LANTRONIX®

ION System

IONMM, ION x323x NID

Command Line Interface (CLI) Reference

Part Number 33461
Revision G September 2025

Intellectual Property

Warranty

For details on the Lantronix warranty policy, please 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
08/21/14	E	Revised for v1.3.10 with IPv6, TACACS+ and Auto Provisioning support. Adds support for Zero Touch Provisioning ONLY in the standalone S3230-10xx and S3231-1040. Changes S3230 default mode from Remote to Local mode.
8/29/23	F	SW v1.3.26 with TLS v1.1 and 1.2 to HTTPS to prevent vulnerabilities to MITM and other security attacks. Add ION106 6-Slot chassis support. Adds support for manage chassis cards in a remote unmanaged chassis from a local managed chassis. Add support for IONPS-D-R1, DC power supply; remove fan-2 from IONPS-D; add cardtype for IONPS-A-R1 and IONPS-D-R1 in upgrade manager to allow field upgrades. Add C3231 VLAN Mode information. Add RMPS (Remote Manage Power Supply) feature, Local Management of Cards in a Remote Un-managed Chassis, and DMI Vendor Specific Information. Update ssh server to v2022.82, Link state now reflects admin state, improve SNMP community string backup and removal behavior, and improve Local and Remote backup in stand-alone modules. See Release Notes for Known Limitations. Remove Glossary and Index.
September 2025	G	SW v1.5.17 Add SFTP configuration commands. Add Backup All and Restore All commands. Updated Chapter 3, Command Matrix, for SFTP and Backup/Restore All.

Contents

Tables

1. Introduction

This manual describes the USB and Telnet command line interface (CLI) commands available for ION System chassis, IONMM (IONMM-232), or standalone x323x Remotely Managed Multiport NID operations. This manual is for experienced network administrators who are responsible for configuring and maintaining the ION system.

CLI offers the most comprehensive set of management features. CLI is used during the initial setup (set IPs etc.) and troubleshooting but can also be used for day-to-day management (device management, firmware upgrades, managing security features, etc.).

This manual documents the following models:

- **IONMM (IONMM-232)** Management Module
- **C3230** OAM/IP-Based Remotely-Managed NID
- **C3230** OAM/IP-Based Remotely-Managed NID (with DMI support)
- **C3230** OAM/IP-Based Remotely-Managed NID (single fiber products)
- **C3231** OAM/IP-Based Remotely-Managed NID (two open SFP slots)
- **S3230** OAM/IP-Based Remotely-Managed NID
- **S3230** OAM/IP-Based Remotely-Managed NID (with DMI support)
- **S3230** OAM/IP-Based Remotely-Managed NID (single fiber products)
- **S3231** OAM/IP-Based Remotely-Managed NID (two open SFP slots)

IMPORTANT

CLI commands are case sensitive. Enter the CLI commands as shown.

To execute the commands described in this manual, you must press the **Enter** key after the command has been entered.

Document Conventions

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

Table 1: Document 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

A printed Documentation Postcard is shipped with each x323x. A substantial set of technical documents, white papers, case studies, etc. are available on the Lantronix web site at https://www.lantronix.com/.
Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

The ION system and related manuals are listed below.

1. ION System 32xx NID User Guide, 33432
2. ION Management Module (IONMM) User Guide, 33457
3. ION219-A 19-Slot Chassis Installation Guide, 33412
4. IONMM Management Module Install Guide, 33420
5. ION106-x Six Slot Chassis User Guide, 33658

6. IONPS-A-R1 Power Supply User Guide, 33614
7. ION Dry Contact Relay (DCR) Kit Install Guide, 33422
8. IONPS-A AC Power Supply Install Guide, 33423
9. IONPS-D-R1 Power Supply User Guide, 33707
10. IONPS-D DC Power Supply Install Guide, 33424
11. IONPS-A ION AC Power Supply Install Guide, 33464
12. ION ADP PointSystem Card Adapter for ION Chassis 33413
13. SFP Modules (model specific)
14. Release Notes (software version specific)

Note: 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 examples may not display the latest version number, all the descriptions and procedures reflect the latest software/firmware version, noted in the Revision History.

Commands' Effect on Stored Files

IMPORTANT

 Certain CLI commands affect important stored files. 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). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key.

These CLI commands can cause a loss of files:

- **reboot** - cold start the system.
- **reset** - reset factory configuration.
- **restart** - restart ACL
- **upgrade** - upgrade firmware modules

See the specific command description for additional information.

2. Command Line Editing

This section describes how to enter CLI commands.

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters.

Display Similar Commands

At the command line, you can use the Tab key or the **?** key to show available commands in a category of commands after entering a part of the command.

For example, use the Tab key to enter part of the command (**show ether** in this example) to display all the available commands that start with **show ether**. The commands display in a single row.

```
C1|S7|L1D>show ether <tab key>
config      loopback    security    statistics  tdr
```

Use the **?** key after a partial CLI command entry to display all the available commands that start with **show ether**, but in a single column:

```
C1|S7|L1D>show ether ?
  config
  loopback
  security
  statistics
  tdr
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember to not leave a space between the command and question mark.) For example, "**s?**" shows all the keywords starting with "**s**."

Recall Commands

To recall recently-entered commands from the command history, perform one of the optional actions below:

Ctrl-P or **Up arrow** (↑) key: Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

Ctrl-N or **Down arrow** (↓) key: Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up arrow key. Repeat the key sequence to recall successively more recent commands.

Keystroke Commands

The table below shows the optional keystrokes available to edit command lines (*indicates HyperTerm support, ** indicates command prompt support, *** indicates both HT and command prompt support by this keystroke).

Table 2: Command Line Editing

Capability	Keystroke	Purpose
Move the command line around to make changes or corrections	Ctrl-B *** or left (←) arrow key ***	Move the cursor back one character
	Ctrl-F *** or right (→) arrow key ***	Move the cursor forward one character
	Ctrl-A ***	Move the cursor to the beginning of the command line
	Ctrl-E ***	Move the cursor to the end of the command line
Recall commands from the buffer and paste them in the command line	Ctrl-Y ***	Recall the most recent entry in the buffer
	Ctrl-T **	Transpose the character to the left of the cursor with the character located at the cursor
	Ctrl-Y **	Recall the most recent entry in the buffer
Delete entries (if you make a mistake or change your mind)	Delete key *** or Backspace key ***	Erase the character to the left of the cursor
	Ctrl-D ***	Delete the character at the cursor
	Ctrl-K ***	Delete all characters from the cursor to the end of the command line
	Ctrl-U *** or Ctrl-X ***	Delete all characters from the cursor to the beginning of the command line
	Ctrl-W ***	Delete the word to the left of the cursor
	Esc D **	Delete from the cursor to the end of the word
Capitalize or lowercase words or capitalize a set of letters	Esc C *	Change case from capital to lower-case (or lower-case to capital) at the cursor
Redisplay the current command line if the switch unexpectedly sends a message to your screen	Ctrl-L *** or Ctrl-R ***	Redisplay the current command line (reverse-i-search)

3. Command Matrix

The table below lists all the CLI commands and categories, and indicates if the command applies to the IONMM, x323x NIDs, or both.

Note: CLI commands are case sensitive. Enter the CLI commands as shown.

Table 3: CLI Command Matrix

System Commands	IONMM	NIDs
Login Password for Access	x	x
Log Out (Quit)	x	x
Clear the Screen	**x**	**x**
Go Back to IONMM	**x**	**x**
Go to Another Location	**x**	**x**
Help	**x**	**x**
List	**x**	**x**
Ping	**x**	**x**
Ping6	**x**	**x**
Reboot	**x**	**x**
Reset Factory Configuration	**x**	**x**
Reset System Uptime	**x**	**x**
Set USB Port State	**x**	**x**
Show USB Port State	**x**	**x**
Slot Power On / Power Off / Reset	**(PS)**	**(PS)**
Set Current Time	**x**	**x**
Set Debug Level	**x**	**x**
Set Power Relay State	**(PS)**	**(PS)**
Set PS Sensor Notification / Relation / Severity / Value	**(PS)**	**(PS)**
Set System Contact	**x**	**x**
Set System Location	**x**	**x**
Set System Name	**x**	**x**

System Commands	IONMM	NIDs
Show Card Information	x	x
Show Card Type	x	x
Show Chassis Information	x	x
Show Device Mode	x	x
Show Power Supply Configuration		x
Show Slot Information	x	x
Show System Information	x	x
Switch Device Mode	x	x
Set Circuit ID		x
Show Circuit ID		x

ACL Commands	IONMM	NIDs
Add a New ACL Condition	x	x
Add a New ACL Rule	x	x
Add IPv6 Tables ACL Condition Type	x	x
Add IPv6 Tables ACL Rule Index		
Add IPv6 Tables ACL Rule Position	x	x
Remove ACL Conditions	x	x
Remove ACL Rules	x	x
Remove IPv6 Tables ACL Condition	x	x
Remove IPv6 Tables ACL Condition All	x	x
Remove IPv6 Tables ACL Rule	x	x
Remove IPv6 Tables ACL Rule All	x	x
Restart ACL	x	x
Restart IPv6 Tables ACL	x	x

ACL Commands	IONMM	NIDs
Set ACL State	x	x
Set ACL Chain Default Policy	x	x
Set Certain Conditions to a Rule	x	x
Set IPv6 Tables ACL Condition / Rule Index	x	x
Set IPv6 Tables ACL Rule / Traprate	x	x
Set IPv6 Tables ACL State	x	x
Set IPv6 Tables ACL Table / Chain / Policy	x	x
Set IPv6 Tables ACL Table	x	x
Set Trap Rate of a Rule	x	x
Show ACL State	x	x
Show All ACL Conditions	x	x
Show All ACL Rules	x	x
Show All IPtable Chain Definitions	x	x
Show IP6 Tables ACL Chain	x	x
Show IP6 Tables ACL Condition	x	x
Show IP6 Tables ACL Rule	x	x
Show IP6 Tables ACL State	x	x

Backup / Restore Commands	IONMM	NIDs
Backup	x	
Restore	x	
Set Backup / Restore Module Index	x	
Show Modules	x	
Backup All	x	
Restore All	x	

Bandwidth Commands	IONMM	NIDs
Set Bandwidth Rate Limiting Mode		x
Set Bandwidth Rate Limit		x

DMI Commands	IONMM	NIDs
Show DMI Configuration		x
Set DMI Receive Power Preset Level		x

Dot1bridge / Dot1dbridge Commands	IONMM	NIDs
Add Dot1bridge Port		x
Assign Dot1bridge Name		x
Remove Dot1bridge		x
Remove Dot1bridge Port		x
Set Dot1bridge Aging Time		x
Set Dot1bridge Community		x
Show Dot1bridge Aging Time		x
Show Dot1dbridge IEEE-Tag Priority Remapping		x
Show Dot1dbridge IP-TC Priority Remapping		x

Ethernet Port Commands	IONMM	NIDs
Clear Ethernet Port Counters		x
Reset All Ports Counters		x
Set Ethernet Port L2CP Configuration		x
Show Ethernet Port L2CP Configuration		x
Set Ethernet Port Admin Status		x
Set Ethernet Port Advertisement Capability		x
Set Ethernet Port AutoCross		x
Set Ethernet Port Auto-Negotiation Status		x
Set Ethernet Port Duplex		x
Set Ethernet Port Far End Fault		x
Set Ethernet Port Filter 802.1Q Tagged Non-Mgmt Frames		x
Set Ethernet Port Filter 802.1Q Untagged Non-Management Frames		x
Set Ethernet Port Loopback Type		x

Ethernet Port Commands	IONMM	NIDs
Set Ethernet Port Pause Frames		x
Set Ethernet Port Source MAC Address Lock		x
Set Ethernet Port Source MAC Address Lock Action		x
Set Ethernet Port Speed		x
Set Port Admin Mode (Ethernet PHY Mode)		x
Show Ethernet Port Configurations		x
Show Ethernet Port Loopback Capability		x
Show Ethernet Port Loopback Running Status		x
Show Ethernet Port Security Configuration		x
Show Ethernet Port TDR Test Configuration		x
Show Ethernet Port TDR Test Result		x
Start/Stop Ethernet Port Loopback Operation		x
Start Ethernet Port TDR Test		x
Show Ethernet Statistics		x

Firmware Upgrade Commands	IONMM	NIDs
Show Firmware Database Update Results	x	
Show Firmware Upgrade Results	x	
Show Upgrade File Name	x	
Update Firmware Database	x	
Upgrade Device Firmware	x	

Forwarding Database Commands	IONMM	NIDs
Add Forwarding Database Entry		x

Forwarding Database Commands	IONMM	NIDs
Remove a Single Forwarding Database Entry		x
Remove All Forwarding Database Entries		x
Set Forwarding Database Connection Port		x
Set Forwarding Database Entry Type		x
Set Forwarding Database Priority		x
Set Forwarding Portlist		x
Set Forwarding Port Management Access		x
Show Forwarding Database Configuration		x
Show Forwarding Database Ports		x

HTTPS Commands	IONMM	NIDs
Set HTTPS Certificate File	x	x
Set HTTPS Certificate Type	x	x
Set HTTPS Port Number	x	x
Set HTTPS Private Key File	x	x
Set HTTPS Private Key File Password	x	x
Set HTTPS State	x	x
Show HTTPS Configuration	x	x
Start HTTPS Certificate Operation	x	x

IP/DNS/DHCP Commands	IONMM	NIDs
Set DCHP Client State	x	x
Set DNS Server Number / Type / Address	x	x
Set IP Type / Address / Subnet Mask	x	x

IP/DNS/DHCP Commands	IONMM	NIDs
Set Gateway Type / Address	x	x
Set IP Address Mode	x	x
Set IP Management State	x	x
Show IP Configuration	x	x
Set IPv6 Management State	x	x
Set IPv6 Address Mode	x	x
Set IPv6 Gateway Mode	x	x

LPT Commands	IONMM	NIDs
Set Link Pass Through Monitoring Port		x
Set Link Pass Through Status		x
Set Selective Link Pass Through Status		x
Set Transparent Link Pass Through Status		x
Show Link Pass Through Configurations		x

LOAM Commands	IONMM	NIDs
Clear LOAM Statistics		x
Get LOAM Peer Vendor OUI		x
Get LOAM Peer Information		x
Set LOAM Admin State		x
Set LOAM Critical Event Notification State		x
Set LOAM Dying Gasp Event Notification State		x
Set LOAM Errored Frame Event Notification State		x
Set LOAM Errored Frame Threshold Value		x

LOAM Commands	IONMM	NIDs
Set LOAM Errored Frame Window Value		x
Set LOAM Errored Frame Period Event Notification State		x
Set LOAM Errored Frame Period Threshold Value		x
Set LOAM Errored Frame Period Window Value		x
Set LOAM Errored Frame Seconds Summary Event Notification State		x
Set LOAM Errored Frame Seconds Summary Threshold Value		x
Set LOAM Errored Frame Seconds Summary Window Value		x
Set LOAM Errored Symbol Period Event Notification State		x
Set LOAM Errored Symbol Period Threshold Value		x
Set LOAM Errored Symbol Period Window Value		x
Set LOAM Ignore Loopback Requests		x
Show LOAM Ignore Loopback Requests		x
Set LOAM Mode		x
Show LOAM Configuration		x
Show LOAM Event Configuration		x
Show LOAM Event Log		x
Show LOAM Peer Configuration		x
Show LOAM Statistics		x

MAC Learning Commands	IONMM	NIDs
Set MAC Learning Enable Portlist		x
Show Port MAC Learning State		x

Performance/RMON Statistics	IONMM	NIDs
Show RMON Statistics	x	x

QoS Commands	IONMM	NIDs
Set Default Priority for a Port		x
Set Frame Priority: Destination MAC Address is Used		x
Set Frame Priority: IEEE Tag is Used		x
Set Frame Priority: IP Tag is Used		x
Set Frame Priority: Source MAC Address is Used		x
Set Frame Priority: VLAN ID is Used		x
Set IEEE Priority Remapping		x
Set Ingress Priority Remapping		x
Set IP Traffic Class Priority Remapping		x
Set Port Egress Queuing Method		x
Set Priority Type		x
Show Priority Remapping		x
Show QoS Configuration of a Port		x

RADIUS Commands	IONMM	NIDs
Set RADIUS Authentication	x	x
Set RADIUS Retry	x	x
Set RADIUS Server	x	x
Set RADIUS Server Secret	x	x
Set RADIUS Timeout	x	x
Show RADIUS Configuration	x	x

Redundancy Commands	IONMM	NIDs
Set Redundancy State	x	x
Show Redundancy Info	x	x

SFTP Commands	IONMM	NIDs
Get SFTP Server IP Address	x	
Set SFTP Server IP Address	x	
Set SFTP Port Number	x	
Show SFTP Configuration	x	
Set SFTP Username	x	
Set SFTP Password	x	
Set SFTP State	x	
Set SFTP Server path	x	
Download remote file from SFTP server	x	
Download and install IONMM firmware via SFTP	x	

Serial File Transfer Protocol (X/Y/Zmodem) Commands	IONMM	NIDs
Serial Get Protocol	x	
Serial Put Protocol	x	
Serial Upgrade Protocol	x	

SNMP Commands	IONMM	NIDs
Add SNMP Community Name / Access Mode	x	
Add SNMP Group	x	
Add SNMP Local User	x	
Add SNMP Remote Engine	x	
Add SNMP Remote User Name / Address Type	x	
Add SNMP Remote User Name / Engine	x	
Add SNMP Traphost	x	
Add SNMP View Name	x	
Remove SNMP Community Name	x	
Remove SNMP Group	x	
Remove SNMP Local User	x	
Remove SNMP Remote Engine	x	
Remove SNMP Remote User Name / Address Type	x	
Remove SNMP Remote User Name / Engine ID	x	
Remove SNMP Traphost	x	
Remove SNMP View	x	
Set SNMP Local Engine	x	
Set SNMP Local User Name	x	
Set SNMP View	x	
Show SNMP Community	x	
Show SNMP Group	x	
Show SNMP Local Engine	x	
Show SNMP Local User	x	
Show SNMP Remote Engine	x	
Show SNMP Remote User	x	

SNMP Commands	IONMM	NIDs
Show SNMP Traphost	x	
Show SNMP View	x	

SNTP Commands	IONMM	NIDs
Set Current Time	x	x
Set SNTP Daylight Saving Time Status	x	x
Set SNTP Daylight Saving Start Time	x	x
Set SNTP Daylight Saving End Time	x	x
Set SNTP Daylight Saving Offset	x	x
Set SNTP Server Address	x	x
Set SNTP Status	x	x
Set SNTP Timezone	x	x
Show SNTP Configuration	x	x
Show SNTP Timezone	x	x

SOAM Commands	IONMM	NIDs
Initialization Commands		
Show Sender ID Configuration		x
Show SOAM Configuration Error List		x
Show SOAM Port		x
Show SOAM Port ID		x
Maintenance Domain Commands		
Add Maintenance Domain		x
Remove Maintenance Domain		x
Set Sender ID Permissions		x
Show Maintenance Domain		x
Maintenance Association Commands		
Add Maintenance Association		x
Remove Maintenance Association		x
Set Maintenance Association Parameters		x
Show Maintenance Association		x
Management Entity Group Commands		
Add Maintenance Entity Group		x
Remove Maintenance Entity Group		x
Set Maintenance Entity Group Parameters		x
Show Maintenance Entity Group		x
SOAM MEP Commands		
Add a MEP		x
Remove MEP		x
Set MEP Parameters		x
Show MEP Configuration		x

Show MEP statistics		x
Show CC Database for a MEP		x
MEP Loopback Commands		
Initiate a Loopback Request		x
Show Status of a Loopback Request		x
MEP Link Trace Commands		
Initiate a Linktrace Request		x
Show Status of a Linktrace Request		x
MEP Frame Loss Measurement Commands		
Configure Periodic Loss Measurement		x
Show Periodic Loss Measurement		x
MEP Delay Measurement Commands		
Initiate a Delay Measurement Request		x
Show Delay Measurement Results		x
MEP ETH TEST Commands		
Initiate an ETH–TST Request		x
Show the Status of the ETH–TST Requests		x
Initiate an ETH–MCC Request		x
SOAM MIP Commands		
Add a MIP		x
Remove a MIP		x
Set MIP Parameters		x
Show MIP Configuration		x
Show MIP Statistics		x

SSH Commands	IONMM	NIDs
Generate SSH Host Key	x	x
Remove SSH Host Key	x	x
Remove SSH Public Key From a User	x	x
Set SSH Authentication Retry	x	x
Set SSH Public Key to a User	x	x
Set SSH Server State	x	x
Set SSH Timeout	x	x
Show SSH Configuration	x	x
Show SSH Host Key	x	x
Show SSH Public Key of a User	x	x

Syslog Commands	IONMM	NIDs
Clear Syslog Records	x	x
Set Syslog Level	x	x
Set Syslog Mode	x	x
Set Syslog Server Port	x	x
Set Syslog Server Type / Address	x	x
Show Syslog Configuration	x	x

System User / Login Commands	IONMM	NIDs
Add a New System User	x	**
Change System User's Access Level	x	**
Change System User's Password	x	**
Remove an Existing System User	x	**

** Supported on IONMM or a standalone SIC only.

TACACS+ Commands		
Set Tacplus Client State	x	x
Set Tacplus Server / Retry	x	x
Set Tacplus Server / Secret	x	x
Set Tacplus Server / Timeout	x	x
Set Tacplus Server / Type / Address	x	x
Show Tacplus Config	x	x
Set Login Method	**x**	**x**

TFTP Transfer / Upgrade Commands		
TFTP Get	**x**	**x**
TFTP Put	**x**	**x**
TFTP Upgrade	**x**	**x**

TNDP Commands	IONMM	NIDs
Set TNDP TX State		x
Show TNDP TX State		x

VLAN Commands		
Management VLAN Commands	**IONMM**	**NIDs**
Set Management VLAN Admin State	**x**	**x**
Set Management VLAN ID	**x**	**x**
Set Management VLAN Ports	**x**	**x**
Show Management VLAN Configuration	**x**	**x**

VLAN Commands		
VLAN Device Level Commands		
Add VLAN Database Entry		**x**
Flush VLAN DB		**x**
Flush VLAN FID		**x**
Remove All VLANs		**x**
Remove a Single VLAN Database Entry		**x**
Set VLAN Database Member/Egress Tagging		**x**
Show VLAN Database Configuration		**x**
Show VLAN Service Configuration		**x**

VLAN Port-Level Commands	IONMM	NIDs
Set Ethernet Type When VLAN Tagging Mode Is Provider		**x**
Set Force Port To Use Default VID		**x**
Set VLAN Network Tagging Mode		**x**
Set VLAN Port Admin State		**x**
Set VLAN Port Default VID		**x**
Set VLAN Port Discard Tagged Non-Management Frames		**x**
Set VLAN Port Discard Untagged Non-Management Frames		**x**
Set VLAN Port Tag Mode		**x**

4. System Commands

The following are basic system level commands. These commands are used to show configuration / mode, show help, reboot the system, reset the configuration, and other basic functions.

Password for Login / Access

Syntax: Password: **private**

Description: The default device CLI password. CLI entry requires a successful password entry.

Example:

```
Password:
Login incorrect
login: ION
Password:private

Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

AgentIII C1|S1|L1D>
```

To control the NIDs via a USB interface, the command line prompt must be showing the location of the module to be managed. Use the procedure below to access the NID and login via USB connection.

1. Start the terminal emulator program (e.g., HyperTerminal).

2. When the emulator screen displays, press **Enter**. The login prompt displays. If your system uses a security protocol (e.g., RADIUS, SSH, etc.), you must enter the login and password required by that protocol.

3. Type **ION** (all upper case) and press **Enter**. The password prompt displays. If a "Login incorrect" message displays, ignore it.

4. Type your password. The default is **private** (all lower case).

5. Press **Enter**. The HyperTerminal command line prompt displays (C1|S3|L1D>).

6. Enter CLI commands to set up, configure, operate, and maintain the NID.

Log Out (Quit)

Syntax : quit

Description: Exit the current mode and return to the previous mode (i.e., the CLI command line prompt).

Example :

```
C1|S3|L1D>q
login:
```

Note: The NID does not automatically log out upon exit or after a timeout period, which could leave it vulnerable if left unattended. Follow your organizational policy on when to log out.

Clear the Screen

Syntax: **cls**

Description: Clears the screen.

Go Back to IONMM

Syntax: **home**

Description: Sets the command prompt back to the location of the IONMM.

Example: If the IONMM card is in chassis 1/slot 1 and the following command was entered.

```
C1|S13|L0AP1|L1P2|L2D>home
```

The new command line prompt would be

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

Go to Another Location

Syntax: **go** [**c=<**vv>] [**s=<**ww>] [**l1ap=**<xx>] [**l2ap=**<yy>] <zz>

Description: Defines the location (card or port) where subsequent commands are destined for. This information displays on the command prompt line as the location where the command will be executed.

where:

c = optional; number (1–16) of the chassis where the card/port is located

s = optional; number (1–32) of the slot in the chassis where the card/port is located. **Note:** if the chassis parameter (c=) is specified, you must specify a slot number.

v = optional; port number (1–16) on a level 1 device used to attach to a level 1 device

w = optional; port number (1–16) on a level 2 device used to attach to a level 2 device

x = mandatory; specifies the port or device where subsequent commands are destined for. Valid choice are:

- **l1d** – indicates the level 1 device
- **l1p=**<port#> – port number (1–16) on a level 1 device
- **l2d** – indicates the level 2 device
- **l2p=**<port#> – port number (1–16) on a level 2 device
- **l3d** – indicates the level 3 device
- **l3p=**<port#> – port number (1–16) on a level 3 device

Usage:

```
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.

Example 1: The following command would cause all subsequent commands to be executed for the device in slot 5 of chassis 1.

```
C1|S1|L1D>go s=5 l1d
```

The new command prompt would be:

```
C1|S5|L1D>
```

Example 2: The following **go** command would cause all subsequent commands to be executed for port 2 on the device in slot 5.

```
C1|S5|L1D>go l1p=2
```

The new command prompt would be:

```
C1|S5|L1P2>
```

Example 3: The following **go** command would cause all subsequent commands to be executed for a remote device connected to port 2 of a chassis-resident module in slot 5.

```
C1|S5|L1D>go l1ap=2 l2d
```

The new command prompt would be:

```
C1|S5|L1AP2|L2D>
```

Help

Syntax: **?**

Description: Display help for CLI commands by typing a question mark (**?**). Typing a **?** at the command line prompt displays a list of base commands (show, set, etc.).
To display a list of the options for a particular command or parameter, type the command/parameter then a space and then **?**. See "Appendix A" for a complete list of CLI commands.

Examples: The following will display a list of all base commands.

```
C1|S2|L1D>?
  add       Add a ACL condition
  cat       Show the content of the FILES
  cd        Change to another directory
  clear     Clear all counters of the specified Ethernet port
  cls       Clear the screen.
  :
```

While the following will display a list of all the second entries for the **add** command.

```
C1|S2|L1D>add ?
     acl
     fwddb
     soam
     vlan
     vlan-db
```

By typing a **?** after each parameter in a command string you can see what the options are, either for what the next parameter is or for what options must be specified following an equal sign.

The following displays that there are two options available after ACL.

```
C1|S2|L1D>add acl ?
     condition
     rule
```

While the following **?** command displays the next parameter that follows condition.

```
C1|S2|L1D>add acl condition ?
     type
```

And finally, the following **?** command shows the options that can be specified for type=.

```
C1|S2|L1D>add acl condition type ?
     macaddr
     ipv4
     ipv4addrrange
     ipv4network
     tcpport
```

```
     tcpportrange
     udpport
     udpportrange
     icmp
```

List

Syntax: **list**

Description: Displays all available command line commands.

Example (partial list):

```
C1|S5|L1D>list
add acl condition type=(macaddr|ipv4addr|ipv4addrrange|ipv4network|tcpport|tcp
 portrange|udpport|udpportrange|icmp) srcdst=(src|dst) oper=(equal|notequal) value=VAL
add acl condition type=(macaddr|ipv4addr|ipv4addrrange|ipv4network|tcpport|tcp
portrange|udpport|udpportrange|icmp) srcdst=(src|dst) oper=(equal|notequal) value=VAL in-
dex=COND_ID
add acl rule index=RULE_ID table=(raw|filter|nat|mangle) chain=(prerouting|input
 |forward|output|postrouting) prio= PRIO policy=(accept|drop|trap) [traprate=TRAPRATE]
:
:
show vlan-db config
start ether tdr test
start https certificate
stat
tftp get iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
  tftp put iptype=(ipv4|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
  tftp upgrade iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE
  update firmware-db file=FILENAME
  upgrade module
C1|S5|L1D>
```

Note: See "Appendix A: CLI Command Summary" for a complete **list** command listing.

Ping

Syntax: **ping**

Description: Sends an ICMP ECHO-REQUEST to a network host and displays ping statistics (e.g., 4 packets received, 0% packet loss if successful or 0 packets received 100% packet loss if unsuccessful).

Example:

```
C1|S7|L1D>ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): 56 data bytes
64 bytes from 192.168.1.10: icmp_seq=0 ttl=64 time=2.3 ms
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.8 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.8 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.8 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.1/2.3 ms
```

Options:

```
C1|S7|L1D>ping [OPTION]... host
where:
  -c  CNT     Send only CNT pings
  -s  SIZE    Send SIZE data bytes in packets (default=56)
  -I  IP      Use IP as source address
  -q          Quiet mode, only displays output at start and when finished
```

Note: the **Ping** command can only be entered from the IONMM.

Ping6

Syntax: **ping6** [-c COUNT] [-t TTL] ADDR

Description: Send ICMP ECHO-REQUEST to network hosts, where:

[**-c COUNT**] = Number of echo requests to send. Stop after sending count ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.

[**-t TTL**] = Timeout in milliseconds to wait for each reply. This sets the IP Time to Live. The TTL value of an IP packet represents the maximum number of IP routers that the packet can go through before being thrown away. In current practice you can expect each router in the Internet to decrement the TTL field by exactly one.

The TCP/IP specification states that the TTL field for TCP packets should be set to 60, but many systems use smaller values (4.3 BSD uses 30, 4.2 used 15).

The maximum possible value of this field is 255, and most UNIX systems set the TTL field of ICMP ECHO_REQUEST packets to 255. This is why you can ''ping'' some hosts, but not reach them via telnet or ftp.

ADDR = Source address to use. -I interface address: Set source address to specified interface address. Argument may be numeric IP address or name of device. This option is required for pinging an IPv6 link-local address. Must be a valid IPv6 address.

Example:

```
Agent III C1|S1|L1D>ping6 fe80::2c0:f2ff:fe20:de9e
PING fe80::2c0:f2ff:fe20:de9e (fe80::2c0:f2ff:fe20:de9e): 56 data bytes
64 bytes from fe80::2c0:f2ff:fe20:de9e: icmp6_seq=0 ttl=64 time=0.9 ms
64 bytes from fe80::2c0:f2ff:fe20:de9e: icmp6_seq=1 ttl=64 time=0.8 ms
64 bytes from fe80::2c0:f2ff:fe20:de9e: icmp6_seq=2 ttl=64 time=0.8 ms
64 bytes from fe80::2c0:f2ff:fe20:de9e: icmp6_seq=3 ttl=64 time=0.8 ms

--- fe80::2c0:f2ff:fe20:de9e ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.9 ms
Agent III C1|S1|L1D>ping6 ?
BusyBox v1.4.1 (2011-11-07 12:05:46 CST) multi-call binary

Usage: ping6 [OPTION]... host

Send ICMP ECHO_REQUEST packets to network hosts

Options:
        -c CNT  Send only CNT pings
        -s SIZE Send SIZE data bytes in packets (default=56)
        -q      Quiet mode, only displays output at start
                and when finished
```

```
Agent III C1|S1|L1D>ping6
  ping6  Send ICMP ECHO-REQUEST to network hosts.
Agent III C1|S1|L1D>
```

Messages:

Error: this command should be executed on a device!
Ping command can only be used on management card!
Ping command can only be used on local standalone card!
Set ipv4 gateway address type
System is busy, please retry this command later!

Process Snapshot

Syntax: **ps**

Description: Displays a snapshot of the current memory processes. For example:

```
Agent III C1|S1|L1D>ps
  PID  Uid     VmSize Stat Command
    1 root        312 S   init
    2 root            SWN [ksoftirqd/0]
    3 root            SW  [watchdog/0]
    4 root            SW< [events/0]
    5 root            SW< [khelper]
    6 root            SW< [kthread]
   37 root            SW< [kblockd/0]
   40 root            SW< [khubd]
   53 root            SW  [pdflush]
   54 root            SW  [pdflush]
   55 root            SW< [kswapd0]
   56 root            SW< [aio/0]
  651 root            SW  [mtdblockd]
  681 root            SW< [spi_gpio.0]
  695 root            SWN [jffs2_gcd_mtd6]
  700 root            SWN [jffs2_gcd_mtd7]
  701 root            SWN [jffs2_gcd_mtd8]
  723 root        296 S   upgradeManager -d -l 1
  733 root       1800 S   snmpd -Lsd -c /etc/snmpd.conf
  734 root        244 S < bpd_linux
  739 root        240 S   pure-ftpd (SERVER)
  742 root       1336 S   entityManager -Lsd
  744 root       2776 S   subagent
  745 root        244 S   xxdp
  746 root        240 S   agent_pm
  757 root       2776 S   subagent
  758 root       2776 S   subagent
  759 root       2776 S   subagent
  760 root       2776 S   subagent
  763 root       2776 S   subagent
  788 root        268 S N monitor /usr/local/bin/taskmonitor.conf /agent3/conf/
  792 root        224 S   init
  798 root        356 S   radiuscd 0
  809 root        284 S   sntpcd
  827 root       1008 S   lighttpd -f /etc/lighttpd.conf
  836 root        176 S   telnetd -p 17800
  840 root        176 S   telnetd -l /usr/local/bin/a3cli
  843 root       2776 S   subagent
  844 root       2776 S   subagent
  845 root       2776 S   subagent
  848 root       2776 S   subagent
  849 root       2776 S   subagent
  850 root       2776 S   subagent
  853 root       2776 S   subagent
  854 root       2776 S   subagent
  859 root        276 S   syslogd -m 0 -L -O /var/log/sys.log -l 6 -s 200 -b 1
  860 root       2776 S   subagent
  867 root        460 S   tacplus
 1297 root       2640 S   /usr/local/bin/a3cli --
18919 root        304 S   sh -c ps
18920 root        284 R   ps
Agent III C1|S1|L1D>
```

Show Current Directory

Syntax: **pwd**

Description: Displays the current directory.

Example:
```
C1|S7|L1D>pwd
/
```

Reboot

Syntax: **reboot**

Description: Performs a reboot ("Cold start the system") of the device in the command line prompt.

Warning: doing a reboot or restart of a NID or the IONMM will cause all configuration backup files to be lost and the USB or Telnet session to drop. This operation deletes **all** configuration information that was saved in the IONMM, including the IP address you assigned to the IONMM or NID. After a reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.

Example:

```
C1|S18|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 Transition Networks.

C1|S1|L1D>
```

The HyperTerminal connection closes, and the Windows Taskbar Notification area displays the message "*A network cable is unplugged!*. "

To recover:

1. Close the Windows Taskbar message.
2. Disconnect and close HyperTerminal.
3. Re-open HyperTerminal.
4. Re-open the HT session.
5. Log back in to the S323x.

Reset System Uptime

Syntax: **reset uptime**

Description: Resets the System Up Time counter to zero, and immediately begins to increment.

Example:
```
C1|S18|L1D>reset uptime
C1|S18|L1D>
```

Note: Use the **show system info** command to display the current device uptime.
Note: the **reset uptime** command is not available for the Power Supply modules.

Reset to Factory Default Configuration

Syntax: **reset factory**

Description: Resets a card to its factory default configuration.

 **Warning:** doing a reboot or restart of the IONMM or NID will cause all configuration backup files to be lost and the USB or Telnet session to drop. This operation deletes **all** configuration information that was saved in the IONMM, including the IP address you assigned to the IONMM or NID.

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

The HyperTerminal connection closes, and the Windows Taskbar Notification area displays the message "*A network cable is unplugged!*."

To recover:

1. Close the Windows Taskbar message.
2. Disconnect and close HyperTerminal.
3. Re-open HyperTerminal.
4. Re-open the HT session.
5. Log back in to the NID.

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). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key.

Slot Power On / Power Off / Reset

Syntax: **set slot xx power**={off|on|reset}

Description: Turns the specified slot power on or off, or performs a slot reset (reboot) function.

Where:

xx = slot number of the device

Example:
```
C1|S16|L1P1>set slot 16 power on
C1|S16|L1P1>
```

Note: Use the **stat** command to view the chassis slot assignments.

Note: Use the **show power config** command to view the existing power supply configuration.

Set Power Relay State

Syntax: **set power relay state**=[disable|enable]

Description: Enables or disables the Power Supply's Power Relay

Example:
```
C1|S22|L1D>set power relay state=enable
C1|S22|L1D
```

Note: This command must be executed on a relay.

Note: Use the **stat** command to view the chassis slot assignments. Use the **show power config** command to view the existing power supply configuration.

Set PS Sensor Notification / Relation / Severity / Value

Syntax: **set sensor stid**=SENSORID **notif**=(enable|disable)

set sensor stid=SENSORID

relation={lessThan|lessOrEqual|greaterThan|greaterOrEqual|equalTo|notEqualTo}

set sensor stid=SENSORID **severity**={other|minor|major|critical)

set sensor stid=SENSORID **value**=VALUE

Description: Sets the Power Supply Sensor or Fan's notification, relation, severity, and/or value.

Where:

SENSORID = { Temperature | Voltage | Power | Fan }

notif = { enable enables sensor notification | disable disables sensor notification }. This variable controls generation of SensorThresholdNotification for this threshold.

relation={ lessThan | lessOrEqual | greaterThan | greaterOrEqual |equalTo | notEqualTo } This variable indicates the relation between sensor value (SensorValue) and threshold value (SensorThresholdValue), required to trigger the alarm.

severity = { other | minor | major | critical }. This variable indicates the severity of this threshold. Critical is the most severe, major is the next most severe, and minor is the least severe value setting.

value = VALUE. This variable indicates the value of the threshold.

Note: This command must be executed on a power sensor or fan.

Example: The following commands set the power supply sensor notification, relation, severity, and value for Sensor Transaction ID (stid) 9.

```
C1|S22|L1D>set sensor stid=9 notif=enable
C1|S22|L1D>set sensor stid=9 relation=lessThan
C1|S22|L1D>set sensor stid=9 severity=major
C1|S22|L1D>set sensor stid=9 value=9
```

Note: Use the **show power config** command to display sensor configuration for the power supply.

Set System Contact

Syntax: **set system contact**=CONTACT

Description: Defines 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, but cannot contain any space characters.

Example:

```
C1|S16|L1D>set system contact=99999999999999999999
C1|S16|L1D>show system information
system descr:          The C3230-1014 of the Transition Networks
                       ION (Chassis Generation III) platform
                       products
system objectID:     1.3.6.1.4.1.868.2.5.1802661751
system uptime:       3 days, 03:09:19
system contact:      99999999999999999999
system name:         C2220-1014
system location:     10900 Red Circle Drive  Minnetonka, MN 5
                       5343 USA
C1|S16|L1D>
```

The default system contact is Lantronix (techsupport@transition.com). The **show system information** command displays the system contact, system location, system name, and other system descriptive information. **Note**: this command does not work on a Power Supply module.

Set System Location

Syntax: **set system location**=LOC

Description: Defines the physical location (e.g., street address) of the system. The location can be alphabetic, numeric or a combination (e.g., room 110, IT lab, etc.), but cannot contain any space characters.

Example:

```
C1|S16|L1D>set system location=Corporate
C1|S16|L1D>show system information
system descr:          The C3230-1014 of the Transition Networks
                       ION (Chassis Generation III) platform
                       products
system objectID:     1.3.6.1.4.1.868.2.5.1802661751
system uptime:       3 days, 03:09:19
system contact:      99999999999999999999
system name:         C3230-1014
system location:     Corporate
C1|S16|L1D>
```

The default system location is 10900 Red Circle Drive. The **show system information** command displays the system contact, system location, system name, and other system descriptive information.

Set System Name

Syntax: **set system name**=NAME

Description: a Defines the identifying name of the device. The name can be alphabetic, numeric or combination, but cannot contain any space characters.

Example:

```
C1|S16|L1D>set system name=<>)|
C1|S16|L1D>show system information
system descr: The C3230-1040 of the Transition networks ION (Chassis
Generation III) platform products
system objectID:     1.3.6.1.4.1.868.2.5.1802661751
system uptime:       3 days, 03:41:07
system contact:      99999999999999999999
system name:         <>)|
system location:     Corporate
C1|S16|L1D>
```

The system name default is C3230-1040 (case sensitive – all capitals). The **show system information** command displays the system contact, location, name, and other system descriptive information.

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.

Note: Once you change the system name, that name must be used to re-login.

Set USB Port State

Syntax: **set usb-port state**=(enable|disable)

Description: Defines the status of the device's USB connection (either enabled or disabled).

Example:
```
C1|S7|L1D>set usb-port state ?
disable
enable
C1|S7|L1D>set usb-port state=enable
C1|S7|L1D>
```

Note: When Console access is disabled, the x323x will not respond to CLI commands entered by a local management station across the USB serial interface. The only access to the x323x NID will then be through either a Telnet session or the Web interface.

Show USB Port State

Syntax: **show usb-port state**

Description: Displays the status of the device's USB connection (either enabled or disabled).

Example:
```
C1|S7|L1D>show usb-port state
USB port state:                          enable
C1|S7|L1D>
```

Show Card Information

Syntax: **show card info**

Description: Displays the system information for the IONMM or slide-in card.

Example 1: (IONMM in slot 1):
```
AgentIII C1|S1|L1D>show card info
System name:        AgentIII
Uptime:             4 days, 02:49:35
CPU MAC:            00-c0-f2-20-de-9e
Port number:        2
Serial number:      SN-agent-001
```

```
Config mode:        software
Software:           1.3.13
Bootloader:         1.2.0
Hardware:           0.0.1
AgentIII C1|S1|L1D>
```

Example 2: (C3230 in slot 4):

```
Agent III C1|S4|L1D>show card info
System name:        C3230-1040
Uptime:             07:50:18
CPU MAC:            00-c0-f2-21-01-77
Port number:        2
        Port-1 MAC address:        00-c0-f2-21-01-78
        Port-2 MAC address:        00-c0-f2-21-01-79
Serial number:      5219475
Config mode:        software
Software:           1.3.13
Bootloader:         1.2.1

Hardware:           1.0.0
Agent III C1|S4|L1D>
```

Example 3: (C3231 in slot 11):

```
AgentIII C1|S6|L1D>show card info
System name:        C3220-1040
Uptime:             4 days, 04:11:05
CPU MAC:            00-c0-f2-20-e2-40
Port number:        2
Serial number:      11615637
Config mode:        software
Software:           1.3.13
Bootloader:         1.2.1

Hardware:           1.0.0
AgentIII C1|S6|L1D>
```

Note: This command does not work for the Power Supply.

Show Card Type

Syntax: **show cardtype**

Description: Displays the ION system device's card type (model number).

Example 1: (C3220 NID in slot 3):

```
AgentIII C1|S6|L1D>show cardtype
Card type:                  C3220-1040
AgentIII C1|S6|L1D>
```

Example 2: (IONMM in slot 1):

```
AgentIII C1|S1|L1D>show cardtype
Card type:                    IONMM
AgentIII C1|S1|L1D>
```

Example 3: IONPS-A power supply in slot 22):

```
AgentIII C1|S22|L1D>show cardtype
Card type:                    IONPS-A
AgentIII C1|S22|L1D>
```

Show Chassis Information

Syntax: **stat**

Description: 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 (Example 1 below). On a remote standalone device, displays device and port information (Example 2 below).

Example 1:

```
AgentIII C1|S1|L1D>stat
ION statck
        Chassis -- BPC
                [  1]  IONMM
                        Port 1
                        Port 2
                [  5]  C6210-3040
                        Port 1
                        Port 2
                                level2 REM: S6210-3040
                                        Port 1
                                        Port 2
                [  7]  C3210-1013
                        Port 1
                        Port 2
                [  8]  C3221-1040
                        Port 1
                        Port 2
                        Port 3
                [ 12]  C2110-1013
                        Port 1
                        Port 2
                [ 14]  C2210-1013
                        Port 1
                        Port 2
                [ 16]  C2220-1014
                        Port 1
                        Port 2
                [ 22]  IONPS-A
                        Temperature Sensor
                        Voltage Sensor
                        Power Sensor
                        Fan-1
                        Fan-2
```

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

Example 2:

```
C3221-1040 C0|S0|L1D>stat
ION statck
        Chassis -- BPC
                [  0]  C3221-1040
                        Port 1
                        Port 2
                        Port 3
C3221-1040 C0|S0|L1D>
```

Show Device Mode (local / remote)

Syntax: **show switch mode**

Description: Displays whether the device is in local or remote switch mode, indicating where the device is managed.

- local – device is managed through direct connection to the device.
- remote – device is managed through the ION Management Module.

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

Use the **set switch mode** command to change device switch modes.

Example:

```
C1|S1|L1D/>show switch mode
Switch mode: remote
```

Show Power Supply Configuration

Syntax: **show power config**

Description: Displays the current configuration of the specified ION system power supply sensors, fan(s) and relay.

Example:

```
C1|S24|L0D/>show power config

Power supply sensors information:

Temperature Sensor:
        Type:                   celsius
        Scale:                  units
        Precision:              0
        Value:                  30
        Operation status:       ok
        Units display:          The data units displayed is degrees

Threshold information:
index          severity       relation       value     evaluation notifEnable
-------------------------------------------------------------------------------
1              other          greaterThan    80          false          false
2              minor          greaterThan    60          false          false
3              major          greaterOrEqual 65          false          false
4              critical       greaterOrEqual 70          false          true

Voltage Sensor:
        Type:                   voltsAC
        Scale:                  millivolts
        Precision:              2
        Value:                  12684
        Operation status:       ok
        Units display:          The data units displayed for volts is mV

Threshold information:
index          severity       relation       value     evaluation notifEnable
-------------------------------------------------------------------------------
1              critical       lessThan       11220       false          true
2              minor          greaterThan    13000       false          false
3              major          greaterOrEqual 14000       false          false
4              critical       greaterOrEqual 14673       false          true

Power Sensor:
        Type:               watts
        Scale:              units
        Precision:          2
        Value:              19
        Operation status:   ok
        Units display:      The data units displayed for watts is units(9)


Threshold information:
index          severity       relation       value   evaluation   notifEnable
-------------------------------------------------------------------------------
1              critical       lessOrEqual    10         false          true
2              minor          greaterThan    225        false          false
3              major          greaterOrEqual 250        false          false
```

```
4              critical       greaterOrEqual 275        false          true

Relay:
        Type:                   other
        Scale:                  units
        Precision:              0
        Value:                  2
        Operation status:       ok
        Units display:          The data units displayed for Relay is units(9)
        Installed:              false
        State:                  disable
        Module type:            acModule
        Oper mode:              master

Fan-1:
        Type:                     rpm
        Scale:                    units
        Precision:                2
        Value:                    3015
        Operation status:         ok
        Units display:            The data units for Fan 1 in RPM is units(9)

Threshold information:
index          severity       relation       value     evaluation notifEnable
-------------------------------------------------------------------------------
1              critical       equalTo        0          false          true
2              minor          greaterThan    9000       false          false
3              major          greaterOrEqual 9500       false          false
4              critical       greaterOrEqual 9900       false          true
```

Show Slot Information

Syntax: show slot info

Description: Displays current ION Chassis slot information when entered from the IONMM.

Example:

```
C1|S1|L1D>show slot info
Chassis BPC information:

Serial number:      3245
Model name:         ION219
Software:           1.2.0
Hardware:           1.0.0
Bootloader:         0.1.0

Slot information:
slot      slot status         description
power status
-------------------------------------------------------------------------------
1         occupied            ION Management Module AGENT        on
2         empty                                                  on
3         occupied            ION Media Conversion Module C3230-1040    on
4         occupied            ION Media Conversion Module C6010-3040    on
5         occupied            ION Media Conversion Module C3230-1040    on
6         empty                                                  on
7         occupied            ION Media Conversion Module C3210-1013    on
8         occupied            ION Media Conversion Module C3221-1040    on
9         empty                                                  on
10        empty                                                  on
11        empty                                                  on
12        occupied            ION Media Conversion Module C2110-1013    on
13        empty                                                  on
14        occupied            ION Media Conversion Module C2210-1013    on
15        empty                                                  on
16        occupied            ION Media Conversion Module C2220-1014    on
17        empty                                                  on
18        occupied            ION Media Conversion Module C3220-1040    on
19        empty                                                  on
C1|S1|L1D>
```

Show System Information

Syntax: show system information

Description: Displays current ION Chassis slot information.

Example 1 (IONMM):

```
C1|S7|L1D>show system info
system descr:              The management module of the Transition networks
                           ION (Chassis Generation III) platform products
system objectID:           1.3.6.1.4.1.868.2.5.544108393
system uptime:             3 days, 18:17:33
system contact:            Transition Networks   (techsupport@transition.com)
system name:               Agent III
system location:           10900 Red Circle Drive  Minnetonka, MN 55343 USA
```

*Example **2*** (C3230):

```
C1|S3|L1D>show system info
system descr:              The C3230-1040 of the Transition networks ION
                           (Chassis Generation III) platform products
system objectID:           1.3.6.1.4.1.868.2.5.1802661751
system uptime:             3 days, 22:28:44
system contact:            Transition Networks (techsupport@transition.com)
system name:               C3230-1040
system location:           10900 Red Circle Drive Minnetonka, MN 55343 USA
```

Note: You cannot **show system information** on the Power Supply.

Switch Device Mode (local / remote)

Syntax: **set switch mode**={local | remote}

Description: Changes the operating mode of a standalone NID. Setting the mode to **local** indicates that the device is not managed by the ION Management Module (IONMM). Instead, it is managed through 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 (the default setting).

After changing the switch mode, reboot the NID for the changes to take effect. At the command prompt type **reboot** and press **Enter**. See the **reboot** command for more information.

 Doing a reboot will cause all configuration backup files, HTTPS certification file, SSH key file, and Syslog file to be lost.

At the command prompt, type **show switch mode** to verify the change.

Example:

```
C0|S0|L1d/>set switch mode=local
C0|S0|L1d/>show switch mode
Switch mode: local
```

Note: The system cannot set/show the switch mode on all card types.

Set Circuit ID

Syntax: **set circuit-ID=<xx>**

Description: Device level command to define an ASCII text string up to 63 bytes and override the default Circuit ID, which is the *vlan-module-port* in binary format, for a device and/or device ports. Use the **show circuit-ID** command to display the Circuit ID information for a device or port.

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>
```

Note: the dash ("**-**") is required, and the letters "ID" must be upper-case.

Show Circuit ID

Syntax: **show circuit-ID**

Description: Device level command to display the current Circuit ID for the device or port. Use the **set circuit-ID** command to define the Circuit ID information for a device or port.

Example:
```
C1|S5|L1D>set circuit-ID=xx
C1|S5|L1D>show circuit-ID
Circuit-ID:         xx
C1|S5|L1D>
```

Note: the dash ("**-**") is required, and the letters "ID" must be upper-case.

Note: The x323x supports a Circuit ID, a company-specific identifier assigned by the user to identify the converter and individual ports in any manner desired. In the ION system, the Circuit ID port identifier is based on the agent-local identifier of the circuit (defined in RFC 3046), as detected by the agent and associated with a particular port.

Set Device Description

Syntax: **set device description**=*CIRCUIT*

Description: Lets you define an ASCII text string up to 63 bytes of ASCII printable characters and override the default Device Description, which is the vlan-module-port in binary format, for a device and/or device ports. Use the show device description command to display the Device Description information for a device.

Example:
```
C1|S16|L1D>set device description=XX/YYYY/000000/111/CC/SEG
C1|S16|L1D>show device description
Circuit-ID:         XX/YYYY/000000/111/CC/SEG
C1|S16|L1D>
```

Note: the dash ("-") is required, and the letters "ID" must be upper-case. The message "Its value must be ASCII printable characters. String less than 64." displays for any invalid entry. The legal characters are: /^[a-zA-Z\d`~!@#$%^&*(){}[\];:'",.<>\-_=+\\|\/?]{0,64}$/; and the space character.

Messages:
Cannot show device description on this card!
Device description should be shorter than 64 characters!
Failed to set circuit-ID on this device.
Fail to set circuit-ID on this port.

Show Device Description

Syntax: **show device description**

Description: Displays the current Device Description information for the device. Use the **set device description** command to define the Circuit ID information for a device.

Example:
```
C1|S5|L1D>set device description=xxxxxx
C1|S5|L1D>show device description
Circuit-ID:         xxxxxx
C1|S5|L1D>
```

Note: the dash ("**-**") is required, and the letters "ID" must be upper-case.

Messages:
Cannot set circle-ID on this port!
Cannot show circuit-ID on this card!
Fail to show device description on this device.
Fail to show circuit-ID on this port.

Note: The x323x supports a Circuit ID and Device Description as company-specific identifiers assigned by the user to identify the ION device and individual ports in any manner desired. In the ION system, the Circuit ID port identifier is based on the agent-local identifier of the circuit (defined in RFC 3046), as detected by the agent and associated with a particular port.

Set Current Time

Syntax: **set curr-time**=TIME

where:

TIME = desired time of day setting in the format dd:hh:mm:ss.ts
(days:hours:minutes:seconds.tenths of a second).

Description: Changes the current time of day.

Example:
```
C1|S3|L1D>set curr-time=”20100106 13:15:30”
C1|S3|L1D>
```

Use the **show sntp config** command to display the current time setting in the format “*Current time: 1970 0103 11:42:26*”.

Set Debug Level

Syntax: 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).

Description: Defines the system debug level.

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>
```

5. System User / Login Commands

These commands let the ION system administrator add, define, display, and remove ION system users. Each user has a user name, access level, and password.

The three levels of ION system login user rights are described in the table below.

Table 4: 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)

- 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 via the Web or 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 though the Web/CLI. When a read-only user logs into the Web interface, the Web interface 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.
- The one default **Admin** user is "ION". Its default password is "private". This user cannot be deleted.
- This user management does not apply to Focal Point.
- Doing an SNMP **get** operation on the password object will return "********" (eight '*'s).

An error message displays if you enter a CLI command outside of your system login user level (e.g., *ERROR: Current user is not authorized to do this operation!* or *% There is no matched command*).

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

Add a New System User

Syntax: **add sysuser name**=NAMESTR **level**=<admin|read-write|read-only> **pass**=PASSSTR **confirmpass**=PASSST

Description: Add (create) a new ION system user and define the new user's access level and pass word. This command is available to Admin users only.
where:

name = NAMESTR = the new user's username.
level = the new user's access level (administrator, read-write, or read-only).
pass = PASSSTR = the new user's password string.
confirmpass = PASSSTR = the new user's password string.

Privilege: Admin level login users only.

Example:
```
C1|S1|L1D>add sysuser name=NAMESTR level=read-write pass=PASSSTR
C1|S1|L1D>
```

Set System User's Access Level

Syntax: **set sysuser name**=NAMESTR **level**=<admin|read-write|read-only>

Description: Edit (change) an existing ION user's name and access level. This command is available to Admin users.

where:

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

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

Example:
```
C1|S1|L1D>add sysuser name=NAMESTR level=read-write pass=PASSSTR
C1|S1|L1D>set sysuser name=NAMESTR level=read-only
C1|S1|L1D>
```

Set System User's Password

Syntax: **set sysuser nam**e=NAMESTR **pass**=PASSSTR **confirmpass**=PASSSTR

Description: Edit (change) an existing ION system user's password.

where:

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

Privilege: An Admin user can set any login password.
A Read-Write user can only change their own password.
A Read-Only user can only change their own password.

Example:
```
C1|S1|L1D>set sysuser name=NAMESTR pass=PASSSTR confirmpass=PASSSTR
C1|S1|L1D>
```

Remove an Existing System User

Syntax: **remove sysuser name**=NAMESTR

Description: Removes an existing ION system user. This command is available to Admin users.

where:

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

Privilege: Only an Admin user can create new users and delete any users other than itself and ION.

Example:
```
C1|S1|L1D>remove sysuser name=NAMESTR
C1|S1|L1D>
```

Show All System Users

Syntax: **show sysuser** <cr>

Description: Displays information on all of the ION users currently configured for use.

The information includes the User name, User level (**admin**istrator, **read-writ**e, or **read-only**) and password. This command only works on an IONMM or a standalone SIC. This command is available to all SNMP users at all privilege levels.

Example 1 (default user):

```
C1|S1|L1D>show sysuser
name                    level           password
ION                     admin           ********
C1|S1|L1D>
```

Example 2 (additional users):

```
C1|S1|L1D>show sysuser
name                    level           password
ION                     admin           ********
AndersonT               read-write      ********T
BensonJ                 read-write      ********T
CarlsonAnn              read-write      ********nn
CarlsonBob              read-only       ********ob
DobsonV                 read-only       ********ob
EffertzC                read-only       ********
Fitz                    read-only       ********
GomesD                  read-only       ********
JeffS                   read-write      ********
C1|S1|L1D>
```

6. ACL Commands

The Access Control List (ACL) is a collection of permit and deny rules and conditions that provide security across an Ethernet connection by blocking unauthorized users and allowing authorized users to access specific resources. Consider the following when configuring ION system ACLs:

1. If the NID is managed by the ION Management Module (IONMM), configuring ACL should be done at the IONMM and not at the NID.
2. The ACL does not control access to the NID through a serial interface (USB connection).
3. 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.
4. 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.
5. 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.
6. If multiple rules are matched to an input packet, the rule with the highest priority will be applied.
7. You can add/modify/delete a rule or a condition whether the ACL is enabled or disabled.
8. 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.
9. The x323x NIDs do not support two ACL conditions with the same condition type.

Note: These commands can only be entered when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D). These commands cannot be entered at the port level.

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 x323x 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 x323x 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 process used to create an ACL generally includes these steps:

1. Enable ACL using the set acl state=enable command.
2. Define default chain policy using the **set acl table=filter chain=input policy=**<ptype> command.
3. Define one or more conditions using the command:

   add acl condition type=<xx> **srcdst=**{**src** | **dst**} **oper=**{**equal** | **notequal**} **value=**<yy>
4. Define one or more rules using the command:

   add acl rule index=<inum> **position=**{head | tail} **table=filter chain=input policy=**{accept | drop | trap} **traprate=**<rate> **condition=**<list>.

The ACL Commands vary between IPv4 and IPv6 as described in the following sections.

ACL Commands (IPv4)

The following commands are used for ACL operations under IPv4.

Add a New ACL Condition

Syntax: **add acl condition type=**<ww> **srcdst=**<xx> **oper=**<yy> **value=**<zz>

Description: Creates a new ACL condition.

where:

ww = condition type; valid choices are:

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

xx = restriction stream; valid choices are:

- **src** (source)
- **dst** (destination)

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 **ipv4addrrange**, **tcpportrange** or **udpportrange** is specified for **type=**, then the two values (range) specified for num must be separated by a hyphen (e.g., 1–4).

Example:

```
C1|S13|L1D/>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.123
C1|S13|L1D/>
```

Add a New ACL Rule

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

Description: Creates a new ACL rule.

where:

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

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

xx = ACL policy type; valid choices are:

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

yy = number (1 – 65535) of times the trap can be sent in a minute

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 (e.g., 2,3,6).

Usage: **add acl rule position**=(head|tail) **table**=(filter) **chain**=(input) policy=(accept|drop|trap) [traprate=TRAPRATE] [condition=CONDLIST]

Example:

```
C1|S5|L1D>add acl rule position=head table=filter chain=input policy=trap
 traprate=100
C1|S5|L1D>show acl rule
index table-type chain-type priority  policy traprate(packets/min)   condition
```

```
------------------------------------------------------------------------------
1     filter      input     1         trap    100                          no
C1|S5|L1D>
```

Remove ACL Condition(s)

Syntax: **remove acl condition** ={<xx> | all}

Description: Removes the specified ACL condition definition.

where:

xx = index number of the condition to be removed

all = remove all conditions

Example:

```
C1|S5|L1D>remove acl condition 1
C1|S5|L1D>show acl ?
  chain
  condition
  rule
  state
C1|S5|L1D>show acl condition
No ACL condition now!
C1|S5|L1D>
```

Remove ACL Rule(s)

Syntax: **remove acl rule=**{<xx> | all}

Description: Removes the specified ACL rule definition.

where:

xx = index number of the rule to be removed

all = remove all rules

Example:

```
C1|S5|L1D>remove acl rule 1
C1|S5|L1D>show acl ?
  chain
  condition
  rule
  state
C1|S5|L1D>show acl rule
No ACL rule now!
C1|S5|L1D>
```

Restart ACL

Syntax: **restart acl**

Description: Restarts the ACL (firewall).

Example:
```
C1|S5|L1D>restart acl
C1|S5|L1D>
```

Set ACL State

Syntax: **set acl state**={enable | disable}

Description: Enables or disables ACL operations.

Example:
```
C1|S5|L1D>set acl state ?
  disable
  enable
C1|S5|L1D>set acl state enable
C1|S5|L1D>show acl state
ACL management state:         enable
```

Set ACL Chain Default Policy

Syntax: **set acl table=filter**=xx **chain=yy policy=**zz

Description: Changes the default policy of an ACL chain. You must specify the filter, chain, and policy for each rule you create.

Where:

xx = filter
yy = chain= input
zz - policy=(accept|drop}

Example:
```
C1|S7|L1D>set acl table=filter chain= input policy=drop
C1|S7|L1D>
```

Note: the defaults are **table=filter** and **chain=input** which cannot be changed.

Set Certain Conditions to a Rule

Syntax: **set acl condition=**<xx> **rule_index=**<yy>

Description: Applies a defined condition to a particular rule.

where:

xx = index number of the condition to be applied to rule yy

yy = index number of the rule to which condition xx is to be applied

Example:
```
C1|S3|L1D>set acl condition=1 rule_index=1
C1|S3|L1D>
```

Note: A rule index must already exist. If the specified ACL rule has not previously been defined, the message "*Invalid ACL rule index!*" displays.

Set Trap Rate of a Rule

Syntax: **set acl rule=**<xx> **traprate=**<yy>

Description: Sets the trap rate of an ACL rule. The Trap Rate is a value indicating the number of traps that will be sent in one minute. This is the trap rate of a 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.

Note: This command only applies to rules with **policy=trap** specified.

where:

xx = index number of the rule to which the trap rate will apply

yy = trap rate (1 - 65,535 ppm)

Example:
```
C1|S3|L1D>set acl rule=2 traprate=500
The specified ACL rule index does not exist!
C1|S3|L1D>set acl rule=1 traprate=500
C1|S3|L1D>
```

Note: The specified ACL rule index must already exist.

Show ACL State

Syntax: **show acl state**

Description: Displays whether ACL is enabled or disabled (as set by the **set acl state** command).

Example:

```
C1|S3|L1D>show acl state
ACL management state:         disable
C1|S3|L1D>
```

Show All ACL Conditions

Syntax: **show acl condition**

Description: Displays all defined ACL conditions.

Example:

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

An ACL condition must already have been created. If no ACL conditions are yet defined, the message "*No ACL conditions now!*" displays.

Show All ACL Rules

Syntax: **show acl rule**

Description: Displays all defined ACL rules.

Example:

```
C1|S7|L1D>show acl rule
index    table-type     chain-type   priority  policy    traprate(packets/min)   conditions
-------------------------------------------------------------------------------------------
1        filter         input        1         trap      1500                    2
2        filter         input        3         accept    10                      1
3        filter         input        6         drop      100                     4
```

An ACL rule must already have been created. If no ACL rules are yet defined, the message "*No ACL rule now!*" displays.

Show All IPtable Chain Definitions

Syntax: **show acl chain**

Description: Displays all defined ACL chains.

Example:
```
C1|S13|L1D/>show acl chain
table-type      contain-type       chain-name         default-policy
-------------------------------------------------------------------
filter          input              INPUT              accept
C1|S13|L0D/>
```

ACL Commands with IPv6

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

The following commands are used for ACL operations under IPv6.

Set IPv6 Tables ACL State

Syntax: **set ip6tables acl state**=(enable|disable)

Description: Device level command (IONMM or a standalone SIC only) to enable or disable the IPv6 ACL function.

Example:
```
Agent III C1|S1|L1D>set ip6tables acl state=enable
Agent III C1|S1|L1D>
```

Messages: *Fail to set IPv6 ACL state!*

Show IPv6 Tables ACL Management State

Syntax: **show ip6tables acl state**

Description: Device level command (IONMM or a standalone SIC only) that displays the current ACL management state.

Example:
```
Agent III C1|S1|L1D>show ip6tables acl state
ACL of IPv6 tables management state:    enable

Agent III C1|S1|L1D>
```

Messages: *Getting ACL IPv6 state fail!*

Restart ACL of IPv6 Tables

Syntax: **restart ip6tables acl**

Description: Device level command (IONMM or a standalone SIC only) to restart the ACL of IPv6 tables.

Example:
```
Agent III C1|S1|L1D>restart ip6tables acl
Agent III C1|S1|L1D>
```

Messages: *Fail to restart IPv6 tables ACL!*

Show IPv6 Tables ACL Chain

Syntax: **show ip6tables acl chain**

Description: Device level command (IONMM or a standalone SIC only) to display the IPv6 tables ACL chains.

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>
```

Messages: *Fail to get ip6tables ACL chain policy!*

Set IPv6 Tables ACL Chain Policy

Syntax: **set ip6tables acl table**=(raw|filter|nat|mangle) **chain**=(prerouting|input|forward|output|postrouting) **policy**=(accept|drop)

Description: Device level command (IONMM or a standalone SIC only) to configure the ACL table, chain, and policy. Note that the value of **table** can only be "filter" and the value of **chain**.

Example:
```
Agent III C1|S1|L1D>set ip6 acl table filter chain input policy accept
Agent III C1|S1|L1D>
```

Messages: *Now the value of table can only be \"filter*
Now the value of chain can only be \"input

Show IPv6 Tables ACL Rules

Syntax: **show ip6tables acl rule**

Description: Device level command (IONMM or a standalone SIC only) to display the current ACL table, chain, and policy. Note that the value of **table** can only be "filter" and the value of **chain** can only be "input".

Example:

```
Agent III C1|S1|L1D>show ip6tables acl rule
index  table-type  chain-type  priority  policy  traprate(packets/min) condition
-------------------------------------------------------------------------------
1      filter      input        1         trap      0                          no
Agent III C1|S1|L1D>
```

Messages: *Fail to find first row of acl rules!*
No ACL rule now!
Fail to get ACL rule!
Fail to get ip6tables ACL rule table type!
Fail to get ip6tables ACL rule chain type!
Fail to get ip6tables ACL rule priority!
Fail to get ip6tables ACL rule policy!
Fail to get ip6tables ACL rule traprate!

Create IPv6 Table New ACL Rule

Syntax: **add ip6tables acl rule position**=(head|tail) **table**=(raw|filter|nat|mangle) **chain**=(prerouting|input|forward|output|postrouting) **policy**=(accept|drop|trap) [**traprate**=TRAPRATE] [**condition**=CONDLIST]

Description: Device level command (IONMM or a standalone SIC only) to add a new ACL rule.

Note that the value of **table** can only be "filter" and the value of **chain** can only be "input".

The **traprate** and **condition** entries are optional. The position part sets the rule being added at the tail or head of the chain.

Example:

```
Agent III C1|S1|L1D>add ip6tables acl rule position=head table=filter chain=input policy= trap
444
Agent III C1|S1|L1D>show ip6tables acl rule
index  table-type    chain-type    priority  policy     traprate(packets/min)    condition
-------------------------------------------------------------------------------
2        filter        input         1        trap      0    no
1        filter        input         2        trap      0    no
Agent III C1|S1|L1D>
```

Messages: *Fail to set ip6tables ACL chain type!*
Fail to set ip6tables ACL policy!
Fail to set ip6tables ACL priority!
Fail to set ip6tables ACL row status!
Fail to set ip6tables ACL table type!

Now the value of table can only be \"filter\"!
Now the value of chain can only be \"input\"!
Please input a digital number to specify the ACL condition index!
Please input a number to specify the ACL rule index!
The specified condition index does not exist!

Create New IPv6 Tables ACL Rule

Syntax: **add ip6tables acl rule index**=RULE_ID **table**=(raw|filter|nat|mangle) **chain**=(prerouting|input|forward|output|postrouting)

prio= **PRIO poicy**=(accept|drop|trap) [**traprate**=TRAPRATE]

Description: Device level command (IONMM or a standalone SIC only) to add a new ACL rule for provisioning. Note that the value of **table** can only be "filter" and the value of **chain** can only be "input". The **traprate** and **condition** entries are optional. The position part sets the rule being added at the tail or head of the chain.

Example:

```
Agent III C1|S1|L1D>add ip6tables acl rule position=head table=filter chain=
input policy=trap traprate=400
Agent III C1|S1|L1D>
```

Set IPv6 Tables ACL Rule Trap Rate

Syntax: **set ip6tables acl rul**e=<1-255> **traprate**=<1-65535>

Description: Device level command (IONMM or a standalone SIC only) to configure an IPv6 ACL rule and its trap rate.

Example:

```
Agent III C1|S1|L1D>set ip6tables acl rule=1 traprate=655
Agent III C1|S1|L1D>
```

Messages:
Cannot set trap rate when policy is not trap!
Fail to get ACL rule traprate!
Fail to set ACL traprate!
The specified ACL rule does not exist!
The specified ACL rule index does not exist!

Remove a Specified IPv6 Tables ACL Rule

Syntax: **remove ip6tables acl rule**=<1-255>

Description: Device level command (IONMM or a standalone SIC only) to delete a specified IPv6 ACL rule from the rules table.

Example:

```
Agent III C1|S1|L1D>remove ip6tables acl rule index 1
Agent III C1|S1|L1D>
```

Messages: *Fail to remove ACL rule!*
The specified ACL rule does not exist!

Remove All IPv6 Tables ACL Rules

Syntax: **remove ip6tables acl rule all**

Description: Device level command (IONMM or a standalone SIC only) to delete all existing IPv6 ACL rules from the rules table.

Example:
```
Agent III C1|S1|L1D>remove ip6tables acl rule all
Agent III C1|S1|L1D>
```

Messages: *Fail to remove ACL rule!*
The specified ACL rule does not exist!

Remove All IPv6 Tables ACL Conditions

Syntax: **remove ip6tables acl condition all**

Description: Device level command (IONMM or a standalone SIC only) to delete all existing IPv6 ACL conditions from the conditions table.

Example:
```
Agent III C1|S1|L1D>remove ip6tables acl condition all
Agent III C1|S1|L1D>
```

Messages: *Fail to remove ACL condition!*

Show All IPv6 Tables ACL Conditions

Syntax: **show ip6tables acl condition**

Description: Device level command (IONMM or a standalone SIC only) to display all currently configured IPv6 ACL conditions.

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>
```

Messages: *Fail to get ip6tables ACL condition!*
Fail to get ip6tables ACL condition index!
Fail to get ip6tables ACL condition operation!
Fail to get ip6tables ACL condition rule index!

Fail to get ip6tables ACL condition src/dst!
Fail to get ip6tables ACL condition type!
Fail to get ip6tables ACL condition value!
Invalid IPv6 network address!
No ip6tables ACL condition now!
Unknown ICMP type!

Set IPv6 Tables ACL Condition Rule Index

Syntax: **set ip6tables acl condition**=<1-255> **rule_index**=<0-255>

Description: Device level command (IONMM or a standalone SIC only) to configure a new IPv6 ACL condition and its rule index.

Example:
```
Agent III C1|S1|L1D>set ip6tables acl condition=1 rule_index=1
Agent III C1|S1|L1D>
```

Messages: *ERROR: already have the same Condition Type under this rule!*
Invalid ip6tables ACL rule index!

Remove an IPv6 Tables ACL Condition

Syntax: **remove ip6tables acl condition**=<1-255>

Description: Device level command (IONMM or a standalone SIC only) to remove (delete) a specified IPv6 ACL condition, or all existing conditions, from the table.

Example:
```
Agent III C1|S1|L1D>remove ip6tables acl condition ?
  all
  index
Agent III C1|S1|L1D>remove ip6tables acl condition index ?
  <1-255>
Agent III C1|S1|L1D>remove ip6tables acl condition index 1
Invalid ACL condition index!
Agent III C1|S1|L1D>
```

Messages: *Invalid ACL condition index!*
Fail to remove ACL condition!

Add an IPv6 Tables ACL Condition

Syntax: **add ip6tables acl condition type**=(macaddr|ipv6addr|ipv6network|tcpport|tcpportrange|udpport|udpportrange|icmp)
srcdst=(src|dst) **oper**=(equal|notequal) **value**=VAL

Description: Device level command (IONMM or a standalone SIC only) to create and define a new IPv6 ACL condition, where:

type=(Mac addr, IPv6 addr, IPv6 network, TCP port, TCP port range, UDP port, UDP port range, or ICMP (Internet Control Message Protocol)).

srcdst=(src|dst) whether this condition is at the source (src) or the destination (dst).

oper=(equal|notequal) the operation for this condition; 'equal to' or 'not equal to'.

value=VAL; a valid IPv6 address (e.g., value=fe80::2c0:f2ff:fe20:de9e).

Example:

```
Agent III C1|S1|L1D>add ip6tables acl condition type ?
  macaddr
  ipv6addr
  ipv6network
  tcpport
  tcpportrange
  udpport
  udpportrange
  icmp
Agent III C1|S1|L1D>add ip6tables acl condition type=ipv6addr srcdst=src
oper=equal value=fe80::2c0:f2ff:fe20:de9e
Agent III C1|S1|L1D>
```

Messages:
Fail to add ACL addition!
Invalid condition valule (e.g., an invalid UDP port range entered - outside the valid range of port 1 - 8).
Inavlid condition value! (e.g., a valid mask has 2 formats; one is a integer of bit mask such as 2001::1002/96, the other is an IPv6 address such as 2001::2000/ffff:ffff::). Enter one of the two valid condition values and continue operation.

ACL CLI Messages

Message: *ERROR: already have a ipv6Condition Type under the same level!*
Meaning: You tried to enter two similar IPv6 ACL Conditions for the same Rule, but the entry failed.
Recovery:
1. Verify the IPv6 ACL parameter entries; see "IPv6 ACL (Access Control List)".
2. Contact Technical Support if the problem persists.

Message:
Bad condition index %u, its range is from 1 to 255!
Please input a digital number to specify rule index!
Invalid rule index!
Please input a digital number to specify trap rate!
Meaning: You tried to enter too many ACL rules.

Recovery:
1. Make sure you enter less than 255 entries; see "IPv6 ACL (Access Control List)".
2. Contact Technical Support if the problem persists.

Message:
All-zero MAC address is not valid for ACL ipv6 condition!
All-zero MAC address is not valid for ACL condition!
Meaning: You tried to enter an invalid IPv6 ACL address of all zeros.
Recovery:
1. Enter a valid IPv6 address; see "IPv6 ACL (Access Control List)".
2. Contact Technical Support if the problem persists.

7. Backup / Restore (Provision) Commands

The following commands are used to show, backup, and restore modules, and to set provision module configuration. **Note**: These commands can only be entered on the IONMM or a standalone SIC by an Admin level login user. **Note**: starting at v 1.3.10, Backup file name and TFTP upload/download file name are extended to maximum 128 characters. **Note** that at FW v 1.3.17 these CLI commands are no longer supported: *refresh provision configure filename*, *set backup module-index x config-file y*, and *set restore module-index x config-file y*.

Backup

Command: **Backup Specified Provision Module(s)**
Syntax: **backup module-list *xx***
Description: Device level command used to perform a configuration Backup of the specified provision modules (up to ten cards at a time). This command can only be executed on IONMM or a standalone SIC. Specify 1-10 provision modules to be backed up. Type **backup module-list=xx** and press **Enter**. This command is available to Admin level users only. Where: module-list = xx = the provision module indexes displayed by the "show provision modules" command.

Example:
```
C1|S1|L1D>backup module-list ?
STR_MODULE_LIST
C1|S1|L1D>backup module-list 1
Processing...
Processing...
Backup finished
C1|S1|L1D>
```

Restore

Command: **Restore Specified Provision Module(s)**
Syntax: **restore module-list=STR_MODULE_LIST**
Description: Device level command used to perform a Restore function on the specified provision modules (up to ten cards at a time). This command can only be executed on IONMM or a standalone SIC. Specify a restore index item number and a config file name.
Type **restore module-list=<1-256> config-file=STR_CFG_FILE** and press **Enter**.
This command is available to Admin level users only. Where:
module-list = the provision module indexes displayed by the "show provision modules" command.

Example:
```
C1|S1|L1D>restore module-list 1
Processing...
Processing...
Processing...
Processing...
Restore finished
C1|S1|L1D>
"Processing...
"Restore finished
```

Set Backup Module Index

Command: **Set Backup Module Configuration**

Syntax: **set backup module-index**=<1-256> **config-file**=STR_CFG_FILE

Description: Device level command used to set the backup configuration file name for one or more specified provision modules (up to 256 modules can be specified). The provision configuration file name maximum length is 64 alphanumeric characters. This command can only be executed on IONMM or a standalone SIC. The specified module must already exist. This command is available to Admin level users only. Note that this command is no longer supported after x323x FW v 1.3.17.

where:

module- index = provision module index displayed by the "show provision modules" command.
config-file = config file name of the specified module- index.

Example:
```
C1|S1|L1D>set backup module-index 1 config-file xxxx
C1|S1|L1D>
```

Set Restore Module Index

Command: **Set Restore Module Configuration**

Syntax: **set restore module-index**=<1-256> **config-file**=STR_CFG_FILE

Description: Device level command used to set the restore configuration file name for one or more specified provision modules (up to 256 modules can be specified). The provision configuration file name maximum length is 64 alphanumeric characters. This command can only be executed on IONMM or a standalone SIC. The specified module must already exist. This command is available to Admin level users only. Note that this command is no longer supported after x323x FW v 1.3.17.

where:

module- index = provision module index displayed by the "show provision modules" command.
config-file = config file name of the specified module- index.

Example:
```
C1|S1|L1D>set restore module-index 1 config-file xxxx
C1|S1|L1D>
```

Show Provision Modules

Syntax: **show provision modules**

Description: Device level command to show all modules that can perform backup and restore operations. This command displays the current provision status {"ongoing", "success", or "fail"}. It causes a search of the physical entity table to find out the physical entity. This command can only be executed on the IONMM or a standalone SIC. This command is available to Admin users only.

Example:

```
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...
Backup finished
C1|S1|L1D>restore module-list 1
Processing...
Restore finished
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>
```

Refresh Configuration Filename

Syntax: **refresh provision configure filename <**filename**>**

Description: Change the name of the "Config File" that displays when using the '**show provision modules**' command. The **refresh** command can be used to refresh a backup or restore configure file name.

Example:

```
Agent III C1|S1|L1D>refresh provision configure filename
Agent III C1|S1|L1D>
```

Messages: *The specified module does not exist!*
Invalid backup module-list, please give the parameter like module-list=1,4,13
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.
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!

Save Configuration Module list

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

Description: Backup the configurations of the specified provision modules. The *string* is a comma separated list of the modules. To get the index, use the command "show provision backup modules" and then select which index matches the cards you want to back up.

Example:

```
Agent III C1|S3|L1D>saveconf module-list 1,2,4
Backing up 3 modules.....
Operation succeeded for module = 1, physical index = 134217728.
.....
Operation succeeded for module = 2, physical index = 147849216.
....
Operation succeeded for module = 4, physical index = 227540992.
.
Operation finished successfully.
Agent III C1|S3|L1D>
```

8. Backup All / Restore All Commands

IONMM v 1.3.18 adds Backup All and Restore All capabilities. The new Backup All and Restore All features can be configured via the ION System Web GUI or CLI commands. The Backup/Restore feature provides Automatic TFTP transfer, Backup and restore of up to 41 modules at one time, Time-stamped filenames that include the stack name and index number, and Time-stamped tarfile containing all the config files. See the *IONMM User Guide, 33457* for details.

Backup All

Syntax: **backup all**

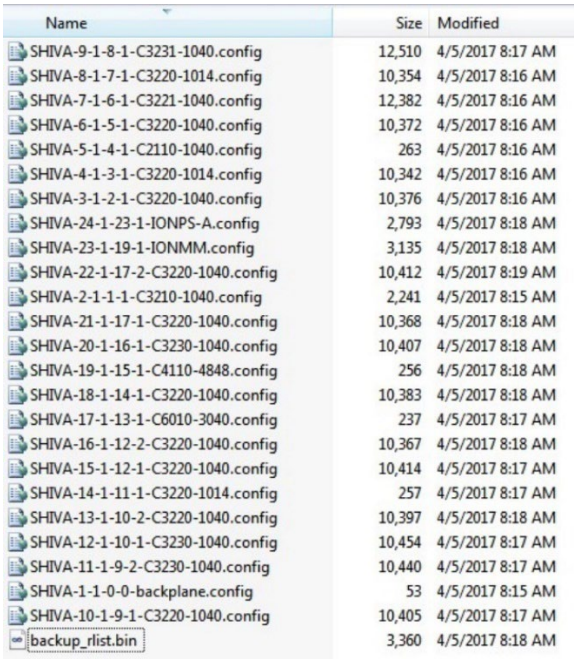
Description: Backup the configuration for all cards in the ION chassis.
This command finds all the cards in the chassis, backs up the configs in a time-stamped TAR file (*.tar), and transfers the file to the PC using TFTP or SFTP. The TFTP or SFTP server address must be set first before running this command.

Example:

```
Agent III C1|S1|L1D>prov set tftp svr type ipv4 addr 192.168.0.61
Agent III C1|S1|L1D>backup all
::-> timeStamp = 19700106_11-45-25-AM
::-> tftpaddr = 192.168.0.10
::-> rm -f /tftpboot/*
==> Found all chassis cards <==

::--> backupname = SN101829_backup_19700106_11-45-25-AM.tar
::--> backupModuleIndex = 18
::--> backupCommand = 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
Processing...
.......................
Backup finished
Agent III C1|S1|L1D>
```

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

```
Agent III C1|S19|L1D>show prov bac mod
Index   Module                          Config File
tus
-------------------------------------------------------------------------------------
---
1       [00]                            SHIVA-1-1-0-0-backplane.config
2       [01]                            SHIVA-2-1-1-1-C3210-1040.config
3       [02]                            SHIVA-3-1-2-1-C3220-1040.config
4       [03]                            SHIVA-4-1-3-1-C3220-1014.config
5       [04]                            SHIVA-5-1-4-1-C2110-1040.config
6       [05]                            SHIVA-6-1-5-1-C3220-1040.config
7       [06]                            SHIVA-7-1-6-1-C3221-1040.config
8       [07]                            SHIVA-8-1-7-1-C3220-1014.config
9       [08]                            SHIVA-9-1-8-1-C3231-1040.config
10      [09]                            SHIVA-10-1-9-1-C3220-1040.config
11      [09:L2]REM:                     SHIVA-11-1-9-2-C3230-1040.config
12      [10]                            SHIVA-12-1-10-1-C3230-1040.config
13      [10:L2]REM:                     SHIVA-13-1-10-2-C3220-1040.config
14      [11]                            SHIVA-14-1-11-1-C3220-1014.config
15      [12]                            SHIVA-15-1-12-1-C3220-1040.config
16      [12:L2]REM:                     SHIVA-16-1-12-2-C3220-1040.config
17      [13]                            SHIVA-17-1-13-1-C6010-3040.config
18      [14]                            SHIVA-18-1-14-1-C3220-1040.config
19      [15]                            SHIVA-19-1-15-1-C4110-4848.config
20      [16]                            SHIVA-20-1-16-1-C3230-1040.config
21      [17]                            SHIVA-21-1-17-1-C3220-1040.config
22      [17:L2]REM:                     SHIVA-22-1-17-2-C3220-1040.config
23      [19]                            SHIVA-23-1-19-1-IONMM.config
24      [23]                            SHIVA-24-1-23-1-IONPS-A.config
Agent III C1|S19|L1D>backup all
::-> timeStamp = 20170405_07-15-31-AM
::-> tftpaddr = 192.168.0.61
::-> rm -f /tftpboot/*
==> Found all chassis cards <==

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



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

Restore All

Syntax: **restore all** <tarfile name>

Description: Restore configuration files in backup TAR file via TFTP or SFTP.
This command will transfer the named TAR file via TFTP or SFTP to the IONMM and write the config files to the cards. This assumes that the cards' model numbers (e.g., C3220-1014) and slot numbers are the same as those in the TAR file.

Example:

```
Agent III C1|S1|L1D>prov set tftp svr type ipv4 addr 192.168.0.61

Agent III C1/S19/L1D>restore all backup_20170131_04-12-04-PM.tar
::-> backupname = backup_20170131_04-12-04-PM.tar
::-> tftpaddr = 192.168.0.61
::-> tftp -r backup_20170131_04-12-04-PM.tar -g 192.168.0.61
::-> mv /tftpboot / tftpboot_old
::-> tar -xvf backup_20170131_04-12-04-PM.tar
::-> restoreCommand = 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Processing...
::-> Restore file name: GP-1-1-1-C3220-1040.config
::-> Restore file name: GP-1-2-1-C3220-1040.config
::-> Restore file name: GP-1-3-1-C3220-1040.config
::-> Restore file name: GP-1-4-1-C3230-1040.config
::-> Restore file name: GP-1-5-1-C3230-1040.config
::-> Restore file name: GP-1-6-1-C3221-1040.config
::-> Restore file name: GP-1-7-1-C3230-1040.config
::-> Restore file name: GP-1-8-1-C3220-1014.config
::-> Restore file name: GP-1-9-1-C2220-1014.config
::-> Restore file name: GP-1-10-1-C3110-1040.config
::-> Restore file name: GP-1-11-1-C6210-3040.config
::-> Restore file name: GP-1-12-1-C6010-3040.config
::-> Restore file name: GP-1-13-1-C3231-1040.config
::-> Restore file name: GP-1-14-1-C4110-4848.config
::-> Restore file name: GP-1-15-1-C3210-1040.config
::-> Restore file name: GP-1-16-1-C3220-1040.config
::-> Restore file name: GP-1-17-1-C3210-1013.config
::-> Restore file name: GP-1-19-1-IONMM.config
::-> Restore file name: GP-1-22-1-IONPS-A-R1.config
```

9. Bandwidth Commands

The following commands are used to set bandwidth limiting rates.

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 or 2 for the x3230, or x is 1, 2 or 3 for the x3231). These commands cannot be entered at the device level – only at the port level.

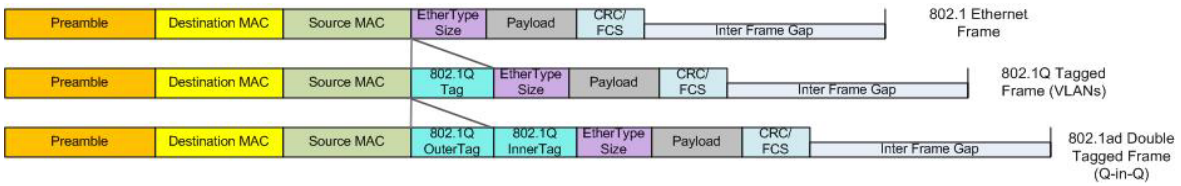
Set Bandwidth Rate Limiting Mode

Syntax: **set bw alloc-type**={countAllLayer1 | countAllLayer2 | countAllLayer3}

Description: Defines which transmission layer is to be counted when determining the rate limit.
Note: this command is not supported on all models.

- **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 **countAllLayer3** selection will skip the Ethernet header, the CRC, and Tags (if any tags exist).



Example:

```
C1|S5|L1P1>set bw alloc-type=countAllLayer2
C1|S5|L1P1>show bandwidth allocation
Bandwidth allocation type:    countAllLayer2
Ingress rate:                 unLimit
Egress rate:                  unLimit
C1|S5|L1P1>
```

Set Bandwidth Rate Limit

Syntax: **set irate=**<xx> **erate=**<yy>

Description: Defines the ingress and egress rate limits of a port. Sets ingress rate and egress rate of a port with increased granularity of Ingress/Egress Rate Limiting per MEF 11.
Provides 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.

where: **xx** = In-rate: Ingress rate in bps.

yy = Egress rate: Egress rate in bps (bits per second).

The valid selections are:

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.

Example:

```
Agent III C1|S1|L1P1>set irate rate10M erate rate10M
Error: Cannot set ingress and egress rate on this card!
Agent III C1|S1|L1P1>go c=1 s=9 l1p=1
Agent III C1|S9|L1P1>set irate rate1M erate rate1M
Agent III C1|S9|L1P1>show bandwidth allocation
Bandwidth allocation type:    countAllLayer1
Ingress rate:                 rate1M
Egress rate:                  rate1M
Agent III C1|S9|L1P1>set irate rate9M erate rate10
% Ambiguous command.
Agent III C1|S9|L1P1>set irate rate9M erate rate10M
Error: Cannot set erate because erate is bigger than port speed!
Agent III C1|S9|L1P1>set irate rate9M erate rate2M
Agent III C1|S9|L1P1>show bandwidth allocation
Bandwidth allocation type:    countAllLayer1
Ingress rate:                 rate9M
Egress rate:                  rate2M
Agent III C1|S9|L1P1>
```

Messages: *Error: Cannot set erate because erate is bigger than port speed!*

Note: The rate parameters are case-sensitive. Use the **show bandwidth allocation** command to verify the setting. This command does not work on the IONMM ports.

Show Bandwidth Allocation Configuration

Syntax: **show bandwidth allocation**

Description: Shows the bandwidth allocation for a port.

Example:

```
C1|S5|L1P1>set bw alloc-type countAllLayer2
C1|S5|L1P1>show bandwidth allocation
Bandwidth allocation type:    countAllLayer2
Ingress rate:                 unLimit
Egress rate:                  unLimit
C1|S5|L1P1>
```

Note: this command is not supported on all models.

10. DMI Commands

The following commands are used for Diagnostic Monitoring Interface (DMI) operations. **Note**: These commands can only be entered for a fiber port that supports DMI. Not all NID models or SFP models support DMI. Lantronix NIDs that support DMI have a "D" at the end of the model number. If you enter a DMI command on a NID model that does not support DMI, the message "*The DMI feature is not supported on current port*." displays.

Show DMI Configuration

Syntax: **show dmi info**

Description: Displays the Diagnostic Monitoring Interface (DMI) information for a fiber port.

Example:

```
Agent III C1|S6|L1D>go c=1 s=7 l1d
Agent III C1|S7|L1D>go l1p=2
Agent III C1|S7|L1P2>show dmi info
Diagnostic monitoring interface information:
-------------------------------------------------------------------------
DMI connector type:                     LC
DMI indentifier:                        SFP/SFP+/SFP28
DMI Nominal bit rate:                   1300*Mbps
DMI Nominal bit rate:                   1300*Mbps
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:                        37.5*C
DMI temperature:                        99.5*F
DMI temperature alarm:                  normal
DMI transmit bias current:              3872*uA
DMI transmit bais alarm:                normal
DMI Transmit power:                     212*uW
DMI Transmit power:                     -6.737*dBM
DMI Transmit power alarm:               normal
DMI Receive power:                      0*uW
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:  0*uW
Agent III C1|S7|L1P2>
```

Set DMI Receive Power Preset Level

Syntax: **set dmi rx–power–preset–level=**<xx>

Description: Defines the lowAlarm threshold for RxPowerAlarm. If a non-zero value (in microwatts) is specified, the module will stop passing traffic when the receive power drops below the new threshold. This feature is sometimes referred to as Intrusion Detection, since tapping into a fiber to intercept traffic leads to a reduction in receive power.

Sets the Diagnostic monitoring interface (DMI) receive preset power level for a fiber port, where:

xx = Pwr-val: A preset level for Rx Power on the Fiber port (0-65535).

Example:

```
Agent III C1|S7|L1P2>set dmi rx-power-preset-level=110
Agent III C1|S7|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:                        38.1*C
DMI temperature:                        100.6*F
DMI temperature alarm:                  normal
DMI transmit bias current:              3904*uA
DMI transmit bais alarm:                normal
DMI Transmit power:                     210*uW
DMI Transmit power:                     -6.778*dBM
DMI Transmit power alarm:               normal
DMI Receive power:                      0*uW
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|S7|L1P2>
```

The **show dmi** command parameters are described in the table below.

Table 4: 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.
Temperature (˚F)	ionDMITemperature(10)	Measured Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). For example: 86.2 ˚F.

Parameter	Associated MIB variable	Description
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

Parameter	Associated MIB variable	Description
		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.

11. Dot1bridge Commands

The following dot1bridge commands are used to add, remove, set, and show Dot1bridge (802.1) functions (reference RFC 1493, “Definitions of Managed Objects for Bridges”).

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Set Dot1bridge Aging Time

Syntax: **set dot1bridge aging–time=<**xx**>**

Description: Defines the aging time of a bridge.

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.

where:

xx = 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 (0 - 63.75 minutes).

Example:

```
C1|S3|L1P2>set dot1bridge aging-time=15
C1|S3|L1P2>set dot1bridge aging-time=0
C1|S3|L1P2>set dot1bridge aging-time ?
  <0-3825>
```

Note: 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.

Note: While the x323x 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 x323x interface (as limited by x323x memory space and CPU capability).

Show Dot1bridge Aging Time

Syntax: **show dot1bridge aging-time**

Description: Displays the aging time for a dot1bridge.

Example:
```
C1|S13|l0d/>show dot1bridge aging-time
Dot1bridge aging time:                    60
```

12. Dot1dbridge Commands

The following Dot1dbridge commands are used to add, remove, set, and show dot1dbridge functions (reference the IEEE 802.1d standard).

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Set Dot1dbridge IEEE Tag Priority

Syntax: **set dot1dbridge ieee-tag-priority**=<x> **remap-priority**=<y>

Description: Defines the IEEE 802.1d tagging priority and remapping priority to be used for the NID.

where:

x=<0-7>
y=<0-3>

Example:
```
C1|S5|L1D>set dot1dbridge ieee-tag-priority=4 remap-priority=3
C1|S5|L1D>
```

Set Dot1dbridge IP Priority Index

Syntax: **set dot1dbridge ip-priority-index**=x

Description: Defines the IEEE 802.1d IP priority index to be used for the NID.

where:

x = <0-63>

Example:
```
C1|S5|L1D>set dot1dbridge ip-priority-index=9 remap-priority=2
C1|S5|L1D>
```

Show Dot1dbridge IEEE Tag Priority Remapping

Syntax: **show dot1dbridge ieee-tag priority remapping**

Description: Displays the current IEEE 802.1d tag priority index and remapping priority configuration of the NID.

Example:

```
C1|S5|L1D>show dot1dbridge ieee-tag priority remapping
IEEE priority-index                    remapping-priority
-------------------------------------------------------
0                                      0
1                                      0
2                                      1
3                                      1
4                                      2
5                                      2
6                                      3
7                                      3
C1|S5|L1D>
```

Show Dot1dbridge IP-TC Priority Remapping

Syntax: **show dot1dbridge ip-tc priority remapping**

Description: Displays the current IEEE 802.1d priority index, traffic class and remapping priority configuration of the NID.

Example:

```
C1|S5|L1D>show dot1dbridge ip-tc priority remapping
priority-index      traffic class       remapping-priority
-------------------------------------------------------------------------
0                   0                   0
1                   4                   0
2                   8                   0
3                   12                  0
4                   16                  0
5                   20                  0
6                   24                  0
7                   28                  0
8                   32                  0
9                   36                  0
10                  40                  0
::                    ::                    :
60                  240                 3
61                  244                 3
62                  248                 3
63                  252                 3
C1|S5|L1D>
```

13. Ethernet Port Commands

The following commands are used for Ethernet port operations. The functions of some of the Ethernet port commands below depend on the type of port, as shown in the "Port Type" column in the table below.

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). An asterisk (*) indicates Read only (ON) capability.

Table 5: Ethernet Port Feature Compatibility

Feature	Port Type			
	10/100/1000 BaseT	100 BaseFX	1000 BaseX	SGM II
Advertised Capabilities	√			
AutoCross	√			
Auto Negotiation	√		*	*
Duplex	√	√		
Far End Fault (FEF)		√	√	
Layer 2 Control Protocol (L2CP)	√	√	√	√
Loopback		√	√	
Pause	√	√		
PHY mode		√	√	√
Speed	√			

Clear Ethernet Port Counters

Syntax: **clear ether all counters**

Description: Clears the Ethernet port counters on a slide-in module' port. The counts (RMON statistics counters, dot3 counters, etc.) are reset to zero and begin incrementing immediately.

Example:
```
C1|S5|L1D>go l1p=1
C1|S5|L1P1>clear ether all counters
C1|S5|L1P1>go l1p=2
C1|S5|L1P2>clear ether all counters
C1|S5|L1P2>
```

Note: Use the **show ether statistics** command to display the current Ethernet port counter information.

Clear All Ports Counters

Syntax: **reset all ports counters**

Description: Resets all counters on all ports of the specified Ethernet device. The device's counts (RMON statistics counters, dot3 counters etc.) are reset to zero and begin incrementing immediately.

Example:
```
C1|S5|L1D>reset all ports counters
C1|S5|L1D>
```

Note: Use the **show ether config** command to show the current Link operation status.

Set Ethernet Port Admin Status

Syntax: **set ether admin state**={up | down}

Description: Specifies whether or not the Ethernet port is available for use.

Example:
```
C1|S3|L1P2>set ether admin state ?
  down
  up
C1|S5|L1P2>set ether admin state up
C1|S5|L1P2>
```

Note: Use the **show ether config** command to show the current link operation status.

Set Ethernet Port Advertisement Capability

Syntax: **set ether adv–cap=**<xx>

Description: Specifies the linking capability to be auto-negotiated for this Ethernet port.

The Auto-negotiate feature must be enabled for this command to have any affect (see "Set Ethernet Port Auto-Negotiation Status"). In addition to the speed and duplex function, the port also advertises whether it supports Pause frames (see "Set Ethernet Port Pause Frames").

Where:

xx = 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).

Example:

```
C1|S5|L1P2>set ether adv-cap 1000XHD
Fail to set port advertisement capability!
C1|S5|L1P2>set ether adv-cap 1000XFD
C1|S5|L1P2>go c=1 s=1 l1p=1
C1|S1|L1P1>set ether adv-cap ?
  STR_ETHER_ADV_CAPABILITY  A combination of 10THD,10TFD,100TFD,
100THD,1000THD
and 1000TFD for copper port, like 10TFD+100TFD+100THD+1000TFD; and N/A
for none
capability; Cannot set this attribute for fiber port
C1|S1|L1P1>set ether adv-cap 100TFD
C1|S1|L1P1>
```

Set Ethernet Port *AutoCross*

Syntax: **set ether autocross=**<xx>

Description: Defines whether the cabling for this Ethernet port is cross-over or straight through, or whether the system will automatically adjust as needed. Lantronix recommends leaving AutoCross in its default mode (auto).

where:
xx = valid choices are:

- **auto** – automatically correct errors in cable selection (default – recommended)
- **mdi** – transmit pair on one end of the cable is connected to the receive pair on the other end
- **mdi-x** – straight through cable (transmit to transmit/receive to receive)

Example:
```
C1|S5|L1P2>set ether autocross mdi
Cannot set autocross on Fiber port!
C1|S5|L1P2>go l1p=1
C1|S5|L1P1>set ether autocross mdi
C1|S5|L1P1>
```

Note: This command is only applicable on a copper port. Use the **show ether config** command to display the current auto-negotiation state.

Set Ethernet Port Auto-Negotiation Status

Syntax: **set ether autoneg state**={enable | disable}

Description: Defines whether the auto-negotiation feature is enabled or disabled for this Ethernet port.
If enabled, speed and duplex information will automatically be exchanged over the link. The information that is advertised for this port is specified by the Set Ethernet Port Advertisement Capability command (page 89).

Example:
```
C1|S3|L1P2>set ether autoneg state=enable
Cannot set auto-negotiation state on this port!
C1|S3|L1P2>go l1p=1
C1|S3|L1P1>set ether autoneg state=enable
C1|S3|L1P1>
```

Note: This command is only applicable on a copper port. Use the **show ether config** command to display the current auto-negotiation state.

Set Ethernet Port Duplex Mode

Syntax: **set ether duplex**={full | half}

Description: Defines whether the Ethernet port operates in full or half-duplex.

Example:
```
C1|S5|L1P1>set ether duplex full
C1|S5|L1P1>set ether duplex half
C1|S5|L1P1>
```

Note: Use the **show ether config** command to display the current auto-negotiation state.

Set Ethernet Port Filter 802.1Q Tagged Non-Management Frames

Syntax: **set ether filter–unknown–unicast**={true | false}

Description: Defines whether 802.1Q tagged non-management frames can be transmitted/received through the Ethernet port.

802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN (and/or 802.1p priority) information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches.

Example:
```
C1|S5|L1P2>set ether filter-unknown-multicast=true
C1|S5|L1P2>set ether filter-unknown-unicast=true
C1|S5|L1P2>
```

Set Ethernet Port Filter 802.1Q Untagged Non-Management Frames

Syntax: **set ether filter–unknown–multicast**={true | false}

Description: Defines whether 802.1Q untagged non-management frames can be transmitted/received through the Ethernet port.

802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. It is important to ensure ports with non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many NICs for PCs and printers are not 802.1Q-compliant. If they receive a tagged frame, they will not understand the VLAN tag and will drop the frame.

Example:
```
C1|S5|L1P2>set ether filter-unknown-multicast=true
C1|S5|L1P2>set ether filter-unknown-unicast=true
C1|S5|L1P2>
```

Set Ethernet Port LOAM Loopback Type

Syntax: **set ether loopback type=**<xx>

Description: Defines the type of LOAM loopback method used on an Ethernet port.

where:

xx = loopback method; the choices are:

- **alternate** - allows the data frames to be forwarded to other ports, while doing the loopback with its peer.
- **noloopback** – the port will not perform any loopback.
- **remote** - Remote Peer - prevents that port from forwarding data frames to other ports when it goes into "loopback" mode ("intrusive loopback").

Example:

```
AgentIII C1|S8|L1D>set ether loopback type ?
  alternate
  maclayer
  noloopback
  phylayer
  remote
AgentIII C1|S8|L1D>set ether loopback type alternate
Error: this command should be executed on a port!
AgentIII C1|S8|L1D>go l1p=1
AgentIII C1|S8|L1P1>set ether loopback type alternate
AgentIII C1|S8|L1P1>set ether loopback type maclayer
Set Ethernet port loopback type failed.
AgentIII C1|S8|L1P1>set ether loopback type noloopback
AgentIII C1|S8|L1P1>set ether loopback type phylayer
Set Ethernet port loopback type failed.
AgentIII C1|S8|L1P1>set ether loopback type remote
AgentIII C1|S8|L1P1>
```

Note: Use the **show loam loopback state** command or the **show loam loopback capability** command to display the current loopback type settings.

Set Ethernet Port Pause Frame Type

Syntax: **set ether pause=**<xx>

Description: Defines whether the Ethernet port supports pause frames (data pacing). Pause frames are used as a method of flow control on full duplex Ethernet connections. If a sending device is transmitting data faster than the receiving device can accept it, the receiving station will send a pause frame to halt the transmission of the sender for a specified period of time.

Pause frames are only used on full duplex Ethernet link segments that are defined by IEEE 802.3x and use MAC control frames to carry the pause commands. Only stations configured for full duplex operation can send pause frames.

where:

xx = pause type; 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
- **pause** (the port will advertise it has pause capability)
- **spause** (symmetric; the port will advertise that it can transmit and receive pause frames)

Example:

```
C1|S5|L1P1>set ether pause=pause
C1|S5|L1P1>set ether pause=nopause
C1|S5|L1P1>set ether pause=apause
C1|S5|L1P1>set ether pause=bpause
Invalid pause value!
C1|S5|L1P1>set ether pause=spause
Invalid pause value!
C1|S5|L1P1>go l1p=2
C1|S5|L1P2>set ether pause=pause
Invalid pause value!
C1|S5|L1P2>set ether pause=nopause
C1|S5|L1P2>set ether pause=apause
C1|S5|L1P2>set ether pause=bpause
C1|S5|L1P2>set ether pause=spause
C1|S5|L1P2>
```

Note : Use the **show ether config** command to display the current pause capability and pause setting.

Set Ethernet Port Source MAC Address Lock

Syntax: **set ether src–addr–lock**={true | false}

Description: Defines whether or not there is a source MAC address lock for the Ethernet port.

In its most basic form, 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.

Example:

```
C1|S5|L1P2>set ether src-addr-lock=enable
C1|S5|L1P2>set ether src-addr-lock action ?
  all
  discard
  discardandnotify
  shutdown
C1|S5|L1P2>set ether src-addr-lock action=discard
C1|S5|L1P2>set ether src-addr-lock action=discardandnotify
C1|S5|L1P2>set ether src-addr-lock action=shutdown
C1|S5|L1P2>set ether src-addr-lock action=all
C1|S5|L1P2>show ether security config
Ethernet port security configuration:
-----------------------------------------------------------------
Source MAC address lock:           enable
Source MAC address lock action:    all
Filter unknown dest unicast:       true
Filter unknown dest multicast:     true
C1|S5|L1P2>
```

Set Ethernet Port Source MAC Address Lock Action

Syntax: **set ether src–addr–lock action=**<xx>

Description: Defines the action to be taken when the MAC address lock feature is enabled through the Set Ethernet Port Source MAC Address Lock command.
where:

xx = valid choices are:

- **discard** (discard any transmissions received on the port)
- **discardandnotify** (discard any transmissions received on the port and send an SNMP trap to the trap server)
- **shutdown** (disables the port)
- **all**

Example:

```
C1|S5|L1P2>set ether src-addr-lock=enable
C1|S5|L1P2>set ether src-addr-lock action ?
  all
  discard
  discardandnotify
  shutdown
C1|S5|L1P2>set ether src-addr-lock action=discard
C1|S5|L1P2>set ether src-addr-lock action=discardandnotify
C1|S5|L1P2>set ether src-addr-lock action=shutdown
C1|S5|L1P2>set ether src-addr-lock action=all
C1|S5|L1P2>show ether security config
Ethernet port security configuration:
------------------------------------------------------------------
Source MAC address lock:           enable
Source MAC address lock action:    all
Filter unknown dest unicast:       true
Filter unknown dest multicast:     true
C1|S5|L1P2>
```

Set Ethernet Port Speed

Syntax: **set ether speed**={10M | 100M | 1000M}

Description: Defines the transmission speed to be used on a Ethernet copper port. If Auto-negotiation is enabled, you cannot set the port speed.

Example (copper port):

```
C1|S5|L1P1>set ether speed ?
  1000M
  100M
  10M
C1|S5|L1P1>set ether speed 1000M
Auto-negotiation is enabled, you cannot set port speed now!
C1|S5|L1P1>set ether autoneg state disable
C1|S5|L1P1>set ether speed 1000M
C1|S5|L1P1>set ether speed 100M
C1|S5|L1P1>set ether speed 10M
```

This command does not work on a fiber port.

Note: Use the **show ether config** command to display the current speed setting of an Ethernet port.

Show Ethernet Port Configurations

Syntax: **show ether config**

Description: Displays the NID Ethernet port configuration.

Different ports have different capabilities, so the display content will vary according to the NID type and port type.

Example 1: An example for a TP Port (copper port) is shown below.

```
Agent III C1|S1|L1P2>go c=1 s=9 l1p=1
Agent III C1|S9|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|S9|L1P1>
```

Example 2: An example of a FIBER port (SFP port) is shown below.

```
Agent III C1|S9|L1P1>go l1p=2
Agent III C1|S9|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|S9|L1P2>
```

Show Ethernet Port Loopback Capability

Syntax: **show ether loopback capability**

Description: Displays the LOAM loopback capability of the Ethernet port.

Example:
```
C1|S5|L1P1>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P1>go l1p=2
C1|S5|L1P2>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P2>
```

Note: The loopback capabilities that can be reported include alternate remotePeer, noloopback, and remote.

Show Ethernet Port Loopback Running Status

Syntax: **show ether loopback state**

Description: Displays the loopback test's running status of the Ethernet port.

Example:
```
C1|S5|L1P2>show ether loopback state
Loopback type: noloopback
Loopback state: noLoopback
C1|S5|L1P2>go l1p=1
C1|S5|L1P1>show ether loopback state
Loopback type: noloopback
Loopback state: noLoopback
C1|S5|L1P1>
```

Note: The loopback states that can be reported include alternate, noloopback, and remote.

Show Ethernet Port Security Configuration

Syntax: **show ether security config**

Description: Displays the security configuration for an Ethernet port.

Example:

```
C1|S5|L1P1>show ether security config
Ethernet port security configuration:
-----------------------------------------------------------------
Source MAC address lock:           false
Source MAC address lock action:    discardandnotify
Filter unknown dest unicast:       false
Filter unknown dest multicast:     false
C1|S5|L1P1>go l1p=2
C1|S5|L1P2>show ether security config
Ethernet port security configuration:
-----------------------------------------------------------------
Source MAC address lock:           false
Source MAC address lock action:    discardandnotify
Filter unknown dest unicast:       false
Filter unknown dest multicast:     false
C1|S5|L1P2>
```

Show Ethernet Port TDR Test Configuration

Syntax: **show ether tdr config**

Description: Displays the Time Domain Reflectometry (TDR) test configuration for the Ethernet port. This command is only available for a copper port.

Example:

```
C1|S5|L1P2>show ether tdr config
No TDR test result on FIBER port!
C1|S5|L1P2>go s=5 l1p=1
C1|S5|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----------------------------------------------------------------
TDR test state:                unknown
TDR test init time:            00:00:00
TDR test result valid:         false
```

Show Ethernet Port TDR Test Result

Syntax: **show ether tdr test result**

Description: Displays the results of an Ethernet port TDR test. This command is only available for a copper port. See the **start ether tdr test** command for more information.

Example:

```
C1|S5|L1P1/>show ether tdr test result
Cable pair :
index               distance to fault(unit)       status
-------------------------------------------------------------------
pair1and2            0(meter)                      open
pair3and6            1(meter)                      open
pair4and5            0(meter)                      open
pair7and8            0(meter)                      open
```

Note: Run the TDR test several times to ensure accurate results. Do not change port status (e.g., remove the cable at the near end or far end) as this may cause inaccurate results.

Show Ethernet Statistics

Syntax: **show ether statistics**

Description: Displays Ether-like counters and If-MIB counters for a port. This command is not available on the IONMM or Power Supply.

Example:

```
C1|S5|L1P1>show ether statistics
Port Counters Received:
------------------------------------------------------------------
Total Octets:                           537241
Unicast Packets:                        0
Broadcast Packets:                      4189
Multicast Packets:                      0
Rx Discards:                            0
Rx Errors:                              0

Port Counters Sent:
------------------------------------------------------------------
Total Octets:                           754674
Unicast Packets:                        0
Broadcast Packets:                      0
Multicast Packets:                      11433
Rx Discards:                            0
Rx Errors:                              0

Dot3 Statistics:
------------------------------------------------------------------
Alignment Errors:                       0
FCS Errors:                             0
SQE Test Errors:                        0
Deferred Frames:                        0
Internal MAC Tx Errors:                 0
Internal MAC Rx Errors:                 0
Carrier Sense Errors:                   0
Symbol Errors:                          0
Single Collisions:                      0
Multiple Collisions:                    0
Late Collisions:                        0
Excessive Collisions:                   0
Oversized Frames:                       0
Duplex Status:                          fullDuplex
Rate Control Ability:                   false
Rate Control Status:                    off

MAC Control Frames:
------------------------------------------------------------------
Rx Unknown Opcodes:                     0
Rx Pause Frames:                        0
Tx Pause Frames:                        0
C1|S5|L1P1>
```

Start/Stop Ethernet Port Loopback Operation

Syntax: **set ether loopback oper**={init|stop}

Description: Defines whether a LOAM loopback test is to be initiated (init) or stopped (stop) on an Ethernet port. The LOAM loopback test can be used as an aid in detecting physical connection problems.

Example:

```
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 admin state=up
C1|S3|L1P1>set ether loopback oper init
C1|S3|L1P1> set ether loopback oper stop
```

Note: LOAM must be enabled on both ends of the link, and LOAM mode must be set to active. The LOAM Admin state for this port must be set to **up** before this command will work. See the **set ether admin state** command.

This command puts a slide-in module in a special mode that enables the device to loop back the signal from the RX port to the TX port on either media for testing and troubleshooting purposes. Test signals from a tester (Firebird, etc.) can then be inserted into the link and looped back as received by a device to test a particular segment of the link (i.e., copper or fiber). Loopback can be either local or remote depending on the location of the converter in the link. Some slide-in modules have separate copper and fiber loopback functions that can be enabled separately, while others will loopback both copper and fiber at the same time when enabled.

Start Ethernet Port TDR Test

Syntax: **start ether tdr test**

Description: Starts a Time Domain Reflector (TDR) test on the Ethernet port. TDR is a method for determining the general characteristics of impedance variations in a transmission line. In this method a test pulse is transmitted down the line and the reflection from an impedance discontinuity is detected together with the time it takes for the pulse to reach the discontinuity and return. The location of the discontinuity is determined by observation of the elapsed time between the transmitted pulse and the reflected pulse.

This technique is highly sensitive, revealing not only gross defects, such as open or short circuited cables and terminations, but also revealing quite minute variations, e.g., cable impedance variations, frayed shields, and impedances introduced by making tap connections to the cable.

Example:

```
C1|S5|L1D>show ether tdr config
Error: this command should be executed on a port!
C1|S5|L1D>go l1p=2
C1|S5|L1P2>show ether tdr config
No TDR test result on FIBER port!
C1|S5|L1P2>go l1p=1
C1|S5|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----------------------------------------------------------------
TDR test state:               unknown
TDR test init time:           00:00:00
TDR test result valid:        false
C1|S5|L1P1>
```

Messages: *Error: No TDR test result on FIBER port!*

Use the **show ether tdr test result** command to display the TDR test results.

Use the **show ether tdr config** command to display the TDR test validity and init time.

Set L2CP Protocol Handling

Syntax: **set l2cp proto=**<xx> **process=**{pass/discard}

where:

xx = the particular L2CP protocol; the valid entries are:

- **spanningTree** - Any STP/RSTP/MSTP protocol frame with a destination address (DA) of 01-80-C2-00-00-00 is discarded at this port or passed. Spanning Tree Protocols (STP) disposition – handling of 802.1D Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP, per IEEE 802.1w).
- **slow** - Any LACP/LAMP protocol frames with DA 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. Provides 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.
- **portAuthentication** – protocol frames with a DA of 01-80-C2-00-00-03 is discarded at this port or passed. Port Authentication Protocols disposition – handling of RADIUS, CHAP, EAP, EAPOL, 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** - E-LMI protocol frames with a DA of 01-80-C2-00-00-07 is discarded at this port or passed. Provides 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 to ease deployment and servicing.
- **lldp** - LLDP protocol frames with a DA of 01-80-C2-00-00-0E which are not TN discovery LLDP frames are discarded at this port or passed. Provides handling of Link Layer Discovery Protocol (LLDP), a Layer 2 protocol defined by IEEE Standard 802.1AB-2005.
- **bridgeMgmt** - Bridge Management protocol frames with a DA of 01-80-C2-00-00-10 are discarded at this port or passed. Provides handling of one of several protocols per IEEE 802, including Bridge Group Address (STP), IEEE Std. 802.3x Full Duplex PAUSE operation, Bridge Management Group Address, GMRP and GVRP.
- **garpmrpBlock** - 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).
- **bridgeBlockOtherMulticast** - 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]. Applies to all addresses in this block that are not covered by the other MIB variables in this table (i.e., this is not applicable for STP, slow protocols, etc.).

Description: Sets the current Layer 2 Control Protocol processing configuration. Layer 2 Control Protocol processing (L2CP) is supported, allowing each of the layer 2 control protocols to be passed or discarded. Layer 2 Control Protocol Processing is supported at the per-port level. By default, all of the L2CP protocols are set to "**pass**".

Example:

```
Agent III C1|S9|L1P1>set l2cp proto ?
   spanningTree
   slow
   portAuthentication
   elmi
   lldp
   bridgeMgmt
   garpmrpBlock
   bridgeBlockOtherMulticast
Agent III C1|S9|L1P1>set l2cp proto=portAuthentication process=discard
Agent III C1|S9|L1P1>set l2cp proto=elmi process=discard
Agent III C1|S9|L1P1>set l2cp proto=lldp process=discard
Agent III C1|S9|L1P1>set l2cp proto=bridgeMgmt process=discard
Agent III C1|S9|L1P1>
```

L2CP LLDP Pass / Discard Function Not Supported

The previously supported L2CP LLDP frame forwarding 'pass or discard' function is no longer supported after version 1.3.0. All of the other L2CP protocols are still supported. It is set to "pass" "slow protocols" by default, but does not allow passing "01:80:C2:00:00:02" data.

For frames whose destination address is 01-80-C2-00-00-02, ION only allows LACP/LAMP protocol frames to pass. Per the standard MIB definition:

Name: ionIfL2CPSlowProtocolsFwd Type: OBJECT-TYPE OID: 1.3.6.1.4.1.868.2.5.3.1.2.7.1.2

Full path: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).transition(868).products(2).tnION-Products(5).tnIonMgmtMIB(3).tnIonMgmtObjects(1).ionInterfaceMgmt(2).ionIfL2CPTable(7).ionIfL2CPEntry(1).ionIf**L2CPSlowProtocolsFwd(2) Module**: TN-ION-MGMT-MIB

Parent: ionIfL2CPEntry Prev sibling: ionIfL2CPSTPProtocolsFwd

Next sibling: ionIfL2CPPortAuthProtocolFwd

Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: current Max access: read-write Value list: 1: pass(1) 2: discard(2) 3: notApplicable(3).

Description: 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.

Note: Currently the ION x2x2x/3x2x/3x3x SICs will only process the lldp from x2x2x/3x2x/3x3x SICs.

Show Ethernet Port L2CP Configuration

Syntax: **show l2cp config**

Description: Displays the current Layer 2 Control Protocol processing configuration. Layer 2 Control Protocol processing (L2CP) is supported, allowing each of the layer 2 control protocols to be passed or discarded. L2CP processing is supported at a per-port level.

Example:

```
Agent III C1|S9|L1P1>show l2cp config
Parameter                                       Value
-------------------------------------------------------------------
Spanning Tree Protocols                         pass
Slow Protocols                                  discard
Port Authentication Protocols                   pass
ELMI Protocols                                  discard
LLDP Protocols                                  discard
Bridge Mgmt Protocols                           pass
GARP/GMRP Block of Protocols                    pass
Bridge Block Other Multicast Protocols          pass
Agent III C1|S9|L1P1>
```

Set Port Admin Mode (Ethernet PHY Mode)

Syntax: **set ether phymode**=xx

Description:Sets the Ethernet PHY mode for a port which is capable of changing PHY mode.

where:

xx = port admin mode = {phySGMII | phy100BaseFX | phy1000BaseX}.

- phy1000BaseX
- phy100BaseFX
- phySGMII

Example:

```
Agent III C1|S9|L1P1>set ether phymode=phy1000BaseX
Error: Cannot set PHY mode on this port!
Agent III C1|S9|L1P1>go l1p=2
Agent III C1|S9|L1P2>set ether phymode=phy1000BaseX
Agent III C1|S9|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|S9|L1P2>
```

Note: use the **show ether config** command to display the current PHY operation mode (*phy1000BaseX* in the example above).

Note:

- The SFP port in 100BaseFx mode is set at 100Mbps with Duplex mode configurable. Far End Fault (FEF) is supported in this mode.
- The SFP port in 1000BaseX mode always has Auto-negotiation mode and Auto-negotiation Bypass mode enabled. Flow control is configurable in this mode.
- The SFP port operates in SGMII mode with Auto-negotiation always on. The Pause function is not available in SGMII Mode.

The default is 1000BaseX.

14. Forwarding Database Commands

The Forwarding Database Commands (FDB) are used to add, remove, set, and show fwddb (forwarding database) functions and parameters.

Note: These commands can only be entered when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Add Forwarding Database Entry

Syntax: **add fwddb mac=<**ww> [**conn–port=<**xx>] [**priority=<**yy>] [**type=<**zz>]

Description: Adds a new entry in the forwarding database.
where:

ww = MAC address

xx = optional; connection port number (factory default is 1)

yy = optional; priority of the entry (factory default is 0)

zz = optional; state of this unicast or multicast entry (factory default is static); valid choices are:

- **static**
- **staticNRL**
- **staticPA**

Example:

```
C1|S16|L1D>add fwddb mac 00-c0-f2-21-02-b3 conn-port=1 priority=7 type=static
C1|S16|L1D>
```

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.

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

Remove a Single Forwarding Database Entry

Syntax: **remove fwddb mac=<**xx**> fdbid=<**yy**>**

Description: Removes an entry from the forwarding database, where:

xx = MAC address

yy = forwarding database ID number (0–255)

Example:
```
C1|S16|L1D>remove fwddb mac 00-c0-f2-21-02-b3 fdbid 1
C1|S16|L1D>
```

Remove All Forwarding Database Entries

Syntax: **remove fwddb all**

Description: Removes all entries from the forwarding database.

Example:
```
C1|S16|L1D>remove fwddb all
C1|S16|L1D>
```

Set Forwarding Database Connection Port

Syntax: **set fwddb mac=<**xx**> fdbid=<**yy**> conn–port=<**zz**>**

Description: Defines the connect port of a row in the forwarding database, where:

xx = MAC address

yy = index of forwarding database index

zz = index of the logical port from which the device received

Example:
```
C1|S16|L1D>set fwddb mac 00-c0-f2-21-02-b3 fdbid=3 conn-port=2
C1|S16|L1D>
```

Set Forwarding Database Entry Type

Syntax: **set fwddb mac=<**xx> **fdbid =<**yy> **type=<**zz>

Description: Defines the entry type for the forwarding database, where:

xx = MAC address

yy = index number in the forwarding database

zz = state of this unicast or multicast entry; valid choices are:

- **static**
- **staticNRL**
- **staticPA**
- **dynamic**

Example:
```
C1|S5|L1D>set fwddb mac=01-11-11-11-11-11 fdbid=1 type=static
C1|S5|L1D>
```

Set Forwarding Database Priority

Syntax: **set fwddb mac=<**xx> **fdbid =<**yy> **priority=<**zz>

Description: Defines the connect port of a row in forwarding database, where:

xx = MAC address

yy = index number in the forwarding database

zz = priority of the entry

Example:
```
C1|S5|L1D>set fwddb mac 00-c0-f2-21-02-b3 fdbid=3 priority=5
C1|S5|L1D>
```

Set Forwarding Portlist

Syntax: **set fwd portlist=**<xx>

Description: Defines the forwarding port list, where:

xx = (0,1,2)

Example:
```
C1|S16|L1P1>set fwd portlist=0,1,2
C1|S16|L1P1>
```

Note: This command can only be entered at the port level - when the last part of the command line prompt indicates the location is a port (LxPx; where x is 1, 2 or 3).

Use the **show fwd portlist** command to display the current configuration.

Set Forwarding Port Management Access

Syntax: **set port mgmtaccess**={enable | disable}

Description: Enables or disables forwarding port management.

Example:
```
C1|S16|L1P1>set port mgmtaccess enable
C1|S16|L1P1>set port mgmtaccess disable
C1|S16|L1P1>
```

Note: This command can only be entered at the port level - when the last part of the command line prompt indicates the location is a port (LxP*z*; where *z* is 1, 2 or 3).

Show Forwarding Database (FDB) Configuration

Syntax: **show fwddb config fdbid=<**xx>

Description: Displays the configuration of forwarding database (0-255) for a device. Displays all dot1bridge MAC entries and related information for the NID in the location shown in the command line prompt. If the forwarding database is not yet configured, the message "*No data in VLAN forward database table now*!" displays.

Where:

xx = MAC address of the dot1bridge

Example 1:

```
C1|S13|l0d/>show fwddb config fdbid=0

Index  MAC               connect-port  priority     type
-----------------------------------------------------------------
1     00-C0-F2-02-03-0a   3             1            static
2     00-C0-F2-02-03-01   4             2            dynamic
```

Example 2:

```
C1|S12|L1D>show fwddb config fdbid 0
index      MAC           connect port  priority      type
1       00-00-74-9d-d1-76 1            0             dynamic
2       00-02-b3-e9-91-1e 1            0             dynamic
3       00-04-75-d0-0d-fe 1            0             dynamic
4       00-04-75-dc-57-9b 1           0             dynamic
5       00-04-75-dc-5c-2e 1           0             dynamic
6       00-0b-cd-3f-27-16 1           0               dynamic
7       00-0e-0c-4b-a2-63 1           0             dynamic
8       00-10-4b-1f-bd-7e 1           0             dynamic
9       00-11-0a-ca-a0-1a 1           0             dynamic
10      00-11-0a-f5-43-c7 1           0             dynamic
11      00-11-11-59-a0-23 1           0             dynamic
12      00-13-fa-01-17-6e 1           0             dynamic
C1|S12|L1D>
```

Show Forwarding Database Ports

Syntax: **show fwd portlist**

Description: Displays the forwarding (fwd) port list of a NID's port (0-255).

Example:
```
C1|S16|L1P1>show fwd portlist
port-id             fwd portlist        mgmt access
-------------------------------------------------------------
1                       2               enable
C1|S16|L1P1>
```

Note: This command can only be entered at the port level - when the last part of the command line prompt indicates the location is a port (LxPx; where x is 1, 2 or 3).

15. HTTPS Commands

For a description on how to configure the ION Management Module for Hypertext Transfer Protocol Secure (HTTPS) see the *IONMM User Guide, 33457*.

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

The following commands are used for HTTPS operations.

Set HTTPS Certificate File

Syntax: **set https certificate–file=**<name>

Description: Defines the name of the file containing the certificate(s) used for HTTPS operations.

Example:
```
C1|S5|L1D>set https certificate-file=scrob
C1|S5|L1D>show https config
HTTPS configuration:
-----------------------------------------------------------------
HTTPS state:                    disable
HTTPS port:                     443
HTTPS certificate file:         scrob
HTTPS private key file:
C1|S5|L1D>
```

Set HTTPS Certificate Type

Syntax: **set https certificate–type**={authorized | self–certificate}

Description: Defines whether the certificate is from an authorized certificate vendor or is self-defined.

Example:
```
C1|S5|L1D>set https certificate-type ?
  authorized
  self-certificate
C1|S5|L1D>set https certificate-type=authorized
C1|S5|L1D>set https certificate-type=self-certificate
C1|S5|L1D>
```

Set HTTPS Port Number

Syntax: **set https port=**<xx>

Description: Defines a port number that is different from the standard port number (443) that is to be used for HTTPS operations.

Example:

```
C1|S5|L1D>set https port=442
C1|S5|L1D>show https config
HTTPS configuration:
-------------------------------------------------------------------
HTTPS state:                  disable
HTTPS port:                   442
HTTPS certificate file:       scrob
HTTPS private key file:
C1|S5|L1D>
```

Set HTTPS Private Key File

Syntax: **set https private–key file=**<xx>

Description: Defines the name of the file containing the private key used for HTTPS operations.

Example:

```
C1|S5|L1D>set https private-key file=privfile
C1|S5|L1D>show https config
HTTPS configuration:
-------------------------------------------------------------------
HTTPS state:                  disable
HTTPS port:                   442
HTTPS certificate file:       scrob
HTTPS private key file:       privfile
C1|S5|L1D>
```

Set HTTPS Private Key File Password

Syntax: **set https private–key password**

Description: Interactive command used to define the HTTPS private key password. After entering this command you will be prompted to enter the password. You will then be prompted to re-enter the password.

Example:

```
C1|S5|L1D>set https private-key password
Please input password:
<your password> <cr>
Please input password again:
<your password> <cr>
C1|S5|L1D>
```

Set HTTPS State

Syntax: **set https state**={enable | disable}

Description: Enables or disables HTTPS.

Enabling HTTPS has no affect on either the USB or Telnet interface. However, access through the Web interface must go through HTTPS authentication after HTTPS is enabled.

Example:
```
Agent III C1|S13|L1P2>set https state enable
Error: this command should be executed on a device!
Agent III C1|S13|L1P2>go l1d
Agent III C1|S13|L1D>set https state enable
Agent III C1|S13|L1D>
```

Show HTTPS Configuration

Syntax: **show https config**

Description: Displays all HTTPS configurations for a device.

Example:
```
C1|S8|L1D>show https config
HTTPS configuration:
-------------------------------------------------------------------
HTTPS state:                  disable
HTTPS port:                   443
HTTPS certificate file:
HTTPS private key file:
C1|S8|L1D>
```

Start HTTPS Certificate Operation

Syntax: **start https certificate**

Description: Starts the HTTPS certificate operation for a device.

This command requires that HTTPS is enabled, the certificate type is defined, the certificate file is defined, a private key file defined, and a password defined.

Example:
```
AgentIII C1|S16|L1D>start https certificate
AgentIII C1|S16|L1D>
```

16. IP / DNS / DHCP Commands

The x222x/32xx supports IPv4- and IPv6-based application protocols. The x222x/32xx can be assigned IP address statically or dynamically using DHCP. The x222x/32xx supports DNS, which lets you assign it a hostname instead of an IP address.

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

The static IP address assignment is part of the initial 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 IPv4 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/32xx 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).

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.)

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)

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

The following commands are for IP, DNS, or DHCP operations.

Set DCHP Client State

Syntax: **set dhcp state**={enable | disable}

Description: Enables or disables the DHCP client state for a device. **Note**: the command "**set dhcp state**" is replaced by "**set ip address mode**" after ION v 1.2.0.
Enabling DHCP allows the IP address of the IONMM to be automatically selected from a list in the DHCP server. Disabling DHCP requires that the IP address, subnet mask and default gateway be set manually.

Example 1:
```
C1|S7|L1D>set dhcp state enable
C1|S7|L1D>set dhcp state disable
C1|S7|L1D>
```

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 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.

Set DNS Server

Command: **Set DNS Server(s)**

Syntax: **set dns-svr svr**=x **type**=y **addr**=z

Description: Configure a DNS Server, where:

svr = x = DNS server index number (1-6). DNS servers 1-3 are for IPv4; DNS servers 4-6 are for IPv6. See "DNS '3 vs. 3' Rule ('Up to 3' Rule)'.

type = y = ipv4 or ipv6. The IP address type; enter **ipv4** or **ipv6**

addr = z = a valid IPv4 or IPv6 address (depending on the type= parameters).

Example:

```
Agent III C1|S1|L1D>set dns-svr svr 1 type ipv4 addr 192.168.1.30
Caution: only the first three valid DNS server can be available, please refer to user
menu for the details
Agent III C1|S1|L1D>set dns-svr svr 1 type ipv6 addr 192.168.1.30
server1 to server3 is just used for ipv4!
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.1.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.1.0
IP address mode :             Static

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

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

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

Static DNS Server Configuration note: 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.

Note: When a DNS server has more than one IP address, the first IP address will be used and the other IP addresses will be ignored. So if the first IP address cannot be used, the other IP addresses will not be checked.

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

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

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

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

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

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

Set IP Type / Address / Subnet Mask

Syntax: **set ip type=** xx **addr=<**yy> **subnet–mask=**(subnet-mask|prefix)=A

Description: Defines the IP address and subnet mask of the card. The static IP address assignment is part of the initial NID setup, and at first the CLI must be used to configure the IP address settings. Thereafter, remote management and/or DHCP addressing can be configured. The defaults are IPv4 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 x323x 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 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).

where:

xx = IP type (IPv4 or IPv6). The default is IPv4.

xx = IP address of the module (IPv4 or IPv6 format).

yy = The subnet mask bit number for IPv4.

prefix = The IPv6 address prefix, in the range of 0 to 127.

Example:

```
C1|S13|L1D>set ip type=ipv4 addr=192.168.0.3 subnet-mask=255.255.255.0
C1|S13|L1D>set ip type=ipv6 addr=2001:1234::1 prefix=64
```

Set IP Address Mode

Syntax: **set ip address mode={bootp|dhcp|static}**

Description: Changes the IP addressing method to BootP, DHCP, or Static addressing,

where:

bootp = (Bootstrap Protocol) uses UDP port number 67 for the server and UDP port number 68 for the BootP client.

dhcp = (Dynamic Host Configuration Protocol) for assigning dynamic IP addresses to devices on a network; a device can have a different IP address every time it connects to the network.

static = a well-defined IP address which this device always uses and which no other computer can use (the default setting).

Example:

```
C1|S10|L1D>set ip address mode ?
  bootp
  dhcp
  static
C1|S10|L1D>set ip address mode=bootp
C1|S10|L1D>set ip address mode=dhcp
C1|S10|L1D>set ip address mode=static
```

Note: Use the **show ip-mgmt config** command to display the current IP address mode setting. **Note**: the command "**set dhcp state**" is replaced by "**set ip address mode**" after ION v 1.2.0.

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.

Set Gateway Type / IP Address

Syntax: **set gateway type**=<xx> **addr=<**yy>

Description: Defines the default gateway IP address on the module, where:

type=<xx> = Gateway type (IPv4 or IPv6)

addr=<yy> = a valid IPv4 or IPv6 address

Example:
```
Agent III C1|S1|L1D>set gateway type=ipv4 addr=192.168.0.1
Agent III C1|S1|L1D>
```

Messages: *Error: the subnet mask of gateway is different from the one of global address*

Note: Use the **show ip–mgmt config** command to display the current gateway IP address information.

Show IP Configuration

Syntax: **show ip–mgmt config**

Description: Displays the IP management configuration parameters on the IONMM or x323x NID.

Example:

```
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
-----------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.1.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.1.0
IP address mode :             Static

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

Dynamic Router Table:
Table1__Destination:          2001:1234::
Table1__PfxLen:               64
Table1__NextHop:              ::
Table1__Age:                  84315

Table2__Destination:          fe80::
Table2__PfxLen:               64
Table2__NextHop:              ::
Table2__Age:                  84315

Table3__Destination:          ff00::
Table3__PfxLen:               8
Table3__NextHop:              ::
Table3__Age:                  84315


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>
```

Set IPv6 Management State

Syntax: **set ipv6-mgmt state**={disable|enable}

Description: A device level command to turn on or turn off control within IPv6. The IPv6 Management State must be set to 'enable' in order to control IPv6 configuration (Link Local Address, Global Address Mode, Global Address, Management Prefix, Duplicate Address Detect, Gateway Mode, and Gateway Address).

Example:

```
Agent III C1|S1|L1D>set ipv6-mgmt state ?
  disable
  enable
Agent III C1|S1|L1D> set ipv6-mgmt state=enable
```

Set IPv6 Management State

Command: **Set IPv6 Mode**

Syntax: **set ipv6 address mode**=<static|dhcpv6|stateless>

Description: This device level command configures the IPv6 method to be used on the device. The default is static. If 'Stateless Auto configuration' is selected, then Route Discovery must first be enabled. The parameters are:

ipv6 = Ipv6 prefix for the interface.

method = IPv6 method, either:

dhcpv6 = DHCPv6 method is used for IPv6.

stateless = stateless method is used (not "stateful" IPv6 mode).

static = static IPv6 method is used (the default).

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 address mode stateless
Stateless Auto Configuration is based on the function of Route Discovery.
Right now, Route Discovery is disabled. Please enable it before switching to Stateless Auto
configuration.
Agent III C1|S1|L1D>set ipv6 address mode dhcpv6
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.1.10
IP subnet mask:               255.255.255.0
```

```
Gateway IP address:           192.168.1.0
IP address mode :             Static

IPv6 management configuration:
-------------------------------------------------------------------------
Management State:             enable
Link Local Address:           fe80::2c0:f2ff:fe20:de9e
Global Address Mode:          dhcpv6
Global Address:               ::
Management Prefix:            0
Duplicate Address Detect:     false
Gateway Mode:                 static
Gateway Address:              fe80::2c0:f2ff:fe21:789a

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

Set IPv6 Gateway Method

Command: **Set IPv6 Gateway Method**

Syntax: **set ipv6 gateway method**=<static|routerdisc>

Description: Device level command to configure the IPv6 gateway method to be used.

where:

static = the static method is to be used (the default).

routerdisc = the dynamic method (Route Discovery) is to be used.

Example:

```
Agent III C1|S1|L1D>set ipv6 gateway mode ?
  routerDisc
  static
Agent III C1|S1|L1D>set ipv6 gateway mode routerDisc
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
------------------------------------------------------------------------
IP management state:          enable
IP address:                   192.168.1.10
IP address:                   192.168.1.10
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>
```

17. LPT Commands

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

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

The following commands are used for link pass through operations.

Set Link Pass Through Monitoring Port

Syntax: **set lpt monitor–port=**<xx>

Description: Defines the port on this slide-in module used for LPT monitoring.

Example:
```
C1|S5|L1D>set lpt monitor-port 1
C1|S5|L1D>
```

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

Set Link Pass Through Status

Syntax: **set lpt state**={enable | disable | notSupported}

Description: Enables or disables the link pass through function on a slide-in module, or configures it as 'not supported'.

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

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

Set Selective Link Pass Through Status

Syntax: **set selective lpt state**={enable | disable}

Description: Enables or disables the selective link pass through (SLPT) feature on a slide-in module.

This feature monitors the fiber Rx port for signal loss. If the fiber Rx goes down, the copper port stops transmitting. TLPT and SLPT are operational with fiber redundancy enabled or disabled.

Example:
```
C1|S5|L1D>set transparent lpt state enable
C1|S5|L1D>set selective lpt state enable
C1|S5|L1D>
```

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

Set Transparent Link Pass Through Status

Syntax: **Set transparent lpt state**={enable | disable}

Description: Enables or disables the transparent link pass through (TLPT) feature on a slide-in module.

With OAM enabled, TLPT with automatic link restoration is available for the copper ports on the local and remote peer devices. When a copper port goes down, the information is passed to the other device and the copper port on that device 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. TLPT and SLPT are operational with fiber redundancy enabled or disabled.

Example:
```
C1|S5|L1D>set transparent lpt state enable
C1|S5|L1D>set selective lpt state enable
```

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

Show Link Pass Through Configuration

Syntax: **show lpt config**

Description: Displays the Link Pass Though (LPT) configuration for the slide-in module.

Example:
```
C1|S3|L1D>show lpt config
Link pass through configuration:
-----------------------------------------------------------------
Link pass through state:                notSupported
Transparent link pass through state:    enable
Selective link pass through state:      disable
Link pass through monitor port:         2
Remote fault detect state:              notSupported
C1|S3|L1D>
```

Set Remote Fault Detect Status

Syntax: **set rfd state**={status}

Description: Sets the remote fault detect (RFD) state on a x3x2x or a x3x3x card.
where:
status = {enable|disable|notSupported}

Example:
```
C1|S3| L1D>set rfd state=enable
C1|S3| L1D>
```

Use the **show lpt config** command to display the current Remote fault detect state setting.

Note: Some product catalog features do not match the actual features (i.e., C2220 / C322x / C323x series: support "TLPT, SLPT features"; do not support "Remote Fault Detect (RFD)".

18. LOAM (Link OAM) Commands

OAM (Operation, Administration and Maintenance) is a set of functions designed to monitor network operation to detect network faults and measure its performance. Ethernet OAM functionality allows network operators to measure quality of service (QoS) attributes such as availability, frame delay, frame delay variation (jitter and frame loss). Such measurements help identify problems before they escalate so that users are not impacted by network defects.

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

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

Note: The LOAM commands can only be entered at the port level - when the last part of the command line prompt indicates the location is a port (LxPx; where x is 1, 2 or 3).

The following commands are used for LOAM operations.

Clear LOAM Statistics

Syntax: **clear loam stats**

Description: Clears the LOAM statistics on a port and resets the LOAM counters.

Use the s**how loam statistics** command to display LOAM counters information.

Get LOAM Peer Information

Syntax: **show loam peer information**

Description: Displays the LOAM peer's configuration information.

Example:

```
C1|S5|L1D>show loam peer info
Error: this command should be executed on a port!
C1|S5|L1D>go l1p=1
C1|S5|L1P2>show loam peer info
Link OAM peer configuration:
------------------------------------------------------------------Link
OAM peer MAC address:     00-00-00-00-00-00
Link OAM peer vendor OUI:      00.00.00
Link OAM peer vendor info:     0
Link OAM peer mode:            unknown
Link OAM peer maximum PDU size:0
Link OAM peer configure revision:0
Link OAM peer function supported:unidirectionalSupport
C1|S5|L1P2>
```

Note: This command Displays the LOAM peer's Organizationally Unique Identifier (OUI) vendor information. The Vendor OUI displays in the format 00.00.00. 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.

Ignore LOAM Loopback Requests

Syntax: **set loam ignore- loopback-request**={enable |disable}

Description: Forces the NID to ignore or respond to all remote loopback requests from peers.

The default is disabled (responds to all remote loopback requests from peers), where:

enable – causes the LOAM enabled x323x NID to ignore all Loopback requests (i.e., not respond to remote loopback requests from peers).
disable – causes the LOAM enabled x323x NID to respond to all remote loopback requests from peers.

Example:
```
C1|S5|L1P2>set loam ignore-loopback-request ?
  disable
  enable
C1|S5|L1P2>set loam ignore-loopback-request disable
C1|S5|L1P2>set loam ignore-loopback-request enable
C1|S5|L1P2
```

Note: Use the **show loam ignore** command to display the NID port's current LBR response mode.

Set LOAM Admin State

Syntax: **set loam admin state**={enable | disable}

Description: Defines whether LOAM is enabled or disabled on this NID port.

Example:
```
C1|S3|L1P1>set loam admin state ?
  disable
  enable
C1|S3|L1P1>set loam admin state enable
C1|S3|L1P1>
```

Set LOAM Critical Event Notification State

Syntax: **set loam critical–evt–notif** ={enable | disable}

Description: Enables or disables whether LOAM notification is done for critical events for a device.

Set LOAM Dying Gasp Event Notification State

Syntax: **set loam dg–evt–notif**={enable | disable}

Description: Enables or disables whether LOAM notification is done for dying gasp events on a device. These are unrecoverable conditions such as loss of power.

Set LOAM Errored Frame Event Notification State

Syntax: **set loam ef–evt–notif**={enable | disable}

Description: Enables or disables whether LOAM notification is done when the number of frame errors exceed the threshold value defined for this event on a device (see Set LOAM Errored Frame Threshold Value).
Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Threshold Value

Syntax: **set loam ef threshold=**<xx>

Description: Defines the number of frame errors that must occur within the defined window before notification of this event is made on a device (see Set LOAM Errored Frame Window Value). The valid Error frame threshold range is 0 – 268435455 frame errors.

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Window Value

Syntax: **set loam ef window=**<xx>

Description: Defines the amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent for a device. The valid Error frame window range is 10 – 600 milliseconds (1 second – 1 minute).

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Period Event Notification State

Syntax: **set loam efp–evt–notif**={enable | disable}

Description: Enables or disables whether OAM notification is done for errored frame period events for a device (see Set LOAM Errored Frame Period Threshold Value).

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Period Threshold Value

Syntax: **set loam efp threshold=**<xx>

Description: Defines the number of frame period errors that must occur within the defined window before notification of this event is made for a device (see Set LOAM Errored Frame Period Window Value). The valid Error frame period threshold range is 0 – 268435455 frame period errors.

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Period Window Value

Syntax: **set loam efp window=**<xx>

Description: Defines the number of frames in which the threshold value must occur before an event notification is sent for a device. The valid Error frame period window range is 174762 – 104857560 frames.

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Seconds Summary Event Notification State

Syntax: **set loam efss–evt–notif**={enable | disable}

Description: Enables or disables whether LOAM notification is done for errored frame seconds summary events (see Set LOAM Errored Frame Seconds Summary Threshold Value).

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Seconds Summary Threshold Value

Syntax: **set loam efss threshold=**<xx>

Description: Defines the number of errored frames that must occur within in the defined window before notification of this event is made (see Set LOAM Errored Frame Seconds Summary Window Value). The valid EFSS threshold range is 0 – 268435455 errored frames.

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Frame Seconds Summary Window Value

Syntax: **set loam efss window=**<xx>

Description: Defines the amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent. The valid EFSS window range is 100 – 9000 ms (1 second – 90 seconds). Use the **show loam event config** command to display the current setting.

Set LOAM Errored Symbol Period Event Notification State

Syntax: **set loam esp–evt–notif**={enable | disable}

Description: Enables or disables whether LOAM notification is done for errored symbol period events (see Set LOAM Errored Symbol Period Threshold Value). Use the **show loam event config** command to display the current setting.

Set LOAM Errored Symbol Period Threshold Value

Syntax: **set loam esp threshold high=**<xx> **low=**<yy>

Description: Defines the number of error symbols that must occur within in the defined window before notification of this event is made (see Set LOAM Errored Frame Seconds Summary Window Value).

where:

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. The valid range is 0 – 4294967295.

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. The valid range is 0 – 4294967295.

Use the **show loam event config** command to display the current setting.

Set LOAM Errored Symbol Period Window Value

Syntax: **set loam esp window high=**<xx> **low=**<yy>

Description: Defines the threshold window in which the threshold value must occur before an event notification is sent. Use the **show loam event config** command to display the current setting.

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. The valid Error symbol period window high range is 0 – 4294967295.

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. The valid Error symbol period window low range is 125000000 – 2684354.

Set LOAM Mode

Syntax: **set loam mode**={active | passive}

Description: Defines whether discovery process is initiated by the interface or by the peer for a port.

active –the NID sends out discovery frames (LOAM Information PDUs). It can initiate OAM Loopback to its remote peer.

passive – the NID can receive and respond to discovery messages (LOAM Information PDUs). It cannot initiate LOAM a Loopback, but it can process loopback requests from a LOAM Peer in active mode.

Use the **show loam event config** command to display the current setting.

Note: To perform Link Fault management, either the local client or the remote peer (or both) must be configured for Active mode operation (**set loam mode=active**).

Show LOAM Configuration

Syntax: **show loam config**

Description: Displays the LOAM configuration of a port.

Example 1:

```
C1|S1|L1P2>show loam config
Cannot get link OAM configuration on this port!
C1|S1|L1P2>go c=1 s=3 l1p=1
C1|S3|L1P1>show loam config
Link OAM configuration:
------------------------------------------------------------------
Link OAM admin state:         enable
Link OAM operation status:linkFault
Link OAM mode:                active
Link OAM maximum PDU size:     1500
Link OAM configuration revision:1
Link OAM function supported:  loopbackSupport+eventSupport
C1|S3|L1P1>go l1p=2
C1|S3|L1P2>show loam config
Link OAM configuration:
------------------------------------------------------------------
Link OAM admin state:         enable
Link OAM operation status:linkFault
Link OAM mode:                active
Link OAM maximum PDU size:     1500
Link OAM configuration revision:0
Link OAM function supported:  loopbackSupport+eventSupport
C1|S3|L1P2>
```

Show LOAM Event Configuration

Syntax: **show loam event config**

Description: Displays the LOAM event configuration of a port.

Example:

```
C1|S5|L1P1>show loam event config
LOAM event configuration:
-----------------------------------------------------------------
Error symbol period event notify:       enable
Error frame period event notify:        enable
Error frame event notify:               enable
Error frame seconds event notify:       enable
Dying gasp event notify:                enable
Critical event notify:                  enable
Error symbol period window high:        0
Error symbol period window low:         125000000
Error symbol period threshold high:     0
Error symbol period threshold low:      1
Error frame period window:              1747626
Error frame period threshold:           1
Error frame window:                     10
Error frame threshold:                  1
Error frame seconds summary window:     100
Error frame seconds summary threshold:  1
```

Show LOAM Event Log

Syntax: **show loam event log**

Description: Displays the LOAM event logs of a port (Time stamp, OUI, Type, Location, Window Hi, Window Lo, Threshold Hi, Threshold Lo, Value, Running Total, and Event Total).

Example:

```
C1|S5|L1P2>show loam event log
timestamp     OUI       type          location  W-hi     W-lo     T-hi          T-lo     value    R-total   E-total
-------------------------------------------------------------------------------------------------------------------
00:24:19      01:80:c2  linkFault     local     -        -        -             -        -        1         1
00:24:19      01:80:c2  critical      local     -        -        -             -        -        1         1
C1|S5|L1P2>go l1p=1
C1|S5|L1P1>show loam event log
timestamp     OUI       type          location  W-hi     W-lo     T-hi          T-lo     value    R-total   E-total
-------------------------------------------------------------------------------------------------------------------
00:24:19      01:80:c2  linkFault     local     -        -        -             -        -        1         1
00:24:19      01:80:c2  critical      local     -        -        -             -        -        1         1
00:24:27      01:80:c2  linkFault     local     -        -        -             -        -        1         1
00:24:27      01:80:c2  critical      local     -        -        -             -        -        1         1
C1|S5|L1P1>
```

Show LOAM Peer Configuration

Syntax: **show loam peer info**

Description: Displays the LOAM peer configuration of a port.

Example:

```
C1|S5|L1P2>show loam peer info
Link OAM peer configuration:
------------------------------------------------------------------
Link OAM peer MAC address:    00-00-00-00-00-00
Link OAM peer vendor OUI:     00.00.00
Link OAM peer vendor info:    0
Link OAM peer mode:           unknown
Link OAM peer maximum PDU size:0
Link OAM peer configure revision:0
Link OAM peer function supported:unidirectionalSupport
C1|S5|L1P2>
```

Show LOAM Statistics

Syntax: **show loam statistics**

Description: Displays the LOAM statistics of a port.

Example:

```
C1|S16|L1P1>show loam statistics
Link OAM counters:
------------------------------------------------------------------
No. of information link OAM PDUs transmitted:         1223
No. of information link OAM PDUs received:            1232
No. of unique Event link OAM PDUs transmitted:        222
No. of unique Event link OAM PDUs received:           2333
No. of duplicate Event link OAM PDUs transmitted:     2121
No. of duplicate Event link OAM PDUs received:        2322
No. of Loopback control link OAM PDUs transmitted:    2114
No. of Loopback control link OAM PDUs received:       494
No. of Variable requests link OAM PDUs transmitted:   2323
No. of Variable requests link OAM PDUs received:      232
No. of Variable response link OAM PDUs transmitted:   644
No. of Variable response link OAM PDUs received:      233
No. of Org. specific link OAM PDUs transmitted:       32545
No. of Org. specific link OAM PDUs received:          117
No. of Unsupported Codes link OAM PDUs transmitted    34
No. of Unsupported Codes link OAM PDUs received:      3445
No. of frames dropped due to link OAM:                123
C1|S16|L1P1>
```

Show LOAM Ignore Loopback Requests State

Syntax: **show loam ignore-loopback-request**

Description: Displays the NID port's current LBR response mode (either ignore or respond to all remote loopback requests from peers).

Example:
```
C1|S5|L1P2>set loam ignore-loopback-request=disable
C1|S5|L1P2>show loam ignore-loopback-request
Link OAM Ignore loopback request:                    disable
C1|S5|L1P2>
```

19. MAC Learning Portlist Commands

MAC Learning Port List Enable / Disable

Syntax: **set mac enable portlist**=x <cr>

Description: Enables or disables the ability to 'learn' MAC addresses on one or more ports, typically for security purposes. With 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.

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.

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.

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).

Example:

```
C1|S3|L1D>show port mac_learning state
Port Mac learning:
Port1:                              disable
Port2:                              disable
C1|S3|L1D>set mac enable portlist 1,2
C1|S3|L1D>show port mac_learning state
Port Mac learning:
Port1:                              enable
Port2:                              enable
C1|S3|L1D>set mac enable portlist ?
  STR_MAC_LEARNING_PORT_LIST
C1|S3|L1D>set mac enable portlist 0
C1|S3|L1D>show port mac_learning state
Port Mac learning:
Port1:                              disable
Port2:                              disable
```

Show Port MAC Learning State

Syntax: **show mac learning port list**<cr>

Description: Displays the current port MAC learning status (port 1, port 2, and/or port 3 enabled or disabled).

Example1:

```
C0|S9|L1D/>show port mac_learning state
Port Mac learning:
Port1:                              enable
Port2:                              disable
Port3:                              enable
C0|S9|L1D/>
```

Example 2:

```
C1|S18|L1D>show port mac_learning state
Port Mac learning:
Port1:                              disable
Port2:                              enable
C1|S18|L1D>
```

20. Performance / RMON Statistics

Remote Network Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs and interconnecting T-1/E-1 and T-3/E-3 lines from a central site. RMON specifically defines the information that any network monitoring system will be able to provide. RMON is specified as part of the MIB as an extension of the SNMP.

Note: this command can only be entered for a port, not a device.

Show RMON Statistics

Syntax: **show rmon statistics**

Description: Displays the Remote Network Monitoring (RMON) statistics for a port.

Sample Syntax:

```
RMON statistics:
----------------------------------------------------------------
Rx octets:                              pp
Rx packets:                             qq
Rx broadcast packets:                   rr
Rx multicast packets:                   ss
Rx CRC align errors:                    tt
Rx undersize packets:                   uu
Rx oversize packets:                    vv
Rx fragments:                           ww
Rx jabbers:                             xx
Rx collisions:                          yy
Rx 64 octets packets:                   zz
Rx 65-127 octets packets:               zz
Rx 128-255 octets packets:              zz
Rx 256-511 octets packets:              zz
Rx 512-1023 octets packets:             zz
Rx 1024-1518 octets packets:            zz
```

where:

pp = Number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.

qq = Number of packets received on the interface, including bad packets, multicast and broadcast packets, since the device was last refreshed.

rr = Number of good broadcast packets received on the interface since the device was last refreshed. This number does not include multicast packets.

ss = Number of good Multicast packets received on the interface since the device was last refreshed.

tt = Number of CRC and Align errors that have occurred on the interface since the device was last refreshed.

uu = Number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.

vv = Number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.

ww = Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.

xx = Number of packets received that were more than 1,518 octets long and had a FCS during the sampling session.

yy = Number of collisions received on the interface since the device was last refreshed.

zz = Number of xx-byte frames received on the interface since the device was last refreshed.

Example:

```
C1|S7|L1P1>show rmon statistics
RMON statistics:
-----------------------------------------------------------------
Rx octets:                              44190203
Rx packets:                             98764
Rx broadcast packets:                   11929
Rx multicast packets:                   4
Rx CRC align errors:                    0
Rx undersize packets:                   0
Rx oversize packets:                    0
Rx fragments:                           7
Rx jabbers:                             0
Rx collisions:                          0
Rx 64 octets packets:                   13745
Rx 65-127 octets packets:               11208
Rx 128-255 octets packets:              2169
Rx 256-511 octets packets:              1628
Rx 512-1023 octets packets:             68673
Rx 1024-1518 octets packets:            1340
C1|S7|L1P1>
```

21. QoS Commands

In QoS (Quality of Service) the bandwidth, error rates and latency can be monitored, sampled and possibly improved. QoS also delivers the set of 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. It 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) will be forwarded first.

These commands let you set QOS Priority either 1) by-dst-mac, 2) by-src-mac, 3) by-vlan-id, 4) ieee-tag, 5) ip-tag, or 6) tag-type.

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).

The following commands are used for QoS operations.

Set QoS Default Priority for a Port

Syntax: **set qos default–priority=**<xx>

Description: Defines the default priority (0–7) of a port (where 0 is the lowest priority).

Example:
```
C1|S3|L1P2>set qos default-priority 4
C1|S3|L1P2>
```

Set Frame Priority: Destination MAC Address is Used

Syntax: **set qos priority by–dst–mac**={enable | disable}

Description: Defines whether the destination MAC address is used to decide frame priority.

Example:
```
C1|S3|L1P2>set qos priority by-dst-mac=enable
C1|S3|L1P2>
```

Set Frame Priority: IEEE Tag is Used

Syntax: **set qos priority ieee–tag**={enable | disable}

Description: Defines whether the IEEE tag is used to decide frame priority of a port.

Example:
```
C1|S3|L1P2>set qos priority ieee-tag=enable
C1|S3|L1P2>
```

Set Frame Priority: IP Tag is Used

Syntax: **set qos priority ip–tag**={enable | disable}

Description: Defines whether the IP tag is used to decide the frame priority of a port.

Example:
```
C1|S3|L1P2>set qos priority ip-tag=enable
C1|S3|L1P2>
```

Set Frame Priority: Source MAC Address is Used

Syntax: **set qos priority by–src–mac**={enable | disable}

Description: Defines whether the source MAC address is used to decide frame priority of a port.

Example:
```
C1|S3|L1P2>set qos priority by-src-mac=enable
C1|S3|L1P2>
```

Set Frame Priority: VLAN ID is Used

Syntax: **set qos priority by–vlan–id**={enable | disable}

Description: Defines whether the VLAN ID (VID) is used to decide frame priority of a port.

Example:
```
C1|S3|L1P2>set qos priority by-vlan-id=enable
C1|S3|L1P2>
```

Set IEEE Priority Remapping

Syntax: **set dot1dbridge ieee-tag-priority=**<xx> **remap-priority=**<yy>

Description: Defines the priority remapping for IEEE.

where:

xx = index number, 0 – 7

yy = priority to remap to, 0 – 3

Example:
```
C1|S3|L1P2>set dot1dbridge ieee-tag-priority=3 remap-priority=2
Error: this command should be executed on a device!
C1|S3|L1P2>go l1d
C1|S3|L1D>set dot1dbridge ieee-tag-priority=3 remap-priority=2
C1|S3|L1D>
```

Set Ingress Priority Remapping

Syntax: **set qos ingress–priority=**<xx>**remap-priority=**<yy>

Description: Defines a port's priority remapping for traffic that originates outside of the network.

where:

xx = index number, 0 – 7

yy = priority to remap to, 0 – 7

Example:
```
C1|S3|L1P2>set qos ingress-priority=4 remap-priority=4
C1|S3|L1P2>
```

Set IP Traffic Class Priority Remapping

Syntax: **set dot1dbridge ip-priority-index=**<xx> **remap-priority=**<y>

Description: Defines a device's priority remapping for IP traffic.

where:

xx = index number, 0 – 63

y = priority to remap to, 0 – 3

Example:
```
C1|S3|L1D>set dot1dbridge ip-priority-index 3 remap-priority 3
C1|S3|L1D>
```

Set Priority Type

Syntax: **set qos priority tag–type**={useIEEE | useIP}

Description: Defines which tag type (IEEE or IP) will be used to decide frame priority type for a port if both tags are available. Both IEEE and IP cannot be configured at the same time.

Example:
```
C1|S3|L1P1>set qos priority tag-type useIEEE
C1|S3|L1P1>set qos priority tag-type useIP
C1|S3|L1P1>
```

Use the **show qos config** command to display the current Tag type for priority if both tag types are available.

Set Port Egress Queuing Method

Syntax: **set port egress queuingmethod**=<wrr|sp>

Description: A port-level command used to set the Egress Queue Mode to either "Weighted Round Robin" or "Strict" queuing method,

where:

wrr = Weighted Round Robin egress port queuing

sp = Strict egress port queuing

Example:

```
AgentIII C1|S8|L1P2>set port egress queuingmethod ?
  sp
  wrr
AgentIII C1|S8|L1P2>set port egress queuingmethod sp
AgentIII C1|S8|L1P2>set port egress queuingmethod wrr
AgentIII C1|S8|L1P2>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
Port Egress Queuing mehod:                  wrr
AgentIII C1|S8|L1P2>
```

WRR (Weighted Round Robin) is a scheduling discipline wherin 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, when enabled, allows only high priority packages to be passed and all low priority packages will be dropped during a network jam condition. 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. 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.

Show Priority Remapping

Syntax: **show qos priority remapping**

Description: Displays the IEEE priority remapping on a port.

Example:
```
C1|S13|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
```

Show QoS Configuration of a Port

Syntax: **show qos config**

Description: Displays the QoS configuration of the port indicated in the command prompt.

Example:
```
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>
```

22. RADIUS Commands

These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

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.

Note: After configuring the x323x for RADIUS, your HyperTerminal session ends, and you will be required to enter the RADIUS defined username and password when connecting to the IONMM.

The following commands are used for RADIUS operations.

Set RADIUS Authentication

Syntax: **set radius client state**={enable | disable}

Description: Enables or disables the RADIUS authentication feature. To determine the current state, use the **show radius config** command.

Note: After configuring the NID for RADIUS, you must enter the RADIUS defined username and password when connecting to the IONMM.

Example:

```
C1|S3|L1D>set radius client state=disable
login: ION
Password: Xxxxxxx

C1|S3|L1D>show radius config
RADIUS client state:          disable
```

Set RADIUS Retry

Syntax: **set radius svr=<**xx> **retry=<**yy>

Description: Defines the number of times the access request will be re-sent to the specified server before being discarded or re-directed to another server, where:

svr = The RADIUS server number (1–6).

retry = The number (0–5) of retry attempts allowed. Factory default is 3.

Example:
```
Agent III C1|S1|L1D>set radius svr=1 retry=3
Agent III C1|S1|L1D>
```

Set RADIUS Server, Type, and Address

Command: **Set RADIUS Server, Type, and Address**

Syntax: **set radius svr**=<1-6> **type**=(ipv4 |dns|ipv6) **addr**=ADDR [**retry**=<1-5>] [**timeout**=<1-60>]

Description: Define one or more RADIUS servers in terms of Index number, Address type, Address, Retries and Timeouts, where:

svr = server number (1–6)

type= server IP address format; valid choices are:

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

addr = RADIUS server IP address

retry = optional; number (0–5) of times the access request will be re-sent to the server before being discarded or re-directed to another server. Factory default is 3.

timeout = optional; number (0–60) of seconds to wait for a response from the server before re-sending the request. Factory default is 30.

Example:
```
Agent III C1|S1|L1D>set radius svr 1 type ipv6 addr fe80::2c0:f2ff:fe20:de9e
Agent III C1|S1|L1D>show radius config
RADIUS client state:          disable

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

Set RADIUS Server Secret

Syntax: **set radius svr=<**xx> **secret=<**yy>

Description: Defines the server secret for a RADIUS server.

where:

xx = RADIUS server number (1–6)

yy = alphanumeric text string used to validate communications between two RADIUS devices. Maximum length of the secret is 128 characters.

Example:
```
C1|S3|L1D>set radius svr=1 secret=Zxytf12a
C1|S3|L1D>
```

Set RADIUS Timeout

Syntax: **set radius svr=<**xx> **timeout=<**yy>

Description: Defines the number of seconds to wait for a response from the Radius server before re-sending the request.

where:

xx = server number (1–6)

xx = number (0–60) of seconds

Example:
```
C1|S3|L1D>set radius svr=1 secret=Zxytf12a
C1|S3|L1D>
```

Show RADIUS Configuration

Command: **Show Current RADIUS Configuration**

Syntax: **show radius config**

Description: Display the existing RADIUS parameters (Client State, and Server Index #, Address Type, Address, number of Retries, and number of Timeouts configured).

Example:

```
Agent III C1|S1|L1D>show radius config
RADIUS client state:          disable

RADIUS authentication server:
index addr-type addr                                                    retry timeout
------------------------------------------------------------------------------------
1     dns       0.0.0.0                                                 3     30
2     dns       0.0.0.0                                                 3     30
3     dns       0.0.0.0                                                 3     30
4     dns       0.0.0.0                                                 3     30
5     dns       0.0.0.0                                                 3     30
6     dns       0.0.0.0                                                 3     30
Agent III C1|S1|L1D>
```

Messages: *Fail to pass the radius authentication!*

23. Redundancy Commands (Fiber Port)

The Fiber Port 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 Port 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. Traffic rerouting occurs within a minimum period after the Primary Port is declared in the fault state. Traffic flow is restored within a minimum set period after a fault occurs.

Restrictions:

1. SOAM is only supported on Port 3 of the x3231 NID regarding redundancy. The x3231 does not function as a 3-port switch regarding SOAM, but rather allows for fiber redundancy, including SOAM. SOAM views Port 3 as a redundant port, so a SOAM MEP or MIP cannot be created on Port 3. This restriction applies whether the "Redundancy" feature is enabled or disabled.

Fiber Redundancy can coexist with all other features. All operating modes are supported.

Set Redundancy State

Syntax: **set redundancy state**=(enable|disable)

Description: Sets the redundancy (automatic protection switching) mode for the fiber port. This card must have at least two fiber ports to do redundancy (e.g., x3231 NID).

Example:

```
C1|S3|L1D>set redundancy state ?
  disable
  enable
C1|S3|L1D>set redundancy state=enable
Redundancy is not supported on this card!
C1|S3|L1D>go l1p=1
C1|S3|L1P1>set redundancy state=enable
Error: this command should be executed on a device!
C1|S3|L1P1>go c=1 s=5 l1d
C1|S5|L1D>set redundancy state=enable
C1|S5|L1D>
```

Show Redundancy Information

Syntax: **show redundancy info**

Description: Displays port redundancy information of a card's fiber ports. This card must have at least two fiber ports to do redundancy (e.g., a model x3231). 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.

Example 1:

```
C1|S13|L1D>show redundancy info
Redundancy information:
---------------------------------------------------------------
Port redundancy state:                  disable
Primary port:                           2
Secondary port:                         3
Active port:                            N/A
```

Example 2:

```
C1|S3|L1P1>show redundancy info
Error: this command should be executed on a device!
C1|S3|L1P1>go l1d
C1|S3|L1D>show redundancy info
Redundancy is not supported on this card!
C1|S3|L1D>go c=1 s=8 l1d
C1|S8|L1D>show redundancy info
Redundancy information:
-----------------------------------------------------------
Port redundancy state:                  disable
Primary port:                           2
Secondary port:                         3
Active port:                            2
C1|S8|L1D>
C1|S8|L1D>set redundancy state ?
  disable
  enable
C1|S8|L1D>set redundancy state=enable
C1|S8|L1D>show redundancy info
Redundancy information:
-----------------------------------------------------------Port redun-
dancy state:                  enable
Primary port:                           2
Secondary port:                         3
Active port:                            2
C1|S8|L1D>
```

24. Serial Protocol (X/Y/Zmodem) Commands

Use the **serial (get / put / upgrade) protocol** commands to transfer a file over a serial line **(xmodem / xmodem-1k / ymodem / zmodem)**. These commands can only be entered at the device level (e.g., when the command line prompt is C1|S8|L1D> or similar). These commands function like 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

You can use HyperTerminal to send and receive text and data files to a remote computer. The status of the transfer is displayed in the HyperTerminal window during the transfer. The remote computer you are connected to must be using the same transfer protocol as your computer when sending or receiving files (xmodem, xmodem-1k, ymodem, or zmodem). File transfer information is usually provided once you sign into the remote system or is sent via an email from an administrator running the remote system. You can have just one connection open for each HyperTerminal session. However,; you can start multiple HyperTerminal sessions, opening a new connection for each session, as long as each connection uses a different communication (COM) port.

Serial Get Protocol

Syntax: **serial get protocol**={xmodem|xmodem-1k|ymodem|zmodem}

Meaning: Sends a request to servers / local file system to download content for a subsequent ***put*** command.

Example:

```
C1|S1|L1D>serial ?
  get
  put
  upgrade
C1|S1|L1D>serial get protocol ?
  xmodem
  xmodem-1k
  ymodem
  zmodem
C1|S1|L1D>serial get protocol zmodem file xxxx

Warning: the input file name will be ignored when using ymodem/zmodem to re-
trieve file!
now start to transfer the file  ...
ŠCCCCCCCCCCCBB0BB0BB0BB0BB0BB0BB0BB0BB0B
BB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>
```

Serial Put Protocol

Syntax: **serial put protocol=xxx**

Meaning: Sends a request to servers / local file system to upload content.

Example:
```
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!
```

Serial Upgrade Protocol

Syntax: **serial upgrade protocol**=xxx

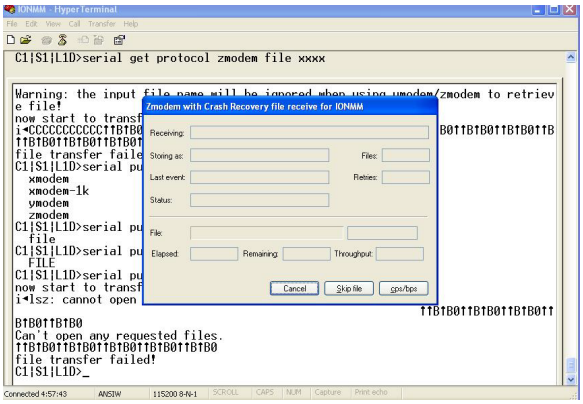
Meaning: Performs a firmware upgrade over the selected serial line.

Example:
```
C1|S1|L1D>serial upgrade protocol ?
  xmodem
  xmodem-1k
  ymodem
  zmodem
C1|S1|L1D>serial upgrade protocol zmodem file xxxx
now start to transfer the file  ...

**B000000063f694ceive.**B000000063f694

CCCCCCCCCCCBB0BBBB0BBBB0BBBB0BB0BB0BB0BB0
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.

Message: Zmodem with Crash Recovery file receive for IONMM
Zmodem with Crash Recovery dialog fields:

Receiving:
Storing as:
Files:
Last event: Connection timed out
Retries:
Status: Connection timed out
File:
Elapsed:
Remaining:
Throughput:



Cancel button:
Skip File button:
cps/bps button: characters per second / bits per second.

ZMODEM timing is receiver driven. The transmitter should not time out at all, except to abort the program if no headers are received for an extended period (e.g., one minute). Accurate crash recovery requires that the receiver's copy of the file match the sender's copy up to the point where the transfer was cut off. If you don't call back instantly the file may change, and simply resuming the transfer will corrupt the file. If this is a concern, choose a program that verifies the accuracy of Crash Recovery.

The X-Y-ZMODEM group of protocols allows you to transfer any kind of data on a disk drive. There are several technical differences between the protocols in this group, but the only thing you really need to be concerned about is to select them in reverse alphabetical order. If the system you are connecting with will allow you to use ZMODEM, then use it. If ZMODEM isn't available, use one of the YMODEM protocols. If XMODEM is the only protocol available, use XMODEM. If other protocols are available, it is still usually best to use one of the X-Y-Z protocols.

With HTPE, for Zmodem downloads, start the download on the host and HTPE will start to receive. For downloads with other protocols, start the download on the host and then tell HTPE which file transfer protocol to use to receive. For HTPE uploads, you must tell the host to start to receive and which file transfer protocol to use, then tell HTPE what file to send using which protocol. Any of these file protocols will timeout if one side starts and doesn't get an acknowledgment from the other side after a certain period.

25. SFTP Commands

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

Show SFTP Configuration

Syntax: **show sftp config**
Description: Show the SFTP configuration
Example:

```
Agent III C1|S3|L1D>show sftp config

SFTP configuration:
------------------------------------------------------------------------
SFTP state:                    Disabled
Server port:                   22
SFTP User :                    sftpuser1
Server Path :                  /C:/user/ionbackup
SFTP password:                 ******
```

Get Current SFTP Address

Syntax: **prov get sftp server addr**
Description: Show the current SFTP server address
Example:

```
Agent III C1|S16|L1D>prov set sftp server type=ipv4 addr=192.168.101.6
Agent III C1|S16|L1D>prov get sftp server addr
sftp server address: 192.168.101.6
Agent III C1|S16|L1D>
```

Set SFTP Server Address

Syntax: **prov set sftp server type=**(ipv4|ipv6|dns) **addr=**ADDR
Description: Set the SFTP server address where:
type = the type of IP addressing
addr = the SFTP server's IP address
Example:

```
Agent III C1|S1|L1D>prov set sftp svr type ipv4 addr 192.168.1.30
Agent III C1|S1|L1D>
```

Set SFTP Username

Syntax: **set sftp username=**USERNAME
Description: Set the SFTP username
Example:

```
Agent III C1|S3|L1D>set sftp username sftpuser1
SFTP username has been set to sftpuser1.
```

Set SFTP Password

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

Example:

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

Please input password again:

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

Set SFTP State

Syntax: **set sftp state=**(enable|disable)
Description: Enable or disable SFTP state
Example:

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

Set Custom SFTP Port

Syntax: **set sftp port=<1-65535>**
Description: Set a custom SFTP port. The default is port 22.
Example:

```
Agent III C1|S3|L1D>set sftp port 4000
SFTP port has been set to 4000.
Agent III C1|S3|L1D>show sftp config
SFTP configuration:
------------------------------------------------------------------------
SFTP state:                    Enabled
Server port:                   4000
SFTP User :                    sftpuser1
Server Path :
SFTP password:                 ******
```

Set SFTP Server Path

Syntax: **prov set sftp server type=**(ipv4|ipv6|dns) **addr=**ADDR

Description: Specify the path on the SFTP server where files come from or go to.
Make sure that the configured directory/folder has required permissions (read and write) on the SFTP server. If no path is configured, the user's home directory will be used as the target for SFTP transfers.

Example 1:

To set or reset the server path to the user's home directory.

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

Example 2:

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

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

Example 3:

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

```
Agent III C1|S3|L1D>set sftp serverpath /C:/user/ionbackup
SFTP server path has been set to /C:/user/ionbackup.
```

Example 4:

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

```
Agent III C1|S3|L1D>set sftp serverpath ion/backup
SFTP server path has been set to ion/backup.
```

Download File from SFTP Server

Syntax: **sftp get remotefile=**<filename>
Description: Download remote file from SFTP server.
Example:

```
Agent III C1|S3|L1D>sftp get remotefile IONMM-1.5.17_AP.bin
SFTP transferring...

File transferred successfully!
Agent III C1|S3|L1D>
```

Upgrade the IONMM Firmware via SFTP

Syntax: **sftp upgrade remotefile=**<filename>
Description: Download and install IONMM firmware file.

Example:

```
Agent III C1|S3|L1D>sftp upgrade remotefile IONMM-1.5.17_AP.bin

Processing...

SFTP upgrade succeeded!
```

26. SNMP Commands

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

No Space or Tab 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" character.

If you enter a "tab" and "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. You must then re-enter the command or field without the "tab" or "space" characters.

SNMP / 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 cannot 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.

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

Each of these SNMP commands is described below.

Add SNMP Community

Syntax: **add snmp community name=**STR_COMM_NAME **access_mode=**(read_only|read_write)

Description: Device-level command to create (add) a new unique SNMP v3 community name and assign it an access level (read only or read/write). The **snmp community name** cannot include "space" characters. This command is available to Write users and Admin users.

where:

name = the SNMP community name, up to 32 characters (no spaces).

access_mode = the SNMP community access mode (either 'read_only' or 'read_write').

Example:

```
C1|S1|L1D>add snmp community name=remcorp access_mode=read_only
C1|S1|L1D>
```

Add SNMP Group

Syntax: **add snmp group name=**STR_SNMP_GRP **security-model=**(any|v1|v2c|v3) **security-level=**(noAuthNoPriv|authNoPriv|authPriv) [**readview** = STR_READ_VIEW] [**writeview** = STR_WRITE_VIEW] [**notifyview** = STR_NOTIF_VIEW]

Description: Device-level command to create (add) a new unique SNMP v3 Group. The security-model can be any, v1, v2c, or v3. The **snmp group name** cannot include "space" characters. This command is used to add a new SNMP group. Three mandatory parameters (name, security-model, security-level) must be given. To make the group work, at least one view (readview, writeview, notifyview) must be specified. You cannot add a new group whose name and security level are the same as an existing group. This command is available to Write users and Admin users.

where:

name: SNMP group name, its length should be shorter than 32;
security-model = the group's access right (v1, v2c, or v3).
security-level = the minimum level of security level (noAuthNoPriv, authNoPriv, or authPriv).
readview = the MIB view that authorize the group's read access (optional).
writeview = the MIB view that authorize the group's write access (optional).
notifyview = the MIB view that authorize the group's notify access (optional).

Example:

```
C1|S1|L1D>add snmp group name=rem-corp security-model=any security-level=noAuthNoPriv
C1|S1|L1D>
```

Add SNMP Local User

Syntax: **add snmp local user name=**STR_USR_NAME **security-level=**(no-AuthNoPriv|authNoPriv|authPriv) **[auth-protocol=**(md5|sha) **password=**STR_AUTH_PASS**] [priv-protocol=**(des|aes) **password=**STR_PRIV_PASS**] [group=**STR_GRP_NAME**]**

Description: Device-level command to Device-level command to create (add) a unique new SNMP v3 local user. The SNMP user's security model can only be v3. The **snmp local user name** and **password** string cannot include "space" characters. This command is available to all Write users and Admin users.
This command is used to add a new SNMP local user. Three mandatory parameters (name, group, security-level) must be given. If security-level is authNoPriv, you must also specify auth-protocol type and password. If security-level is authPriv, you must specify auth-protocol type and password, and priv-protocol type and password.
where:
name = the SNMP user name (less than 32 characters).
security-level = the minimum level of security (noAuthNoPriv, authNoPriv, or authPriv).
auth-protocol = optional, the type of authentication protocol which is used;
password = the authentication protocol password (optional).
priv-protocol = the type of privacy protocol to be used (optional).
password = the privacy protocol password (optional).

Example:

```
C1|S1|L1D>add snmp local user name=Fitz group=remcorp security-level=authPriv
auth-protocol=md5 password=abcd1234 priv-protocol=aes password=abcd1234
C1|S1|L1D>
```

Add SNMP Remote Engine

Syntax: **add snmp remote engine addrtype**=ipv4|ipv6 **addr**=STR_SVR_ADDR **port**=<1-65535> **engine_id**= STR_ENGINE_NAME

Description: Device-level command to add and define a new SNMP v3 remote engine in the configuration. This command is available to users with Write or Admin user privileges.

where:

addrtype = the IP addressing type to use (IPv4 or IPv6).
addr = an IP address for the remote engine to be added.
port = the port number of the remote trap host that will receives traps <1-65535>.
engine_id = the remote engine ID to be added.

Example:

```
Agent III C1|S1|L1D>add snmp remote engine addrtype ipv6 addr
fe80::2c0:f2ff:fe20:de9e port 55 engine_id 800003640300C0F2208DCE
Agent III C1|S1|L1D>
```

Messages: *This engineID already exists!*

Add SNMP Remote User by IP Address / Port

Syntax: **add snmp remote user name=**STR_USR_NAME **addrtype=**ipv4 **addr=**STR_SVR_ADDR **port=**<1-65535> **security-level=**(noAuthNoPriv|authNoPriv|authPriv) [**auth-protocol=**(md5|sha) **password=**STR_AUTH_PASS] [**priv-protocol=**(des|aes) **password=**STR_PRIV_PASS]

Description: Device-level command to create (add) a new unique SNMP v3 remote user. The SNMP user's security model can only be v3. The **snmp remote user name** and **password** string cannot include "space" characters. This command is available to users with Write or Admin user privileges. This command adds a new SNMP remote user by IP address and port number. Four mandatory parameters (user name, IP addr, port #, and security-level) must be given. If the security level is authNoPriv, you must also specify auth-protocol type and password. If the security-level is authPriv, you must specify the auth-protocol type and password, and the priv-protocol type and password.

where:

name = SNMP user name, up to 32 characters long.
addrtype = type of remote trap host address (ipv4).
addr = remote trap host address (e.g., 192.168.0.111).
port = remote trap host port that will receive traps (e.g., port # 162).
security-level = the minimum level of security (noAuthNoPriv, authNoPriv, or authPriv).
auth-protocol = an optional type of authentication protocol to be used (MD5 or SHA).
password = an optional authentication protocol password.
priv-protocol = an optional type of privacy protocol to be used (DES or AES).
password = an optional privacy protocol password.

Example:

```
C1|S1|L1D>add snmp remote user name=JeffS addrtype=ipv4 addr=192.168.1.80 port=162 security-
level=authPriv auth-protocol=md5 password=abcd1234 priv-protocol=aes password=abcd1234
Remote engine address is not valid!
C1|S1|L1D>add snmp remote user name rmtusr1 addrtype ipv4 addr 192.168.0.111 port 162
security-level authNoPriv auth-protocol md5 password 1222223333
C1|S1|L1D>
```

Add SNMP Remote User by Engine

Syntax: **add snmp remote user name=**STR_USR_NAME **engine=**STR_ENGINES **security-level=**(noAuthNoPriv|authNoPriv|authPriv) [**auth-protocol=**(md5|sha) **password=**STR_AUTH_PASS] [**priv-protocol=**(des|aes) **password=**STR_PRIV_PASS]

Description: Device-level command to create (add) a new SNMP v3 remote user. The SNMP user's security model can only be v3. The **snmp remote user name** and **password** string cannot include "space" characters. This command is available to users with Write or Admin user privileges.
This command adds a new SNMP remote user by remote engine ID. Three mandatory parameters (name, engine, and security-level) must be given. If security-level is authNoPriv, you must also specify auth-protocol type and password. If security-level is authPriv, you must specify auth-protocol type and password, and priv-protocol type and password.

where:

name = the SNMP user name of up to 32 characters.
engine = SNMP remote engine to which this remote user belongs (9-64 characters).
security-level = the minimum level of security (noAuthNoPriv, authNoPriv, authPriv).
auth-protocol = optional, the type of authentication protocol to be used.
password = optional, the authentication protocol password.
priv-protocol = an optional type of privacy protocol to be used, either DES or AES.
password = an optional privacy protocol password.

Example:

```
C1|S1|L1D>add snmp remote user name=JeffS engine=800003640300C0F2208DCE security-
level=authPriv auth-protocol=md5 password=abcd1234 priv-protocol=aes password=abcd1234
C1|S1|L1D>
```

Add SNMP Traphost

Syntax: **add snmp traphost version=**(v1|v2c|v3) **type=**ipv4|ipv6 **addr=**STR_SVR_ADDR **port=**<1-65535> **(community|security_name)=**STR_CS_NAME **security_level=**(noAuthNoPriv|authNoPriv|authPriv) [**notify=**TRAP_TYPE] [**timeout=**<0-2147483647>] [**retry=**<0-255>]

Description: Device-level command to add and define a new SNMP trap host to the set of trap hosts configured. Up to 6 trap hosts can be created. The SNMP community/security name length must be less than 32 alphanumeric characters. The “notify”, timeout”, and “retry” parameters are optional. The **community|security_name** string cannot include "space" characters. This command is available to users with Write or Admin user privileges.

This command is used to add a new SNMP traphost. Six mandatory parameters (version, type, addr, port, community, and security-level) must be specified.

When the SNMP version is v3, the notify type can be “inform”, and you can set “timeout” and “retry” values.

where:

version = the SNMP version of the new trap server (v1, v2c, or v3).

type = the IP address type to be used (IPv4 or IPv6).

addr = the IP address of the trap server being added.

port = the port number for the remote trap host that receive traps <1-65535>.

community|security_name = community name for v1 and v2c; security name for v3.

security-level = the minimum level of security (noAuthNoPriv, authNoPriv, authPriv).

notify = the type of notification - either ‘trap’ or ‘inform’ (optional).

timeout = optional timeout value <0-2147483647 ms> used when notify=inform.

retry = an optional retry value used when notify=inform.

Example:

```
C1|S1|L1D>add snmp traphost version=v3 type=ipv4 addr=192.168.1.30 port=162 community=xxxxx
security_level=authPriv notify=trap timeout=123456789 retry=100
The specified trap host has existed!
C1|S1|L1D>add snmp traphost version=v3 type=ipv4 addr=192.168.1.90 port=162 community=xxxxx
security_level=authPriv notify=trap timeout=123456789 retry=100
C1|S1|L1D>
```

Add SNMP View

Syntax: **add snmp view name**=STR_SNMP_VIEW **oid**=STR_VIEW_OID **type**=(include|exclude)

Description: Device-level command to create (add) a new unique SNMP v3 View. The **snmp view name** string cannot include "space" characters. Add a new SNMP view by specifying its name, OID and type. You cannot add a default view or a view whose name and OID equal to an existing view. This command is available to users with Write or Admin user privileges.

where:

name = SNMP view name, its length should be shorter than 32 character with no spaces.
oid = family subtree OID that this view includes or excludes.
type = indicate this view is to include or exclude the OID.

Example:

```
C1|S1|L1D>add snmp view name=primeView oid=1 type=include
C1|S1|L1D>
```

Remove SNMP Community

Syntax: **remove snmp community name**=STR_COMM_NAME

Description: Device-level command to delete (remove) an existing SNMP community from the V1/V2C Community String table. The **snmp community name** string cannot include “space" characters. This command is available to users with Write or Admin user privileges.

where:

name = SNMP community name (less than 32 characters).

Example:

```
C1|S1|L1D>remove snmp community name=xxxxxx
Cannot find the specified community!
C1|S1|L1D>remove snmp community name=xxxxxxx
C1|S1|L1D>
```

Remove SNMP Group

Syntax: **remove snmp group name**=STR_SNMP_GRP [**security-model**=(any|v1|v2c|v3) **security level**=(noAuthNoPriv|authNoPriv|authPriv)]

Description: Device-level command to delete (remove) an existing SNMP v3 Group from the system. Note that when the security model is v1 or v2c, the groups "public" and "private" cannot be removed; but when the security model is v3 the groups "public" and "private" can be removed. The **snmp group name** string cannot include or "space" characters.
This command is used to remove an existing SNMP group by specifying its name, security model and security level. You can also just give the group name to remove all groups that share the same group name. This command is available to all Write users and Admin users.

where:

name = SNMP group name (less than 32 characters).
security-model = the group's access right (v1, v2c, or v3).
security-level = the minimum level of security (noAuthNoPriv, authNoPriv, or authPriv).

Example:
```
C1|S1|L1D>remove snmp group name=private2
C1|S1|L1D>
```

Remove SNMP Local User

Syntax: **remove snmp local user name**=STR_USER_NAME

Description: Device-level command to delete (remove) a unique new SNMP v3 local user. The SNMP user's security model can only be v3. The **snmp local user name** string cannot include "space" characters. This command is available to all Write users and Admin users.

where:

name = SNMP group name (less than 32 characters).

Example:
```
C1|S1|L1D>remove snmp local user name=Fitz
C1|S1|L1D>
```

Remove SNMP Remote Engine

Syntax: **remove snmp remote engine addrtype**=ipv4 **addr**=STR_SVR_ADDR **port**=<1-65535>

Description: Interactive, device-level command to delete (remove) an existing remote engine from the SNMP v3 configuration. Note that if you remove a remote engine, all remote users related to this engine will also be removed. An error message displays if the specified address, address type, or port number is entered incorrectly or does not exist.
This command is available to users with Write or Admin level privileges.

where:

addr = the remote engine's IP address.

addrtype = the type of the remote engine's IP address (ipv4).

port = the port number of the remote trap host that receives traps <1-65535>.

Example:

```
C1|S1|L1D>show snmp remote engine
Remote Address                          Remote port         Remote Engine ID
------------------------------------------------------------------------------
192.168.1.20                            162                 800003640300c0f2209ede
192.168.1.70                            162                 800003640300c0f2208dce
C1|S1|L1D>remove snmp remote engine addrtype=ipv4 addr=192.168.1.70 port=162
If you remove this remote engine, all remote users related to this engine will also
be removed, continue? (y: yes, n: no)
y
C1|S1|L1D>show snmp remote engine
Remote Address                  Remote port     Remote Engine ID
------------------------------------------------------------------------------
192.168.1.20                    162             800003640300c0f2209ede
C1|S1|L1D>
```

Remove SNMP Remote User by IP Address / Port

Syntax: **remove snmp remote user name**=STR_USER_NAME **addrtype**=ipv4 **addr**=STR_SVR_ADDR **port**=<1-65535>

Description: Device-level command to delete (remove) an existing remote SNMP user by address type. The **snmp remote user name** string cannot include or "space" characters. This command is available to users with Write or Admin level privileges.
This command removes (deletes) an existing SNMP remote user by IP address and port number.

where:

name = the SNMP user name, less than 32 characters.
engine = the SNMP remote engine to which the remote user belongs (9-64 characters).

Example:

```
C1|S1|L1D>remove snmp remote user name=AliceB addrtype=ipv4 addr=192.168.1.30 port=162
No engine ID is specified for this address!
C1|S1|L1D>
```

Remove SNMP Remote User by Engine ID

Syntax: **remove snmp remote user name=**STR_USER_NAME **engine=**STR_ENGINE_ID

Description: Device-level command to delete (remove) an existing remote SNMP user by its Engine ID. The **snmp remote user name** string cannot include "space" characters. This command is available to users with Write or Admin level privileges.

where:

name = the SNMP user name, less than 32 characters.
engine = the SNMP remote engine to which the remote user belongs (9-64 characters).

Example:

```
C1|S1|L1D>remove snmp remote user name=AliceB engine=800003640300c0f2209ede
C1|S1|L1D>
```

Remove SNMP Traphost

Syntax: **remove snmp traphost type=**ipv4 **addr=**STR_SVR_ADDR **port=**<1-65535>

Description: Device-level command to remove a specified SNMP trap host. The specified trap host must have already been created and defined. This command is available to users with Write or Admin level privileges.

where:

type = ipv4.
addr = the IP address of the existing traphost to be removed.
port = the trap host port number that receives traps <1-65535> to be removed (e.g., 162).

Example:

```
C1|S1|L1D>remove snmp traphost type=ipv4 addr=192.168.1.30 port=162
C1|S1|L1D>
```

Remove SNMP View

Syntax: **remove snmp view name=**STR_SNMP_VIEW [**oid=**STR_VIEW_OID]

Description: Device-level command to delete (remove) an existing SNMP v3 View. The **snmp view name** string cannot include "space" characters. Removes an existing SNMP view by specifying its name and OID. You can just enter the view name to review all views with that name. The default view cannot be removed. This command is available to users with Write or Admin level privileges. This command deletes an existing OID sub tree.

where:

name = SNMP view name (less than 32 characters).
oid = family subtree OID that this view includes or excludes.

Example:

```
C1|S1|L1D>remove snmp view name=defaultView oid=1
Invalid OID for this view
```

Set SNMP Local Engine

Syntax: **set snmp local engine**=STR_LOCAL_ENGINE

Description: Interactive, device-level command to edit (reset) an existing SNMP v3 local Engine. Note that executing this command will delete all exist local users. This command sets the engine name of the local IONMM card. This command is available to all Write users and Admin users.

where:

engine = the local engine name (less than 64 characters).

Example:

```
C1|S1|L1D>show snmp local engine
Local engine ID:    80.00.03.64.03.00.c0.f2.20.de.9e (hex)
C1|S1|L1D>show snmp local user
User Name   Group Name          Security Model  Security Level    Auth Protocol  Privacy Protocol
------------------------------------------------------------------------------
Adam      G1V3AuthPriv      MD5    DES       v3  authPriv    MD5             DES
JeffS     private2Priv      MD5    DES      v3  noAuthNoPriv
C1|S1|L1D>set snmp local engine=800003640300c0f2209ede
Reseting local Engine ID will delete all exist local users, continue?(y: yes, n: no)
y
C1|S1|L1D>show snmp local engine
Local engine ID:    80.00.03.64.03.00.c0.f2.20.9e.de (hex)
C1|S1|L1D>
```

Note: If you enter the **show snmp remote engine** command with no existing remote engines, the message "*No SNMP remote engine created now!*" displays.

Set SNMP Group Name for Local User

Syntax: **set snmp local user name**=STR_USR_NAME **group**=STR_GRP_NAME

Description: Device-level command to set (edit / change) the group name for an existing SNMP local user. This command is available to all Write users and Admin users.

where:

name = the SNMP user name (less than 32 characters).

group = SNMP group name to which the new user is assigned (less than 32 characters).

Example:

```
C1|S13|L1D>set snmp local user name=newusr1 group=public
C1|S13|L1D>
```

Set SNMP View Filter Type

Syntax: **set snmp view name**=STR_SNMP_VIEW **oid**=STR_VIEW_OID **type**=(include|exclude)

Description: Device-level command to edit (change) the filter type of an existing SNMP v3 View. The **snmp view name** string cannot include "space" characters. This command is available to users with Write and Admin level privileges.

where:

name = SNMP view name, its length must be shorter than 32 characters.

oid = family subtree OID that this view include or exclude.

type = indicate this view is to include or exclude the OID.

Example:

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

Show SNMP Community

Syntax: **show snmp community**

Description: Device-level command to display all current (existing) SNMP communities' information. This command is available to all SNMP users.

Example:

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

Show SNMP Group

Syntax: **show snmp group** [**name**=STR_SNMP_GRP]

Description: Device-level command that displays a current (existing) SNMP v3 Group by name, or all Groups currently defined. After you display a specific Group name, you must log in to the system again. If no group name is specified, displays all available group information on the IONMM card or stand-alone card. If a group name is entered, displays just that group's configuration. This command is available to all users at all privilege levels.

where:

name = the name of a SNMP group (optional)

Example:

```
C1|S1|L1D>show snmp group
Name      Security Model  Security Level     Read View    Write View        Notify View
------------------------------------------------------------------------------
public    v1              noAuthNoPriv      defaultView
public    v2c             noAuthNoPriv      defaultView
private   v1              noAuthNoPriv      defaultView  defaultView
private   v2c             noAuthNoPriv      defaultView  defaultView
rem-corp  any             noAuthNoPriv      xxxxxx     zzzzzzz
C1|S1|L1D>show snmp group public
Name      Security Model Security Level     Read View      Write View        Notify View
------------------------------------------------------------------------------
login: ION
Password:*******

Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C1|S1|L1D>
```

Show SNMP Local Engine

Syntax: **show snmp local engine**

Description: Device-level command to display the local SNMP engines configured for the ION system. This command displays the engine ID of the local IONMM card. This command is available to users at all privilege levels.

Example:
```
C1|S1|L1D>show snmp local engine
Local engine ID:    80.00.03.64.03.00.c0.f2.20.9e.de (hex)
C1|S1|L1D>
```

Show SNMP Local User

Syntax: **show snmp local user**

Description: Device-level command to display information about all local SNMP users configured for the system. This command is available to all users at all privilege levels.

Example:
```
C1|S1|L1D>show snmp local user
User Name   Group Name         Security Model   Security Level   Auth Protocol   Privacy Protocol
-------------------------------------------------------------------------------
BobB       rem-corp v3             authNoPriv    MD5
TedT                        v3             noAuthNoPriv
CarolC                              authPriv       SHA             AES
C1|S1|L1D>
```

Show SNMP Remote Engine

Syntax: **show snmp remote engine**

Description: Device-level command that displays a list of all SNMP v3 remote engines currently configured. This command is available to all SNMP v3 users.

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

Show SNMP Remote User

Syntax: **show snmp remote user**

Description: Device-level command to display a list of all SNMP emote users currently configured. This command is available to all users at all privilege levels.

Example 1 (no existing remote users):

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

Example 2 (one existing remote user):

```
User Name       Engine ID             Security Model Security Level Auth Protocol Privacy Protocol
--------------------------------------------------------------------------------
Rmtusr1         002fedfe334343535 noAuthNoPriv v3
```

Show SNMP Traphost

Syntax: **show snmp traphost**

Description: Device-level command to display the specified SNMP v3 traphost server information or display the traphost server information for all defined and configured SNMP v3 trap hosts. This command is available to all SNMP v3 user levels.

Example:

```
C1|S1|L1D>show snmp traphost
Trap version   IP           Port   Community/Security name Security level Trap/inform Timeout Retry times
-----------------------------------------------------------------------------------------------------
v3             192.168.1.40  162    private                 authNoPriv     trap
v3             192.168.1.50  162    public                  authPriv       trap
v2c            192.168.1.10  162    public                  noAuthNoPriv   inform       1500      3
v1             192.168.1.20  162    public                  noAuthNoPriv   trap
C1|S1|L1D>
```

Note: If you enter the **show snmp traphost** command with no existing remote engines, the message "*No SNMP trap host is created now!*" displays.

Show SNMP View

Syntax: **show snmp view** [**name**=STR_SNMP_VIEW]

Description: Device-level command that displays one or all current SNMP View(s). If no view name is specified, show all available views' information on IONMM card or stand-alone card. If a view name is entered, only that view is displayed.

Example:

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

C1|S1|L1D>show snmp view=primeView

login: ION
Password:*******

Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C1|S1|L1D>
```

27. SNTP Commands

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

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.

The following commands are used for SNTP operations.

Set Current Time

Syntax: **set curr–time=<"**xx**">**

Description: Defines the current time for a module.

where:

xx = current time in the format: "yyyymmdd hh:mm:ss".

Note: the quote marks are required.

Set SNTP Daylight Saving Time Status

Syntax: **set sntp dst–state**={enable | disable}

Description: Enables or disables the SNTP daylight savings time function on a card.

Example:
```
C1|S3|L1D>set sntp dst-state=enable
C1|S3|L1D>
```

Set SNTP Daylight Saving Start Time

Syntax: **set sntp dst–start=<"**xx**">**

Description: Defines the date and time that SNTP daylight savings is to begin.

where:

xx = start time in the format: "yyyymmdd hh:mm". **Note:** the quote marks are required.

Example:
```
C1|S3|L1D>set sntp dst-start="2010-05-30 02:00"
C1|S3|L1D>
```

The above command sets the daylight savings time to begin at 2 a.m. on May 30, 2010.

Set SNTP Daylight Saving End Time

Syntax: **set sntp dst–end=<"**xx**">**

Description: Defines the date and time that SNTP daylight savings is to end.

where:

xx = end time in the format: "yyyy-mm-dd hh:mm".
Note: the quote marks are required.

Example:
```
C1|S3|L1D>set sntp dst-end="2010-11-30 12:00"
C1|S3|L1D>
```

The above command sets daylight savings time to end at 12 a.m. on November 30, 2010.

Set SNTP Daylight Saving Offset

Syntax: **set sntp dst–offset=<**xx**>**

Description: Defines the amount of time, in minutes (1–720), that clocks are to shift because of daylight savings. **Note:** the usual time shift (offset) is one hour (60 minutes).

Example:
```
C1|S3|L1D>set sntp dst-offset=30
C1|S3|L1D>
```

Set SNTP Server Address

Syntax: **set sntp-svr svr**=<1-6> **type**=(ipv4|ipv6|dns) **addr**=ADDR [retry

Description: Defines the address of an SNTP server. Up to six SNTP servers can be defined in the system.

where:

svr = The DNS server number (1–6). Up to 6 can be configured.

type = IP address format; the valid choices are:

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

addr = IP address of the SNTP server.

retry = optional number of retry attempts.

Example:

```
C1|S3|L1D>set sntp-svr svr=1 type=ipv4 addr=192.168.1.30
C1|S3|L1D>set sntp-svr svr=1 type=ipv6 addr=fe80::2c0:f2ff:fe21:b243
```

Set SNTP Status

Syntax: **set sntp state**={enable | disable}

Description: Enables or disables the SNTP function on an x323x NID or IONMM card.

Example:

```
Agent III C1|S1|L1D>set sntp state=enable
Agent III C1|S1|L1D>show sntp config
SNTP configuration:
------------------------------------------------------------------------
SNTP state:                              enable
:
:
Agent III C1|S1|L1D>
```

Set SNTP Timezone

Syntax: **set sntp timezone=<**xx>

Description: Defines the timezone of an IONMM. The value for "zone" is a number from 1–63 as shown in the table below.

Example:

```
Agent III C1|S1|L1D>set sntp timezone=47
Agent III C1|S1|L1D>show sntp config
SNTP configuration:
--------------------------------------------------------------------------
SNTP state:                              enable
SNTP daylight saving time state:         disable
Sntp timezone:                           (GMT+8:00) Beijing, Chongqing, Hong
                                              Kong, Urumqi
Current time:
```

Table 6: Timezones

Zone	Description
1	(GMT –12:00) Eniwetok, Kwajalein
2	(GMT –11:00) Midway, Island, Samoa
3	(GMT –10:00) Hawaii
4	(GMT –09:00) Alaska
5	(GMT –08:00) Pacific Time, US and Canada, Tijuana
6	(GMT –07:00) Arizona
7	(GMT –07:00) Mountain Time, US and Canada
8	(GMT –06:00) Central Time, US and Canada
9	(GMT –06:00) Mexico, City, Tegucigalpa
10	(GMT –06:00) Saskatchewan
11	(GMT –05:00) Bogota, Lima, Quito
12	(GMT –05:00) Eastern Time US and Canada
13	(GMT –05:00) Indiana, East
14	(GMT –04:00) Atlantic Time, Canada
15	(GMT –04:00) Caracas, La, Paz
16	(GMT –04:00) Santiago

17	(GMT –03:30) Newfoundland
18	(GMT –03:00) Brasilia
19	(GMT –03:00) Buenos, Aires, Georgetown
20	(GMT –02:00) Mid-Atlantic
21	(GMT –01:00) Azores, Cape, Verde, Is
22	(GMT) Casablanca, Monrovia
23	(GMT) Greenwich, Mean, Time, Dublin, Edinburgh, Lisbon, London
24	(GMT +01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
25	(GMT +01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
26	(GMT +01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius
27	(GMT +01:00) Sarajevo, Skopje, Sofija, Warsaw, Zagreb
28	(GMT +02:00) Athens, Istanbul, Minsk
29	(GMT +02:00) Bucharest
30	(GMT +02:00) Cairo
31	(GMT +02:00) Harare, Pretoria
32	(GMT +02:00) Helsinki, Riga, Tallinn
33	(GMT +02:00) Jerusalem
34	(GMT +03:00) Baghdad, Kuwait, Riyadh
35	(GMT +03:00) Moscow, St, Petersburg, Volgograd
36	(GMT +03:00) Nairobi
37	(GMT +03:30) Tehran
38	(GMT +04:00) Abu, Dhabi, Muscat
39	(GMT +04:00) Baku, Tbilisi
40	(GMT +04:30) Kabul
41	(GMT +05:00) Ekaterinburg
42	(GMT +05:00) Islamabad, Karachi, Tashkent
43	(GMT +05:30) Bombay, Calcutta, Madras, New, Delhi
44	(GMT +06:00) Astana, Almaty, Dhaka
45	(GMT +06:00) Colombo

46	(GMT +07:00) Bangkok, Hanoi, Jakarta
47	(GMT +08:00) Beijing, Chongqing, Hong, Kong, Urumqi
48	(GMT +08:00) Perth
49	(GMT +08:00) Singapore
50	(GMT +08:00) Taipei
51	(GMT +09:00) Osaka, Sapporo, Tokyo
52	(GMT +09:00) Seoul
53	(GMT +09:00) Yakutsk
54	(GMT +09:30) Adelaide
55	(GMT +09:30) Darwin
56	(GMT +10:00) Brisbane
57	(GMT +10:00) Canberra, Melbourne, Sydney
58	(GMT +10:00) Guam, Port, Moresby
59	(GMT +10:00) Hobart
60	(GMT +10:00) Vladivostok
61	(GMT +11:00) Magadan, Solomon Is, New Caledonia
62	(GMT +12:00) Auckland, Wllington
63	(GMT +12:00) Fiji, Kamchatka, Marshall, Islands

Show SNTP Configuration

Syntax: **show sntp config**

Description: Displays all SNTP configurations on the IONMM or a NID.

Example:

```
Agent III C1|S1|L1D>show sntp config
SNTP configuration:
------------------------------------------------------------------------
SNTP state:                             enable
SNTP daylight saving time state:        disable
Sntp timezone:                          (GMT+8:00) Beijing, Chongqing, Hong Kong
, Urumqi
Current time:                           1970 0102 10:17:17
Sntp daylight saving start time:        1970 0101 08:00:00
Sntp daylight saving end time:          1970 0101 08:00:00
sntp daylight saving offset:            0

Sntp server:
index               addr-type           address
------------------------------------------------------------------------
1                   dns                 0.0.0.0
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
Agent III C1|S1|L1D>
```

Show SNTP Timezone

Syntax: **show timezone**

Description: Displays all of the time zones that can be specified.

Example:

```
Agent III C1|S1|L1D>show timezone
Available timezone:
-------------------------------------------------------------------
1 :      (GMT-12:00) Eniwetok, Kwajalein
2 :      (GMT-11:00) Midway Island, Samoa
3 :      (GMT-10:00) Hawaii
4 :      (GMT-9:00) Alaska
5 :      (GMT-8:00) Pacific Time US and Canada Tijuana
6 :      (GMT-7:00) Arizona
7 :      (GMT-7:00) Mountain Time US and Canada
8 :      (GMT-6:00) Central Time US and Canada
9 :      (GMT-6:00) Mexico City, Tegucigalpa
10:     (GMT-6:00) Saskatchewan
11:     (GMT-5:00) Bogota, Lima, Quito
12:     (GMT-5:00) Eastern Time US and Canada
13:     (GMT-5:00) Indiana East
14:     (GMT-4:00) Atlantic Time Canada
15:     (GMT-4:00) Caracas, La Paz
16:     (GMT-4:00) Santiago
17:     (GMT-3:00) Newfoundland
:         :
60:     (GMT+10:00) Vladivostok
61:     (GMT+11:00) Magadan, Solomon Islands, New Caledonia
62:     (GMT+12:00) Auckland, Wllington
63:     (GMT+12:00) Fiji, Kamchatka, Marshall Islands

Agent III C1|S1|L1D>
```

28. SOAM (Service OAM) Commands

OAM (Operation, Administration and Maintenance) is a set of functions designed to monitor network operation to detect network faults and measure its performance. Ethernet OAM functionality allows network operators to measure quality of service (QoS) attributes such as availability, frame delay, frame delay variation (jitter and frame loss). Such measurements help identify problems before they escalate so that users are not impacted by network defects.

Ethernet Connectivity Fault Management (CFM) is provided per IEEE 802.1AG. Ethernet CFM comprises three protocols that help administrators debug Ethernet networks: continuity check, link trace and loop-back protocols.

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

SOAM Restrictions

1. There is a maximum limit on the number of MEGs and MEPs that the ION system can support (up to 16 VLANs per port and 8 levels on each VLAN).
2. SOAM is only supported on Port 3 of the x3231 NID in regard to redundancy. The x3231 does not function as a 3-port switch in regard to SOAM, but rather allows for fiber redundancy, including SOAM. SOAM views Port 3 as a redundant port, so a SOAM MEP or MIP cannot be created on Port 3. This restriction applies whether the “Redundancy” feature is enabled or disabled.

SOAM can coexist with all other features. All operating modes are supported.

Note: For Service OAM configuration, you must finish all settings on the MA/MEG page before going to the MEP configuration. After the MEP is created, any configuration changed in MA/MEG may not take effect on that MEP. You must restart the card or recreate this MEP for the new MA/MEG changes to take effect.

Note: Some product catalog features do not match the actual features:
C2220 series: support "TLPT, SLPT" features; do not support "Remote Fault Detect (RFD)".
C322x / C323x series: support "TLPT, SLPT features"; do not support "Remote Fault Detect (RFD)".

Note: The SOAM commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

SOAM Initialization Commands

Show SOAM Sender ID Configuration

Syntax: **show soam senderid**

Description: Displays the content of the Sender ID TLV which will be included in frames originated by this system.

Example:
```
C1|S5|L1D>show soam senderid
Chassis id subtype : MAC Address
Chassis id         : 00-C0-F2-21-01-77
Management domain  : 0.1 (udpIpv4)
Management address : 192.168.1.10
C1|S5|L1D>
```

Show SOAM Configuration Error List

Syntax: **show soam conferror vid=**<xx> **port=**<yy>

Description: Displays the configuration error list for the given port and VLAN.
The IEEE802.1ag standard lists the possible errors (CFM Leak, Conflicting VIDs, Excessive Levels, and Overlapped Levels). If error free, displays "*No config errors.*"

Example 1:
```
C1|S3|L1D>show soam conferror vid=1 port=1
 No config errors.
```

Example 2:
```
C1|S13|L0D/>show soam conferror vid=12 port=1
List : CFMleak
```

CFM leak: Max is associated with a specific VID list, one or more of the VIDs in Max can pass through the Bridge Port, no Down MEP is configured on any Bridge Port for Max, and some other May, at a higher MD Level than Max, and associated with at least one of the VID(s) also in Max, does have a MEP configured on the Bridge Port.

Conflicting Vids: Max is associated with a specific VID list, an Up MEP is configured on Max on the Bridge Port, and some other May, associated with at least one of the VID(s) also in Max, also has an Up MEP configured on some Bridge Port.

Excessive Levels: The number of different MD Levels at which MIPs are to be created on this port exceeds the Bridge's capabilities.

Overlapped Levels: A MEP is created for one VID at one MD Level, but a MEP is configured on another VID at that MD Level or higher, exceeding the Bridge's capabilities.

Show SOAM Port

Syntax: **show soam port**

Description: Displays the status (enabled or disabled) of all of the NID's SOAM ports.

Example:

```
C1|S3|L1D>show soam port
Port index   : 1
SOAM state   : enabled

Port index   : 2
SOAM state   : enabled
C1|S3|L1D>
```

Show SOAM Port ID

Syntax: **show soam portid**

Description: Displays the NIDs SOAM port parameters (index, sub-type and ID).

Example:

```
C1|S3|L1D>show soam portid
Port index   : 1
Port subtype : Locally Assigned
Port ID      : 00 00 00 01

Port index   : 2
Port subtype : Locally Assigned
Port ID      : 00 00 00 02
C1|S3|L1D>
```

SOAM Maintenance Domain (MD) Commands

Note: These commands are for the IEEE 802.1ag standard.

Add Maintenance Domain

Syntax: **add soam md local–md–id=**<xx> **md–name=**{<yy> | **none**} **md–level=**<zz>

Description: Adds a new maintenance domain to the SOAM configuration.

where :

xx = maintenance domain identifier (1–4294967295)

yy = maintenance domain name or **none**. If a name is specified, it can be a maximum of 43 characters in length.

zz = level (0–7) assigned to the added maintenance domain

Example:
```
C1|S5|L1D>add soam md local-md-id 99999 md-name=none md-level=5
C1|S5|L1D>
```

Remove Maintenance Domain

Syntax: **remove soam md local–md–id=**<xx>

Description: Removes an existing SOAM MD (maintenance domain) from the configuration.

where :

xx = maintenance domain identifier (1–4294967295)

Example:
```
C1|S5|L1D>remove soam md local-md-id=99999

C1|S5|L1D>
```

Note: An MD cannot be deleted if there are lower level entities (Mas, MIPs) configured on it. The MD's configured lower level entities (Mas, MIPs) must be deleted first.

Set Sender ID Permissions

Syntax: **set soam md local–md–id=**<xx> **permission–id=**<yy>

Description: Defines the sender ID permissions of an existing SOAM maintenance domain (MD).

where:

xx = maintenance domain identifier (1–4294967295)

yy = fields of the Sender ID that are to be sent; the valid choices are:

- **none** – **no permissions -** does not send or receive LLDPDUs.
- **chassis** - Chassis ID TLV - carries the bridge MAC address of the sender.
- **mgmtaddr** - Management Address TLV - carries the management address, the corresponding port number, and OID. If the management address is not configured, uses the IP address of the VLAN interface with the lowest VLAN ID among those permitted on the port. If the VLAN interface IP address is not configured, 127.0.0.1 is used as the management address.
- **chassismgmtaddr -** Chassis ID TLV and Management Address TLV – carries both **chassis** and **mgmtaddr.**

Example:

```
C1|S3|L1D>set soam md local-md-id 567 permission-id ?
  chassis
  chassismgmtaddr
  mgmtaddr
  none
C1|S5|L1D>set soam md local-md-id=999 permission-id=chassismgmtaddr
C1|S5|L1D>
```

Note: An MD with this id must have already been configured.

Use the **show soam md** command to determine the current SOAM MD permissions.

Show Maintenance Domain

Syntax: **show soam md** [local–md–id=<xx>]

Description: Displays the details of existing SOAM maintenance domain(s).

where:

xx = optional ; maintenance domain identifier (1–4294967295). If omitted, all maintenance domains are displayed.

Example 1:

```
C1|S3|L1D>show soam md
Local MD ID            Name Level  Mas MIPs      Permission
-------------------------------------------------------------
         3      OperatorMD     3    1    1            none
         6      ProviderMD     6    1    1            none
        11         UNIbcMD     0    1    0            none
       111         UNIcdMD     0    1    0            none
C1|S3|L1D>
```

Example 2:

```
C1|S5|L1D>show soam md local-md-id=999
Local MD ID            Name Level  Mas MIPs      Permission
-------------------------------------------------------------
       999          nameit     4    0    0 chassismgmtaddr

C1|S5|L1D>
```

SOAM Maintenance Association (MA) Commands

Note: These commands are for the IEEE 802.1ag standard.

Add Maintenance Association

Syntax: **add soam ma local–ma–id=**<uu> **local–md–id=**<vv> **ma–name=**<ww> **vlan–type=**<xx> [**vlan–id–list=**<yy>] [**s–vid=**<zz>]

Description: Adds a new SOAM maintenance association (MA).

where:

uu = maintenance association identifier (1–4294967295)

vv = maintenance domain identifier (1–4294967295)

ww = maintenance association name (maximum of 44 characters)

xx = VLAN type of VLAN ID list to associate with the MA; valid choices are:

- **none**
- **ctype**
- **stype**
- **doubletag**

Note: If **doubletag** is selected, then **s–vid=** must be specified.

yy = optional; a list of one or more VLAN IDs. Omit this parameter if **vlan–type=none** is specified.

zz = conditional; VLAN ID of the secondary VID. S-VID is available only for the double-tagged or 802.1D tagged MEPs. The S-VID will be used in the Provider tag.

Example:

```
C1|S5|L1D>add soam ma local-ma-id 99 local-md-id 999 ma-name maid9 vlan-type ctype
Vlans ID list is empty.
C1|S5|L1D>
```

Remove Maintenance Association

Syntax: **remove soam ma local–ma–id=**<xx>

Description: Removes an existing SOAM maintenance association (MA).
where:

xx = maintenance association identifier (1–4294967295)

Note: An MA cannot be removed if there are lower level entities (MEPs) configured on it.

Set Maintenance Association Parameters

Syntax: **set soam ma local–ma–id=**<xx> **attr_name=**<yy> **attr_value=**<zz>

Description: Defines parameters of an existing maintenance association of the SOAM engine.
where:

xx = maintenance association identifier (1–4294967295)

yy = name of the attribute to be changed (see table below)

zz = new value to be associated with attribute yy (see table below)

If yy equals:	Then zz can be:
permission Determines which fields of the maintenance domain are to be sent.	• **none** • **chassis** • **mgmtaddr** • **chassismgmtaddr** • **MD defer**
ccmininterval The interval at which CC messages are transmitted.	• **cci1s** • **cci10s** • **cci1min** • **cci10min**
mepid–add Configure local and remote MEPs belonging to this MA.	ID (1–8191) of the MEP to be configured.
mepid-remove Remove local and remote MEPs belonging to this MA.	ID (1–8191) of the MEP to be deleted.
vlan–add Add a VLAN to this MA.	ID of the VLAN to be added.
vlan-remove Remove a VLAN from this MA.	ID of the VLAN to be removed.
primary–vlan The primary VID used for all CFM frames belonging to this MA.	VLAN ID.
autodetection–timeout	Number of milliseconds.

If yy equals:	Then zz can be:
The amount of time before a remote peer MEP is removed from the CCM Database on loss of CCMs from the remote MEP.	
autodetectrmep Whether MEPs are discovered automatically based on received CCM messages.	• **enable** • **disable**

Example:

```
C1|S3|L1D>set soam ma local-ma-id 1 attr_name ?
  permission
  ccminterval
  mepid-add
  mepid-remove
  vlan-add
  vlan-remove
  primary-vlan
  autodetection-timeout
  autodetectrmep
C1|S3|L1D>set soam ma local-ma-id 1 attr_name permission ?
attr_value permission
  ..
  cci10min
  cci10s
  cci1min
  cci1s
  chassis
  chassismgmtaddr
  defer
  disable
  enable
  mgmtaddr
  none
  <cr>
C1|S3|L1D>C1|S3|L1D>set soam ma local-ma-id 1 attr_name permission attr_value permission ena-
ble

login: ION
Password:

Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C1|S1|L1D>
```

Show Maintenance Association

Syntax: **show soam ma** [local–ma–id=<xx>]

Description: Displays details of a existing SOAM MA(s). An MA and a MD must have already been created. If no MA's have been created, displays the message "*The Mas table is empty*.".

where:

xx = optional; maintenance association identifier (1–4294967295). If omitted, a list of all configured maintenance associations is displayed. *Example* (3 Mas defined):

```
C1|S3|L1D>show soam ma
MA index               : 3
MD index               : 3
MD level               : 3
MD name                : OperatorMD
MA name                : OperatorSTag100
CCM interval           : 1s
MEPs                   : 1
MEP ID list            : (2 MepIds) 310 320
Permission             : defer
VLAN ID list           : stype: 100 1
Primary VLAN ID        : 100
Auto detection timeout : 0
Auto detect remote MEP : disabled

MA index               : 6
MD index               : 6
MD level               : 6
MD name                : ProviderMD
MA name                : ProviderCTag200
CCM interval           : 1s
MEPs                   : 0
MEP ID list            : (0 MepIds)
Permission             : defer
VLAN ID list           : ctype: 200 2
Primary VLAN ID        : 200
Auto detection timeout : 0
Auto detect remote MEP : disabled

MA index               : 11
MD index               : 11
MD level               : 0
MD name                : UNIbcMD
MA name                : UNIbcUntagged
CCM interval           : 1s
MEPs                   : 1
MEP ID list            : (2 MepIds) 30 40
Permission             : defer
VLAN ID list           : none
Auto detection timeout : 0
Auto detect remote MEP : disabled
```

SOAM Management Entity Group (MEG) Commands

Note: These commands are for Y.1731 mode only.

Add Maintenance Entity Group

Syntax: **add soam meg local–meg–id=**<uu> **meg–name=**<vv> **meg–level=**<ww> **vlan–type=**<xx> [**vlan–id–list=**<yy>] [**s–vid=**<zz>]

Description: Adds a new SOAM maintenance entity group (MEG).

where:

uu = maintenance entity group identifier (1–4294967295)

vv = maintenance entity group name

ww = maintenance entity group level (0 –7) assigned to the new MEG

xx = VLAN type of VLAN ID list to associate with the MEG; valid choices are:

- **none**
- **ctype**
- **stype**
- **doubletag**

Note: If **doubletag** is selected, then **s–vid=** must be specified.

yy = optional; a list of one or more VLAN IDs (2-4095). Omit this parameter if **vlan–type=none** is specified.

zz = conditional; VLAN ID of the secondary VID (2-4095). The S-VID is available only for the double-tagged or 802.1D tagged MEPs. The S-VID will be used in the Provider tag.

Example:

```
C1|S3|L1D>add soam meg local-meg-id 5 meg-name megid5 meg-level 5 vlan-type stype
VLANs ID list is empty.
C1|S3|L1D>add soam meg local-meg-id 5 meg-name megid5 meg-level 5 vlan-type none
C1|S3|L1D>
```

Remove Maintenance Entity Group

Syntax: **remove soam meg local–meg–id=**<xx>

Description: Removes an existing SOAM maintenance entity group (MEG).
where:

xx = maintenance entity group identifier (1–4294967295)

If no MEGs have yet been created, displays the message "*MEG with this id has not been configured yet*.".

Example:

```
C1|S3|L1D>add soam meg local-meg-id 5 meg-name megid5 meg-level 5 vlan-type none

C1|S3|L1D>remove soam meg local-meg-id 5

C1|S3|L1D>show soam meg
MEG index              : 1
MEG level              : 1
MEG name               : MEGID1
CCM interval           : 1s
MEPs                   : 0
MIPs                   : 1
MEP ID list            : (0 MepIds)
Permission             : chassismgmtaddr
VLAN ID list           : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking       : enabled

C1|S3|L1D>
```

Set Maintenance Entity Group Parameters

Syntax: **set soam meg local–meg–id=**<xx> **attr_name=**<yy> **attr_value=**<zz>

Description: Defines parameters of an existing maintenance entity group of the SOAM configuration.

where:

xx = maintenance entity group identifier (1–4294967295)

yy = name of the attribute to be changed (see table below)

zz = new value to be associated with attribute yy (see table below)

If yy equals:	Then zz can be:
permission Determines which fields of the maintenance domain are to be sent.	• **none** • **chassis** • **mgmtaddr** • **chassismgmtaddr** • **defer**
ccmininterval The interval at which CC messages are transmitted.	• **cci1s** • **cci10s** • **cci1min** • **cci10min**
mepid–add Configure local and remote MEPs belonging to this MEG.	ID (1–8191) of the MEP to be configured.
mepid-remove Remove local and remote MEPs belonging to this MEG.	ID (1–8191) of the MEP to be deleted.
vlan–add Add a VLAN to this MEG.	ID of the VLAN to be added.
vlan-remove Remove a VLAN from this MEG.	ID of the VLAN to be removed.
primary–vlan The primary VID used for all CFM frames belonging to this MEG.	VLAN ID.
autodetection–timeout The amount of time before a remote peer MEP is removed from the CCM Database on loss of CCMs from the remote MEP.	Number of milliseconds.
autodetectrmep Whether MEPs are discovered automatically based on received CCM messages.	• **enable** • **disable**
y.1731–802.lag–interop Status of the interoperability.	• **enable** • **disable**

Example:

```
C1|S3|L1D>set soam meg local-meg-id 5 attr_name ?
  permission
  ccminterval
  mepid-add
  mepid-remove
  vlan-add
  vlan-remove
  primary-vlan
  autodetection-timeout
  autodetectrmep
  y.1731-802.1ag-interop
C1|S3|L1D>set soam meg local-meg-id=4 attr_name=y.1731-802.1ag-interop attr_value enable
C1|S3|L1D>
```

Show Maintenance Entity Group

Syntax: **show soam meg** [**local–meg–id=**<xx>]

Description: Displays details of one or all existing SOAM Maintenance Entity Group (MEG).

where:

xx = optional; maintenance association identifier (1–4294967295). If omitted, a list of all configured maintenance entity groups is displayed.

Example:

```
C1|S3|L1D>show soam meg
MEG index              : 10
MEG level              : 0
MEG name               : UNIabUntagY
CCM interval           : 1s
MEPs                   : 0
MIPs                   : 0
MEP ID list            : (0 MepIds)
Permission             : none
VLAN ID list           : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking       : disabled

MEG index              : 20
MEG level              : 0
MEG name               : UNIbcUntagY
CCM interval           : 1s
MEPs                   : 0
MIPs                   : 0
MEP ID list            : (2 MepIds) 13 14
Permission             : none
VLAN ID list           : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking       : disabled

MEG index              : 30
MEG level              : 0
MEG name               : UNIcdUntagY
CCM interval           : 1s
MEPs                   : 0
MIPs                   : 0
MEP ID list            : (2 MepIds) 15 16
Permission             : none
VLAN ID list           : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking       : disabled
```

```
MEG index              : 300
MEG level              : 3
MEG name               : OperCTag300Y
CCM interval           : 1s
MEPs                   : 0
MIPs                   : 1
MEP ID list            : (2 MepIds) 31 32
Permission             : none
VLAN ID list           : ctype: 300 600
Primary VLAN ID        : 300
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking       : disabled

MEG index              : 600
MEG level              : 6
MEG name               : ProvCTag600Y
CCM interval           : 1s
MEPs                   : 0
MIPs                   : 1
MEP ID list            : (0 MepIds)
Permission             : none
VLAN ID list           : ctype: 600 300
Primary VLAN ID        : 600
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking       : disabled
C1|S3|L1D>
```

SOAM Maintenance End Point (MEP) Commands

MEPs are common entities between Y.1731 and 802.1ag modes. Some attributes, however, do not apply to both modes.

Add a MEP

Syntax: **add soam mep mep–id=**<ww> **local–parent–id=**<xx> **direction=**<yy> **port=**<zz>

Description: Adds a new MEP to the SOAM engine.

where:

ww = MEP identifier (1–8191)

xx = ID of the local MA or MEG to be associated with the MEP

yy = direction of the MEP; **up** or **down**

zz = number of the port the MEP will be associated with

Example:

```
C1|S5|L1D>add soam mep mep-id 9 local-parent-id 99 direction up port=2
```

Note: A MA/MEG with this MEP ID must have previously been configured.

Remove MEP

Syntax: r**emove soam mep mep–id=**<xx> **local–parent–id=**<yy>

Description: Removes an existing MEP from the SOAM engine.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MA or MEG associated with the MEP

Example:

```
C1|S5|L1D>remove soam mep mep-id 99 local-parent-id 9
MA/MEG with this id has not been configured yet.
C1|S5|L1D>
```

Set MEP Parameters

Syntax: **set soam mep config mep–id=**<ww> **local–parent–id=**<xx> **attr_name=**<yy> **attr_value=**<zz>

Description: Defines parameters of an existing SOAM MEP. **Note**: your HyperTerminal session will be lost and you must log in to the ION system again after executing this command.

where:

ww = MEP identifier (1–8191)

xx = ID of the local MA or MEG associated with the MEP (1-4294967295)

yy = name of the attribute to be changed (see table below)

zz = new value to be associated with attribute yy (see table below)

If yy equals:	Then zz can be:
admin Admin status of the MEP.	• **enable** • **disable**
cci CCM generation status.	• **enable** • **disable**
primary–vid ID of the primary VLAN for the MEP.	VLAN ID.
ccmltmpriority Priority of the CCM and LTM.	0–7
faultalarmdetect Value, in milliseconds, of the fault alarm detect timer.	2500–10000
faultalarmreset Value, in milliseconds, of the fault alarm reset timer.	2500–10000
lowestprilevel The lowest alarm priority.	• **alldef** • **ais** • **macremerrxcon** • **remerrxconn** • **errxconn** • **xconn** • **noxcon**
aisclient–add List of AIS clients to be added (Y.1731 only).	client list (e.g.,: MEP153 MIP4, etc.)
aisclient–remove List of AIS clients to be deleted (Y.1731 only).	client list (e.g.,: MEP153 MIP4, etc.)
aistransmit Status of the AIS transmission (Y.1731 only).	• **enable** • **disable**
aisinterval The AIS transmission interval (Y.1731 only).	• **1min** • **1s**
aisnotifyup	• **enable**

The AIS notify up status (Y.1731 only).	• **disable**
aisframepriority The AIS frame priority (Y.1731 only).	0–7

Example:

```
C1|S3|L1D>set soam mep config mep-id=1 local-parent-id=10 attr_name=admin
attr_value=cci
login:
```

Show MEP Configuration

Syntax: **show soam mep config** [**mep–id=**<xx> **local–parent–id=**<yy>]

Description: Displays a list of existing SOAM MEPs and related configuration information.
where:

xx = optional; MEP identifier (1–8191). If omitted, a list of all configured MEPs is displayed

yy = conditional; ID of the local MA or MEG to be associated with the MEP. This parameter must be specified if **mep–id=** is entered.

Example 1:

```
C1|S3|L1D>show soam mep config
MEP id                    : 10
MD local ID               : 1
MD level                  : 0
MD name                   : UNIabMD
MA local ID               : 1
MA name                   : UNIabUntagged
Direction                 : down
Port                      : 1
VLANs                     : none
Primary VLAN              : 0
Admin status              : enabled
CCI status                : disabled
Fault notification state  : Defect Reported
Defects                   : RemoteCCM
Next LTM transaction ID   : 1
Next LBM transaction ID   : 1
CCM and LTM priority      : 0
Fault Alarm Detect Time   : 2500 ms
Fault Alarm Reset Time    : 10000 ms
Lowest Alarm priority     : macremerrxcon

MEP id                    : 20
MD local ID               : 1
MD level                  : 0
MD name                   : UNIabMD
MA local ID               : 1
MA name                   : UNIabUntagged
Direction                 : down
Port                      : 2
VLANs                     : none
Primary VLAN              : 0
Admin status              : enabled
CCI status                : enabled
Fault notification state  : Defect Reported
Defects                   : RemoteCCM
Next LTM transaction ID   : 1
Next LBM transaction ID   : 1
CCM and LTM priority      : 0
Fault Alarm Detect Time   : 2500 ms
Fault Alarm Reset Time    : 10000 ms
```

```
Lowest Alarm priority    : macremerrxcon
```

Example 2:

```
C1|S3|L1D>show soam mep config
MEP id                   : 320
MD local ID              : 3
MD level                 : 3
MD name                  : OperatorMD
MA local ID              : 3
MA name                  : OperatorSTag100
Direction                : up
Port                     : 2
VLANs                    : stype: 100 1
Primary VLAN             : 100
Admin status             : enabled
CCI status               : enabled
Fault notification state : Defect Reported
Defects                  : RemoteCCM
Next LTM transaction ID  : 1
Next LBM transaction ID  : 1
CCM and LTM priority     : 7
Fault Alarm Detect Time  : 2500 ms
Fault Alarm Reset Time   : 10000 ms
Lowest Alarm priority    : macremerrxcon
```

Show MEP statistics

Syntax: **show soam mep stats** [**mep–id=**<xx> **local–parent–id=**<yy>]

Description: Displays the statistics of one or all SOAM MEP(s). **Note**: An MA/MEG with this MEP ID must have previously been configured.

where:

xx = optional; MEP identifier (1–8191). If omitted, the statistics of all configured MEPs is displayed.

yy = conditional; ID of the local MA or MEG to be associated with the MEP. The valid range is 1-4294967295. This ID parameter must be specified if the optional **mep–id=** is entered.

Example:

```
C1|S3|L1D>show soam mep stats
MEP id                                          : 320
CCMs sent                                       : 80232
CCMs with RDI bit sent                          : 80229
CCMs received                                   : 0
CCMs discarded due to SenderID TLV invalid      : 0
CCMs discarded due to Port Status TLV invalid   : 0
CCMs discarded due to Interface Status TLV invalid : 0
CCMs with sequence errors received              : 0
CCMs with RDI bit received                      : 0
In order LBRs received                          : 0
Out of order LBRs received                      : 0
LBRs with bad msdu received                     : 0
LBRs sent                                       : 0
LTMs received                                   : 0
LTRs received                                   : 0
LTRs sent                                       : 0
LTRs with bad dest MAC discarded                : 0
```

Show CC Database for a MEP

Syntax: **show soam mep cc mep–id=**<xx> **local–parent–id=**<yy>

Description: Displays the CC database for a given SOAM MEP.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MA or MEG associated with the MEP.

Example: C1|S3|L1D>**show soam mep cc mep-id=320 local-parent-id=3**

```
MEP ID                : 320
MD Local ID           : 3
MD level              : 3
MD name               : OperatorMD

Remote MEP ID         : 310
State                 : Failed
TimeStamp             : 7.58 sec
MAC                   : FF:FF:FF:FF:FF:FF
RDI BIT               : False
Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype    : None
Chassis id            :
Manage address domain : 0.0
Manage address        :
Autodetected          : No
```

Note: A MA/MEG with this MEP ID must have previously been configured.

MEP Loopback Commands

Initiate a Loopback Request

Syntax: **send soam mep loopback mep–id=**<vv> **local–parent–id=**<ww> **dest=**<xx> **amount–frames=**<yy> [**data=**<zz>]

Description: Initiates a loopback request for a given SOAM MEP. This command is only available on x323x cards. The multicast loopback request is available only in ITU-T Y.1731 mode.
where:

vv = MEP identifier (1–8191)

ww = ID of the local MA or MEG associated with the MEP (1-4284967295)

xx = type of destination. For a single destination enter either a MAC address or a remote MEP ID. For multiple destinations enter **multicast**.

yy = number of packets to send. For a destination of multicast, only a value of 1 is supported.

zz = optional; data to be transmitted in loopback message

aa = transmission-rate (1-80); allowed for unicast loopback only.

Example:

```
C1|S3|L1D>send soam mep loopback mep-id=10 local-parent-id=1 dest=10 amount-frames=1
Send SOAM Unicast Loopback failed.
Can't read last soam error description
```

Note: A MA/MEG with this MEP ID must have previously been configured.

Show Status of a Loopback Request

Syntax: **show soam mep loopback mep–id=**<xx> **local–parent–id=**<yy> **dest=**<zz>

Description: Displays the status of a loopback request for a given SOAM MEP.
Note: A MA/MEG with this MEP ID must have previously been configured.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MA or MEG associated with the MEP

zz = destination type;

valid choices are:

- **unicast**
- **multicast**

Example:

```
C1|S3|L1D>show soam mep loopback mep-id=10 local-parent-id=1 dest=unicast
C1|S3|L1D>show soam mep loopback mep-id=10 local-parent-id=1 dest=multicast
Remote MEPs MAC addresses list:
First sent LBM sequence number  :   11977
Destination MAC address         :   00-C0-F2-42-00-26
LBMs sent                           :   1000
LBRs received                       :   33
Status                              :   Failed
C1|S3|L1D>
```

MEP Link Trace Commands

Initiate a Linktrace Request

Syntax: **send soam mep linktrace mep–id=**<vv> **local–parent–id=**<ww> **dest=**<xx> **use–fdb–only=**<yy> **ttl=**<zz>

Description: Initiates a linktrace request for a given SOAM MEP. **Note**: a MA/MEG with this MEP ID must have previously been configured.
where:

vv = MEP identifier (1–8191)

ww = ID of the local MA or MEG associated with the MEP

xx = type of destination. Enter either a MEP ID or a MAC address.

yy = indicates whether the linktrace relies only on the forwarding database; valid choices are:

- **true**
- **false**

zz = time to live value for the initial LTM request (0–255)

Example:

```
C1|S5|L1D>send soam mep linktrace mep-id 1 local-parent-id 11 dest 1 use-fdb-only true ttl=25
C1|S5|L1D>
```

Show Status of a Linktrace Request

Syntax: **show soam mep linktrace mep–id=**<xx> **local–parent–id=**<yy> **tid=**<zz>

Description: Displays the status of a linktrace request for a given SOAM MEP.
Note: a MA/MEG with this MEP ID must have previously been configured.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MA or MEG associated with the MEP

zz = Transaction ID (TID) of the initiated link trace to display

Example:
```
C1|S3|L1D>show soam mep linktrace mep-id=10 local-parent-id=1 tid=0
C1|S3|L1D>
```

MEP Frame Loss Measurement Commands

Frame loss measurement is a MEP-to-MEP function. It is performed as part of continuity check messages.

This feature is only supported for MEPs which have a VLAN type of 'none'.

The periodic loss measurement feature is available only in Y.1731 mode.

Note that Frame Loss measurement can be enabled only for point-to-point MEGs (i.e., MEGs with only one peer MEP).

Configure Periodic Loss Measurement

Syntax: **set soam mep lmperiodic mep–id=**<xx> **local–parent–id=**<yy> **state=**<zz>

Description: Configures the SOAM MEP periodic loss measurement for a given MEP with the VLAN type set to 'none'.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MEG associated with the MEP

zz = status of the periodic loss measurement; valid choices are:

- **enable**
- **disable**
- **clearcounters**

Note: The periodic LM function cannot be enabled on a MEP which has the CC function disabled. Entering the **clearcounters** parameter resets the accumulated results for a port, and can be applied only if the LM periodic mode is enabled.

Example:

```
C1|S5|L1D>set soam mep lmperiodic mep-id=1 local-parent-id=11 state=enable
C1|S5|L1D>
```

Note: An MA/MEG with this ID must have previously been configured.

Show Periodic Loss Measurement

Syntax: **show soam mep lmperiodic mep–id=**<xx> **local–parent–id=**<yy> **far–end–mep–id=**<zz>

Description: Displays the periodic loss measurement results for a given SOAM MEP.

where:

xx = MEP identifier (1–8191)

yy = ID of the local parent MEG associated with the MEP (1-4294967295)

zz = far end (remote) MEP ID (1–8191)

Example:

```
C1|S5|L1D>show soam mep lmperiodic mep-id 1 local-parent-id 11 far-end-mep-id 9

Usage: show soam mep lmperiodic [mep-id=<1-8191> local-parent-id=<1-4294967295>
far-end-mep-id=<1-8191>]
C1|S5|L1D>
```

Note: a MA/MEG with this MEP ID must have previously been configured.

MEP Delay Measurement

Frame delay measurement and frame delay variation measurement are executed on demand for a given MEP to MEP pair.

Note: Delay measurement can be enabled only for point-to-point MEGs (i.e., for MEGs with only one peer MEP).

Initiate a Delay Measurement Request

Syntax: **send soam mep dm mep–id=**<vv> **local–parent–id=**<ww> **dest=**xx **period=**<yy> **frame–num=**<zz>

Description: Initiates the delay measurement for a given MEP. **Note**: a MA/MEG with this MEP ID must have previously been configured.

where:

vv = MEP identifier (1–8191)

ww = ID of the local MEG associated with the MEP

xx = MEP ID or MAC address of the destination for which the delay is to be measured

yy = period, in seconds, of the delay measurement; **1s** or **10s**

zz = number (3–32) of frames to be transmitted periodically

Example:

```
C1|S5|L1D>send soam mep dm mep-id 1 local-parent-id 11 dest 1 period 1s frame-num 3
C1|S5|L1D>
```

Note: Only one delay measurement request is supported at a time for a given MEP.

Show Delay Measurement Results

Syntax: **show soam mep dm status mep–id=**<xx> **local–parent–id=**<yy>

Description: Displays the delay measurement results for a given SOAM MEP. **Note**: a MA/MEG with this MEP ID must have previously been configured.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MEG associated with the MEP

Example:

```
C1|S13|L0D/>show soam mep dm status mep-id=2 local-parent-id=2
Local MEP id                        : 2
Remote MEP mac address              : 00-01-02-03-04-05
Status                              : completed
Far end processing                  : Not included
Average round trip delay            : 12.500000 ms
Minimum round trip delay            : 11.100000 ms
Maximum round trip delay            : 9.200000 ms
Average far end processing          : 0.200000 ms
Minimum far end processing          : 0.100000 ms
Maximum far end processing          : 0.300000 ms
Average round trip delay variation : 0.100000 ms
Minimum round trip delay variation : 0.000000 ms
Maximum round trip delay variation : 0.200000 ms
Total DMM frames transmitted        : 182
Total DMR frames received           : 172
C1|S13|L0D
```

MEP ETH-TEST Commands

ETH–TST procedures are applicable only for MEPs configured in Y.1731 mode. The ETH–TST procedures are uni–directional. One MEP is designated as originator, and the far end MEP is the receiver. A test request is requested at the originator, while the result of the procedure is checked at the receiver.

Initiate an ETH–TST Request

Syntax: **send soam mep test mep–id=**<uu> **local–parent–id=**<vv> **dest=**ww **pattern=**<xx> **size=**<yy> **frame–num=**<zz>

Description: Sends an ETH–TST from a local MEP towards a given destination. **Note:** the command will fail if another request is still in progress. **Note**: a MA/MEG with this MEP ID must have previously been configured.

where:

uu = MEP identifier (1–8191)

vv = ID of the local MEG associated with the MEP

ww = MEP ID or MAC address of the destination for which the delay is to be measured

xx = pattern to be used in the message; valid choices are:

- **nullnocrc**
- **nullcrc**
- **prbs231nocrc**
- **prbs231crc**

yy = pattern size, in bytes (0–1467), excluding CRC

zz = number of packets (1–32) to be sent

Example:

```
C1|S5|L1D>send soam mep test mep-id 1 local-parent-id 11 dest 1 pattern nullcrc size=1 frame-
num 2
C1|S5|L1D>
```

Show the Status of the ETH–TST Requests

Syntax: **show soam mep test mep–id=**<xx> **local–parent–id=**<yy>

Description: Displays the status and statistics information regarding the ETH–TST procedures which have been executed on a given MEP. **Note**: a MA/MEG with this MEP ID must have previously been configured.

where:

xx = MEP identifier (1–8191)

yy = ID of the local MEG associated with the MEP

Example:

```
C1|S13|L1D>show soam mep test mep-id=2 local-parent-id=2
ETH-TEST status for MEP            : 2
Transmit status
  Last Transmitted Sequence Number : 4
  Transmit Request State           : Completed
  Transmitted Requests             : 4
Received status
  Last Received Sequence Number    : 0
  Missed Sequence Numbers          : 0
  Valid ETH-TEST frames received   : 0
  Invalid ETH-TEST frames received : 0
  Discarded ETH-TEST frames        : 0
C1|S13|L1D/>
```

Initiate an ETH–MCC Request

Syntax: **send soam mep mcc mep–id=**<vv> **local–parent–id=**<ww> **dest=**<xx> **oui=**<yy> **data=**<zz>

Description: Sends an ETH–MCC from a local MEP towards a given destination. This command provides a maintenance communication channel between a pair of MEPs.
Note: a MA/MEG with this MEP ID must have previously been configured.

where:

vv = MEP identifier (1–8191)

ww = ID of the local MEG associated with the MEP

xx = MEP ID or MAC address for which the message is destined

yy = three bytes in hex representing the Organizationally Unique Identifier (OUI) of the organization defining the format of MCC Data

zz = data to send to the destination

Example:

```
C1|S5|L1D>send soam mep mcc mep-id 1 local-parent-id 11 dest 1 oui 1.3.6.1.4.1 data XXX
C1|S5|L1D>
```

Message: *OUI: It's value must have a correct form like '00.00.00'*

SOAM Maintenance Intermediate Point (MIP) Commands

These commands let you add, remove, set parameters, and display configuration and statistics for the SOAM MIPs (Maintenance Intermediate Points).

Add a MIP

Syntax: **add soam mip mip–type=**<ww> **local–mip–id=**<xx> **local–parent–id=**<yy> **port=**<zz>

Description: Adds a new SOAM MIP to the system. .

where:

ww = MIP type; valid choices are:

- **y.1731**
- **802.1ag**

xx = MIP identifier (1–4294967295).

yy = ID of the local MA or MEG associated with the MEP.

zz = number of the port the MIP will be associated with.

Example:

```
C1|S5|L1D>add soam mip mip-type 802.1ag local-mip-id 1 local-parent-id 11 port 1

Add SOAM MIP failed.
None
C1|S5|L1D>add soam mip mip-type 802.1ag local-mip-id 1 local-parent-id 11 port 1
C1|S5|L1D>add soam mip mip-type 802.1ag local-mip-id 1 local-parent-id 11 port 1
MIP with this id has been configured already.
C1|S5|L1D>
```

Remove a MIP

Syntax: **remove soam mip local–mip–id=**<xx>

Description: Removes an existing SOAM MIP. **Note**: a MIP with this ID must previously been configured.

where:

xx = MIP identifier (1–4294967295)

Example:

```
C1|S5|L1D>remove soam mip ?
  local-mip-id
C1|S3|L1D>remove soam mip local-mip-id ?
  <1-4294967295>
C1|S3|L1D>remove soam mip local-mip-id 2
MIP with this id has not been configured yet.
C1|S3|L1D>remove soam mip local-mip-id 1

C1|S3|L1D>
```

Set MIP Parameters

Syntax: **set soam mip local–mip–id=**<xx> **attr–name=**<yy> **attr–val=**<zz>

Description: Defines the parameters of an existing SOAM MIP.

where:

xx = MIP identifier (1–4294967295)

yy = name of the attribute to be changed (see table below)

zz = new value to be associated with attribute yy (see table below)

If yy equals:	Then zz can be:
admin Admin state of the MIP.	• **up** • **down**
aistransmit Status of the AIS transmission (Y.1731 only).	• **enable** • **disable**
aisinterval The AIS transmission interval (Y.1731 only).	• **1min** • **1s**
aisframepriority The AIS frame priority (Y.1731 only).	0–7

Example:

```
C1|S5|L1D>set soam mip local-mip-id=1 attr-name=admin attr-val=up aistransmit=enable
aisinterval=1s aisframepriority=4

login: ION
Password:xxxxxxx

Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C1|S7|L1D>
```

Show MIP Configuration

Syntax: **show soam mip config** [**local–mip–id=**<xx>]

Description: Displays details of an existing SOAM MIP.

where:

xx = optional; MIP identifier (1–4294967295). If omitted, a list of all configured MIPs is displayed.

Example 1:

```
C1|S3|L1D>show soam mip config
MIP id             : 33
MEG local ID       : 300
MEG level          : 3
MEG name           : OperCTag300Y
VLANs              : ctype: 300 600
Port               : 1
Admin status       : disabled
AIS transmit       : enabled
AIS interval       : 1 second
AIS frame priority : 0

MIP id             : 63
MEG local ID       : 600
MEG level          : 6
MEG name           : ProvCTag600Y
VLANs              : ctype: 600 300
Port               : 1
Admin status       : disabled
AIS transmit       : enabled
AIS interval       : 1 second
AIS frame priority : 0
C1|S3|L1D>
```

Note: a MIP table entry must previously been configured. If none are configured, the message "*The MIPs table is empty*." displays.

Example 2:

```
C1|S3|L1D>show soam mip config
MIP id             : 312
MD local ID        : 3
MD level           : 3
MD name            : OperatorMD
VLANs              : stype: 100 1
Port               : 1
Admin status       : enabled
MIP id             : 612
MD local ID        : 6
```

```
MD level           : 6
MD name            : ProviderMD
VLANs              : ctype: 200 2
Port               : 2
Admin status       : enabled
C1|S3|L1D>
```

Show MIP Statistics

Syntax: **show soam mip stats** [**local–mip–id=**<xx>]

Description: Displays the statistics for an existing SOAM MIP.

where:

xx = optional; MIP identifier (1–4294967295). If omitted, the statistics of all configured MIPs is displayed.

Example:

```
C1|S3|L1D>show soam mip stats
MIP id  : 312
LBM In  : 0
LBR Out : 0
LTM In  : 0
LTM Out : 0
LTR Out : 0

MIP id  : 612
LBM In  : 0
LBR Out : 0
LTM In  : 0
LTM Out : 0
LTR Out : 0
```

Note: a MIP table entry must previously been configured. If none are configured, the message "*The MIPs table is empty.*" displays.

29. SSH Commands

The SSH (Secure Shell) protocol allows data to be exchanged using a secure channel between two networked devices.

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

The following commands are used for SSH operations.

Generate SSH Host Key

Syntax: **generate ssh host–key**={dsa | rsa | both}

Description: Defines the type of host key to be generated.

Example:
```
C1|S3|L1D>generate ssh host-key=both
Processing...
Processing...
Processing...
Processing...
Processing...
Processing...
Host-key generated!
```

Remove SSH Host Key

Syntax: **remove ssh host–key**={dsa | rsa | both}

Description: Removes the specified host key for the secure shell.

Example:
```
C1|S3|L1D>remove ssh ?
  host-key
  public-key
C1|S3|L1D>remove ssh host-key ?
  both
  dsa
  rsa
C1|S3|L1D>remove ssh host-key=dsa
C1|S3|L1D>
```

Remove SSH Public Key from a User

Syntax: **remove ssh public–key user=**<xx> **type**={dsa | rsa | both}

Description: Removes the public-key from a specified user.

Example:
```
C1|S3|L1D>remove ssh public-key user=guest type=dsa
C1|S3|L1D>
```

Set SSH Authentication Retry

Syntax: **set ssh auth–retry=**<xx>

Description: Defines the number of times (1–5) that a user can retry a failed authentication, such as trying to correct a wrong password. The SSH server terminates the connection when the limit is exceeded.

Example:
```
C1|S3|L1D>set ssh auth-retry ?
  <1-5>
C1|S3|L1D>set ssh auth-retry 3
C1|S3|L1D>
```

Note: The SSH server state must be enabled before this command has an affect.

Set SSH Public Key to a User

Syntax: **set ssh public–key user=**<xx> **type**={dsa | rsa} **file=**<yy>

Description: Sets the public key to a user from a key file. This file should first be obtained by doing either a TFTP or FTP **get** command.

where:

xx = user name used to log in to SSH

yy = name of the file that contains the public key

Example:
```
C1|S3|L1D>set ssh public-key user=1 type=dsa file=certfile
Invalid user!
C1|S3|L1D>set ssh public-key user=root type=dsa file=certfile
Set SSH public key failed.

C1|S3|L1D>set ssh server state=enable
C1|S3|L1D>set ssh public-key user=root type=dsa file=certfile
C1|S3|L1D
```

Set SSH Server State

Syntax: **set ssh server state**={enable | disable}

Description: Enables or disables the Secure Shell (SSH) server state.

Example:

```
C1|S3|L1D>set ssh public-key user root type dsa file certfile
Set SSH public key failed.
C1|S3|L1D>set ssh server state ?
  disable
  enable
C1|S3|L1D>set ssh server state=enable
C1|S3|L1D>set ssh public-key user=root type=dsa file=certfile
C1|S3|L1D>
```

Set SSH Timeout

Syntax: **set ssh client timeout=**<xx>

Description: Defines the maximum number of seconds (1–120) that protocol negotiation, including user authentication, can take before the SSH server terminates the connection.

Example:

```
C1|S3|L1D>set ssh client timeout ?
  <1-120>
C1|S3|L1D>set ssh client timeout=15
Fail to set SSH client timeout!
C1|S3|L1D>set ssh server ?
  state
C1|S3|L1D>set ssh server state ?
  disable
  enable
C1|S3|L1D>set ssh server state disable
C1|S3|L1D>set ssh client timeout 15
C1|S3|L1D>
```

Note: The SSH server state must be enabled before this command has an affect.

Show SSH Configuration

Syntax: **show ssh config**

Description: Displays the current configuration of the secure shell.

Example:

```
C1|S3|L1D>show ssh config
Secure Shell configuration:
---------------------------------------------------------------
Secure shell server state:                                disable
Secure shell major version:                                 2
Secure shell minor version:                                 0
Secure shell time out:                                      60
Secure shell authentication retries:                        3
C1|S3|L1D>
```

Show SSH Public Key of a User

Syntax: **show ssh public–key user=**<xx>

Description: Displays the secure shell public key of a specified user.

Example:

```
C1|S13|L1D/>show ssh public-key user=root
RSA public key:
00 00 00 00 00 00 00 00 00 00
DSA public key:
00 00 00 00 00 00 00 00 00 00
C1|S13|L1D/>
```

Show SSH Host Key

Syntax: **show ssh host–key**

Description: Displays both the DSA and RSA host keys that were generated via the **generate ssh host–key**= command.

Example:

```
Host-key generated!
C1|S3|L1D>show ssh ?
  config
  host-key
  public-key
C1|S3|L1D>show ssh host-key
RSA host key:
00 00 00 07 73 73 68 2d 72 73 61 00 00 00 03 01 00 01 00 00 00 83 00 91 bd c1 d5
 9a 01 16 5c 60 33 3b 18 db bf d4 d8 b2 cc 71 3e f7 8a 0e 80 26 b0 c1 a0 09 83 3
7 98 75 17 a9 41 bf 52 6b f1 33 5a 35 17 a2 4f 04 1d d9 b8 30 9f 4b 83 03 ef 6c
39 e0 c8 37 19 ed 9b 63 6b 90 60 05 27 68 89 49 07 b7 85 64 cb 5a 27 c7 a9 1e b4
 ed f4 42 b9 1e 37 88 9b 9b ad 98 64 b1 dd c1 5f 05 2f ac 91 c6 b5 94 0b 54 85 c
5 47 2e 71 26 0c 31 4c 78 14 2f bb f2 ad be a1 44 8e 9b a1 00 00 00 82 17 82 47
ff 98 29 7f bd 63 e9 2f a9 b9 5c ce cd 2b be 4d b0 2e 06 ef 82 dd 7a da a8 e1 8f
 f0 8a 5f ac f2 e8 ff 9f 20 79 56 62 c1 38 b0 3e 55 b8 28 f4 0c a7 cd 6a f3 5a 0
e 17 a1 fa 39 e5 2d 4e 48 b2 f6 02 ef 94 6b 2a ea 0e d4 d1 b4 01 b9 dc b0 c6 f7
8d e3 0c c7 14 86 92 15 94 1d 64 4c a1 97 28 c5 79 6d b7 2c 90 24 5d 47 28 81 f2
 5c 67 b4 f4 cf bd e8 3a 6b 5c 4e 91 fc 8f 29 94 7a c7 85 27 00 00 00 42 00 da e
0 6e 0f ee 78 a1 a3 f9 41 15 b0 9e 30 4d b0 71 dd 62 91 60 f8 c6 d3 43 04 dc 18
73 4f 22 7b c3 de 3a db e4 86 90 d0 2a 46 32 4d 19 a2 28 65 ab 2f f6 c5 fa 84 da
 65 ef 4d 3a 93 5e 4a 27 70 bb 00 00 00 42 00 aa 75 ce 0e 2e 3a 46 c2 8b b2 ed 5
d 78 f9 9a 7b dd b5 51 f5 a4 1a 8f 76 a3 63 22 e8 7a 21 98 6c f1 14 7a 03 c4 ae
9c 68 5c 8d f0 d4 b1 66 10 5a d8 15 09 e1 88 f4 68 26 ce 5f e5 d4 20 fb 71 bd 53

DSA host key:
00 00 00 07 73 73 68 2d 64 73 73 00 00 00 81 00 f7 a6 f5 42 a6 0c cb b7 1b 83 e4
 c8 98 d4 49 c1 22 83 db 33 7b 36 8a 33 7f a2 73 34 1b cd 72 33 cd 45 b4 28 8f 5
7 c1 f9 a3 e5 11 48 ef fa ce 52 c3 6f 39 24 2e 21 d1 69 7e 0f 8e e2 ef 33 47 7a
76 8c 75 37 a1 15 b5 86 af af 8f 1f fa 7d 1a a5 ba b5 76 01 6f 23 f6 d9 f7 c3 a3
 64 0c 1b 9b 5e 03 ae 6f f0 f3 43 6b b8 bc fe 3d 4a 6f 35 24 8c 23 41 06 25 81 0
d 6e 20 9a d1 3a cb 46 ea ff c3 00 00 00 15 00 b1 33 d1 9f 61 8b 8c f3 6f 5d 49
4f 73 25 80 3f 6a d9 c5 9d 00 00 00 81 00 ed a1 75 26 55 2e d0 b3 3c a3 b3 4d 33
 d3 f0 3c 5f cd 7c ed 54 26 a7 9e 45 eb 27 4b 32 a6 de 3e 22 94 9d ca 4a a4 2b 5
8 6b a9 52 a8 ba 37 0a 7a ca 7b 62 1b 85 2b 86 dc 01 af 40 f1 ab b3 8a 3f 38 e2
0a 2d 86 9a 97 e4 27 0b b4 fa aa 34 b1 71 2b 5f a3 66 03 56 49 cb 1f 30 8f 17 99
 32 e7 84 48 77 cd db 4f 35 41 30 ff 09 9e b9 30 1c ec ef 4f 26 41 35 c0 3c 89 0
7 91 a2 65 8e 1b 9a c9 86 00 00 00 81 00 ea f3 2d 22 bf 53 a3 84 c9 24 bc 45 07
b0 3d 86 93 d0 82 31 41 7b 38 d5 f4 e7 3e 84 98 47 11 c9 f2 55 eb c8 85 19 b2 2c
 cf d2 92 94 3a 52 40 75 81 a4 ca f3 3a ed 31 30 dc 98 ac 30 d6 9e 90 64 be 81 8
a 24 7d b6 94 47 e3 98 84 15 51 ef ef 9a ae 66 27 2b f8 8f 56 0e ad e0 fd 20 dc
06 be 15 e2 b7 da c3 74 2a 7c c4 2b 15 ff 80 ad dd d4 60 66 e7 31 c6 42 8e d3 78
 75 04 38 01 dc da bc 0e 00 00 00 14 59 73 2e 18 63 71 73 c7 84 1e 6d ca 05 6d d
1 44 15 4c e6 94
C1|S3|L1D>
```

30. System Logging (Syslog) Commands

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.

Syslog messages refer to a facility (auth, authpriv, daemon, cron, ftp, lpr, kern, subagent, bpd_linux, syslog, user, uucp, local0 - local7) that are assigned a priority/level (Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug) by the sender of the message. Configuration allows directing messages to various local devices (console), files, ports, or remote syslog daemons. **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.

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. See the related ION NID User Guide for more information.

Note that the syslog protocol does not provide for acknowledgment of message delivery.

Set Syslog Configuration

Command: **set syslog**

Description: Device level commands used to define Syslog operations (the Syslog server address and port, and Syslog level and mode). When **syslog svr type=ipv4**, enter an IP address, like 192.168.0.2; when **syslog svr type=dns**, enter a hostname, like www.transition.com. The default is **set syslog mode=off**.

Syntax:
set syslog svr port=<1-65535>
set syslog svr type=<ipv4|ipv6|dns>
set syslog mode=(local|remote|localAndRemote|off)
set syslog level=(emerg|alert|crit|err|warning|notice|info|debug)
set syslog svr type=(ipv4|dns) addr=SYSLOG_SVR_ADDR

Example:
```
C1|S1|L1D>set syslog svr type=ipv4 addr=192.168.1.30
C1|S1|L1D>set syslog svr port=667
C1|S3|L1D>set syslog set syslog level=err
C1|S3|L1D>set syslog set syslog mode=LocalandRemote
C1|S3|L1D>
```

Defaults:

Syslog Server Address default:	**192.168.0.2**
Server Port default: port #	**514**
Level default:	**Notice**
Mode default:	**Log local**

Note : The **set syslog svr type** command accepts an IPv4, IPv6, or DNS Syslog server type. Use the Linux commands "**cd /var/log**" and "**cat sys.log**" to view the log.

Example:

```
Agent III C1|S1|L1D>show syslog config
Syslog server address type:             dns
Syslog server address:                  0.0.0.0
Syslog server port:                     1
Syslog level:                           notice
Syslog mode:                            local
Agent III C1|S1|L1D>set syslog svr type=ipv4 addr=192.168.1.30
Agent III C1|S1|L1D>set syslog svr type=ipv6 addr=fe80::2c0:f2ff:fe20:de9e
Agent III C1|S1|L1D>show syslog config
Syslog server address type:             ipv6
Syslog server address:                  fe80::2c0:f2ff:fe20:de9e
Syslog server port:                     1
Syslog level:                           notice
Syslog mode:                            local
Agent III C1|S1|L1D>
```

```
Agent III C1|S9|L1D>cd /var/log
Agent III C1|S9|L1D>cat sys.log
Dec 31 19:00:35 (none) user.notice syslog: attach platform info in shared memory
 at 0x40006000
Dec 31 19:00:39 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsa
p 10 is released already.
Dec 31 19:00:39 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsa
p 15 is released already.
Dec 31 19:00:39 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsa
p 11 is released already.
Dec 31 19:00:41 (none) daemon.warn ION-EM[742]: Warning: Failed to connect to th
e agentx master agent ([NIL]):
Dec 31 19:00:41 (none) daemon.notice ION-EM[742]: attach platform info in shared
 memory at 0x40006000
Dec 31 19:00:41 (none) daemon.notice ION-EM[742]: Entity Manager running in Mast
er Mode
Dec 31 19:00:43 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsa
p 8 is released already.
Dec 31 19:00:43 (none) user.notice subagent[744]: subAgent Started.
Dec 31 19:00:44 (none) user.notice subagent[744]: attach platform info in shared
 memory at 0x40006000
Dec 31 18:20:19 (none) user.notice syslog: attach platform info in shared memory
 at 0x40006000
Agent III C1|S9|L1D>
```

Parameter Descriptions:

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. The enumeration values are equal to the values that syslog uses + 1; a messages with a severity level lower than or equal to this level will be logged.

Emergency	Emergency; system is unusable (most critical)
Alert	Action must be taken immediately
Critical	A critical condition exists
Error	Error condition

Warning	Warning condition
Notice	Normal but significant condition (the default setting)
Info	Informational message
Debug	Debug-level messages (least critical)

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.

Show Syslog Configuration

Command: **show syslog config**

Description: Device level command to display the current Syslog configuration, including the Syslog server address and port, and the Syslog level and mode.

Syntax: **show syslog config** <cr>

Example:

```
C1|S8|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
C1|S8|L1D>
```

Clear Syslog Records

Syntax: **clear syslog**

Description: Device level command to erase all existing records on the configured Syslog server.

Example 1:

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

Messages:
Error: this command should be executed on a device!
System is busy, please retry this command later!
Syslog is not supported on this card! (only available in FBRM card)

Example 2:

```
Agent III C1|S1|L1D>cd /var/log
Agent III C1|S1|L1D>cat sys.log
Dec 31 19:00:36 (none) user.notice syslog: attach platform info in shared memory at 0x40006000
Dec 31 19:00:39 (none) local5.notice bpd_linux[734]: BPD Started.
Dec 31 19:00:44 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 14 is released already.
Dec 31 19:00:44 (none) daemon.warn ION-EM[742]: Warning: Failed to connect to the agentx master agent
([NIL]):
Dec 31 19:00:44 (none) daemon.notice ION-EM[742]: attach platform info in shared memory at 0x40006000
Dec 31 19:00:44 (none) daemon.notice ION-EM[742]: Entity Manager running in Master Mode
Dec 31 19:00:45 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 13 is released already.
Dec 31 19:00:45 (none) user.notice subagent[744]: subAgent Started.
Dec 31 19:00:45 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 8 is released already.
Dec 31 19:00:46 (none) user.notice subagent[744]: attach platform info in shared memory at 0x40006000
Dec 31 19:00:47 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 10 is released already.
Dec 31 19:00:47 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 11 is released already.
Dec 31 19:00:47 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 9 is released already.
Dec 31 19:00:48 (none) daemon.err snmpd[733]: attach old snmp configuration in shared memory at 0x40006000
Dec 31 19:00:48 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 12 is released already.
Dec 31 19:00:48 (none) daemon.notice ION-EM[742]: Discovered Chassis: 1
Dec 31 19:00:48 (none) user.notice upgradeManager[723]: location = 134217728
Dec 31 19:00:48 (none) user.notice upgradeManager[723]: just reply OK ...
Dec 31 19:00:48 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 7 is released already.
Dec 31 18:00:48 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[11], relpos-[1]
Dec 31 18:00:48 (none) user.notice upgradeManager[723]: location = 181403648
Dec 31 18:00:48 (none) user.notice upgradeManager[723]: just reply OK ...
Dec 31 18:00:49 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 12 is released already.
Dec 31 18:00:49 (none) daemon.notice syslog[793]: attach platform info in shared memory at 0x40006000
Dec 31 18:00:49 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[5], relpos-[1]
Dec 31 18:00:49 (none) user.notice upgradeManager[723]: location = 156237824
Dec 31 18:00:49 (none) user.notice upgradeManager[723]: just reply OK ...
Dec 31 18:00:49 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 8 is released already.
Dec 31 18:00:49 (none) local5.err bpd_linux[734]: BPD ERROR: the application dsap 7 is released already.
Dec 31 18:00:49 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[14], relpos-[1]
Dec 31 18:00:49 (none) user.notice upgradeManager[723]: location = 193986560
Dec 31 18:00:49 (none) user.notice upgradeManager[723]: just reply OK ...
Dec 31 18:00:49 (none) syslog.notice xxdp: attach platform info in shared memory at 0x40006000
Dec 31 18:00:49 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[1], relpos-[1]
Dec 31 18:00:49 (none) user.notice upgradeManager[723]: location = 139460608
Dec 31 18:00:49 (none) user.notice upgradeManager[723]: It is AGENT card itself!

Agent III C1|S1|L1D>clear syslog
Agent III C1|S9|L1D>cat sys.log

Agent III C1|S9|L1D>
```

31. TACACS+ Commands

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).

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.

The TACACS+ commands for an IONMM or a standalone SIC are described below.

Set TACACS+ Client State

Command: **Set TACACS+ Client State**

Syntax: **set tacplus client state**=(enable|disable)

Description: Device level command used to enable or disable logging in to the ION system using TACPLUS (TACACS+). Execute this command on an IONMM or a standalone SIC only.

where:

enable = the TACACS+ client is enabled and logging in to the ION system via TACACS+ is required.

disable = the TACACS+ client is disabled and logging in to the ION system.

Example:

```
Agent III C1|S1|L1D>set tacplus client state ?
  disable
  enable
Agent III C1|S1|L1D>set tacplus client state enable
Agent III C1|S1|L1D>show tacplus config
TACPLUS client state:         enable

 TACPLUS authentication server:
index   type    addr                                retry  timeout
-------------------------------------------------------------------
1       dns     0.0.0.0                             3      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>
```

Messages:
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!"
Error: The parameter is wrong!
Fail to set TACPLUS client state!

Set TACACS+ Server Retry Value

Command: **Set TACPLUS Server Retry Value**

Syntax: **set tacplus svr**=<1-6> **retry**=<1-5>

Description: Device level command to define the TACACS+ server index number and retries parameter.

Make sure the command is entered on an IONMM or a standalone SIC.

where:

svr = a configured TACACS+ server in the range of 1-6.

retry = the number of attempts to connect to this server, in the range of 1-5 retries. Resend the connect request this many times before trying to connect to the next TACACS server.

Example:
```
Agent III C1|S1|L1D>set tacplus svr=1 retry=3
Agent III C1|S1|L1D>
```

Messages:
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Please input a digital number to specify radius server index!
Please input a digital number to specify RADIUS server retry!
TACPLUS authentication server index is out of range!

Set TACACS+ Server Timeout Value

Command: **Set TACPLUS Server Timeout Value**

Syntax: **set tacplus svr**=<1-6> **timeout**=<1-60>

Description: Device level command to define the amount of time (in seconds) to wait for a reply from a TACACS+ server before trying the next server. Make sure the command is entered on an IONMM or a standalone SIC.

where:

svr = a configured TACACS+ server in the range of 1-6.

timeout = the amount of time (in seconds) to wait for a reply from a TACACS server before trying another server.

Example:

```
Agent III C1|S1|L1D>set tacplus svr=1 timeout 25
Agent III C1|S1|L1D>
```

Messages:

Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Fail to set TACPLUS server time out!
Please input a digital number to specify tacplus server index!
Please input a digital number to specify tacplus server time out!
TACPLUS authentication server index is out of range!
TACPLUS server time out is out of range!

Set TACACS+ Server Secret

Command: **Set TACPLUS Server Secret**

Syntax: **set tacplus svr**=<1-6> **secret**=SECRET

Description: Device level command to define a specific TACACS+ server's secret (password). This is a string well known to both client and server and is used to validate and/or encrypt data, transmitted between them.
Make sure this command is entered on an IONMM or a standalone SIC.

where:

svr = a configured TACACS+ server in the range of 1-6.

secret = the TACACS+ AAA password to connect with a TACACS server. Alpha, numeric, and special characters are allowed. Do not enter any space characters.

User Level: Admin user login user level required.

Example:
```
Agent III C1|S1|L1D>set tacplus svr=1 secret=123about time
% Unknown command.
Agent III C1|S1|L1D>set tacplus svr=1 secret=123abouttime
Agent III C1|S1|L1D>
```

Note: After refreshing the page, all shared secrets will be "********". This is by design for most types of password applications. This is also caused by adding letters after the "*" after refreshing the page. After a refresh, just '********' is returned instead of the actual password which was entered previously. So after refresh, any characters added following the previous password (actually is '********' now), the '********' and added characters will be saved.

Messages:

Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Please input a digital number to specify TACPLUS server index!
Set TACPLUS server secret
TACPLUS authentication server index is out of range!
The TACPLUS authentication server specified does not exist!

Set TACACS+ Server Values

Command: **Set a TACPLUS Server / Type / Address / values**

Syntax: **set tacplus svr**=<1-6> **type**=(ipv4 |ipv6|dns) **timeout**=(1-60) **retry** (1-5)

Description: Device level command to define a specific TACACS+ server in terms of its server IP addressing method, number of retries, and timeout value. The TACACS server must be up and running and configured properly. Make sure the command is excecuted on IONMM or a standalone SIC.

where:

svr = TACACS+ server index number (1-6). A configured TACACS+ server in the range of 1-6.

svr-type = The TACACS+ Server address type (ipv4 |ipv6|dns).

type = the TACACS+ server's IPv4, IPv6 or DNS address, in the correct syntax for the type of addressing used.

timeout = the amount of time (1-60 seconds) to wait for a reply from a TACACS server before trying another server.

retry = the number of attempts to connect to this server, in the range of 1-5 retries (optional). Resend the connect request this many times before trying the next TACACS server.

Example:

```
Agent III C1|S1|L1D>set tacplus svr 1 type ipv4 addr 192.168.1.30 1
Wrong parameter number!
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 Buffrey
Agent III C1|S1|L1D>set tacplus svr 1 timeout 30
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 ?
  [retry
Agent III C1|S1|L1D>set tacplus svr 1 type ipv6 addr fe80::2c0:f2ff:fe21:b100
Agent III C1|S1|L1D>
```

Messages:

Error: this command should be executed on a device!

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

Fail to set Tacplus server address type!

Invalid TACPLUS server address!

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!

Show TACACS+ Configuration

Command: **Show TACPLUS Configuration**

Syntax: **show tacplus config**

Description: Displays the current TACACS+ configuration for an IONMM or a standalone SIC. Make sure the command is executed on IONMM or a standalone SIC.

Example:

```
Agent III C1|S1|L1D>set tacplus svr 1 retry 2
Agent III C1|S1|L1D>set tacplus svr 1 secret terces11
Agent III C1|S1|L1D>set tacplus svr 1 timeout
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 ipv4 addr 192.168.1.30
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    ::                                                      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>set tacplus svr 2 type ipv6 addr fe80::2c0:f2ff:fe21:b24c
retry=3 timeout=10
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|L1D>
```

Messages:
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!")
Getting TACPLUS server fail
Invalid IP address!
When you hit **Save** after any TACACS+ re-configuration, a re-login is required; the message "*The TAC-ACS+ settings have been changed and a re-login will be performed right now.*"

Set Login Method

Command: **Set Login Method**

Syntax: set login method=(local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal)

Description: Sets 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):

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.

Example:

```
Agent III C1|S1|L1D>set login method ?
  local
  radiuslocal
  radiustacpluslocal
  tacpluslocal
  tacplusradiuslocal
Agent III C1|S1|L1D>set login method radiustacpluslocal
Agent III C1|S1|L1D>set login method local
Agent III C1|S1|L1D>
```

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

TACACS+ Messages

Error: The parameter is wrong!
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!"
Fail to get system user name!
Fail to set TACPLUS client state!
Fail to set Tacplus server address type!
Fail to set TACPLUS server address!
Fail to set TACPLUS server retry
Fail to set TACPLUS server time out!
Fail to set TACPLUS server row status!
Fail to set TACPLUS server time out!
Getting TACPLUS server fail
Invalid TACPLUS server address!
Please input a digital number to specify radius server index!
Please input a digital number to specify RADIUS server retry!
Please input a digital number to specify tacplus server time out!
Please input a digital number to specify TACPLUS server retry!
Please input a digital number to specify TACPLUS server time out!
Please input a digital number to specify tacplus server index!
Please input a digital number to specify TACPLUS server index!
Please input a number to specify the TACPLUS server index!
Set TACPLUS server secret
TACPLUS authentication server index is out of range!
TACPLUS server retry is out of range!
TACPLUS server time out is out of range!
The ipv6 address is multicast address
The TACPLUS authentication server specified does not exist!
Wrong parameter number!

Meaning: You entered a TACACS+ (Tacplus) command, but the command was unsuccessful.
Recovery: 1. Make sure you enter the TACACS+ command on an IONMM or a standalone SIC at the device level.
2. Make sure the TACACS+ client is enabled and that the TACACS+ server is correctly configured and running.
3. Make sure you enter the command parameters within the valid ranges and in the proper syntax. See "TACACS+ Commands".
4. Check the RADIUS configuration.
5. Retry the command. See the related manual or section.
6. Check your third party TACACS+ server documentation and helps (e.g., ClearBox Server, etc.).
7. If the problem persists, contact Technical Support.

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"

32. TNDP Commands

TNDP (TN Topology Discovery Protocol) is the Lantronix' implementation of LLDP. When the TNDP TX state is set to Enabled, the device entering this command will no longer be discovered by the IONMM if it is remotely managed through this port.

Set TNDP (TN Topology Discovery Protocol) State

Command: **set tndp tx state**=<enable|disable>

Description: Port level command to enable or disable the TN topology discovery protocol on a port. This is TN's LLDP implementation. 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.

Syntax: **set tndp tx state**=<enable|disable><cr>

Example:

```
C1|S3|L1P2>set tndp tx state=enable
C1|S3|L1P2>
```

Show TNDP (TN Topology Discovery Protocol) State

Command: **show tndp tx state**

Description: 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.
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.

Syntax: **show tndp tx state** <cr>

Example:

```
C1|S3|L1D>set tndp tx state ?
  disable
  enable
C1|S3|L1D>show tndp tx state
Error: this command should be executed on a port!
C1|S3|L1D>go l1p=1
C1|S3|L1P1>show tndp tx state
TNDP Tx state:                          enable
C1|S3|L1P1>go l1p=2
C1|S3|L1P2>show tndp tx state
TNDP Tx state:                          enable
C1|S3|L1P2>
```

33. TFTP Transfer / Upgrade Commands

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

The Trivial File Transfer Protocol (TFTP) can be used to transfer files between the IONMM or a standalone local NID and a TFTP server. These commands are available to an Admin level login user only.

Note: A TFTP server must be online, configured and operational. **Note**: starting at v 1.3.10, Backup file name and TFTP upload/download file name are extended to maximum 128 characters.

The following commands are used for TFTP operations.

TFTP Get

Command: **TFTP Get**

Syntax: **tftp get iptype**=(ipv4|ipv6|dns) **ipaddr**=ADDR **remotefile**=**RFILE** [localfile=LFILE]

Description: This command gets (downloads) a file from a TFTP server, where:

iptype = the type of IP addressing to be used (IPv4, IPv6, or DNS).

ipaddr = the TFTP server's IPv4 or IPv6 address. This TFTP server must be configured and running.

remotefile = the name of the remote file to be transferred with a ***.bin*** suffix.

localfile = the name of the local file when transferred (optional) with a ***.bin*** suffix.

Example:

```
Agent III C1|S1|L1D>tftp get iptype ?
  ipv4
  ipv6
  dns
Agent III C1|S1|L1D>tftp get iptype ipv4 ipaddr 192.168.1.30 remotefile
x323x_0.8.5_AP.bin
TFTP transferring...
Agent III C1|S1|L1D>

Usage: tftp get iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE [lo-
calfile=LFILE]
```

Example:

```
C1|S3|L1D>tftp get iptype=ipv4 ipaddr=192.168.1.30 remotefile=cert localfile=cert
TFTP transferring...

File transfer successful!
```

TFTP Put

Command: **TFTP Put**

Syntax: **tftp put iptype**=(ipv4|ipv6|dns) **ipaddr**=ADDR **localfile**=LFILE [**remotefile**=RFILE]

Description: This command puts (uploads) a file to a TFTP server. This server must be configured and running, where:

iptype = the type of IP addressing to be used (IPv4,IPv6, or DNS).

ipaddr = the TFTP server's IPv4 or IPv6 address. This TFTP server must be configured and running.

remotefile = the name of the remote file to be transferred with a ***.bin*** suffix.

localfile = the name of the local file when transferred (optional).

Example:

```
Agent III C1|S1|L1D>tftp put iptype ipv4 ipaddr 192.168.1.30 localfile
x323x_0.8.5_AP.bin
TFTP transferring...

Fail to transfer the file!
Agent III C1|S1|L1D>tftp put iptype ipv6 ipaddr fe80::2c0:f2ff:fe20:de9e localfile
IONMM_0.8.5_AP.bin
TFTP transferring...

Fail to transfer the file!
Agent III C1|S1|L1D>
```

TFTP Upgrade

Command: **TFTP Update**

Syntax: **tftp upgrade iptype**=(ipv4|ipv6|dns) **ipaddr**=ADDR **remotefile**=RFILE

Description: This command gets (downloads) a file from a TFTP server. The TFTP server must be configured and running, where:

iptype = the type of IP addressing to be used (IPv4,IPv6, or DNS).

ipaddr = the TFTP server's IP address. This server must be configured and running.

remotefile = the name of the remote file to be transferred with a ***.bin*** suffix.

Example:

```
Agent III C1|S1|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remotefile
IONMM_0.8.5_AP
Processing...
TFTP transfer failed!
Agent III C1|S1|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remote-
file IONMM_0.8.5_AP.bin
Processing...
TFTP upgrade succeeded!
Agent III C1|S1|L1D>
```

Prov Get TFTP Server Address

Command: **Set TFTP Server**

Syntax: **prov set tftp svr type**=(ipv4|ipv6|dns) **addr**=ADDR

Description: This command sets the current TFTP server type and address, where:

type = the type of IP addressing (IPv4, IPv6 or DNS).

addr = the TFTP server's IP address (IPv4, IPv6 or DNS server address).

Mode: Global mode

Example:
```
Agent III C1|S1|L1D>prov set tftp svr type ipv4 addr 192.168.1.30
Agent III C1|S1|L1D>
```

Prov Set TFTP Server Type

Syntax: **prov set tftp svr type**=(ipv4|ipv6}dns) **addr**=ADDR

Description: Provision the TFTP Server type and address. Available to an Admin level login user only.

where:

x = type = (ipv4|ipv6|dns)
y = addr = ADDR

Example:
```
Agent III C1|S1|L1P1>prov set tftp svr type ?
  ipv4
  ipv6
  dns
Agent III C1|S1|L1P1>prov set tftp svr type ipv4 addr 192.168.1.10
Agent III C1|S1|L1P1>prov set tftp svr type ipv6 addr e80::2c0:f2ff:fe20:de9e
Agent III C1|S1|L1P1>
```

34. Upgrade / Update Firmware Commands

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Show Firmware Database Update Results

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

Description: Displays the results of the "Update Firmware Database" command (whether the update was successful). If the firmware update failed, this command will display the reason. This command must be entered from the IONMM card.

Example 1:

```
C1|S7|L1D>show firmware-db update result
Database file name:           db.idx
Database update result:       failure
Database update fail reason:  invalid input file
C1|S7|L1D>
```

Example 2:

```
C1|S7|L1D>show firmware-db update result
Database file name:           x323x.bin.1.0.5
Database update result:       success
C1|S7|L1D>
```

Example 3:

```
C1|S7|L1D>show firmware-db update result
Database file name:           db.idx.zip
Database update result:       success
C1|S7|L1D>
```

Example 4:

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

Show Firmware Upgrade Results

Syntax: **show firmware upgrade result**

Description: Displays the results of the most recent "**upgrade module**" command (in progress, success, failure, etc.). If the result is "failure", a reason is provided, such as 'no firmware' at a newer version is available.
If the firmware upgrade was successful, the *time started* and *time completed* display.
This **show firmware upgrade result** command can only be entered on the IONMM by an Admin level login user.

Example 1 (5 modules successfully updated):

```
C1|S7|L1D>show firmware upgrade result
index module                status   reason  time started    time completed
-------------------------------------------------------------------------
1     C3230-1040 c=1 s=3 l1d  success                     00:51:15        00:54:16
2     C3230-1040 c=1 s=5 l1d  success                     00:51:15        00:54:06
3     C3231-1040 c=1 s=10 l1d success                     00:51:15        00:56:50
4     C2220-1014 c=1 s=16 l1d success                     00:51:15        00:55:59
5     C3220-1040 c=1 s=18 l1d success                     00:51:15        00:54:09
6                                                         00:00:00        00:00:00
7                                                         00:00:00        00:00:00
8                                                         00:00:00        00:00:00
C1|S7|L1D>
```

Example 2 (7 modules successfully updated, 1 failed):

```
C1|S7|L1D>show firmware upgrade result
index     module                    status      reason           time started  time completed
-------------------------------------------------------------------------------------------
1         C3230-1040 c=1 s=3 l1d    success                      00:22:39       00:25:54
2         C3230-1040 c=1 s=5 l1d    success                      00:22:39       00:28:33
3         card registering...       success                      00:22:39       00:25:41
4         C3231-1040 c=1 s=10 l1d   success                      00:22:39       00:26:05
5         C2210-1013 c=1 s=13 l1d   failure   no firmware        00:22:39       00:22:39
6         C2220-1014 c=1 s=16 l1d   success                      00:22:39       00:25:28
7         C3220-1040 c=1 s=18 l1d   success                      00:22:39       00:26:28
8         IONPS-A c=1 s=22 l1d      success                      00:22:39       00:22:46
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 "Appendix C: CLI Messages and Recovery" for error messages and recovery procedures.

Show Upgrade File Name

Syntax: **show upgrade firmware file**

Description: Displays the names of the upgrade files and the current revisions. This command can only be entered from the IONMM by an Admin level login user.

Example 1:

```
C1|S7|L1D>show upgrade firmware file
Card type                                   Revision          Firmware file name
-------------------------------------------------------------------
IONMM                                       1.0.5             IONMM_1.0.5_AP.bin
x222x_x322x                                 1.0.5             x222x_x322x_1.0.5_AP.bin
x323x                                       1.0.5             x323x_1.0.5_AP.bin
C1|S7|L1D>
```

Example 2:

```
C1|S7|L1D>show upgrade firmware file
Card type                           Revision              Firmware file name
-------------------------------------------------------------------------
x211x                               1.0.4                 C2110_1.0.4_AP.bin
x323x                               1.0.4                 x323x_1.0.4_AP.bin
x321x                               1.0.4                 C3210_1.0.4_AP.bin
ION219                              1.0.4                 ION219_1.0.4_AP.bin
IONMM                               1.0.4                 IONMM_1.0.4_AP.bin
x311x                               1.0.4                 C3110_1.0.4_AP.bin
x222x_x322x                         1.0.4                 x222x_x322x_1.0.4_AP.bin
IONPS                               1.0.4                 IONPS_1.0.4_AP.bin
x221x                               1.0.4                 C2210_1.0.4_AP.bin
C1|S7|L1D>
```

Example 3:

```
C1|S1|L1D>show upgrade firmware file
Card type                       Revision      Firmware file name
-----------------------------------------------------------------------------
x621x                           0.6.2         C6210-0.6.2.bin
x222x_x322x                     0.6.3         x222x_x322x-0.6.3.bin
x323x                           0.6.3         x323x-0.6.3.bin
x601x                           0.6.3         C6010_0.6.3_AP.bin
C1|S1|L1D>
```

Update Firmware Database

Syntax: **update firmware-db file=**<xx>

Description: Causes the upgrade file specified (xx) to be moved from the temporary location in the IONMM/standalone module to the permanent location. The temporary location is where the file is stored after a "tftp get" operation. This command can only be entered on the IONMM by an Admin level login user. Note that a TFTP server must be online, configured and operational.

Example:
```
C1|S7|L1D>update firmware-db file x323x_1.0.5_AP.bin
Updating is in progress...
Update failed!
Reason: invalid input file
C1|S7|L1D>
```

Note: You must use the "tftp get" command to copy the upgrade file from the TFTP server to the IONMM or standalone module. See "TFTP Commands".

Upgrade Device Firmware

Syntax: **upgrade module**

Description: Causes the firmware in the device selected in the command line prompt to be upgraded. This upgrade can only be entered on the IONMM by an Admin level login user.

 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). A Factory Reset also removes the permanent settings (e.g. configuration files, HTTPS certification file, SSH key.

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         IONMM                                     c=1 s=7 l1d
5         C3231-1040                                c=1 s=10 l1d
6         C2110-1013                                c=1 s=12 l1d
7         C2210-1013                                c=1 s=13 l1d
8         C2220-1014                                c=1 s=16 l1d
9         C3220-1040                                c=1 s=18 l1d
10        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)
```

Select one or more modules to upgrade by entering the displayed index number (e.g., 1, 3, 6) and press **Enter**. (Do not enter any space in the command string.) The message "*processing ...*" displays. Type the letter "**q**" and press the **Enter** key to exit (quit) the command.

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

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

If a module upgrade was unsuccessful, the reason for the failure displays in the "reason" column of the table (e.g., *invalid input file*, *protocol timeout*).

35. VLAN Commands

The VLAN commands can be divided into three categories:

- Management VLAN commands
- Device-level VLAN commands and Port-level VLAN commands
- Device-level VLAN Database commands and Port-level VLAN Database commands

Device-level commands can only be entered when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D). Port-level 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).

Only the Management VLAN commands are applicable for the IONMM or NID. The device-level and port-level Management VLAN commands do not function when entered from an IONMM or NID.

The following configuration restrictions apply to the Management VLAN feature:

1) Management VLAN Status cannot be changed to “Enabled” with VLAN “1” and valid VLAN ID allowed is “2 to 4094”. However, VLAN “1” can be selected when Management VLAN status is set to “Disabled”. Thus:
    - a VLAN ID of 2-4094 is valid with Management VLAN enabled.
    - a VLAN ID of 1-4094 is valid with Management VLAN disabled.
2) Management VLAN status cannot be changed to “Enabled” when no port members are selected.
3) Management VLAN Status “Disabled” means that Management access is allowed on all the ports; the values in Management VLAN ID and port members are ignored.
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.
6) The card must be in “Network” mode to set the VLAN ID. If it is not set to “Network”, an SNMP operation error displays.
7) A port with its Frame Tag mode set to "Customer" (default) cannot be added to Member Ports for Management VLAN.

The Management VLAN default values are:

- VLAN ID: **2**
- Port members checked: none
- Status: Disabled

Management VLAN Commands

Set Management VLAN Admin State

Syntax: **set mgmt vlan state**={enable | disable}

Description: Enables or disables management VLAN for the NID.

Example:
```
C0|S0|L1D>set mgmt vlan state enable
C0|S0|L1D>
```

Set Management VLAN ID

Syntax: **set mgmt vlan vid=<**xx>

Description: Defines the management VLAN ID (2–4094) that the NID is associated with.

Example:
```
C0|S0|L1D>set mgmt vlan vid 6
C0|S0|L1D>
```

Set Management VLAN Port(s)

Syntax: **set mgmt vlan port=<**xx>

Description: Specifies the port(s) on the IONMM or NID that will be part of the management VLAN. If more than one port is specified, they must be separated by a comma (i.e., port=1,2). where:

xx = port number(s) (e.g., port=1 or port=1,2)

Example:
```
C1|S7|L1D>set mgmt vlan port=1
C1|S7|L1D>set mgmt vlan port=2
C1|S7|L1D>
```

Show Management VLAN Configuration

Syntax: **show mgmt vlan config**

Description: Displays the management VLAN configuration of a NID.

Example 1:

```
C1|S7|L1D>show mgmt vlan config
vlan id   vlan state          vlan portlist
-------------------------------------------------------------------
100       enable             1,2
```

Example 2:

```
C1|S7|L1D>set mgmt vlan port=1
C1|S7|L1D>set mgmt vlan port=2
C1|S7|L1D>show mgmt vlan config
vlan id   vlan state          vlan portlist
-------------------------------------------------------------------
3         disable            1,2
C1|S7|L1D>
```

VLAN Device-Level Commands

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Add VLAN VID

Syntax: **add vlan vid**=<2-4094> [**priority**=NUM] [**pri-override**=(enable|disable)]

Description: Create a new VLAN and assign a VLAN ID to it, where:

Vlan-id = 2-4094 = a number to uniquely identify a VLAN, in the range of 2 to 4094.

VID 1 is reserved for the default VLAN and cannot be assigned or changed.

[pri-override = (enable|disable)] optional parameter to include or exclude priority override capability.

This command can be entered by users with admin or read-write user privileges.

Example:

```
AgentIII C1|S8|L1D>add vlan vid 2
AgentIII C1|S8|L1D>show vlan config
vid:1       fid:0       priority:0         priv_override:disable
port1:     noMod  port2:     noMod  port3:     noMod
vid:2       fid:0       priority:0         priv_override:disable
port1: notMember  port2: notMember  port3: notMember
AgentIII C1|S8|L1D>
```

Remove VLAN VID

Syntax: **remove vlan vid**=<2-4094> [priority=NUM] [pri-override=(enable|disable)]

Description: Remove a specified VLAN from a card, where:

Vlan-id = a number that identifies a VLAN (2 to 4094). VID 1 is reserved for the default VLAN and cannot be assigned or changed.

This command can be entered by users with admin or read-write user privileges.

Example:

```
AgentIII C1|S8|L1D>show vlan config
vid:1       fid:0       priority:0         priv_override:disable
port1:     noMod  port2:     noMod  port3:     noMod
vid:2       fid:0       priority:0         priv_override:disable
port1: notMember  port2: notMember  port3: notMember
AgentIII C1|S8|L1D>remove vlan vid 2
AgentIII C1|S8|L1D>show vlan config
vid:1       fid:0       priority:0         priv_override:disable
port1:     noMod  port2:     noMod  port3:     noMod
AgentIII C1|S8|L1D>
```

Set VLAN Entry Tagging

Syntax: **set vlan vid=**<xx> **port=**<yy> **memetag=**{zz}

Description: Sets a port and VLAN tagging mode for the device. By default, VLAN ID one (VID 1) is defined for internal use.

where:

xx = ID (2–4094) of the VLAN to which the device is to become a member (VID).

yy = the port number (1-2 for x3230 or 1-3 for x3231).

Example:

```
C1|S3|L1D>set vlan vid=10 port=2 memetag ?
  noMod
  notMember
  tag
  unTag
C1|S3|L1D>set vlan vid=10 port=2 memetag=unTag
C1|S3|L1D>
```

Set VLAN Entry Priority

Syntax: **set vlan vid=**<xx> **priority=**<yy>

Description: Sets a VLAN priority for the device. By default, VLAN ID one (VID 1) is defined for internal use.

where:

xx = ID (2–4094) of the VLAN (VID) to which the device is to become a member.

yy = priority for frames; 0-7, where 7 is the highest priority.

Example:

```
C1|S3|L1D>set vlan vid=10 fid=10 priority=<0-7>
C1|S3|L1D>
```

Set VLAN Entry Priority Override

Syntax: **set vlan vid=**<xx> **pri–override=**{zz}

Description: Sets the VLAN priority override for the device. By default, VLAN ID one (VID 1) is defined for internal use.

where:

xx = ID (2–4094) of the VLAN to which the device is to become a member

yy = optional; priority for frames; 0-7, where 7 is the highest priority

zz = optional: priority override: {enable | disable}

Example: `C1|S3|L1D>set vlan vid=10 fid=10 pri-override=enable`

Show VLAN Configuration

Syntax: **show vlan vid**

Description: Displays the current VLAN configuration settings.

Example 1: (2-port device)

```
C1|S3|L1D>show vlan config
vid:10       fid:0       priority:2         priv_override:disable
port1:     noMod  port2:     Tag
C1|S3|L1D>
```

Example 2: (3-port device)

```
AgentIII C1|S8|L1D>show vlan config
vid:1       fid:0       priority:0         priv_override:disable
port1:     noMod  port2:     noMod  port3:     noMod
AgentIII C1|S8|L1D>
```

Flush VLAN FID

Syntax: **flush fiddb type**=<all|dynamic>

Description: Device level command to clear the dynamic entries or all of the entries in the VLAN forwarding information database.

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 progess!
Flush VLANdb succeeded!
C1|S3|L1D>flush fiddb type all
Flushing fiddb is in progess!
Flush VLANdb succeeded!
C1|S3|L1D>
```

Flush VLAN DB

Syntax: **flush vlandb all**

Description: Device level command to erase all VLAN database entries except for the default VLAN database entry (which cannot be deleted).
When the 'FIDDb Flush Operation' is 'Flush All FIDs' or Flush All Dynamic FIDs', the value (1..4094) specifies the FID to be flushed. A value of 0 means no FID is specified.

Example:

```
C1|S3|L1D>flush vlandb all
Flushing VLANdb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>
```

VLAN Port-Level Commands

Note: These commands can only be entered at the port level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Set Port VLAN Tag Mode

Syntax: **set port vlan tag mode=**<xx>

Description: Sets the port's VLAN type.
where:

xx = Customer, Network, or Provider. If Provider is entered, you must also define the Provider ETH Type (see below).

Example:

```
C1|S3|L1D>set port vlan tag mode ?
  customer
  network
  provider
C1|S3|L1P1>set port vlan tag mode=network
C1|S3|L1P1>
```

Set Port VLAN Tag Provider Eth Type

Syntax: **set port vlan tag provider ethtype=**<xx>

Description: Sets the port's VLAN Provider ETH type.

where:

xx = x8100, x88a8, or x9100. You only need to define the Provider Ethtype if you entered 'Provider' via the **set port vlan tag mode** command (see above).

Example:

```
C1|S3|L1P1>set port vlan tag provider ethtype?
  x8100
x88a8
x9100
C1|S3|L1P1>set port vlan tag provider ethtype=x9100
Current VLAN tagging mode is not 'provider'!
C1|S3|L1P1>set port vlan tag mode=provider
C1|S3|L1P1>set port vlan tag provider ethtype=x9100
C1|S3|L1P1>
```

Note: If you enter this command with the current VLAN tagging mode not set to 'Provider', the message "*Current VLAN tagging mode is not 'provider'!*" displays.

Set Force Port to Use Default VID

Syntax: **set port force–default–vid**={true | false}

Description: If set =true, forces all untagged and 802.1Q tagged frames to use the default VLAN-ID.

Example:
```
C1|S3|L1P1>set port force-default-vid=true
C1|S3|L1P1>
```

Use the **show port vlan config** command to display the current setting.

Set VLAN Port Default VID

Syntax: **set port default–vid=**<xx>

Description: Sets the default VLAN ID (VID) for this port. The factory default is 1.

where:

xx= VID: (2-4094)

Example:
```
C1|S3|L1P1>set port default-vid=2
C1|S3|L1P1>go l1p=2
C1|S3|L1P2>set port default-vid=2
C1|S3|L1P2>
```

Use the **show port vlan config** command to display the current default VID.

Set VLAN Port Discard Tagged Non-Management Frames

Syntax: **set port discard–tagged**={true | false}

Description: Sets if tagged non-management frames are to be discarded for this port.

Example:
```
C1|S3|L1P2>set port discard-tagged ?
  false
  true
C1|S3|L1P2>set port discard-tagged true
C1|S3|L1P2>set port discard-tagged false
C1|S3|L1P2>
```

Use the **show port vlan config** command to display the current VLAN Discard-tagged state.

Set VLAN Port Discard Untagged Non-Management Frames

Syntax: **set port discard–untagged**={true | false}

Description: Sets if untagged non-management frames are to be discarded for this port.

Example:
```
C1|S3|L1P2>set port discard-untagged ?
  false
  true
C1|S3|L1P2>set port discard-untagged true
C1|S3|L1P2>set port discard-untagged false
C1|S3|L1P2>
```

Use the **show port vlan config** command to display the current VLAN Discard-untagged state.

Show VLAN Port Configuration

Syntax: **show port vlan config**

Description: Displays the VLAN configuration of a port.

Example:
```
C1|S3|L1P2>show port vlan config
Dot1q state:                  vlanEnabled
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              22
Force use default VLAN id:    false
C1|S3|L1P2>
```

Show VLAN Port Tag Configuration

Syntax: **show port vlan tag config**

Description: Displays the VLAN tag configuration of a port.

Example 1:
```
C1|S3|L1P2>show port vlan tag config
Tagging mode:           network
Network tagging:        addTag
```

Example 2:
```
C1|S3|L1P2>show port vlan tag config
Tagging mode:           customer
```

Example 3:
```
C1|S3|L1P2>show port vlan tag config
Tagging mode:            provider
Provider Ethernet type:  x88a8
```

VLAN Database Device-Level Commands

Note: These commands can only be entered at the device level - when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D).

Add VLAN Database Row Entry

Syntax: **add vlan–db vid=**<xx> [**priority=**<yy>] [**pri–override=**{zz}]

Description: Adds a new VLAN to the device. By default, VLAN ID one (VID 1) is defined for internal use. Adds a new row in VLAN forwarding database.
where:

xx = ID (2–4094) of the VLAN to which the device is to become a member

yy = optional; priority for frames; 0-7, where 7 is the highest priority

zz = optional: priority override: {enable | disable}

Example:

```
C1|S3|L1P1>add vlan-db vid=4
Error: this command should be executed on a device!
C1|S3|L1P1>go l1d
C1|S3|L1D>add vlan-db vid=4
C1|S3|L1D>
```

Remove All VLANs

Syntax: **remove vlan all**

Description: Removes all VLANs from the device.
Note: you cannot remove VID 1 as it is used for internal purposes.

Example:

```
C1|S3|L1D>remove vlan ?
  all
  vid
C1|S3|L1D>remove vlan all
C1|S3|L1D>
```

Remove a Single VLAN Database Row Entry

Syntax: **remove vlan–db vid=**<xx>

Description: Removes the specified VLAN forwarding database VLAN ID (2-4094). Removes a specified row from VLAN forwarding database.

Example:

```
AgentIII C1|S8|L1D>add vlan-db vid 3
AgentIII C1|S8|L1D>show vlan-db config
vid:1       fid:0       priority:0         priv_override:disable
port1:     noMod  port2:     noMod  port3:     noMod
vid:2       fid:0       priority:0         priv_override:disable
port1: notMember  port2: notMember  port3: notMember
vid:3       fid:0       priority:0         priv_override:disable
port1: notMember  port2: notMember  port3: notMember
AgentIII C1|S8|L1D>remove vlan-db vid 3
AgentIII C1|S8|L1D>show vlan-db config
vid:1       fid:0       priority:0         priv_override:disable
port1:     noMod  port2:     noMod  port3:     noMod
vid:2       fid:0       priority:0         priv_override:disable
port1: notMember  port2: notMember  port3: notMember
AgentIII C1|S8|L1D>
```

Set VLAN Database Member/Egress Tagging

Syntax: **set vlan–db vid=**<xx> **port=**<yy> **memetag=**<zz>

Description: Sets the VLAN member egress tagging for a row of the VLAN forwarding database.

where:

xx = number that identifies the VLAN (2–4094)

yy = logical port index (1-10) (enter physical ports 1-2)

zz = valid **memetag** choices are:

- **noMod** (case sensitive) – a VLAN member with no modifications
- **notMember** (case sensitive) – not a VLAN member
- **tag** (case sensitive) - a VLAN member with egress tagging
- **unTag** (case sensitive) – a VLAN member with no egress tagging

Example:

```
C1|S5|L1D>set vlan-db vid 4 port=10 memetag ?
  noMod
  notMember
  tag
  unTag
C1|S5|L1D>set vlan-db vid 4 port=10 memetag=tag
C1|S5|L1D>
```

Set VLAN Database Priority Override

Syntax: **set vlan-db vid=**<1-4094> **fid=**FID **pri-override=**(enable|disable)

Description: Sets the priority override of a row of the VLAN forwarding database.

where:

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

Example:
```
C1|S5|L1D>set vlan-db vid=22 fid=23 pri-override=enable
C1|S5|L1D>set vlan-db vid=22 fid=23 pri-override=disable
C1|S5|L1D>set vlan-db vid=22 fid=55 pri-override=enable
C1|S5|L1D>set vlan-db vid=22 fid=55 pri-override=disable
C1|S5|L1D>
```

Set VLAN Database Priority

Syntax: **set vlan-db vid=**<1-4094> **fid**=FID **priority=**<0-7>

Description: Sets the priority of a row of the VLAN forwarding database.

where:

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

Example:
```
C1|S5|L1D>set vlan-db vid=23 fid=56 priority=2
C1|S5|L1D>set vlan-db vid=23 fid=55 priority=2
C1|S5|L1D>set vlan-db vid=22 fid=23 priority=2
C1|S5|L1D>set vlan-db vid=22 fid=23 priority=2
C1|S5|L1D>set vlan-db vid=22 fid=56 priority=2
C1|S5|L1D>
```

Show VLAN Database Configuration

Syntax: **show vlan–db config**

Description: Displays the VLAN database entries for a device.

Example 1:

```
C1|S13|l0ap1|l1p2/>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
```

Example2:

```
C1|S5|L1D>show vlan-db config
vid:1    fid:0      priority:0       priv_override:disable    port1: noMod      port2: noMod
vid:2    fid:0      priority:0       priv_override:disable    port1: notMember  port2: tag
vid:3    fid:0      priority:0       priv_override:disable    port1: tag                port2: notMember
vid:4    fid:0      priority:0       priv_override:disable    port1: notMember  port2: notMember
vid:100  fid:0      priority:0       priv_override:disable    port1: tag        port2: unTag
vid:200  fid:0      priority:0       priv_override:disable    port1: tag        port2: unTag
vid:222  fid:0      priority:0       priv_override:disable    port1: notMember  port2: notMember
vid:300  fid:0      priority:0       priv_override:disable    port1: tag        port2: noMod
vid:600  fid:0      priority:0       priv_override:disable    port1: unTag      port2: tag
C1|S5|L1D>
```

Example 3:

```
C1|S3|L1D>show vlan-db config
vid:1      fid:0      priority:0     priv_override:disable    port1: noMod  port2: noMod
vid:200    fid:0      priority:0     priv_override:disable    port1: tag    port2: unTag
vid:600    fid:0      priority:0     priv_override:disable    port1: unTag  port2: tag
C1|S3|L1D>
```

36. Zero Touch Provisioning (ZTP)

Note: ZTP is supported only in the standalone S3230-10xx at version 1.3.10. The support for Zero Touch Provisioning changes the default behavior of the ION standalone S3220-10xx. The Chassis card C3220-10xx behavior stays the same as with prior releases.

When an ION S3220-10xx unit 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.

The switch mode can be changed by connecting to the ION S3220-10xx via the USB port and typing the command “set switch mode remote”. When an ION C3220-10xx or C3221-1040 card is powered up, it will come up in remote mode by default.

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. The term "**server**" refers to a host providing initialization parameters through DHCP, and "**client**" refers to a host requesting initialization parameters from a DHCP server.

DHCP supports three mechanisms for IP address allocation. In "**automatic allocation**", DHCP assigns a permanent IP address to a client. In "**dynamic allocation**", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "**manual allocation**", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network uses one or more of these mechanisms, depending on the policies of the network administrator. **Dynamic allocation** is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned.
DHCP uses UDP as its transport protocol.DHCP messages from a client to a server are sent to the 'DHCP server' port (67), and DHCP messages from a server to a client are sent to the 'DHCP client' port (68). A server with multiple network address (e.g., a multi-homed host) may use any of its network addresses in outgoing DHCP messages.

A **DHCP *client*** is an Internet host using DHCP to obtain configuration parameters such as a network address.

A **DHCP *server*** is an Internet host that returns configuration parameters to DHCP clients.

A **BOOTP *relay agent*** is an Internet host or router that passes DHCP messages between DHCP clients and DHCP servers. DHCP is designed to use the same relay agent behavior as specified in the BOOTP protocol specification.

For more information on DHCP see http://www.ietf.org/rfc/rfc2131.txt.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the 'options' field of the DHCP message. The data items themselves are also called “**DHCP options**". For more information on DHCP Options see http://tools.ietf.org/html/rfc2132

Refer to your DHCP server documentation for configuration instructions.

Vendor Class Identifier (DHCP Option 60)

The code for this option is 60, and its minimum length is 1.This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors choose to define specific vendor class identifiers to convey configuration or other identification information about a client. For example, the identifier may encode the client's hardware configuration. Servers not equipped to interpret the class-specific information sent by a client ignores it (although it may be reported). Servers that respond should only use option 43 to return the vendor-specific information to the client. Per RFC 2132 - DHCP Options and BOOTP Vendor Extensions - March 1997.

A DHCP option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters or octets which has a meaning specified by the vendor of the DHCP client. One method that a DHCP client can utilize to communicate to the server that it is using a certain type of hardware or firmware is to set a value in its DHCP requests called the Vendor Class Identifier (VCI) (Option 60). This method allows a DHCP server to differentiate between the two kinds of client machines and process the requests from the two types of modems appropriately. Some types of set-top boxes also set the VCI (Option 60) to inform the DHCP server about the hardware type and functionality of the device. The value this option is set to gives the DHCP server a hint about any required extra information that this client needs in a DHCP response.

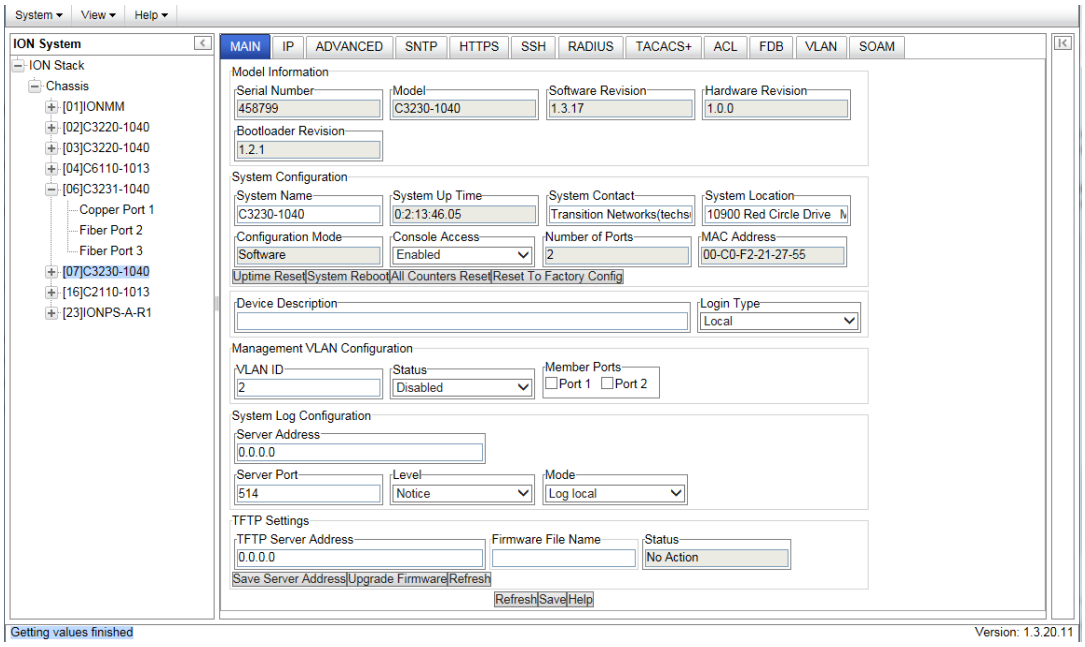
ZTP Notes and Exceptions

The ZTP feature is used by the Converge EMS server to auto discover the S323x. It is used only for auto-provision purposes and is a one-time only process. If necessary, you can change the switch mode to Remote, and then reboot the device.

37. Recording System Information for Support

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible to help the Technical Support Specialist.

1. Select the ION system **MAIN** tab. (From the CLI, use the commands needed to gather the information requested below. This could include commands such as **show card info**, **show slot info**, **show system information**, **show ether config**, **show ip-mgmt config**, **show loam config**, or others as request by the Support Specialist.)



2. Record the **Model Information** for your system.

   Serial Number: _____ Model: _____

   Software Revision: _____ Hardware Revision: _____

3. Record the **System Configuration** information for your system.

   System Up Time: _____ Console Access: _____

   Number of Ports: _____ MAC Address: _____

4. Record the **IP Configuration** information for your system.

   IP Address Mode: _____ IP Address: _____

5. Provide additional Model and System information to your Technical Support Specialist.

   Your Lantronix service contract number: _____

   A description of the failure: _____

_____

_____

_____

A description of any action(s) already taken to resolve the problem (e.g., changing switch mode, rebooting, etc.): _____

_____

_____

_____

The serial and revision numbers of all involved Lantronix products in the network:

_____

_____

A description of your network environment (layout, cable type, etc.): _____

_____

_____

Network load and frame size at the time of trouble (if known): _____

_____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

_____

_____

Any previous Return Material Authorization (RMA) numbers: _____

Appendix A. CLI Command Summary

This appendix lists CLI commands available via the help (?) command and the list command. Commands are arranged in alphabetical order. CLI commands are case sensitive; enter the CLI commands as shown. Press **Enter** after the command text is entered. These are the **Help** (**?**) commands available at the Admin user level.

ION CLI Commands via the *help* Command (C1|S7|L1D>*?*)

```
Agent III C1|S1|L1D>help
   1. add       Add a ACL condition
   2. backup    Backup specified provision modules.
   3. cat       Show the content of the FILES
   4. cd        Change to another directory
   5. clear     Clear all counters of the specified Ethernet port
   6. cls       Clear the screen.
   7. flush     Flush VLAN db.
   8. generate  Generate the specified SSH host key.
   9. go        set location to device/port of the SIC to be operated.
   10. home     go back to IONMM card
   11. list     Print command list
   12. ls       List the information about the FILES
   13. more     A filter for paging through text one screenful at a time.
   14. ping     Send ICMP ECHO-REQUEST to network hosts.
   15. ping6    Send ICMP ECHO-REQUEST to network hosts.
   16. prov     Get current TFTP server address.
   17. ps       Report a snapshot of the current processes
   18. pwd      Show current directory
   19. quit     Exit current mode and down to previous mode
   20. reboot   Warm start the system.
   21. refresh  Refresh backup and restore configure file name.
   22. remove   Remove all ACL conditions
   23. reset    Reset all ports' counters of the specified Ethernet port
   24. restart  Restart ACL
   25. restore  Restore specified provision modules.
   26. send     Initiates the delay measurement for a MEP. Note that one DM request is
       supported at a time for a given MEP.
   27. serial   transfer file through a serial line.
   28. set      Set bakup/restore configuration file name for a specified provision mod-
       ule.
   29. show     Show ACL chains
   30. start    Start TDR test of the specified Ethernet port
   31. stat     Show topology information of a chassis.
   32. tftp     Get a file from a TFTP server.
   33. update   Update fireware database
   34. upgrade  Upgrade firmware modules
Agent III C1|S1|L1D>
```

Note: The list numbers (above) are added for reference only. The list above is for Admin level users; the list below is displayed for users with Read-Only and Read-Write level privileges.

Help (**?**) command (Read-Only or Read-Write user levels):

```
Agent III C1|S1|L1D>?
   1. cat    Show the content of the FILES
   2. cd     Change to another directory
   3. cls    Clear the screen.
   4. go     set location to device/port of the SIC to be operated.
   5. home   go back to IONMM card
```

```
   6. list   Print command list
   7. ls     List the information about the FILES
   8. more   A filter for paging through text one screenful at a time.
   9. ping   Send ICMP ECHO-REQUEST to network hosts.
   10. ps    Report a snapshot of the current processes
   11. pwd   Show current directory
   12. quit  Exit current mode and down to previous mode
   13. set   Set password for a system user
   14. show  Show ACL chains
   15. stat  Show topology information of a chassis.
Agent III C1|S1|L1D>
```

ION CLI Commands via the *list* Command (C1|S8|L1D>*list*)

CLI commands are case sensitive. Enter the CLI commands as shown. To execute these commands, you must press the **Enter** key after the command has been entered. Not all commands listed here are functional on all NID models. For example, the "set tdm" and "show tdm" commands only function on the ION x61xx. See the ION System x6110/x6120 Managed 4xT1/E1-to-Fiber NID User Guide for x61xx commands.

List command (Admin user level):

AgentIII C1|S1|L1D>**list**

1. add acl condition type=(srcmacaddr|ipv4addr|ipv4addrrange|ipv4network|tcpport|tcpportrange|udpport|udpportrange|icmp) srcdst=(src|dst) oper=(equal|notequal) value=VAL
2. add acl rule position=(head|tail) table=(raw|filter|nat|mangle) chain=(prerouting|input|forward|output|postrouting) policy=(accept|drop|trap) [traprate=TRAPRATE] [condition=CONDLIST]
3. add fwddb mac=MAC [conn-port=PORT] [priority=PRIO] [type=(static|staticNRL|staticPA)]
4. add ip6tables acl condition type=(srcmacaddr|ipv6addr|ipv6network|tcpport|tcpportrange|udpport|udpportrange|icmp) srcdst=(src|dst) oper=(equal|notequal) value=VAL
5. add ip6tables acl rule position=(head|tail) table=(raw|filter|nat|mangle) chain=(prerouting|input|forward|output|postrouting) policy=(accept|drop|trap) [traprate=TRAPRATE] [condition=CONDLIST]
6. add snmp community name=STR_COMM_NAME access_mode=(read_only|read_write)
7. add snmp group name=STR_SNMP_GRP security-model=(v1|v2c|v3) security-level=(noAuthNoPriv|authNoPriv|authPriv) [readview = STR_READ_VIEW] [writeview = STR_WRITE_VIEW] [notifyview = STR_NOTIF_VIEW]
8. add snmp local user name=STR_USR_NAME security-level=(noAuthNoPriv|authNoPriv|authPriv) [auth-protocol=STR_AUTH_PROTOCOL password=STR_AUTH_PASS] [priv-protocol=STR_PRIV_PROTOCOL password=STR_PRIV_PASS] [group=STR_GRP_NAME]
9. add snmp remote engine addrtype=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535> engine_id= STR_ENGINE_NAME
10. add snmp remote user name=STR_USR_NAME addrtype=(ipv4|ipv6) addr=STR_SVR_ADDRport=<1-65535> security-level=(noAuthNoPriv|authNoPriv|authPriv) [auth-protocol=(md5|sha) password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]
11. add snmp remote user name=STR_USR_NAME engine=STR_ENGINES security-level=(noAuthNoPriv|authNoPriv|authPriv) [auth-protocol=(md5|sha) password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]
12. add snmp traphost version=(v1|v2c|v3) type=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535> (community|security_name)=STR_CS_NAME security_level=(noAuthNoPriv|authNoPriv|authPriv) [notify=TRAP_TYPE] [timeout=<0-2147483647>] [retry=<0-255>]
13. add snmp view name=STR_SNMP_VIEW oid=STR_VIEW_OID type=(include|exclude)
14. add soam ma local-ma-id=<1-4294967295> local-md-id=<1-4294967295> ma-name=NAMEvlan-type=(none|ctype|stype|doubletag) [primary-vlan=<1-4095>] [s-vid=<1-4095>]
15. add soam md local-md-id=<1-4294967295> md-name=(NAME|none) md-level=<0-7>
16. add soam meg local-meg-id=<1-4294967295> meg-name=NAME meg-level=<0-7> vlan-type=(none|ctype|stype|doubletag) [primary-vlan=<1-4095>] [s-vid=<1-4095>]
17. add soam mep mep-id=<1-8191> local-parent-id=<1-4294967295> direction=(up|down) port=<1-2>
18. add soam mip mip-type=(y.1731|802.1ag) local-mip-id=<1-4294967295> local-parent-id=<1-4294967295> port=<1-2>
19. add sysuser name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR
20. add vlan-db vid=<1-4094> [priority=NUM] [pri-override=(enable|disable)]
21. backup module-list=STR_MODULE_LIST
22. cat [OPTION] [FILE]
23. cd [DIR]
24. clear ether all counters
25. clear loam stats
26. clear syslog
27. cls
28. flush fiddb type=(all|dynamic)
29. flush vlandb all
30. generate ssh host-key=(dsa|rsa|both)
31. go [c=STR_CHA] [s=STR_SLOT] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|
32. l3p=<1-15>|l1d|l2d|l3d)
33. home
34. list
35. ls [OPTION] [FILES]
36. more [OPTION] [+linenum] FILE ...
37. ping [-c COUNT] [-t TTL] A.B.C.D
38. ping6 [-c COUNT] [-t TTL] ADDR
39. prov get tftp svr addr
40. prov set tftp svr type=(ipv4|ipv6|dns) addr=ADDR
41. ps [OPTION]
42. pwd
43. quit

44. reboot
45. refresh provision configure filename
46. remove acl condition all
47. remove acl condition index=<1-255>
48. remove acl rule all
49. remove acl rule index=<1-255>
50. remove fwddb all
51. remove fwddb mac=MAC fdbid=<0-255>
52. remove ip6tables acl condition all
53. remove ip6tables acl condition index=<1-255>
54. remove ip6tables acl rule all
55. remove ip6tables acl rule index=<1-255>
56. remove snmp community name=STR_COMM_NAME
57. remove snmp group name=STR_SNMP_GRP [security-model=(v1|v2c|v3) security-level=(noAuthNoPriv|authNoPriv|authPriv)]
58. remove snmp local user name=STR_USER_NAME
59. remove snmp remote engine addrtype=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535>
60. remove snmp remote user name=STR_USER_NAME addrtype=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535>
61. remove snmp remote user name=STR_USER_NAME engine=STR_ENGINE_ID
62. remove snmp traphost type=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535>
63. remove snmp view name=STR_SNMP_VIEW [oid=STR_VIEW_OID]
64. remove soam config all
65. remove soam ma local-ma-id=<1-4294967295>
66. remove soam md local-md-id=<1-4294967295>
67. remove soam meg local-meg-id=<1-4294967295>
68. remove soam mep mep-id=<1-8191> local-parent-id=<1-4294967295>
69. remove soam mip local-mip-id=<1-4294967295>
70. remove ssh host-key=(dsa|rsa|both)
71. remove ssh public-key user=USER type=(dsa|rsa|both)
72. remove sysuser name=NAMESTR
73. remove vlan all
74. remove vlan-db vid=<2-4094>
75. reset all ports counters
76. reset factory
77. reset uptime
78. restart acl
79. restart ip6tables acl
80. restore module-list=STR_MODULE_LIST
81. send soam mep dm mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID) period=(1s|10s) frame-num=<3-32>
82. send soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID) use-fdb-only=(true|false) ttl=<0-255>
83. send soam mep loopback mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID|multicast) amount-frames=<1-1024> [transmission-rate=<1-80>] [data=DATA-TLV] [priority=<1-7>] [drop-enable=(enable|disable)]
84. send soam mep mcc mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID) oui=OUI data=DATA
85. send soam mep test mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID) pattern=(nullnocrc|null-crc|prbs231nocrc|prbs231crc) size=<0-1467> frame-num=<1-32>
86. serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem) file=FILE
87. set (backup|restore) module-index=<1-255> config-file=STR_CFG_FILE
88. set acl condition=<1-255> rule_index=<1-255>
89. set acl rule=<1-255> traprate=<1-65535>
90. set acl state=(enable|disable)
91. set acl table=(raw|filter|nat|mangle) chain=(prerouting|input|forward|output|postrouting) policy=(accept|drop)
92. set ais format=(blue|allones)
93. set ais transmit=(enable|disable)
94. set bw alloc-type=(countAllLayer1|countAllLayer2|countAllLayer3)
95. set circuit-ID=CIRCUIT
96. set curr-time=STR_CURR_TIME
97. set dbg level=<0-2>
98. set device description=CIRCUIT
99. set dmi rx-power-preset-level=<0-65535>
100. set dns-svr svr=<1-6> type=(ipv4|ipv6) addr=ADDR
101. set dot1bridge aging-time=<0-3825>
102. set dot1dbridge ieee-tag-priority=<0-7> remap-priority=<0-3>
103. set dot1dbridge ip-priority-index=<0-63> remap-priority=<0-3>
104. set ether admin state=(up|down)
105. set ether adv-cap=STR_ETHER_ADV_CAPABILITY
106. set ether autocross=(mdi|mdi-x|auto)
107. set ether autoneg state=(enable|disable)
108. set ether dot3 pause=(disabled|enableTx|enableRx|enableTxRx)
109. set ether duplex=(full|half)
110. set ether fef=(enable|disable)
111. set ether filter-unknown-multicast=(enable|disable)

112. set ether filter-unknown-unicast=(enable|disable)
113. set ether loopback oper=(init|stop)
114. set ether loopback type=(noloopback|phylayer|maclayer|alternate|remote)
115. set ether pause=STR_ETHER_PAUSE
116. set ether phymode=(phySGMII|phy100BaseFX|phy1000BaseX)
117. set ether speed=(10M|100M|1000M)
118. set ether src-addr-lock action=(discard|discardandnotify|shutdown|all)
119. set ether src-addr-lock=(enable|disable)
120. set fwd portlist=PORT_LIST
121. set fwddb mac=MAC fdbid=INDEX conn-port=PORT
122. set fwddb mac=MAC fdbid=INDEX priority=<0-7>
123. set fwddb mac=MAC fdbid=INDEX type=(static|staticNRL|staticPA)
124. set gateway type=(ipv4|ipv6) addr=ADDR
125. set https certificate-file=FILE
126. set https certificate-type=(self-certificate|authorized)
127. set https port=<1-65535>
128. set https private-key file=FILE
129. set https private-key password
130. set https state=(enable|disable)
131. set ip address mode =(dhcp|bootp|static)
132. set ip type=(ipv4|ipv6) addr=ADDR (subnet-mask|prefix)=A
133. set ip6tables acl condition=<1-255> rule_index=<1-255>
134. set ip6tables acl rule=<1-255> traprate=<1-65535>
135. set ip6tables acl state=(enable|disable)
136. set ip6tables acl table=(raw|filter|nat|mangle) chain=(prerouting|input|forward|output|postrouting) policy=(accept|drop)
137. set ipv6 address mode =(static|dhcpv6|stateless)
138. set ipv6 gateway mode=(static|routerDisc)
139. set ipv6-mgmt state=(enable|disable)
140. set irate=(unLim-
ited|rate1M|rate2M|rate3M|rate4M|rate5M|rate6M|rate7M|rate8M|rate9M|rate10M|rate15M|rate20M|rate25M|rate30M|rate35M|rate40M|rate
45M|rate50M|ra
te55M|rate60M|rate65M|rate70M|rate75M|rate80M|rate85M|rate90M|rate95M|rate100M|rate150M|rate200M|rate250M|rate300M|rate350M|
rate400M|rate450M|rate500M|rate550M|
rate600M|rate650M|rate700M|rate750M|rate800M|rate850M|rate900M|rate950M) **erate**=(unLim-
ited|rate1M|rate2M|rate3M|rate4M|rate5M|rate6M|rate7M|rate8M|rate9M|rate10M
|rate15M|rate20M|rate25M|rate30M|rate35M|rate40M|rate45M|rate50M|rate55M|rate60M|rate65M|rate70M|rate75M|rate80M|rate85M|rate9
0M|rate95M|rate100M|rate150M|rate2
00M|rate250M|rate300M|rate350M|rate400M|rate450M|rate500M|rate550M|rate600M|rate650M|rate700M|rate750M|rate800M|rate850M|ra
te900M|rate950M)
141. set l2cp proto=(spanningTree|slow|portAuthentication|elmi|lldp|bridgeMgmt|garpmrpBlock|bridgeBlockOtherMulticast) process=(pass|dis-
card)
142. set loam admin state=(enable|disable)
143. set loam critical-evt-notif=(enable|disable)
144. set loam dg-evt-notif=(enable|disable)
145. set loam ef threshold=<0-268435455>
146. set loam ef window=<10-600>
147. set loam ef-evt-notif=(enable|disable)
148. set loam efp threshold=<0-268435455>
149. set loam efp window=<1-104857560>
150. set loam efp-evt-notif=(enable|disable)
151. set loam efss threshold=<0-9000>
152. set loam efss window=<100-9000>
153. set loam efss-evt-notif=(enable|disable)
154. set loam esp threshold high=<0-268435455> low=<0-268435455>
155. set loam esp window high=<0-4294967295> low=<1-268435455>
156. set loam esp-evt-notif=(enable|disable)
157. set loam ignore-loopback-request=(enable|disable)
158. set loam mode=(passive|active)
159. set login method=(local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal)
160. set lpt monitor-port=PORT
161. set lpt state=(enable|disable|notSupported)
162. set mac_learning enable portlist=STR_MAC_LEARNING_PORT_LIST
163. set mgmt vlan port=PORTLIST
164. set mgmt vlan state=(enable|disable)
165. set mgmt vlan vid=<1-4094>
166. set port default-vid=<1-4094>
167. set port discard-tagged=(true|false)
168. set port discard-untagged=(true|false)
169. set port dot1-state=(vlanEnabled|vlanDisabled)
170. set port egress queuingmethod =(wrr|sp)

171. set port force-default-vid=(true|false)
172. set port mgmtaccess=(enable|disable)
173. set port vlan tag mode=(network|provider|customer)
174. set port vlan tag network tagging=(unmodified|removeTag|addTag)
175. set port vlan tag provider ethtype=(x8100|x9100|x88a8)
176. set power relay state=(enable|disable)
177. set qos default-priority=<0-7>
178. set qos ingress-priority=<0-7> remap-priority=<0-7>
179. set qos priority by-dst-mac=(enable|disable)
180. set qos priority by-src-mac=(enable|disable)
181. set qos priority by-vlan-id=(enable|disable)
182. set qos priority ieee-tag=(enable|disable)
183. set qos priority ip-tag=(enable|disable)
184. set qos priority tag-type=(useIEEE|useIP)
185. set radius client state=(enable|disable)
186. set radius svr=<1-6> retry=<1-5>
187. set radius svr=<1-6> secret=SECRET
188. set radius svr=<1-6> timeout=<1-60>
189. set radius svr=<1-6> type=(ipv4 |dns|ipv6) addr=ADDR [retry=<1-5>] [timeout=<1-60>]
190. set redundancy state=(enable|disable)
191. set rfd state=(enable|disable|notSupported)
192. set selective lpt state=(enable|disable)
193. set sensor stid=SENSORID notif=(enable|disable)
194. set sensor stid=SENSORID relation=(lessThan|lessOrEqual|greaterThan|greaterOrEqual|equalTo|notEqualTo)
195. set sensor stid=SENSORID severity=(other|minor|major|critical)
196. set sensor stid=SENSORID value=VALUE
197. set slot=SLOT power=(on|off|reset)
198. set snmp local engine=STR_LOCAL_ENGINE
199. set snmp local user name=STR_USER_NAME group=STR_GRP_NAME
200. set snmp view name=STR_SNMP_VIEW oid=STR_VIEW_OID type=(include|exclude)
201. set sntp dst-end=TIME
202. set sntp dst-offset=OFFSET
203. set sntp dst-start=TIME
204. set sntp dst-state=(enable|disable)
205. set sntp state=(enable|disable)
206. set sntp timezone=<1-63>
207. set sntp-svr svr=<1-6> type=(ipv4|dns|ipv6) addr=ADDR
208. set soam ma local-ma-id=<1-4294967295> attr_name=(permission|ccminterval|mepid-add|mepid-remove|vlan-add|vlan-remove|primary-vlan|autodetection-timeout|autode
tectrmep) attr_value=(none|chassis|mgmtaddr|chassismgmtaddr|defer|cci1s|cci10s|cci1min|cci10min|enable|disable|...)
209. set soam md local-md-id=<1-4294967295> permission-id=(none|chassis|mgmtaddr|chassismgmtaddr)
210. set soam meg local-meg-id=<1-4294967295> attr_name=(permission|ccminterval|mepid-add|mepid-remove|vlan-add|vlan-remove|primary-vlan|autodetection-timeout|auto
detectrmep|y.1731-802.1ag-interop) attr_value=(none|chassis|mgmtaddr|chassismgmtaddr|cci1s|cci10s|cci1min|cci10min|enable|disable|...)
211. set soam mep config mep-id=<1-8191> local-parent-id=<1-4294967295> attr_name=(admin|cci|primaryvid|ccmltmprior-ity|faultalarmdetect|faultalarmreset|lowestprilevel|aisclient-add|aisclient-remove|aistransmit|aisinterval|aisnotifyup|aisprocess|aisframeprior-ity) attr_value=(enable|disable|alldef|macremerrxcon|remerrxconn|errxconn|xconn|noxcon|...)
212. set soam mep lmperiodic mep-id=<1-8191> local-parent-id=<1-4294967295> state=(enable|disable|clearcounters)
213. set soam mip local-mip-id=<1-4294967295> attr_name=(admin|aistransmit|aisinterval|aisframepriority) attr_value=(enable|disa-ble|1s|1min|...)
214. set ssh auth-retry=<1-5>
215. set ssh client timeout=<1-120>
216. set ssh public-key user=USER type=(dsa|rsa) file=FILENAME
217. set ssh server state=(enable|disable)
218. set switch mode=(local|remote)
219. set syslog level=(emerg|alert|crit|err|warning|notice|info|debug)
220. set syslog mode=(local|remote|localAndRemote|off)
221. set syslog svr port=<1-65535>
222. set syslog svr type=(ipv4|ipv6|dns) addr=SYSLOG_SVR_ADDR
223. set system contact=CONTACT
224. set system location=LOC
225. set system name=NAME
226. set sysuser name=NAMESTR level=(admin|read-write|read-only)
227. set sysuser name=NAMESTR pass=PASSSTR confirmpass=PASSSTR)
228. set tacplus client state=(enable|disable)
229. set tacplus svr=<1-6> retry=<1-5>
230. set tacplus svr=<1-6> secret=SECRET
231. set tacplus svr=<1-6> timeout=<1-60>
232. set tacplus svr=<1-6> type=(ipv4 |ipv6|dns) addr=ADDR [retry=<1-5>] [timeout=<1-60>]
233. set taos transmit=(enable|disable)

234. set tdm inband start pattern=PATTERN
235. set tdm inband stop pattern=PATTERN
236. set tdm inband timeout=(enable|disable)
237. set tdm inband=(enable|disable)
238. set tdm loopback oper=(init|stop)
239. set tdm loopback type=(noloopback|phylayer|maclayer)
240. set tdm peer inband start pattern=PATTERN
241. set tdm peer inband stop pattern=PATTERN
242. set tdm peer inband=(enable|disable)
243. set tndp tx state=(enable|disable)
244. set transparent lpt state=(enable|disable)
245. set usb-port state=(enable|disable)
246. set vlan-db vid=<1-4094> fid=FID pri-override=(enable|disable)
247. set vlan-db vid=<1-4094> fid=FID priority=PRIO
248. set vlan-db vid=<1-4094> port=<1-10> memetag=(noMod|unTag|tag|notMember)
249. show acl chain
250. show acl condition
251. show acl rule
252. show acl state
253. show bandwidth allocation
254. show cable length
255. show card info
256. show cardtype
257. show circuit-ID
258. show device description
259. show dmi info
260. show dot1bridge aging-time
261. show dot1dbridge ieee-tag priority remapping
262. show dot1dbridge ip-tc priority remapping
263. show ether config
264. show ether loopback capability
265. show ether loopback state
266. show ether security config
267. show ether statistics
268. show ether tdr config
269. show ether tdr test result
270. show firmware upgrade result
271. show firmware-db update result
272. show fwd portlist
273. show fwddb config fdbid=<0-255>
274. show https config
275. show ip-mgmt config
276. show ip6tables acl chain
277. show ip6tables acl condition
278. show ip6tables acl rule
279. show ip6tables acl state
280. show l2cp config
281. show loam config
282. show loam event config
283. show loam event log
284. show loam ignore-loopback-request
285. show loam peer info
286. show loam statistics
287. show lpt config
288. show mgmt vlan config
289. show port mac_learning state
290. show port vlan config
291. show port vlan tag config
292. show power config
293. show provision (backup|restore) modules
294. show qos config
295. show qos priority remapping
296. show radius config
297. show redundancy info
298. show rmon statistics
299. show slot info
300. show snmp community
301. show snmp group [name=STR_SNMP_GRP]
302. show snmp local engine
303. show snmp local user

304. show snmp remote engine
305. show snmp remote user
306. show snmp traphost
307. show snmp view [name=STR_SNMP_VIEW]
308. show sntp config
309. show soam conferror vid=<1-4095> port=<1-2>
310. show soam ma [local-ma-id=<1-4294967295>]
311. show soam md [local-md-id=<1-4294967295>]
312. show soam meg [local-meg-id=<1-4294967295>]
313. show soam mep cc mep-id=<1-8191> local-parent-id=<1-4294967295>
314. show soam mep config [mep-id=<1-8191> local-parent-id=<1-4294967295>]
315. show soam mep dm status mep-id=<1-8191> local-parent-id=<1-4294967295>
316. show soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> tid=<0-4294967295>
317. show soam mep lmperiodic [mep-id=<1-8191> local-parent-id=<1-4294967295> far-end-mep-id=<1-8191>]
318. show soam mep loopback mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(unicast|multicast)
319. show soam mep stats [mep-id=<1-8191> local-parent-id=<1-4294967295>]
320. show soam mep test mep-id=<1-8191> local-parent-id=<1-4294967295>
321. show soam mip config [local-mip-id=<1-4294967295>]
322. show soam mip stats [local-mip-id=<1-4294967295>]
323. show soam port
324. show soam portid
325. show soam senderid
326. show ssh config
327. show ssh host-key
328. show ssh public-key user=USER
329. show switch mode
330. show syslog config
331. show system information
332. show sysuser
333. show tacplus config
334. show tdm config
335. show tdm inband config
336. show tdm loopback capability
337. show tdm loopback state
338. show tdm peer inband config
339. show tdm port config
340. show timezone
341. show tndp tx state
342. show upgrade firmware file
343. show usb-port state
344. show vlan-db config
345. start ether tdr test
346. start https certificate
347. stat
348. tftp get iptype=(ipv4|ipv6|dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
349. tftp put iptype=(ipv4|ipv6|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
350. tftp upgrade iptype=(ipv4|ipv6|dns) ipaddr=ADDR remotefile=RFILE
351. update firmware-db file=FILENAME
352. upgrade module

Agent III C1|S1|L1D

List command (Read-Only or Read-Write user levels):

Agent III C1|S1|L1D>list

1. cat [OPTION] [FILE]
2. cd [DIR]
3. cls
4. go [c=STR_CHA] [s=STR_SLOT] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
5. home
6. list
7. ls [OPTION] [FILES]
8. more [OPTION] [+linenum] FILE ...
9. ping [-c COUNT] [-t TTL] A.B.C.D
10. ps [OPTION]
11. pwd
12. quit
13. set sysuser name=NAMESTR pass=PASSSTR confirmpass=PASSSTR)
14. show acl chain
15. show acl condition
16. show acl rule

17. show acl state
18. show bandwidth allocation
19. show cable length
20. show card info
21. show cardtype
22. show circuit-ID
23. show dmi info
24. show dot1bridge aging-time
25. show dot1dbridge ieee-tag priority remapping
26. show dot1dbridge ip-tc priority remapping
27. show ether config
28. show ether loopback capability
29. show ether loopback state
30. show ether security config
31. show ether statistics
32. show ether tdr config
33. show ether tdr test result
34. show fwd portlist
35. show fwddb config fdbid=<0-255>
36. show https config
37. show ip-mgmt config
38. show l2cp config
39. show loam config
40. show loam event config
41. show loam event log
42. show loam ignore-loopback-request
43. show loam peer info
44. show loam statistics
45. show lpt config
46. show mgmt vlan config
47. show port mac_learning state
48. show port vlan config
49. show port vlan tag config
50. show power config
51. show qos config
52. show qos priority remapping
53. show radius config
54. show redundancy info
55. show rmon statistics
56. show slot info
57. show snmp community
58. show snmp group [name=STR_SNMP_GRP]
59. show snmp local engine
60. show snmp local user
61. show snmp remote engine
62. show snmp remote user
63. show snmp traphost
64. show snmp view [name=STR_SNMP_VIEW]
65. show sntp config
66. show soam conferror vid=<1-4095> port=<1-2>
67. show soam ma [local-ma-id=<1-4294967295>]
68. show soam md [local-md-id=<1-4294967295>]
69. show soam meg [local-meg-id=<1-4294967295>]
70. show soam mep cc mep-id=<1-8191> local-parent-id=<1-4294967295>
71. show soam mep config [mep-id=<1-8191> local-parent-id=<1-4294967295>]
72. show soam mep dm status mep-id=<1-8191> local-parent-id=<1-4294967295>
73. show soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> tid=<0-4294967295>
74. show soam mep lmperiodic [mep-id=<1-8191> local-parent-id=<1-4294967295> far-end-mep-id=<1-8191>]
75. show soam mep loopback mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(unicast|multicast)
76. show soam mep stats [mep-id=<1-8191> local-parent-id=<1-4294967295>]
77. show soam mep test mep-id=<1-8191> local-parent-id=<1-4294967295>
78. show soam mip config [local-mip-id=<1-4294967295>]
79. show soam mip stats [local-mip-id=<1-4294967295>]
80. show soam port
81. show soam portid
82. show soam senderid
83. show ssh config
84. show ssh host-key
85. show ssh public-key user=USER
86. show switch mode

87. show syslog config
88. show system information
89. show sysuser
90. show tdm config
91. show tdm inband config
92. show tdm loopback capability
93. show tdm loopback state
94. show tdm peer inband config
95. show tdm port config
96. show timezone
97. show tndp tx state
98. show usb-port state
99. show vlan-db config
100. stat

Agent III C1|S1|L1D>

Appendix B. Web Interface vs. CLI Commands

This appendix provides a cross-reference of configurable parameters via the Web interface versus CLI commands.

Device Level Fields / Commands

Web Field	CLI Command
MAIN tab	**System Level Ops**
System Name	set system name / show system info
System Contact	set system contact / show system info
System Location	set system location / show system info
Console Access	set usb-port state / show usb-port state
Uptime Reset	reset uptime
System Reboot	reboot
All Counters Reset	reset all ports counters
Reset to Factory Config	reset factory
Device Description	blank
L2CP Disposition	set ethernet port l2cp configuration show ethernet port l2cp configuration
Login Type	set login method
VLAN ID	set management vlan id
Status	set management vlan admin state
Member Ports	set management vlan ports
Server Address (Syslog)	set syslog svr type=x addr=y
Server Port (Syslog)	set syslog svr port
Level (Syslog)	set syslog level
Mode (Syslog)	set syslog mode
TFTP Server Address	prov set tftp svr type=x addr=y
Firmware File Name	tftp put iptype=x ipaddr=y localfile=z tftp get iptype=x ipaddr=y remotefile=z

IP tab	IP operations
IP v4 Address Mode	set ip address mode (**Note**: "set dhcp state" replaced by "set ip address mode" after ION v 1.2.0.)
IP Address, Subnet Mask	set ip address
Default Gateway	set gateway address
DNS servers	set dns server
IPv6 Status	set ipv6-mgmt state
IPv6 IP Address Mode	set ipv6 addr mode
IPv6 IP Address	
IPv6 Prefix Length	
IPv6 Gateway Mode	set ipv6 gateway mode

ADVANCED tab	Advanced operations
FDB Aging Time	set dot1bridge aging-time=x
MAC Address Learning	set mac enable portlist=x
Transparent LPT	set transparent lpt state=x
Selective LPT	set selective lpt state=x
Monitoring Port	set lpt monitor-port
IEEE Priority Class: Remap x to (PID)	set dot1dbridge ieee-tag-priority=x remap-priority=y
IP Traffic Class: Remap 0 to: (DSCP)	set dot1dbridge ip-priority-index=x remap-priority=y
SNTP tab	**SNTP operations**
SNTP Client	set sntp status
Device Time	set current time
UTC Timezone	set sntp timezone
Daylight Saving Time	set sntp daylight savings time status
Daylight Saving Period Start	set daylight savings start time
Daylight Saving Period End	set daylight savings end time
Daylight Saving Offset	set daylight savings offset
SNTP Server x	set sntp server address

HTTPS tab	HTTPS operations
HTTPS Status	set https state
HTTPS Port	set https port number
Certificate Type	set https certificate-type
TFTP Server Address	prov set tftp svr type=x addr=y
Certificate File Name	set https certificate file
Private File Name	set https private key file
Private Password	set https private key file password
Copy Certificate button	start https certificate operations

SSH tab	SSH operations
SSH Server Status	set ssh server state
SSH Auth Timeout	set ssh timeout
SSH Auth Retries	set ssh authentication retry
Host Key Type	set ssh public-key user=x type=y
Save host key to flash	none; reserved for future use
Generate button	generate ssh host key
Delete	remove ssh host-key remove ssh public-key
User Name	set ssh public-key user=x
Public Key Type	set ssh public-key user=x type=y
TFTP Server Address	prov get tftp svr addr=x prov set tftp svr type=x addr=y
Source File Name	set ssh public-key user=x type=y file=z
Copy Public Key button	none
Delete button	remove ssh host-key remove ssh public-key

RADIUS tab	RADIUS operations
RADIUS Client	set radius authentication
Server Address	set radius server
Server Secret	set radius server secret

Retries	set radius retry
Timeout	set radius timeout

TACACS+ tab	TACACS+ operations
TACACS+ Client	set tacplus client state
Server Address	set tacplus Server / type / address
Server Secret	set tacplus server / secret
Retries	set tacplus server / retry
Timeout	set tacplus server / timeout

ACL tab	ACL operations
ACL Status	set acl state
Chain Name	set acl table=filter chain=input policy=x
Chain Policy	set acl table=filter chain=input policy=x
Rules: Priority	
Rules: Policy	add acl rule index=x position=y table=filter chain=input policy=z traprate=v condition=w
Rules: Trap Rate	set acl rule=x traprate=y
Rules: Add	add acl rule
Rules: Delete	remove acl rule
Condition: Type	set acl condition=x rule_index=y
Condition: Source or Destination	add acl condition type=x srcdst=y oper=z value=w
Condition: Operation	add acl condition type=x srcdst=y oper=z value=w
Condition: Value	add acl condition type=x srcdst=y oper=z value=v index=w
Condition: Add button	add acl condition type=x srcdst=y oper=z value=v index=w
Condition: Delete button	remove acl condition
ACL Status: Enabled/Disabled	restart acl

FDB tab	FDB operations
MAC Address	add fwddb mac=xx-xx-xx-xx-xx-xx
Port	add fwddb mac=x conn-port=y priority=z type=w
Priority	add fwddb mac=x conn-port=y priority=z type=w
Entry Type	add fwddb mac=x conn-port=y priority=z type=w
Add button Edit button Delete button	add fwddb set fwddb remove fwddb all/mac
Flush FDBs	flush fiddb type/all

VLAN tab	VLAN operations
VLAN ID	add vlan vid=x priority=y priority-override=z
Priority Override	set vlan vid=x priority=y priority-override=z
Priority	set vlan vid=x priority=y priority-override=z
Member Tag Port x	set vlan vid=x port=y memetag=z
Flush VLANs	flush vlandb all
Add button	add vlan vid=
Edit button	set vlan vid=x priority=y priority-override=z
Delete button	remove vlan=x

BACKUP-RESTORE tab (IONMM)	Backup - Restore operations
TFTP Server Address	none
Backup	none
Backup: Download button	tftp put
Restore	none
Restore: Upload button	tftp get

Upgrade tab (IONMM)	Upgrade operations
TFTP Server Address	prov get tftp svr addr=x prov set tftp svr type=x addr=y
Firmware File Name	tftp put iptype=x ipaddr=y localfile=z tftp get iptype=x ipaddr=y remotefile=z
Upload button	tftp upgrade
Upgrade (Targets)	none

SOAM tab	SOAM operations
MD sub-tab	set soam md=
MA/MEG sub-tab	set soam ma= set soam meg=
MEP sub-tab	set soam mep config= set soam mep lmperiodic=
MIP sub-tab	set soam mip

USERS Tab

Web Field	CLI Command
User Name	set sysuser name=nn
Password	set sysuser name= nn pass=xx
Confirm Password	set sysuser name= nn pass=xx confirmpass=xx
Level	set sysuser name= nn level=xxx

SNMP Tab (IONMM)

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 Group Name / Notify View Set SNMP Group Name / Read View Set SNMP Group Name / Write View 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

x323x Port Level Fields / Commands

MAIN Tab (Port Level)

Web Field	CLI Command
MAIN tab	**Main Port Level Ops**
Circuit ID	set circuit id, show circuit id
Admin Status	set ether admin state
Port Admin Mode	set port mgmtaccess
Far End Fault Mode	set ether fef=
Force Duplex	set duplex=x
Pause Admin Mode	set ether pause set ether dot3 pause
Port Forward Management – Forward Settings	set fwd portlist
L2CP Disposition	set l2cp configuration show l2cp configuration
Reset Counters	clear ether all counters
TN Topology Discovery Protocol TX	set tndp tx state=x

ADVANCED Tab (Port Level)

Web Field	CLI Command
ADVANCED tab	**Advanced Port Level Ops**
Rate Limiting Mode	set irate=x erate=y
Egress Rate Limit	set irate=x erate=y
Ingress Rate Limit	set irate=x erate=y
SA Lock	set ether src-addr-lock
SA Lock Action	set ether src-addr-lock
Filter Unknown Unicast	set ether filter-unknown-unicast
Filter Unknown Multicast	filter-unknown-multicast
Discard Tagged	set port discard-tagged
Discard Untagged	set port discard-untagged
Force Default VLAN	set ether force-default-vid
Default VLAN ID	set port default-vid
Default Priority	set qos default-priority=x
IEEE Priority Class	set dot1dbridge ieee-tag-priority=x set dot1dbridge ip-priority-index=x
IP Traffic Class	set qos priority tag-type=x
Priority Precedence	set vlan vid=x fid=y priority=z set qos priority by-dst-mac set qos priority by-src-mac set qos priority by-vlan-id set qos priority ieee-tag set qos priority ip-tag set qos priority tag-type
SA Priority Override	set qos priority by-src-mac
DA Priority Override	set qos priority by-dst-mac
VID Priority Override	set vlan vid=x fid=y pri-override=z
Frame Tag Mode	set port vlan tag mode=
Provider Ether Type	set port vlan tag provider ethtype
User Priority - Remap 0 to:	set fwd portlist
Egress Queue Mode	set port egress queingmethod

COUNTERS tab (Port Level)

Web Field	CLI Command
COUNTERS tab	**Port Level Counters Ops**
Reset Counters button	reset all ports counters

LOAM tab (Port Level)

Web Field	CLI Command
LOAM tab	**Port Level LOAM operations**
Main sub-tab:	
Admin Status	show loam config show loam event config show loam event log show loam ignore-loopback-request show loam peer show loam statistics
LOAM Mode	set loam mode
LOAM Peer Information	show loam peer info
LOAM Vendor OUI	show loam peer info
Loopback Type	set loam loopback type
Ignore Loopback Request	set loam ignore (loopback request)
Counters sub-tab:	
Reset LOAM Counters button	reset all ports counters
Event Configuration sub-tab:	
Error Symbol Period Window High Bits Error Symbol Period Window Low Bits Error Symbol Period Threshold High Bits Error Symbol Period Threshold Low Bits Error Symbol Period Event Notification Error Frame Period Window Error Frame Period Threshold Error Frame Period Event Notification Error Frame Window Error Frame Threshold Error Frame Event Notification Error Frame Seconds Summary Window Error Frame Seconds Summary Threshold Error Frame Seconds Event Notification	set loam critical-evt-notif set loam dg-evt-notif set loam ef set loam ef-evt-notif set loam efp set loam efp-evt-notif set loam efss set loam efss-evt-notif set loam esp set loam esp-evt-notif
Dying Gasp	set loam dg-evt-notif
Critical Event	set loam critical-evt-notif

DMI tab

Web Field	CLI Command
DMI tab (Port 2 only)	**Port Level DMI Ops**
Rx Power Intrusion Threshold (µW)	set power relay state
IONPS-A or IONPS-D chassis device: Temperature Sensor tab Voltage Sensor tab Power Sensor tab Fan tab	 set sensor stid x notif set sensor stid x relation set sensor stid x severity set sensor stid x value

Remote Device Level

Web Field	CLI Command
BACKUP-RESTORE tab	**Backup - Restore operations**
TFTP Server Address	tftp put iptype=x ipaddr=y localfile=z tftp get iptype=x ipaddr=y remotefile=z
Backup	none
Backup: Download button	tftp put
Restore	none
Restore: Upload button	tftp get
UPGRADE tab (IONMM)	**Upgrade operations**
TFTP Server Address	prov set tftp svr type=x addr=y
Firmware File Name	update firmware-db file=x
Upload button	upgrade module
Upgrade (Targets)	none

Remote Device Port Level

Web Field	CLI Command
MAIN tab	**Port Level MAIN Ops**
AutoCross Mode	set ether autocross=x
Auto Negotiation	set ether autoneg state=x
Capabilities Advertised	set ether adv-cap=x
Force Speed	set ether speed=x
Force Duplex	set ether duplex=x

Appendix C. CLI Messages and Recovery

This section documents the messages may display during CLI operations, and recommended recovery procedures.

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 "Appendix A: CLI Command Summary".
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. For example:

```
C1|S5|L1P2>set ether adv-cap 1000TFD
Bad advertisement capability!
```

1. Verify the command syntax.
2. Verify the NID supports the capability.
3. Retry the operation. For a complete list of the available commands, see "Appendix A: CLI Command Summary".
4. If the problem persists, contact Technical Support. US Tel: 952.941.7600 or Toll free: 1.800.526.9267 or Fax: 952.941.2322. Int'l web.

Cannot get link pass through information on this card

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

1. Use the **go** command to change from the IONMM to the specific slide-in module. The **go** command format is:
   go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a slide in card, or
   go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a Standalone card
2. Retry the operation. For a complete list of the available commands, see "Appendix A: CLI Command Summary".
3. If the problem persists, contact Technical Support.

Cannot get LOAM configuration on this port!
Cannot get LOAM event log on this port!
Cannot get LOAM peer information on this port!

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

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a slide in card, or
   go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a Standalone card
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Cannot get port security on this port!

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

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a slide in card, or
   go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a Standalone card
1. Retry the operation. For a complete list of the available commands, see "Appendix A: CLI Command Summary".
2. 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. Make sure you enter all the keywords or values required by this command.
2. 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.
3. Retry the operation.
4. 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 a Standalone card
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Error: this command should be executed on a port

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

1. Use the **go** command to change location of where the command operates. The **go** command format is:
   go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a slide in card, or
   go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   for a Standalone card
2. Retry the operation.
3. For a complete list of the available commands, see the ION System CLI Reference Manual, 33461.
4. If the problem persists, contact Technical Support.

Fail to get MAC address!

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

1. Verify that the correct hierarchy has been specified in the command.
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds 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.

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.

3. If the problem persists, contact Technical Support.

Incomplete location command!
Incomplete location parameters, lack of level1 attachment port!

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

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

1. Verify the command syntax.
2. Re-enter the **go** command and be sure to include all of the location parameters:

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

   for a slide in card, or

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

   for a Standalone card

3. If the problem persists, contact Technical Support.

Invalid ACL condition index!

This message indicates that you tried to associate an ACL condition with an ACL rule but the condition does not exist.

1. Check what conditions exist; type:

   show acl condition

2. Associate the correct condition with the correct rule, or create the condition if it does not exist.

3. If the problem persists, contact Technical Support.

Invalid ACL rule index!

This message indicates that you tried to associate an ACL condition with an ACL rule that does not exist.

1. Check what rules exist; type:

   show acl rule

2. Associate the correct condition with the correct rule, or create the rule if it does not exist.

3. If the problem persists, contact Technical Support.

Invalid condition value: xxxx

This message indicates that the input for the value= parameter on the **add acl condition** command in not valid.

1. Verify the value being input; it must match with the value input for type=.

2. Retry the operation.

3. If the problem persists, contact Technical Support.

Invalid location parameters, cannot find the physical entity!

This message indicates that the system cannot detect the presence of the device or port specified in the **go** command. For example, you entered the command **go l1p=3** on a device that supports two ports.

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

Invalid user!

This message indicates that the specified user is not valid.

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

Login incorrect

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

1. Verify the login/password.

   Note: the login and password are case sensitive. The default login is **ION** and the default password is **private**.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

No DMI support on this port!

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

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

Now the value of table can only be "filter"!

You entered an unsupported ACL table or chain parameter value. For example:

```
C1|S7|L1D>set acl table {raw|nat|mangle}
C1|S7|L1D>set acl table raw chain prerouting|input|forward|output|postrouting}
C1|S7|L1D>set acl table nat chain {prerouting|input|forward|output|postrouting}
C1|S7|L1D>set acl table mangle chain {prerouting|forward|output|postrouting}
```

1. Enter the parameters table=filter and chain=input.
2. Retry the operation.
3. If the problem persists, contact Technical Support.

There is no matched command

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

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

Unable to open xx. Please check your port settings.

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

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

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

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 (PC).
7. Reboot the IONMM.
8. If the problem persists, contact Technical Support.

Error, you should first give full location parameters

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

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

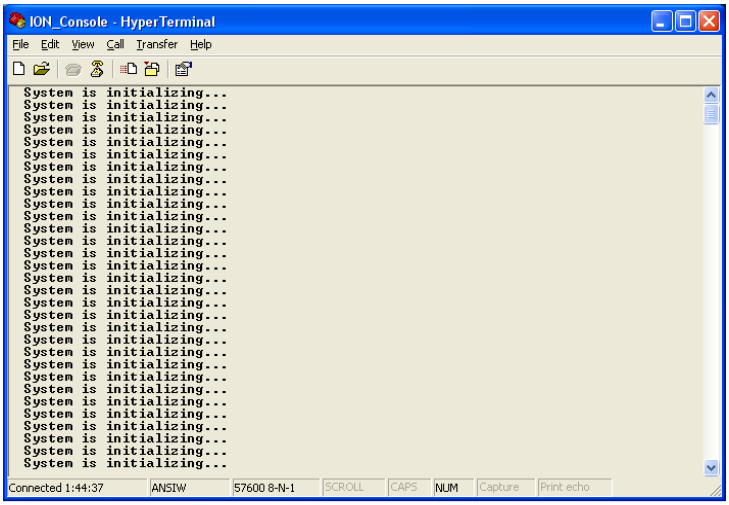
If the value of module, slot and port are not set in later commands, and then you run a device-level command (e.g., **show lpt config**), this error message displays.

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

go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
for a slide in card, or
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
for a Standalone card

System is initializing...

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



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

Start HTTPS certificate failed.

1. Verify the HTTPS parameters (HTTPS is enabled, the certificate type is defined, certificate file defined, private key file defined, password defined).
2. Verify that the HTTPS server is operational.
3. Retry the operation (i.e., type **start https certificate** and press **Enter**).
4. If the problem persists, contact Technical Support.

This command is only available on <x323x> card!

1. Verify the command entered is the one you want.
2. Verify that the device for the command entered can support the function of the command (e.g., SOAM functions / commands are supported by NID models S323x / C323x NIDs).
3. Retry the operation (i.e., type **show soam port** and press **Enter**).
4. If the problem persists, contact Technical Support.

Error: this command should be executed on a port!

1. Verify the command entered is the one you want.
2. Change to the desired port; enter the **go** command with all 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, "Appendix A: CLI Command Summary".
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 "Appendix A: CLI Command Summary".
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=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
   (on 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)
   (on a Standalone card).
2. For a complete list of the available commands, "Appendix A: CLI Command Summary".
3. If the problem persists, contact Technical Support. .

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. If the problem persists, contact Technical Support.

Invalid dot1dbridge MAC address!

You tried to add a fwddb (Forwarding Database) with an unacceptable address. For example, you typed:

```
C1|S3|L1D>add fwddb mac 11
```

and then pressed **Enter**.

1. Verify the CLI command syntax. See "Forwarding Database Commands".
2. Retry the operation with a valid MAC address.
3. If the problem persists, contact Technical Support.

Invalid erate!
Invalid irate!

You tried to set the Ingress or Egress rate to an unacceptable limit. For example, you typed:

```
C1|S3|L1D>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.
3. If the problem persists, contact Technical Support.

TFTP transfer failed!

The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.

1. Verify the CLI command syntax.
2. Verify the firmware version.
3. Be sure the TFTP server is configured and running.
4. Check that the remotefile is in the proper location (e.g., the file *x323x.bin.1.0.5* is at *C:\TFTP-Root*).
5. Retry the operation. See the **tftp upgrade** command section.
6. 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.
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 (e.g., C1|S7|L1D>set rfd state enable).

1. Verify that the card you entered the command on supports this function. See "Set RFD State".
2. Retry the operation. See the **dot1bridge aging-time** command.
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).

1. Verify that the card you entered the command on supports this function.
2. Retry the operation. See the **dot1bridge aging-time** command.
3. If the problem persists, contact Technical Support.

Fail to set aging time!

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

1. Verify the **dot1bridge aging-time** command syntax. See "Configure Forwarding Learning Aging Time".
2. Retry the operation. See the **dot1bridge aging-time** command.
3. If the problem persists, contact Technical Support.

Get aging time failed!

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

1. Verify the **dot1bridge aging-time** command syntax. See "Configure Forwarding Learning Aging Time".
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.
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.
3. If the problem persists, contact Technical Support.

The MD with this id has been configured already.

The MD that you tried to create has already been defined. For example, you entered the command: **add soam md local-md-id 1 md-name none md-level 7**, but that local-md-id already exists.

1. Verify that the local-md-id you entered is the one you want.
2. Retry the operation with a unique MD ID. See the "Add Maintenance Domain" command.
3. If the problem persists, contact Technical Support.

MA/MEG with this id has been configured already.
MIP with this id has been configured already.

The MA or MEG that you tried to create has already been defined. For example, you entered the command: **add soam ma local-ma-id=1 local-maid=1 ma-name=maid1 vlan-type=ctype**, but that local-ma-id already exists. Or you entered the command a**dd soam mip mip-type y.1731 local-mip-id 1 local-parent-id 1 port 1**, but the MIP already exists.

1. Verify that the **local-ma-id** or **local-mip-id** that you entered is the one you want.
2. Retry the operation with a unique MA, MEG or MIP. See the "Add Maintenance Association" command.
3. If the problem persists, contact Technical Support.

Add SOAM MIP failed.
Such MIP (port, level, VID(s)) already configured.

The MIP that you tried to create has already been defined. For example:

C1|S3|L1D>**add soam mip mip-type y.1731 local-mip-id 2 local-parent-id 1 port 1**

1. Verify that the **local-ma-id** or **local-mip-id** that you entered is the one you want.
2. Retry the operation with a unique MA, MEG or MIP and/and parameters. See the "Add Maintenance Association" command.
3. If the problem persists, contact Technical Support.

MD cannot be deleted. There are MAs configured on this MD.

The MD that you tried to delete has MAs defined for it. For example, you entered the command: **remove soam md local-md-id=1**, but an MA has been defined for and associated with it.

1. Verify that the local-md-id you entered is the one you want.
2. Delete the associated MA(s).
3. Try again to delete the MD. See the "Remove Maintenance Domain" command section.
4. If the problem persists, contact Technical Support. .

MEP with this id not been configured yet.
MIP with this id not been configured yet.

You entered a command to show or set MEP or MIP configuration information, but you have not yet defined the MEP (or MIP). For example, you entered the command **show soam mep cc mep-id=1 local-parent-id=10**, but that MEP ID does not yet exist.

1. Verify that the local-mep-id you entered is the one you want.
2. Create a unique MEP. See the "Add a MEP" command.
3. Retry the operation with the unique MEP (or MIP).

4. If the problem persists, contact Technical Support.

Send SOAM Unicast Loopback failed.

Can't read last soam error description

You entered the command **send soam mep loopback**, but the last soam error description was unreadable.

For example, you entered the command:

send soam mep loopback mep-id=10 local-parent-id=1 dest=10 amount-frames=1.

1. Make sure the SOAM port is configured and enabled.
2. Verify the command parameter entries.
3. See the "Initiate a Loopback Request" command.
4. Enter the **show soam conferror vid=x port=y** to verify there are "No config errors".
5. If the problem persists, contact Technical Support.

An error has been occurred during LTM sending.

A problem occurred when performing a Linktrace function. For example, you entered the command:

send soam mep linktrace mep-id=10 local-parent-id=1 dest=10 use-fdb-only=false ttl=1.

1. Verify that the parameters were entered correctly.
2. Verify the forwarding database is configured and enabled.
3. Enter the **show soam conferror vid=x port=y** to verify there are "No config errors".
4. Retry the operation.
5. If the problem persists, contact Technical Support.

Add SOAM MIP failed.
Can't read last soam error description

You entered the command **add soam mip mip-type**, but the last soam error description was unreadable.

For example, you entered the command:

send soam mep loopback mep-id=10 local-parent-id=1 dest=10 amount-frames=1.

1. Make sure the SOAM port is configured and enabled.
2. Verify the parameter entries. See the "Add SOAM MIP" command.
3. Enter the **show soam conferror vid=x port=y** to verify there are "No config errors".
4. Retry the operation.
5. If the problem persists, contact Technical Support.

Get SOAM MIP stats no such object.

You entered the command **show soam mip stats**, but that object does not yet exist.

1. Make sure the SOAM MIP is configured and enabled.
2. Verify the command parameters. See the "show mip statistics" command.
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Invalid user!

You entered the command **show ssh public-key user admin**, but specified the wrong user.

1. Retry the operation using the correct user information. See "Show SSH Public Key of a User".
2. If the problem persists, contact Technical Support.

Fail to set SSH server state!

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

1. Use the **get** command to obtain the key file. See the "TFTP Commands".
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.
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.
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 service** command.
2. Review the set mgmt vlan command syntax for the port / state / vid. See the "VLAN Commands".
3. If the problem persists, contact Technical Support.

Upgrade is only supported on IONMM card!

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

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

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

Cannot set bandwidth alloc type on this card!

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

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

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

Cannot set ingress and egress rate on this card!

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

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

1. Verify if the card supports rate limiting. Try the syntax **set irate=unLimit erate=unLimit**.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands".
4. If the problem persists, contact Technical Support.

DMI is only supported on FIBER port!

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

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

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

Link OAM is not supported on this card!

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

```
C1|S7|L1P1>show loam 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 "LOAM Commands".
4. If the problem persists, contact Technical Support.

Cannot clear loopback counters on this card!
Cannot clear counters on this port!
Cannot get port security configuration on this port!
Cannot remove VLAN from the database!
Cannot reset all ports' counters on this cards!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set aging time on this card!
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 management VLAN on this card!
Cannot set PHY mode on this port!
Cannot set pause on this port!
Cannot set source address lock action on this port!
Cannot set USB port state on this card!
Cannot show aging time on this card!
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!
Fail to get MAC control frames statistics!
Fail to get auto-negotiation state!
Fail to get port redundancy state!
Fail to set dot3 pause
No Time-domain reflectometer support on this card!

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

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

1. Verify if the device or port supports the desired function. See Table 5 in the section "Ethernet Port Commands".
2. Use the **go** command to switch to a different card or port supporting the desired feature (e.g., loop-back).
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".

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 service
Cannot show VLAN service configuration on this card!
```

1. Verify if the card supports the desired function.
2. Use the **go** command to switch to a different card port supporting VLAN.
3. Verify the command entry. See "VLAN Commands".

Fail to get system name!

You entered a command to display 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. Use the **set system name** command to enter the **System Name** information (e.g., **set system name**=NAME). 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.
3. Remove and reset the card.
4. Try the operation again.
5. 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 ! or # or % or & characters).
2. Remove and reset the card.
3. Try the operation again.
4. If the problem persists, contact Technical Support.

System is busy, please retry this command later!
You entered a **show** or **set** command, but the command was not accepted by the system.

For example:

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

1. Wait 1-2 minutes minute 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 192.168.1.10 (192.168.1.10): 56 data bytes
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

1. Verify the IP address.
2. Check the cable connection.
3. Refer to the p**ing** 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 loam 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 LOAM admin state=enable** command to enable OAM administration.
3. Use the **show loam loopback** commands and **show loam 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.

Cannot 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
Cannot 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 maker 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. US Tel: 952.941.7600 or Toll free: 1.800.526.9267 or Fax: 952.941.2322. Int'l web.

Set Ethernet port loopback type failed.

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

```
C1|S16|L1P1>set loam loopback type=phylayer
Set Ethernet port loopback type failed.
C1|S16|L1P1>
```

1. Verify the command syntax.
2. Use the **set loam loopback type** command to set the device's type of loopback support.
3. If the problem persists, contact Technical Support. US Tel: 952.941.7600 or Toll free: 1.800.526.9267 or Fax: 952.941.2322. Int'l web.

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 loam ef threshold 100099
```

1. Enter the command **set loam ef threshold=** with a threshold number from 0-999999.
2. See the **set loam ef threshold** command for details.

3. If the problem persists, contact Technical Support. US Tel: 952.941.7600 or Toll free: 1.800.526.9267 or Fax: 952.941.2322. Int'l web.

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.
2. Create an ACL rule. See "Add a New ACL Rule".
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 x323x card).
2. Try entering the **show system information g** command again.
3. If the problem persists, contact Technical Support.

Getting remapping priority fail

You entered a **show dot1dbridge** command but the command failed to execute. For example:

```
C1|S10|L1D>show dot1dbridge ieee-tag priority remapping
IEEE priority-index              remapping-priority
------------------------------------------------------
Getting remapping priority fail
```

1. Verify the command syntax.
2. Use the **set dot1dbridge** command to set the remapping priority. See the "Dot1dbridge Commands".
3. If the problem persists, contact Technical Support.

Set IEEE tag priority remapping failed!

You entered a **set dot1dbridge** command but the command failed to execute. For example:

```
C1|S10|L1D>set dot1dbridge ieee-tag-priority 0 remap-priority 1
Set IEEE tag priority remapping failed!
```

1. Verify the command syntax.
2. Use the **show dot1dbridge** command to display the remapping priority setting. See the "Dot1dbridge Commands".
3. Try the **set dot1dbridge** command again.
4. If the problem persists, contact Technical Support.

Set IP traffic class priority remapping failed!

You entered a **set dot1dbridge** command but the command failed to execute. For example:

```
C1|S10|L1D>set dot1dbridge ip-priority-index 2 remap-priority 1
Set IP traffic class priority remapping failed!
```

1. Verify the command syntax.
2. Use the **show dot1dbridge** command to display the remapping priority setting. See the "Dot1dbridge Commands".
3. Try the **set dot1dbridge** command again.
4. If the problem persists, contact Technical Support.

No such file or directory

You entered a **cat** or **ls** command, but the parameters you specified could not be found. For example:

```
C1|S16|L1P1>ls 1 2
ls: 1: No such file or directory
ls: 2: No such file or directory
C1|S16|L1P1>
```

or

```
C1|S16|L1P1>cat 1 2
cat: 1: No such file or directory
cat: 2: No such file or directory
2C1|S16|L1P1>
```

1. Verify the [OPTION] and [FILE] parameters are entered accurately.
2. Review the **cat** or **ls** command section of this manual.
3. Try entering the **cat** or **ls** command again.
4. If the problem persists, contact Technical Support.

Cannot set slot power on this card!

You entered a s**et slot power=** command on a device that does not support it. For example:

```
C1|S16|L1P1>set slot 16 power on
Cannot set slot power on this card!
```

1. Verify this is the command you want.
2. Verify the command parameter; make sure you are not trying to power up a slot that already has power.
3. Use the **go** command to switch to the slot you want.
4. If the problem persists, contact Technical Support.

Error: this command should be executed on a power sensor or fan!

You entered a s**et sensor** command on a device that does not support it. For example:

```
C1|S16|L1P1>set sensor stid 1 notif enable
Error: this command should be executed on a power sensor or fan!
```

1. Verify this is the command you want.
2. Use the **stat** command to show the chassis configuration. For example:

```
[ 22]  IONPS-A
  Temperature Sensor
  Volatage Sensor
  Power Sensor
  Fan-1
  Fan-2
```

3. Use the **go** command to switch to the power sensor or fan.
4. If the problem persists, contact Technical Support.

MA with this id has not been configured yet.
MA/MEG with this id has not been configured yet.
MD with this id hasn't been configured yet.
The MAs table is empty.
The MEGs table is empty.
Vlans ID list is empty.

You entered a SOAM command before creating a prerequisite entity. For example:

```
C1|S10|L1D>show soam mep lmperiodic mep-id 1 local-parent-id 10 far-end-mep-id 3
MA/MEG with this id has not been configured yet.
```

1. Create the required SOAM entity (an MA or a MEG in the example above).

2. Try entering the SOAM command again (e.g., show soam mep Imperiodic in the example above).
3. Use the **show soam mep config** command to check the configuration.
4. If the problem persists, contact Technical Support.

The MEP ID parameter is out of range.

You entered a SOAM command for an undefined parameter entry. For example:

```
C1|S10|L1D>show soam mep stats mep-id=1
The MEP ID parameter is out of range.
```

1. Verify the SOAM parameter entry is valid (e.g., a MEP ID of 0 is invalid; the valid range is 1-8191).
2. Use the **show soam mep config** command to check the configuration.
3. Enter the SOAM command again.
5. If the problem persists, contact Technical Support.

Get SOAM MEPs first index timeout.

You entered a SOAM command but a timeout occurred before the item was found. For example:

```
C1|S10|L1D>show soam mep config
Get SOAM MEPs first index timeout.
```

1. Verify the SOAM parameter entries are valid and complete.
2. Use the **show soam mep config** command to check the configuration.
3. Enter the SOAM command 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. Do not enter any space in the command string. Do not enter more than 8 modules.
2. See the "upgrade module" command for more information.
3. If the problem persists, contact Technical Support.

L2CP is not supported on this card!

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

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

Please 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".
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".
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".
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.
2. Continue the operation.
3. 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 loam 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 loam admin state enable**" command).
2. Verify the command syntax.
3. Use the **set loam loopback ?** command to display the card's loopback capabilities. For example:

```
C1:S7:L1P1>set loam loopback type ?
 alternate
 noloopback
 remote
```

4. Re-enter the **set loam loopback=** command with a loopback capability supported by the card (alternate, or remote or noloopback).
5. Verify the loopback capability with the **show loam loopback capability** command. For example:

```
C1|S5|L1P2>show loam loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P2>
```

6. If the problem persists, contact Technical Support.

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
Cannot 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!

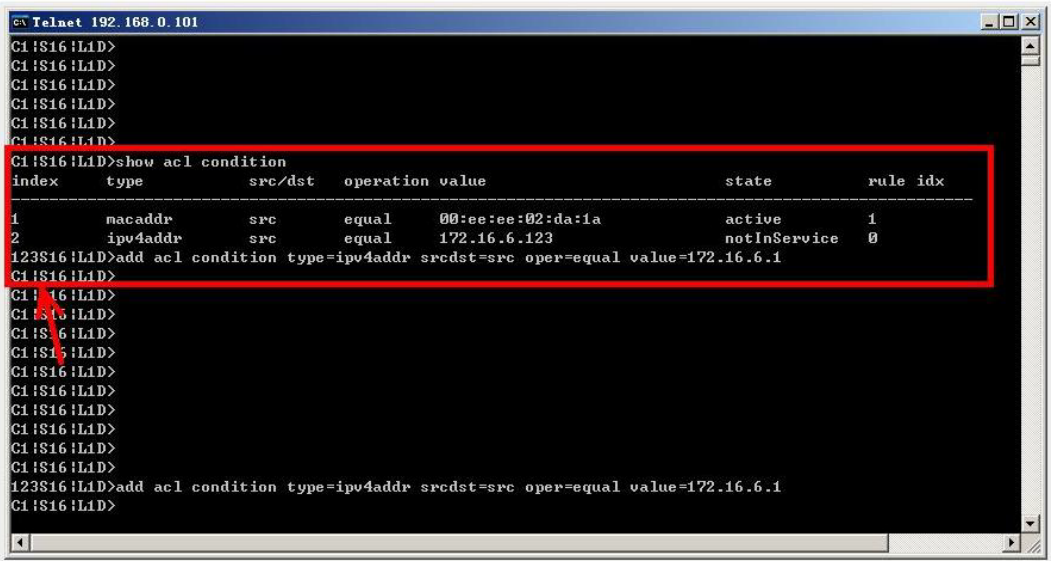
This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability (**set ether adv-cap**) command are not valid choices. For example:

```
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".
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. .

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.

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 cannot 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 1 - 268435455!
Error frame period window is out of range, its range is 1 - 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 - 9000!

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" in the *ION System x323x Remotely Managed Network Interface Device (NID) User Guide*, 33432.
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 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!
Unknown MAC type!

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" to create the VLAN FDB entry. See the *ION x323x NID User Guide* for more information.
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" in the *ION x323x NID User Guide* 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.

Show SOAM FLM Error!

You tried to display SOAM MEP FLM (Frame Loss Measurement) results, but the information was not available. For example:

```
C1|S5|L1D>show soam mep lmperiodic
Show SOAM FLM Error!
C1|S5|L1D>
```

1. Make sure this is the function that you want.
2. Review the "MEP Frame Loss Measurement Commands".
3. If the problem persists, contact Technical Support.

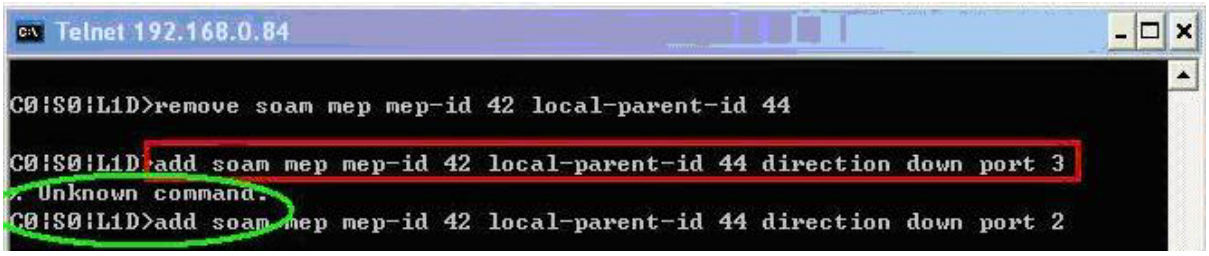
Error: location parameter should be digital number!
You entered a letter or special character as part of the **go** command. For example:

```
C1|S7|L1P2>go c=s s=5 l1d
Error: location parameter should be digital number!
C1|S7|L1P2>
```

1. Re-enter the **go** command with the correct syntax (e.g., change the letter **s** to a number in the example above).
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support.

Unknown command.

Problem: Can't add a MEP on Port 3 either via the Web interface or the CLI.
Meaning: You entered the **add soam mep** command, and the message "*Unknown command.*" displays.



Recovery:
1. See "SOAM Configuration Prerequisites and Restrictions".
2. Retry the operation using a different port (i.e., Port 1 or Port 2).
3. If the problem persists, contact Technical Support.

Problem: SOAM 802.1ag MIP can't be deleted via Web or CLI.
Problem: SOAM MIP vanishes after a reboot.
Problem: Cannot configure AIS on SOAM 802.1ag MIP.
Message: MIP with this ID has not been configured yet.
Message: Add SOAM MIP failed. MEP on such port, VLAN(s) and higher/same level already configured.
Message: Deleting MIP failed. MEP ID is absent in the MA MEP's ID list. (snmp operation error)

Meaning: 802.1ag SOAM does not support AIS. This manifests in several ways, including:

1. AIS attributes cannot be created if MIP type is 802.1ag.
2. AIS attributes do not display in table if MIP type is 802.1ag.
3. Adding a new MIP apparently fails.
4. Deleting an existing MIP apparently fails.
5. An existing MIP apparently ceases to exist after a reboot.

The add new MIP issue occurs when you either try to create an 802.1ag type MIP via the Web interface, or you enter an invalid configuration for the MIP, such as trying to create to create two MIPs on the same port with same level.

Trying to add two 802.1ag type MIPs on ports 1 and 2 fails, with the "*Add SOAM MIP failed*." Web interface message displayed on the bottom left of the screen. This fails because when an 802.1ag MIP is created via the Web interface, AIS attributes are also sent with the create request. Since AIS attributes are invalid under 802.1ag, the MIP creation fails in the SOAM stack. However, in spite of the failure when a refresh is done on the web, the entries for the MIPs are shown on the Web as if they actually were created in the system. Because the MIP creation actually did not succeed, the entries are not saved in flash, so when a card power cycles or reboot is done, these entries are lost from RAM and not shown at all on the Web interface.

If you try to create a new MIP ID on a same port using the same MEG ID, the CLI displays the "Add SOAM MIP failed." message indicating that the MIP was not successfully created. But when a refresh is done via CLI or Web, the new MIP entry is displayed. In this case, the MIP is not actually created in the SOAM stack and hence not saved in flash, so after a reset the MIP entry is lost. The reason that MIP creation is not allowed is because only one MIP is allowed per MEG level and per port.

For example:

```
C1|S6|L1D>add soam mip mip-type y.1731 local-mip-id 1 local-parent-id 1 port 2
Add SOAM MIP failed. MEP on such port, VLAN(s) and higher/same level already configured.
C1|S6|L1D>show soam mip config
MIP id : 1
MEG local ID : 1
MEG level : 3
MEG name : Test
MEG VLANs : ctype: 500
Port : 2
Admin status : disabled
AIS transmit : disabled
AIS interval : 1s
AIS frame priority : 7
C1|S6|L1D>
```

An issue can occur if you try to delete an existing MIP, but deleting the MIP fails. For example:

```
C1|S6|L1D>remove soam mip local-mip-id 6
MIP with this id has not been configured yet.
C1|S6|L1D>show soam mip config
MIP id          : 6
MD local ID     : 7
MD level        : 7
MD name         : Level7MD
VLANs           : ctype: 500
Port            : 2
Admin status    : enabled
C1|S6|L1D>
```

Recovery:

1. Make sure this is the function you want. See "SOAM (Service OAM) Configuration" in the x323x User Guide.
2. Review the "SOAM Configuration Prerequisites and Restrictions" and read the Notes information below.
3. Use the CLI to create either an 802.1ag MIP or Y.1731 MIP. See "SOAM MIP Config – CLI Method" in the x323x User Guide.
4. Use Y.1731 for SOAM operations via the Web interface. See "ITU-T Y.1731 Configuration" in the x323x User Guide. Via the Web interface, create one or more Y.1731 MIPs.
5. Reboot and retry the SOAM MIP operation.
6. If the problem persists, contact Technical Support.

Notes:

1. AIS is not recommended for environments utilizing STP (spanning tree protocol), since STP provides its own restore capability. Due to AIS' STP (and other) limitations, the IEEE decided not to support AIS in 802.1ag.
2. For point-to-point S-VLANs/Ethernet connections, there is just one remote peer MEP that cannot be reached. But for multipoint S-LANs/Ethernet connections, a client layer MEP, on receiving an AIS, cannot determine which of its remote peers have lost connectivity. It is recommended that for multipoint, the client layer MEP should suppress alarms for all peer MEPs.

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 cannot set port duplex now!

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

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

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.

Add SOAM MEP failed.
Port not a member of the VLAN.

Add SOAM MIP failed.
Port not a member of the VLAN.

You tried to add a MEP or MIP, but the VLAN does not recognize the associated port. For example:

```
S3230>add soam mep mep-id 1 local-parent-id 1 direction up port 5
Add SOAM MEP failed.
Port not a member of the VLAN.
S3230>
```

1. Select a different port number and continue operation.
2. Review the **add soam mep** command or **add soam mip** command description.
3. Use the **show soam port** command to verify the current SOAM ports' state configurations.
4. 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 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 "default values and valid ranges".
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. 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!

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. Warning message that the **set tndp=disable** command disables management of the device from the IONMM. 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. The **set tndp=disable** command is a port level command; use the go command to switch to a port and re-enter this command.
6. Verify that this card supports the TNDP disable function.
7. Check the syntax and re-enter the command. Refer to the "TNDP Commands".

5. If the problem persists, contact Technical Support.

IP management is not supported on this card!
TAOS status setting is not supported on this card!
You entered a command for a function that is not supported on the x323x. 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 x323x.
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".
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".

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".

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 x323x.
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!
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!
TDM config is not supported on this card!

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 that supports this function.
3. Use the ION Web interface to perform this 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.
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 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 x323x 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 x3230.
3. Refer to the "Configuring MAC Address Learning" section 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.
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: Cannot 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 (edit) , or delete an ION user, but the operation failed.

1. Verify that this is the operation you want.

2. Retry the operation; be sure to type the parameters as shown in the "Configuring System / Login Users" section.

3. If the problem persists, contact Technical Support.

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

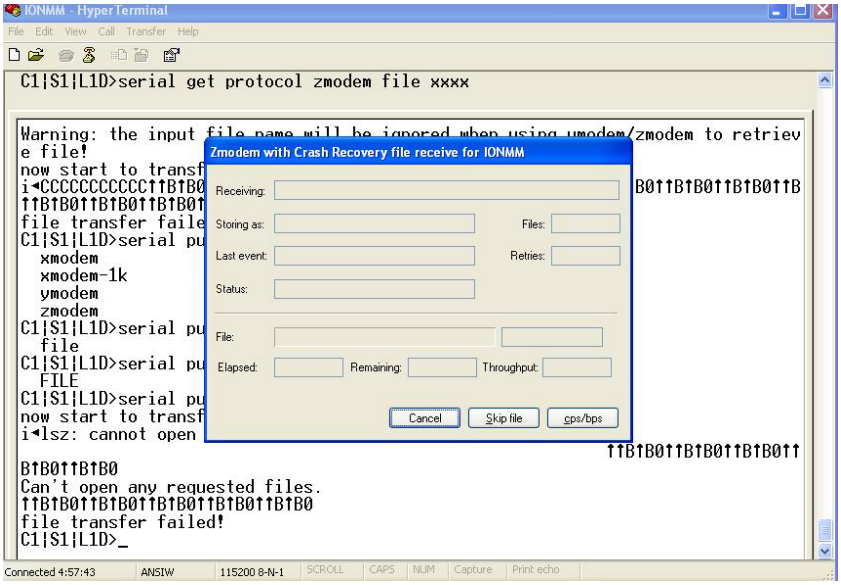
You entered a Serial File Transfer command, but the operation failed.

1. Verify that this is the operation you want (e.g., serial get/put/upgrade command).

2. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section.

3. If the problem persists, contact Technical Support.

File Transfer Failed - ZModem Crash Recovery dialog box:



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

1. Either enter the requested information and click **cps/bps**, or click **Skip file**, or click **Cancel**.

2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.

3. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section.

4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.

5. If the problem persists, contact Microsoft or Hilgraeve Technical Support:

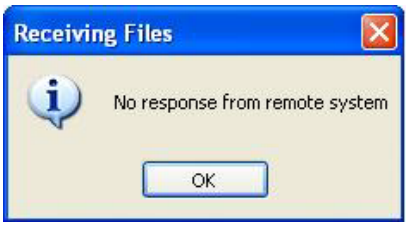
HyperTerminal Support

HyperTerminal is part of certain Microsoft Windows versions and is supported by Microsoft with 24-hour worldwide responsibility for Windows communications components. Contact Microsoft Windows Support at (425) 635-7000, or contact your computer manufacturer. See the Microsoft Support knowledge base for articles regarding your topic: http://support.microsoft.com/directory/ and do a key word search using your issue keywords.

HyperACCESS Support

Certain other Microsoft Windows versions do not include HyperTerminal support. HyperACCESS is the official, full powered Hilgraeve version of HyperTerminal Private Edition. Hilgraeve's HyperACCESS is available f you need a more powerful HyperTerminal alternative. For questions call (734)-243-0576 ext. 1# or see http://www.hilgraeve.com/support/ .

Receiving Files - No response from remote system



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

1. Click the **OK** button to clear the message dialog box.

2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.

3. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section.

4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.

5. If the problem persists, contact Technical Support.

The specified module does not exist!

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

1. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section.

2. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.

3. If the problem persists, contact Technical Support.

Cannot find software version of this card!

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

1. Check the card's current firmware version.
2. Upgrade the firmware. See "TFTP Transfer / Upgrade Commands" or "Upgrade / Update Firmware Commands". Retry the operation.
3. If the problem persists, contact Technical Support.

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

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

1. Upgrade the card firmware. See "TFTP Transfer / Upgrade Commands" or "Upgrade / Update Firmware Commands".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

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

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

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

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

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

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

The confirm password is not identical with the password!
The user name length must be in range [1..64]!
The user name must begin with an alphanumeric char!
You can only change your own password, not others!

You entered a command to create a new system user, but the command failed.

1. Verify the command syntax ("add sysuser name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR").
2. Retry the operation, making sure the "pass" and "confirmpass" entries match. See the related command section.
3. If the problem persists, contact Technical Support.

Cannot set irate because irate is bigger than port speed!
Cannot set erate because erate is bigger than port speed!
Egress Rate Limit - Web interface and CLI behaviors do not match
Web Egress Rate Limit and CLI "show ether config" command rates do not match.

At the C3220 > Port 1 > ADVANCED tab > Egress Rate Limit field, you modified the bandwidth allocation display value successfully, but the Web interface and CLI behaviors do not match.
For instance, you link up the C3220-1040 copper port at 1000Mfull, and set copper port Egress Rate Limit to 900M. If you then uncheck the copper port "Capabilities Advertised" options of "1000M - Half Duplex" and "1000M - Full Duplex", and set the copper port link up at 100Mfull, in the Web, the copper port Egress Rate Limit will return to "Unlimited"; but in the CLI, the copper port Egress Rate Limit still shows "rate900M" (i.e., the port speed is 100M-full, but you still can display/set the rate limit to rate900M through the CLI).

1. Re-enter the irate / erate command bandwidth settings.
2. Retry the operation.
3. See "Bandwidth Commands" for more information.

ERROR: There is already a same named user!
ERRPR: User name cannot be modified!

You tried to add or change a user's User Name via the Web or the CLI, but the action was rejected.

1. Verify the command syntax (e.g., "**add sysuser name**=NAMESTR).
2. Retry the operation, making sure the user name entry is unique.
3. Retry the operation, making sure you are not trying to change the user name of the default user.
4. If the problem persists, contact Technical Support.

ERROR: Current user is not authorized to do this operation!

You tried an operation (e.g., login password entry, set user name) to which you are not authorized (only the super user level can perform this function).

1. Check with your system administrator.
2. Make sure this is the user you want - check the Users table entry.
3. Verify the user's access level (admin, read write, or read only) in the command syntax ("add sysuser name=NAMESTR level=(admin|read-write|read-only").
4. See the "Configuring System / Login Users" section.

This card is in hardware mode and no setting allowed!

You tried to make a configuration change via the Web interface or the CLI, but the action was rejected. For example:

```
AgentIII C1|S3|L1D>set tdm inband enable
This card is in hardware mode and no setting allowed!
AgentIII C1|S3|L1D>
```

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

1. Make the required changes via DIP switch configuration. See the related section of the manual.
2. Change the Hardware/Software Jumper setting to Software mode.
3. Retry the configuration change via the Web interface or the CLI.
4. Contact Lantronix for more information.

It must be a valid oid.

When you add a SNMP view/group/local user/remote user and the name contains "&" character, it can be added successfully, but the rest characters after "&" cannot be seen from web table list, CLI shows correctly.

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.

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.

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!

SNMP Messages

For any error condition, you can check the Lantronix web site for possible solutions. For any problem that persists, contact Lantronix Tech Support

Basic Recovery Steps

You entered a command, but the operation failed or is still in process.

1. Wait for a few moments for the operation to complete.
2. Use the **Help** or **?** command to get assistance (help) on a group of commands or on a specific command.
3. Make sure this is the command you want and that the device/port/configuration supports this command.
4. Make sure this device/port supports the function attempted. Use the **go** command to switch locations.
5. Verify the command syntax and re-enter the command. See the related section of the manual for specifics.
6. Try using the Web interface to perform the function.
7. If the "continue **y**(es) **n**(o)" prompt displays, type **y** and press **Enter** to continue.
8. If the problem persists, contact Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix Tech Support.

Message:
Cannot create SNMP group on this card!
Cannot remove SNMP view on this card!
Cannot remove this group!
Cannot remove this view!
Cannot set filter type of a SNMP view on this card!
Cannot set SNMP local engine ID on this card!
Cannot set notify view of a SNMP group on this card!
Cannot set read view of a SNMP group on this card!
Cannot set write view of a SNMP group on this card!
Cannot show SNMP group on this card!
Cannot show SNMP local engine ID on this card!
Cannot show SNMP view on this card!
Fail to create SNMP group!
Fail to get SNMP group!
Fail to get SNMP local engine ID!
Fail to get SNMP local user!
Fail to get SNMP remote user!
Fail to get SNMP user!
Fail to remove SNMP group!
Fail to set SNMP local engine ID!
Fail to set SNMP notify view!
Fail to set SNMP read view!
Fail to set SNMP view status!
Fail to set SNMP write view!
Invalid OID for this view!
Local Engine ID length range is <5 - 32>!
No SNMP group created now!
No SNMP local user created now!
No SNMP user created now!
No such SNMP group name!
SNMP view name length should be shorter than 32!
The specified user does not exist!
Meaning: You entered an SNMP v3 command, but the command failed. For example, when the security model is v1 or v2c, the groups "public" and "private" cannot be removed; but when the security model is v3 the groups "public" and "private" can be removed.
Recovery: 1) Make sure this is the command you want. 2) Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) Make sure the group, engine or user to be edited exists. 7) If the problem persists, contact Lantronix 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 Lantronix 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 cannot 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 cannot be deleted!
ERROR: This group cannot 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 Lantronix 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 Lantronix Tech Support. S

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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 cannot 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix 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 Lantronix Tech Support.

Message:
ERROR Software version of this card ("cardVersion") is not supported, please upgrade to the same version as the IONMM
Getting card version failed
The failure get template config handler was called.
Meaning: You attempted a function that is not supported by this version of firmware.
Recovery: 1) Enter another (supported) function at this card's firmware version, or use the "go" command to switch to another card. 2) Upgrade to a newer firmware version. See "TFTP Transfer / Upgrade Commands"or "Upgrade / Update Firmware Commands". 3) Retry the operation. 4) If the problem persists, contact Technical Support.

Message:
The confirm password is not identical with the password!
The user name length must be in range [1..64]!
The user name must begin with an alphanumeric char!
You can only change your own password, not others!
Meaning: You entered a command to create a new system user, but the command failed.
Recovery: 1) Verify the command syntax ("**add sysuser name**=NAMESTR **level**=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR"). 2) Retry the operation, making sure the "pass" and "confirmpass" entries match. See the related command section.
3) If the problem persists, contact Technical Support.

Message: *Invalid input of timout value!*
Meaning: You set an unsupported SNMP trap timeout boundary value.
Recovery: 1) In the "**add snmp traphost**" command, specify a valid timeout (-15s%-16s%-5u%-30s%-16s%-12s%-12u%-12u%s (change from 8u to 12us). For example:

C1|S1|L1D>**add snmp traphost** version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6 security_level authPriv notify trap timeout=<0-2147483647>]
C1|S1|L1D>**add snmp traphost** version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6 security_level authPriv notify trap timeout 1000 retry 25

Problem: An SNMP user cannot access the IONMM.
Meaning: The User security level is not compatible with the Group level. For example, you added an SNMPv3 User to a SNMP v1 Group, or added a User to a non-existing Group, so this user cannot access the IONMM.
Recovery: 1) Make sure the Group exists. Verify the User's security level. See the "Configure SNMP" section for specific details.

Problem: Can't assign a SNMPv3 User to multiple Groups.
Meaning: The SNMPv3 standards do not allow you to assign a SNMPv3 user to multiple groups.
Recovery: 1) Create an additional, unique user. 2) Assign the new user to a different group. 3) Make sure that each user belongs to just one group.

Problem: Can't configure SNMPv3 for chassis ION NIDs.
Meaning: The SNMPv3 features currently only apply to the IONMM and standalone S323x/S322x/S222x devices.
Recovery: 1) Contact Tech Support. .

Message: *Its value must be a-f or A-F or 0-9 and the total length must be a dual from 18 to 128*
Meaning: The engine ID is specified by hexadecimal characters. Each two input characters correspond to one octet character. For engine ID "80 00 03 64 03 00 c0 f2 00 01 02", the first two characters '80' correspond to the first octet character '\128' with ASCII value of 128 (8*16 + 0 = 128). The second two characters "00" correspond to the second octet character '\0' with ASCII value of 0 (0*16 + 0 = 0).
Recovery: 1) This applies only for SNMP v3 Engine ID converting. Enter this.pattern = /^[A-F\d]{18,128}$/.

Message: *It must be a valid oid.*
Meaning: You entered an invalid OID.
Recovery: 1) Enter this pattern = /^[1-9]+(\.\d{1,5})*$/.

Message: *It must be a string which consists of letters and numbers.*
Meaning: You entered an invalid string.
Recovery: 1) Enter this pattern = /^[\w]{1,256}$/;
2) Enter this min = lengthMin;
3) Enter this max = lengthMax;

Message: *It can be set to any characters combination except the character tab and space.*
Meaning: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "tab" and "space" characters.
If you enter a "tab" and/or "space" character in these fields (via CLI or Web interface) the message "It can be set to any characters combination except the character tab and space." and "this.pattern is required: /^[\S]*{1,256}$/." display.
Recovery: 1) Re-enter the command or field without the "tab" or "space" characters.

Problem: Entries display in red in SNMP v3 fields (e.g., at **IONMM** > **SNMP** > **Users** sub-tab, the **User Name** / **Group Name** / **Password** entry displays in red)
Meaning: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "tab" and "space" characters.
If you enter a "tab" and/or "space" character in these fields (via the Web interface) the characters display in red and the message “Getting records failed (http server error)” displays in the lower-left corner of the page.
Recovery: 1) Re-enter the command or field without the "tab" or "space" characters.

Message:
The default group whose name is \"public\" or \"private\" and security-model is v1 or v2c cannot be removed!
While the group whose name is \"public\" or \"private\" and security-model is v3 can be removed!
Meaning: The default group cannot be removed (deleted) from the ION system configuration.
Recovery: 1) Make sure this is the command you want. 2) Delete another existing Group. 3) See the related section of the manual for specifics. 4) If the problem persists, contact Lantronix 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 Technical 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 Lantronix Tech Support.

Problem: SNMP Local or Remote Users are deleted when you modify the SNMPv3 Local or Remote Engine ID.
If you enter a "show snmp group name" command without entering a specific group name, the session is ended and the ION login prompt displays.
Meaning: You configured the SNMPv3 Local or Remote Engine ID before you configure the Local or Remote Users for this engine. For example:

```
AgentIII C1|S1|L1D>show snmp group name
Name         Security Model     Security Level    Read View   Write View   Notify View
-------------------------------------------------------------------------------------
login: ION
Password:
```

Recovery: 1. Log in to the ION system again. 2. Configure the SNMPv3 Local or Remote Engine ID before you configure the Local or Remote Users for this engine. See "Configuring SNMP". Retry the operation.

Message: The local MD id parameter is out of range.
Meaning: You entered
For example:
Agent III C1|S8|L1D> **add soam md local-md-id 11 md-name aa md-level 1**
Agent III C1|S8|L1D>**add soam md local-md-id 11 md-name aa md-level 1**
The MD with this id has been configured already.
Agent III C1|S8|L1D>**show soam md local-md-id 11**
Incorrect parameter number.
Usage: **show soam md [local-md-id=<1-4294967295>]**
Recovery:
1) The show command should be something like "**show soam md**" or "**show soam md 11**" .
2) If the problem persists, contact Lantronix Tech Support.

Message:
Getting DNS server%u address fail%s
Invalid Ipv6 Gateway address!
Invalid Ipv6 Global address!
Invalid SNTP server address!
Invalid TFTP server address!
Please input a number to specify the DNS server index!"
prefix is out of range!
Meaning: An error was detected in IPv6 configuration information (e.g., you set a SNTP server address incorrectly).
Recovery:
1. CLI: Make sure the **set sntp-svr** format follows "set sntp-svr svr=<1-6> type=(ipv4|dns|ipv6) addr=ADDR". See the “IPv6 CLI Commands” section.
2. Web: Verify the IPv6 Management Status, Method, Prefix, and Gateway Method selections and the IPv6 Management Link Local Address, Management Address and Management Gateway settings.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to set DNS server address!
Fail to set gateway address!
Failed to set ip address mode state!
Fail to set Ipv6 address prefix!
Fail to set IPv6 management state!
Fail to set RADIUS server address!
Fail to set RADIUS server address type!
Meaning: An IPv6 configuration change attempt failed (e.g., you entered an incorrect RADIUS, TACACS+, DNS server, or IPv6 address). For example, the RADIUS server configuration entry was invalid; only the first three valid DNS servers are available.
Recovery:
1. Enter only up to three RADIUS server addresses / types.
2. See the "Set RADIUS Server" command.
Recovery:
1. Check the “RADIUS Commands” section. For example, enter only up to three RADIUS server addresses / types.
2. Verify the “ION IPv6 CLI Commands’ . For example, see the "**set radius svr**" command.

Message: *IP management is not supported on this card!*
Meaning: Try another function on this device, or switch to another device and try this function again.
Recovery:
1. Try another function on this device, or switch to another device and try this function again.
2. Upgrade the device(s) to the latest firmware version.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to set Ipv6 Global address!
Fail to set gateway address!
Fail to set DNS server address!
Invalid address!
Invalid IP address!
Please input a digital number to port number!
Please input a valid ip address!
This trap address already exists!
Meaning: You made an invalid IP address entry.
Recovery:
1. For IPv4, enter a unique, valid fixed address length of 6. For IPv6, enter a fixed address length of 18.
2. Retry the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to analyse remote engine address!
Fail to get addr domain addr!
Invalid engineID!
No engine ID is specified for this address!
Remote engine address or port is not valid!
Example:

```
C1|S1|L1D>remove snmp remote user name=AliceB addrtype=ipv4
addr=192.168.1.30 port=162
No engine ID is specified for this address!
C1|S1|L1D>
```

Meaning: You tried to change an SNMP element but the engine ID was not recognized.
Recovery:
1. Check the **add snmp rmt engine** command parameters. See “IPv6 CLI Commands”.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Caution: only the first three valid DNS server can be available, please refer to user menu for the details
DNS server index is out of range!
Fail to set DNS server address type!
Invalid OID for this view
It must be a valid oid.
Now ipv4 mode is BOOTP, so you cannot configurate dns server1 to server3.
Now ipv4 mode is DHCP, so you cannot configurate dns server1 to server3.
Now ipv6 mode is dhcpv6, so you cannot configurate dns server4 to server6.
Example:

```
C1|S1|L1D>remove snmp view name=defaultView oid=1
Invalid OID for this view
```

Meaning: A problem exists in DNS server configuration. You can set the DNS server when IPv4 address mode is not DHCP and IPv6 address mode is not DHCPv6. Only the first three valid DNS servers are available. Do not configure unselected mode parameters when another mode is enabled.
Recovery:
1. See "DNS" section.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Stateless mode is based on route discovery function, please switch the gateway mode to route discovery.

Stateless Auto Configuration is based on the function of Route Discovery. Right now, Route ***Discovery*** *is disabled. Please enable it before switching to Stateless Auto configuration.*

Meaning: You tried to enable IPv6 Stateless Autoconfiguration, but you have not enabled Route Discovery or changed the gateway mode to 'route discovery' ('stateless'), which is required first.
Recovery:
1. Check the device's type the port belongs to.
2. Check if iIP6 Address Mode is set to "static", "dhcpv6", or "stateless".
3. Enable Static IP.
4. Verify the IPv6 Gateway Mode setting.
5. Contact Lantronix Tech Support if the problem persists.

Message:
Error IP V6 Gateway Address
Multicast IPv6 address cannot be set.
Local host IPv6 address cannot be set.
Meaning: You entered an IPv4 value for the IPv6 address, or an IPv6 value for the IPv4 address.
Recovery:
1. Verify the IPv4 and/or IPv6 DNS address settings.
2. Enter a valid IPv6 address and retry the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Error IPv6 Address!
Error IPv6 Network Address
Its value must be an IPv4 address like '192.168.0.1'.
Its value must be an IPv6 address.
Its value must be an IP address or a domain name.
Its value must be an IPv4 address or IPv6 address.
Its value must be a valid subnet mask IP
Meaning: You entered an incorrect value for the IPv6 address, or there was an error with the IPv6 Condition value conversion.
Recovery:
1. Enter a valid IPv6 address and retry the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Its value must be an integer or IPv6 address like 'ffff:0:0:0:0:0:0:0'.
Its value must be an integer ranging from {from} to {to} or IPv6 address like 'ffff:0:0:0:0:0:0:0'.", {from: from, to: to}
Its value must be an integer greater than or equal to {from} or IPv6 address like 'ffff:0:0:0:0:0:0:0'.", {from: from}
Its value must be an integer less than or equal to {to} or IPv6 address like 'ffff:0:0:0:0:0:0:0'.", {to: to}
Meaning: You entered an incorrect value for the IPv6 address, or there was an error with the IPv6 Condition value conversion.
Recovery:
1. Enter a valid IPv6 address and retry the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message:
It can be set to any characters combination except the space character.
Its value must be a character string less than 64 bytes
Its value must be a MAC address like 'XX-XX-XX-XX-XX-XX' (separated by '-').
Its value must be consist of a-f or A-F or 0-9 and the total length must be a dual from 18 to 128
Meaning: Information on the entry field.
Recovery:
1. Follow the entry field instructions.
2. Retry the operation. See the related section of this manual.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to get syslog server address type!
Fail to set syslog server address!
Example:

```
Agent III C1|S1|L1D>set syslog svr type dns addr www.tndvt.com
Fail to set syslog server address!
C1|S1|L1D>show syslog config
C1|S1|L1D>set syslog svr type ipv4 addr 192.168.0.33
Fail to get SIC configure mode!
C1|S1|L1D>
```

Meaning: You tried to add a new syslog server, but the server IP address entry was not valid.
Recovery:
1. Enter a valid syslog server IP address and retry the operation. See the related section of this manual.
2. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to set group of the user!
Invalid group parameter for user!
Meaning: You tried to add a new SNMP local user, but the group entry was not valid.
Recovery:
1. Enter a valid SNMP group and retry the operation. See the "Add SNMP local user' command.
2. Contact Lantronix Tech Support if the problem persists.

Message:
Invalid ipv6 input found!
IPv6 Address and Gateway should be at the same sub-net!
IPv4 Address and Gateway should be at the same sub-net!
the subnet mask of gateway is different from the one of global address
Meaning: You set up the IP address and gateway on different sub-nets. The subnet mask of the gateway is different from the subnet mask of the global address.
Recovery:
1. Change either the IP address or the subnet mask for the NID.
2. Contact Lantronix Tech Support if the problem persists.

Message:
Error: need set subnet-mask when ipv4 address is set!
Error: need subnet-mask when ipv4 address is set!
Fail to set IPv4 address! (need set subnet-mask when ipv4 address is set!)
Fail to set Ipv6 Global address!
Fail to set Ipv6 address prefix!
Fail to set subnet mask! (need set subnet-mask when ipv4 address is set!)
Meaning: An error was detected in the attempted IP Address setup.
Recovery:
1. Verify the IP address, gateway address, DNS server or other related IP address setting.
2. See the "**Set IP address and subnet mask**" command.

3. Contact Lantronix Tech Support if the problem persists.

Message:
Invalid address!
Invalid DNS server address!
Invalid gateway address!
Invalid IP address! (need set subnet-mask when ipv4 address is set!)
Invalid ipv6 address! (need set prefix when ipv6 address is set!)
Invalid RADIUS server address!
Invalid SNTP server address!
Invalid subnet mask!
Invalid TFTP server address:x
Please input a number to specify the DNS server index!
prefix is out of range!
Set ipv4 gateway address type
Meaning: An error was detected in the attempted IP Address setup.
Recovery:
1. Verify the IP address, gateway address, DNS server or other related IP address setting.
2. See the "**Set IP address and subnet mask**" command.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Inavlid network mask value, correct format like 2001:ef:201:3213::2000/ffff:ffff:: or 2001::1002/96\n
invalid ACL condition value, correct format like 2001:ef:201:3213::2000/ffff:ffff:: or 2001::1002/96\n
This is ipv6 multicast address which cannot be set
This is ipv6 Unspecified address which cannot be set
This is ipv6 loopback address which cannot be set
Meaning: An error was detected in the attempted IP Address setup.
Recovery:
1. Verify the IPv6 address setting.
2. See the "**Set IP address and subnet mask**" command.
3. Contact Lantronix Tech Support if the problem persists.

Message: *ERROR: The current mib table can only have a maximum of " + maximum + " records!*
Get Dynamic Table Length Failed1!
Get dynamic table capability failed!
Meaning: The dynamic table length limitation reached; the dynamic table is full and not available for adding records. The maximum of dynamic table that ION supports is 1024.
Recovery:
1. Limit the number of table entries to 1024.
2. Contact Lantronix Tech Support if the problem persists.

Message:
ERROR: already have a ipv6Condition Type under the same level!
ERROR: already have a Condition Type under the same level!
ERROR: already have the same Condition Type under this rule!
ERROR: already have the same Condition Type under this rule!
ERROR: already have the same layer Condition under this rule!
Invalid ip6tables ACL condition index!
One ACL rule can only has one layer2 ACL condition(macaddr)!
One ACL rule can only has one layer3 ACL condition(ipv4addr or ipv4addrrange or ipv4network)!
One ACL rule can only has one layer4 ACL condition(tcpport or tcpportrange or udpport or udpportrange or icmp)!
One ip6tables ACL rule can only has one layer2 ACL condition(macaddr)!
One ip6tables ACL rule can only has one layer3 ACL condition(ipv6addr or ipv6network)!
One ip6tables ACL rule can only has one layer4 ACL condition(tcpport or tcpportrange or udpport or udpportrange or icmp)!
Meaning: An ACL Rule configuration problem exists. When IPv6 is enabled, you can have up to three of an IP style (IPv4 or IPv6).
Recovery:
1. Check the ACL Rule configuration settings.
2. Contact Lantronix Tech Support if the problem persists.

Message:
Get Ipv6 Management Address
Get Ipv6 Management Prefix
IP address
IP subnet mask
Meaning: You entered a gateway IP address or IP subnet mask outside of the valid range.
Recovery:
1. Enter a valid gateway IP address and IP subnet mask.
2. Contact Lantronix Tech Support if the problem persists.

Message:
VID already exist!
ERROR: already have the same layer Condition under this rule!
Fail to add ACL addition!
There is already a same named view!
Fail to create SNMP view!
We can create at most 6 trap hosts!
Meaning: There was a problem with an ip6tables ACL command.
Recovery:
1. Verify the IPv6 ACL command parameters.
2. Retry the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to create parameter entry!
Fail to security name!
Notification type can only be trap or inform!
Meaning: An SNMP v3 operation failed.
Recovery:
1. Verify the SNMP v3 notify, security model, and security level parameter values.
2. Verify the "**add snmp traphost**" command. See "SNMP Configuration".
3. Contact Lantronix Tech Support if the problem persists.

Message:
Notification type can only be trap or inform!
When notify type is not \"inform\", you cannot set the value of \"timeout!
When notify type is not \"inform\", you cannot set the value of \"retry!
When traphost version is v1, the setting for notify, timeout and retry will be ignored!
Meaning: You entered an SNMP parameter that does not apply to the current SNMP configuration settings.
(You tried setting 'timeout' or 'retry' value when 'notify' type is set to trap').
Recovery:
1. Verify the SNMP 'notify' parameter value.
2. See "SNMP Configuration".
3. Contact Lantronix Tech Support if the problem persists.

Message:
The specified SNMP group does not exist!
The specified SNMP view does not exist!
Meaning: You tried to remove an SNMP v3 group or view that does not exist.
Recovery:
1. Confirm the group or view that you want to delete.
2. Retry the operation. See "SNMP Configuration".
3. Contact Lantronix Tech Support if the problem persists.

Message: *the value of dupAddr detect beyond the scope.*
Meaning: The IPv6 Duplicate Address Detect mechanism detected a duplicate address or invalid address.
A station may have failed the IPv6 stateless auto-configuration process because the router is not presented on the same link or its DAD cycle is failed.
Recovery:
1. Check the attached device's IPv6 address.
2. Verify the attempted operation; refer to the related section of this manual.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Adding VLAN failed
Deleting VLAN failed
Modifying VLAN failed
The default VLAN 1 cannot be modified or removed!
Meaning: The VLAN operation is very slow when adding multiple VLANs to the system, or modifying or deleting a VLAN fails.
Recovery:
1. Upgrade to the latest firmware version if not currently at the latest version.
2. Retry the operation. Make sure you are not creating more VLANs that are supported. See the 'VLAN Configuration" section.
3. Contact Lantronix Tech Support if the problem persists.

Message:
All-zero MAC address is not valid for ACL condition!
invalid ACL condition value, correct format like 2001:ef:201:3213::2000/ffff:ffff:: or 2001::1002/96\n
Meaning: You entered an invalid IPv6 MAC address in the ACL Condition field.
Recovery:
1. Verify the IPv6 MAC address entered in the ACL Condition field is valid.
2. Contact Lantronix Tech Support if the problem persists.

Message: *This vlan has already been used as the management vlan, please modify.*
Meaning: You tried to add a VLAN whose VID is the same as the existing Management VLAN ID.
Recovery:
1. Enter a valid, unique VLAN ID.
2. See "VLAN Configuration".
3. Contact Lantronix Tech Support if the problem persists.

Message: *RADIUS authentication server: index addr-type addr retry timeout*
Meaning: An invalid user and password to login ION was attempted.
Recovery:
1. Verify the user name and password entries.
2. Verify the RADIUS configuration setting, e.g.:

```
Agent III C1|S1|L1D>show radius config RADIUS client state: enable
```

3. Contact Lantronix Tech Support if the problem persists.

Message: *The certificate file(s) is being copied. Please wait...*
Meaning: Information only.
Recovery:
1. Wait for the process to complete.
2. Contact Lantronix Tech Support if a problem occurs.

Message: *Invalid syslog server address!*
Meaning: You entered a server address for the Syslog server.
Recovery:
1. Re-enter the command using a valid Syslog server address.
2. See the related section of this manual for more information.
3. Contact Lantronix Tech Support if the problem persists.

Message:
All-zero MAC address is not valid for ACL condition!
Invalid condition valule: %
Meaning: You entered a command with an invalid MAC address.
For example:

```
Agent III C1|S1|L1D>add acl condition type macaddr srcdst src oper equal value 00-00-00-00-00-00
All-zero MAC address is not valid for ACL condition!
```

Recovery:
1. Re-enter the command using a valid MAC address.
2. See the related section of this manual for more information.
3. Contact Lantronix Tech Support if the problem persists.

Message: *snmp operation error, possible reasons: invalid data, error data sequence, dynamic table capability limit, etc.*
Meaning: You exceeded the limitation of 255 ACL/ACLv6 rules or conditions. When you try to add more than 255 ACL /ACLv6 rules, or try to add more than 255 ACL/ACLv6 conditions, this warning displays.
Recovery:
1. Make sure you remain within the limit for ACL/ACLv6 rules or conditions.
2. See the related section of this manual for more information.
3. Contact Lantronix Tech Support if the problem persists.

Message:
The maxium length of system contact is 255!
The maxium length of system name is 255!")
The maxium length of system location is 255!
The maxium string length of circuit ID is 64
The maxium string length of device description is 255
Meaning: You entered too many characters in an entry field.
Recovery:
1. Re-enter the text in the entry field using fewer characters.
2. Verify the new entry is accepted without any errors.
3. Contact Lantronix Tech Support if the problem persists.

Message: *Failed to transfer the certificate file(s)!*
Meaning: The HTTPS certificate file transfer failed.
Recovery:
1. At the message "*Please input Private File Name!*" enter a valid name. See "Configuring HTTPS".
2. Verify the name of the certificate file to be copied and/or the private key file to be copied.
3. Only tftp supported in web and should be set at the end. See "TFTP (Trivial File Transfer Protocol)". Try uploading the Private File using the CLI method.
4. Contact Lantronix Tech Support if the problem persists.

Message: **Connection closed by foreign host.**
Meaning 1: An SSH operation caused the connection to close. For example:

```
Agent III C1|S1|L1D>set ssh server state disable
Agent III C1|S1|L1D>Connection closed by foreign host.
```

Meaning 2: A SOAM operation caused the connection to close. For example:

```
Agent III C1|S8|L1D>show soam md 1
Connection closed by foreign host.
```

Recovery:
1. Restart the operation.
2a. Verify the SSH configuration.
2b. Verify the SOAM configuration. See the "SOAM' section.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Please input a digital number to specify radius server index!
RADIUS authentication server index is out of range!
Set RADIUS server secret Failed
The RADIUS authentication server specified does not exist!
This card cannot set RADIUS secret!
Meaning: You entered a RADIUS CLI command incorrectly, or the RADIUS server was not configured, or the card does not support RADIUS.
Recovery:
1. Check the CLI command syntax and re-enter the command.
2. Make sure the RADIUS server is up and running.
3. Contact Lantronix Tech Support if the problem persists.

Message: *Error: Set egress/ingress rate failed!*
Meaning: You used the CLI command to select 5M/7M/9M/90M in "Egress Rate Limit" or "Ingress Rate Limit" drop-down list and clicked **Save**. ION cannot accept the configuration that you entered.
Recovery: 1. Check the CLI command syntax and re-enter the command.
2. Contact Lantronix Tech Support if the problem persists.

Message:
fdbid must equal to 0 now!
No data in VLAN forward database table now!
Please input a number to specify the fdbid!
The specified conn-port does not exist!
Meaning:

```
Agent III C1|S3|L1D>show fwddb config fdbid 0
No data in VLAN forward database table now!
Agent III C1|S3|L1D>add fwddb mac 00-00-00-00-00-01 conn-port 1 priority 2 type static
Agent III C1|S3|L1D>add fwddb mac 00-00-00-00-00-02 conn-port 1 priority 2 type static
```

Recovery:
1. Check the CLI command syntax and re-enter the command. See the related section of this manual.
2. Verify the FDB configuration. See the related section of this manual.
3. Verify that the card on which the command was entered can support the function attempted (e.g., the case where an ION FBRM BFFG card entered a command that only an ION_NID supports, such as a **fwddb config** command).
4. Contact Lantronix Tech Support if the problem persists.

Message:
Invalid priority override value!
The range of priority is 0 .. 7!
Meaning: You entered the command "**add vlan vid**" or "**add vlan vid**" or "**add fwddb mac**" with a priority outside of the valid range.
Recovery:
1. Check the CLI command syntax and re-enter the command. See the related section of this manual.
2. Verify the VLAN configuration. See the related section of this manual.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Fail to find first row of acl rules!
Fail to get ACL rule!
Fail to get ip6tables ACL rule chain type!
Fail to get ip6tables ACL rule priority!
Fail to get ip6tables ACL rule policy!
Fail to get ip6tables ACL rule table type!
Fail to get ip6tables ACL rule traprate!
No ACL rule now!
Meaning: You entered a command (**show ip6tables acl rule**) to display the current ACL table, chain, and/or policy, but the command failed.
Recovery:
1. Note that the value of table can only be "filter" and the value of chain can only be "input".
2. Verify the ACL configuration.
3. Contact Lantronix Tech Support if the problem persists.

Message: *Fail to get SIC configure mode!*
Meaning: The 'reset to factory configuration' failed. For example:

```
C1|S1|L1D>reset factory
Fail to get SIC configure mode!
```

Recovery:
1. Verify the card configuration.
2. Verify the card firmware version.
3. Contact Lantronix Tech Support if the problem persists.

Message: *Setting values failed (snmp operation error, possible reasons: invalid data, error data sequence, dynamic table capability limit, etc)*
Meaning: Possible reasons include 1) You exceeded the ION system support maximum of 64 ACL rules and/or 128 ACL conditions. 2) You entered an invalid or unrecognized IP address setting.
Recovery:
1. Reduce the number of ACL entries.
2. Verify the IP address, IP Gateway address, IPv6 Prefix length, etc.
3. See "IPv6 Troubleshooting".
4. Contact Lantronix Tech Support if the problem persists.

Message: *An error occurred during a connection to 2001:db8:2:f101:14a:9732:7d4d:aef5:443.*
Peer's Certificate issuer is not recognized.
(Error code: sec_error_unknown_issuer)
Meaning: FireFox cannot support IPv6 mode to login to the ION system. The ION system cannot support the FireFox browser to login in SSL mode in IPv6.
Recovery:
1. Temporarily switch to IPv4 or to another browser.
2. Complete the login and switch back per step 1 as needed.
3. Contact Lantronix Tech Support if the problem persists.

Message: *No DMI support on this port!*
Meaning: You tried to set DMI on a port that does not support DMI.
Recovery:
1. Choose another port that supports DMI.
2. Contact Lantronix Tech Support if the problem persists.

Message: *SNMP community name length cannot be 0!*
SNMP community name length should be shorter than 32!
Meaning: You entered an invalid community name for SNMP operation.
Recovery:
1. Enter an SNMP community name with 1-31 characters.
2. See "SNMP" section.
3. Contact Lantronix Tech Support if the problem persists.

Message:
DB is full. Max of MAs and MEGs per system reached
MEG with this index already exists. MA and MEG have shared index space
Parent of MA is MD. Try to find MD with given index. It must be configured.
Meaning: The SOAM MD/MA/MEG configuration cannot be supported.
Recovery:
1. Verify the SOAM configuration. See "SOAM' section.
2. Remove any unused MA or MEGs and restart the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message:
Error - Send the command failed: Ambiguous input: group MAC address provided while isMulticastLb flag not set.
Invalid input: Destination MAC address is invalid.
Invalid MAC address.
Storage failed!
This MA is in used.
Unknown error!
Meaning: A SOAM MIB error was logged during SOAM operation / configuration.
Recovery:
1. Verify the SOAM configuration. See "SOAM' section.
2. Remove any unused MA or MEGs and retry the operation.
3. Contact Lantronix Tech Support if the problem persists.

Message: *Please select the MEP from the table!*
Meaning: You tried to perform part of a SOAM function and clicked the **Refresh** button before completing the SOAM function.
Recovery:
1. Complete the SOAM function and click the **Refresh**" button when completed.
2. See "SOAM' section.
3. Contact Lantronix Tech Support if the problem persists.

Message:
4_T1 port display name enhanced/Remote card version checking with stand alone card.
Cannot find software version of this card!
Error: Set egress/ingress rate failed!
IONMM card version is 1.3, and ARM-based card is 1.2, the SIC needs upgrade
Software version of this card (" + cardVersion + ") is not supported, please upgrade to the same version as the Standalone Card
Software version of this card (" + cardVersion + ") is not supported, please upgrade to the same version as the IONMM
Various FP and ION web interface and CLI compatibility messages.
Meaning: An ION NID compatibility issue occurred. There is a mismatch between a NID and the IONMM firmware versions. For example, you selected 5M/7M/9M/90M at the "Egress Rate Limit" or "Ingress Rate Limit" dropdown, clicked **Save**, and the message displayed.
Recovery:
1. Verify your configuration using the information below.

- ION version 1.2.2 is released for these AVR-based SIC cards with some bug fixes: C3110, C3210, C2110, C2210, C611x, C612x, C6210, BPC and Power Supply.

- ION version 1.3.0 is released for these ARM-based SIC cards with fixes and powerful new features: IONMM, C/S222x, C/S322x, and C/S323x.

- IONMM v1.3 supports the v1.2 AVR-based SIC cards. IONMM v1.3 does not support the v1.2 ARM-base SIC cards.

ARM-based SIC; IONMM revision	1.1	1.2	1.3
1.1	Y	N	N
1.2	N*	Y	N
1.3	N*	N*	Y

Note 1: ARM-base SIC cards include IONMM, C/S222x, C/S322x, and C/S323x.
Note 2: N* means an error interface will display to remind you to upgrade the SIC firmware to the same revision of IONMM.

AVR-based SIC; IONMM revision	1.1	1.2	
1.1	Y	N	
1.2	N*	Y	
1.3	N*	Y	

Note 1: AVR-base SIC cards include C3110, C3210, C2110, C2210, C611x, C612x, C6210, BPC, and Power Supply.

1. Check the firmware versions of the NID and IONMM and upgrade as needed.
2. Check the Release Notes for possible installation scenarios.
3. Re-try the operation.
4. Contact Lantronix Tech Support if the problem persists.

Problem: S3231 port 1 link is down and the S3231 can't be managed anymore.
Meaning: The S3231 port 1 and attached switch ports should all have link up and S3231 should be able to be managed. If the Management VLAN config has not changed, the S3231 should be manageable all the time.
For example, after the S3231 has run for about two days under Management VLAN, you performed some get and set operations on this card during this time, but made no changes to the Management VLAN configuration. You reboot S3231 to try to recover the Management but it doesn't work.
Recovery: Verify if MAC security is enabled; if so, the port is closed when more than one MAC address arrives at this port (normal operation)

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

Meaning: The DNS 1 through DNS 6 entries can be in IPv4 or IPv6 format, or both (a combination of up to three of each). DNS servers 1-3 are for IPv4; DNS servers 4-6 are for IPv6.
Recovery:
1. Change the DNS server settings to make them valid.
2. See "DNS '3 vs. 3' Rule ('Up to 3' Rule)".

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

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!
Meaning*:* 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.
Recovery:
1. Verify the limit of values.
2. Verify the SNMP Engine ID parameter settings.
3. See the "SNMP Web Interface" section for more information.

Message*:*
Error: Incorrect parameter number.
Error: The MEP ID parameter is out of range.
Error: The Parent's ID parameter is out of range.
Meaning*:* You entered an invalid parameter (outside the valid range).
Recovery:
1. Verify the limit of values.
2. Verify the MEP ID parameter settings.
3. See the "SOAM MEP" section for more information.

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.

Message*:*
agentx_mapset Error
agentx_ot_add Error

Meaning: possible internal error
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message*:**Fail for sending ionSyslogMgmtTable ,ignored...\n*
Meaning: possible internal error.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support. .

Message*:*
Fail to get syslog server address type!
Fail to get syslog server address type!
Fail to get syslog server port!
Fail to get syslog level!
Fail to get syslog level!
Fail to get syslog server address!
Meaning: the **show syslog config** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

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: 1. Follow your organization's procedure or process for detection of a defined IDS.

Message*:*
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** command entry failed.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message*: **Invalid syslog server address!***
Meaning: the **set syslog svr** attempt failed (e.g., **set syslog svr type**=ipv4 addr=192.168.01).
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message*: **Number of subid is not correct when ionSyslogMgmtTable_get, expect %d, get %d \n***
Meaning: possible internal error
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message*: **Please input a digital number to specify syslog server port!***
Meaning: the **set syslog svr port** attempt failed.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation with a valid, unused UDP port number.
3. If the problem persists, contact Technical Support.

Message*:*
Session reset, Reregister from begging\n
STATUS_INVALID, should be session reset, Reregister from beginning\n
Meaning: possible internal error.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message*: **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.

Message*: 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.

Message*: **System initializing or SNMP service busy, please wait..." : "Invalid password!***
Meaning: possible internal error.
Recovery:
1. Wait for several seconds for the message to clear.
2. Verify the Syslog configuration. See "Configuring System Logging (Syslog).
3. Retry the operation.
4. If the problem persists, contact Technical Support.

Message*: **unknown column in ionSyslogMgmtTable_get\n***
Meaning: possible internal error.
Recovery:
1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)".
2. Retry the operation.
3. If the problem persists, contact Technical Support.

Message*: **Unknown command.*** message displays when entering system name/contact/location.
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.

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[716]: 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
```

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.

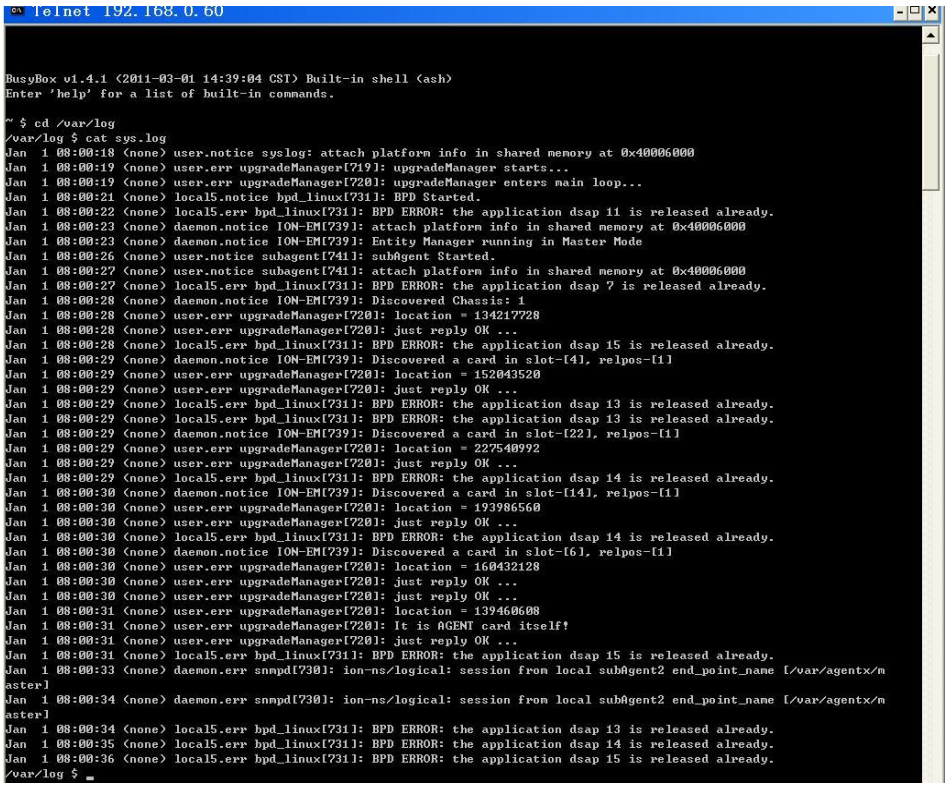
Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support.

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)



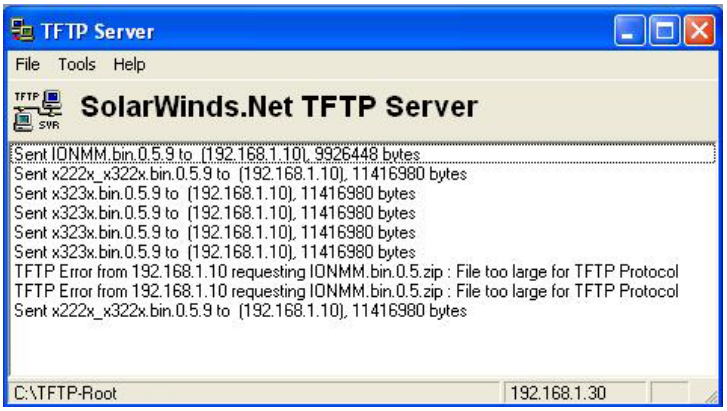
TFTP Server Messages

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

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.

Appendix D. Linux Commands

The ION system supports certain standard Linux file system commands such as **cat**, **cd**, **ls**, **more**, **pwd**, and **rm**. These commands are restricted to the user directories; internal Linux file systems are not accessible.

The ION standard Linux file system commands are based on BSD 4; refer to the related documentation for more information.

cat Command

Command: cat

Description: Show the content of the FILES. Concatenate files and print on the standard output.

Example: C1|S7|L1D>cat [OPTION]

Options: Refer to the BSD 4 documentation for options and Interactive commands for the **cat** command.

cd Command

Command: cd

Description: Change to another directory.

Example:

Options: Refer to the BSD 4 documentation for options and Interactive commands for the **cd** command.

ls Command

Command: ls

Description: Unix and Unix-like operating systems maintain the concept of a current working directory, (i.e., where you are currently positioned in the hierarchy of directories).

When invoked without any arguments, **ls** lists the files in the current working directory. This command is restricted to the IONMM user directories; internal Linux file systems are not accessible.

The IONMM card stores all configuration backup files, HTTPS certification file, SSH key file, and Sys-log file. For example, the HTTPS certificate is stored in *'/agent3/conf/lighttpd*'. For SSH, the host keys (RSA and DSA) are stored in *'/agent3/conf/dropbear'*.

Example:

```
C1|S7|L1D>ls
    agent3
    app
    bin
    dev
    etc
    lib
    linuxrc
    mnt
    proc
    root
    sbin
    sys
    tftpboot
    tmp
    usr
    var
    www
C1|S7|L1D>
```

Options:

Without options, **ls** displays files in a bare format. This bare format however makes it difficult to establish the type, permissions, and size of the files. The most common options to reveal this information or change the list of files are:

-l long format, displaying Unix file types, permissions, number of hard links, owner, group, size, date, and filename

-F appends a character revealing the nature of a file, for example, * for an executable, or / for a directory. Regular files have no suffix.

-a lists all files in the given directory, including those whose names start with "." (which are hidden files in Unix). By default, these files are excluded from the list.

-R recursively lists subdirectories. The command ls -R / would therefore list all files.

-d shows information about a symbolic link or directory, rather than about the link's target or listing the contents of a directory.

-t sort the list of files by modification time.

-h print sizes in human readable format. (e.g., 1K, 234M, 2G, etc.)

Example:

```
C1|S3|L1D>ls etc
    TZ
    VERSION
    dropbear
    factory
    fstab
    group
    gshadow
    host.conf
    hostname
    hosts
    init.d
    inittab
    lighttpd
    lighttpd.conf
    motd
    openssl
    passwd
    profile
    protocols
    radius
    rcS.d
    resolv.conf
    rpc
    script
    services
    shadow
    snmpd.conf
    sysconfig
    terminfo
C1|S3|L1D>
```

Refer to the BSD 4 documentation for additional options and Interactive commands for the **ls** command.

more Command

Command: more

Description: A filter for paging through text one screenful at a time.

Example: C1|S7|L1D>more [OPTION]

Options: Refer to the BSD 4 documentation for options and Interactive commands for the **more** command.

pwd Command

Command: pwd

Description: Show current directory.

Example:

```
C1|S7|L1D>pwd
/
C1|S7|L1D>
```

Options: Refer to the BSD 4 documentation for options and Interactive commands for the **pwd** command.

rm Command

Command: rm

Description: Removes each specified file. By default, it does not remove directories.

Example:

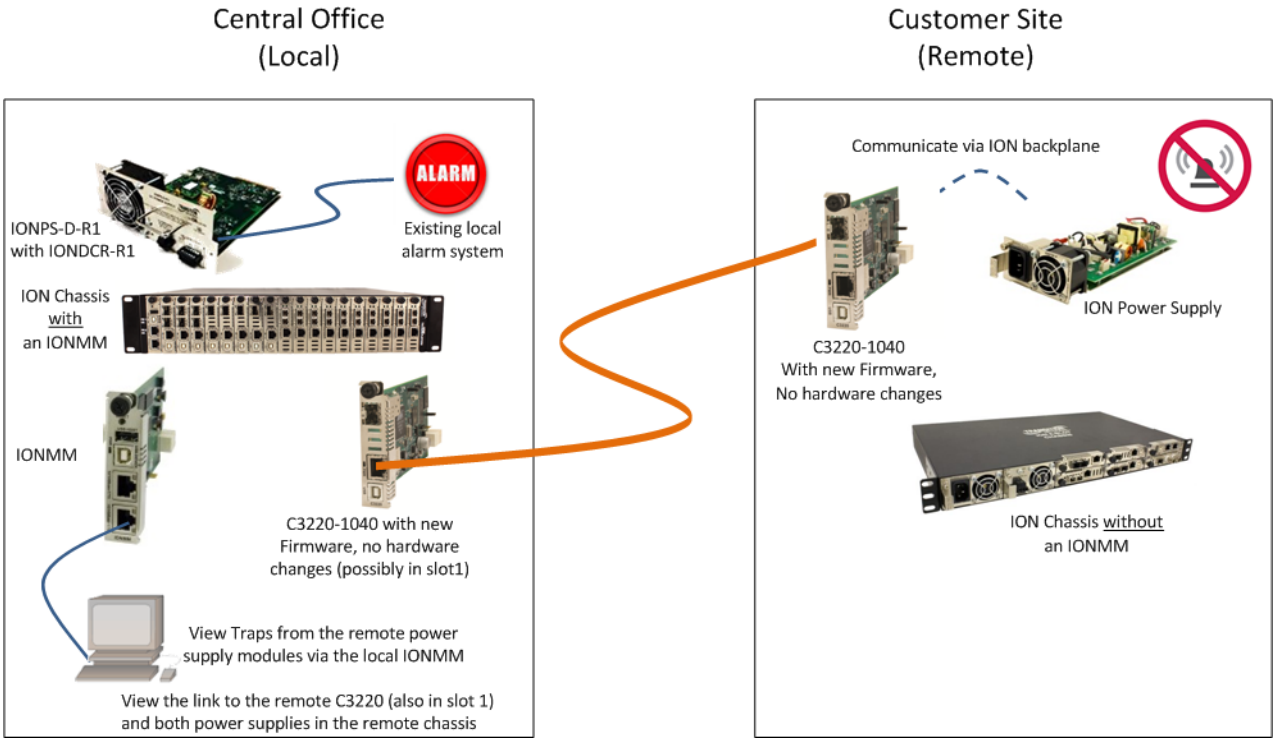
Options: Refer to the BSD 4 documentation for options and Interactive commands for the **rm** command.

Appendix E. Remote Manage Power Supply (RMPS)

The RMPS 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. This requires the C3220 to be installed in ION Chassis slot #1. 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 Web GUI as described in the ION x222x / x32xx User Guide. You can monitor the remote power supply via the CLI as described in the following sections.

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.

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

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.