDs

The x2220-1040 connectors and LEDs are described in the table below.

Table 8: Model x2220-1040 Connectors and LED Descriptions

Connector/LED	Description
100/1000 SFP port connector	Lets you install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection.
USB connector	Used to connect the NID to a PC for a direct serial interface. Through this connection, a system administrator can access and control the NID using CLI commands.
10/100/1000 (Copper port) connector	One connector for Ethernet 10/100/1000 Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either remote Telnet session or the Web interface.
PWR (Power) LED	When lit, indicates that there is power to the NID.
LACT (Link active) LED	Yellow – operation is 10 MBps (10Base-T). Green – operation is 100 MBps, 100Base-T.
DUP (Duplex) LED	When lit, indicates duplex mode: • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Model x3221-1040

The x3221-1040 connectors and LEDs are shown in the two figures below, and described in Table 7.

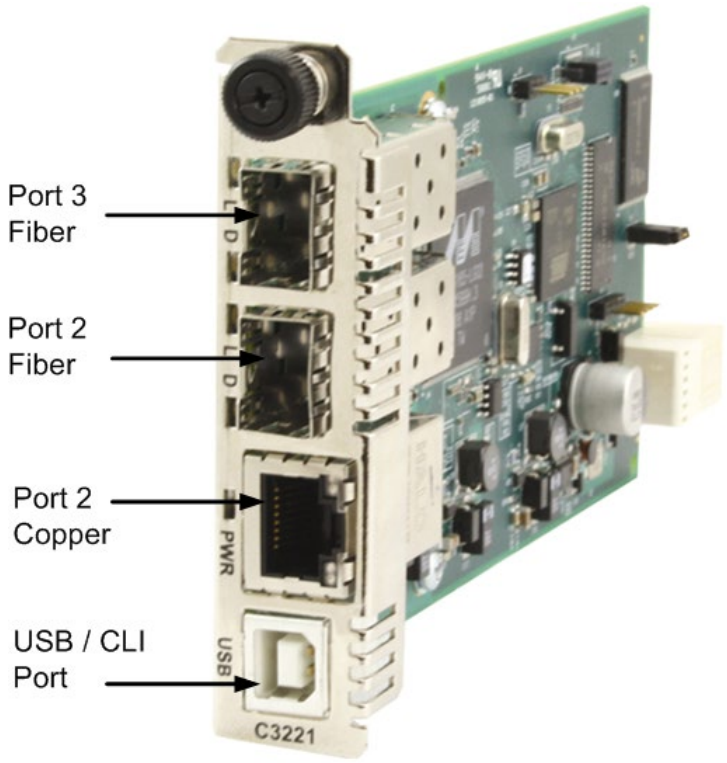


Figure 14: Model C3221-1040 Connectors and LEDs

Figure 15: Model S3221-1040 Connectors and LEDs

The x3221-1040 connectors and LEDs are described in the table below.

Table 9: Model x3221-1040 Connectors and LED Descriptions

Connector/LED	Description
100/1000 SFP port connector	Lets you install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection.
USB connector	Used to connect the NID to a PC for a direct serial interface. Through this connection a system administrator can access and control the NID using CLI commands.
10/100/1000 (Copper port) Network connectors	One connector for Ethernet 10/100Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either remote Telnet session or the Web interface.
PWR (Power) LED	When lit, indicates that there is power to the NID.
LACT (Link active) LED	Yellow – operation is 10 MBps, 10Base-T. Green – operation is 100 MBps, 100Base-T.
DUP (Duplex) LED	When lit, indicates duplex mode: • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Model x32x0-10xx

The x32x0-1040 connectors and LEDs are shown in the two figures below and described in Table 8.

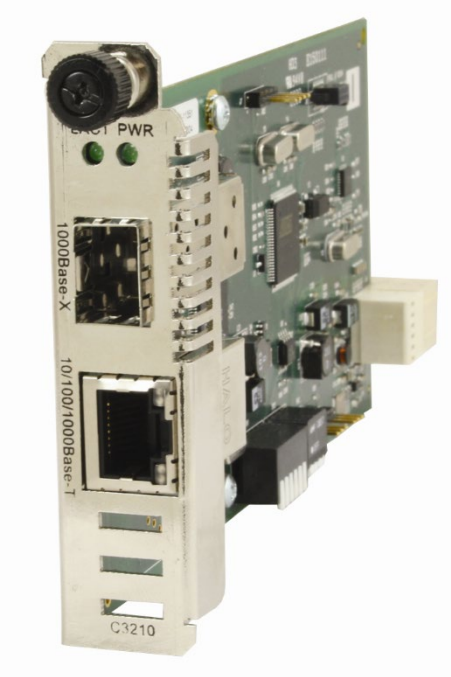


Figure 16: Model C32x0-10xx Connectors and LEDs

Figure 17: Model S32x0-10xx Connectors and LEDs

The x32x0-10xx connectors and LEDs are described in the table below.

Table 10: Model x32x0-10xx Connectors and LED Descriptions

Connector/LED	Description
100/1000 100Base-X SFP port connector	Lets you install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection. Used to connect the NID via fiber to a device (switch, router, NID, etc.).
USB connector	Used to connect the NID to a PC for a direct serial interface. Through this connection a system administrator can access and control the NID using CLI commands.
10/100/1000 (Copper port) Network connectors	One connector for Ethernet 10/100Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either a remote Telnet session or the Web interface.
PWR (Power) LED	When lit, indicates that there is power to the NID.
LACT (Link active) LED	Yellow – operation is 10 MBps, 10Base-T. Green – operation is 100 MBps, 100Base-T.
DUP (Duplex) LED	When lit, indicates duplex mode: • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Operating Systems Supported

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

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

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

Installing the USB Driver (Windows XP)

IMPORTANT

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

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

1. Extract the driver ~~(from the Lantronix website)~~ from the ION Platform product page and place it in an accessible folder on the local drive of the PC.
2. Connect the NID to the USB port on the PC.

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

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

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

Installing the USB Driver (Windows 8)

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.

To install the USB driver on a computer with the *Windows 8* operating system, do the following.

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 HyperTerminal

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

1. On the desktop, right-click on **My Computer**.
2. Select **Manage**. The **Computer Management** window displays.
3. Click on **Device Manager** to open the Device Manager panel. (If a Device Manager message displays, click **OK** and continue.)
4. In the right panel, expand the list for **Ports (COM & LPT)**.

   Write down the USB COM port number for the "*TNI CDC USB to UART*" listing (COM 5 in the example above). You will need to provide this COM port number in step 8 below.
5. Launch the HyperTerminal software.

   a) Click **Start**.

   b) Select: **All Programs > Accessories > Communications**

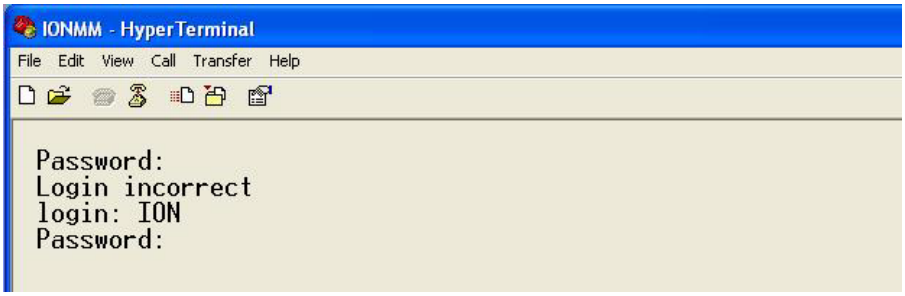
   c) Click **HyperTerminal**.

   The Connection Description window displays.
6. Type in a name and select an icon that will be used for this connection.
7. Click **OK**. The **Connect To** window displays.
8. From the drop-down list in the **Connect using** field, select the COM port noted in step 4.
9. Click **OK**. The **Port Settings** window displays.
10. Set the COM port properties as follows:
    - Bits per second: **115200**
    - Data bits: **8**
    - Parity: **None**
    - Stop bits: **1**
    - Flow control: **None**
11. Click **OK**. A blank HyperTerm window displays.
12. In the HyperTerm window, select **File > Properties**. The Properties window displays the **Connect To** tab.
13. Click the **Settings** tab.
14. In the **Emulation** field, select **VT100**.
15. Click the **ASCII Setup…** button.
16. Verify that **Wrap lines that exceed terminal width** is selected.
17. Click **OK** twice.
18. Login (see Starting a USB Session below).

Starting a USB Session in HyperTerminal

The procedure below describes how to access the x222x/x32xx via a USB connection. The x222x/x32xx can be controlled from a remote management station via a HyperTerminal session over an Ethernet connection. The x222x/x32xx is controlled and configured through CLI commands. Use the following procedure to connect to and access the x222x/x32xx via a HyperTerminal (HT) session.

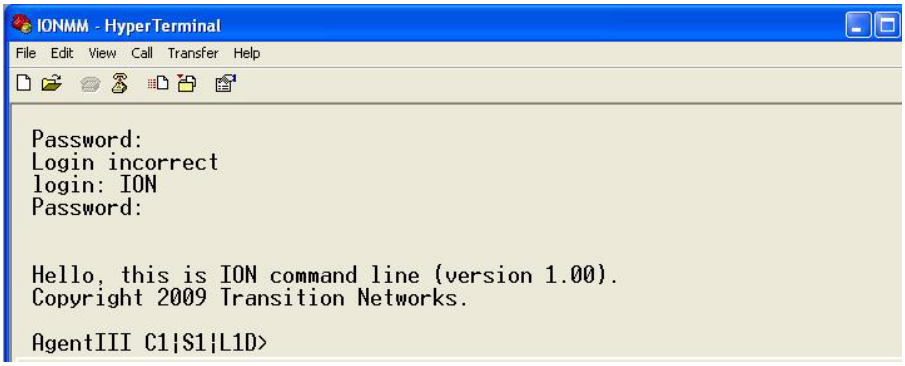
1. Click Windows **Start**.
2. Select **All Programs > Accessories > Communications > HyperTerminal**.
3. Create a new HT connection (select **File** > **New**) or select an existing connection (**File** > **Open**).
4. Press the **Enter** key. The Password prompt displays. If "*Login incorrect*" displays, ignore it.



If the login prompt does not display, try unplugging and re-plugging the USB cable at the IONMM.

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

5. Type **ION** (all upper case) and press the **Enter** key. The login prompt displays.
6. Type **private** (all lower case) and press the **Enter** key. The ION system command prompt displays. For example:




```
Hello, this is ION command line (version 1.00).
Copyright 2009 Lantronix.

Agent III C1|S1|L1D>
```

7. Continue by entering ION CLI commands to the right of the > symbol. Press the **Enter** key after each command.
8. If the NID controlled by the IONMM, go to step 9. Otherwise continue with step 10.

9. Enter a **go** command to change the location for the command prompt. 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).

10. Enter commands to set up the various configurations for the NID. For configuration information, see "Section 4: Configuration" on page 87. For a description of all available CLI commands see the *ION Systems CLI Reference Manual, 33461*.

Note: If required by your organization's security policies and procedures, use the CLI command **set community write=<xx>** to change the default password. See the *ION Systems CLI Reference Manual*, 33461.

Terminating a USB Connection from HyperTerminal

To terminate the USB connection, do the following.

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

Access via an Ethernet Network

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

IMPORTANT

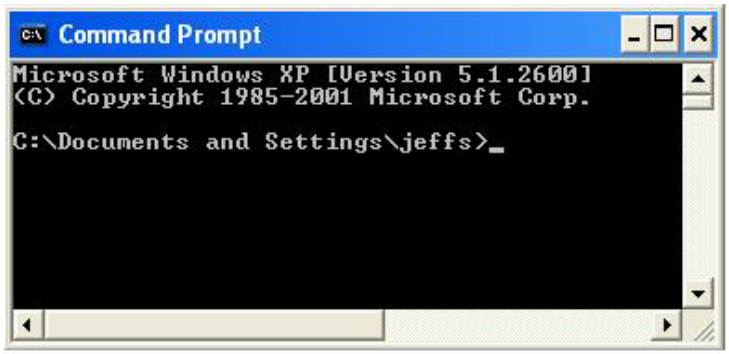
It is recommended that you initially set up the IP configuration through the serial interface (USB connection). See "Performing Initial System Setup" on page 56.

Otherwise, in order to communicate with the NID 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 NID (see "Appendix B: Factory Defaults" on page 534). Make note of the original settings for the PC as you will need to reset them after setting the IP configuration for the NID.

Starting a Telnet Session

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

1. Click **Start**.
2. Select **All Programs > Accessories**.
3. Click **Command Prompt**. The command prompt window displays.



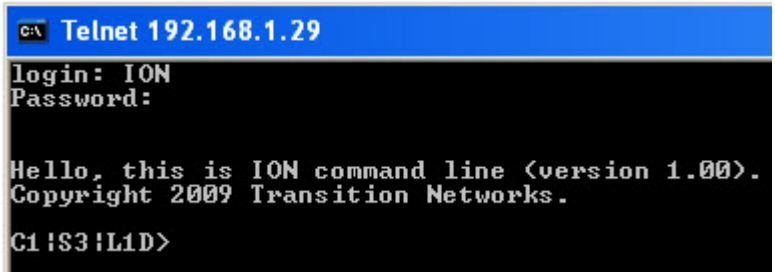
4. At the command line type: **telnet** <xx> where:

   xx = IP address of the NID

5. Press **Enter**. The login prompt displays.

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

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



10. If the NID is controlled by the ION Management Module, go to step 11.
    If the NID is not controlled by the ION Management Module, go to step 12.
11. Enter a **go** command to change the location for the command prompt. 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 Standalone card
12. Enter commands to set up the various configurations for the NID. For configuration information, see Section 4: “Configuration” on page 89. For a description of all available CLI commands see the *ION Systems CLI Reference Manual, 33473*.

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

Terminating a Telnet Session

To terminate the Telnet session:

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

Initial Setup with a Static IP Address via the CLI

The x222x/x32xx supports IPv4-based application protocols. The x222x/x32xx can be assigned IP address statically or dynamically using DHCP. The x222x/x32xx supports DNS, which lets you assign it a hostname instead of an IP address. The static IP address assignment is part of the initial x222x/x32xx setup, and at first the CLI (command line interface) is used to configure the IP address settings. Thereafter, remote management and/or DHCP addressing can be configured.

The default values are IP Address = 192.168.0.10, Subnet Mask = 255.255.255.0, Default Gateway = 192.168.0.1, with no DNS address assigned, and no DHCP client enabled. When manually setting the x222x / x32xx NID'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).

The following procedure is for setting a static IP address for the x222x/x32xx NID. When this procedure is completed, you can communicate with the x222x/x32xx across the network via either a Telnet session or the Web interface.

1. Start a USB session (see "Starting a USB Session" on page 67).
2. At the command prompt type **set ip type=ipv4 addr**=<xx> **subnet–mask** =<yy> where:

   xx = IP address of the NID

   yy = subnet mask
3. Press **Enter**.
4. Set the IP address mode. Type **set ip address mode**=<xx> where:

   xx = the IP addressing mode (bootp, dhcp, or static).
5. Type **set gateway type**=**ipv4 addr**=<xx> where:

   xx = default gateway address (note that only one default gateway can be set)
6. Press **Enter**.
7. Verify the setup. Type **show ip-mgmt config** and press **Enter**. The current configuration displays.

   For example:

```
Agent III C1|S9|L1D>set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0
Agent III C1|S9|L1D>set ip address mode=static
Agent III C1|S9|L1D>set gateway type=ipv4 addr=192.168.0.1
Agent III C1|S9|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:fe21:177
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        192.168.1.30
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|S9|L1D>
```

For more information about IP configurations see “Setting the IP Addressing” on page 92.

Accessing the NIDs

The x222x / x32xx NIDs can be accessed through either a local serial interface via a USB connection or through an Ethernet network connection. The network connection can be done via a Telnet session or a Web graphical user interface (GUI).

Access via Local Serial Interface (USB)

The x222x / x32xx NIDs can be connected to a local management station (PC) through a serial interface using a USB connection. The NID is controlled by entering command line interface (CLI) commands at the local management station. To use the serial interface (USB) the following is required:

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

IMPORTANT

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

Web Browsers Supported

The ION system supports the latest version of most popular web browsers.

Starting the Web Interface

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

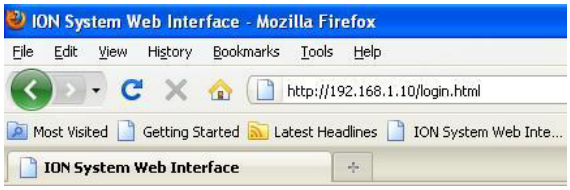
A Web session can be used to connect to and set up the NID.

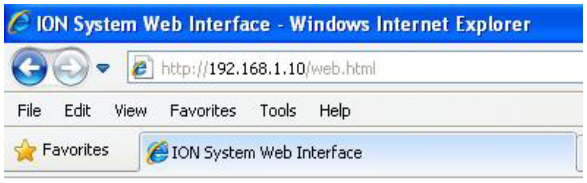
IMPORTANT

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

To sign in to the NID via the Web, do the following.

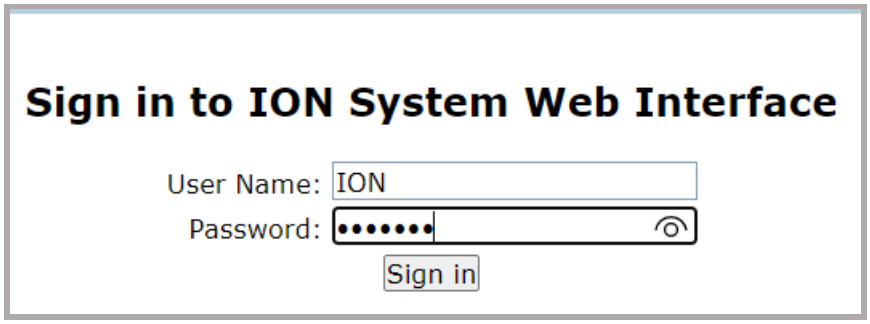
1. Open a web browser.





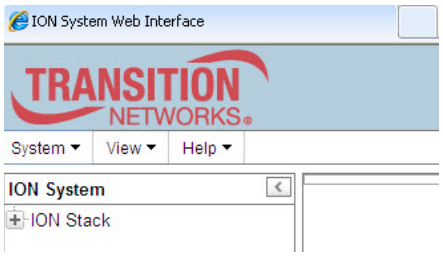
2. In the address (URL) block, type the IP address of the NID (the default address is 192.168.1.1).
3. Click **Go** or press **Enter**.

The ION System sign in screen displays.

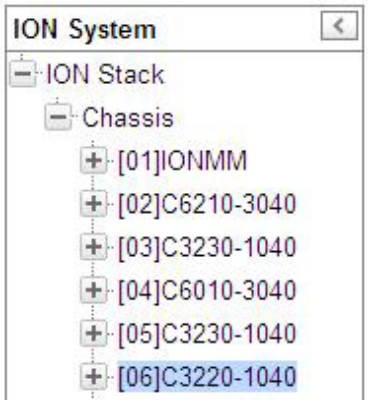


Note: If your systems uses a security protocol (e.g., RADIUS, SSH, etc.), you must enter the login and password required by that protocol.

4. Type the System name (the default is **ION**). **Note:** the System name is case sensitive.
5. Type the password (the default is **private**). **Note:** the password is case sensitive.
   : Click to display the Password text as you type it.
   : Click to hide the Password text as you type it.
6. Click **Sign in** or press **Enter**. The opening screen displays.

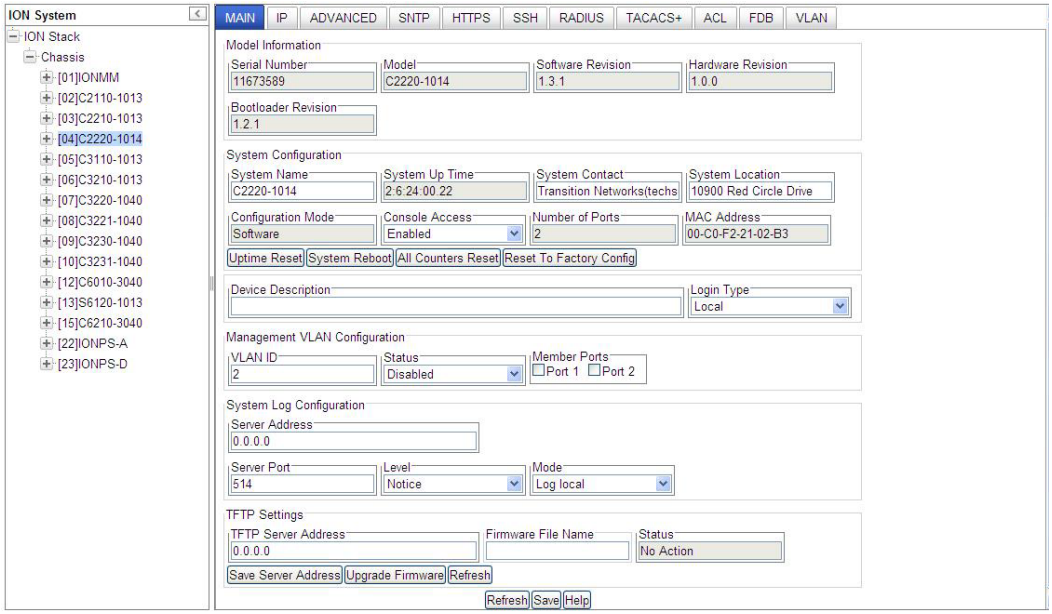


7. Click the plus sign [**+**] next to **ION Stack**. This unfolds "ION Stack" node in the left tree view and will refresh device status.
8. Click the plus sign [+] next to **Chassis** to unfold the chassis devices.

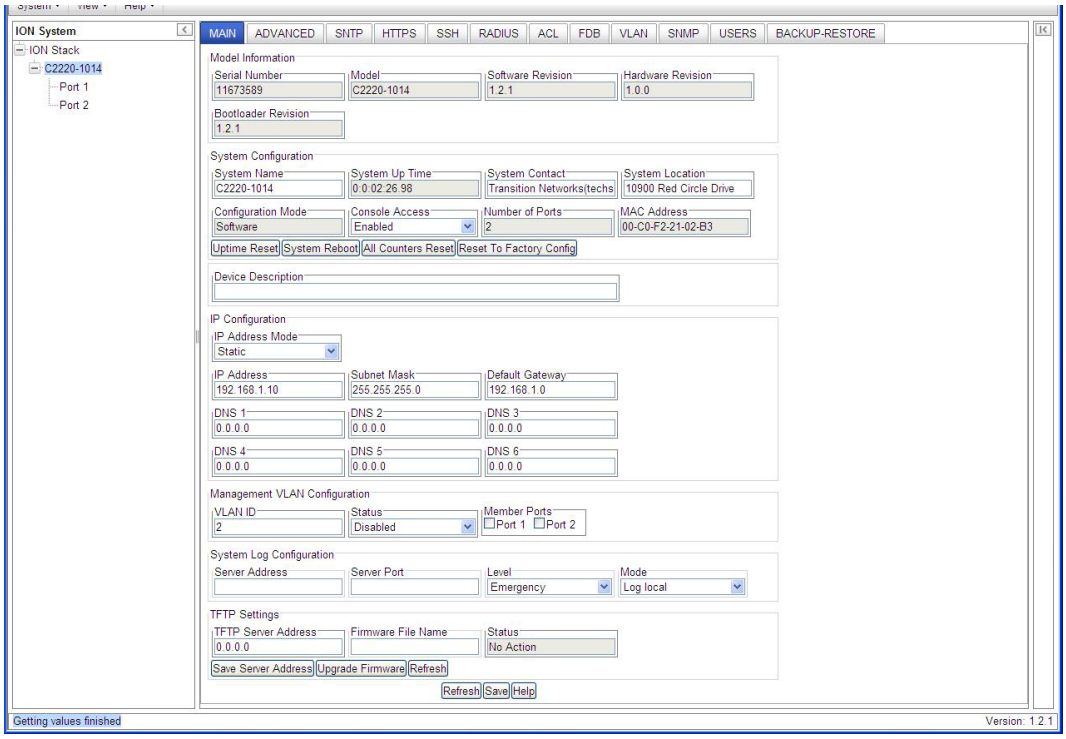


9. Select the appropriate model NID. The **MAIN** screen displays for the selected NID.

A Model C2220 **MAIN** screen is shown below:



A Model C2220 **MAIN** screen is shown below (for a device in Local switch mode).

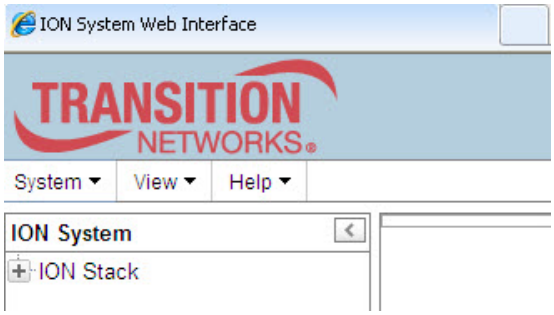


10. You can use the various tabs to configure the system, devices and ports. For configuration information, see “Section 4: Configuration” on page 165.

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

Terminating the Web Interface

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



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

The sign in screen displays.

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

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

Changing Switch Mode (Local / Remote)

Management and configuration control can be switched between local management control (via CLI, Telnet or Web) or remote management control (via the IONMM).

The switch mode can be changed for the NID using only the CLI method.

The CLI command **set switch mode={local | remote}** changes the operating mode of a standalone device.

Remote Mode: the device can only be managed and configured via the IONMM. Setting the switch mode to remote indicates that the device is managed through the IONMM. The device cannot perform any IP management when in 'remote' mode. Remote mode is the C222x/C32xx default mode for all firmware versions. This is the S222x/S32xx (standalone) default mode at version 1.2 and below.

Local Mode: the device can only be configured and managed directly via CLI, Telnet or Web. Setting the mode to **local** indicates that the device is managed through either a direct USB connection or a direct network connection via Telnet or the Web interface (i.e., the device is no longer managed by the IONMM). This is the S222x/S32xx (standalone) default mode at version 1.3.10 and above. If deployed as a standalone, this must be set to Local.

To change the device switch mode to local, do the following:

1. Start a USB session (see "Starting a USB Session" on page 67).
2. At the command prompt type **set switch mode=local**.
3. Press the **Enter** key.
4. Reboot the card for the changes to take effect. At the command prompt type **reboot**.

   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).
5. Press the **Enter** key to reboot the module.
6. At the command prompt type **show switch mode**.
7. Press the **Enter** key. This displays the device's management mode - local or remote - indicating where the device is managed:
   - **local** – device is managed through direct connection to the device.
   - **remote** – device is managed through the IONMM.

Note: The system can not show the switch mode on all card types.

3. Management Methods

General

The x222x / x32xx NIDs are managed either directly or through the IONMM. Whether the NID is managed directly or indirectly, management is accomplished through one of the following methods.

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

IONMM Managed NIDs

NIDS that are managed through the IONMM are either chassis resident (C32xx) or standalone modules (S32xx) that are connected as remotes to chassis resident modules. Communications between the IONMM and the NIDs is through the ION Chassis backplane. See the *IONMM User Guide* for details.

Managing Slide-In and Remote Modules Using CLI Commands

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

For example:

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

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

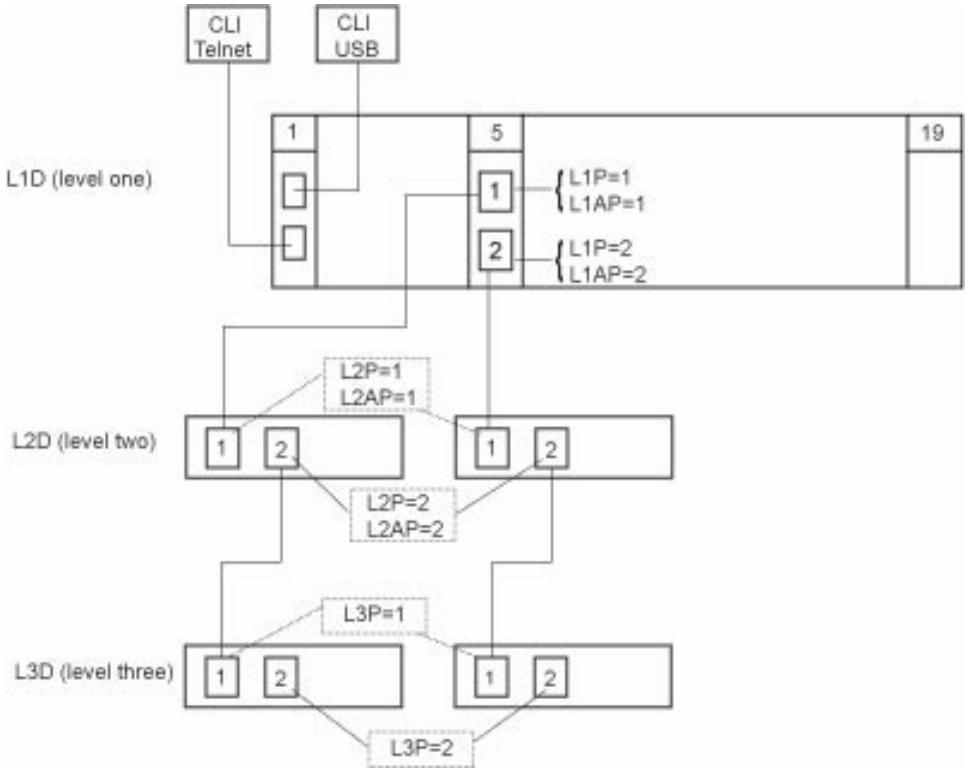


Figure 18: CLI Location Hierarchy

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

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

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

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

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

Example 1

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

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

The resulting command line prompt would be:

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

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

Example 2

In the CLI location hierarchy, to go to device L2D in the network topology shown in Figure 19, you would enter the following command from the base prompt.

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

The resulting command line prompt would be:

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

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

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

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Use the **go** command to change the operational location to the device/port to be managed. 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 Standalone card
3. Configure the NID using the appropriate commands. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
4. To return the location to the IONMM, type **home** and press **Enter**.

Example 3:

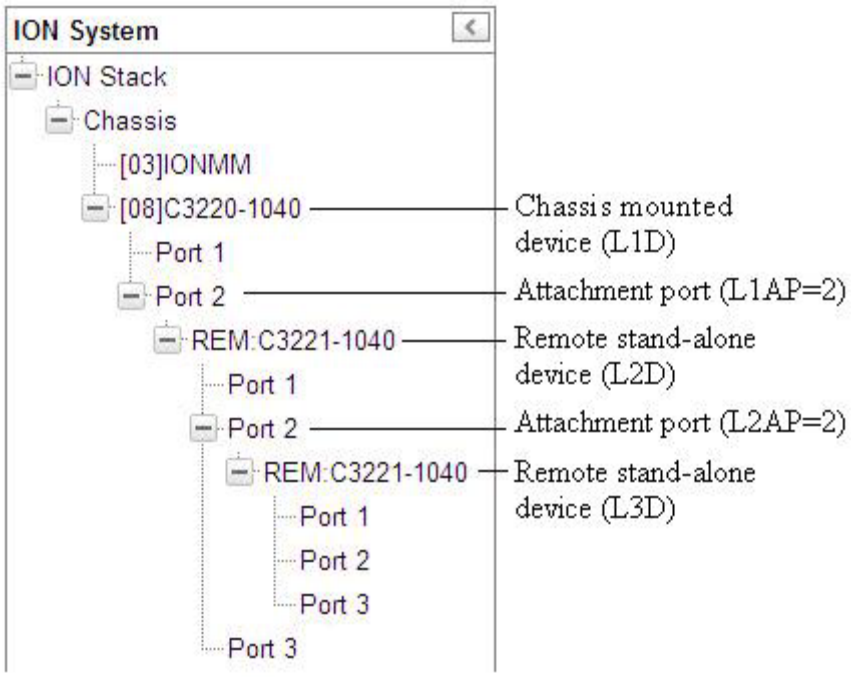
The CLI prompt (>) displays an editable name prefix based on the "System Name" field. You can add or modify the System Name via the CLI. For example if the name was "lab", the IONMM "System Name" is carried through to every prompt/card that you are logged into (e.g., lab C1|S3|L1D>, lab C1|S5|L1D>, lab C1|S8|L1D>, etc.).

If you don't enter a name in the "System Name" field, the CLI prompt default remains (e.g., C1|S3|L1D>, C1|S5|L1D>, C1|S8|L1D>, etc.).

So if you enter "Agent" in the System Name field, the CLI prompt would display as Agent C1|S3|L1D>, Agent C1|S5|L1D>, Agent C1|S8|L1D>, etc., but the module name in the Stack and other places in the ION Web interface would still show IONMM.

Managing Slide-In and Remote Modules via the Web Interface

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).



2. Click on the slide-in module or port to be managed.
3. The operations that can be performed depend on the type of slide-in module. Refer to the product documentation for the information. See the "Related Manuals" section on page 38.

Direct Managed NIDs

Direct management is for standalone NIDs (S32xx) that are not connected to a module that is managed through the ION Management Module. In direct management the network and/or USB cable is connected directly to the module to be managed.

Managing Standalone Modules Using CLI Commands

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

For example:

```
C1|S3|L1D>
```

or

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

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

```
go [c=<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 Standalone card

For example:

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

```
C0|S0|L1D>go l1p=1
```

The resulting command line prompt would be:

```
C0|S0|L1P1>
```

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

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

```
C0|S0|L1P1>go l1d
```

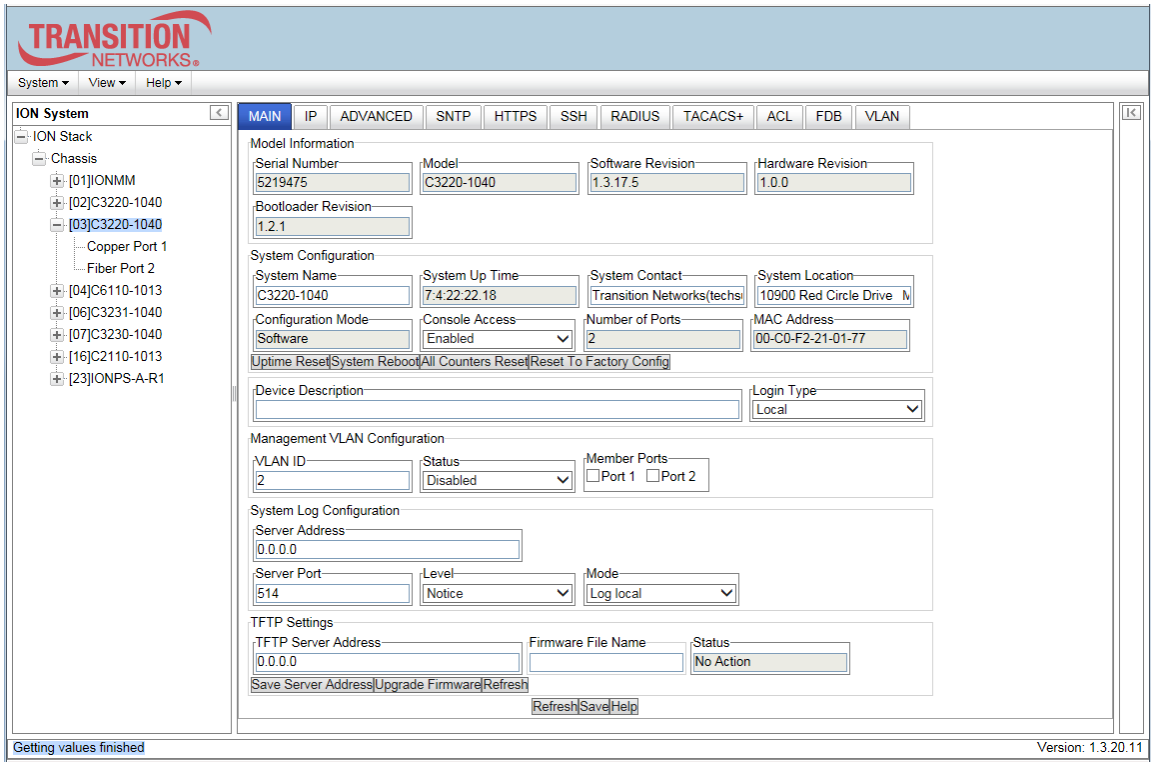
The resulting command line prompt would be:

```
C0|S0|L1D>
```

Managing a Standalone Module via the IONMM Web Interface

You can manage standalone modules from the ION web interface via the IONMM.

1. Access the NID via the Web interface (see "Starting the Web Interface" on page 45).
2. Click the plus sign **[+]** next to **ION Stack** to unfold the "ION Stack" node in the left tree view if not already done.
3. Click the plus sign **[+]** next to **Chassis** and click the plus sign [**+**] next to a module.
4. Click on the module or port to be managed (e.g., C3220-1040 in slot 03 shown below).

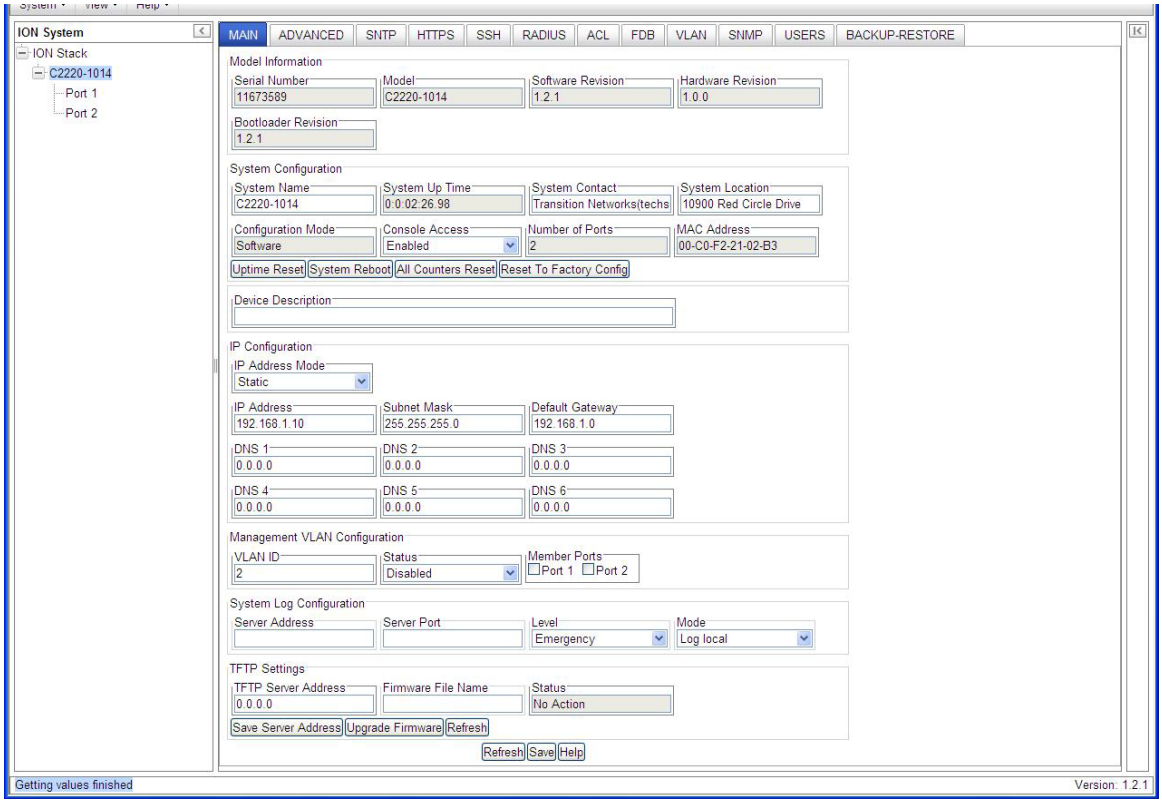


5. Select the various tabs to perform the applicable operations.

Managing a Standalone Module via the Web Interface

You can also manage standalone modules from the ION web interface without an IONMM.

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



4. Click on the module or port to be managed (e.g., C2220-1040 on the screen above).
5. Select the various tabs to perform the applicable operations.

You can perform the same functions as with the IONMM management, as well as the SNMP, Login USERS, and BACKUP/RESTORE functions.

Menu System Descriptions

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

Table 11: System-Level Menu Description

Dropdown / Tab	Description
ION System pane	**ION Stack** - consists of one standalone chassis. The Stack Members table lists the Stack's chassis and its type (e.g., ION219). **Chassis** - The Chassis View shows a summary view of one ION chassis. Model Information includes: * Serial Number - The serial number of the chassis itself. Individual NIDs also have their own serial numbers. * Model Name - The exact model name of this device. When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number. * Software Revision, Hardware Revision, and Bootloader Revision. * Chassis Members table - lists local physical components in slots 1 to 19. **Device** – provides tabs and sub-tabs for the IONMM and NIDs in the ION system. **Port** - provides tabs and sub-tabs for a selected NID port.
System dropdown	Sign out.
View dropdown	Refresh.
Help dropdown	Online Help, ION Product Home Page, About ION System Web Interface.
MAIN tab	Model Information, System Configuration, Device Description, IP Configuration, Management VLAN Configuration, SNMP Configuration, System Log Configuration, and TFTP Server Settings sections.
IP Tab	Sections: IPv4, IPv6, and DNS Configuration. Buttons: Refresh, Save Help.
ADVANCED tab	FDB Aging Time, MAC Address Learning, Link Pass Through (LPT), IEEE Priority Class, and IP Traffic Class sections.
SNTP tab	SNTP Configuration, Daylight Saving Time Configuration, and SNTP Servers sections.
HTTPS tab	HTTPS Status, HTTPS Port, Certificate Type, and Copy HTTPS Certification functions.

SSH tab	SSH Server Status, Version, SSH Auth Timeout, SSH Auth Retries, Host Public-Key Settings, and User Public-Key Settings.
RADIUS tab	RADIUS Client enable/disable and RADIUS Server(s) configuration.
TACACS+ Tab	Sections: TACACS+ Client and TACACS Server 1 - TACACS Server 6 sections. Buttons: Refresh, Save, Help.
ACL tab	Set ACL Status and Chain Policy, Add/View/Modify Rules, and Add/View/Modify Conditions for Rules. Set Priority, Policy and Trap Rate for Rules. Define Type, Source or Destination, Operation, and value for Conditions for Rule(s).
FDB tab	Add, Edit or Delete MACs (MAC Address / Port / Priority and Entry Type). Flush FDBs operations.
VLAN tab	Add, Edit or Delete VLANs and related parameters. Flush VLANs operations (Flush All / Flush All Dynamic).
SNMP tab	Sub-tabs: General, Users, Groups, Views, Trap Hosts, Remote Users. Fields: Community String, Access Mode, SNMP V3 Engine ID. Buttons: Add, Delete, Refresh, Save, Help buttons.
USERS tab	Fields: User Name, Password, Confirm Password, Level fields. Buttons: Refresh, Add, Edit, Delete, Help buttons.
BACKUP / RESTORE tab*	Sub-tabs: Backup and Restore. TFTP Server Address and Status fields. *Backup* - lets you select modules from a list to Back Up (you must download config files after backing up is done). Buttons: Download, Refresh, Back Up, Help. *Restore* - lets you select modules to Restore (you must upload config files before restoring is started). Buttons: Upload, Refresh, Restore, Help.

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

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

Table 12: Port-Level Menu Description

Tab	Description
MAIN tab	Sections: Circuit ID, Port Configuration, Auto Negotiation Settings, Control Frames Management / Capabilities Advertised, Port Forward Management, L2CP Disposition, TN Topology Discovery Protocol TX, and Virtual Cable Test (VCT). Buttons: *Virtual Cable Test, Refresh, Save,* and *Help.*
ADVANCED tab	Sections: Bandwidth Allocation, MAC Security, VLAN Forwarding Rules, Priority Forwarding Rules, VLAN Tag Management, User Priority, and Egress Queue Mode.
COUNTERS tab	Sections: RMON Counters, RX Counter, TX Counter, Dot3 Statistics, and MAC Control Frames.
LOAM tab	Sections: LOAM Configuration, LOAM Peer Information, Loopback Management (Start / Stop). Sub-tabs: Main, Counters (Reset LOAM Counters), Event Configuration (Dying Gasp / Critical Events), and Event Log.
DMI tab (Port 2 only)	Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length. The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, supported media lengths, and Vendor Specific Information. See “DMI (Diagnostic Maintenance Interface) Parameters” on page 248 for more information. **Note**: not all NID models / SFPs 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 that does not support DMI, the message “*The DMI feature is not supported on current port*.”

Reboot, Reset, and Power Off Function Notes

Certain functions such as a System Reboot, Reset to Factory Configuration, Reset Power to a Slot, and Power Off a Slot) cause the system to delete certain stored files. ***Caution***: In some circumstances, these stored files are lost unless you first perform a System Backup. See the "Backup and Restore Operations" section starting on page 199 for information on how to save the stored files from deletion.

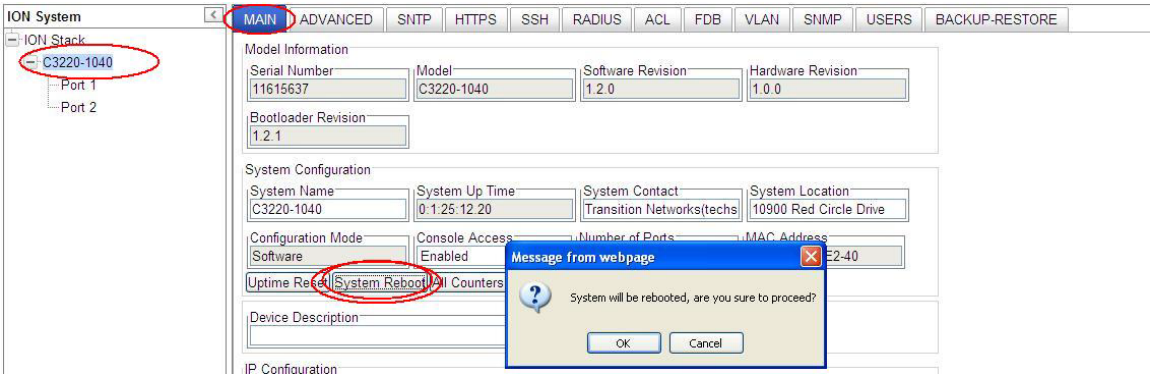
For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- Table 15: Back Up and Restore File Content and Location on page 209
- Table 16: File Status after a Reset to Factory Defaults on page 214
- Table 17: File Content and Location after a System Reboot on page 218
- Table 18: File Content and Location after a Firmware Upgrade on page 233

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

System Reboot

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



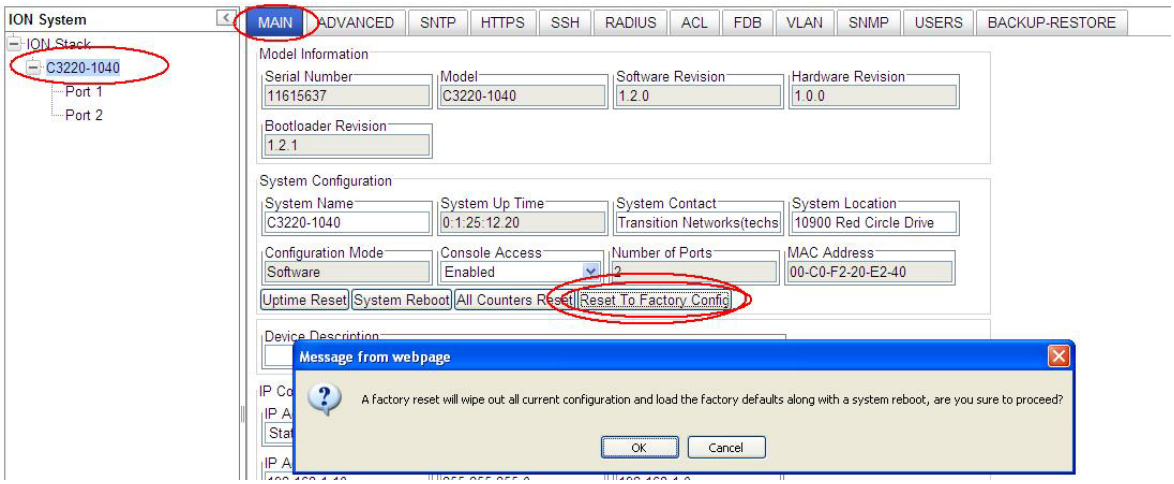
Press the **Cancel** button if you are not sure you want a system reboot to occur.
Press the **OK** button to clear the webpage message and begin the reboot process.

The message "*Loading, please wait...* displays.

Note that a System Reboot can take several minutes.

Reset To Factory Config

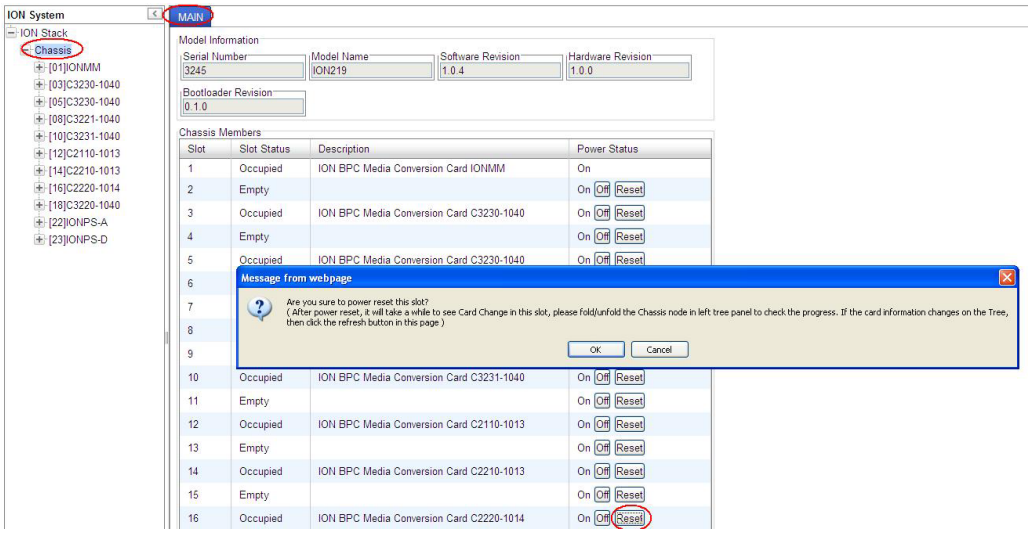
Clicking the **Reset To Factory Config** button resets the entire system configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the factory default settings. The message "*A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*" displays.



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

Reset Power to a Slot

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

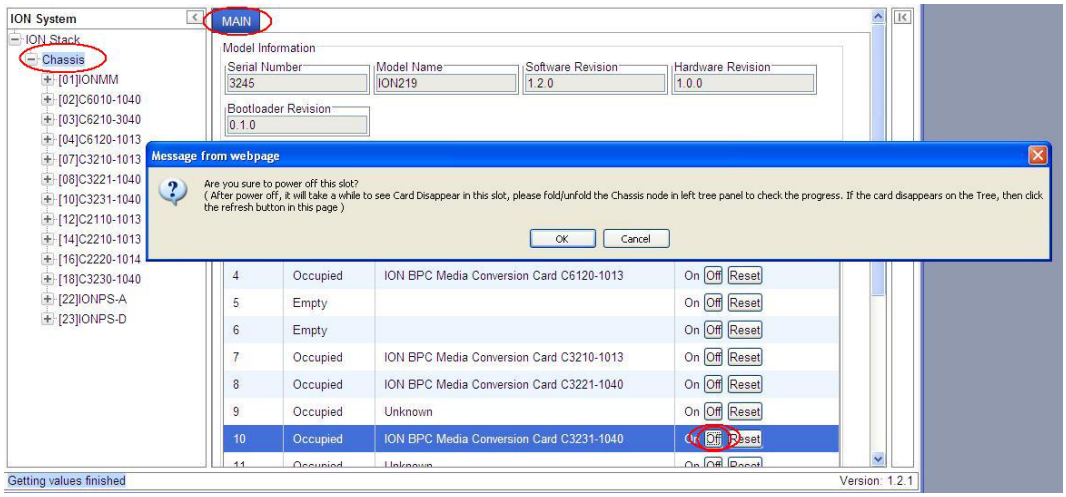


After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page.

If you are not sure that you want to reset this chassis, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.

Power Off a Slot

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



If you are <u>not</u> sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.

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

4. Configuration

General

After the NID has been installed and access has been established, the device and its ports must be configured to operate within your network. The configuration establishes operating characteristics of the device and the ports associated with the NID.

Configurations can be done either by entering CLI commands (USB / Telnet) or through a Web interface. For complete descriptions of all CLI commands, see the *ION System CLI Reference Manual, 33473*.

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

- IP addressing / Device Description / Circuit ID / System setup
- Features
  - Ethernet Interface *(AutoCross,* Auto negotiation, Bandwidth allocation, Speed, Duplex mode)
  - Ethernet LOAM (Link level OAM)
  - Fault detection
  - Flow control (pause frames/back pressure)
  - Forwarding
  - IP/IEEE priority remapping
  - Selective and transparent link pass through
  - Simple network management protocol (SNMP)
  - Simple network time protocol (SNTP)
  - Layer 2 Control Protocol (L2CP)
  - MAC Learning
  - System Logging (Syslog)
  - TNDP (Lantronix Discovery Protocol)
- Security
  - Access control list (ACL)
  - Hypertext transfer protocol secure (HTTPS)
  - Media access control (MAC) filtering
  - Remote authentication dial in user service (RADIUS)
  - TACACS+
  - Secure shell (SSH)
  - Management VLAN
  - Login User administration

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.

Setting the IPv4 Addressing

The IP configuration allows the NID 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, default gateway address and subnet mask of the NID. Additionally, Domain Name System (DNS) servers can be set up as part of the IP configuration.

The IP address assigned to the NID can either be a static (permanent) address that you enter, or a dynamic (temporary) address assigned by a DHCP server, or the IP address can be assigned by a BootP server.

- The BootP (Bootstrap Protocol) network protocol used by a network client to obtain an IP address from a configuration server. 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 UDP port number 67 for the server and UDP port number 68 for the BootP client.
- A DHCP server can assign a dynamic (temporary) IP address. 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.
- A static IP address is one that is permanently assigned to the NID. The static IP address, subnet mask and default gateway address can be configured in the NID using either the CLI or Web method.

Note: When changing the IP address, you must reenter the subnet mask and gateway even if those values have not changed; otherwise, you will get the error message: *"% Unknown command."*

IMPORTANT

For standalone NIDs that will not be controlled by the ION Management Module, it is recommended that you initially set up the IP configuration through the serial interface (USB connection). See IP Static Config – CLI Method below.

Otherwise, in order to communicate with the NID 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 NID (see "Appendix B: Factory Defaults" on page 534). Make note of the original settings for the PC as you will need to reset them after setting the IP configuration for the NID.

The factory default settings are:

IP Address = 192.168.0.10
Subnet Mask =255.255.255.0
Default Gateway addr = 192.168.1.0
IP Type = IPv4
IP Addr = 192.168.0.10
Subnet–mask = 255.255.255.0
IP Address mode = Static

IPv4 Static Config – CLI Method

Note: Once the IP address is changed in stand-alone mode, communication will be lost.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Define the IP address and subnet mask for the NID. Type:

   ```
   set ip type=ipv4 addr=<xx> subnet-mask=<yy>
   ```

   where:

   xx = IP address of the NID (e.g., 192.168.1.29 in the example)

   yy = subnet mask (e.g., 255.255.255.1 in the example)
3. Press **Enter**.
4. Set the IP addressing mode. Type **set ip address mode**=<bootp|dhcp|static> and press **Enter**.
5. Define the default gateway address. Type:

   ```
   set gateway type=ipv4 addr=<xx>
   ```

   where:

   xx = default gateway address (e.g., 192.168.1.2 in the example)
6. Press **Enter**.
7. Verify the configuration has been set. Type: **show ip config** and press **Enter**. The current configuration displays. For example:

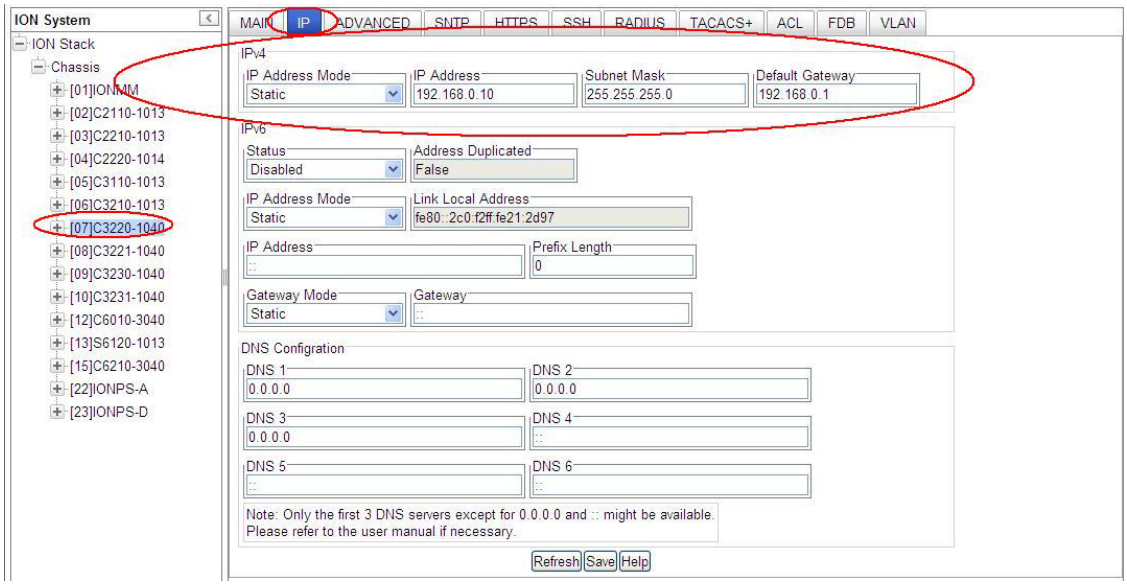
```
Agent III C1|S9|L1D>set ip type=ipv4 addr=192.168.0.10
Agent III C1|S9|L1D>set ip address mode=static
Agent III C1|S9|L1D>set gateway type=ipv4 addr=192.168.1.0
Agent III C1|S9|L1D>show ip- config
IPv4 management configuration:
------------------------------------------------------------------------
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:fe21:177
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|S9|L1D>
```

IPv4 Address Config – Web Method

Note: Once the IP address is changed in Remote mode, communication will be lost.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **IP** tab.
3. Locate the **IPv4** section.



4. At the **IP Address Mode** dropdown, select **DHCP**, **Static**, or **BootP**. The default is **Static** addressing for versions through 1.2. The default is **DHCP** addressing for versions 1.3 and above.
5. Enter the **IP Address**, **Subnet Mask** and **Default Gateway** address into the appropriate fields.
6. Scroll down and click **Save** when done.

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 can not 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 RDNSSes 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.

Assigning a Dynamic IP Address via DHCP

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 Configuration backup does not back up the leased IP address; only the DHCP state is backed up.
- A DHCP server must be on the network, configured, and accessible for dynamic IP address assignment via DHCP.
- 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 the 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 x222x / x32xx via either the CLI or Web method.

IP Dynamic Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable DHCP. Type:

```
set dhcp state=enable
```

3. Press **Enter**.

Defining 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. They may also have names assigned. 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, translating names to IP addresses.

One or more DNS servers can be defined using either the CLI or Web method.

DNS Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command prompt type: **set dns svr=**<xx> **type=**<yy> **addr=**<zz> where:

   xx = the number (1–6) of the DNS server being defined. Up to six DNS servers can be defined.
   yy = the type of addressing; select **dns** (domain name address format).
   zz = the IP address of the DNS server.
3. Press **Enter**.
4. Repeat steps 2 and 3 for each DNS server to be defined.
5. Verify the DNS server(s) defined. Type **show ip config** and press **Enter**. For example:

```
Agent III C1|S7|L1D>set dns svr 1 type ipv4 addr 192.168.1.20
Note: only the first three valid DNS server can be available, please refer to user menu
    for the details
Agent III C1|S7|L1D>set dns svr 2 type ipv4 addr 192.168.1.30
Note: only the first three valid DNS server can be available, please refer to user menu
    for the details
Agent III C1|S7|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:fe21:2d97
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        192.168.1.20
DNS server2    ipv4        192.168.1.30
DNS server3    ipv4        0.0.0.0
DNS server4    ipv6        ::
```

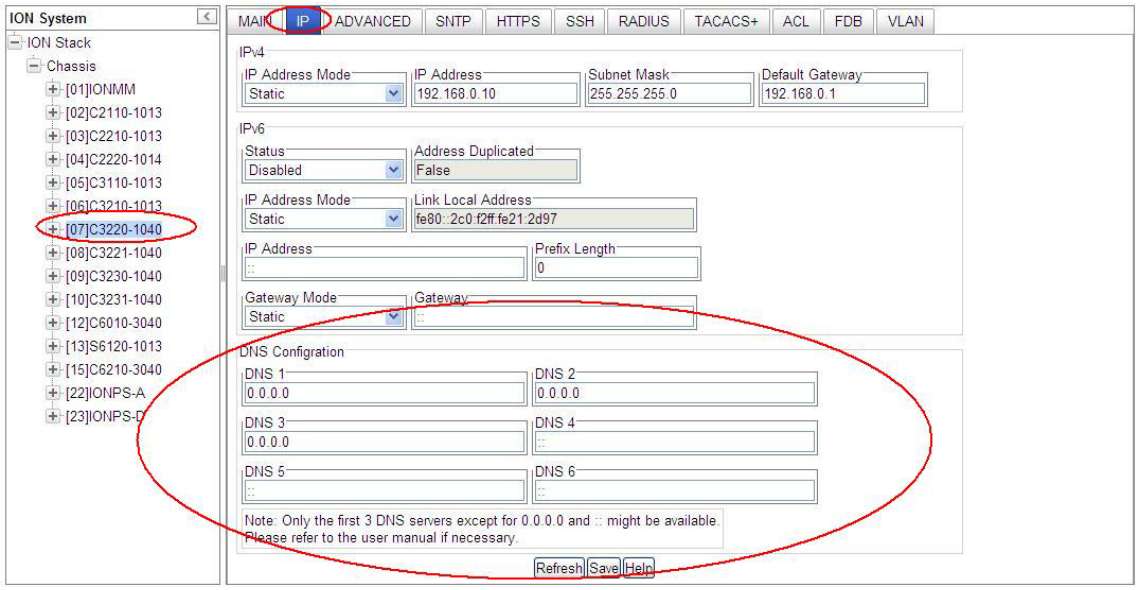
```
DNS server5    ipv6        ::
DNS server6    ipv6        ::
Agent III C1|S7|L1D>
```

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)' on page 85.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **IP** tab.
3. Locate the **DNS Configuration** section.

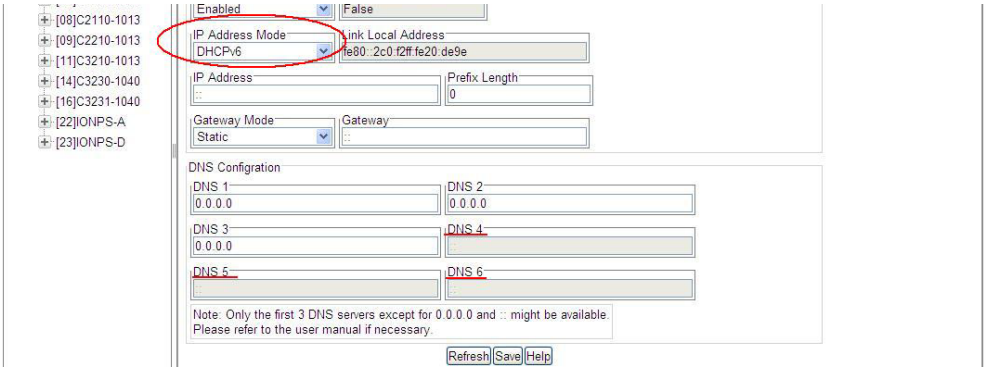


Note: Only the first 3 DNS servers except for 0.0.0.0 and :: might be available.

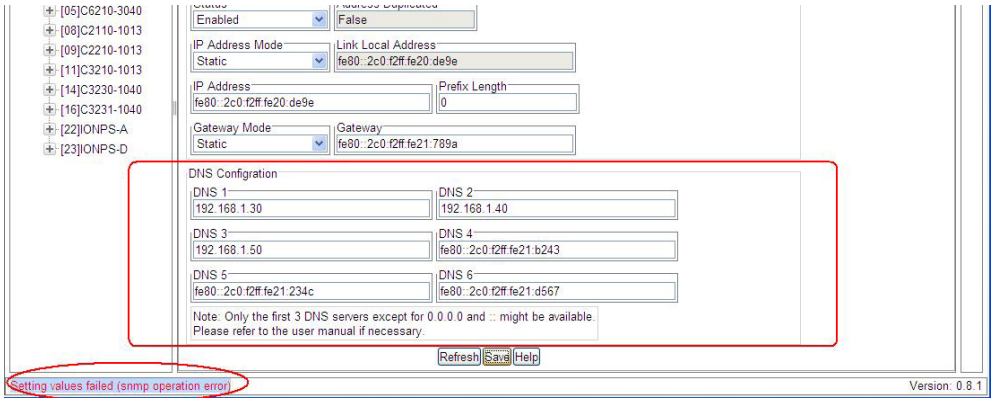
4. In the DNS 1- DNS 3 fields, enter a valid IPv4 IP address (not applicable if DHCP is selected for IPv4 Address Mode).
5. In the DNS 4- DNS 6 fields, enter a valid IPv6 IP address (not applicable if DHCP v6 is selected for IPv6 Address Mode).
6. Scroll down and click **Save** when done.

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

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



The figure below shows an invalid configuration:



See the “DNS ‘3 vs. 3’ Rule (‘Up to 3’ Rule)” above for more information.

IPv6 Description

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

- **Expanded Addressing Capabilities**: IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. A new type of address called an "anycast address" is defined, which is used to send a packet to any one of a group of nodes.
- **Header Format Simplification**: Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.
- **Improved Support for Extensions and Options**: Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- **Flow Labeling Capability**: A new capability is added to enable the labeling of packets belonging to 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} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456
Payload	IPv4 limits packets to 64 KB of payload	optional support for “jumbogram” packets - up to 4 GB
TTL / Hop limit	Time-to-Live field	Hop-Limit field
Multicast	Optional, but usually implemented	Part of the base specification in IPv6
QoS support	No standard support	IPv6 has standardized support for QoS

IPv6 Features

The ION system provides the following IPv6 features.

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

These features are described in the following sections.

ION IPv6 Function Descriptions

IPv6 Dual Protocol Stacks and Multiple Server Support

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

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

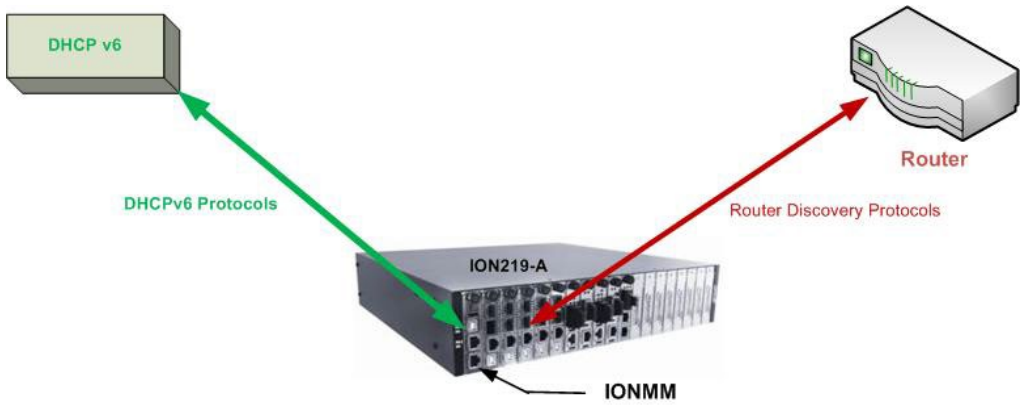


Figure x. Multiple Routers - One DHCPv6 server and One Router

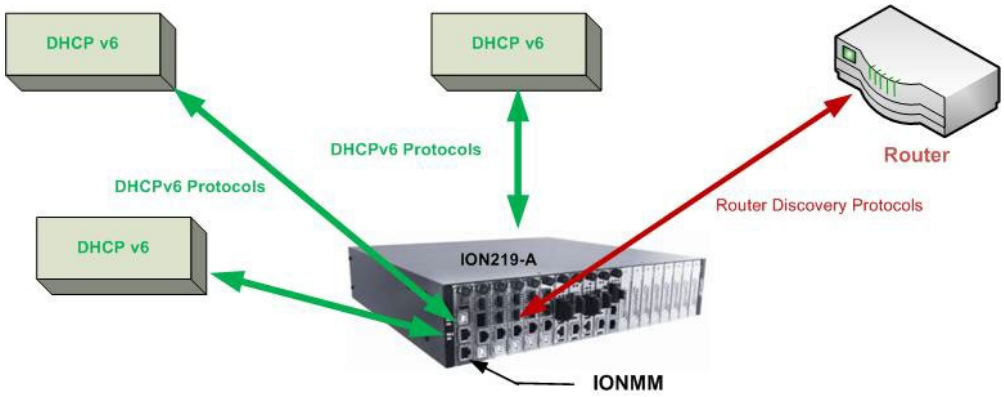


Figure x. Multiple DHCPv6 servers and One Router

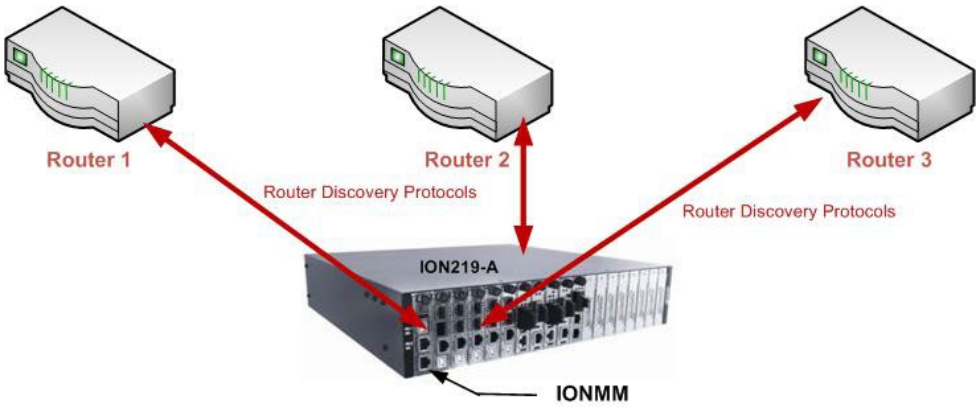


Figure x. Multiple Routers

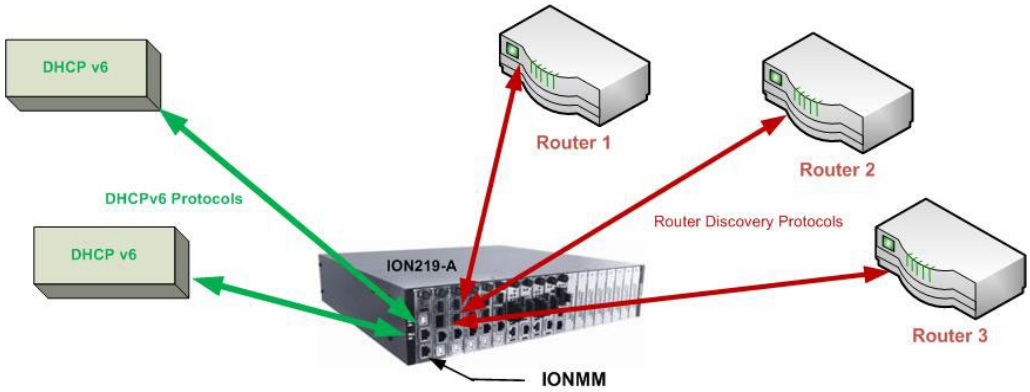


Figure x. Multiple DHCPv6 Servers and Routers

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

IPv6 Unicast Addresses

ION IPv6 Unicast Address support includes:

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

Note: ION supports one Link-local IPv6 address which is read-only and one Global Address or Unique Local address. The Link-local address is configured on ION device using the link-local prefix FE80:: /10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. The Global Address or Unique Local address can be configured via the static method, DHCPv6, and stateless auto-configuration.
Other IP v6 addresses can be set in ION system by Web/CLI/FP, but only to test in certain situations.
ION does not allow Loopback [::1/128] in any address field user can input. Unspecified address [::/128] is used for user to clear current address.)

IPv6 Multicast Addresses

ION IPv6 multicast support includes:

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

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

ICMP v6 (Internet Control Message Protocol for IPv6)

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

IPv6 Neighbor Discovery Protocol

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

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

The Neighbor Discovery protocol uses the following messages:

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

IPv6 DAD (Duplicate Address Detection)

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

IPv6 Auto Configuration per IETF RFC 2462

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

IPv6 supports the following types of auto-configuration:

- Stateless auto-configuration
- Stateful auto-configuration

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

IPv6 addresses are leased to an interface for a fixed (possibly infinite) length of time. Each address has an associated lifetime that indicates how long the address is bound to an interface. When a lifetime expires, the binding (and address) become invalid and the address may be reassigned to another interface elsewhere 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 you switch IPv6 address mode from Stateless to static, this configuration will be set to default:
   a. IPv6 address (::)
   b. IPv6 prefix (0)
3. When you 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 can not be executed successfully:
    a. Add vlan-db.
    b. Add fwddb

    After adding a VLAN or FWDDB by script, add a 3 second sleep in the script before adding another VLAN or FWDDB.
9. The SOAM MD name can not 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.

The changes incurred by IPv6 are explained in the following sub-sections.

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 can not 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” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
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:           192.168.1.0
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>
```

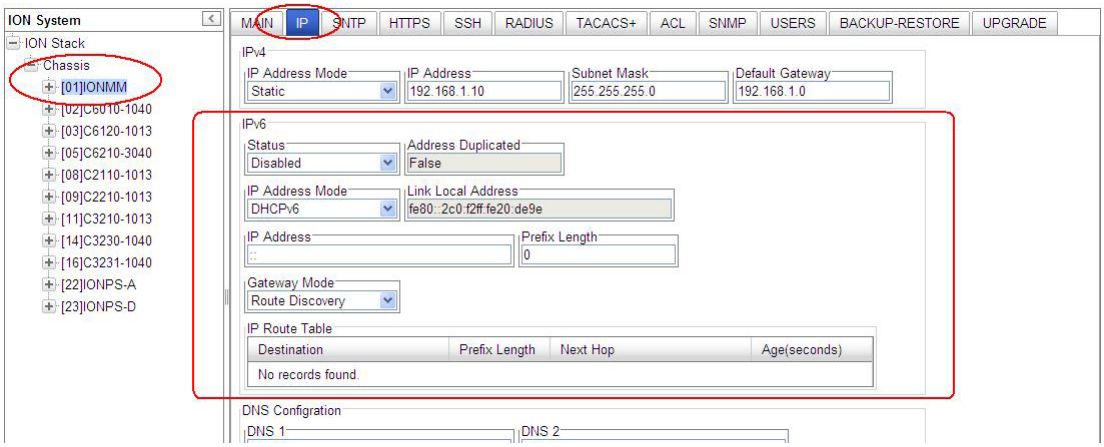
Note: the command "set dhcp state" is replaced by "set ip address mode" after ION v 1.2.0.

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” on page 45).
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:

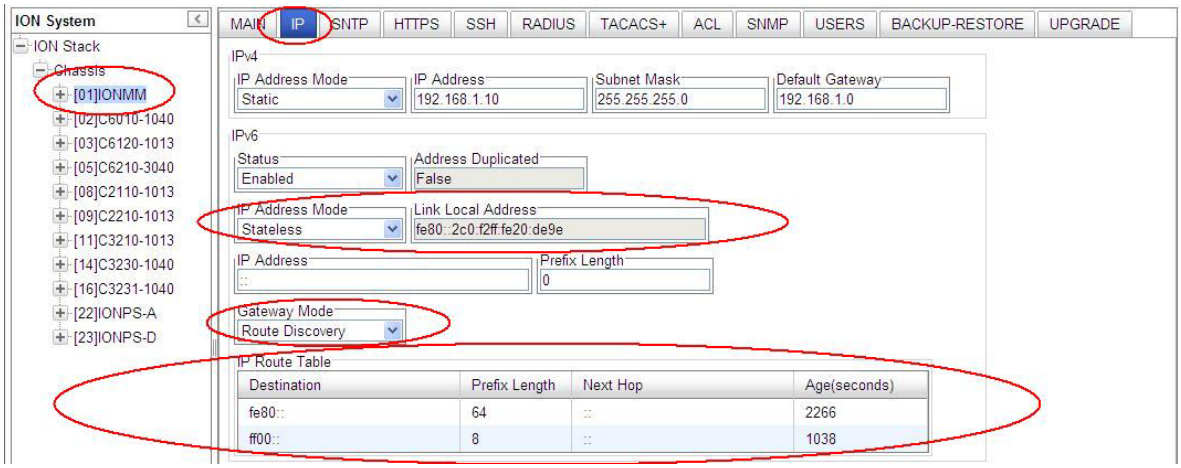
   Static: selects static IPv6 addressing.

   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:

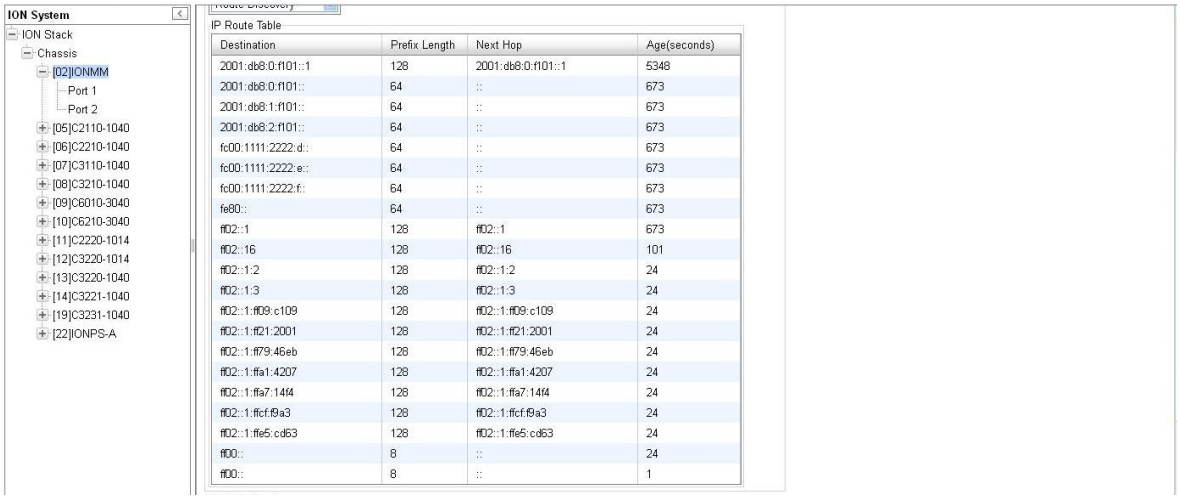


The screen above shows an **IONMM** > **IP** tab with **IP Addr Mode** = **Stateless** and **Gateway Mode** = **Route Discovery**. The IP Route table holds a maximum of 16 entries.

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 enroute. 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.

System Configuration

The system configuration defines:

- a name for the NID and contact and location information, and
- whether the 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" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command prompt type **set system contact=**CONTACT, where CONTACT is the new contact, and press **Enter**.
3. Type **set system location=LOC**, where LOC is the new location description, and press **Enter**.
4. Type **set system name**=NAME, where NAME is the new system name, and press **Enter**.

   For example:

```
C1|S5|L1D>set system contact=support
C1|S5|L1D>set system location=headquarters
C1|S5|L1D>set system name=C2220-1014
```

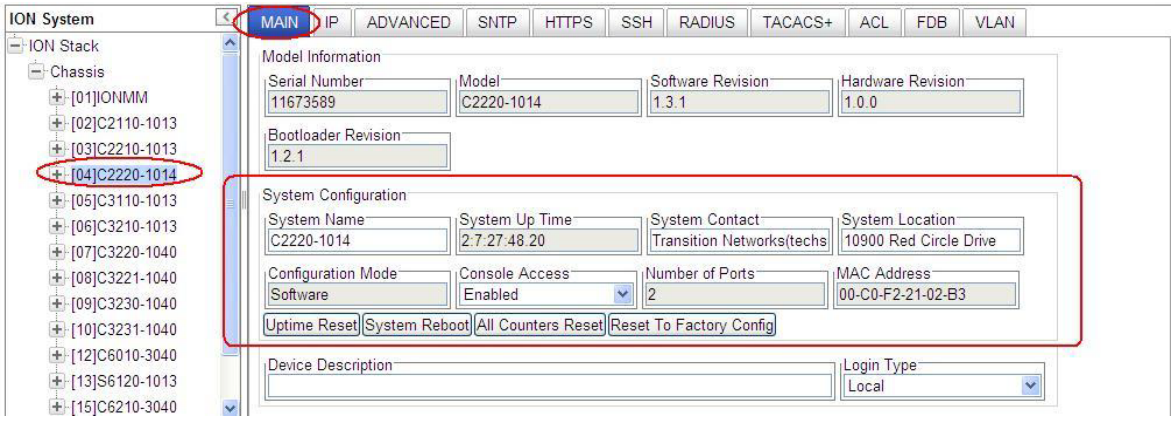
5. Verify the new system definition. Type **show system information** and press **Enter**. For example:

```
C1|S5|L1D>show system information
system descr:              The C2220-1014 of the Transition networks
                       ION (Chassis Generation III) platform products
system objectID:           1.3.6.1.4.1.868.2.5.1802661751
system uptime:             10 days, 21:03:31
system contact:            support
system name:               C2220-1014
system location:           headquarters
C1|S16|L1D>
```

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

System Configuration – Web Method

1. Access the x222x/x32xx via the Web interface (see "Starting the Web Interface" on page 45).
2. At the **MAIN** tab, locate the **System Configuration** section.



3. In the **System Name** field, enter the name and for the x222x/x32xx. The name can be alphabetic, numeric or a combination. Do not enter spaces between System Name characters.
4. 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.
5. 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.
6. 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).
7. Verify the value displayed in the **Configuration Mode** field. The NID has a jumper that disables software management of the x222x/x32xx. When the **Configuration Mode** field displays **Hardware**, the NID takes some of its configuration from DIP switches or jumpers on the x222x/x32xx. In **Software** mode, all configuration parameters are controlled by management. Refer to the "Jumper Settings" section on page 450 for details on **Hardware** mode configuration.
8. Scroll to the bottom and click **Save**.

Device Description Configuration

The x222x/x32xx supports a Device Description at the device level and a Circuit ID at the port level.

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

The Device Description can be configured in the x222x/x32xx using either the CLI or Web method.

Device Description– CLI Method

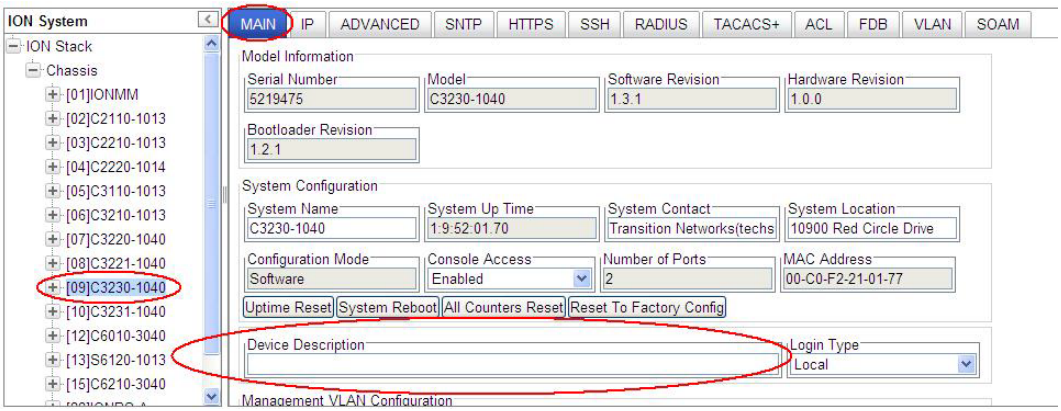
1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the device's command prompt type: **set device description=**<xx> where:

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

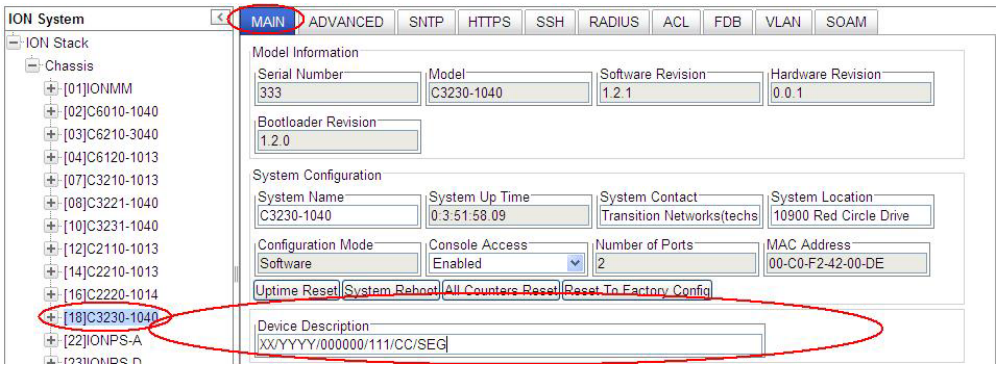
```
Agent III C1|S9|L1P1>set device description  zzzzzzz
Error: this command should be executed on a device!
Agent III C1|S9|L1P1>go l1d
Agent III C1|S9|L1D>set device description  zzzzzzz
Agent III C1|S9|L1D>show device description
Device description: zzzzzzz
Agent III C1|S9|L1D>
```

Device Description Config – Web Method

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. At the x222x/x32xx **MAIN** tab, locate the **Device Description** section.



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



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

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

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

Circuit ID Configuration

The x222x/x32xx supports a Device Description at the device level and a Circuit ID at the port level.

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

The Circuit ID can be configured in the x222x/x32xx using either the CLI or Web method.

Circuit ID Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the device's command prompt type: **set circuit-ID=**<xx> where:

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

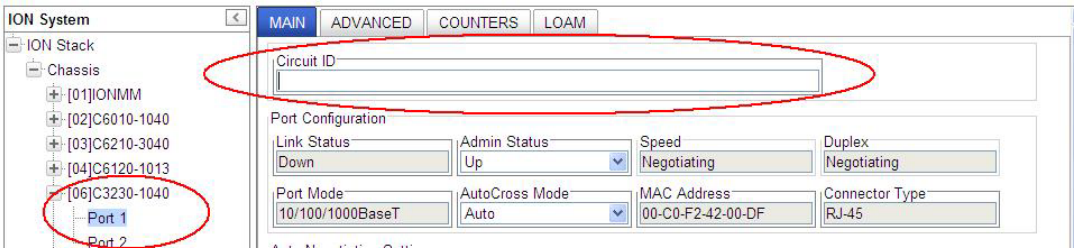
```
C1|S16|L1D>set circuit XX/YYYY/000000/111/CC/SEG
C1|S16|L1D>show circuit-ID
Circuit-ID:         XX/YYYY/000000/111/CC/SEG
C1|S16|L1D>
```

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

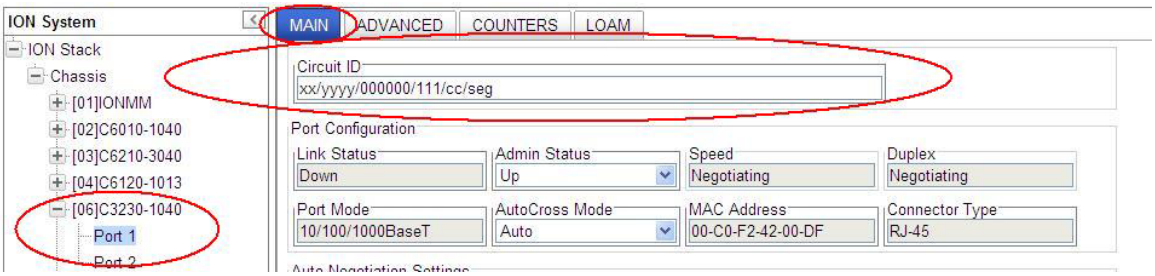
```
C1|S16|L1D>go l1p=1
C1|S16|L1P1>set circuit-ID=xx/yyyy/000000/111/cc/seg
C1|S16|L1P1>show circuit-ID
Circuit-ID:         xx/yyyy/000000/111/cc/seg
C1|S16|L1P1>

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

Circuit ID Config – Web Method

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the appropriate port and locate the **Circuit ID** field.



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



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

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

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

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 on page 99.

Login Type Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
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.

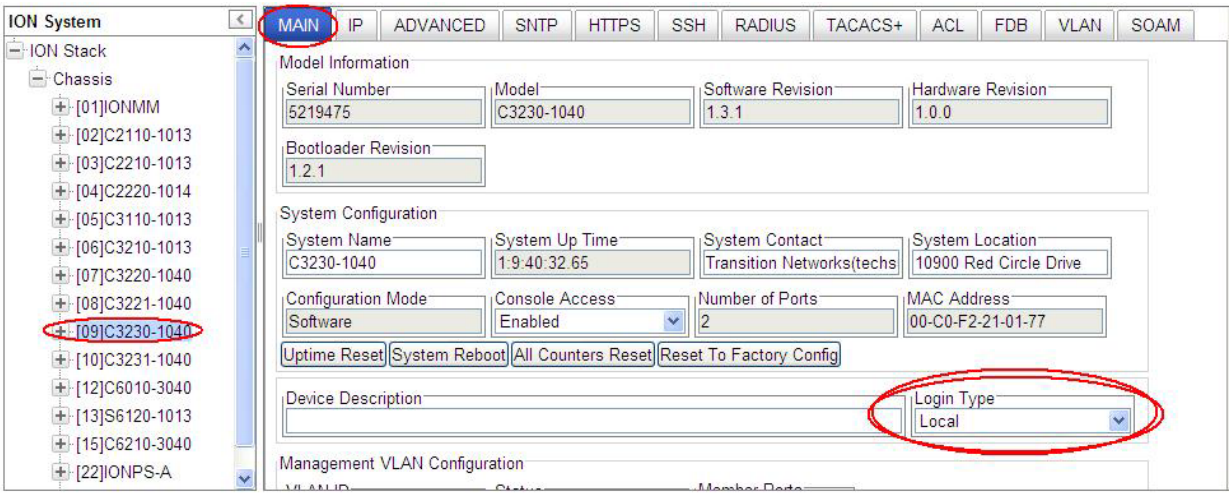
   tacplusradiuslocal = the ION software will validate the TACACS+ login, then the RADIUS login, and then the local login.
4. Verify the TACACS+ and/or RADIUS configuration. For example:

```
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>
```

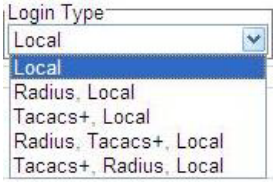
Login Type Config – Web Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).



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 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.

Configuring AutoCross

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

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

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

On x222x / x32xx devices the *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection, making the distinction between a straight through cable and a crossover cable unimportant.

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

AutoCross Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the device port's command line, type: **set ether autocross**=xx where:

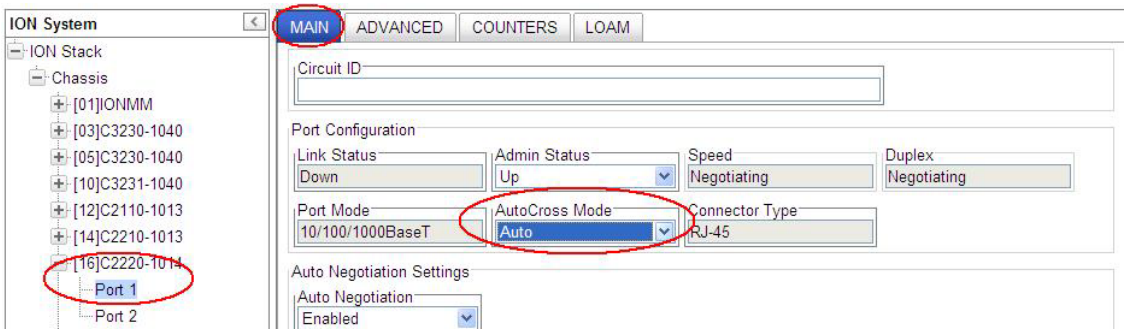
   xx = cable type. Valid choices are:

   - **Auto** – hardware will automatically correct errors in cable selection.
   - **MDI** – transmit pair on one end of the cable is connected to the receive pair on the other end.
   - **MDIX** – cross over cable is used.

3. Press **Enter**.

AutoCross Config – Web Method

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



4. In the **AutoCross Mode** field, select the mode to be used.
   - **Auto** – ION System hardware will automatically correct errors in cable selection (default mode - recommended).
   - **MDI** – the transmit pair on one end of the cable is connected to the receive pair on the other end.
   - **MDIX** – a cross over cable is used.
5. Click **Save** when done.

Configuring Auto Negotiation

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

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

- Speed
- Duplex
- Pause capability (whether Pause frames are supported)

When one device supports auto negotiation and the other does not, the device that has auto negotiation abilities can determine the speed of the other device, and then select the same speed for itself. However, this procedure can not determine the duplex setting of the other device, so half-duplex is always assumed. If one device is using full duplex while the other one is using half-duplex, a duplex mismatch occurs. The usual effect of this mismatch is that the connection works but at a very low speed.

Disabling the auto negotiate feature allows you to force the connection to the desired speed and duplex mode of operation as long as both devices can support the operation.

Note: The auto negotiate feature is always enabled for gigabit devices/ports. The pause default value for a copper port is “disabled”.

10/100/1000BaseT Port – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the command line, type: **set ether autoneg state**=xx where:

   xx = **enable** or **disable**
3. Press **Enter**.

4. If auto negotiation is enabled go to step 5.
   If auto negotiation is disabled go to step 6.
5. Set the advertised speed/duplex capabilities; type: **set ether adv-cap** where:

   xx = advertised speed capability; valid choices are:

   - **10TFD** (TP port 10 Mbps full duplex)
   - **10THD** (TP port 10 Mbps half-duplex)
   - **100TFD** (TP port 100 Mbps full duplex)
   - **100THD** (TP port 100 Mbps half-duplex)
   - **1000TFD** (TP port 1000 Mbps full duplex)
   - **1000THD** (TP port 1000 Mbps half-duplex)
   - **1000XFD** (fiber port 1000 Mbps full duplex)
   - **1000XHD** (fiber port 1000 Mbps half-duplex)

   To specify more than one capability use a plus sign (+) between entries (e.g., adv-cap=10TFD+100TFDl+1000THD).
6. Press **Enter**.
7. Set the advertised pause frame capability; type: **set ether pause=xx** where:

   xx = advertised pause capability; valid choices are:

   - **nopause** (the port will advertise that is has no pause capabilities)
   - **apause** (asymmetric; the port will advertise that it can only transmit pause frames)
   - **bpause** (asym/sym; the port will advertise that it supports both asymmetric and symmetric capabilities (not supported on all models)
   - **pause** (the port will advertise it has pause capability)
   - **spause** (symmetric; the port will advertise that it can transmit and receive pause frames) (not supported on all models)
8. Press **Enter**.
9. Set the speed of this port; type **set ether speed=xx** where:

   xx = speed setting; valid choices are:

   - **10M**
   - **100M**
   - **1000M**
10. Press **Enter**.
11. Set the duplex of this port; type **set ether duplex=xx** where:

    xx = duplex setting; valid choices are:

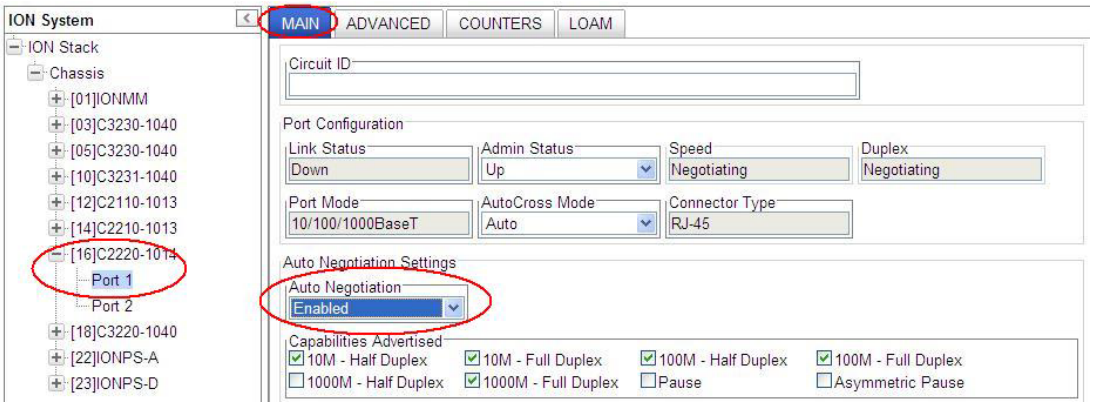
    - **full**
    - **half**

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

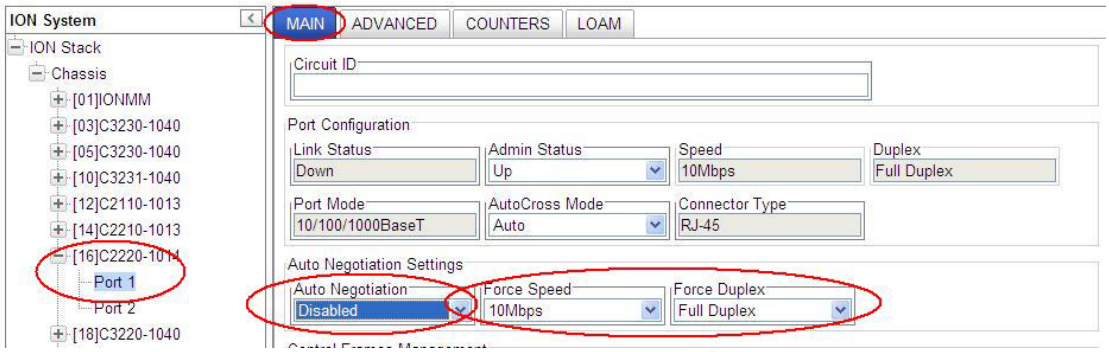
```
Agent III C1|S7|L1P1>show ether config
Port-11040
TP port:
------------------------------------------------------------------------
Link operation status:        down
Admin status:                 up
Port mode:                    RJ-45
PHY operation mode:           phy10-100-1000BaseT
Speed:                        Negotiating
Duplex:                       Negotiating
Autocross:                    auto
PHY mode change cap:          false

AutoNeg admin state:          enable
Advertisement:
Capability:                   10THD+10TFD+100THD+100TFD+1000TFD
Pause:                        nopause
Agent III C1|S7|L1P1>
```

10/100/1000BaseT Port – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the appropriate port. Select the port's **MAIN** tab if not already displayed.
3. Locate the **Auto Negotiation Settings** section.



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



7. Click **Save**.

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

Disabling the auto negotiate feature lets you force the connection to the desired speed and duplex mode of operation as long as both devices can support the operation.

Note: The Auto Negotiate feature is always enabled for gigabit devices/ports.

A port's Ethernet port speed and Duplex mode can be configured in the x222x / x32xx using either the CLI or Web method. **Note** that 1000M / Half duplex is not a valid selection.

Set Ethernet Port Speed / Duplex Mode – CLI Method

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

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

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command line, type **set ether autoneg state=disable** and press **Enter**.
3. Set the speed of this port; type **set ether speed=xx** where:

   xx = speed setting; valid choices are:

   - **10M**
   - **100M**
   - **1000M**
4. Press **Enter**.
5. Set the Duplex mode for this port; type **set ether duplex=xx** where:

   xx = duplex setting; valid choices are:

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

```
Agent III C1|S7|L1P1>show ether config
Port-11040
TP port:
------------------------------------------------------------------------
Link operation status:        down
Admin status:                 up
Port mode:                    RJ-45
PHY operation mode:           phy10-100-1000BaseT
Speed:                        Negotiating
Duplex:                       Negotiating
Autocross:                    auto
PHY mode change cap:          false
```

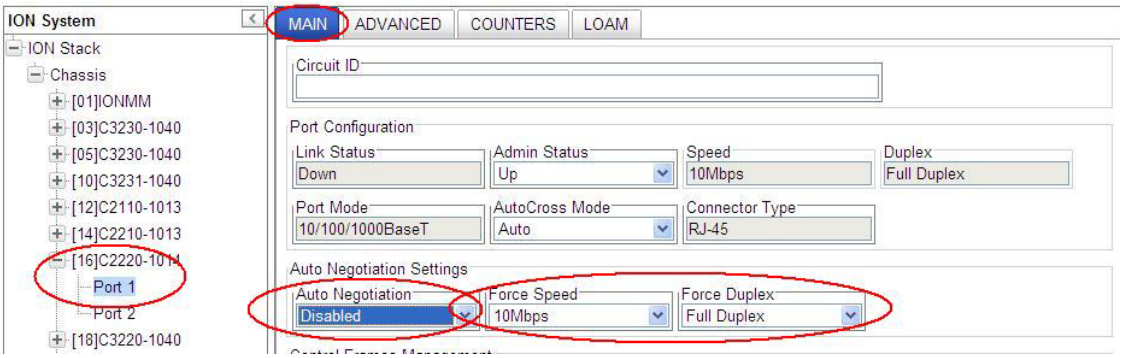
```
AutoNeg admin state:          enable
Advertisement:
Capability:                   10THD+10TFD+100THD+100TFD+1000TFD
Pause:                        nopause
Agent III C1|S7|L1P1>go l1p=2
Agent III C1|S7|L1P2>show ether config
Port-21040
FIBER port:
------------------------------------------------------------------------------
Link operation status:        down
Admin status:                 up
Port mode:                    SFP Slot
PHY operation mode:           phy1000BaseX
Speed:                        Negotiating
Duplex:                       Negotiating
PHY mode change cap:          true

AutoNeg admin state:          enable
Advertisement:
Capability:                   1000XFD
Pause:                        nopause
Agent III C1|S7|L1P2>
```

Set Ethernet Port Speed / Duplex Mode – Web Method

Use this procedure to define the transmission speed and Duplex mode to be used on the Ethernet port. The defaults are 10 Mbps and Full Duplex. Note that 1000M / Half duplex is not a valid selection.

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

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



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

Set Port Admin Mode (Ethernet PHY Mode)

Use this procedure to define the port's admin mode as 1000BaseX, 1000BaseFX, or SGMII. This is used to set the Ethernet PHY mode of this interface. The default is 1000BaseX.

The C3220-1040 and C3221-1040 NIDs support SGMII with 10/100/1000BASE-T copper SFPs.
The C3221-1040 NID provides 10/100/1000BASE-T (RJ-45) [100 m] to two 100/1000Base-X open SFP slots. The SGMII (Serial Gigabit Media Independent Interface) provides network data and port speed information between a 10/100/1000 PHY and a MAC, operating in both half duplex and full duplex at all port speeds. If SGMII is configured, the auto negotiation feature is disabled.

A port's Ethernet PHY mode can be configured in the x222x/x32xx using either the CLI or Web method.

Set Port Admin Mode (Ethernet PHY Mode) – CLI Method

Use this procedure to set the Ethernet PHY mode for a port which is capable of changing PHY mode.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command line, type **set ether phymode=xx** and press **Enter**.

   where:

   xx = port admin mode setting (phySGMII|phy100BaseFX|phy1000BaseX); valid choices are:

   - SGMII
   - 100BaseFX
   - 1000BaseX

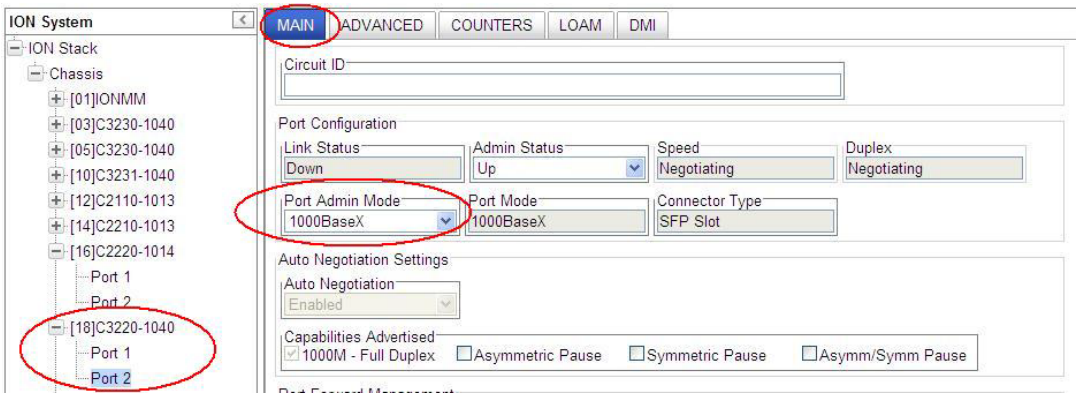
   Example: C1|S13|L0AP1|L1P2/>**set ether phymode=SGMII**

3. Verify the configuration has been set. Type **show ether config** and press **Enter**. The Ethernet configuration displays.

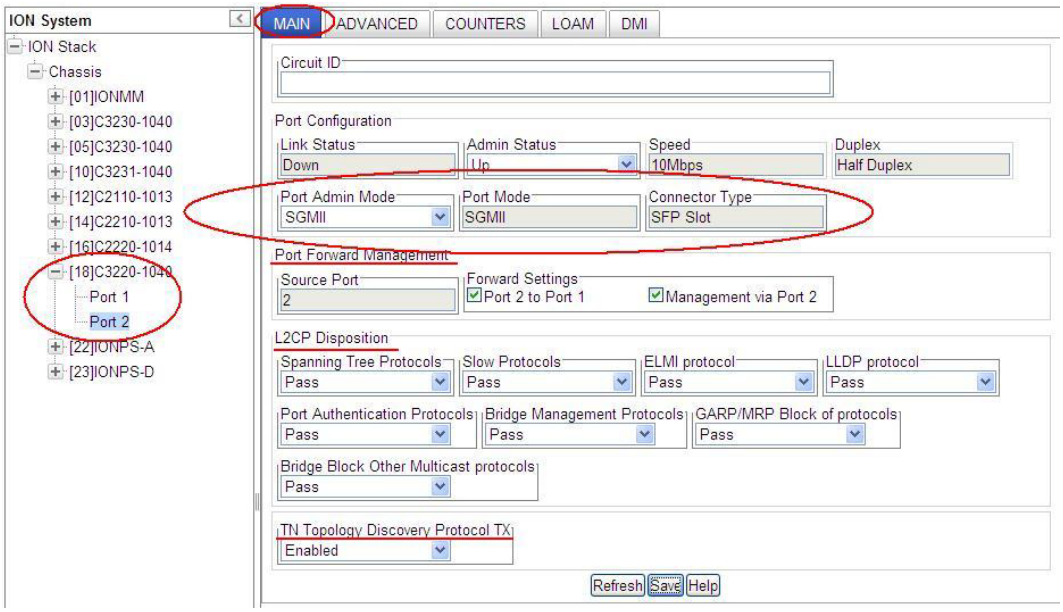
```
C1|S16|L1P1>set ether phymode ?
  phy1000BaseX
  phy100BaseFX
  phySGMII
C1|S16|L1P1>set ether phymode phySGMII
Cannot set PHY mode on this port!
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>set ether phymode phySGMII
C1|S16|L1P2>show ether config
Port-21014
FIBER port:
------------------------------------------------------------------------
Link operation status:        down
Admin status:                 up
Port mode:                    SC Singlemode Fiber
Speed:                        100M
Duplex:                       full
PHY mode change cap:          false
PHY operation mode:           phy100BaseFX
Far End Fault mode:           enable

AutoNeg admin state:          disable
C1|S16|L1P2>
```

Port Admin Mode Config – Web Method

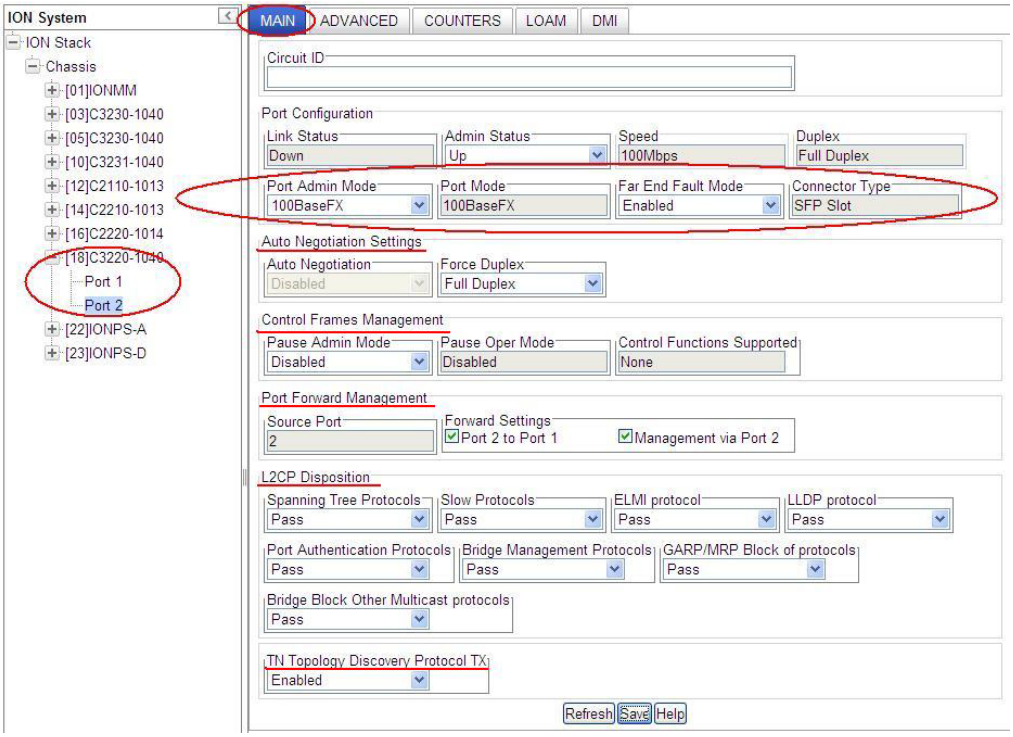
1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Locate the **Port Admin Mode** field on the x3220 Port 2 **MAIN** tab.



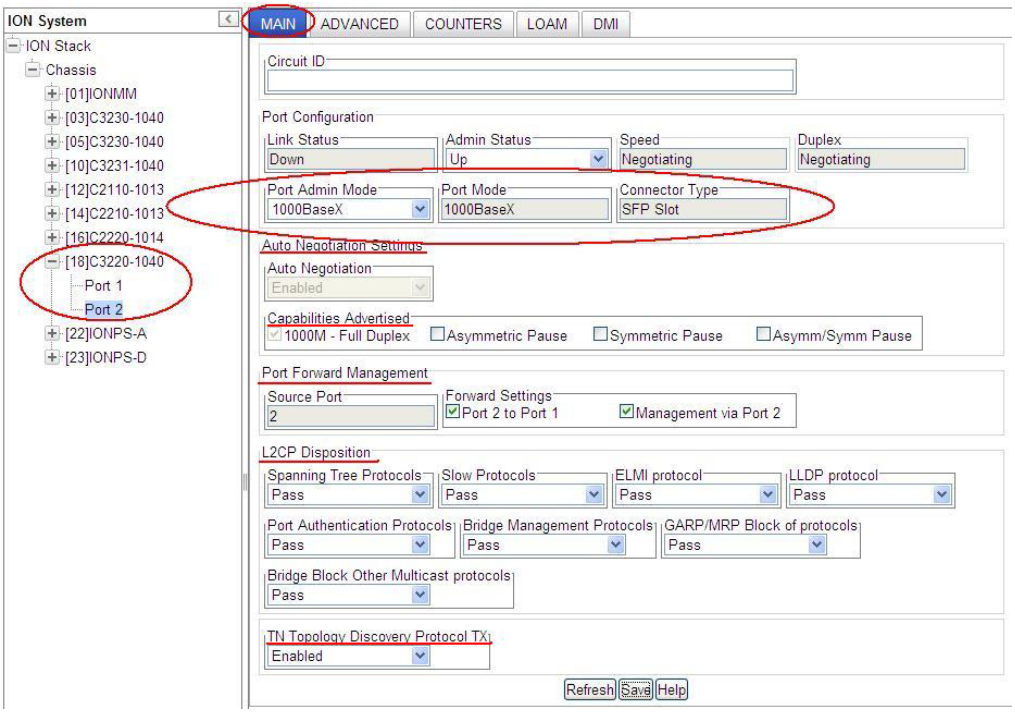
3. Select **100BaseX**, **100BaseFX**, or **SGMII** as the **Port Admin Mode**.
4. Click **Save**. The displayed function set changes based on the **Port Admin Mode** selected in step 3.



With **SGMII** selected (see above), the **Port Forward Management**, **L2CP Disposition**, and **TN Topology Discovery Protocol TX** sections display (the **Far End Fault** and **Control Frames Management** sections do not display with **SGMII** selected.)



With **100BaseFX** selected (see above), the **Far End Fault**, **Auto Negotiation Settings**, **Control Frames Management**, **Port Forward Management**, **L2CP Disposition**, and **TN Topology Discovery Protocol TX** sections display.



With **1000BaseX** selected (see above), the **Auto Negotiation Settings**, **Capabilities Advertised**, **Port Forward Management**, **L2CP Disposition**, and **TN Topology Discovery Protocol TX** sections display.

Far End Fault Mode Configuration

With Far End Fault (FEF) mode enabled, the x222x / x32xx can track and report FEF capabilities and setting information.

The x222x / x32xx Far End Fault (FEF) mode can be configured using the CLI method.

Far End Fault Mode Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the device's command prompt type **set ether fef=xx** where:

   xx=enable or disable

3. Press **Enter**.
4. Use the **show ether config** command to verify the FEF mode capability and mode settings (e.g., *Far End Fault cap: true, Far End Fault mode: enable*). For example:

```
C1|S16|L1P1>set ether fef=disable
Only 100M fiber port can set far end fault!
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>set ether fef=disable
C1|S16|L1P2>show ether config
Port-21014
FIBER port:
--------------------------------------------------------------------------
Link operation status:        down
Admin status:                 up
Port mode:                    SC Singlemode Fiber
Speed:                        100M
Duplex:                       full
PHY mode change cap:          false
PHY operation mode:           phy100BaseFX
Far End Fault mode:           disable

AutoNeg admin state:          disable
C1|S16|L1P2>
```

Set Bandwidth Allocation / Rate Limiting

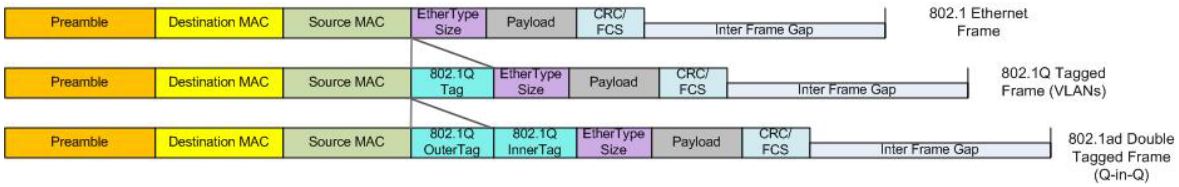
The x222x/x32xx Bandwidth Allocation (Rate Limiting) can be configured to limit both Ingress bandwidth and Egress bandwidth. If so configured, traffic at rates over this CIR (Committed Information Rate) is discarded. Note that these limits cannot be set faster than the port speed.

Bandwidth Allocation / Rate Limiting can be configured in the x222x / x32xx NID using either the CLI or Web method.

Set Bandwidth Allocation / Rate Limiting – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command line, define which transmission layer is to be counted when determining the rate limit. Type **set bw alloc-type={countAllLayer1 | countAllLayer2 | countAllLayer3}**. The default is Count all Layer 1 bytes.
   - **Counts All Layer 1**: (the default): in determining the rate limit, this selection counts the following bytes in a frame: Preamble (8 Bytes) + DA to CRC + Inter Frame Gap (12 bytes).
   - **Counts All Layer 2**: in determining the rate limit, this selection counts the bytes in a frame from the DA to the CRC in determining the rate limit.
   - **Counts All Layer** 3: in determining the rate limit, this selection counts the following bytes in a frame:
     - from the DA (Destination MAC Address) to the CRC (18 bytes if untagged)
     - from the DA (Destination MAC Address) to the CRC (22 bytes if tagged)

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



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

   xx= In-rate: Ingress rate in kbps

   yy = Egress-rate: Egress rate in kbps

See below for valid selections for in-rate (ingress) and egress-rates.

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

   For example:

```
C1|S16|L1P2>set irate=rate1M erate=rate1M
C1|S16|L1P2>show bandwidth allocation
Bandwidth allocation type:    countAllLayer1
Ingress rate:                 rate1M
Egress rate:                  rate1M
C1|S16|L1P2>
```

Note: The rate parameters are case-sensitive.

Rate Limits Summary

Set ingress rate and egress rate of a port - increase granularity of Ingress/Egress Rate Limiting per MEF 11: 1 Mbps steps up to 10 Mbps, 5 Mbps steps beyond 10 Mbps and up to 100 Mbps, and 50 Mbps steps beyond 100 Mbps and up to 1 Gbps.

x222x, x322x, x323x ingress and egress rate limiting:

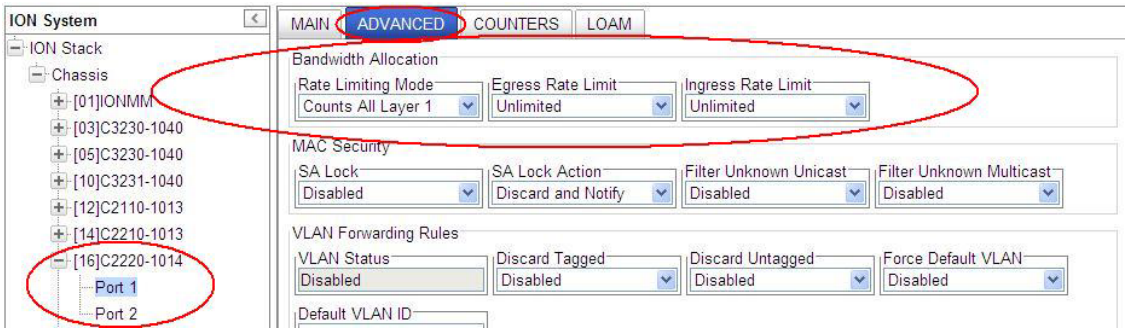
On 1000M port: Unlimited, 1M, 2M, 3M, 4M, 5M, 6M, 7M, 8M, 9M, 10M, 15M, 20M, 25M, 30M, 35M, 40M, 45M, 50M, 55M, 60M, 65M, 70M, 75M, 80M, 85M, 90M, 95M, 100M, 150M, 200M, 250M, 300M, 350M, 400M, 450M, 500M, 550M, 600M, 650M, 700M, 750M, 800M, 850M, 900M, and 950M bps.
On 100M port: 1M, 2M, 3M, 4M, 5M, 6M, 7M, 8M, 9M, 10M, 15M, 20M, 25M, 30M, 35M, 40M, 45M, 50M, 55M, 60M, 65M, 70M, 75M, 80M, 85M, 90M, and 95M bps.

x3210 ingress and egress rate limiting:

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

Set Bandwidth Allocation / Rate Limiting – Web Method

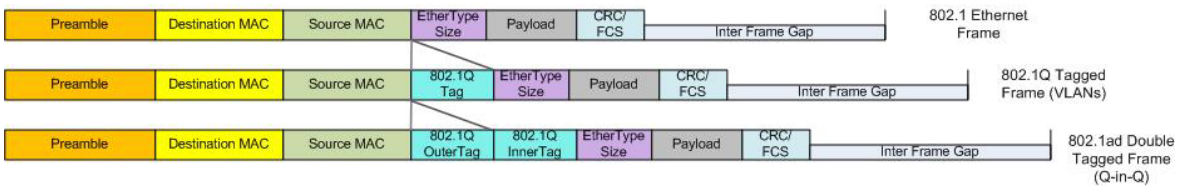
1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the appropriate port's **ADVANCED** tab.
3. Locate the **Bandwidth Allocation** section.



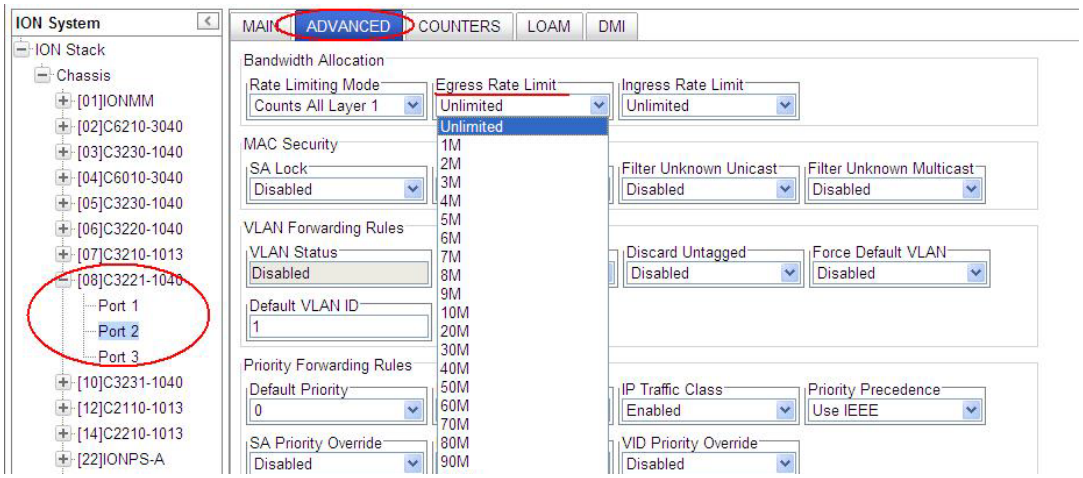
4. In the **Rate Limiting Mode** field, select which bytes in a frame are to be counted in determining the rate limit:

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

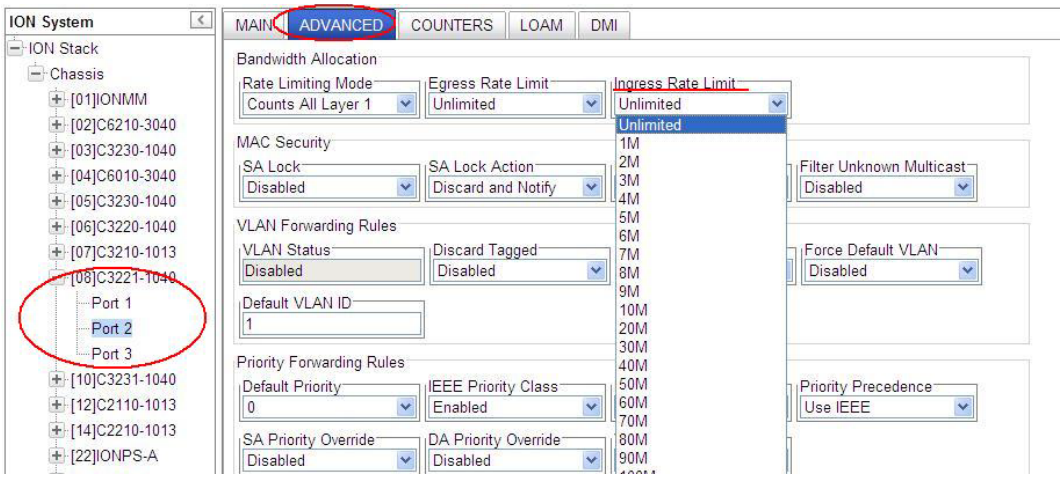
     Note: The Counts All Layer 3 selection will skip the Ethernet header, the CRC, and Tags (if any tags exist).



5. In the **Egress Rate Limit** field, select the Egress bandwidth limit in bits per second. Traffic which goes over this rate is discarded. The default is **Unlimited**.



6. In the **Ingress Rate Limit** field, select the Ingress bandwidth limit in bits per second. This is the Committed Information rate (CIR) on this interface for Ingress. Traffic which goes over this rate is discarded. The default is **Unlimited**.



7. Click **Save** when done. The Rate Limits vary depending on the device and port selected.

Rate Limits Summary

Set ingress rate and egress rate of a port - increase granularity of Ingress/Egress Rate Limiting per MEF 11: 1 Mbps steps up to 10 Mbps, 5 Mbps steps beyond 10 Mbps and up to 100 Mbps, and 50 Mbps steps beyond 100 Mbps and up to 1 Gbps.

x222x, x322x, x323x ingress and egress rate limiting:

On 1000M port: Unlimited, 1M, 2M, 3M, 4M, 5M, 6M, 7M, 8M, 9M, 10M, 15M, 20M, 25M, 30M, 35M, 40M, 45M, 50M, 55M, 60M, 65M, 70M, 75M, 80M, 85M, 90M, 95M, 100M, 150M, 200M, 250M, 300M, 350M, 400M, 450M, 500M, 550M, 600M, 650M, 700M, 750M, 800M, 850M, 900M, and 950M bps.

On 100M port: 1M, 2M, 3M, 4M, 5M, 6M, 7M, 8M, and 9M bps.

x3210 ingress and egress rate limiting:

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

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

Problem: Bandwidth Ingress rate limiting on the C3221 failed on 150M.
Solution: Make sure that ingress rate limiting settings are at or above the advertised speeds.

Configuring Priority Queuing

The x322x/x32xx lets you configure the Egress Queue mode to either “Weighted Round Robin (WRR)” or “Strict” via either the CLI or the Web interface.

WRR (Weighted Round Robin) is a scheduling discipline wherein each packet flow or connection has its own packet queue. It is a simple approximation of GPS (generalized processor sharing). While GPS serves a near infinite amounts of data from each nonempty queue, WRR serves a number of packets for each nonempty queue (number = normalized (weight / meanpacketsize).

(SP) Strict priority queuing

(SP) Strict priority queuing is a response to the disadvantages of FIFO in a congested environment. Strict priority queuing assumes that types of traffic can be differentiated and treated preferentially. With the Strict Priority Queuing function enabled, only high priority packages will be passed and all low priority packages will be dropped during a network jam condition (the queuing is based ‘strictly’ on the assigned priority).

Priority Queuing Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the command line, use the **go** command to switch to port 1.
3. Define the port queuing method. Type set port queuingmethod=<wrr|sp>
   where:
   wrr = sets the Egress Queue Mode to the "Weighted Round Robin" queuing method.
   sp = sets the Egress Queue Mode to the "Strict" queuing method.
4. Press the **Enter** key.

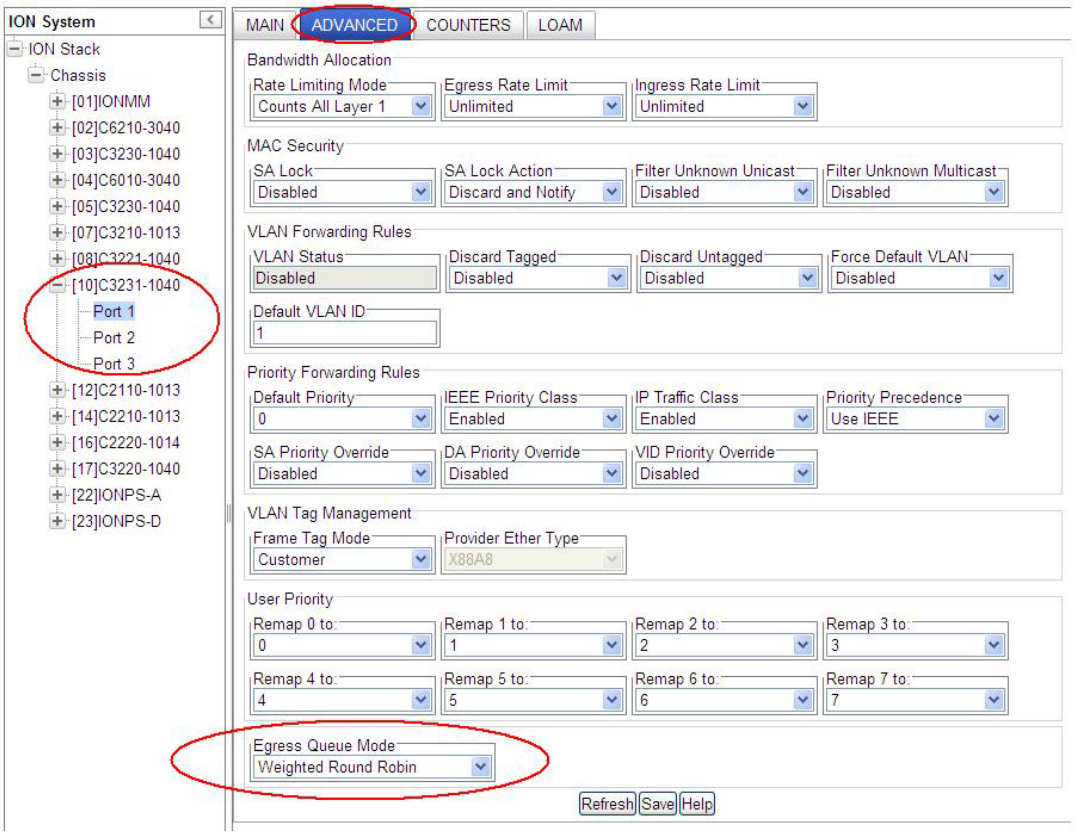
For example:

```
C1|S3|L1P1>set port egress queuingmethod ?
  sp
  wrr
C1|S3|L1P1>set port egress queuingmethod=sp
C1|S3|L1P1>set port egress queuingmethod=wrr
C1|S3|L1P1>show qos config
Default priority:                           7
Use IEEE tag for priority:                  enable
Use IP tag for priority:                    enable
Tag type for priority if both tag available: useIP
Use source MAC address for priority:        disable
Use destination MAC address for priority:   disable
Use VLAN id for priority:                   disable
Port Egress Queuing mehod:    wrr
C1|S3|L1P1>
```

5. Repeat steps 2-4 above for other device ports as required.

Priority Queuing Config – Web Method

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the Port 1 **ADVANCED** tab.
3. Locate the **Egress Queue Mode** field.



4. At the dropdown select either "**Weighted Round Robin**" (the default setting) or "**Strict**".
5. Click the **Save** button when done.
6. Repeat steps 3-5 above for other device ports as required.

Configuring Ethernet LOAM (Link OAM)

Ethernet Operations, Administration and Maintenance (OAM) protocol is used for monitoring and troubleshooting Ethernet networks.

The x222x / x32xx NIDs support Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57).

LOAM Configuration

The x222x / x32xx NID supports the LOAM standard IEEE 802.3–2005 Clause 57 which defines mechanisms for monitoring and troubleshooting Ethernet access links. Specifically it defines tools for discovery, remote failure indication, remote and local loopback, and status and performance monitoring.

LOAM Configuration Prerequisites and Restrictions

For the latest feature information and caveats, see the release notes for your particular device/system and soft-ware release. The prerequisites and restrictions below apply to all x222x / x32xx models unless otherwise noted.

The x222x / x32xx products implement LOAM on both the fiber and twisted pair interfaces. The LOAM-enabled port is user selectable. By default, the fiber port is the default LOAM enabled port. With dual fiber ports, Port 2 is the default.

LOAM Configuration Prerequisites

1. Network topology and network administration have been reviewed.
2. Business and service policies have been established.
3. In a typical application, you connect a cable from the Active local device (chassis) to the Passive remote device. The Active local device manages its Passive remote peer. The relationship between the Active local device and its Passive remote peer is established via LOAM functionality.
4. To change any of the IP parameters through the CLI interface, the management state must be enabled (see “Performing Initial System Setup” on page 71).
5. To remotely manage specific LOAM critical events, set up SNMP trap host managers in the IONMM (see “Configuring SNMP” on page 227 for set-up instructions).
6. The x222x / x32xx NIDs support both private and public MIBs for SNMP management including RFC 4878 (Definitions and Managed Objects for Operations, Administration, and Maintenance (LOAM). See “Supported MIBs” on page 29 for more information.
7. Provisioning a standalone x222x / x32xx NID for remote operation without IONMM management requires a change to the switch mode. By default, the x222x / x32xx is managed by the ION MM. Setting the switch mode to local indicates that the device is not managed by the IONMM, but by either a direct USB connection or a direct network connection via Telnet or the Web interface. Setting the mode to remote indicates that the device is managed through the IONMM. Use the **set switch mode=** command to change management mode between local and remote. To change any of the IP parameters through the CLI interface, the management state must be enabled.

LOAM Configuration Restrictions

1. The x222x / x32xx NIDs do not support variable retrieval nor unidirectional link. They support loopback and event notifications only.
2. LOAM on Ethernet interfaces may be in 'Active' mode or 'Passive' mode. These two modes differ in that Active mode provides additional capabilities to initiate monitoring activities with the remote LOAM peer entity, while Passive mode generally waits for the peer to initiate LOAM actions with it. For example, an active LOAM entity can put the remote LOAM entity in a loopback state, where a passive LOAM entity cannot.

At initialization and at failure conditions, two LOAM entities on the same full-duplex Ethernet link begin a discovery phase to determine which LOAM capabilities may be used on that link.

LOAM can be configured in the x222x / x32xx NID using either the CLI or Web method.

LOAM Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Go to the port where LOAM is to operate (use the **go** command). 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 Standalone card
3. Enable LOAM for the port. Type: **set loam admin state=enable** and press **Enter**.
4. Set the LOAM operating mode. Type:

   set loam mode=<xx>

   where:

   xx = operating mode:

   - **active** –the NID sends out discovery frames (OAM Information PDUs). It can initiate OAM Loopback to its remote peer.
   - **passive** – the NID can receive and respond to discovery messages (OAM Information PDUs). It can not initiate OAM Loopback but can process loopback requests from an OAM Peer in active mode.
5. Press **Enter**.

6. Enable or disable Event notifications and define the values associated with the events. The table below describes the various events and the commands associated with them.

Table 13: LOAM Events

Event/Value	Description/Command
Critical Event Notification	Whether LOAM notification is done for critical events. Factory default is **enable**. **set loam critical–evt–notif** ={enable | disable}
Dying Gasp Event Notification	Whether LOAM notification is done for a loss of power condition. Factory default is **enable**. **set loam dg–evt–notif**={enable | disable}
Errored Frame Events	
Notification	Whether LOAM notification is done when the number of frame errors exceeds the threshold value defined for this event. Factory default is **enable**. **set loam ef–evt–notif**={enable | disable}
Threshold Value	The number of frame errors that must occur within the defined window before notification of this event is made. **set loam ef threshold=**<xx>
Window Value	The amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent. **set loam ef window=**<xx>

Errored Frame Period Events	
Notification	Whether LOAM notification is done for errored frame period events. Factory default is **enable**. **set loam efp–evt–notif={enable | disable}**
Threshold Value	The number of frame period errors that must occur within the defined window before notification of this event is made. **set loam efp threshold=**<xx>
Window Value	The number of frames in which the threshold value must occur before an event notification is sent. **set loam efp window=**<xx>
Errored Frame Seconds Summary Events	
Notification	Whether LOAM notification is done for errored frame seconds summary events. Factory default is **enable**. **set loam efss–evt–notif=**{enable | disable}
Threshold Value	The number of errored frame that must occur within in the defined window before notification of this event is made. **set loam efss threshold=**<xx>
Window Value	The amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent. **set loam efss window=**<100-9000>

Errored Frame Seconds Summary Events	
Notification	Whether LOAM notification is done for errored frame seconds summary events. Factory default is **enable**. **set loam efss–evt–notif=**{enable | disable}
Threshold Value	The number of errored frame that must occur within in the defined window before notification of this event is made. **set loam efss threshold=**<xx>
Window Value	The amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent. **set loam efss window=**<100-9000>
Errored Symbol Period Events	
Notification	Whether LOAM notification is done for errored symbol period events. **set loam esp–evt–notif**={enable | disable}
Threshold Value	The number of error symbols that must occur within in the defined window before notification of this event is made. **set loam esp threshold high=**<xx> **low=**<yy> xx = the high errored symbol threshold as a number of error symbols. If the number of error symbols in the window period is equal to or greater than xx, then a user defined action will be triggered. yy = the low errored symbol threshold as a number of symbol errors. If the number of error symbols in the window period is equal to or greater than yy, then the Errored Symbol Period Link Event will be generated.

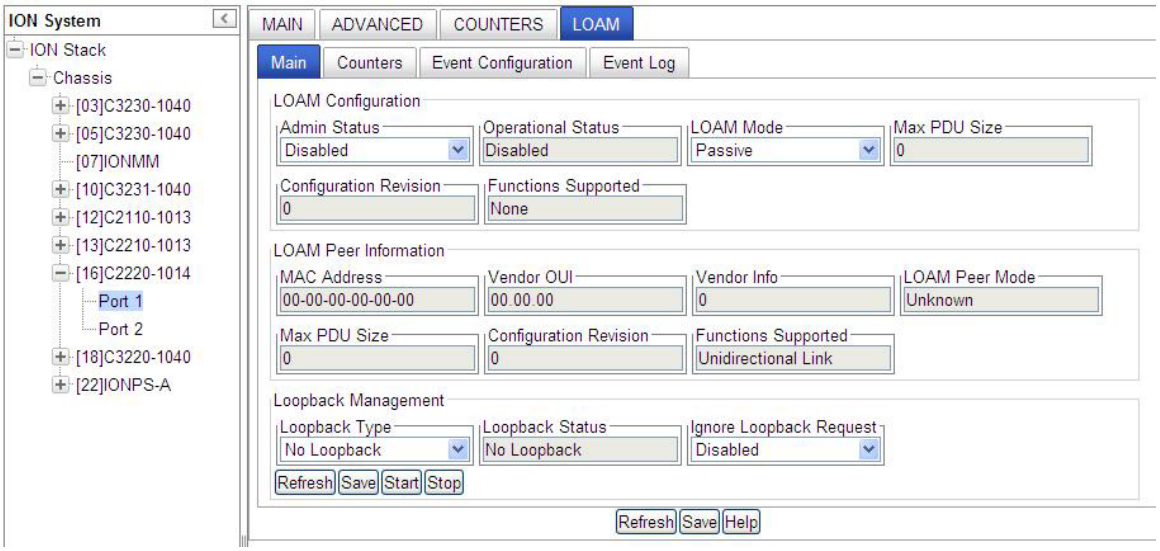
Window Value	The threshold window in which the threshold value must occur before an event notification is sent. **set loam esp window high=**<xx> **low=**<yy> xx = the high errored symbol window threshold as a number of error symbols. If the number of error symbols in the window period is equal to or greater than xx, then a user defined action will be triggered. yy = the low errored symbol window threshold as a number of symbol errors. If the number of error symbols in the window period is equal to or greater than yy, then the Errored Symbol Period Link Event will be generated.

For example:

```
AgentIII C1|S16|L1P1>set loam mode ?
  active
  passive
AgentIII C1|S16|L1P1>set loam admin state=enable
AgentIII C1|S16|L1P1>set loam mode=active
AgentIII C1|S16|L1P1>set loam ?
  admin
  critical-evt-notif
  dg-evt-notif
  ef
  ef-evt-notif
  efp
  efp-evt-notif
  efss
  efss-evt-notif
  esp
  esp-evt-notif
  ignore-loopback-request
  mode
AgentIII C1|S16|L1P1>
```

LOAM Config – Web Method

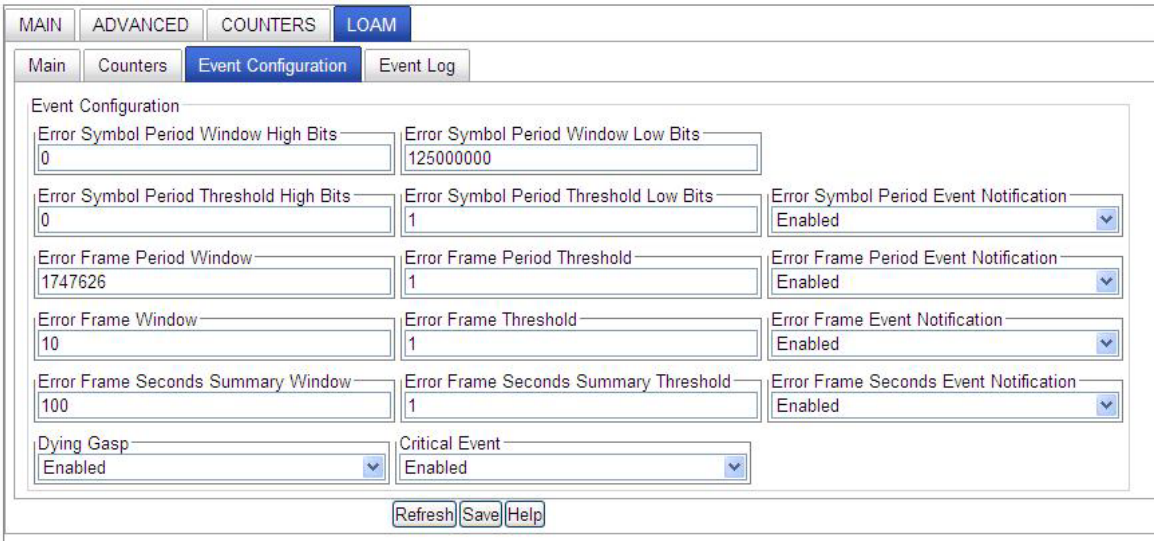
1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the port where LOAM is to operate.
3. Select the **LOAM** tab. Select the **Main** sub-tab if not already selected.



4. In the **Admin Status** field, select **Enabled**.
5. In the **LOAM Mode** field, select the operating mode:
   - **Active** – the NID can initiate LOAM communications and can issue queries and commands to a peer device. When in Active mode, the NID sends out discovery frames (OAM Information PDU). In the Active mode, the NID can initiate LOAM Loopback to its remote peer.
   - **Passive** – the NID waits for the peer device to initiate LOAM communications and responds to, but does not initiate, commands and queries. When in Passive mode, the NID can receive and respond to discovery messages (OAM Information PDU). It cannot initiate LOAM Loopback, but can process loopback requests from a LOAM peer if that LOAM peer is in Active mode.

   Note: To perform Link Fault management, either the local client or the remote peer (or both) must have **LOAM Mode** set to **Active** (configured for Active mode operation).
6. Locate the **Loopback Management** section.

7. In the **Loopback Type** field, select the operating mode:
   - **No Loopback** – disables LOAM loopback testing.
   - **Remote Peer**- prevents that port from forwarding data frames to other ports when it goes into "loopback" mode. (AKA "intrusive loopback").
   - **Alternate** – allows the data frames to be forwarded to other ports, while doing the loopback with its peer.
8. The **Loopback Status** field displays the loopback status for this interface when enabled. The only two possible values for a SET operation are *intiateLoopback(2)* and *terminateLoopback(3)*. All other values are read-only to show the status of the loopback operation (No Loopback, Local in Loopback, Remote in Loopback).
9. In the **Ignore Loopback Request** field, select:
   - **Enabled** – causes the LOAM enabled x222x/x32xx NID to ignore all Loopback requests (i.e., not respond to remote loopback requests from peers).
   - **Disabled** – causes the LOAM enabled x222x/x32xx NID to respond to all remote loopback requests from peers.
10. Click **Save** to perform the loopback action. Click **Start** to begin the loopback request; click **Stop** to end the loopback request.
11. Select the **Event Configuration** sub-tab.

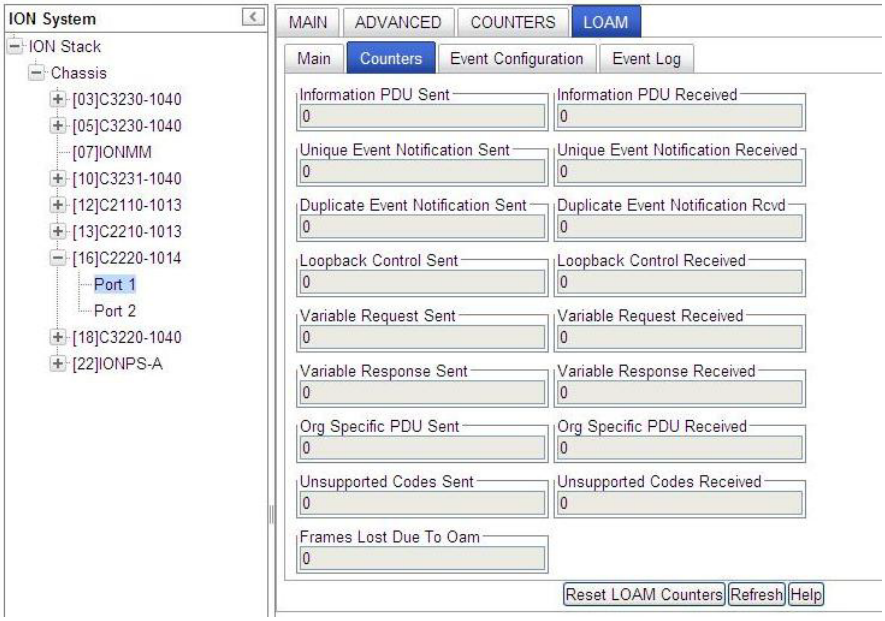


12. Enable or disable **Event Notification**s as required (**Error Symbol Period Event Notification**, **Error Frame Period Event Notification**, **Error Frame Event Notification**, and/or **Error Frame Seconds Event Notification**).

13. For the Event Notifications enabled in step 13, enter the appropriate values for the related window and threshold fields (defaults are shown in parenthesis):
    - **Error Symbol Period Event Notification** – if enabled, set these window and threshold fields:
        - Error Symbol Period Window High Bits (0) and Error Symbol Period Window Low Bits (125000000). The valid ranges are Error Symbol Period Window High (0 - 4294967295) and Error Symbol Period Window Low (125000000 - 268435455).
        - Error Symbol Period Threshold High Bits (0) and Error Symbol Period Threshold Low Bits (1). The valid range for each is (0 - 4294967295).
    - **Error Frame Period Event Notification** – if enabled, set the Error Frame Period Window (1747626) and Error Frame Period Threshold (1). The Error frame period window valid range is 174762 – 104857560.
    - **Error Frame Event Notification** – if enabled, set the Error Frame Window (10) and Error Frame Threshold (1). The Error frame window valid range is 10 – 600. The valid Error frame threshold range is 0 – 268435455.
    - **Error Frame Seconds Event Notification** – if enabled, set the Error Frame Seconds Summary Window (100) and Error Frame Seconds Summary Window Threshold (1). The Error frame seconds summary window valid range is 100 – 9000. The Error frame seconds summary window threshold valid range is 0 – 268435455.

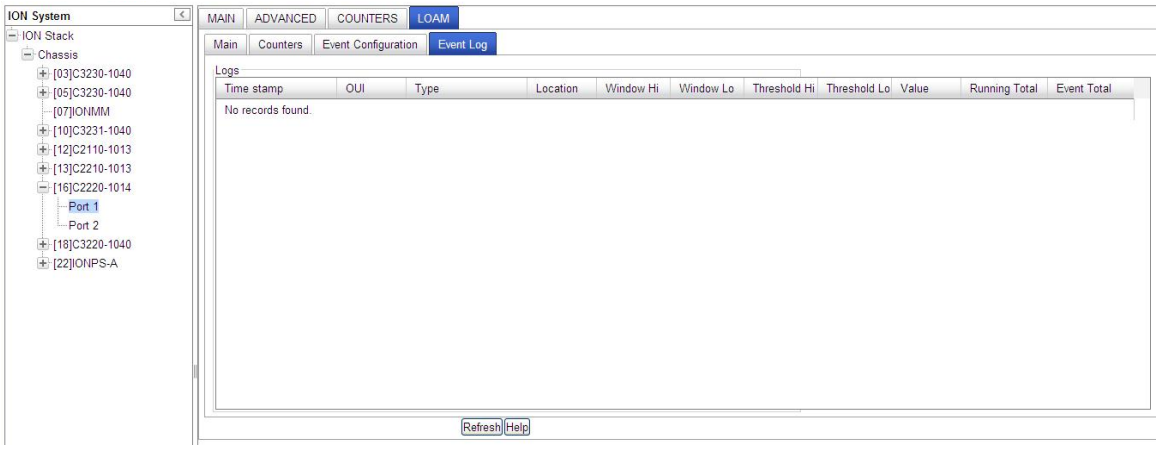
    Threshold Value: The number of frame errors that must occur within the defined window before notification of this event is made.

    Window Value: The amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent.
14. Enable or disable the **Dying Gasp** function as needed. The default is **Enabled** (LOAM notification is done for a loss of power condition).
15. Enable or Disable the **Critical Event** function as needed. The default is **Enabled** (LOAM notification is performed for critical events).
16. Click the **Save** button.
17. Select the **Counters** sub-tab.



18. To update the displayed Counters information, click the **Refresh** button. To reset the Counters to zero, click the **Reset LOAM Counters** button.

19. Select the **Event Log** sub-tab.



20. Click the **Refresh** button. Updated Event Log information displays.

21. Note the Event Log **Type** column for troubleshooting purposes. It lists the type of event that generated this entry in the event log.

The Event log Type column types are shown and described below.

Logs

Time stamp	OUI	Type	Location	Window Hi	Window Lo	Thresh
0:0:35:45.19	01.80.C2	Link Fault	Local			
0:0:00:03.31	01.80.C2	Link Fault	Local			
0:0:00:03.31	01.80.C2	Critical Link	Local			
0:0:00:06.62	01.80.C2	Critical Link	Remote			
0:0:02:53.94	01.80.C2	Error Symbol	Local	0	125000000	0
0:0:03:22.62	01.80.C2	Error Symbol	Remote	0	125000000	0
0:0:15:39.90	01.80.C2	Link Fault	Local			
0:0:15:41.28	01.80.C2	Critical Link	Remote			
0:0:15:43.34	01.80.C2	Error Frame Period	Remote	0	1747626	0
0:0:15:46.65	01.80.C2	Error Frame	Remote	0	10	0
0:0:16:40.04	01.80.C2	Error Frame Seconds	Remote	0	100	0

- **Link Fault** - generated when a local or remote link fault is detected (a non-threshold crossing event).
- **Dying Gasp** - generated when a loss of power condition is detected (a non-threshold crossing event).
- **Critical Link** - generated when LOAM notification is done for critical events (a non-threshold crossing event).

22. The **Location** column identifies whether the event report was for a local or remote device.
23. When the **OUI** (Organizationally Unique Identifier) column displays something other than **01.80.C2**, then an organization other than IEEE 802.3 has defined the event space. When the **OUI** column displays **01.80.C2** (the IEEE 802.3 OUI), the following event types are defined:
    - **Errored Symbol Event** – a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of symbol errors exceeds a threshold within a given window by a number of symbols (e.g., 1,000 symbols out of 1,000,000 had errors).
    - **Errored Frame Period Event** - a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of frame errors exceeds a threshold within a given window defined by a number of frames (e.g., 10 frames out of 1000 had errors).
    - **Errored Frame Event** - a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of frame errors exceeds a threshold within a given window defined by a period of time (e.g., 10 frames in 1 second had errors).
    - **Errored Frame Seconds Event** - a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of errored frame seconds exceeds a threshold within a given time period (e.g., 10 errored frame seconds within the last 100 seconds). An errored frame second is defined as a 1 second interval which had more than 0 frame errors.

The other LOAM Event Log table parameters (besides **Type**) are Time stamp, OUI, Type, Location, Window Hi, Window Lo, Threshold Hi, Threshold Lo, Value, Running Total, and Event Total. These parameters are described below.

Time stamp - the value of Up Time at the time of the logged event. For locally generated events, the time of the event can be accurately retrieved from Up Time. For remotely generated events, the time of the event is indicated by the reception of the Event Notification OAMPDU indicating that the event occurred on the peer.

OUI - the Organizationally Unique Event (OUI) of the entity defining the object type. All IEEE 802.3 defined events use the IEEE 802.3 OUI of *01 80 C2*.

Location - whether this event occurred locally (local), or was received from the LOAM peer via Ethernet LOAM (remote).

Window - if the event represents a threshold crossing event, two objects (Loam Event Window Hi and Loam Event Window Lo) form an integer yielding the window over which the value was measured for the threshold crossing event (e.g., 5, when 11 occurrences happened in 5 seconds while the threshold was 10).

Threshold - if the event represents a threshold crossing event, two objects (Loam Event Threshold Hi and Loam Event Threshold Lo) form an integer yielding the value that was crossed for the threshold crossing event (e.g., 10, when 11 occurrences happened in 5 seconds while the threshold was 10).

Value - if the event represents a threshold crossing event, this value indicates the value of the parameter within the given window that generated this event (e.g., 11, when 11 occurrences happened in 5 seconds while the threshold was 10).

Running Total - each Event Notification TLV contains a running total of the number of times an event has occurred, as well as the number of times an Event Notification for the event has been transmitted. For non-threshold crossing events, the number of events (Loam Log Running Total) and the number of resultant Event Notifications (Loam Log Event Total) should be identical.

For threshold crossing events, since multiple occurrences may be required to cross the threshold, these values are likely different. This value represents the total number of times this event has happened since the last reset (for example, 3253, when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset).

Event Total - each Event Notification TLV contains a running total of the number of times an event has occurred, as well as the number of times an Event Notification for the event has been transmitted. For non-threshold crossing events, the number of events (Log Running Total) and the number of resultant Event Notifications (Log Event Total) should be identical. For threshold crossing events, since multiple occurrences may be required to cross the threshold, these values are likely different. This value represents the total number of times one or more of these occurrences have resulted in an Event Notification (for example, 51 when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset).

LOAM Operational Status

Each of the nine possible Device > Port > **LOAM** > **MAIN** tab **Operational Status** field parameters are discussed below.

At initialization and failure conditions, two LOAM entities on the same full-duplex Ethernet link begin a discovery phase to determine what LOAM capabilities may be used on that link. The progress of this initialization is controlled by the OA sublayer.

Disabled - This value is always Disabled(1) if LOAM is disabled on this interface via the 'Admin Status'.
LinkFault - If the link has detected a fault and is transmitting OAMPDUs with a link fault indication, the value is LinkFault(2). Also, if the interface is not operational ('Link Status' is not Up(1)), LinkFault(2) is returned. Note that the object 'Link Status' may not be Up(1) as a result of link failure or administrative action (ifAdminState being Down(2) or Testing(3)).
PassiveWait - The PassiveWait(3) state is returned only by LOAM entities in passive mode ('LOAM Mode') and reflects the state in which the LOAM entity is waiting to see if the peer device is OA capable.
Active Send Local - The Active Send Local(4) value is used by active mode devices ('LOAM Mode') and reflects the LOAM entity actively trying to discover whether the peer has LOAM capability but has not yet made that determination.
SendLocalAndRemote - The state SendLocalAndRemote(5) reflects that the local OA entity has discovered the peer but has not yet accepted or rejected the configuration of the peer. The local device can, for whatever reason, decide that the peer device is unacceptable and decline LOAM peering.
SendLocalAndRemoteOk - If the LOAM peering is allowed by the local device, the state moves to SendLocalAndRemoteOk(6).
LoamPeeringLocallyRejected - If the local LOAM entity rejects the peer LOAM entity, the state becomes OamPeeringLocallyRejected(7). Note that both the SendLocalAndRemote(5) and OamPeeringLocallyRejected(7) states fall within the state SEND_LOCAL_REMOTE of the Discovery state diagram [see 802.3ah, Figure 57-5], with the difference being whether the local LOAM client has actively rejected the peering or has just not indicated any decision yet. Whether a peering decision has been made is indicated via the local flags field in the OAMPDU (reflected in the aOAMLocalFlagsField of 30.3.6.1.10).
LamPeeringRemotelyRejected - If the remote LOAM entity rejects the peering, the state becomes LoamPeeringRemotelyRejected(8). Note that both the SendLocalAndRemoteOk(6) and LoamPeeringRemotelyRejected(8) states fall within the state SEND_LOCAL_REMOTE_OK of the Discovery state diagram [802.3ah, Figure 57-5], with the difference being whether the remote LOAM client has rejected the peering or has just not yet decided. This is indicated via the remote flags field in the OAMPDU (reflected in the aLOAMRemoteFlagsField of 30.3.6.1.11).
Operational - When the local LOAM entity learns that both it and the remote LOAM entity have accepted the peering, the state moves to Operational(9) corresponding to the SEND_ANY state of the Discovery state diagram [802.3ah, Figure 57-5].
NonOperHalfDuplex - Since Ethernet LOAM functions are not designed to work completely over half-duplex interfaces, the value NonOperHalfDuplex(10) is returned whenever Ethernet LOAM is enabled ('Admin Status' is Enabled(1)), but the interface is in half-duplex operation.

LOAM Peer Information Fields

Each port's **LOAM** > **Main** tab > **LOAM Peer Information** section field is described below.

MAC Address - in the format 00-00-00-00-00-00.

Vendor OUI - in the format 00.00.00. The OUI of the entity defining the object type. All IEEE 802.3 defined events (as appearing in [802.3ah] except for the Organizationally Unique Event TLVs) use the IEEE 802.3 OUI of 0x0180C2. Organizations defining their own Event Notification TLVs include their OUI in the Event Notification TLV that gets reflected here.

Vendor Info – e.g., 0 or 1.

LOAM Peer Mode – e.g., Active, Passive, or Unknown. This object configures the mode of LOAM operation for this Ethernet-like interface. LOAM on Ethernet interfaces may be in 'Active' mode or 'Passive' mode. These two modes differ in that active mode provides additional capabilities to initiate monitoring activities with the remote LOAM peer entity, while passive mode generally waits for the peer to initiate OA actions with it. As an example, an active LOAM entity can put the remote LOAM entity in a loopback state, where a passive OA entity cannot. The default value of *dot3OamMod*e is dependent on the type of system on which this Ethernet-like interface resides. The default value should be '*Active(2)*' unless it is known that this system should take on a subservient role to the other device connected over this interface. Changing this value results in incrementing the configuration revision field of locally generated OAMPDUs and potentially re-doing the LOAM discovery process if the 'Operational Status' was already Operational.

Max PDU Size - e.g., 0 or xxxx. The largest OAMPDU that the LOAM entity supports. OA entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers. This value is determined by the local implementation.

Configuration Revision - e.g., 0 or 1. The configuration revision of the LOAM entity as reflected in the latest OAMPDU sent by the LOAM entity. The config revision is used by LOAM entities to indicate that configuration changes have occurred, which might require the peer LOAM entity to re-evaluate whether OAM peering is allowed.

Functions Supported –The LOAM functions supported on this Ethernet-like interface. LOAM consists of separate functional sets beyond the basic discovery process that is always required. These functional groups can be supported independently by any implementation. These values are communicated to the peer via the local configuration field of Information OAMPDUs.

- '*Unidirectional*(0)' indicates that the LOAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
- '*Loopback*(1)' indicates that the LOAM entity can initiate and respond to loopback commands.
- '*Event Notification*(2)' indicates that the LOAM entity can send and receive Event Notification OAMPDUs.
- '*Variable Request and Response*(3)' indicates that the LOAM entity can send and receive Variable Request and Response OAMPDUs.

The default value of "**LOAM Configuration** > **Functions Supported**" is "Loopback, Event Notification". Note that the x222x/x32xx NIDs do not support variable retrieval nor unidirectional link.

LOAM Event Configuration Default Values and Valid Ranges

The LOAM Event Config (dot3oam) commands have the following default values and valid ranges.

802.3 LOAM Event	Default Value	Low Limit	High Limit
ErrSymPeriodWindowHi	0	0	0x0FFFFFFF
ErrSymPeriodWindowLo	0x07735940	1	0x0FFFFFFF
ErrSymPeriodThreshold Hi	0	0	0x0FFFFFFF
ErrSymPeriodThresholdLo	1	0	0x0FFFFFFF

ErrFramePeriodWindow	0x1AAAAA	1	0x63FFFFD8
ErrFramePeriodThreshold	1	0	0x0FFFFFFF
ErrFrameWindow	10	10	600
ErrFrameThreshold	1	0	0x0FFFFFFF
ErrFrameSecsSummaryWindow	100	100	9000
ErrFrameSecsSummaryThreshold	1	0	9000

Dying Gasp Management

When a device detects the power is going to be lost, a system dying gasp procedure is triggered internally, and the dying gasp trap is sent out. If the *ionSysDyingGaspTrap* is set to enabled, a *ionDyingGaspEvt* is sent out. Other events may also be sent out in this procedure (e.g., LOAM events). The LOAM event enabled by *dot3OamDyingGaspEnable* and this Trap event are processed at the same time if both are enabled.

If LOAM is enabled in multiple ports, the LOAM event will be sent out one port at a time, beginning with the smaller port number (i.e., smallest one is copper port, port 1). If multiple trap servers are enabled, the trap will be sent out one server at a time, beginning with server 1.

Dying Gasp can be enabled via the CLI using the **set loam dg–evt–notif** command, or via the Web method from the device port's **LOAM** > **Event Configuration** tab.

Note: Dying gasp reserve power may be not enough for sending out all the LOAM events and Traps, so keep as few targets as possible.

Copper Port Loopback Procedure

The procedure below is for performing a copper Port Loopback via direct link between a C32330 and an S3220. In this procedure, the S3220 Port1 is connected to a switch, and a Management PC is also connected this switch so the Management PC can reach the S3220 or C3220. There are no other devices between C3220 and S3220; if you connect a device between S3220 and C3220, make sure this device can forward LOAM messages.

In this example, the LOAM settings of port 1 of the C3220 and port 1 of S3220:

C3220 Port 1 **LOAM Mode** = Active, **Admin Status** = Enabled
S3220 Port 1 **LOAM Mode** = Passive, **Admin Status** = Enabled

You can inter-change LOAM Active/Passive modes between the C3220 and S3220 (be sure one is **Active** the other is **Passive**).

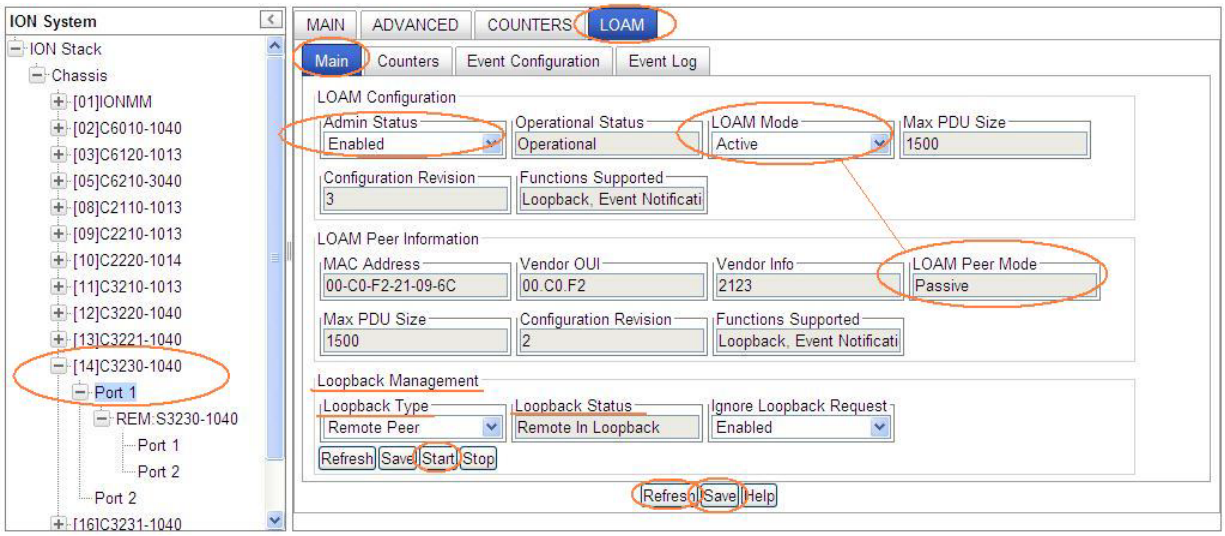
This procedure has an ION chassis with a C3220 and a stand-alone S3220 when using the web interface method:

1. Make sure the copper ports on both sides show **Links Status** = **Up** when you run the loopback test from one of the copper sides (local or remote side). See Figure 1 for this sample Loopback Configuration.
2. For all S3220 and C3220 copper and fiber ports, set LOAM **Admin Mode** to **Enabled** (at **x323x** > **Port 1** > **LOAM** > **Main** > **Admin Status** = **Enabled**).
3. One side of copper port can be LOAM **Admin Status** = **Active** and other can be **Passive**; or both can be **Active**.
4. One of the Fiber ports LOAM **Admin Status** must be **Active** for the MAC address to display.
5. At both the C3220 and the S3220, at the **Loopback Type** dropdown, select **Remote Peer**.
6. From the Active side, click the **Start** button to begin the loopback test; you may have to wait a minute or more for the loopback test to start.
7. Verify the **Operational Status** on both sides (**Operational** or **Passive Wait**). Click Refresh if necessary.
8. Verify the **Loopback Status** (**Remote in Loopback** on the local side, **Local in Loopback** on the remote side).
9. At both the C3220 and the S3220 **Port 1** > **LOAM** > **Main** > **Counters** tab, compare the counters data (e.g., Information PDU Sent, Information PDU Received, Unique Event Notification Sent, Unique Event Notification Received, Loopback Control Sent, Loopback Control Received, etc.). See Figure 2 for sample Loopback Counters information.
10. Click the **Refresh** button to update the **Counters** data as desired.
11. When done click the **Stop** button on the Active side. The Loopback Status changes to **No Loopback**.
12. When the test results are completed as required, click the **Reset LOAM Counters** on both sides. (You may have to click the Reset LOAM Counters button twice, or click Reset LOAM Counters and then click Refresh to clear the counters.) The counters will begin incrementing again immediately.

Each time you change the loopback configuration and run a loopback test, the **Configuration Revision** field increments by one on both sides.
Note that there is a field in the GUI for the MAC address, but you cannot add a MAC peer address to the GUI or via the CLI.

If the cable between the C3220 and the S3220 is disconnected, the remote S3220 fields display in red boxes (at both the device level and at the port level). To recover, plug the cable back in and on the remote S3220 at **Port 1** > **LOAM** > **Main**, click both of the **Refresh** buttons.

Local C3220 > Port 1 > LOAM > Main > Active > Remote In Loopback Status:



Remote S3220 > Port 1 > LOAM > Main > Passive > Local In Loopback Status:

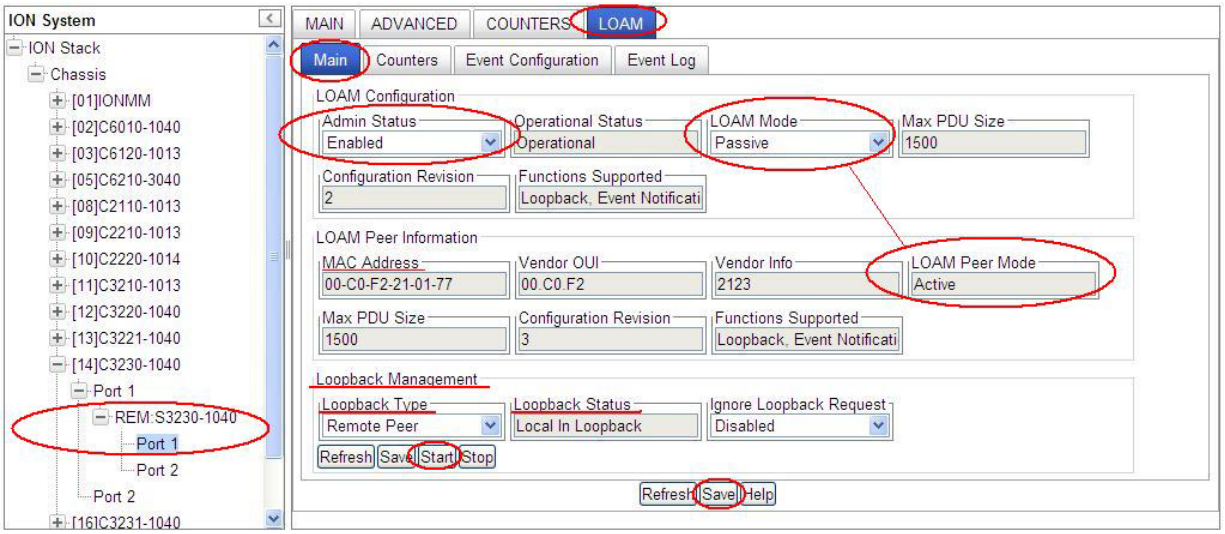


Figure 20: Sample Loopback Configuration

C3220 - Port 1 - LOAM - Counters tab:

S3220 - Port 1 - LOAM - Counters tab:

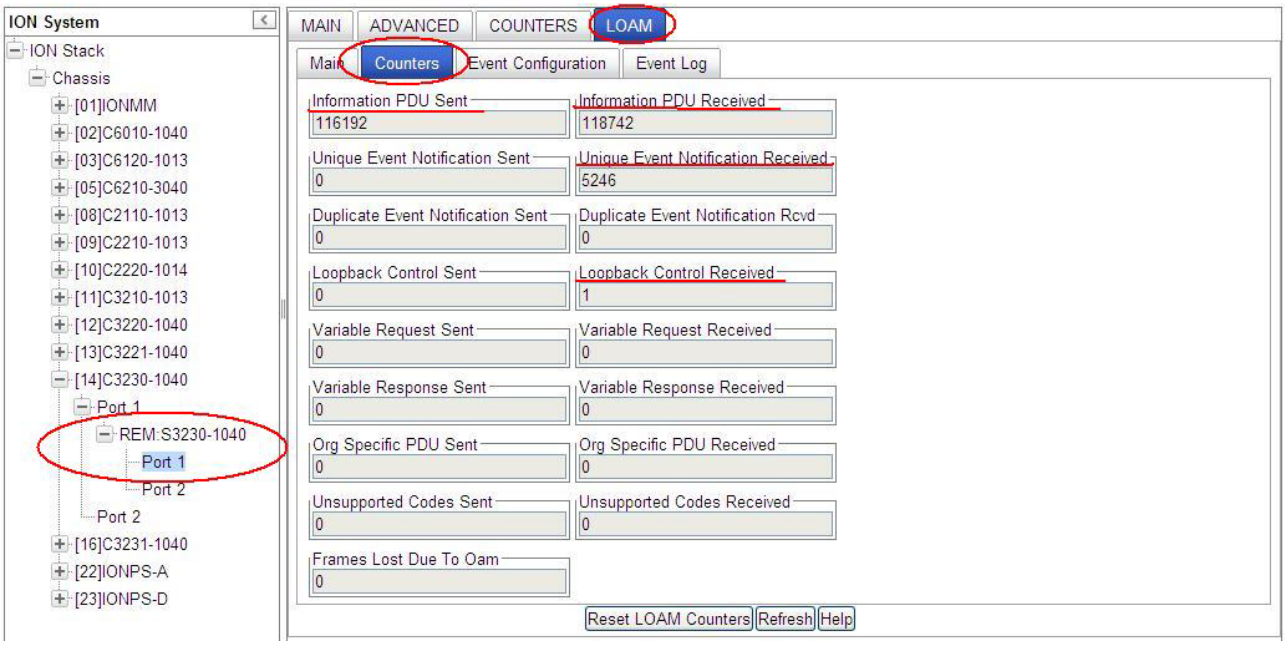


Figure 21: Sample Loopback Counters Information

Configuring Selective and Transparent Link Pass Through

Selective and Transparent Link Pass Through are troubleshooting features that allow the NID 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 NID will automatically disable the TX signal of the other media port, thus passing through the link loss. Note that both TLPT and SLPT can be enabled at the same time, and both can be operational together.

In Selective Link Pass Through, the fiber port (port 2) is monitored for signal loss. If a loss is detected, the NID sends a signal and stops transmitting to the device on the copper port (port 1).

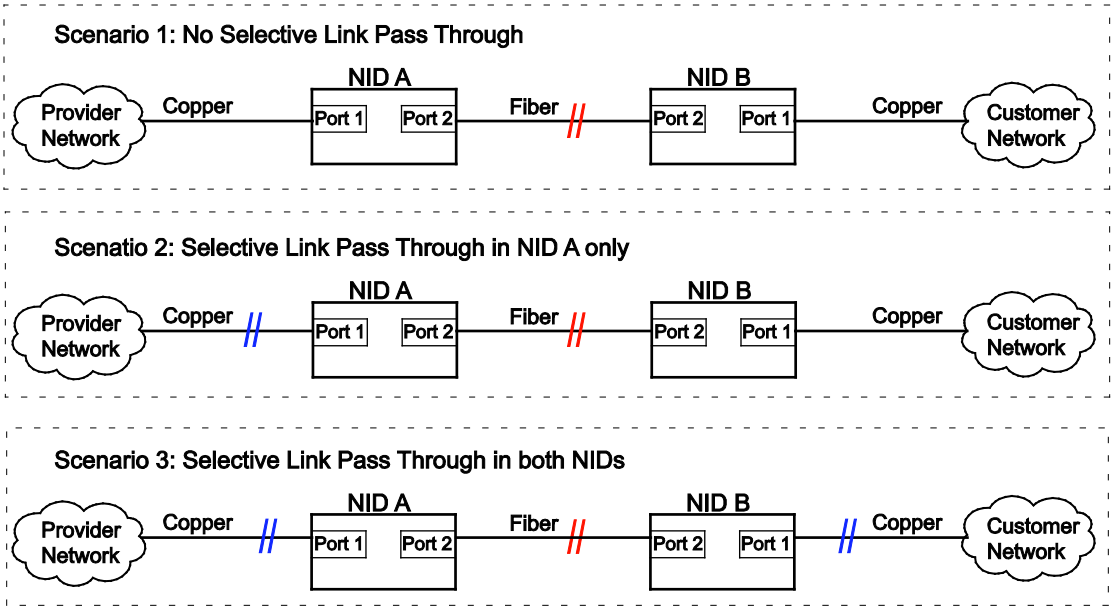


Figure 19: Selective Link Pass Through (SLPT)

The three scenarios shown in the figure above are explained as follows:

- Scenario 1 – If Selective Link Pass Through is not in either of the NIDs and the fiber link goes down, neither network is notified of the problem.
- Scenario 2 – If the fiber link goes down, NID A stops transmitting over its copper port (port 1). The provider network is thus notified that a problem exists. Once the fiber link is restored, the NID will resume transmitting over the copper link.
- Scenario 3 – If the fiber link goes down, each NID stops transmitting over its copper port, thus notifying their respective networks that a problem exists. Once the fiber link is restored, the NIDs will resume transmitting over the copper links.

Transparent Link Pass Through monitors the remote copper port (Port 1) of a NID. It the fiber link is lost, a link-loss signal is sent instructing the remote NID to shut down the copper port thus notifying the end device, while maintaining the fiber link between the two NIDs.

Note: Transparent Link Pass Through is active only when LOAM is active between the peers.

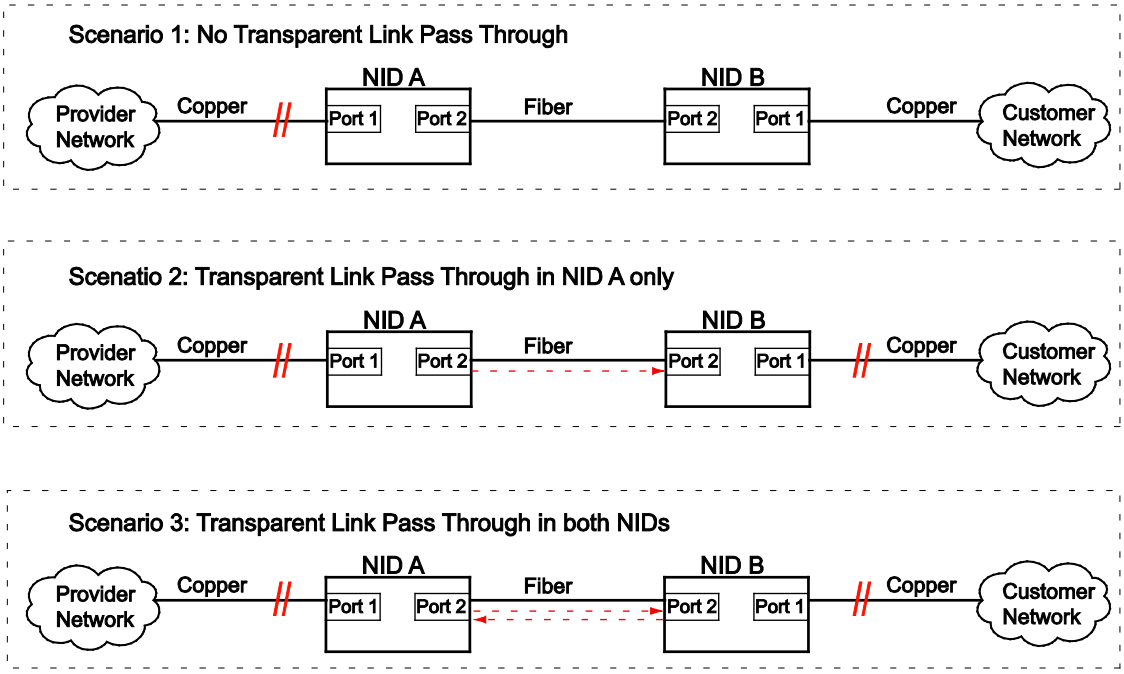


Figure 20: Transparent Link Pass Through (TLPT)

The three scenarios shown in the figure above are explained as follows:

- Scenario 1 – If Transparent Link Pass Through is not in either of the NIDs and the copper link on NID A goes down, the customer network connected to NID B is not notified of the problem.
- Scenario 2 – If the copper link (port 1) of NID A goes down, then NIB B is notified and it brings down its copper port. Once the copper link on NID A is restored, NID B will resume transmitting over its copper port.
- Scenario 3 – If the copper port (port 1) on either NID is lost, the other NID is notified and it brings down its copper port. Once the original link is restored, the other NID will resume transmitting over its copper port.

Note: Link Pass Through – SLPT or TLPT, or both - can be configured via the CLI method or via the Web interface.

Link Pass Through Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable the Link Pass Through capability.
   - For Selective Link Pass Through, type **set selective lpt state=enable** and press **Enter**.
   - For Transparent Link Pass Through, type **set transparent lpt state=enable** and press **Enter**.
3. Define the port to be monitored. Type:

   set lpt monitor-port=<xx>

   where:

   xx = the port to be monitored. **Note:** this should always be the port that the fiber cable is connected to.
4. Was Transparent Link Pass Through enabled?

Yes	**No**
Continue with step 5 below.	Go to step 9 below.

5. Go to the port where the fiber cable is connected. Type:

   go l<x>**p**=<y>

   where:

   x = the hierarchical level of the device:**1**, **2** or **3**

   y = the port number. **Note:** it is recommended that this be the port that the fiber cable is connected to.
6. Check whether LOAM is enabled and active. Type: **show loam config** and press **Enter.**

7. Is the LOAM admin state enabled?

Yes	**No**
Continue with step 8.	a) Type: **set loam admin state=enable** b) Press **Enter**. c) Continue with step 8.

8. Is the LOAM mode active?

Yes	**No**
Continue with step 9.	a) Type: **set loam mode=active** c) Press **Enter**. c) Continue with step 9.

9. Verify the configuration has been set.

   a) Type: **show loam config**

   b) Press **Enter**.

   c) Go to the device level.

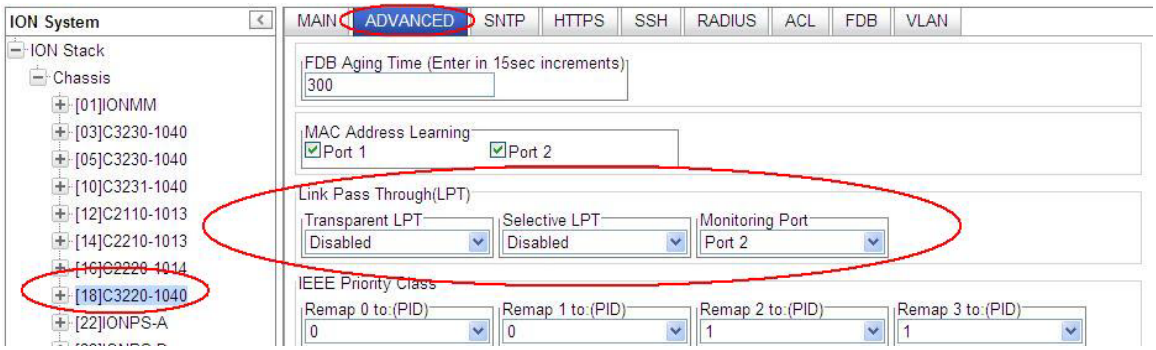
   d) Type: **show lpt config**.

   d) Press **Enter**. Examples of LOAM and LPT commands and displays are shown below:

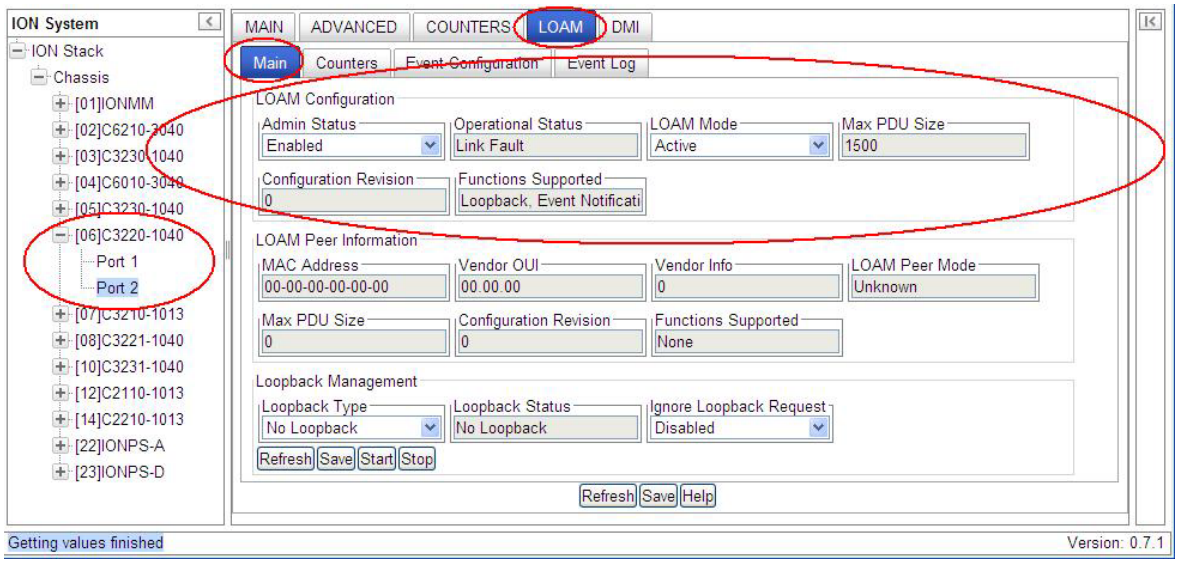
```
C1|S3|L1P1>set loam mode active
C1|S3|L1P1>set loam admin state enable
C1|S3|L1P1>show loam config
Link OAM configuration:
------------------------------------------------------------------------
Link OAM admin state:         enable
Link link OAM operation status:linkFault
Link OAM mode:                active
Link OAM maxium PDU size:     1500
Link OAM configuration revision:1
Link OAM function supported:  loopbackSupport+eventSupport
C1|S3|L1P1>go l1d
C1|S3|L1D>show lpt config
Link pass through configuration:
------------------------------------------------------------------------
Link pass through state:                enable
Transparent link pass through state:    notSupported
Selective link pass through state:      notSupported
Link pass through monitor port:         0
Remote fault detect state:              notSupported
C1|S3|L1D>
```

Link Pass Through Config – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **ADVANCED** tab and locate the **Link Pass Through (LPT)** section.



3. In the **Transparent LPT** field, select **Enabled**.
4. In the **Selective LPT** field, select **Enabled**.
5. In the **Monitoring Port** field, select the port to be monitored. **Note:** it is recommended that this be the port to which the fiber cable is connected.
6. Click **Save**.
7. In the ION Stack tree, select the port that was set as the monitoring port (Port 2 in this example).
8. Select the **LOAM** tab, select the **Main** sub-tab, and locate the L**OAM Configuration** section.



9. Is **Admin Status** set to **Enabled**?

Yes	**No**
Go to step 10 below.	a) Set the **Admin Status** field to **Enabled**. b) Click **Save**. c) Go to step 10 below.

10. Is **OAM Mode** set to **Active**?

Yes	**No**
Procedure complete.	a) Set the **LOAM Mode** field to **Active**. b) Click **Save**. c) Procedure complete.

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

Configure Forwarding Learning (FDB) Aging Time

This function allows setting and viewing the aging time (in seconds) for entries in the forwarding database (FDB) of the switch. The Aging Time must be entered in 15 second increments (e.g., 15, 45, 300 seconds, etc.). The aging time is the number of seconds an entry will be kept in the forwarding database.

The aging time is the number of seconds a MAC address will be kept in the forwarding database after having received a packet from this MAC address. The entries in the forwarding database are periodically timed out to ensure they do not stay around forever.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance.

Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned.

While the x222x / x32xx can learn up to 8192 entries, there is a limit of 1000 entries that it can manage via the Web/CLI/FP interfaces. So even if the NID learns more than 1000 entries, only 1000 entries (including static entries) can be displayed/managed though the x222x / x32xx interface (as limited by x222x / x32xx memory space and CPU capability).

Forwarding Learning (FDB) Aging Time Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).

2. Set the aging time of a bridge on a device. Type **set dot1bridge aging-time**=ag-time

   where:

   ag-time= the Aging Time for how long (from 0-3825 seconds) entries are to remain in the forwarding database (FDB) of the switch, in 15 second increments (e.g., 15, 45, 300 seconds, etc.). The default is 300 seconds. The valid range is 0– 3825 seconds (63.75 minutes).

3. Press **Enter**. The dot1 bridge aging time is set.

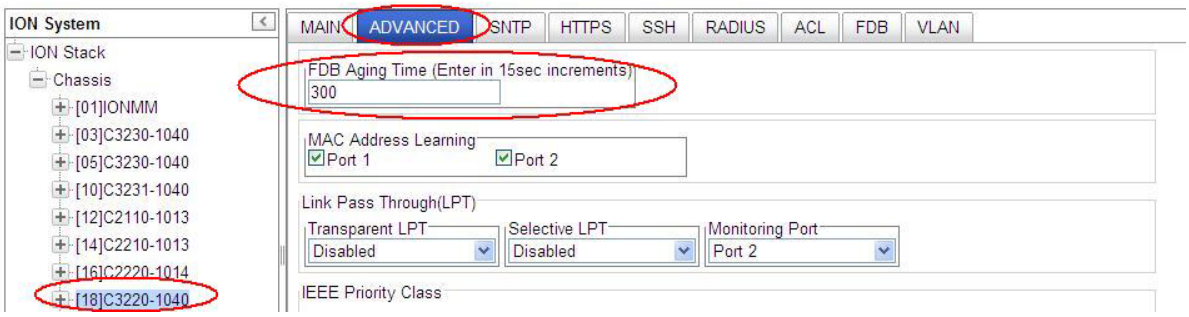
4. Verify the dot1 bridge aging time setting. Type **show dot1bridge aging-time** and press **Enter**. The dot1 bridge aging time is displayed. For example:

```
AgentIII C1|S16|L1P1>set dot1bridge aging-time=60
Error: this command should be executed on a device!
AgentIII C1|S16|L1P1>go l1d
AgentIII C1|S16|L1D>set dot1bridge aging-time=60
AgentIII C1|S16|L1D>show dot1bridge aging-time
Dot1bridge aging time:                  60
AgentIII C1|S16|L1D>
```

FDB Aging Time Config – Web Method

The Forwarding Learning - Aging Time is the number of seconds an entry will be kept in the forwarding database (FDB).

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **ADVANCED** tab and locate the **FDB Aging Time** field.



3. Enter the Aging Time (in seconds) for how long you want entries to remain in the forwarding database (FDB) of the switch, in 15 second increments (e.g., 15, 30, 45, 300 seconds, etc.). The default is 300. The valid range is 0 seconds – 3825 seconds (63.75 minutes).
4. Click the **Save** button near the bottom of the screen. When the" *Setting values succeeded*" message displays, the entry is accepted and the procedure is complete.

Configuring SNTP

IMPORTANT

If the NID is managed by the ION Management Module (IONMM), configuring SNTP should be done at the IONMM and not at the NID.

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 x222x / x32xx NID supports only client implementations of SNTP. You can use the client implementation of SNTP to synchronize the clock on the x222x / x32xx NID with 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 NID using either the CLI or Web method.

SNTP Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable SNTP. Type: **set sntp state=enable**
3. Press **Enter**.
4. Set the current time. Type: s**et curr–time=<"**xx**">** where:

   xx = the current date and time in the format "yyyymmdd hh:mm:ss". **Note:** the entire string must be enclosed in quotes.

5. Press **Enter**.
6. Set your timezone. Type: **set sntp timezone=<**xx> where:

   xx = a number indicating the time zone. See the table below.

Table 14: 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, Wellington
63 (GMT +12:00) Fiji, Kamchatka, Marshall, Islands

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

Yes	**No**
Continue with step 8 below.	Go to step 16 of this procedure.

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 "yyyymmdd 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 "yyyymmdd 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>

    where:

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

    yy = IP address format; valid choices are:

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

    zz = IP address of the server

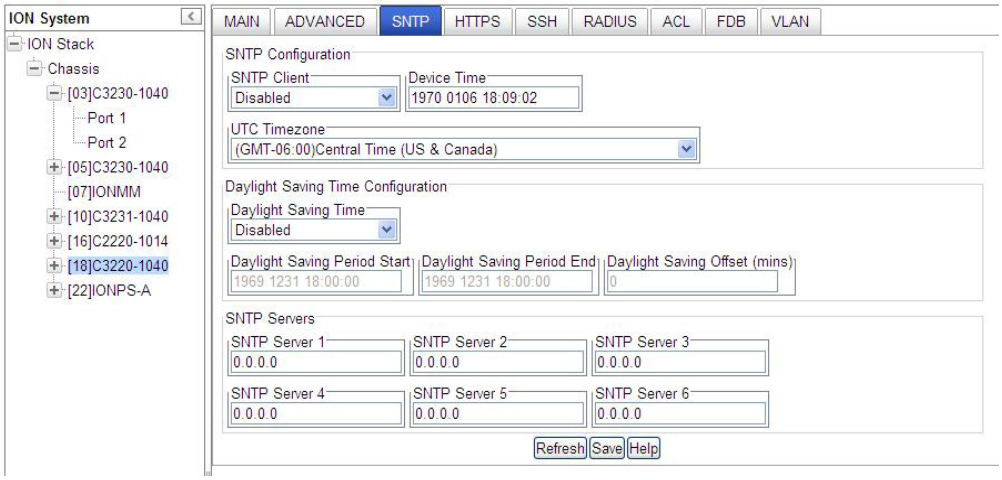
17. Press **Enter**.
18. Verify the configuration has been set. Type: **show sntp config**
19. Press **Enter**. The SNTP Configuration displays. For example:

```
C1|S3|L1D>set sntp state=enable
C1|S3|L1D>set curr-time=”20100106 13:15:30”
C1|S3|L1D>set sntp timezone=8
C1|S3|L1D>set sntp dst-state=enable
C1|S3|L1D>set sntp dst-start=”20100307 02:00:00”
C1|S3|L1D>set sntp dst-end=”20101107 02:00:00”
C1|S3|L1D>set sntp dst-offset=60
C1|S3|L1D>set sntp-svr svr=1 type=ipv4 addr=192.168.1.20
C1|S3|L1D>show sntp config
SNTP configuration:
------------------------------------------------------------------------
SNTP state:                             enable
SNTP daylight saving time state:        disable
Sntp timezone:                          (GMT-6:00) Central Time US and Canada
Current time:                           1970 0103 11:42:26
Sntp daylight saving start time:        1969 1231 18:00:00
Sntp daylight saving end time:          1969 1231 18:00:00
sntp daylight saving offset:            60

Sntp server:
index               addr-type           address
------------------------------------------------------------------------
1                   ipv4                192.168.1.30
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|S3|L1D>
```

SNTP Config – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **SNTP** tab.



3. In the **SNTP Client** field select **Enabled**.
4. In the **Device Time** field, enter the current time in the format *yyyymmdd hh:mm:ss*.
5. In the **UTC Timezone** field, select your timezone.
6. Do you want to set daylight savings time (DST)?

Yes	**No**
Continue with step 7.	Go to 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). This is usually set to 60 minutes. When SNTP Client and DST are Enabled and current time at Daylight Saving Period, the current time of the switch will be offset by the entry here
11. Enter the IP address of each SNTP Server - the IPv4 or IPv6 address of DNS server(s).
12. Click the **Save** button when done.

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 15: 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 can not 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 can not use their SNMP login credentials to log in to the ION Web/CLI (and vice-versa). See "Configuring SNMP Users" on page 104 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 x222x/x32xx via either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).

2. Check the existing set of system users. At the device's command prompt type **show sysuse**r 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 = <**admin**istrator, **read-writ**e, or **read-only**>

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

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

4. Press the **Enter** key.

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

   where:

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

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

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

   where:

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

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

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

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

For example:

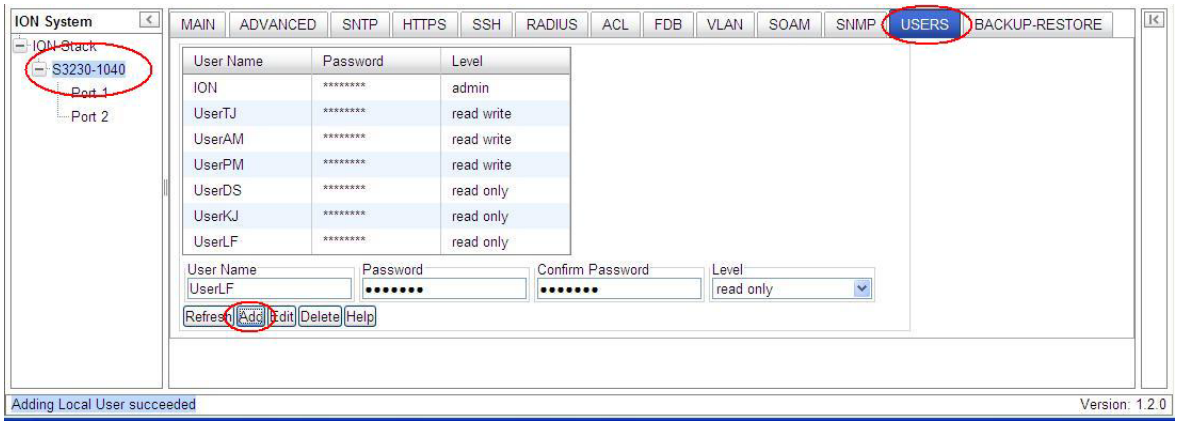
```
S3220-1040 C0|S0|L1D>show sysuser
name                    level           password
ION                     admin           ********
S3220-1040 C0|S0|L1D>add sysuser name AndersonT level read-only pass ******** confirmpass ********
S3220-1040 C0|S0|L1D>add sysuser name BensonJ level read-only pass ******** confirmpass ********
S3220-1040 C0|S0|L1D>add sysuser name CarlsonAnn level read-only pass ******** confirmpass ********
S3220-1040 C0|S0|L1D>add sysuser name CarlsonAndy level read-only pass ******** confirmpass ********
S3220-1040 C0|S0|L1D>add sysuser name Fitz level read-only pass ********** confirmpass **********

S3220-1040 C0|S0|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       ********
S3220-1040 C0|S0|L1D>
```

8. Backup the configuration. See “Backup and Restore Operations (Provisioning)” on page 324.

Configuring System / Login Users - Web Method

1. Access the 222x/32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. At the **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.

Changes to Existing ION Applications with IPv4 / IPv6

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

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

Dynamic Table Entry Limits

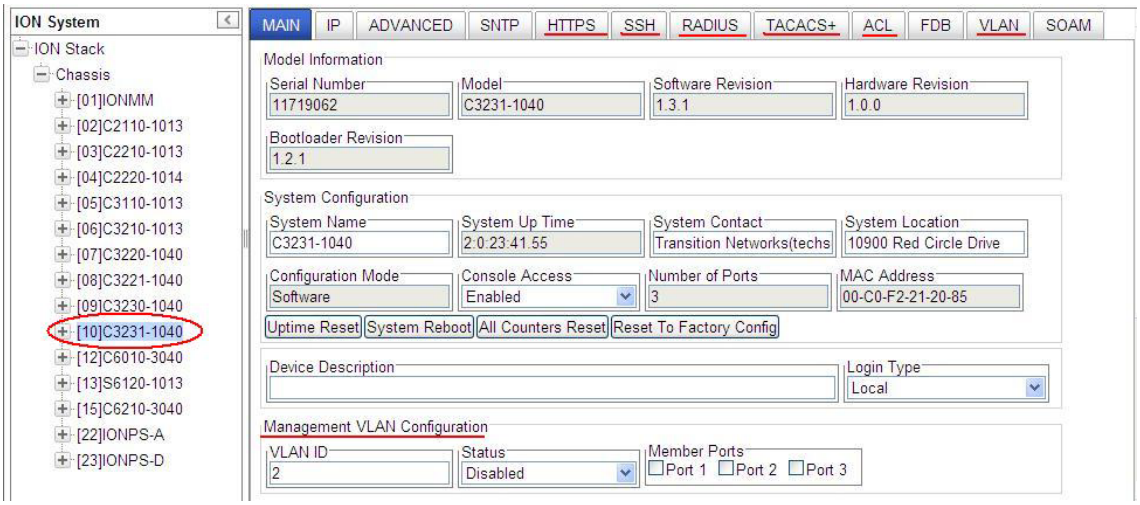
Theses IPv6 changes bring the entry limitations for several dynamic tables shown below.

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

Configuring Security Features

One or more of the following can be defined for the x222x / x32xx NID:

- Access Control List (ACL)
- Hypertext Transfer Protocol Secure (HTTPS)
- Media Access Control (MAC) addressing
- Remote Authentication Dial In User Service (RADIUS)
- Terminal Access Controller Access Control System (TACACS+) authentication, authorization and accounting services from the **TACACS+** tab.
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Virtual LANs (VLANs)



Configuring an ACL

IMPORTANT

- If the NID is managed by the ION Management Module (IONMM), configuring ACL should be done at the IONMM and not at the NID.
- An ACL does not control access to the NID through a serial interface (USB connection).
- 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.
- Configure both a rule and a condition; even if a rule is configured without a condition, the top ACL condition applies to all packets.
- The x222x / x32xx NIDs do not support two ACL conditions with the same condition type.

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.

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 x222x / x32xx NID is INPUT. This chain contains the rules and conditions for accessing the NID through an Ethernet connection (via 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 x222x / x32xx NID:

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

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

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

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

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

For IPv6:

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

For IPv4:

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

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

ACL Config – CLI Method

For a complete list of all CLI commands for ACL operations see the *ION System CLI Reference Manual, 33473*.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable ACL. Type: set acl state=enable and press **Enter**.
3. Define the default chain policy. **Note:** the factory 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)
   - **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>

   where:

   ww = what the condition applies to; 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 **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 6 and 7 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 (head) or end (tail) 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 of times (1–65535) 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**. The Condition List index information displays (e.g. *cond_list=1*).
10. Repeat steps 9 and 10 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|S13|L0D/>set acl state=enable
C1|S13|L0D/>set acl table=filter chain=input policy=accept
C1|S13|L0D/>add acl condition type=ipv4addr srcdst=src oper=equal value=192.168.1.30
C1|S13|L0D/>add acl condition type=ipv4addr srcdst=src oper=notequal value=192.168.1.30
C1|S13|L0D/>add acl rule position=head table=filter chain=input policy=accept condition=1 condlist=1
C1|S13|L0D/>add acl rule position=tail table=filter chain=input policy=trap condition=2 condlist=2
C1|S13|L0D/>show acl rule
index table-type   chain-type   policy    traprate  conditions
-------------------------------------------------------------------------------
1      filter       input       drop        no          2
2      filter       input       accept      no          1
3      filter       input       trap        100         4
```

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:

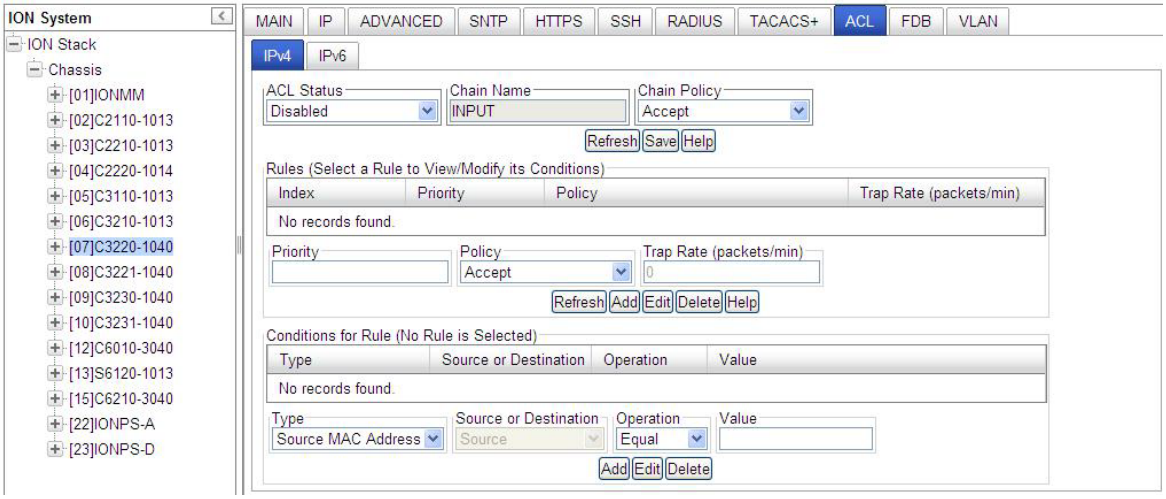
```
C1|S7|L1D>show acl condition
index      type           src/dst   operation  value          rule idx
-------------------------------------------------------------------------------
1          ipv4addrsrc       equal      172.11.1.1  0
2          ipv4addrsrc       equal      192.168.1.30       1
```

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
```

ACL Config (IPv4) – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **ACL** tab.



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 in one minute. This is the trap rate of rule if this rule is a used for trap. The valid range is from 1 - 65,535 packets/minute. The default is 1 packet/minute.

The **Trap Rate** field is only valid if:

- The policy selected is **Trap**.
- A trap server (Trap Manager) is defined on the device's **MAIN** tab.
- A trap server is on the network and available.

d) Click **Add**.

7. Define additional rules as needed.
8. Define a condition for the Rule:

a) Select a rule by clicking its index number.

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. This is the restriction stream for source or destination.

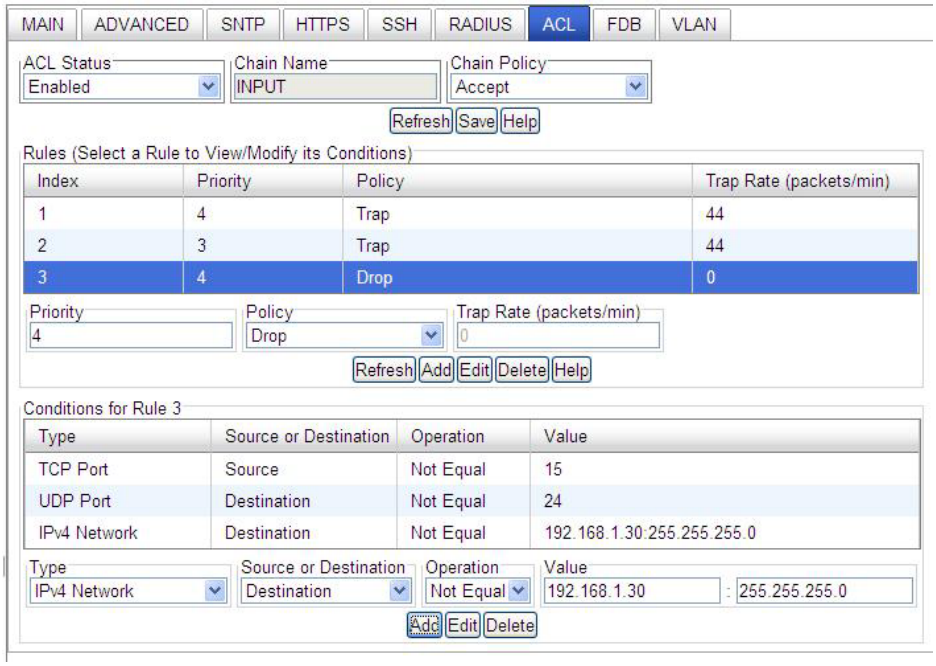
d) In the **Operation** field, select whether the match for this condition is equal to type or not equal to type. Select ***Equal*** or ***Not Equal***. This is the operation between the Condition Type and Value.

e) In the **Value** field, specify the MAC address, IP 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**.

9. Define additional conditions as needed.
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 newly-defined Rules and Conditions.



12. When 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” on page 23) or a Telnet session (see “Starting a Telnet Session” on page 24).
2. Enable ACL. Type: **set ip6tables acl state** and press **Enter**.
3. Define the default chain policy. Type: **set ip6tables acl table=filter chain=input policy=accept** and press **Enter**.
4. Define a condition that will be associated with a rule. Type: **set ip6tables acl condition=1 rule_index=1** and press **Enter**.
5. Repeat step 4 for each condition to be defined.
6. Define a rule to be associated with the chain. Type: **add ip6tables acl rule position=head table=filter chain=input policy=1 trap=444** and press **Enter**.
7. Repeat step 6 to define a rule for each condition to be associated with the chain.
8. Verify that ACL has been enabled. Type: **show ip6tables acl state** and press **Enter**. The current ACL management state information displays:

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

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

```
Agent III C1|S9|L1D>set ip6tables acl state=enable
Agent III C1|S9|L1D>set ip6tables acl table=filter chain=input policy=accept
Agent III C1|S1|L1D>add ip6tables acl rule position=head table=filter chain=input
policy=1 trap=444
Agent III C1|S1|L1D>add ip6tables acl rule index=2 table=filter chain=input
prio=2 policy=trap traprate=100
Agent III C1|S1|L1D>set ip6tables acl condition=1 rule_index=1
Agent III C1|S1|L1D>add ip6tables acl condition type= ipv6addr srcdst=src
oper=equal value=VAL
Agent III C1|S1|L1D>show ip6tables acl rule
index    table-type   chain-type   priority  policy  traprate(pkts/min)   condi-
tion
```

```
-------------------------------------------------------------------------------
----
2         filter         input          1      trap      0                no
1         filter         input          2      trap      0                no

Agent III C1|S1|L1D>
```

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

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

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

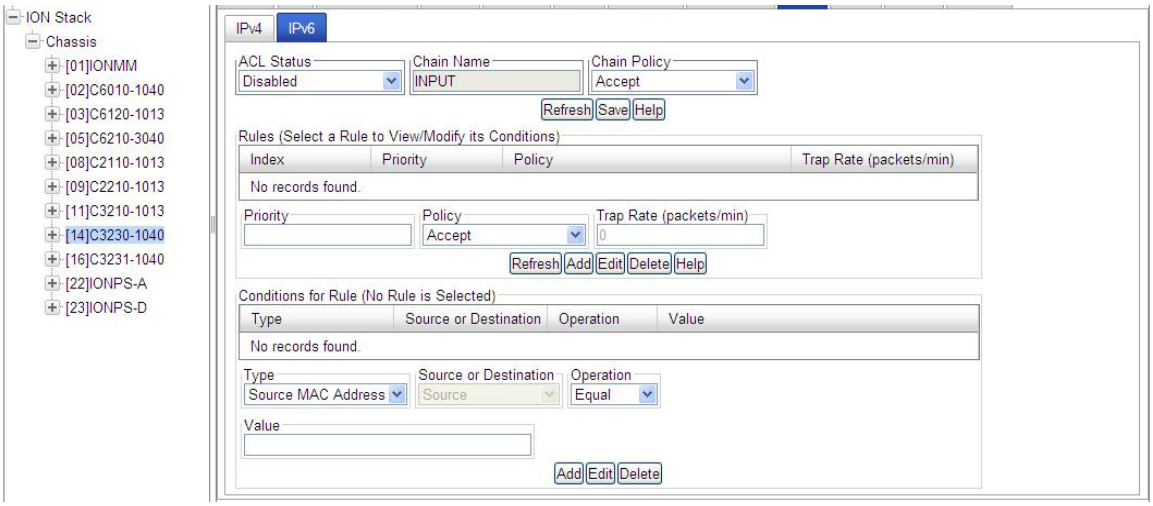
11. To verify the ACL chain configuration, type **show ip6tables acl chain** and press **Enter**. The current ACL chain displays. For example:

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

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

ACL Config (IPv6) – Web Method

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



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

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

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.

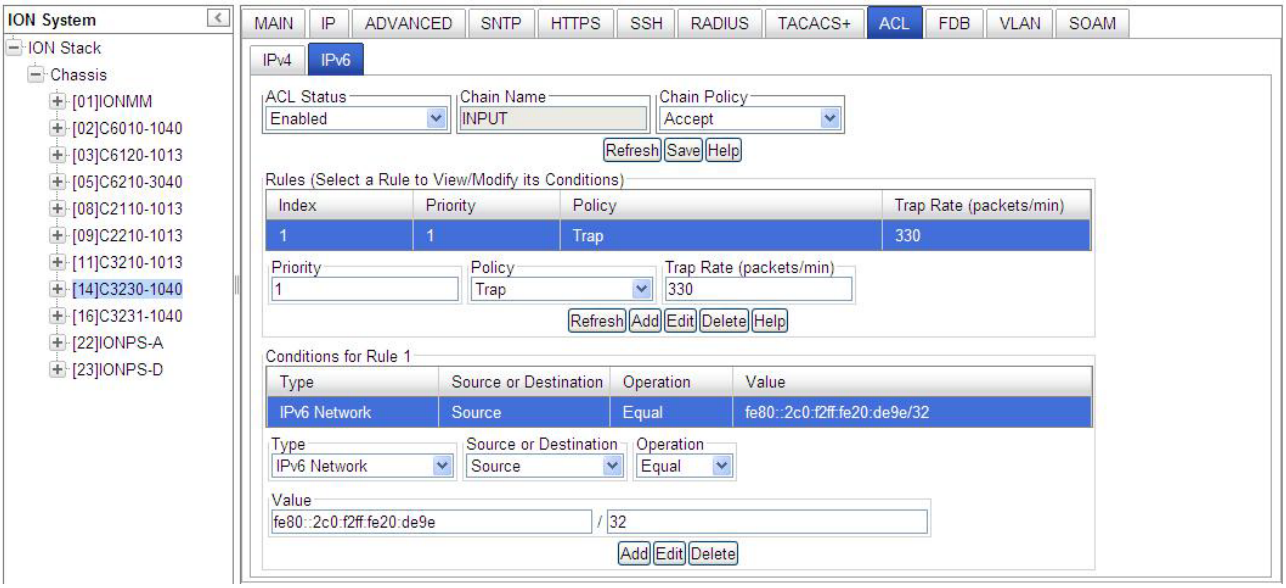
IPv6 Condition Type Values

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.



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

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.

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.

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 secure socket layer (SSL) 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 NID, HTTPS can be used for client authentication in order to limit access to the NID 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.

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 NID using either the CLI or Web method.

HTTPS Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable HTTPS. Type **set https state=enable** and press **Enter**.

   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. Set the port number to be used. The default is 443. Type **set https port=**<xx> and press **Enter**.
4. 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–certificated**
5. Press **Enter**.
6. Specify the name of the certificate file. Type: **set https certificate–file=**<xx> where:

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

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

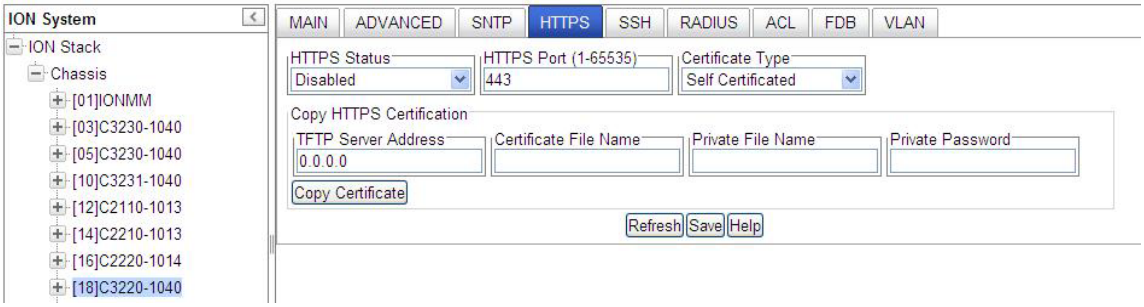
    The current HTTPS configuration table displays. For example:

```
C1|S8|L1D>set https state=enable
C1|S8|L1D>set https port=443
C1|S8|L1D>set https certificate-type=authorized
```

```
C1|S8|L1D>set https certificate-file-name=name.cer
C1|S8|L1D>set https private-key file-name=name.key
C1|S8|L1D>set https private-key password
Please input password:
xxxxxxx
Please input password again:
xxxxxxx
C1|S8|L1D>show https config
HTTPS configuration:
-----------------------------------------------------------------
HTTPS state:                  disable
HTTPS port:                   443
HTTPS certificate file:
HTTPS private key file:
```

HTTPS Config – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **HTTPS** tab.



3. In the **HTTPS Status** field, select **Enabled**. The default is **Disabled**.

   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.
5. At the **Certificate Type** dropdown, select either **Self Certificated** or **Authorized**.
6. In the **TFTP Server IP Address** field, enter the IP address of your remote TFTP server (or client). This entry must be an IP address or a domain name.
7. 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*).

8. In the **Private File Name** field, enter the name of the private key file.
9. In the **Private Password** field, enter the private key password. This is the password to access the private key file.
10. Click the **Copy Certificate** button. The message "*The certificate file(s) is being copied, please wait...*" displays momentarily.
11. Click the **Save** button. A re-login occurs immediately; and the ION login prompt displays.
12. 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.
13. For subsequent logins, use **https** instead of **http** as the URL prefix (e.g., https://192.168.0.10/web.html).
14. Enter the ION system *User Name* and *Password*. The default entries are case sensitive (**ION** and **private**).

15. Click the **Sign In** button. The **MAIN** screen 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 MAC Address Filtering

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

MAC Filtering can be configured in the NID using either the CLI or Web method.

MAC Address Filtering – CLI Method

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

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable HTTPS. Type **set https state=enable** and press **Enter**.
3. Set the filter for unknown multicasts. Enter **set ether filter-unknown-multicast=(**true|false**)** and press **Enter**.
4. Set the filter for unknown unicasts. Enter **set ether filter-unknown-unicast=(**true|false**)** and press **Enter**.
5. Set the Fwd DB port, priority and type of entry / MAC address database. Type **add fwddb mac=**MAC **[conn-port=**PORT**] [priority=**PRIO] **[type=(**static|staticNRL|staticPA)] and press **Enter**. The priority can be 0-7, where 0 is the lowest priority.
6. Set the Fwd DB index and type. Type the following command:
   set fwddb mac=MAC **index=**INDEX **type**=(static|staticNRL|staticPA) and press **Enter**.

Note: A Static Non Rate Limit (staticNRL) entry must have a multicast MAC address.

FDB Entry Type Notes: The Entry state of this unicast or multicast entry, {static, staticNRL, staticPA, dynamic}:

static - a Valid entry that does not age.

staticNRL - a static entry that has no ingress rate limiting (multicast entry only).

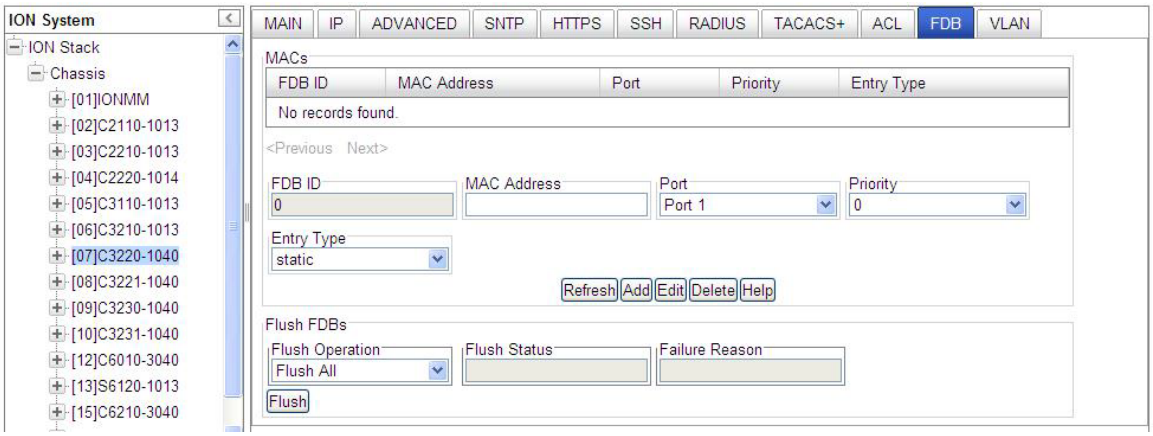
staticPA - a static entry that has priority override enabled.

dynamic -a valid entry with no special attributes which ages and is ultimately removed from the forwarding database.

A unicast entry can be static or staticPA, but not staticNRL. For MAC addresses that are learned, a read-only value of dynamic entry is returned.

MAC Address Filtering – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **FDB** tab.



3. In the **MAC Address** field, enter the MAC address to be filtered. This is the unicast or multicast MAC address associated with this entry.
4. In the **Port** field, select the port to be filtered (Port 1 or Port 2 on the x3230 or x3220, or Port 1, 2 or 3 on the x3221 NID). This is the logical port that this Address is connected.
5. In the **Priority** field, select the priority to be assigned (0-7, where 0 is the lowest priority). The priority specified here is used when Priority Override is enabled.
6. In the **Entry Type** field, select the type of entry / MAC address database. This is used to define the entry state, depending on whether it is a unicast or a multicast address in the entry. The selections are "static", "staticNRL" or "staticPA" ("dynamic" is not selectable).

   Note: A Static Non Rate Limit (**staticNRL**) entry must have a multicast MAC address.

   For Unicast frames:

   static: a static entry, not aged out of the Address database. A valid entry that does not age.

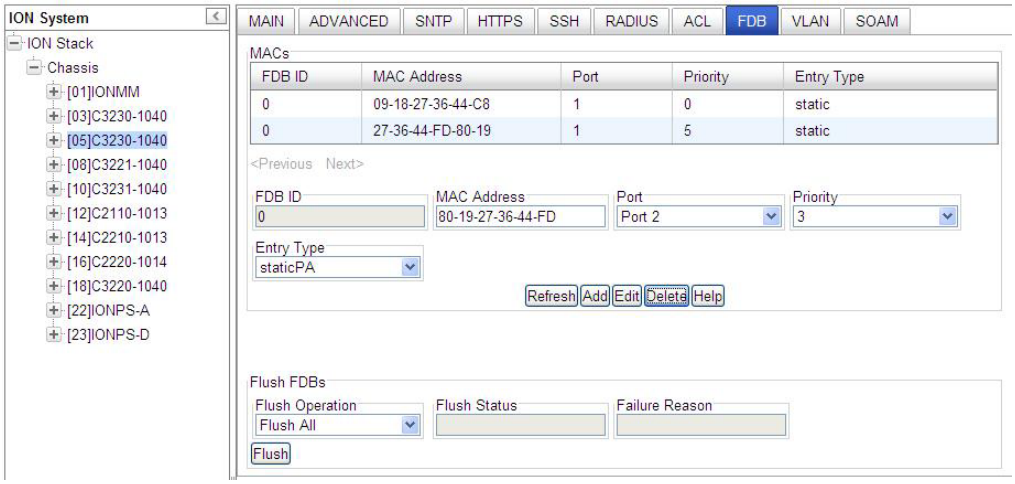
   staticPA (static with priority override): this is a static entry not aged, and the priority (sC3231100FwdPriority) indicates the priority to use for this frame's source/destination address. A static entry that has priority override enabled.

   For Multicast frames:

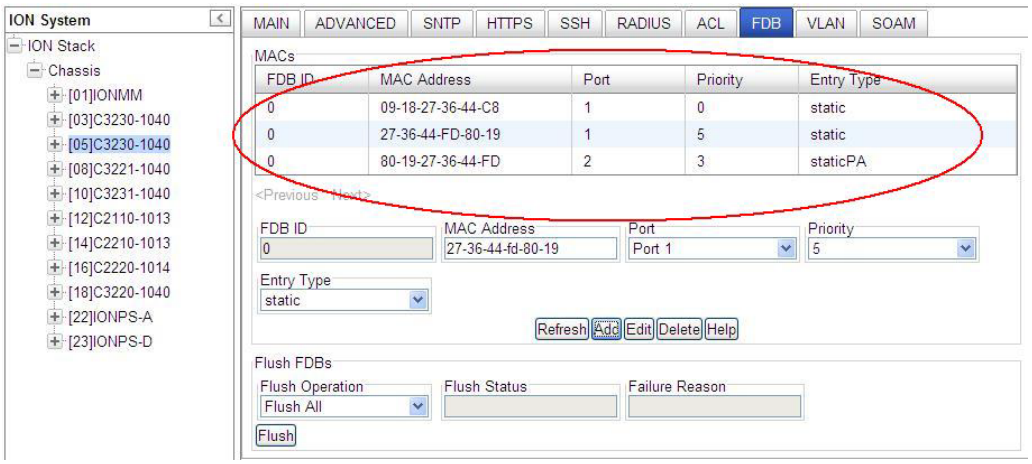
   staticNRL (static with no ingress rate limiting): this entry is a static entry, not aged out of the Address database and not subject to ingress rate limiting. A static entry that has no ingress rate limiting (multicast entry only).

   staticPA (static with priority override): this is a static entry not aged and the priority (sC3231100FwdPriority) indicates the priority to use for this frame's source/destination address.

   dynamic - A valid entry with no special attributes which ages and is ultimately removed from the forwarding database (not selectable; read-only value only).
7. Select the **Add** button. The message "*Adding MAC succeeded*" displays and the entry is added to the MACs table.



7. To edit an existing entry, select the entry and click the **Edit** button.
8. To delete an existing entry, select the entry and click the **Delete** button. The MACs table displays "*No records found.*" in place of the entry.
9. When done, verify your FDB configuration. For example:



Note:

The FDB Entry Type is the state of this unicast or multicast entry (static, staticNRL, staticPA, or dynamic). The **dynamic** parameter is a valid entry with no special attributes which ages and is ultimately removed from the forwarding database. The **dynamic** parameter is read-only and cannot be selected.

A unicast entry can be **static** or **staticPA**, but not **staticNRL**. For MAC addresses that are learned, a read-only value of **dynamic** entry is returned.

Configuring MAC Address Blocking

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

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

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

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

MAC Address Blocking – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Use the **go** command to access the desired port.
3. Enable the Ethernet Source Address Lock. Type: **set ether src-addr-lock=enable** and press **Enter**.
4. Select the Ethernet Source Address Lock Action. Type: **set ether src-addr-lock action=x**

   where:

   x = the SA lock action to perform = {all | discard | discardandnotify | shutdown }

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

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

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

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

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

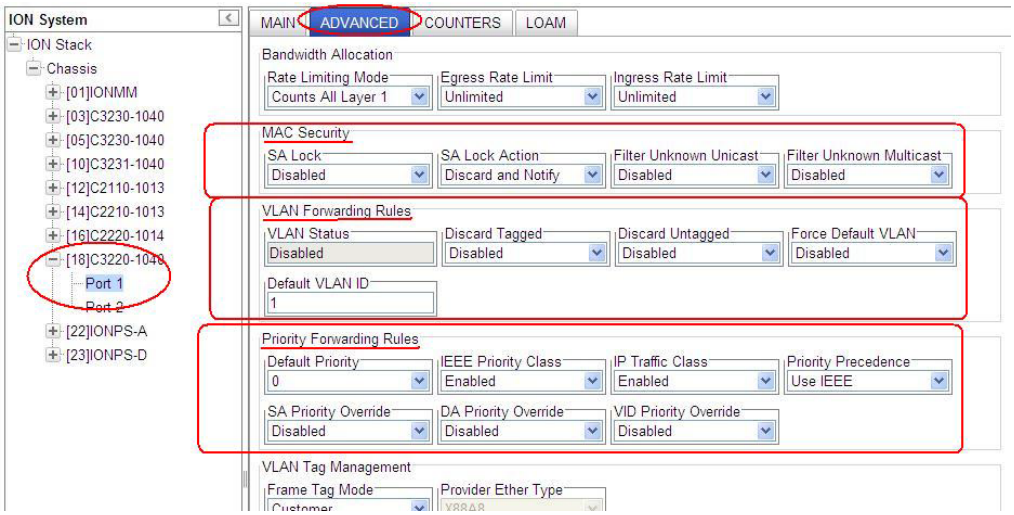
6. Verify the security configuration. Type **show ether security config** and press **Enter**.

   The Ethernet Port Security configuration table displays. For example:

```
C1|S13|L1P1>set ether src-addr-lock=enable
C1|S13|L1P1>set ether src-addr-lock action=discardandnotify
C1|S13|L1P1>show ether security config
Ethernet port security configuration:
------------------------------------------------------------------------
Source MAC address lock:           enable
Source MAC address lock action:    discardandnotify
Filter unknown dest unicast:       enable
Filter unknown dest multicast:     disable
```

MAC Address Blocking – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the desired port.
3. Select the **ADVANCED** tab.



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

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

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

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

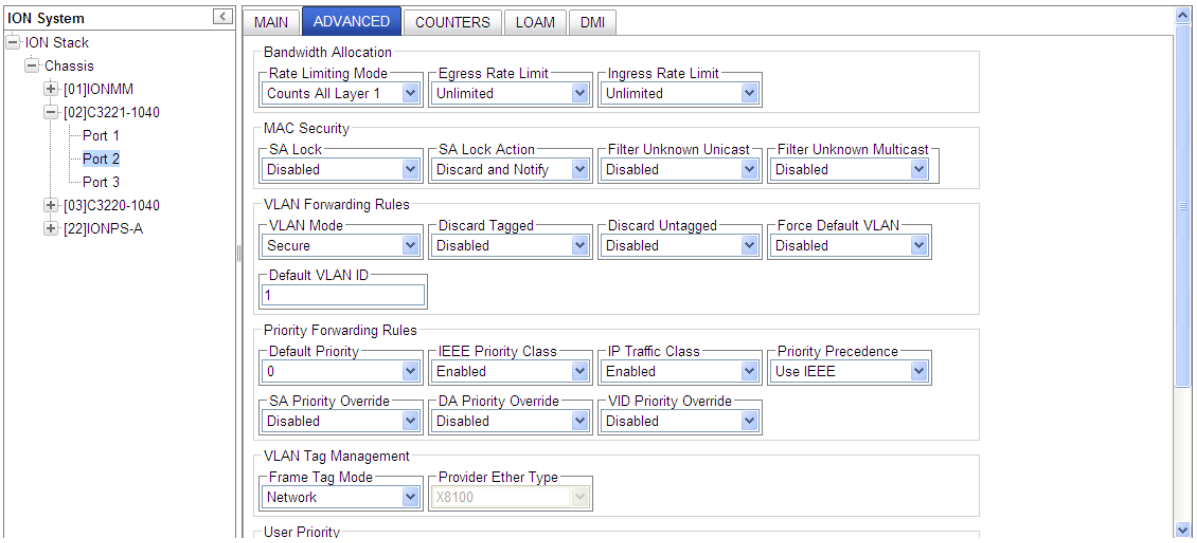
   Shutdown: This will shut down the interface on receiving the frame.

   All: All the above actions take place. The frame is discarded, a trap is sent and the port is shutdown to prevent intrusion attack.
7. In the **Filter Unknown Unicast** field, select **Enabled** to filter all unicast frames with an unknown destination address from egressing this Port.
8. In the **Filter Unknown Multicast** field, select **Enabled** to filter all multicast frames with unknown destination address from egressing this Port.

9. Locate the **VLAN Forwarding Rules** section.
10. At the **Discard Tagged** field, select Enabled or Disabled. At **Discard Untagged** select Enabled or Disabled. At **Force Default VLAN** select Enabled or Disabled.
11. Enter a **Default VLAN ID** in the range of 2-4093.
12. Locate the **Priority Forwarding Rules** section.
13. In the **Default Priority** field, select the default priority (**0**-**7**, where 0 is the lowest priority) for frames ingressing this port, if it doesn't have any IEEE 802.3ac tag or any IP TOS/Diffserv traffic class fields.
14. In the **IEEE Priority Class** field, select **Enabled** so that if the frame is IEEE tagged, and this mib variable is set to 'true', the 802.1p bits are used as the frame's priority.
15. In the **IP Traffic Class** field, select **Enabled** so that if the frame has IP TOS/Diffserv traffic class fields, and this mib variable is set to 'true', the traffic class fields will be used as the frame's priority.
16. In the **Priority Precedence** field, select **Enabled** so that if the frame has IP TOS/Diffserv traffic class fields, and IEEE 802.3ac tagged, then 'Priority Precedence' decides which one is to be considered as the frame's priority.
17. In the **SA Priority Override** field, select **Enabled** to let a frame's Source MAC address decide the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.
18. In the **DA Priority Override** field, select **Enabled** to let a frame's Destination MAC address decide the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.
19. In the **VID Priority Override** field, select Enabled to let a frame's VLAN ID (VID) decide the priority of the frame. The new priority value is assigned based on the priority assigned to that VLAN ID in the VLAN database.
20. Click the **Save** button at the bottom of the screen.

Configure VLAN Mode (Secure/Disable/Fallback/Check) via Web GUI

Set x3221 to a transparent LAN service (tagged and untagged traffic) from the C322xx > Port x > VLAN Forwarding Rules > VLAN Mode menu path.



The VLAN table specifies certain forwarding rules for packets that have a specific 802.1q tag. Those rules are of higher priority than switch groups configured using 'master-port' property. The table contains entries that map specific VLAN tag IDs to a group of one or more ports. Packets with VLAN tags leave the switch chip through one or more ports that are set in the corresponding table entry. The specific logic controlling how packets with VLAN tags are treated is controlled by a VLAN Mode parameter that is configurable per switch. This forwarding based on VLAN tag IDs also takes into account the MAC addresses learned or manually added in the host table.

The VLAN Mode parameters are described below.

• **Secure**: drop packets with VLAN tag that is not present in VLAN table. Packets with VLAN tags that are present in the VLAN table, but if an incoming port does not match any port in the VLAN table, then that entry gets dropped.

• **Disable**: ignore VLAN table, treat packet with VLAN tags just as if they did not contain a VLAN tag.
Note: VLAN Mode = Disable and Frame Tag Mode - Customer must be set at the same time.

• **Fallback**: the default mode - handle packets with VLAN tag that is not present in vlan table just like packets without VLAN tag. Packets with VLAN tags that are present in VLAN table, but incoming port does not match any port in VLAN table entry does not get dropped.

• **Check**: drop packets with VLAN tag that is not present in VLAN table. Packets with VLAN tags that are present in VLAN table, but incoming port does not match any port in VLAN table entry does not get dropped. Packets without a VLAN tag are treated just as if they had a VLAN tag with a default port VLAN ID. This means that if VLAN Mode = Check or Secure is to be able to forward packets without VLAN tags, then you must add a special entry to the VLAN table with the same VLAN ID set according to the default VLAN ID.

Message: *Vlan Mode Disable and Frame Tag Mode Customer should be set at same time.*
Meaning: The setting at C322xx > Port x > VLAN Tag Management > Frame Tag Mode must be first set to "Customer". For Frame Tag Mode, Customer VLAN Should Be In Disable Mode.

Configure VLAN Mode (Secure/Disable/Fallback/Check) via Web CLI

Command: **set port dot1-state**

Description: Configure a copper or fiber port's IEEE 802.1q state.

Example: Change the IEEE 802.1q state and show the resulting configuration.

```
Agent III C1|S2|L1P2>set port dot1-state ?
  check
  fallback
  secure
  vlanDisabled
  vlanEnabled
Agent III C1|S2|L1P2>set port dot1-state check
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  check
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              1
Force use default VLAN id:    false
Agent III C1|S2|L1P2>set port dot1-state fallback
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  fallback
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              1
Force use default VLAN id:    false
Agent III C1|S2|L1P2>set port dot1-state secure
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  secure
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              1
Force use default VLAN id:    false
Agent III C1|S2|L1P2>set port dot1-state vlanEnabled
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  secure
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              1
Force use default VLAN id:    false
Agent III C1|S2|L1P2>set port dot1-state vlanDisabled
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  vlanDisabled
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              1
Force use default VLAN id:    false
Agent III C1|S2|L1P2>
```

Configuring Port Forward Management / IP Access Blocking

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

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

Port Forward Management / IP Access Blocking – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Access the desired port.
3. Set the forwarding port list. Type: **set fwd portlist=y**

   where: y = the port number{1, 2, 3}
4. Press **Enter**.
5. Enable port management access. Type **set port mgmtaccess**=z

   where: z = enable or disable port management access.
6. Press **Enter**.
7. View the port list. Type **show fwd portlist** and press **Enter**. The FWD Portlist table displays. For example:

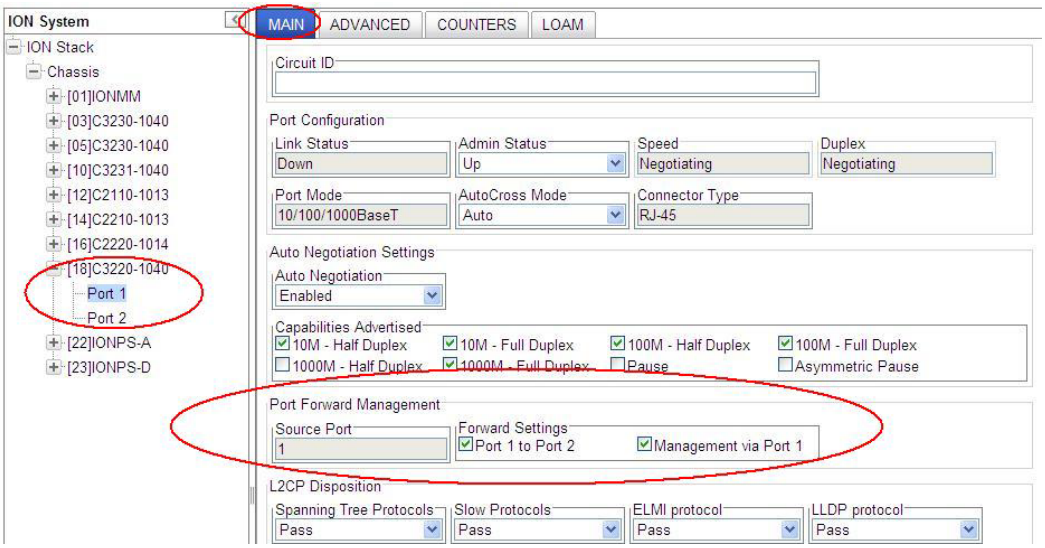
```
C1|S1|L1D>go s=13 l1p=1
C1|S13|L1P1>set fwd portlist 2
C1|S13|L1P1>show fwd portlist
port-id             fwd portlist        mgmt access
-------------------------------------------------------------------------
1                   2                   disable
```

```
C1|S13|L1P1>set port mgmtaccess enable
C1|S13|L1P1>show fwd portlist
port-id             fwd portlist        mgmt access
-------------------------------------------------------------------------
1                   2                   enable
```

```
C1|S13|L1P1>set fwd portlist 2,3
C1|S13|L1P1>show fwd portlist
port-id             fwd portlist        mgmt access
-------------------------------------------------------------------------
1                   2,3                 enable
```

Port Forward Management / IP Access Blocking – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the appropriate port.
3. On the port's **MAIN** tab, locate the **Port Forward Management** section.



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

Configuring RADIUS

IMPORTANT

If the NID is managed by the ION Management Module (IONMM), configuring RADIUS should be done at the IONMM and not at the NID.

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 (called 'clients') to communicate with a central server to authenticate users and authorize their access to the requested system or service.

Transactions between the client (NID) 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 NID and RADIUS server.

From the user's perspective, the entire authentication process takes place seamlessly and transparently. When the user seeks access, the NID, 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 NID.
- Logs, by means of the RADIUS accounting feature, such information as when, how often, and for how long the user logged on.

The NID 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 NID 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 often a background process running on a *UNIX* or *Windows NT* machine.

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

IMPORTANT

After configuring the NID for RADIUS, a re-login occurs immediately; you must then enter the RADIUS defined username and password in order to re-connect to the ION system. This procedure will end your current session, and you must then log in using your RADIUS log in and password.

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 before performing this configuration: After configuring the x222x / x32xx for RADIUS, you will be required to enter the RADIUS defined username and password when connecting to the IONMM.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable RADIUS. Type **set radius client state=enable** and press **Enter**.
3. Define a single RADIUS server. Type:

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

   where:

   vv = RADIUS server number (1–6)

   ww = IP address format; the valid choices are:

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

   xx = RADIUS server IP address

   yy = optional; number of times the access request will be re-sent to the RADIUS server before being discarded or re-directed to another server. The default is 3.

   zz = optional; number of seconds to wait for a response from the RADIUS server before re-sending the request. The default is 30.
4. Define a secret. Type: **set radius svr=<**xx> **secret=<**yy>

   where:

   xx = server number (enter the same as entered in Step 4).

   yy = an alphanumeric text string used to validate communications. Maximum length of the secret is 128 characters.
5. Press **Enter**.
6. Repeat Steps 4 and 5 for each server to be defined. Up to six RADIUS servers can be defined in the system.

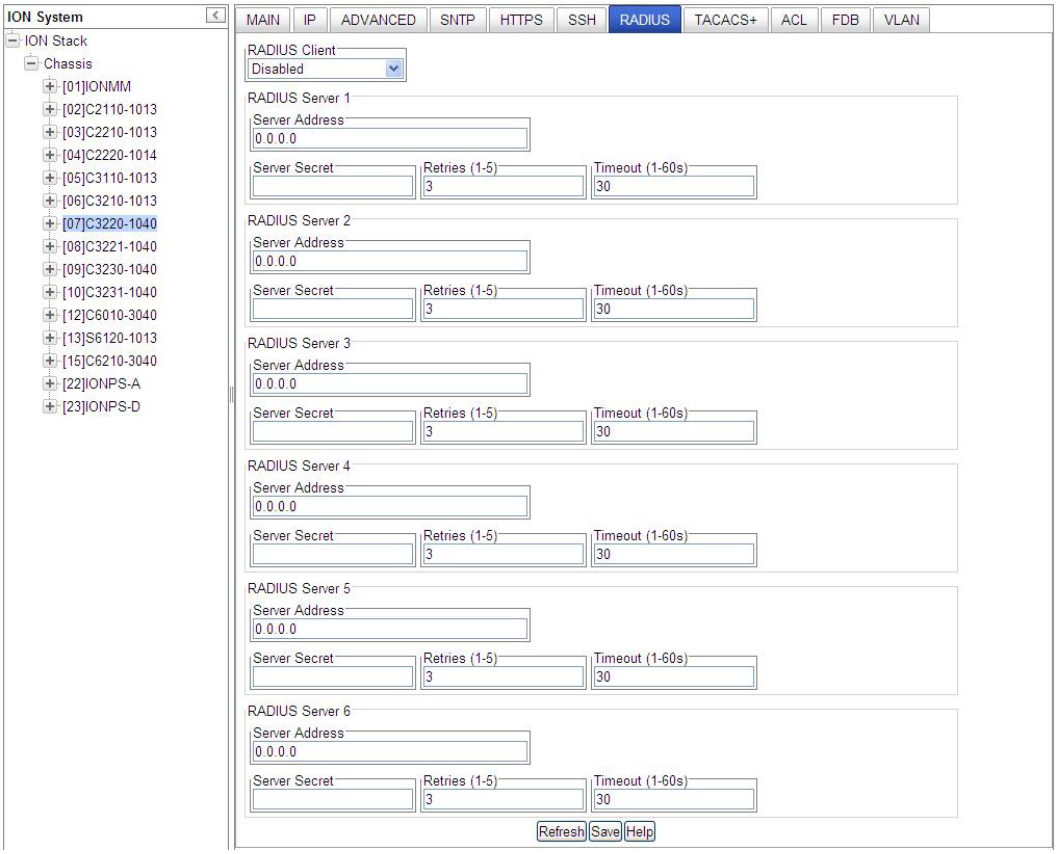
7. Verify that the configuration has been set. Type **show radius config** and press **Enter**.
   The RADIUS Configuration table information displays. For example:

```
C1|S3|L1D>set radius svr=1 type=ipv4 addr=192.168.1.30 retry=2 timeout=15
C1|S3|L1D>set radius svr=1 secret=private
C1|S3|L1D>set radius client state=disable
C1|S3|L1D>show radius config
RADIUS client state:          disable

RADIUS authentication server:
index     addr-type      addr           retry     timeout
-----------------------------------------------------------------
1         ipv4           192.168.1.30   2         15
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
```

RADIUS Config – Web Method

Note before performing this configuration: After configuring the x222x / x32xx for RADIUS, you will be required to enter the RADIUS defined username and password when connecting to the IONMM.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **RADIUS** tab.



3. In the **Radius Client** field, select **Enabled**. The default is **Disabled**.
4. Configure the RADIUS Server.
    - In the **Server Address x** field, enter the IP address of the RADIUS server. This is the IPv4 or IPv6 address of a RADIUS server.
    - In the **Server Secret x** field, enter the secret. It can be written but displays only a series of dots (e.g., ●●●●●).
    - In the **Retries x** field, enter the number of times the access request will be re-sent to the RADIUS server before being discarded or re-directed to another server. This is the maximum number of RADIUS Access-Request packets sent to this server before it times out or receives a response. The factory default is 3. The valid range of entries is from 1-5 retries.
    - In the **Timeouts x** field enter the number of seconds to wait for a response from the RADIUS server before re-sending the request. This is the second number of authentication timeouts to this server. After a timeout, the client may retry to the same server, send to a different server, or give up. The default is 30 seconds. 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 for specific error messages.

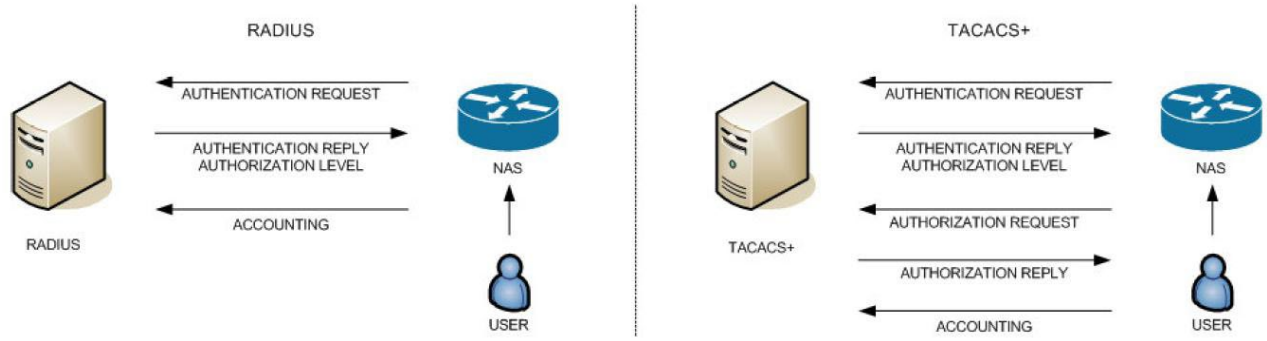
Configuring TACACS+

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, RE-START, ERROR, and FOLLOW.

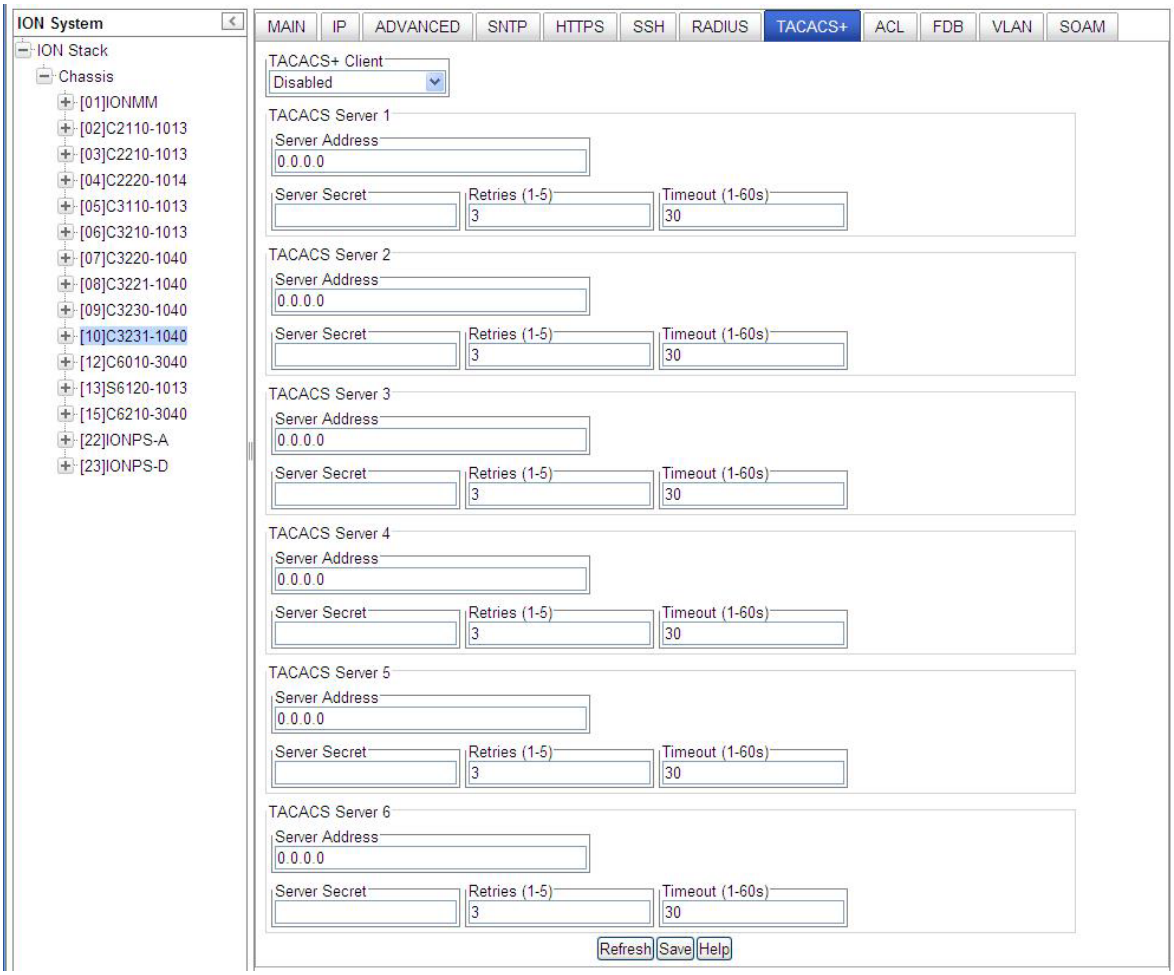
The authen_method indicates the authentication method used by the client to acquire the user information. These methods can include NOT_SET, NONE, KRB5, LINE, ENABLE, LOCAL, TACACSPLUS, GUEST, RADIUS, KRB4, and RCMD.

- 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 x222x/x3x3x card, navigate to the **TACACS+** tab.



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

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

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

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

TACACS+ Config - CLI Method

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

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 23) or a Telnet session (see “Starting a Telnet Session” on page 24).
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” on page 111.
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 Lantronix 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” on page 111.
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 SSH

IMPORTANT

- If the NID is managed by the ION Management Module (IONMM), configuring SNTP should be done at the IONMM and not at the NID.
- SSH has no affect when accessing the IONMM through either the USB or the Web interface.

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.

SSH is widely used by network administrators to control servers remotely (i.e., a Web server). SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. 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 NID.

For the SSH implementation, the NID 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.

Notes:

- 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.).
- You must install an SSH client on the management station (PC) 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.
- On ION systems, SSH can be configured for either Login/Password authentication or for 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 and then will be prompted for the ION System password.

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

SSH Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable SSH. Type **set ssh server state=enable** and press **Enter**.
3. 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
4. Press **Enter**.
5. Set the retry limit. Type: **set ssh auth–retry=**<xx> where:

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

   xx = type of key to be generated; the valid choices are:
   - **rsa**
   - **dsa**
   - **both**
7. Obtain the public key file using the TFTP **get** command.
8. 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**

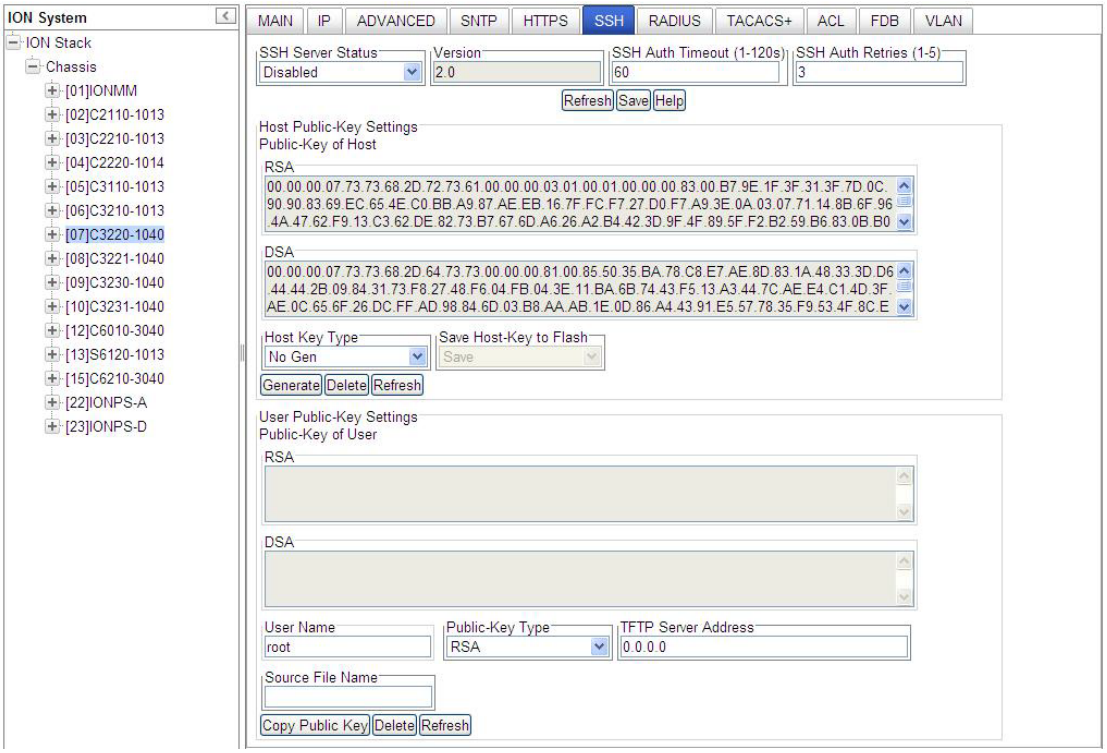
   zz = name of the file that contains the public key
9. Press **Enter**.

10. Verify the configuration has been set. Type **show ssh config** and press **Enter**. The Secure Shell (SSH) configuration table displays. For example:

```
C1|S3|L1D>set ssh server state=enable
C1|S3|L1D>set ssh client timeout=15
C1|S3|L1D>set ssh auth-retry=3
C1|S3|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
C1|S3|L1D>show ssh config
Secure Shell configuration:
-----------------------------------------------------------------
Secure shell server state:                              enable
Secure shell major version:                               2
Secure shell minor version:                               0
Secure shell time out:                                    15
Secure shell authentication retries:                      3
```

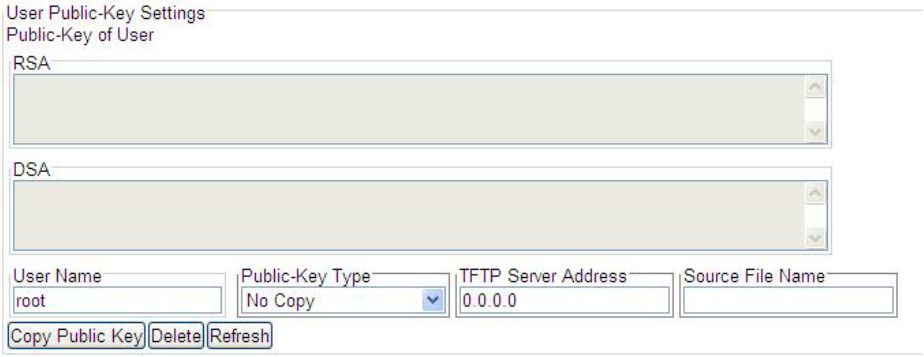
SSH Config – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **SSH** tab.



3. In the **SSH Server Status** field, select **Enabled**. The default is **Disabled**.
4. If SSH is being configured for Login/Password authentication, go to step 10.
   If SSH is being configured for Public/Private key and Certificate, continue with step 5 below.
5. 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.
6. 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. The default is 3 retries.
7. 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 SSH function)
   - **RSA** – generate an RSA key (the generated key will appear in the RSA block)
   - **DSA** – generate a DSA key (the generated key will appear in the DSA block)
   - **Both** – generate both an RSA key and a DSA key
8. Leave the default setting in the **Save Host-Key to Flash** field (for future use).
9. Click the **Generate** button. The message "*The host key is being generated, please wait...*" displays while the host key(s) are generated.

10. Scroll down to the **User Public-Key Settings** section.



11. In the **User Name** field, enter the name of the user to be associated with the user public key. The default user name is **root**.
12. In the **Public-Key Type** field, select one of the following (this is the type of user's public key to be copied or deleted):
    - **No Copy** - no public key is generated (the default)
    - **RSA** - an RSA public key is generated
    - **DSA** - a DSA public key is generated
13. In the **TFTP Server Address** field, enter the IP address of your TFTP server. Note that the TFTP server must be running and configured for the copy process to work.
14. In the **Source File Name** field, enter the name of the file for the public key.
15. Click **Copy Public Key**.
16. At the top of the screen, click **Save** to set the configuration.

You can click the **Delete** button to delete the chosen host key.

You can click the **Refresh** button to refresh the RSA / DSA host key.

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 SNMP

Simple Network Management Protocol (SNMP) is a request-response protocol that defines network communication between a managed device and a network management station (NMS).

The following terms will help in understanding SNMP:

- Managed Device or Agent – A hardware device with embedded firmware connected to a network with SNMP management capabilities. An example of a managed device/agent is the ION Management Module.
- Network Management Station (NMS) – A high-end workstation or computer used by the network administrator to work with and manage various agents around the network.
- Management Information Base (MIB) – A set of variables used to monitor and control a managed device.
- Managed Object or MIB variable – The individual variables that make up the MIB. These variables are the individual features of the managed device. The administrator can use these variables to monitor and configure the managed device. For example, a slide-in module can have up to 20 or more managed objects (MIB variables) associated with it. Some examples are:
  - Power ON/OFF the card
  - Enable the *AutoCross* feature
  - Display activity on the fiber link, etc.
- Trap – A one-way notification from the IONMM 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 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.

See “Supported MIBs” on page 11 for more information.

For information on the traps that the IONMM supports, see “Appendix G: SNMP Traps Supported” on page 543.

The NID 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 accomplished through traps, which are unsolicited messages sent to the management station in response to certain events that have taken place (e.g., cold start, etc.).

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 can not use their SNMP login credentials to log in to the ION Web/CLI (and vice-versa). See “Configuring System / Login Users” on page 104 for information on configuring Web/CLI login users.

SNMP Definition and Description

Simple Network Management Protocol (SNMP) is a request-response protocol that defines network communication between a managed device and a network management station (NMS).

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more." It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

An SNMP-managed network consists of three key components:

1. Managed device(s),
2. Agent - software which runs on the managed devices, and
3. Network management system (NMS) - software which runs on the manager.

The following terms will help in understanding SNMP:

- Managed Device or Agent – A hardware device with embedded firmware connected to a network with SNMP management capabilities. An example of a managed device/agent is the NID.
- Network Management Station (NMS) – A high-end workstation or computer used by a network administrator to work with and manage various agents around the network.
- Management Information Base (MIB) – A set of variables used to monitor and control a managed device.
- Managed Object or MIB variable – The individual variables that make up the MIB. These variables are the individual features of the managed device. The administrator can use these variables to monitor and configure the managed device. For example, a slide-in module can have up to 20 or more managed objects (MIB variables) associated with it. Some examples are:
  - Power ON/OFF the card,
  - Enable the *AutoCross* feature,
  - Display activity on the fiber link, etc.
- Trap – 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.

An ION NID can act as an agent in an SNMP environment, enabling the NID to notify the management station (PC) of significant events within the network. Notification is accomplished through traps, which are unsolicited messages sent to the management station in response to certain events that have taken place (e.g., cold start, etc.).

Management Information Base (MIB)

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

MIBs use the notation defined by ASN.1; for example:

1.3.6.1.4.1.868 Transition Network private MIB root OID

A MIB Example - ionDevSysCfgTable

A sample MIB tree is shown below.

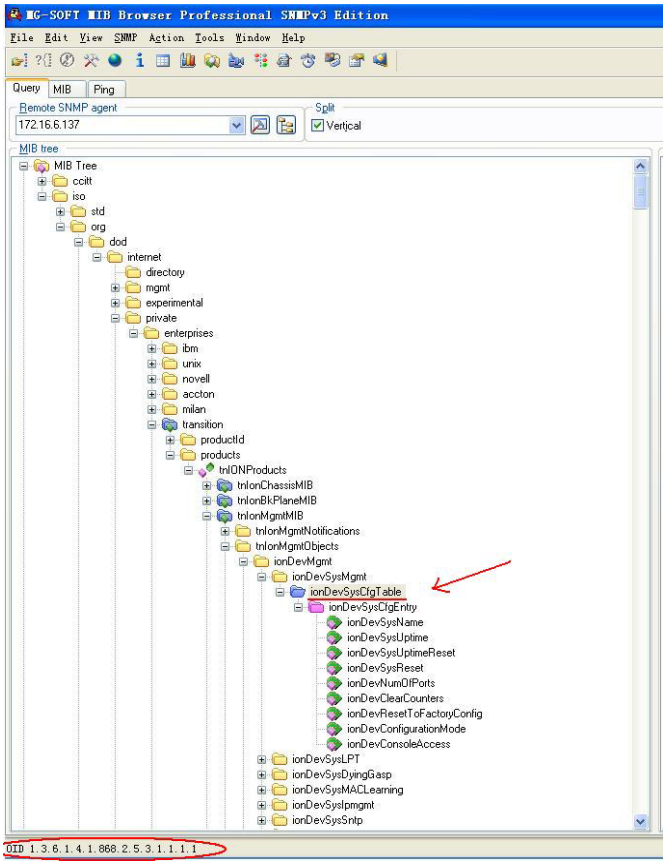


Figure 21. MIB Example

SNMP PDUs

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The SNMP agent may generate notifications from any available port.

SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs, GetBulkRequest and InformRequest were added in SNMPv2 and carried over to SNMPv3.

SNMP PDUs are constructed as follows:

IP header	UDP header	version	community	PDU-type	request-id	error-status	error-index	variable bindings

Figure 22. SNMP PDU Format

The seven SNMP protocol data units (PDUs) are:

- GetRequest
- SetRequest
- GetNextRequest
- GetBulkRequest (Only v2 and v3)
- Response
- Trap
- InformRequest (SNMP v2 and v3 only)

Each of the seven SNMP PDUs is described below.

GetRequest: A manager-to-agent request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A Response with current values is returned.

SetRequest: A manager-to-agent request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A Response with (current) new values for the variables is returned.

GetNextRequest: A manager-to-agent request to discover available variables and their values. Returns a Response with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of GetNextRequest starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

GetBulkRequest: Optimized version of GetNextRequest. A manager-to-agent request for multiple iterations of GetNextRequest. Returns a Response with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific non-repeaters and max-repetitions fields are used to control response behavior. GetBulkRequest was introduced in SNMPv2.

Response: Returns variable bindings and acknowledgement from agent to manager for GetRequest, SetRequest, GetNextRequest, GetBulkRequest and InformRequest. Error reporting is provided by error-status and error-index fields. Although it was used as a response to both gets and sets, this PDU was called GetResponse in SNMPv1.

Trap: 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.

InformRequest: An acknowledged asynchronous notification from manager to manager. This PDU uses the same format as the SNMPv2 version of Trap. Manager-to-manager notifications were already possible in SNMPv1 (using a Trap), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a Trap was not guaranteed. InformRequest fixes this by sending back an acknowledgement on receipt. Receiver replies with Response parroting all information in the InformRequest. This PDU was introduced in SNMPv2.

SNMP Version v1, v2c, v3 Considerations

1. SNMPv3 provides secure access to the ION system by a combination of authenticating and encrypting packets over the network. With the SNMPv3 feature, users can enable SNMPv1/v2c or SNMPv3 access to ION system as follows:

SNMP Access	How To Configure	Description
SNMP v1/v2c only	• Add SNMPv1/v2c community strings. • Remove all SNMPv3 users.	Only allow SNMPv1/v2c access to ION system though community strings.
SNMPv3 only	• Remove all SNMPv1/v2c community strings. • Add SNMPv3 users, assign the users to groups, enable the groups to have access to views, add views to have access to MIBs.	Only allow SNMPv3 access to ION system though SNMPv3 users.
SNMPv1/v2c/v3	• Add SNMPv1/v2c community strings • Add SNMPv3 users, assign the users to groups, enable the groups to have access to views, add views to have access to MIBs.	Allow SNMPv1/v2 access to ION system though community strings. Also allow SNMPv3 access to ION system though SNMPv3 users.

2. You can configure the SNMPv1/v2c write community string and read only community string. SNMPv1 and v2c share the same community strings.

3. You can set the local SNMPv3 engine ID in the **SNMP** > **GENERAL** tab. An SNMPv3 engine is an independent SNMP agent that resides on the IONMM. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

   A local engine ID is automatically generated that is unique to the IONMM. The input engine ID is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users are cleared, and you must reconfigure all existing users.

   A new engine ID can be specified by entering 9 to 64 hexadecimal characters. An engineID can not be empty. At default the SNMPv3 engine ID string of an IONMM is “80 00 03 64 03 00 c0 f2 xx xx xx” (“03 64” is the enterprise number of Lantronix; “00 c0 f2 xx xx xx” is the MAC address of an ION device). In other words, the default IONMM SNMPv3 engine ID string is: *the MAC address of the IONMM* **+** *’Lantronix*’.

   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).

SNMP v1, v2c, v3 Descriptions

Each SNMP version is described below.

SNMPv1

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used and is the de facto network-management protocol in the Internet community.

The first RFCs for SNMP, now known as SNMPv1, appeared in 1988: RFC 1065, RFC 1066, and RFC 1067. These protocols were obsoleted by SNMPv1: RFC 1155, RFC 1156 and RFC 1157. After a short time, RFC 1156 (MIB-1) was replaced by more often used

RFC 1213 - Version 2 of management information base (MIB-2) for network management of TCP/IP-based internets

SNMPv1 was criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext. The '80s design of SNMP V1 was done by a group of collaborators who viewed the officially sponsored OSI/IETF/NSF (National Science Foundation) effort (HEMS/CMIS/CMIP) as both unimplementable in the computing platforms of the time as well as potentially unworkable. SNMP was approved based on the belief that it was an interim protocol needed for taking steps towards large scale deployment of the Internet and its commercialization. In that time period Internet-standard authentication/security was considered a dream and was discouraged by focused protocol design groups.

SNMPv2

SNMPv2 (RFC 1441–RFC 1452) revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced GetBulkRequest, an alternative to iterative GetNextRequests for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMPv2, viewed by many as overly complex, was not widely accepted.

Community-Based Simple Network Management Protocol version 2, or SNMPv2c, is defined in RFC 1901–RFC 1908. In its initial stages, this was also informally known as SNMPv1.5. SNMPv2c comprises SNMPv2 without the controversial new SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1. While officially only a "Draft Standard", this is widely considered the de facto SNMPv2 standard.

User-Based Simple Network Management Protocol version 2, or SNMPv2u, is defined in RFC 1909–RFC 1910. This is a compromise that attempts to offer greater security than SNMPv1, but without incurring the high complexity of SNMPv2. A variant of this was commercialized as SNMP v2*, and the mechanism was eventually adopted as one of two security frameworks in SNMP v3.

SNMPv3

Simple Network Management Protocol Version 3 (SNMPv3) 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 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.

Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.

Authentication - to verify that the message is from a valid source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combined security model / security level determines which security mechanism is used when handling an SNMP packet. Three security models are available: SNMPv1, v2c, and v3. The table below shows the combinations of security models / levels.

Table 16. SNMPv3 Private MIB Levels / Auth / Encryption

Model	Level	Authentication	Encryption	Results
v1	noAuthNoPriv	Community String	None	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	None	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	None	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	None	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES/AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES/AES encryption in addition to authentication based on the DES/AES standard.

SNMPv3 Summary and Key Features

SNMPv3 includes the following key features:

- SNMPv3 EngineID
- SNMPv3 USM

- SNMP VACM
- SNMP Trap/Inform (v1/v2c/v3 trap, v2c/v3 inform)

SNMPv3 Services Provided

The SNMPv3 function supports these services:

- SNMP v3 user management, authentication and encryption.
- SNMP VACM management.
- SNMP v1/v2c/v3 selection.
- SNMP notification (v1/v2c/v3 trap, v2c/v3 inform) functionality.

SNMPv3 features can be configured via the Web interface, CLI, Telnet, or SSH. The SNMPv3 configuration can be backed up and restored. These services are further detailed below.

Table 17: SNMPv3 Services

No.	Function	Description	Reference
1	SNMP v3 USM	SNMP v3 User-based Security Model.	RFC 3414
2	SNMP VACM	SNMP View-based Access Control Model.	RFC 3415
3	SNMP v1/v2c/v3 version selection	SNMP v1/v2c/v3 version selection	Private MIB
4	SNMP v1/v2c/v3 Trap	SNMP v1/v2c/v3 Trap functionality	Private MIB
5	SNMP v1/v2c/v3 Inform	SNMP v1/v2c/v3 Inform functionality	Private MIB
6	Web for SNMP v3	Configure SNMP v3 via Web	None
7	CLI for SNMP v3	Configure SNMP v3 via CLI	None
8	Backup/Restore for SNMP v3	Backup/Restore SNMP v3 configuration.	None

SNMPv3 Public MIBs

Table 18. SNMPv3 Private MIBs

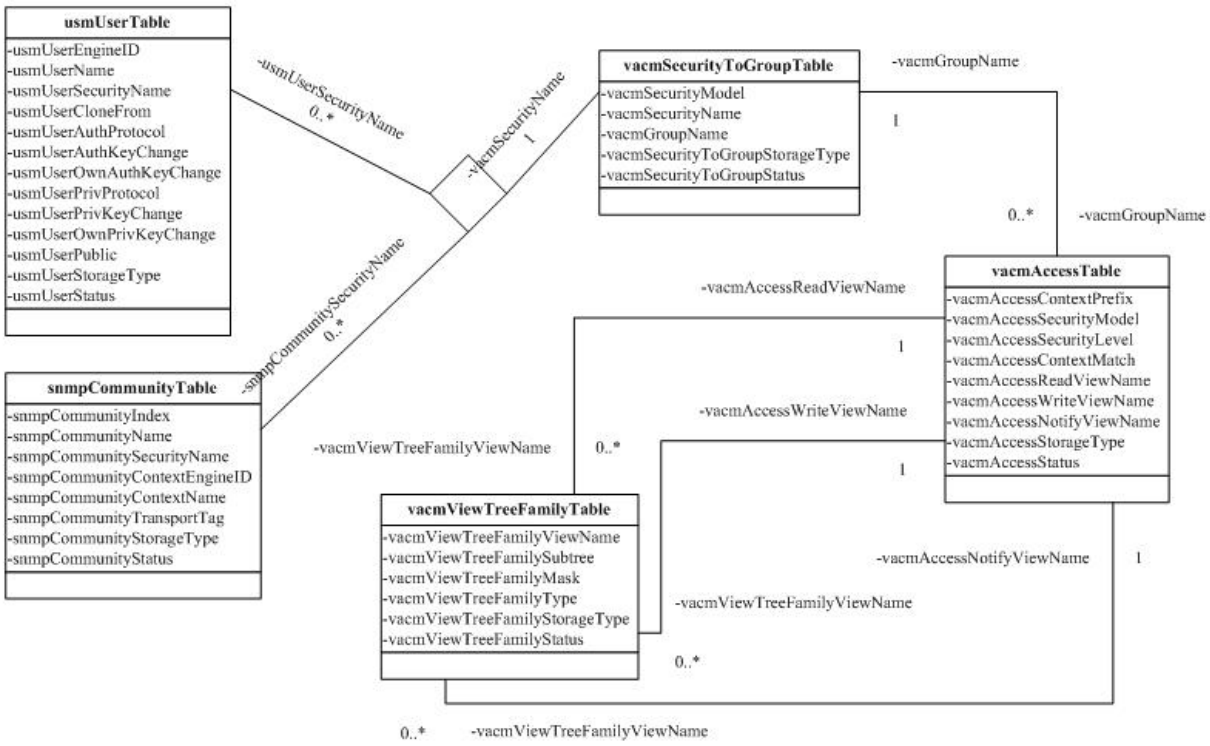
MIB	MIB tables or variables	Function
snmpFrameworkMIB (RFC 3411)	snmpEngine	local SNMPv3 engine information
snmpTargetMIB (RFC 3413)	snmpTargetSpinLock	Lock for modifying the snmpTargetAddr TagList of snmpTargetAddrTable
	snmpTargetAddrTable	SNMP v1/v2c/v3 trap(v2c/v3 inform) host address, udp port number, v2c/v3 inform timeout and retries
	snmpTargetParamsTable	SNMP v1/v2c/v3 trap(v2c/v3 inform) version selection, trap security level, trap community or security name
snmpNotificationMIB (RFC 3413)	snmpNotifyTable	SNMP v2c/v3 trap/inform selection
	snmpNotifyFilterProfileTable	Relate snmpTargetParamsTable with snmpNotifyFilterTable
	snmpNotifyFilterTable	Trap/inform view filtering
snmpUsmMIB (RFC 3414)	usmStats	USM user access error statistic
	usmUserSpinLock	Lock for altering the secrets of usmUserTable
	usmUserTable	USM user management table
snmpVacmMIB (RFC 3415)	vacmContextTable	The table of locally available contexts
	vacmSecurityToGroupTable	Mapping USM user or v1/v2c community string to group
	vacmAccessTable	Group access rights to view
	vacmViewSpinLock	Lock for creating and modifying views
	vacmViewTreeFamilyTable	View to OID tree management table
snmpCommunityMIB (RFC 3584)	snmpCommunityTable	Multiple v1/v2c community string management table

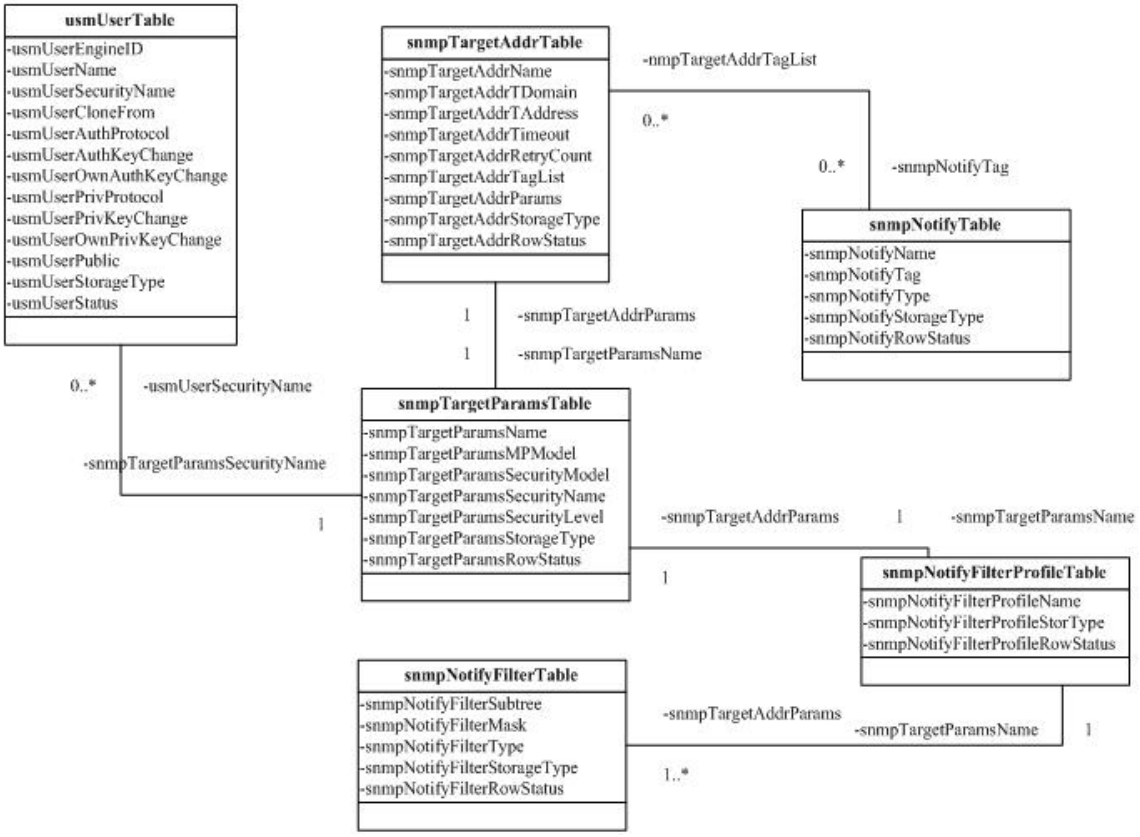
SNMPv3 Private MIBs

Table 19. SNMPv3 Private MIBs

MIB	MIB tables or variables	Function
ionDevSysSnmpmgmt	ionDevSysSnmpLocal	Modify the local engineID
	ionDevSysSnmpTrapManagerTable	Maintain the mapping from SNMPv3 trap hosts to their engine IDs.

SNMP v3 MIB Relationships




usmUserTable
-usmUserEngineID
-usmUserName
-usmUserSecurityName
-usmUserCloneFrom
-usmUserAuthProtocol
-usmUserAuthKeyChange
-usmUserOwnAuthKeyChange
-usmUserPrivProtocol
-usmUserPrivKeyChange
-usmUserOwnPrivKeyChange
-usmUserPublic
-usmUserStorageType
-usmUserStatus
snmpTargetAddrTable
-snmpTargetAddrName
-snmpTargetAddrTDomain
-snmpTargetAddrTAddress
-snmpTargetAddrTimeout
-snmpTargetAddrRetryCount
-snmpTargetAddrTagList
-snmpTargetAddrParams
-snmpTargetAddrStorageType
-snmpTargetAddrRowStatus
-nmpTargetAddrTagList
0..*
0..*
-snmpNotifyTag
snmpNotifyTable
-snmpNotifyName
-snmpNotifyTag
-snmpNotifyType
-snmpNotifyStorageType
-snmpNotifyRowStatus
1
-snmpTargetAddrParams
1
-snmpTargetParamsName
0..*
-usmUserSecurityName
-snmpTargetParamsSecurityName
1
snmpTargetParamsTable
-snmpTargetParamsName
-snmpTargetParamsMPModel
-snmpTargetParamsSecurityModel
-snmpTargetParamsSecurityName
-snmpTargetParamsSecurityLevel
-snmpTargetParamsStorageType
-snmpTargetParamsRowStatus
-snmpTargetAddrParams
1
-snmpTargetParamsName
1
snmpNotifyFilterProfileTable
-snmpNotifyFilterProfileName
-snmpNotifyFilterProfileStorType
-snmpNotifyFilterProfileRowStatus
snmpNotifyFilterTable
-snmpNotifyFilterSubtree
-snmpNotifyFilterMask
-snmpNotifyFilterType
-snmpNotifyFilterStorageType
-snmpNotifyFilterRowStatus
-snmpTargetAddrParams
-snmpTargetParamsName
1
1..*

Examples of SNMP v3 private MIB objects trees are shown in the figures below.

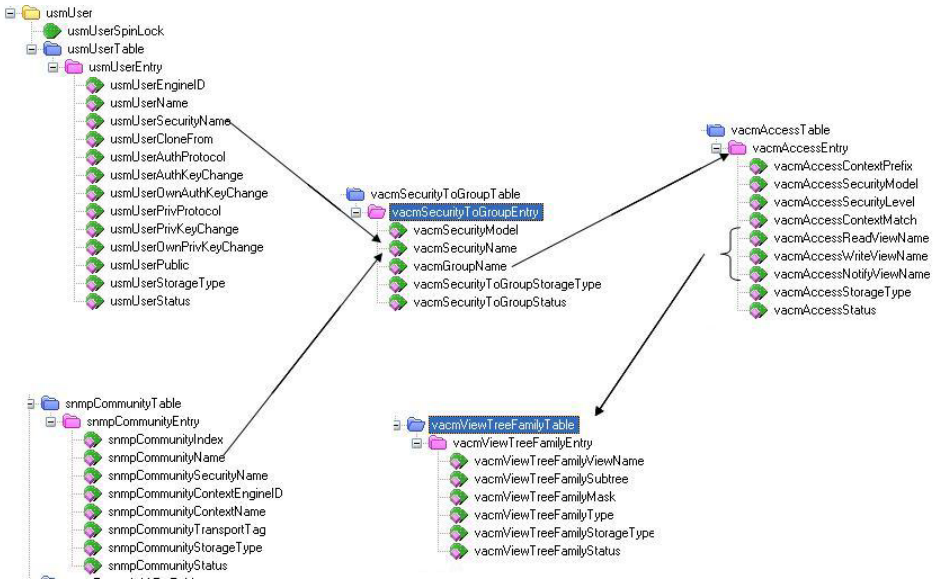


Figure 23. SNMP v3 MIBs

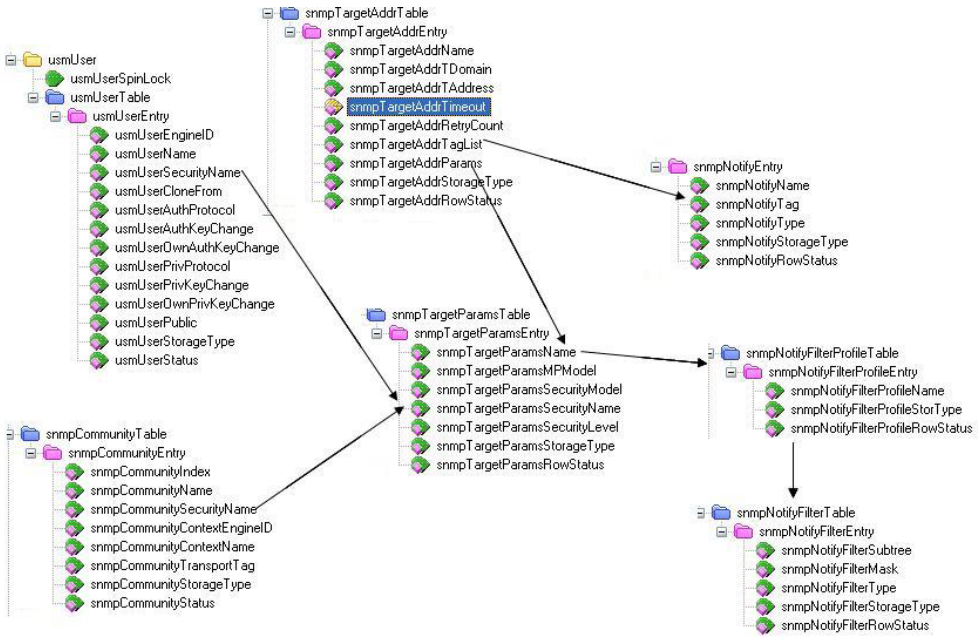


Figure 24. SNMP v3 Trap-Inform MIBs

SNMP v3 EngineID Concept

An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity which contains it. The SNMP v3 engine contains:

- a Dispatcher
- a Message Processing Subsystem
- a Security Subsystem, and
- an Access Control Subsystem.

Within an administrative domain, an snmpEngineID is the unique and unambiguous identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, it also uniquely and unambiguously identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for snmpEngineID. Federation of administrative domains may necessitate assignment of new values.

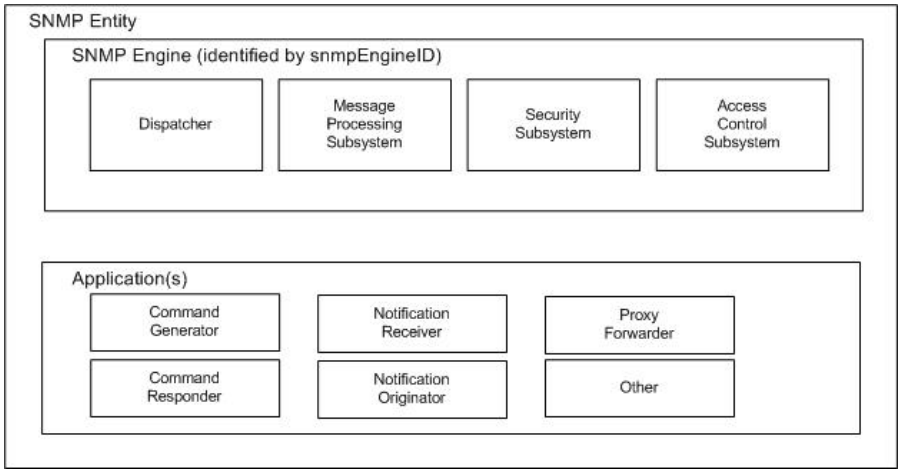


Figure 25. SNMP v3 Entity / Engine / Applications

Local engineID:

- The engineID for the local SNMP engine.
- The engineID for the SNMP engine residing in the managed IONMM or standalone S2x2x/S3x2x/S3240.

Remote engineID:

- The engineID for a remote SNMP engine.
- In the ION system, the remote engineID is only used to configure the engineID of the remote SNMPv3 inform receipt server.

RFC standard: RFC 3411.

SNMPv3 EngineID MIBs

Public MIB for enginID: snmpEngine

- OID is 1.3.6.1.6.3.10.2.1
- For local engineID
- Read-only

Private MIB for local enginID:

- OID is 1.3.6.1.4.1.868.2.5.3.1.1.14.3.1
- Read-write
- Used to modify the local engineID.
- When modifying the local engineID, all the local SNMPv3 USM users will be deleted.

Private MIB for remote enginID:

- OID is 1.3.6.1.4.1.868.2.5.3.1.1.14.4.1
- Read-write
- The combination of *ionDevSysSnmpTrapManagerAddrTDomain* and *ionDevSysSnmpTrapManagerAddrTAddress* must be unique.
- The engineID in this table must be unique (it can not be the same as the local engineID).
- Used to add/delete remote engineIDs.
- When deleting a remote engineID, all the SNMPv3 USM users belonging to the SNMP engine will be deleted.

You must add a remote engine before you can add remote users for this engine.

SNMPv3 USM (User-Based Security Model)

The ION SNMP v3 implementation uses the traditional concept of a user (identified by a *userName*) with associated security information. This is a key SNMPv3 security feature implemented per RFC 3414.

SNMP v3 USM Service: USM provides the following security service:

- Data Integrity is the provision of the property that data has not been altered or destroyed in an unauthorized manner, nor have data sequences been altered to an extent greater than can occur non-maliciously.
- Data Origin Authentication is the provision of the property that the claimed identity of the user on whose behalf received data was originated is corroborated.
- Data Confidentiality is the provision of the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Message timeliness and limited replay protection is the provision of the property that a message whose generation time is outside of a specified time window is not accepted. Note that message reordering is not dealt with and can occur in normal conditions too.

SNMP v3USM User: Management operations using this Security Model make use of a defined set of user identities. For any user on whose behalf management operations are authorized at a particular SNMP engine, that SNMP engine must have knowledge of that user. An SNMP engine that wishes to communicate with another SNMP engine must also have knowledge of a user known to that engine, including knowledge of the applicable attributes of that user.

SNMPv3 USM User and SNMP Engine

- A USM user must belong to a SNMP engine.
- You must add a remote engine before you can add remote users for this engine.
- If a user belongs to the local SNMP engine, it is called a local USM user.
- If a user belongs to a remote SNMP engine, it is called a remote USM user.
- If an engineID of an SNMP engine is changed or deleted, its USM users are deleted.

SNMPv3 USM MIB

Public MIB for USM: usmUser

- OID is 1.3.6.1.6.3.15.1.2
- Used to add/modify/delete USM users
- Store information for both local USM users and remote USM users

SNMPv3 VACM (View-based Access Control Model)

The View-based Access Control Model defines a set of services that an application (such as a Command Responder or a Notification Originator application) can use for checking access rights.

Access Control occurs (either implicitly or explicitly) in an SNMP entity when processing SNMP retrieval or modification request messages from an SNMP entity.

Access Control also occurs in an SNMP entity when an SNMP notification message is generated (by a Notification Originator application).

VACM includes these elements:

- Groups
- SecurityLevel
- Contexts
- MIB Views and View Families
- Access Policy

SNMPv3 USM – VACM MIBs

Public MIB for VACM: snmpVacmMIB

- OID is 1.3.6.1.6.3.16
- Used to manage VACM configurations including the mapping from user to groups, groups access, view table.
- RFC 3415

Table 20: SNMP v3 Default Values

snmpVacmMIB (RFC 3415)	vacmContextTable	The table of locally available contexts.
	vacmSecurityToGroup Table	Mapping USM user or v1/v2c community string to Group.
	vacmAccess Table	Group access right to View
	vacmViewSpinLock	Lock for creating and modifying Views.
	vacmViewTree Family Table	View to OID tree management table.

SNMPv3 VACM – Groups

A Group is a set of zero or more <*securityModel*, *securityName*> tuples on whose behalf SNMP management objects can be accessed. A Group defines the access rights afforded to all securityNames which belong to that group. The combination of a *securityModel* and a securityName maps to at most one Group. A Group is identified by a *groupName*.

The Access Control module assumes that the *securityName* has already been authenticated as needed and provides no further authentication of its own.

The View-based Access Control Model uses the *securityModel* and the *securityName* as inputs to the Access Control module when called to check for access rights. It determines the *groupName* as a function of *securityModel* and *securityName*.

Note that 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.

SNMPv3 VACM – Views

Views are used to restrict the access rights of some groups to only a subset of the management information in the management domain.

A view subtree is the set of all MIB object instances which have a common ASN.1 OBJECT IDENTIFIER prefix to their names.

A family of view subtrees is a pairing of an OBJECT IDENTIFIER value (called the family name) with a bit string value (called the family mask). The family mask indicates which sub-identifiers of the associated family name are significant to the family's definition.

SNMPv3 Traps and Informs

A Trap is an SNMP message sent from one application to another (which is typically on a remote host). Their purpose is merely to notify the other application that something has happened, has been noticed, etc. The big problem with Traps is that they're unacknowledged, so you don't actually know if the remote application received your -important message. The trap is available for SNMP v1, v2c and v3.

An Inform is an acknowledged Trap. When the remote application receives an inform it sends back an acknowledgement message. Inform is available for SNMP v2c and v3. For SNMP v3, an inform must be sent to a specific remote USM user resided in the inform receiver.

SNMPv3 Trap/Inform MIBs

- Public MIB for trap/inform: *snmpTargetMIB* and *snmpNotificationMIB*
- OIDs are 1.3.6.1.6.3.12 and 1.3.6.1.6.3.13
- Used to manage trap/inform server configuration.
- RFC 3413

Table 21: SNMP v3 Trap and Inform MIBs

snmpTargetMIB (RFC 3413)	snmpTargetSpinLock	Lock for modifying the snmpTargetAddr TagList of snmpTargetAddrTable.
	snmpTargetAddrTable	SNMP v1/v2c/v3 trap(v1/v2c/v3 inform) host address, udp port #, v2c/v3 inform timeout & retries.
	snmpTargetParamsTable	SNMP v1/v2c/v3 trap(v1/v2c/v3 inform) version selection, trap security level, trap community or security name.
snmpNotificationMIB (RFC 3413)	snmpNotifyTable	SNMP v2c/v3 trap/inform selection.
	snmpNotifyFilterProfileTable	Relate snmpTargetParamsTable with snmpNotifyFilterTable.
	snmpNotifyFilterTable	Trap/inform view filtering.

The MIB tables used for each tab are shown in the table below. Some MIB tables are used in several tabs.

Table 22: Web Interface Tabs to MIB Tables Mapping

Tab	sub-tab	Used MIB tables
SNMP	General	snmpCommunityTable vacmSecurityToGroupTable ionDevSysSnmpLocal(private)
	Users	usmUserSpinLock usmUserTable vacmSecurityToGroupTable vacmAccessTable
	Groups	vacmAccessTable vacmViewTreeFamilyTable
	Views	vacmViewSpinLock vacmViewTreeFamilyTable
	Trap hosts	snmpTargetSpinLock snmpTargetAddrTable snmpTargetParamsTable snmpNotifyTable
	Remote Users	ionDevSysSnmpTrapManagerTable(private) usmUserSpinLock usmUserTable
USERS		ionDevSysUserTable

ION System SNMP Support

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. Note that if the IONMM sends out v2c/v3 informs, the trap servers will send responses.

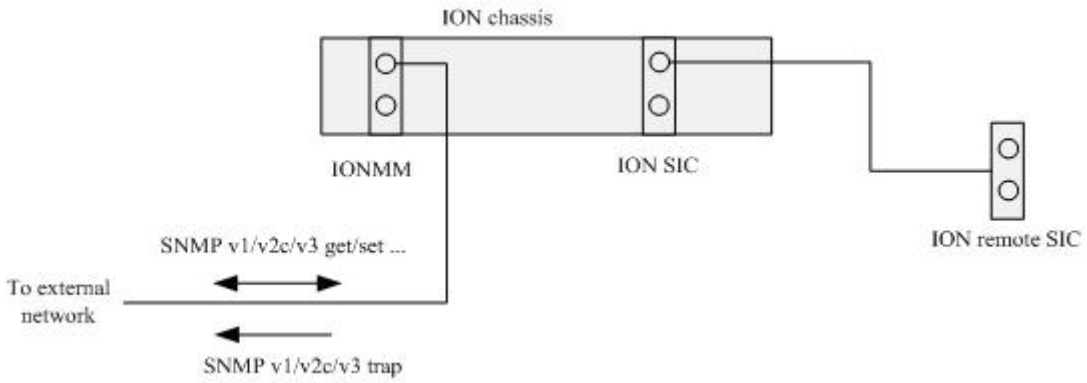


Figure 26: ION System Managed via SNMP

The ION system provides several interfaces (Web /CLI/Telnet/SSH) to configure the SNMPv3 features for the IONMM. The IONMM can backup and restore SNMPv3 configurations for the IONMM when doing a backup or restore operation.

SNMP Command Line Interface (CLI) Support

The SNMP Command Line Interface (CLI) is implemented with device-level and port-level CLI commands.

SNMP v3 Users, Groups, and Views Configuration

SNMP v3 configuration involves setting up SNMP v3 Users, Groups, and Views, with the caveats discussed below.

With SNMPv3, you can define SNMP users, groups, and views to provide access control to SNMP devices, and restrict certain users so they can only access the parts of the MIB that they have been given access rights to. The SNMP views, groups and users are described below.

Note: the concept of SNMP communities that was introduced in SNMPv2 is not relevant to SNMPv3, and has been replaced by SNMP groups/users. However, you can configure an ION system NID to respond to both SNMPv2 and SNMPv3 commands. If both SNMPv2 and SNMPv3 are to be used, you must configure SNMP communities and SNMP groups and users. To use SNMPv1/v2c, all you need to do is add a Community at **IONMM** > **SNMP** > **General** tab; nothing else needs to be configured. You can add or delete any Communities including the default communities.

SNMP Users have a specified username, authentication password, privacy password, (if required) and authentication and privacy algorithms assigned. The authentication algorithm options are none, MD5, or SHA. The privacy algorithm options are none, AES, or DES. When a new User is created, it is associated

with an SNMP group. (MD5 is Message Digest Algorithm version 5, SHA is the Secure Hash Algorithm, DES is the Data Encryption Standard, and AES is the Advanced Encryption Standard.)

SNMP Groups are basically access control policies to which users can be added. Each SNMP Group is configured with a security level, and is associated with an SNMP View. These parameters specify the type of authentication and privacy a user within the SNMP group will use, and also which objects in the MIB the User can access. Each SNMP Group name and security level pair must be unique within the device.

SNMP MIB Views are defined lists of objects within a MIB that can be used to control which parts of a MIB can be accessed by Users belonging to the SNMP Group associated with that particular View. Objects in the View may be from anywhere in the MIB, and are not required to be in the same MIB sub-tree. When you have defined your Views, you must configure for your SNMP Groups the type of access Users will have to those Views. There are three possible types of access configurable, and at least one must be configured in order for Users in that SNMP Group to have access to an SNMP View.
The three types of access that you can configure are 1. ReadView specifies the SNMP View to which the Group has read access, 2. WriteView specifies the SNMP View to which the group has write access, and 3. NotifyView specifies the SNMP View for which the group will receive notifications. **Views**: one default View (defaultview) exists which cannot be modified or deleted. You can configure an SNMP v3 Group with read access to one SNMP View, and write access to a different SNMP View.

Summary: You can create multiple Views. You can then create multiple Groups, and associate them with a View. You can configure multiple Groups (each with a different Group name and security level) and associate them with a particular View. You can also configure more than one View associated with a Group (e.g., a Group with read access to the entire MIB tree, but with only write access to certain objects). You could then create multiple Users, and associate them with a Group (you can associate multiple Users with a particular Group).

With SNMPv3 you can define SNMP views, groups and users to provide access control to SNMP devices, as shown below.

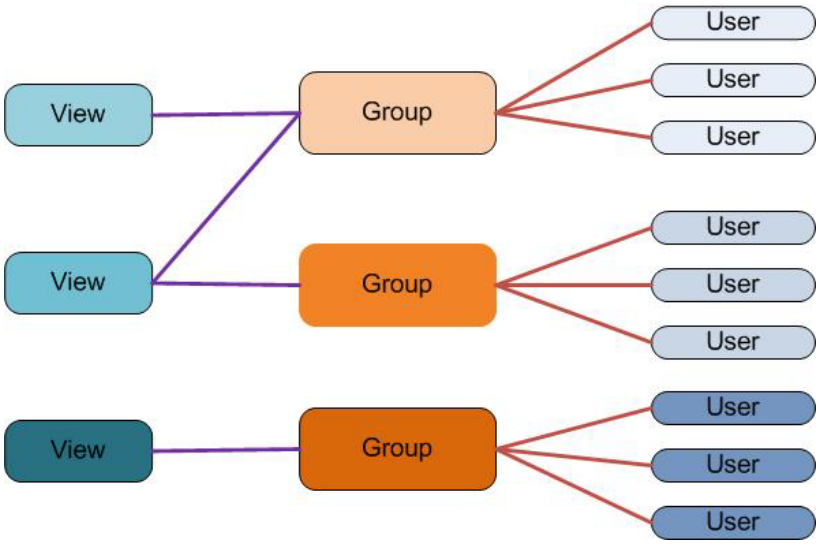


Figure 27 .SNMP v3 Users, Groups, and Views

You can create multiple Views. You can then create multiple Groups, and associate them with a View. You can configure multiple Groups (each with a different Group name and security level) and associate them with a particular View. You can also configure more than one View associated with a Group (e.g., a Group with read access to the entire MIB tree, but with only write access to certain objects). You could then create multiple Users, and associate them with a Group (you can associate multiple Users with a particular Group).

Configuring SNMP v3 Users

With the introduction of USM and SNMP VACM in SNMPv3 comes the ability to manage the SNMPv3 users. SNMPv3 users are configured as follows:

- The user levels (admin/read-write/read-only) which is described in the USERS tab section are used for Web/CLI login user. There is no level definition for SNMPv3 users. At default there are no SNMPv3 users.
- SNMPv3 users cannot log in to the ION system via Web/CLI. Users must log in via the Web/CLI USERS path, not the SNMPv3 Users path.
- If the RADIUS client is enabled, all login is through the RADIUS server (via the Web interface or the CLI). Any user that logs in successfully via RADIUS is treated as a super user.

Configuring SNMP v3 Groups

With the introduction of SNMPv3 users comes the ability to manage groups of SNMP v3 users.
An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read, write, and notify views.

An SNMPv3 user must belong to a SNMPv3 group. There are four default groups. The default group is defined for the super 'ION' user. The Public group and the Private group are used by SNMP v1/v2c community strings.

The four default group entries are:

Public Group:

- 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 Group:

- Private v1: this entry has SNMPv1 read and write access to the default view.
- Private v2c: this entry has SNMPv2c read and write access to the default view.

These groups cannot be deleted or modified.

Configuring SNMP v3 Views

With the introduction of SNMPv3 users and groups comes the ability to manage SNMP v3 users' views.

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The default view includes access to the entire MIB tree. This default view cannot be deleted or modified.

SNMP v3 Limitations

No Space Characters Allowed: 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 "space" characters. If you enter a "space" character in these fields (via CLI or Web interface) the messages "*It can be set to any characters combination except the character space*." and “this.pattern is required: /^[\S]*{1,256}$/.” display. You must then re-enter the command or field without any "space" characters.

Other ION system SNMP v3 limitations are:

- Changing the engine ID will delete all previously configured USM users.
- Changing the remote engine ID will delete all remote users belonged to this engine.
- Trap filtering can only be configured through SNMP interface (not via Web interface or CLI).
- Mapping from SNMPv1/v2c communities to group can only be configured via the SNMP interface; Web interface / CLI only supports configuring two types of SNMP v1/v2c communities: read-only and read-write. These two types of communities will be mapped to the default groups automatically.
- Supports a maximum of six trap hosts.
- Only one local Engine ID can be configured.
- Up to 255 remote Engine IDs can be configured.
- The length range of an Engine ID is from 8 to 64 characters (no space characters).
- Up to 255 SNMPv3 users can be configured
- Up to 255 SNMPv3 remote users can be configured
- Up to 255 SNMPv3 groups can be configured
- Up to 255 SNMPv3 views can be configured
- Up to 255 Communities can be configured.
- The length range of each Community name is from 1 to 32 characters (no space characters).

SNMP and IPv6

With IPv6 support, ION SNMP support includes the following IPv6 functions:

- If IPv6 is enabled, the SNMPv1/v2c communities can be used to do get/set operations though either the IPv4 address or the IPv6 global address of a device. Up to 16 SNMP communities are supported on one device.

- If IPv6 is enabled, the SNMPv3 USM local users can be used to do get/set operations though either the IPv4 address or the IPv6 global address of a device. The SNMPv3 USM remote users can be configured for either an IPv4 trap host or an IPv6 trap host. Up to 255 USM users (local and remote) are supported on one device.

- The trap host can be either an IPv4 address or an IPv6 address. If IPv6 is enabled and one trap (or inform) is generated, this trap (or inform) can be sent to all the trap servers. If IPv6 is disabled, the traps can not be sent to any IPv6 trap host. Up to 6 trap servers can be supported on one device.

The maximum number of SNMP group/view/community/local user entries is 255. An error message displays if more than 255 entries are attempted.

The SNMP Community String entry can be any ASCII printable characters except :: and @; otherwise the message "Its value must be ASCII printable characters except \"::\" and \"@\".” displays.

Configuring SNMP

The x222x/x32xx 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" on page 46.

1. Access the IONMM through either a USB connection (see "Starting a USB Session" on page 23) or a Telnet session (see "Starting a Telnet Session" on page 24).
2. Define the General configuration. For example, type:

```
S3230-1040 C0|S0|L1D>add snmp community name xxxxxxx
   access_mode={read_only|read_write}
S3230-1040 C0|S0|L1D>add snmp remote engine addrtype=ipv4 addr=xx port=xx
   engine_id=xx
S3230-1040 C0|S0|L1D>set snmp local engine=xx
```

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

```
S3230-1040 C0|S0|L1D>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]

S3230-1040 C0|S0|L1D>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**.

```
S3230-1040 C0|S0|L1D>set snmp local user group=xxx
```

5. Define one or more Views. Type **set snmp view name**= STR_SNMP_VIEW and press **Enter**.
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:

```
S3230-1040 C0|S0|L1D>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:

```
S3230-1040 C0|S0|L1D>show snmp ?
  community
  group
```

```
  local
  remote
  traphost
  view
```

```
S3230-1040 C0|S0|L1D>show snmp community
Community string                    Access mode
-------------------------------------------------------------------------------
comm1                               read_write
public                              read_write
private                             read_only
xxxxxxx                             read_only
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|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
```

```
S3230-1040 C0|S0|L1D>show snmp local engine
Local engine ID:    80.00.03.64.03.00.c0.f2.20.de.9e (hex)
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|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
S3230-1040 C0|S0|L1D>>
```

```
S3230-1040 C0|S0|L1D>show snmp remote engine
Remote Address                  Remote port     Remote Engine ID
192.168.1.20                    162             800003640300c0f2209ede
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|L1D>show snmp remote user
User Name  Engine ID  Security Model Security Level Auth Protocol  Privacy Protocol
-------------------------------------------------------------------------------
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|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
S3230-1040 C0|S0|L1D>
```

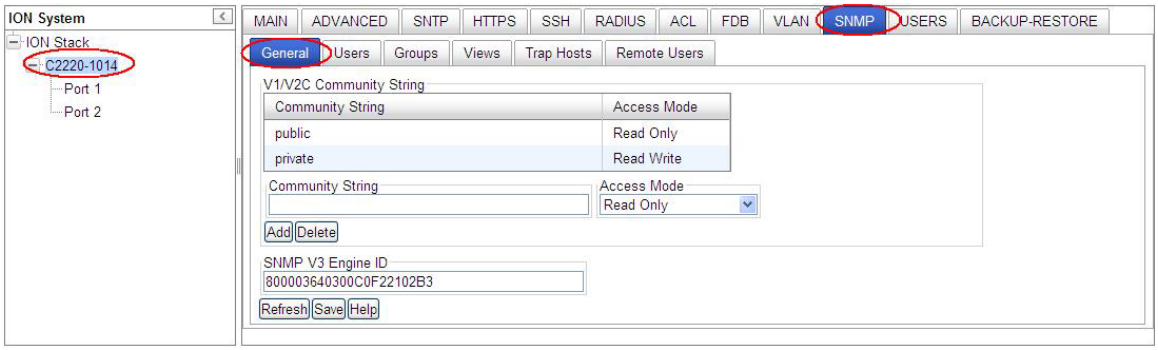
```
S3230-1040 C0|S0|L1D>show snmp view
name               OID Sub Tree          type
-------------------------------------------------------------------------------
defaultView        0                     include
defaultView        1                     include
defaultView        2                     include
S3230-1040 C0|S0|L1D>
```

8. Backup the configuration. See “Backup and Restore Operations (Provisioning)” on page 324.

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" on page 26).
2. Select the **SNMP** tab.
3. Select the **General** sub-tab if not already displayed.



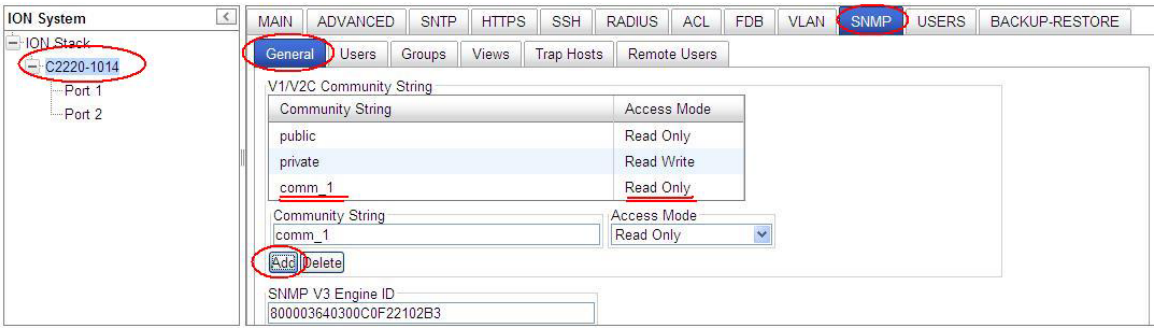
4. Add a new community string as required:

   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 can not 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).

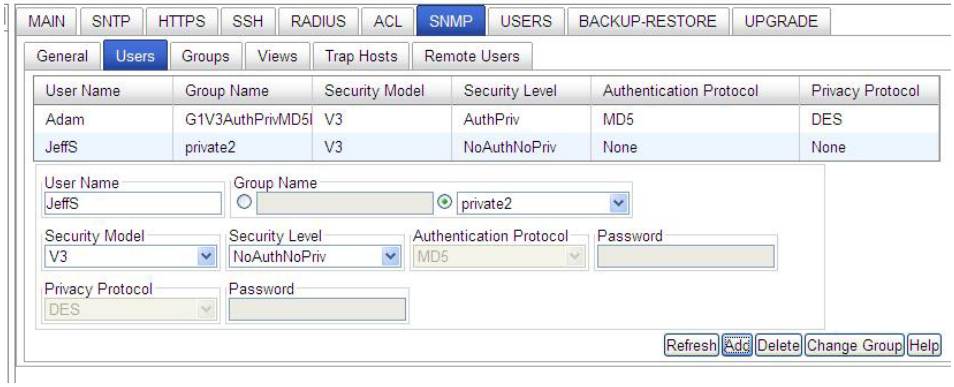
Privacy Protocol: The encryption algorithm used for data privacy. (Options: **DES** or **AES**; Default: **DES**.)

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

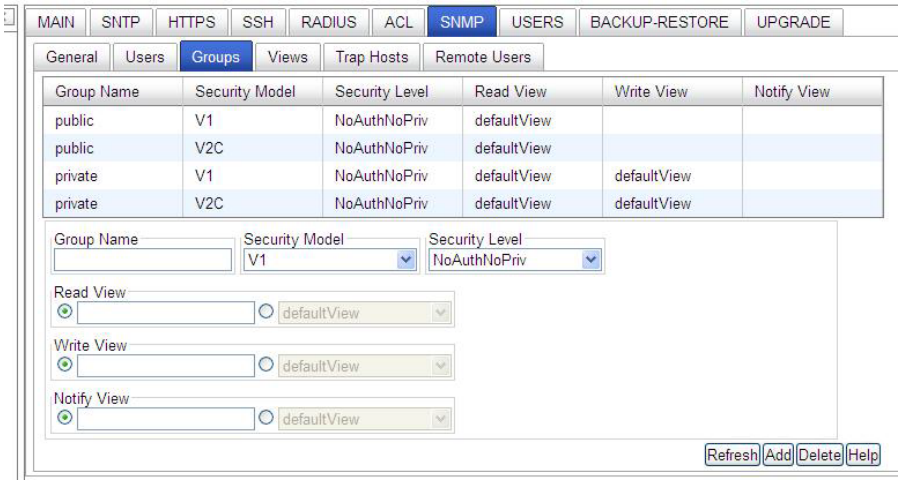
securityName (implied): A human-readable string representing the user in a format that is Security Model independent. There is a one-to-one relationship between *userName* and *securityName*. In ION system, the security name is the same as user name.

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 can not be the same as the local engine ID.

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



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



11. Add and Edit the fields as required:

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

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

Security Level: The security level used for the group:

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

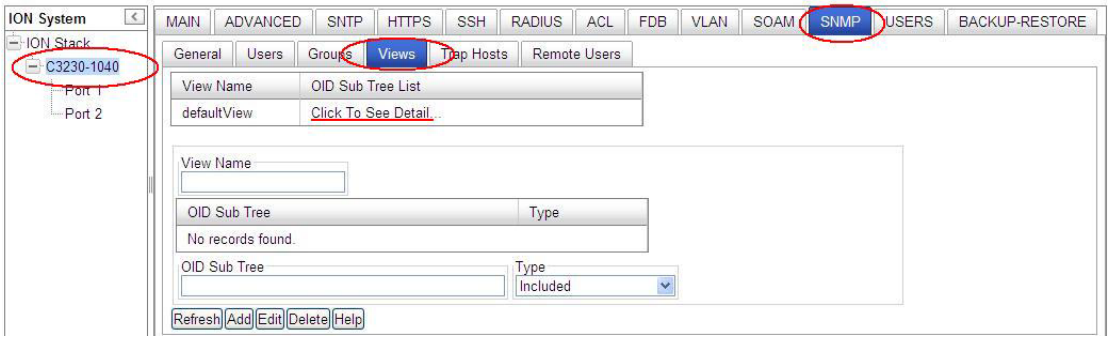
  The Group Security Level is the minimum level of security required in order to gain the access rights to the views (read/write/notify). If the User Security Level is less than the Group Security Level, this user will have no access rights to the views. A Security Level of ***noAuthNoPriv*** is less than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

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

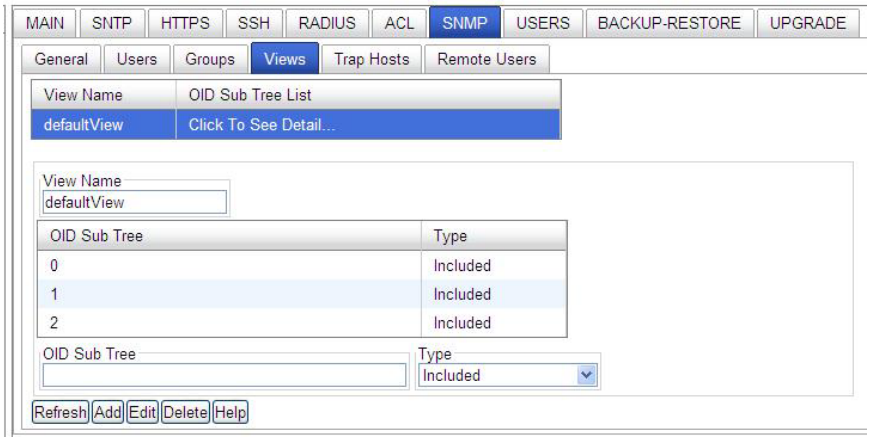
Write View: The configured view for write access. You can leave this view blank (none), or enter a specific view name (1-64 characters, no space characters), or select the **defaultView** radio button. **Note** that an entry here does not mean this view already exists in the view table.

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

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



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



14. Add / Edit the fields as required:

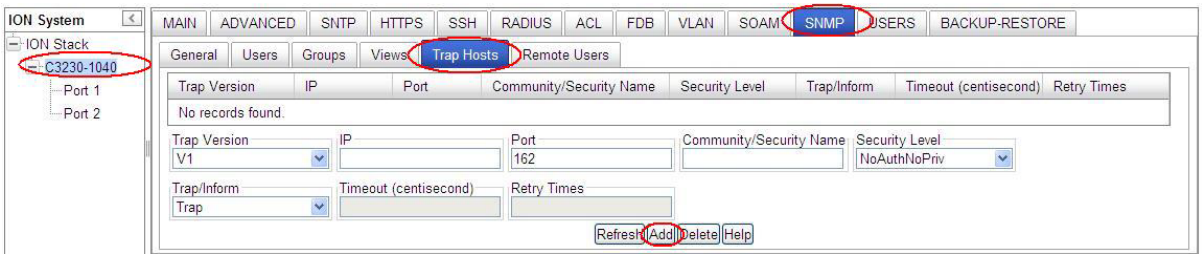
    View Name: enter a name (1-64 characters) for this SNMP view (e.g., ***Default View***, ***Test View*** above).

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

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

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

15. Select the **Trap Host** 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.

    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 can not 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 can not be sent out.

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

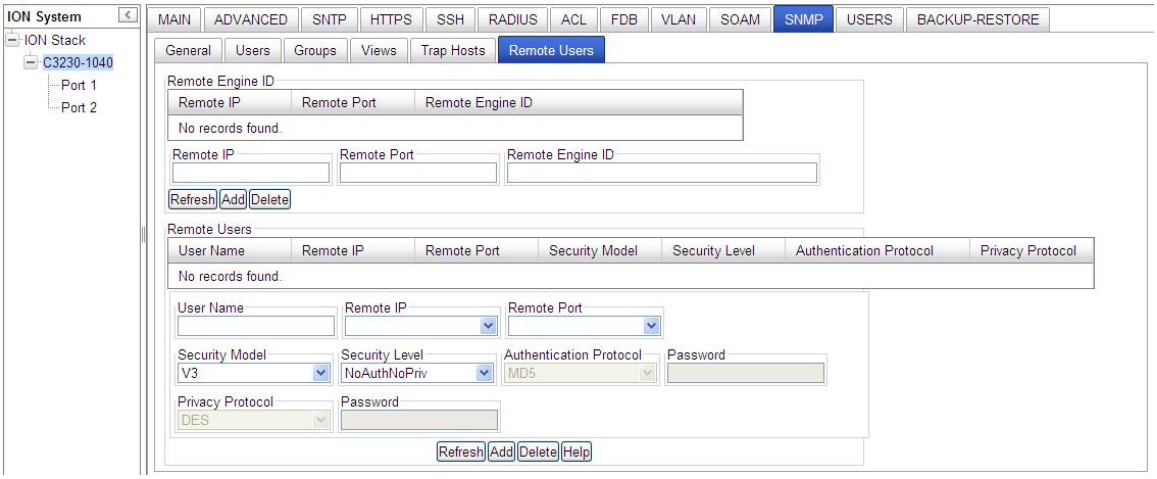
- ***NoAuthNoPriv*** – There is no authentication or encryption used in SNMP communications (the default setting).
- ***AuthNoPriv*** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
- ***AuthPriv*** – SNMP communications use both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

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

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

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

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

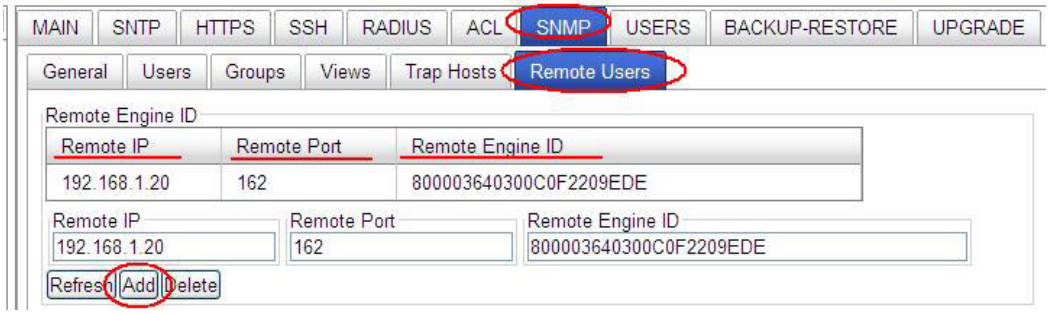


19. Add / Edit the **Remote Engine ID** section fields as required.

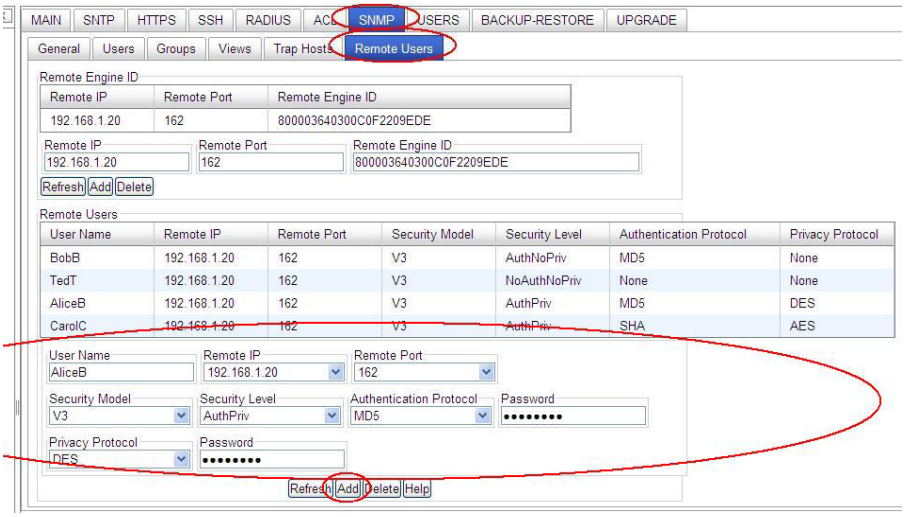
Remote IP: enter the trap host IP address of a remote management station to receive notification messages.

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 can not 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**.

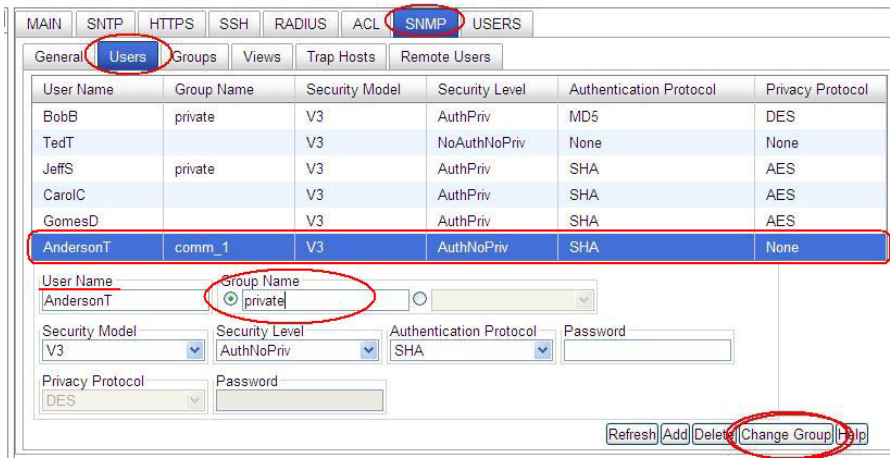
Privacy Password: Enter at least eight plain text characters. The valid range is 8-64 characters.

22. Verify the Remote Users table selections and click the **Add** button when done.
23. Backup the configuration. See "Backup and Restore Operations (Provisioning)" on page 324.

Change a SNMP User's Group - Web Method

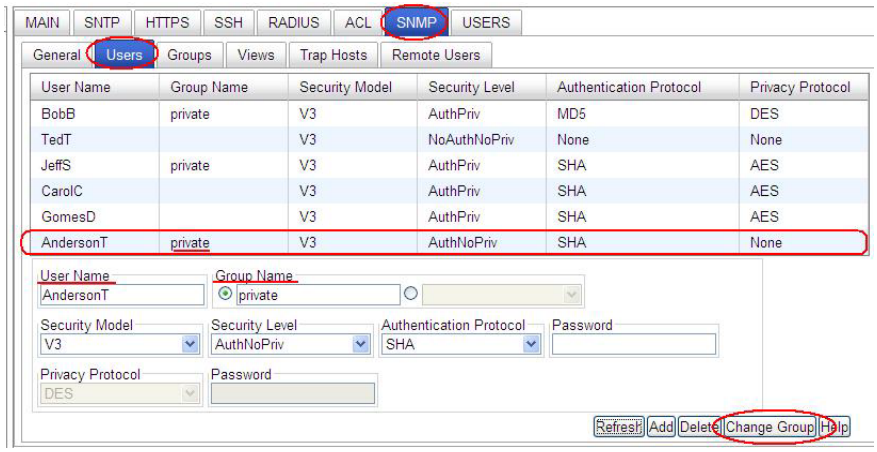
You can change an existing User from one group to another group via the Web interface.

1. Access the IONMM through the Web interface (see "Starting the Web Interface" on page 26).
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.



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.



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 23: 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 24: SNMP v3 Web Interface Default Values

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

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

SNMP v3 Commands

Command Categories

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 28: 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 on page 27 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 on page 27 for more information.

Configuring VLANs, VLAN Management, and VLAN Tunneling

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

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

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

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

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

This section covers VLAN, Management VLAN, and VLAN Tunneling configurations including:

Management VLAN Config - CLI Method on page 265
Management VLAN Config – Web Method on page 269
VLAN Config – Network Port - CLI Method on page 271
VLAN Config – Network Port - Web Method on page 283
VLAN Config – Provider Port – CLI Method on page 284
VLAN Config – Provider Port - Web Method on page 287
VLAN Config – Customer Port – CLI Method on page 291
VLAN Config – Customer Port - Web Method on page 292
VLAN Tunneling on page 296

Note that VLAN and Management VLAN configurations can be configured together or separately.

Configuring Management VLAN

The Management VLAN is used to separate management traffic from other network traffic to and from the x222x/x32xx. 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 x222x/x32xx, you specify a VLAN ID which is to be used for all management traffic to and from the device. The management station that belongs to that VLAN is the only one able to manage the x222x/x32xx. This VLAN ID is given to untagged frames on ingress into the x222x/x32xx. By default it is disabled or zero. When the value is non-zero, the management traffic is expected to be tagged with the management VLAN ID configured when Management VLAN is enabled.

Also when configuring x222x/x32xx Management VLAN, you can specify whether one or several or all of the ports on the x222x/x32xx are part of the Management VLAN. Note that you must create the Management VLAN before you create any other VLANs.

Note before performing this configuration: When you specify a Management VLAN, your Web and Telnet interfaces to the x222x/x32xx are lost, unless the management station (PC) is on the same VLAN. Only management stations in the same VLAN can communicate with the x222x/x32xx through the network. Enabling a Management VLAN does not disable a USB serial interface to the x222x/x32xx.

IMPORTANT

1) When you specify a Management VLAN, your Web and Telnet interfaces to the x222x/x32xx are lost, unless the management station is on the same VLAN. Only management stations in the same VLAN will be allowed to communicate with the x222x/x32xx through the network. If a remote x222x/x32xx is configured, make sure that the management station/PC is part of the same VLAN as the x222x/x32xx.
2) A series of messages display after you enable Management VLAN either via the x222x/x32xx Web interface or the CLI. In both cases, management control is given to the Management VLAN that you enabled. To regain control, turn off Management VLAN via the CLI (**set mgmt vlan state=enable**) or via the Web interface (x222x/x32xx **MAIN** > **Management VLAN Configuration** > **Status** = **Enabled**).
3) Enabling a Management VLAN does not disable a USB serial interface to the x222x/x32xx.
4) See Appendix B for VLAN tab factory default settings.

The following configuration restrictions apply to the x222x/x32xx Management VLAN feature:

1) For Management VLAN, a VLAN ID of 2-4094 is valid. The default is a VLAN ID of VID 2.
2) Management VLAN status can not 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).
4) Management VLAN can be enabled in "Network" mode or "Provider" mode. Before adding the ports for Management VLAN, set the Frame Tag mode of that port to “Network". When Provider tagging is required in that port, then set the Frame Tag mode to "Provider".
5) Port members cannot be checked without first enabling “Network/Provider” mode on those ports (at **Device** > **Port** > **ADVANCED** tab > **VLAN Tag Management** section > **Frame Tag Mode** field).
6) The card must be in “Network” mode (**Port 1** > **Advanced** > **Frame Tag Mode**) to set the VLAN ID. If it is not set to “Network”, an SNMP error will occur.
7) A port with its Frame Tag mode set to "Customer" (default) can not be added to Member Ports for Management VLAN.

The Management VLAN default values for x222x/x32xx NIDs are:

- VLAN ID: **2**
- Port members checked: none
- Status: Disabled

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

Management VLAN Config –CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Check the current Management VLAN configuration. Type **show mgmt vlan config** and press **Enter**.

   Note: In the following three steps to enable Management VLAN, the first is at the port level, the other two steps are at the device level. These three steps (3, 4, and 5) must be performed in the order shown.
3. Change the Management port from default "Customer" mode to "Network" mode.
4. Set this port as Management port. Enter the ports to be associated with this VLAN ID (VID). This sets the device ports which are to be members of this Management VLAN. This is for security, to make some ports non-members, which blocks all management access from this port. If multiple ports are specified, they must be separated by commas with no spaces between the numbers (i.e., **port=1,2,3**).
5. Enable Management VLAN mode. Type **set mgmt vlan state=enable** and press **Enter**.
6. Change the Management VID. Type **set mgmt vlan vid=10** and press **Enter**. This is the VLAN ID number (2–4094). The default is **2**. This sets the VLAN ID which is to be used for all management traffic to and from the device. The management station that belongs to this VLAN is the only one able to manage the x32xx. By default the VLAN ID is set to 1 (Management VLAN 1 enabled). When the Management VLAN ID value is not 0 or 1, the Management traffic is expected to be tagged with the Management VLAN ID configured when Management VLAN is enabled.
7. Add a VLAN. Type **add vlan vid=10** and press **Enter**.

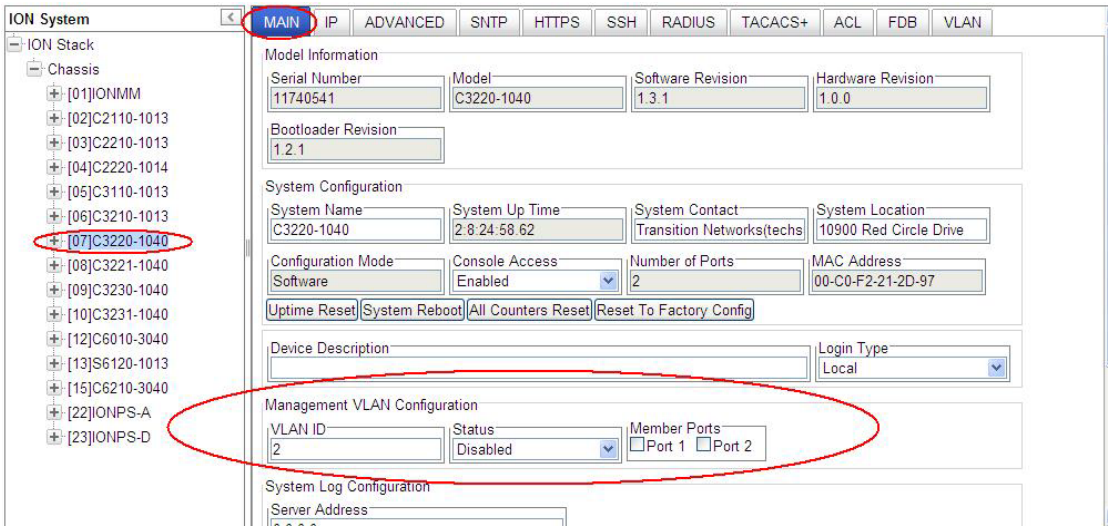
Other Management VLAN or Port VLAN attributes could be changed without strict order. For example:

```
C1|S3|L1P1>set port vlan tag mode=network
C1|S3|L1P1>home
C1|S3|L1D>set mgmt vlan port=1
C1|S3|L1D>set mgmt vlan state=enable
C1|S3|L1D>set mgmt vlan vid=10     << to change the Mgmt VID>>
C1|S3|L1D>add vlan vid=10
C1|S3|L1D>show mgmt vlan config    <<to verify the port VLAN configuration>>
   vlan id   vlan state          vlan portlist
   ---------------------------------------------------------------------------
   2         enable              1
C1|S3|L1D>set port vlan tag mode=network
C1|S3|L1D>set mgmt vlan port=2
C1|S3|L1D>set mgmt vlan state=enable
C1|S3|L1D>set mgmt vlan vid=10
C1|S3|L1D>add vlan vid=10
C1|S3|L1D>show mgmt vlan config
   vlan id   vlan state          vlan portlist
   ---------------------------------------------------------------------------
   3         enable              1


C1|S3|L1D>go l1p=1
C1|S3|L1P1>set port default-vid or set port force-default-vid
```

```
C1|S3|L1P1>set port=discard-tagged or set port=discard-untagged
C1|S3|L1P1>set port mgmtaccess=enable    <<to configure port vlan>>
C1|S3|L1P1>show port vlan config     <<to verify the port VLAN configuration>>
    C1|S3|L1P1> go l1p=2
    C1|S3|L1P1>show port vlan config
    Dot1q state:                  vlanEnabled
    Discard-tagged:               false
    Discard-untagged:             false
    Default VLAN id:              5
    Force use default VLAN id:    true
C1|S3|L1P1>
```

Management VLAN Config –Web Method

1. Access the x222x/x32xx via the Web interface (see "Starting the Web Interface" on page 45).
2. At the device's **MAIN** tab, locate the **Management VLAN Configuration** section.



3. In the **VLAN ID** field, enter the **VLAN ID** number. The valid range is from 2–4094. This sets the VLAN ID which is to be used for all management traffic to and from the device.
   The management station that belongs to this VLAN is the only one able to manage the x222x/x32xx. By default the VLAN ID is set to 2). When the value is not 0 or 1, the Management traffic is expected to be tagged with the Management VLAN ID configured when Management VLAN is enabled.
4. In the **Status** field, select **Enabled**. This enables a secure channel for all associated management traffic. The default Status is Disabled.
5. In the **Member Ports** field, select the ports to be associated with this VLAN ID (VID).
   This sets the ports on this device which are to be members of this Management VLAN.
   This is for security, as some ports can be made non-members, which blocks all management access from this port. Check the checkbox for ports that you want to be VLAN member ports. The default is all Ports unchecked (not associated with this VID).
6. Scroll to the bottom and click the **Save** button.

Configuring VLANs – Network / Provider / Customer Mode

The following sections document how to configure VLAN network, provider and customer modes via the CLI and Web interface.

VLAN Config – Network Port - CLI Method

In a VLAN enabled network, you can assign a VLAN as a Management VLAN. The VLAN ID will be used in all management frames. This separates the management traffic from the data. Network mode is the normal network operating mode. It can take untagged and 802.3ac tagged frames. In this mode, Management VLAN can be enabled on the interface. Frames with an ethertype of 0x8100 are considered as tagged.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Check the current VLAN configuration. Type **show vlan config** and press **Enter**.
3. Define VLAN VID 10 port 2 tagging.
   Type **set vlan vid=10 port=2 memetag=<**noMod|notMember|tag|unTag> and press **Enter**.
4. Enable or disable Priority Override for VLAN VID 10 as desired.
   Type **set vlan vid 10 pri-override=**<enable|disable> and press **Enter**.
5. Set the Priority level for VLAN VID 10. Type **set vlan vid 10 priority 2** and press **Enter**.
6. Enable and configure Management VLAN as required; see previous section.
7. Switch to the applicable port. Type **go l1p=1** and press **Enter**.
8. Set the port's VLAN tagging mode to **Network**. Type **set port vlan tag mode=network** and press **Enter**.
9. Verify the VLAN configuration. Type **show vlan config** and press **Enter**.

Configure the x222x/x32xx and each of the ports as required. An example is provided on the next page.

Example (VLAN Config – Network Port - CLI Method):

The following command sequence places the NID in VLAN 10, creates a Network port, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

```
C1|S3|L1D>set vlan vid 10 port 2 memetag<noMod|notMember|tag|unTag>
C1|S3|L1D>set vlan vid 10 pri-override<enable|disable>
C1|S3|L1D>set vlan vid 10 priority 2
C1|S3|L1D>go l1p=1
C1|S3|L1P1>set port vlan tag mode<network>
C1|S3|L1P1show vlan config
vid:10       fid:0       priority:2         priv_override:disable
port1:     noMod  port2:     Tag
C1|S3|L1P1
```

Enable and configure Management VLAN as required; see previous section.

This procedure places the NID in the VLAN specified, creates a Network port, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

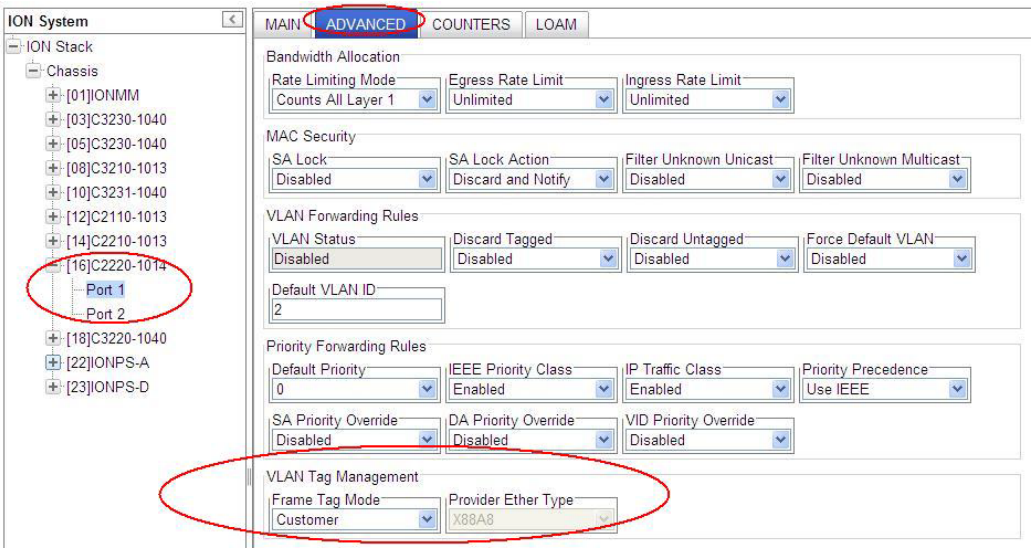
VLAN Config – Network Port - Web Method

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

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Click the **Save** button.
3. Select the desired port's **ADVANCED** tab.
4. Locate the **VLAN Forwarding Rules** section.

5. For each Port, at the **ADVANCED** tab in the **VLAN Forwarding Rules** section:
   a) Set **Discard Tagged** to Enabled or Disabled (the default is Disabled).
   b) Set **Discard Untagged** to Enabled or Disabled (the default is Disabled).
   c) Set **Force Default VLAN** to Enabled or Disabled (the default is Disabled).
   d) Set the **Default VLAN ID** to <**2**-4094>. The default is VID **2**.
6. Locate the **VLAN Tag Management** section.

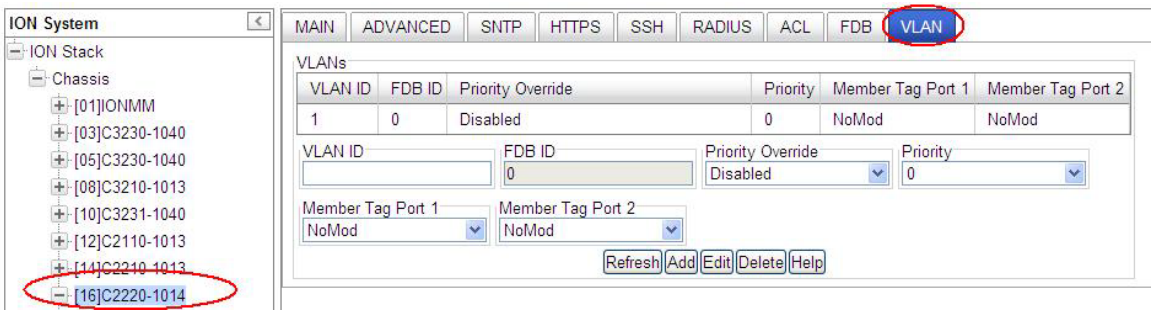
7. For each port, at the **Frame Tag Mode** field, select **Network**.



8. Note: Leave the Provider Ether Type field at the default setting. The Provider Ether Type field is not selectable when the Frame Tag Mode is set to Network.

9. If required, enable and configure **Management VLAN**; see the previous section.

10. Select the x222x/x32xx **VLAN** tab.



11. Create VLAN VID **10**:

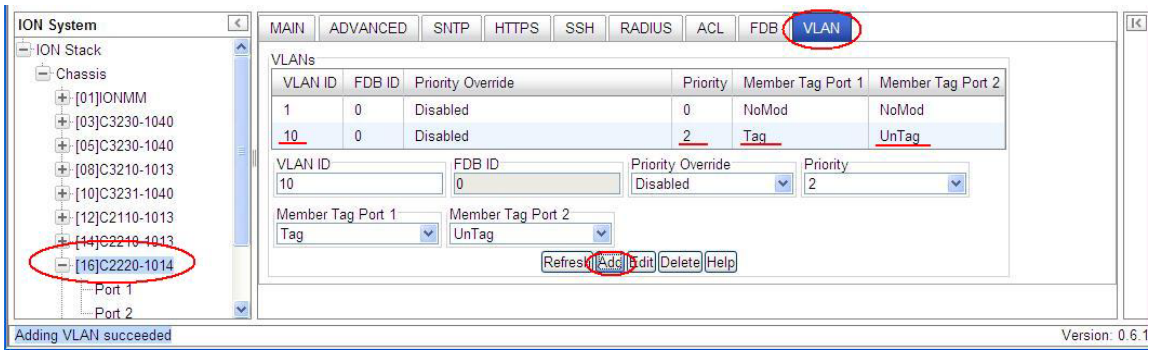
    a) In the **VLAN ID** field, enter **10**.

    b) At the **Priority Override** dropdown, select **Disabled**.

    c) At the **Priority** dropdown, select **2**.

    d) At the **Member Tag Port x** dropdowns, select **noMod**, **notMember**, **tag**, or **unTag** as the membership / action for this VID. Set each of the ports as not a member of the VLAN, or to either not modify, or add a tag to, or remove the tag from management traffic.

12. Click the **Add** button to add the new VLAN to the VLANs table.



13. Click the **Save** button when done. The example above shows **VLAN VID 10** added with **Priority 2** with **Member Tag Port 1** set to **Tag** and **Member Tag Port 2** set to **Untag**.

Enable and configure Management VLAN as required; see previous section.

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

VLAN Config – Provider Port – CLI Method

In a VLAN enabled network, you can assign a VLAN as a Management VLAN. The VLAN ID will be used in all management frames. This separates the management traffic from the data.

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

Use the following steps to configure Management VLAN over S-tag for a Provider port.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Check the current VLAN configuration. Type **show vlan config** and press **Enter**.
3. Define VLAN VID 10 port 2 tagging.
   Type **set vlan vid=10 port=2 memetag=<**noMod|notMember|tag|unTag> and press **Enter**.
4. Enable or disable VLAN VID 10 Priority Override as desired.
   Type **set vlan vid 10 pri-override=**<enable|disable> and press **Enter**.
5. Set the Priority level for VLAN VID 10. Type **set vlan vid 10 priority 2** and press **Enter**.
6. Enable Management VLAN. Type **set mgmt vlan state**=**enable** and press **Enter**.
7. Switch to the applicable port. Type **go l1p=1** and press **Enter**.
8. Set the port's VLAN tagging mode to **Network**. Type **set port vlan tag mode=provider** and press **Enter**.
9. Set the provider port's VLAN tag EtherType.
   Type **set port vlan tag provider ethtype**=<x8100|x88a8|x9100> and press **Enter**.
10. Verify the VLAN configuration. Type **show vlan config** and press **Enter**.

Configure the x222x/x32xx and each of the ports as required. An example is provided on the next page.

Example (VLAN Config – Provider Port - CLI Method):
The following command sequence places the NID in VLAN 10, creates a Provider port, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

```
C1|S3|L1D>set vlan vid 10 port 2 memetag<noMod|notMember|tag|unTag>
C1|S3|L1D>set vlan vid 10 pri-override<enable|disable>
C1|S3|L1D>set vlan vid 10 priority 2
C1|S3|L1D>go l1p=1
C1|S3|L1P1>set port vlan tag mode=provider
C1|S3|L1P1>set port vlan tag provider ethtype=<x8100|x88a8|x9100>
C1|S3|L1P1>show vlan config
vid:10       fid:0       priority:2         priv_override:disable
port1:     noMod  port2:     Tag
C1|S3|L1P1>
```

Enable and configure Management VLAN as required; see the previous section.

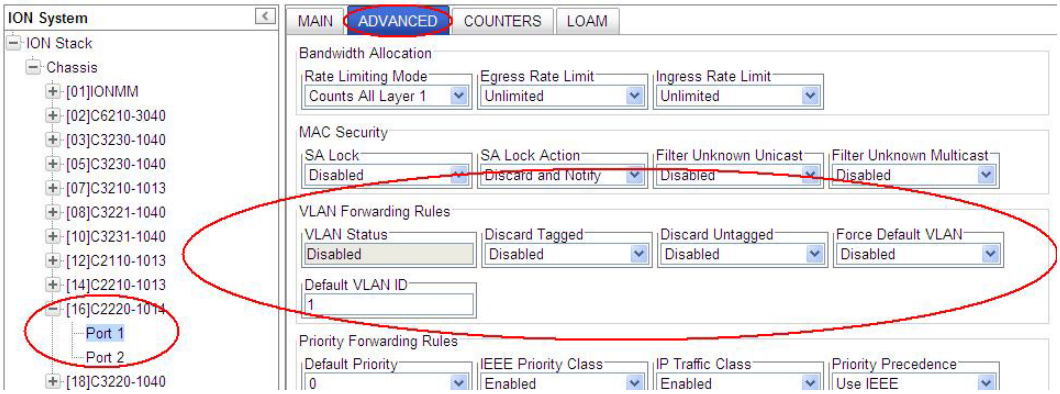
This procedure places the NID in the VLAN specified, creates a Provider port, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

VLAN Config – Provider Port – Web Method

In a VLAN enabled network, you can assign a VLAN as a Management VLAN. The VLAN ID will be used in all management frames. This separates the management traffic from the data.

Use the following steps to configure Management VLAN over S-tag.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the desired port's **ADVANCED** tab.
3. Locate the **VLAN Forwarding Rules** section.



4. For each Port, at the **ADVANCED** tab in the **VLAN Forwarding Rules** section:

   a) Set **Discard Tagged** to Enabled or Disabled (the default is Disabled).

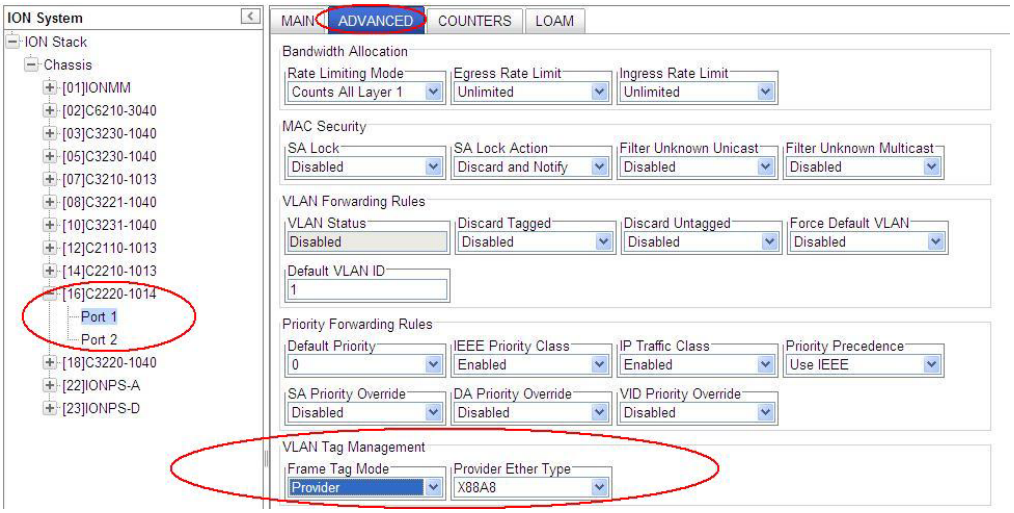
   b) Set **Discard Untagged** to Enabled or Disabled (the default is Disabled).

   c) Set **Force Default VLAN** to Enabled or Disabled (the default is Disabled).

   d) Set the **Default VLAN ID** to <**2**-4094>. The default is VID **2**.

5. Locate the **VLAN Tag Management** section.

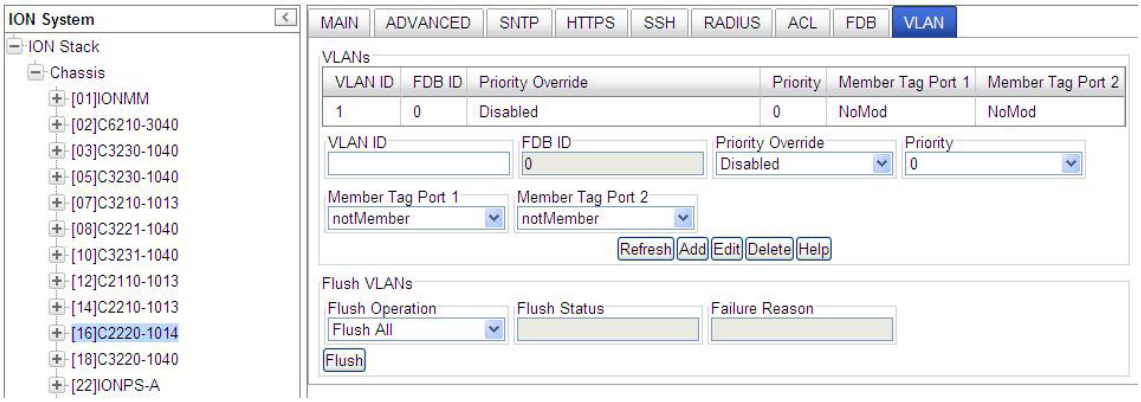
6. At the **Frame Tag Mode** field, select **Provider**.



7. At the **Provider Ether Type** field, select **X8100**, or **X9100**, or **X88A8**. In Provider mode, a frame is considered Provider tagged if it matches the 'Provider Ether Type'. Frames that are ingress with a Provider tag are stripped of their Provider tag on egressing this interface. If the frame's Ethertype doesn't match the **Provider Ether Type** it is considered as untagged. The default **x88a8**.

8. Click the **Save** button.

9. Select the x222x/x32xx **VLAN** tab.



10. Create VLAN VID **10**:

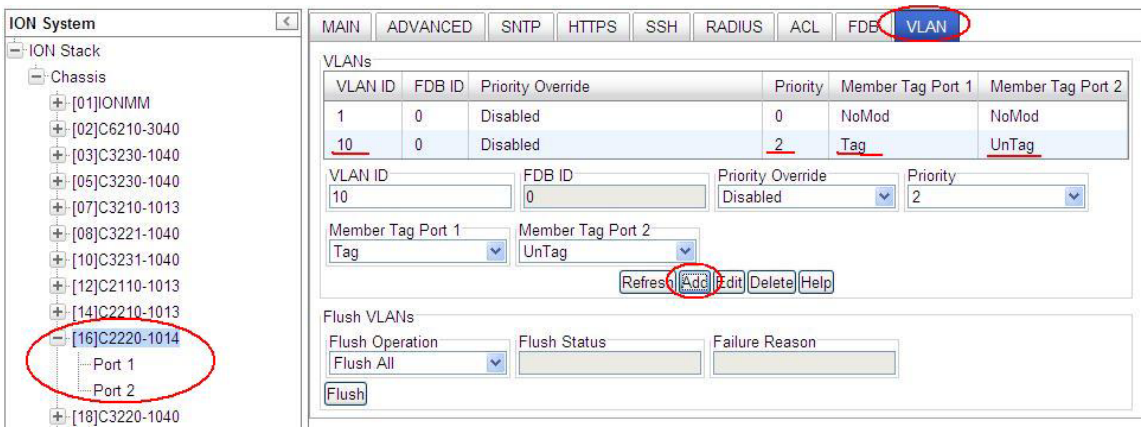
    a) In the **VLAN ID** field, enter **10**.

    b) At the **Priority Override** dropdown, select **Disabled**.

    c) At the **Priority** dropdown, select **2**.

    d) At the **Member Tag Port x** dropdowns, select **NoMod**, **UnTag**, **Tag**, or **notMember** as the membership / action for this VID. Set each of the ports as not a member of the VLAN, or to either not modify, or add a tag to, or remove the tag from management traffic.

11. Click the **Add** button to add the new VLAN to the VLANs table.



12. Click the **Save** button when done. The example above shows **VLAN VID 10** added with **Priority 2** with **Member Tag Port 1** set to **Tag** and **Member Tag Port 2** set to **Untag**.

This procedure places the x222x/x32xx in the VLAN specified, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

Enable and configure Management VLAN as required; see previous section.

Use the **Flush Operation** functions as needed; see the "Flush VLAN Databases Config" section on page 198.

VLAN Config – Customer Port – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Check the current VLAN configuration. Type **show vlan config** and press **Enter**.
3. Define VLAN VID 10 port 2 tagging.
   Type **set vlan vid=10 port=2 memetag=<**noMod|notMember|tag|unTag> and press **Enter**.
4. Enable or disable VLAN VID 10 Priority Override as desired.
   Type **set vlan vid 10 pri-override=**<enable|disable> and press **Enter**.
5. Set the Priority level for VLAN VID 10. Type **set vlan vid 10 priority 2** and press **Enter**.
6. Switch to the applicable port. Type **go l1p=2** and press **Enter**.
7. Set the port's VLAN tagging mode to **Network**. Type **set port vlan tag mode=customer** and press **Enter**.
8. Verify the Management VLAN configuration. Type **show mgmt vlan config** and press **Enter**.
9. Verify the VLAN configuration. Type **show vlan config** and press **Enter**.

Enable and configure Management VLAN as required; see previous section.

Configure the x222x/x32xx and each of the ports as required. An example is provided below.

Example (VLAN Config – Customer Port - CLI Method):
The following command sequence places the NID in VLAN 10, creates a Customer port, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

```
C1|S3|L1D>set vlan vid 10 port 2 memetag<noMod|notMember|tag|unTag>
C1|S3|L1D>set vlan vid 10 pri-override<enable|disable>
C1|S3|L1D>set vlan vid 10 priority 2
C1|S3|L1D>go l1p=1
C1|S3|L1P1>set port vlan tag mode<customer>
C1|S3|L1P1>show vlan config
vid:10       fid:0       priority:2         priv_override:disable
port1:     noMod  port2:     Tag
C1|S3|L1D>
```

Enable and configure Management VLAN as required; see previous section.

This procedure places the NID in the VLAN specified, creates a Customer port, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

VLAN Config – Customer Port - Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the desired port's **ADVANCED** tab.
3. Locate the **VLAN Forwarding Rules** section.

4. For each Port, at the **ADVANCED** tab in the **VLAN Forwarding Rules** section:

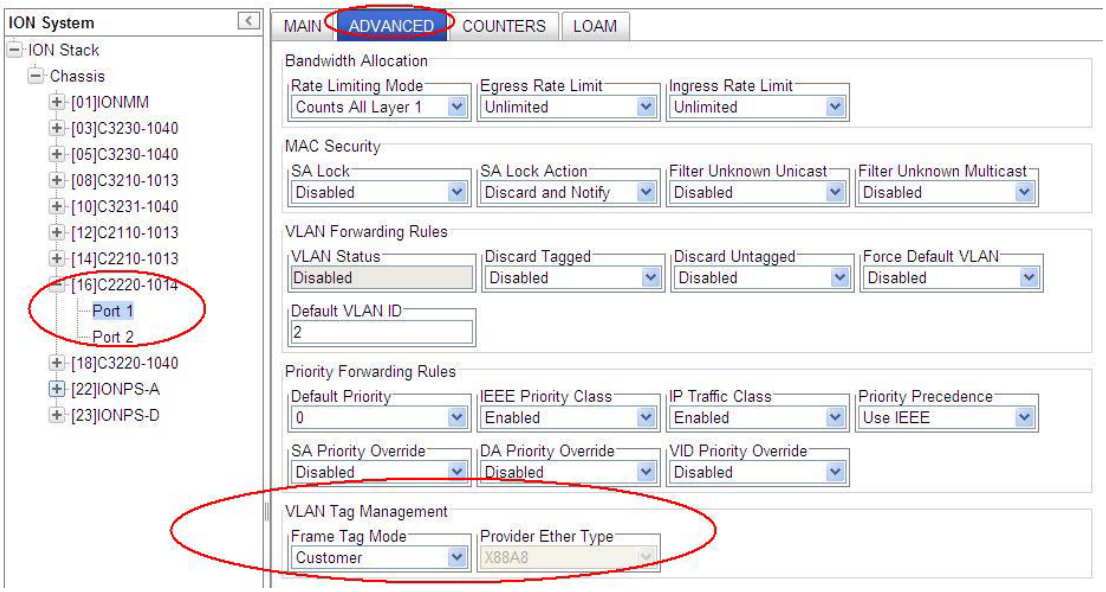
   a) Set **Discard Tagged** to Enabled or Disabled (the default is Disabled).

   b) Set **Discard Untagged** to Enabled or Disabled (the default is Disabled).

   c) Set **Force Default VLAN** to Enabled or Disabled (the default is Disabled).

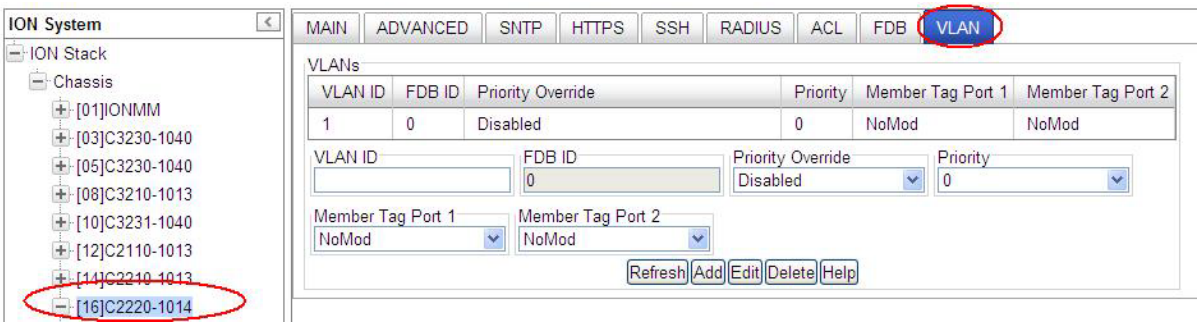
   d) Set the **Default VLAN ID** to <**2**-4094>. The default is VID **2**.

5. Locate the **VLAN Tag Management** section.
6. For each port, at the **Frame Tag Mode** field, select **Customer**.



Note: the **Provider Ether Type** field is not selectable when the **Frame Tag Mode** is set to **Customer**.

7. Select the x222x/x32xx **VLAN** tab.



8. Create VLAN VID **10**:

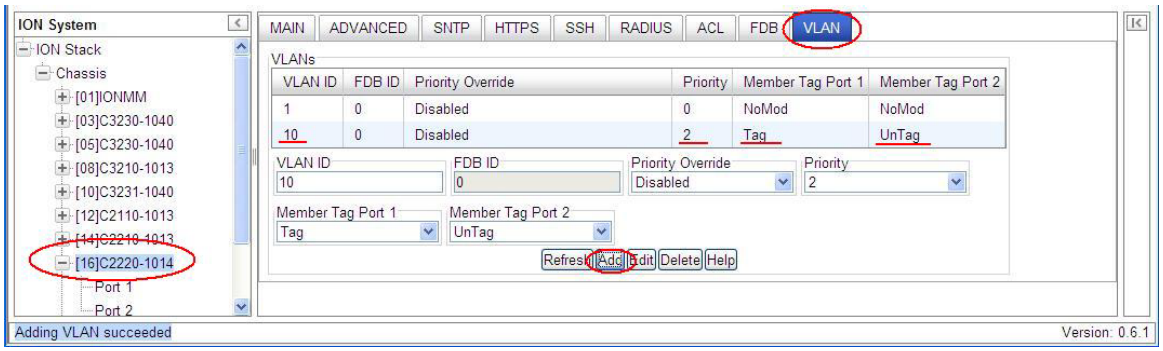
   a) In the **VLAN ID** field, enter **10**.

   b) At the **Priority Override** dropdown, select **Disabled**.

   c) At the **Priority** dropdown, select **2**.

   d) At the **Member Tag Port x** dropdowns, select **NoMod**, **NotMember**, **Tag**, or **UnTag** as the membership / action for this VID. Set each of the ports as not a member of the VLAN, or to either not modify, or add a tag to, or remove the tag from management traffic.

9. Click the **Add** button to add the new VLAN to the VLANs table.



10. Click the **Save** button when done. The example above shows **VLAN VID 10** added with **Priority 2** with **Member Tag Port 1** set to **Tag** and **Member Tag Port 2** set to **Untag**.

This procedure places the x222x/x32xx in the VLAN specified, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

Enable and configure Management VLAN as required; see the previous section.

Use the **Flush Operation** functions as needed; see the "Flush VLAN Databases Config" section below.

Flush VLAN Databases Config

You can delete (flush) the VLAN FID DB and the VLAN DB entries via the x222x / x32xx CLI or the Web interface.

Flush FID DB – CLI Method

The **flush fiddb type** command is a port level command that clears the dynamic entries or all of the entries in the VLAN forwarding information database. **Note**: The **flush fiddb type=dynamic** command only deletes the dynamic entries; it does not affect the static, staticNRL, or staticPA Entry Types. The **flush fiddb type=all** command deletes all of the Entry Types (static, staticNRL, staticPA, and dynamic) for all FIDs.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enter the CLI command to Flush the VLAN FID. Type **flush fiddb type**=<all|dynamic> and press **Enter**. The message "*Flushing fiddb is in progress!*" displays momentarily. If the Flush FID DB process completes successfully, the message "*Flush VLANdb succeeded!*" displays.

Example:

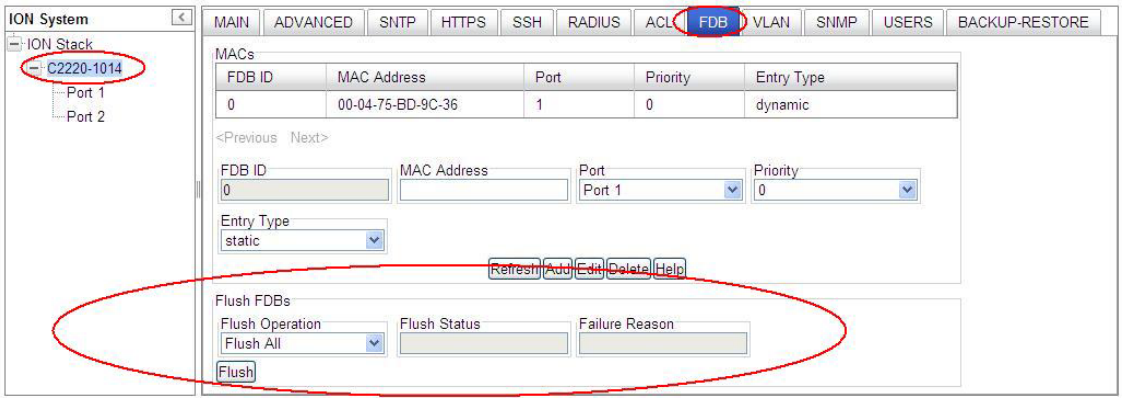
```
C1|S1|L1D>flush fiddb type ?
  all
  dynamic
C1|S1|L1D>flush fiddb type dynamic
Cannot flush vlandb on this card!
C1|S1|L1D>go c=1 s=3 l1d
C1|S3|L1D>flush fiddb type dynamic
Flushing fiddb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>flush fiddb type all
Flushing fiddb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>
```

The VLAN FID database flush operation status displays **failure** to indicate the last flush operation failed.

Note: if a FID Db flush operation is currently in progress, wait for the "*Flush VLANdb succeeded!*" message before starting another FID DB flush process.

Flush FID DB – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the device's **FDB** tab.



3. In the **Flush VLANs** section at the **Flush Operation** dropdown, select **Flush All** or **Flush All Dynamic** and click the **Flush** button. The webpage message "*Are you sure to flush all*?" displays.
   If this is the operation that you want, click the **OK** button. The "*Flush is being processed*" message displays momentarily.

   If the Flush was successful, the **Flush Status** field displays "***Success***".
   If the Flush was unsuccessful, the **Failure** field displays the reason for the Flush failure. See "Section 6: Troubleshooting" on page 271 for the set of **Failure Reason** codes that may be displayed.

Note: The **Flush All Dynamic** selection only deletes the dynamic entries; it does not affect the static, staticNRL, or staticPA Entry Types. The **Flush All** selection deletes all of the Entry Type entries (static, staticNRL, staticPA, and dynamic) for all FIDs.

Flush VLAN DB – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enter the CLI command to flush the VLAN FID. Type **flush vlandb=all** and press **Enter**. This is a port level command to erase all VLAN database entries except for the default VLAN database entry (which cannot be deleted).
3. The message "*Flushing VLANdb is in progress!*" displays momentarily. If the Flush FID DB process completes successfully, the message "*Flush VLANdb succeeded!*" displays.

For example:

```
C1|S1|L1D>flush vlandb ?
  all
C1|S3|L1D>flush vlandb all
Flushing VLANdb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>
```

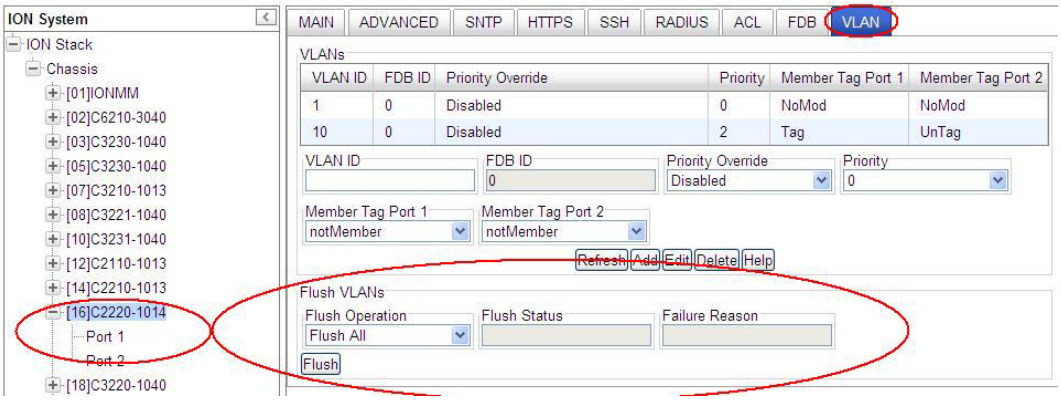
The VLAN database flush operation status displays **failure** to indicate the last flush operation failed.

Note: if a FID Db flush operation is currently in progress, wait for the "*Flush VLANdb succeeded!*" message before starting another FID DB flush process.

VLAN Db Flush Operation Status
The current VLAN database flush operation status; either:
unknown: no flush operation has been performed.
success: the last flush operation was finished successfully.
failure: indicates the last flush operation failed.
inProgress: a flush operation is currently in progress.

Flush VLAN DB – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the device's **VLAN** tab.



3. In the **Flush VLANs** section at the **Flush Operation** dropdown, select **Flush All** and click the **Flush** button. The web page message "*Are you sure to flush all*?" displays. If this is the operation that you want, click the **OK** button. The "*Flush is being processed*" message displays momentarily.

   If the Flush was successful, all of the VLANs in the VLANs table are deleted except for VLAN ID 1, and the **Flush Status** field displays "***Success***".

   If the Flush was unsuccessful, the **Failure** field displays the reason for the Flush failure.

   See "Section 6: Troubleshooting" on page 271 for the set of **Failure Reason** codes that may be displayed.

Configuring VLAN Tunneling (802.1q Tunneling)

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

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

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

VLAN Tunneling accomplishes the following:

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

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

How VLAN Tunneling Works

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

VLAN Tunneling refers to multiple tagging of dot1Q frames as they enter a service provider switch from a client switch. VLAN Tunneling can tag or untag any frames that it receives from the customer tag. VLAN Tunneling also has native VLAN frames that are untagged. The service provider switch adds the outer VLAN tag.
Tagged and untagged customer traffic comes from a port on a customer device and enters the service-provider edge switch through a tunnel port. Each customer edge port that is connected to a VLAN tunnel

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

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

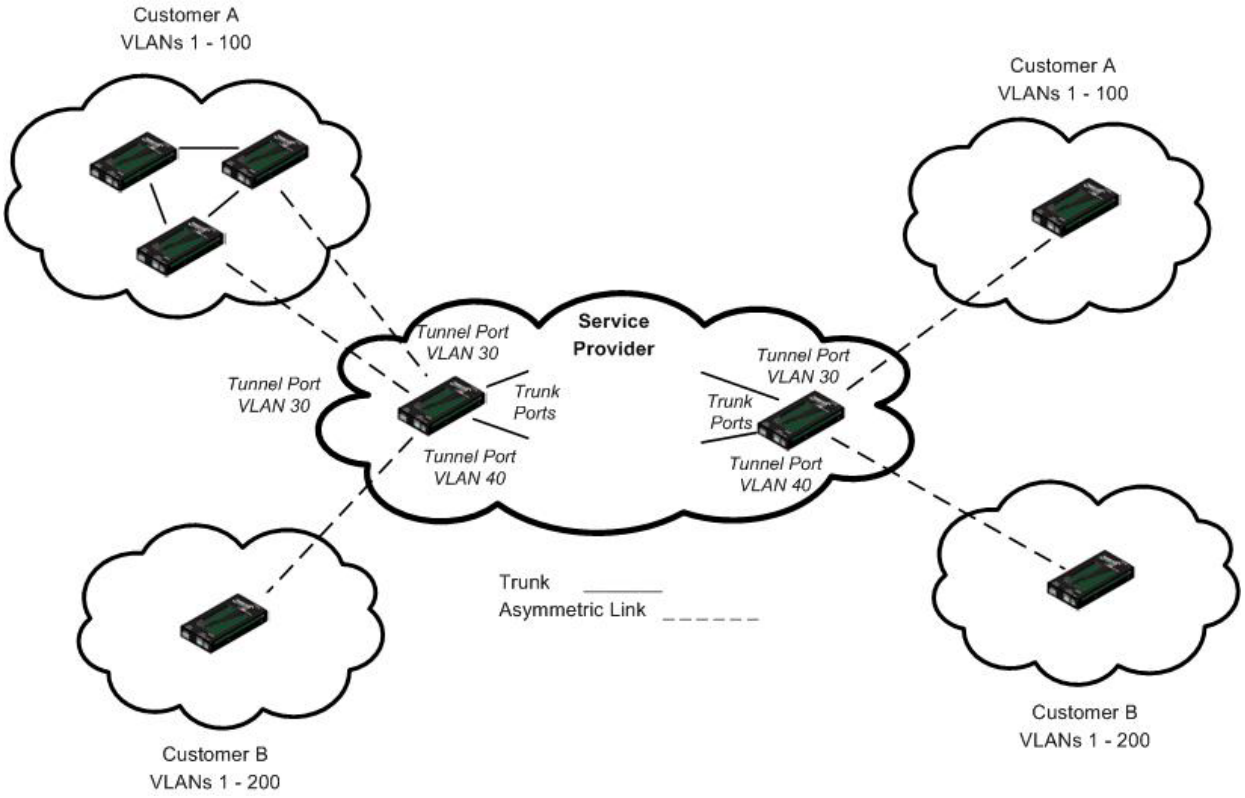


Figure 28: VLAN Tunneling Example

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

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

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

Summary

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

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

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

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

Prerequisites for VLAN Tunneling Functions

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

Restrictions for Configuring VLAN Tunneling Functions

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

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

For specific procedures on configuring VLAN Tunneling via the CLI or Web method, see "Appendix F: VLAN Tunneling Configuration Examples" on page 524.

Configuring QOS

QoS (Quality of Service) can be set up on Lantronix ION modules either:

- At the Layer 2 level using CoS (Class of Service) bits per IEEE 802.1p, or
- at the Layer 3 level based on DSCP/ToS (Differentiated Services Code Point/Type of Service).

QoS (Quality of Service) can be set up on ION modules that support the layer-2 switch QoS functions of priority classification, queuing and remarking. The C2x2x/C3x2x NIDs provide QoS at the Layer 2 level using CoS bits per IEEE 802.1p. The priority bits in the 802.3ac tag can be remapped as frames ingress the device based on Ingress port, Source MAC address, Destination MAC address, or VLAN ID in the 802.1q tag, or on the basis of remapping to a user-defined priority on a per-port basis.

The C2x2x/C3x2x NIDs also provide QoS based on DSCP/ToS bits in the IP header. Three precedence bits have a value from 0 to 7 and are used to indicate the importance of a datagram. The default is 0 (higher indicates more importance). Bits 3, 4, and 5 represent the following:

D: requests low delay

T: requests high throughput

R: requests high reliability

QoS can be configured in the NID using either the CLI or the Web method.

QoS Config – CLI Method

QoS (Quality of Service) allows the bandwidth, error rates and latency to be monitored, sampled and possibly improved. QoS also delivers tools to help deliver data efficiently by reducing the impact of delay during peak times when networks are approaching full capacity. QoS does not add capacity, nor does it multiplex the signals like WDM. QoS simply tries to manage data traffic better so that top priority traffic will not be compromised. QoS helps manage the use of bandwidth by applying a set of tools like priority scheme, so certain packets (mission critical must go packets) are forwarded first.

Note: These commands can only be entered when the last part of the command line prompt indicates the location is a port (LxPx; where x is 1, 2 or 3).

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Select the desired device port.
3. Set the Default Priority for the Port. Type **set qos default–priority={**0-7**}** and press **Enter**.
   For example: C1|S7|L1D>**set qos default-priority 7**.

4. Set a Frame Priority for the Port. Select either:
   - **Destination MAC Address** is Used {enable | disable}
   - **IEEE Tag** is Used {enable | disable}
   - **IP Tag** is Used {enable | disable}
   - **Source MAC Address** is Used {enable | disable}
   - **VLAN ID is Used** {enable | disable}

5. If selected in step 4, set IEEE Priority Remapping.
   Type **set dot1dbridge ieee-tag-priority={0-3} remap-priority={0-7}** and press **Enter**.

6. Set the Ingress Priority Remapping. Type **set qos ingress-priority {0-7} {0-7)}** and press **Enter**.

7. Define the priority remapping for IP traffic.
   Type **set dot1dbridge ip-priority-index={0 – 63} remap-priority={0 – 3}**

8. Set the tag type (IEEE or IP) to be used to decide frame priority type of a port if both tags are available. Type **set qos priority tag–type={useIEEE | useIP}** and press **Enter**.

9. Show the Priority Remapping to verify the selected configuration. Type **show qos priority remapping** and press **Enter**. The QOS Priority Remapping configuration displays:

```
C1|S13|l0ap1|l1p2/>show qos priority remapping
ingress-priority                  remapping-priority
-------------------------------------------------------------------
0                                       0
1                                       1
2                                       2
3                                       3
4                                       4
5                                       5
6                                       6
7                                       7
```

10. Show the QoS Configuration of the port to verify the selected configuration. Type **show qos config** and press **Enter**. The QOS configuration information displays:

```
C1|S16|L1P1>show qos config
Default priority:                              0
Use IEEE tag for priority:                     enable
Use IP tag for priority:                       enable
Tag type for priority if both tag available: useIEEE
Use source MAC address for priority:           disable
Use destination MAC address for priority:      disable
Use VLAN id for priority:                      disable
```

QoS Config – Web Method

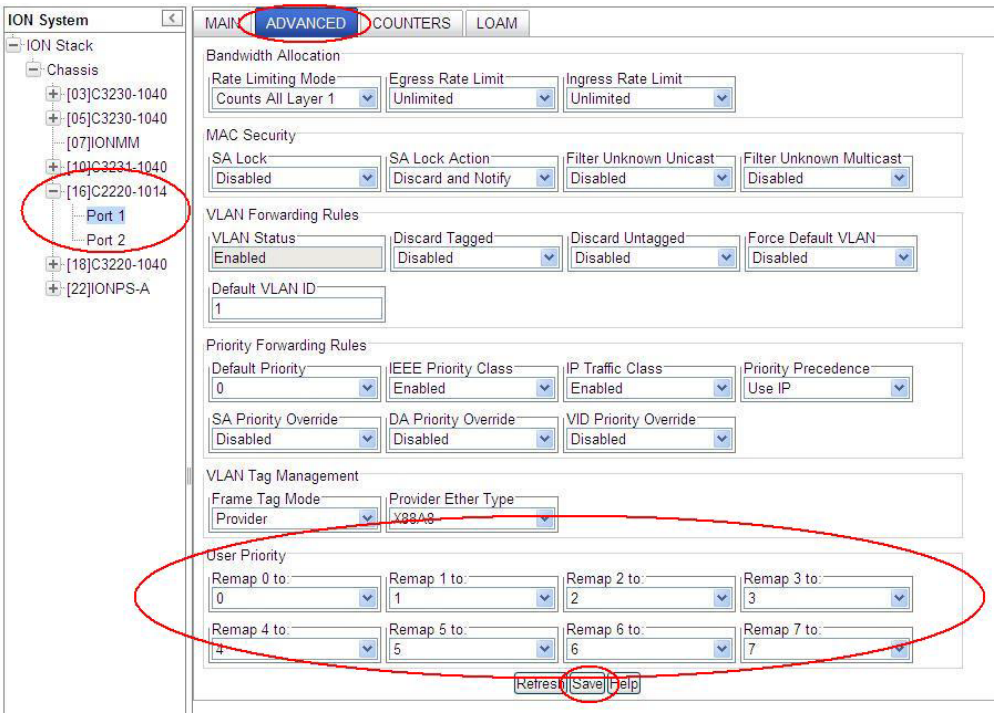
1. Port Priority Queues: Each port contains four different classes of output priority queues.

Priority Queue	Frame Type	Weight
0	Best Effort	1
1	Background	2
2	Excellent Effort	4
3	Critical Applications	8

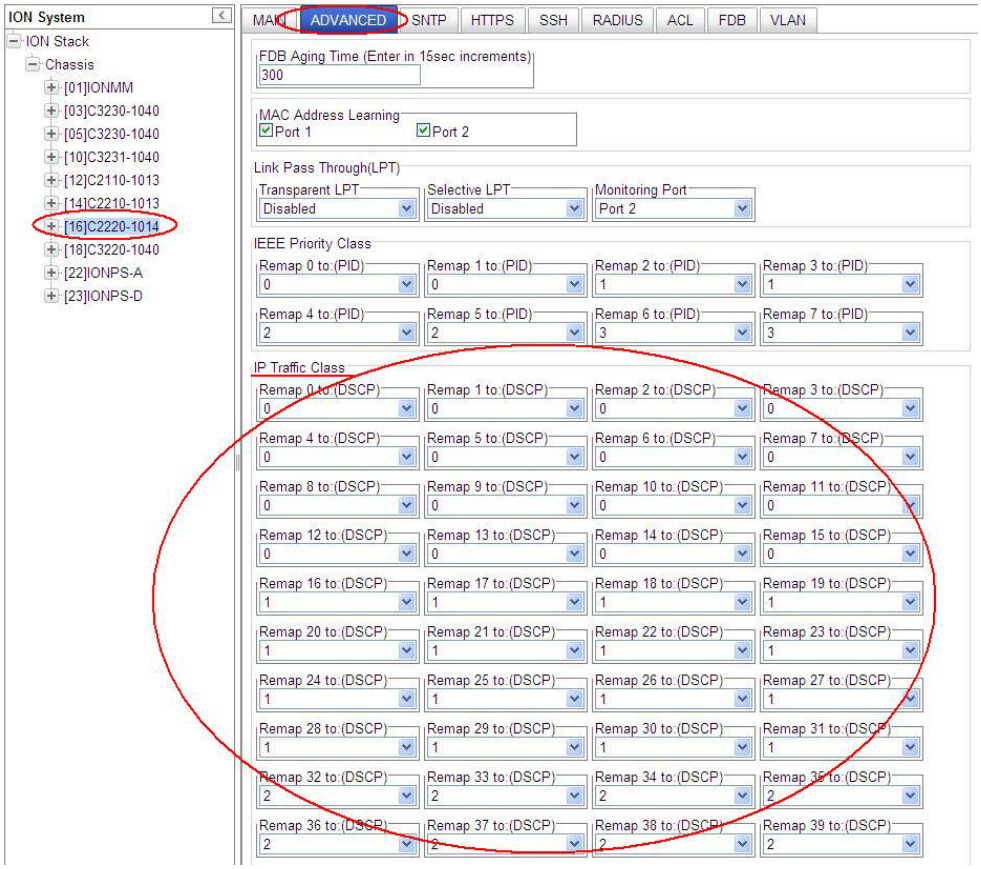
Packets will be transmitted from these queues in weighted round-robin fashion with the weights of 8:4:2:1 for class queues 3, 2, 1 and 0.

2. Classification: Incoming Packets to a port can be classified based on L2 CoS (IEEE 802.1p) or L3 IP DiffServ (IPv4/IPv6) priority field or port default priority. See the Priority Override section for details on how port/L2/L3 classification can be configured per port.

IEEE priority re-mapping: When a packet is classified by L2 CoS priority, it will be re-mapped to another L2 priority value as defined in the per-port priority re-mapping table.



IP Traffic Class priority re-mapping: When a packet is classified by IP priority, it will be re-mapped by the global IP remapping table.



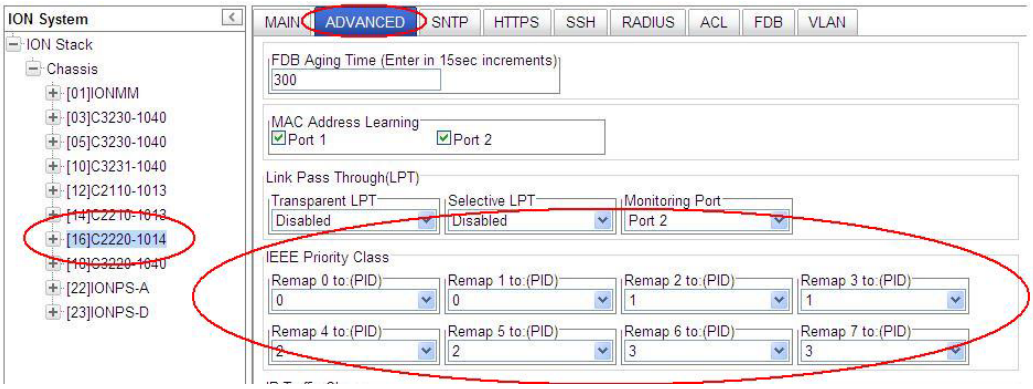
The re-mapped 2-bit priority value would be used for two purposes:

1) These 2-bit class values would directly map to the output queue of the egress port

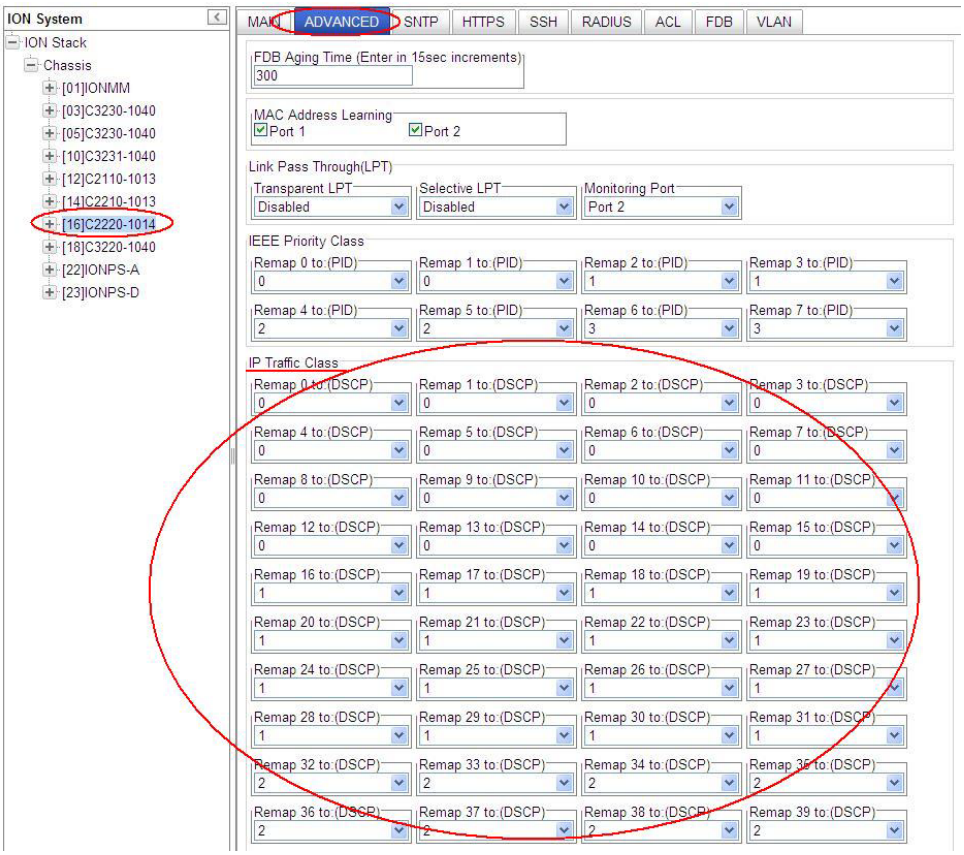
2) Egress priority re-marking of the frame. When the packet is eligible for remarking, it would be scaled up to 3-bits, by borrowing the least significant bit of the port default priority.

3. Queuing: Once the incoming packet is classified/re-mapped based on port/L2/L3 priority, the packet is queued to the egress port queue based on the global system queue remapping table.

a) L2 Priority Queuing: Packet classified by port L2 default or frame L2 priority will be queued based on the "IEEE Priority Class" re-mapping.



b) IP Priority Queuing: Packet classified by IP priority will be queued based on the "IP Traffic Class" remapping table.



4. Classification and Queuing configuration options: The following classification/queuing options are available and can be configured per port at the device port's **ADVANCED** tab.

a) Port default priority: This can be enabled per port by disabling "IEEE Priority Class" and "IP Traffic Class". All frames will be assigned to the port Default Priority. In the following example, port Default Priority has been set to "4".

b) IEEE priority only: This can be configured per port by enabling "IEEE Priority Class" and disabling "IP Traffic Class". All untagged frames (including IP) will be assigned to the port Default Priority.

c) IP priority only: This can be configured per port by enabling "IP Traffic Class" and disabling "IEEE Priority Class". Tagged and non-IP frames will be assigned to the port Default Priority.

d) IP and IEEE priority with the precedence of IP: This can be configured per port by enabling both "IEEE Priority Class" and "IP Traffic Class" and "Priority Precedence" set to "Use IP".

Note: The Tagged IP packet would get queued to one of the egress port priority queues per the global IP-remapping table. However, the remapped IEEE priority value will be used for re-marking the packet.

e) IP and IEEE priority with the precedence of IEEE: This can be configured per port by enabling both "IEEE Priority Class" and "IP Traffic Class" and "Priority Precedence" set to "Use IEEE."

Note: Tagged IP packet would get queued on the egress port as per the global IEEE remapping table.

The last two options above ("d) IP and IEEE priority with the precedence of IP" and "e) IP and IEEE priority with the precedence of IEEE") differ only in how a packet gets queued. The frame re-marking priority works the same way for both options.

5. Priority Override: The initial re-mapped priority value can be further over-ridden by VLAN or per frame SA/DA.

One or more of the following overrides can be enabled per port. Should more than one override match, the following order of priority is applied (i.e., DA would override all others):

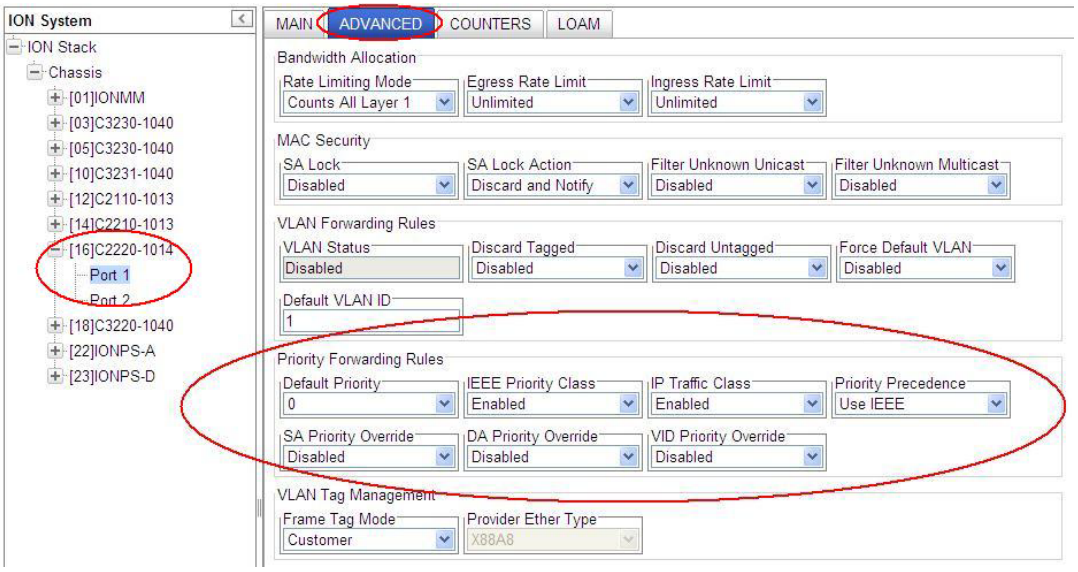
1) **VID** Priority Override

2) **SA** Priority Override

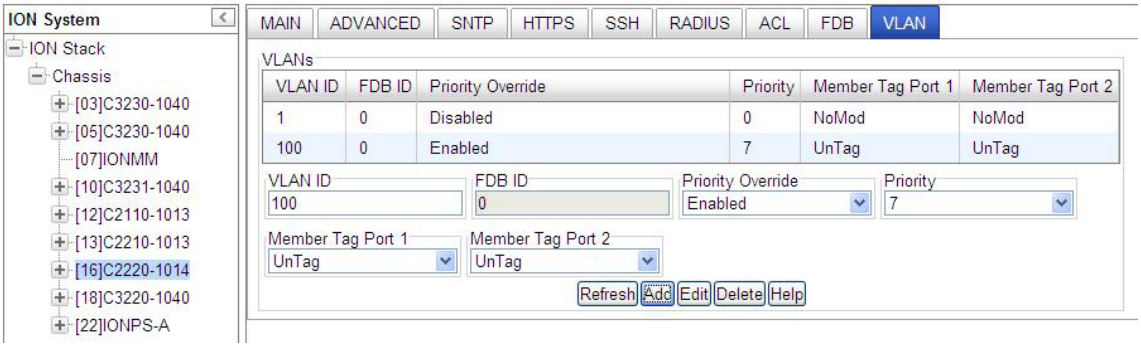
3) **DA** Priority Override

The higher order 2 bits of the VID/MAC priority will be used as the queue re-mapped priority.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the desired Port's **ADVANCED** tab.
3. Locate the **Priority Forwarding Rules** section.

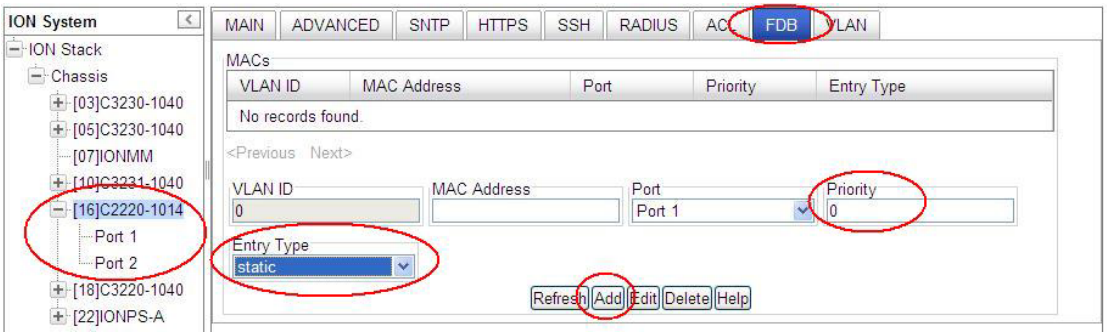


a) VID Priority Override: This requires the VLAN entry to be configured with the desired priority in the VLAN database.

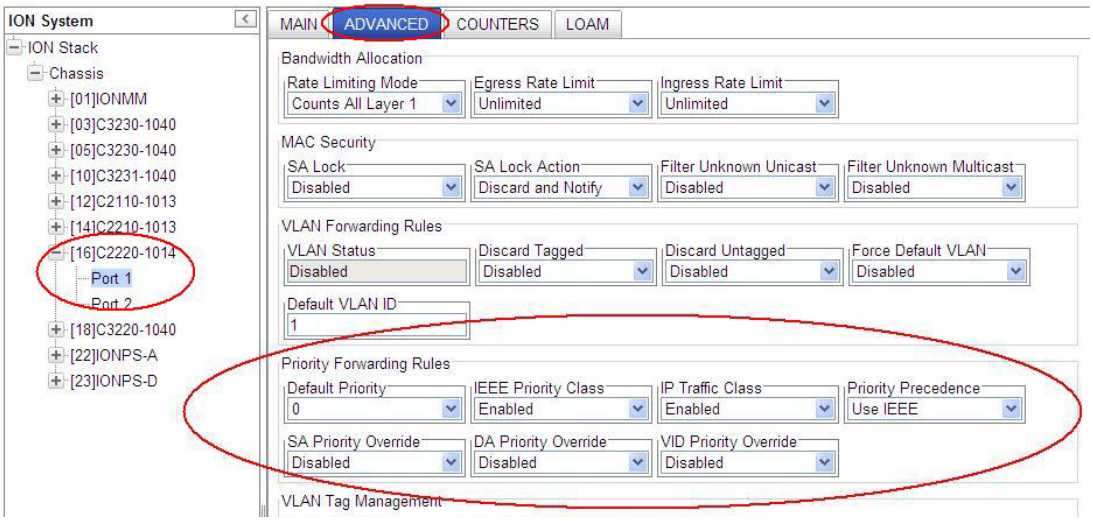


In the above example, the VLAN 100 packets egress on port with the priority marked/remarked to priority "7". The higher 2 bits of the VID priority (0x7) will be used as the queue priority. Hence, the packets will get queued to the output queue "3".

b) SA/DA Priority Override: At the FDB tab, add Priority Override for SA/DA to the MACs table as a static Entry Type with the desired priority.

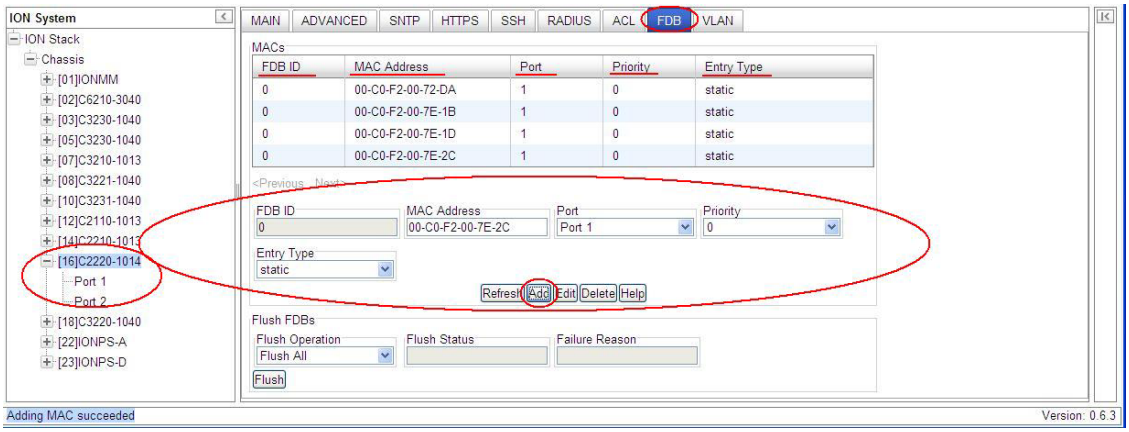


Locate the device port **ADVANCED** tab's **Priority Forwarding Rules** section.



With **SA Priority Override** set to **Enabled**, a frame's Source MAC address (SA) decides the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.

With **DA Priority Override** set to **Enabled**, a frame's Destination MAC address (DA) decides the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.



6. Remapping: Packet IEEE priority could be re-marked with the value assigned during the ingress classification/priority override. This would require proper VLAN configuration with the egress port defined as “memEgressTag” in the VLAN DB. See the “Configuring VLANs” section on page 251 for VLAN configuration application example details.

Configuring Fiber Port Redundancy

The Port Redundancy state can be set to enable or disable on a card with 2 or more fiber ports.

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.

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.

Fiber Port Redundancy Use Cases

For a 3-port card used as a converter, assuming port 2 and 3 are in a group as one side, port 1 as one side; provides the following use cases:

- Case 1 (disabled): no LPT
- Case 2 (Monitoring Port = 1): port 1 down, cause port 2 down, port 3 unchanged.
- Case 3 (monitor port = 2 or 3): port 2 or 3 down, cause port 1 down.
- Case 4 (monitor port = a special number like 100, means all copper ports): all copper ports down causes all fiber ports down.
- Case 5 (monitor port = a special number like 101, means all fiber ports): all fiber ports down causes all copper ports down.

If used as a 3-ports switch, another case could be:

- Case 6 (add a target port in the MIB; like monitor port = port 2, target port = 3): user can use any specific port to do the LPT case any other specific port link up/down.

On a 3-port card, the Customer Port is Port 1, Primary Port is Port 2, Secondary Port is Port 3, and the ‘Active Port’ is the Port that on which the Redundancy function is active.

Fiber Port Redundancy can be configured in the NID using either the CLI or Web method.

Redundancy Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Set the Redundancy state to enable. Type: **set redundancy state**=<state>

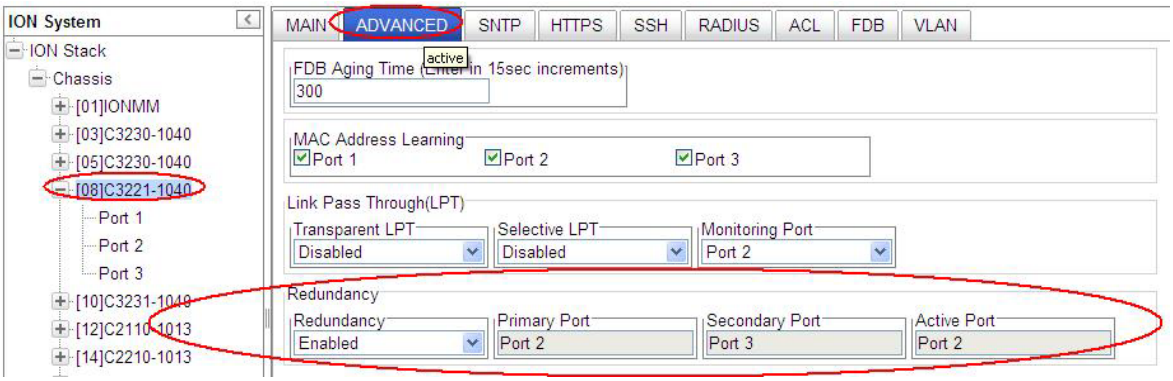
   where:
   state = enable or disable
3. Press **Enter**.
4. Verify the configuration has been set. Type **show redundancy info** and press **Enter**.
   The port's redundancy state displays. For example:

```
C1|S18|L1D>show redundancy info
Redundancy is not supported on this card!
C1|S18|L1D>go s=8 l1d
C1|S8|L1D>show redundancy info
Redundancy information:
------------------------------------------------------------------------
Port redundancy state:                  enable
Primary port:                           2
Secondary port:                         3
Active port:                            2
C1|S8|L1D>
```

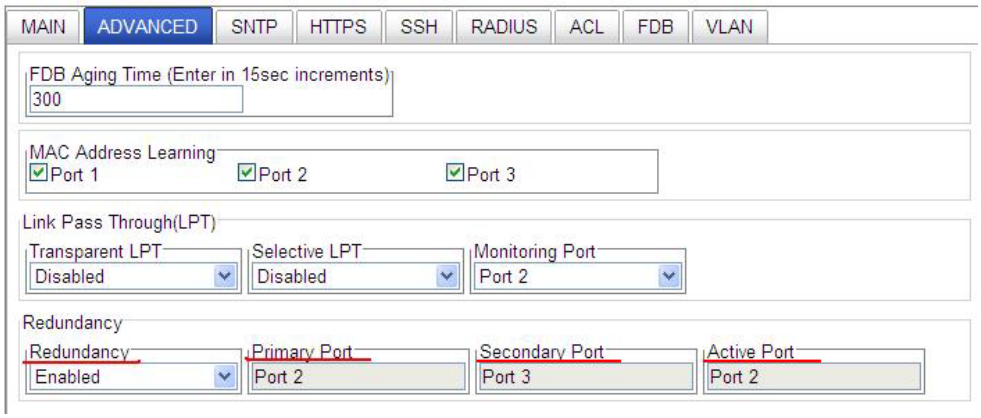
Redundancy Config – Web Method

Note: With the fiber port Redundancy state set to enabled, a Primary Port, Secondary Port, and/or Active Port may still display with the field grayed out.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **ADVANCED** tab.



3. Locate the **Redundancy** section.
4. Set the **Primary Port** and **Secondary Port** redundancy (failover) port numbers.
   The default configuration is Redundancy = Disabled, Primary Port = 2, Secondary Port = N/A, and Active Port = 1.
5. Select Redundancy **Enabled**.
6. Click **Save** and then click **Refresh**. The Redundancy configuration shows Primary Port = 2, Secondary Port = 3, and Active Port = 2.



Configuring L2CP

Layer 2 Control Protocol (L2CP) processing is supported, allowing each of the layer 2 control protocols to be passed or discarded. L2CP is supported at a per-port level.

Layer 2 Control protocols are designed to interact with various entities and peer-entities for the proper flow of Layer-2 traffic though the network. Depending on the customer's network configuration or the operator's service offering, this traffic is handled in one of three ways:

1. **Pass** 'as-is' between network-side and customer-side ports. "Peer" (pass) means that the MEN will actively participate with the Customer Equipment (CE). This is the default setting (pass to an EVC for tunneling).
2. **Discard** so that no specified L2CP traffic is ingressed, as this may lead to network instability. "Discard" means that the MEN will discard ingress L2CP frames of a given protocol, and will not generate that protocol on egress from the MEN.
3. **Tunnel** encapsulated traffic to another x222x / x32xx NID to allow a network operator to offer a transparent Ethernet service. "Tunnel" means that frames associated with a given protocol are transparently passed to a given EVC for transport across the MEN to the destination UNI.

The MEF (Metro Ethernet Forum) introduced the L2CP attribute for Ethernet services and UNI in MEF 6. L2CP processing for both the EPL and EVPL is discussed in the following sections.

L2CP Protocol Descriptions

The following L2CP protocols are supported:

- STP Protocols
- Slow Protocols
- ELMI Protocol
- LLDP Protocol
- Port Authentication Protocols
- Bridge Management Protocols
- GARP/GMRP Block of Protocols
- Bridge Block Other Multicasts

Most Layer 2 control protocols use untagged frames; the exception being certain SOAM (802.1ag) protocols that use VLAN tags.

These addresses are known limitations for L2CP tunneling:

01:80:c2:00:00:01 Pause address, needed by switch itself. Switch will not work correctly without this. Pause frames cannot be forwarded, they are consumed by the device itself.

01:80:c2:00:00:02 ION only supports specific applications for this tunnel, e.g. LOAM, not this whole address. It is possible to fully implement tunnel, but LOAM will not work. LOAM and other protocols like LACP and LAMP use the same slow protocol multicast MAC address. At the driver level, the NID looks for the subtype field and if not LOAM, then the NID should forward it.

01:80:c2:00:00:0e ION internally uses it for topology. Possible to fully implement the tunnel, but the topology will not work. The subtype field should tell if its an xxDP or LLDP frame.

01:80:c2:00:00:30 to **01:80:c2:00:00:3f** SOAM uses them, and they are not implemented for tunnel. It is possible to fully implement the tunnel, but SOAM will not work.

The L2CP protocols are described in the following sections. The x222x / x32xx handling syntax for each protocol is 1) **discard** (discard frames at the UNI) or 2) **pass** (pass frames to an EVC for tunneling). The default for each protocol is **pass**.

STP Protocols Fwd

Spanning Tree Protocols (STP) disposition – handling of 802.1D Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP, per IEEE 802.1w. Any STP/RSTP/MSTP protocol frames with destination address of 01-80-C2-00-00-00 are discarded at this port or passed.

Slow Protocols Fwd

Slow Protocols disposition – handling of Slow Protocols, one of two distinct classes of protocols used to control various operating aspects of IEEE 802.3 devices; protocols such as LACP, with less stringent frequency and latency requirements.

Any LACP/LAMP protocol frames with destination address of 01-80-C2-00-00-02 is discarded at this port or passed. Since this device pairs link OAM frames, these frames will not be forwarded or discarded.

Port Auth Protocol Fwd

Port Authentication Protocols disposition – handling of RADIUS, CHAP, EAP, PEAP, FCPAP, and/or other port authenticating protocols. Port authentication protocol frames with a destination address of 01-80-C2-00-00-03 are discarded at this port or passed.

ELMI Protocol Fwd

ELMI protocol disposition – handling of Ethernet Local Management Interface (ELMI), a MEF 16 protocol between the service provider network and the customer equipment that lets the customer equipment communicate its status and service characteristics to the service provider network for faster and easier deployment and troubleshooting.

E-LMI protocol frames with destination address of 01-80-C2-00-00-07 is discarded at this port or passed.

ELMI Support Prerequisites and Restrictions

ELMI relies on Ethernet CFM for the status of an EVC, the remote EVC's UNI identifier, and the remote UNI status; therefore:

1. Ethernet LOAM (e.g., CFM) must be implemented and operational on the service provider's network.
2. LOAM must be enabled on the NID. See "LOAM Configuration Prerequisites and Restrictions" on page 133.
3. ELMI can coexist with all other features. All operating modes are supported.

LLDP Protocol Fwd

LLDP protocol disposition – handling of Link Layer Discovery Protocol (LLDP), a Layer 2 protocol defined by IEEE Standard 802.1AB-2005.

LLDP protocol frames with destination address of 01-80-C2-00-00-0E which are not TN discovery LLDP frames are discarded at this port or passed.

Bridge Mgmt Protocols Fwd

Bridge Management Protocols disposition – handling of One of several protocols standardized by IEEE 802, including Bridge Group Address (STP), IEEE Std. 802.3x Full Duplex PAUSE operation, Bridge Management Group Address, GMRP and GVRP.

Bridge Management protocol frames with destination address of 01-80-C2-00-00-10 is discarded at this port or passed.

GARP/GMRP Block Protocols Fwd

GARP/ GMRP Block of protocols disposition – handling of GARP (Generic Attribute Registration Protocol) and GMRP (GARP Multicast Registration Protocol) per IEEE 802.1ak. GARP/GMRP traffic with destination address of 01-80-C2-00-00-20 to 01-80-C2-00-00-2F is discarded at this port or passed.

Select 'Pass' (pass to an EVC for tunneling) or 'Discard' (discard at the UNI). The default is 'Pass'.

Bridge Block Other Multicasts Fwd

Bridge Block Other Multicast protocols disposition – Passes or discards all of the IEEE multicast frames in the bridge block of addresses [01-80-C2-00-00-04 to 01-80-C2-00-00-0F]. This applies to all addresses in this block that are not covered by the other mib variables in the table (i.e., this is not applicable for STP, slow protocols, etc.).

L2CP can be configured in the NID using either the CLI or Web method.

L2CP Config – CLI Method

Note that the default setting for each protocol is "pass" (pass frames to an EVC for tunneling).

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Set the L2CP protocol parameters. As required, change the default "pass" setting to "discard" for Spanning Tree Protocol, Slow Protocols, Port Authentication Protocols, ELMI Protocols, LLDP Protocols, Bridge Mgmt Protocols, GARP/MRP Block of Protocols, and/or Bridge Block Other Multicast Protocols.

   Type **set l2cp proto**=xx **process**={pass/discard} for each L2CP protocol to be set to "**discard**" (discard at the UNI) or "pass" and press **Enter**. For example:

```
C1|S10|L1P2>set l2cp proto=elmi process=discard
C1|S10|L1P2>set l2cp proto=lldp process=discard
C1|S10|L1P2>set l2cp proto=bridgeMgmt process=discard
```

3. Verify the L2CP configuration. Type **show l2cp config** and press **Enter**.

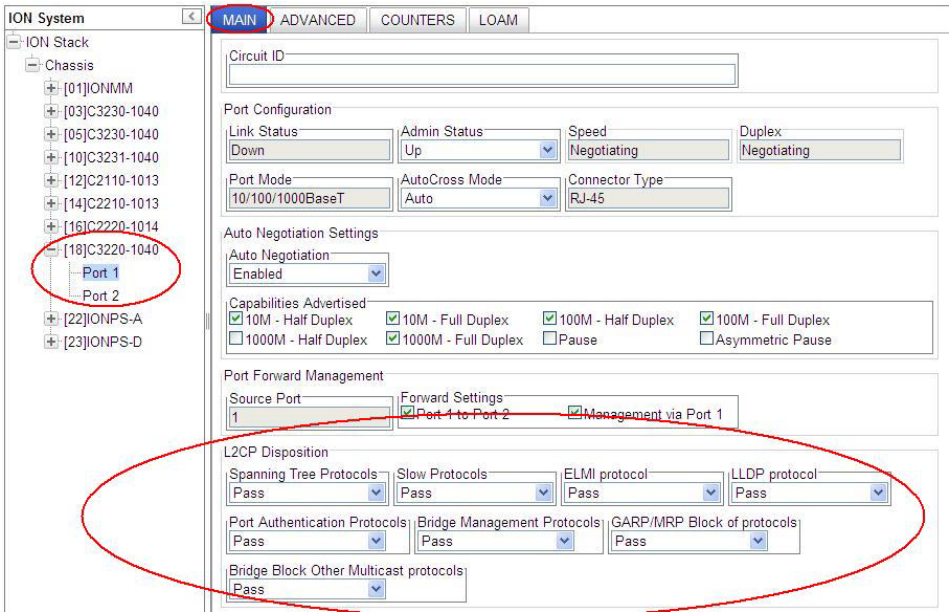
The L2CP configuration parameter settings display:

```
C1|S10|L1P2>show l2cp config
Parameter                                       Value
------------------------------------------------------------------------------
Spanning Tree Protocols                         pass
Slow Protocols                                  pass
Port Authentication Protocols                   pass
ELMI Protocols                                  discard
LLDP Protocols                                  discard
Bridge Mgmt Protocols                           discard
GARP/MRP Block of Protocols                     pass
Bridge Block Other Multicast Protocols          pass
C1|S10|L1P2>
```

L2CP Config – Web Method

Note that the default setting for each protocol is “Pass” (pass to an EVC for tunneling).

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port.
3. Locate the **L2CP Disposition** section.



4. Set the L2CP protocol forward disposition parameters. For each field, select **Pass** (pass to an EVC for tunneling) or **Discard** (discard at the UNI).

   The default setting for each protocol is **Pass** (pass to an EVC for tunneling).

5. Click **Save** when done configuring L2CP for this port.
6. Repeat steps 2-5 for other device port(s).
7. Click **Save** when done configuring L2CP for all ports on the device.

TNDP (TN Topology Discovery Protocol) Disable/Enable

TNDP (TN Topology Discovery Protocol) is 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.

If using the NID with a switch or router, the NID continues to send out LLDP-based information (proprietary - sent once every second). While this does not impact the data traffic seen, it drops for unrecognized upper-level protocols in the switch / router. Disabling TNDP can help eliminate invalid errors and make troubleshooting simpler. This ability to enable or disable MAC learning is supported via the Web interface and the CLI).

TNDP can be configured in the NID using either the CLI or Web method.

TNDP Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Enable or disable the TN Topology Discovery Protocol. Type **set tndp**=<enable|disable> and press **Enter**. This is a Port level command to enable or disable the TN topology discovery protocol (TN's LLDP implementation) on a port. When set to Enabled, the device entering this command will not be discovered by the IONMM if it is remotely managed through this port. If enabled, TN Topology Discovery Data will be sent out from this interface. If disabled, TN Topology Discovery Data will not be sent out from this interface. The default is enabled.

   For example:

```
C1|S3|L1P2>set tndp tx state=enable
C1|S3|L1P2>
```

3. Verify the entry. Type **show tndp tx state** and press **Enter**. This displays the current setting *(*Enabled or Disabled) of the TN topology discovery protocol on a port. When Enabled, the device is not being discovered by the IONMM if the device is remotely managed through this port.

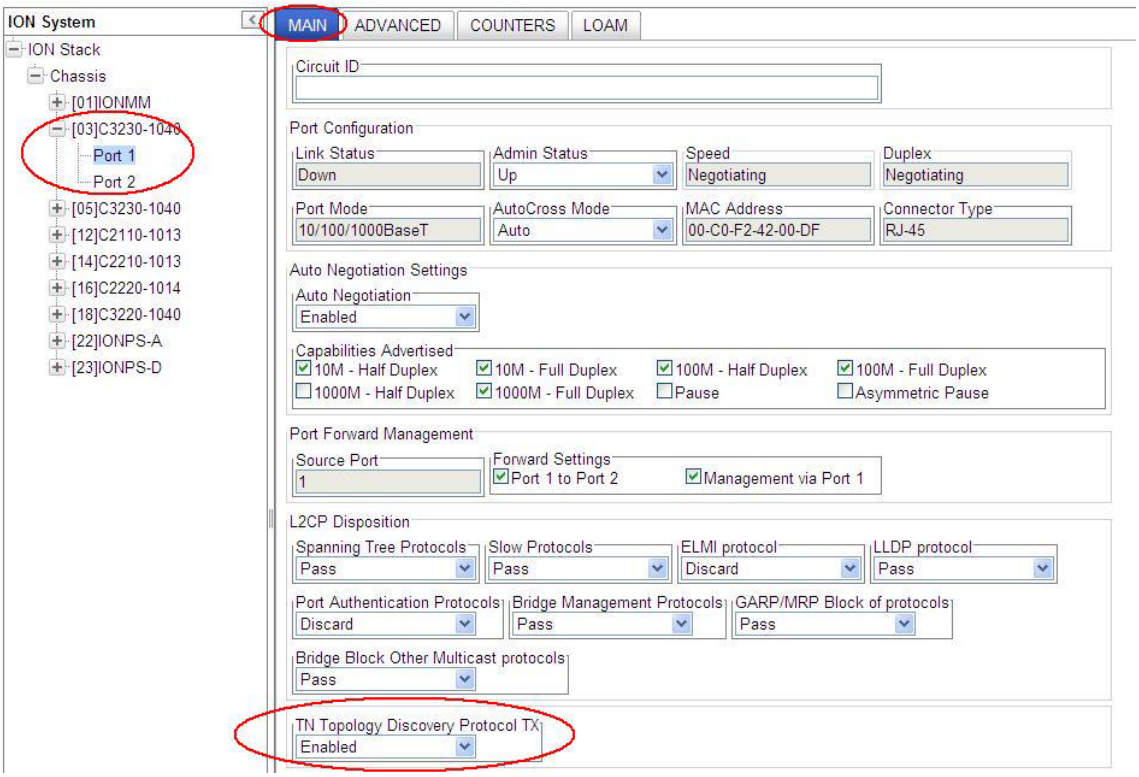
   For example:

```
C1|S13|L0AP1|L1P2/>show tndp tx state
TNDP Tx state:                          enable
```

Note: The traffic related to remote management on these converters is transmitted in-band and is unnecessary on customer facing ports, therefore the TN Topology Discovery Protocol TX should be disabled on these ports. The TN Topology Discovery Protocol TX should only be enabled on the port that is the uplink port, back to another x222x or x322x card in an ION chassis that is utilizing the IONMM management module.

TNDP Config – Web Method

1. Access the x222x / x32xx through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port.
3. Locate the **TN Topology Discovery Protocol TX** section.



4. Set TN Topology Discovery Protocol TX to enabled or disabled. The default setting is Enabled.
   If **Enabled**, TN Topology Discovery Data will be sent out from this interface.
   If **Disabled**, TN Topology Discovery Data will not be sent out from this interface.

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

Configuring Loopback

You can define the x222x/x32xx Loopback type and operation at the port level.

Loopback can be configured in the NID using either the CLI or Web method.

Loopback Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Select the desired port.
3. If desired, check the port’s loopback capabilities. Type **show ether loopback cap** and press **Enter**. This displays the current loopback functionality that has been set for the port specified in the command. The loopback capabilities that can display are "noloopback", "phyLayer", "macLayer", "alternate", or "remotePeer".
4. Set the Loopback Type of the selected TDM Port. At the device’s command prompt type **set ether loopback type**={noloopback|phylayer} and press **Enter**.
5. Set the TDM Loopback operation. Type **set ether loopback oper**={init|stop} and press **Enter**. This alternately initiates or stops the loopback test.
6. Check the TDM Loopback state. Type **show ether loopback state** and press **Enter**. This displays the current loopback operating state for the port entering the command. The loopback capabilities that can display are ""noLoopback", "intiateLoopback", "terminateLoopback", "inProcess", "localInLoopback", or "remoteInLoopback".

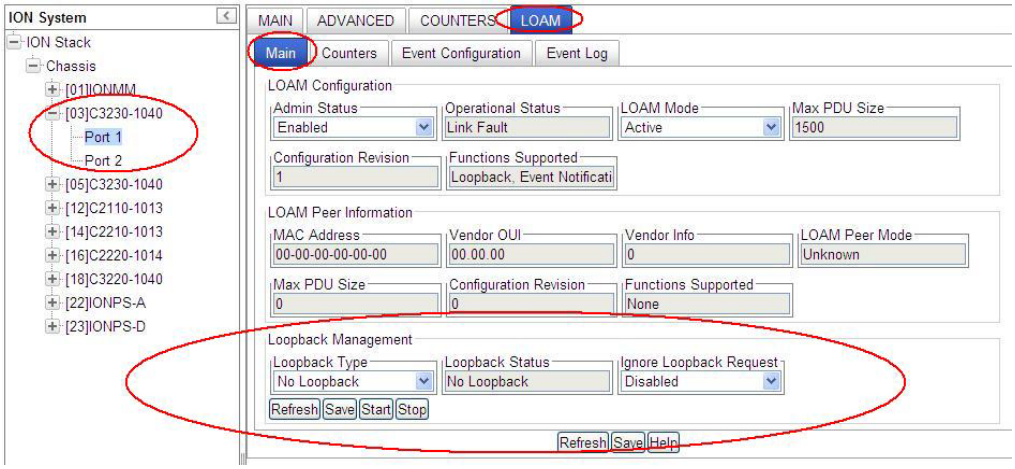
   For example:

```
C1|S3|L1P1>set ether loopback ?
  oper
  type
C1|S3|L1P1>set ether loopback oper ?
  init
  stop
C1|S3|L1P1>set ether loopback oper init
Fail to set Ethernet port loopback operation, please check if Link OAM admin
state of remote peer port is enabled, link status and other issues.
C1|S3|L1P1>set ether loopback oper stop
C1|S3|L1P1>set ether loopback type ?
  alternate
  maclayer
  noloopback
  phylayer
  remote
C1|S3|L1P1>set ether loopback type phylayer
Set Ethernet port loopback type failed.
C1|S3|L1P1>set ether loopback type alternate
C1|S3|L1P1>show ether loopback ?
  capability
  state
C1|S3|L1P1>show ether loopback state
Loopback type: alternate
```

```
Loopback state: noLoopback
C1|S3|L1P1>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S3|L1P1>set ether loopback type alternate
C1|S3|L1P1>
```

Loopback Config – Web Method

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the desired port.
3. Locate the **Loopback Management** section.



4. At the **Loopback Type** dropdown, select **No Loopback**, **Alternate**, or **Remote Peer**.
5. At the **Ignore Loopback Request** dropdown, select **Enabled** or **Disabled**.
   Enabled causes the LOAM enabled x222x/x32xx to ignore all Loopback requests (i.e., not respond to remote loopback requests from peers).
   Disabled causes the LOAM enabled x222x/x32xx to respond to all remote loopback requests from peers.
6. Click the **Save** button when done.
7. Click the **Start** button to initiate the selected loopback test type.
8. Click the **Stop** button to end the loopback test.
9. Check the **Loopback Status** field for results. This field displays the loopback status for this interface when enabled. The values are read-only to show the status of the loopback operation (*No Loopback*, *Local in Loopback*, or *Remote in Loopback*).

Configuring System Logging (Syslog)

The IONMM and x222x/x32xx 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 25: Syslog Severity Levels

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

Messages used to enable debugging or software testing are assigned Severity 7. Severity 0 is reserved for messages of very high importance (e.g., serious hardware failures or imminent power failure). Refer to your organizations policy administrator for this level of severity. Note that the syslog protocol does not provide for acknowledgment of message delivery. See “Syslog Messages and Sys.log Output” on page 193 for more information.

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

Syslog Config – CLI Method

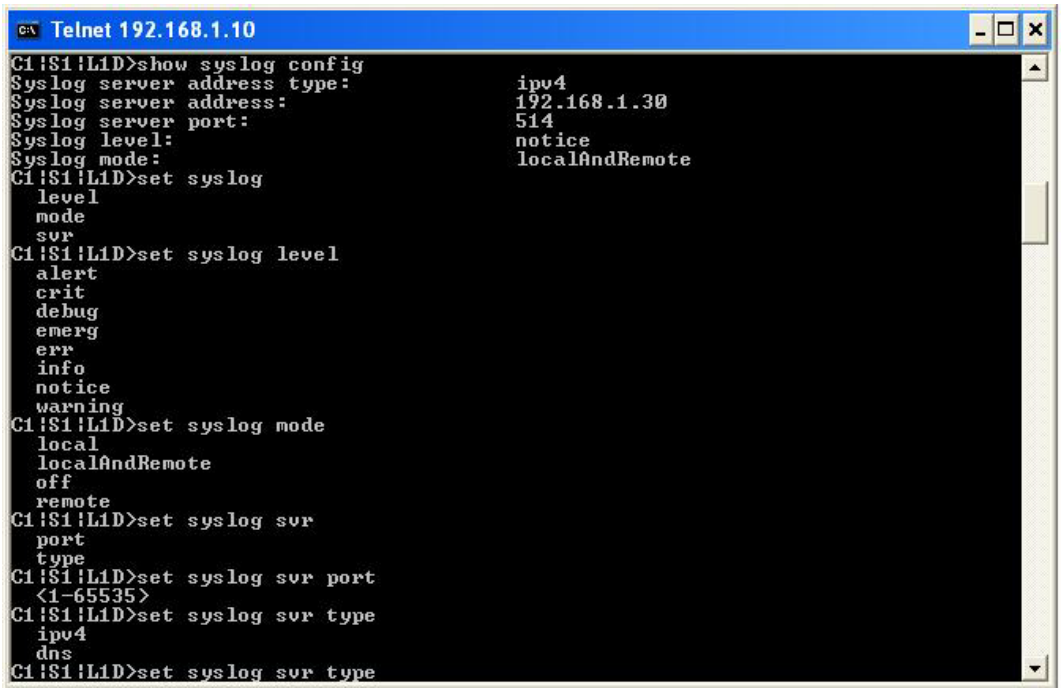
1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the device's command prompt type the following set of four CLI commands to define Syslog operations (the Syslog server address and port, and Syslog level and mode). Press the **Enter** key after each command.

   set syslog svr port=<1-65535> <cr>
   set syslog mode=(local/localAndRemote/off/remote) <cr>
   set syslog level=(alert/crit/debug/emerg/err/info/notice/warning) <cr>
   set syslog svr type=(ipv4|dns) **addr**=SYSLOG_SVR_ADDR <cr>

3. Verify the Syslog configuration using the **show syslog config** command. For example:

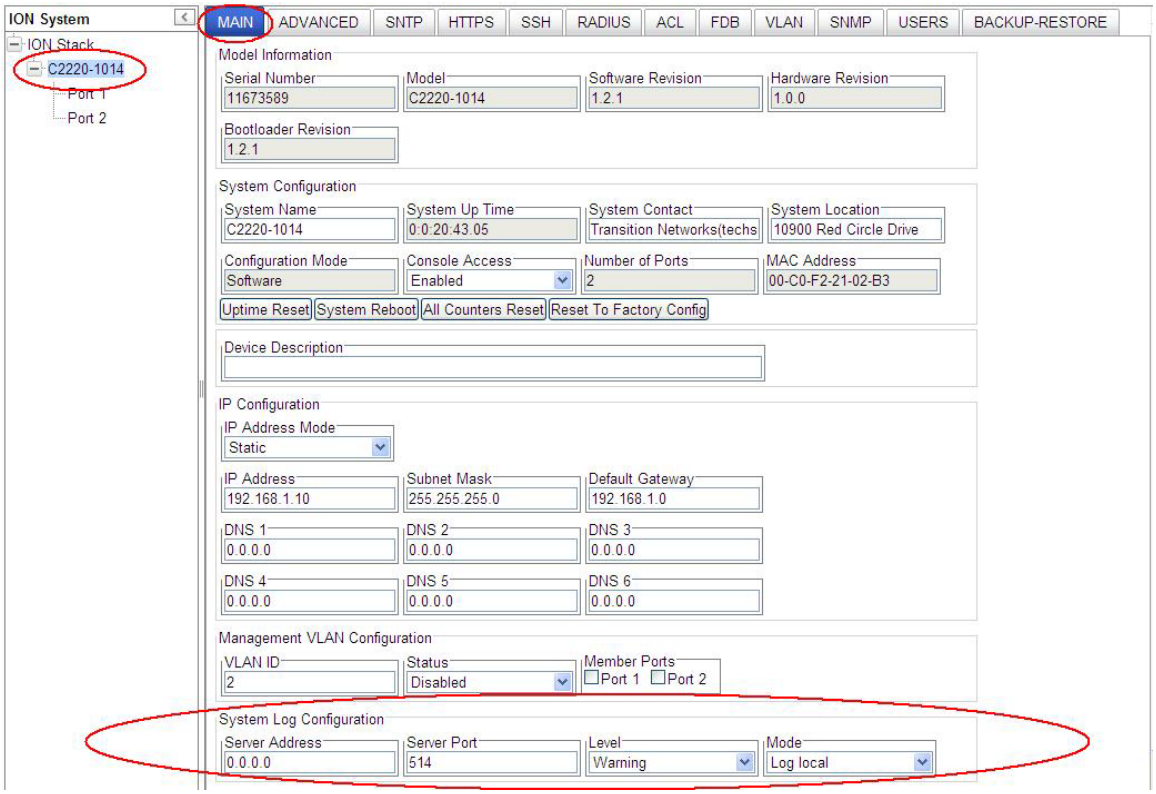
```
C0|S16|L1D>show syslog config
Syslog server address type:             ipv4
Syslog server address:                  192.168.0.2
Syslog server port:                     514
Syslog level:                           info
Syslog mode:                            local
C0|S0|L1d/>
```

Telnet Example:



Syslog Config – Web Method

1. Access the IONMM or NID through the Web interface (see "Starting the Web Interface" on page 45).
2. At the IONMM **MAIN** tab, locate the **System Log Configuration** section.



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

Server Address - The address of the Remote Syslog server (e.g., 192.168.0.2 above).
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. All messages with a severity level lower than or equal to this level will be logged.

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

See Table 15 above for full Syslog severity level descriptions.

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

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

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

See "Syslog Messages and Sys.log Output" on page 193 for more Syslog information.

Configuring MAC Address Learning

MAC address learning can be disabled on a per-port basis for security purposes. If MAC address learning is disabled, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port. When enabled, sets the port state to allow learning (the other port states - Flooding, Filtering and Forwarding – are disabled).

The MAC Learning function can be disabled via the CLI or the Web interface.

MAC Address Learning Portlist Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the device's command prompt type **set mac enable portlist**=x

   where x=1, 2 or 3 (port 1, port 2, and/or port 3)

   Disable learning ports <portlist> disables MAC address learning on one or more ports for security purposes. If MAC address learning is disabled, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port. The default setting is enabled.

   Enable learning ports <portlist> enables MAC address learning on one or more ports. The default setting is enabled. Sets the port state to Learning (the other port states - Flooding, Filtering and Forwarding – are disabled).

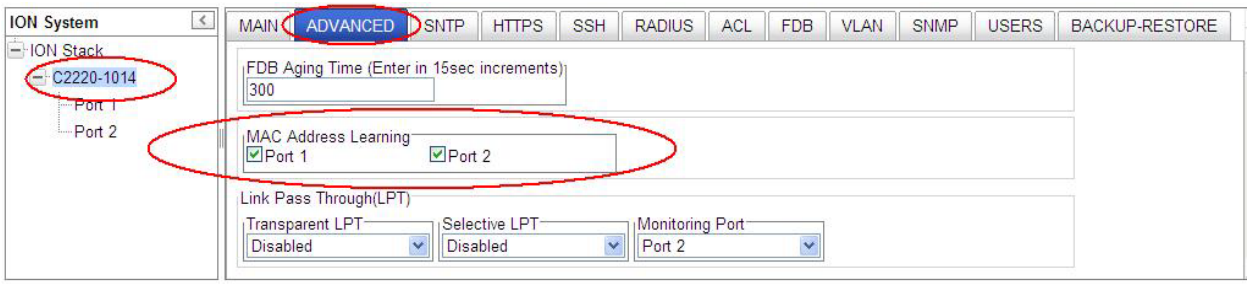
```
C1|S1|L1D>set mac enable portlist ?
  STR_MAC_LEARNING_PORT_LIST
C1|S1|L1D>set mac_learning enable portlist=1,3
C1|S8|L1D>set mac enable portlist 1
C1|S8|L1D>set mac enable portlist 2,3
Fail to set port MAC learning!
C1|S8|L1D>set mac enable portlist 2
C1|S8|L1D>set mac enable portlist 3
C1|S8|L1D>set mac enable portlist 4
Invalid forward port list!
C1|S8|L1D>set mac enable portlist 1
Fail to set port MAC learning!
C1|S8|L1D>
```

3. Verify the MAC Learning Portlist configuration. Type **show mac learning port list** and press **Enter**. For example:

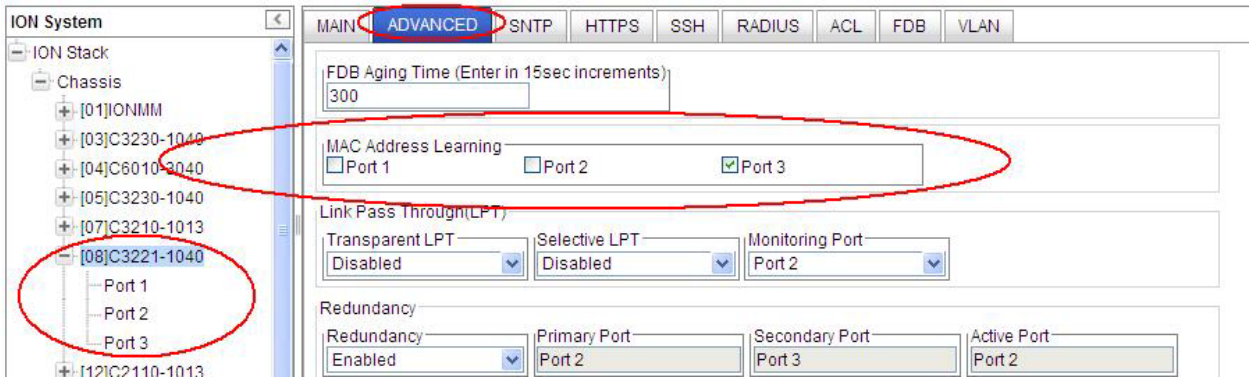
```
C1|S8|L1D>show port mac_learning state
Port Mac learning:
Port1:                          disable
Port2:                          disable
Port3:                          enable
```

MAC Address Learning Portlist Config – Web Method

1. Access the x222x / x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. At the device's **ADVANCED** tab, locate the **MAC Address Learning** section.



A Model C2220 with 2 ports is shown above; a Model C2221 with three ports is shown below.



3. Check (enable) or uncheck (disable) the Port checkboxes as desired.
   Disabled: with MAC address learning **Disabled**, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port.
   Enabled: with MAC address learning **Enabled**, sets the port state to allow learning. The other port states (Flooding, Filtering and Forwarding) are disabled.
4. Click the **Save** button when done. The message "*Setting values succeeded*" displays in the lower left corner of the screen when successfully saved.

5. Operation

General

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

Backup and Restore Operations (Provisioning)

Through the Web interface you can back up and restore the configuration information for the IONMM and any or all of the NIDs in the ION system.

A Backup is used to get the SIC card running configuration, convert it to CLI commands, and save those CLI commands into the backup file. The backup file is stored in the IONMM.
Note: Lantronix recommends as a "best practice" to back up each SIC card's configuration after it is fully configured, so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored.

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

Lantronix recommends that you to enter a "**show card info**" CLI command to view the SIC card's current configuration before a backup/restore operation to verify the desired configuration settings. There are several CLI **show** commands that allow you to display (show) information about a SIC card's configuration. For a complete description of these and other CLI commands see the *ION System CLI Reference Manual, 33473*.

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

IMPORTANT

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

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

- Table 15. Back Up and Restore File Content and Location on page 333
- Table 16. File Status after a Reset to Factory Defaults on page 338
- Table 17. File Content and Location after a System Reboot on page 345
- Table 18. File Content and Location after a Firmware Upgrade on page 351

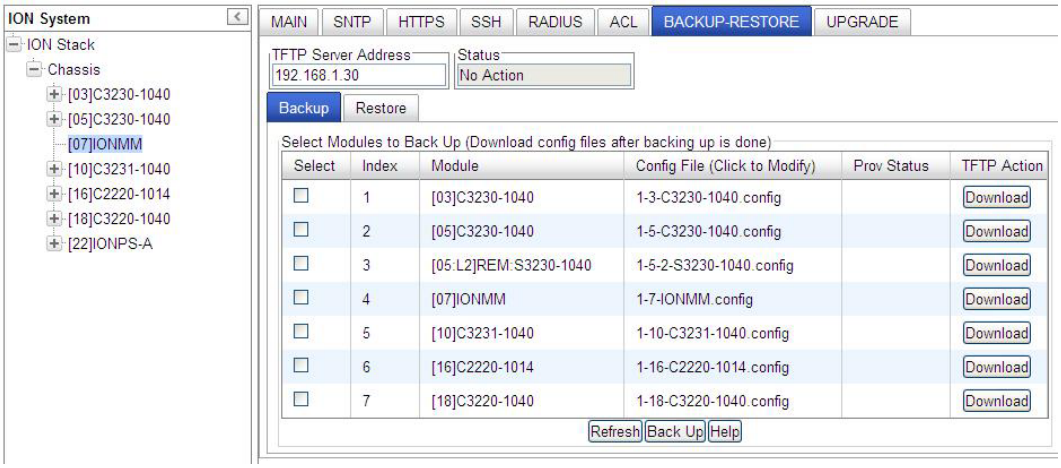
Backing Up Slide-In and Remote Modules

The following procedure describes how to back up the configuration of one or more slide-in or remote modules in the ION system. The backup file is stored in the x222x/32xx 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" on page 170.

1. Access the IONMM through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **BACKUP-RESTORE** tab. Select the **Backup** sub-tab if not already displayed.



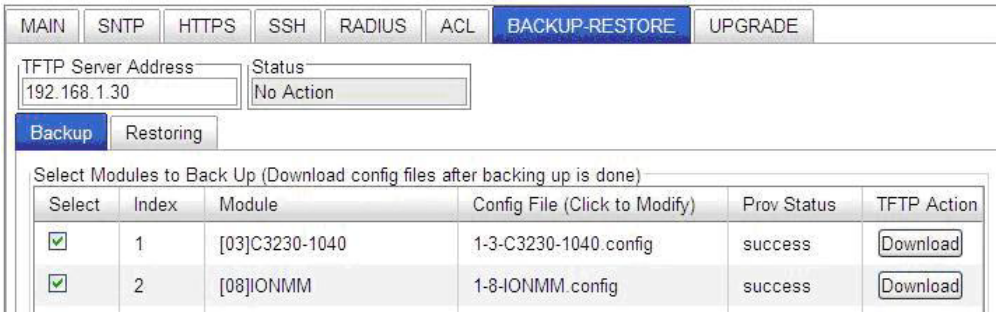
3. Verify that the TFTP Server address shown is correct, that the TFTP Server is running and configured, and that the file to be downloaded is located correctly (e.g., at *C:\TFTP-Root*).
4. Verify that the card list shown in the table is correct; if not correct, fold and then unfold the "ION Stack"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

7. Do you want to rename the backup file?

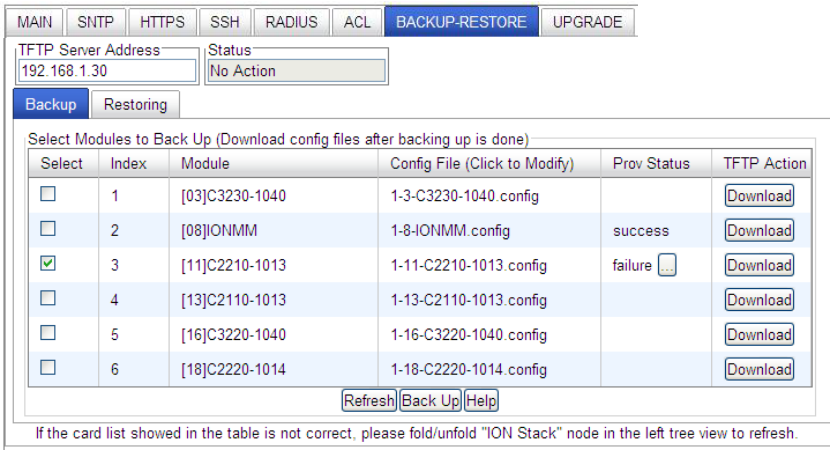
Yes	No
a) In the **Config File** column, click the file name. b) Type a new name for the backup file. **Note:** the file name must be 1–63 characters long and must end with **.config**. c) Continue with step 8 below.	Continue with step 9 below.

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

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



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 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 on page 397 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 330
- Restoring Slide-In and Remote Modules on page 331
- Restoring Standalone Modules on page 334

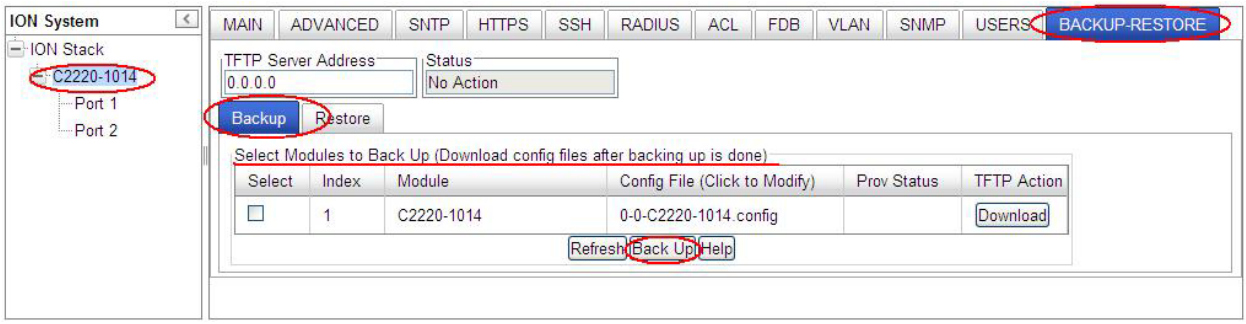
Backing Up Standalone Modules

The following procedure describes how to back up the configuration of a standalone module. Note that a TFTP Server must be configured and running.

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" on page 45).
2. Select the **BACKUP-RESTORE** tab.



3. In the **TFTP Server Address** field enter the address of the TFTP Server.
4. In the **Select** column, check the checkbox of the module to be backed up.
5. 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 6.	Continue with step 6.

6. Click the **Back Up** button.
7. When the message "*Backup following modules: S3220-1040, are you sure to proceed?*" displays, click **OK**.

   The message "*Backup is being processed*. " displays as the backup file is saved in the IONMM module. When the Backup is successfully completed, the message "success" displays in the Prov Status column.
8. Click the **Download** button. When completed, the message "*File has successfully transferred via TFTP*" displays.
9. Click the **OK** button to clear the web page message. The config file (e.g., *0-0-S3220-1040*) is saved to the *C:\TFTP-Root* folder.
10. At the confirmation message, click **OK**. The message "*Backup is being processed …*" displays. The Back Up operation can take several minutes.

To send a copy of the backup file to the TFTP server, be sure to:

a. Make sure the TFTP Server is running and configured.

b. Enter the IP address of the TFTP server in the **TFTP Server Address** field.

c. Click the **Download** button. 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 330
- Restoring Slide-In and Remote Modules on page 331
- Restoring Standalone Modules on page 334

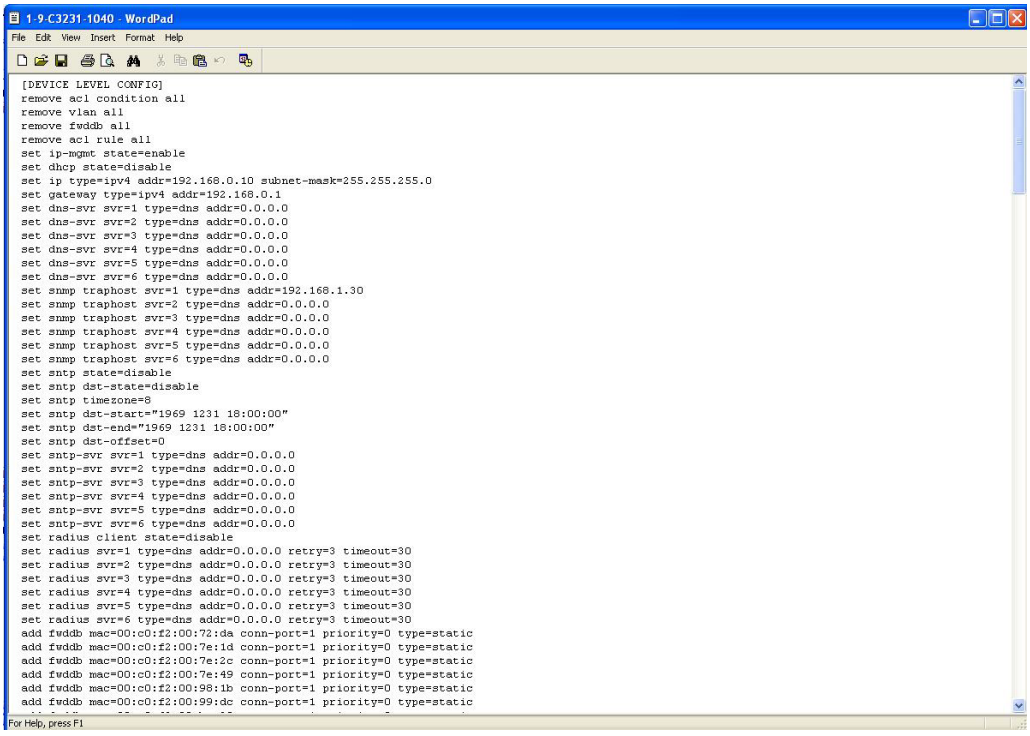
Editing the Config File (Optional)

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-C3221-1040.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 x3221).
4. Save the edited Config file back to the TFTP server location (e.g., *C:\TFTP-Root\1-9-C3221-1040.config*).
5. Continue with the applicable Restore procedure from the following section using the edited Config file.

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



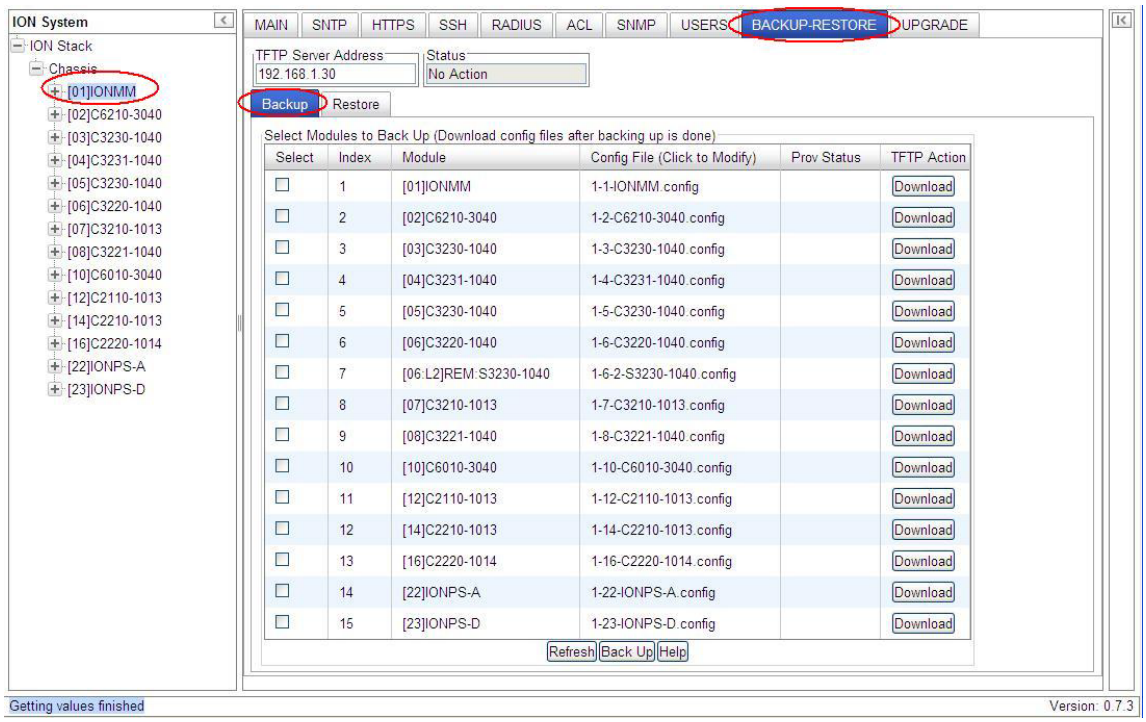
Restoring Slide-In and Remote Modules

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

IMPORTANT

A restore operation can only be performed for a module that had its configuration file backed up (see Backing Up Standalone Modules on page 233).

1. Access the IONMM through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **BACKUP-RESTORE** tab and select the **Restore** sub-tab. The "Modules to Restore" table displays.



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

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

Yes	**No**
a) In the **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 step 6.	Continue with step 5.

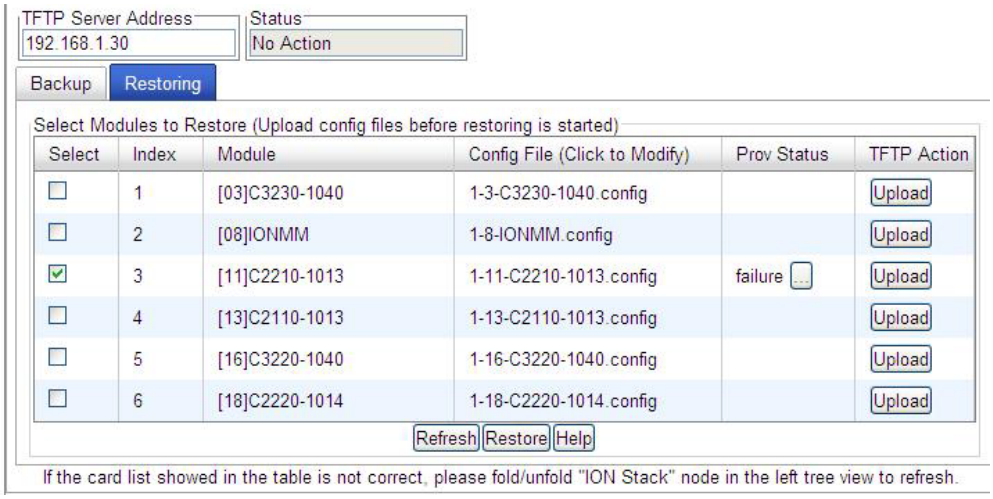
6. Does the configuration file need to be retrieved from the TFTP server?

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 6.

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

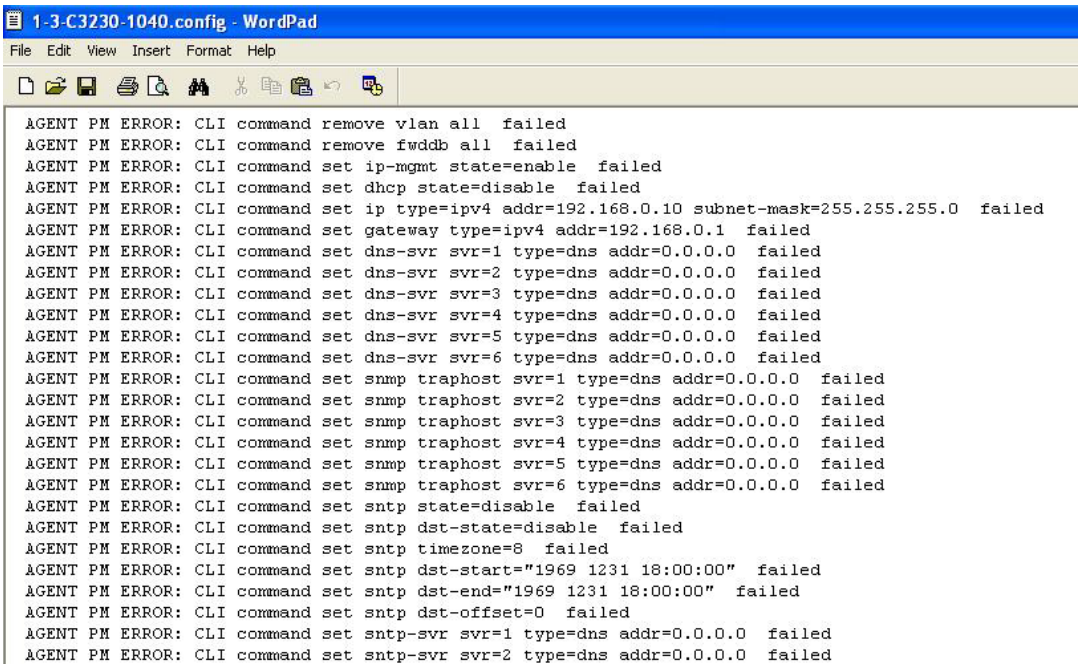
    The configuration will be restored from the specified file. During the Restore operation the message "*Restoring is being processed ...*" displays, and the **Prov Status** column displays "ongoing".
    When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.

11. If the **Restore** operation fails, the **Prov Status** column displays failure ... 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.



See "The Config Error Log (config.err) File" on page 353 for message descriptions.

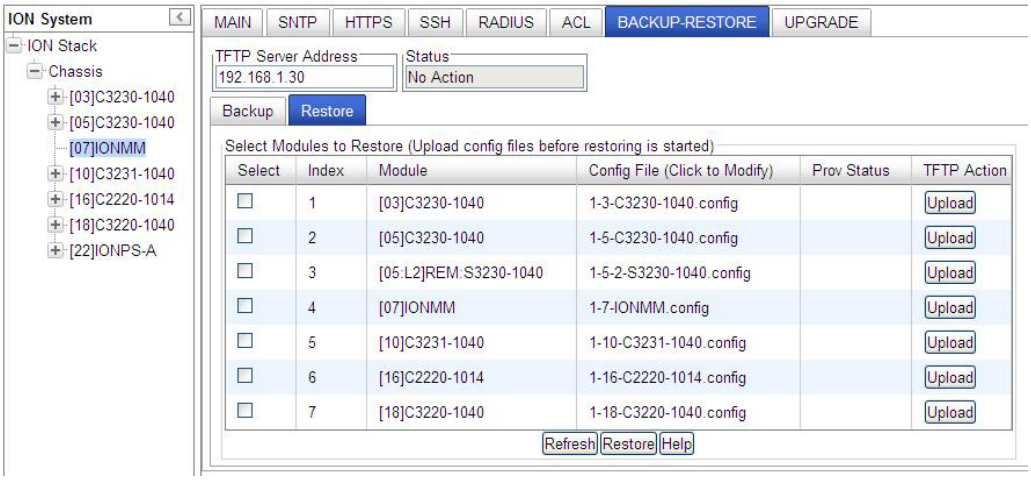
Restoring Standalone Modules

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

IMPORTANT

A restore operation can only be performed for a module that had its configuration file backed up (see Backing Up Standalone Modules on page 233).

1. Access the IONMM module through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **BACKUP-RESTORE** tab.
3. Select the **Restore** sub-tab. The "Modules to Restore" table displays.



4. In the **Select** column, check the checkbox of the 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 step 5.	Continue with step 5.

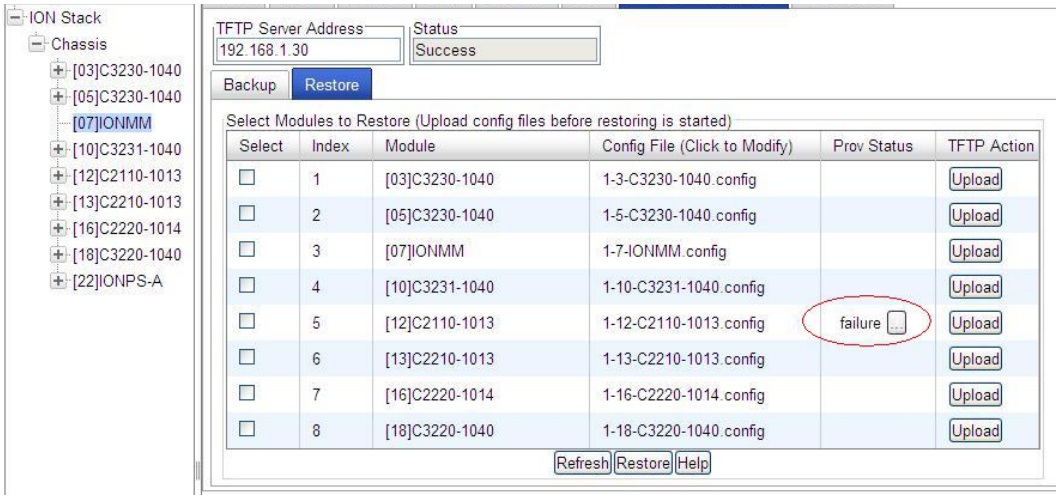
6. Does the configuration file need to be retrieved from the TFTP server?

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 6.	Continue with step 6.

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

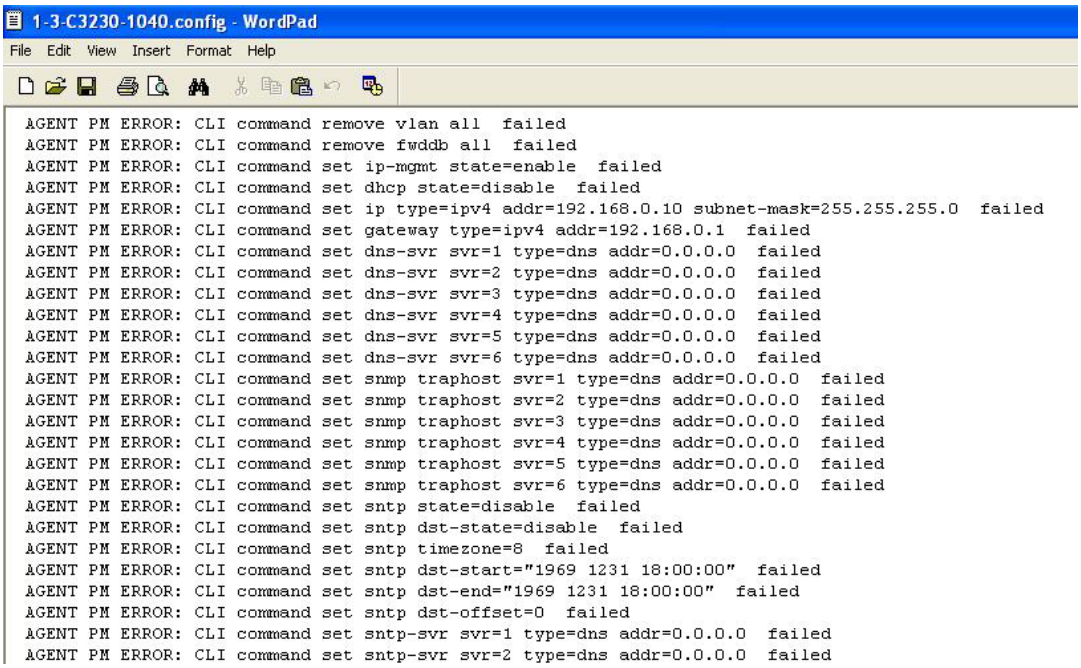
    The configuration will be restored from the specified file. During the Restore operation the message "*Restoring is being processed ...*" displays, and the **Prov Status** column displays "ongoing".
    When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.

11. If the **Restore** operation fails, the **Prov Status** column displays failure [...]. 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.



See "The Config Error Log (config.err) File" on page 353 for message descriptions.

Back Up and Restore File Content and Location

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

The Back Up operation backs up all of the SNMP settings (the same as what can be set via the Web interface / CLI) for one SIC into a file containing a list of CLI commands. This file can be downloaded from IONMM. When restoring for one SIC, you can upload a provisioning backup file (this file must have been made via the Backup operation and must be for the same SIC type) to the IONMM and do a Restore. See the IONMM **BACKUP-RESTORE** (Provisioning) 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 26: 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 (see Note 1)	No
SSH user key file**	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	No (see Note 2)	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No	Always changes
MIB configuration files	e.g., 'agent3.conf ' 'ifMib.conf '	The MIB configuration files for SNMP setting	/agent3/conf	No - not needed; the configurations included in this file will be backed up by SNMP set operations	Yes

Back Up and Restore Notes:

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

Messages

***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.

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 (Provisioning) - CLI Method

These commands can only be executed on an IONMM or a standalone SIC.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command prompt, check the current provisioning status. Type **show prov modules** and press **Enter**.
3. 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**.
4. 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**.
5. Specify 1-10 provision modules to be backed up. Type **backup module-list=xx** and press **Enter**.
6. Specify 1-10 provision modules to be restored. Type **restore module-list=xx** and press **Enter**.
7. Verify the configuration. Type **show prov modules** and press **Enter**. For example:

```
C1|S1|L1D>show prov modules
Index   Module                          Config File               Prov Status
-------------------------------------------------------------------------------
1       [01]IONMM                       1-1-IONMM.config
2       [02]C6210-3040                  1-2-1-C6210-3040.config
3       [02:L2]REM:S6210-3040           1-2-2-S6210-3040.config
4       [03]C3230-1040                  1-3-1-C3230-1040.config
5       [04]C6010-3040                  1-4-1-C6010-3040.config
C1|S1|L1D>set backup module-index 1 config-file xxxxx
C1|S1|L1D>set restore module-index 1 config-file 1
C1|S1|L1D>backup module-list 1
Processing...
Processing...
Backup finished
C1|S1|L1D>restore module-list 1
Processing...
Restore finished
C1|S1|L1D> C1|S1|L1D>show prov modules
Index   Module                          Config File               Prov Status
-------------------------------------------------------------------------------
1       [01]IONMM                       1-1-IONMM.config          success
2       [02]C6210-3040                  1-2-1-C6210-3040.config
3       [02:L2]REM:S6210-3040           1-2-2-S6210-3040.config
4       [03]C3230-1040                  1-3-1-C3230-1040.config
5       [04]C6010-3040                  1-4-1-C6010-3040.config
C1|S1|L1D>
```

An example of the backup / restore of a standalone C2220 is shown below.

```
C2220-1014 C0|S0|L1D>set backup module-index 1 config-file 0-0-S3230-1040
C2220-1014 C0|S0|L1D>set restore module-index 1 config-file 1
C2220-1014 C0|S0|L1D>backup module-list 1
Processing........
Backup finished
C2220-1014 C0|S0|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.

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 Lantronix Tech Support if the problem persists.

IONMM Backup All / Restore All

IONMM v 1.4.2 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 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. See the IONMM User Guide for details.

Disabling USB Console Access to the x222x / x32xx

Console access to the x222x / x32xx through the USB serial interface can be disabled as a security precaution. When Console access is disabled, the x222x / x32xx will not respond to CLI commands entered by a local management station across the USB serial interface. The only access to the x222x / x32xx will then be through either a Telnet session or the Web interface.

Note: Access via the USB serial Console interface can be disabled using either the CLI or Web method.

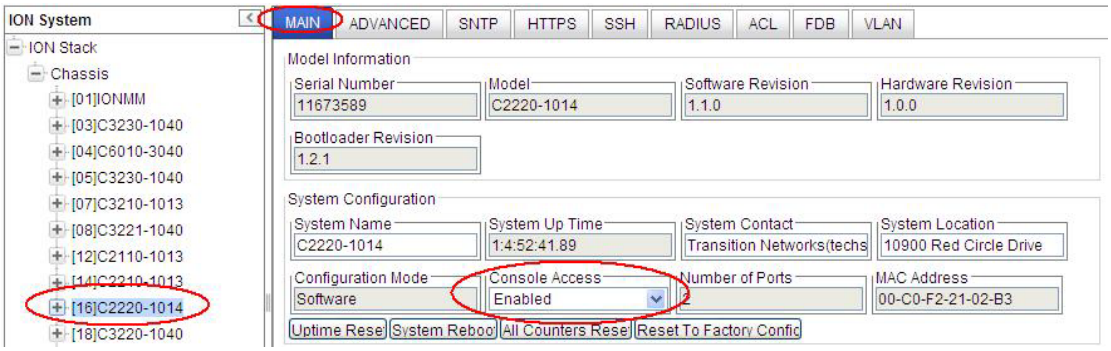
Disabling Console Access – CLI Method

1. Set the status of the device's USB connection to disabled. Type **set usb state=disable**.
2. Press **Enter**.
3. Verify the status of the device's USB connection is disabled. Type **show usb state**.
4. Pres **Enter**. The USB state displays:

```
C1|S3|L1D>set usb state=enable
C1|S3|L1D>show usb-port state
USB port state:                          enable
C1|S3|L1D>
```

Disabling Console Access – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 71).
2. At the **MAIN** tab locate the **System Configuration** section.



3. In the **Console Access** field, select **Disabled**. The default is **Enabled**.
4. Scroll to the bottom and click **Save**. With the x222x / x32xx USB connection disabled, the NID will no longer respond to CLI commands entered by a local management station (console) via the USB serial interface. The only access to the x222x / x32xx will now be through either a Telnet session or the Web interface.

Displaying Information

There are several CLI commands that allow you to display (show) information about x222x / x32xx configuration. For a complete description of these and other CLI commands see the *ION System CLI Reference Manual, 33473*.

Reset to Factory Defaults

If need be, you can reset all configurations in the x222x / x32xx back to their original factory defaults. This operation can be accomplished through either the CLI or Web method.

IMPORTANT

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

Resetting Defaults – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command prompt type: **reset factory**
3. Press **Enter**. The following displays:

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

All configuration parameters will be reset to their factory values. For a list of all factory defaults, see "Appendix B: Factory Defaults" on page 534).

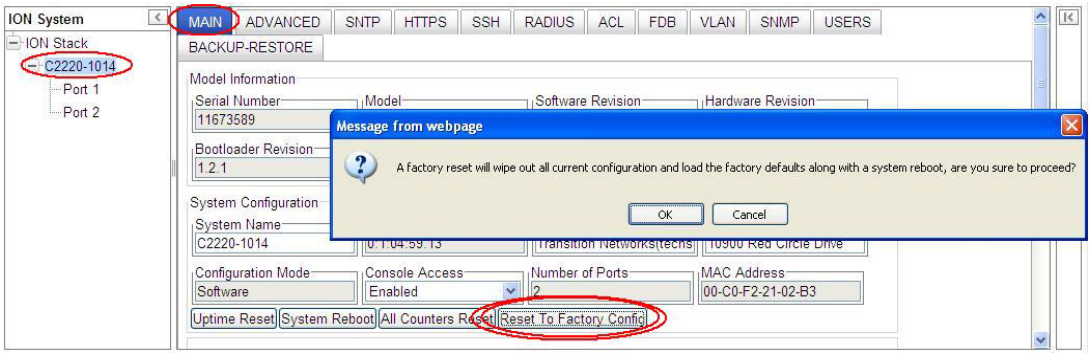
NOTE: Your USB and/or Telnet session will be disconnected.

4. Set the IP configuration (see "Doing the Initial System Setup" on page 48).

Resetting Defaults – Web Method

Caution: This operation deletes all configuration information that was saved in the x222x/x32xx, including the IP address you assigned to the x222x/x32xx NID.

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



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

   All configuration parameters will be reset to their factory values. For a list of all factory defaults, see "Appendix B: Factory Defaults" on page 534).

   Note: Your Web session will be discontinued.

6. Set the IP configuration (see "Doing the Initial System Setup" on page 48).

File Status after Reset to Factory Defaults

The table below shows the status of various system files after a reset to factory defaults.

Table 27: File Status after a Reset to Factory Defaults

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

Resetting Uptime

The ION system uptime field displays the amount of time that the ION system has been in operation.

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

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

Reset System Uptime – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command prompt type: **reset uptime** and press **Enter**. The System Up Time field resets to zero, and immediately begins to increment.

   For example:

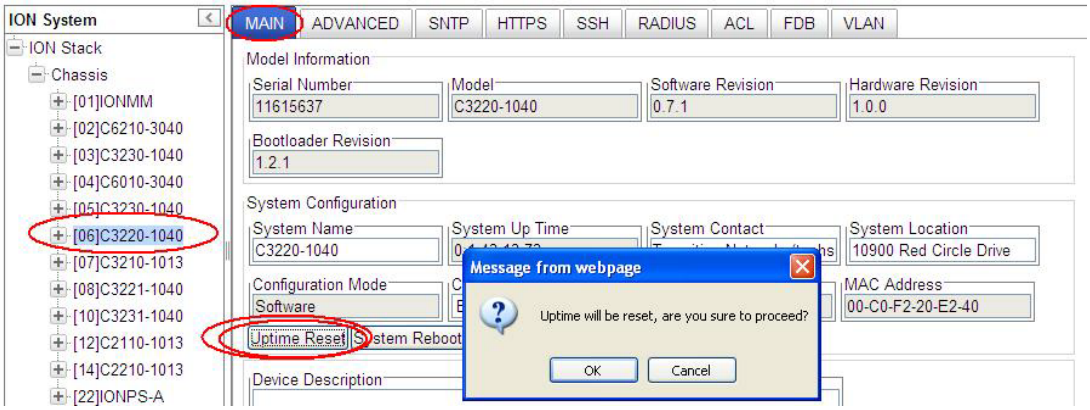
```
C2220-1014 C0|S0|L1D>reset uptime
C2220-1014 C0|S0|L1D>
```

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

Note: The **reset uptime** command is not available for all ION devices.

Reset System Uptime – Web Method

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 26).
2. At the **MAIN** tab, locate the **System Configuration** section.
3. If desired, observe and record the **System Up Time** field count.



4. Click the **Uptime Reset** button.
5. At the "*Uptime reset, are you sure*" window displays, click **OK** to reset the system up time.

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

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

Resetting Counters

Before running certain diagnostics / tests, you may want to reset (zero out) all or some x222x/x32xx device and/or port counters.

The x222x/x32xx counters can be reset via the CLI method or Web method.

Reset All Ports Counters – CLI Method

This is a device-level command to reset all of the x222x/x32xx ports counters.

1. Access the x222x/x32xx through either a USB connection (see "Start a USB Session in HyperTerminal and Log In " on page 70) or a Telnet session (see "Starting a Telnet Session" on page 72).
2. At the command prompt type: **reset all ports counters** and press **Enter**. For example:

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

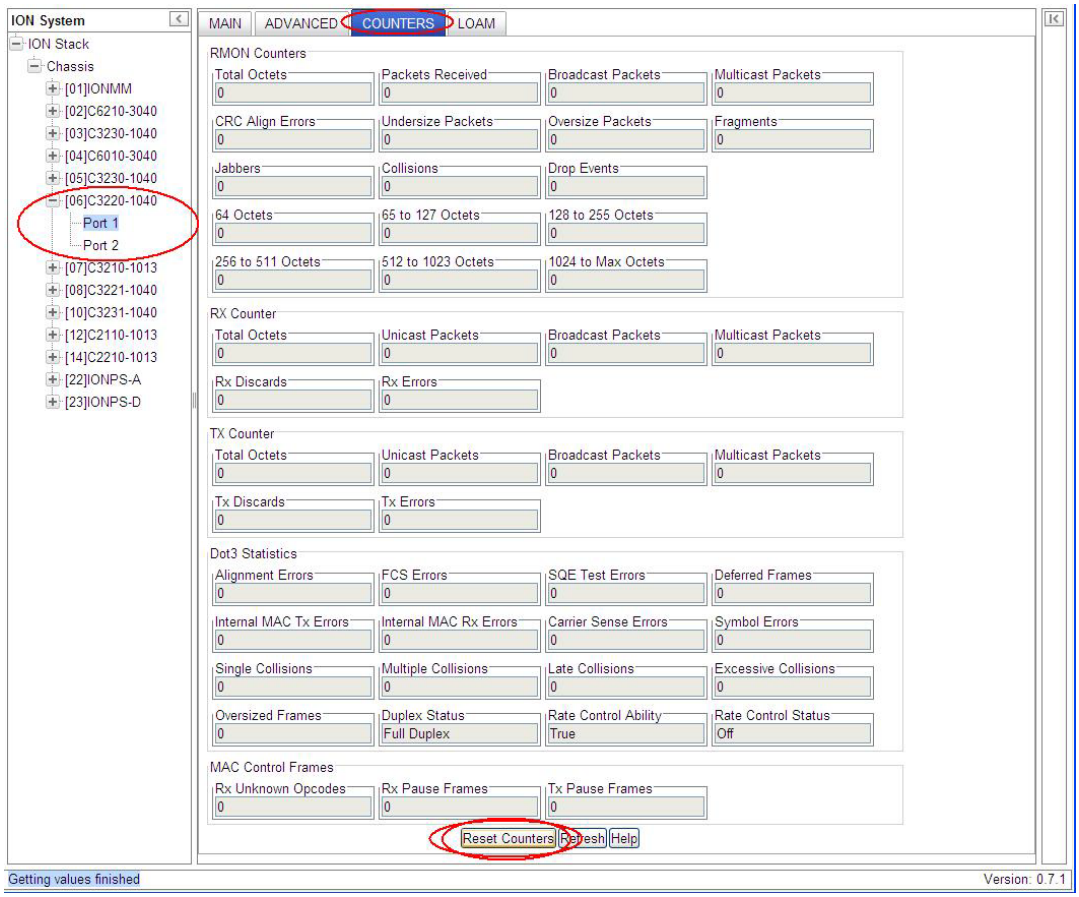
Use the **show ether statistics** command to display Port Counters Received, Port Counters Sent, and related information.

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

Reset Port Counters– Web Method

This is a port-level function used to reset all of an x222x/x32xx port's counters.

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 26).
2. Select the desired x222x/x32xx port.
3. Select the **COUNTERS** tab.



4. If desired, click the **Refresh** button and observe and record the various counter field counts for later comparison.
5. Click the **Reset Counters** button. The x222x/x32xx port-level counters are reset to zero and begin incrementing immediately. The counters that are reset include:
   - RMON Counters
   - Rx Counter
   - Tx Counter
   - Dot3 Statistics
   - MAC Control Frames

Clear All Ethernet Port Counters – CLI Method

This is a port-level command to reset all of an x222x/x32xx port's Ethernet counters.

1. Access the x22xx/x322x through either a USB connection (see "Start a USB Session in HyperTerminal and Log In " on page 70) or a Telnet session (see "Starting a Telnet Session" on page 66).
2. Select the desired x222x/x32xx port.
3. At the command prompt type **clear ether all counters** and press **Enter**. For example:

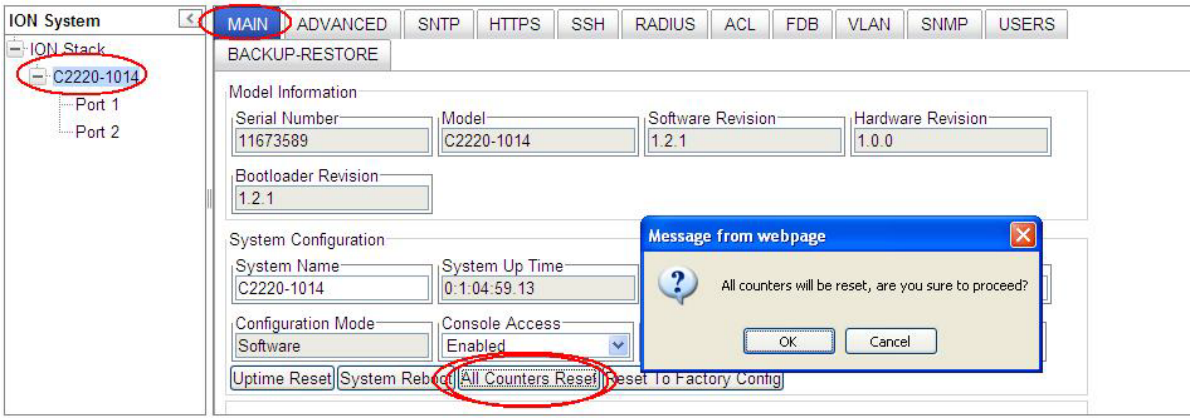
```
C1|S3|L1D>clear ether all counters
Error: this command should be executed on a port!
C1|S3|L1D>go l1p=1
C1|S3|L1P1>clear ether all counters
C1|S3|L1P1>
```

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

All Counters Reset – Web Method

This is a device-level function to reset all of the x222x/x32xx counters.

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 26).
2. At the **MAIN** tab, locate the **System Configuration** section.
3. If desired, observe and record the various counter field counts for later comparison.
4. Click the **All Counters Reset** button. The message "*All counters will be reset, are you sure to proceed?*" displays.



5. Click the **OK** button to proceed. The x222x/x32xx device counters are reset to zero and begin incrementing immediately. These counters are reset:
   - Port > COUNTERS
   - Port > LOAM > Counters
   - Port > LOAM > Event Configuration
   - Port > LOAM > Event Log
   - Port > DMI >

Reboot

At times you may have to reboot (restart) the ION system. This operation can be accomplished by either the CLI or Web method.

Note: this operation can take several minutes. The amount of time for the reboot to complete depends on the ION system configuration. When the reboot is finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The 'red box' condition occurs while the devices are resetting; this condition can continue several minutes after the reboot.

See Table 19 in this section for file content and location after a System Reboot.

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

Rebooting – CLI Method

After an x222x/x32xx reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.

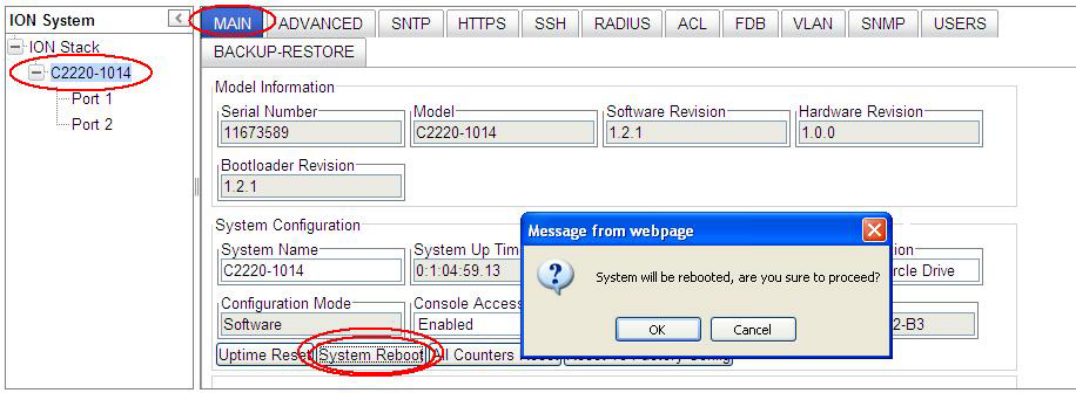
1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and 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" on page 41).
   - For a Telnet session
     a) Press **Enter**.
     b) Start a Telnet session (see "Starting a Telnet Session" on page 43).

Rebooting – Web Method

Caution: Doing a system reboot will cause all configuration backup files, HTTPS certification file, SSH key file, and Syslog file to be lost.

Note: If you have a USB or Telnet session established, terminate the session before doing the reboot.

1. Access the x222x/x32xx through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



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

   The x222x/x32xx will restart and will be available for operations after about one minute.

Reboot File Content and Location

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

Table 28: File Content and Location after a System Reboot

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

Upgrade the IONMM and/or 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 on the Product Support webpage (no logon required). Ideally, all the cards in a chassis will be upgraded to the latest versions at the same time; running devices with a mix of old and new firmware can cause a "red box" condition. See "Section 5: Troubleshooting" on page 368.
Note: You can not upgrade a module with multiple BIN files.

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

You can upgrade the IONMM or 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" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
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 Product Support web page.
5. Locate the "**Agent Firmware**" section and click the link in the right hand column (e.g., "**Download IONMM.bin.0.5.bin**").
6. Zip the downloaded file.
7. Retrieve the firmware database file using the **tftp get** command to get the file from the TFTP Server, and then press **Enter**. For example:

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

    A table of available modules displays with upgrade instructions.

```
C1|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 the module(s) 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.

```
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” on page 368 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 Upgrading Slide-In and Remote Modules.

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" on page 45).
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 x222x / x32xx NID or IONMM firmware for use in steps D1 and D2 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 Product Support web page.
2. Locate the "**Agent Firmware**" section and examine the link in the right hand column (e.g., "**Download x222x / x32xx_1.0.3_AP.bin**").
3. Compare the IONMM / 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 1 above to download the new firmware file.

C. Run TFTP Server

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

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

D. Upgrade the IONMM / NID Firmware

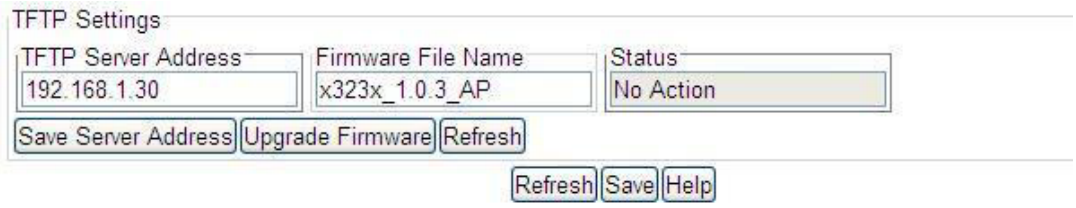
Perform this procedure to upgrade the IONMM / NID Firmware from either

- 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" on page 45).
2. Select the **MAIN** tab.
3. Locate the **TFTP Settings** section at the bottom of the screen.

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



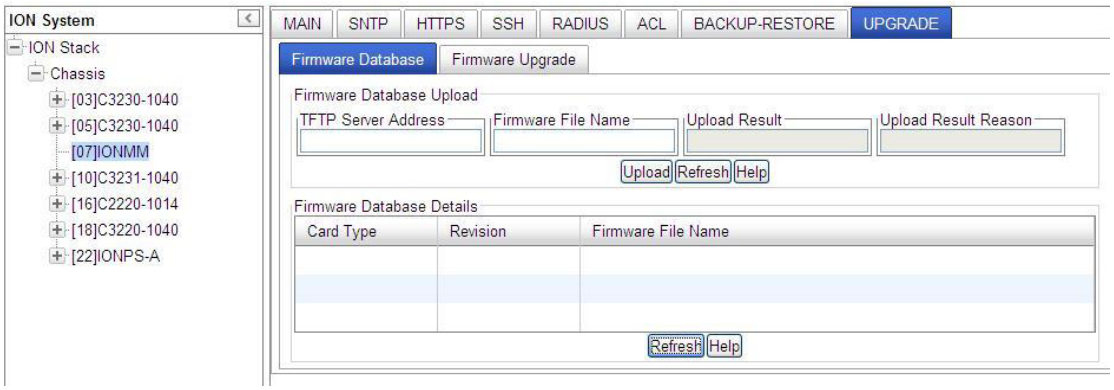
6. Click the **Upgrade Firmware** button.

   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 x222x / x32xx and/or IONMM reboots. When the reboot is complete, the message "*[xx]IONMM rebooting finished*" displays.
8. Click the **Refresh** button. The **Software Revision** area is updated from the old version number to the new version number (e.g., from 1.0.1 to 1.0.3).
9. If you will be using the same TFTP Server Address for future upgrades, click the **Save Server Address** button.

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

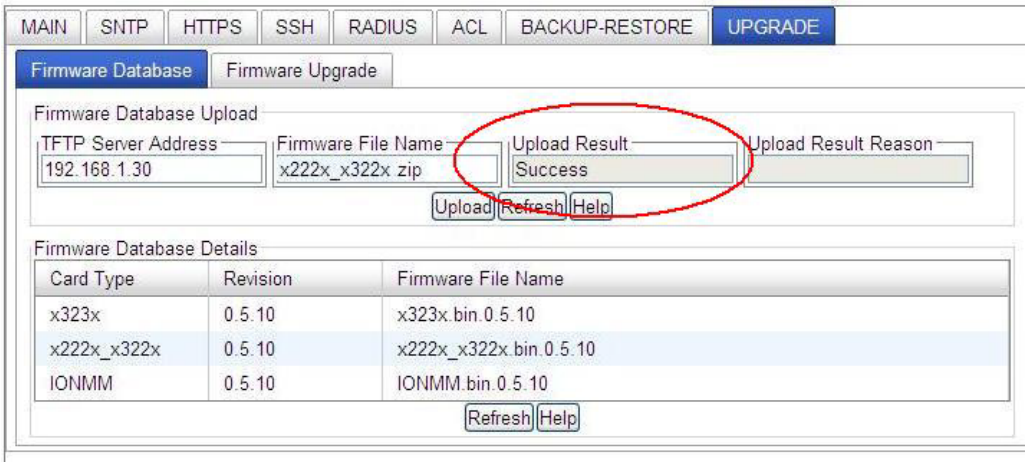
1. Access the IONMM card through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **UPGRADE** tab.
3. Select the **Firmware Database** sub-tab if not already selected.
4. Locate the **Firmware Database Upload** section.



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 C sub-step 5 above.
7. Click the **Upload** button.

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

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



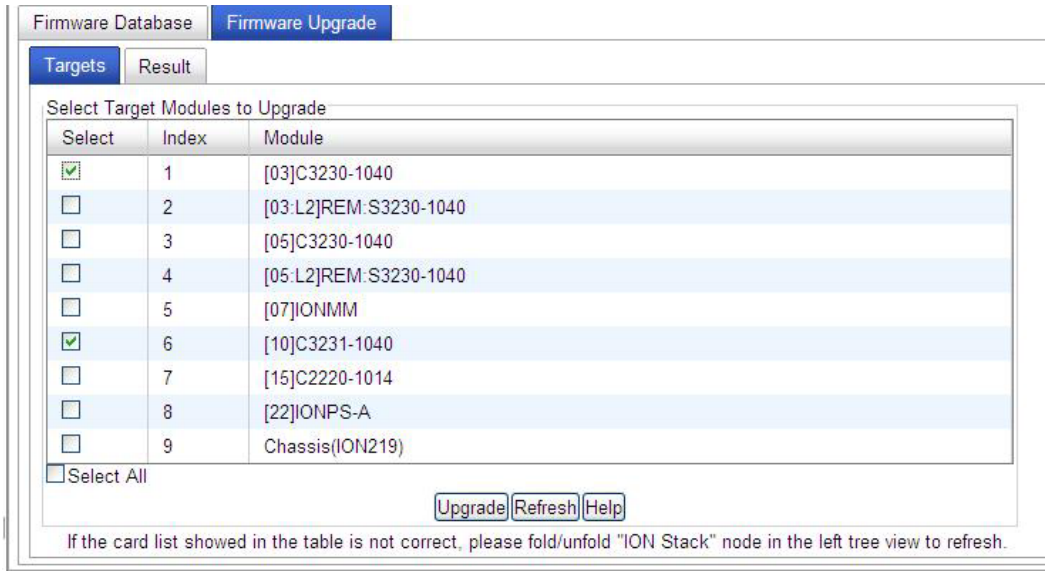
8. If the firmware upload operation failed, the **Upload Result** area displays either:

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

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

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

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

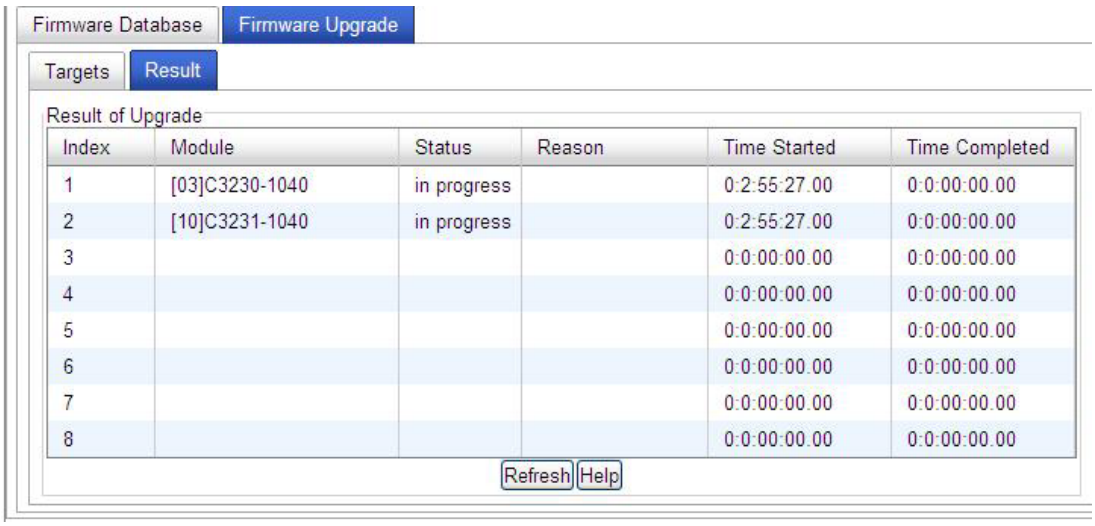


11. In the **Select** column, check the **IONMM** and/or one or more NIDs as the Target Module(s) to be upgraded.

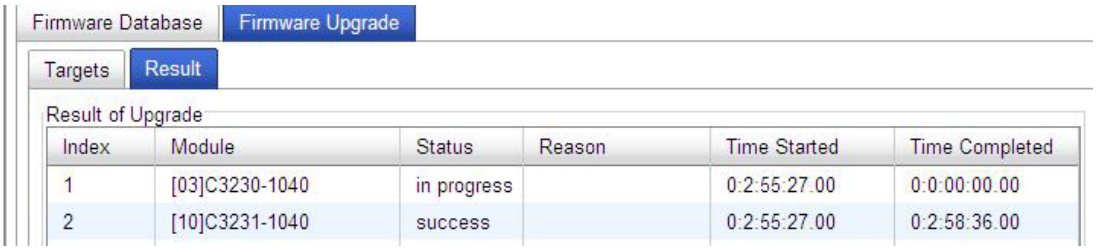
12. Click the **Upgrade** button.

13. Click the **OK** button to proceed.
    During the upload, the message "*Getting records in progress...*" displays.
    If the upload was successful, the message "*Getting all records finished*" displays.
    If the upload was unsuccessful, "*Getting records failed (http server error)*" displays.

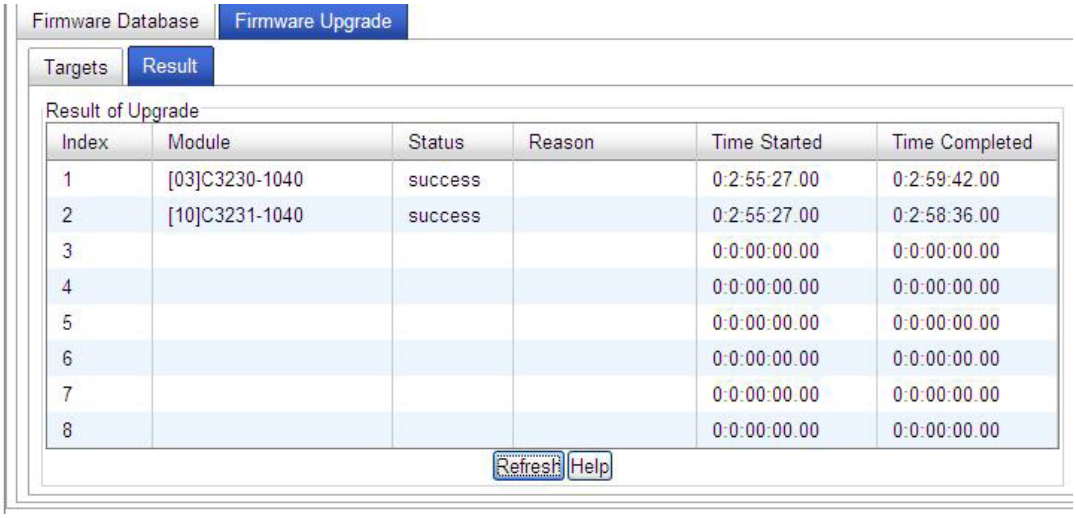
14. Click the **Result** sub-tab. A table displays with upgrade status information.



15. Click the **Refresh** button.



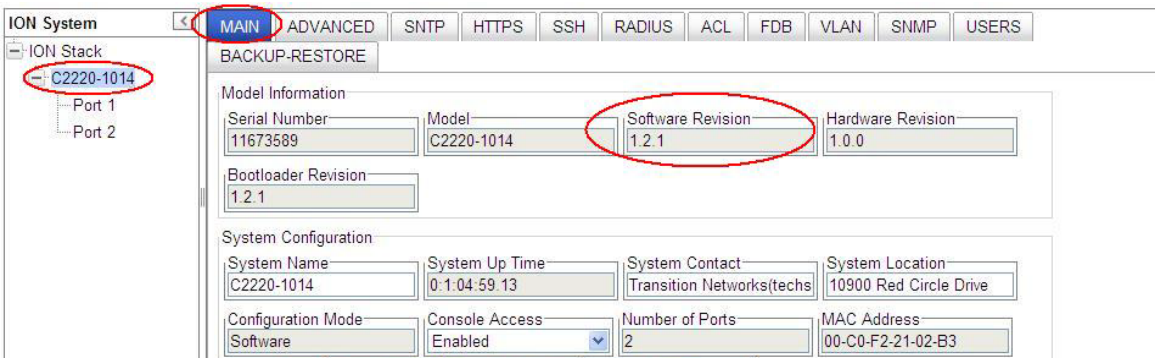
16. If upgrading more than one device, you may have to click **Refresh** again.



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

17. After the upgrade has successfully completed, "*success*" displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See "Section 5 – Troubleshooting" on page 368 for error messages and recovery procedures.

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



The sample screen above shows the C2220 **MAIN** tab with the Software Revision field indicating a successful firmware upgrade to version 1.2.1.

Upgrading Slide-In and Remote Modules Firmware via TFTP

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

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

- Have the upgrade files resident in the default directory on the TFTP Server (normally *C:/TFTP-Root*). To find the latest version of the firmware, go to the Product Support webpage.
- Create the Database Index and Archive Files (below).
- Perform the Module Firmware Upgrade (page 299).

Creating the Database Index and Archive Files

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

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

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

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

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

   model rev file
   Where:
   model = name of the module
   rev = revision level of the firmware upgrade file
   file = name of the firmware upgrade file

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

   Example: the example below shows a **db.idx** file for a system that has three modules (IONMM, x32xx, and x222x), and no second level remotes.

   x32xx 1.0.5 x32xx_1.0.5_AP
   x222x 1.0.5 x222x_x322x_1.0.5_AP
   IONMM1.0.5 IONMM_1.0.5_AP

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

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

4. Create a zip file that contains each of the upgrade files and the index file. Save the .zip file to the TFTP Server root directory (e.g., filename of **x222x / x32xx.bin.1.0.5.zip**).

   For example, using the files listed in the Example above, the **db.zip** file would contain the following four files:

   - db.idx

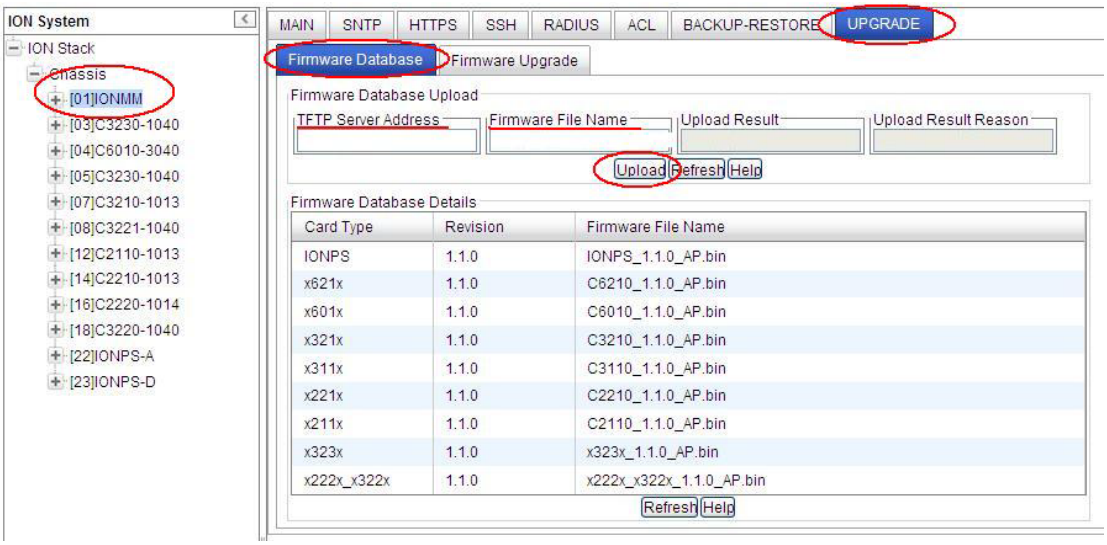
- x32xx_1.0.5_AP
- x222x_x322x_1.0.5_AP
- IONMM_1.0.5_AP

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

Performing the Module Firmware Upgrade

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

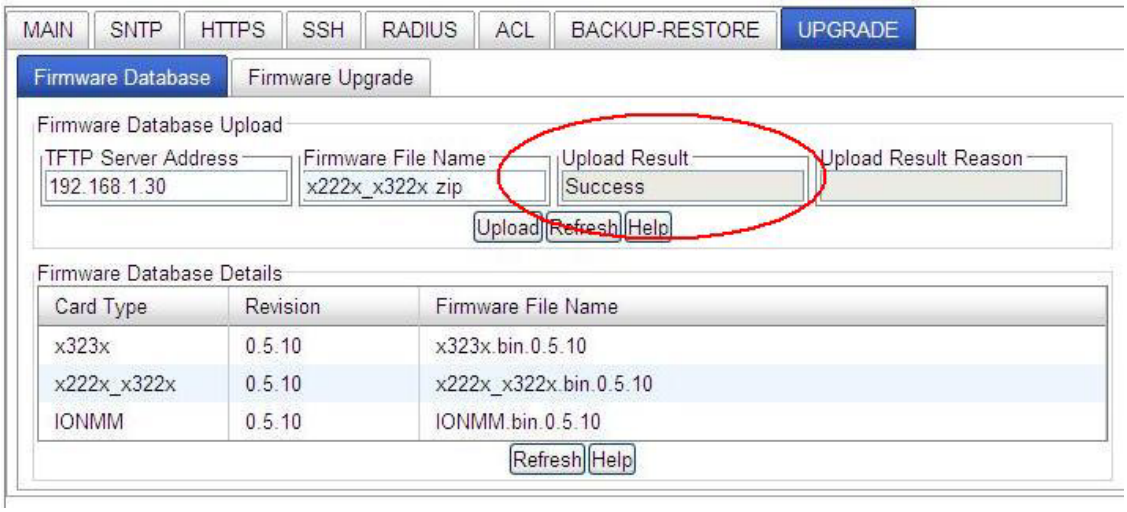
1. Access the IONMM through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **Upgrade** tab. The **Firmware Database** sub-tab displays.



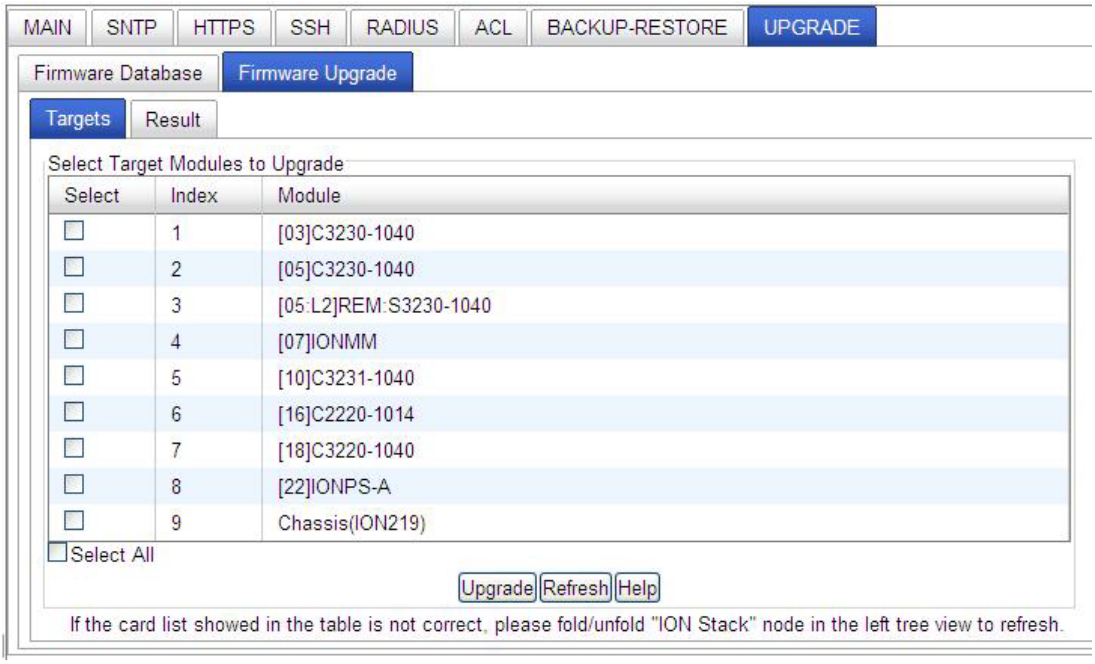
3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP Server where the upgrade (zip) file is located.
4. In the **Firmware File Name** field, enter the name of the zip file you created (e.g., **x222x / x32xx.bin.10.5.zip**). **Note**: Be sure to include the .zip extension in the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

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

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



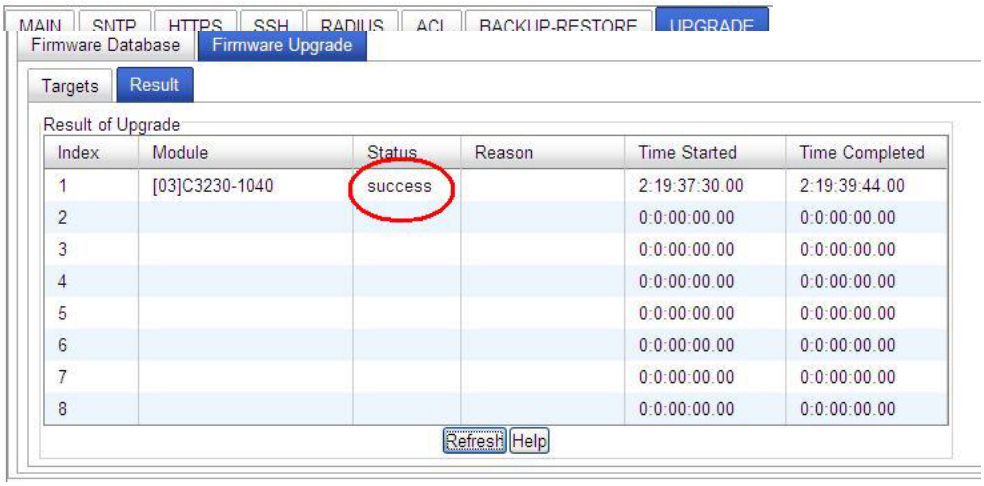
7. Select the **Firmware Upgrade** sub-tab. The **Targets** sub-tab displays.



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

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

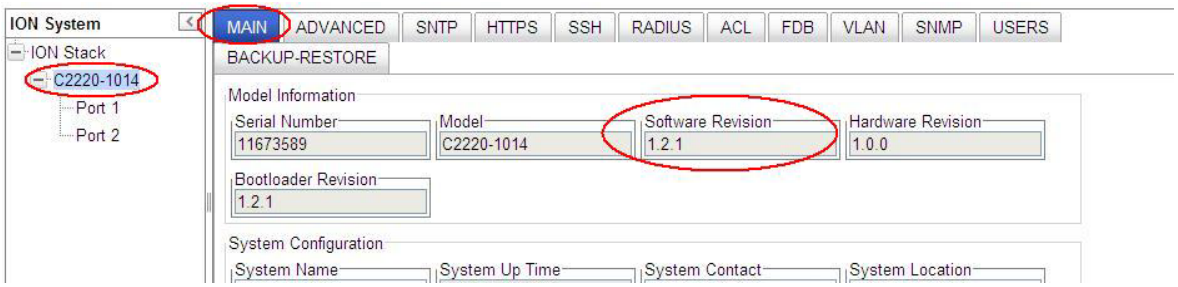
9. Click the **Upgrade** button.
10. When the confirmation window displays, click **OK**.
11. To monitor the progress, select the **Result** sub-tab and click **Refresh**.



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

After the upgrade has successfully completed, "*success*" displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See "Section 5 – Troubleshooting" on page 368 for error messages and recovery procedures.

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



The sample screen above shows the C2220 **MAIN** tab with the **Software Revision** field indicating a successful firmware upgrade to version **1.2.1**.

Upgrading Standalone Module Firmware via TFTP Server

This procedure is used to upgrade a remote stand-alone x222x / x32xx NID, a local stand-alone Cx2xx module installed in the ION Chassis, or a remote x222x / x32xx module connected to a slide-in module.

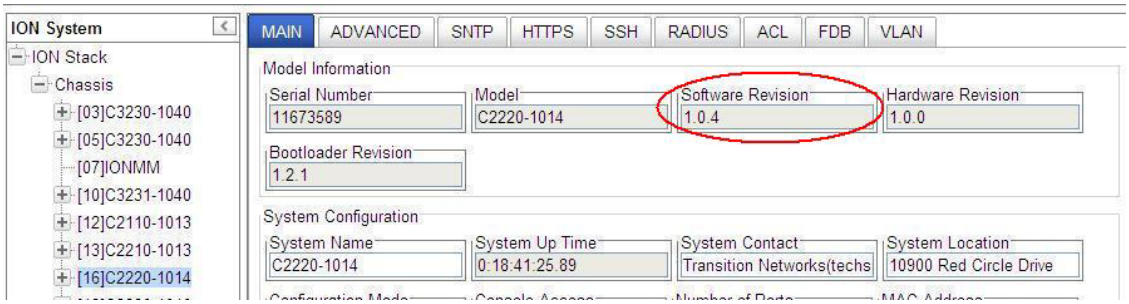
Before you can upgrade the firmware in the ION system modules you must do the following:

- Have the TFTP Server configured and running.
- Have the upgrade files resident in the default directory on the TFTP Server (normally TFTP-Root).

  To find the latest version of the firmware, go to the Product Support webpage.
- Verify that the standalone module is in the correct Switch Mode (local / remote mode). See "Changing Switch Mode (Local / Remote)" on page 69.

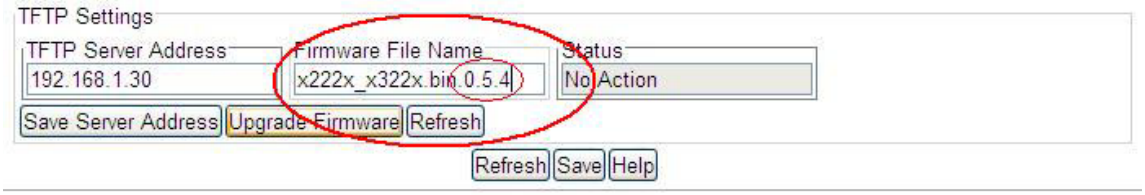
Use the procedure below for upgrading the firmware for a standalone module.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **MAIN** tab. Check the **Software Revision** field in the **Model Information** section (***0.5.1*** in the sample screen below).



3. Locate the **TFTP Settings** section at the bottom of the screen.

4. In the **TFTP Server Address** field, enter the IP address of the TFTP server that has the upgrade file (e.g., ***192.168.1.30*** in the sample screen below).



5. In the **Firmware File Name** field, enter the name of the upgrade file (***x222x_x322x.bin.0.5.4*** in the sample screen above).
6. Click the **Upgrade Firmware** button.

7. When the confirmation window displays, click the **OK** button.

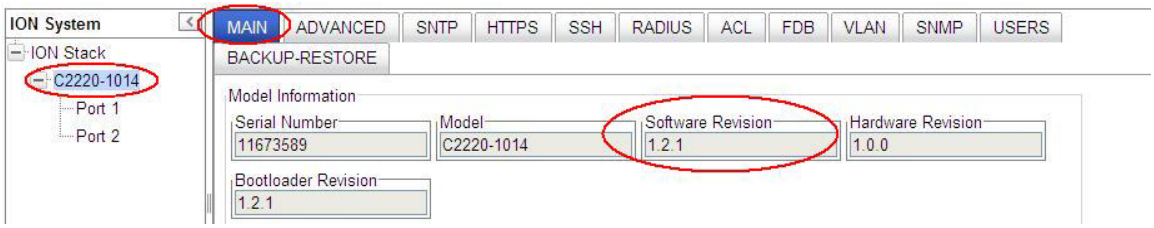
   The upgrade begins. The message "*The firmware is being upgraded ...*" displays. Note that this will take one or more minutes to complete. The exact amount of time for the upgrade depends on the module being upgraded.

   On successful firmware upgrade completion, the message "*S3230-1040 rebooting finished*" displays at the bottom of the screen, and the **MAIN** screen **TFTP Settings** section **Status** field displays "Success".

   If the upgrade fails, see "Section 5 – Troubleshooting" on page 261 for error messages and recovery procedures.

8. You can click the **Save Server Address** button to retain the TFTP Server address that you entered in step 4 above.

9. Check the module's **MAIN** tab to ensure that the correct revision level is displayed in the **Software Revision** field (e.g., successful x222x / x32xx firmware upgrade from revision ***0.5.4*** to revision ***1.2.1*** in the sample screens above and below).



10. After the upgrade has successfully completed, continue with Section 4: Configuration procedures on page 82 or Section 5: Operations on page 242.

Firmware Upgrade File Content and Location

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

Table 29: File Content and Location after a Firmware Upgrade

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

Additional Upgrade Procedures

Additional upgrade procedures are available for the ION system. Refer to the *IONMM User Guide* for these IONMM upgrade procedures:

- Upgrade the IONMM and/or NID Firmware.
- Upgrade Slide-In and Remote Modules Firmware via TFTP. This procedure is used to upgrade one or more of the slide-in modules installed in the ION Chassis or a remote module connected to a slide-in module. Requires you to 1) Create Database Index and Archive Files, and 2) Perform the Module Firmware Upgrade.
- Perform the Module Firmware Upgrade - the upgrade consists of two parts: uploading the archive file to the IONMM, and then loading the upgrade file into the appropriate modules. This procedure is for upgrading the ION family modules.

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 the USB 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 USB port by entering the corresponding CLI commands.

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

Perform this procedure to upgrade the x222x/x32xx firmware from the CLI.

1. Access the IONMM through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
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:

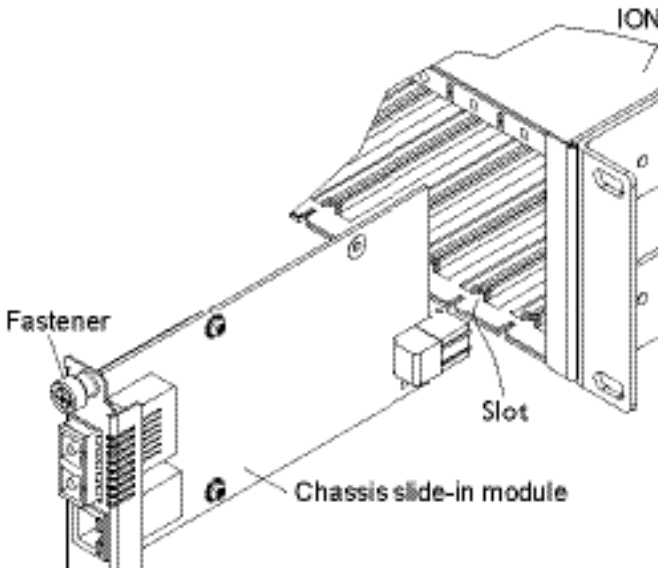
```
C1|S1|L1D>serial ?
  get
  put
  upgrade
C1|S1|L1D>serial get protocol zmodem file=xxxx
Warning: the input file name will be ignored when using ymodem/zmodem to retrieve file!
now start to transfer the file  ...
ŠCCCCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0BB0B
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file  ...
Šlsz: cannot open /tftpboot/xxxx: No such file or directory
BB0BB0BB0
BB0BB0
Can't open any requested files.
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>serial upgrade protocol zmodem file=xxxx
now start to transfer the file  ...
**B000000063f694ceive.**B000000063f694
CCCCCCCCCCBB0BBBB0BBBB0BBBB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>
```

If the serial file transfer causes HyperTerminal (HT) to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT.

Replacing a Chassis Resident NID

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

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



3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the NID from the Chassis.
5. Carefully slide the new NID fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the NID to the chassis.
7. Connect the appropriate cables to the NID.
8. Load the configuration into the new NID (see “Restoring Slide-In and Remote Modules” on page 234).

6. Troubleshooting

General

This section provides basic and specific problem determination processes, and a description of problem conditions that may occur or messages that may be displayed. This section also documents ION system tests and x222x / x32xx and jumpers, and describes where and how to get technical support.

IMPORTANT

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

Basic ION System Troubleshooting

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

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

- ION Chassis
- ION NIDs (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web Interface or ION command line interface - CLI).
- ION power supply
- ION Options (ION SFPs, ION LG Kit, etc.)
- Data cables, electrical cables, and electrical outlets
- Third party network equipment (circuit protection equipment, battery backup, 3rd party client or server software – RADIUS or TFTP, etc.)

When troubleshooting an ION system / network problem on site:

1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the 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 tests if functional, etc.).
6. Write down your initial 2-3 guesses as to the cause of the problem.
7. Verify that the Lantronix product supports the function you are attempting to perform. Your particular Lantronix product or firmware version may not support all the features documented

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

8. Use the Web interface or command line interface (CLI) to obtain all possible operating status information (log files, test results, **show** command outputs, counters, etc.)
9. If LOAM is configured, check the LOAM Event Log table parameters,. Print the output if possible.
10. Use the ION system manual procedure to retry the failed function or operation.
11. For the failed function or operation, verify that you entered valid parameters using the cursor-over-help (COH) and/or the ION system manual.
12. Based on the symptoms recorded, work back through each step in the process or operation to recall a point at which the problem occurred, and examine for a possible failure point and fixe for each.
13. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
14. 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).
15. If you find a sequence of actions that causes the problem to recur, replicate the full sequence several times and document it if possible.
16. 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.
17. Review the "Recording Model Information and System Information" section on page 338 before calling for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED Fault and Activity Displays (page 372)
- Problem Conditions (page 375)
- CLI Messages (page 392)
- Web Interface Messages (page 437)
- Windows Event Viewer Messages (page 463)
- Config Error Log (config.err) File (page 464)
- Webpage Messages (page 475)
- Third Party Troubleshooting Messages (page 516)

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, review the "Front Panel Connections and LEDs" section on page 54, and then perform the following steps.

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

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

1. Check for a loose power cord.
2. Check for a power supply failure. Replace power supply if failed.
3. Make sure all circuit protection and connection equipment and devices are working.
4. Verify that the ION system power supply is within operating range.
5. Remove the card from the chassis and re-insert it. Replace if failed.
6. Make sure the mode displayed matches the hardware setting on the device. See the "Jumper Settings" section on page 352.

LACT (Link Activity) LED off (not lit):

1. Check the data cables for obvious problems, incorrect type, incorrect wiring, etc.
2. See if the administrator has manually disabled the console device (PC) via the Web interface.
3. Check if other network devices are working properly.
4. Remove the suspect card from the chassis and re-insert it.
5. Check Auto-Negotiation setting.
6. See if the port transmission mode / speed (full or half-duplex, etc.) match those of the attached device.
7. Verify that the ION system devices have the latest firmware versions (see "Upgrade the Firmware" on page 123). Download the latest firmware version and upgrade as necessary.

Fault LED is lit:

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

TX or RX LED off (not flashing):

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

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 Auto Negotiation.

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 addres**s command displays each interface IPv6 address including the interface ID after the % character (the configuration can be accessed via the GUI).

Verify IPv6 Connectivity

Try to **ping** the local address. Note that if pinging link-local addresses from one host to another, you must include the destination adapter interface ID (e.g., ping fe80::38e7:3df1:f5ff:fdf0%13). When pinging site-local (equal to IPv4 Private) addresses you can add the interface ID to ensure that the address is configured on the desired interface. You must add an 'allow' rule for ICMPv6 traffic to pass through each computer's firewall.

Command examples - third party CLI commands for IPv6:

```
ipconfig /all
netsh interface ipv6 show address
ping fe80::38e7:3df1:f5ff:fdf0%13)
netsh interface ipv6 delete neighbors
netsh interface ipv6 show neighbors
netsh interface ipv6 delete destinationcache
netsh interface ipv6 show destinationcache
netsh interface ipv6 show route
route print
tracert -d <destination IPv6 address>
pathping -d <destination IPv6 address>
```

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
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. Check that the USB driver is installed on the PC/workstation. See "Installing the USB Driver" on page 31.
3. Check that the terminal emulator software is configured properly for the USB port and launched. See "Configuring HyperTerm" on page 35.
4. Check that the serial access is not disabled.
   a) Access the IONMM through the Web interface (see "Starting the Web Interface" on page 45).
   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**.
5. Restart the local management station (PC).
6. Power cycle the IONMM.
7. If the problem persists, contact Technical Support.

Cannot access the IONMM via Telnet

1. Check whether SSH is enabled.

   a) Access the IONMM through either a USB connection (see "Starting a USB Session" on page 41) or the Web interface (see "Starting the Web Interface" on page 45).

   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" on page 127). Is access restored? • Yes – end of procedure. • No – continue with step 3.	Continue with step 3.

3. Check whether Management VLAN is enabled.

   a) At the USB command prompt, type: **show mgmt vlan config**

   b) Press **Enter**.

4. Is Management VLAN enabled?

Yes	**No**
a) Make sure that the management station/PC is part of the same VLAN as the IONMM. b) Make sure that the correct port is being used on the IONMM. c) Is access restored? • Yes – end procedure. • No – continue with step 5.	Continue with step 5.

5. If the problem persists, contact Technical Support.

Cannot access the IONMM via the Web

1. Does the sign in screen appear?

Yes	No
Sign in using the default password; **private**. **Note:** the password is case sensitive.	Continue with step 2.

2. Verify that the default password has not been changed.
3. Check with your IT department that the network is up and running.
4. Check that the network cable is connected to the IONMM and the network port.
5. Check the IP addressing. At the command prompt, type **show ip-mgmt config** and press **Enter**. Verify the assigned IP address, Gateway IP address, and sub-net mask.
6. Check if HTTPS is enabled.
   a) Access the IONMM through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).

   Note: if you are unable to access the IONMM through the Telnet interface, go to step 7.

   b) At the command prompt, type: **show https config** and press **Enter**.

7. Is HTTPS enabled?

Yes	No
Access the IONMM through HTTPS or disable HTTPS (see "Configuring HTTPS" on page 115). Is access restored? • Yes – end procedure. • No – continue with step 7.	Continue with step 7.

8. Check if Management VLAN is enabled. At the USB command prompt, type **show mgmt vlan config** and press **Enter**.
9. Is Management VLAN enabled?

Yes	No
a) Make sure that the management station/PC is part of the same VLAN as the IONMM. b) Make sure that the correct port is being used on the IONMM. c) Is access restored? • Yes – end procedure. • No – continue with step 10.	Continue with step 9.

10. Disable the Management VLAN function. At the USB command prompt, type **set mgmt vlan state=disable** and press **Enter**.
11. If the problem persists, contact Technical Support.

Cannot access the NID via USB port

1. Can you access the IONMM?

Yes	No
Continue with Step 2.	See "Cannot access the IONMM via USB port" on page 168.

13. Check that the syntax for the **go** command is correct. 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 Standalone card

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

Cannot access the NID via Telnet

1. Can you access the IONMM?

Yes	No
Continue with Step 2.	See Cannot access the IONMM via Telnet on page 169.

14. Check that the syntax used for the **go** command is correct. The **go** command syntax 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 Standalone card

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

Cannot access the NID via the Web

1. Can you access the IONMM?

Yes	No
Continue with Step 2.	See "Cannot access the IONMM via the Web" on page 172.

2. Power cycle the NID.
3. If the NID is a remote, power cycle the local NID.
4. If the problem persists, contact Technical Support.

Cannot activate IP-based management

1. Verify that the IP, gateway, and subnet mask are configured correctly.
2. With DHCP enabled, DHCP could have failed leaving the system with the old static IP configuration. Check the configuration via the USB port.
   a) Access the IONMM through a USB connection (see "Starting a USB Session" on page 41).
   b) At the command prompt, type: **show ip–mgmt config**.
   c) Press **Enter**.
3. If the problem persists, contact Technical Support.

Cannot upgrade modules

See Upgrade fails on page 177.

Cannot upload upgrade files

See Upload fails on page 177.

Management Module does not power on

1. Does the chassis have power?

Yes	No
Check that the IONMM is seated properly in the chassis.	a) Check that the power cord is plugged into the unit and the wall socket. b) Plug the IONMM into a different outlet.

2. If the problem persists, contact Technical Support.

Telnet connection is lost after a CLI command is executed

1. Can you connect to the IONMM through the Web interface (see "Starting the Web Interface" on page 45)?

Yes	No
Go to step 3.	Continue with step 2.

2. Check the following:
   - the IONMM is seated properly in the chassis
   - the IONMM is powered up
   - the network cable is seated
   - the network is operational
3. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
4. Cycle power for the module in question. **Note**: for slide-in cards, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. If the problem persists, contact Technical Support.

Trap Server does not record traps

1. Ensure the Trap Server application is running.
2. SNMP traps may be blocked by a router or firewall. Consult your Network administrator to determine if this is the case.

3. Check that the correct SNMP trap manager IP address has been defined for the module.
   - For Web Interface – go to the **SNMP Configuration** section on the **MAIN** tab.
   - For CLI – at the device level, type: **show snmp config**.
4. If the problem persists, contact Technical Support.

Upgrade fails

1. Check the following:
   - The correct module(s) has been selected.
   - 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 modules are powered on.
2. Wait two minutes, and then retry the operation. If the operation still fails, continue with step 3 below.
3. Reboot the IONMM and all modules in the upgrade stream.
4. Retry the operation. **Note:** you will have to do another upload of the upgrade files.
5. If the problem persists, contact Technical Support.

Upload fails

1. Check the following:
   - The IONMM is powered on.
   - The IP address of the TFTP server is correct.
   - The TFTP server is online and available.
   - The correct file name (**db.zip** in Windows XP, just "**db**" in Windows 7) is specified (include the .zip extension in Windows XP, but not in Windows 7).
   - The **db.zip** (or **db**) file is in the default directory on the TFTP server.
   - The **db.zip** (or **db**) file contains the db.idx file and the upgrade files.
   - The db.idx file is formatted correctly ("Creating the Database Index and Archive Files" on page 148).
2. Wait three minutes then retry the operation. If the operation still fails, continue with step 3.
3. Reboot the IONMM.
4. Retry the upload operation.
5. If the problem persists, contact Technical Support.

USB connection resets after a CLI command is executed

1. Can you connect to the IONMM through the Web interface (see "Starting the Web Interface" on page 45)?

Yes	**No**
Go to step 4 of "Telnet connection is lost after a CLI command is executed" on page 168.	Continue with step 2.

2. Check the following:
   - the IONMM is seated properly in the chassis
   - the IONMM is powered up
   - the network cable is seated
   - the network is operational
3. For all modules (slide-in and remote) check the following:
   - the module is properly seated/connected
   - the module is powered up
4. Cycle power for the module in question.

5. If the problem persists, contact Technical Support.

Configuration Mode Mismatch

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

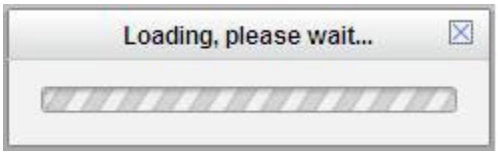
The device may have a jumper or switch that disables software management of the device. When Configuration Mode is **hardware**, the devices take some of the configurations from DIP switches or jumpers on the device. In **software** mode, configuration is controlled by management.

1. Refer to the "Jumper Settings" section on page 312 for details on hardware mode configuration.
2. Contact Lantronix for more information. Contact Technical Support.

Ethernet connection works, but at a very low speed

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

loading, please wait ... Displays continuously



1. Wait for one or more minutes for discovery to complete.
2. Click the ☒ icon to close the message.
3. Check the parameter entries and retry the operation.
4. Click the **Refresh** button and try the operation again.
5. If the problem persists, contact Technical Support.

No ACL condition now!

You entered a **show acl condition** CLI command, but you have not yet defined an ACL Condition.

1. Define the associated ACL condition. See "Configuring an ACL" on page 211.
2. Verify the ACL Condition. For example:

   C1|S7|L1D>**show acl condition**

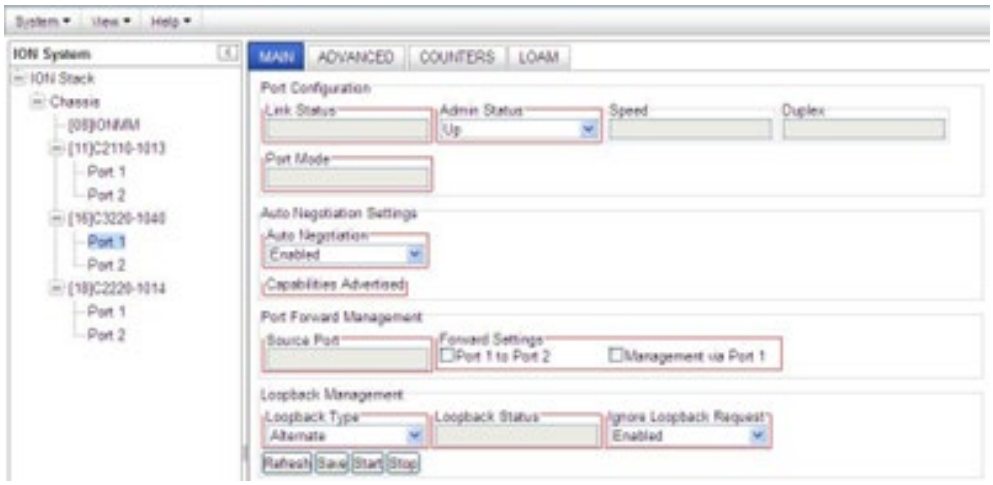
3. If the problem persists, contact Technical Support.

No ACL rule now!

When doing a backup of the IONMM and several other modules, an error was detected when the IONMM was initially backed up (AGENT PM ERROR: CLI command show acl rule failed).

1. Execute a System reboot on the IONMM.
2. Execute a backup on the IONMM alone.
3. If the problem persists, contact Technical Support.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



1. Check if the device is physically connected and powered on.
2. Refresh the IONMM or NID by clicking the **Refresh** key.
3. Collapse and then expand the ION System tree (i.e., fold and then unfold the "ION Stack" node in the left tree view) to refresh.
4. Cycle power for the module in question.
5. Upgrade the devices to the latest software version.
6. Reboot the device by clicking the **Reboot** key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
7. If the problem persists, contact Technical Support.

Red box Condition after Reboot

When the reboot is finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The ‘red box’ condition occurs while the devices are resetting; this condition can continue several minutes after the reboot. Until the system is ready to be fully managed, certain fields may display within "red boxes". The "red boxes" will disappear when the system is ready to be fully managed.

1. Wait a couple of minutes for the current operation to complete, and then continue operation.
2. Check the devices’ firmware versions. For example, a C2220 has only certain items ‘red boxed’. The IONMM in this case is at latest version and shows certain new functions on the GUI, while the 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 on page 285 for more information.
4. Contact Lantronix for more information. Contact Technical Support.

TFTP Server Address is empty or invalid!

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

Windows XP Cannot Find Drivers For My Device

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

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

Windows XP Forces a Reboot after Installing a Device

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

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

Driver Installation Fails and Windows XP Gives Error Code 10

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

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

Windows XP Displays an Error and then Terminates Installation

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

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

1. To change the current driver signing setting, in Windows XP, go to "Control Panel\System", click on the "Hardware" tab and then click "Driver Signing".
2. Select the desired signing option.

For other USB Driver / OS Messages (Win2K, Vista, Windows 7, Linux, Mac) refer to the separate document with Driver / OS install, uninstall and troubleshooting information.

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

Meaning: If a power supply is powered down or loses input power, the only indication on the web interface is a Power reading of 0.0. The "Power Status OK" means that the Power Sensor is operating normally, not that the input power is OK.
Recovery: To check the loss of power, check at **IONPS-A** > **MAIN** tab > **Sensor and Fan(s)** section > **Power** value field. See Appendix H on page 653 for more information.

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

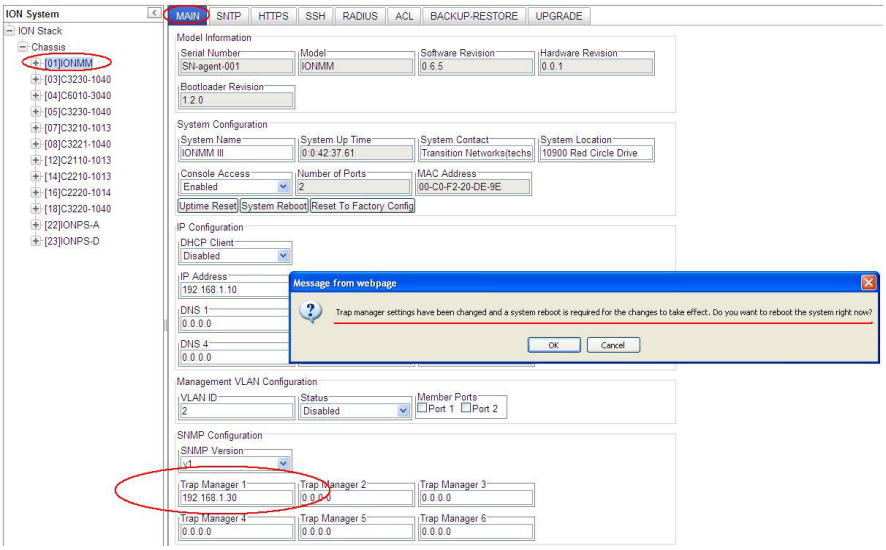
Meaning: In ION v1.0.3, the user-public key is binding with the Linux root user and is stored in the root file system (/root/.ssh/). This file system will be replaced after this version upgrade, so this key will be lost.

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: "*Unknown command.*" message displays when entering system name/contact/location.
Problem: The **System Name** can not be restored when the system name contains special character "space" in the middle.
Meaning: The "Unknown command." message displays when the system name/contact/location contains a "space" character within the text using the CLI command "**set system name**" or "**set system contact**" or "**set system location**" is entered. The entry for the system contact, system location, and system name must be a text string with no spaces between characters. Note that numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed.
Recovery: From the Web interface, at the device's **MAIN** tab in the **System Configuration** section, re-enter the "**System Name**" or "**System Contact**" or "**System Location**", making sure there are no spaces between the text characters.
From the CLI, re-enter the "**set system name**" or "**set system contact**" or "**set system location**" CLI command, making sure there are no spaces between the text characters. 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!@#$%
C1|S1|L1D>
```

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

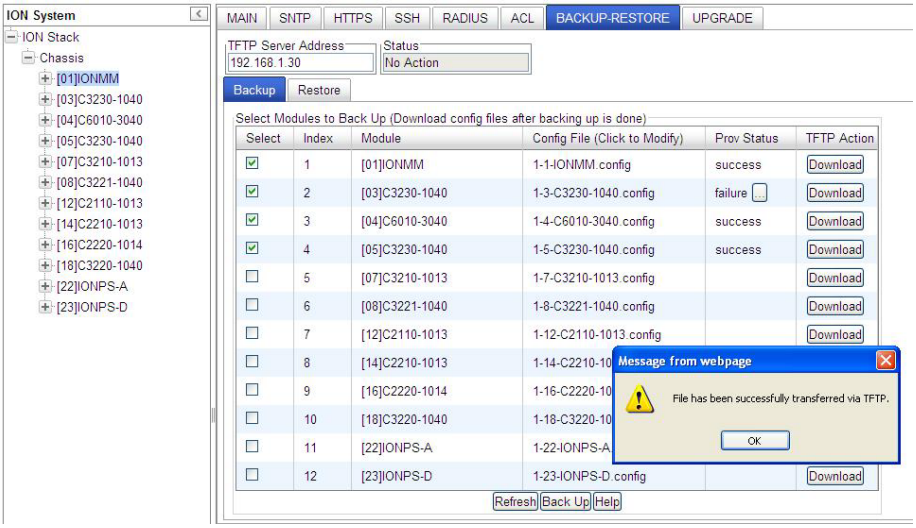


Meaning: Information only. At **IONMM > MAIN** > **SNMP Configuration** > **Trap Manager x** you entered an IP address for a trap server.

Recovery:

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

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



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

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

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

CLI Messages

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

Add ACL rule failed.

This message indicates that the rule could not be added.

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

Ambiguous command

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

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

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

C1|S7|L1D>**add v**

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

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

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

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See the *ION System CLI Reference Manual, 33473*.
4. If the problem persists, contact Technical Support.

Bad advertisement capability!

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

1. Verify the command syntax.
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.
3. If the problem persists, contact Technical Support.

Cannot get link pass through information on this card

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

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

1. Use the go command to change from the IONMM to the specific slide-in module. The **go** command format is:

   go [c=<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 Standalone card
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Cannot get OAM configuration on this port!

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

1. 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 Standalone card
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.
3. If the problem persists, contact Technical Support.

Cannot get port security on this port!

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

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.
3. If the problem persists, contact Technical Support.

Command incomplete

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

1. Verify the command syntax. Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

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

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

1. Ensure that the Telnet port is set to 23 for both the server and the client. This will require someone with administrative rights in order to make a change.
2. Add the port number to the Telnet command. Example:

   Telnet <ipaddr> <port#>

3. If the problem persists, contact Technical Support.

Error: this command should be executed on a device

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

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=<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 Standalone card
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Error: this command should be executed on a port

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

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)

   for a Slide in card, or

   go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for Standalone card
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Fail to get MAC address!

This message indicates that communications to the module can not be established.

1. Verify that the correct hierarchy has been specified in the command (see "Managing Slide-In and Remote Modules Using CLI Commands" on page 49).
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
6. If the problem persists, contact Technical Support.

Fail to get port type!

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

1. Use the **go** command to change location of where the command operates.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Failed to set DHCP client state!

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

1. Verify the operation in the "Assigning a Dynamic IP Address" section on page 91.
2. Retry the operation. See the related DHCP command in *the ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

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

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

1. Verify the operation in the "Configuring SNTP" section on page 203.
2. Retry the operation. See the related SNTP command in *the ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Incomplete location command!

This message indicates that one or more parameters for the **go** command are missing. The go command was entered to set location parameters, but the module, slot and/or port value(s) were no included in the command string.

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

1. Verify the command syntax.
2. Re-enter the **go** command and be sure to include all of the location parameters:

```
go [c=CHASSIS] [s=SLOT] [l1ap=L0APORT] [l2ap=L1APORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

3. If the problem persists, contact Technical Support.

Invalid ACL condition index!

This message indicates that you tried to associate an ACL condition with an ACL rule but the condition does not exist.

1. Check what conditions exist; type:

   show acl condition

2. Associate the correct condition with the correct rule, or create the condition if it does not exist.
3. If the problem persists, contact Technical Support.

Invalid ACL rule index!

This message indicates that you tried to associate an ACL condition with an ACL rule that does not exist.

1. Check what rules exist; type:

show acl rule

2. Associate the correct condition with the correct rule, or create the rule if it does not exist.
3. If the problem persists, contact Technical Support.

Invalid condition value: xxxx

This message indicates that the input for the value= parameter on the **add acl condition** command in not valid.

1. Verify the value being input; it must match with the value input for type=.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid location parameters, cannot find the physical entity!

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

1. Verify that the correct hierarchy has been specified in the command (see "Managing Slide-In and Remote Modules Using CLI Commands" on page 49).
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation.
6. If the problem persists, contact Technical Support.

Invalid user!

This message indicates that the specified user is not valid.

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

Login incorrect

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

1. Verify the login/password.

   Note: the login and password are case sensitive. The default login is **ION** and the default password is **private**.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

No DMI support on this port!

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

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

Now the value of table can only be "filter"!
This message indicates that 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|out-
put|postrouting}
C1|S7|L1D>set acl table nat chain {prerouting|input|forward|out-
put|postrouting}
C1|S7|L1D>set acl table mangle chain {prerouting|forward|out-
put|postrouting}
```

1. Enter the parameters table=filter and chain=input.
2. See "Configuring an ACL" on page 211.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

There is no matched command

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

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

Unable to open xx. Please check your port settings.

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

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

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

4. In the HyperTerminal window, select **File>Properties**.
5. Check that the correct port is listed in the **Connect using** field.

6. Restart the management station.
7. Reboot the IONMM.
8. If the problem persists, contact Technical Support.

Error, you should first give full location parameters

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

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

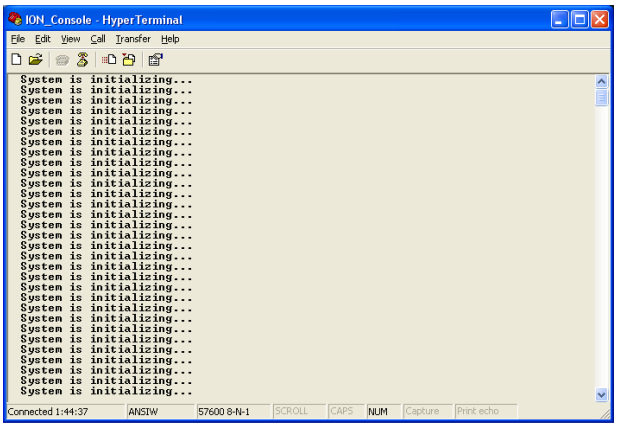
If the value of module, slot and port are not set in later commands, and then you run a device-level command (e.g., **show lpt config**), this error message displays.

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

go [c=CHASSIS] [s=SLOT] [l1ap=L0APORT] [l2ap=L1APORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)

System is initializing...

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



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

Start HTTPS certificate failed.

1. Verify the HTTPS parameters (HTTPS is enabled, the certificate type is defined, certificate file defined, private key file defined, password defined).
2. Verify that the HTTPS server is operational.
3. Retry the operation (i.e., type **start https certificate** and press **Enter**).
4. If the problem persists, contact Technical Support.

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

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

Error: this command should be executed on a port!

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

Unknown command!

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

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
4. If the problem persists, contact Technical Support.

There is no matched command.

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

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
4. If the problem persists, contact Technical Support.

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

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

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

```
go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

Fail to set link pass through state!

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

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

and then pressed **Enter**.

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

   If either is set to **notSupported**, change the setting to enable (e.g., type **set rfd state enable** and press **Enter**).
4. Retry the operation.
5. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
6. If the problem persists, contact Technical Support.

Invalid erate!
Invalid irate!

You tried to set the Ingress or Egress rate to an unacceptable limit. For example, you typed:

```
C1|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, 33473*.
3. If the problem persists, contact Technical Support.

TFTP transfer failed!

1. The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.
2. Verify the CLI command syntax.
3. Verify the firmware version.
4. Be sure the TFTP server is configured and running.
5. Check that the remotefile is in the proper location (e.g., the file *x222x / x32xx.bin.0.5.4* is at *C:\TFTP-Root*).
6. Retry the operation. See the **tftp upgrade** command in the *ION System CLI Reference Manual, 33473*.
7. If the problem persists, contact Technical Support.

Fail to transfer the file!
tftp get: set address type failed.
tftp put failed.

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

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

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

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” on page 190.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Cannot set service translation type on this card!

The attempted command was rejected. For example, you entered:

`C1|S7|L1D>set dot1bridge service-translate addProviderTag`).

1. Verify that the card you entered the command on supports this function.
2. Retry the operation. See the **dot1bridge** commands section in the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Cannot set service vid for tag on this card!

The attempted **set dot1bridge vid** command was rejected (e.g., `C1|S7|L1D>set dot1bridge vid 2`).

4. Verify that the card you entered the command on supports this function.
5. Retry the operation. See the **dot1bridge aging-time** command.
6. If the problem persists, contact Technical Support.

Fail to set aging time!

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

1. Verify the **dot1bridge aging-time** command syntax. See "Configure Forwarding Learning Aging Time" on page 191.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

Get aging time failed!

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

1. Verify the **dot1bridge aging-time** command syntax. See "Configure Forwarding Learning Aging Time" on page 191.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

CLI command remove fwddb all failed

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

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

1. Retry the operation. See "Backup/Restore Operations" on page 256.
2. See the *ION System CLI Reference Manual, 33473*.
3. If the problem persists, contact Technical Support.

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

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

1. Retry the operation with the correct parameter entry.
2. See the *ION System CLI Reference Manual, 33473* for the full set of available command parameters.
3. If the problem persists, contact Technical Support.

Redundancy is not supported on this card!

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

1. Verify that the card you entered the command on supports this function.
2. Retry the operation on a card that supports this function. See the "Fiber Redundancy Commands" section on page 104.
3. If the problem persists, contact Technical Support.

Invalid user!

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

1. Retry the operation using the correct user information. See "Show SSH Public Key of a User" on page 156.
2. If the problem persists, contact Technical Support.

Fail to set SSH server state!

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

1. Use the **get** command to obtain the key file. See the "TFTP Commands" on page 157.
2. Use the **set ssh public–key user** command to set the public key to a user from a key file.
3. Try the **set ssh server state=enable** command again. See "SSH Commands" commands on page 152.
4. If the problem persists, contact Technical Support.

Fail to transfer the file!

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

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

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

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

1. Verify the VLAN Management configuration using the **show vlan** command and the **show vlan service** command.
2. Review the set mgmt vlan command syntax for the port / state / vid. See the "VLAN Commands" on page 159.
3. If the problem persists, contact Technical Support.

Upgrade is only supported on IONMM card!

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

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

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

Cannot set bandwidth alloc type on this card!

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

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

1. Verify if the card supports bandwidth allocation.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands" on page 53.
4. If the problem persists, contact Technical Support.

Cannot set ingress and egress rate on this card!

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

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

1. Verify if the card supports rate limiting.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands" on page 53.
4. If the problem persists, contact Technical Support.

DMI is only supported on FIBER port!

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

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

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

Link OAM is not supported on this card!

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

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

1. Verify if the card supports loopback.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. See "OAM Commands" on page 58.
4. If the problem persists, contact Technical Support.

Cannot clear loopback counters on this card!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set autocross on this card!
Cannot set auto negotiation state on this port!
Cannot set Ethernet port speed for this card!
Cannot set Ether port duplex mode on this card!
Cannot set far end fault on this card!
Cannot set filter unknown dest multicast frames on this port!
Cannot set filter unknown dest unicast frames on this port!
Cannot set pause on this port!
Cannot set source address lock action on this port!
No Time-domain reflectometer support on this card!
Cannot get port security configuration on this port!
Fail to get MAC control frames statistics!
Cannot show forwarding port list on this card!
Cannot show slot info on this card!
Cannot show USB port state on this card!
Cannot show USB port configure on this card!
Cannot show TP port cable length on this card!
Cannot set management VLAN on this card!
Cannot set PHY mode on this port!
Cannot clear counters on this port!
Cannot reset all ports' counters on this cards!

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

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

1. Verify if the card supports the desired function. See Table 3 in the section "Ethernet Port Commands" on page 64.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. The command functions include 1) admin, 2) adv-cap, 3) autocross, 4) autoneg, 5) duplex, 6) fef, 7) filter-unknown-multicast, 8) filter-unknown-unicast, 9) loopback, 10) pause, 11) speed, and 12) src-addr-lock, 13) tdr, 14) ether security config, 15) fwddb, etc.

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

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

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

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

1. Verify if the card supports the desired function.
4. Use the **go** command to switch to a different card port supporting loopback.
2. Verify the command entry. See "QoS Commands" on page 98.

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" on page 160.

Fail to get system name!

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

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

1. Try entering the **show cardtype** command.
2. Select the **MAIN** tab > **System Configuration** section **> System Name** field, and verify the name and for the device.
3. Use the set system name command to enter the **System Name** information (e.g., **set system name**=NAME).
4. Remove and reset the card.
5. Try the operation again.
6. If the problem persists, contact Technical Support.

Set system name timeout.

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

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

1. Use the set system name command to enter the System Name information (e.g., **set system name=NAME**) without any special characters (e.g., without the ! or # or % or & characters).
2. Remove and reseat the card.
3. Try the operation again.
4. Select the **MAIN** tab > **System Configuration** section **> System Name** field, and verify the name and for the device.
5. If the problem persists, contact Technical Support.

System is busy, please retry this command later!

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

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

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

Get HTTPS state no such object.
Get management VLAN state no such object.
IP management state no such object.

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

```
C1|S10|L1D>show https config
HTTPS configuration:
------------------------------------------------------------------------
Get HTTPS state no such object.


C1|S10|L1D>show mgmt vlan config
vlan id   vlan state          vlan portlist
------------------------------------------------------------------------
Get management VLAN state no such object.

C1|S10|L1D>show ip-mgmt config
IP management configuration:
------------------------------------------------------------------------
IP management state no such object.
```

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

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

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

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

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

The attempted ping command failed. For example:

```
PING 192.168.0.10 (192.168.0.10): 56 data bytes
--- 192.168.0.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

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

Ping command can only be used on management card!

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

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

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

Admin state of Link OAM of this port is disable, please enable it first!

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

```
C1|S16|L1P1>set oam loopback oper=stop
```

```
Admin state of Link OAM of this port is disable, please enable it first!
```

1. Use the **set ether admin state=up** command to enable the Ethernet port for use.
2. Use the **set oam admin state=enable** command to enable OAM administration.
3. Use the **show oam loopback** commands and **show oam config** commands to verify the configuration.
4. Re-enter the **loopback** command.
5. If the problem persists, contact Technical Support.

Only 100M fiber port can set far end fault!

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

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

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

Can not set 1000M speed for this card!

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

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

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

Fail to set Ethernet port speed!

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

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

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

Invalid pause value!

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

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

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

Set Ethernet port loopback type failed.

You tried to use the **set oam loopback type** command to set the device's type of loopback support, but the command was not accepted. For example:

```
C1|S16|L1P1>set oam loopback type=phylayer
Set Ethernet port loopback type failed.
C1|S16|L1P1>
```

1. Verify the command syntax.
2. Use the **set oam loopback type** command to set the device's type of loopback support (alternate, maclayer, noloopback, phylayer, or remote).
3. If the problem persists, contact Technical Support.

Please input a number to specify threshold!
You entered a number to specify the errored frame (ef) threshold, but the number was not accepted. For example:

```
Please input a number to specify threshold!
C1|S16|L1P1>set oam ef threshold 100099
```

1. Enter the command **set oam ef threshold=** with a threshold number from 0-999999.
2. See the **set oam ef threshold** command for details.
3. If the problem persists, contact Technical Support.

The specified ACL rule index does not exist!

You tried to set an ACL Rule ID and traprate, but did not first create the associated rule.
For example:

```
C1|S16|L1D>set acl rule 1 traprate 4444
The specified ACL rule index does not exist!
```

1. Make sure ACL operations are enabled; see the **set acl state** command on page 48.
2. Create an ACL rule. See "Add a New ACL Rule" on page 48.
3. Try entering the **set acl rule command** again.
4. If the problem persists, contact Technical Support.

Current VLAN tagging mode is not 'provider'!

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

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

1. Set the VLAN tag mode to the desired mode using the **set port vlan tag mode** command.
2. If the problem persists, contact Technical Support.

Cannot set VLAN network tagging on this port!

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

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

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

Cannot show system information on this card!

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

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

1. Use the **go** command to switch to a different device (e.g., from the Power Supply to the IONMM or an x222x/x32xx card).
2. Try entering the **show system information g** command again.
3. If the problem persists, contact Technical Support.

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

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

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

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

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

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

Invalid forward port list!
```

1. Re-enter the command, wait for the prompt, and then enter a response in the correct syntax.
2. See the related command / function section of this manual.
3. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.
4. If the problem persists, contact Technical Support.

L2CP is not supported on this card!
You tried to perform an L2CP function but the device does not support L2CP.
1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports L2CP.
3. Try entering the command again. See “Configuring L2CP” on page 268.
4. If the problem persists, contact Technical Support.

Please give parameters for L2CP configuration:%s
You tried to perform an L2CP function but have not defined the L2CP parameter(s).
1. Verify the L2CP command parameters. See “Configuring L2CP” on page 268.
2. Try entering the command again.
3. If the problem persists, contact Technical Support.

Cannot show circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.
1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports Circuit ID display.
3. Try entering the command again. See "Circuit ID" on page 268.
4. If the problem persists, contact Technical Support.

Cannot set circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.
1. Verify the Circuit ID parameters. See "Circuit ID" on page 268.
2. Try entering the command again.
3. If the problem persists, contact Technical Support.

Please reboot the card for the changes to take effect!

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

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

1. Reboot the card. See the "Reboot" section on page 292.
2. Continue the operation.
3. If a problem persists, contact Technical Support.

Get DMI identifier no such object.

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

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

1. Make sure this is the command / function that you wanted.
2. Try entering the command again. See "DMI (Diagnostic Maintenance Interface) Parameters" on page 395.
3. If a problem persists, contact Technical Support.

Get SNMP version no such object.

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

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

1. Make sure this is the command / function that you wanted.
2. Verify the command syntax. See "Configuring SNMP" on page 245.
3. For complete command descriptions, see the *ION System CLI Reference Manual, 33473*.
4. Try entering the command again. See "DMI (Diagnostic Maintenance Interface) Parameters" on page 395.
5. If a problem persists, contact Technical Support.

Fail to set Ethernet port loopback operation, please check if Link OAM admin state of remote peer port is enabled, link status and other issues.

You entered the CLI command to define the type of Ethernet loopback test, but the command failed. For example:

```
C1|S5|L1P2>set oam loopback oper init
Fail to set Ethernet port loopback operation, please check if Link OAM
admin state of remote peer port is enabled, link status and other issues.
C1|S5|L1P2>
```

1. Make sure the Link OAM admin state of remote peer port is enabled (see "**set oam admin state enable**" command).
2. Verify the command syntax.
3. Use the **set oam loopback ?** command to display the card's loopback capabilities. For example:

```
C1:S7:L1P1>set oam loopback type ?
 alternate
 noloopback
 remote
```

4. Re-enter the **set oam loopback=** command with a loopback capability supported by the card (alternate, or remote or noloopback).
5. Verify the loopback capability with the **show oam loopback capability** command. For example:

```
C1|S5|L1P2>show oam loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P2>
```

6. If the problem persists, contact Technical Support.

Fail to remove ACL condition!
Fail to remove ACL rule!

You tried to delete an ACL rule or condition, but the operation failed.

1. Make sure ACL Status is enabled.
2. Verify the command syntax. See "Configuring an ACL" on page 219.
3. For complete command descriptions, see the *ION System CLI Reference Manual, 33473*.
4. If a problem persists, contact Technical Support.

Fail to get cable length

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

1. Make sure the NID supports the VCT Test (TDR Test) or the **show cable length** command (available for x2110).
2. Make sure you enter the Time Domain Reflector (TDR) test on an Ethernet copper port.
3. Verify the command syntax. See "Virtual Cable Test (VCT)" on page 409.
4. Type **show ether tdr config** to show the Ethernet port TDR Test configuration.
5. If the problem persists, contact Technical Support.

Can not set speed on this port!

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

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

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

Fail to set port advertisement capability!

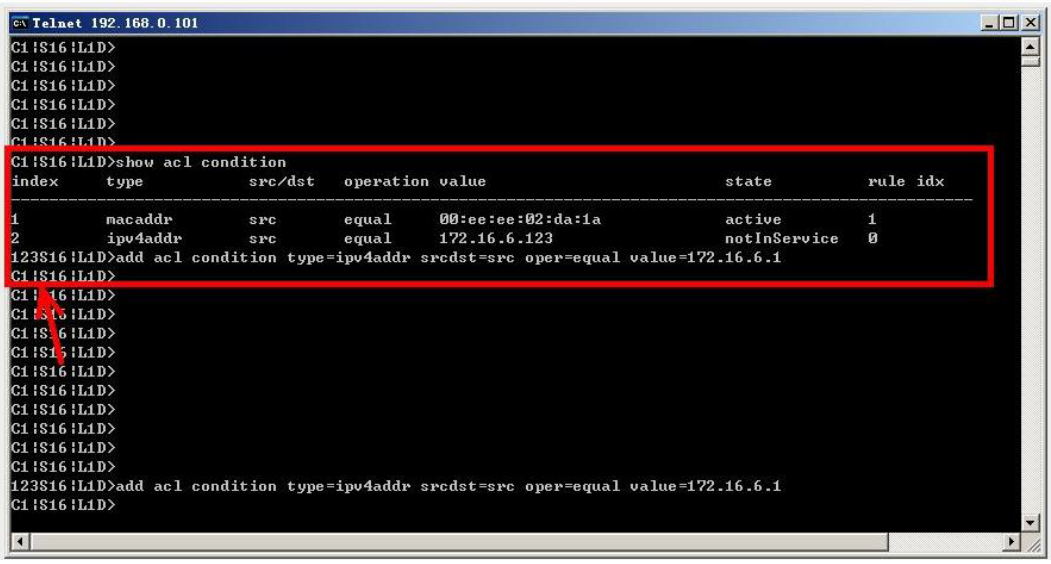
This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability (set ether adv-cap) command are not valid choices. For example:

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

1. Verify the NID supports this capability.
2. Verify the command syntax.
3. Retry the operation. For a complete list of the available commands, see “Appendix A: CLI Command Summary” on page 174.
4. If the problem persists, contact Technical Support.

Long Command Causes Cursor Wrap to Same Line

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



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

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

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

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

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

Currently HTTPS certification type is self-certificated, so you need not set private key file!

You entered a command to set the private key file, but the HTTPS certification type is currently set to "self-certificated". For example:

```
C1|S5|L1D>set https private-key file=privkey
Currently HTTPS certification type is self-certificated, so you need
not set private key file!
```

1. Make sure this is the HTTPS certification type that you want.
2. Use the **set https certificate–type** command to change the HTTPS certification type.
3. If the problem persists, contact Technical Support.

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

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

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

Cannot create VLAN database on this card!

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

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

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

Cannot remove vlan on this card!

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

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

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

Cannot remove forward database rows on this card!

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

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

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

Error symbol period window low is out of range, its range is 125000000 - 268435455!
Error frame period window is out of range, its range is 174762 - 104857560!
Error frame period threshold is out of range, its range is 0 - 268435455!
Error frame window is out of range, its range is 10 - 600!
Error frame threshold is out of range, its range is 0 - 268435455!
Error frame seconds summary window is out of range, its range is 100 - 9000!
Error frame seconds summary threshold is out of range, its range is 0 - 268435455!

A parameter entered in the "Event Configuration" has exceeded the range limitation.

1. Enter a parameter within the valid range displayed. See “LOAM Event Configuration Default Values and Valid Ranges” on page 130.
2. If the problem persists, contact Technical Support.

No data in VLAN forward database table now!
You entered the command to display FWDDB information, but the VLAN forward database table has no data to report. For example:

```
C1|S16|L1D>show fwddb config fdbid 1
No data in VLAN forward database table now!
```

1. Make sure this is the function that you want.
2. Use the Forwarding Database Commands on page 92 to create the VLAN FDB entry.
3. If the problem persists, contact Technical Support.

set forward database connection port failed.
set forward database priority failed.
set forward database entry type failed.
Please input a number to specify the priority!
The range of priority is 0 .. 7!

You tried to create a new FWDDB entry but the effort failed. For example:

```
C1|S16|L1D>add fwddb mac 00:c0:f2:21:02:b3 conn-port=1 priority=7 type=static
set forward database connection port failed.
C1|S16|L1D>
```

1. Make sure this is the function that you want.
2. Use the Forwarding Database Commands on page 92 to create the VLAN FDB entry.
3. If the problem persists, contact Technical Support.

The specified conn-port does not exist!

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

1. Make sure this is the function that you want.
2. See "Configuring MAC Address Filtering" on page 234 for more information.
3. If the problem persists, contact Technical Support.

The specified monitor-port does not exist!
You specified a monitoring port (monitor-port) number outside the valid range.

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

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

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

Auto-negotiation is enabled, you can not set port duplex now!
You entered the command to assign a duplex mode, but the command is not functional if Auto-negotiation is currently enabled.

1. Either leave the Auto-negotiation setting and use the current duplex setting, or disable AutoNegotiation and set the Duplex mode as required.
2. See the "Set Ethernet Port Speed / Duplex Mode" section on page 105 for more information.
3. Use the **show ether config** command to display the current Auto-negotiation and Duplex settings.

4. If the problem persists, contact Technical Support.

Parameter value is out of range.

One or more of the entered CLI command parameters was not within the valid range.

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 display.
2. Retry the command. For a complete description of each available command, see the *ION System CLI Reference Manual,* 33461.
3. If the problem persists, contact Technical Support.

Fail to set errored frame period window!
Fail to set errored symbol period window low!

You entered an EFP Window parameter or ESP Window parameter that was outside the valid range. For example, you entered:

```
C0|S0|L1P2>set loam efp window 300
Fail to set errored frame period window!
C0|S0|L1P2>
```

1. Verify the valid range. See "LOAM Event Configuration Default Values and Valid Ranges" on page 133.
2. Re-enter the command.
3. Use the **show loam event config** command to verify the setting.
4. If the problem persists, contact Technical Support.

AIS transmit setting is not supported on this card!

You entered a command to enable or configure AIS, but the device does not support the AIS function. For example:

```
C1|S3|L1D>set ais transmit=enable
AIS transmit setting is not supported on this card!
C1|S3|L1D>
```

1. Verify that this is the command you want.
2. Either select another device that supports AIS, or enter another command that this device supports.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Disable transmitting the TN topology discovery protocol on this port would make the device not be discovered by the Management unit if the device is remotely managed through this port. Are you sure?
Error: this command should be executed on a port!

Fail to get TNDP Tx state!
Fail to set TNDP Tx state of this port!
TNDP is not supported on this card!

1. Warning message that the **set tndp=disable** command disables management of the device from the IONMM.
2. The **set tndp=disable** command is a port level command; use the go command to switch to a port and re-enter this command.
3. Check the syntax and re-enter the command. Refer to the “TNDP Commands” on page 197.
5. If the problem persists, contact Technical Support.

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

You entered a command for a function that is not supported on the x32xx. For example:

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

1. Try another command on the x32xx.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support.

Speed and duplex capability advertised by local auto-negotiation entity
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

You entered a command to set the rate for a port that does not support this rate command.

1. Verify that this is the command you want.
2. Either select another device that supports this rate command, or enter another command that this port supports.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Pause capability advertised by local auto-negotiation entity
If no pause capability, setting nopause; otherwise, for copper port , use a combination of pause and apause, like pause+apause or pause or apause; for fiber port, use a combination of apause and spause, like apause+spause or spause or apause

You entered a command to set the Pause function that did not match the port or device's capability.

1. Verify that this is the command you want.
2. Either select another device that supports this rate command, or enter another command that this port supports.
3. Retry the operation. Refer to the "Pause Commands" on page 187.
4. If the problem persists, contact Technical Support.

please use \"show timezone\" to see detailed value of each timezone

You entered a command to set or show the UTC time data.

1. Verify that this is the command you want.
2. Enter the show timezone command.
3. Refer to the "SNTP Commands" on page 197.

The value of current time should time should follow this format, \"YYYY MMDD HH:MM:SS\", such as \"1999 1211 13:22:34
Please reboot the card for the changes to take effect!
You entered a **set sntp** command to set the UTC time data, and a reboot is required to implement the change.

1. If this is the command you want, start the reboot process.
2. Continue the operation.
3. Refer to the "SNTP Commands" on page 197.

Redundancy is enabled, so cannot set the administration state of fiber ports!

You entered a command to set the USB port state (**set usb-port state**=disable|enable) but that command does not work when the Redundancy feature is enabled.

1. Use the **go** command to switch to a different port.
2. Use the ION Web interface to disable the USB port.
3. Disable the Redundancy feature and then re-enter the **set usb-port state** command.
4. If the problem persists, contact Technical Support.

Cannot proceed because some other TFTP operation is currently in progress!
Please input config file name!
TFTP file transferring failed! Please make sure the TFTP server is up and the file being transferred does exist.
TFTP Server Address is empty or invalid!
The firmware has been successfully upgraded and the system will be rebooted soon
The specified firmware on the TFTP server will be upgraded to the current module, operation is currently in progress!
The sys.log file will be transferred to the TFTP server, are you sure to proceed?

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

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

Cannot get port VLAN configuration on this card!
Cannot get VLAN tag management configuration on this port!
Cannot set discard tagged frame on this card!

You entered a VLAN command on a device or port that does not support this function.

1. Try another command on the x222x / x32xx.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support.

Disable transmitting the TN topology discovery protocol on this port would make the device not be discovered by the Management unit if the device is remotely managed through this port. Are you sure?
Error: this command should be executed on a port!
Fail to get TNDP Tx state!
Fail to set TNDP Tx state of this port!
TNDP is not supported on this card!

You tried to enter the **set tndp** command but either the function is not supported or you entered it at the device level or you are being asked to verify the command entry.

1. Verify that this is the function you want.
2. Use the **go** command to switch to a port.
3. Use the ION Web interface to perform the function.
4. Use the **go** command to switch to a device that supports this function.
5. Refer to the "TNDP Disable/Enable" section on page 416.
6. If the problem persists, contact Technical Support.

No loopback supported on this card!
Error: this command should be executed on a port!
No TDM loopback supported on this card!
Fail to set Ethernet port loopback operation, please check if Link OAM admin state of remote peer port is enabled, link status and other issues.
Fail to get loopback type!

You tried to enter the **set tdm** command but either the function is not supported or you entered it at the device level or you are being asked to verify the command entry.

1. Verify that this is the function you want.
2. Use the **go** command to switch to a port.
3. Use the ION Web interface to perform the function.
4. Use the **go** command to switch to a device that supports this function.
5. Verify that the Link OAM admin state of the remote peer port is enabled, the link status is Up, and other prerequisites are met. Refer to the "Configuring TDM Loopback" section on page 418.
6. If the problem persists, contact Technical Support.

Fail to set port MAC learning!
You entered a CLI command to set the MAC Address Learning port(s) to enabled or disabled, but the entry failed.
1. Make sure this is the command / function that you want.
2. Verify the MAC Address Learning port setting(s).
3. Refer to the "Configuring MAC Address Learning" section on page 325 for more information.
4. Retry the operation.
5. If the problem persists, contact Technical Support.

Invalid forward port list!
You entered a CLI command to set the MAC Address Learning port(s) to enabled or disabled, but the entry was not accepted. For example:

```
C1|S3|L1D>set mac_learning enable portlist 1,2,3
Invalid forward port list!
```

1. Make sure this is the command / function that you want.
2. Verify the port number(s) that you entered are valid for this particular x222x / x32xx device (i.e., you cannot enter the command in the example above (**set mac_learning enable portlist 1,2,3**) on a 2-port device such as the x323x.
3. Refer to the "Configuring MAC Address Learning" section on page 325 for more information.
4. Retry the operation.
5. If the problem persists, contact Technical Support.

Message: *Are you sure to (flushOp) ?*
Cannot flush fwddb on this card!
Cannot flush vlandb on this card!
Flush is being processed...
Send flush command successfully
Fail to flush all entries to chip.

Meaning: You entered a command to clear all of the FWDDB or VLAN DB entries, but the function is either not supported or is already in process or successfully completed.

Recovery:

1. Wait for a few moments for the operation to complete.
2. Make sure this is the command you want.
3. Make sure this card supports the Flush function attempted.
4. Verify the Flush command parameters and re-enter the Flush command.
5. If the problem persists, contact Technical Support.

The two passwords do not match!

You tried to generate a private key, but the operation failed. For example:

```
C1|S3|L1D>set https private-key password
Please input password:
xxxxxx
Please input password again:
yyyyyyy
The two passwords do not match!
C1|S3|L1D>
```

1. Verify that this is the operation you want.
2. Retry the operation; be sure to type the password the same both times.
3. If the problem persists, contact Technical Support.

VID already exist!

You tried to add a VLAN-DB, but the operation failed. For example:

```
C1|S3|L1D>add vlan-db vid=20 priority=3 pri-override=enable
VID already exist!
C1|S3|L1D>
```

1. Verify that this is the operation you want.
2. Retry the operation; be sure to type a unique VLAN-DB VID.
3. If the problem persists, contact Technical Support.

Sys.log file lost on reboot

The device will dump all syslog files from RAM to flash on re-boot or if a system crash occurs.
The last (most recent) syslog is stored as last_sys.log which can be retrieved using the tftp command.
The filename sys.log is the current syslog file. The filename last_sys.log is the old syslog file.

At one time we can only backup at most 10 cards!
At one time we can only restore at most 10 cards!
Backup finished
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Fail to set card entity index!
Processing...
The MAX provision configure file name is 64!
The specified module does not exist!

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

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

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 on page 103.

3. If the problem persists, contact Technical Support.

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

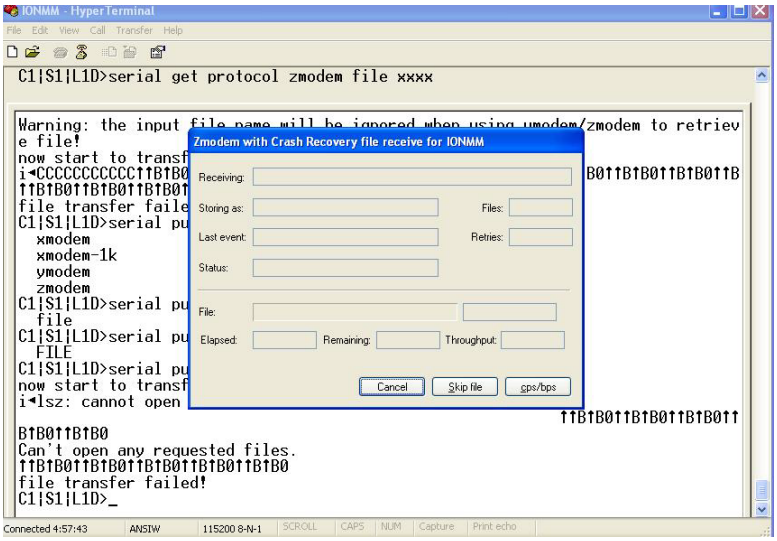
You entered a Serial File Transfer command, but the operation failed.

1. Verify that this is the operation you want.

2. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section on page 103.

3. If the problem persists, contact Technical Support.

File Transfer Failed - ZModem Crash Recovery dialog box:



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

1. Either enter the requested information and click **cps/bps**, or click **Skip file**, or click **Cancel**.

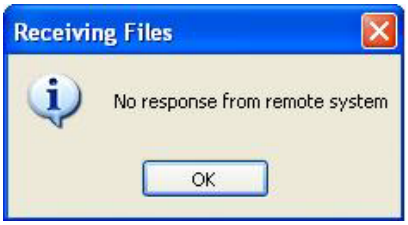
2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.

3. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section on page 103.

4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.

5. If the problem persists, contact Technical Support.

Receiving Files - No response from remote system



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

1. Click the **OK** button to clear the message dialog box.

2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.

3. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section on page 103.

4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.

5. If the problem persists, contact Technical Support.

Cannot find software version of this card!

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

1. Check the card's current firmware version.
2. Upgrade the card firmware if not latest version. See "Upgrade the IONMM and/or NID Firmware" on page 261.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

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

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

1. Upgrade the card firmware. See "Upgrade the IONMM and/or NID Firmware" on page 261.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

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

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

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

Web Interface Messages

IMPORTANT

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

Cannot Ping IONMM Device

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

Cannot Ping IONMM Device

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

Getting values failed (snmp operation timeout)

This message indicates that you entered an invalid parameter value.

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

Failed to start Virtual Cable Test.

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

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

Firmware DB operation failed, unzip failed.

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

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

invalid input file

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

1. Verify the parameter value entered; see "Upgrading IONMM Firmware – Web Method" on page 250 for valid input information.
2. Retry the operation with a valid firmware file name (e.g., *IONMM.bin.0.5.4*, or *x222x / x32xx.bin.0.5.4*).
3. If the problem persists, contact Technical Support.

Invalid input found!

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

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

Invalid password!

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

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

   Note: the password is case sensitive.
2. If the problem persists, contact Technical Support.

Failed to retrieve DMI info on current port.

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

1. Verify that the NID and SFP support DMI.
2. See "DMI (Diagnostic Maintenance Interface) Parameters" on page 248 for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

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

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

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

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

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

This is the current operational state of the interface.

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

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

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

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

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

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

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

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see "Section 2: Installation and System Setup" on page 40.
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization and discovery to take place.
5. If the problem persists, contact Technical Support.

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

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

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

1. Verify the ION system installation; see "Section 2: Installation and System Setup" on page 40.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

Link Status: *Testing*: The ION system interface 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.

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

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

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See "Configuring HTTPS" on page 208.
3. If the problem persists, contact Technical Support.

Message: *Setting values failed (snmp operation error)*

This message indicates that the SNMP Configuration entered had an invalid SNMP entry (e.g., an unrecognized Trap Manager address entry).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See "Configuring SNMP" on page 226.
3. If the problem persists, contact Technical Support.

Message: *TFTP file transferring failed!*

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

TFTP for Backup download operation:

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

TFTP for Restore upload operation:

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

Message: *TFTP operation failed!*

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

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

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

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

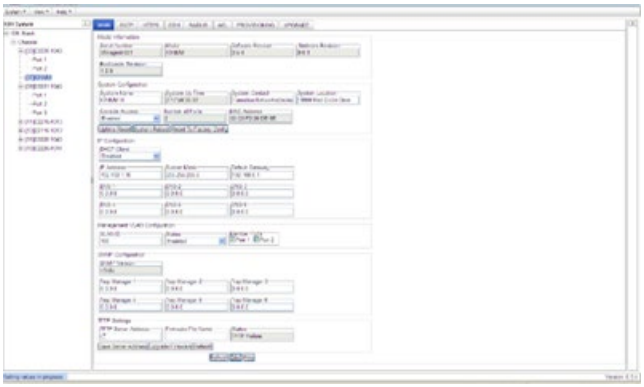
1. Click the Continue to this website... selection.
2. See the "Configuring HTTPS" section on page 192.

Message: *Web UI Management connection Lost*

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

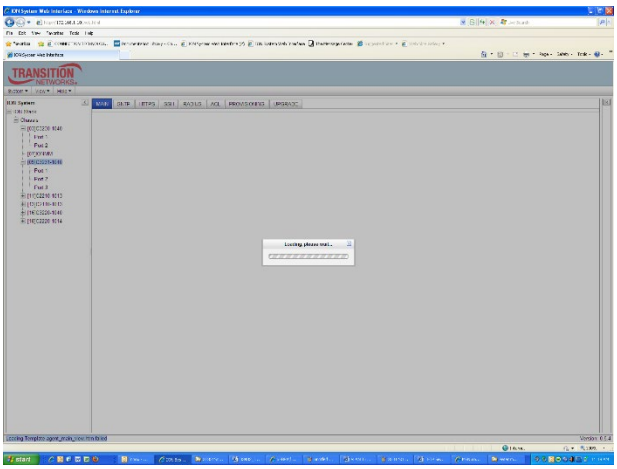
Message: "*Setting values in progress ...*" displays continuously

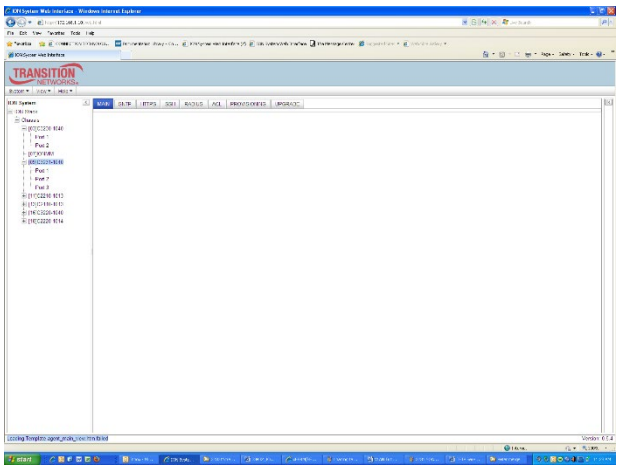
The message "Setting values in progress ..." displays for over 10 minutes after you set up a VLAN 100, then set Management VLAN to Enabled and clicked Save.



Getting values failed (http server error) then displays.

Loading Template agent_main_view.htm failed displays:





MAIN tab displayed is blank after you close the **Loading ...** dialog box.

Meaning: These messages display after you turn on the Management VLAN function either via the ION Web interface or the CLI. (The CLI command is **set mgmt vlan state=enable**, and the Web interface is from the IONMM **MAIN** screen in the **Management VLAN Configuration** section, where the **Status** field is set to **Enabled**. In both cases, management control is given to the Management VLAN that you enabled.

The recovery (re-gaining control from the CLI or Web interface) is to turn off Management VLAN via the CLI (**set mgmt vlan state=enable**) or via the Web interface (IONMM **MAIN** > **Management VLAN Configuration** > **Status** > **Enabled**).

Message: *Loading Template agent_main_view.htm failed*
Loading htm files failed
Loading htm file succeeded
Loading JavaScript file failed
Loading Template Config file failed

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

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

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

Meaning: Not all 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.”

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” on page 248 for more information.

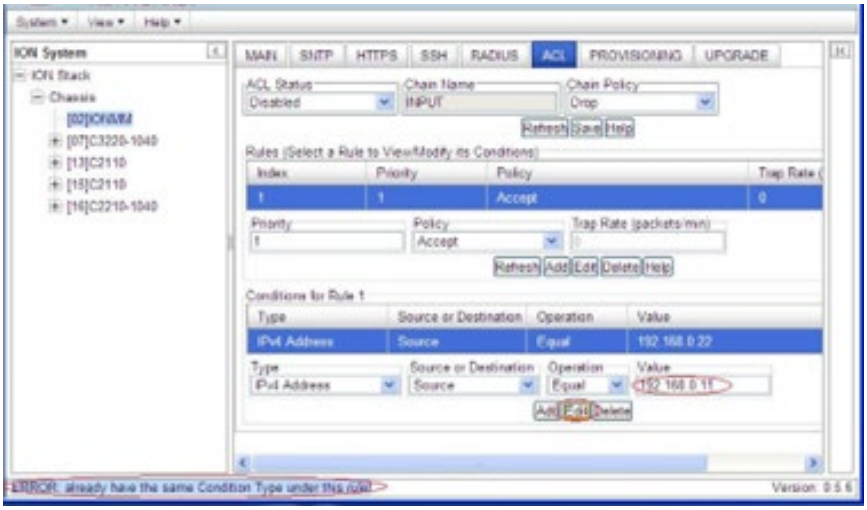
Message: *priority is empty or invalid*

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” on page 201.

2. If the problem persists, contact Technical Support.

Message: *Error - already have the same Condition Type under this rule*



Meaning: At **IONMM** > **ACL** tab, when you try to edit or add a Condition to an IP address, the error message displays.

Recovery: 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.

Message: *Loading Template agent_main_view.htm failed*

Message: *Loading htm files failed*

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

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

Message: *xxxxxxx is out of range, its range is yyyyyy*
Error symbol period window low is out of range, its range is 125000000 - 268435455!
Error frame period window is out of range, its range is 174762 - 104857560!
Error frame period threshold is out of range, its range is 0 - 268435455!
Error frame window is out of range, its range is 10 - 600!
Error frame threshold is out of range, its range is 0 - 268435455!
Error frame seconds summary window is out of range, its range is 100 - 9000!
Error frame seconds summary threshold is out of range, its range is 0 - 268435455!
Meaning: A parameter entered in the "Event Configuration" has exceeded the range limitation.
Recovery: Enter a parameter within the valid range displayed for the parameter.

Message: *Getting Records failed (snmp operation timeout)*
Message: *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 (e.g., "Upgrade" section on page 321 or page 327, or "Backup and Restore Operations (Provisioning)" on page 324.

3. Reboot the NID. See "Reboot" on page 317.

4. If the problem persists, contact Technical Support.

Message: *System initializing or SNMP service busy, please wait...*

Meaning: The system password was accepted, but the system did not proceed completely.

Recovery: Sign in using the correct password. The default password is private. Note that the password is case sensitive.

1. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. Verify the SNMP configuration.
4. If the problem persists, contact Technical Support.

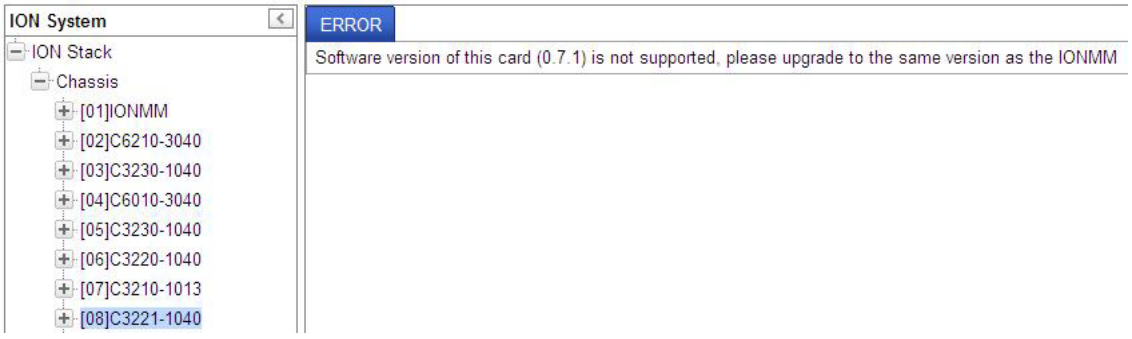
Message: *Online Help is not available until a specific configuration is entered.*

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

Recovery:

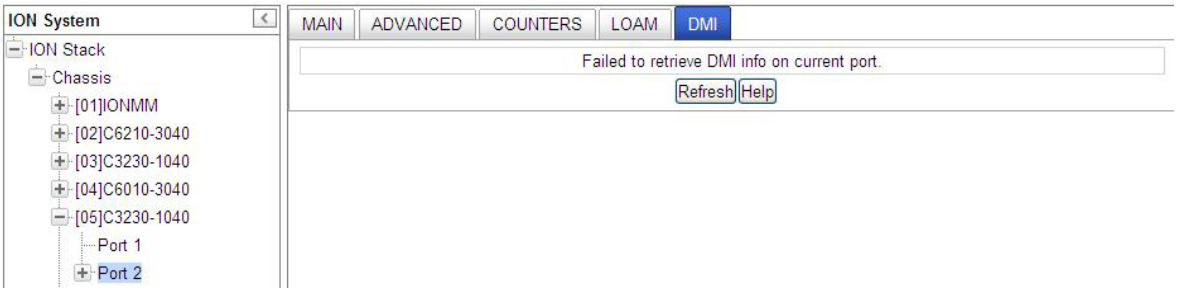
1. Click the **OK** button to close the webpage message.
2. Select an ION device.
3. Click on **Help** > **Online Help** again.

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



Meaning: You selected a device in the tree, but its firmware version is not compatible with the IONMM. **Recovery**: 1) Select the IONMM device. 2) Select the UPGRADE tab. 3) Perform a firmware upgrade to this card (and others that may have outdated firmware). See the Upgrade section on page 347. 4) If a problem persists, contact Technical Support.

Message: *Failed to retrieve DMI info on current port*

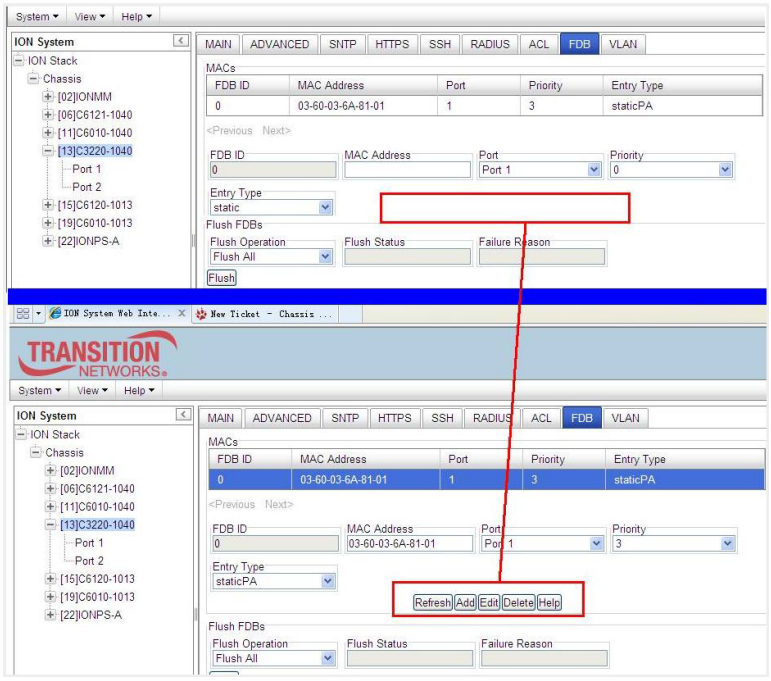


Meaning: You selected **C3230** > **Port 2** > **DMI** but the DMI information does not display.
Recovery: 1) Click **Refresh**. 2) Expand and contract the tree. 3) If a problem persists, contact Technical Support.

Message: *Current power status of this slot is off, please turn it on before you reset it!*
Meaning: The reset function only works when the slot power is in the On position for the unit to re-boot/reset.
Recovery: 1) At **Chassis** > **MAIN** > **Chassis Members** click the "**On**" button in the **Power Status** column of the device before you click the "**Reset**" button. 2) If a problem persists, contact Technical Support.

Problem: Setting the VLANID failed with an SNMP operation error message:
Message: Setting values failed (snmp operation error) or
Adding VLAN failed (snmp operation error)
Meaning: You tried to add or edit a VLAN ID but the effort failed.
Recovery: The card must be in “Network” mode (at Port 1 > Advanced > Frame Tag Mode) to set the VLAN ID. If it is not set to "Network", an SNMP error will occur. Before adding the ports for Management VLAN, set the Frame Tag Mode of that port to "Network". When Provider tagging is required for that port, then set the Frame Tag Mode to "Provider". A port with the Frame Tag Mode set to the default setting "Customer" can not be added to Member Ports for Management VLAN.

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



This is an IE8 bug which can only be fixed by Microsoft. MS IE8 has an issue with the <fieldset> tag, which is a well known bug for which web developers are awaiting a patch.

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

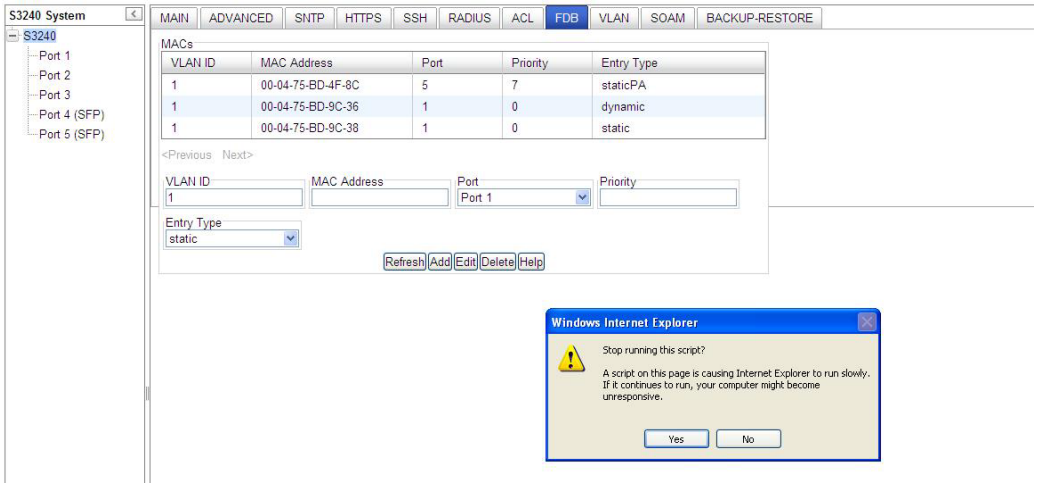
Websites that were designed for earlier versions of Internet Explorer might not display correctly in the current version. However, you can often improve how a website will look in Internet Explorer by using the new 'Compatibility View' feature. When you turn on Compatibility View, the webpage displayed (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 on page 266.
5. Check the Microsoft Support Online website http://support.microsoft.com/ph/807/en-us/#tab0 for more information.
6. See also: http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx
http://support.microsoft.com/kb/960321
http://blogs.msdn.com/b/ie/archive/2008/08/27/introducing-compatibility-view.aspx
7. In IE9, click the **Compatibility View** toolbar button on the Address bar to display the website as if you were using an earlier version of Internet Explorer. See the Microsoft Support website Article ID: 956197 at http://support.microsoft.com/kb/956197.

Script error message received.
Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No
Error: Object doesn't support this property or method.
A Runtime Error has occured. Do you wish to Debug?
Done, but with errors on page.



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

Problem: OAM loopback can be enabled and is working on the fiber ports, but not on the copper ports.
Meaning: The documented loopback procedure does not work on copper ports.
Recovery:
1. You must first enable OAM on the fiber ports to be able to establish OAM on the copper side.
The OAM PDU's can only be received from copper ports if the fiber ports are also OAM enabled. The fiber port is the network connection between the two devices, and this is the path that the copper ports send their OAM PDU's between remote peer devices.
2. Follow the procedure in the section "Copper Port Loopback Procedure" on page 144.
3. To determine if the loopback was successful, the LOAM counters show "loopback sent" and "loopback received".

SNMP Messages

For any error condition, you can check the Tech Support web site for possible solutions. For any problem that persists, contact Tech Support in the US or Canada at 1-800-260-1312, International at + 1 952-358-3601; via fax at +1 952-941-2322; or via Email at techsupport@transition.com.

Basic Recovery Steps

You entered a command, but the operation failed or is still in process.
1. Wait for a few moments for the operation to complete.
2. Use the **Help** or **?** command to get assistance (help) on a group of commands or on a specific command.
3. Make sure this is the command you want and that the device/port/configuration supports this command.
4. Make sure this device/port supports the function attempted. Use the **go** command to switch locations.
5. Verify the command syntax and re-enter the command. See the related section of the manual for specifics.
6. Try using the Web interface to perform the function.
7. If the "continue **y**(es) **n**(o)" prompt displays, type **y** and press **Enter** to continue.
8. If the problem persists, contact Tech Support.

Message:
Bad engine ID value after -3E flag.\n
Bad key value after -3m flag.\n
bad mask
bad mask length
bad source address
cannot resolve source hostname
Can't set up engineID of type text from an empty string.\n
community name too long
could not generate localized authentication key (Kul) from the master key (Ku).
could not generate localized privacy key (Kul) from the master key (Ku).
could not generate the authentication key from the supplied pass phrase.
could not generate the privacy key from the supplied pass phrase.
Could not get proper authentication protocol key length
could not get proper key length to use for the privacy algorithm.
example config COMMUNITY not properly configured
example config NETWORK not properly configured
Meaning: You entered an SNMP v3 command, but the command failed due to an invalid or misinterpreted entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
improper key length to -l
Invalid authentication protocol specified after -3a flag: %s\n
invalid EngineID argument to -e
invalid key value argument to -l
invalid key value argument to -m
Invalid privacy protocol specified after -3x flag: %s\n
Invalid security level specified after -3l flag: %s\n
Meaning: You entered an SNMP v3 command, but the command failed due to an invalid or improper parameter entry.
Recovery: 1) Make sure this is the command you want. Use the Help **(?)** command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
malloc failure processing -3e flag.\n
malloc failure processing -e flag
Missing argument after SNMPv3 '-3%c' option.\n
missing COMMUNITY parameter\n
missing CONTEXT_NAME parameter
missing NAME parameter
missing SOURCE parameter
Need engine boots value after -3Z flag.\n
Need engine time after \"-3Z engineBoot,\".\n
no authentication pass phrase
no IP address for source hostname
security name too long
Unknown authentication protocol
Unknown authentication type
Unknown EngineID type requested for setup (%d). Using IPv4.\n
Unknown privacy protocol
Unknown privacy type
Unknown SNMPv3 option passed to -3: %c.\n
Unknown version specification
Unsupported enginedIDType, forcing IPv4
Meaning: You entered an SNMP v3 command, but the command failed due to an unrecognized entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
Are you sure to delete all the views with the name xx? (confirm)
Are you sure to delete this view ? (confirm)
Adding Community String failed!
Adding group failed!
Adding View failed!
Add Security group failed!
Add user failed!
bad security model, should be: v1, v2c or usm or a registered security plugin name
bad security level (noauthnopriv, authnopriv, authpriv)
bad prefix match parameter \"0\", should be: exact or prefix - installing anyway
bad prefix match parameter, should be: exact or prefix
Delete community string failed!
Delete user failed!
Delete vacm security group failed!
Delete view failed!
Edit view failed!
Failed to change group!
failed to create group entry
Illegal configuration line: missing fields
Illegal view name
Meaning: You entered an SNMP v3 command, but the command failed due to an unrecognized entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
missing GROUP parameter
missing SECURITY parameter
missing NAME parameter
missing CONTEXT parameter
missing MODEL parameter
missing LEVEL parameter
missing PREFIX parameter
Nothing changed!
Meaning: You entered an SNMP v3 command, but the command failed due to a missing parameter entry.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message:
Adding Remote Engine ID failed!
Add remote user failed!
Adding Target Address failed!
Delete Remote Engine ID failed!
Delete remote user failed!
** Delete remote user successfully! Trying to delete group... (status message only - displays momentarily)*
ERRPR: There is already a same host with the input IP and Port!
ERROR: There is already a same named community string!
~~*ERROR: There is already a 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.

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.

Message:
ERROR: Remote engine ID could not be the same as local engine ID!
ERROR: There is already a same remote engine ID!
ERROR: There is already a same remote engine ID with the input ip and port!
Meaning: You entered an SNMP v3 command, but the command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
Reseting local Engine ID will delete all exist local users, continue?(y: yes, n: no)
Meaning: You entered an SNMP v3 command, but a confirmation message displayed.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Enter **n** if you are not sure you want to reset the local Engine ID, or enter y to continue to reset the local Engine ID and delete all existing local users.

Message:
ERROR: Adding sub oid tree to defaultView is prohibited!
ERROR: defaultView can not be deleted!
ERROR: Modifying defaultView is prohibited!
ERROR: Please do not modify the View Name or the OID Sub Tree!
ERROR: Sub oid tree in defaultView can not be deleted!
ERROR: This group can not be deleted!
Meaning: You entered an SNMP v3 command, but the add/delete/modify command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
EngineID length must be in range [9..64]!
Invalid engineID!
Password is too long!
The password name length must be in range [1..64]!
The authentication password length must be in range [8..64]!
The privacy password length must be in range [8..64]!
Meaning: You entered an SNMP v3 command, but the command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
Cannot add SNMP view on this card!
Cannot show SNMP view on this card!
Cannot show SNMP trap hosts on this card!
Fail to get SNMP target address!
Fail to get SNMP view!
No SNMP view created now!
No SNMP trap host is created now!
Trap version is out of range!
Meaning: You entered a "**show snmp traphost**" or "**show all SNMP trap hosts**" or "**show snmp view**" command that failed to complete.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
Cannot add SNMP trap hosts on this card!
Fail to create notif table!
Fail to create parameter entry!
Fail to create trap host!"
Fail to set domain!
Fail to set traphost address!
Fail to set traphost parameters!
Fail to set traphost tag list!
Fail to security model! <set?>
Fail to security message process model! <set?>
Fail to security name! <set?>
Fail to security level! <set?>
Fail to set notif tag!
Fail to set notif type!
Invalid address!
SNMP community/security name length should be shorter than 32!
We can create at most 6 trap hosts!
Meaning: You entered a "**add snmp traphost**" command that failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
Fail to get SNMP target address!
The specified trap host does not exist!
Meaning: You entered a "**remove snmp traphost**" command that failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
Cannot show SNMP trap hosts on this card!
Fail to get SNMP target address!
Cannot remove SNMP community on this card!
SNMP community name length should be shorter than 32!
Fail to get SNMP target address!
The specified community has existed!
Cannot find the specified community!
Fail to get remote engine!
Fail to get user_to_group entry!
Fail to remove snmp user!
Fail to remove snmp view!
Fail to remove snmp group!
Fail to remove snmp user-group mapping!
Fail to remove snmp community!
Fail to remove snmp traphost!
Meaning: You entered an SNMP community command (get/set/show/add/remove), but the command failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
When security level is v1 or v2c, security model can only be noAuthNoPriv
Fail to get community name! (*the device will search all rows of the SNMP Community Table, and if the community name can not be found, will add it*)
Fail to create community!
Meaning: You entered an SNMP Traphost or SNMP Trap Manager CLI command, but the command failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact Tech Support.

Message:
Cannot add SNMP trap hosts on this card!
The specified trap host has existed!
Meaning: You tried to enter an "**add snmp community name**" command, but the command failed to complete.
Recovery:
1) Verify the "**access mode**" and "**community name**" parameter syntax. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If required, at the command prompt, enter the ION login and Password information. 5) If the problem persists, contact Tech Support.

Message:
Fail to get SNMP view!
Cannot show SNMP view on this card!
No such SNMP view name!
No SNMP view created now!
Meaning: You entered a "**show snmp view**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP Group Name of 8-32 characters. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If required, at the command prompt, enter the ION login and Password information. 5) If the problem persists, contact Tech Support.

Message:
authentication protocol is invalid!
Fail to create SNMPv3 usmuser!
Fail to get response from snmpd!
Fail to get response from snmpd!
Fail to send message to snmpd!
Fail to set group of the user!
Privacy protocol is invalid!
Meaning: You entered a "**add snmp local user**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP user. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message: *SNMP group name length should be shorter than 32!*
Meaning: You entered a "**set snmp local user name**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP group name of 8-32 characters. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
Fail to create SNMPv3 usmuser!
Remote engine address is not valid!
Meaning: You entered a "**add snmp remote user**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP user name and engine ID. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
Fail to analyse remote engine address!
Fail to create SNMPv3 usmuser!
Meaning: You entered a "**add snmp remote user name**" command but the operation failed.
Recovery:

Message: *Cannot show SNMP remote engine on this card!*
Meaning: You entered a "**show snmp remote engine**" command but the operation failed.
Recovery: 1) Verify that you entered a unique SNMP remote engine ID. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
Fail to get SNMP remote engine!
Please input a digital number to specify trap rate!
The specified remote engine has existed!
Meaning: (e.g., you entered an "**add snmp remote engine**" command but the operation failed.
Recovery: 1) Verify that you want this operation performed. If you are not sure, enter **n** and press **Enter**. 2) To continue, type **y** and press **Enter**. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message: *If you remove this remote engine, all remote users related to this engine will also be removed, continue?(y: yes, n: no)*
Meaning: You entered a "**remove snmp remote engine**" command but the confirmation message displayed.
Recovery: 1) Verify that you want this operation performed. If you are not sure, type **n** and press **Enter**. 2) To continue, type **y** and press **Enter**. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message: *Notification type can only be trap or inform!*
Meaning: You entered a "**get prov tftp svr**" or "**set prov tftp svr**" command but the operation failed.
Recovery: 1) Re-enter the command with "Trap" or "Inform" as the parameter. 2) Make sure the SNMP user's security model is v3. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact Tech Support.

Message: *ERROR: There is already a remote user with the same name, ip and port!*
Meaning: You entered a duplicate record using the "add snmp rmt user" command.
Recovery: 1) Re-enter the command with a unique user name, IP address, and Port number. 2) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 3) Try using the ION Web interface to perform the function. 4) If the problem persists, contact Tech Support.

Message:
SNMP user name length should be shorter than 32!
This user already exists!
Meaning: The user already exists or you entered too many characters (32 characters maximum) for the SNMP User Name.
(The SNMP user's security model can only be v3.)
Recovery: 1) Re-enter the command with a unique user name, IP address, and Port number. 2) Make sure the user name entered has less than 32 characters in it. 3) Make sure the SNMP user's security model is **v3**. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact Tech Support.

Message:
ERROR Software version of this card ("cardVersion") is not supported, please upgrade to the same version as the IONMM
Getting card version failed
The failure get template config handler was called.
Meaning: You attempted a function that is not supported by this version of firmware.
Recovery: 1) Enter another (supported) function at this card's firmware version, or use the "go" command to switch to another card. 2) Upgrade to a newer firmware version. See "TFTP Transfer / Upgrade Commands" on page 204 or "Upgrade / Update Firmware Commands" on page 207. 3) Retry the operation. 4) If the problem persists, contact Technical Support.

Message:
The confirm password is not identical with the password!
The user name length must be in range [1..64]!
The user name must begin with an alphanumeric char!
You can only change your own password, not others!
Meaning: You entered a command to create a new system user, but the command failed.
Recovery: 1) Verify the command syntax ("**add sysuser name**=NAMESTR **level**=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR"). 2) Retry the operation, making sure the "pass" and "confirmpass" entries match. See the related command section.
3) If the problem persists, contact Technical Support.

Message: *Invalid input of timout value!*
Meaning: You set an unsupported SNMP trap timeout boundary value.
Recovery: 1) In the "**add snmp traphost**" command, specify a valid timeout (-15s%-16s%-5u%-30s%-16s%-12s%-12u%-12u%s (change from 8u to 12us). For example:

```
C1|S1|L1D>add snmp traphost version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6
security_level authPriv notify trap timeout=<0-2147483647>]
C1|S1|L1D>add snmp traphost version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6
security_level authPriv notify trap timeout 1000 retry 25
```

Problem: An SNMP user cannot access the IONMM.
Meaning: The User security level is not compatible with the Group level. For example, you added an SNMPv3 User to a SNMP v1 Group, or added a User to a non-existing Group, so this user can not access the IONMM.
Recovery: 1) Make sure the Group exists. Verify the User's security level. See the "Configure SNMP" section for specific details.

Problem: Can't assign a SNMPv3 User to multiple Groups.
Meaning: The SNMPv3 standards do not allow you to assign a SNMPv3 user to multiple groups.
Recovery: 1) Create an additional, unique user. 2) Assign the new user to a different group. 3) Make sure that each user belongs to just one group.

Problem: Can't configure SNMPv3 for chassis ION NIDs.
Meaning: The SNMPv3 features currently only apply to the IONMM and standalone S323x/S322x/S222x devices.
Recovery: 1) Contact U.S. Headquarters at 10900 Red Circle Drive, Minnetonka, MN 55343 USA; Telephone: 952-941-7600; Toll Free: 800-526-9267; Fax: 952-941-2322. EMEA Headquarters: Telephone: +49 611 974 8460; Fax: +49 611 950 4672. Email sales@transition.com.

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.

Message: *Invalid group parameter for user!*
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: *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:

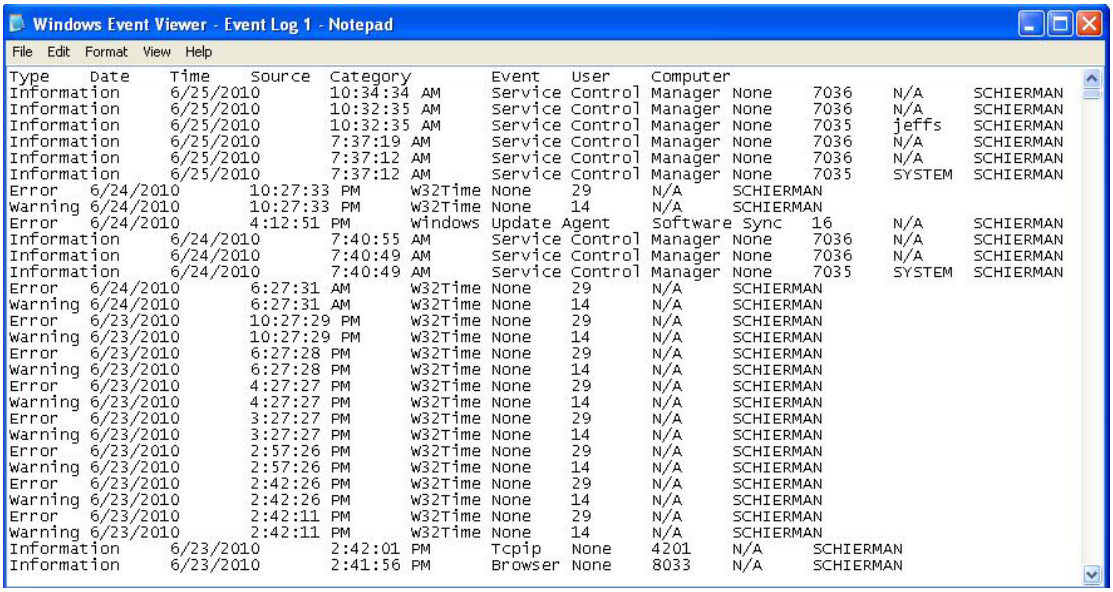
```
S3230-1040 C0|S0|L1D>show snmp group name
Name         Security Model      Security Level    Read View   Write View   Notify View
------------------------------------------------------------------------------------
login: ION
Password:
```

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" on page 27. Retry the operation.

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:



Windows Event Viewer - Event Log 1 - Notepad

File Edit Format View Help

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

Message: `Information 6/25/2010 7:37:12 AM Service Control Manager None 7035 SYSTEM`

Meaning: Information message regarding SCM.

Recovery: No action required.

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

Meaning: Error level message regarding W32Time.

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

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

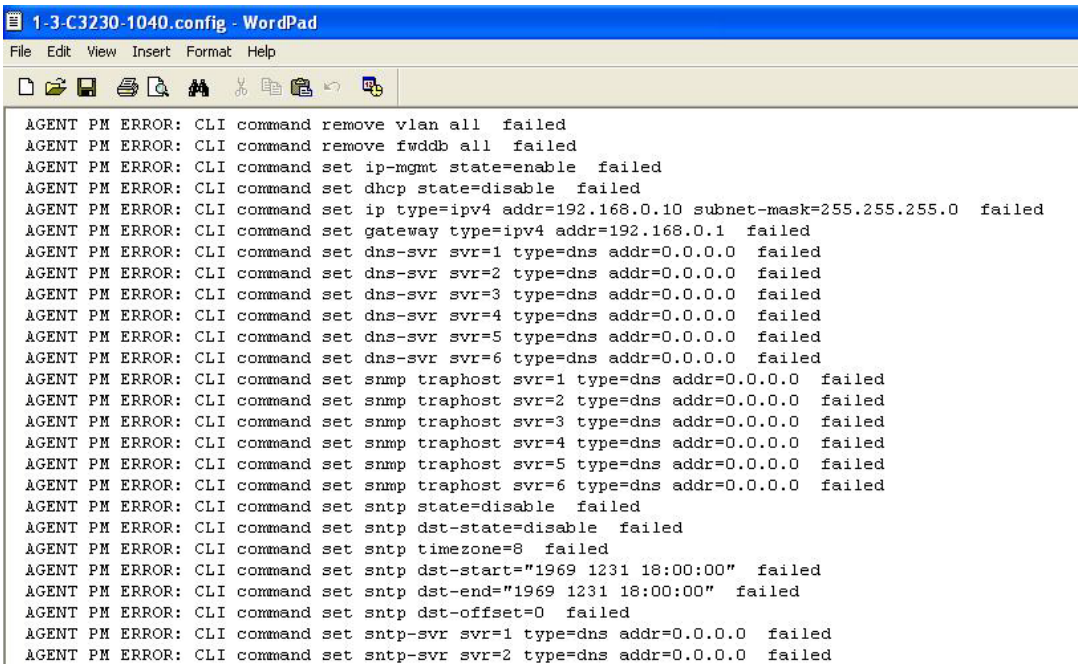
Meaning: Warning level message regarding W32Time.

Recovery: Check the other system logs for related messages. If the problem persists, contact Technical Support.

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.



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, 33473*. 4. If the problem persists, contact Technical Support.

Message: `remove fwddb all failed`

Response: 1. Check if this is a recurring problem. 2. Verify the Forwarding Database (FWDB) operation in the related section of this manual. Retry the FWDB operation. 3. See the related FWDB command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set dhcp state=disable failed`

Response: 1. Check if this is a recurring problem. 2. Verify the DHCP operation in the related section of this manual. Retry the DHCP operation. 3. See the related DHCP command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed`

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set gateway type=ipv4 addr=192.168.0.1  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the DNS Server operation in the related section of this manual. Retry the operation. 3. See the related DNS server command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set sntp state=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set sntp dst-state=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set sntp timezone=8  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set sntp dst-start="1969 1231 18:00:00"  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set sntp dst-end="1969 1231 18:00:00"  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set sntp dst-offset=0  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set radius client state=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the RADIUS operation in the related section of this manual. Retry the RADIUS operation. 3. See the related RADIUS command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set radius svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30  failed`

Response: 1. Check the RADIUS server setup, configuration and documentation. 2. Verify the RADIUS operation in the related section of this manual. Retry the RADIUS operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `add vlan-db vid=100 priority=0 pri-override=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set acl state=disable  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `set acl table=filter chain=input policy=accept  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

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

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related dot1dbridge command in the *ION System CLI Reference Manual, 33473*. 4. If the problem persists, contact Technical Support.

Message: `AGENT PM ERROR: CLI command show dot1dbridge ip-tc priority remapping failed`

Response: 1. Check if this is a recurring problem with ACL Rules and Conditions. 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, 33473*. 4. If the message was the result of recent backup/restore, retry the operations. 5. If the problem persists, contact Technical Support.

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)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Fail for sending ionSyslogMgmtTable ,ignored...\n
Meaning: possible internal error.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Fail to get syslog server address type!
Fail to get syslog server address type!
Fail to get syslog server port!
Fail to get syslog level!
Fail to get syslog level!
Fail to get syslog server address!
Meaning: the **show syslog config** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Fail to set syslog server port!
Fail to set syslog mode!
Fail to set syslog level!
Fail to set syslog server address!
Fail to set syslog server address type!
Meaning: the **set syslog level / mode / svr** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Invalid syslog server address!
Meaning: the **set syslog svr** attempt failed (e.g., **set syslog svr type**=ipv4 addr=192.168.01).
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Number of subid is not correct when ionSyslogMgmtTable_get, expect %d, get %d \n
Meaning: possible internal error
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Please input a digital number to specify syslog server port!
Meaning: the **set syslog svr port** attempt failed.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation with a valid, unused UDP port number.
3. If the problem persists, contact Technical Support.

Session reset, Reregister from begging\n
STATUS_INVALID, should be session reset, Reregister from beginning\n
Meaning: possible internal error.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Syslog is not supported on this card!
Meaning: You tried to configure a Syslog parameter, but this device does not support the Syslog feature.
Recovery:
1. Verify that this is the command / function you wanted.
2. Switch to a device that supports Syslog.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

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.

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)" on page 112.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

unknown column in ionSyslogMgmtTable_get\n
Meaning: possible internal error.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Syslog Warning: A defined IDS is detected.
Meaning: The Upgrade file failed, the Web interface reports an error, the system can't login and keeps initializing. For example:

```
Line  1 Jan  1 19:33:01 (none) user.warn subagent[818]: A defined IDS is detected.
```

At the ACL tab, you selected rule 1 and edited policy to "Trap", Trap Rate to "4", selected Condition 1, and then edited the Condition 1 value to the local host's IP address. Then uploaded upgrade file by TFTP server tried to upgrade the system. The upgrade file failed, the Web interface reported an error, and the system can't login and keeps initializing. After enabling the ACL trap for the same source IP as the TFTP server and doing tftp operation to the TFTP server, a large amount of packets with the source TFTP server IP are received by the IONMM and each packet is looked at as an IDS packet which caused the subagent and snmpd to become overburdened.
Recovery: None; this issue appears as something like a manual IDS attack to the ION system, which may not be an issue for most users.

Sample Sys.log Output

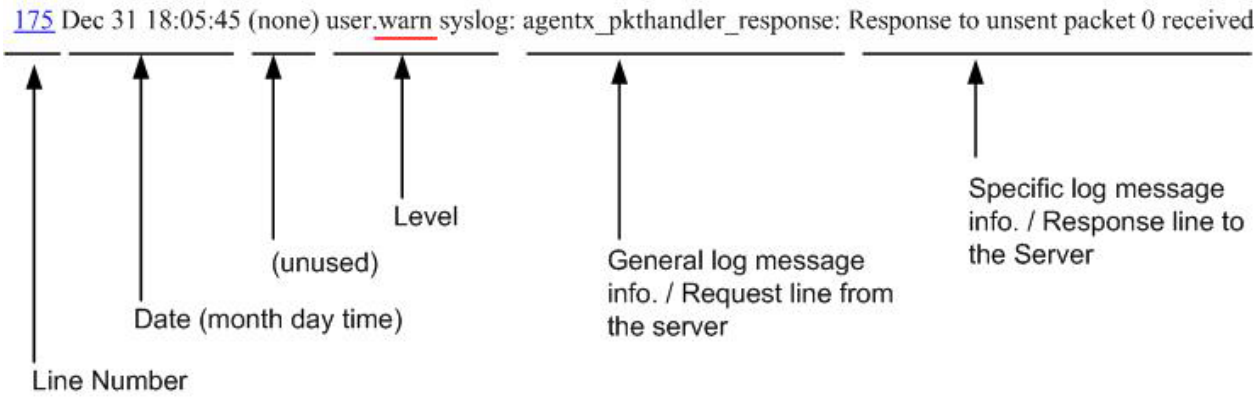
A typical Syslog output is shown below.

```
Line
   1 C0|S0|L1D>cat sys.log
   2 Dec 31 18:00:07 (none) local5.notice bpd_linux[716]: BPD Started.
   3 Dec 31 18:00:08 (none) local5.notice loam[715]: LOAM started
   4 Dec 31 18:00:12 (none) user.notice subAgent2[726]: subAgent Started.
   5 Dec 31 18:00:16 (none) daemon.notice ION-EM[742]: Entity Manager running in Mast
   6 er Mode
   7 Dec 31 18:00:17 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[0],
   8  relpos-[1]
   9 Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=1
  10 Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=2
  11 Dec 31 18:00:19 (none) user.notice subAgent2[726]: subAgent session connected.
  12 Dec 31 18:00:19 (none) user.notice subAgent2[726]: Standalone mode, Send the col
  13 dStart trap.
  14 Dec 31 18:00:21 (none) daemon.err snmpd[719]: ion-ns/logical: session from local
  15  subAgent2 end_point_name [/var/agentx/master]
  16 Dec 31 18:28:58 (none) local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a
  17 ppPduFrameLen == 0 when recvMsgFromAppSAP
  18 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  19 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  20 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  21 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  22 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  23 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  24 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  25 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  26 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  27 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  28 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  29 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
  30 Dec 31 18:29:08 (none) daemon.warn ION-EM[742]: AgentX master agent failed to re
  31 spond to ping.  Attempting to re-register.
```

A typical syslog message is shown below:

```
16 Dec 31 18:28:58 (none) local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a
17 ppPduFrameLen == 0 when recvMsgFromAppSAP
```

The Syslog format is shown below.



Syslog messages, their meanings, and suggested responses are provided below.

Message: `local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a ppPduFrameLen == 0 when recvMsgFromAppSAP`

Meaning: Level 3 Error (err) severity; received a frame with a frame length of 0.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Retry the operation. 3. If the problem persists, contact Technical Support.

Message: `daemon.warn ION-EM[742]: AgentX master agent failed to respond to ping. Attempting to re-register.`

Meaning: Level 4 Error (warn) severity; the IONMM did not respond to a ping.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Retry the operation. 3. If the problem persists, contact Technical Support.

Message: `Dec 31 18:31:39 (none) user.crit subAgent2[822]: agentx_protocol_disconnect: Subagent disconnected from master.`

Meaning: Level 2 - Critical condition.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

Message: `61Dec 31 18:31:39 (none) user.crit subAgent2[822]: agentx_protocol_disconnect: Subagent disconnected from master.`

Meaning: Level 2 - Critical condition.

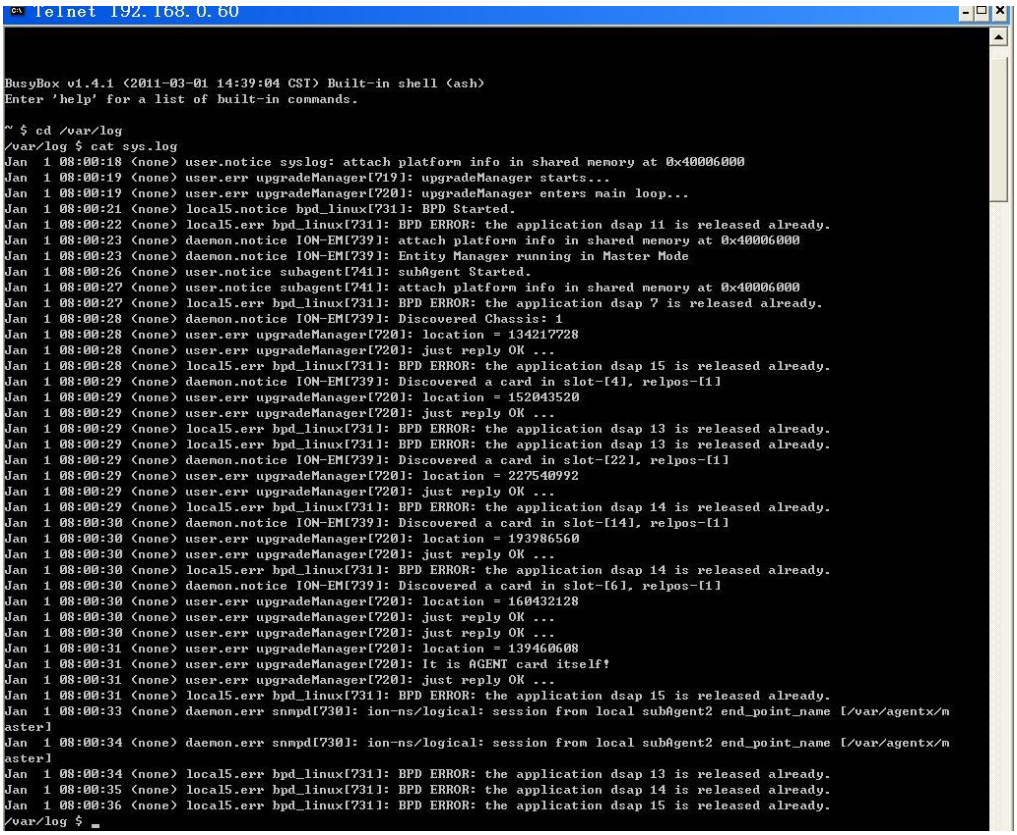
Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

Message: `user.err upgradeManager`

Meaning: you unplugged the SIC card, system will send a syslog which descript as "user.err upgradeManager", that not match the event.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

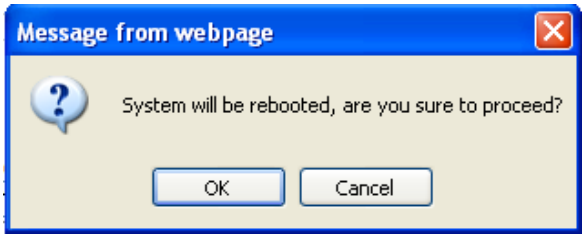
Sys.log sample - A typical Syslog output is shown below (Telnet screen)



Webpage Messages

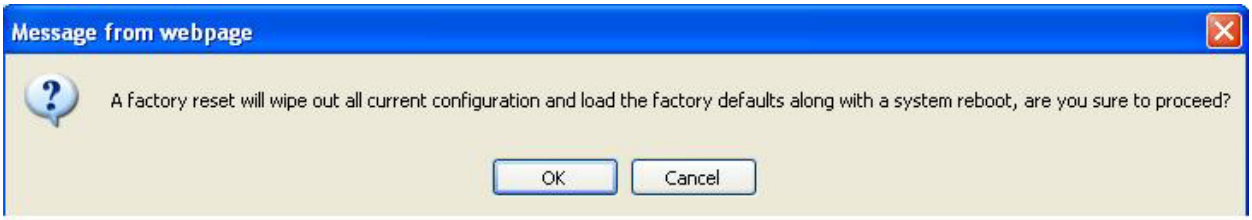
Certain menu operations will display a webpage verification message to verify that you want to proceed. These messages also provide information on the effect that the operation will have if you continue. These messages display for operations such as **Reset to Factory Config**, **Reboot the System,**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

See Menu System Notes on page 79 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*?

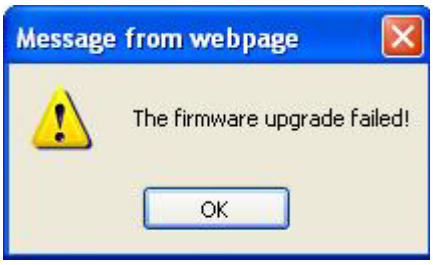
Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

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 on page 229.

Message: *The firmware upgrade failed*!



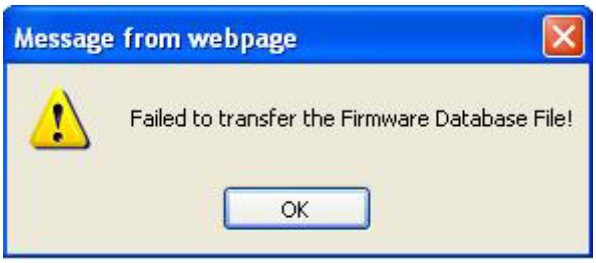
The **MAIN** tab **>** **TFTP Settings** section **Status** area displays "*TFTP Failure*".

Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the Upgrade the IONMM Firmware section on page 205.

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.0.5.3**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.0.5.3 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Make sure that the Management VLAN function is disabled.
8. Reset the IONMM card. The **TFTP Settings** section **Status** area should display "*Success*" when done.
9. If the problem persists, contact Technical Support.

Message: *Failed to Transfer the Firmware Database File*!

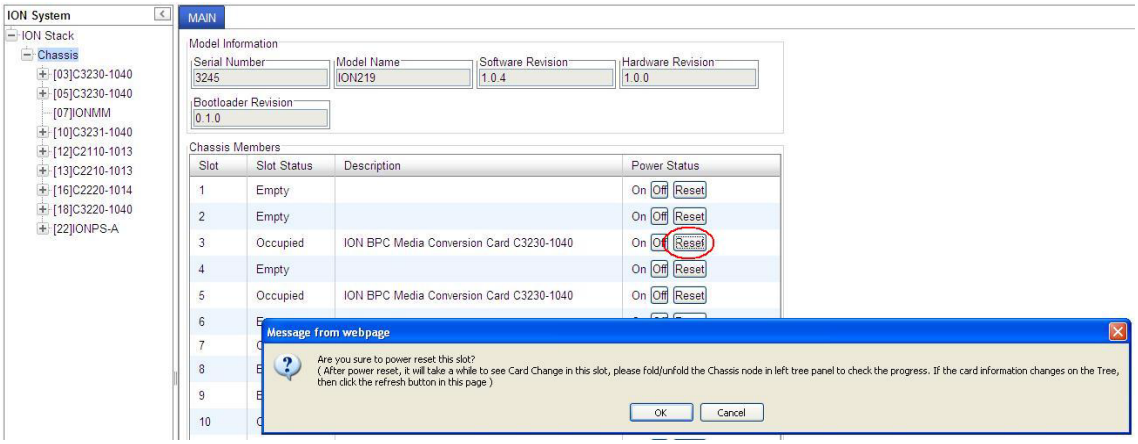


Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the Upgrade the IONMM Firmware section on page 205.

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.0.5.3**).
6. Check the log status in the TFTP Server package; when successful, it should show something like "*Sent IONMM.bin.0.5.3 to (192.168.1.30), 9876543 bytes*". The **TFTP Settings** section **Status** area should display "*Success*" when done.
7. Reset the IONMM card. The **TFTP Settings** section **Status** area should display "*Success*" when done.
8. If the problem persists, contact Technical Support.

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

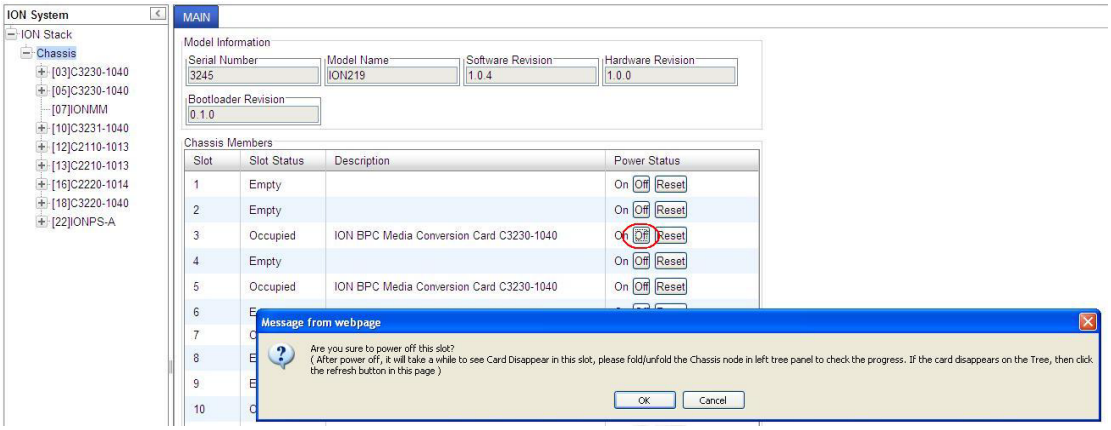


Meaning: A caution message generated at the **Chassis** > **MAIN** tab. You clicked the **Reset** button for a particular slot.

Recovery:

1. If you are not sure that you want to reset this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to reset this chassis, click the **OK** button to clear the message and reset power to the slot.
3. At the **Chassis** > **MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See the "Menu System Notes" section on page 77.
6. If the problem persists, contact Technical Support.

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



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

1. **Recovery**: If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to power off this slot, click the **OK** button to clear the message and remove power to the slot.
3. At the **Chassis** > **MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See the "Menu System Notes" section on page 77.
6. If the problem persists, contact Technical Support.

Message: *TFTP file transferring failed!*

Meaning: Either the TFTP Server is not running, or the filename entered was incorrect or not found. See the "Backup/Restore Operations" section on page 218.

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 Lantronix website .

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" on page 192.
3. If a message displays regarding a problem with the website's security certificate, select "*Continue to this website*".

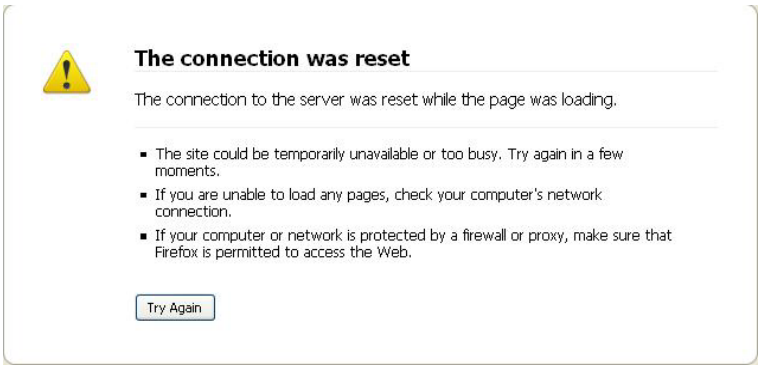
Message*: The RADIUS settings have been changed and a re-login will be performed right now.*

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" on page 192.
3. If a message displays regarding a problem with the website's security certificate, select "Continue to this website".

Message: *The Connection was Reset*

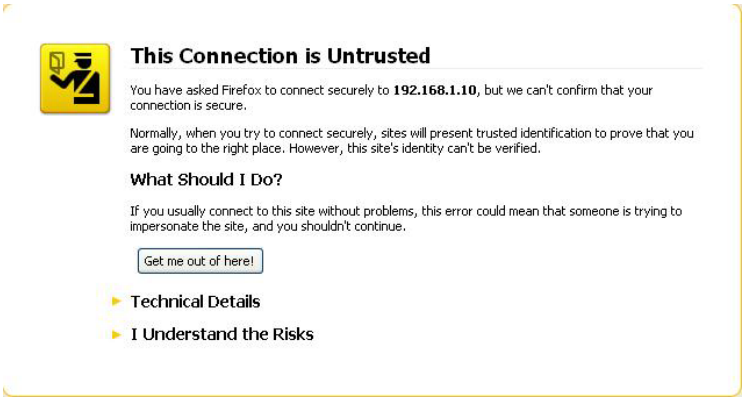


Meaning: The FireFox web browser connection failed to load the page.

Recovery:

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

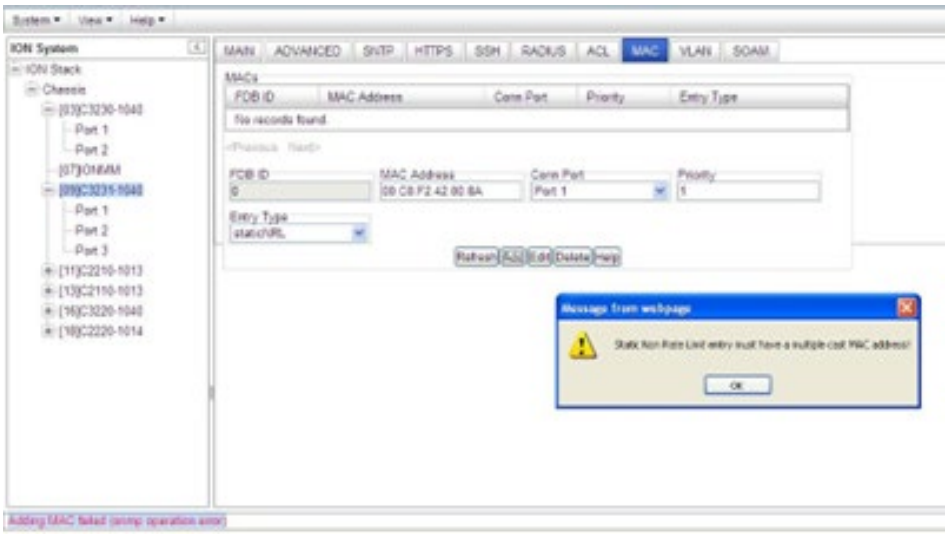
Message: *This Connection is Untrusted*



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

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

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

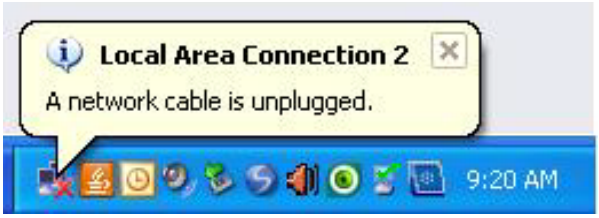


Meaning: When setting up MAC filtering, you entered a unicast MAC address and selected a Static NRL (Non Rate Limit) Entry Type.

Recovery:

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

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

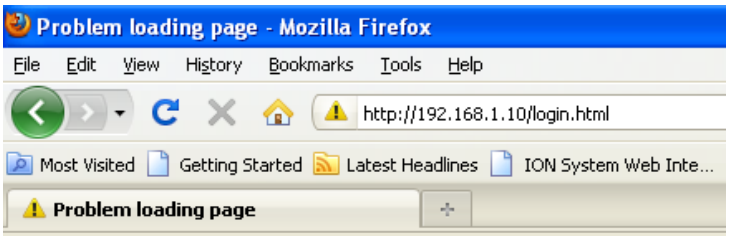


Meaning: You unplugged the USB cable at the NID or IONMM, or the NID or IONMM was unplugged from the ION chassis, or you pressed the Reset button on the IONMM.

Recovery:

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

Message: *Problem loading page – Mozilla Firefox*

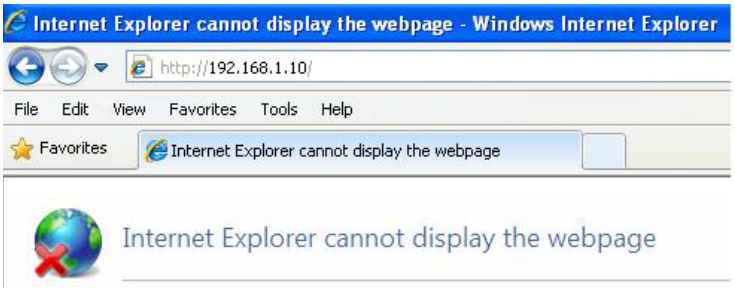


Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

Recovery:

1. Make sure the web browser you are using is supported. See "Web Browsers Supported" on page 72.
2. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI" on page 59.
3. Verify NID access. See "Accessing the NIDs" on page 69.
4. Verify the IP address setting. See "Setting the IP Addressing" on page 89.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

Message: *Internet Explorer cannot display webpage*



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

Recovery:

1. Make sure the web browser you are using is supported. See "Web Browsers Supported" on page 72.
2. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI" on page 59.
3. Verify NID access. See "Accessing the NIDs" on page 69.
4. Verify the IP address setting. See "Setting the IP Addressing" on page 89.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support.

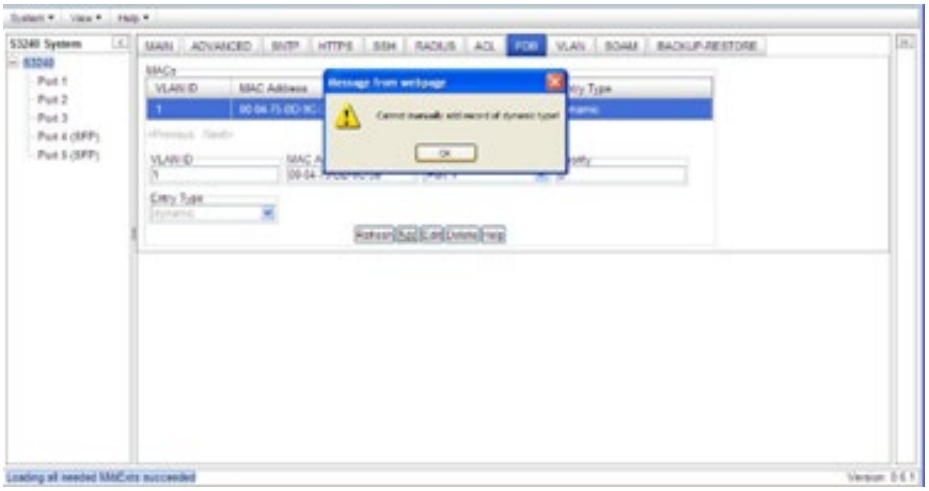
Message: *The webpage cannot be found*
Message: *HTTP 404 Not Found – Windows Internet Explorer*

Meaning: There might be a typing error in the address, or the link you clicked on may be out of date.

Recovery:

1. Retype the address.
2. Go back to the previous page.
3. Make sure the web browser / version you are using is supported. See "Web Browsers Supported" on page 72.
4. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI" on page 59.
5. Verify NID access. See "Accessing the NIDs" on page 69.
6. Verify the IP address setting. See "Setting the IP Addressing" on page 89.
7. Verify the URL (e.g., http:// versus https://).
8. Try to log in to the S3240 again.
9. If the problem persists, contact Technical Support.

Message: *Cannot manually add record of the dynamic type!*

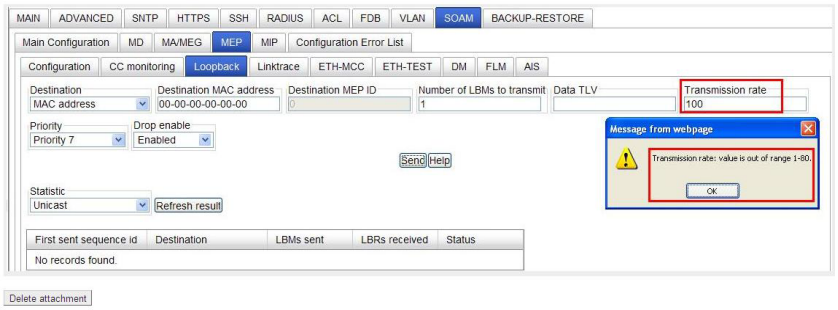


Meaning: At the **FDB** tab, you tried to create a MACs table entry with an **Entry Type** of ***dynamic***.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Try entering a different MAC address for the MACs table entry.
3. Select another Entry Type (**static**, **staticPA**, or **staticNRL**).
4. Continue with other MACs table entries and press the **Add** button.
5. If the problem persists, contact Technical Support.

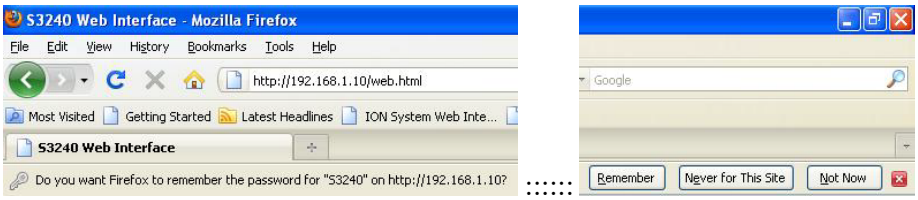
Message: *Transmission rate: value is out of range 1-80*



Meaning: You entered an invalid LBM transmission rate at S3240 **SOAM** > **MEP** > **Loopback**.

Recovery: 1. Click **OK** to clear the webpage message. 2. In the **Transmission rate** field, enter the number of loopback messages (LBMs) to be sent per second. The valid range is 1 – 80 LBMs per second. 3. Continue operation; see "Loopback (LB) Config – Web Method" on page 185. 4. If the problem persists, contact Technical Support.

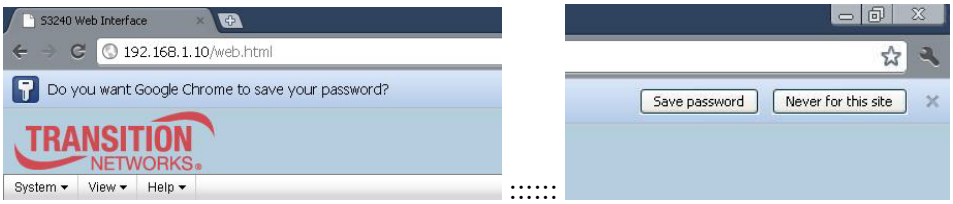
Message: *Do you want Firefox to remember the password for "S3240" on http://192.168.0.10?*



Meaning: The Mozilla Firefox login security option screen.

Recovery: Select one of the three options as desired or according to your organization's security policy. Select **Remember** to avoid entering the password at the next login, or select **Never for this site** to eliminate this option at future logins, or select **Not Now** to avoid password entry at the next login but keep the option available for future logins.

Message: *Do you want Google Chrome to save your password?*



Meaning: The Google Chrome login security option screen.

Recovery: Select one of the two options as desired or according to your organization's security policy. Select **Save password** to avoid entering the password at the next login, or select **Never for this site** to eliminate this option at future logins.

ION System Tests

The x222x/32xx NID provides a set of system level tests, DMI functions, and related test functions.

Virtual Cable Test (VCT)

The VCT feature uses TDR (Time Domain Reflectometry) to determine the quality of cables, connectors, and terminations. Problems that can be determined include opens, shorts, cable impedance mismatches, failed connectors, and termination mismatches.

The VCT runs the cable diagnostic by transmitting a signal of known amplitude sequentially along each of the TX and RX pairs of an attached cable. The transmitted signal continues along the cable until it is reflected from a cable imperfection, and that distance is displayed. If the test status returned is Normal, the distance displayed is the actual cable length. The VCT test is intrusive, as the tested port's link is brought down during the test.

When the VCT is activated, a pre-defined amount of time elapses before a VCT test pulse is transmitted. This ensures that the link partner loses link, so that it stops sending 100BASE-TX idles or 10 Mbps data packets. The VCT can be performed either when there is no link partner, or when the link partner is Auto-Negotiating or sending 10 Mbps idle link pulses.

Use the VCT test to determine if cabling is at fault when you cannot establish a link. Problems can include opens, shorts, cable impedance mismatches, failed connectors, and termination mismatches, bad magnetics.

Do not change the port configuration while the TDR test is running.

Due to cable characteristics, run the TDR test several times to get accurate results.

Do not change port status (e.g., remove the cable at the near or far end) as the results may be inaccurate.

The VCT test can be configured via the CLI method or the Web method.

VCT Test – CLI Method

Use the VCT test to determine if cabling is at fault when you cannot establish a link for an x222x/x32xx copper port.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Start the VCT Test. Type **start ether tdr test** and press **Enter**.
   The Time Domain Reflector (TDR) test starts on the specified Ethernet copper port.
3. Show the Ethernet port TDR Test configuration. Type **show ether tdr config** and press **Enter**.
   The Time Domain Reflectometry (TDR) test configuration displays for the Ethernet copper port. For example:

```
C1|S16|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----------------------------------------------------------------
TDR test state:               success
TDR test init time:           22:39:18
TDR test result valid:        true
C1|S16|L1P1>
```

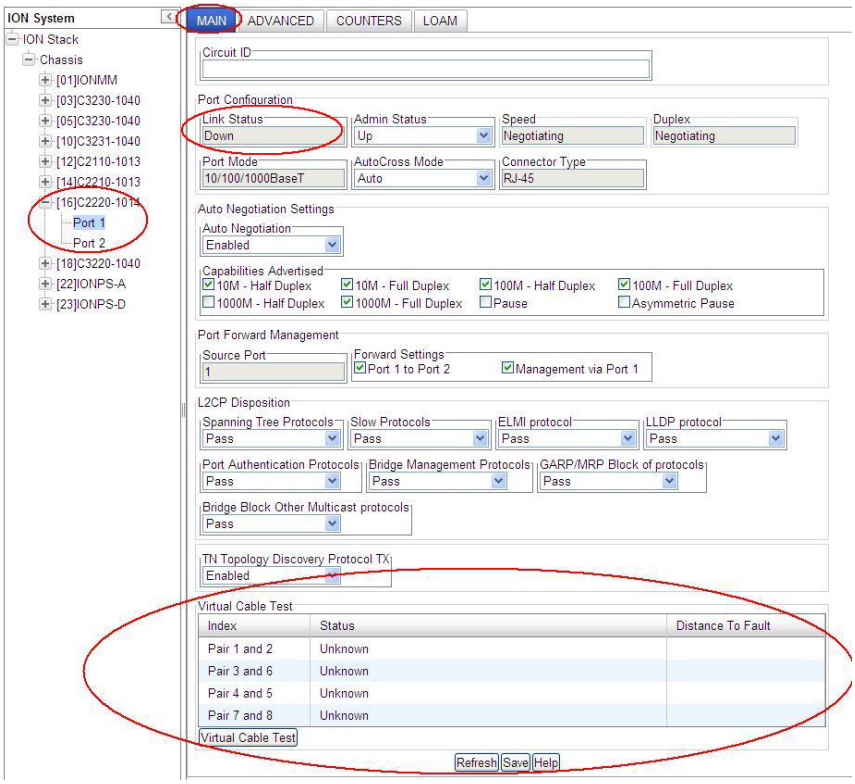
4. Show the Ethernet port TDR Test results. Type **show ether tdr test result** and press **Enter**.
   The results of an Ethernet port TDR test display for the copper port. For example:

```
C1|S5|L1P1>show ether tdr test result
Cable pair :
index                distance to fault(unit)       status
-------------------------------------------------------------------------
pair1 and 2           0(meter)                      open
pair3 and 6           0(meter)                      open
pair4 and 5           0(meter)                      open
pair7 and 8           1(meter)                      open
C1|S5|L1P1>
```

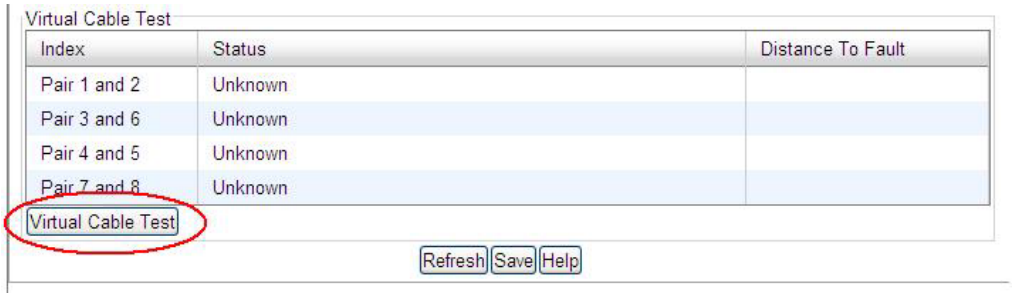
5. Run the TDR test several times to ensure accurate results. Do not change port status (e.g., remove the cable at the near or far end) as this may cause inaccurate results.

VCT Test – Web Method

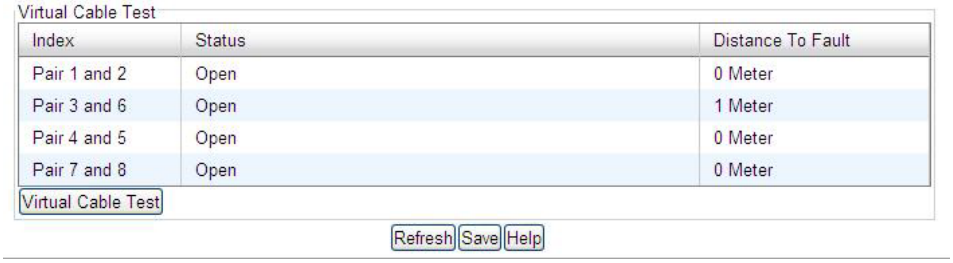
1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the desired port.
3. At the port-level **MAIN** tab, check the information displayed in the **Link Status** and **Virtual Cable Test** areas.



4. Click the **Virtual Cable Test** button. The VCT test runs and test information displays.



5. Check the information displayed in the **Link Status** (*Up* or *Down*) and **Virtual Cable Test** sections.



The possible VCT Test parameters and states are described in the table below.

Table 30: VCT Parameters

Parameter	Fault State	Meaning
Link Status Down		VCT Test failed due to lost link.
Link Status Up		VCT Test passed; link is up. No action needed.
Index - Pair x to y		There are four pairs of standard category 5 cable. Each pair displays one of these states: Open, Broken, Shorted, Terminated, Impedance Mismatch, or Unknown.
Status – Normal		The pair is properly terminated at the remote end (not a fault state). The 'Distance To Fault' is blank.
Status – Open	X	Open (not connected) connection failure status. Cable impedance is greater than 333 ohms.
Status – Broken	X	Broken connection failure status.
Status – Shorted	X	Shorted connection failure status. Cable impedance is less than 333 ohms.
Status – Terminated		Connection terminated status (non-fault state).
Status – Impedance Mismatch	X	The impedance of the pair is mismatched.
Status – Unknown	X	None of the above (i.e., not Normal, Open, Shorted, Terminated, Impedance Mismatch, or Unknown).
Distance To Fault - 0 Meter		The overall distance to the fault in Meters (Open or no fault found).
Distance To Fault > 0 Meter		The overall distance to the fault in Meters.

DMI (Diagnostic Maintenance Interface) Parameters

The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. **Note**: Lantronix NIDs that support DMI have a "-D" at the end of the model number.

Note: If the message "*ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*" displays, follow your organization's policy and procedure for intrusion detection.

DMI can be configured in the NID using either the CLI or Web method.

DMI Config – CLI Method

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Set the Diagnostic Monitoring Interface receive preset power level. Type:

   set dmi rx-power-preset-level=xx
   where: xx is a preset level for Rx Power on the Fiber port, in the range of 1 to 10.

3. Press **Enter**. For example: **set dmi preset-power-level=10**.
4. Display the DMI information. Type: **show dmi info** and press **Enter**. For example:

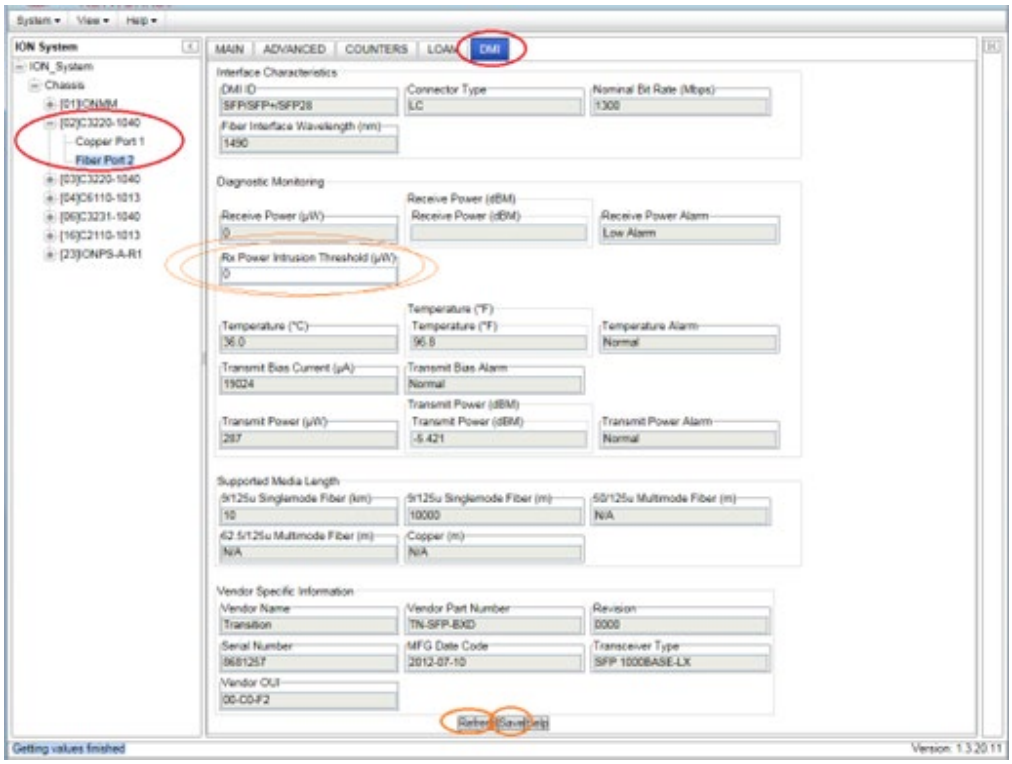
```
Agent III C1|S3|L1P1>show dmi info
Error: DMI is only supported on FIBER port!
Agent III C1|S3|L1P1>go l1p=2
Agent III C1|S3|L1P2>show dmi info
Diagnostic monitoring interface information:
-------------------------------------------------------------------------
DMI connector type:                     LC
DMI indentifier:                        SFP/SFP+/SFP28
DMI Nominal bit rate:                   1300*Mbps
DMI 9/125u Singlemode Fiber (k):        N/A
DMI 9/125u Singlemode Fiber (m):        N/A
DMI 50/125u Multimode Fiber (m):        500*m
DMI 62.5/125u Multimode Fiber (m):      30*10m
Copper(m):                              N/A
DMI fiber interface wavelength:         850*nm
DMI temperature:                        38.7*C
DMI temperature:                        101.7*F
DMI temperature alarm:                  normal
DMI transmit bias current:              3824*uA
DMI transmit bais alarm:                normal
DMI Transmit power:                     211*uW
DMI Transmit power:                     -6.757*dBM
DMI Transmit power alarm:               normal
DMI Receive power:                      1*uW
DMI Receive power:                      -30.000*dBM
DMI Receive power alarm:                lowAlarm
DMI Vendor name:                        Transition
DMI Vendor Part Number:                 TN-SFP-SXD
DMI Vendor serial number:               0000
DMI Vendor revision:                    8672299
DMI Vendor date code:                   2011-08-23
DMI Vendor Transceiver type:            SFP 1000BASE-SX
DMI Vendor OUI:                         00-C0-F2
```

```
DMI Receive power intrusion threshold:  110*uW
Agent III C1|S3|L1P2>
```

The DMI tab parameters are described in Table 22 later in this section.

DMI Config – Web Method

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select Port 2 of the desired device.
3. Select the **DMI** tab.



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

4. Change the "**Rx Power Intrusion Threshold**" setting as desired. The default is 0 uW. The valid range is 0 - 65,535 uW (microwatts).
5. Click the **Refresh** button to update the information displayed.
6. Click the **Save** button to save the updated information.

NID models with Diagnostic Monitoring Interface (DMI) support allow diagnosing problems within the network. The DMI function displays x3220 NID diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. All DMI events will trigger notification. Intrusion detection, based on Rx Power level, is available for triggering any drop in the Rx power.

DMI devices display four main functions: Transmit power, Receive power, Transmit bias current, and Temperature.

Within each function, the DMI device will send a trap whenever a high or low warning event or high or low alarm event occurs (for a total of 16 traps). If both the local and remote NIDs are DMI models, the DMI device will indicate whether the trap event is from a local or remote device.

The DMI parameters are explained below.

Table 31: DMI Parameters

Parameter	Associated MIB variable	Description
Interface Characteristics		
DMI ID	ionDMIId(8)	Specifies the physical DMI device ID from the standard; for example: SFP/SFP+/SFP28, SG, Optical pigtail, SFP, 300-pin XBI , XENPAK, XFP, XFF, XFP-E, XPAK, X2, DWDM-SFP/SFP+, QSFP, QSFP+, CXP, Copper Pigtail, RJ45 (Registered Jack), No separable connector, etc.
Connector Type	ionDMIConnectorType(1)	The external optical or electrical cable connector provided as the interface. For example: LC, SC, Dual BNC coax connectors, DB9 for RS232 and RS485, RJ-11, unshielded twisted pair, SC fiber, 1550nm 40km, SC fiber, 1 x 9, 125km Gigiabit , ST Single-Fiber 155Mbps, LC Multimode Fiber, SFP cage, Single-Fiber Multimode, SC Multimode (long haul), LC Singlemode (long haul), XFP slot, SFP+ slot, etc..
Nominal Bit Rate (Mbps)	ionDMIBitRate(2)	Bitrate in units of 100Mbps (for example: 10500, or 10.G Gbps) (measured rate).
Fiber Interface Wavelength (nm)	ionDMILaserWavelength(9)	The Nominal transmitter output wavelength at room temperature (measured wavelength). The unit of measure is nanometers (for example: 1550 nm or 850 nm).
Diagnostic Monitoring		
Receive Power (uW)	ionDMIRxPowerLevel(16)	Receive power (measured power measurement) on local fiber measured in microwatts (for example: 11 uW).
Receive Power (dBM)	ionDMIRxPowerLevel(16)	Receive power (measured signal strength) on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. For example: -19.586 dBM.
Receive Power Alarm	ionDMIRxPowerAlarm(17)	Alarm status for receive power on local fiber: Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Rx Power Intrusion Threshold (uW)	ionDMIRxPwrLvlPreset(18)	A preset level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated (0-10). The message displays: *ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress*. **Note**: C4110 port 2 DMI data is not shown if there is no SFP in port 1. Without an SFP in port 1, the port 2 DMI will display "*The DMI feature is not supported on the current port.*". When an SFP is inserted into port 1, the port 2 DMI displays as expected. To recover, insert an SFP in Port 1 and click the **Refresh** button.
Temperature (˚C)	ionDMITemperature(10)	Measured temperature of fiber transceiver in tenths of degrees C (Celsius). For example: 30.1˚C.

Parameter	Associated MIB variable	Description
Temperature (˚F)	ionDMITemperature(10)	Measured Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). For example: 86.2 ˚F.
Temperature Alarm	ionDMITempAlarm(11)	Alarm status for temperature of fiber transceiver. An *ionDMITemperatureEvt* event is sent when there is a warning or alarm on DMI temperature. Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Transmit Bias Current (uA)	ionDMITxBiasCurrent(12)	Measured transmit bias current on local fiber interface, in uA (microamperes). For example, 5936 uA (microamps).
Transmit Bias Alarm	ionDMITxBiasAlarm(13)	Alarm status for transmit bias current on local fiber interface. Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Transmit Power (uW)	ionDMITxPowerLevel(14)	Measured transmit power on local fiber measured in microwatts.For example, 240 uW (microwatts).
Transmit Power (dBM)	ionDMITxPowerLevel(14)	Transmit power on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. For example: -2.291 dBM.
Transmit Power Alarm	ionDMITxPowerAlarm(15)	Alarm status for transmit power on local fiber. Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Supported Media Length		
9/125u Single-mode Fiber (km)	ionDMILenFor9x125umKM(3)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is kilometers (km). For example, 8Km.
9/125u Single-mode Fiber (m)	ionDMILenFor9x125umM(4)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). For example, 80m.
50/125u Multi-mode Fiber (m)	ionDMILenFor50x125um10M(5)	Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters.
62.5/125u Multimode Fiber (m)	ionDMILenFor625x125um10M(6)	Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters.
Copper (m)	ionDMILenForCopper(7)	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters.

Vendor Specific Information		
Vendor Name	ionDMIInfoEntry 19	A 16 character field that contains ASCII characters. The full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation. For example: Transition or other.
Vendor Part Number	ionDMIInfoEntry 20	A 16-byte field that contains ASCII characters, defining the vendor part number or product name. A value of all zeroes in the 16-byte field indicates that the vendor PN is unspecified. For example, TN-SFP-LX1, TN-SFP-BXD, TN-SFP-OC3M, TN-SFP-OC3S, TN-10GSFP-SR or similar. For the TN-DWDM-SFP-xxxx, the xxxx indicates the center wavelength (e.g., for a TN-DWDM-SFP-5012, the 5012 indicates 1550.12 nm center wavelength laser support).
Revision	ionDMIInfoEntry 21	A 4-byte field that contains ASCII characters, defining the vendor product revision number. A value of all zeroes in the 4-byte field indicates that the vendor revision is unspecified. For example e.g., 2.0.
Serial Number	ionDMIInfoEntry 22	A 16 character field that contains ASCII characters, defining the vendor's serial number for the transceiver. A value of all zeroes in the 16-byte field indicates that the vendor SN is unspecified. For example: TWDW34Z001, 8800022, 102201102, or similar.
MFG Date Code	ionDMIInfoEntry 23	An 8-byte field that contains the Vendor's date code in ASCII characters: 84-85 ASCII code, two low order digits of year (00 = 2000). 86-87 ASCII code, digits of month (01 = Jan through 12 = Dec). 88-89 ASCII code, day of month (01-31). 90-91 ASCII code, vendor specific lot code, may be blank. For example 2016-07-30.
Transceiver Type	tnDMIInfoEntry xx	The SFP transceiver type. For example: None, Not Supported, SFP 100FX, SFP 1000BASE-T, SFP 1000BASE-CX, SFP 1000BASE-SX, SFP 1000BASE-LX, SFP 1000BASE-X, SFP 2G5, SFP 5G, or SFP 10G.
Vendor OUI	tnDMIInfoEntry 25	The vendor Organizationally Unique Identifier field (Vendor OUI) is a 3-byte field that contains the IEEE Company Identifier for the vendor (e.g., 00-C0-F2). A value of all zeroes in the 3-byte field indicates that the Vendor OUI is unspecified.

Connector Types

The DMI connector type indicates the external optical or electrical cable connector provided as the interface. The information below is from SFF 8472 Rev 9.5.

Value	Description of connector
00h	Unknown or unspecified
01h	SC
02h	Fibre Channel Style 1 copper connector
03h	Fibre Channel Style 2 copper connector
04h	BNC/TNC
05h	Fibre Channel coaxial headers
06h	FiberJack
07h	LC
08h	MT-RJ
09h	MU
0Ah	SG
0Bh	Optical pigtail
0C-1Fh	Reserved
20h	HSSDC II
21h	Copper Pigtail
22h-7Fh	Reserved
80-FFh	Vendor specific

The LC, MT-RJ LC, SC, ST, or VF-45 connector types (jacks) are shown below.

ST

SC

LC

MT-RJ

VF-45

Set Debug Level

You can use the CLI method to define the system debug level.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Set the desired debug level. Type:

   set dbg level=<0-2>

   where:

   0=debug Severity level 0 (Emergency: system is unusable - e.g., serious hardware failure or imminent power failure).

   1=debug Severity level 1 (Alert: action must be taken immediately).

   2=debug Severity level 2 (Critical condition).
3. Press **Enter**.

For example:

```
C1|S5|L1D>set dbg level 0
C1|S5|L1D>set dbg level 1
C1|S5|L1D>set dbg level 2
C1|S5|L1D>
```

Ethernet Statistics Counter Descriptions

In a situation where performance, particularly rate or error counts, is suspect, you can use the **show ether statistics** command to display Ether-like counters and If-MIB counters for a copper or fiber port.

These counters are described below.

Total Octets: The total number of octets transmitted out of the interface, including framing characters. (Displayed for “Port Counters Received” and “Port Counters Sent”.)
Unicast Packets: The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. (Displayed for “Port Counters Received” and “Port Counters Sent”.)
Broadcast Packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Multicast Packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. (Displayed for “Port Counters Received” and “Port Counters Sent”.)
Rx Discards: The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. (Displayed for “Port Counters Received” and “Port Counters Sent”.)
Rx Errors: For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. (Displayed for “Port Counters Received” and “Port Counters Sent”.)
Alignment Errors: A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors: A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
SQE Test Errors: A count of times that the SQE TEST ERROR is received on a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6. This counter does not increment on interfaces operating at speeds greater than 10 Mb/s, or on interfaces operating in full-duplex mode.
Deferred Frames: A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal MAC Tx Errors: A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the *dot3StatsExcessiveCollisions* object, or the *dot3StatsCarrierSenseErrors* object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Internal MAC Rx Errors: A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the *dot3StatsFrameTooLongs* object, the *dot3StatsAlignmentErrors* object, or the *dot3StatsFCSErrors* object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
Carrier Sense Errors: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. This counter does not increment when the interface is operating in full-duplex mode.
Symbol Errors: For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. This counter does not increment when the interface is operating at 10 Mb/s.
Single Collisions: A count of frames that are involved in a single collision, and are subsequently transmitted successfully. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the '*Unicast Packets*', '*Multicast Packets*', or '*Broadcast Packets*' (Port Counters Sent), and is not counted by the corresponding instance of the '*Multiple Collisions*' object. This counter does not increment when the interface is operating in full-duplex mode.
Multiple Collisions: A count of frames that are involved in more than one collision and are subsequently transmitted successfully. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the *ifOutUcastPkts*, *ifOutMulticastPkts*, or *ifOutBroadcastPkts*, and is not counted by the corresponding instance of the '*Single Collisions*' object. This counter does not increment when the interface is operating in full-duplex mode.
Late Collisions: The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. This counter does not increment when the interface is operating in full-duplex mode.
Excessive Collisions: A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Oversized Frames: A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the *frameTooLong* status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Duplex Status: The current mode of operation of the MAC entity. *'Unknown'* indicates that the current duplex mode could not be determined.
Rate Control Ability: '*True*' for interfaces operating at speeds above 1000 Mb/s that support Rate Control through lowering the average data rate of the MAC sublayer, with frame granularity, and '*False*' otherwise.
Rate Control Status: The current Rate Control mode of operation of the MAC sublayer of this interface (Rate Control either *on* or *off*).
Rx Unknown Opcodes: A count of MAC Control frames received on this interface that contain an opcode that is not supported by this device.
Rx Pause Frames: A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Tx Pause Frames: A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

DIP Switches and Jumper Settings

The x222x/x32xx NIDs have on-board components that can be used to configure device operation, typically at the direction of a technical support specialist. In most cases, the factory default settings provide optimal configuration settings; however, DIP Switch and Jumper setting changes may be required for operating mode changes or troubleshooting purposes.

PCB Identification

This section covers the following PCBs (printed circuit boards):

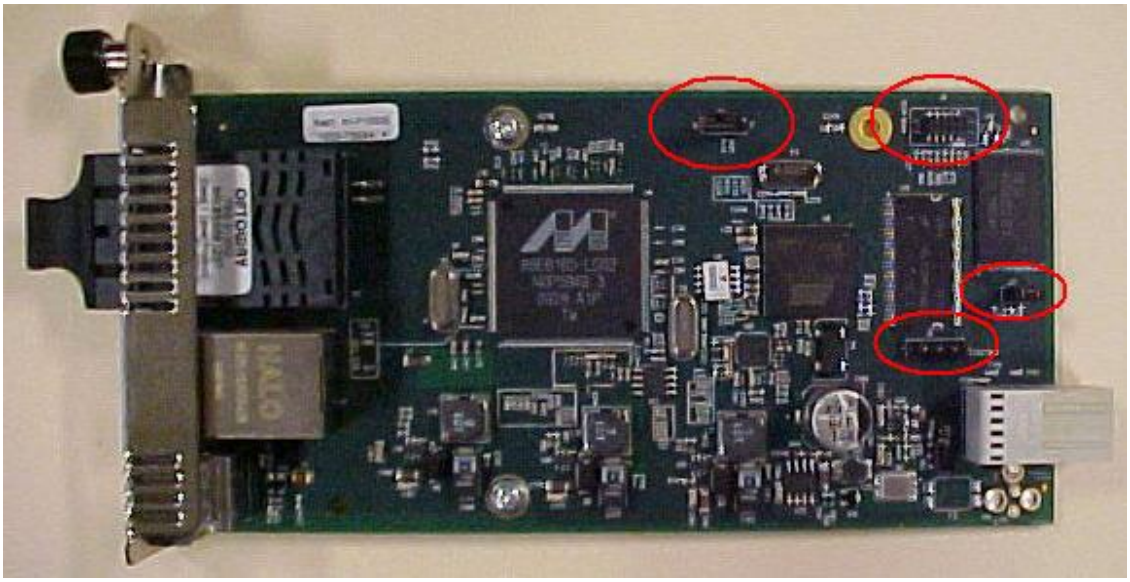
- **x2220** NID - PCB: 11321 Rev. 04 (this information is silkscreened on the bottom of the PCB).
- **x3220** NID - PCB: 11320 Rev. 04 (this information is silkscreened on the bottom of the PCB).

Each PCB has jumpers and / or DIP switches. Not all of these jumpers / DIP switches are intended for use in the field.

Note: Do not change these configurable items except at the direction of a technical support specialist.

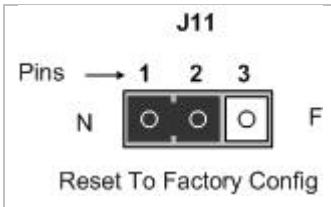
x2220 NID

PCB: 11321 Rev. 04 (this information is silkscreened on the bottom of the PCB). This PCB has four jumpers and no DIP switches. Only Jumper J11 is used in the field.



J11 – Reset to Factory Defaults (N/F)

Doing a **Reset To Factory Config** resets the NID 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. See "Reset To Factory Config" on page 80 for more information.



J11

Jumper Pin #s	Function
1-2 (N)	None.
2-3 (F)	Reset the unit to factory defaults.

J9 (Not Used)

Do not use. Jumper J9 is used for manufacturing / debug purposes only.

J12 (Not Used)

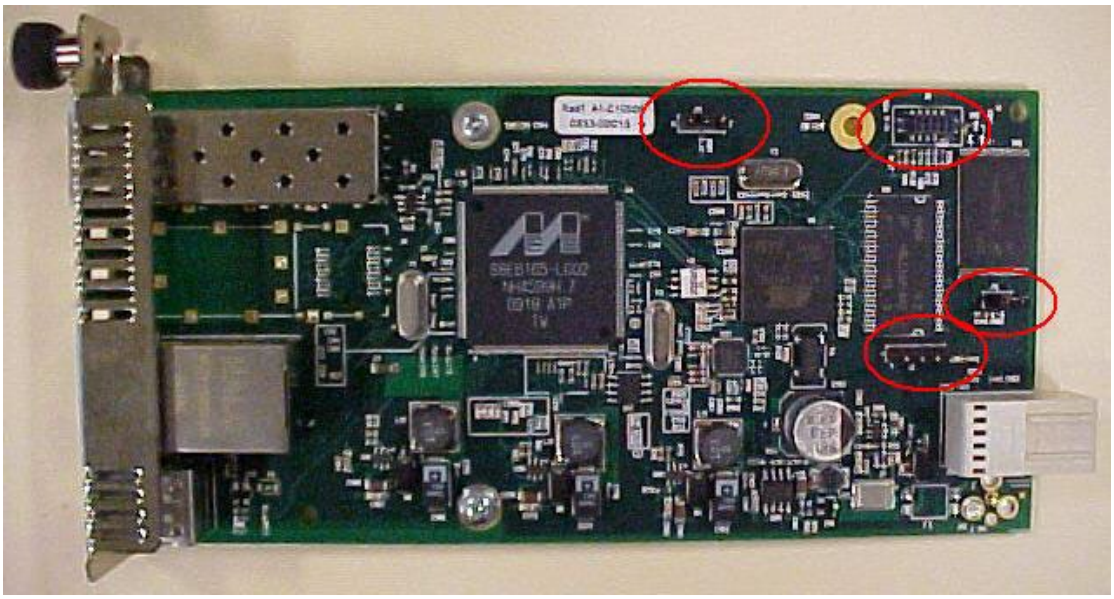
Do not use. Jumper J12 is used for manufacturing / debug purposes only.

J8 (Not Used)

Do not use. Jumper J8 is used for manufacturing / debug purposes only.

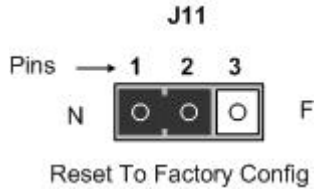
x3220 NID

PCB: 11320 Rev. 04 (this information is silkscreened on the bottom of the PCB). This PCB has no DIP switches and four jumpers. Only Jumper J11 is used in the field.



J11 – Reset to Factory Defaults (N/F)

Doing a **Reset To Factory Config** resets the S3220 NID 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. See "Reset To Factory Config" on page 80 for more information.



J11

Jumper Pin #s	Function
1-2 (N)	None.
2-3 (F)	Reset the unit to factory defaults.

J9 (Not Used)

Do not use. Jumper J9 is used for manufacturing / debug purposes only.

J12 (Not Used)

Do not use. Jumper J12 is used for manufacturing / debug purposes only.

J8 (Not Used)

Do not use. Jumper J8 is used for manufacturing / debug purposes only.

Third Party Troubleshooting Tools

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

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

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

Ipconfig

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

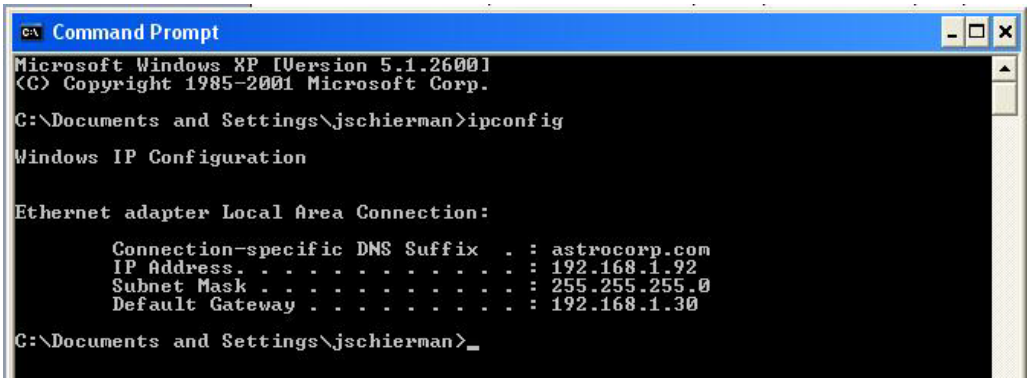
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway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

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

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

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

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



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

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

ifconfig

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

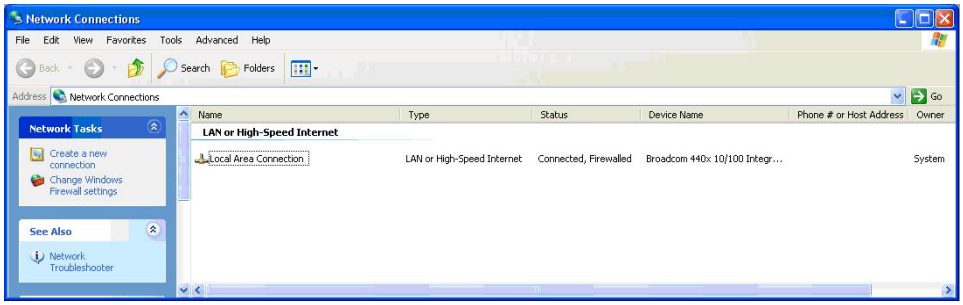
```
[root@sleipnir root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:6E:0A:3D:26
          inet addr:192.168.168.11  Bcast:192.168.168.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13647 errors:0 dropped:0 overruns:0 frame:0
      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

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

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

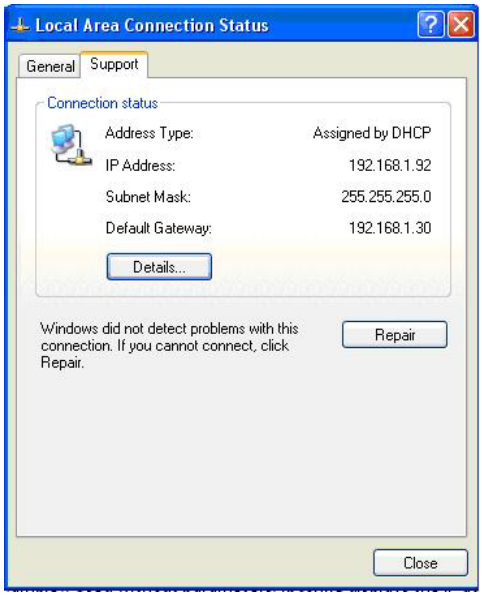
Windows Network Connections

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

1. Open Network Connections from **Start** → **Settings** → **Network Connections**.



2. Right-click a network connection.
3. Click **Status**.
4. Click the **Support** tab. Your connection status information displays.

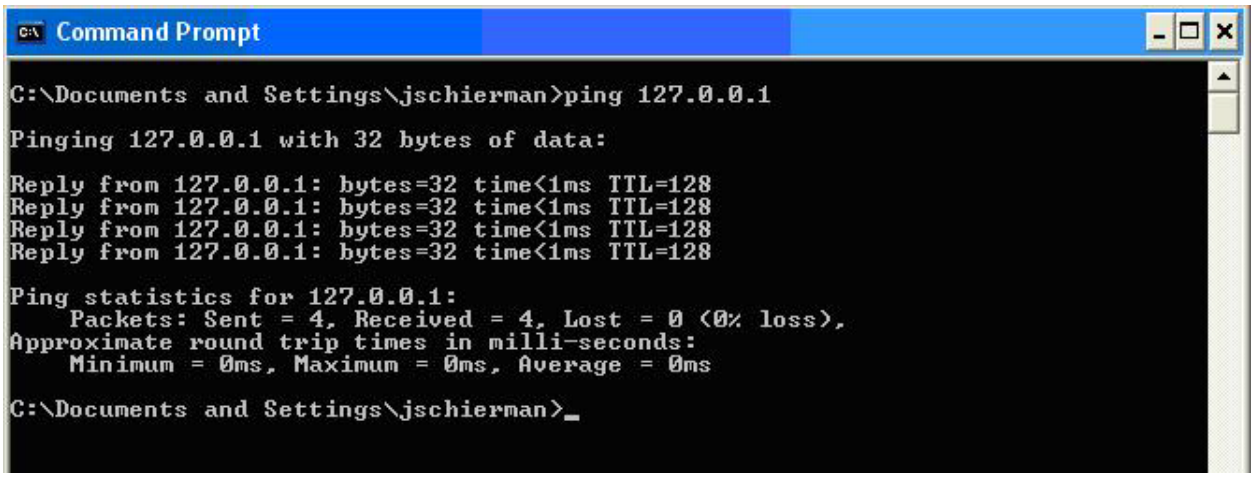


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

Ping

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

1. Open a Command Prompt**.** To open a command prompt, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, ping the loopback address by typing **ping 127.0.0.1**.



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

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

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

Telnet

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

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

Telnet Client

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

To install Telnet Client:

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

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

To open the Telnet Client:

1. Clicking the **Start** button, type **Telnet** in the Search box, and then click **OK**.
2. To see the available telnet commands, type a question mark (**?**) and then press **Enter**.

Telnet Server

In Windows Server 2003 for most Telnet Server functions, you do not need to configure Telnet Server options to connect a Telnet client to the Windows Server 2003-based Telnet Server. However, in Windows Server 2003 you must configure Telnet Server options to be able to do certain functions.

For example, the following command uses the credentials of the user who is currently logged on to the client to create a Telnet connection on port 23 with a host named server01.

telnet server01

The following example creates the same Telnet connection and enables client-side logging to a log file named c:\telnet_logfile.

telnet -f c:\telnet_logfile server01

The connection with the host remains active until you exit the Telnet session (by using the **Exit** command), or you use the Telnet Server administration tool to terminate the Telnet session on the host.

For more information, see the Windows Server TechCenter at http://technet.microsoft.com/en-us/library/cc787407(WS.10).aspx.

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

PuTTY

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

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

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

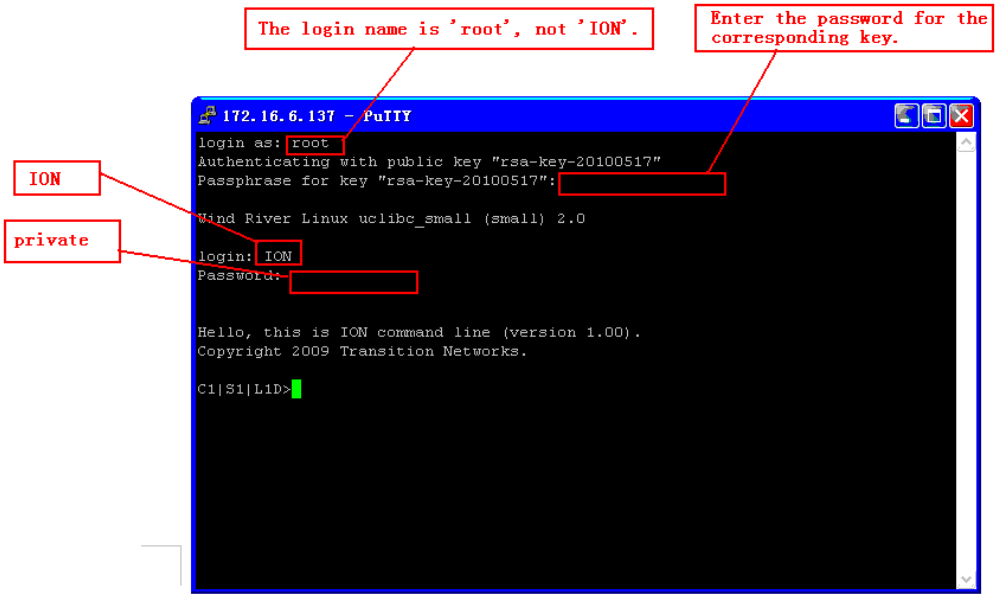
For PuTTY legal and technical details, see the PuTTY download page at http://putty.org/ or at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Note:

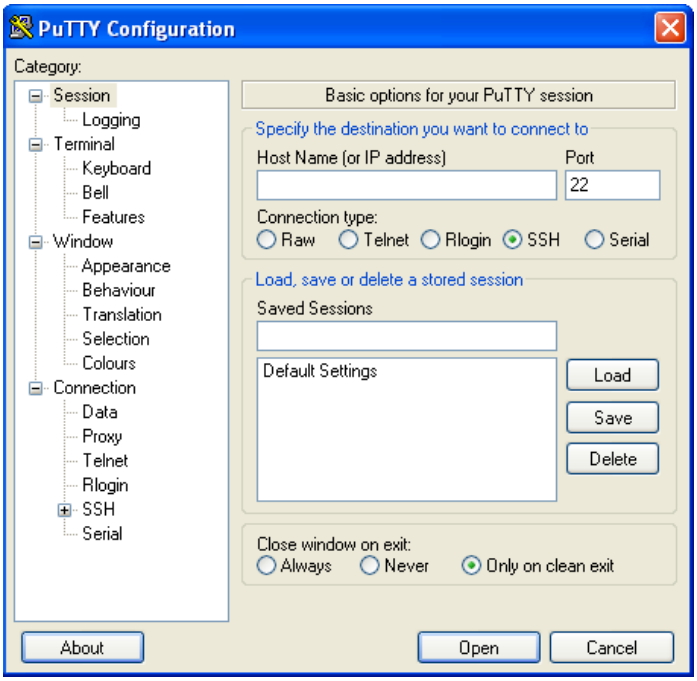
1) When the user-public key is loaded into the IONMM successfully, the key will take effect immediately; you do not need to restart the SSH server.

2) The ION system supports SSH2 keys only; SSH1 keys are not supported. When generating using puttyGen.exe, do not select the SSH1 keys.

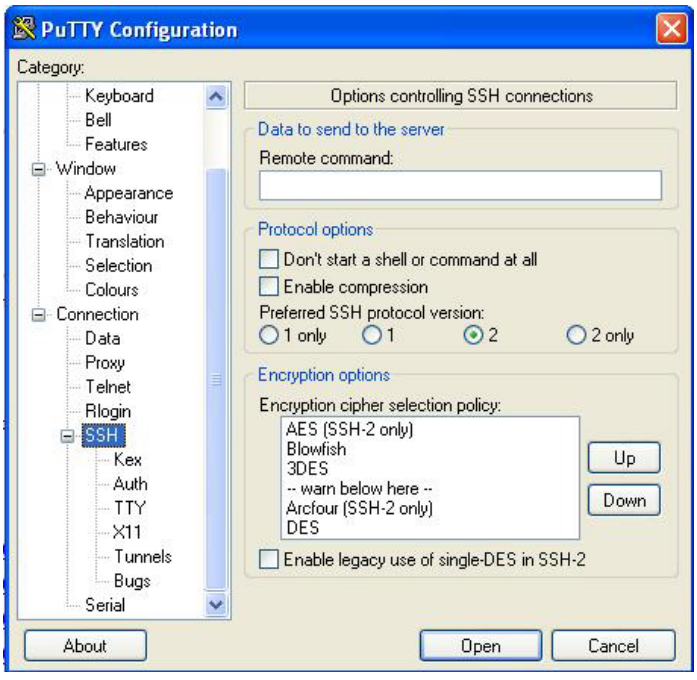
3) The ION system currently supports one user named 'root' with public key authentication.



PuTTY Basic Options:



PuTTY SSH Options:



Tracert (Traceroute)

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

Tracert is a Windows based tool that allows you to help test your network infrastructure. In this article we will look at how to use tracert while trying to troubleshoot real world problems. This will help to reinforce the tool's usefulness and show you ways in which to use it when working on your own networks.

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

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

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

Tracert options include:

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

Netstat

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

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

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

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

Winipcfg

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

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

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

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

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

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

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

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

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

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

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

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

Nslookup

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

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

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

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

1. The syntax for noninteractive mode is:

   nslookup [-option] [hostname] [server]

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

   C:\> nslookup

Default Server: nameserver1.domain.com

Address: 10.0.0.1

>

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

Notes

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

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by DHCP clients (devices) to obtain configuration information for operation in an Internet Protocol network. DHCP reduces system administration workload, allowing devices to be added to the network with little or no manual intervention.

DHCP was initially defined in RFC 1531 as a standard-track protocol in October 1993, succeeding the BOOTP. The next update was RFC 2131, which is the current DHCP definition for IPv4 networks.

DHCP automates network parameter assignment to network devices from one or more fault-tolerant DHCP servers. DHCP is useful even in small networks, because it makes it easy to add new machines to the network.

DHCP is also recommended for servers whose addresses rarely change, so that if a server needs to be readdressed (RFC 2071), changes need be made in as few places as possible. For devices such as routers and firewalls that should not use DHCP, it can be useful to put SSH servers on the same host that runs DHCP, which serves to centralize administration.

DHCP is an Internet-standard protocol by which a computer can be connected to a local network, ask to be given configuration information, and receive from a server enough information to configure itself as a member of that network. ISC DHCP is open source software that implements the Dynamic Host Configuration Protocols for connection to a local network. It is a reference implementation of those protocols, but it is also production-grade software, suitable for use in high-volume and high-reliability applications. ISC's DHCP software is the most widely used open source DHCP implementation on the Internet. See http://www.isc.org/software/dhcp.

Dr. Watson

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

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

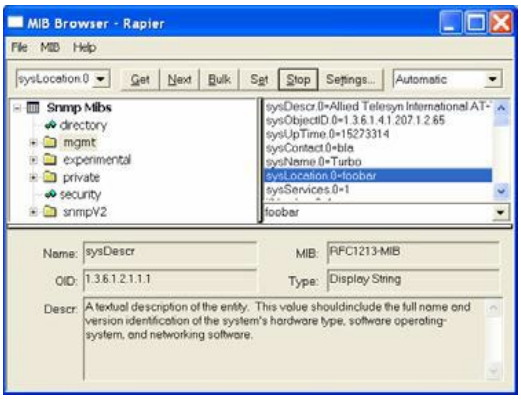
- The line *Application exception occurred*:.
- Program error information.
- System information about the user and the computer on which the program error occurred.
- The list of tasks that were running on the system at the time that the program error occurred.
- The list of modules that the program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

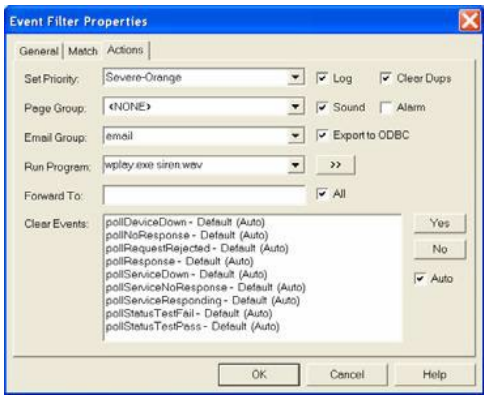
The default log file path is:
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson.

The default Crash Dump path is:
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

SNMPc

SNMPc is a secure distributed network management system that can monitor an entire network infrastructure. It lets you visualize, monitor and pro-actively manage your network. The SNMPc MIB Browser screen and the SNMPc Event Filter screen are shown below.





See the Castel Rock Computing Knowledge Base, How To Guides, and FAQs at http://www.castlerock.com/support/default.htm for more information.

HPOV (HP OpenView)

HP OpenView was the former name for a Hewlett Packard product family that consisted of network and systems management products. The main OpenView product was Network Node Manager (NNM), a network monitoring application based on SNMP. In 2007, along with integrated Mercury Interactive, Peregrine Systems and Opsware products, HP OpenView products were rebranded into HP Software & Solutions, and "OpenView" and "Mercury" names were eliminated. The HP OpenCall product remains a part of the HP Software & Solutions business. The HP Network Management Center support web site is at https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-119_4000_100.

You can access patches from the HP Software Support Online system, search for the products of interest, find Release Notes, and refer to the NNM Documentation List using your HP passport credentials at

https://ovrd.external.hp.com/rd/sign-in?TYPE=33554433&REALMOID=06-000dbac2-dc02-1680-9aa0-a14d91440000&GUID=1&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SMi%2bVqGd4Zrg0nzFPTAbCG%2fQrn0f2UZowYfT2RitHvQEb1t1qlFq3Rt65IHxgfcRnD&TARGET=SMhttp%3a%2f%2fsupport%2eopenview%2ehp%2ecom%2fselfsolve%2fmanuals.

US-CERT

The National Cyber Alert System is America's first cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. Managed by the US-CERT, the system relays computer security update and warning information to all users. It provides all citizens—from computer security professionals to home computer users with basic skills—with free, timely, actionable information to better secure their computer systems. The National Cyber Alert System provides valuable cyber security information in the form of Technical Cyber Security Alerts, Cyber Security Alerts, Cyber Security Tips, and Cyber Security Bulletins.

You can sign up to receive this information via email at https://forms.us-cert.gov/maillists/.
An example of a recent alert is at http://www.us-cert.gov/cas/techalerts/TA08-162A.html.

Third Party Tool Messages

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

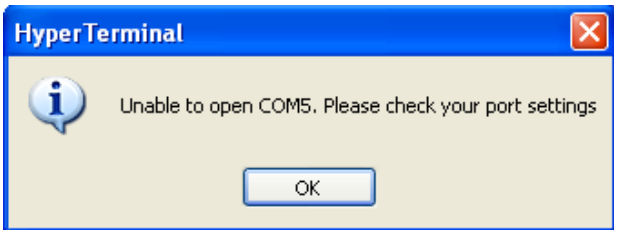
HyperTerminal Messages

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

Response:

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

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



Response:

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

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

Meaning: HyperTerminal (HT) is a terminal emulation program developed by Hillgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate

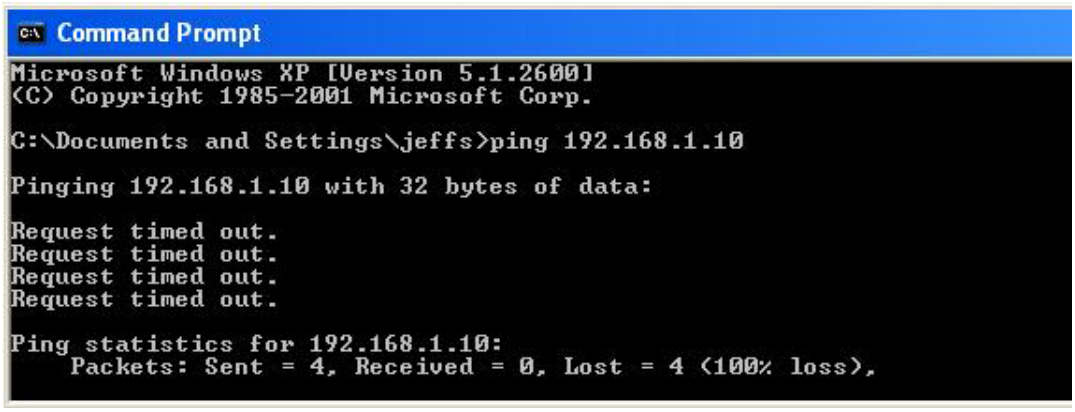
within a text entry. Overtyping an entry should automatically replace the previous characters. This is a HyperTerminal problem that the ION CLI stack cannot resolve.

Response:

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

Ping Command Messages

Message: *Request timed out*.

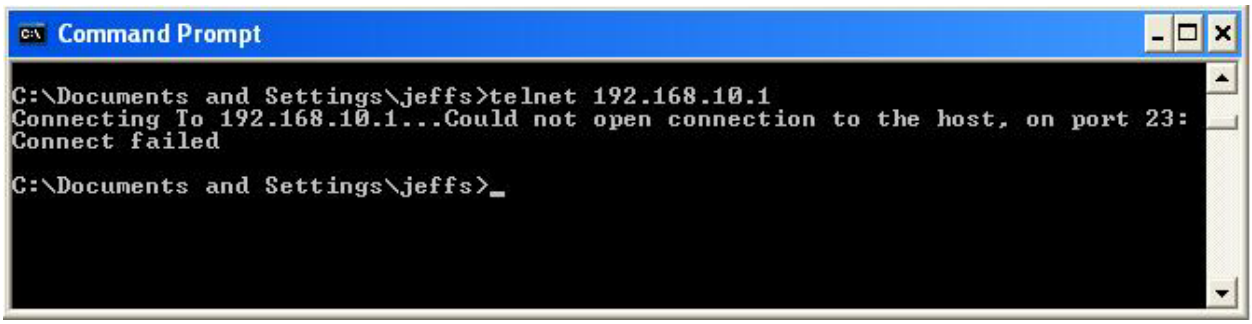


Meaning: The Ping command failed.
Recovery:

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

Telnet Messages

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

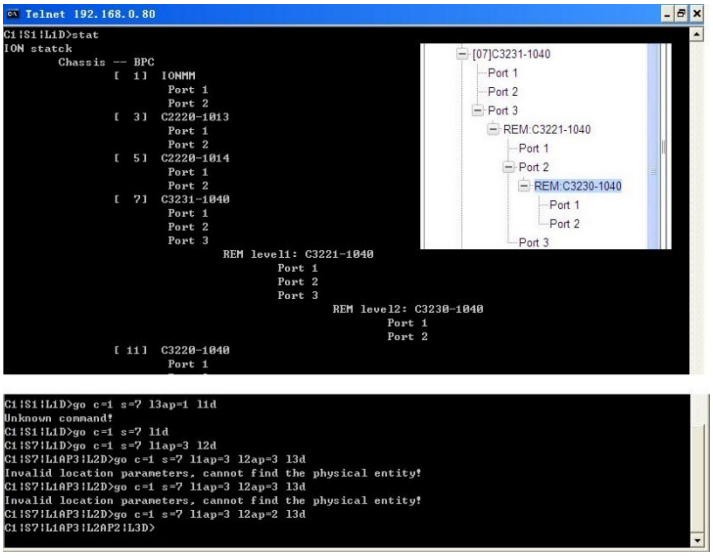


Meaning: The attempted Telnet connection failed.
Recovery:
1. Verify the physical connection, verify correct IP address entry, and retry the operation.
2. Check if the default IP address has changed using the Ipconfig (or similar) command.

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

Meaning: The **go** command you entered includes a location that does not exist or that you entered incorrectly.
Recovery:

1. Run the **stat** command to verify your configuration.
2. Click the plus sign [**+**] next to **ION Stack** to unfold the "ION Stack" node in the left tree view to refresh device status.
3. Click the plus sign [+] next to **Chassis** to unfold the chassis devices.



4. Compare the **stat** command results to the Web interface tree view configuration information.

5. Re-run the **stat** command with the correct location parameters.
6. Ping the device in question.
7. Unplug and re-plug the USB connector on the IONMM card.
8. If the problem persists, contact Technical Support.

Message: *Unknown command*!

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

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

Recovery:

1. Verify the CLI command syntax.
2. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33473*.

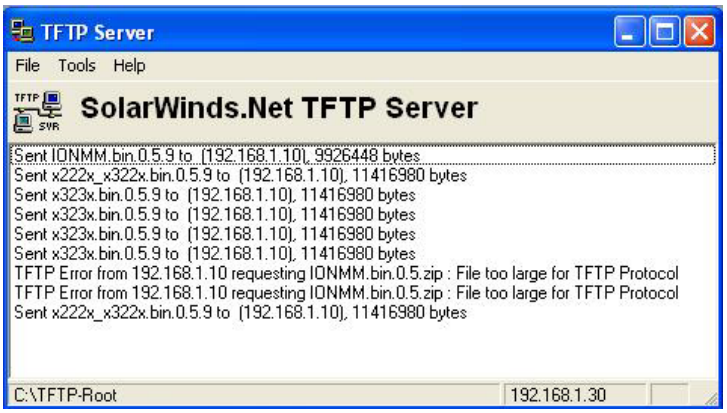
TFTP Server Messages

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

Message: *File does not exist*

Meaning: A TFTP Server error - the TFTP Server Address that you specified does not contain the Firmware File Name specified.
Recovery: 1) Verify the TFTP server's correct file location (e.g., local disk at *C:\TFTP-Root*). 2) Make sure of the filename / extension. 3) Check the TFTP Server's online helps for suggestions.

Message: *File too large for TFTP Protocol*



Meaning: A TFTP Server error - you tried to upload a file e.g., (IONMM.bin.0.5 – 50Mb) but the TFTP server failed. The file you tried to upload via the TFTP server exceeded the file size capability.
Recovery: 1) Check if some extra files ended up in the zip folder – some repeated – 6 FW files total.
2) Remove some of the files from the zip folder and try the upload again. 3) Send the remaining files in a separate file. 4) Check the TFTP Server's online helps for suggestions.

PuTTY Messages

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

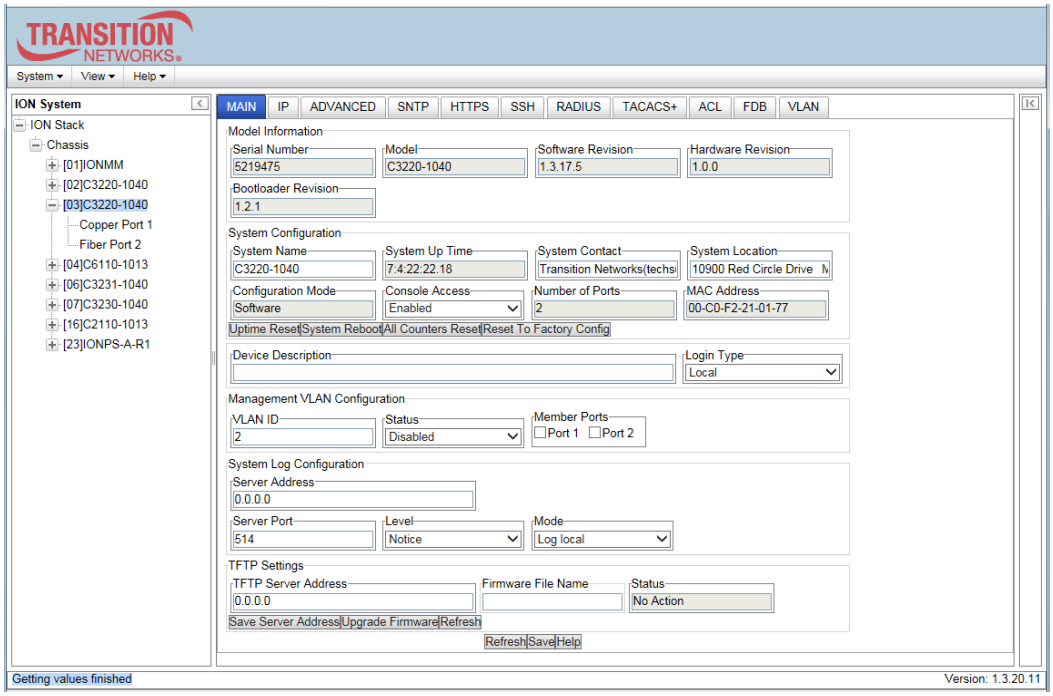
Message: *Server refused key*
Meaning: You can connect to a secure telnet session using password authentication, but when you try to connect using public key authentication, you receive a "*Server refused our key*" message on the client (PuTTy) session. For example, you generated a public/private key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

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

Recording Model Information and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible to help the Technical Support Specialist.

1. Select the device **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 loam config**, or others as requested by the Support Specialist.)



2. Record the **Model Information** for your system.

   Serial Number: _____ Model: _____

   Software Revision: _____ Hardware Revision: _____

   Bootloader Revision: _____ System Up Time: _____ ___

3. Record the **System Configuration** information for your system.

   Configuration Mode: _____ Console Access: _____

   Number of Ports: _____ MAC Address: _____

   Device Description: _____ IP Address Mode: _____

4. Provide additional Model and System information to your Technical Support Specialist. See "Basic ION System Troubleshooting" on page 370.

   Your Lantronix service contract number: _____

A description of the problem: _____

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

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

_____

_____

Any previous Return Material Authorization (RMA) numbers: _____

Appendix A. Compliance and Safety Information

Compliance Information

Standards CISPR22/EN55022 Class A, CE Mark

FCC Regulations

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own 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 Class A digital apparatus complies with Canadian ICES-003.

French: Cet appareil numériqué de la classe A est conformé à la norme NMB-003 du Canada.

European Regulations

WARNING:

This is a Class A product. In a domestic environment, this product could cause radio interference in which case the user may be required to take adequate measures.

Achtung !

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fäll ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention !

Ceci est un produit de Classe A. Dans un environment domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilsateur de prende les measures spécifiques appropriées.

In accordance with European Union Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, Lantronix will accept post usage returns of this product for proper disposal. The contact information for this activity can be found in the 'Contact Us' portion of this document.

CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.

Der Anschluss dieses Gerätes an ein öffentlickes Telekommunikationsnetz in den EG-Mitgliedstaaten verstösst gegen die jeweligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur

Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Declaration of Conformity

Manufacture's Name: Lantronics, Inc.
Manufacture's Address: 48 Discovery, Suite 250, Irvine, California 92618 USA

Declares that the products: ION x222x & x32xx multi-port NIDs
C3230-10xx, C3231-10xx, C3220-10xx, C3221-10xx, S3230-10xx,
S3231-10xx, S3220-10xx, S3221-10xx, S3221-10xx-T

Conform to the following Product Regulations:
EMC Directive 2004/108/EC; EN55022:2006+AI:2007 Class A; EN55024:1998+AI:2001+A2:2003; EN6100-2-3; EN6100-3.3; CFR Title 47 Part 15 Subpart B Class A. Low Voltage Directive; 2006/95/EC; IEC60950-I:2005; CFR Title 21 Section 1040.10 Class 1; CE Mark

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: June 20, 2023
Signature: *Eric Bass*
Full Name: Eric Bass
Position: Vice President of Engineering

MEF Certifications

Lantronix has received MEF 9, 14, and 21 certification for the x2220, x3220, x3230 and S3240 products at the time of this publication. The MEF Carrier Ethernet Certification Program is designed to ensure that global equipment and services comply with MEF standards and pave the way for interoperability.

The latest list of MEF certified Lantronix products, and the MEF certificates and test reports are available on the Lantronix Product Support webpage (no logon required).

Electrical Safety Warnings

Electrical Safety

IMPORTANT: This equipment must be installed in accordance with safety precautions.

Elektrische Sicherheit

WICHTIG: Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

Elektrisk sikkerhed

VIGTIGT: Dette udstyr skal 518nstallers i overensstemmelse med sikkerhedsadvarslerne.

Elektrische veiligheid

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

Sécurité électrique

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

Sähköturvallisuus

TÄRKEÄÄ : Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

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

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal 518nstallers 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 Defaults

The x222x / x32xx *Device* Level Factory Defaults are shown in Table 32 below.
The x222x / x32xx *Port* Level Factory Defaults are shown in Table 33.

Device-Level Factory Defaults

Note: The default settings shown are as seen in the tabs/fields of the Web interface.

Table 32: 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., C3220-1040) Software Revision: FW vs. dependent (e.g., 1.3.17) Hardware Revision: HW vs. dependent (e.g., 0.0.1) Bootloader Revision: BL vs. dependent (e.g., 1.2.0)
System Configuration	System Name: C2220-1040 System Contact: Lantronix (techsupport@tn.com) System Location: 10900 Red Circle Drive Console Access: Enabled
Device Description	blank
DNS x	0.0.0.0
VLAN ID	0
Status	Disabled
Member Ports	none checked
SNMP Version	v1/v2c

Trap Manager x	0.0.0.0
System Log Configuration (Syslog)	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
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
Advanced Tab	
FDB Aging Time	300
MAC Address Learning	Port 1 and Port 2 unchecked
Transparent LPT	Disabled
Selective LPT	Disabled
Monitoring Port	Port 2
Redundancy Primary Port Secondary Port	Enabled Port 1 Port 2

Active Port	Port 1
IEEE Priority Class	Remap → To 0 → PID 0 1 → PID 0 2 → PID 1 3 → PID 1 4 → PID 2 5 → PID 2 6 → PID 3 7 → PID 3
IP Traffic Class	Remap → To 0 – 15 → 0 16 – 31 → 1 32 – 47 → 2 48 – 63 → 3
SNTP Tab	
SNTP Client	Disabled
UTC Timezone	(GMT-06:00)Central Time (US & Canada)
Daylight Saving Time	Disabled
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
SSH Auth Timeout	60
SSH Auth Retries	3
Public-Key of Host	RSA: 00.00.00.07. ... B0.44.AB.F0.79 DSA: 00.00.00.07. ... 3C.00.4A.1F.89
Host Key Type	No Gen
Save Host-Key to Flash	**Save** (not configurable)
Public-Key of User	RSA: blank DSA: blank
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	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	none
Priority	blank
Policy	Accept
Trap Rate	0
Conditions	none

Type	Source MAC Address
Source or Destination	Source
Operation	Equal
Value	blank
FDB Tab	
VLAN ID	0
MAC Address	blank
Conn Port	Port 1
Priority	blank
Flush Operation Flush Status Failure Reason	Flush All blank blank
Entry Type	static
VLAN Tab	
VLAN ID	blank
FDB ID	0
Priority Override	Disabled
Priority	0
Member Tag Port 1	NoMod
Member Tag Port 2	NoMod
Member Tag Port 3*	NoMod

Flush Operation Flush Status Failure Reason	Flush All blank 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

Port-Level Factory Defaults

Note: The default settings shown are as seen in the tabs/fields of the Web interface.

The x222x / x32xx *Device* Level Factory Defaults are shown in Table 32 above.
The x222x / x32xx *Port* Level Factory Defaults are shown in Table 33 below.

Table 33: Port-Level Factory Defaults

Item/Field	Default Setting
Main Tab	
Circuit ID	blank
Link Status	Down
Admin Status	Up
Speed Duplex	Negotiating Negotiating
Port Mode (Port 1)	1000BaseX
Port Admin Mode (Port 2)	100BaseFX
AutoCross Mode	Auto
MAC Address	00-C0-F2-42-00-E0
Connector Type	RJ-45 (Port 1) SFP slot (ports 2 and 3)
Auto Negotiation	Enabled
Force Speed Force Duplex	100Mbps Full Duplex
Capabilities Advertised	All speed/duplex boxes checked Pause and Asymmetric Pause boxes unchecked
Pause Admin Mode (Port 2) Pause Oper Mode	Disabled Disabled

Control Functions Supported	None
Source Port Forward Settings	2 All boxes checked
Loopback Type	Alternate
Clear Counters	Do Nothing
L2CP Disposition	All set to “Pass”
TN Topology Discovery Protocol TX	Enabled
Virtual Cable Test	No records found
Advanced Tab	
Rate Limiting Mode	Counts All Layer 1
Egress Rate Limit	Unlimited
Ingress Rate Limit	Unlimited
SA Lock	Disabled
SA Lock Action	Discard and Notify
Filter Unknown Multicast	Disabled
Filter Unknown Unicast	Disabled
VLAN Status	Disabled
Discard Tagged	Disabled
Discard Untagged	Disabled
Force Default VLAN	Disabled

Default VLAN ID	2
Default Priority	0
IEEE Priority Class	Enabled
IP Traffic Class	Enabled
Priority Precedence	Use IEEE
SA Priority Override	Disabled
DA Priority Override	Disabled
VID Priority Override	Disabled
Pause Admin Mode	Disabled
User Priority	Remap → To 0 → 0 1 → 1 2 → 2 3 → 3 4 → 4 5 → 5 6 → 6 7 → 7
LOAM Tab	
Main Sub-Tab	
Admin Status	Disabled
Operational Status	Link Fault
LOAM Mode	Passive
Max PDU Size	1500

Configuration Revision	1
Functions Supported	None / Loopback, Event Notification
LOAM Peer Information	MAC Address: 00-00-00-00-00-00 Vendor OUI: 00:00:00 Vendor Info: 0 LOAM Peer Mode: Unknown Max PDU Size: 0 Configuration Revision: 0 Functions Supported: None
Loopback Type	Alternate
Loopback Status	No Loopback
Ignore Loopback Request	Enabled
Event Configuration Sub-Tab	
Error Symbol Period Window High Bits	0
Error Symbol Period Window Low Bits	125000000
Error Symbol Period Threshold High Bits	0
Error Symbol Period Threshold Low Bits	0
Error Symbol Period Event Notification	Enabled
Error Frame Period Window	0
Error Frame Period Threshold	0
Error Frame Period Event Notification	Enabled

Error Frame Window	0
Error Frame Threshold	0
Error Frame Event Notification	Enabled
Error Frame Seconds Summary Window	0
Error Frame Seconds Summary Threshold	0
Error Frame Seconds Event Notification	Enabled
Dying Gasp	Enabled
Critical Event	Enabled
Event Log Sub-Tab	
Event Log	No record found.

Switch Mode Default: By default, the x222x / x32xx is managed by the IONMM. Setting the mode to local indicates that the device is not managed by the IONMM but either a direct USB connection or a direct network connection via Telnet or the Web interface. Setting the mode to remote indicates that the device is managed through the IONMM. See the **switch mode** command for details.

Appendix C. Configuration Quick Reference – CLI

IPv4 Configuration

1. Define IP address and subnet mask.

   set ip type={ipv4 | dns} **addr=**<ipaddr> **subnet–mask =**<subnet>

2. Define the IP address mode.

   set ip address mode={bootp|dhcp|static}

2. Define default gateway.

   set gateway type={ipv4 | dns} **addr=<**gway>

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 index=<inum> **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 and Restore

1. Show provision modules.

   show prov modules

2. Set Backup Module Configuration.

   set backup module-index=<1-256>

3. Set Restore Module Configuration.

   set restore module-index=<1-256>

4. Backup module list.

   backup module-list=<1-10>

5. Restore module list.

   restore module-list=<1-10>

6. Show provision 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. Access the x222x/x32xx via either a USB connection or a Telnet session.
2. Check the current Management VLAN configuration. Type **show mgmt vlan config** and press **Enter**.

   Note: In the following steps to enable Management VLAN, the first is at the port level, the other steps are at the device level. These steps must be performed in the order shown.

3. Change the Management port from the default “Customer” mode to “Network” mode.
   Type **set port vlan tag mode=network** and press **Enter**.
4. Set this port as Management port; enter the ports to be associated with this VLAN ID (VID).
   Type **set mgmt vlan port=2** and press **Enter**.
5. Enable Management VLAN mode. Type **set mgmt vlan state=enable** and press **Enter**.
6. Change the Management VID. Type **set mgmt vlan vid=10** and press **Enter**.
7. Add a VLAN. Type **add vlan vid=10** and press **Enter**.
8. Other Management VLAN or Port VLAN attributes can be changed without strict order.
   See “Configuring Management VLAN” on page 272.

RADIUS Configuration

1. Define the RADIUS server.

   set radius svr=<index> **type**={ipv4 | 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>

SNTP Configuration

1. Enable SNTP.

   set sntp state=enable

2. Set the current time.

   s**et curr–time=<“**time**”>**

3. Define your timezone.

   set sntp timezone=<zone>

4. Enable daylight savings time (DST).

   set sntp dst–state=enable

5. Define DFST 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>

Fiber Port Redundancy Configuration

1. Set the Redundancy state to enable.

   set redundancy state=<state>

2. Verify the configuration has been set.

   show redundancy config

Syslog Configuration

1. Define the Syslog server port.

   set syslog svr port=<1-65535>

2. Set the Syslog operating mode.

   set syslog mode=<local|remote|localAndRemote|off>

3. Set the level of Syslog operation.

   set syslog level=<emerg|alert|crit|err|warning|notice|info|debug)>

4. Set the Syslog server type and address.

   set syslog svr type=<ipv4|ipv6|dns> **add**r=<ipaddr>

System (Login) User Configuration

1. Create a new system user.

add sysuser name=NAMESTR **level**=<admin|read-write|read-only> **pass**=PASSSTR confirm**pass**=PASSSTR

2. Edit an existing user's access level.

   set sysuser name=NAMESTR **level**=<admin|read-write|read-only)>

3. Set a new password for an existing ION system user.

   set sysuser name=NAMESTR **pass**=PASSSTR **confirmpass**=PASSSTR

4. Remove an existing system user.

   remove sysuser name=NAMESTR

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

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**.

Appendix D. VLAN Tunneling Configuration Examples

This appendix provides sample VLAN configurations using both the CLI method and the Web method.

There are four different VLAN properties for a port configured in a VLAN entry at the ION System Level in the VLAN database:

1) **NoMod**: the frame maps to this VLAN egress unmodified out on this port (frame maps to a VLAN ID when it ingresses a port, the VLAN id is mapped based on either the existing VID if it is already tagged or the port default VLAN ID if untagged).
2) **Tag**: the frame maps to this VLAN egress tagged out on this port.
3) **UnTag**: the frame maps to this VLAN egress untagged out on this port.
4) **notMember**: frame maps to this VLAN will not be forwarded out on this port.

The ports can be configured in one of three Frame Tag modes:

1) **Customer**: this is VLAN unaware mode. This means that if a VLAN entry has this port member property as memegressTag or Untag.
2) **Network**: enables Dot1.Q Mode. Whenever tagging/untagging is required, all of the participating ports must be configured as Network. This includes the port that is facing the untagged traffic as well.
3) **Provider**: (Provider EtherTypes 8100, 9100, X88A8) - this mode will ensure that the frame egressing this port will always have the S-Tag added, regardless of whether the ingress frame was already C-Tagged (Case E) or plain untagged (Case B).

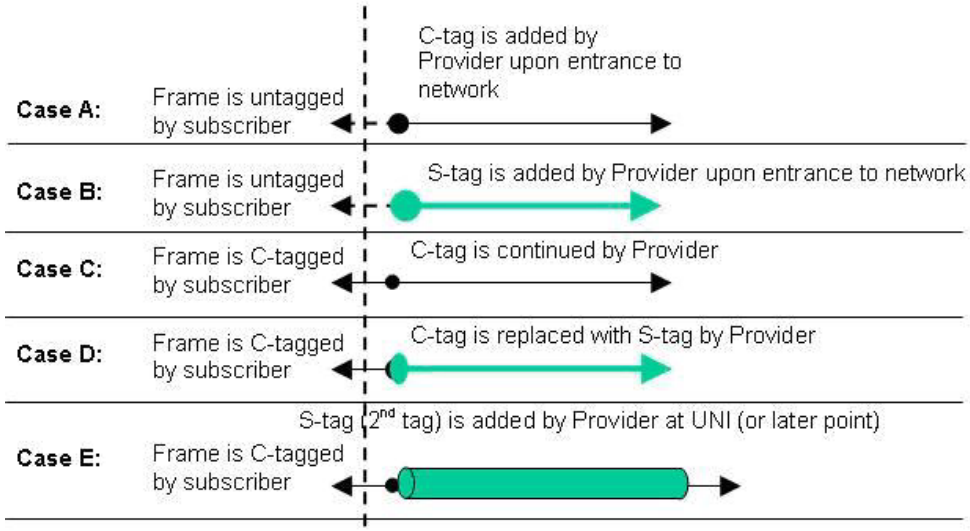


Figure D-1: VLAN Tagging Example

In the ION system, VLAN Tunneling can be configured using either the CLI or Web method.

VLAN Tunneling Config – CLI Method

See the "*ION Systems CLI Reference Manual – 33461*" for the various VLAN commands (Management VLAN, Device-level, and Port-level VLAN commands). Certain commands can only be entered when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D). Not all of the steps (CLI commands) below are required for each possible VLAN configuration. **Note**: VLAN 1 is the default VLAN and you cannot Edit or Delete it.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Add a VLAN Database Entry. This adds a new VLAN to the device. By default, VLAN ID one (VID 1) is defined for internal use. Type:
   add vlan–db vid=<xx> [priority=<yy>] [pri–override={enable | disable}]
   where:
   xx = ID (2–4094) of the VLAN to which the device is to become a member
   yy = optional; priority for frames
3. Set the VLAN Database Member/Egress Tagging. This sets the priority of a row of the VLAN forwarding database. Type:
   set vlan-db vid=<xx> port=<yy> ETag=<zz>
   set vlan-db vid= <xx> fid=<yy> pri-override=<aa> priority=<bb>
   Where:
   ww = dot1bridge MAC address
   xx = number that identifies the VLAN (1–4094)
   yy = logical port index or fid
   zz = valid memetag choices are:
   - noMod
   - unTag
   - Tag
   - notMember

   aa = pri-override={enable | disable}
   bb = priority = {0-7}
4. Press **Enter**.
5. Set the Management VLAN admin state to enable. Type:
   set mgmt vlan state=enable
6. Press **Enter**.
7. Select the management VLAN ports. Type:
   set vlan mgmt vlan port=port-list
   Where:
   Port-list = a management VLAN port (1-19)
   Example: C1|S13|I0d/>**set mgmt vlan port=2,4,5**
8. Press **Enter**.
9. Set the port discard untagged non-management frames option to true if untagged non-management frames are to be discarded for this port. Type:
   set port discard-untagged=truth-val
   Where:
   Truth-val = true or false
   Example: C1|S13|I0ap1|I1p2/>**set port discard-untagged=true**
10. Press **Enter**.

11. Set the port discard tagged non-management frames option to true if the tagged non-management frames for this port are to be discarded. Type:
    set port discard-tagged=truth-val
    Where:
    Truth-val = true or false
    Example: C1|S13|l0ap1|l1p2/>**set port discard-tagged=true**
12. Press **Enter**.
13. Set the port default VLAN-ID for this port. Type:
    set port default-vid=vid
    Where:
    vid = 2 - 4094
    Example: C1|S13|l0ap1|l1p2/>**set port default-vid=2**
14. Press **Enter**.
15. Set if force port to use default VLAN-ID. If set to true, this forces all untagged and 802.1Q tagged frames to assume the default VLAN-ID. Type:
    set port force-default-vid=truth-val
    Where:
    Truth-val = true or false
    Example: C1|S13|l0ap1|l1p2/>**set port force-default-vid=true**
16. Press **Enter**.
17. Set the port VLAN tag mode of a port interface. Type:
    set port vlan tag mode=tagmode
    Where:
    tagmode = **network**, **provider**, or **customer**
    Example: C1|S13|l0ap1|l1p2/>**set port vlan tag mode=provider**
18. Press **Enter**.
19. Set Ethernet type if the VLAN tagging mode was set to ***provider*** in step 19.
    Type:
    set port vlan tag provider ethtype=type
    Where:
    ethtype = x8100, x88a8, or x9100
    Example: C1|S13|l0ap1|l1p2/>**set port vlan tag provider ethtype=x8100**
    OR:
    Set network tagging if the VLAN tagging mode was set to ***network*** in step 19. Type:
    set port vlan tag network tagging=tagtype
    Where:
    tagtype = **unmodified**, **removeTag**, or **addTag**
    Example: C1|S13|l0ap1|l1p2/>**set port vlan tag network tagging=addTag**
25. Press **Enter**.
26. Add a new row in the VLAN forwarding database. Type:
    add vlan-db vid=vlan-id **[pri-override=**override**] [priority=**prio**]**
    Where:
    vlan-id = 1-4094
    override = enable or disable
    prio = the priority for frames (0-7)
    Example:
    C1|S13|l0ap1|l1p2/>**add vlan-db vid=3 pri-override=enable priority=1**
27. Press **Enter**.

28. Set the priority override of a VLAN forwarding database row. This sets the override priority on frames associated with this VID of VLAN forwarding database. Type:
    set vlan-db vid=vlan-id **fid=**fid **pri-override=**override
    Where:
    vlan-id =1-4094
    fid = 0
    override = enable or disable (specify if override priority on frames enabled in step 26)
    Example:
    C1|S13|l0ap1|l1p2/>**set vlan-db vid=3 fid=0 pri-override=enable**
29. Press **Enter**.
30. Set the priority of a VLAN forwarding database row. Type:
    set vlan-db vid=vlan-id fid=fid priority=prio
    Where:
    vlan-id = 2-4094
    fid = 0
    Prio = priority for frames (0-8)
    Example: C1|S13|l0ap1|l1p2/>**set vlan-db vid=3 fid=0 priority=2**
31. Press **Enter**.
32. Set the member and egress tagging of a VLAN forwarding database row. Type:
    set vlan-db vid=vlan-id **port=**port-id **memetag=**memetag_mode
    Where:
    vlan-id = 1-4094
    port-id = logical port index
    Memetag_mode = noMod, unTag, Tag, or notMember
    Example:
    C1|S13|l0ap1|l1p2/>**set vlan-db vid=3 port=2 memetag=ETag**
33. Press **Enter**.
34. Use the CLI commands to verify your VLAN configuration(s).
    - Show all existing VLAN(s) on the NID. Type **show vlan** and press **Enter**. For example:

      C1|S13|L0D/>**show vlan mac=00:23:a2:3d:12:01**

      vid fid priority p-override port1 port2 port3
      ---
      1 0 0 disable NoMod NoMod notApp
    - Show the Management VLAN configuration. Type **show mgmt vlan config** and press **Enter** to show the management VLAN configuration on a device. Example:

      C1|S13|l0d/>**show mgmt vlan config**

      vlan id vlan state vlan portlist
      ---
      0 enable none
    - Show the VLAN Service Management configuration on a device. Type **show vlan service** and press **Enter**. Example:
    - C1|S13|l0d/> **show vlan service**

```
VLAN service connection type:                customerProvider
VLAN service VID for tag:                    8
VLAN service Ethernet Type for tag:    0x8100
VLAN translation type:                       untagged to untagged
```

- Show the Port VLAN configuration. Type **show port vlan config** and press **Enter**. For example:

```
C1|S13|l0ap1|l1p2/>show port vlan config

Dot1q state:              vlanEnabled
Discard-tagged:           false
Discard-untagged:         false
Default VLAN id:          22
Force use default VLAN id:    false
```

- Show the Port VLAN Tag configuration. Type **show port vlan tag config** and press **Enter**. For example:

```
C1|S13|l0ap1|l1p2/>show port vlan tag config
Tagging mode:         network
Network tagging:      addTag
```

- Show the VLAN forwarding database configuration for the device. Type **show vlan-db config** and press **Enter**. For example:

```
C1|S16|L1D>show vlan-db config

vid:1     fid:0     priority:0       priv_override:disable
port1:   NoMod            port2: NoMod
vid:100   fid:0     priority:0       priv_override:disable
port1:              notMem          port2: notMember
```

35. Click the **Add** button to add the recently-defined VLAN.
36. Verify the configuration. Type **show vlan service** and press **Enter**. For example:

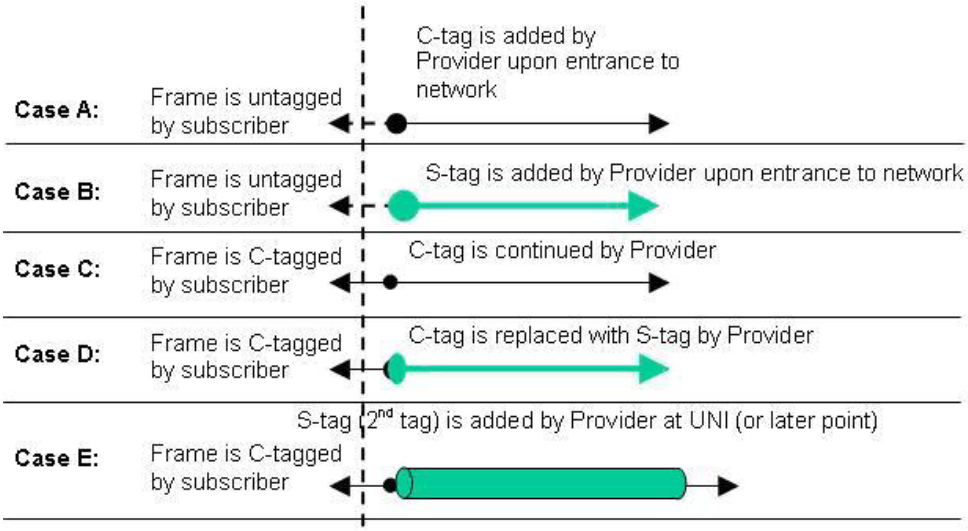
```
C1|S16|L1D>show vlan service
VLAN service connection type:        customerProvider
VLAN service VID for tag:            0
VLAN service Ethernet Type for tag:    0x0
VLAN translation type:               noTranslation
C1|S16|L1D>
```

37. You can use the **Refresh** button to clear the entry fields.
    You can use the **Edit** button to modify the configuration of an existing VLAN; click to highlight the existing VLAN in the table first.
    You can use the **Delete** button to remove an existing VLAN from the database click to highlight the existing VLAN in the table first.

VLAN Tunneling Config – Web Method

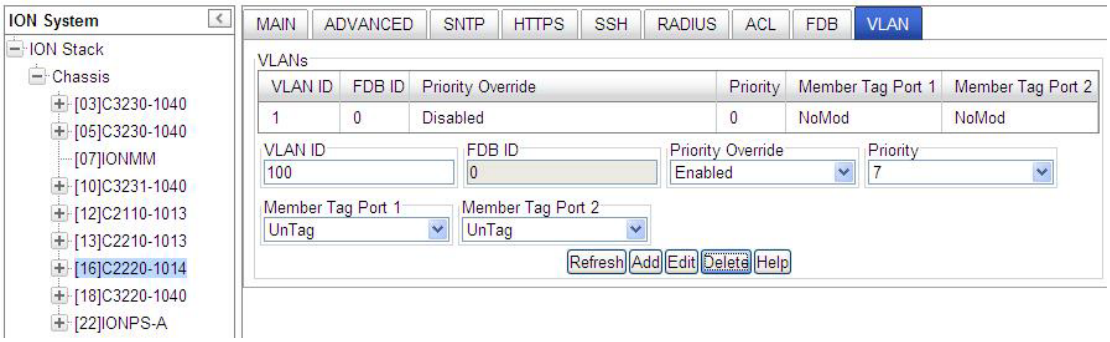
Configuring VLAN 100 with Provider S-Tag

This procedure is used to configure an untagged customer VLAN (e.g., VLAN 100) on C322x and x222x / x32xx models and how to add an S-Tag (x88A8) by the Provider once the packet enters the network, based on Case B in the graphic below.

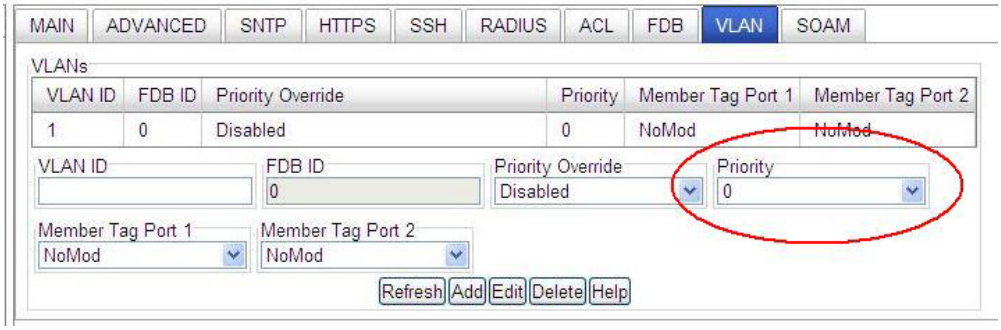


Not all of the steps below are required for each possible VLAN configuration. **Note**: VLAN 1 is the default VLAN and you cannot Edit or Delete it.

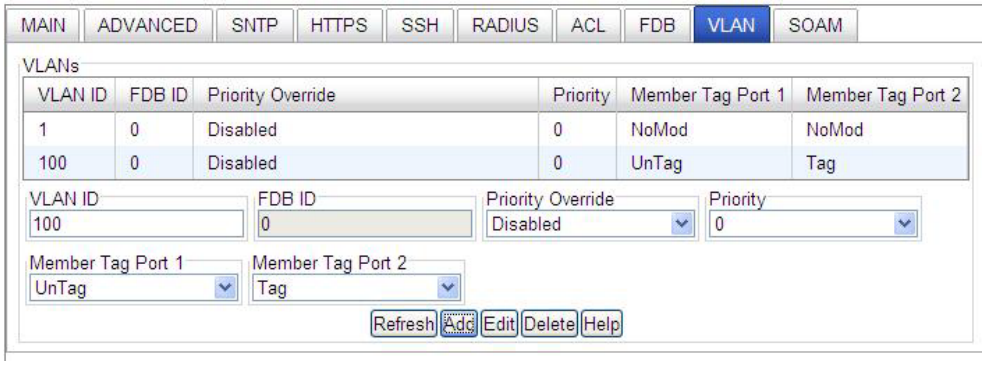
1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the **VLAN** tab.



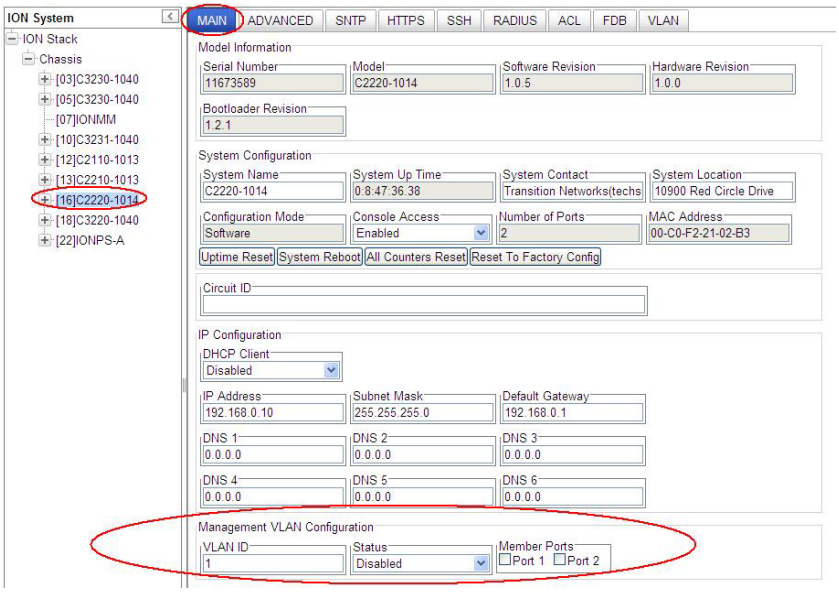
3. Enter the **VLAN ID** (e.g., **VLAN 100**) into the VLAN ID field.
4. Set **Member Tag Port 1** to ***Untag*** and set **Member Tag Port 2** for ***Tag***. (On the S3231 model, set **Member Tag Port 3** to ***Tag***.)
5. In the **Priority Override** field, select **Enabled** or **Disabled**.
6. In the **Priority** field, select **0** – **7**. The frame's priority is remapped to this value. Frames that egress tagged will have this remapped priority. Priority 0 is the lowest priority selection.



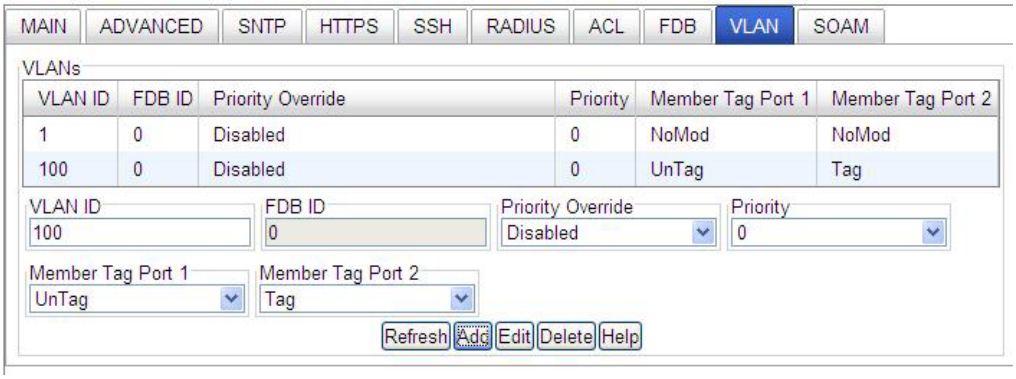
7. Click the **Add** button.
   The new VLAN ID (100) is added.



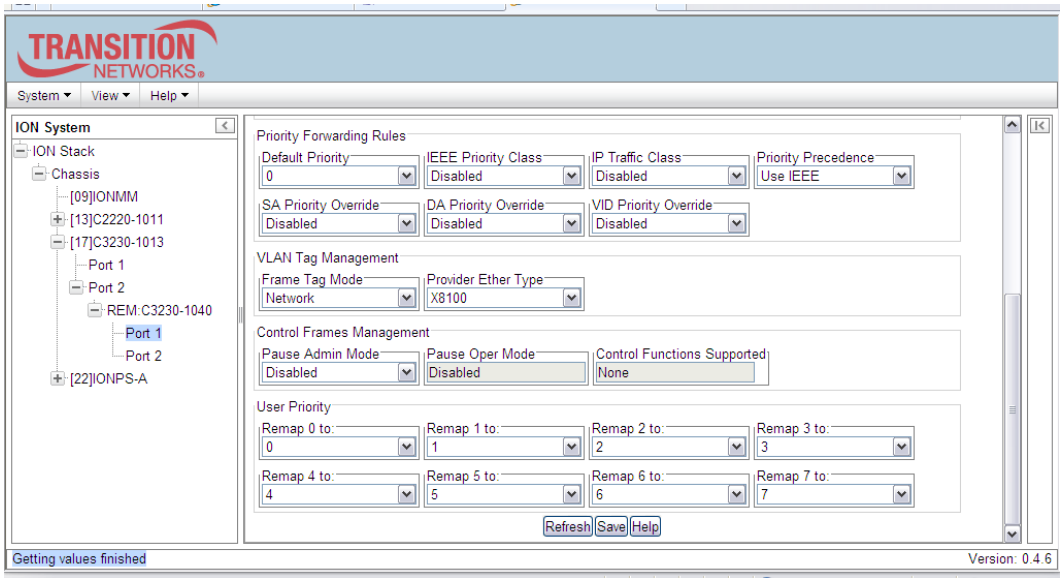
8. Select the **MAIN** tab and locate the **Management VLAN Configuration** section.



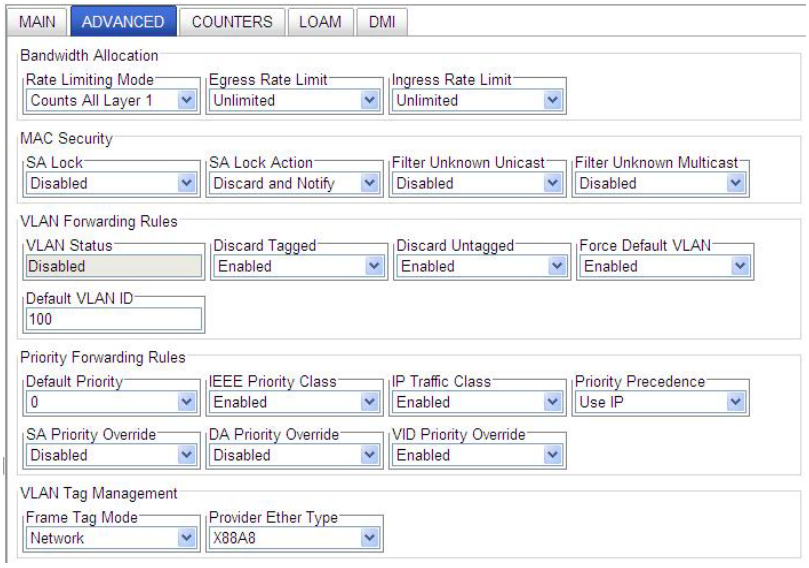
9. In the **VLAN ID** field enter ***100***. In the **Status** dropdown, select ***Enabled***.
10. In the **Member Ports** section, check the **Port 1** and **Port 2** checkboxes.
11. Repeat steps 1 - 10 above for the C322x NID, if applicable, and then click the **Add** button.
    The message "*Adding VLAN succeeded*" displays, and the new VLAN 100 is added to the VLANs table.



12. Go to REM S3230-1040 NID, select **Port 1**, and click on the **ADVANCED** tab.



13. In the **VLAN Tag Management** section, set **Frame Tag Mode** to ***Network***, set **EtherType** to ***X88A8***, enter the default **VLAN ID** (***100***), and then click the **Save** button.

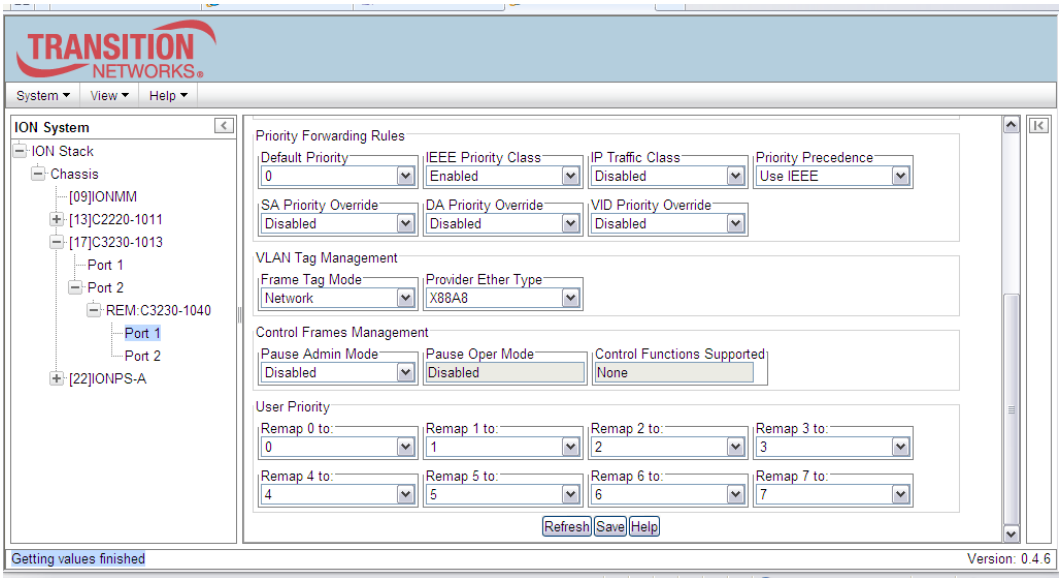


14. In the **VLAN Forwarding Rules** section, set **Discard Tagged**, **Discard Untagged** and **Force Default VLAN** to **Enabled** or **Disabled**.

    Discard Tagged filters all tagged non-management frames ingressing this port. All untagged and priority tagged frames are processed as normal frames.

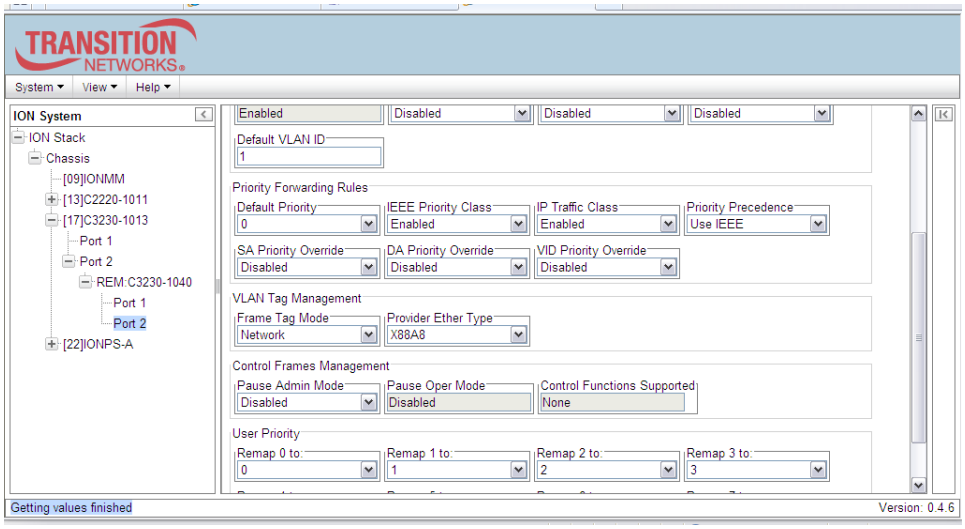
    Discard Untagged filters all untagged and priority tagged non-management frames ingressing this port. All 802.1Q tagged frames are processed as normal frames.

    Force Default VLAN forces all untagged and (802.1Q) tagged frames to take up the interface's Default VLAN ID.



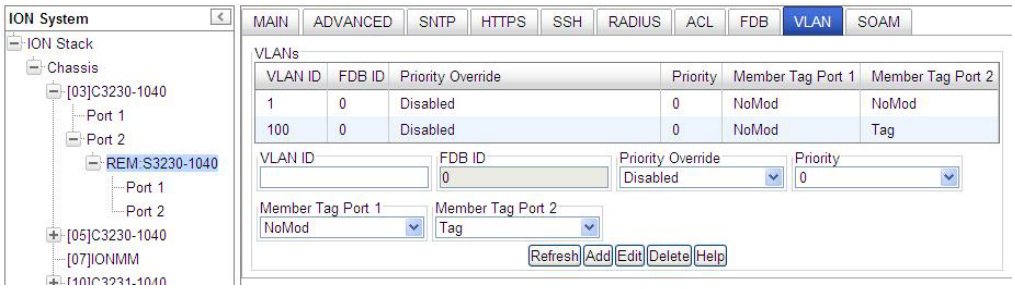
15. Go to Port 2 of REM x222x / x32xx and select the **ADVANCED** tab

16. In the **VLAN Tag Management** section, set **Frame Tag Mode** to ***Network***, set **EtherType** to ***X88A8***, and then click the **Save** button.



17. Repeat Steps 2 through 16 above on the C322x NID, if applicable.

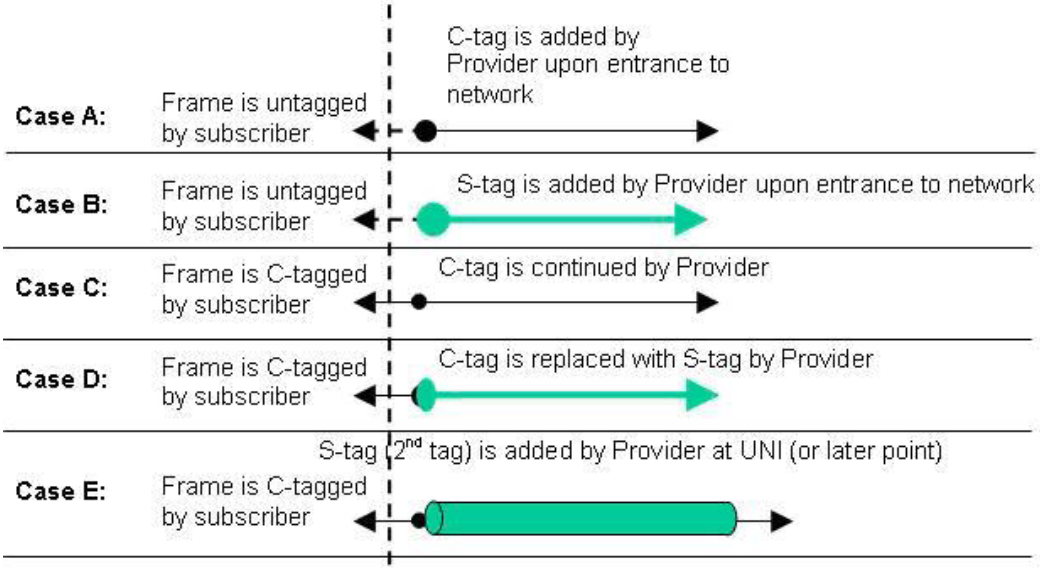
18. Verify that VLAN 100 is correctly set up in the VLAN Database with **Port 1** set to "***Untag***" and **Port 2** set to "***Tag***".



19. When VLAN 100 is correctly set up, click the **Save** button.
20. You can use the **Refresh** button to clear the current entry data.
21. To make changes to an existing VLAN table entry, select the VLAN in the table to highlight it, and then click the **Edit** button. **Note**: VLAN 1 is the default VLAN and you cannot Edit or Delete it.
22. To remove an existing VLAN table entry, select the VLAN in the table to highlight it, and then click the **Delete** button. The selected VLAN entry is deleted.

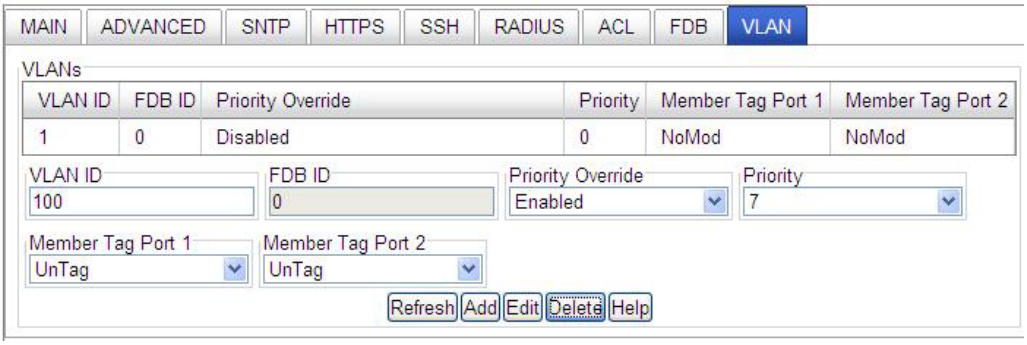
Configuring a VLAN with C-Tags and S-Tags

This procedure is used to configure customer and service provider tags (EtherType x88A8) using case studies B and E below simultaneously.



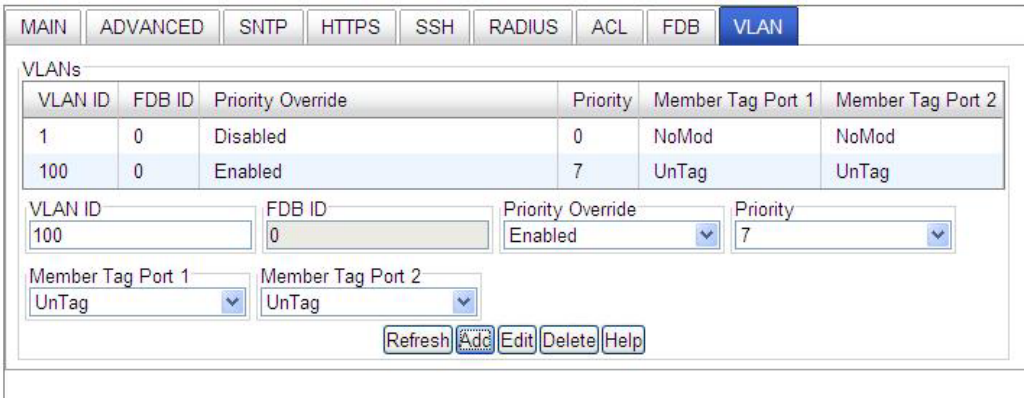
The procedure below is used to configure VLAN C-Tags and S-Tags.

1. Select the REM-S323x device and then select the **VLAN** Tab.

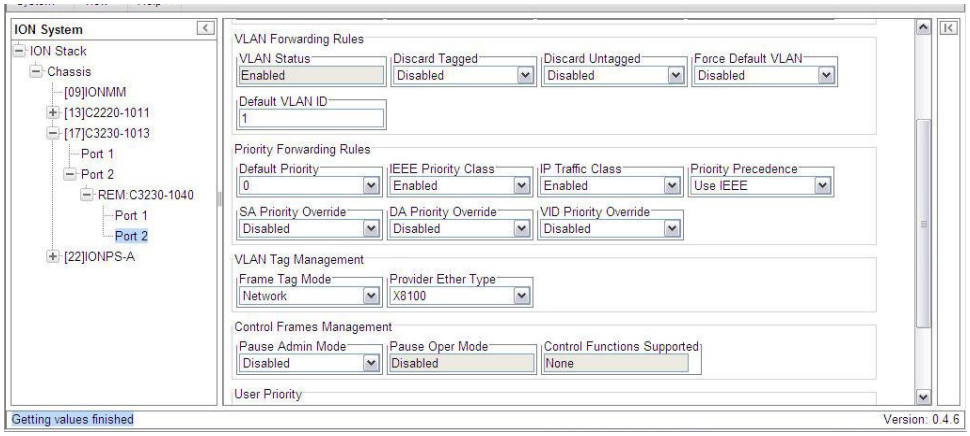


2. Add a new **VLAN ID** in the **VLANs** section:
   a. Enter **VLAN ID** =***100***.
   b. Set **Member Tag Port 1** to ***NoMod***.
   c. Set **Member Tag Port 2** to ***NoMod***.
   d. Click the **Add** button.

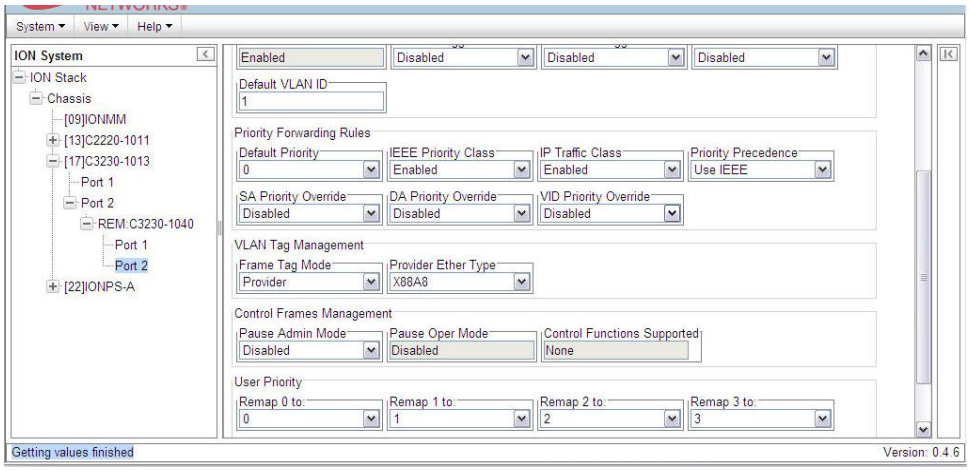
The new VLAN ID 100 displays in the VLANs table:



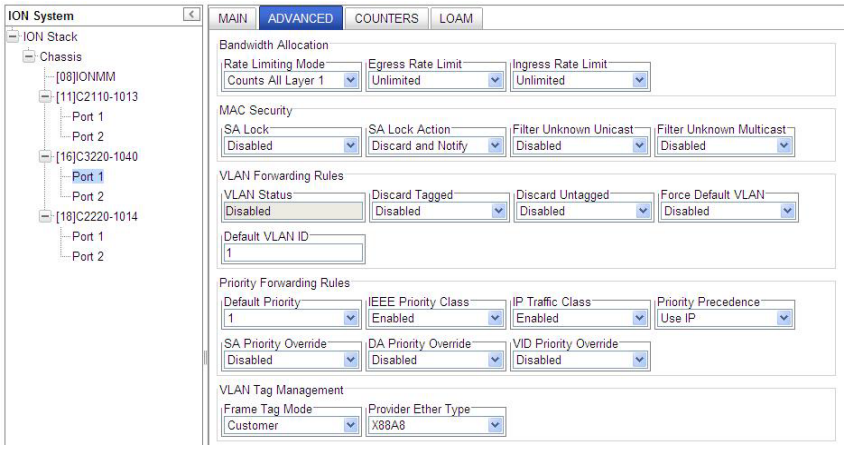
3. Go to REM S3230-1040, Port 2 and click on the **ADVANCED** tab, and configure the "Provider Port" under port level config in the **VLAN Tag Management** section.



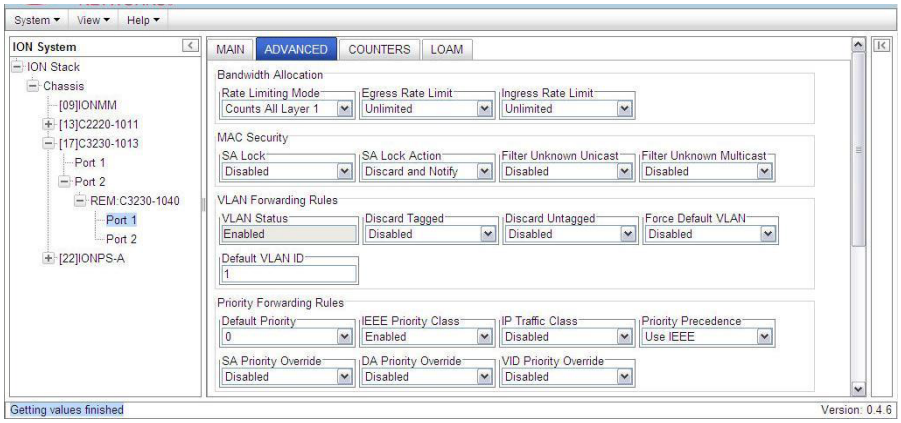
4. Set the **Frame Tag Mode** to ***Provider***, set the **EtherType** as ***x88A8***, and click the **Save** button.



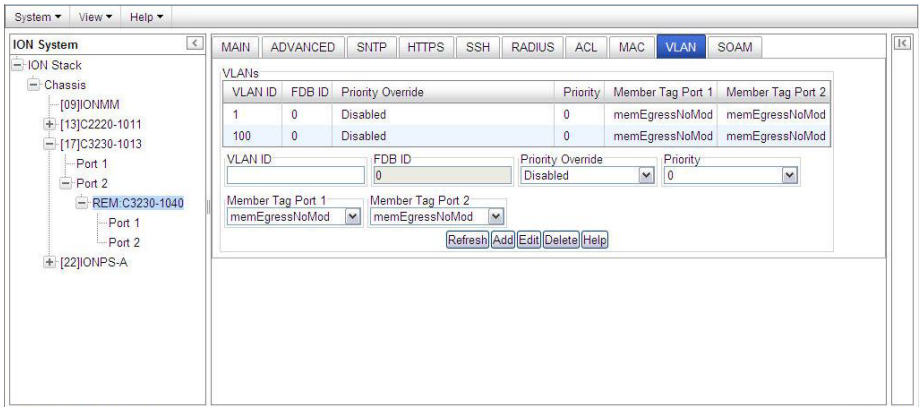
5. Go to REM S3230-1040, Port 1 and click on the **ADVANCED** tab.



6. Configure the "Customer Port" under port-level configuration. In the **VLAN Tag Management** section in the **Frame Tag Mode** field, select ***Customer***.
7. In the **Provider Ether Type** field, select ***x88A8***.



8. Select REM-C323x, select the **VLAN** tab, and verify the VLAN database configuration.



Verify:

a. **VLAN ID** =***100***.
b. **Member Tag Port 1** set to ***NoMod***.
c. **Member Tag Port 2** set to ***NoMod***.
d. **Member Tag Port 3** for ***NoMod***. (S3231 model only).

Configuring Q-in-Q (Provider Tagging)

The ION system supports Q-in-Q service, where a frame may contain one or more tags. Complete IEEE802.1ad support is not supported, but provider tags can be added or stripped on a per-port basis. There are different cases for VLAN service translation, providing options for dealing with C-Tags and S-Tags. Using IEEE 802.1Q-in-Q frames is an effective way to construct Layer 2 tunnels, apply QoS policies, etc.

The figure below illustrates tagging options that exist for using C-Tags and S-Tags.

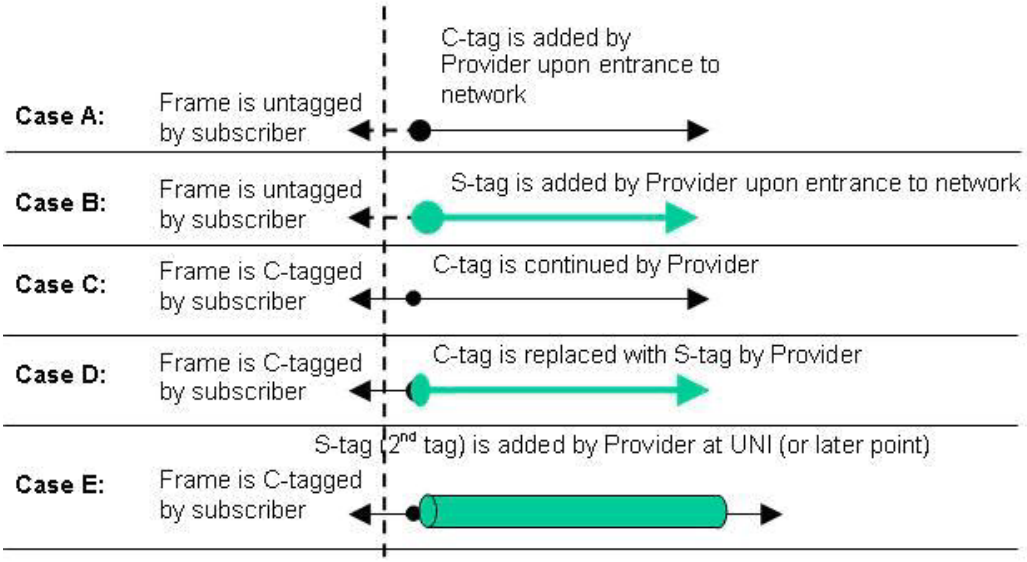


Figure D-2: Q-in-Q (Provider Tagging)

Case B and Case E above are more widely used by providers when subscriber's traffic enters and leaves the provider network at the UNI.

Q-in-Q implies a C-tag followed by the S-Tag or another C-Tag.

Not all of the steps below are required for each possible VLAN configuration. **Note**: VLAN 1 is the default VLAN and you cannot Edit or Delete it.

Q-in-Q service can be configured in the NID using either the CLI or the Web method.

Q-in-Q Config – CLI Method

This procedure configures Q-in-Q using **ethtype = 0x9100**.

1. Access the NID through either a USB connection (see "Starting a USB Session" on page 41) or a Telnet session (see "Starting a Telnet Session" on page 43).
2. Add a VLAN Database Entry. This adds a new VLAN to the device. By default, VLAN ID one (VID 1) is defined for internal use. Type:

   add vlan–db vid=<xx> **[priority**=<yy>] [**pri–override**={enable | disable}]

   where:

   xx = ID (2–4094) of the VLAN to which the device is to become a member

   yy = optional; priority for frames
3. Set the VLAN Database Member/Egress Tagging. This sets the priority of a row of the VLAN forwarding database. Type:

   set vlan-db vid=<xx> port=<yy> memetag=<zz>

   set vlan-db vid= <xx> fid=<yy> pri-override=<aa> priority=<bb>

   Where:

   ww =

   xx = number that identifies the VLAN (2–4094)

   yy = logical port index or fid

   zz = valid memetag choices are:

   - noMod
   - notMember
   - tag
   - unTag

   aa = pri-override={enable | disable}

   bb = priority = {0-7}
4. Press **Enter**.
5. Set the Management VLAN admin state to enable. Type:

   set mgmt vlan state=enable
6. Press **Enter**.
7. Select the management VLAN ports. Type:

   set mgmt vlan port=port-list

   Where:

   Port-list = a management VLAN port (1-19)

   Example: C1|S13|l0d/>**set mgmt vlan port=2,4,5**
8. Press **Enter**.
9. Set the port discard untagged non-management frames option to true if untagged non-management frames are to be discarded for this port. Type:

   set port discard-untagged=truth-val

   Where:

   Truth-val = true or false

   Example: C1|S13|l0ap1|l1p2/>**set port discard-untagged=true**
10. Press **Enter**.
11. Set the port discard tagged non-management frames option to true if the tagged non-management frames for this port are to be discarded. Type:

    set port discard-tagged=truth-val

    Where:

    Truth-val = true or false

Example: C1|S13|l0ap1|l1p2/>**set port discard-tagged=true**

12. Press **Enter**.
13. Set the port default VLAN-ID for this port. Type:
    set port default-vid=vid
    Where:
    vid = 2 - 4094
    Example: `C1|S13|l0ap1|l1p2/>set port default-vid=2`
14. Press **Enter**.
15. Set if force port to use default VLAN-ID. If set to true, this forces all untagged and 802.1Q tagged frames to assume the default VLAN-ID. Type:
    set port force-default-vid=truth-val
    Where:
    Truth-val = true or false
    Example: `C1|S13|l0ap1|l1p2/>set port force-default-vid=true`
16. Press **Enter**.
17. Set the port VLAN tag mode of a port interface. Type:
    set port vlan tag mode= provider
    Example: `C1|S13|l0ap1|l1p2/>set port vlan tag mode=provider`
18. Press **Enter**.
19. Set the Ethernet type for the VLAN tagging mode that was set to ***provider*** in step 17. Type:
    set port vlan tag provider ethtype= x9100
    Example: C1|S13|l0ap1|l1p2/>**set port vlan tag provider ethtype=x9100**
20. Press **Enter**.
21. Add a new row in the VLAN forwarding database. Type:
    add vlan-db vid=vlan-id **[pri-override=**override**] [priority=**prio**]**
    Where:
    vlan-id = 1-4094
    override = enable or disable
    prio = the priority for frames (0-7)
    Example:
    `C1|S13|l0ap1|l1p2/>add vlan-db vid=3 pri-override=enable priority=1`
22. Press **Enter**.
23. Set the priority override of a VLAN forwarding database row. This sets the override priority on frames associated with this VID of the VLAN forwarding database. Type:
    set vlan-db vid=vlan-id **fid=**fid **pri-override=**override
    Where:
    vlan-id =1-4094
    fid = 0
    override = enable or disable (specify if override priority on frames enabled in step 18)
    Example:
    `C1|S13|l0ap1|l1p2/>set vlan-db vid=3 fid=0 pri-override=enable`
24. Press **Enter**.

25. Set the priority of a VLAN forwarding database row. Type:
    set vlan-db vid=vlan-id fid=fid priority=prio
    Where:
    vlan-id = 2-4094
    fid = 0
    Prio = priority for frames (0-8)
    Example: `C1|S13|l0ap1|l1p2/>`**`set vlan-db vid=3 fid=0 priority=2`**
26. Press **Enter**.
27. Set the member and egress tagging of a VLAN forwarding database row. Type:
    `set vlan-db vid=``vlan-id` **`port=`**`port-id` **`memetag=`**`tag_mode`
    where:
    vlan-id = 1-4094
    port-id = logical port index
    tag_mode = noMod, notMember, tag, unTag
    Example:
    `C1|S13|l0ap1|l1p2/>`**`set vlan-db vid=3 port=2 memetag=Tag`**
28. Press **Enter**.
29. Use CLI commands to verify your VLAN configuration(s).
    - Show all existing VLAN(s) on the NID. Type **show vlan** and press **Enter**. For example:

      ```
      C1|S13|L0D/>show vlan

      vid     fid     priority  p-override  port1     port2     port3
      ------------------------------------------------------------------
      1       0       0         disable     NoMod     NoMod     notApp
      ```

    - Show the Management VLAN configuration. Type **show mgmt vlan config** and press **Enter** to show the management VLAN configuration on a device. Example:

      ```
      C1|S13|l0d/>show mgmt vlan config

      vlan id   vlan state         vlan portlist
      ------------------------------------------------------------------
      0         enable             none
      ```

    - Show the VLAN Service configuration on a device. Type **show vlan service** and press **Enter**. Example:

      ```
      C1|S13|l0d/> show vlan service

      VLAN service connection type:             customerProvider
      VLAN service VID for tag:                 8
      VLAN service Ethernet Type for tag:       0x8100
      VLAN translation type:                    untagged to untagged
      ```

    - Show the Port VLAN configuration. Type **show port vlan config** and press **Enter**. For example:

      ```
      C1|S13|l0ap1|l1p2/>show port vlan config

      Dot1q state:                  vlanEnabled
      Discard-tagged:               false
      Discard-untagged:             false
      Default VLAN id:              22
      Force use default VLAN id:    false
      ```

- Show the Port VLAN Tag configuration. Type **show port vlan tag config** and press **Enter**. For example:

```
C1|S13|l0ap1|l1p2/>show port vlan tag config
Tagging mode:           provider
Network tagging:        addTag
```

- Show the VLAN forwarding database configuration for the device. Type **show vlan-db config** and press **Enter**. For example:

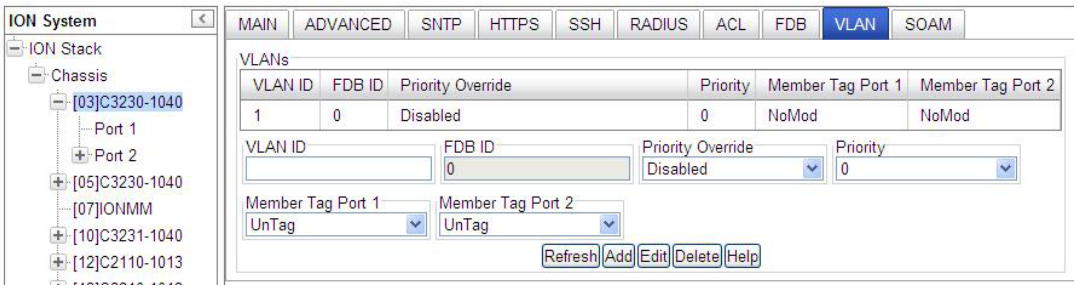
```
C1|S13|l1d> show vlan-db config

vid:1       fid:0       priority:0          priv_override:disable
port1:      NoMod       port2: NoMod
vid:100     fid:0       priority:0          priv_override:disable
port1:      notMember   port2: notMember
```

30. Click the **Add** button to add the newly-defined VLAN.

Q-in-Q Config – Web Method

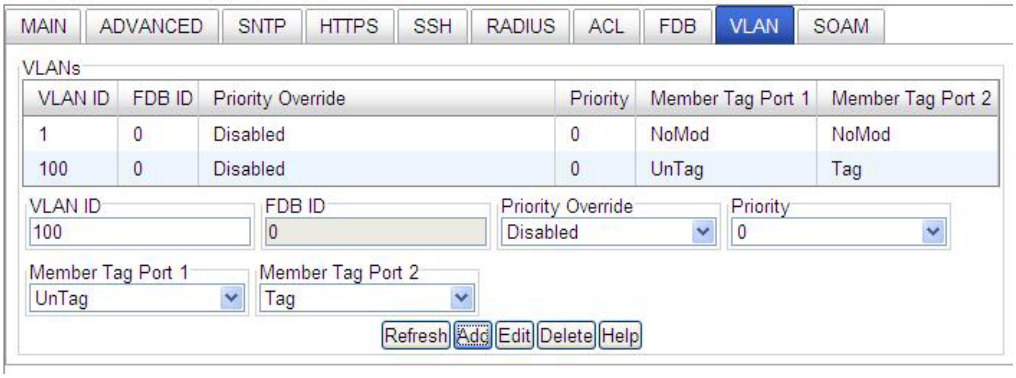
This procedure configures Q-in-Q using **ethtype = 0x9100**.

1. Access the NID through the Web interface (see "Starting the Web Interface" on page 45).
2. Select the REM-S323x device and then select the **VLAN** tab.

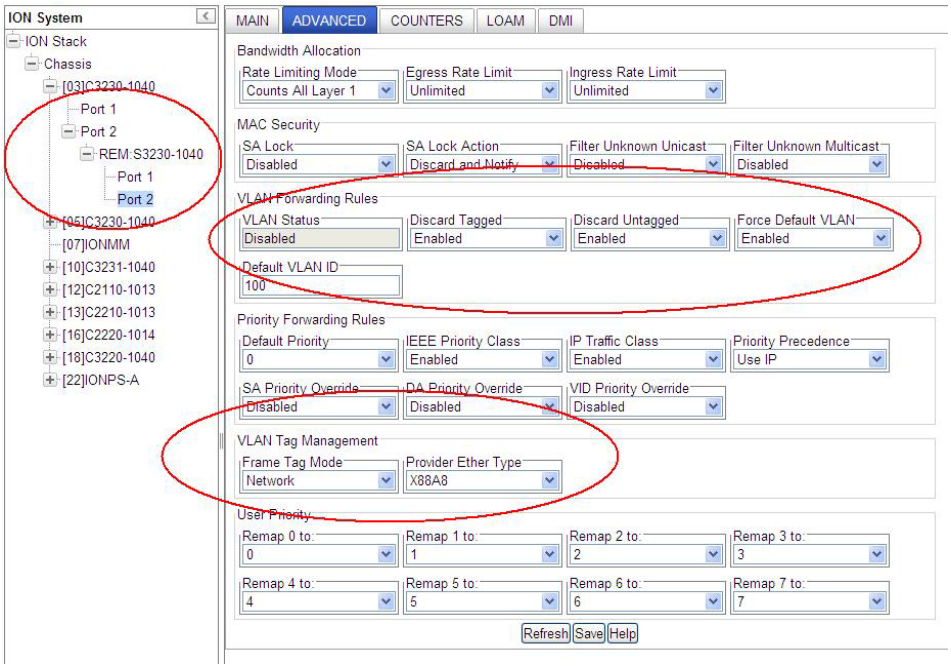


3. Add a new **VLAN ID** in the **VLANs** section:
   e. Enter **VLAN ID** =***100***.
   f. Set **Member Tag Port 1** to ***NoMod***.
   g. Set **Member Tag Port 2** to ***NoMod***.
   h. Set **Member Tag Port 3** to ***NoMod*** (3-port models only).
   i. Click the **Add** button.

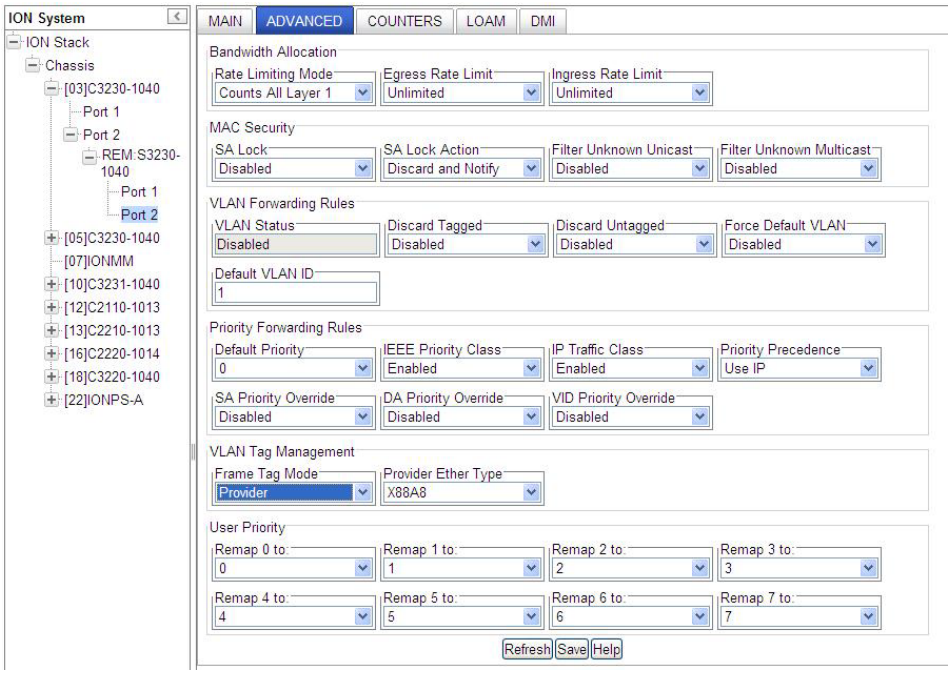
   The new VLAN ID 100 displays in the VLANs table:



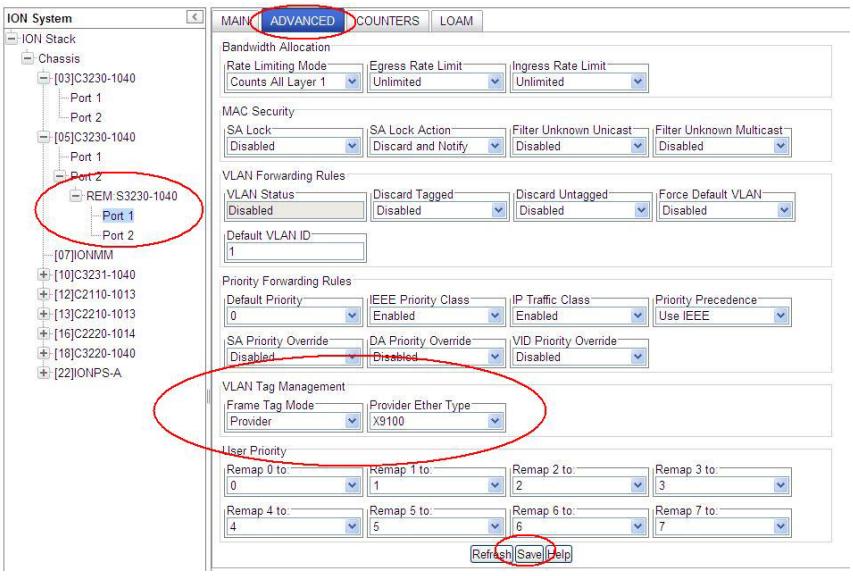
4. Go to REM S32xx-1040, Port 2 and click on the **ADVANCED** tab, and configure the "Provider Port" under port level config in the **VLAN Tag Management** section.



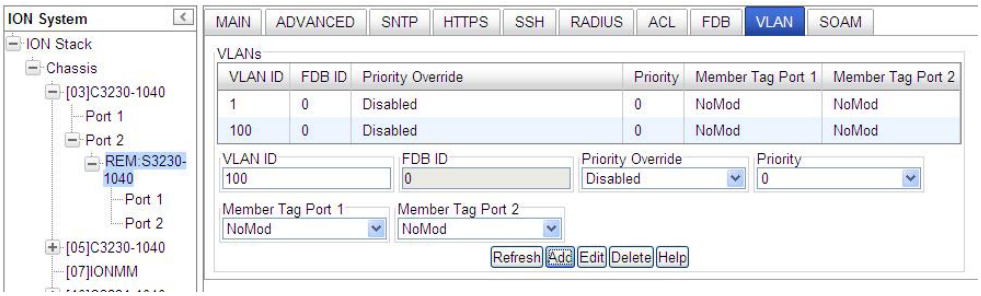
5. Set the **Frame Tag Mode** to ***Provider***, set the **EtherType** as ***x88A8***, and click the **Save** button.



6. Go to REM S3230-1040, Port 1 and click on the **ADVANCED** tab.



7. Configure the "***Provider*** Port" under port-level configuration. In the **VLAN Tag Management** section in the **Frame Tag Mode** field, select ***Provider***.
8. In the **Provider Ether Type** field, select **0x9100**.
9. Select REM-C323x, select the **VLAN** tab, and verify the VLAN database for correct set-up.



Verify the desired **Priority** and **Priority Override** settings and verify these settings:

e. **VLAN ID =*100***.
f. **Member Tag Port 1** set to ***NoMod***.
g. **Member Tag Port 2** set to ***NoMod***.
h. **Member Tag Port 3** for ***NoMod*** (three port models only).

Appendix E. SNMP Traps Supported

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

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

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

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

Traps List

1. ionSlotStatusChangeEvt
2. ionChassisDiscoveredEvt
3. ionChassisRemovedEvt
4. entSensorThresholdNotification
5. ionDMIRxIntrusionEvt
6. ionDMIRxPowerEvt
7. ionDMITxPowerEvt
8. ionDMITxBiasEvt
9. ionDMITemperatureEvt
10. ionSysDyingGaspTrap
11. ionSoamCCMDefectTrap
12. ionSoamRemoteMepAddTrap
13. ionSoamRemoteMepRemoveTrap
14. dot1agCfmFaultAlarm
15. newroot
16. topologyChange
17. dot3OamThresholdEvent
18. linkDown
19. linkUp
20. risingAlarm
21. fallingAlarm
22. ionIfSourceAddrChangeEvt
23. ionDevSysAclIdsEvt

SNMP v1 Traps

Most SNMPv1 messages follow a model where a client (Network Management System) makes a request and a server (agent) responds to that request. Traps are the exception. An SNMP agent will transmit a trap to the NMS when it has a condition to report that is deemed too important to wait until asked. A common example of this is the failure of a communications link.

With most traps, the agent will include something called "'Interesting' variable bindings," which are the OID(s) and value(s)of MIB variable(s) that provide more information about the condition. So, for example, when a communications channel fails, the agent will send a pSError trap, which will have the OID of the "Link" or "Signal Detect" variable for that channel, and the value "down." Newer versions of Management Module firmware will also include bindings for the BIA (Cabinet serial number), slot, and (if applicable) subdevice of the entity in question. This information is always embedded in the first binding (as above), but are repeated separately for more convenient viewing under certain NMS packages.

SNMP v2 Traps

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

See the "Supported MIBs" section on page 32 for information on the x222x / x32xx NIDs support for public (standard) and private MIBs. For information on "Configuring SNMP" see page 234. See the *ION Management Module (IONMM) User Guide* manual for SNMP traps supported on the IONMM.

A sample SNMP message sequence is shown below.

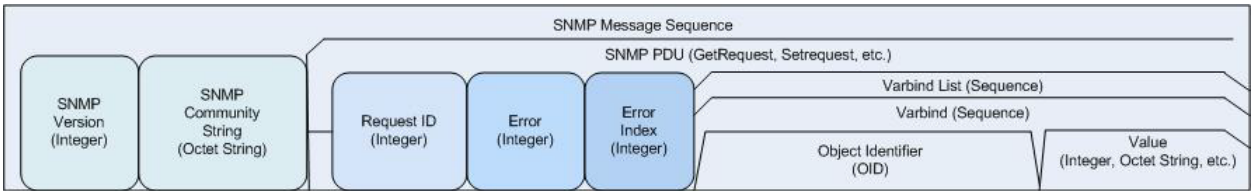


Figure E-1: SNMP Message Sequence

SNMP v3 Traps

SNMP v3 traps are mainly SNMPv2 traps with added authentication and privacy capabilities. SNMPv3 Traps use the engineID of the local application sending the trap rather than the engineID of the remote application. This means that you must create users in your remote user database and create one for each engineID you wish to send traps from.

MIB Traps Summary

The ION system MIB Traps are summarized in the table below in terms of related MIB and varbinds.

Table 34: MIB Traps Summary

MIB (linked to section)	TRAP (linked to section)	VARBINDS
TN-ION-BPC-MIB	ionSlotStatusChangeEvt	entPhysicalIndex, ionChassisSlotNumber ionChassisSlotStatus
TN-ION-Chassis-MIB	ionChassisDiscoveredEVt	entPhysicalIndex ionChassisStackSerialNo
	ionChassisRemovedEvt	entPhysicalIndex ionChassisStackSerialNo
TN-ION-ENTITY-SEN-SOR-MIB	entSensorThresholdNotification	entSensorThresholdValue entSensorValue
TN-ION-MGMT-MIB	ionDMIRxIntrusionEvt	ifIndex ionDMIRxPwrLvlPreset ionDMIRxPowerLevel
	ionDMIRxPowerEvt	ifIndex ionDMIRxPowerAlarm ionDMIRxPowerLevel
	ionDMITxPowerEvt	ifIndex ionDMITxPowerAlarm ionDMITxPowerLevel
	ionDMITxBiasEvt	ifIndex, ionDMITxBiasAlarm, ionDMITxBiasCurrent
	ionDMITemperatureEvt	ifIndex ionDMITempAlarm ionDMITemperature
	ionSysDyingGaspTrap rxPwrThreshold	
IEEE8021-CFM-MIB	dot1agCfmFaultAlarm	dot1agCfmMepHighestPrDefect
BRIDGE-MIB	newroot	

MIB (linked to section)	TRAP (linked to section)	VARBINDS
	topologyChange	
DOT3-OAM-MIB	dot3OamThresholdEvent	dot3OamEventLogTimestamp, dot3OamEventLogOui, dot3OamEventLogType, dot3OamEventLogLocation, dot3OamEventLogWindowHi, dot3OamEventLogWindowLo, dot3OamEventLogThresholdHi, dot3OamEventLogThresholdLo, dot3OamEventLogValue, dot3OamEventLogRunningTotal, dot3OamEventLogEventTotal
IF-MIB	linkDown	ifIndex, ifAdminStatus, ifOperStatus
	linkUp	ifIndex, ifAdminStatus, ifOperStatus
RMON	risingAlarm	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmFallingThreshold
	fallingAlarm	alarmIndex, alarmVariable, alarmSample-Type, alarmValue, alarmFallingThreshold
TN-ION-VLAN-MGMT-MIB	ionIfSourceAddrChangeEvt	
ION-DEV-SYS-ACL-MIB	ionDevSysAclIdsEvt	

TN-ION-MGMT-MIB.smi

```
ionDevSysMgmt          OBJECT IDENTIFIER ::= { ionDevMgmt 1 }
ionDevSysLPT               OBJECT IDENTIFIER ::= { ionDevMgmt 2 }
ionDevSysDyingGasp                 OBJECT IDENTIFIER ::= { ionDevMgmt 3 }

ionDevSysCfgTable OBJECT-TYPE
        ::= { ionDevSysLPTEntry 5 }

--
-- Dying Gasp management
--
ionDevSysDyingGaspTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF IonDevSysDyingGaspEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
        "This table supplements the ENTITY-MIB for 2-port devices managed by this Agent."
        ::= { ionDevSysDyingGasp 1 }

ionDevSysDyingGaspEntry OBJECT-TYPE
        SYNTAX      IonDevSysDyingGaspEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
        "An entry in the table contains additional information related to a device."
       INDEX       { entPhysicalIndex }
        ::= { ionDevSysDyingGaspTable 1 }

IonDevSysDyingGaspEntry ::= SEQUENCE
{
   ionSysDyingGaspTrap       INTEGER
}

ionSysDyingGaspTrap OBJECT-TYPE
        SYNTAX         INTEGER { enabled(1), disabled(2), notSupported(3) }
        MAX-ACCESS      read-write
    STATUS current
    DESCRIPTION
    "Devices which support this feature allow write for enabling or disabling the feature.

        When a device detects the power is going to be lost, a system dying gasp procedure will be triggered inter-
nally.
        If this ionSysDyingGaspTrap is set to enabled, a ionDyingGaspEvt will be sent out.
        Other events may also be sent out in this procedure, e.g. LOAM event.

        The LOAM event (enabled by dot3OamDyingGaspEnable) and this Trap event will be processed at the same
time if both enabled.
       If LOAM is enabled in multiple ports, the LOAM event will be sent out one port by one port beginning from
the smaller port number (e.g. smallest one is copper port, port 1)
        If multiple trap servers are enabled, the trap will be sent out one server by one server beginning from the server
1.

        Depends on different hardware, the dying gasp's power may be not enough for sending out all the LOAM
event and Traps.
```

```
        So, it is suggested that users should keep as few targets as possible."
        ::= { ionDevSysDyingGaspEntry 1 }


--
 --ION Ethernet Interface management
… …
    ::= { tnIonMgmtNotifications 6 }

ionDyingGaspEvt  NOTIFICATION-TYPE
    STATUS  current
    DESCRIPTION
    "when the device lost power, this dying gasp trap will be sent out."
    ::= { tnIonMgmtNotifications 7 }
```

Agent_III_Private MIBS

ION-DEV-SYS-ACL-MIB

The **ionDevSysAclIdsEvt** event is included in 'ION-DEV-SYS-ACL-MIB.my'. This event is related to 'iptableRulesTable' which is also defined in 'ION-DEV-SYS-ACL-MIB.my'.

```
 ionDevSysAclIdsEvt  NOTIFICATION-TYPE
     OBJECTS {
                 entPhysicalIndex, gRuleIndex
             }
STATUS  current
DESCRIPTION
```

"An ionDevSysAclIdsEvt event is sent if an IDS (Intrusion Detection Systems) is detected.
The entPhysicalIndex event indicates in which SIC the IDS is detected.
The entPhysicalIndex/gRuleIndex indicates which ACL rule is matched for this IDS."
::= { tnIonMgmtNotifications 16 }

ION-DEV-SYS-HTTPS-MIB

None

ION-DEV-SYS-IPMGMT-MIB

None

ION-DEV-SYS-RADIUS-MIB

None

ION-DEV-SYS-SNMPMGMT-MIB

None

ION-DEV-SYS-SNTP-MIB

None

ION-DEV-SYS-SSH-MIB

None

ION-DEV-SYS-TFTP-MIB

None

TN-ION-VLAN-MGMT-MIB.mib

The **ionIfSourceAddrChangeEvt** event is included 'TN-ION-VLAN-MGMT-MIB.mib'.
The 'ionIfSourceAddrChangeEvt' event is related to 'ionIfMACSecurityTable' which is defined in 'TN-ION-MGMT-MIB.smi'.

```
 ionIfSourceAddrChangeEvt  NOTIFICATION-TYPE
     OBJECTS {
                 ionFIDDbMacAddress, ionFIDDbConnPort
             }
STATUS  current
DESCRIPTION
```
"An ionIfSourceAddrChangeEvt event is sent when the ionIfSourceAddrLock is set to 'true', the ionIfSourceAddrLockAction is set to 'discardAndNotify' or 'all' and there is an intrusion/SA change on this port."
::= { tnIonVlanQoSMgmtNotifications 1 }

TN_ION Private MIBS

TN-ION-BPC-MIB

ionSlotStatusChangeEvt

An ionSlotStatusChangeEvt event is sent when a new module is inserted in this slot or when it is removed. The chassis is identified by its entPhysicalIndex.

Varbinds

entPhysicalIndex

```
SYNTAX INTEGER

DESCRIPTION
"The entPhysicalIndex in this chassis."
```

ionChassisSlotNumber,

```
SYNTAX INTEGER
DESCRIPTION
```
"The slot number in this chassis."

ionChassisSlotStatus

```
SYNTAX INTEGER { empty(1), occupied(2) }
DESCRIPTION
```
"The status of the slot, whether occupied or empty."

OID

MIB Description

ionSlotStatusChangeEvt NOTIFICATION-TYPE
OBJECTS {
entPhysicalIndex,
ionChassisSlotNumber,
ionChassisSlotStatus
}
STATUS current
DESCRIPTION
"An ionSlotStatusChangeEvt event is sent when a new module is inserted in this slot or when it is removed. The chassis is identified by its entPhysicalIndex."
::= { tnIonBkPlaneNotifications 1 }

TN-IONCHASSIS-MIB

ionChassisDiscoveredEvt

An ionChassisDiscoveredEvt event is sent when a new chassis is discovered.

Varbinds

entPhysicalIndex

```
SYNTAX INTEGER
DESCRIPTION
```
"The entPhysicalIndex in this chassis."

ionChassisStackSerialNo

```
SYNTAX OCTET STRING
DESCRIPTION
```
"The chassis serial number, this is unique to each chassis."

OID

MIB Definition

```
ionChassisDiscoveredEvt NOTIFICATION-TYPE
OBJECTS {
         entPhysicalIndex,
         ionChassisStackSerialNo
         }
STATUS  current
DESCRIPTION
```
"An ionChassisDiscoveredEvt event is sent when a new chassis is discovered."
```
::= { tnIonChassisNotifications 1 }
```

ionChassisRemovedEvt

An ionChassisRemovedEvt event is sent when a managed chassis is removed.

Varbinds

entPhysicalIndex

```
SYNTAX INTEGER
DESCRIPTION
```
"The entPhysicalIndex in this chassis."

ionChassisStackSerialNo

```
SYNTAX OCTET STRING
DESCRIPTION
```
"The chassis serial number, this is unique to each chassis."

OID

MIB Description

```
ionChassisRemovedEvt NOTIFICATION-TYPE
OBJECTS {
           entPhysicalIndex,
                ionChassisStackSerialNo
         }
STATUS  current
DESCRIPTION
```
"An ionChassisRemovedEvt event is sent when a managed chassis is removed."
```
::= { tnIonChassisNotifications 2 }
```

TN-ION-ENTITY-SENSOR-MIB

entSensorThresholdNotification

The sensor value crossed the threshold listed in entSensorThresholdTable.

This notification is generated once each time the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification.

Varbinds

entSensorThresholdValue

```
SYNTAX        SensorValue
DESCRIPTION
```
"This variable indicates the value of the threshold.

To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision.

However, you can directly compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."

entSensorValue

```
SYNTAX        SensorValue
DESCRIPTION
```
"This variable reports the most recent measurement seen by the sensor.

To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision.

However, you can compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."

SensorValue TEXTUAL-CONVENTION

```
SensorValue ::= TEXTUAL-CONVENTION
STATUS       current
DESCRIPTION
```
"For sensors that measure volts AC, volts DC, amperes, watts, hertz, Celsius, or cmm, this item is a fixed point number ranging from -999,999,999 to +999,999,999. Use the value -1000000000 to indicate underflow. Use the value +1000000000 to indicate overflow. Use SensorPrecision to indicate how many fractional digits the SensorValue has.

For sensors that measure percentRH, this item is a number ranging from 0 to 100.

For sensors that measure rpm, this item can take only nonnegative values, 0..999999999.

For sensors of type truthvalue, this item can take only two values: true(1), false(2).

For sensors of type specialEnum, this item can take any value in the range (-1000000000..1000000000),

but the meaning of each value is specific to the sensor.

For sensors of type other and unknown, this item can take any value in the range (-1000000000..1000000000), but the meaning of the values are specific to the sensor.

Use Entity-MIB entPhysicalTable.entPhysicalVendorType to learn about the sensor type."
SYNTAX INTEGER (-1000000000..1000000000)

OID

MIB Description

```
entSensorThresholdNotification NOTIFICATION-TYPE
OBJECTS { entSensorThresholdValue, entSensorValue }
STATUS current
DESCRIPTION
```
"The sensor value crossed the threshold listed in entSensorThresholdTable.

This notification is generated once each time the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification."
::= { entitySensorMIBNotifications 1 }

TN-ION-LOAM-EXT-MIB

None

TN-ION-MGMT-MIB

ionDMIRxIntrusionEvt

An ionDMIRxIntrusionEvt event is sent if the ionDMIRxPowerLevel falls below the ionDMIRxPwrLvlPreset indicating an intrusion on the fiber.

Varbinds

ifIndex

```
SYNTAX      INTEGER32()
DESCRIPTION
```
"IF-MIB Index of the port this was relevant to."

ionDMIRxPwrLvlPreset

```
SYNTAX      INTEGER(0..65535)
DESCRIPTION
```
"A preset level for Rx Power on the Fiber port, if the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated."

ionDMIRxPowerLevel

```
SYNTAX      INTEGER
DESCRIPTION
```
"DMI: Diagnostic Monitoring Interface for fiber transceivers. Receive power on local fiber measured in microwatts."

OID

MIB Description

ionDMIRxIntrusionEvt NOTIFICATION-TYPE

```
OBJECTS {
            ifIndex, ionDMIRxPwrLvlPreset, ionDMIRxPowerLevel
         }
STATUS  current
DESCRIPTION
```
"An ionDMIRxIntrusionEvt event is sent if the ionDMIRxPowerLevel falls below the ionDMIRxPwrLvlPreset indicating an intrusion on the fiber."

```
::= { tnIonMgmtNotifications 1 }
```

ionDMIRxPowerEvt

An ionDMIRxPowerEvt event is sent when there is a warning or alarm on Rx Power.

Varbinds

ifIndex

ionDMIRxPowerAlarm

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),
lowAlarm(6), highAlarm(7) }
DESCRIPTION "."
```

ionDMIRxPowerLevel

```
SYNTAX      INTEGER
DESCRIPTION
```
"DMI: Diagnostic Monitoring Interface for fiber transceivers. Receive power on local fiber, measured in microwatts."

OID

MIB Description

```
ionDMIRxPowerEvt  NOTIFICATION-TYPE
OBJECTS {
        ifIndex, ionDMIRxPowerAlarm, ionDMIRxPowerLevel
         }
STATUS  current
DESCRIPTION
```
"An ionDMIRxPowerEvt event is sent when there is a warning or alarm on Rx Power."
```
::= { tnIonMgmtNotifications 2 }
```

ionDMITxPowerEvt

An ionDMITxPowerEvt event is sent when there is a warning or alarm on Tx Power.

Varbinds

ifIndex

ionDMITxPowerAlarm

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),
lowAlarm(6), highAlarm(7) }
DESCRIPTION "."
```

ionDMITxPowerLevel

```
SYNTAX      INTEGER
DESCRIPTION "DMI: Diagnostic Monitoring Interface for fiber transceiv-
ers. Transmit power on local fiber measured in microwatts."
```

OID

MIB Definition

```
ionDMITxPowerEvt  NOTIFICATION-TYPE
OBJECTS {
       ifIndex, ionDMITxPowerAlarm, ionDMITxPowerLevel
        }
STATUS  current
DESCRIPTION
"An ionDMITxPowerEvt event is sent when there is a warning or alarm on Tx Power."
::= { tnIonMgmtNotifications 3 }
```

ionDMITxBiasEvt

An ionDMITxBiasEvt event is sent when there is a warning or alarm on Tx Bias current,

Varbinds

ifIndex

ionDMITxBiasAlarm

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),
lowAlarm(6), highAlarm(7) }
DESCRIPTION "."
```

ionDMITxBiasCurrent

```
SYNTAX INTEGER
DESCRIPTION
```
"Transmit bias current on local fiber interface, in microamperes."

OID

MIB Description

```
ionDMITxBiasEvt  NOTIFICATION-TYPE
OBJECTS {
         ifIndex, ionDMITxBiasAlarm, ionDMITxBiasCurrent
         }
STATUS  current
DESCRIPTION
```
"An ionDMITxBiasEvt event is sent when there is a warning or alarm on Tx Bias current."
```
::= { tnIonMgmtNotifications 4 }
```

ionDMITemperatureEvt

Varbinds

ifIndex

ionDMITempAlarm

SYNTAX INTEGER
DESCRIPTION "."

ionDMITemperature

```
SYNTAX      INTEGER
STATUS      current
DESCRIPTION
```
"Temperature of fiber transceiver in tenths of degrees C."

OID

MIB Description

```
ionDMITemperatureEvt  NOTIFICATION-TYPE
OBJECTS {
           ifIndex, ionDMITempAlarm, ionDMITemperature
            }
STATUS  current
DESCRIPTION
```
"An ionDMITemperatureEvt event is sent when there is a warning or alarm on DMI temperature."
```
::= { tnIonMgmtNotifications 5 }
```

TN-PROVBRIDGE-MIB

None

TN Private MIB OID Assignments (ION System)

OID	ION MIB module Name
tnProducts.1	tnIonChassisMIB
tnProducts.2	tnIonBkPlaneMIB
tnProducts.3	tnIonMgmtMIB
tnProducts.4	tnIonVlanQoSMgmtMIB
tnProducts.5	tnProvBridgeMIB
tnProducts.6	ionEntitySensorMIB
tnProducts.7	tnIonLOAMExtMIB
tnProducts.8	tnIonSOAMIdxMIB
tnProducts.99	tnSoamExtMIB

tnMgmtMIB subtree OID assignments

OID	ION MIB module Name
tnMgmtMIB.1.1	ionDevMgmt
tnMgmtMIB.1.2	ionInterfaceMgmt
tnMgmtMIB.1.3	ionInterfaceDiagMgmt
tnMgmtMIB.1.4	ionIfMACSecurityMgmt
tnMgmtMIB.1.5	ionIfQOSMgmt

- **tnDevMgmt subtree OID assignments**

OID	ION MIB module Name
tnDevMgmt.1	ionDevSysMgmt
tnDevMgmt.2	ionDevSysLPT
tnDevMgmt.3	ionDevSysDyingGasp
tnDevMgmt.4	ionDevSysMACLearning
tnDevMgmt.10	ionDevSysIpmgmt
tnDevMgmt.11	ionDevSysSntp
tnDevMgmt.12	ionDevSysHttps
tnDevMgmt.13	ionDevSysSsh
tnDevMgmt.14	ionDevSysSnmpmgmt
tnDevMgmt.15	ionDevSysTftp
tnDevMgmt.16	ionDevSysAcl
tnDevMgmt.17	ionDevSysRadius
tnDevMgmt.18	ionDevSyslogMgm
tnDevMgmt.19	ionDevSysUser
tnDevMgmt.20	ionDevSysTacPlus
tnDevMgmt.30	ionDevSysUpgraderMIB
tnDevMgmt.40	ionDevSysProvMgmt
tnDevMgmt.41	ionDevSysStateMgmt
tnDevMgmt.50	ionDevSysIPv6Acl
tnDevMgmt.60	ionDevSysIonPsAlCfg

ION Public MIBS

BRIDGE-MIB

newRoot

The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.

Varbinds

None

OID

MIB Description

```
newRoot NOTIFICATION-TYPE
-- OBJECTS     { }
STATUS      current
DESCRIPTION
"The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional."
::= { dot1dNotifications 1 }
```

topologyChange

A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newroot trap is sent for the same transition. Implementation of this trap is optional.

Varbinds

None

OID

MIB Description

```
topologyChange NOTIFICATION-TYPE
-- OBJECTS     { }
STATUS      current
DESCRIPTION
"A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newroot trap is sent for the same transition. Implementation of this trap is optional."
::= { dot1dNotifications 2 }
```

DOT3-OAM-MIB

dot3OamThresholdEvent

A dot3OamThresholdEvent notification is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event.

This notification should not be sent more than once per second.

The OAM entity can be derived from extracting the ifIndex from the variable bindings.
The objects in the notification correspond to the values in a row instance in the dot3OamEventLogTable.

The management entity should periodically check dot3OamEventLogTable to detect any missed events.

Varbinds

dot3OamEventLogTimestamp

SYNTAX TimeStamp
DESCRIPTION
"The value of sysUpTime at the time of the logged event. For locally generated events, the time of the event can be accurately retrieved from sysUpTime. For remotely generated events, the time of the event is indicated by the reception of the Event Notification OAMPDU indicating that the event occurred on the peer. A system may attempt to adjust the timestamp value to more accurately reflect the time of the event at the peer OAM entity by using other information, such
as that found in the timestamp found of the Event Notification TLVs, which provides an indication of the relative time between events at the peer entity. "

dot3OamEventLogOui

SYNTAX EightOTwoOui
DESCRIPTION
"The OUI of the entity defining the object type. All IEEE 802.3 defined events (as appearing in [802.3ah] except for the Organizationally Unique Event TLVs) use the IEEE 802.3 OUI of
0x0180C2. Organizations defining their own Event Notification TLVs include their OUI in the Event Notification TLV that gets reflected here. "

dot3OamEventLogType

SYNTAX Unsigned32
DESCRIPTION
"The type of event that generated this entry in the event log. When the OUI is the IEEE 802.3 OUI of 0x0180C2, the following event types are defined:

erroredSymbolEvent(1),
erroredFramePeriodEvent(2),
erroredFrameEvent(3),
erroredFrameSecondsEvent(4),
linkFault(256),
dyingGaspEvent(257),
criticalLinkEvent(258)

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.

When the OUI is not 71874 (0x0180C2 in hex), then some other organization has defined the event space. If event subtyping is known to the implementation, it may be reflected here.
Otherwise, this value should return all F's (2^32 - 1). "
REFERENCE "[802.3ah], 30.3.6.1.10 and 57.5.3."

dot3OamEventLogLocation

SYNTAX INTEGER { local(1), remote(2) }
DESCRIPTION
"Whether this event occurred locally (local(1)), or was received from the OAM peer via Ethernet OAM (remote(2)).
"

dot3OamEventLogWindowHi

SYNTAX Unsigned32
DESCRIPTION
"If the event represents a threshold crossing event, the two objects dot3OamEventWindowHi and dot3OamEventWindowLo, form an unsigned 64-bit integer yielding the window over which the value was measured for the threshold crossing event (for example, 5, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:
dot3OamEventLogWindow = ((2^32) * dot3OamEventLogWindowHi) + dot3OamEventLogWindowLo.

Otherwise, this value is returned as all F's (2^32 - 1) and adds no useful information.
"
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogWindowLo

SYNTAX Unsigned32
DESCRIPTION
"If the event represents a threshold crossing event, the two objects dot3OamEventWindowHi and dot3OamEventWindowLo form an unsigned 64-bit integer yielding the window over which the value was measured for the threshold crossing event (for example, 5, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

dot3OamEventLogWindow = ((2^32) * dot3OamEventLogWindowHi) + dot3OamEventLogWindowLo

Otherwise, this value is returned as all F's (2^32 - 1) and adds no useful information. "
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogThresholdHi

SYNTAX Unsigned32
DESCRIPTION
"If the event represents a threshold crossing event, the two objects dot3OamEventThresholdHi and dot3OamEventThresholdLo form an unsigned 64-bit integer yielding the value that was crossed for the threshold crossing event (for example, 10, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

dot3OamEventLogThreshold = ((2^32) * dot3OamEventLogThresholdHi) + dot3OamEventLogThresholdLo

Otherwise, this value is returned as all F's (2^32 -1) and adds no useful information. "
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogThresholdLo

SYNTAX Unsigned32
DESCRIPTION
"If the event represents a threshold crossing event, the two objects dot3OamEventThresholdHi and dot3OamEventThresholdLo form an unsigned 64-bit integer yielding the value that was crossed for the threshold crossing event (for example, 10, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

dot3OamEventLogThreshold = ((2^32) * dot3OamEventLogThresholdHi) + dot3OamEventLogThresholdLo

Otherwise, this value is returned as all F's (2^32 - 1) and adds no useful information. "
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogValue

SYNTAX CounterBasedGauge64
DESCRIPTION
"If the event represents a threshold crossing event, this value indicates the value of the parameter within the given window that generated this event (for example, 11, when 11 occurrences happened in 5 seconds while the threshold was 10).

Otherwise, this value is returned as all F's (2^64 - 1) and adds no useful information. "
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2.

dot3OamEventLogRunningTotal

SYNTAX CounterBasedGauge64
DESCRIPTION
"Each Event Notification TLV contains a running total of the number of times an event has occurred, as well as the number of times an Event Notification for the event has been transmitted. For non-threshold crossing events, the number of events (dot3OamLogRunningTotal) and the number of resultant Event Notifications (dot3OamLogEventTotal) should be identical.

For threshold crossing events, since multiple occurrences may be required to cross the threshold, these values are likely different. This value represents the total number of times this event has happened since the last reset (for example, 3253, when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset). "
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogEventTotal

SYNTAX Unsigned32
DESCRIPTION

"Each Event Notification TLV contains a running total of the number of times an event has occurred, as well as the number of times an Event Notification for the event has been transmitted. For non-threshold crossing events, the number of events (dot3OamLogRunningTotal) and the number of resultant Event Notifications (dot3OamLogEventTotal) should be identical.

For threshold crossing events, since multiple occurrences may be required to cross the threshold, these values are likely different. This value represents the total number of times one or more of these occurrences have resulted in an Event Notification (for example, 51 when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset).
"
REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

OID

MIB Description

```
dot3OamThresholdEvent NOTIFICATION-TYPE
OBJECTS { dot3OamEventLogTimestamp,
          dot3OamEventLogOui,
          dot3OamEventLogType,
          dot3OamEventLogLocation,
          dot3OamEventLogWindowHi,
          dot3OamEventLogWindowLo,
          dot3OamEventLogThresholdHi,
          dot3OamEventLogThresholdLo,
          dot3OamEventLogValue,
          dot3OamEventLogRunningTotal,
          dot3OamEventLogEventTotal
        }
STATUS  current
DESCRIPTION
"A dot3OamThresholdEvent notification is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event.

This notification should not be sent more than once per second.

The OAM entity can be derived from extracting the ifIndex from the variable bindings.
The objects in the notification correspond to the values in a row instance in the dot3OamEventLogTable.

The management entity should periodically check dot3OamEventLogTable to detect any missed events."
::= { dot3OamNotifications 1 }

dot3OamNonThresholdEvent NOTIFICATION-TYPE
OBJECTS { dot3OamEventLogTimestamp,
          dot3OamEventLogOui,
          dot3OamEventLogType,
          dot3OamEventLogLocation,
          dot3OamEventLogEventTotal
        }
```

STATUS current
DESCRIPTION
"A dot3OamNonThresholdEvent notification is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is
detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event.

This notification should not be sent more than once per second.

The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance of the
dot3OamEventLogTable.

The management entity should periodically check dot3OamEventLogTable to detect any missed events."
::= { dot3OamNotifications 2 }

ENTITY-MIB

entConfigChange NOTIFICATION-TYPE
STATUS current
DESCRIPTION
"An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.

An agent should not generate more than one entConfigChange 'notification-event' in a given time interval (five seconds is the suggested default). A 'notification-event' is the transmission of a single trap or informs PDU to a list of notification destinations.

If additional configuration changes occur within the throttling period, then notification-events for these changes should be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event should be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started right away.

An NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events, e.g., due to throttling or transmission loss."
::= { entityMIBTrapPrefix 1 }

EtherLike-MIB

None

IANA-MAU-MIB

None

IEEE8021-CFM-V2-MIB

None

IEEE8021-TC-MIB

None

IF-MIB

linkDown

varbinds

ifIndex

```
SYNTAX      InterfaceIndex
DESCRIPTION
```

"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

ifAdminStatus

```
SYNTAX  INTEGER {
      up(1),       -- ready to pass packets
      down(2),
      testing(3)   -- in some test mode
            }
DESCRIPTION
"The desired state of the interface.  The testing(3) state indicates that no
operational packets can be passed.  When a managed system initializes, all
interfaces start with ifAdminStatus in the down(2) state.  As a result of ei-
ther explicit management action or per configuration information retained by
the managed system, ifAdminStatus is then changed to either the up(1) or
testing(3) states (or remains in the down(2) state)."
```

ifOperStatus

```
SYNTAX  INTEGER {
                up(1),        -- ready to pass packets
                down(2),
                testing(3),   -- in some test mode
                unknown(4),   -- status can not be determined
                              -- for some reason.
                dormant(5),
                notPresent(6),    -- some component is missing
                lowerLayerDown(7) -- down due to state of
                                  -- lower-layer interface(s)
            }

DESCRIPTION
```

"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1)then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

InterfaceIndex ::= TEXTUAL-CONVENTION

```
DISPLAY-HINT "d"
DESCRIPTION
```
"A unique value, greater than zero, for each interface or interface sub-layer in the managed system. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."
```
SYNTAX       Integer32 (1..2147483647)
```

OID

MIB Description

```
linkDown NOTIFICATION-TYPE
OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
STATUS  current
DESCRIPTION
```
"A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOper-Status object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."
```
::= { snmpTraps 3 }
```

linkUp

varbinds

ifIndex
```
SYNTAX      InterfaceIndex
DESCRIPTION
```
"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

ifAdminStatus
```
SYNTAX  INTEGER {
      up(1),        -- ready to pass packets
      down(2),
      testing(3)    -- in some test mode
            }
DESCRIPTION
```
"The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state)."

ifOperStatus

```
SYNTAX  INTEGER {
      up(1),         -- ready to pass packets
      down(2),
      testing(3),    -- in some test mode
      unknown(4),    -- status can not be determined -- for some reason.
      dormant(5),
      notPresent(6),     -- some component is missing
      lowerLayerDown(7) -- down due to state of -- lower-layer interface(s)
            }
DESCRIPTION
```

"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

InterfaceIndex ::= TEXTUAL-CONVENTION

```
DISPLAY-HINT "d"
DESCRIPTION
```

"A unique value, greater than zero, for each interface or interface sub-layer in the managed system. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

```
SYNTAX       Integer32 (1..2147483647)
```

OID

MIB Description

```
linkUp NOTIFICATION-TYPE
OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
STATUS  current
DESCRIPTION
```

"A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus."

```
::= { snmpTraps 4 }
```

LLDP-MIB

None

NOTIFICATION-LOG-MIB

None

P-BRIDGE-MIB

None

Q-BRIDGE-MIB

None

RFC1213-MIB

None

RMON-MIB (RFC 2819)

risingAlarm

SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP.

Varbinds

alarmIndex

```
SYNTAX      Integer32 (1..65535)
DESCRIPTION
```

"An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device."

alarmVariable

```
SYNTAX      OBJECT IDENTIFIER
DESCRIPTION
```

"The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.

Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

alarmSampleType

```
SYNTAX INTEGER {
      absoluteValue(1),
      deltaValue(2)
      }
DESCRIPTION
```

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

This object may not be modified if the associated alarmStatus object is equal to valid(1).

alarmValue

```
SYNTAX      Integer32
DESCRIPTION
```
"The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds.

The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes."

alarmRisingThreshold

```
SYNTAX      Integer32
DESCRIPTION
```
"A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.
A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3).

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

OID

MIB Description

```
risingAlarm NOTIFICATION-TYPE
OBJECTS  { alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmRis-
ingThreshold }
STATUS   current
DESCRIPTION
```
"The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps."
::= { rmonEventsV2 1 }

fallingAlarm

The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Varbinds

alarmIndex

```
SYNTAX     Integer32 (1..65535)
DESCRIPTION
```

"An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device."

alarmVariable

```
SYNTAX     OBJECT IDENTIFIER
DESCRIPTION
```

"The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.

Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

alarmSampleType

```
SYNTAX INTEGER {
            absoluteValue(1),
            deltaValue(2)
            }
DESCRIPTION
```

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

This object may not be modified if the associated alarmStatus object is equal to valid(1).

alarmValue

```
SYNTAX      Integer32
DESCRIPTION
```
"The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds.

The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes."

alarmRisingThreshold

```
SYNTAX      Integer32
DESCRIPTION
```
"A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3).

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

MIB Description

```
fallingAlarm NOTIFICATION-TYPE
OBJECTS { alarmIndex, alarmVariable, alarmSampleType,
          alarmValue, alarmFallingThreshold }
STATUS    current
DESCRIPTION
```
"The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps."
```
::= { rmonEventsV2 2 }
```

RMON2-MIB

None

SNMP-COMMUNITY-MIB

None

SNMP-NOTIFICATION-MIB

None

SNMP-TARGET-MIB

None

Trap Server Log

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

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

Line
1
2
3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 | iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
12
13 E=
14 Ebig=
15 IP=192.251.144.220
16 com=trap
17 GT=Notification
18 ST=
19 TS=Thu May 13 10:06:42 2010
20 VB-Count=3
21 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266790) 326 days, 15:37:47.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 | iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
22
23 E=
24 Ebig=
25 IP=192.251.144.220
26 com=trap
27 GT=Notification
28 ST=
29 TS=Thu May 13 10:10:17 2010
30 VB-Count=3
31 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288348) 326 days, 15:41:23.48 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 | iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
32
33 E=
34 Ebig=
35 IP=192.251.144.220
36 com=trap
37 GT=Notification
38 ST=
39 TS=Thu May 13 10:10:18 2010
40 VB-Count=5
41 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288428) 326 days, 15:41:24.28 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.4.1.868.2.5.2.0.1 | iso.3.6.1.2.1.47.1.1.1.1.1.134217728 = 134217728 | iso.3.6.1.4.1.868.2.5.2.1.1.1.1.134217728.6 = 6 | iso.3.6.1.4.1.868.2.5.2.1.1.1.2.134217728.6 = 1

The trap server log file lines are listed and described below.

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

Table 35: Trap Server Log File Description

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

For Additional SNMP MIB Trap Information

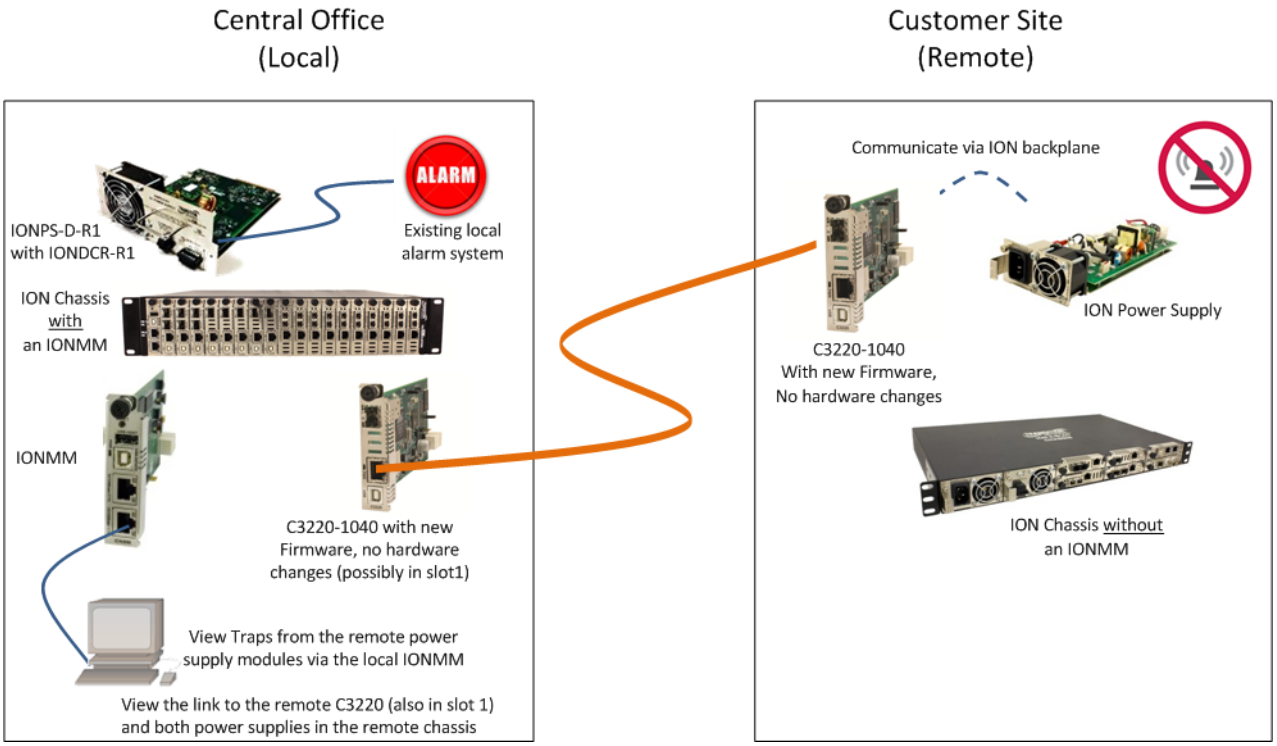
For information on Network Management for Microsoft Networks Using SNMP, see http://technet.microsoft.com/en-us/library/cc723469.aspx or the MSDN Library.

The notification MIB is described in section 4.2 and section 7.2 of RFC 2573, available from the IETF web site at http://www.ietf.org/rfc/rfc2573.txt.

Appendix F Remote Manage Power Supply (RMPS) Feature

This feature is provided with ION C3220-1040 firmware version 1.3.17 or above and IONMM firmware version1.3.20 or above. ION Power supply support includes IONPS-D, IONPS-A, IONPS-D-R1 and IONPS-A-R1.

ION Chassis support includes the ION 6-slot chassis (ION106) or the ION 19-slot chassis (ION219) deployed as the remote chassis.
The RMPS feature lets you view and manage ION power supplies in a remote unmanaged chassis, in-band, over the fiber, using a pair of C3220-1040 converters. This feature improves visibility of equipment installed in areas with limited accessibility such as a service provider's customer site.



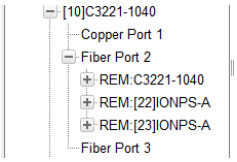
From the C3220 management interface in the local managed chassis through its port 2 (the fiber port) you can view the remote C3220 as well as Remote PS 1 and Remote PS 2.. You can actively manage converter cards and power supply modules in both the local managed chassis and the remote unmanaged chassis.

On the local ION Chassis, the IONDCR-R1 in the IONPS-D power supply is connected to the existing local alarm system, which alerts you to power supply issues.

You can log in to the IONMM and check the status of power supply modules and also check the status of all the cards in the chassis. In the IONMM Web UI, looking at the local C3220 (in slot 1) shows the link to the remote C3220 (also in slot 1) and both power supplies in the remote chassis.

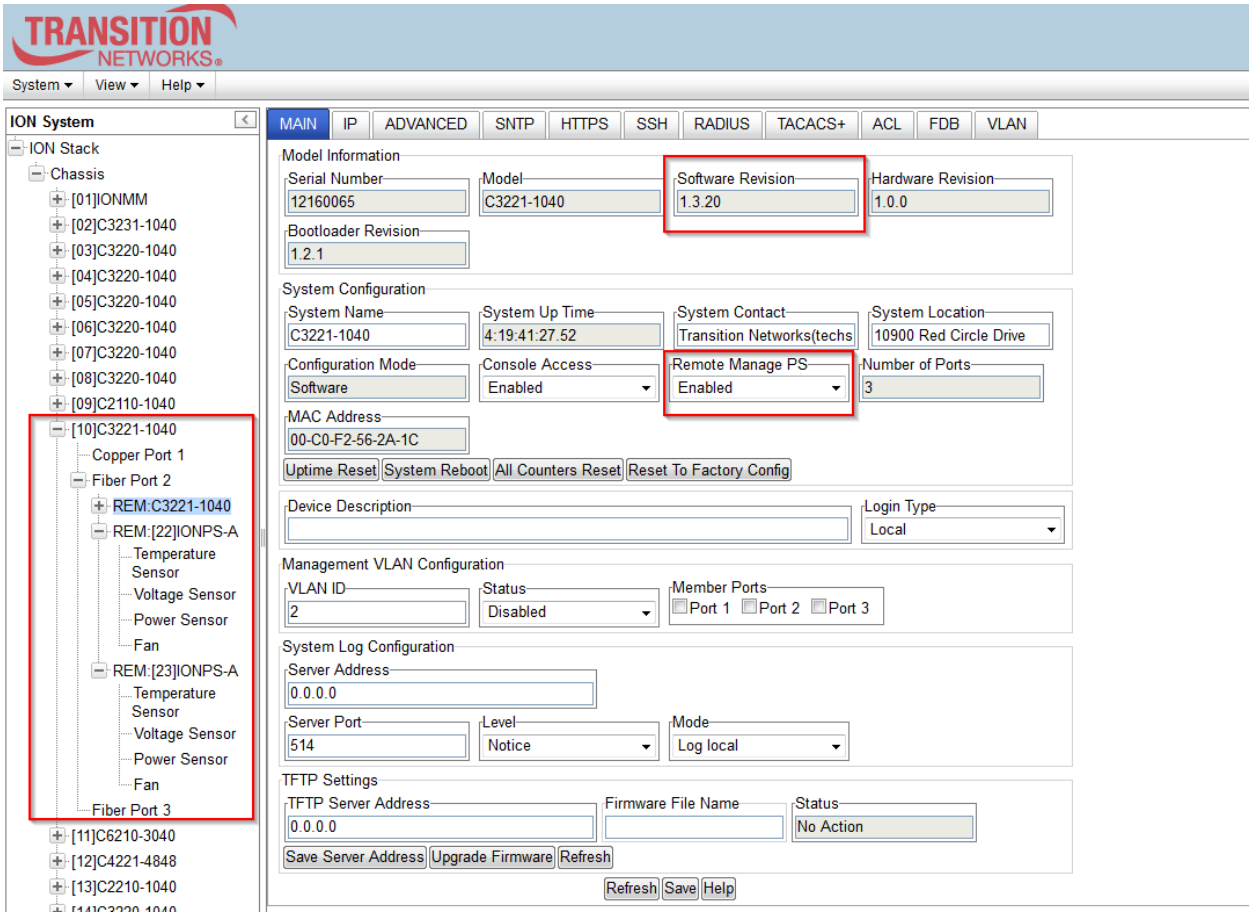
Since there are no alarms at the remote chassis power supply modules, you must log into the local IONMM to check the status of remote power supplies. Traps from the remote power supply modules are accessible via the local IONMM.

You can monitor the remote power supply via the CLI or via the Web GUI as described in the following sections.



Remote Power Supply Monitoring (Web GUI)

1. Navigate to the C3221-1040 (slot 10 in the example below).
2. Expand the Fiber Port (Fiber Port 2 in the example below).
3. Expand the Remote Power Supply (e.g., REM:[22]IONPS-A below) to display the Power Supply parameters.



Software Revision: The Remote Manage PS feature requires C3230 firmware version 1.3.17 or above and IONMM firmware v 1.4.2 or above.

Remote Manage PS: At the dropdown, select Enabled or Disabled as the Remote Manage PS feature state. The default is Disabled.

View and manage the selected remote ION power supply's sensors (Temperature, Voltage, Power, and Fan).

Refer to the related power supply manual for model-specific parameter information. See Related Manuals on page 628.

Remote Power Supply Monitoring (CLI)

These C3220-1040 CLI commands are available for managing remote power supplies in an ION106 or ION219 chassis.

```
set rmps=(enable|disable)
set sensor stid
show card info
stat
```

Command: **Set remote manage PS on a C32xx remote card**

Syntax: **set rmps**=(enable|disable)

Description: Enable or Disable the Remote Manage Power Supply (rpms) feature on a C3220. Use this command to enable forwarding Remote unmanaged chassis power supply frames. The default is to not forward Power Supply frames.

Example 1:

```
Agent III C1|S2|L1D>set rmps ?
  disable
  enable
Agent III C1|S2|L1D>set rmps enable
Agent III C1|S2|L1D>show card info
System name:        C3220-1040
Uptime:             00:33:54
CPU MAC:            00-c0-f2-21-2d-97
Port number:        2
Manage Remote PS:   enable
Serial number:      12243313
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1

Hardware:           1.0.0
Agent III C1|S2|L1D>
Agent III C1|S2|L1D>set rmps disable
Agent III C1|S2|L1D>show card info
System name:        C3220-1040
Uptime:             00:38:14
CPU MAC:            00-c0-f2-21-2d-97
Port number:        2
Manage Remote PS:   disable
Serial number:      12243313
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1

Hardware:           1.0.0
Agent III C1|S2|L1D>
```

Command: **Display Card Information**

Syntax: **show card info**

Description: Existing command updated at v 1.3.17 to display the Remote Manage PS (rmps) status (either hardware, enable, or disable) that was set by the “set rmps” command.

Example 1:

```
Agent III C1|S2|L1D>show card info
System name:        C3220-1040
Uptime:             00:31:55
CPU MAC:            00-c0-f2-21-2d-97
Port number:        2
Manage Remote PS:   hardware
Serial number:      12243313
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1

Hardware:           1.0.0
Agent III C1|S2|L1D>
```

Command: **Set PS Sensor Threshold Parameters**

Syntax: **set sensor stid**=(notification/relation/severity/value)

Description: Sets the current IONPS-A-R1 Sensor Transaction ID (stid) settings. The STID is used for power supply / sensor configuration via the set sensor stid command to define notification, relation, severity, and value parameters. There are 5 sensors on each power supply. 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.
The stid is the port number, where Temperature = port 1, Voltage = port 2, Power = port 3, and Fan = port 4 (some older power supplies had a second fan as the fifth port).
See the related power supply manual for specific stid (Sensor Transaction ID) parameters.

Use the **show power config** command to display the related current status.

Use the **stat** command to view the chassis slot assignments. Power Supplies are assigned slot 22 and slot 23 by default. The ION219 chassis has PS 1 ON and PS 2 ON LEDs to indicate power supply presence and function.
The **stat** command displays information about all slide-in modules installed in the chassis and all standalone modules connected to the remote slide-in modules, and their ports. On a remote standalone device, the **stat** command displays device and port information.

Example 1: Enable and disable the option on the remote C3220, get to the remote power supply, show the power config, and set the sensor thresholds. To see the remote C3220 and enable/disable “Manage Remote PS”:

1. Start at the IONMM in slot 19.
2. Go to the local C3220 in slot 1 port 2.
3. Go to the remote C3220 level 2 device.

```
Agent III C1|S19|L1D>go s=1 l1ap=2 l2d
Agent III C1|S19|L1AP2|L2D>show card info
System name:        C3220-1040
Uptime:             1 day, 22:23:36
CPU MAC:            00-c0-f2-20-ff-c7
Port number:        2
Manage Remote PS:   enable
Serial number:      11649161
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1
Hardware:           1.0.0
Agent III C1|S19|L1AP2|L2D>
Agent III C1|S19|L1AP2|L2D>set rmps disable
Agent III C1|S19|L1AP2|L2D>show card info
System name:        C3220-1040
Uptime:             1 day, 22:32:57
```

```
CPU MAC:            00-c0-f2-20-ff-c7
Port number:        2
Manage Remote PS:   disable
Serial number:      11649161
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1
Hardware:           1.0.0
Agent III C1|S19|L1AP2|L2D>set rmps enable
```

```
// To see the remote C3220 and enable|disable "Manage Remote PS":
// Start at the IONMM. Go the local C3220 (mine is in slot #1), port 2
// to the remote C3220, level 2 device.
Agent III C1|S19|L1D>
Agent III C1|S19|L1D>go s=1 l1ap=2 l2d
Agent III C1|S1|L1AP2|L2D>
Agent III C1|S1|L1AP2|L2D>show card info
System name:        C3220-1040
Uptime:             1 day, 22:23:36
CPU MAC:            00-c0-f2-20-ff-c7
Port number:        2
Manage Remote PS:   enable
Serial number:      11649161
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1
Hardware:           1.0.0
Agent III C1|S1|L1AP2|L2D>
Agent III C1|S1|L1AP2|L2D>set rmps disable
Agent III C1|S1|L1AP2|L2D>show card info
System name:        C3220-1040
Uptime:             1 day, 22:32:57
CPU MAC:            00-c0-f2-20-ff-c7
Port number:        2
Manage Remote PS:   disable
Serial number:      11649161
Config mode:        software
Software:           1.3.17
Bootloader:         1.2.1

Hardware:           1.0.0
Agent III C1|S1|L1AP2|L2D>
Agent III C1|S1|L1AP2|L2D>set rmps enable
```

Example 2: To see the remote power supply(s):

1. Start at the IONMM in slot 19.
2. Go to the local C3220 in slot 1 port 2.
3. Go to the remote C3220 port 2 level 3 device.

```
go s=1  1ap=2 l2ap=6 l3d
show power config
Agent III C1|S19|L1D>go s=1 l1d
Agent III C1|S1|L1AP2|LAP0|L3D>go l1p=2
Agent III C1|S1|L1P2>go l1ap=2 l2ap=6 l3d
Agent III C1|S19|L1AP6|L3D>
```

// To see the IONPS Sensors (Ports 1-4):

go s=1 1ap=2 l2ap=6 l3d

go l3p=1 (Temperature)

```
Agent III C1|S1|L1AP2|L2AP6|L3D>go l3p=1
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=1 notif <tab>
disable        enable
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=1 notif disable
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=1 value 5
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=2 severity <tab>
critical       major   minor   other
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=2 severity critical
Agent III C1|S1|L1AP2|L2AP6|L3P1>go l1p=3
```

```
// To see the remote power supply(s):
// Start at the IONMM. Go the local C3220 (mine is in slot #1), port 2
// to the remote C3220, port 2, level 3 device.
go s=1 l1ap=2 l2ap=6 l3d
show power config
Agent III C1|S19|L1D>go s=1 l1d
Agent III C1|S1|L1AP2|L2AP0|L3D>go l1p=2
Agent III C1|S1|L1P2>go l1ap=2 l2ap=6 l3d
Agent III C1|S1|L1AP2|L2AP6|L3D>
// To see the IONPS sensors (Ports 1-4)
go s=1 l1ap=2 l2ap=6 l3d
go  l3p=1 (Temperature)
Agent III C1|S1|L1AP2|L2AP6|L3D>go l3p=1
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=1 notif (tab)
  disable
  enable
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=1 notif disable
Agent III C1|S1|L1AP2|L2AP6|L3P1>
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=1 value 5
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=2 severity (tab)
  critical
  major
  minor
  other
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=2 severity
Agent III C1|S1|L1AP2|L2AP6|L3P1>set sensor stid=2 severity critical
Agent III C1|S1|L1AP2|L2AP6|L3P1>go l3p=2
Agent III C1|S1|L1AP2|L2AP6|L3P2>set sensor stid=1 severity critical
Agent III C1|S1|L1AP2|L2AP6|L3P2>go l3p=3
Agent III C1|S1|L1AP2|L2AP6|L3P3>set sensor stid=3 relation (tab)
  equalTo
  greaterOrEqual
  greaterThan
  lessOrEqual
  lessThan
  notEqualTo
Agent III C1|S1|L1AP2|L2AP6|L3P3>set sensor stid=3 relation
Agent III C1|S1|L1AP2|L2AP6|L3P3>go l3p=4
```

If there are 2 supplies, reach the second one with **`go s=1 l1ap=2 l2ap=7 l4d`**. Refer to the related power supply manual for model-specific parameter information. See Related Manuals on page 628.

Command: **ION statck**

Syntax: **stat**

Description: Use the **stat** command to view the chassis slot assignments. Power Supplies are assigned slot 22 and slot 23 by default. The ION219 chassis has PS 1 ON and PS 2 ON LEDs to indicate power supply presence and function. The **stat** command displays information about all slide-in modules installed in the chassis and all standalone modules connected to the remote slide-in modules, and their ports. On a remote standalone device, the **stat** command displays device and port information.

Example:

```
Agent III C1|S19|L1D>stat
ION stack
        Chassis -- BPC
                [  1]  C3220-1014
                        Port 1
                        Port 2
                [  2]  C3220-1014
                        Port 1
                        Port 2
                [  4]  C6010-1040
                        Port 1
                        Port 2
                [  5]  C6210-3040
                        Port 1
                        Port 2
                [  7]  C3220-1040
                        Port 1
                        Port 2
                                level2 REM: C3220-1040
                                        Port 1
                                        Port 2
                                                level3 REM: IONPS6-A
                                                        Temperature Sensor
                                                        Voltage Sensor
                                                        Power Sensor
                                                        Fan-1
                                                        Fan-2
                                                level3 REM: IONPS6-D
                                                        Temperature Sensor
                                                        Voltage Sensor
                                                        Power Sensor
                                                        Fan-1
                                                        Fan-2
                [  9]  C6110-1040
                        Port 1
                                level2 REM: S6110-1013
                                        Port 1
                                        Port 2
```

```
                                    Port 3
                                    Port 4
                                    Port 5
                        Port 2
                        Port 3
                        Port 4
                        Port 5
                [ 14]  C6120-1040
                        Port 1
                        Port 2
                        Port 3
                        Port 4
                        Port 5
                        Port 6
                [ 19]  IONMM
                        Port 1
                        Port 2
                [ 22]  IONPS-A-R1
                        Temperature Sensor
                        Voltage Sensor
                        Power Sensor
                        Fan
Agent III C1|S19|L1D>
```

RMPS CLI Messages

Manage Remote PS is not available before card rev v1.3.17.

Error: Cannot set Manage Remote PS on this card!

Error: Software version of this card is too old, please upgrade it!

Error: this command should be executed on a device!

Error: this command should be executed on a port

Error: Please input a number to specify slot number!

Error: Get chassis slot power state fail

Error: Get chassis slot state fail

Manage Remote PS:", "Not Supported

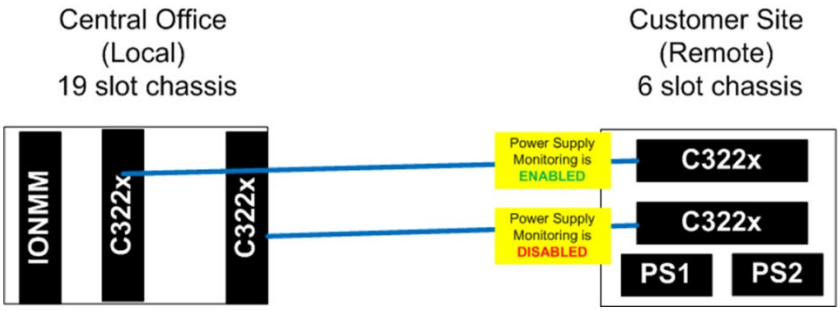
Model name %s does not match the feature

Manage Remote PS:,Not Supported

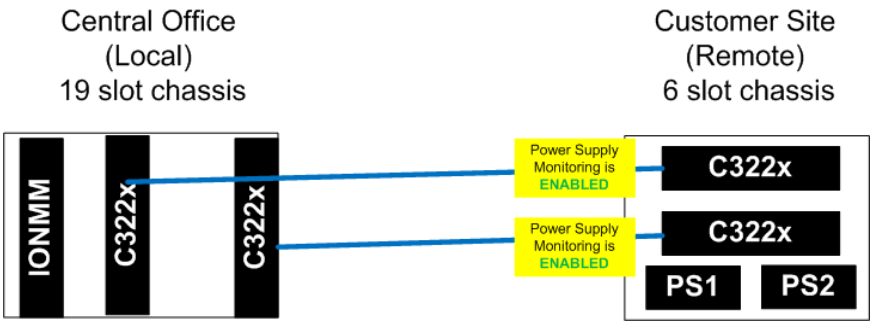
Limitations

The Remote Power Supply Management feature has some limitations. It is intended to work with a single Locally Managed chassis managing a Remote Unmanaged chassis. Both the remote C322x and the local C322x must be at 1.3.17 in order for the remote power supply management function to work. The older remote management functions will work, but the remote power supplies will not be connected.

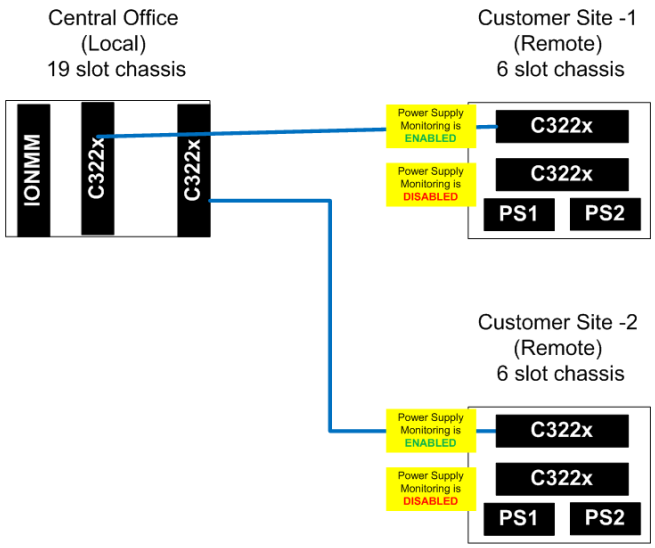
Scenario 1: This scenario works, where Remote Power Supply Monitoring is only Enabled on 1 card in the Remote chassis.



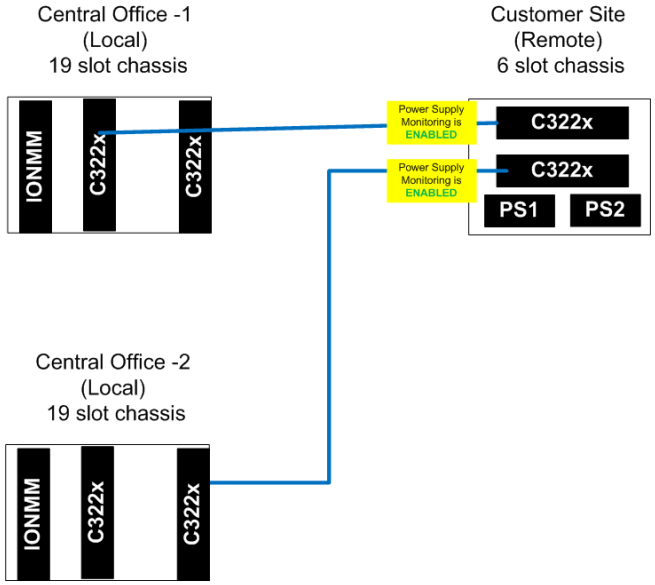
Scenario 2: This scenario where Remote Power Supply Monitoring is only Enabled on 2 cards in the Remote chassis DOES NOT WORK



Scenario 3: This scenario works, where Remote Power Supply Monitoring is only Enabled on 1 card each in two Remote chassis.



Scenario 4: This scenario where Remote Power Supply Monitoring is only Enabled on 2 cards each in one Remote chassis connected to two Local chassis DOES NOT WORK



Related Manuals

ION x222x32xx Web User Guide, 33472
ION x222-x32xx CLI Reference, 33473
ION Management Module (IONMM) User Guide, 33457 and Install Guide, 33420
IONMM-232 Install Guide, 33725
ION219-x 19-Slot Chassis Installation Guide, 33412
ION106-x Six Slot Chassis User Guide, 33658
IONPS-A-R1 AC Power Supply User Guide, 33614
IONPS-D-R1 DC Power Supply Install Guide, 33707
IONPS-A AC Power Supply Install Guide, 33423
IONPS-D DC Power Supply Install Guide, 33424

Appendix G: Local Management of Cards in a Remote Un-Managed Chassis

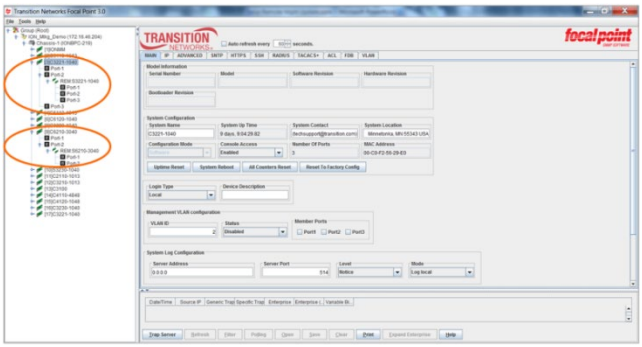
This section discusses managing the link between an ION Managed Chassis (MC) and an Un-managed Chassis (UC), and performing remote firmware upgrades.

Previous Status

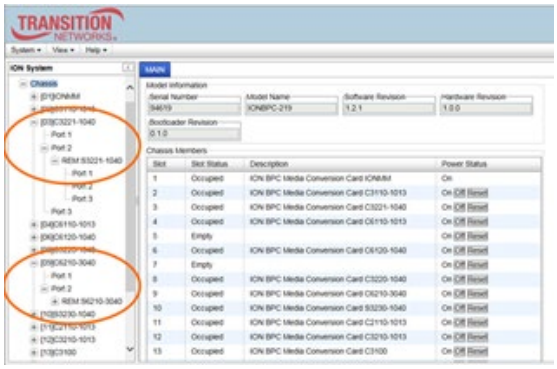
In previous firmware versions (e.g., x6110 / x6120 before v 1.2.8):

- All cards in an ION chassis can be managed via the IONMM.
- Some cards support remote management of a linked stand-alone, in-band, over the fiber, by the card in a local Managed Chassis (MC):
  - Ethernet: x2220, x3220, x3230, x4120
  - TDM: x6010, x6110, x6120, x6210
- Some cards do not support remote management of a linked stand-alone:
  - x2110, x2210, x3100, x3110, x3210, x4110

Local Management of a Remote Unit:



Focal Point



ION System

In firmware versions before v 1.2.8, support includes:

- A local Managed Chassis with an IONMM can manage a remotely managed standalone
- A local Managed Chassis with an IONMM can manage a remotely managed card in a 1- or 2-Slot ION Chassis

Not supported in firmware versions before v 1.2.8:

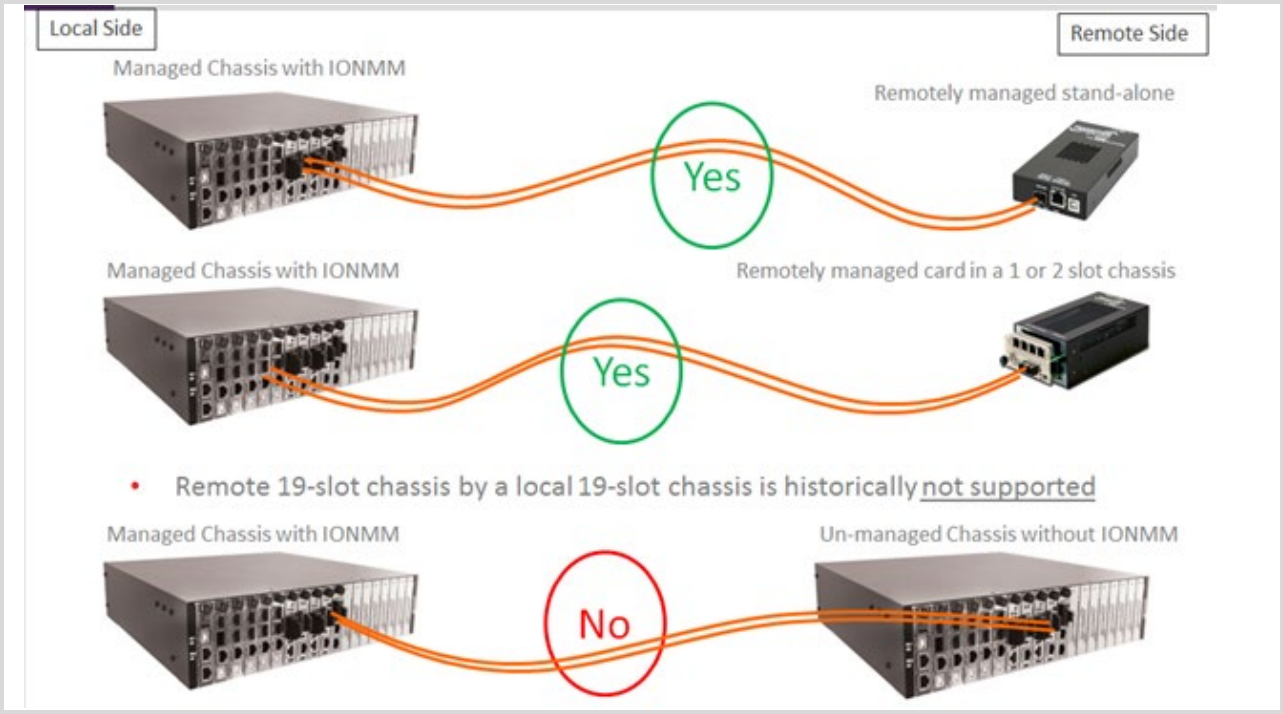
- Remote 19-slot Managed Chassis cannot manage a remote Un-managed Chassis that has no IONMM

In x6110 / x6120 firmware versions v 1.2.8 and after, Managed Chassis (MC) to Un-managed Chassis (UC) is supported with a firmware upgrade to the slide-in-card (S6110/S6120 v 1.28).

Note that no firmware upgrade to the IONMM is required.

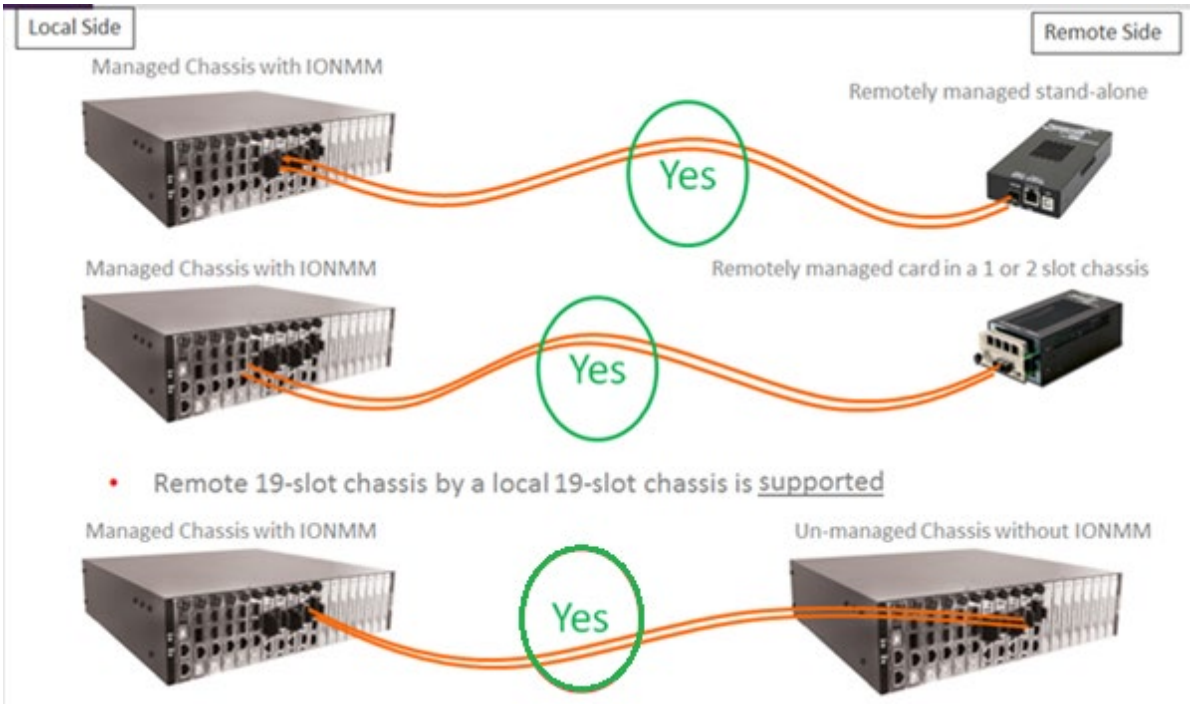
Previous Management of a Managed Chassis

Previously supported and un-supported configurations are shown below (before v 1.3.13).



New Chassis-to-Chassis Operation

Managed Chassis (MC) to Un-managed Chassis (UC) is now supported with a firmware upgrade (v 1.3.13 or above) to the slide-in-cards. No firmware upgrade to IONMM is required.



1. When a chassis is first powered up, the IONMM boots and sends LLDP discovery packets out to the chassis backplane to let the cards know that this is a managed chassis
   a) If IONMM exists: cards enter normal local management mode
   b) If no IONMM exists: cards enter remote management mode
2. When a managed chassis (MC) is first powered up:
   a) In approximately 40 seconds, the IONMM boots and the x6110 / x6120 / C4120 cards display in the Management interface.
   b) In 50 seconds to 1:25 minutes, the IONMM boots and the OAM Ethernet cards display in the Management interface.
3. During power up of an Un-managed Chassis (UC), the discovery (or non-discovery) of a Management Module takes time:
   a) Time for the TDM cards in the UC to be displayed in the MC: 1:05 minutes.
   b) Time for the remote cards in the UC to show up in the management interface of the MC: 3:40 minutes.

Required Firmware Versions

Slide-In-Card (SIC)	Environment	Minimum Firmware Version
x2220, x3220, x3230	Ethernet	Firmware v 1.3.13
x4120	Ethernet	Firmware v 1.2.6
x6010	TDM	Firmware v 1.2.6
x6110, x6120	TDM	Firmware v 1.2.8
x6210	TDM	Firmware v 1.2.5

ECO 1196 updated the Application .bin for C3230, C3231, S3230, and S3231 models:

□ C3230-1013	□ S3230-1013
□ C3230-1014	□ S3230-1014
□ C3230-1029-A1	□ S3230-1029-A1
□ C3230-1029-A2	□ S3230-1029-A2
□ C3230-1040	□ S3230-1040
□ C3231-1040	□ S3231-1040

Remote Firmware Upgrade

Remote firmware upgrade of cards in an UC is also supported. **Note** that:

- OAM Ethernet cards are easily upgraded in the field.
- TDM cards and x4120 require a boot loader upgrade first:
    - Can only be done in the factory
    - Field firmware upgrades can be done in a MC, and then the cards can be moved to the UC.
    - Field firmware upgrades in the UC cannot be done until the boot loader is upgraded at the factory.

C2220, C3220, & C3230 Series (OAM Managed 10/100 and 10/100/1000 Ethernet Media Converters):

- Firmware needed: x222x_x322x_1.3.13_AP.bin
- Firmware needed: x323x_1.3.13_AP.bin
- No bootloader upgrade required
- Time required for a card to be displayed in the Management interface:
    - Managed Chassis (MC):
        - Inserting a card in a MC takes 0:10 – 0:20 seconds
        - On chassis power up, cards appear in 0:50 – 1:25 seconds
    - Un-managed Chassis (UC):
        - Inserting a card in an UC takes 3:30 minutes
        - Upgrading a card in an UC takes 3:40 minutes

Issues

1. The bootloader upgrade requirement only affects cards in the field.
   a) New production units will already have the bootloader upgrade done in the factory.
2. On initial power up of chassis:
   b) The remote cards will take a few minutes longer to show up in the management display.
   c) Accessing management at a later date, on a chassis that is already powered up is much quicker; delays only occur on initial power up.
3. Adding at card to an already powered up chassis is 40 seconds quicker that times listed, because the IONMM is already booted up.
4. If a chassis is up and running as a remotely located, un-managed chassis, and you decide at a later date to add an IONMM, the chassis will have to be power cycled in order for the cards to report their status to the new local management module.

Default Configurations

The default configurations for ION cards are as follows:

Chassis cards (e.g., C2220, C3220, C3221 ...) defaults:

- Remote mode so the IONMM can see them.
- The IP stack is disabled so they don't have an IP address.
- USB is enabled.

Standalone cards S2220, S3220, S3230 defaults:

- Local mode.
- The IP stack is enabled.
- The local IP address is 192.168.0.10.
- USB is enabled.

Standalone cards S3221 and S3221 defaults:

- Remote mode so they can be seen by the IONMM hanging off a port of the local card.
- The IP stack is disabled so they don't have an IP address.
- USB is enabled.

Note: For the Local Management of Cards in a Remote Un-managed Chassis feature to work the card in the remote chassis must be set to "Remote" mode so the IONMM in the local chassis can see it hanging off the port of the local card. See “Changing Switch Mode (Local / Remote)” on page 74.

Changing Switch Mode (Local / Remote)

The NID default is changed to Local mode (instead of Remote mode) at ION v 1.3.10. When an ION NID is powered up, it will no longer come up in Remote mode. Instead it will come up in Local mode with DHCP enabled. If a DHCP server is not accessible, it will timeout and revert to the default static IP address 192.168.0.10.

Management and configuration control can be switched between local management control (via CLI, Telnet or Web) or remote management control (via the IONMM). By default, the x323x is managed by the IONMM.

The switch mode can only be changed for the NID using the CLI method.

The CLI command **set switch mode={local | remote}** changes the operating mode of a standalone device.

Remote Mode (default mode): the device can only be managed and configured via the IONMM. Setting the switch mode to remote indicates that the device is managed through the IONMM. The device cannot perform any IP management when in 'remote' mode.

Local Mode: the device can only be configured and managed directly via CLI, Telnet or Web. Setting the mode to **local** indicates that the device is managed through either a direct USB connection or a direct network connection via Telnet or the Web interface (i.e., the device is no longer managed by the IONMM).

Note: The x323x NIDs are shipped with switch mode set to "remote."

To change the device switch mode to local, do the following:

1. Start a USB session.
2. At the command prompt type **set switch mode=local**.
3. Press the **Enter** key.
4. Reboot the card for the changes to take effect. At the command prompt type **reboot**.

   Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory remove temporary files (e.g. configuration backup files, Syslog file).
5. Press the **Enter** key to reboot the module.
6. At the command prompt type **show switch mode**.
7. Press the **Enter** key. This displays the device's management mode - local or remote - indicating where the device is managed:
   - **local** – device is managed through direct connection to the device.
   - **remote** – device is managed through the IONMM.

Note: The system cannot show the switch mode on all card types.

Troubleshooting

Message: *Error: System is busy, please retry this command later!*

Symptom: long delay in CLI response for a C2220 in a 1 or 2 slot ION chassis.

Meaning: C2220 software v1.3.13 adds a new feature that allows a chassis card to be seen in an unmanaged chassis. The card looks for an IONMM in the chassis before completing its initialization, and in a 1 or 2 slot chassis it delays the longest before deciding there isn't an IONMM present.
When setting the card to **Local** mode you must wait for a timeout period of up to 5 minutes.
After the 5 minutes the card comes back and you can set the IP address to static and you will no longer get the error message of the card being “busy”.

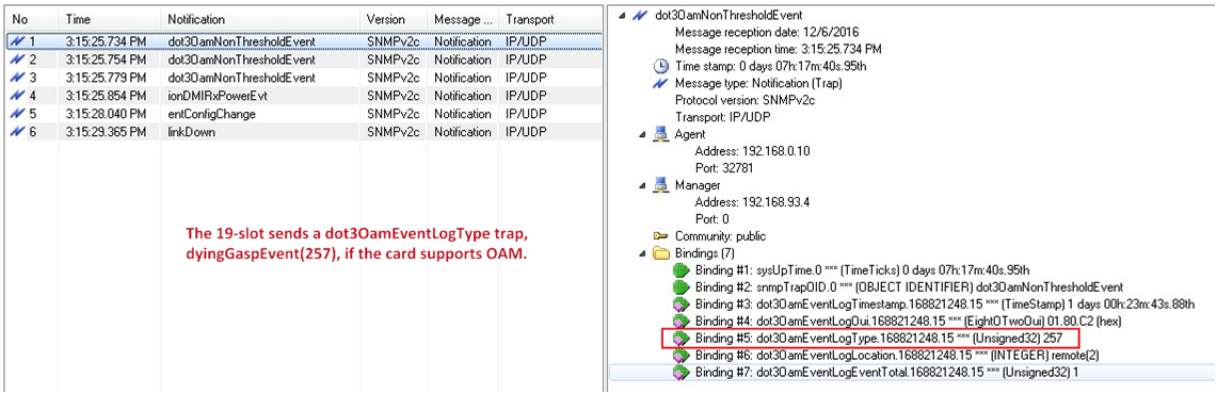
Example:

```
C0|S0|L1D>set switch mode local
Please reboot the card for the changes to take effect!
C0|S0|L1D>reboot
Warning: this command will restart system, connection will be lost and

please login again!

login: ION
Password:
Hello, this is ION command line (version 1.00).
Copyright 2009 Lantronix.

C0|S0|L1D>set curr-time="20180118 9:44:50"
Error: System is busy, please retry this command later!
C0|S0|L1D>show ip-mgmt cond fig
Error: System is busy, please retry this command later!
C0|S0|L1D>show system info
Error: System is busy, please retry this command later!

**************************************************
It takes 5 minutes to display the following response:
**************************************************

C0|S0|L1D>
```

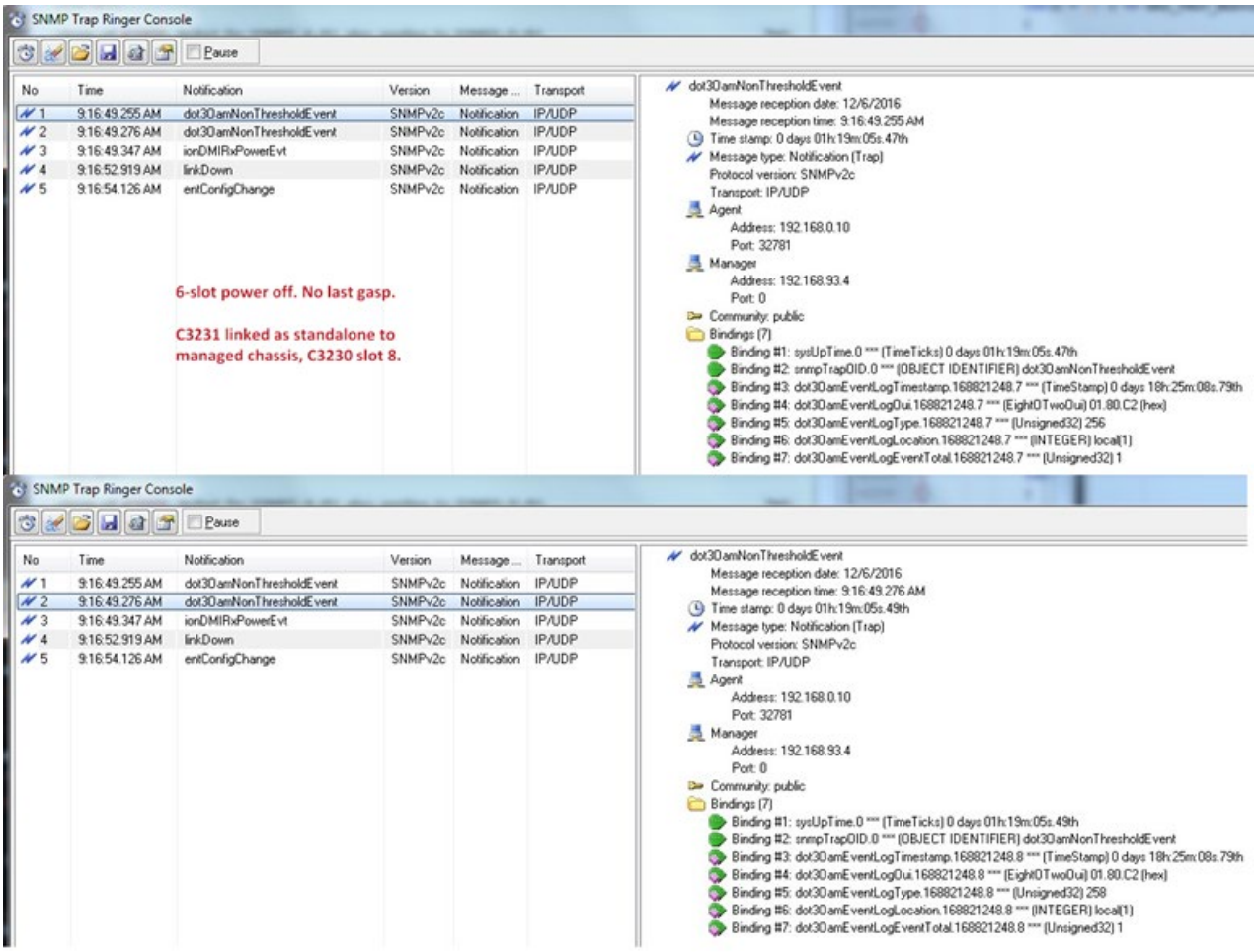
Recovery: Wait 5 minutes for the card to come back and the command prompt to display again.

Traps

The 19-Slot as a Remote Chassis: The ION219-x sends a *dot3OamEventLogType* trap; it also sends a *dyingGaspEvent(257)* **if** the card supports OAM.

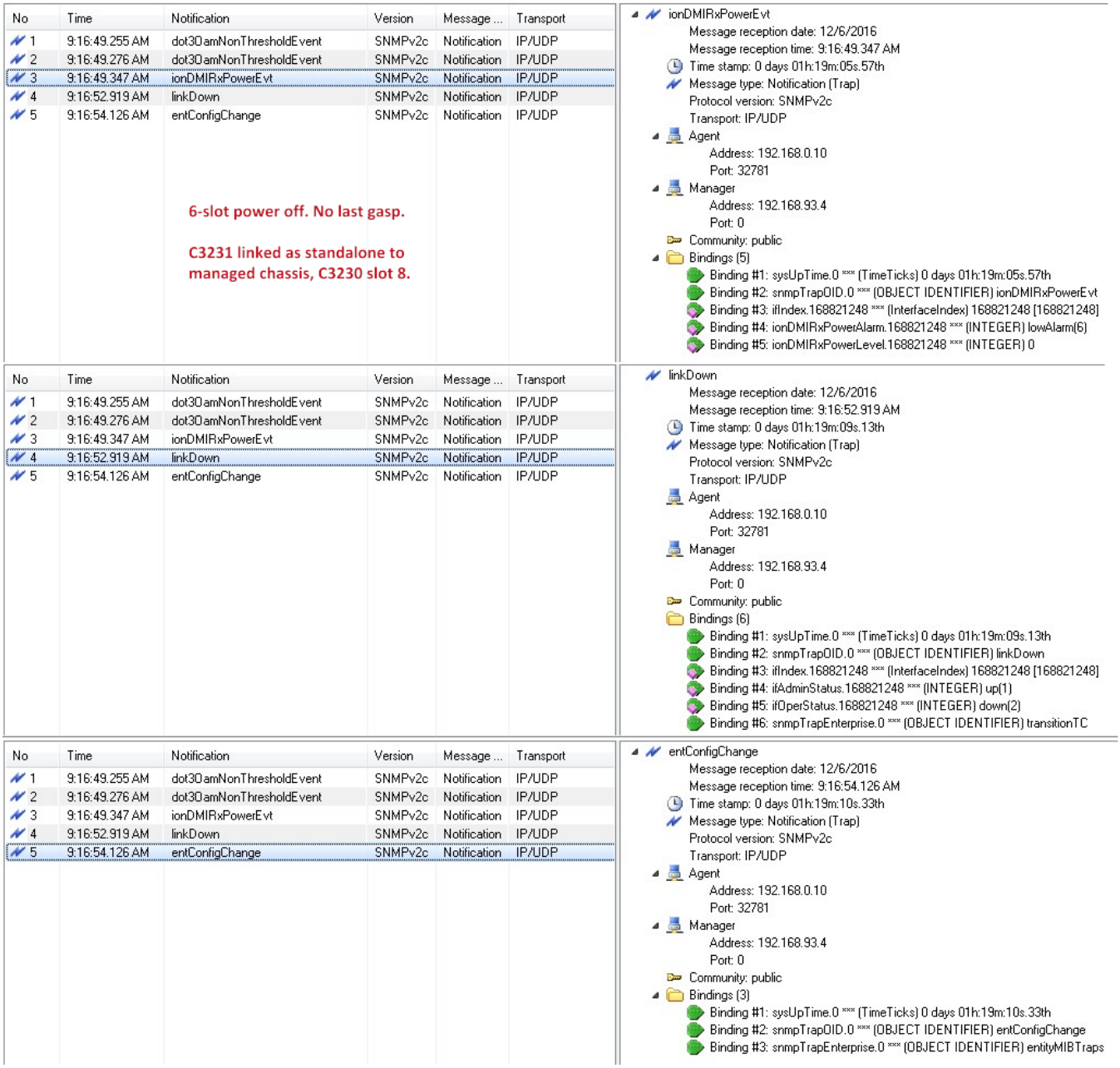


Unmanaged 6-slot with remote C3231 connected to a managed 19-slot, C3230 slot 8. Below are the traps seen by MG-Soft when the ION106-x lost power. There is no last gasp trap.

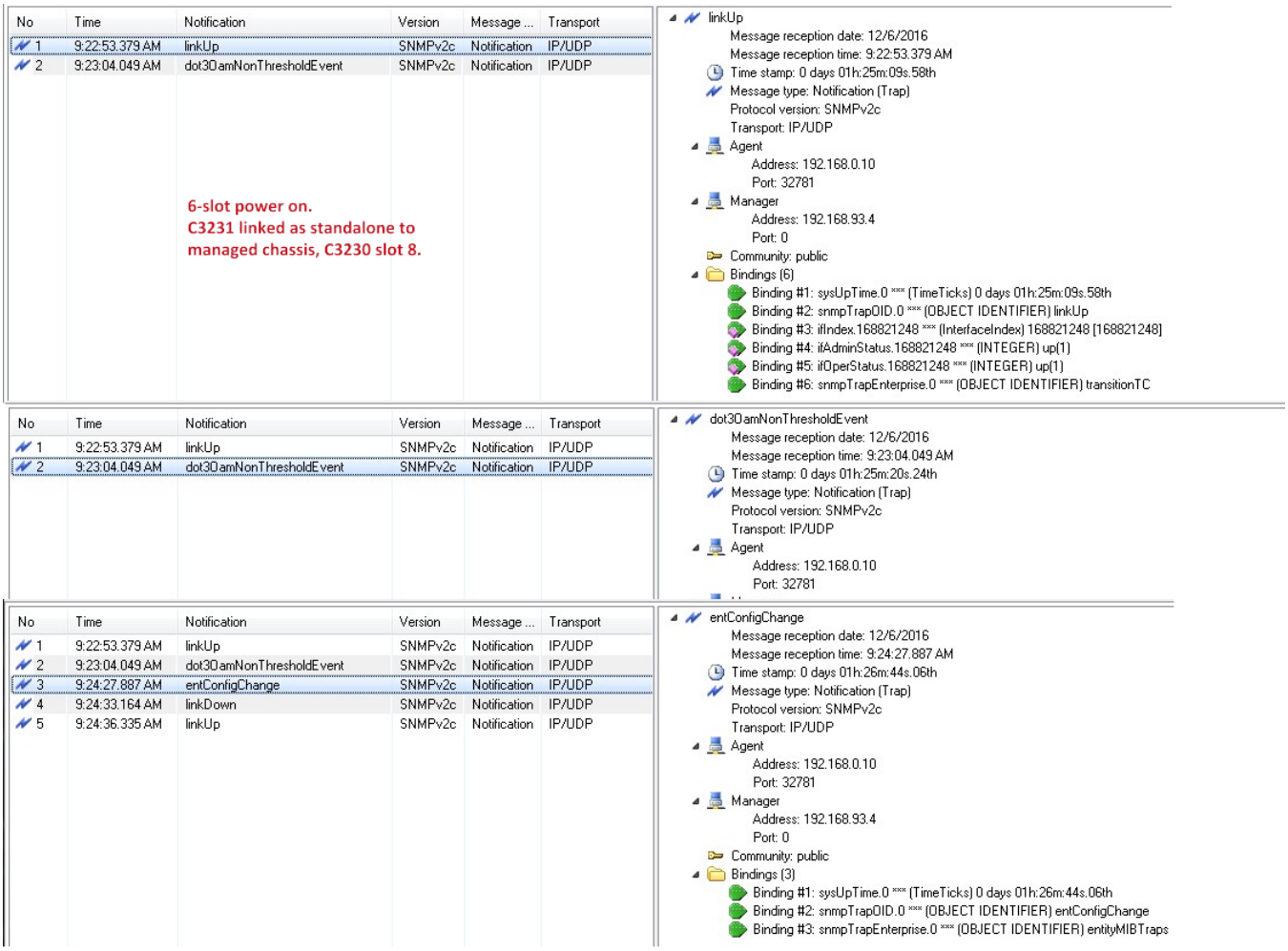


ION106-x power off. No last gasp. C3231 linked as standalone to managed chassis; C3230 in slot 8.

ION106-x power off. No last gasp. C3231 linked as standalone to managed chassis; C3230 in slot 8.



ION106-x power on. C3231 linked as standalone to managed chassis; C3230 in slot 8.



Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.