ION System

x222x / x32xx Multiport NIDs

Command Line Interface (CLI)

```
C1|S12|L1AP2|L2D>#### DEVICE A ###
C1|S12|L1AP2|L2D>show soam md
Local MD ID             Name Level  MAs MIPs       Permission
------------------------------
          1         UNIabMD
          6      ProviderMD

C1|S12|L1AP2|L2D>show soam ma
MA index                : 1
MD index                : 1
MD level                : 0
MD name                 : UNIab
MA name                 : UNIab
CCM interval            : 1s
MEPs                    : 1
MEP ID list             : (2 Me
Permission              : defer
VLAN ID list            : none
Auto detection timeout  : 4000
Auto detect remote MEP  : disabled
```

Reference Manual

33473 Rev. G

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

Printed in the U.S.A.

ION System CLI Reference Manual for x222x / x32xx Multiport NIDs, 33473 Rev. G

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Revision History

Rev	Date	Description
D	09/12/11	Revised for ION Rel. 1.2.1 with: 1) Increased Rate Limiting options. 2) SNMPv3. 3) DHCP, Static, and BootP Address Modes. 4) WRR or Strict Egress Queue Modes. 5) Serial File Transfer (X/Y/Zmodem) commands. 6) IONMM System Name displays in CLI prompt. 7) Password can be changed using the community write string, and any login or password that is not fixed. 8) When using SSH client to login to ION, the userid and password are editable. 9) Minor enhancements to SSH package. 10) Backdoor password change. 11) Fixed MEF-related bugs. 12) Added MEF certifications. 13) Enhanced login User management.
E	08/21/14	Revised for v1.3.10 with IPv6, TACACS+ and Auto Provisioning support. Adds support for Zero Touch Provisioning only in the standalone S2220-10xx and S3220-10xx.
F	06/15/15	Update C3220 / C3221 port labeling, Well Known ports, Switch Mode (Local / Remote), configuring VLAN Mode, and DHCP default mode information.
G	07/27/15	Add S3221-1040-T information.

Table of Contents

Tables

General

This manual describes the USB and Telnet command line interface (CLI) commands available for ION System chassis or standalone operation of the ION x222x / x32xx Multiport NID. 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:

- **C2220** LOAM/IP-Based Remotely-Managed NID
- **C3220** LOAM/IP-Based Remotely-Managed NID
- **C3221** LOAM/IP-Based Remotely-Managed NID (2 open SFP slots)*
- **S2220** LOAM/IP-Based Remotely-Managed NID
- **S3220** LOAM/IP-Based Remotely-Managed NID
- **S3221** LOAM/IP-Based Remotely-Managed NID (2 open SFP slots)*
- **S3221-1040-T** LOAM/IP-Based Remotely-Managed Hardened NID. For Extended Temp (-40°C to +65°C; use PS PN 25138)

Models shown with an asterisk (*****) are available in a model with an open SFP port. SFP models that support DMI have a D at the end of the model number (e.g., **TN-SFP-SXD**).

CLI commands are case sensitive. Enter the CLI commands as shown in this document.

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

Documentation Conventions

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

Table 1: Documentation Conventions

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

Related Manuals

The ION system and related manuals are listed below.

1. ION System x222x & x32xx NID User Guide, 33472
2. ION Management Module (IONMM) User Guide, 33457
3. ION Systems CLI Reference Manual, 33473 (this manual)
4. ION219-A 19-Slot Chassis Installation Guide, 33412
5. ION Dry Contact Relay (DCR) Kit Install Guide, 33422
6. IONPS-A AC Power Supply Install Guide, 33423
7. IONPS-D DC Power Supply Install Guide, 33424
8. IONPS-A ION AC Power Supply Install Guide, 33464
9. ION ADP PointSystem Card Adapter for ION Chassis 33413
10. SFP Module manuals (model specific)
11. Release Notes (software version specific)
12. Product Documentation Postcard, 33504

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

Reboot and Reset Command Notes

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

These CLI commands 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.

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 of 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 of 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: Editing Commands

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)

Command Matrix

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

Note: CLI commands are case sensitive. Enter the CLI commands in lower case.

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**
Reboot	**x**	**x**
Reset Factory Configuration	**x**	**x**
Reset System Uptime	**x**	**x**
Set Circuit ID		**x**
Show Circuit ID		**x**
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
Set USB Port State	x	x
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
Show USB Port State	x	x
Slot Power On / Power Off / Reset	(PS)	(PS)
Switch Device Mode	x	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
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	

Bandwidth Commands	IONMM	NIDs
Set Bandwidth Rate Limiting Mode	x	x
Set Bandwidth Rate Limit	x	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
Set Dot1bridge Translation Type		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 State		x
Set Ethernet Port L2CP Configuration		x
Set Port Admin Mode (Ethernet PHY Mode)		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
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
Show Ethernet Port Configurations		x
Show Ethernet Port Loopback Capability		x
Show Ethernet Port Loopback Running Status		x
Show Ethernet Port L2CP Configuration		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
Show TP Port Cable Length		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**
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
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
Ignore Loopback Request		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
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

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**	

SNMP Commands	IONMM	NIDs
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	
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

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	IONMM	NIDs
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 Device Level Commands		
Add VLAN Database Entry		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		
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**

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>
```

In order 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 will appear on the command prompt line as the location where the command will be executed.

where:

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

ww = 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.

xx = optional; port number (1–16) on a level 1 device that is used to attach to a level 1 device.

yy = optional; port number (1–16) on a level 2 device that is used to attach to a level 2 device.

zz = 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 3device

Usage: ***go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)***

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 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 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 then **?**. See Appendix A for a list of 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 are the options, 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 displays the next parameter that follows condition.

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

And finally, the following 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
 index=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” 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 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.

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 NID.

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

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**=(true|false)

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, or value.

where:

SENSORID = { Temperature | Voltage | Power | Fan }

notif = {true enables sensor notification | false 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 = 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=true
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.

Set System Contact

Syntax: **set system contact**

Description: 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 with no spaces within the text. Numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed.

Example:

```
C1|S16|L1D>set system contact=99999999999999999999
C1|S16|L1D>show system information
system descr:        The C2220-1014 of the Transition Networks
                     ION (Chassis Generation III) platform
                     products
system objectID:     1.3.6.1.4.1.868.2.5.1802661751
system uptime:       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 Transition Networks (techsupport@transition.com). The **show system information** command displays the system contact, system location, system name, and other system descriptive information.

Set System Location

Syntax: **set system location**=LOC

Description: 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 with no spaces within the text. Numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed.

Example:

```
C1|S16|L1D>set system location=Corporate
```

```
C1|S16|L1D>show system information
system descr:        The C2220-1014 of the Transition Networks
                     ION (Chassis Generation III) platform
                     products
system objectID:     1.3.6.1.4.1.868.2.5.1802661751
system uptime:       3 days, 03:09:19
system contact:      99999999999999999999
system name:         C2220-1014
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: Defines the identifying name of the device. The name can be alphabetic, numeric or a combination, but with no spaces within the text. Numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed.

Example:

```
C1|S16|L1D>set system name=<>)|
C1|S16|L1D>show system information
system descr:  The C2220-1014 of the Transition networks ION
               (Chassis Generation III) platform products
system objectID:     1.3.6.1.4.1.868.2.5.1802661751
system uptime:       3 days, 03:41:07
system contact:      999999999999999999999
system name:         <>)|
system location:     Corporate
C1|S16|L1D>
```

The system name default is C2220-1040 (case sensitive – all capitals). The **show system information** command displays the system contact, system location, system 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 NID will not respond to CLI commands entered by a local management station across the USB serial interface. The only access to the x222x/32xx 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 module.

Example 1: (C2220 in slot 16):

```
AgentIII C1|S16|L1D>show card info
System name:        C2220-1014
Uptime:             4 days, 05:56:22
CPU MAC:            00-c0-f2-21-02-b3
Port number:        2
Serial number:      11673589
Config mode:        software
Software:           1.3.1
Bootloader:         1.2.1

Hardware:           1.0.0
AgentIII C1|S16|L1D>
```

Example 2: (C3220 NID in slot 18):

```
AgentIII C1|S6|L1D>show card info
System name:        C3220-1040
Uptime:             4 days, 04:06:23
CPU MAC:            00-c0-f2-20-e2-40
Port number:        2
Serial number:      11615637
Config mode:        software
Software:           1.3.1
Bootloader:         1.2.1

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

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

Show Card Type

Syntax: **show cardtype**

Description: Displays the 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 / remote0

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 a direct connection to the device.
- remote – device is managed through the IONMM.

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

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

Example:

```
C1|S3|L1D>show switch mode
Switch mode: remote
C1|S3|L1D>
```

Show Power Supply Configuration

Syntax: **show power config**

Description: Displays the current configuration of the specified ION system power supply.

Example:

```
C1|S22|L1D/>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
```

```
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
        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 in units

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|S5|L1D>show slot info
Cannot show slot info on this card!
C1|S5|L1D>home
C1|S7|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|S7|L1D>
```

Show System Information

Syntax: **show system information**

Description: Displays current ION Chassis slot information.

Example 1 (C2220 in slot 16):

```
C1|S16|L1D>show system info
system descr:              The C2220-1014 of the Transition networks ION
                           ION (Chassis Generation III) platform products
system objectID:           1.3.6.1.4.1.868.2.5.1802661751
system uptime:             2 days, 00:12:20
system contact:            Transition Networks(techsupport@transition.com)
system name:               C2220-1014
system location:           10900 Red Circle Drive  Minnetonka, MN 55343 USA
C1|S16|L1D>
```

Example 2 (C3220 in slot 18):

```
C1|S18|L1D>show system info
system descr:              The C3220-1040 of the Transition networks ION
                           (Chassis Generation III) platform products
system objectID:           1.3.6.1.4.1.868.2.5.1802661751
system uptime:             22:56:43
system contact:            Transition Networks(techsupport@transition.com)
system name:               C3220-1040
system location:           10900 Red Circle Drive, Minnetonka, MN 55343 USA
C1|S18|L1D>
```

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 device. 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 card for the changes to take effect. At the command prompt type **reboot** and press **Enter**.

⚠ 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 can not set/show the switch mode on all card types.

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

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

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

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

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

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 *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 **show circuit-ID** command to display the current Circuit ID information defined 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 (in capital letters).

Note: The NID 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* (in the format 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>
```

Note: 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>
```

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 can not 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>
```

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 x222x/x32xx 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 x222x / x32xx NID is INPUT. This chain contains the rules and conditions for accessing the NID through an Ethernet connection (via Telnet session or Web interface).

An ACL rule defines the policy to be followed for certain defined conditions. There are three different policies (rules) that can be defined for the 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 for 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**
- **ipv4addr**
- **tcpport**
- **ipv4network**
- **ipv4addrrange**
- **tcpportrange**
- **udpport**
- **udpportrange**
- **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 (i.e., 1–4).

Example:

```
C1|S18|L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=172.16.6.123
C1|S18|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 with no spaces (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|S18|L1D>add acl rule position=head table=filter chain=input policy=trap
 traprate=100
C1|S18|L1D> show acl rule
index table-type chain-type priority  policy traprate(packets/min)
            condition
-----------------------------------------------------------------------------
1     filter      input     1         trap    100                       no
C1|S18|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 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=accept
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.

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 condition 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|L0D/>show acl chain
```

```
table-type     contain-type      chain-name        default-policy
-----------------------------------------------------------------
filter         input             INPUT             accept
```

ACL Commands for IPv6

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

The following commands are used for ACL operations under IPv6.

Command: **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!*

Command: **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!*

Command: **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!*

Command: **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!*

Command: **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

Command: **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!

Command: **Create an IPv6 Tables 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 pol-
icy= trap 444
Agent III C1|S1|L1D>show ip6tables acl rule
index  table-type   chain-type   priority  policy    traprate(packets/min)    condi-
tion
--------------------------------------------------------------------------------------
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!

Command: **Create a 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>
```

Command: **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!

Command: **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!

Command: **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!

Command: **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!*

Command: **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!

Command: **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!

Command: **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!

Command: **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)" on page 6.
2. Contact TN 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)" on page 6.
2. Contact TN 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)" on page 6.
2. Contact TN Technical Support if the problem persists.

Backup / Restore (Provision) Commands

The following commands are used to show, backup, and restore prov modules, and to set provision module configuration. **Note**: These commands can only be entered on the IONMM or a standalone SIC. **Note**: starting at v 1.3.10, Backup file name and TFTP upload/download file name are extended to maximum 128 characters.

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.

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...
Buckup 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.
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.

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.

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...
Buckup 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>
```

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). These commands cannot be entered at the device level – only at the port level.

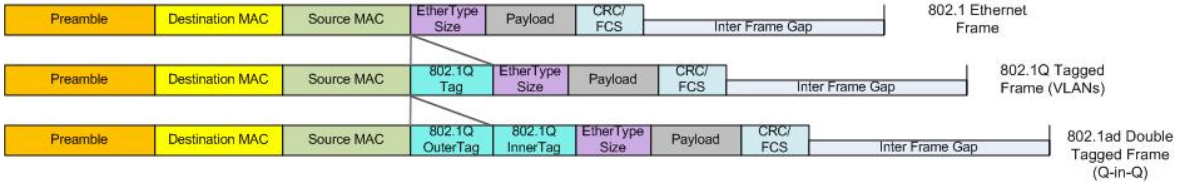
Set Bandwidth Rate Limiting Mode

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 Counts All Layer 3 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.

where:

xx= In-rate: Ingress rate in kbps

yy = Egress-rate: Egress rate in kbps

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.

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 type and ingress and egress rates 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.

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 support DMI. Transition Networks 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 configuration of the Diagnostic Monitoring Interface (DMI).

Example:

```
Agent III C1|S9|L1P2>show dmi info
Diagnostic monitoring interface information:
-----------------------------------------------------------------
DMI connector type:                                    LC
DMI indentifier:                                       SFP
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:                                       38.0*C
DMI temperature:                                       100.4*F
DMI temperature alarm:                                 normal
DMI transmit bias current:                             14752*uA
DMI transmit bais alarm:                               normal
DMI Transmit power:                                    247*uW
DMI Transmit power:                                    -6.073*dBM
DMI Transmit power alarm:                              normal
DMI Receive power:                                     0*uW
DMI Receive power alarm:                               lowAlarm
DMI Receive power intrusion threshold:                 0*uW
Agent III C1|S9|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.

where:

xx = Pwr-val: A preset level for Rx Power on the Fiber port (1-100).

Example:

```
Agent III C1|S9|L1P2>set dmi rx-power-preset-level=110
Agent III C1|S9|L1P2>show dmi info
Diagnostic monitoring interface information:
------------------------------------------------------------------------
DMI connector type:                                    LC
DMI indentifier:                                       SFP
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:                                       38.7*C
DMI temperature:                                       101.7*F
DMI temperature alarm:                                 normal
DMI transmit bias current:                             14704*uA
DMI transmit bais alarm:                               normal
DMI Transmit power:                                    246*uW
DMI Transmit power:                                    -6.091*dBM
DMI Transmit power alarm:                              normal
DMI Receive power:                                     0*uW
DMI Receive power alarm:                               lowAlarm
DMI Receive power intrusion threshold:                 110*uW
Agent III C1|S9|L1P2>
```

Dot1bridge Commands

The following dot1bridge commands are used to add, remove, set, and show dot1bridge 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 x222x & x32xx can learn up to 8192 entries, there is a limit of 1000 entries that it can manage via the Web/CLI/FP interfaces. So even if the NID learns more than 1000 entries, only 1000 entries (including static entries) can be displayed/managed though the x222x & x32xx interface (as limited by x222x & x32xx memory space and CPU capability).

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
```

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>
```

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	√		*	*
Cable Length	√			
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 NID. The port's counts (RMON statistics counters, dot3 counters, etc.) are reset to zero.

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 copper port.

The auto-negotiate feature must be enabled for this command to have any affect (see "Set Ethernet Port Auto-Negotiation Status" on page 31). In addition to the speed and duplex function, the port also advertises whether it supports pause frames (see "Set Ethernet Port Pause Frames" on page 33).

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|S16|L1D>set ether adv-cap 1000XHD
Error: this command should be executed on a port!
C1|S16|L1D>go l1p=1
C1|S16|L1P1>set ether adv-cap 1000XHD
Bad advertisement capability!
C1|S16|L1P1>set ether adv-cap 100FXD
Bad advertisement capability!
C1|S16|L1P1>set ether adv-cap 100TFD
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>set ether adv-cap 100TFD
Bad advertisement capability!
C1|S16|L1P2>
C1|S16|L1P2>set ether autoneg state enable
Cannot set auto-negotiation state on this port!
C1|S16|L1P2>go l1p=1
C1|S16|L1P1>set ether autoneg state enable
C1|S16|L1P1>set ether adv-cap 10TFD
C1|S16|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. Transition Networks recommends leaving AutoCross in 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
```

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 49).

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 loopback method 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 (AKA “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 ether loopback state** command or the **show ether loopback capability** command to display the current loopback type settings.

Set Ethernet Port Pause Frames

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|S16|L1P1>set ether pause=pause
C1|S16|L1P1>set ether pause=nopause
C1|S16|L1P1>set ether pause=apause
Fail to set pause capability!
C1|S16|L1P1>set ether pause=bpause
Invalid pause value!
C1|S16|L1P1>set ether pause=spause
Invalid pause value!
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>set ether pause=spause
C1|S16|L1P2>set ether pause=bpause
C1|S16|L1P2>set ether pause=apause
C1|S16|L1P2>set ether pause=nopause
C1|S16|L1P2>set ether pause=pause
Invalid pause value!
C1|S16|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 the Ethernet copper port. If Auto-negotiation is enabled, you can not set the port speed.

Example (copper port):

```
C1|S16|L1P1>set ether speed ?
  1000M
  100M
  10M
C1|S16|L1P1>set ether speed 1000M
Can not set 1000M speed for this card!
C1|S16|L1P1>set ether speed 100M
C1|S16|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 Configuration

Syntax: **show ether config**

Description: Displays the Ethernet port configurations on a slide-in module.

Different ports have different capabilities, so the display content will vary according to the slide-in module 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 loopback capability of the Ethernet port.

Example:

```
C1|S16|L1P1>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S16|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 running status of the Ethernet port.

Example:

```
C1|S16|L1P1>show ether loopback state
Loopback type: noloopback
Loopback state: noLoopback
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>show ether loopback state
Loopback type: noloopback
Loopback state: noLoopback
C1|S16|L1P2>
```

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|S16|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|S16|L1P1>go l1p=2
C1|S16|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|S16|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|S16|L1P2>show ether tdr config
No TDR test result on FIBER port!
C1|S16|L1P2>go l1p=1
C1|S16|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----------------------------------------------------------------
TDR test state:               success
TDR test init time:           08:35:26
TDR test result valid:        true
C1|S16|L1P1>
```

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.

Example:

```
C1|S18|L1P1>show ether tdr test result
```

```
Cable pair :
index               distance to fault(unit)       status
-----------------------------------------------------------------
pair1and2           unknown                       unknown
pair3and6           unknown                       unknown
pair4and5           unknown                       unknown
pair7and8           unknown                       unknown
C1|S18|L1P1>
```

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|S16|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|S16|L1P1>
```

Start/Stop Ethernet Port Loopback Operation

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

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

Example:

```
C1|S16|L1P1>set ether loopback oper ?
  init
  stop
C1|S16|L1P1>set ether loopback oper init
Admin state of Link OAM of this port is disable, please enable it
first!
C1|S16|L1P1>set ether admin state=up
C1|S16|L1P1>set ether loopback oper init
C1|S16|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|S16|L1P1>start ether tdr test
C1|S16|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
C1|S16|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----------------------------------------------------------------
TDR test state:               success
TDR test init time:           2 days, 03:29:24
TDR test result valid:        true
C1|S16|L1P1>go l1p=2
C1|S16|L1P2>show ether tdr config
No TDR test result on FIBER port!
C1|S16|L1P2>
```

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 protocol=**<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
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).tnIONProducts(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. Layer 2 Control Protocol Processing is supported at a per port level.

Example:

```
Agent III C1|S4|L1P2>show l2cp config
Parameter                                    Value
-----------------------------------------------------------------
Spanning Tree Protocols                      pass
Slow Protocols                               pass
Port Authentication Protocols                pass
ELMI Protocols                               pass
LLDP Protocols                               pass
Bridge Mgmt Protocols                        pass
GARP/GMRP Block of Protocols                 pass
Bridge Block Other Multicast Protocols       pass
Agent III C1|S4|L1P2>
```

Set Port Admin Mode (Ethernet PHY Mode)

Syntax: **set ether phymode**

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

where:

xx = port admin mode (SGMII | 100BaseFX | 1000BaseX); the valid choices are:

- 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 status (PHY mode change cap and PHY operation mode).

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.

Show TP port cable length

Syntax: **show cable length**

Description: Displays the TP (copper) port cable length of the specified x2110 NID.

Example:

```
C1|S12|L1P1>show cable length
Cable length: N/A (no cable/broken/>140 meters)
C1|S12|L1P1>
```

The Cable lengths returned can include:

- <20 meters
- >20 meters and <40 meters
- >40 meters and <60 meters
- >60 meters and <80 meters
- >80 meters and <100 meters
- >100 meters and <120 meters
- >120 meters and <140 meters
- N/A (no cable/broken/>140 meters)

Note: Not all NIDs support this command. If this command is entered on an unsupported NID, the message "*Cannot show TP port cable length on this card!*" displays. See "Appendix C: CLI Messages and Recovery" on page 194.

Forwarding Database Commands

The following commands are used to add, remove, set, and show fwddb (forwarding database) functions and parameters.

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 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 entry 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: Sets 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|S16|L1D>set fwddb mac=01-11-11-11-11-11 fdbid=1 type=static
C1|S16|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|S16|L1D>set fwddb mac 00-c0-f2-21-02-b3 fdbid=3 priority=5
C1|S16|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=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 or 2).

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

Set Forwarding Port Management Access

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

Description: Enables/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 (LxPx; where x is 1, 2 or 3).

Show Forwarding Database (FDB) Configuration

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

*Syntax:*Displays the configuration of forwarding database. 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>
```

Note: If the forwarding database is not yet configured, the message "*No data in VLAN forward database table now!*" displays.

Show Forwarding Database Ports

Syntax: **show fwd portlist**

Description: Displays the forwarding (fwd) port list of a device port.

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).

HTTPS Commands

For a description on how to configure the ION Management Module for Hypertext Transfer Protocol Secure (HTTPS) see “Configuring HTTPS” on page 43).

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

Example:

```
C1|S8|L1D>show https config
```

```
HTTPS configuration:
-----------------------------------------------------------------
HTTPS state:                  disable
HTTPS port:                   443
HTTPS certificate file:
HTTPS private key file:
```

Start HTTPS Certificate Operation

Syntax: **start https certificate**

Description: Starts the HTTPS certificate operation.

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>
```

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 x222x/32xx setup, and at first the CLI (command line interface) is used to configure the IP address settings. Thereafter, remote management and/or DHCP addressing can be configured.

The default values are IP Address = 192.168.0.10, Subnet Mask = 255.255.255.0, Default Gateway = 192.168.0.1, with no DNS address assigned, and no DHCP client enabled. When manually setting the x222x/32xx NID’s IP address, it can only be given a Class A, Class B or Class C address; it can not 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. **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:

```
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 DHCP server.

Set DNS Server

Syntax: **set dns–svr svr=**<xx> **type=**<yy> **addr=**<zz>

Description: Defines a single DNS server. Up to six servers can be defined in the system, 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)' on page **Error! Bookmark not defined.**.

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!

Use the **show ip–mgmt config** command to display the current DNS server information.
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 can not 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 can not be used, though one of them might be valid and available. ION DNS Servers 1, 2, and 3 are reserved for IPv4 only, and DNS Servers 4, 5, and 6 are just for IPv6.

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

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

Set IP Type / Address / Subnet Mask

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

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 IP Address = 192.168.0.10, Subnet Mask = 255.255.255.0, Default Gateway = 192.168.0.1, with no DNS address assigned, and no DHCP client enabled. When manually setting the NID's IP address, it can only be given a Class A, Class B or Class C address; it can not 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 address of the module

yy = subnet mask

Example:

```
C1|S13|L0D/>set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0
```

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

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 (the default setting).

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

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 IP Address

Syntax: **set gateway type=ipv4 addr=**<xx>

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:

```
C1|S7|L1D>set gateway type=ipv4 addr=192.168.0.1
C1|S7|L1D>
```

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

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 NID.

Example:

```
C1|S18|L1D>set ip type=ipv4 addr=192.168.1.10 subnet-mask=255.255.255.0
C1|S18|L1D>set gateway type=ipv4 addr=192.168.1.0
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>
```

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 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 LOAM 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
```

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|S16|L1D/>set rfd state=enable
C1|S16|L1D/>
```

Use the **show lpt config** command to display the current RFD configuration.

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)".

LOAM (Link OAM) Commands

OAM (Operation, Administration and Maintenance) is a set of functions designed to monitor network operation in order 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 x222x/x32xx NIDs support 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 (LxPy; where y 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 restarts the counters.

Note: 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|S16|L1D>show loam peer info
Error: this command should be executed on a port!
C1|S16|L1D>go l1p=1
C1|S16|L1P1>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|S16|L1P1>
```

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 Loopback Requests

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

where:

enable – causes the LOAM enabled x222x/32xx NID to ignore all Loopback requests (i.e., not respond to remote loopback requests from peers).
disable – causes the LOAM enabled x222x/32xx NID to respond to all remote loopback requests (LBRs) from peers.

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).

Example:

```
C1|S16|L1P2>set loam ignore-loopback-request ?
  disable
  enable
C1|S16|L1P2>set loam ignore-loopback-request disable
C1|S16|L1P2>set loam ignore-loopback-request enable
C1|S16|L1P2>
```

Note: Use the **show loam ignore-loopback-request** 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 device port.

Example:

```
C1|S16|L1P2>set loam admin state ?
  disable
  enable
C1|S16|L1P2>set loam admin state disable
C1|S16|L1P2>set loam admin state enable
C1|S16|L1P2>
```

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).

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 LOAM 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 OAM 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>

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}

Enables or disables whether OAM 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.

where:

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 (OAM Information PDUs). It can initiate OAM Loopback to its remote peer.

passive – the NID can receive and respond to discovery messages (OAM Information PDUs). It can not initiate LOAM Loopback but 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:

```
C1|S16|L1P1>show loam config
Link OAM configuration:
-----------------------------------------------------------------
Link OAM admin state:         disable
Link OAM operation status:    disabled
Link OAM mode:                passive
Link OAM maximum PDU size:     0
Link OAM configuration revision:0
Link OAM function supported:  loopbackSupport+eventSupport

C1|S16|L1P1>go l1p=2
C1|S16|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|S16|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
Link OAM 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.

Exampl1:

```
C1|S13|L0AP1|L1P1/>show loam event log
timestamp  OUI      type        location W-hi   W-lo   T-hi  T-lo    value   R-total E-total
--------------------------------------------------------------------------------------------
00:00:01  01:80:c2  linkFault   local    -          -      -     -      -       1      1
00:00:01  01:80:c2  critical    local    -          -      -     -      -       1      1
```

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 (ignore or respond to all remote loopback requests from peers).

Example:

```
C1|S16|L1P1>show loam ignore-loopback-request
Link OAM Ignore loopback request:             disable
C1|S16|L1P1>
```

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.

Used with the current MAC Filtering feature (FDB tab, MACs table)?? or used with the current MAC Addresses Blocking ?

The MAC address can be added to the static MAC address database with the ‘connected port’ as zero. This will cause any frames from that MAC address database to cause an ATU-member violation on that port, resulting in sending a trap.

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

Description: Displays the current port MAC learning status (port 1, port 2, and/or port 3 enabled or disabled).

Syntax: show mac learning port list <cr>

Example 1:

```
C0|S0|L1D/>show port mac_learning state
Port Mac learning:
Port1:                             enable
Port2:                             disable
Port3:                             enable
```

Example 2:

```
C1|S18|L1D>show port mac_learning state
Port Mac learning:
Port1:                             disable
Port2:                             enable
C1|S18|L1D>
```

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. It's specified as part of the MIB as an extension of the SNMP.

Note: this command can only be entered for the port, not the 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>
```

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 at the port level - when the last part of the command line prompt indicates the location is a port (e.g., `C1|S3|L1P2`>).

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**=<x> **remap-priority**=<y>

Description: Defines the priority remapping for IEEE.

where:

x = index number, 0 – 7

y = 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**=<x>**remap-priority**=<y>

Description: Defines a port’s priority remapping for traffic that originates outside of the network.

where:

x = index number, 0 – 7

y = 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" priority queuing method,

where:
wrr = Weighted Round Robin egress port queuing
sp = Strict egress port queuing

Example:

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

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

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>
```

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 NID for RADIUS, your HyperTerminal session ends, and you will be required to enter the RADIUS defined username and password when connecting to the NID.

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:

xx = server number (1–6)

yy = number (0–5) of retry attempts allowed. The 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

Syntax: **show radius config**

Description: Displays all RADIUS configurations on the device.

Example:

```
C1|S3|L1D>show radius config
```

```
RADIUS client state:          enable

RADIUS authentication server:
index     addr-type      addr           retry     timeout
-----------------------------------------------------------------
1         ipv4           192.168.1.30   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
```

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.

The fault discovery method is LOS at the receiving interface for a set continuous period of time. Traffic rerouting occurs within a minimum period of time after the Primary Port is declared in the fault state. Traffic flow is restored within a minimum set period of time after a fault occurs.

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., x3221 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. This card must have at least two fiber ports to do redundancy (e.g., S3231 NID). 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
redundancy state:                   enable
Primary port :                            2
Secondary port :                          3
Active port :                             2
C1|S8|L1D>
```

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

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

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  ...
Š□CCCCCCCCCCC□□B□B0□□B□B0□□B□B0□□□□B□B0□□B□B0□□B□B0□□□□B□B0□□B□B0□□B□B0□□B□B0
□□B
□□B□B0□□B□B0□□B□B0□□B□B0□□B□B0
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  ...
Š□lsz: cannot open /tftpboot/xxxx: No such file or directory
□□B□B0□□B□B0□□B□B0□□
B□B0□□B□B0
Can't open any requested files.
□□B□B0□□B□B0□□B□B0□□B□B0□□B□B0
file transfer failed!
```

Serial Upgrade Protocol

Command: **Serial Upgrade Protocol**

Syntax: **serial upgrade protocol**=xxx

Meaning: Performs a firmware upgrade over the selected serial line.

Example:

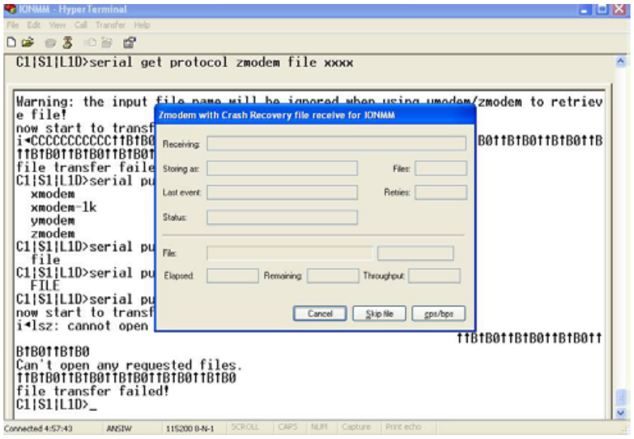
```
C1|S1|L1D>serial upgrade protocol ?
  xmodem
  xmodem-1k
  ymodem
  zmodem
C1|S1|L1D>serial upgrade protocol zmodem file xxxx
now start to transfer the file  ...

**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



```
C1|S1|L1D>serial get protocol zmodem file xxxx

Warning: the input file name will be ignored when using ymodem/zmodem to retriev
e file!
now start to transf
i◄CCCCCCCCCCCC↑↑B↑B0                               B0↑↑B↑B0↑↑B↑B0↑↑B
↑↑B↑B0↑↑B↑B0↑↑B↑B0↑
file transfer faile
C1|S1|L1D>serial pu
  xmodem
  xmodem-1k
  ymodem
  zmodem
C1|S1|L1D>serial pu
  file
C1|S1|L1D>serial pu
  FILE
C1|S1|L1D>serial pu
now start to transf
i◄lsz: cannot open
                                                    ↑↑B↑B0↑↑B↑B0↑↑B↑B0↑↑
B↑B0↑↑B↑B0
Can't open any requested files.
↑↑B↑B0↑↑B↑B0↑↑B↑B0↑↑B↑B0↑↑B↑B0
file transfer failed!
C1|S1|L1D>_
```

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 of time (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 a number of 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 of time.

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).

Command Categories

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

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

Command Summaries

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

SNMP v3 Command Parameters

1. add snmp community name=STR_COMM_NAME access_mode=(read_only|read_write)
2. 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]
3. add snmp local user name=STR_USR_NAME security-level=(noAuthNoPriv|authNoPriv|authPriv) [auth-protocol=(md5|sha) password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS] [group=STR_GRP_NAME]
4. add snmp remote engine addrtype=ipv4 addr=STR_SVR_ADDR port=<1-65535> engine_id= STR_ENGINE_NAME
5. 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|sh password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]
6. 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]
7. add snmp traphost version=(v1|v2c|v3) type=ipv4 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>]
8. add snmp view name=STR_SNMP_VIEW oid=STR_VIEW_OID type=(include|exclude)
9. remove snmp community name=STR_COMM_NAME
10. remove snmp group name=STR_SNMP_GRP [security-model=(v1|v2c|v3) security-level=(noAuthNoPriv|authNoPriv|authPriv)]
11. remove snmp local user name=STR_USER_NAME
12. remove snmp remote engine addrtype=ipv4 addr=STR_SVR_ADDR port=<1-65535>
13. remove snmp remote user name=STR_USER_NAME addrtype=ipv4 addr=STR_SVR_ADDR port=<1-65535>
14. remove snmp remote user name=STR_USER_NAME engine=STR_ENGINE_ID
15. remove snmp traphost type=ipv4 addr=STR_SVR_ADDR port=<1-65535>
16. remove snmp view name=STR_SNMP_VIEW [oid=STR_VIEW_OID]
17. set snmp local engine=STR_LOCAL_ENGINE
18. set snmp local user name=STR_USER_NAME group=STR_GRP_NAME
19. set snmp view name=STR_SNMP_VIEW oid=STR_VIEW_OID type=(include|exclude)
20. show snmp community
21. show snmp group [name=STR_SNMP_GRP]
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 [name=STR_SNMP_VIEW]

Each of these SNMP commands is described below.

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.

Command: **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>
```

Command: **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 can not add a new group whose name, security level 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>
```

Command: **Add SNMP Local User**

Syntax:

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

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>
```

Command: **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:

```
C1|S1|L1D>add snmp remote engine addrtype=ipv4 addr=192.168.1.70 port=162 engine_id=
800003640300C0F2209EDE
This engineID already exists!
C1|S1|L1D>add snmp remote engine addrtype=ipv4 addr=192.168.1.70 port=162 engine_id=
800003640300C0F2208DCE
C1|S1|L1D>
```

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!*

Command: **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>
```

Command: **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>
```

Command: **Add SNMP Traphost**

Syntax:

add snmp traphost version=(v1|v2c|v3) type=ipv4 **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. Five mandatory parameters (version, 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).

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>
```

Command: **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 can not 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>
```

Command: **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>
```

Command: **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" can not 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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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 can not be removed. This command is available to users with Write or Admin level privileges.

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
```

Command: **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.

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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>
```

Command: **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
```

Command: **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.

Command: **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>
```

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 (e.g., `C0|S1|L1D>`).

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: s**et 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:

```
C0|S1|L1D>set sntp dst-state enable
C0|S1|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:

```
C0|S1|L1D>set sntp dst-start=<”2010-05-30 02:00”
C0|S1|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=<”2009-11-01 02:00”
C1|S3|L1D>
```

The above command sets daylight savings time to end at 2 a.m. on November 1, 2009.

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 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 servers can be defined in the system.

where:

xx = server number (1–6)

yy = IP address format; valid choices are:

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

zz = IP address of the SNTP server

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
C1|S3|L1D
```

Set SNTP Status

Syntax: **set sntp state**=<{enable | disable}

Description: Enables or disables the SNTP function on an x222x/32xx NID or IONMM card.

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 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:

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

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 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!
C1|S3|L1D>
```

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 login 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 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 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.

Example:

```
Host-key generated!
C1|S16|L1D>show ssh ?
  config
  host-key
  public-key
C1|S16|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 b7 9e 1f 3f
 31 3f 7d 0c 90 90 83 69 ec 65 4e c0 bb a9 87 ae eb 16 7f fc f7 27 d0 f7 a9 3e 0
a 03 07 71 14 8b 6f 96 4a 47 62 f9 13 c3 62 de 82 73 b7 67 6d a6 26 a2 b4 42 3d
9f 4f 89 5f f2 b2 59 b6 83 0b b0 c3 ed db d4 23 c2 9f 71 55 58 4f 0b 51 f4 67 1b
 cd 50 75 4c 4b a9 42 27 99 f1 d8 97 77 4a ce a3 47 a8 2f 5d 95 8d 9e a3 d7 cb 9
c 9d 35 ae c0 d6 d4 d8 08 8e 89 10 90 35 82 28 ce 77 42 1b 00 00 00 82 32 ed 5f
5b 46 8c 86 61 72 c3 32 3f b1 ba 53 82 6f 4a 51 00 b9 e1 6e b4 39 d4 c8 47 b8 a0
 25 64 bb ae a8 75 18 09 06 27 10 93 66 e0 dd 4e 3b be 5e 93 08 3d 7a 1f cc 81 4
6 d8 25 d6 43 4f 6c 1a 27 65 94 72 bb e8 c0 1b f7 ba 41 d4 98 f4 02 8f ef 5f 45
47 aa 23 80 92 9f ef ae 2f f0 87 0e 46 e8 f8 0a 76 11 73 73 3e c0 ce a8 03 a2 46
 9a 29 86 81 06 e5 98 a4 f1 01 ac d3 3e 76 91 dc 4b 93 b7 71 00 00 00 42 00 d2 4
a 84 8a e2 11 38 80 ec 7a b3 1e 9f 5e 12 7a d3 0b a5 55 04 49 13 d1 0b 58 bc 22
59 5e 2e 59 fe e6 8f 90 22 da 99 12 8d 39 57 a0 7a d7 ef 56 17 a5 27 e8 30 07 45
 44 e9 9f 40 cd a9 c1 36 aa 33 00 00 00 42 00 df 87 61 fd 4f 64 a1 b1 c3 18 2e b
0 82 8e 87 0b 72 ce f3 46 28 38 95 97 eb b9 01 59 aa f1 d7 54 8c 34 f1 ca 57 ed
f0 7e 96 6b 0a 2f fd 17 35 43 d8 36 2a 80 66 b0 89 14 fc a1 30 30 b0 44 ab f0 79

DSA host key:
00 00 00 07 73 73 68 2d 64 73 73 00 00 00 81 00 85 50 35 ba 78 c8 e7 ae 8d 83 1a
 48 33 3d d6 44 44 2b 09 84 31 73 f8 27 48 f6 04 fb 04 3e 11 ba 6b 74 43 f5 13 a
3 44 7c ae e4 c1 4d 3f ae 0c 65 6f 26 dc ff ad 98 84 6d 03 b8 aa ab 1e 0d 86 a4
43 91 e5 57 78 35 f9 53 4f 8c e5 79 63 7d 79 d5 96 61 c5 3a 27 63 cd d5 d6 55 a6
 60 c1 66 d4 ff d5 9b 56 f6 be b0 87 6d 43 6b 30 5d e0 f9 a7 50 65 89 b1 1a e9 9
e 5c 02 be 69 4a 1f 0d 3a 84 6b 00 00 00 15 00 81 8e 44 eb 64 95 94 19 ca 97 b8
86 97 7b 6f 17 1a 2e 5d 45 00 00 00 80 32 61 e7 16 21 ff 97 7c 2d 8c b3 44 ed 5c
 cc 0d d5 31 73 6f b0 08 bc b0 ae 1e 09 b1 ad 8a d4 3e 95 89 72 d2 f7 79 e8 24 6
b 1c c8 a4 9a ef 2c 87 27 0e a2 28 11 04 89 c4 4e 58 5b 5a 20 b3 40 a9 ea 84 ce
ce 17 15 9e 0d 40 d9 ca 0d 0e 68 99 61 61 8b 64 df ba 7a 80 5b 3b b9 46 eb ef 8b
 aa 14 5f 3b fe a9 ac 4e be 79 42 72 c4 6d 32 fb 5b c2 d5 ef cf d0 79 36 e9 fb e
2 b7 7c 8b f8 0a 22 ee 00 00 00 80 5d 72 75 dc 99 3f ac 43 49 fb dd fb f5 6e de
3c 8d d7 c6 d7 0f d7 4f 89 7c 35 34 30 58 89 1f 8e 95 9a ef 46 b8 58 22 07 db e2
 c6 cc 6e 3d aa 35 bc fa b7 66 05 2d ae 48 37 38 2e b7 c2 ad 0d b5 ef f1 cf 5e 5
3 fc 20 0c 02 11 56 62 d5 13 86 13 78 4c cf aa 3e 51 ec f7 a0 8f b1 a0 58 c8 81
98 2c 81 1a bd 69 ec dc 98 24 af 7f 20 01 8f 18 da c2 0d 1e ee 9e b0 e4 4c 0c c2
 25 65 a4 74 68 d8 00 00 00 14 14 79 a9 8a bf 47 65 a5 55 21 62 c5 90 43 4a 3c 0
0 4a 1f 89
C1|S16|L1D>
```

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.

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> <cr>
set syslog mode=(local|remote|localAndRemote|off) <cr>
set syslog level=(emerg|alert|crit|err|warning|notice|info|debug)
<cr>
set syslog svr type=(ipv4|dns) addr=SYSLOG_SVR_ADDR <cr>
```

Example:

```
C1|S3|L1D> set syslog set syslog svr addr=192.168.1.30
C1|S3|L1D> set syslog 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>
```

Command: **Clear Syslog Records**\n

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>
```

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.

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 re quired.

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!

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!

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 try ing 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!

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!

Command: **Set a TACPLUS Server / Type / Address / values**

Syntax: **set tacplus svr**=<1-6> **type**=(ipv4 |ipv6|dns) timeout=

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!
TACPLUS server retry is out of range!
Wrong parameter number!

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 excecuted 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 TACACS+ settings have been changed and a re-login will be performed right now.*"

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” on page 111.
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" on page 111.
4. Check the RADIUS configuration.
5. Retry the command. See the related manual or section.
6. Check your third party TACACS+ server documentation and helps (e.g., ClearBox Server, etc.).
7. If the problem persists, contact TN 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"

TNDP Commands

TNDP (TN Topology Discovery Protocol) is the Transition Networks implementation of LLDP. When set to Enabled, the device entering this command will no longer be discovered by the IONMM if it is remotely managed through this port.

Set TNDP (TN Topology Discovery Protocol) State

Command: **set tndp**=<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>
```

Backed up/Restored: Yes

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>
```

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 can not 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 Admin level login users only.

Note: A TFTP server must be online, configured and operational.

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 re-
motefile x323x_0.8.5_AP.bin
TFTP transferring...
Agent III C1|S1|L1D>

Usage: tftp get iptype=(ipv4|dns) ipaddr=ADDR remotefile=RFILE
[localfile=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 lo-
calfile 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 remote-
file IONMM_0.8.5_AP

Processing...

TFTP transfer failed!
Agent III C1|S1|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30
remotefile IONMM_0.8.5_AP.bin

Processing...

TFTP upgrade succeeded!
```

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>
```

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 or not the update was successful). If the update failed, this command will display the reason. This command must be entered from the IONMM card.

Example 1:

```
C0|S0|L1d/>show firmware-db update result
Database file name:           binary.zip
Database update result:       failure
Database update fail reason:  invalid input file
```

Example 2:

```
C1|S5|L1P2>show firmware-db update result
Upgrade is only supported on IONMM card!
C1|S5|L1P2>home
C1|S7|L1D>show firmware-db update result
Database file name:           IONMM.bin.1.1.0.zip
Database update result:       success
C1|S7|L1D>
```

Example 3:

```
C1|S7|L1D>show firmware-db update result
Database file name:           x323x.bin.1.1.0
Database update result:       success
```

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 upgrade command is only supported from the IONMM.

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" on page 207 for error messages and recovery procedures.

Show Upgrade File Name

Syntax: **show upgrade firmware file**

Description: Displays the name of the upgrade files. This upgrade is only supported on the IONMM.

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 (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 is only supported on the IONMM.

Example:

```
C1|S7|L1D>update firmware-db file x323x.bin.1.0.5
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“ on page 157.

Upgrade Device Firmware

Syntax: **upgrade module**

Description: Causes the firmware in the device selected in the command line prompt to be upgraded. This upgrade is only supported on the IONMM.

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

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**. The message “*processing* ...” displays.

Note: It may take some time to finish the task; you can continue with other work, then use "**show firmware upgrade result**" to check 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*). See “Section 5 – Troubleshooting” on page 201 for error messages and recovery procedures.

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 can not 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 can not be changed to “Enabled” when no port members are selected.
3) Management VLAN Status “Disabled” means that Management access is allowed on all the ports; the values in Management VLAN ID and port members are ignored.
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) can not 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 x3220 or 1-3 for x3221).

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: **set vlan vid=**<xx> [**priority=**<yy>] [**pri–override=**{zz}]

Description: Displays the current VLAN configuration settings.

Example:

```
C1|S3|L1D>show vlan config
vid:10       fid:0       priority:2         priv_override:disable
port1:     noMod  port2:     Tag
S3240>
```

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 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>
```

Configure VLAN Mode (Secure/Disable/Fallback/Check)

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

The VLAN Mode parameters are described below.

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

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

• **Fallback**: the default mode - handle packets with VLAN tag that is not present in vlan table just like packets without VLAN tag. Packets with VLAN tags that are present in VLAN table, but incoming port does not match any port in VLAN table entry does not get dropped.

• **Check**: drop packets with VLAN tag that is not present in VLAN table. Packets with VLAN tags that are present in VLAN table, but incoming port does not match any port in VLAN table entry does not get dropped. Packets without a VLAN tag are treated just as if they had a VLAN tag with a default port VLAN ID. This means that if VLAN Mode = Check or Secure is to be able to forward packets without VLAN tags, then you must add a special entry to the VLAN table with the same VLAN ID set according to the default VLAN ID.

Set Port VLAN Tag Mode

Syntax: **set port dot1-state**

Description: Configure a copper or fiber port’s IEEE 802.1q state.

Example:

```
Agent III C1|S2|L1P2>set port dot1-state ?
  check
  fallback
  secure
  vlanDisabled
  vlanEnabled
Agent III C1|S2|L1P2>set port dot1-state check
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  check
Discard-tagged:               false
Discard-untagged:             false
Default VLAN id:              1
Force use default VLAN id:    false
Agent III C1|S2|L1P2>set port dot1-state fallback
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                  fallback
Discard-tagged:               false
```

```
Discard-untagged:              false
Default VLAN id:               1
Force use default VLAN id:     false
Agent III C1|S2|L1P2>set port dot1-state secure
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                   secure
Discard-tagged:                false
Discard-untagged:              false
Default VLAN id:               1
Force use default VLAN id:     false
Agent III C1|S2|L1P2>set port dot1-state vlanEnabled
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                   secure
Discard-tagged:                false
Discard-untagged:              false
Default VLAN id:               1
Force use default VLAN id:     false
Agent III C1|S2|L1P2>set port dot1-state vlanDisabled
Agent III C1|S2|L1P2>show port vlan config
Dot1q state:                   vlanDisabled
Discard-tagged:                false
Discard-untagged:              false
Default VLAN id:               1
Force use default VLAN id:     false
Agent III C1|S2|L1P2>
```

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 port (e.g., `C1|S3|L1P1>`).

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|L1P1>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. This command sets Ethernet tagging type when VLAN tagging mode is set to “Provider” on a port interface.

where:

xx = x8100, x88a8, or x9100. You only need to define the Provider ETH Type if Provider was selected 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 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.

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 can not remove VID 1 as this is used for internal purposes.

Example:

```
C1|S3|L1D>remove vlan ?
  all
  vid
C1|S3|L1D>remove vlan all
```

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>
```

Zero Touch Provisioning (ZTP)

Note: ZTP is supported only in the standalone S3230-10xx and S3220-10xx at version 1.3.10.
The support for Zero Touch Provisioning changes the default behavior of the ION standalone S2220xx-10xx and S3220-10xx. The Chassis card C2220-10xx and C3220-10xx behavior stays the same as with prior releases.

When an ION S222x-10xx or 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 S222x-10xx or S3220-10xx via the USB port and typing the command "set switch mode remote". When an ION C3220-10xx or C3221-1040 Chassis card is powered up, it will come up in remote mode by default.

Zero Touch Provisioning (ZTP) lets you provision new switches in your network automatically, without manual intervention. When you physically connect a switch to the network and boot it with a default configuration, it tries to upgrade the software automatically and auto-install a configuration file from the network. The switch uses information that you configure on a Dynamic Host Control Protocol (DHCP) server to determine whether to perform these actions and to locate the necessary software image and configuration files on the network.

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.

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 particular 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 S222x-10xx and S322x-1-xx. ZTP 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.

Technical Support

Technical support is available 24-hours a day at:

United States:	1-800-260-1312
International:	00-1-952-941-7600

Live Web chat

Chat live via the Web with a Transition Networks Technical Support Specialist.

Go to: http://www.transition.com/TransitionNetworks/Now.aspx

Click Transition NOW to begin a live chat session.

Web-based training

Transition Networks provides 12-16 seminars per month via live web-based training.

Log onto www.transition.com and click the Learning Center link at the top of the page.

E-Mail

Ask a question anytime by sending an e-mail message to our technical support staff: **techsupport@transition.com**

Address

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343, U.S.A.

Telephone: 952-941-7600

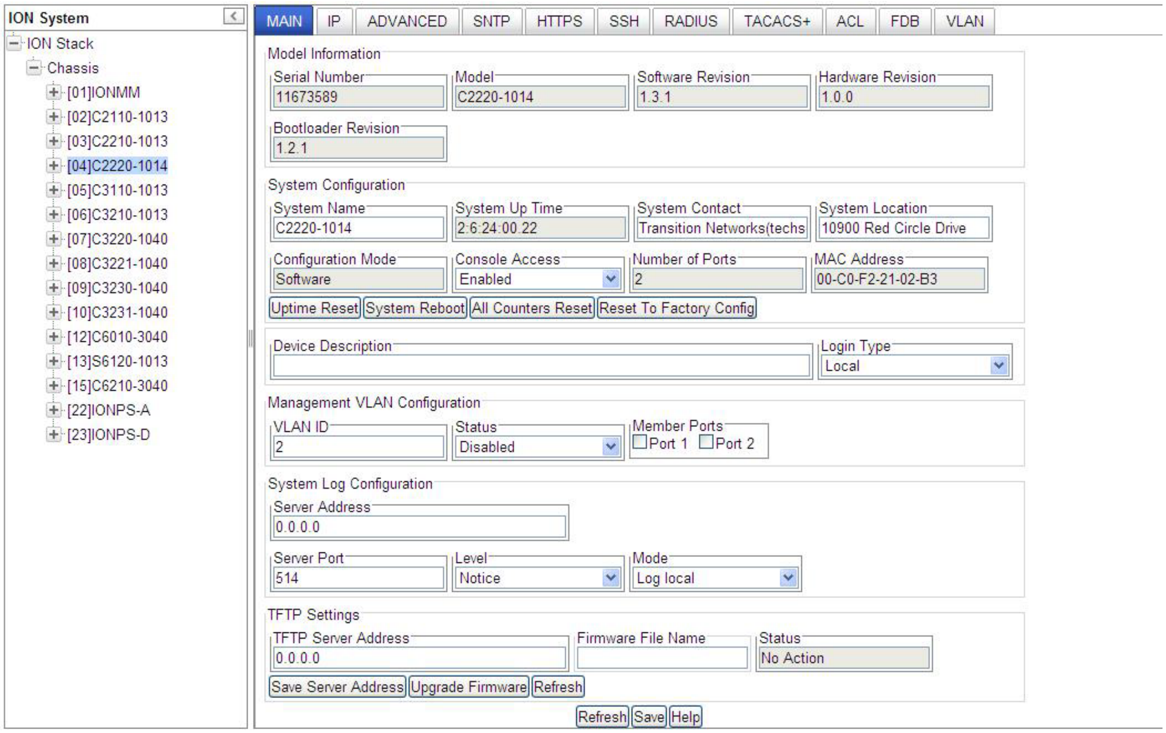
Toll free U.S.A & Canada: 800-526-9267

Fax: 952-941-2322

Recording Model Information and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible in order to help the TN 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 TN Support Specialist.)



Model Information

Serial Number: 11673589
Model: C2220-1014
Software Revision: 1.3.1
Hardware Revision: 1.0.0
Bootloader Revision: 1.2.1

System Configuration

System Name: C2220-1014
System Up Time: 2:6:24:00.22
System Contact: Transition Networks(techs
System Location: 10900 Red Circle Drive
Configuration Mode: Software
Console Access: Enabled
Number of Ports: 2
MAC Address: 00-C0-F2-21-02-B3

Device Description:
Login Type: Local

Management VLAN Configuration

VLAN ID: 2
Status: Disabled
Member Ports: □Port 1 □Port 2

System Log Configuration

Server Address: 0.0.0.0
Server Port: 514
Level: Notice
Mode: Log local

TFTP Settings

TFTP Server Address: 0.0.0.0
Firmware File Name:
Status: No Action

2. Record the **Model Information** for your system.

Serial Number: ______________________ Model: ___________________

Software Revision: ___________________ Hardware Revision: ___________________

Bootloader Revision: ___________________

3. Record the **System Configuration** information for your system.

System Up Time: ______________________ Configuration Mode: ______________________

Console Access: ______________________ Device Description: _______________________

Number of Ports: ______________________ MAC Address: ________________________

4. Provide additional Model and System information to your Technical Support Specialist. See “Basic ION System Troubleshooting” on page 190.

Your Transition Networks 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 Transition Networks 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: ______________________________

Important note on product identification: When the full part number of a ION System device is abbreviated for use in catalogs and marketing literature, the first set of numeric digits in the string is dropped and replaced by the last. In most ION System products, the first set of numeric digits in the full part number is the same as the last, so this process is transparent. With the IONMM, this is not true.

Appendix A: CLI Command Summary

This appendix provides the list of available CLI commands 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. To execute these commands, press the **Enter** key after the command has been entered.

ION CLI Commands via the *help* Command (C1|S8|L1D>*?*)

```
Agent III C1|S7|L1D>?
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 given MEP. Please note that only 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 module.
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|S7|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 in lower case. 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.

Agent III C1|S7|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=
11. (md5|sha) password=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]
12. 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]
13. 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>]
14. add snmp view name=STR_SNMP_VIEW oid=STR_VIEW_OID type=(include|exclude)
15. add soam ma local-ma-id=<1-4294967295> local-md-id=<1-4294967295> ma-name=NAME vlan-type=(none|ctype|stype|doubletag) [primary-vlan=<1-4095>] [s-vid=<1-4095>]
16. add soam md local-md-id=<1-4294967295> md-name=(NAME|none) md-level=<0-7>
17. 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>]
18. add soam mep mep-id=<1-8191> local-parent-id=<1-4294967295> direction=(up|down) port=<1-2>
19. add soam mip mip-type=(y.1731|802.1ag) local-mip-id=<1-4294967295> local-parent-id=<1-4294967295> port=<1-2>
20. add sysuser name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR
21. add vlan-db vid=<1-4094> [priority=NUM] [pri-override=(enable|disable)]
22. backup module-list=STR_MODULE_LIST
23. cat [OPTION] [FILE]
24. cd [DIR]
25. clear ether all counters
26. clear loam stats
27. clear syslog
28. cls
29. flush fiddb type=(all|dynamic)
30. flush vlandb all
31. generate ssh host-key=(dsa|rsa|both)
32. go [c=STR_CHA] [s=STR_SLOT] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|
33. l3p=<1-15>|l1d|l2d|l3d)
34. home
35. list

```
36.  ls [OPTION] [FILES]
37.  more [OPTION] [+linenum] FILE ...
38.  ping [-c COUNT] [-t TTL] A.B.C.D
39.  ping6 [-c COUNT] [-t TTL] ADDR
40.  prov get tftp svr addr
41.  prov set tftp svr type=(ipv4|ipv6|dns) addr=ADDR
42.  ps [OPTION]
43.  pwd
44.  quit
45.  reboot
46.  refresh provision configure filename
47.  remove acl condition all
48.  remove acl condition index=<1-255>
49.  remove acl rule all
50.  remove acl rule index=<1-255>
51.  remove fwddb all
52.  remove fwddb mac=MAC fdbid=<0-255>
53.  remove ip6tables acl condition all
54.  remove ip6tables acl condition index=<1-255>
55.  remove ip6tables acl rule all
56.  remove ip6tables acl rule index=<1-255>
57.  remove snmp community name=STR_COMM_NAME
58.  remove snmp group name=STR_SNMP_GRP [security-model=(v1|v2c|v3) security-level=(noAuthNoPriv|authNoPriv|authPriv)]
59.  remove snmp local user name=STR_USER_NAME
60.  remove snmp remote engine addrtype=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535>
61.  remove snmp remote user name=STR_USER_NAME addrtype=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535>
62.  remove snmp remote user name=STR_USER_NAME engine=STR_ENGINE_ID
63.  remove snmp traphost type=(ipv4|ipv6) addr=STR_SVR_ADDR port=<1-65535>
64.  remove snmp view name=STR_SNMP_VIEW [oid=STR_VIEW_OID]
65.  remove soam config all
66.  remove soam ma local-ma-id=<1-4294967295>
67.  remove soam md local-md-id=<1-4294967295>
68.  remove soam meg local-meg-id=<1-4294967295>
69.  remove soam mep mep-id=<1-8191> local-parent-id=<1-4294967295>
70.  remove soam mip local-mip-id=<1-4294967295>
71.  remove ssh host-key=(dsa|rsa|both)
72.  remove ssh public-key user=USER type=(dsa|rsa|both)
73.  remove sysuser name=NAMESTR
74.  remove vlan all
75.  remove vlan-db vid=<2-4094>
76.  reset all ports counters
77.  reset factory
78.  reset uptime
79.  restart acl
80.  restart ip6tables acl
81.  restore module-list=STR_MODULE_LIST
82.  send soam mep dm mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPI
83.  D) period=(1s|10s) frame-num=<3-32>
84.  send soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(M
85.  AC|MEPID) use-fdb-only=(true|false) ttl=<0-255>
```

86. 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)]
87. send soam mep mcc mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID) oui=OUI data=DATA
88. send soam mep test mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID) pattern=(nullnocrc|nullcrc|prbs231nocrc|prbs231crc) size=<0-1467> frame-num=<1-32>
89. serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem) file=FILE
90. set (backup|restore) module-index=<1-255> config-file=STR_CFG_FILE
91. set acl condition=<1-255> rule_index=<1-255>
92. set acl rule=<1-255> traprate=<1-65535>
93. set acl state=(enable|disable)
94. set acl table=(raw|filter|nat|mangle) chain=(prerouting|input|forward|output|postrouting) policy=(accept|drop)
95. set ais format=(blue|allones)
96. set ais transmit=(enable|disable)
97. set bw alloc-type=(countAllLayer1|countAllLayer2|countAllLayer3)
98. set circuit-ID=CIRCUIT
99. set curr-time=STR_CURR_TIME
100. set dbg level=<0-2>
101. set device description=CIRCUIT
102. set dmi rx-power-preset-level=<0-65535>
103. set dns-svr svr=<1-6> type=(ipv4|ipv6) addr=ADDR
104. set dot1bridge aging-time=<0-3825>
105. set dot1dbridge ieee-tag-priority=<0-7> remap-priority=<0-3>
106. set dot1dbridge ip-priority-index=<0-63> remap-priority=<0-3>
107. set ether admin state=(up|down)
108. set ether adv-cap=STR_ETHER_ADV_CAPABILITY
109. set ether autocross=(mdi|mdi-x|auto)
110. set ether autoneg state=(enable|disable)
111. set ether dot3 pause=(disabled|enableTx|enableRx|enableTxRx)
112. set ether duplex=(full|half)
113. set ether fef=(enable|disable)
114. set ether filter-unknown-multicast=(enable|disable)
115. set ether filter-unknown-unicast=(enable|disable)
116. set ether loopback oper=(init|stop)
117. set ether loopback type=(noloopback|phylayer|maclayer|alternate|remote)
118. set ether pause=STR_ETHER_PAUSE
119. set ether phymode=(phySGMII|phy100BaseFX|phy1000BaseX)
120. set ether speed=(10M|100M|1000M)
121. set ether src-addr-lock action=(discard|discardandnotify|shutdown|all)
122. set ether src-addr-lock=(enable|disable)
123. set fwd portlist=PORT_LIST
124. set fwddb mac=MAC fdbid=INDEX conn-port=PORT
125. set fwddb mac=MAC fdbid=INDEX priority=<0-7>
126. set fwddb mac=MAC fdbid=INDEX type=(static|staticNRL|staticPA)
127. set gateway type=(ipv4|ipv6) addr=ADDR
128. set https certificate-file=FILE
129. set https certificate-type=(self-certificate|authorized)
130. set https port=<1-65535>
131. set https private-key file=FILE
132. set https private-key password
133. set https state=(enable|disable)
134. set ip address mode =(dhcp|bootp|static)

135. set ip type=(ipv4|ipv6) addr=ADDR (subnet-mask|prefix)=A
136. set ip6tables acl condition=<1-255> rule_index=<1-255>
137. set ip6tables acl rule=<1-255> traprate=<1-65535>
138. set ip6tables acl state=(enable|disable)
139. set ip6tables acl table=(raw|filter|nat|mangle) chain=(prerouting|input|forward|output|postrouting) policy=(accept|drop)
140. set ipv6 address mode =(static|dhcpv6|stateless)
141. set ipv6 gateway mode=(static|routerDisc)
142. set ipv6-mgmt state=(enable|disable)
143. set irate=(unLimited|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|rate90M|rate95M|rate100M|rate150M|rate200M|rate250M|rate300M|rate350M|rate400M|rate450M|rate500M|rate550M|rate600M|rate650M|rate700M|rate750M|rate800M|rate850M|rate900M|rate950M) erate=(unLimited|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|rate90M|rate95M|rate100M|rate150M|rate200M|rate250M|rate300M|rate350M|rate400M|rate450M|rate500M|rate550M|rate600M|rate650M|rate700M|rate750M|rate800M|rate850M|rate900M|rate950M)
144. set l2cp proto=(spanningTree|slow|portAuthentication|elmi|lldp|bridgeMgmt|garpmrpBlock|bridgeBlockOtherMulticast) process=(pass|discard)
145. set loam admin state=(enable|disable)
146. set loam critical-evt-notif=(enable|disable)
147. set loam dg-evt-notif=(enable|disable)
148. set loam ef threshold=<0-268435455>
149. set loam ef window=<10-600>
150. set loam ef-evt-notif=(enable|disable)
151. set loam efp threshold=<0-268435455>
152. set loam efp window=<1-104857560>
153. set loam efp-evt-notif=(enable|disable)
154. set loam efss threshold=<0-9000>
155. set loam efss window=<100-9000>
156. set loam efss-evt-notif=(enable|disable)
157. set loam esp threshold high=<0-268435455> low=<0-268435455>
158. set loam esp window high=<0-4294967295> low=<1-268435455>
159. set loam esp-evt-notif=(enable|disable)
160. set loam ignore-loopback-request=(enable|disable)
161. set loam mode=(passive|active)
162. set login method=(local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal)
163. set lpt monitor-port=PORT
164. set lpt state=(enable|disable|notSupported)
165. set mac_learning enable portlist=STR_MAC_LEARNING_PORT_LIST
166. set mgmt vlan port=PORTLIST
167. set mgmt vlan state=(enable|disable)
168. set mgmt vlan vid=<1-4094>
169. set port default-vid=<1-4094>
170. set port discard-tagged=(true|false)
171. set port discard-untagged=(true|false)
172. set port dot1-state=(check| fallback| secure| vlanDisabled| vlanEnabled)
173. set port egress queuingmethod =(wrr|sp)
174. set port force-default-vid=(true|false)
175. set port mgmtaccess=(enable|disable)
176. set port vlan tag mode=(network|provider|customer)
177. set port vlan tag network tagging=(unmodified|removeTag|addTag)
178. set port vlan tag provider ethtype=(x8100|x9100|x88a8)
179. set power relay state=(enable|disable)

```
180. set qos default-priority=<0-7>
181. set qos ingress-priority=<0-7> remap-priority=<0-7>
182. set qos priority by-dst-mac=(enable|disable)
183. set qos priority by-src-mac=(enable|disable)
184. set qos priority by-vlan-id=(enable|disable)
185. set qos priority ieee-tag=(enable|disable)
186. set qos priority ip-tag=(enable|disable)
187. set qos priority tag-type=(useIEEE|useIP)
188. set radius client state=(enable|disable)
189. set radius svr=<1-6> retry=<1-5>
190. set radius svr=<1-6> secret=SECRET
191. set radius svr=<1-6> timeout=<1-60>
192. set radius svr=<1-6> type=(ipv4 |dns|ipv6) addr=ADDR [retry=<1-5>] [timeout=<1-60>]
193. set redundancy state=(enable|disable)
194. set rfd state=(enable|disable|notSupported)
195. set selective lpt state=(enable|disable)
196. set sensor stid=SENSORID notif=(enable|disable)
197. set sensor stid=SENSORID relation=(lessThan|lessOrEqual|greaterThan|greaterOrEqual|equalTo|notEqualTo)
198. set sensor stid=SENSORID severity=(other|minor|major|critical)
199. set sensor stid=SENSORID value=VALUE
200. set slot=SLOT power=(on|off|reset)
201. set snmp local engine=STR_LOCAL_ENGINE
202. set snmp local user name=STR_USER_NAME group=STR_GRP_NAME
203. set snmp view name=STR_SNMP_VIEW oid=STR_VIEW_OID type=(include|exclude)
204. set sntp dst-end=TIME
205. set sntp dst-offset=OFFSET
206. set sntp dst-start=TIME
207. set sntp dst-state=(enable|disable)
208. set sntp state=(enable|disable)
209. set sntp timezone=<1-63>
210. set sntp-svr svr=<1-6> type=(ipv4|dns|ipv6) addr=ADDR
211. set soam ma local-ma-id=<1-4294967295> attr_name=(permission|ccminterval|mepid-add|mepid-remove|vlan-add|vlan-remove|primary-vlan|autodetection-timeout|autodetectrmep)
     attr_value=(none|chassis|mgmtaddr|chassismgmtaddr|defer|cci1s|cci10s|cci1min|cci10min|enable|disable|...)
212. set soam md local-md-id=<1-4294967295> permission-id=(none|chassis|mgmtaddr|chassismgmtaddr)
213. set soam meg local-meg-id=<1-4294967295> attr_name=(permission|ccminterval|mepid-add|mepid-remove|vlan-add|vlan-remove|primary-vlan|autodetection-timeout|autodetectrmep|y.1731-
     802.1ag-interop) attr_value=(none|chassis|mgmtaddr|chassismgmtaddr|cci1s|cci10s|cci1min|cci10min|enable|disable|...)
214. set soam mep config mep-id=<1-8191> local-parent-id=<1-4294967295> attr_name=(admin|cci|primaryvid|ccmltmpriority|faultalarmdetect|faultalarmreset|lowestprilevel|aisclient-add|aisclient-
     remove|aistransmit|aisinterval|aisnotifyup|aisprocess|aisframepriority) attr_value=(enable|disable|alldef|macremerrxcon|remerrxconn|errxconn|xconn|noxcon|...)
215. set soam mep lmperiodic mep-id=<1-8191> local-parent-id=<1-4294967295> state=(enable|disable|clearcounters)
216. set soam mip local-mip-id=<1-4294967295> attr_name=(admin|aistransmit|aisinterval|aisframepriority) attr_value=(enable|disable|1s|1min|...)
217. set ssh auth-retry=<1-5>
218. set ssh client timeout=<1-120>
219. set ssh public-key user=USER type=(dsa|rsa) file=FILENAME
220. set ssh server state=(enable|disable)
221. set switch mode=(local|remote)
222. set syslog level=(emerg|alert|crit|err|warning|notice|info|debug)
223. set syslog mode=(local|remote|localAndRemote|off)
224. set syslog svr port=<1-65535>
225. set syslog svr type=(ipv4|ipv6|dns) addr=SYSLOG_SVR_ADDR
226. set system contact=CONTACT
```

227. set system location=LOC
228. set system name=NAME
229. set sysuser name=NAMESTR level=(admin|read-write|read-only)
230. set sysuser name=NAMESTR pass=PASSSTR confirmpass=PASSSTR)
231. set tacplus client state=(enable|disable)
232. set tacplus svr=<1-6> retry=<1-5>
233. set tacplus svr=<1-6> secret=SECRET
234. set tacplus svr=<1-6> timeout=<1-60>
235. set tacplus svr=<1-6> type=(ipv4 |ipv6|dns) addr=ADDR [retry=<1-5>] [timeout=<1-60>]
236. set taos transmit=(enable|disable)
237. set tdm inband start pattern=PATTERN
238. set tdm inband stop pattern=PATTERN
239. set tdm inband timeout=(enable|disable)
240. set tdm inband=(enable|disable)
241. set tdm loopback oper=(init|stop)
242. set tdm loopback type=(noloopback|phylayer|maclayer)
243. set tdm peer inband start pattern=PATTERN
244. set tdm peer inband stop pattern=PATTERN
245. set tdm peer inband=(enable|disable)
246. set tndp tx state=(enable|disable)
247. set transparent lpt state=(enable|disable)
248. set usb-port state=(enable|disable)
249. set vlan-db vid=<1-4094> fid=FID pri-override=(enable|disable)
250. set vlan-db vid=<1-4094> fid=FID priority=PRIO
251. set vlan-db vid=<1-4094> port=<1-10> memetag=(noMod|unTag|tag|notMember)
252. show acl chain
253. show acl condition
254. show acl rule
255. show acl state
256. show bandwidth allocation
257. show cable length
258. show card info
259. show cardtype
260. show circuit-ID
261. show device description
262. show dmi info
263. show dot1bridge aging-time
264. show dot1dbridge ieee-tag priority remapping
265. show dot1dbridge ip-tc priority remapping
266. show ether config
267. show ether loopback capability
268. show ether loopback state
269. show ether security config
270. show ether statistics
271. show ether tdr config
272. show ether tdr test result
273. show firmware upgrade result
274. show firmware-db update result
275. show fwd portlist
276. show fwddb config fdbid=<0-255>

277. show https config
278. show ip-mgmt config
279. show ip6tables acl chain
280. show ip6tables acl condition
281. show ip6tables acl rule
282. show ip6tables acl state
283. show l2cp config
284. show loam config
285. show loam event config
286. show loam event log
287. show loam ignore-loopback-request
288. show loam peer info
289. show loam statistics
290. show lpt config
291. show mgmt vlan config
292. show port mac_learning state
293. show port vlan config
294. show port vlan tag config
295. show power config
296. show provision (backup|restore) modules
297. show qos config
298. show qos priority remapping
299. show radius config
300. show redundancy info
301. show rmon statistics
302. show slot info
303. show snmp community
304. show snmp group [name=STR_SNMP_GRP]
305. show snmp local engine
306. show snmp local user
307. show snmp remote engine
308. show snmp remote user
309. show snmp traphost
310. show snmp view [name=STR_SNMP_VIEW]
311. show sntp config
312. show soam conferror vid=<1-4095> port=<1-2>
313. show soam ma [local-ma-id=<1-4294967295>]
314. show soam md [local-md-id=<1-4294967295>]
315. show soam meg [local-meg-id=<1-4294967295>]
316. show soam mep cc mep-id=<1-8191> local-parent-id=<1-4294967295>
317. show soam mep config [mep-id=<1-8191> local-parent-id=<1-4294967295>]
318. show soam mep dm status mep-id=<1-8191> local-parent-id=<1-4294967295>
319. show soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> tid=<0-4294967295>
320. show soam mep lmperiodic [mep-id=<1-8191> local-parent-id=<1-4294967295> far-end-mep-id=<1-8191>]
321. show soam mep loopback mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(unicast|multicast)
322. show soam mep stats [mep-id=<1-8191> local-parent-id=<1-4294967295>]
323. show soam mep test mep-id=<1-8191> local-parent-id=<1-4294967295>
324. show soam mip config [local-mip-id=<1-4294967295>]
325. show soam mip stats [local-mip-id=<1-4294967295>]
326. show soam port

```
327.  show soam portid
328.  show soam senderid
329.  show ssh config
330.  show ssh host-key
331.  show ssh public-key user=USER
332.  show switch mode
333.  show syslog config
334.  show system information
335.  show sysuser
336.  show tacplus config
337.  show tdm config
338.  show tdm inband config
339.  show tdm loopback capability
340.  show tdm loopback state
341.  show tdm peer inband config
342.  show tdm port config
343.  show timezone
344.  show tndp tx state
345.  show upgrade firmware file
346.  show usb-port state
347.  show vlan-db config
348.  start ether tdr test
349.  start https certificate
350.  stat
351.  tftp get iptype=(ipv4|ipv6|dns) ipaddr=ADDR remotefile=RFILE [localfile=LFILE]
352.  tftp put iptype=(ipv4|ipv6|dns) ipaddr=ADDR localfile=LFILE [remotefile=RFILE]
353.  tftp upgrade iptype=(ipv4|ipv6|dns) ipaddr=ADDR remotefile=RFILE
354.  update firmware-db file=FILENAME
355.  upgrade module
Agent III C1|S7|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 the functions configurable via the Web interface versus CLI 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
Reset Uptime	reset system uptime
System Reboot	reboot
Reset to Factory Config	reset factory
All counters Reset	reset all ports counters
Device Description	set circuit id
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
Enable/disable SNMP access	set snmp status
SNMP version	set snmp version
Trap manager	set snmp trap host
none	set snmp read community set snmp write community
Server Address (Syslog)	set syslog svr type xxxx addr y.y.y.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

Web Field	CLI Command
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 savings 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	set sntp server address

HTTPS tab	HTTPS operations
HTTPS Status	set https state
HTTPS port	set https port number
TFTP Server Address	prov set tftp svr type=x addr=y
Certificate file name	set https certificate file
Certificate Type	set https certificate type
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 chain default policy (chain= parameter)
Chain policy	set acl chain default policy (policy= parameter)
Rules: Priority	set acl
Rules: Policy	set acl
Rules: Traprate	set acl
Rules: Add	add acl
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

LOAM Tab	LOAM operations
Admin Status	set usb-port state
LOAM Mode	set loam mode
Loopback Type	set ether loopback type
Ignore Loopback Request	Ignore loopback request
LOAM Peer Information field	get loam peer information
LOAM Peer Vendor OUI field	get loam peer vendor oui

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

x222x/x32xx Port Level Fields / Commands

MAIN tab

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 ethernet port l2cp configuration show ethernet port l2cp configuration
Reset Counters	clear ether all counters
TN Topology Discovery Protocol TX	set tndp tx state=x

ADVANCED tab

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

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 (IONMM)	**Backup - Restore operations**
TFTP Server Address	tftp put iptype=x ipaddr=y localfile=z tftp get iptype=x ipaddr=y remotefile=z
Backup	set backup
Backup: Download button	tftp put
Restore	restore
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

The following messages may display during CLI operations.

Add ACL rule failed.

This message indicates that the rule could not be added.

1. Verify the CLI command syntax.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. See Appendix A.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. Retry the operation. For a complete list of the available commands, see Appendix A.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)**

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)

2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
   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)

2. Retry the operation.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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)**
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Command incomplete

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

1. Verify the command syntax.
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33473.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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)**
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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)**
2. Retry the operation.
3. For a complete list of the available commands, see Appendix A.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to get MAC address!

This message indicates that communications to the module can not be established.

1. Verify that the correct hierarchy has been specified in the command (see “Managing Slide-In and Remote Modules Using CLI Commands” on page 49).
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds, then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Incomplete location command!

This message indicates that one or more parameters for the **go** command are missing. The go command was entered to set location parameters, but the module, slot and/or port value(s) were no included in the command string.

The go command can operate on a local or remote card/port, and you must give the last parameter to specify the target is a port or device. For example, the input go c=1 s=14 does not include the port parameter, so the CLI module displays “Incomplete location parameters”.

1. Verify the command syntax.
2. Re-enter the **go** command and be sure to include all of the location parameters:

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

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid location parameters, cannot find the physical entity!

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

1. Verify that the correct hierarchy has been specified in the command (see "Managing Slide-In and Remote Modules Using CLI Commands" on page 49).
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 Transition Networks NIDs and SFPs, the model number has a “-D” at the end.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 (PC).
   a) On the desktop, right-click on **My Computer**.
   b) Select **Manage**.
   c) Click **Device Manager**.
   d) In the right panel, expand the list for **COM & LPT**.
3. Is the COM port in the list?

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

4. In the HyperTerminal window, select **File>Properties**.

5. Check that the correct port is listed in the **Connect using** field.

6. Restart the management station.

7. Reboot the IONMM.

8. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error, you should first give full location parameters

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

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

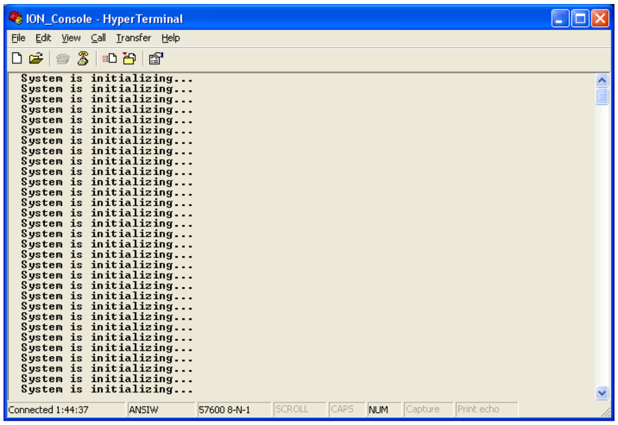
If the value of module, slot and port are not set in later commands, and then you run a device-level command (e.g., **show lpt config**), this error message displays.

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

```
go [c=CHASSIS] [s=SLOT] [l1ap=L0APORT] [l2ap=L1APORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
```

System is initializing...

CLI is receiving continuous error message "*system is initializing...*"



```
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
System is initializing...
```

1. Wait for a few minutes for the message to clear.
2. Cycle power to the IONMM.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

This command is only available on <x323x> card!

The command you entered is not supported on the card from which it was entered (e.g., you entered **set soam ma**, **set soam meg**, or **set soam mep** from a x222x or x32xx card, which does not support SOAM).

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., functions / commands are supported by NID models x222x / x32xx NIDs).
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error: this command should be executed on a port!

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

Unknown command!

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

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see Appendix A.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error location parameter number!
Error: parameter out of range, chassis-id range is (0 .. 15)!)
Error: parameter out of range, slot-id range is (1 .. 32)
Error: parameter out of range, slot-id range is (0 .. 32)
Incomplete location command!

The go command you entered had an invalid or missing parameter.

1. Enter the go command with all of the location parameters (chassis / slot / port) in the format:

go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
for a slide in card, or
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
for a standalone card.

Fail to set link pass through state!
You tried to set the LPT state to an unacceptable state. For example, you typed:

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

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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" on page 76.
2. Retry the operation with a valid MAC address.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid erate!
Invalid irate!

You tried to set the Ingress or Egress rate to an unacceptable limit. For example, you typed:

C1|S3|L1D> **C1|S7|L1D>set irate=100m erate=100m**

and then pressed **Enter**.

1. Verify the CLI command syntax.
2. Retry the operation. See the "Set Bandwidth Rate Limit**"** command on page 53.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 *x32xx.bin.0.5.4* is at *C:\TFTP-Root*).
5. Retry the operation. See the **tftp upgrade** command.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to transfer the file!
tftp get: set address type failed.
tftp put failed.

The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., **tftp get** or **tftp put** or **tftp transfer**). For example:

```
C1|S4|L1D>tftp get iptype ipv4 ipaddr 192.168.1.30 remotefile xxxx
tftp get: set address type failed.
C1|S4|L1D>tftp put iptype ipv4 ipaddr 192.168.1.30 localfile xxxx
tftp put failed.
C1|S4|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remotefile xxxx
tftp get: set address type failed.
```

1. Check the command syntax. See “TFTP Commands” page on page 157.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred, its location, and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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” on page 190.
2. Retry the operation. See the **dot1bridge aging-time** command.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set aging time!

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

1. Verify the **dot1bridge aging-time** command syntax. See "Configure Forwarding Learning Aging Time" on page 191.
2. Retry the operation. See the **dot1bridge aging-time** command.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Get aging time failed!

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

1. Verify the **dot1bridge aging-time** command syntax. See "Configure Forwarding Learning Aging Time" on page 191.
2. Retry the operation. See the **dot1bridge aging-time** command
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 (must have at least 2 fiber ports) .
2. Retry the operation on a card that supports this function. See the "Fiber Redundancy Commands" section on page 104.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid user!

You entered the command **show ssh public-key user admin**, but specified the wrong user (e.g., you typed **admin** instead of **root**).

1. Retry the operation using the correct user information. See "Show SSH Public Key of a User" on page 156.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set SSH server state!

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

1. Use the **get** command to obtain the key file. See the "TFTP Commands" on page 157.
2. Use the **set ssh public–key user** command to set the public key to a user from a key file.
3. Try the **set ssh server state=enable** command again. See "SSH Commands" commands on page 152.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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

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

1. Verify the VLAN Management configuration using the **show vlan** command and the **show vlan service** command.
2. Review the set mgmt vlan command syntax for the port / state / vid. See the "VLAN Commands" on page 119.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Upgrade is only supported on IONMM card!

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

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

1. Make sure of the command you want to enter. See "Firmware Upgrade Commands" on page 137.
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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot set bandwidth alloc type on this card!

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

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

1. Verify if the card supports bandwidth allocation.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands" on page 53.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 unLimit erate noLimit
Cannot set ingress and egress rate on this card!
```

1. Verify if the card supports rate limiting.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See "Bandwidth Commands" on page 43.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

DMI is only supported on FIBER port!

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

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

1. Verify if the card supports DMI.
2. Use the **go** command to switch to a different card port supporting Fiber.
3. Verify the command entry. See "DMI Commands" on page 55.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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" on page 58.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot clear loopback counters on this card!

Cannot set administrate state on this port!

Cannot set advertisement capability on this port!

Cannot set autocross on this card!

Cannot set auto negotiation state on this port!

Cannot set Ethernet port speed for this card!

Cannot set Ether port duplex mode on this card!

Cannot set far end fault on this card!

Cannot set filter unknown dest multicast frames on this port!

Cannot set filter unknown dest unicast frames on this port!

Cannot set pause on this port!

Cannot set source address lock action on this port!

No Time-domain reflectometer support on this card!

Cannot get port security configuration on this port!

Fail to get MAC control frames statistics!

Cannot show forwarding port list on this card!

Cannot show slot info on this card!

Cannot show USB port state on this card!

Cannot show 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

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

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

1. Verify if the card supports the desired function. See Table 3 in the section "Ethernet Port Commands" on page 64.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. The command functions include 1) admin, 2) adv-cap, 3) autocross, 4) autoneg, 5) duplex, 6) fef, 7) filter-unknown-multicast, 8) filter-unknown-unicast, 9) loopback, 10) pause, 11) speed, and 12) src-addr-lock, 13) tdr, 14) ether security config, 15) fwddb, etc.

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

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

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

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

1. Verify if the card supports the desired function.
2. Use the **go** command to switch to a different card port supporting loopback.
3. Verify the command entry. See "QoS Commands" on page 98.

Cannot get VLAN database configuration on this card!

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

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

1. Verify if the card supports the desired function.
2. Use the **go** command to switch to a different card port supporting VLAN.
3. Verify the command entry. See "VLAN Commands" on page 160.

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/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

The specified ACL rule index does not exist!

You tried to set an ACL Rule ID and traprate, but did not first create the associated rule.
For example:

```
C1|S16|L1D>set acl rule 1 traprate 4444
The specified ACL rule index does not exist!
```

1. Make sure ACL operations are enabled; see the **set acl state** command on page 48.
2. Create an ACL rule. See "Add a New ACL Rule" on page 48.
3. Try entering the **set acl rule command** again.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot show system information on this card!

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

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

1. Use the **go** command to switch to a different device (e.g., from the Power Supply to the IONMM or an x222x/32xx card).
2. Try entering the **show system information g** command again.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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” on page 64.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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” on page 64.
3. Try the **set dot1dbridge** command again.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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” on page 64.
3. Try the **set dot1dbridge** command again.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 true
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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid forward port list!

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

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

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

Invalid forward port list!
```

1. Re-enter the command, wait for the prompt, and then enter a response in the correct syntax.
2. See the related command / function section of this manual.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

L2CP is not supported on this card!

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

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports L2CP.
3. Try entering the command again. See "Configuring L2CP" on page 268.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Please give parameters for L2CP configuration:%s

You tried to perform an L2CP function but have not defined the L2CP parameter(s).

1. Verify the L2CP command parameters. See "Configuring L2CP" on page 268.
2. Try entering the command again.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot show circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.

1. Make sure this is the command / function that you wanted.
2. Use the **go** command to switch to a device that supports Circuit ID display.
3. Try entering the command again. See "Circuit ID" on page 268.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot set circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.

1. Verify the Circuit ID parameters. See "Circuit ID" on page 268.
2. Try entering the command again.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot set circuit-ID on this card!
You tried to display the Circuit ID information, but the function is not supported.

4. Verify the Circuit ID parameters. See "Circuit ID" on page 268.
5. Try entering the command again.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 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|S5|L1P2>
```

1. Make sure the Link OAM admin state of remote peer port is enabled (see "**set loam admin state**" command).
2. Verify the command syntax.
3. Use the **set ether loopback ?** command to display the card's loopback capabilities. For example:

```
C1:S7:L1P1>set ether loopback type ?
 alternate
 noloopback
 remote
```

4. Re-enter the **set ether loopback=** command with a loopback capability supported by the card (alternate, or remote or noloopback).

5. Verify the loopback capability with the **show ether loopback capability** command. For example:

```
C1|S5|L1P2> set ether loopback=
C1|S5|L1P2>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P2>
```

6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Can not set speed on this port!

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

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

1. Verify the NID supports this speed.
2. Verify the command syntax.
3. Re-enter the **set ether speed=** command with a speed supported by the card.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set port advertisement capability!

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

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

1. Verify the NID supports this capability.
2. Verify the command syntax.
3. Retry the operation. For a complete list of the available commands, see “Appendix A: CLI Command Summary” on page 174.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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

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

1. Make sure of the port speed that you want.
2. Use the **set ether autoneg state** command and/or the set ether speed command as required.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error symbol period window low is out of range, its range is 125000000 - 268435455!
Error frame period window is out of range, its range is 174762 - 104857560!
Error frame period threshold is out of range, its range is 0 - 268435455!
Error frame window is out of range, its range is 10 - 600!
Error frame threshold is out of range, its range is 0 - 268435455!
Error frame seconds summary window is out of range, its range is 100 - 9000!
Error frame seconds summary threshold is out of range, its range is 0 - 268435455!

A parameter entered in the "Event Configuration" has exceeded the range limitation.

1. Enter a parameter within the valid range displayed.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

No data in VLAN forward database table now!

You entered the command to display FWDDB information, but the VLAN forward database table has no data to report. For example:

```
C1|S16|L1D>show fwddb config fdbid 1
No data in VLAN forward database table now!
```

1. Make sure this is the function that you want.
2. Use the Forwarding Database Commands on page 92 to create the VLAN FDB entry.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

set forward database connection port failed.
set forward database priority failed.
set forward database entry type failed.
Please input a number to specify the priority!
The range of priority is 0 .. 7!

You tried to create a new FWDDB entry but the effort failed. For example:

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

1. Make sure this is the function that you want.
2. Use the “Forwarding Database Commands” to create the VLAN FDB entry. See the *ION x32xx NID User Guide* for more information.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 x32xx NID User Guide* for more information.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Auto-negotiation is enabled, you can not set port duplex now!
You entered the command to assign a duplex mode, but the command is not functional if Auto-negotiation is currently enabled.

1. Either leave the Auto-negotiation setting and use the current duplex setting, or disable AutoNegotiation and set the Duplex mode as required.
2. See the "Set Ethernet Port Speed / Duplex Mode" section on page 105 for more information.
3. Use the **show ether config** command to display the current Auto-negotiation and Duplex settings.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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:

```
S3240>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.
S3240>
```

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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" on page 113.
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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. See "TAOS and AIS Commands" on page 194.
2. Either select another device that supports AIS, or enter another command that this device supports.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Disable transmitting the TN topology discovery protocol on this port would make the device not be discovered by the Management unit if the device is remotely managed through this port. Are you sure?
Error: this command should be executed on a port!
Fail to get TNDP Tx state!
Fail to set TNDP Tx state of this port!
TNDP is not supported on this card!

1. Warning message that the **set tndp=disable** command disables management of the device from the IONMM.
2. The **set tndp=disable** command is a port level command; use the go command to switch to a port and re-enter this command.
3. Verify that this card supports the TNDP disable function.
4. Check the syntax and re-enter the command. Refer to the "TNDP Commands" on page 197.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Pause capability advertised by local auto-negotiation entity
If no pause capability, setting nopause; otherwise, for copper port , use a combination of pause and apause, like pause+apause or pause or apause; for fiber port, use a combination of apause and spause, like apause+spause or spause or apause

You entered a command to set the Pause function that did not match the port or device's capability.

1. Verify that this is the command you want.
2. Either select another device that supports this rate command, or enter another command that this port supports.
3. Retry the operation. Refer to the "Pause Commands" on page 187.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

please use \"show timezone\" to see detailed value of each timezone

You entered a command to set or show the UTC time data.

1. Verify that this is the command you want.
2. Enter the show timezone command.
3. Refer to the "SNTP Commands" on page 197.

The value of current time should time should follow this format, \"YYYY MMDD HH:MM:SS\", such as \"1999 1211 13:22:34
Please reboot the card for the changes to take effect!

You entered a **set sntp** command to set the UTC time data, and a reboot is required to implement the change.

1. If this is the command you want, start the reboot process.
2. Continue the operation.
3. Refer to the "SNTP Commands" on page 197.

Redundancy is enabled, so cannot set the administration state of fiber ports!

You entered a command to set the USB port state (**set usb-port state**=disable|enable) but that command does not work when the Redundancy feature is enabled.

1. Use the **go** command to switch to a different port.
2. Use the ION Web interface to disable the USB port.
3. Disable the Redundancy feature and then re-enter the **set usb-port state** command.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot get port VLAN configuration on this card!

Cannot get VLAN tag management configuration on this port!

Cannot set discard tagged frame on this card!

You entered a VLAN command on a device or port that does not support this function.

1. Try another command on the x222x/x32xx.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 on page 418.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set port MAC learning!

You entered a CLI command to set the MAC Address Learning port(s) to enabled or disabled, but the entry failed.

1. Make sure this is the command / function that you want.
2. Verify the MAC Address Learning port setting(s).
3. Refer to the "Configuring MAC Address Learning" section on page 325 for more information.
4. Retry the operation.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid forward port list!

You entered a CLI command to set the MAC Address Learning port(s) to enabled or disabled, but the entry was not accepted. For example:

```
C1|S3|L1D>set mac_learning enable portlist 1,2,3
Invalid forward port list!
```

1. Make sure this is the command / function that you want.
2. Verify the port number(s) that you entered are valid for this particular x222x/x32xx device (i.e., you cannot enter the command in the example above (**set mac_learning enable portlist 1,2,3**) on a 2-port device such as the x3220.
3. Refer to the "Configuring MAC Address Learning" section on page 325 for more information.
4. Retry the operation.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 contac**t" 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 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.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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!
Buckup finished
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Fail to set card entity index!
Processing...
The MAX provision configure file name is 64!
The specified module does not exist!

You entered a "**backup**" or "**restore**" command to do a backup or restore function, but a problem was encountered or the process is not yet finished. You entered a "**prov**" command to do a backup or restore function, but a problem was encountered or the process is not yet finished.

1. Wait a few moments for the command to complete and the *Restore finished* or *Backup finished* message to display.
2. Retry the backup or restore operation with 10 or fewer devices listed.
3. Use the **go** command to switch to a device that supports this feature (IONMM or a standalone SIC).
4. Enter a config filename with less than 64 characters. See the "Configuring Backup / Restore" section on page 103.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Adding Local User failed
Cannot add an system user on this card!
Default ION user is forbidden to be deleted!
Deleting Local User failed
ERROR: Can not delete current logined user!
ERROR: Current user is not authorized to do this operation!
ERROR: The two passwords are not the same, please check!
Error: this command should be executed on IONMM or a standalone SIC!
ERROR: This user could not be deleted!
Fail to activate the user!
Fail to create a system user!
Fail to create user!
Fail to get system user level!
Fail to get system user name!
Fail to get system user password!
Fail to remove the system user!
Fail to set system user level!
Fail to set system user name!
Fail to set system user password!
Modifying Local User failed
Password is too long!
The confirm password is not identical with the password!
There is no such user!
The user name must begin with an alphanumeric char!
The user password must begin with an alphanumeric char!
This user already exists!
To modify default ION user's level is not allowed!
User name is too long!

You tried to add (create), modify, or delete an ION user, but the operation failed.

1. Verify that this is the operation you want.

2. Retry the operation; be sure to type the parameters as shown in the "Configuring System / Login Users" section on page 143.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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!

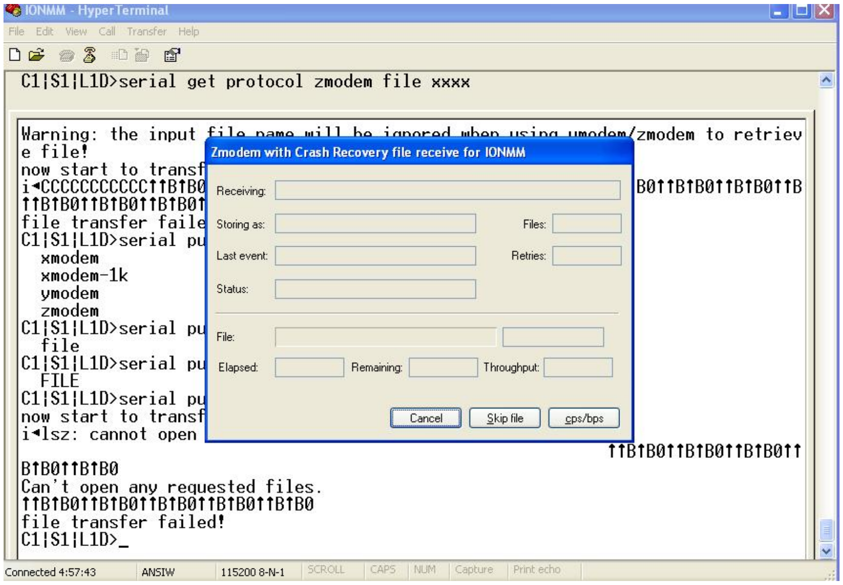
You entered a Serial File Transfer command, but the operation failed.

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 on page 143.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

File Transfer Failed - ZModem Crash Recovery dialog box:



```
C1¦S1¦L1D>serial get protocol zmodem file xxxx

Warning: the input file name will be ignored when using ymodem/zmodem to retriev
e file!
now start to transf
i◂CCCCCCCCCCCC↑↑B↑B0                                        B0↑↑B↑B0↑↑B↑B0↑↑B
↑↑B↑B0↑↑B↑B0↑↑B↑B0↑
file transfer faile
C1¦S1¦L1D>serial pu
  xmodem
  xmodem-1k
  ymodem
  zmodem
C1¦S1¦L1D>serial pu
  file
C1¦S1¦L1D>serial pu
  FILE
C1¦S1¦L1D>serial pu
now start to transf
i◂lsz: cannot open
                                                       ↑↑B↑B0↑↑B↑B0↑↑B↑B0↑↑
B↑B0↑↑B↑B0
Can't open any requested files.
↑↑B↑B0↑↑B↑B0↑↑B↑B0↑↑B↑B0↑↑B↑B0
file transfer failed!
C1¦S1¦L1D>_
```

You entered a Serial File Transfer command, but the operation failed.

1. Either enter the requested information and click **cps/bps**, or click **Skip file**, or click **Cancel**.

2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.

3. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section on page 143.

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:

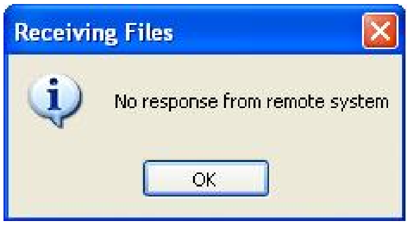
HyperTerminal Support

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



No response from remote system

You entered a Serial File Transfer command, but the ZModem file transfer failed.

1. Click the **OK** button to clear the message dialog box.

2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.

3. Retry the operation; be sure to type the parameters as shown in the "Transfer Files via Serial Protocol (X/Y/Zmodem)" section on page 143.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 on page 143.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot find software version of this card!

The ION card's firmware version must be newer than a specified version, otherwise this message is returned. You used the go command to switch to another card, but the system checked its version and decided that the new CLI can not be run on this card at this firmware version.

1. Check the card's current firmware version.
2. Upgrade the firmware. See "TFTP Transfer / Upgrade Commands" on page 204 or "Upgrade / Update Firmware Commands" on page 207. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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" on page 204 or "Upgrade / Update Firmware Commands" on page 207.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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" on page 204 or "Upgrade / Update Firmware Commands" on page 207.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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" on page 72 for more information.

ERROR: There is already a same named user!
ERRPR: User name can not be modified!

You tried to add or change a user's User Name via the Web or the CLI, but the action was rejected.

1. Verify the command syntax (e.g., "**add sysuser name**=NAMESTR).
2. Retry the operation, making sure the user name entry is unique.
3. Retry the operation, making sure you are not trying to change the user name of the default user.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 on page 103.

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 Transition Networks for more information. Contact Technical Support in the US/Canada at 1-800-260-1312, or International at 00-1-952-941-7600.

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 "&" can not be seen from web table list, CLI shows correctly.

Changeset 6591 / ref #2452 - special character display problem in web browser
From: 305 this.pattern = /^[1-9]+(\.\d{1,5})*$/;
To: 305 this.pattern = /^\d+(\.\d+)*$/;

Bandwidth Ingress fault

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).

1. Change the rate, duplex mode, frame size, packet size, or Ingress Rate Limit. See the related section of this manual for details.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

ERROR: Current user is not authorized to do this operation!
% There is no matched command.

You tried to enter a CLI command but the entry failed because of your login user privilege level.
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.

1. Try another command on the x222x/x32xx.
2. Check with the Admin if the command should be supported.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

SNMP Messages

For any error condition, you can check the TN Tech Support web site for possible solutions. For any problem that persists, contact TN Tech Support in the US or Canada at 1-800-260-1312, International at 00-1-952-941-7600; via fax at +1 952-941-2322; or via Email at techsupport@transition.com.

Basic Recovery Steps

You entered a command, but the operation failed or is still in process.
1. Wait for a few moments for the operation to complete.
2. Use the **Help** or **?** command to get assistance (help) on a group of commands or on a specific command.
3. Make sure this is the command you want and that the device/port/configuration supports this command.
4. Make sure this device/port supports the function attempted. Use the **go** command to switch locations.
5. Verify the command syntax and re-enter the command. See the related section of the manual for specifics.
6. Try using the Web interface to perform the function.
7. If the "continue **y**(es) **n**(o)" prompt displays, type **y** and press **Enter** to continue.
8. If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600; TN Tech Support web; fax: +1 952-941-2322; Email: techsupport@transition.com.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message:
Cannot create SNMP group on this card!
Cannot remove SNMP view on this card!
Cannot remove this group!
Cannot remove this view!
Cannot set filter type of a SNMP view on this card!
Cannot set SNMP local engine ID on this card!
Cannot set notify view of a SNMP group on this card!
Cannot set read view of a SNMP group on this card!
Cannot set write view of a SNMP group on this card!
Cannot show SNMP group on this card!
Cannot show SNMP local engine ID on this card!
Cannot show SNMP view on this card!
Fail to create SNMP group!
Fail to get SNMP group!
Fail to get SNMP local engine ID!
Fail to get SNMP local user!
Fail to get SNMP remote user!
Fail to get SNMP user!
Fail to remove SNMP group!
Fail to set SNMP local engine ID!
Fail to set SNMP notify view!
Fail to set SNMP read view!
Fail to set SNMP view status!
Fail to set SNMP write view!
Invalid OID for this view!
Local Engine ID length range is <5 - 32>!
No SNMP group created now!
No SNMP local user created now!
No SNMP user created now!
No such SNMP group name!
SNMP view name length should be shorter than 32!
The specified user does not exist!
Meaning: You entered an SNMP v3 command, but the command failed. For example, when the security model is v1 or v2c, the groups "public" and "private" can not be removed; but when the security model is v3 the groups "public" and "private" can be removed.
Recovery: 1) Make sure this is the command you want. 2) Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) Make sure the group, engine or user to be edited exists. 7) If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message:
Reseting local Engine ID will delete all exist local users, continue?(y: yes, n: no)
Meaning: You entered an SNMP v3 command, but a confirmation message displayed.
Recovery: 1) Make sure this is the command you want. Use the Help (**?**) command for details. 2) Enter **n** if you are not sure you want to reset the local Engine ID, or enter y to continue to reset the local Engine ID and delete all existing local users.

Message:
ERROR: Adding sub oid tree to defaultView is prohibited!
ERROR: defaultView can not be deleted!
ERROR: Modifying defaultView is prohibited!
ERROR: Please do not modify the View Name or the OID Sub Tree!
ERROR: Sub oid tree in defaultView can not be deleted!
ERROR: This group can not be deleted!
Meaning: You entered an SNMP v3 command, but the add/delete/modify command failed.
Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (**?**) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message:
When security level is v1 or v2c, security model can only be noAuthNoPriv
Fail to get community name! (*the device will search all rows of the SNMP Community Table, and if the community name can not be found, will add it*)
Fail to create community!
Meaning: You entered an SNMP Traphost or SNMP Trap Manager CLI command, but the command failed to complete.
Recovery: 1) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 2) Try using the ION Web interface to perform the function. 3) If required, at the command prompt, enter the ION login and Password information. 4) If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message:
ERROR Software version of this card ("cardVersion") is not supported, please upgrade to the same version as the IONMM
Getting card version failed
The failure get template config handler was called.
Meaning: You attempted a function that is not supported by this version of firmware.
Recovery: 1) Enter another (supported) function at this card's firmware version, or use the "go" command to switch to another card. 2) Upgrade to a newer firmware version. See "TFTP Transfer / Upgrade Commands" on page 204 or "Upgrade / Update Firmware Commands" on page 207. 3) Retry the operation. 4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Invalid input of timout value!*
Meaning: You set an unsupported SNMP trap timeout boundary value.
Recovery: 1) In the "**add snmp traphost**" command, specify a valid timeout (-15s%-16s%-5u%-30s%-16s%-12s%-12u%-12u%s (change from 8u to 12us). For example:

```
C1|S1|L1D>add snmp traphost version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6
security_level authPriv notify trap timeout=<0-2147483647>]
C1|S1|L1D>add snmp traphost version v3 type ipv4 addr 192.168.1.30 port 162 security_name TrpHstA6
security_level authPriv notify trap timeout 1000 retry 25
```

Problem: An SNMP user cannot access the IONMM.
Meaning: The User security level is not compatible with the Group level. For example, you added an SNMPv3 User to a SNMP v1 Group, or added a User to a non-existing Group, so this user can not access the IONMM.
Recovery: 1) Make sure the Group exists. Verify the User's security level. See the "Configure SNMP" section for specific details.

Problem: Can't assign a SNMPv3 User to multiple Groups.
Meaning: The SNMPv3 standards do not allow you to assign a SNMPv3 user to multiple groups.
Recovery: 1) Create an additional, unique user. 2) Assign the new user to a different group. 3) Make sure that each user belongs to just one group.

Problem: Can't configure SNMPv3 for chassis ION NIDs.
Meaning: The SNMPv3 features currently only apply to the IONMM and standalone S323x/S322x/S222x devices.
Recovery: 1) Contact U.S. Headquarters at 10900 Red Circle Drive, Minnetonka, MN 55343 USA; Telephone: 952-941-7600; Toll Free: 800-526-9267; Fax: 952-941-2322. EMEA Headquarters: Telephone: +49 611 974 8460; Fax: +49 611 950 4672. Email sales@transition.com.

Message: *Its value must be a-f or A-F or 0-9 and the total length must be a dual from 18 to 128*
Meaning: The engine ID is specified by hexadecimal characters. Each two input characters correspond to one octet character. For engine ID "80 00 03 64 03 00 c0 f2 00 01 02", the first two characters '80' correspond to the first octet character '\128' with ASCII value of 128 (8*16 + 0 = 128). The second two characters "00" correspond to the second octet character '\0' with ASCII value of 0 (0*16 + 0 = 0).
Recovery: 1) This applies only for SNMP v3 Engine ID converting. Enter this.pattern = /^[A-F\d]{18,128}$/.

Message: *It must be a valid oid.*
Meaning: You entered an invalid OID.
Recovery: 1) Enter this pattern = /^[1-9]+(\.\d{1,5})*$/.

Message: *It must be a string which consists of letters and numbers.*
Meaning: You entered an invalid string.
Recovery: 1) Enter this pattern = /^[\w]{1,256}$/;
2) Enter this min = lengthMin;
3) Enter this max = lengthMax;

Message: *It can be set to any characters combination except the character tab and space.*
Meaning: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "tab" and "space" characters. If you enter a "tab" and/or "space" character in these fields (via CLI or Web interface) the message "It can be set to any characters combination except the character tab and space." and "this.pattern is required: /^[\S]*{1,256}$/." display.
Recovery: 1) Re-enter the command or field without the "tab" or "space" characters.

Problem: Entries display in red in SNMP v3 fields (e.g., at **IONMM** > **SNMP** > **Users** sub-tab, the **User Name** / **Group Name** / **Password** entry displays in red)
Meaning: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "tab" and "space" characters. If you enter a "tab" and/or "space" character in these fields (via the Web interface) the characters display in red and the message "Getting records failed (http server error)" displays in the lower-left corner of the page.
Recovery: 1) Re-enter the command or field without the "tab" or "space" characters.

Message:
The default group whose name is \"public\" or \"private\" and security-model is v1 or v2c cannot be removed!
While the group whose name is \"public\" or \"private\" and security-model is v3 can be removed!
Meaning: The default group can not be removed (deleted) from the ION system configuration.
Recovery: 1) Make sure this is the command you want. 2) Delete another existing Group. 3) See the related section of the manual for specifics. 4) If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600; TN Tech Support web; fax: +1 952-941-2322; Email: techsupport@transition.com.

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 TN Tech Support.

Message: *AGENT PM ERROR: CLI command prov show snmp user failed*
Meaning: The IONMM backup failed after no group SNMP local user added to the system.
Recovery: 1) Check if the ION firmware is the latest and upgrade if possible. 2) Try the IONMM backup procedure again. 3) If the problem persists, contact TN 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" on page 27. Retry the operation.

Syslog Messages and Sys.log Output

This section documents Syslog messages and related Sys.log output.

Syslog Messages

The set of messages displayable while using the Syslog function are provided below with possible meanings and suggested recovery procedures.

agentx_mapset Error
agentx_ot_add Error

Meaning: possible internal error
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail for sending ionSyslogMgmtTable ,ignored...\n
Meaning: possible internal error.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to get syslog server address type!
Fail to get syslog server address type!
Fail to get syslog server port!
Fail to get syslog level!
Fail to get syslog level!
Fail to get syslog server address!
Meaning: the **show syslog config** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set syslog server port!
Fail to set syslog mode!
Fail to set syslog level!
Fail to set syslog server address!
Fail to set syslog server address type!
Meaning: the **set syslog level / mode / svr** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid syslog server address!
Meaning: the **set syslog svr** attempt failed (e.g., **set syslog svr type**=ipv4 addr=192.168.01).
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Number of subid is not correct when ionSyslogMgmtTable_get, expect %d, get %d \n
Meaning: possible internal error
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Please input a digital number to specify syslog server port!
Meaning: the **set syslog svr port** attempt failed.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation with a valid, unused UDP port number.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Session reset, Reregister from begging\n
STATUS_INVALID, should be session reset, Reregister from beginning\n
Meaning: possible internal error.
Recovery:

1. Verify the Syslog configuration. See "Configuring System Logging (Syslog)" on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Sys.log file lost on reboot
Meaning: 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.
Recovery:

1. Informational message.
2. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

System initializing or SNMP service busy, please wait..." : "Invalid password!
Meaning: possible internal error.
Recovery:

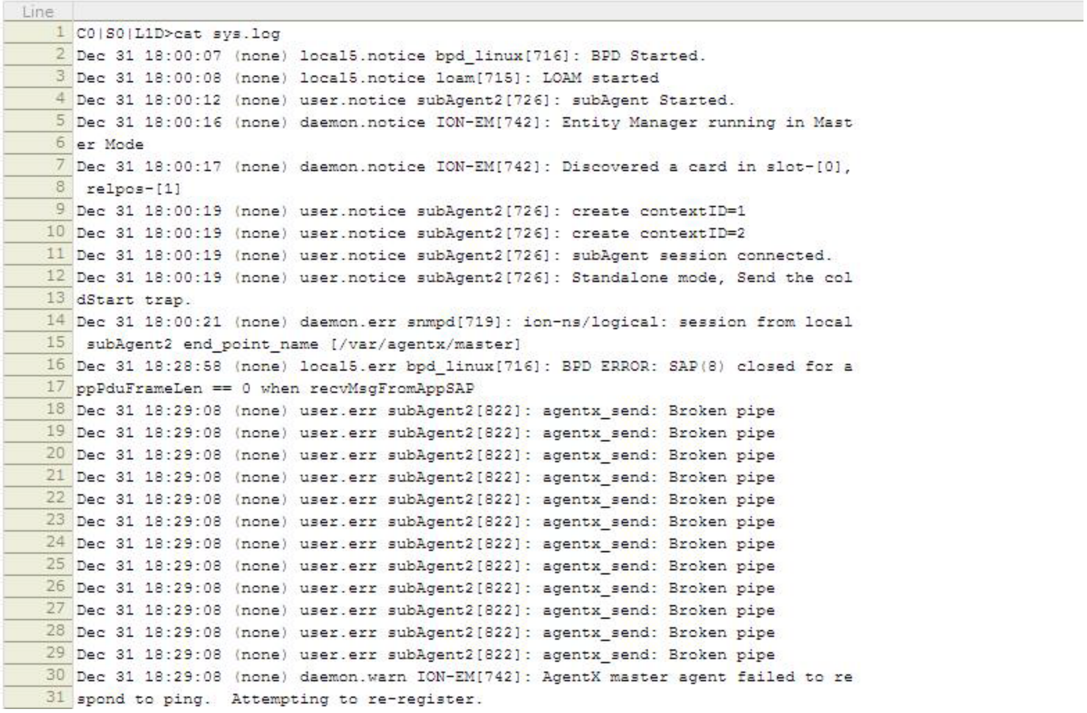
1. Wait for several seconds for the message to clear.
2. Verify the Syslog configuration. See “Configuring System Logging (Syslog)” on page 112.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

unknown column in ionSyslogMgmtTable_get\n
Meaning: possible internal error.
Recovery:

1. Verify the Syslog configuration. See “Configuring System Logging (Syslog)” on page 112.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Sample Sys.log Output

A typical Syslog output is shown below.



```
C0|S0|L1D>cat sys.log
Dec 31 18:00:07 (none) local5.notice bpd_linux[716]: BPD Started.
Dec 31 18:00:08 (none) local5.notice loam[715]: LOAM started
Dec 31 18:00:12 (none) user.notice subAgent2[726]: subAgent Started.
Dec 31 18:00:16 (none) daemon.notice ION-EM[742]: Entity Manager running in Mast
er Mode
Dec 31 18:00:17 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[0],
 relpos-[1]
Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=1
Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=2
Dec 31 18:00:19 (none) user.notice subAgent2[726]: subAgent session connected.
Dec 31 18:00:19 (none) user.notice subAgent2[726]: Standalone mode, Send the col
dStart trap.
Dec 31 18:00:21 (none) daemon.err snmpd[719]: ion-ns/logical: session from local
 subAgent2 end_point_name [/var/agentx/master]
Dec 31 18:28:58 (none) local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a
ppPduFrameLen == 0 when recvMsgFromAppSAP
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
Dec 31 18:29:08 (none) daemon.warn ION-EM[742]: AgentX master agent failed to re
spond to ping.  Attempting to re-register.
```

A typical syslog message is shown below:

```
Dec 31 18:28:58 (none) local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for
a
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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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 TN Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `61Dec 31 18:31:39 (none) user.crit subAgent2[822]: agentx_protocol_disconnect: Subagent disconnected from master.`

Meaning: Level 2 - Critical condition.

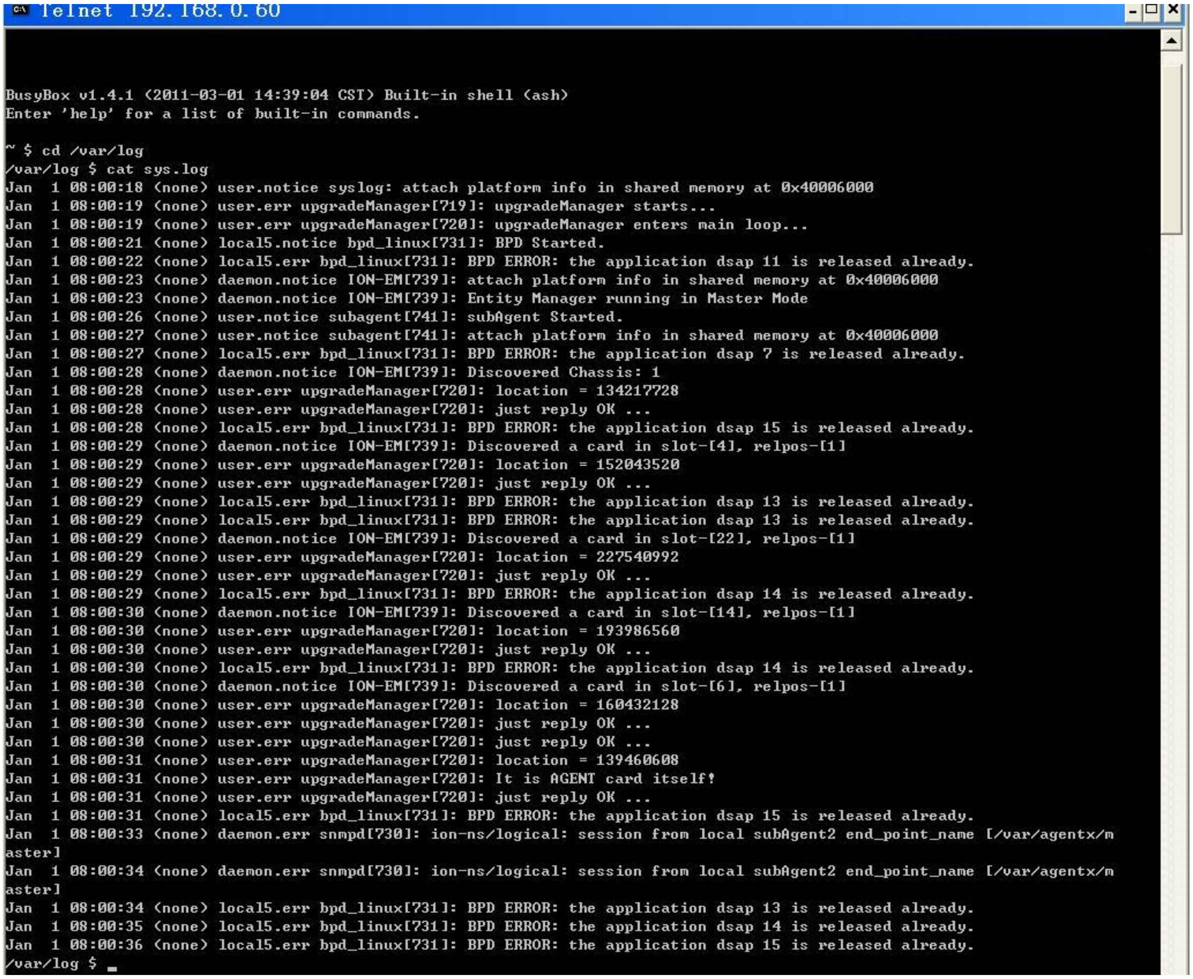
Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `user.err upgradeManager`

Meaning: you unplugged the SIC card; system will send a syslog described as "user.err upgradeManager” that does not match the event.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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



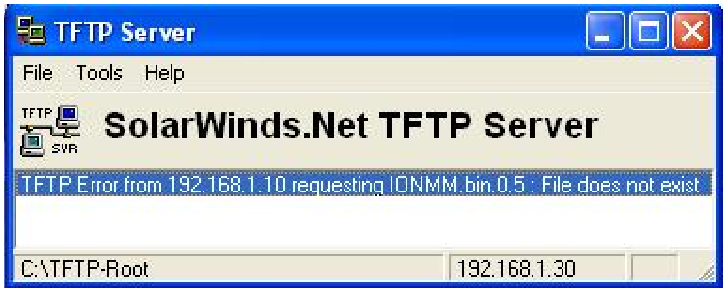
```
BusyBox v1.4.1 (2011-03-01 14:39:04 CST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ cd /var/log
/var/log $ cat sys.log
Jan  1 08:00:18 (none) user.notice syslog: attach platform info in shared memory at 0x40006000
Jan  1 08:00:19 (none) user.err upgradeManager[719]: upgradeManager starts...
Jan  1 08:00:19 (none) user.err upgradeManager[720]: upgradeManager enters main loop...
Jan  1 08:00:21 (none) local5.notice bpd_linux[731]: BPD Started.
Jan  1 08:00:22 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 11 is released already.
Jan  1 08:00:23 (none) daemon.notice ION-EM[739]: attach platform info in shared memory at 0x40006000
Jan  1 08:00:23 (none) daemon.notice ION-EM[739]: Entity Manager running in Master Mode
Jan  1 08:00:26 (none) user.notice subagent[741]: subAgent Started.
Jan  1 08:00:27 (none) user.notice subagent[741]: attach platform info in shared memory at 0x40006000
Jan  1 08:00:27 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 7 is released already.
Jan  1 08:00:28 (none) daemon.notice ION-EM[739]: Discovered Chassis: 1
Jan  1 08:00:28 (none) user.err upgradeManager[720]: location = 134217728
Jan  1 08:00:28 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:28 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 15 is released already.
Jan  1 08:00:29 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[4], relpos-[1]
Jan  1 08:00:29 (none) user.err upgradeManager[720]: location = 152043520
Jan  1 08:00:29 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:29 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 13 is released already.
Jan  1 08:00:29 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 13 is released already.
Jan  1 08:00:29 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[22], relpos-[1]
Jan  1 08:00:29 (none) user.err upgradeManager[720]: location = 227540992
Jan  1 08:00:29 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:29 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 14 is released already.
Jan  1 08:00:30 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[14], relpos-[1]
Jan  1 08:00:30 (none) user.err upgradeManager[720]: location = 193986560
Jan  1 08:00:30 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:30 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 14 is released already.
Jan  1 08:00:30 (none) daemon.notice ION-EM[739]: Discovered a card in slot-[6], relpos-[1]
Jan  1 08:00:30 (none) user.err upgradeManager[720]: location = 160432128
Jan  1 08:00:30 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:30 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:31 (none) user.err upgradeManager[720]: location = 139460608
Jan  1 08:00:31 (none) user.err upgradeManager[720]: It is AGENT card itself!
Jan  1 08:00:31 (none) user.err upgradeManager[720]: just reply OK ...
Jan  1 08:00:31 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 15 is released already.
Jan  1 08:00:33 (none) daemon.err snmpd[730]: ion-ns/logical: session from local subAgent2 end_point_name [/var/agentx/m
aster]
Jan  1 08:00:34 (none) daemon.err snmpd[730]: ion-ns/logical: session from local subAgent2 end_point_name [/var/agentx/m
aster]
Jan  1 08:00:34 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 13 is released already.
Jan  1 08:00:35 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 14 is released already.
Jan  1 08:00:36 (none) local5.err bpd_linux[731]: BPD ERROR: the application dsap 15 is released already.
/var/log $ _
```

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*

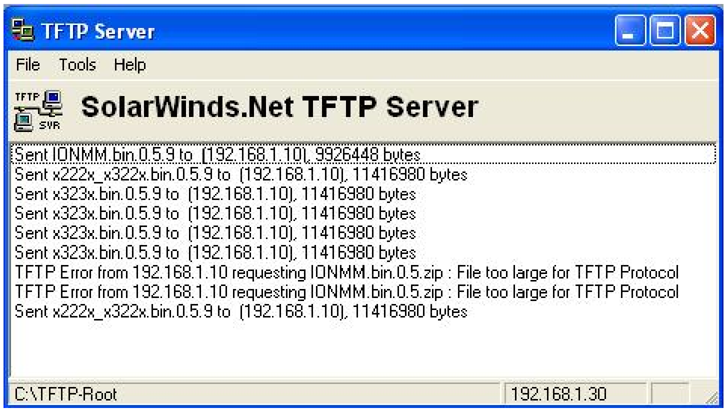


```
TFTP Error from 192.168.1.10 requesting IONMM.bin.0.5 : File does not exist
```

C:\TFTP-Root | 192.168.1.30

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*



```
Sent IONMM.bin.0.5.9 to  (192.168.1.10), 9926448 bytes
Sent x222x_x322x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
Sent x323x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
TFTP Error from 192.168.1.10 requesting IONMM.bin.0.5.zip : File too large for TFTP Protocol
TFTP Error from 192.168.1.10 requesting IONMM.bin.0.5.zip : File too large for TFTP Protocol
Sent x222x_x322x.bin.0.5.9 to  (192.168.1.10), 11416980 bytes
```

C:\TFTP-Root | 192.168.1.30

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

ION 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 **more** 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 **more** 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 Syslog 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'*. For the SSH user key, there is a root user and the user key stored in *'/root/.ssh'*.

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 **more** 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.

Glossary

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

100BASE-FX

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

1000BASE-X

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

802.1

The IEEE standard for port-based Network Access Control. IEEE 802.1 is a working group of the IEEE 802 project of the IEEE Standards Association. It’s concerns include 802 LAN/MAN architecture, internetworking among 802 LANs, MANs and other wide area networks, 802 Link Security, 802 overall network management, and those protocol layers above the MAC and LLC layers.

802.1ad

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

802.1ah

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

802.1p

The IEEE standard for QoS packet classification.

802.1p Prioritization

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

802.1q

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

802.1Q VLAN

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

AC

(Alternating Current) Electrical power that comes from wall outlets. Contrast with DC.

ACL

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

ANSI

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

API

(Application Program Interface) A set of routines, data structures, object classes and/or protocols provided by libraries and/or operating system services in order to support the building of applications.

ARP

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

Auto-Negotiation

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

Auto MDI / MDIX

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

Auto-provisioning

A process that enables centralized management for multiple end user devices. It uses DHCP option 60, 66 and 67 to provide centralized firmware and configuration management. The feature provides mass firmware upgrade capability as well as booting-up full end device configuration without any manual intervention.

BIA

(Burned-In Address) The last six bytes of a MAC address that are assigned by the manufacturer of a network interface card (NIC).

BPC

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

BPDU

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

Bridge

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

BT

(Bit Time) The time it takes for one bit to be ejected from a Network Interface Card (NIC) operating at some predefined standard speed, such as 10 Mbit/s. The time is measured between the time the logical link control layer 2 sublayer receives the instruction from the operating system until the bit actually leaves the NIC. The bit time has nothing to do with the time it takes for a bit to travel on the network medium, but has to do with the internals of the NIC.

CAT 1 – CAT 7 Cabling

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

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

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

CBN

(Common Bonding Network) The set of metallic components that are intentionally or incidentally interconnected to provide the principal means for effecting bonding and grounding inside a telecommunications building. These components include: structural steel or reinforcing rods, metallic plumbing, AC power conduit, cable racks, and bonding conductors. The CBN is connected to the exterior grounding electrode system.

CBS

(Committed Burst Size) a Bandwidth Profile parameter that limits the maximum number of bytes available for a burst of Service Frames sent at the UNI speed to remain CIR-conformant. It defines the average rate in bps of ingress Service Frames up to which the network delivers Service Frames and meets the performance objectives (as defined by the CoS Service Attribute). CIR/CBS determines frame delivery per service level objectives; CBS/EBS is measured in Bytes per second. Defined in MEF 6, 6.1, 7, 8, 10, 10.1, 11, 13, 14, 15, 19.

CE

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

CFM

(Connectivity-Fault Management) part of standard 802.1ag defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs) to managed objects to support transport fault management. These allow discovery and verification of the path, through bridges and LANs, taken for frames addressed to and from specified network users, detection, and isolation of a connectivity fault to a specific bridge or LAN.

CIR

(Committed Information Rate) a Bandwidth Profile parameter that defines the average rate in bps of ingress Service Frames up to which the network delivers Service Frames and meets the performance objectives defined by the CoS Service Attribute. A Bandwidth Profile property where a pre-determined level of Bandwidth Profile compliance for each Service Frame, if present, is ignored when determining the level of compliance for each Service Frame. CIR/CBS determines frame delivery per service level objectives; CIR/EIR is measured in bits per second. Defined in MEF 2, 7, 8, 10, 10.1, 11, 13, 14, 15, 19, 6, and 6.1.

Circuit ID

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

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

The x222x / x32xx NID 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.

CISPR

(Comité Internationale Spécial des Perturbations Radioelectrotechnique) An International Special Committee on Radio Interference.

CLI

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

Community

Two levels of ION system access privileges are password protected:

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

Community string

A text string used to authenticate messages between a management station and an SNMP v1/v2c engine. A string that is used as the name of the community; acts as a password by controlling access to the SNMP community.

CoS

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

CoS Queues

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

CPU

(Central Processing Unit) The portion of a computer system that carries out the instructions of a computer program, and is the primary element carrying out the computer's functions.

CRC

(Cyclic Redundancy Check) A technique for detecting errors in digital data, but not for making corrections when errors are detected. It is used primarily in data transmission. In the CRC method, a certain number of check bits, often called a checksum, are appended to the message being transmitted. The receiver can determine whether or not the check bits agree with the data, to ascertain with a certain degree of probability whether or not an error occurred in transmission. If an error occurred, the receiver sends a negative acknowledgement (NAK) back to the sender, requesting that the message be retransmitted.

CSA

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

C-Tag

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

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

dBm

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

DC

(Direct Current) Electrical power that comes from a battery. Contrast with AC.

DCE

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

DHCP

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

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

DiffDerv

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

Discovery

Discovery allows a Service OAM-capable device to learn sufficient information (e.g. MAC addresses etc.) regarding other SOAM capable NEs so that OAM frames can be exchanged with those discovered devices. With EVCs, discovery allows SOAM capable NEs to learn about other Service OAM capable devices that support the same EVCs. These devices are expected to be at the edges of the OAM domain in which the discovery is carried out. See "LLDP" and "TNDP" for discovery mechanisms. Discovery occurs when a SOAM-capable NID learns sufficient information (e.g. MAC addresses etc.) regarding other SOAM capable NIDs to exchange OAM frames with those discovered NIDs.

DMI

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

DMM / DMR

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

DNS

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

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

DNS server

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

Dr. Watson

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

DSCP

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

DST

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

DTE

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

Dynamic IP addressing

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

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

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

EBS

(Excess Burst Size) a bandwidth profile parameter; EIR/EBS determines amount of excess frame delivery allowed; CBS/EBS is measured in Bytes per second.

EEA

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

Egress Frame

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

Egress rules

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

EIR

(Excess Information Rate) a bandwidth profile parameter; EIR/EBS determines the amount of excess frame delivery allowed; EIR is measured in bits per second.

ELMI Protocols

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

ESD

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

EtherType

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

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

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

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

Event log

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

FCC

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

FDB

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

FDX

(Full Duplex) Communication in both directions simultaneously.

FEF

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

FID

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

Filtering Database

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

- *Static Entries*: Static information is added, modified, and deleted by management only. Entries are not automatically removed after some time (ageing), but must be explicitly removed by management.
- *Dynamic Entries*: Dynamic entries are "learned" by the bridge and cannot be created or updated by management. The learning process observes the port from which a frame with a given source addresses and VLAN ID (VID) is received, and updates the filtering database. The entry is updat-

ed only if a) this port allows learning, b) the source address is a workstation address and not a group address, and c) there is space available in the database.

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

Firmware

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

Flow Control

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

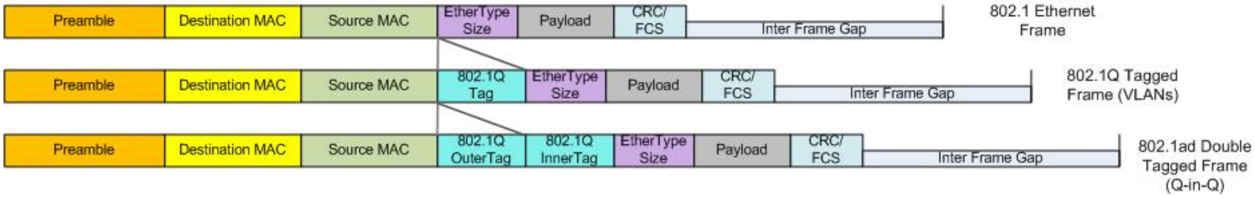
Frame

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

Frame Format

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

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



FTP

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

GBIC

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

Gbps

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

GUI

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

HSCP

(High-Security Console Password)

HTML

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

HTTPS

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

Hz

(Hertz) A unit of frequency that defines the number of complete cycles per second.

ICMP

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

IEC

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

IEEE

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

IETF

(Internet Engineering Task Force) an organized activity of the Internet Society (ISOC). ISOC is a non-profit organization founded in 1992 to provide leadership in Internet-related standards, education, and policy. It is dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world. The goal of the IETF is to make the Internet work better. The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The IETF's official products are documents, published free of charge as RFCs (Request for Comments). The IETF is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies.
It is the principal body engaged in the development of new Internet standard specifications.
See http://www.ietf.org/.

IGMP

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

IGMP snooping

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

Inform

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

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

Ingress

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

Ingress rules

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

IP

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

IPC

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

IP Stacking

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

IPToS

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

ITU

ITU is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services. For nearly

145 years, ITU has coordinated the shared global use of the radio spectrum, worked to improve telecommunication infrastructure in the developing world, and established worldwide standards that foster seamless interconnection of a vast range of communications systems. See http://www.itu.int/net/about/itu-t.aspx.

ITU-T LOAM Performance Monitoring

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

Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size, which is 1518 bytes (1522 if VLAN-tagged). Though this is not a standard, more vendors are adding support for jumbo frames. An initiative to increase the maximum size of the MAC Client Data field from 1500-bytes to 9000-bytes. The initiative was not adopted by the IEEE 802.3 Working Group, but it was endorsed by a number of other companies. Larger frames would provide a more efficient use of the network bandwidth while reducing the number of frames that have to be processed. The Jumbo Frame proposal restricts the use of Jumbo Frames to full-duplex Ethernet links, and defines a "link negotiation" protocol that allows a station to determine if the station on the other end of the segment is capable of supporting Jumbo Frames.

L2CP

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

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

The MEF and IEEE 802.1 terms are related as follows:

MEF Term	*IEEE 802.1 Term*
Peer	Participate
Tunnel	Forward (relay)
Discard	Not forward, Not participate

L2CP Service Frame

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

L2CP Service Frame Delivery

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

L2CP Tunneling

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

L2/L3/L4 Access Control List Port Based ACLs

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

LACP

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

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

LAN

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

Last Gasp

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

Layer 2 Switch

A network device that functions as multi-port switch.

Layer 3 Switch

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

Layer 4 Switch

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

Leaky bucket

An algorithm used in packet switched computer networks and telecommunications networks to verify that a data transmission conforms to a pre-defined limit on bandwidth and burstiness (variations in traffic flow). The leaky bucket algorithm is also used in leaky bucket counters (e.g., to detect when the average or peak rate of certain events or processes exceed pre-defined limits). The Leaky bucket algorithm is based on an analogy of a bucket with a hole in the bottom through which its contents will leak out at a constant rate, until / unless it becomes empty. Water can be added intermittently (i.e., in bursts) but if too much is added at once, or if added at too high an average rate, the water will exceed the capacity of the bucket, and it will overflow.

LED

(Light Emitting Diode) An electronic light source.

LLDP

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

LOAM

(Link OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.3ah OAM. The major features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, and Remote Loopback. The x222x/32xx NIDs support Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57).

LOAM Event

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

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

The first four are considered threshold crossing events, as they are generated when a metric exceeds a given value within a specified window. The other three are not threshold crossing events.

LPT

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

MAC

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

MAC-based Security

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

MAC Table Size

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

MAU

(Media Attachment Unit) In an Ethernet LAN, a device that interconnects the attachment unit interface port on an attached host computer to the Ethernet network medium (such as Unshielded Twisted Pair or coaxial cable). The MAU provides the services that correspond to the physical layer of the Open Systems Interconnection (OSI) reference model. A MAU can be built into the computer workstation or other device or it can be a separate device.

Mbps

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

MDI

(Medium Dependent Interface) A type of Ethernet port connection using twisted pair cabling. The MDI is the component of the media attachment unit (MAU) that provides the physical and electrical connection to the cabling medium. MDI ports connect to MDIX ports via straight-through twisted pair cabling; both MDI-to-MDI and MDIX-to-MDIX connections use crossover twisted pair cabling. See also MDIX.

The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX). The x222x/32xx device’s *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection.

MDIX

(MDI Crossover) A version of MDI that enables connection between like devices. The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX).
The x222x/32xx device’s *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection. See also MDI.

MIB

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

MIBs stems from the OSI/ISO Network management model and are a type of database used to manage the devices in a communications network. A MIB comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using a subset of Abstract Syntax Notation One (ASN.1) called "Structure of Management Information Version 2 (SMIv2)" RFC 2578. The database is hierarchical (tree-structured) and entries are addressed through object identifiers. IETF RFCs discuss MIBs, notably RFC 1155, "Structure and Identification of Management Information for TCP/IP based internets", RFC 1213, "Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, "A Simple Network Management Protocol".

MIB Module

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

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

MIB object identifier

See “OID”.

MIB variable

See “OID”.

MSA

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

MSDU

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

MT-RJ

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

Multicast

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

Multicast destination

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

MVRP

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

Native VLAN

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

NIC

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

NID

(Network Interface Device) A device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In telecommunications, a NID is a device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In fiber-to-the-premises systems, the signal is transmitted to the customer premises using fiber optic technologies.
In general terms, a NID may also be called a Network Interface Unit (NIU), Telephone Network Interface (TNI), Slide-in-card (SIC), or a slide-in-module.

NMS

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

Non Intrusive test

Ability to troubleshoot a circuit while it is in use.

Notification

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

Notification host

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

Notifview

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

NTP

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

OAM

(Operation, Administration and Maintenance) A group of network management functions that provide network fault indications, performance information, data, and diagnosis.

OAM Event

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

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

The first four are considered threshold crossing events, as they are generated when a metric exceeds a given value within a specified window. The other three are not threshold crossing events.

OAMPDU

(Ethernet OAM protocol data unit) The mechanism by which two directly connected Ethernet interfaces exchange OA information.

OID

(Object Identifier) Known as a “**MIB** object identifier” or “MIB variable” in the SNMP network management protocol, an OID is a number assigned to devices in a network for identification purposes.

Each branch of the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an Object ID or OID.

OSI

(Open Systems Interconnection) A standard description or reference model for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementors so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication.

OUI

(Organizationally Unique Identifier) the Ethernet Vendor Address component. Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits, which specify the interface serial number for that interface vendor. These high-order 3 octets (6 hex digits) are called the Organizationally Unique Identifier or OUI.

Pause

The Pause feature (data pacing) uses Pause frames for flow control on full duplex Ethernet connections. If a sending device is transmitting data faster than the receiving device can accept it, the receiving station will send a pause frame to halt the transmission of the sender for a specified period of time.

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

PD

(Powered Device) Modules that are designed to extract power from a conventional twisted pair Category 5 Ethernet cable. All PD modules are IEEE802.3af compatible, with built-in signature chip, output voltage adjustment and class programming.

PDU

(Protocol Data Units) **1.** Information that is delivered as a unit among peer entities of a network and that may contain control information, address information or data. **2.** In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol control information and possibly user data of that layer.

PID

(Priority ID) on the x222x/x32xx NID, the PID is configured at the ADVANCED tab in the “IEEE Priority Class” section; the selections are Remap 0 to: (PID) 0123.

PoE

(Power over Ethernet) A system to safely transfer electrical power, along with data, to remote devices over standard category 5 cable in an Ethernet network. It does not require modification of existing Ethernet cabling infrastructure.

Port-Based Rate Limiting

The ability to regulate throughput on a per-port basis. (AKA, metering, Rate Limiting.)

Port Labeling

The ability to assign names to ports through the management interface.

Protocol Endpoint

A communication point from which data may be sent or received. It represents communication points at various levels on an Open Systems Interconnection (OSI) structure.

Primary VID

The VID, among a list of VIDs associated with a service instance, on which all CFM PDUs generated by MPs except for forwarded LTMs are to be transmitted.

PSE

(Power Sourcing Equipment) In power over Ethernet (PoE), equipment that serves as power injectors to provide output of 48V DC power over the twisted-pair cable plant to terminal units with PoE compliant devices known as powered devices (PDs). For devices not PoE-compliant, splitters inserted into the Ethernet cabling provide 12V or 6V DC output.

PVID

(Port VID) A default VID that is assigned to an access port to designate the virtual LAN segment to which this port is connected. The PVID places the port into the set of ports that are connected under the designated VLAN ID. Also, if a trunk port has not been configured with any memberships, the virtual switch's PVID becomes the default VLAN ID for the ports connection.

PVLAN

(Private Virtual-LAN) a non-standardized way of segmenting ports into separate groups. (Contrast “802.1Q VLAN”.)

Q-in-Q (or “QinQ” or “Q in Q”)

(IEEE 802.1Q in 802.1Q) an Ethernet networking standard for Ethernet frame formats (actually, 802.1Q-in-Q is an amendment to IEEE 802.1Q, and not a separate specification). It is also known simply as "QinQ" or "Q in Q". The original 802.1Q specification allows a single VLAN header to be inserted into an Ethernet frame. Q-in-Q allows multiple VLAN headers to be inserted into a single frame. In the context of an Ethernet frame, a Q-in-Q frame has 2 VLAN 802.1Q headers (i.e., the Q-in-Q frame is ‘double-tagged’).

QoS

(Quality of Service) A mechanism to allow different classes of services to the customers.
The QoS varies on a per customer basis, depending on their Service Level Agreement (SLA) they chose, and the kind of service they want. Customer traffic priorities are assigned based on their SLAs. QoS is standardized at both layer 2 and layer 3.

Service providers offering Layer 2 services can use the IEEE 802.1 Q/p standard for QoS.
It allows a service provider to attach special tags, called VLAN IDs, to all incoming frames from a customer. With this, the service provider can have multiple customers using the same circuit, but still maintain separation between them. Each customer’s traffic is identified by a different VLAN tag. The method also allows for the addition of a priority value to be associated to the VLAN tag. By using the priority field, service providers can offer various classes of service.

The two current Layer 3 (IP) QoS standards are IETF RFC-791, which defines the ToS, and RFC-2475, which defines DSCP. Both standards use the same field in the IP packet header to identify the level of service for the packet.

The various QoS parameters (either for Layer 2 or 3) are stored as part of the overhead in the transmitted frames. See also CoS and ToS.

RADIUS

(Remote Authentication Dial In User Service) Is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service.

Redundancy

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

On the ION system, the Fiber Redundancy feature adds a form of automatic protection switching using a LOS mechanism that triggers the switch to the surviving line. The ION system uses 1:1 protection, with a modified form of bi-directional switching. TLPT and SLPT are operational with fiber redundancy enabled or disabled. The fault discovery method is LOS at the receiving interface for a set continuous period of time. Traffic rerouting occurs within a minimum period of time after the Primary Port is declared in the fault state. Traffic flow is restored within a minimum set period of time after a fault occurs.

RJ-45

The standard connector utilized on 4-pair (8-wire) UTP (Unshielded Twisted Pair) cable. The RJ-45 connector is the standard connector for Ethernet, T1, and modern digital telephone systems.

RMON

(Remote Network Monitoring) Software that supports the monitoring and protocol analysis of LAN.
A part of SNMP, RMON is a network management protocol that gathers remote network information.
(Standard: RFC 1271.)

RS-232

(Recommended Standard 232) A standard for serial binary data signals connecting between a **Error! Reference source not found.** (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

SAP

(Service Access Point) The point at which an Ethernet service is offered.

Sender ID

Defined in RFC 4406, Sender ID is a Microsoft protocol derived from SPF (hence the identical syntax), which validates one of a message's address header fields defined by RFC 2822. Which header field it validates is selected according to the PRA (Purported Responsible Address) algorithm per RFC 4407.
The PRA algorithm selects the header field with the e-mail address responsible for sending the message.
Sender ID can be compared to other RFC 2822 layer protocols like DomainKeys IM (DKIM).
The purpose of Sender ID is to help fight spoofing, one of the major deceptive practices used by spammers. Sender ID works by verifying that each e-mail message did indeed originate from the Internet domain from which it was sent. See http://www.ietf.org/rfc/rfc4406.txt and http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx for more information.

SFP

(Small Form-Factor Pluggable) A compact, hot-pluggable transceiver used in telecommunication and data communications applications. It interfaces a network device mother board (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. The SFP transceiver is specified by a multi-source agreement (MSA) between competing manufacturers. The SFP was designed after the GBIC interface, and allows greater port density (number of transceivers per inch along the edge of a mother board) than the GBIC, thus SFP is also known as “mini-GBIC”. Optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature lets you monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. AKA, Digital Optical Monitoring (DOM), DMI (Diagnostic Monitoring Interface), or DMM (Diagnostic Maintenance Monitoring).

SGMII

(Serial Gigabit Media Independent Interface) A standard Gigabit Ethernet interface used to connect an Ethernet MAC-block to a PHY. To carry frame data and link rate information between a 10/100/1000 PHY and an Ethernet MAC, SGMII uses a different pair for data signals and for clocking signals, with both being present in each direction (i.e., TX and RX). S3240 NIDs have SGMII support for use with 10/100/1000BASE-T copper SFPs. The S3240 uses the **set ether phymode=SGMII** CLI command to select SGMII mode.

SLA

(Service Level Agreement) In general terms, a part of a service contract where the level of service is formally defined in terms of a contracted delivery time or performance. In Metro Ethernet, the contract between the Subscriber and Service Provider specifying the agreed to service level commitments and related business agreements.

SLAs and CIR/EIR

For a sample SLA, Service Frames sent up to the "CIR" rate are allowed into the provider's network and delivered as defined in the service performance objectives (e.g., delay, loss, and availability) specified in the Service Level Agreement (SLA) or Service Level Specification (SLS). These Service Frames are referred to as `in-profile' or `conformant' to the bandwidth profile. Service Frames sent up to the "EIR" rate are allowed into the provider's network but are delivered without any service performance objectives. These Service Frames are referred to as `out-of-profile' or `non-conformant' to the bandwidth profile. Any Service Frames sent at rates above the EIR are discarded.

SMAC

(Static MAC) A MAC address that is manually entered in the address table and must be manually removed. It can be a unicast or multicast address. It does not age and is retained when the switch restarts. You can add and remove static addresses and define the forwarding.

SMI

(Structure of Management Information) The original SMI, as described in RFCs 1155 (STD 16), 1212 (STD 16), and RFC 1215, is termed the SMI version 1 (SMIv1). RFC 1215 describes a "Convention for Defining Traps for use with SNMP". The current version is SMI version 2 (SMIv2).

SMIv2

RFC 2580 ("Conformance Statements for SMIv2") defines the format for compliance statements which are used for describing requirements for agent implementations and capability statements which can be used to document the characteristics of particular implementations. The term "SMIv2" is somewhat ambiguous because it can have at least two different meanings. Sometimes the term is used to refer to the entire data definition language of RFCs 2578 - 2580; at other times it refers to only the portion of the data definition language defined in RFC 2578. According to the IETF, this ambiguity is unfortunate but is rarely a significant problem in practice. The SMI is divided into three parts (module definitions, object definitions, and notification definitions).

SNMP

(Simple Network Management Protocol) A request-response protocol that defines network communication between a Managed Device and a Network Management Station (NMS). A set of protocols for managing complex IP networks. (Standard: RFC 1157.) A protocol for network management that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. Various SNMP versions exist.

SNMP Community String

An Octet String that may contain a string used to add security to SNMP devices.

SNMP engine

A copy of SNMP that can reside either on the local device or the remote device.

SNMP Group

A collection of SNMP users that belongs to a common SNMP list that defines an access policy, in which OIDs are both read-accessible and write-accessible. Users belonging to a particular SNMP Group inherit all of the attributes defined by the group.

SNMP Message

A sequence representing the entire SNMP message, which consists of the SNMP version, Community String, and SNMP PDU.

SNMP PDU

An SNMP PDU contains the body of an SNMP message. There are several types of PDUs (e.g., GetRequest, GetResponse, and SetRequest).

SNMP SMI

(SNMP Structure of Management Information) a collection of managed objects, residing in a virtual information store. The SMI is divided into three parts: module definitions, object definitions, and, notification definitions. There are two types of SMI: SMIv1 and SMIv2. For additional information see IETF RFC 1155 v1 and RFC 2578 v2.

SNMP User

The person for which an SNMP management operation is performed. For informs, the user is a person on a remote SNMP engine who receives the informs.

SNMP Version

An integer that identifies the version of SNMP (e.g., SNMPv1 = 0).

SNMPv1

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

SNMPv2

(SNMP version 2) the SNMPv2 Framework as derived from the SNMPv1 Framework. SNMP v2 is described in STD 58, RFCs 2578, 2579, 2580, and RFCs 1905-1907. SNMPv2 has no message definition.

SNMPv2c

(Community-based SNMP version 2) an experimental SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to the SNMPv1 message format. The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

SNMPv2 with community-based security (SNMPv2c) had the most support within the IETF but had no security and administration whereas both SNMPv2u and SNMPv2* had security but lacked IETF support consensus.

SNMPv3

(SNMP version 3) an extensible SNMP Framework which supplements the SNMPv2 Framework by supporting a new SNMP message format, Security for Messages, Access Control, and Remote configuration of SNMP parameters. The SNMPv3 protocol adds encryption and authentication mechanisms into the SNMP protocol for a secure management protocol where SNMP agents can not be accessed by unauthorized parties.

SNMP View

A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

SNTP

(Simple Network Time Protocol) A less complicated version of Network Time Protocol, which is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled via the Internet. SNTP is used to synchronize times on IP devices over a network. (Standard: RFC 2030.)

SSH

(Secure Shell) A network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet. SSH is used to provide a secure Telnet session to the console/command line interface of a network device through an insecure environment. (AKA, Secured Telnet; Standard: SSH RFC 1034).

SSL

(Secure Socket Layer) A protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data; a public key known to everyone and a private or secret key known only to the recipient of the message. SSL is used to manage a network device via its web interface. (AKA, HTTPS, Standard: RFC 2818).

Static IP addressing

"Static" comes from the word stationary, meaning not moving. A static IP address means it never changes. A static IP address is an IP address permanently assigned to a workstation. If a network uses static addressing, it means that each network interface has an assigned IP address that it always uses whenever it is online. With static addressing, the computer has a well-defined IP address which it uses always and which no other computer ever uses.

Static MAC Entry

Static MAC entry support means that users can assign MAC addresses to ports manually that never age out.

STID

(Sensor Transaction Identifier) The STID is used for power supply / sensor / IONDCR configuration via the set sensor stid command to define notification, relation, severity, and value parameters. The show power config command displays the power supply sensors information. The STID is shown in the Web interface at the Power Supply tab > Temp, Volt, Power, and Fan sub-tabs.

STP

(Spanning-Tree Protocol) A link layer network protocol that ensures a loop-free topology for any bridged LAN. STP prevents loops from being formed when switches are interconnected via multiple paths.

STP

(Shielded Twisted Pair) A special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground.

S-VLAN

Service VLAN (also referred to as Provider VLAN).

Syslog

A service run mostly on Unix and Linux systems (but also available for other OSes) to track events that occur on the system. Analysis can be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

Can refer to a method of general system logging, a log format, and/or a network log transmission mechanism. The Syslog function is implemented in the ION system via the **set syslog** CLI commands and via the device **MAIN** tab > **System Log Configuration** section parameters.

Tag (IEEE 802.1Q tag)

An IEEE 802.1Q tag, if present, is placed between the Source Address and the EtherType or Length fields. The first two bytes of the 802.1Q tag are the Tag Protocol Identifier (TPID) value of 0x8100. The TPID is located in the same place as the EtherType/Length field in untagged frames, so an EtherType value of 0x8100 means the frame is tagged, and the true EtherType/Length is located after the Q-tag. The TPID is followed by two bytes containing the Tag Control Information (TCI), the IEEE 802.1p priority (QOS) and the VLAN ID. The Q-tag is followed by the rest of the frame.

Tagged frame

A packet that contains a header that carries a VLAN identifier and a priority value. Also called a VLAN tagged packet. A Tagged frame contains a tag header immediately following the Source MAC Address field of the frame or, if the frame contains a Routing Information field, immediately following the Routing Information field. There are two types of tagged frames: VLAN-tagged frames and priority-tagged frames.

Tagging / Tag Header

Sending frames across the network requires a way to indicate to which VLAN the frame belongs, so that the bridge will forward the frames only to those ports that belong to that VLAN, instead of to all output ports. This indication is added to the frame in the form of a tag header. The tag header a) allows user priority information to be specified, b) allows source routing control information to be specified, and c) indicates the format of MAC addresses. Frames in which a tag header has been added are called “tagged” frames. These tagged frames convey the VLAN information throughout the network.

TCP

(Transmission Control Protocol) One of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

TCP/IP

(Transmission Control Protocol/Internet Protocol) The basic communication language or protocol of the Internet and/or a private network (either an intranet or an extranet).

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol (TCP), manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol (IP), handles the address part of each packet so that it gets to the right destination.

TDM

(Time Division Multiplexing) A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing.

TDR

1. (Time Domain Reflectometry) A measurement technique used to determine the characteristics of electrical lines by observing reflected waveforms. **2.** (Time Domain Reflector) An electronic instrument used to characterize and locate faults in metallic cables (for example, twisted wire pairs, coaxial cables). It can also be used to locate discontinuities in a connector, printed circuit board, or any other electrical path.

Telnet

A user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. Telnet is a terminal emulation program for TCP/IP networks that runs on your computer and connects your PC to a switch management. (Standard: RFC 854.)

TFTP

(Trivial File Transfer Protocol) A file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). Due to its simple design, TFTP can be implemented using a very small amount of memory. Because it uses UDP rather than TCP for transport, TFTP is typically used to transfer firmware upgrades to network equipment.

TFTP Download / Upload

The ability to load firmware, configuration files, etc. through a TFTP server. (AKA, TFTP. Standard: RFC 1350.)

TFTP Root Directory

The location on the console device (PC) where files are placed when received, and where files to be transmitted should be placed (e.g., *C:\TFTP-Root*).

TFTP Server

An application that uses the TFTP file transfer protocol to read and write files from/to a remote server. In TFTP, a transfer begins with a request to read or write a file, which also serves to request a connection. If the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and must be acknowledged by an acknowledgment packet before the next packet can be sent. Examples of available packages include Open TFTP Server, Tftpd32, WinAgents TFTP Server for Windows, SolarWinds free TFTP Server, TFTP Server 1.6 for Linux, and TftpServer 3.3.1, a TFTP server enhancement to the standard Mac OSX distribution.

Threshold crossing event

See OAM Event.

Throughput

The maximum rate at which no frame is dropped. This is typically measured under test conditions.

TLS

(Transport Layer Security) A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

TLV

Type, Length, Value format - LLDP frames are sent by each equipment on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type, length, value (TLV) structures. An LLDP frame should start with mandatory TLVs (e.g., Chassis ID, Port ID, and Time to live). These mandatory TLVs are followed by any number of optional TLVs. The frame should end with a special TLV named end of LLDPDU. The IEEE 802.1ab specification contains a description of all of the TLV types.

TNDP

(TN Topology Discovery Protocol) the Transition Networks implementation of LLDP. When set to Enabled, the device entering this command will no longer be discovered by the IONMM if it is remotely managed through this port. See also “LLDP” and the “**set tndp**” and “**show tndp**” CLI commands.
See also "Discovery".

TOS

(Type of Service) The ToS byte in the IPv4 header has had several purposes over time, and has been defined in various ways by IETF RFC 791, RFC 1122, RFC 1349, RFC 2474, and RFC 3168. Currently, the ToS byte is a six-bit Differentiated Services Code Point and a two-bit Explicit Congestion Notification field. The ToS model described in RFC 2474 uses the Differentiated Services Field (DS field) in the IPv4 Header and IPv6 Header. See also CoS and QoS.

TPID

(Tag Protocol Identifier) a field in a VLAN Tag for which EEE802.1Q specifies a value of 0x8100.

Traffic colors (Green, Yellow, Red)

MEF 10 Specifies traffic “coloring” as an optional way to mark traffic as ‘in profile’ or ‘out of profile’ as it leaves the ingress UNI. MEF 10 specifies three levels of Bandwidth Profile compliance:

Green: Service Frame subject to SLA
Yellow: Service Frame not subject to SLA
Red: Service Frame discarded.

A service frame is red if it is conformant with neither the CIR nor EIR of the bandwidth profile.
A service frame is yellow if it is not conformant with the EIR of the bandwidth profile.
A service frame is green if it is conformant with the CIR of the bandwidth profile.

Trap

In SNMP, a trap is a type of PDU used to report an alert or other asynchronous event about a managed subsystem.

Also, a place in a program for handling unexpected or unallowable conditions - for example, by sending an error message to a log or to a program user. If a return code from another program was being checked by a calling program, a return code value that was unexpected and unplanned for could cause a branch to a trap that recorded the situation, and take other appropriate action.

An ION system trap is a one-way notification (e.g., from the IONMM to the NMS) that alerts the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the IONMM rather than the NMS. For a management system to understand a trap sent to it by the IONMM, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Traps

One of two types of SNMP notifications that can be sent. See also "informs".

A one-way notification from the NID to the NMS. Its purpose is to alert the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the Agent rather than the NMS. In order for a management system to understand a trap sent to it by the NID, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Each Trap is an asynchronous notification from agent to manager. Includes current sysUpTime value and OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.

TCP/UDP Port Prioritization

The ability to prioritize traffic internally based on a TCP or UDP port number. (AKA, Layer 4 Prioritization.)

TTL

(Time to live) an Ethernet counter that records the number of times a transmission is sent/received without errors. TTL specifies how long a datagram is allowed to “live” on the network, in terms of router hops. Each router decrements (reduces by one) the value of the TTL field prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

The default TTL for ION software is 64. This means that a test packet must be successfully sent and received 63 times before a TTL expired message is generated. You can change the TTL value (e.g., a value of 255 is a demanding test because the packet must be sent and received error free 254 times).

Tunnel

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one (as in L2TP and VPN).

Tunneling

Encapsulating one type of packet inside the data field of another packet. This allows transmitting data that is structured in one protocol within the protocol or format of a different protocol. Tunneling can involve most OSI or TCP/IP protocol layers.

UAC

(User Account Control) Technology and security infrastructure of some *Microsoft* operating systems that improve OS security by limiting application software to standard user privileges until an administrator authorizes an increase.

UDP

(User Datagram Protocol) A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

UNI

(User-to-Network Interface) a demarcation point between the responsibility of the service provider and the responsibility of the subscriber. This is distinct from a Network to Network Interface or NNI that defines a similar interface between provider networks. UNI functions include:

- UNI-C (Subscriber side UNI functions)
- UNI-MA (User-to-Network Interface Maintenance Association)
- UNI-N (Network side UNI functions)

The UNI is the physical interface or port that provides the demarcation between the customer and the service provider/Cable Operator/Carrier/MSO.

Unicast

One of the four forms of IP addressing, each with its own unique properties. The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient. See also “Multicast”.

Untagged frame

A frame that does not contain a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or, through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).

USB

(Universal Serial Bus) A plug-and-play interface between a computer and add-on devices, such as media players, keyboards, telephones, digital cameras, scanners, flash drives, joysticks and printers.

UTC

(Coordinated Universal Time) A time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich. Coordinated Universal Time (abbreviated UTC) is the time standard by which the world regulates clocks and time. Computers, servers, online services, and other entities that rely on a universally-accepted time use UTC for such purposes. Time zones around the world are expressed as positive or negative offsets from UTC; UTC replaced GMT as the basis for the main reference time scale in various regions on January 1, 1972.

UTP

(Unshielded Twisted Pair) The most common form of twisted pair wiring, because it is less expensive and easier to work with than STP (Shielded Twisted Pair). UTP is used in Ethernet 10Base-T and 100Base-T networks, as well as in home and office telephone wiring. The twist in UTP helps to reduce crosstalk interference between wire pairs.

VAC

Volts AC (alternating current, as opposed to DC – direct current). See also “DC”.

Varbind

In SNMP, a sequence of two fields, an Object ID and the value for/from that Object ID. The term ‘Varbinds’ is short for Variable bindings. It’s the variable number of values that are included in an SNMP packet. Each varbind is made of an OID, type, and value.

VCP

(Virtual Com Port) A driver that allows a USB device to appear as an additional COM port. The USB device can be accessed by an application in the same manner as a regular COM port.

VDC

Volts DC (direct current, as opposed to AC – alternating current).

VID

(VLAN Identifier) The identification of the VLAN, which is defined by the standard IEEE 802.1Q. VID has 12 bits and allows the identification of 4096 VLANs.

VLAN

(Virtual LAN) Refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

VLAN Endstation Endpoint

A protocol endpoint representing an endstation network port and its VLAN-specific attributes.

VLAN Switch Endpoint

A protocol endpoint representing a switch port and its VLAN-specific attributes.

VLAN-tagged frame

A tagged frame whose tag header carries both VLAN identification and priority information. A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs (i.e., it carries a tag header that carries a non-null VID). A VLAN-tagged frame is classified as belonging to a particular VLAN based on the value of the VID that is included in the tag header. The presence of the tag header carrying a non-null VID means that some other device, either the originator of the frame or a VLAN-aware Bridge, has mapped this frame into a VLAN and has inserted the appropriate VID. Contrast “untagged frame”.

VLAN Tunneling

(Virtual LAN Tunneling) A mechanism that allows service providers to use a single VLAN to support multiple VLANs of customers, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. At the same time, it significantly reduces the number of VLANs required to support the VPNs. VLAN Tunneling encapsulates the VLANs of the enterprise customers into a VLAN of the service provider. Also called 802.1q Tunneling.

VOIP

(Voice over Internet Protocol) A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks.

Web-based Management

Allows users to manage the switch through a web browser. (AKA, Web GUI, Web interface, Web IF.)

Well Known Ethernet Multicast Addresses

Some common Ethernet multicast MAC addresses are shown below with their related Field Type and typical usage.

Ethernet Multicast Address	Usage
01-00-0C-CC-CC-CC	CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)
01-00-0C-CC-CC-CD	Cisco Shared Spanning Tree Protocol Address
01-80-C2-00-00-00	Spanning Tree Protocol (for bridges) (IEEE 802.1D)
01-80-C2-00-00-01	Ethernet OAM Protocol (IEEE 802.3ah)
01-80-C2-00-00-02	IEEE Std 802.3 Slow Protocols multicast address
01-80-C2-00-00-03	IEEE Std 802.1X PAE address
01-80-C2-00-00-04	IEEE MAC-specific control protocols
01-80-C2-00-00-08	Spanning Tree Protocol (for provider bridges) (IEEE 802.1AD)
01-00-5E-xx-xx-xx	IPv4 Multicast (RFC 1112)
33-33-xx-xx-xx-xx	IPv6 Multicast (RFC 2464)

Well Known Ports

The set of all available port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. The Well Known Ports are 0 - 1023. The Registered Ports are 1024 - 49151. The Dynamic and/or Private Ports are 49152 - 65535. Port 443 is reserved for the HTTPS, port 179 for the BGP Border Gateway Protocol, and port 161 for SNMP. To see all the used and listening ports on your computer, use the **netstat** (or similar) command line command. For more on port assignments, see IETF RFC 1700. RFC 1700 is replaced by an On-line Database. See also the IANA Service Name and Transport Protocol Port Number Registry.

Port Number	Description
20	FTP
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
143	Interim Mail Access Protocol (IMAP)
161	SNMP/UDP
162	SNMPTRAP/UDP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
546	DHCP Client
547	DHCP Server

Web-based Management

Allows users to manage the switch through a web browser. (AKA, Web GUI, Web interface, Web IF.)

Write View

A view name (up to 64 characters) for each SNMP group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

Xmodem

A simple file transfer protocol developed in 1977 as the MODEM.ASM terminal program. XMODEM, like most file transfer protocols, breaks up the original data into a series of "packets" that are sent to a receiver, along with information that allows the receiver to tell if the packet was correctly received. It provides single file transfer using 128-byte packets with CRC or checksum error detection.

Xmodem-1K

An expanded version of XMODEM. Like other backward-compatible XMODEM extensions, it was intended that a -1K transfer could be started with any implementation of XMODEM on the other end, backing off features as required.
It provides simple serial file transfer between a server and client across a point-to-point link using fixed-length packets. Each server packet contains 1024 bytes of file data and is individually acknowledged by the receiving client. One file can be sent per transmission, and the transmission must be restarted from the beginning if it fails.

xSTP

Spanning Tree Protocol (multiple variations) defined in MEF specification 17. See also “STP”.

Y.1731

The ITU-T OAM Recommendation. Some ION 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).

Ymodem

A protocol for file transfers between modems. YMODEM was developed as the successor to XMODEM. The original YMODEM was much the same as XMODEM except that it sent the file name, size, and timestamp in a regular XMODEM block before actually transferring the file. It provides multiple file transfer using 1 Kbyte packets, and is similar to Xmodem in other aspects.

Zmodem

A file transfer protocol developed in 1986 to improve file transfer performance on an X.25 network. ZMODEM also offers restartable transfers, auto-start by the sender, an expanded 32-bit CRC, control character quoting, and sliding window support. It provides multiple file transfer, sending packets without waiting for acknowledgement, and permits an interrupted transfer to restart.

Index

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA

Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Printed in the U.S.A.

ION Systems CLI Reference Manual
33473 Rev. G