



ION System

x323x Remotely Managed Network Interface Device (NID)



User Guide

33432 Rev. E

Trademarks

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

Copyright Notice/Restrictions

Copyright © 2010, 2011, 2012 Transition Networks
All rights reserved.

No part of this work may be reproduced or used in any form or by any means (graphic, electronic or mechanical) without written permission from Transition Networks.

Printed in the U.S.A.

ION System x323x Remotely Managed Network Interface Device (NID) User Guide
33432 Rev. E

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
2	05/10/10	Revised for firmware version 0.5.x.
A	08/24/10	Revised for firmware version 1.0.3.
B	12/21/10	Revised for firmware version 1.0.5. New features include Circuit ID support, L2CP support, Redundancy enhancements, SNMP v1/v2c setting, and Web Interface enhancements.
C	05/17/11	Revised for ION Rel. 1.1.0, Hardware Rev. 0.0.1, and Bootloader Rev. 1.2.0. New features include 1) ION x6010 T1/E1 support, 2) Syslog function, 3) Backup and restore of SOAM config and IONPS card, 4) SSH web interface cleanup, 5) Port mode / MAC Learning Enable portlist, 6) TNDP Enable/Disable, and 7) Updated Help files.
D	12/05/11	Revised for ION Rel. 1.2.1 with: 1) Increased Rate Limiting options. 2) SNMPv3. 3) BOOTP IP addressing. 4) Strict Priority Queuing. 5) USB 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 not fixed. 9) Minor enhancements to SSH package. 10) Backdoor password change. 11) Fixed MEF-related bugs. 12) Enhanced login User management.
E	04/11/12	Revised for 1.3.1 with IPv6, TACACS+ and Auto Provisioning support.

Cautions and Warnings

Definitions

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. Warnings indicate that there is the possibility of injury to person.

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

Cautions



Do not ship or store devices near strong electrostatic, electromagnetic, magnetic, or radioactive fields.



Caution: When handling chassis Network Interface Devices (NIDs) observe electrostatic discharge precautions. This requires proper grounding (i.e., wear a wrist strap).



Caution: Copper based media ports, e.g., Twisted Pair (TP) Ethernet, USB, RS232, RS422, RS485, DS1, DS3, Video Coax, etc., are intended to be connected to intra-building (*inside plant*) link segments that are not subject to lightening transients or power faults. They are **not** to be connected to inter-building (*outside plant*) link segments that are subject to lightening.



Caution: **Do not** install the NIDs in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor NID performance.



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



Caution: Only trained and qualified personnel should install or perform maintenance on the x323x. Failure to observe this caution could result in poor performance or damage to the equipment.



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



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

Warnings



Warning: Use of controls, adjustments or the performance of procedures other than those specified herein may result in hazardous radiation exposure.



Warning: Visible and invisible laser radiation when open. **Do not** look into the beam or view the beam directly with optical instruments. Failure to observe this warning could result in an eye injury or blindness.



Warning: DO NOT connect the power supply module to external power before installing it into the chassis. Failure to observe this warning could result in an electrical shock or death.



Warning: Select mounting bracket locations on the chassis that will keep the chassis balanced when mounted in the rack. Failure to observe this warning could allow the chassis to fall, resulting in equipment damage and/or possible injury to persons.



Warning: Do not work on the chassis, connect, or disconnect cables during a storm with lightning. Failure to observe this warning could result in an electrical shock or death.

See [Appendix A](#) on page 542 for Electrical Safety Warnings translated into multiple languages.

Table of Contents

Section 1: Introduction	16
Document Overview.....	16
Product Overview.....	16
Features.....	16
Auto-Negotiation (802.3u).....	18
Pause.....	18
AutoCross (10/100/1000Base-T).....	18
Configuration Backup and Restore.....	19
DMI Optical Management.....	19
Backwards Compatibility / Point System Support.....	19
DHCP Client.....	20
DNS Client.....	20
Far End Fault (FEF).....	20
Management Access Methods.....	21
TFTP (Trivial File Transfer Protocol).....	21
SLPT (Selective Link Pass Through).....	21
TLPT (Transparent Link Pass Through).....	22
TLPT and Auto Link Restoration.....	23
Fiber Port Redundancy.....	23
IP-Based Remote Management Mode.....	24
Security Features.....	24
IP Address Modes (IPv4 / IPv6, DHCP, Static, BootP).....	25
Applicable Standards.....	26
IEEE 802.1p QoS Packet Classification.....	26
IEEE 802.1ag Service OAM (SOAM).....	26
ITU-T Y.1731 Alarm Processing and Performance Monitoring.....	27
IEEE 802.3ah Clause 57 OAM Recommendation.....	27
Service OAM Recommendations.....	28
VLAN Tunneling (802.1q Tunneling).....	34
L2CP (Layer 2 Control Protocol).....	35
Device Description / Circuit ID.....	36
MAC Address Learning.....	36
System Logging (Syslog).....	36
TDM Loopback.....	36
TNDP (TN Topology Discovery Protocol) Disable.....	36
RFC 2544 Benchmarking.....	37
SNMP Support.....	37
WRR or Strict Priority Queuing.....	38
Serial File Transfer (X/Y/Zmodem).....	38
Supported MIBs.....	39
Public MIBs.....	39
Private MIBs.....	39
Downloading, Compiling and Integrating MIBs.....	42
NID Models.....	43
Standard Models.....	43
Single Fiber Models.....	44
Physical Specifications.....	45
Documentation Conventions.....	47

Contents

Related Manuals and Online Help.....	48
Section 2: Installation and System Setup.....	49
General	49
Installing the Chassis Model (C323x)	49
Installing the Standalone Model (S323x)	50
Rack Mount Installation.....	50
Tabletop Installation.....	51
Wall Mount Installation	52
Connecting to AC Power.....	53
Installing SFPs.....	54
Connections and LEDs	55
Model x3230-1040	55
Model x3231-1040	57
Model x3230-10xx	59
Access via an Ethernet Network	71
Initial Setup with a Static IP Address via the CLI.....	73
Accessing the NIDs	75
Access via Local Serial Interface (USB).....	75
Changing Switch Mode (Local / Remote).....	80
Section 3: Management Methods.....	81
General	81
IONMM Managed NIDs	81
Managing Slide-In and Remote Modules Using CLI Commands.....	81
Managing Slide-In and Remote Modules via the Web Interface	84
Direct Managed NIDs.....	85
Managing Standalone Modules Using CLI Commands.....	85
Managing a Standalone Module via the IONMM Web Interface	86
Managing a Standalone Module via the Web Interface	87
Menu System Descriptions.....	88
Reboot, Reset, and Power Off Function Notes	92
Section 4: Configuration.....	95
General	95
Setting the IPv4 Addressing	96
DNS Lookups over IPv6 Transport.....	101
Assigning a Dynamic IPv4 Address via DHCP	103
Defining DNS Servers.....	104
IPv6 Dual Protocol Stacks and Multiple Server Support	110
Telnet IPv4 and IPv6 Connections.....	117
TFTP IPv4 and IPv6 Connections.....	117
System Configuration	122
System Configuration – CLI Method.....	122
System Configuration – Web Method.....	123
Device Description Configuration.....	124
Device Description– CLI Method	124
Device Description Config – Web Method	125
Circuit ID Configuration	126
Circuit ID Config – CLI Method.....	126
Circuit ID Config – Web Method	127
Login Type Config – CLI Method	128
Ports Configuration.....	131
Configuring AutoCross.....	131

<i>AutoCross</i> Config – CLI Method	131
<i>AutoCross</i> Config – Web Method	132
Configuring Auto Negotiation	133
10/100/1000BaseT Port – CLI Method	133
10/100/1000BaseT Port – Web Method	136
Set Ethernet Port Speed / Duplex Mode (Force Speed / Duplex Mode)	138
Set Ethernet Port Speed / Duplex Mode – CLI Method	138
Set Ethernet Port Speed / Duplex Mode – Web Method	140
Set Port Admin Mode (Ethernet PHY Mode)	141
Set Port Admin Mode (Ethernet PHY Mode) – CLI Method	141
Set Port Admin Mode (Ethernet PHY Mode) – Web Method	142
Far End Fault Mode Configuration	144
Far End Fault Mode Config – CLI Method	144
Set Bandwidth Allocation / Rate Limiting	145
Set Bandwidth Allocation / Rate Limiting – CLI Method	145
Set Bandwidth Allocation / Rate Limiting – Web Method	147
Configuring Priority Queuing	150
Priority Queuing Config – CLI Method	150
Priority Queuing Config – Web Method	151
Configuring Ethernet OAM	152
LOAM (Link OAM) Configuration	152
LOAM Configuration Prerequisites and Restrictions	152
LOAM Config – CLI Method	153
LOAM Config – Web Method	158
Copper Port Loopback Procedure	167
SOAM (Service OAM) Configuration	170
SOAM Configuration Prerequisites and Restrictions	170
SOAM CLI Commands	171
SOAM Menu System	171
Configuring a SOAM MD/MA	172
Configuring a SOAM MEG	181
Configuring a SOAM MEP	187
Configuring a SOAM MIP	194
Verifying the SOAM Main Configuration	198
Viewing SOAM MEP Defects	199
Viewing SOAM FNG (Fault Notification Generation) States	200
SOAM MEP Tests	201
CC Monitoring (Continuity Checks Monitoring)	203
Loopback (LB)	209
Linktrace	214
ETH-MCC (Ethernet Maintenance Communication Channel)	220
ETH-TEST	224
DM (Frame Delay Measurement)	229
FLM (Frame Loss Measurement)	236
Ethernet Alarm Indication Signal (AIS)	240
Ethernet Remote Defect Indication (RDI)	245
SOAM MEP Test Summary	247
SOAM Terminology Differences between IEEE, ITU-T, and MEF	247
Configuring Selective and Transparent Link Pass Through	248
Link Pass Through Config – CLI Method	250
Link Pass Through Config – Web Method	252

Contents

Configure Forwarding Learning (FDB) Aging Time	254
Forwarding Learning (FDB) Aging Time Config – CLI Method	254
FDB Aging Time Config – Web Method.....	255
Configuring SNTP.....	256
SNTP Config – CLI Method	257
SNTP Config – Web Method	262
Configuring System Login Users	263
Note Regarding SNMPv3 Users vs. Web/CLI Login Users	263
Configuring System Login Users - CLI Method.....	264
Configuring System / Login Users - Web Method.....	266
Dynamic Table Entry Limits.....	267
Configuring Security Features.....	268
Configuring an ACL.....	269
ACL Config (IPv6) – Web Method.....	279
Configuring HTTPS	282
Configuring MAC Address Filtering	287
Configuring MAC Address Blocking.....	290
Configuring Port Forward Management / IP Access Blocking.....	294
Configuring RADIUS	296
Configuring TACACS+	301
Configuring SSH.....	307
Configuring SSH and RADIUS	312
Configuring SNMP	313
Note Regarding SNMPv3 Users vs. Web/CLI Login Users	314
SNMP Definition and Description.....	314
Management Information Base (MIB).....	315
A MIB Example - ionDevSysCfgTable	316
SNMP PDUs	316
SNMP Version v1, v2c, v3 Considerations.....	318
SNMP v1, v2c, v3 Descriptions	319
SNMPv1	319
SNMPv2 and v2c	319
SNMPv3	320
SNMPv3 USM MIB.....	328
SNMPv3 VACM – Groups	329
SNMPv3 VACM – Views.....	330
SNMPv3 Traps and Informs	330
ION System SNMP Support	332
SNMP Command Line Interface (CLI) Support	332
SNMP v3 Users, Groups, and Views Configuration.....	332
Configuring SNMP.....	336
SNMP Config – CLI Method	337
SNMP Config – Web Method.....	340
Change a SNMP User’s Group - Web Method	348
SNMP v3 Default Values.....	349
SNMP v3 Commands	351
Web Interface-to-CLI Command Cross Reference	353
Configuring VLANs, VLAN Management, and VLAN Tunneling.....	356
Configuring Management VLAN	357
Configuring VLANs – Network / Provider / Customer Mode.....	362
Flush VLAN Databases Config.....	375

Configuring VLAN Tunneling (802.1q Tunneling).....	379
Configuring QOS.....	383
Configuring Fiber Port Redundancy.....	392
Configuring L2CP.....	395
L2CP Protocol Descriptions.....	395
L2CP Config – CLI Method.....	397
L2CP Config – Web Method	398
TNDP (TN Topology Discovery Protocol) Disable/Enable.....	399
TNDP Config – CLI Method	399
TNDP Config – Web Method	400
Configuring Loopback.....	401
Loopback Config – CLI Method.....	401
Loopback Config – Web Method.....	402
Configuring System Logging (Syslog).....	403
Syslog Config – CLI Method	405
Syslog Config – Web Method.....	406
Configuring MAC Address Learning	408
MAC Address Learning Portlist Config – CLI Method.....	408
MAC Address Learning Portlist Config – Web Method.....	409
Section 5: Operations.....	410
General	410
Backup and Restore Operations (Provisioning)	410
Backing Up Slide-In and Remote Module Configuration.....	411
Backing Up Standalone Modules.....	414
Editing the Config File (Optional)	416
Restoring Slide-In and Remote Modules' Configuration.....	417
Restoring Standalone Modules.....	421
Back Up and Restore File Content and Location	424
Backup / Restore (Provisioning) - CLI Method	426
Disabling USB Console Access to the x323x.....	428
4. Displaying Information.....	429
Reset to Factory Defaults	429
Resetting Defaults – CLI Method	429
Resetting Defaults – Web Method	430
File Status after Reset to Factory Defaults	431
Resetting Uptime	432
Reset System Uptime – CLI Method	432
Reset System Uptime – Web Method	433
Resetting Counters.....	434
Reset All Ports Counters – CLI Method	434
Reset Port Counters– Web Method	435
Clear All Ethernet Port Counters – CLI Method.....	436
All Counters Reset – Web Method	437
Reboot.....	438
Rebooting – CLI Method	438
Rebooting – Web Method	439
Reboot File Content and Location	440
Upgrade the IONMM and/or NID Firmware.....	441
Upgrading IONMM and/or NID Firmware – CLI Method.....	441
Upgrading IONMM and/or NID Firmware – Web Method.....	443
Upgrading Slide-In and Remote Modules Firmware via TFTP	449

Contents

Upgrading Standalone Module Firmware via TFTP Server.....	454
Firmware Upgrade File Content and Location.....	456
Additional Upgrade Procedures	456
Transfer Files via Serial Protocol (X/Y/Zmodem) - CLI Method.....	457
Replacing a Chassis Resident NID	458
Section 6: Troubleshooting.....	459
General	459
Basic ION System Troubleshooting	459
Error Indications and Recovery Procedures	460
LED Fault and Activity Displays	461
IPv6 Troubleshooting	462
Problem Conditions	464
CLI Messages	479
Web Interface Messages	545
SNMP Messages.....	562
Basic Recovery Steps	562
The Config Error Log (config.err) File.....	573
config.err Messages.....	574
config.err Message Responses	574
Syslog Messages and Sys.log Output	579
Syslog Messages	579
Sample Sys.log Output.....	582
Webpage Messages.....	585
SOAM Configuration Error List.....	603
SOAM Configuration Error List - CLI Method	603
SOAM Configuration Error List - Web Method	604
Windows Event Viewer Messages	614
ION System Tests.....	615
Virtual Cable Test (VCT).....	615
DMI (Diagnostic Maintenance Interface) Parameters.....	620
Set Debug Level.....	625
Show Ethernet Statistics Counter Descriptions.....	626
Jumper Settings.....	628
PCB Identification.....	628
C3230 NID	629
C3231 NID	630
Third Party Troubleshooting Tools	631
Ipconfig	631
ifconfig	633
Windows Network Connections.....	634
Ping	635
Telnet.....	636
PuTTY	637
Tracert (Traceroute)	639
Netstat	640
Winipcfg.....	641
Nslookup	642
DHCP	643
Dr. Watson	644
SNMPc	644
HPOV (HP OpenView).....	645

US-CERT	645
Third Party Tool Messages	646
HyperTerminal Messages	646
Ping Command Messages	649
Telnet Messages	649
TFTP Server Messages	651
PuTTY Messages	652
Technical Support	653
Recording Model Information and System Information	654
Appendix A: Warranty and Compliance Information	656
Warranty	656
Compliance Information	659
Declaration of Conformity	661
MEF Certifications	661
Electrical Safety Warnings	662
Electrical Safety	662
Elektrische Sicherheit	662
Elektrisk sikkerhed	662
Elektrische veiligheid	662
Sécurité électrique	662
Sähköturvallisuus	662
Sicurezza elettrica	663
Elektrisk sikkerhet	663
Segurança eléctrica	663
Seguridad eléctrica	663
Elsäkerhet	663
Appendix B: Factory Defaults	664
Device-Level Factory Defaults	664
Port-Level Factory Defaults	679
Appendix C: Configuration Quick Reference – CLI	684
IPv6 Configuration	684
ACL Configuration (IPv6)	685
TACACS+ Configuration	689
System (Login) User Configuration	692
Transfer Files via Serial Protocol (X/Y/Zmodem)	692
SNMP Configuration	693
Appendix D: SOAM Configuration Example – Web Method	694
SOAM Sample Configuration – Web Method	694
IEEE 802.1ag Configuration	695
ITU-T Y.1731 Configuration	721
Appendix E: SOAM Configuration Example – CLI Method	738
SOAM Sample Configuration – CLI Method	738
IEEE 802.1ag Configuration	739
1BY.1731 Configuration Example	758
2BFor More Information	776
Appendix F: VLAN Tunneling Configuration Examples	777
VLAN Tunneling Config – CLI Method	778
VLAN Tunneling Config – Web Method	782
Configuring VLAN 100 with Provider S-Tag	782
Configuring a VLAN with C-Tags and S-Tags	787
Configuring Q-in-Q (Provider Tagging)	791

Contents

Q-in-Q Config – CLI Method	792
Q-in-Q Config – Web Method	796
Appendix G: SNMP Traps Supported	799
Traps List.....	799
SNMP v3 Traps.....	800
MIB Traps Summary	801
TN-ION-MGMT-MIB.smi.....	803
Agent_III_Private MIBS	805
ION-DEV-SYS-ACL-MIB	805
TN-ION-VLAN-MGMT-MIB.mib.....	806
TN_ION Private MIBS.....	807
TN-ION-BPC-MIB	807
TN-IONCHASSIS-MIB.....	808
TN-ION-ENTITY-SENSOR-MIB	810
TN-ION-LOAM-EXT-MIB	812
TN-ION-MGMT-MIB	812
ionDMIRxPowerEvt.....	813
ionDMITxPowerEvt.....	814
ionDMITxBiasEvt.....	815
ionDMITemperatureEvt.....	816
TN-ION-SOAM-EXT-MIB	817
ionSoamCCMDefectTrap.....	817
ionSoamRemoteMepAddTrap	818
ionSoamRemoteMepRemoveTrap	820
TN-ION-SOAM-IDX-MIB	821
TN-PROVBRIDGE-MIB	821
ION Public MIBS	822
IEEE8021-CFM-MIB	822
dot1agCfmFaultAlarm	822
BRIDGE-MIB	825
newRoot	825
topologyChange	826
DOT3-OAM-MIB	827
dot3OamThresholdEvent	827
ENTITY-MIB	831
EtherLike-MIB	831
IANA-MAU-MIB.....	831
IEEE8021-CFM-V2-MIB.....	832
IEEE8021-TC-MIB	832
IF-MIB.....	832
linkDown.....	832
linkUp.....	833
LLDP-MIB	835
NOTIFICATION-LOG-MIB.....	835
P-BRIDGE-MIB	835
Q-BRIDGE-MIB	835
RFC1213-MIB.....	835
RMON-MIB (RFC 2819)	836
risingAlarm	836
fallingAlarm	838
RMON2-MIB	839

SNMP-COMMUNITY-MIB	839
SNMP-NOTIFICATION-MIB	839
SNMP-TARGET-MIB	839
Trap Server Log	840
For Additional SNMP MIB Trap Information.....	841
Appendix H: ION Power Supply / DCR / ADP / LG Configuration	842
Power Supply Config – CLI Method.....	842
Power Supply Config – Web Method.....	845
Temperature Sensor Configuration	846
Voltage Sensor Configuration.....	848
Power Sensor Configuration	850
Fan Configuration	852
IONDCR (Dry Contact Relay) Module.....	854
IONDCR with IONPS-A (AC) Power Supply	854
IONDCR with IONPS-D (DC) Power Supply	855
IONADP (Point System™ -to-ION Adapter).....	857
IONADP Config – CLI Method.....	857
IONADP Config – Web Method.....	857
IONLG (ION Last Gasp) Kit.....	858
IONLG Config – CLI Method	858
IONLG Config – Web Method	858
Glossary	859
Index.....	924

List of Figures

Figure 1: Far End Fault (FEF)	20
Figure 2: Selective Link Pass Through (SLPT)	22
Figure 3: Transparent Link Pass Through (TLPT)	22
Figure 4: IEEE 802.1ag SOAM (Service OAM)	26
Figure 5: Sample SOAM Application.....	29
Figure 6: Up / Down MEPs, MIPs, and MD Levels	32
Figure 7: Maintenance Levels and Domains.....	33
Figure 8: VLAN Tunneling	34
Figure 9: Private MIB Objects	41
Figure 10: Chassis Installation.....	49
Figure 11: Tabletop Installation.....	51
Figure 12: Wall Mount Installation.....	52
Figure 13: AC Power Connection.....	53
Figure 14: SFP Installation	54
Figure 15: Model C3230-1040 Connectors and LEDs	55
Figure 16: Model S3230-1040 Connectors and LEDs.....	55
Figure 17: Model C3231-1040 Connectors and LEDs	57
Figure 18: Model S3231-1040 Connectors and LEDs.....	57
Figure 19: Model C3230-10xx Connectors and LEDs	59
Figure 20: Model S3230-10xx Connectors and LEDs.....	59
Figure 21: CLI Location Hierarchy	82
Figure 20: Sample Loopback Configuration.....	168
Figure 21: Sample Loopback Counters Information.....	169
Figure 22: SOAM Menu System	171

Contents

Figure 23: Continuity Checks (CC)	203
Figure 24: Loopbacks (LB).....	209
Figure 25: Link Trace (LT).....	214
Figure 26: Alarm Indication Signal (AIS)	240
Figure 27: Selective Link Pass Through (SLPT)	248
Figure 28: Transparent Link Pass Through (TLPT)	249
Figure 29. MIB Example	316
Figure 30. SNMP PDU Format.....	316
Figure 31. SNMP v3 MIBs	325
Figure 32. SNMP v3 Trap-Inform MIBs	325
Figure 33. SNMP v3 Entity / Engine / Applications.....	326
Figure 34: ION System Managed via SNMP.....	332
Figure 35 .SNMP v3 Users, Groups, and Views.....	333
Figure 36: VLAN Tunneling Example	381
Figure D-1: SOAM Configuration	694
Figure D-2: MEG Level Layouts	695
Figure D-3: IEEE 802.1ag Test Configuration	695
Figure D-4: ION Chassis / Device Configuration.....	696
Figure D-5: ITU-T Y.1731 Configuration Example.....	721
Figure D-6: ION Chassis / Device Configuration.....	721
Figure E-1: SOAM Configuration	738
Figure E-2: MEG Level Layouts	739
Figure E-3: IEEE 802.1ag Configuration	739
Figure E-4: ION Chassis / Device Configuration	740
Figure E-5: ITU-T Y.1731 Configuration Example	758
Figure F-1: VLAN Tagging Example.....	777
Figure F-2: Q-in-Q (Provider Tagging)	791
Figure G-1: SNMP Message Sequence.....	800
Figure H-1: The IONDCR Module.....	854
Figure H-2: IONDCR Installed in IONPS-A Power Supply	854
Figure H-3: IONDCR Installed in IONPS-D (DC) Power Supply	855
Figure H-4: The IONADP Module	857
Figure H-5: The IONLG Module.....	858

List of Tables

Table 1: Supported MIBs.....	39
Table 2: Standard Models	43
Table 3: Single Fiber Models*	44
Table 4: Physical Specification for Chassis Models.....	45
Table 5: Physical Specifications for Standalone Models.....	46
Table 6: Documentation Conventions.....	47
Table 7: Model x3230-1040 Connectors and LED Descriptions.....	56
Table 8: Model x3231-1040 Connectors and LED Descriptions.....	58
Table 9: Model x3230-10xx Connectors and LED Descriptions.....	60
Table 10: System-Level Menu Description	88
Table 11: Port-Level Menu Description	90
Table 12: LOAM Events.....	154
Table 13: SOAM MA Attributes	173
Table 14: SOAM MEG Attributes	182

Table 15: SOAM MEP Attributes.....	188
Table 16: SOAM MIP Attributes.....	194
Table 17: Timezones.....	257
Table 18: User Level Rights via Web / CLI	263
Table 19: SNMPv3 Private MIB Levels / Auth / Encryption	320
Table 20: SNMPv3 Services.....	321
Table 21: SNMPv3 Private MIBs	322
Table 22: SNMPv3 Private MIBs	323
Table 23: SNMP v3 Default Values	329
Table 24: SNMP v3 Trap and Inform MIBs.....	330
Table 25: Web Interface Tabs to MIB Tables Mapping	331
Table 26: SNMP v3 Initialization (Default) Values	349
Table 27: SNMP v3 Web Interface Default Values.....	350
Table 28: Web Interface to CLI Command Cross Reference	353
Table 29: Syslog Severity Levels.....	403
Table 30: Back Up and Restore File Content and Location.....	424
Table 31: File Status after a Reset to Factory Defaults.....	431
Table 32: File Content and Location after a System Reboot	440
Table 33: File Content and Location after a Firmware Upgrade	456
Table 34: DMI Parameters.....	622
Table 35: Device-Level Factory Defaults	664
Table 36: Port-Level Factory Defaults.....	679
Table 37: MIB Traps Summary	801
Table 38: Trap Server Log File Description	841

Section 1: Introduction

Document Overview

The purpose of this manual is to provide the user with an understanding of the Transition Networks x323x network interface devices (NIDs). This manual documents the following models:

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

Product Overview

The x323x are a group of Ethernet Network Interface Devices (NIDs) that are designed as either a standalone module (S323x) or a slide-in module (C323x) that is installed in an ION system chassis. In either configuration, these devices are designed to manage devices remotely through the copper and fiber ports.

Standalone devices can also be managed via IP (Web-based) or Telnet.

The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). These devices implement the IEEE 802.3ah standard (OAM) in the Ethernet first mile. OAM is a group of network management functions that provide network fault indications, performance information, data, and diagnosis. These devices implement remote management via OAM per the IEEE 802.3ah standard.

Features

The x323x NIDs support the following features.

- 10K Jumbo Frame Support
- Auto-Negotiation
- Pause
- *AutoCross*TM
- Bandwidth profiling
- Cable diagnostic function for TP ports
- Multiple IP addressing modes (IPv4 / IPv6, DHCP, Static, Bootp)

- DHCP client
- DMI Optical Management
- Backwards Compatibility / Point System Support
- Far-End-Fault (FEF)
- MAC filtering for network access control (authentication and authorization)
- Ipv4 IP TOS, DiffDerv and IPv6 traffic class QoS classification
- Multiple management methods
- Remote Firmware Upgrade
- Remote Loopback
- RMON Counters for each port
- SNMP
- TFTP
- Selective Link Pass Through (SLPT)
- Transparent Link Pass Through (TLPT) and Auto Link Restoration
- IP-Based Remote Management
- Link layer OAM (LOAM) per IEEE 802.3ah
- Service layer OAM (SOAM) per IEEE 802.1ag and ITU-T Y.1731 recommendations
- IEEE 802.1p QoS packet classification
- IEEE 802.1q VLAN and double VLAN tagging with 4096 VIDs
- VLAN Tunneling and Management VLAN
- Fiber Port Redundancy
- Layer 2 Control Protocols (L2CP)
- Circuit ID and Device Description
- TNDP (TN Topology Discovery Protocol) Disable
- TDM Loopback
- System Logging (Syslog)
- MAC Learning Disable
- SNMP v1, v2c, and v3 support
- BOOTP Addressing support
- WRR or Strict Priority Queuing
- Serial File Transfer (X/Y/Zmodem) commands

These features are discussed in the following sections.

10K Jumbo Frame Support

The x32x NID devices support jumbo frames. The MTU (Maximum Transmission Unit) frames size is 10240 bytes (not configurable).

Auto-Negotiation (802.3u)

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

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

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

Pause

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

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

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

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

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

AutoCross (10/100/1000Base-T)

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

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

Bandwidth Profiling

A Bandwidth Profile is a method of characterizing Service Frames for the purpose of rate enforcement or policing. The x32x NID devices support bandwidth profiling at the per-port level. Each port has an

ingress bandwidth profile used to control the ingress traffic and an egress bandwidth profile for regulating traffic leaving the port. This feature provides TX and RX rate limiting from a pre-defined list of values in order to accommodate bursty traffic.

Configuration Backup and Restore

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

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

For more information see “[Backup and Restore Operations](#)” on page 267.

DMI Optical Management

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

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

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

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

Backwards Compatibility / Point System Support

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

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

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

Section 1: Introduction

DHCP Client

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

When a DHCP-configured client (x323x) connects to a network, it sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the DNS servers, other servers such as time servers, etc. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters (e.g., subnet mask, default gateway). The query is typically initiated right after a re-boot, and must complete before the client can initiate IP-based communication with other hosts.

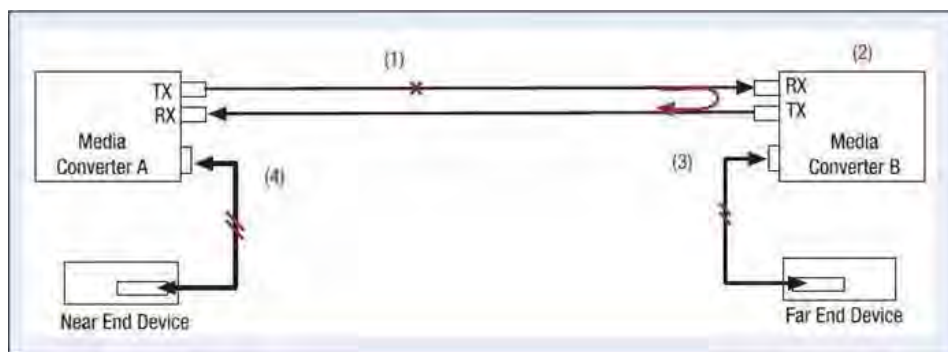
The x323x provides DHCP client support (no DHCP server features). DHCP provides for dynamic IP address assignment to the x323x. An x323X CLI command is available to find out the DHCP assigned IP address.

DNS Client

The x323x provides DNS client support (no DNS server features). DNS will allow use of a name instead of an IP address when using features like TFTP server, Trap Manager, SNTP server, etc. DHCP client and DNS server usage are independent; however, depending on the network setup, DHCP could automatically configure a DNS server as part of DHCP IP address assignment.

Far End Fault (FEF)

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



- 1) Device B loses fiber RX link.
- 2) Device B disables copper TX via Link Pass Through (LPT) to alert far end device of link loss.
- 3) Device B sends FEF signal back on fiber TX to alert Device A of link loss.
- 4) Device A disables copper TX via LPT to alert near end device of link loss.

Figure 1: Far End Fault (FEF)

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

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

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

Management Access Methods

Management of the x323x, and subsequently the other slide-in modules, is accomplished through one of the following methods.

- Universal Serial Bus (USB) – uses a command line interface (CLI) to access and control the x323x through a locally connected workstation.
- Telnet session – uses the CLI to access and control the x323x through the network.
- Secure Shell (SSH) – uses the CLI to access and control the x323x through the network. Web browser – access and control the x323x using a standard web browser and a graphical user interface (GUI).
- Simple Network Management Protocol (SNMP) – both public and private Management Information Bases (MIBs) allow a user to easily integrate and manage the ION platform with an SNMP based network management system (NMS).

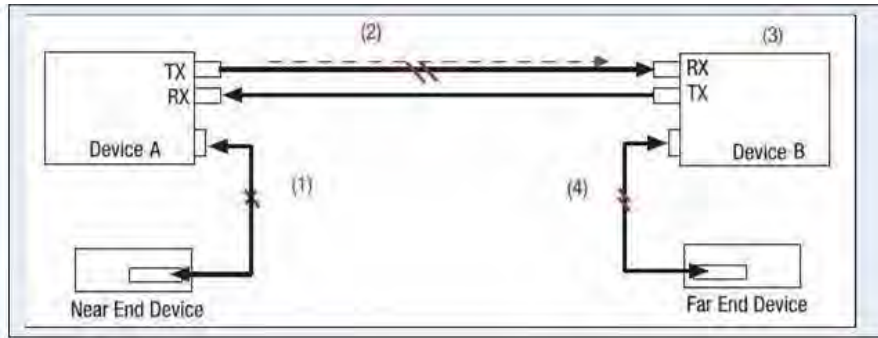
TFTP (Trivial File Transfer Protocol)

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

SLPT (Selective Link Pass Through)

This feature monitors the fiber Rx port for signal loss. If the fiber Rx goes down, the copper port stops transmitting.

SLPT monitors the link status of one port on Device A, and any change in its operational state is passed on to the device's other port to bring down its link, and vice-versa. SLPT is similar to LPT, except SLPT only works in one direction - from Port 1 to Port 2, or from Port 2 to Port 1, but not in both directions.



- 1) Device A loses copper RX link with end device.
- 2) Device A sends a link loss signal over the fiber.
- 3) Device B receives link loss signal and disables the copper TX port.
- 4) End device is notified of link failure.

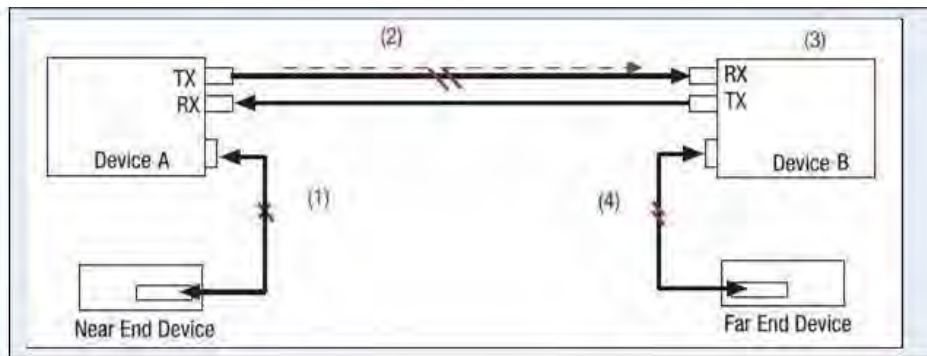
Figure 2: Selective Link Pass Through (SLPT)

Selective LPT is typically supported by devices which support 'Transparent LPT'.

TLPT (Transparent Link Pass Through)

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

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



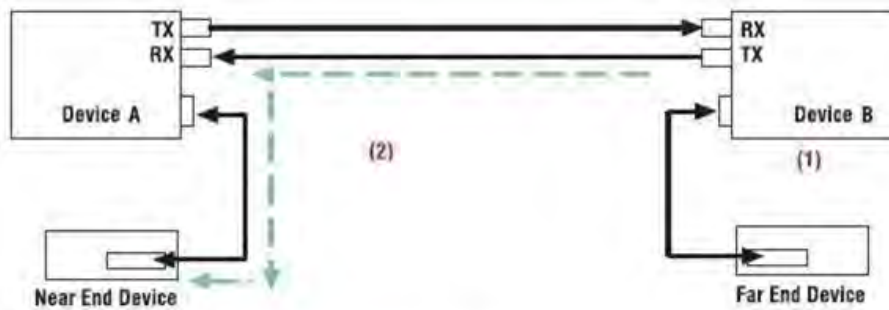
- 1) Device A loses copper RX link with end device.
- 2) Device A sends a link loss signal over the fiber.
- 3) Device B receives link loss signal and disables the copper TX port.
- 4) End device is notified of link failure.

Figure 3: Transparent Link Pass Through (TLPT)

TLPT and Auto Link Restoration

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

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



1) Original Link Restored.

2) Links Automatically Restored without any user intervention.

Fiber Port Redundancy

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

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

The Redundancy feature adds a form of automatic protection switching using a LOS mechanism that triggers the switch to the surviving line. The ION system uses 1:1 protection, with a modified form of bi-directional switching.

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

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

IP-Based Remote Management Mode

The x323x NIDs can be managed through SNMP. Select stand-alone products can also be managed through SNMP. Some remotely managed converters are IP addressable, while others must be used in conjunction with a managed chassis-based device. While chassis based products are generally placed in the telecommunications room, stand-alone converters are generally placed in remote locations away from network administrators. Remote in-band management over fiber allows administrators access to the remote device to check status and enable/disable features or the device itself.

Security Features

The security features allow you to control access to the ION Chassis via the x323x NID to ensure that only authorized personnel are able to view and change the settings of the slide-in modules.

- Access Control Lists (ACLs) – ACLs can be configured in the x323x NID to allow access to authorized users and to deny access to all others. For more information see [“Configuring an ACL”](#) on page 197.
- Hypertext Transfer Protocol Secure (HTTPS) – the x323x NID supports the use of HTTPS, which utilizes the secure socket layer (SSL) protocol for transmitting private documents via the Internet. For more information see [“Configuring HTTPS”](#) on page 204.
- Management VLAN – In a VLAN enabled network, the administrator can assign a VLAN as a management VLAN. This VLAN ID will be used in all management frames. This separates the management traffic from the data. For more information see [“Configuring Management VLAN”](#) on page 132.
- RADIUS authentication – The x323x NID supports authentication using the Remote Authentication Dial In User Service (RADIUS) protocol. When enabled, RADIUS is used to authenticate and authorize users trying to access the x323x NID through either the Web login, serial port (USB), or Telnet session. The RADIUS server must be configured before RADIUS authentication is enabled. For more information see [“Configuring RADIUS”](#) on page 119.
- Secure Shell (SSH) authentication – the x323x NID supports both the Rivest-Shamir-Adleman (RSA) and Digital Signature Algorithm (DSA) for public key cryptography for both connection and authentication. For more information see [“Configuring SSH”](#) on page 218.
- Simple Network Management Protocol (SNMP) access – If desired the administrator can stop all SNMP access to the x323x NID. This will prevent unauthorized access to the system configuration through SNMP, but the desired/configured SNMP traps will still be sent. For more information see [“Configuring SNMP”](#) on page 123.
- USB access – The USB port can be turned off to prevent unauthorized access to the system through the serial interface. For more information see [“Disabling USB Access to the IONMM”](#) on page 278.

IP Access

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

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

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

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

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

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

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

MAC Filtering

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

MAC Addresses Blocking

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

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

Applicable Standards

- IEEE 802.1p QoS packet classification
- ITU-T Y.1731 OAM Recommendation
- IEEE 802.1ag Service OAM (SOAM)
- IEEE 802.3ah Clause 57 Link OAM (LOAM)
- IEEE 802.1q VLAN and double VLAN tagging
- IEEE 802.1 Port-based Network Access Control

IEEE 802.1p QoS Packet Classification

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

The x323x NIDs provide QoS at the Layer 2 level using CoS bits as per IEEE 802.1p. The priority bits in the 802.3ac tag can be remapped as frames ingress the device based on Ingress port, Source MAC address, Destination MAC address, or VLAN ID in the 802.1q tag, or on the basis of remapping to a user-defined priority on a per port basis.

The x323x NIDs also provide QoS based on DSCP/ToS bits in the IP header.

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

IEEE 802.1ag Service OAM (SOAM)

The IEEE 802.1ag recommendation for Connectivity Fault Management defines standards for continuity checks, loopbacks and link trace for enterprise and carrier networks, and partitions the network into eight hierarchical administrative domains.

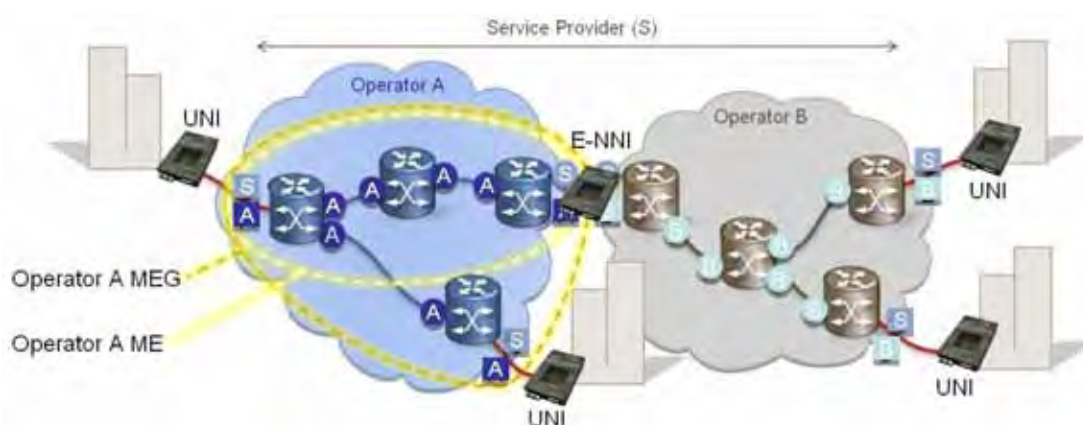


Figure 4: IEEE 802.1ag SOAM (Service OAM)

ITU-T Y.1731 Alarm Processing and Performance Monitoring

Y.1731 adds alarm processing, Ethernet Alarm Indication Signal (AIS) and Ethernet Remote Defect Indication (RDI), and Performance Monitoring including Frame Loss Measurements (ETH-LM) and Frame Delay Measurements (ETH-DM).

ETH-AIS lets you suppress alarms when defects are detected at the server (sub) layer.

ETH-RDI is used by a MEP to notify its peer MEPs that it detects a defect condition. The OAM performance monitoring functions, ETH-LM and ETH-DM, allow measurement of various performance parameters for point-to-point ETH connections.

IEEE 802.3ah Clause 57 OAM Recommendation

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

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

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

Critical Event

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

Discovery

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

Event Notification with Logs

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

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

Last Gasp/Dying Gasp

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

Section 1: Introduction

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

Remote Loop Back

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

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

Ethernet Performance - CFM and SOAM

Measuring Ethernet performance is driven by two standards groups, namely:

1. IEEE 802.1ag, Connectivity Fault Management.
2. ITU-T Y.1731, OAM Functions and Mechanisms for Ethernet networks (performance monitoring).

The two standards build off of each other and provide the basic mechanisms to measure an Ethernet service. The standards rely on the in-network devices to actively participate in measuring the service to provide five KPIs (key performance indicators): 1. Availability, 2. Frame Loss, 3. Frame Delay, 4. Frame Delay Variation, and 5. Throughput.

Connectivity Fault Management Protocols

Ethernet Connectivity Fault Management (CFM) per IEEE 802.1ag comprises three protocols that work together to help administrators debug Ethernet networks: continuity check, link trace and loopback protocols.

- Continuity Check - These are "heartbeat" messages issued periodically by maintenance endpoints. They let maintenance endpoints detect loss of service connectivity amongst themselves. They also allow maintenance endpoints to discover other maintenance endpoints within a domain, and allow maintenance intermediate points to discover maintenance endpoints.
- Link Trace - These are transmitted by a maintenance endpoint on the request of the administrator to track the path (hop-by-hop) to a destination maintenance endpoint. They allow the transmitting node to discover vital connectivity data about the path. Link trace is similar in concept to UDP Traceroute.
- Loopback - These are transmitted by a maintenance endpoint at the request of the administrator to verify connectivity to a particular maintenance point. Loopback indicates whether the destination is reachable or not; it does not allow hop-by-hop discovery of the path. It is similar in concept to ICMP Echo (Ping).

Service OAM Recommendations

The Service OAM feature from Transition Networks supports connectivity fault management (CFM) via both the IEEE 802.1AG and the ITU-T Y.1731 standards, which define protocols and practices for paths through bridges and local area networks.

IEEE 802.1ag defines standardized continuity checks, loopbacks and link trace for fault management capabilities in enterprise and carrier networks. This standard also partitions the network into eight hierarchical administrative domains.

The ITU-T Y.1731 standard is similar to the 802.1ag recommendation, but Y.1731 also defines performance monitoring measurements such as frame loss ratio, frame delay and frame delay variation to assist with SLA assurance and capacity planning. For fault management the standard defines continuity checks, loopbacks, link trace and alarm suppression for effective fault detection, verification, isolation and notification in carrier networks.

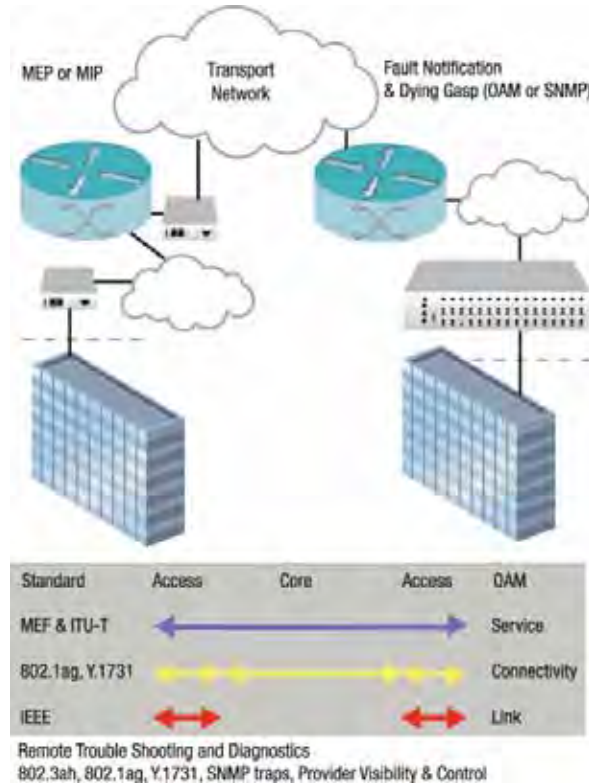


Figure 5: Sample SOAM Application

Maintenance Domains and Maintenance Points

Below are some definitions of terms from the IEEE and ITU standards and recommendations that are used in this section. Note that IEEE and ITU have their own definitions, and areas where they differ are noted.

Connectivity Fault Management (CFM) provides capabilities for detecting, verifying, and isolating connectivity failures in Virtual Bridged LANs.

Continuity Check Message (CCM) is a multicast CFM PDU transmitted periodically by a MEP to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to a received CCM.

Down MEP is a MEP residing in a Bridge that receives CFM PDUs from, and transmits them towards, a LAN. A down MEP sends CCMs away from the MAC Relay Entity.

Section 1: Introduction

Fault Alarm is an out-of-band signal (which can be an SNMP Notification) reporting a connectivity failure.

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

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

Loopback Message (LBM) is a unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR per IEEE. The ITU allows unicast and multicast Loopback messages. The x323x NIDs support both the ITU and the IEEE standards for LBMs.

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

Maintenance Association (MA) is a set of MEPs, each configured with the same MAID and MD Level, used to verify the integrity of a single service instance.

Maintenance association End Point (MEP) is an actively managed CFM entity that generates and receives CFM PDUs and tracks responses. It is an end point of a single MA and is an end point of a separate ME for each of the other MEPs in the same MA. MEPs reside at the edge of a MD, and define its boundaries. MEPs generate and terminate CFM packets. When you create a MEP, you associate it with a specific MD, MA, Ethernet service (EVC), and port number.

Maintenance association End Point Identifier (MEPID) is a small integer, unique over a given MA, which identifies a specific MEP.

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

Maintenance domain Intermediate Point (MIP) is a CFM entity consisting of two MHFs (MIP Half Functions). The MIPs are internal to the Maintenance Association (MA). MIPs forward CFM packets, while MEPs generate and terminate CFM packets. MIPs will respond to a loopback or link trace command. The MIPs in the Operator MAs represent Operator network equipment within their respective Maintenance Associations (MAs).

Maintenance Domain Name is the identifier, unique over the domain for which CFM is to protect against accidental concatenation of service instances, of a particular MD.

Maintenance Entity (ME) is any point-to-point relationship between two MEPs in a single MA.

Maintenance Point (MP) is either a MEP or a MIP. Any port on a Maintenance Association can be assigned as a Maintenance point. A Maintenance point is classified as either a Maintenance End Point (MEP) or a Maintenance Intermediate Point (MIP).

MD Level is a small integer in a field in a CFM PDU that is used, along with the VID in the VLAN tag, to identify to which MD among those associated with the CFM frame's VID, and thus to which MA, a CFM PDU belongs. The MD Level determines the MPs that are a) interested in the contents of a CFM PDU, and b) through which the frame carrying that CFM PDU is allowed to pass.

MEP CCM Database is the database, maintained by every MEP, which maintains received information about other MEPs in the Maintenance Association.

MIP CCM Database is the database, maintained optionally by a MIP or MEP, that maintains received information about the MEPs in the Maintenance Domain.

Operations, Administration, and Maintenance (OAM) is a group of network management functions that provide network fault indication, performance information, and data and diagnosis functions (e.g., IEEE 802.3 Clause 57 OAM).

Passive SAP is a SAP, bounding an MP, which is on the side of the MP away from the monitored MA.

Primary VID is 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.

Service Access Point (SAP) is any point at which a service is offered.

Up MEP is a MEP residing in a Bridge that transmits CFM PDUs towards, and receives them from, the direction of the Bridge Relay Entity. An Up MEP sends CCMs towards the MAC Relay Entity.

The OAM MD, MEP and MIP

Both the IEEE 802.1AG and the ITU-T Y.1731 standards define maintenance points, which are points on an interface that participate in CFM within a Maintenance Domain (MD). A Maintenance Point (MP) drops all lower-level frames and forward all higher-level frames. There are two types of maintenance points:

- **Maintenance end points (MEPs)** – A MEP sends and receives CFM frames through the relay function. It drops all CFM frames of its level or lower that come from the wire side. For CFM frames from the relay side, it processes the frames at its level and drops frames at a lower level. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or wire side.
Up MEPs at the edge of the domain define the boundary and confine CFM messages within these boundaries. ‘Up MEP’ means that it communicates through the relay function side, not the wire side (connected to the port).
- **Maintenance intermediate points (MIPs)** are internal to a domain, not at the boundary, and respond to CFM only when triggered by trace route and loopback messages. They forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level, and forward all CFM frames at a higher level, regardless of whether they are received from the relay or wire side.

Section 1: Introduction

These OAM concepts are depicted in the figure below.

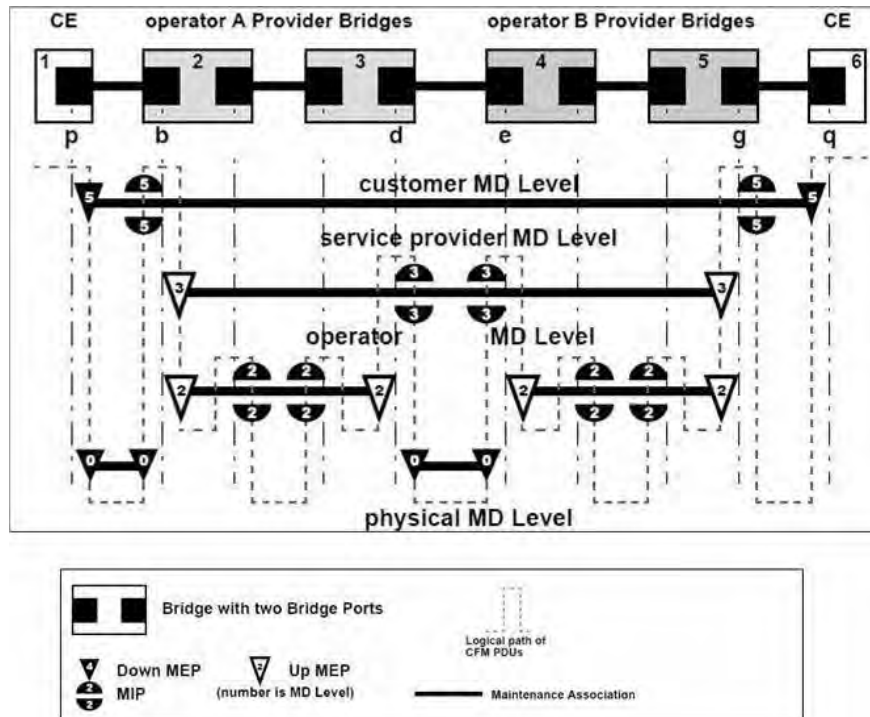


Figure 6: Up / Down MEPs, MIPs, and MD Levels

The MEP functions provided under the IEEE 802.1AG standard include:

- Periodically transmits Continuity Check Messages (CCMs);
- Validates received CFM PDUs;
- Discards those CFM PDUs at a lower MD Level to that configured in the MEP;
- Transmits Loopback Messages (LBMs) and receives Loopback Replies (LBRs);
- Transmits Linktrace Messages (LTMs), and transmits and receives Linktrace Replies (LTRs);
- Responds to LBMs with LBRs;
- Responds to LTMs with LTRs;
- Maintains the MEP CCM Database;
- May maintain the MIP CCM Database; and
- Maintains the variables.

Maintenance Levels and Domains

A service network is partitioned into Customer, Provider, and Operator maintenance levels. Providers have end-to-end service responsibility. Operators provide service transport across a subnetwork. The ETH Layer consists of customer service Ethernet frames that may include both Customer VLAN tags and Provider VLAN tags.

A unique Maintenance Level in the range of 0 to 7 is assigned to each domain by a network administrator. Levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallels the structure of Customer, Service provider, and Operator maintenance levels.

The larger the domain, the higher the Maintenance Level value. A numerically higher MA level corresponds to domains with the greatest physical reach. MA levels 5 through 7 are suggested for customer domains, MA levels 3 and 4 for service provider domains, and MA levels 0 through 2 for operator domains:

<u>MA Level</u>	<u>Reserved for</u>	<u>Size/Reach</u>
5-7	Customer domains	Largest
3-4	Service provider domains	Next largest
0-2	Operator domains	Smallest

For example, a Customer domain would be larger than an Operator domain. The Customer domain may have a Maintenance Level of 7 and the Operator domain may have a Maintenance Level of 0. Typically, Operators would have the smallest domains and Customers the largest domains, with Service provider domains between them in size. All levels of the hierarchy must operate together.

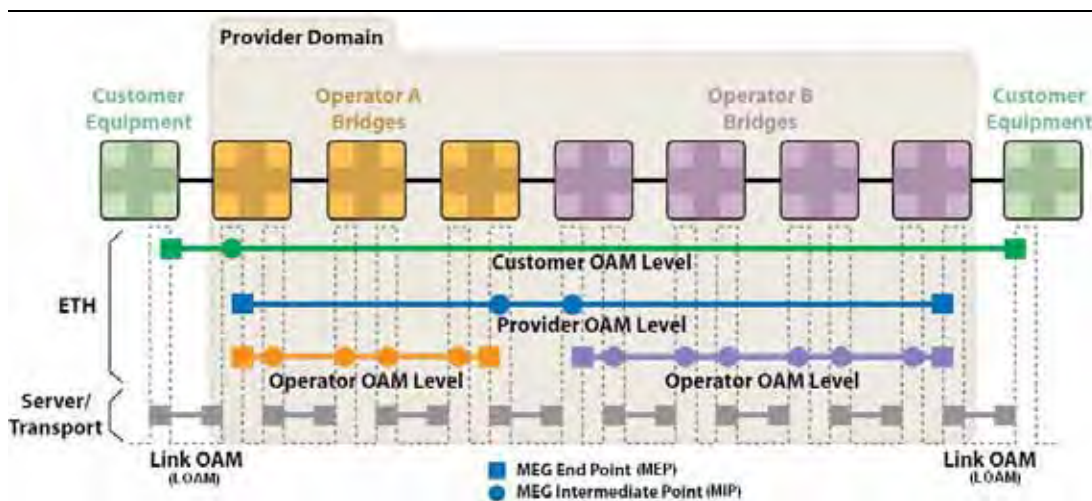


Figure 7: Maintenance Levels and Domains

A Maintenance Domain is a management space for the purpose of managing and administering a network. A Maintenance Domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary.

Domains should not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch, but when two domains nest, the outer domain must have a higher Maintenance level than the domain nested within it. Nesting maintenance domains is useful

Section 1: Introduction

in a business model where a Service provider contracts with one or more Operators to provide Ethernet service to a customer. Each operator would have its own Maintenance Domain and the Service Provider would define its domain—a superset of the Operator domains. Furthermore, the Customer has its own end-to-end domain which is in turn a superset of the Service provider domain. Maintenance levels of various nesting domains should be communicated among the administering organizations. For example, one approach would be to have the Service provider assign Maintenance Levels to Operators.

VLAN Tunneling (802.1q Tunneling)

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

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

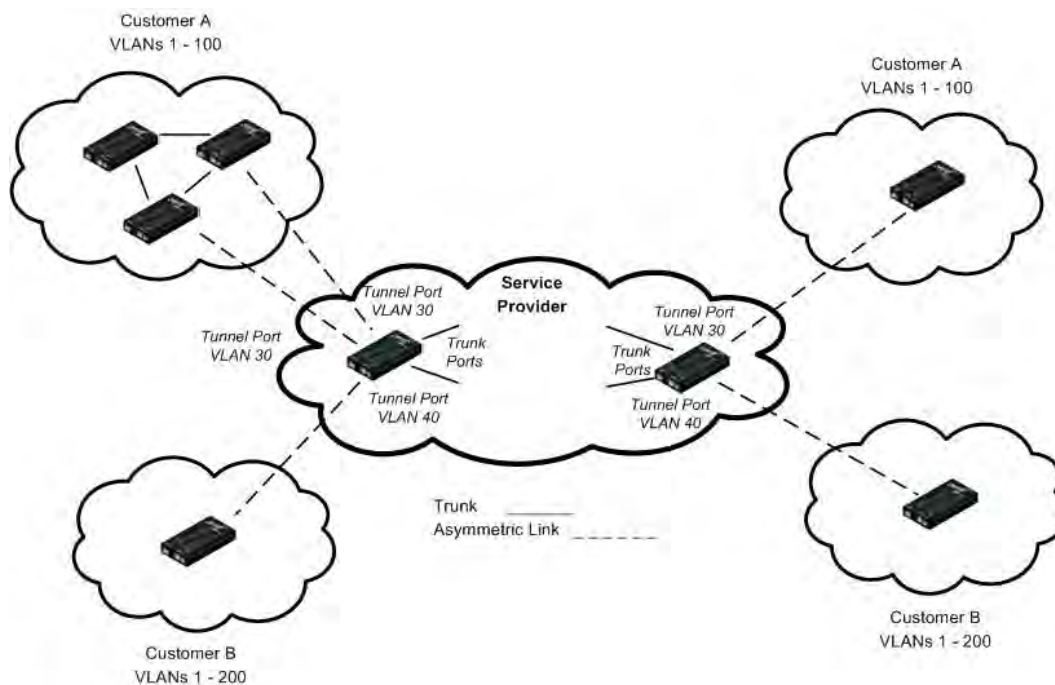


Figure 8: VLAN Tunneling

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

VLAN Tunneling accomplishes the following:

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

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

See “[Configuring VLANs](#)” on page 259 for more information.

L2CP (Layer 2 Control Protocol)

The x323x NIDs support the Layer 2 Control Protocol (L2CP), a network control protocol standardized by the IETF, IEEE and MEF.

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

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

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

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

Device Description / Circuit ID

The x323x supports the Circuit ID, a company-specific identifier assigned by a provider to a data or voice network between two locations. This circuit is then leased to a customer by that ID. If a subscriber has a problem with the circuit, the subscriber contacts the telecom provider with this Circuit ID to initiate service action on the specified circuit. The ION Circuit ID port identifier is based on the agent-local identifier of the circuit (defined in RFC 3046), detected by the agent and associated with a particular port. The x323x supports the Circuit ID, a company-specific identifier assigned by the user to identify the converter and individual ports in any manner desired. At the device level, the x323x supports a 'Device Description' character string entry of up to 64 bytes.

MAC Address Learning

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

System Logging (Syslog)

The x323x supports system logging via the Syslog function. Syslog can be used for system management and security auditing, as well as generalized information, analysis, and message debugging. Since Syslog is supported by a wide variety of devices and receivers across multiple platforms, it is used to integrate log data from many different types of devices into a central repository. The syslog protocol conveys event notification messages using a layered architecture, allowing a variety of transport protocols, and providing a message format of vendor-specific extensions to be provided in a structured way.

The x323x System Log lets you configure the Syslog Server Address, Server Port, Level (one of eight levels of reporting), and logging Mode (local, remote, local and remote, or no logging). A recommended practice is to use the Notice or Informational level for normal messages.

TDM Loopback

This feature lets you define and display the type of loopback for a specified TDM port to either no loopback support or to Phy Layer Loopback support. (This feature depends on factors such as the Link OAM admin state of the remote peer port must be active, the link status must be up, and other issues).

TNDP (TN Topology Discovery Protocol) Disable

The x323x lets you disable the TN Topology Discovery Protocol (TNDP). The TN Topology Discovery Protocol is the Transition Networks implementation of LLDP (Link Layer Discovery Protocol). 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.

RFC 2544 Benchmarking

The x323x supports IETF RFC 2544 (Benchmarking Methodology for Network Interconnect Devices). RFC 2544 defines several tests that can be used to describe the performance characteristics of a network interconnecting device, as well as specific formats for reporting the results of the tests (e.g., throughput, latency, frame loss rate, system recovery). The following RFC2544 testing reports are available for the x323x: Back-to-Back Test Report, Frame Loss Test Report, Latency Test Report, and Throughput Test Report.

SNMP Support

Simple Network Management Protocol (SNMP) is a network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

The IONMM supports three security models: SNMPv1, SNMPv2c, and SBNMv3.

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

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

Both versions (SNMPv1 and SNMPv2) of the Internet Standard Management SNMP Framework share the same basic structure and components, and all versions follow the same architecture. The SNMP framework consists of 1) a data definition language, 2) definitions of management information (the Management Information Base, or MIB), 3) a protocol definition, and 4) security and administration.

SNMPv3 (Simple Network Management Protocol Version 3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.

SNMPv3 provides important security features: 1) Confidentiality - Encryption of packets to prevent snooping by an unauthorized source. 2) Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism. 3) Authentication - to verify that the message is from a valid source.

Section 1: Introduction

WRR or Strict Priority Queuing

The x323x supports WRR (Weighted Round Robin) or “Strict” Egress Queue modes.

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

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

Serial File Transfer (X/Y/Zmodem)

The x323x supports serial get, put, and upgrade commands using the Xmodem, Xmodem-1k, Ymodem, and Zmodem protocols. These commands function similar to the TFTP download function; technical support can download configuration files and firmware files through the x323x USB port by entering the corresponding CLI commands.

Supported MIBs

The x323x supports public (standard) and private Management Information Bases (MIBs).

Public MIBs

The x323x provides complete management through the SNMP interface. It supports the following standard MIBs for management using SNMPv1/v2 as shown in the table below.

Private MIBs

The Transition Networks private MIBs for SNMP IP-based management feature extensive management options as shown in the table below.

Table 1: Supported MIBs

#	MIB	RFC # or Private	Description
1	BRIDGE-MIB	RFC4188	Bridge MIB module for managing devices that support IEEE 802.1D
2	DOT3-OAM-MIB	RFC4878	MIB module for managing the new Ethernet OAM features introduced by the Ethernet in the First Mile taskforce (IEEE 802.3ah)
3	ENTITY-MIB	RFC 4133	MIB module for representing multiple logical entities supported by a single SNMP agent
4	ENTITY-SENSOR-MIB	RFC 3433	Defines Entity MIB extensions for physical sensors
5	EtherLike-MIB	RFC3635	Describe generic objects for Ethernet-like network interfaces
6	IANA-MAU-MIB	RFC 4836	Defines dot3MauType OBJECT-IDENTITIES and IANAifMauListBits, IANAifMauMediaAvailable, IANAifMauAutoNegCapBits, and IANAifJackType
7	IEEE8021-CFM-MIB	RFC _____	Connectivity Fault Management module for managing IEEE 802.1ag
8	IEEE8021-TC-MIB	RFC _____	Textual conventions used throughout the various IEEE 802.1 MIB modules
9	IF-MIB	RFC 2863	Describes generic objects for network interface sub-layers
10	MAU-MIB	RFC 4836	Management information for 802.3 MAUs
11	P-BRIDGE-MIB	RFC 4363	Module for managing Priority and Multicast Filtering
12	Q-BRIDGE-MIB	RFC 4363	Module for managing Virtual Bridged LANs
13	RFC1213-MIB (MIB-II)	RFC 1213	Defines the second version of the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets
14	RMON-MIB	RFC 1757	Defines objects for managing remote network monitoring devices (i.e., monitors or probes)
15	TRANSITION-SMI	Private	Transition Networks Enterprise Structure of Management Information; assigns ION platform module identities

Section 1: Introduction

16	TRANSITION-TC	Private	Transition Networks Inc MIB Textual Conventions module; defines textual conventions used in the Transition enterprise MIBs
17	TN-ION-BPC-MIB	Private	Transition Networks, Inc. Enterprise MIB for Chassis Management).
18	TN-ION-CHASSIS-MIB	Private	Transition Networks, Inc. Enterprise MIB for Chassis Management
19	TN-ION-MGMT-MIB	Private	Transition Networks, Inc. Enterprise MIB for basic management of the ION Platform
20	TN-PROV-BRIDGE-MIB	Private	Transition Networks, Inc. Enterprise MIB for IEEE Bridge provisioning, i.e., IEEE MAC/VLAN bridges
21	TN-ION-VLAN-MGMT-MIB	Private	Transition Networks, Inc. Enterprise module for managing VLAN and QoS in ION platform products
22	TN-ION-LOAM-EXT-MIB	Private	Transition Networks, Inc. module for managing Link OAM (IEEE 802.3ah Clause 57) enterprise extensions in ION platform products
23	TN-ION-SOAM-EXT	Private	Module that extends the support of standard IEEE 802.1ag MIB for Service OAM functionality, including ITU-T Y.1731 entities
24	TN-ION-SOAM-IDX-MIB	Private	Module for managing SOAM enterprise extensions in ION platform products
25	TN-ION-ENTITY-SENSOR-MIB	Private	Transition Networks, Inc. module for managing all ION power supply and fan modules)
26	ION-DEV-SYS-ACL-MIB	Private	Transition Networks Enterprise MIB for ION device ACL feature
27	ION-DEV-SYS-HTTPS-MIB	Private	Transition Networks Enterprise MIB for ION device HTTPS feature
28	ION-DEV-SYS-IPMGMT-MIB	Private	Transition Networks Enterprise MIB for ION device IP management feature
29	ION-DEV-SYS-PROV-MIB	Private	Transition Networks Enterprise MIB for ION device Provision feature
30	ION-DEV-SYS-RADIUS-MIB	Private	Transition Networks Enterprise MIB for ION device RADIUS management feature
31	ION-DEV-SYS-SNMPMGMT-MIB	Private	Transition Networks Enterprise MIB for ION device SNMP management feature
32	ION-DEV-SYS-SNTP-MIB	Private	Transition Networks Enterprise MIB for ION device SNTP management feature
33	ION-DEV-SYS-SSH-MIB	Private	Transition Networks Enterprise MIB for ION device SSH feature
34	ION-DEV-SYS-STATE-MIB	Private	Transition Networks Enterprise MIB for ION device state
35	ION-DEV-SYS-TFTP-MIB	Private	Transition Networks Enterprise MIB for ION device TFTP feature
36	ION-DEV-SYS-UPGRADER-MIB	Private	Transition Networks Enterprise MIB for ION device upgrader feature

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

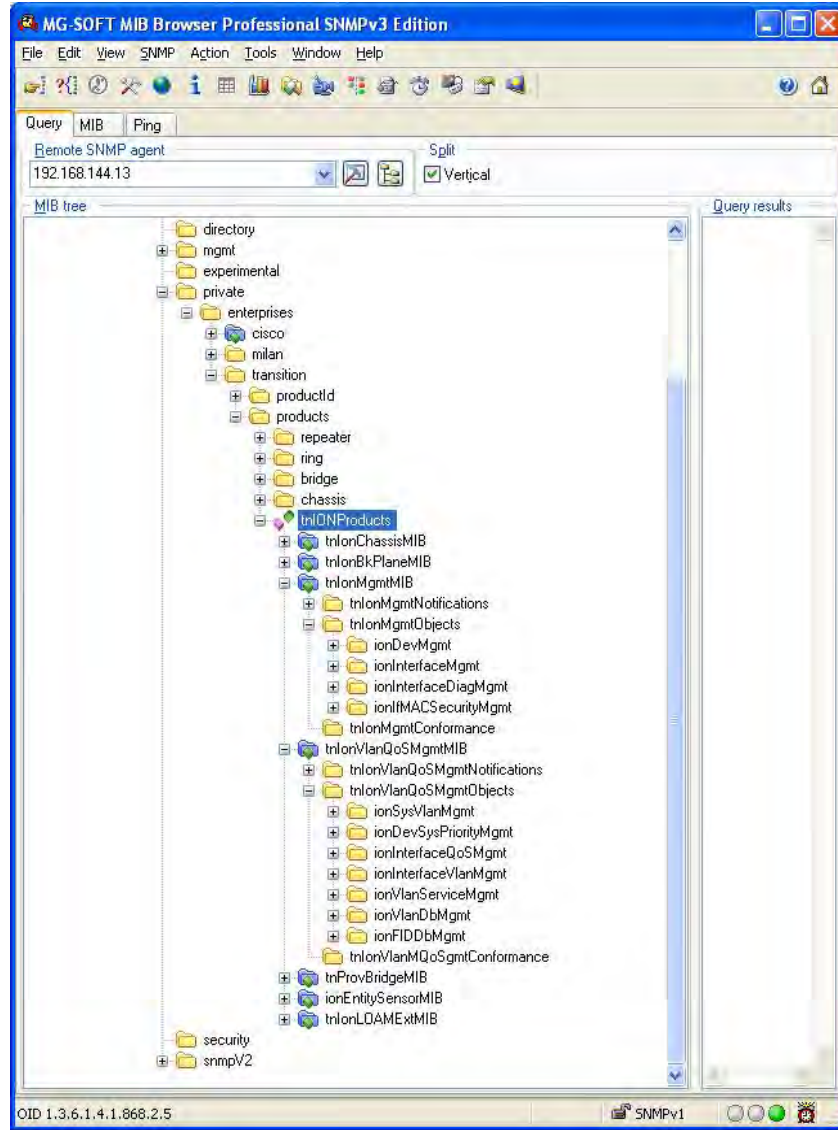


Figure 9: Private MIB Objects

Downloading, Compiling and Integrating MIBs

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

To download ION system private MIBs:

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

Set up your ION system SNMP configuration via the command line interface (CLI). Refer to “[Configuring SNMP](#)” on page 214. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.

For Additional MIB Information

For information on traps that the IONMM supports, see “[Appendix G: SNMP Traps Supported](#)” on page 543.

For more information on the SNMP Agent, Network Management Station (NMS), MIBs, MIB modules and MIB Variables, the Object ID (OID), the MIB Tree / branch /node, MIB Table Indices, values, notations and transaction types, etc., see the SNMP Primer at <http://www.transition.com/pshelp/snmp.html#indices>

NID Models

The various x323x NID models are described in Table 1: Standard Models and Table 2: Single Fiber Models below.

Standard Models

Note: the -D after the model number indicates DMI option support. The asterisk (*) indicates x3230-1040 and x3231-1040 support of Service OAM (SOAM).

Table 2: Standard Models

Model	Port 1: Copper	Port 2: Fiber
x3230-1013 x3230-1013-D	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-SX 850nm MM (SC) Max distance: 62.5/125 μ m fiber: 220 m (722 ft) 50/125 μ m fiber: 550 m (1804 ft) Link Budget: 8.5 dB
x3230-1014 x3230-1014-D	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1310nm SM (SC) Max distance: 10 km (6.2 mi.) Link Budget: 16.0 dB
x3230-1015 x3230-1015-D	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1310nm SM (SC) Max distance: 30 km (18.6 mi.) Link Budget: 15.0 dB
x3230-1017	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1550nm SM (SC) Max distance: 80 km (49.7 mi.) Link Budget: 21.0 dB
x3230-1035	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1550nm SM (SC) Max distance: 120 km (77.7 mi.) Link Budget: 27.0 dB
*x3230-1040	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	100/1000Base-X One open SFP Slot
*x3231-1040	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	100/1000Base-X Two open SFP Slots

Section 1: Introduction

Single Fiber Models

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

The x323x NID Single Fiber Models are described below.

Table 3: Single Fiber Models*

Model	Port 1: Copper	Port 2: Fiber
x3230-1029-A1 x3230-1029-DA1	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1310nm TX / 1490 nm RX (SC) Max distance: 20 km (12.4 mi.) Link Budget: 11.0 dB
x3230-1029-A2 x3230-1029-DA2	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1490nm TX / 1310 nm RX (SC) Max distance: 20 km (12.4 mi.) Link Budget: 11.0 dB
x3230-1029-B1	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1310nm TX / 1490 nm RX (SC) Max distance: 40 km (24.8 mi.) Link Budget: 20.0 dB
x3230-1029-B2	10/100/1000BASE-T (RJ-45) Max distance: 100 m (328 ft)	1000BASE-LX 1490nm TX / 1310 nm RX (SC) Max distance: 40 km (24.8 mi.) Link Budget: 20.0 dB

*It is recommended these Single Fiber Models be used in pairs.

Physical Specifications

The physical specifications for the chassis slide-in modules are described in Table 4 and for the standalone models in Table 5.

Chassis Model Specifications

Table 4: Physical Specification for Chassis Models

Standards	IEEE Std. 802.3, IEEE Std. 802.3ah, IEEE Std 802.1P, IEEE Std 802.1Q
Data Rate	Copper: 10/100/1000Mbps Fiber: 1000Mbps
Filtering Addresses	8K MAC Addresses
Max Frame Size	10,240 bytes
Dimensions	Width: 0.86 in. (22 mm) Depth: 6.5 in. (165 mm) Height: 3.4 in. (86 mm)
Power Consumption	4.5 Watts
Environment	See chassis specifications
Shipping Weight	1 lb (0.45 kg)
Regulatory Compliance	EN55022 class A, EN55024, CE Mark
Warranty	Lifetime

Standalone Model Specifications

Table 5: Physical Specifications for Standalone Models

Standards	EEE Std. 802.3, IEEE Std. 802.3ah, IEEE Std 802.1P, IEEE Std. 802.1Q
Data Rate	Copper: 10/100/1000Mbps Fiber: 1000Mbps
Filtering Address	8K MAC Addresses
Max Frame Size	10,240 bytes
Dimensions	Width: 3.25 in. (82 mm) Depth: 6.5 in. (165 mm) Height: 1.0 in. (25 mm)
Power	Input:100-240VAC,1A Output: 12VDC, 1.25A
Operating Temperature	32°F to 122°F (0°C to 50°C)
Altitude	0-10,000 ft.
Operating Humidity	5-95% (non-condensing)
Shipping Weight	2.0 lbs (0.90 kg)
Regulatory Compliance	EN55022 Class A, EN55024, UL60950, CE Mark
Warranty	Lifetime

Documentation Conventions

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

Table 6: Documentation Conventions

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

Related Manuals and Online Help

A printed documentation card is shipped with each x323x. Context-sensitive Help screens and cursor-over-help (COH) facilities are built into the Web interface. A substantial set of technical documents, white papers, case studies, etc. are available on the Transition Networks web site at www.transition.com.

The ION system and related device manuals are listed below.

1. ION System x323x Remotely Managed NID User Guide, 33432 (this manual)
2. ION Management Module (IONMM) User Guide, 33457
3. ION Systems CLI Reference Manual, 33461
4. ION219-A 19-Slot Chassis Installation Guide, 33412
5. IONADP Installation Guide, 33413
6. ION Dry Contact Relay (DCR) Kit Install Guide, 33422
7. IONPS-A AC Power Supply Install Guide, 33423
8. IONPS-D DC Power Supply Install Guide, 33424
9. IONFM Fan Module Install Guide, 33425
10. IONPS-A ION AC Power Supply Install Guide, 33464
11. ION System x6010 Managed T1/E1-to-Fiber NID User Guide, 33493
12. E-MCR-05 Media Converter Rack User's Guide, 33392
13. SFP manuals (product specific)
14. Release Notes (firmware version specific)
15. Product Documentation Postcard, 33504

This manual provides 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.

Section 2: Installation and System Setup

General

This section describes how to install the x323x and the procedures to access and initially set up the NID through either a local serial interface (USB) or a remote Ethernet connection (Telnet session or Web interface).

Installing the Chassis Model (C323x)

The C323x is a slide-in module that can only be installed in a Transition Networks ION chassis (ION001-x and ION219-x). For a complete list of ION platform products, go to the Transition Networks website at: <http://www.transition.com>.

The following describes how to install the C323x in the ION chassis.



Caution: Failure to wear a grounding device and observe electrostatic discharge precautions when installing the C323x could result in damage or failure of the module.

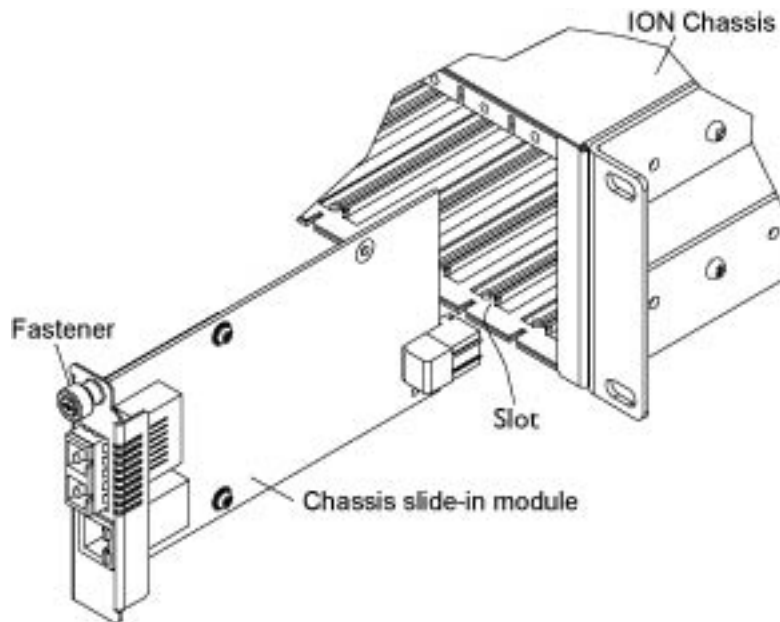


Figure 10: Chassis Installation

Section 2: Installation and System Setup

IMPORTANT

The C323x slide-in card is a “hot swappable” device, and can be installed with chassis power on.

1. Locate an empty slot in the ION System chassis.
2. Grasp the edges of the card by its front panel.
3. Align the card with the upper and lower slot guides, and carefully insert the card into the installation slot.
4. Firmly seat the card against the chassis back panel.
5. Push in and rotate clockwise the panel fastener screw to secure the card to the chassis (see [Figure 10: Chassis Installation](#) on the previous page).
6. Note that the card’s Power LED lights. See [Accessing the NIDs](#) on page 39.

Installing the Standalone Model (S323x)

The standalone model can be installed in any of the following ways.

- Rack mounted
- Table top
- Wall mounted

Rack Mount Installation

The S323x standalone module can be mounted into a Transition Networks E-MCR-04 media converter rack, which can be installed on a tabletop or in a standard site rack. For installation details, see the *E-MCR-04 Media Converter Rack User Guide, 33297*.

Tabletop Installation

The S323x is shipped with four rubber feet for optional installation on a table or other flat, stable surface in a well-ventilated area.

1. Remove the [rubber](#) feet from the card.
2. On the bottom of the NID, place one rubber foot in each corner of the NID.

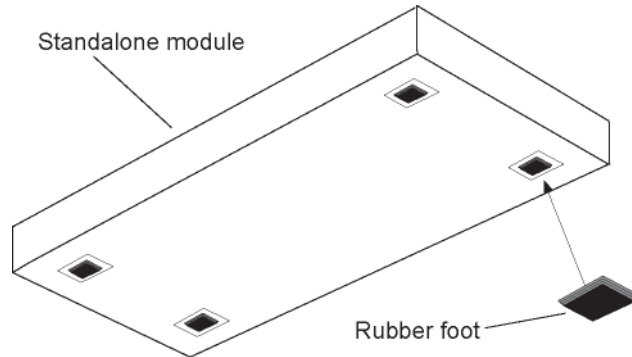


Figure 11: Tabletop Installation

3. Set the NID in place and connect the AC power adapter (see [Connecting to AC Power](#) on page 39).

Wall Mount Installation

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

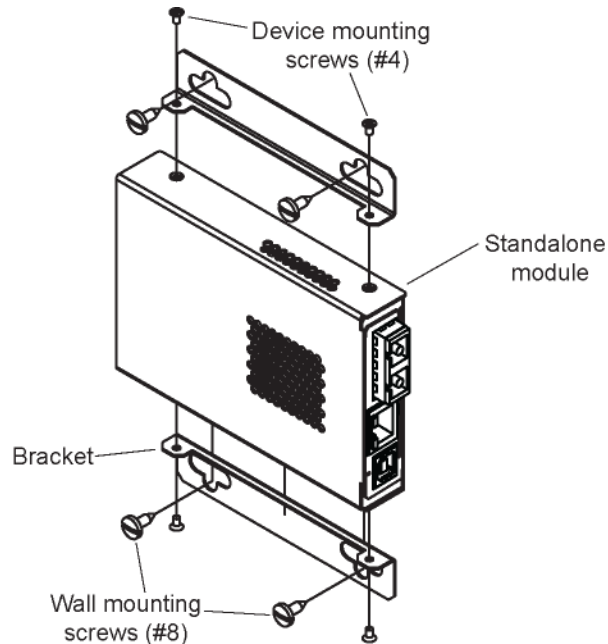


Figure 12: Wall Mount Installation

2. Mount one of the bracket assemblies to the device using two of the #4 Philips head screws.
3. Mount the other bracket assembly to the other side of the device using the other two #4 Philips head screws.
4. Position the device on the mounting surface.
5. Use the four #8 screws to mount the bracket to the mounting surface.
6. Connect the AC power adapter (see [Connecting to AC Power](#) on page 39).

Connecting to AC Power

After the standalone NID has been installed, connect the module to the AC power supply that shipped with the x323x (TNPN 25025).



Warning: Risk of electrical shock.

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

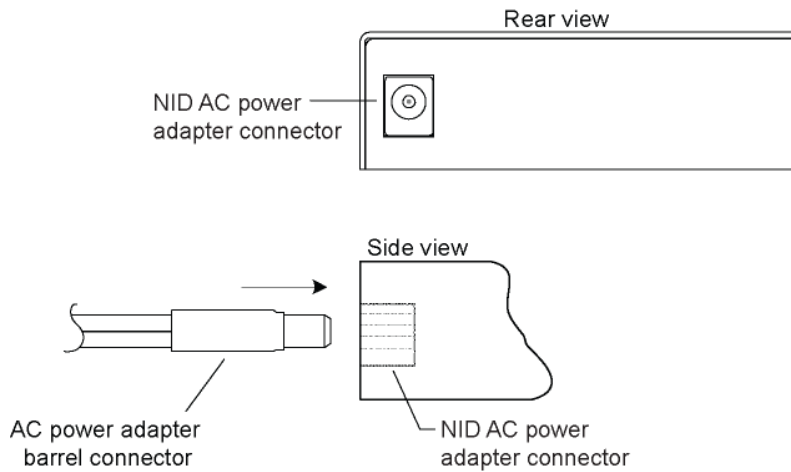


Figure 13: AC Power Connection

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

Installing SFPs

Some models allow you to install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection. The C3230-1040 and S3230-1040 have a single SFP port. The C3231-1040 and S3231-1040 have two SFP ports.

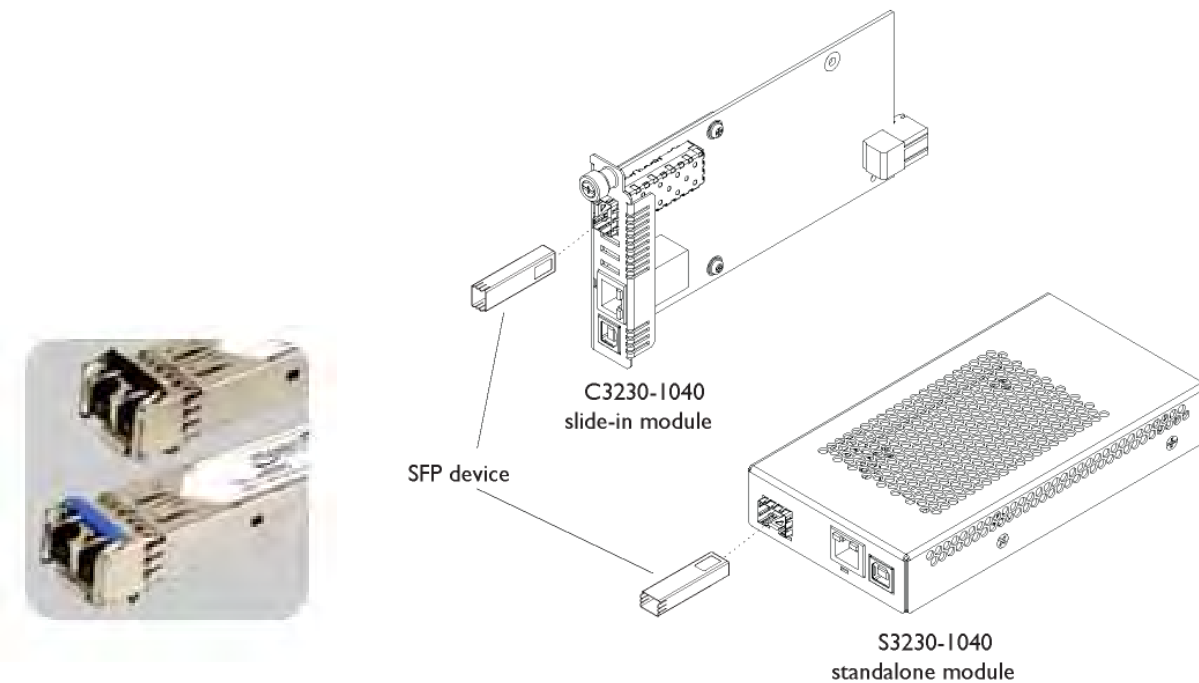


Figure 14: SFP Installation

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

Connections and LEDs

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

Model x3230-1040

The x3230-1040 connectors and LEDs are shown in the two figures below, and described in Table 7.

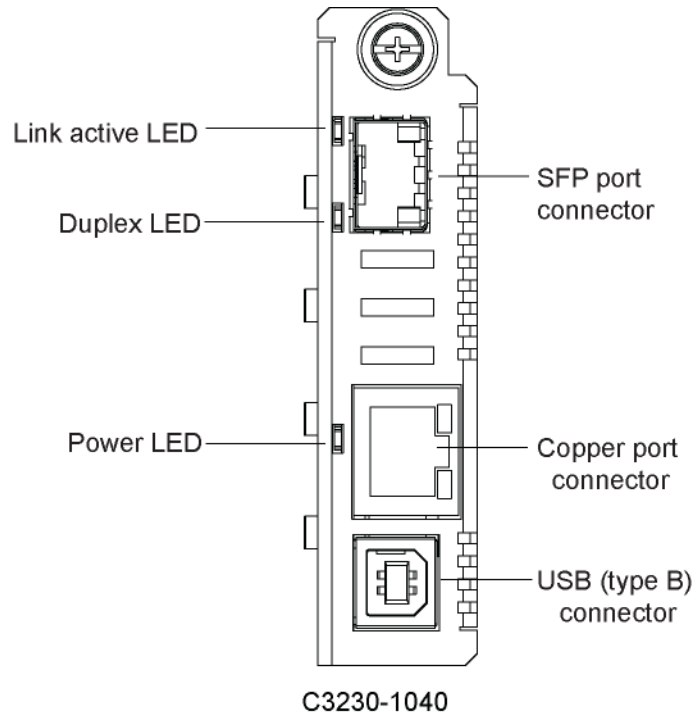


Figure 15: Model C3230-1040 Connectors and LEDs

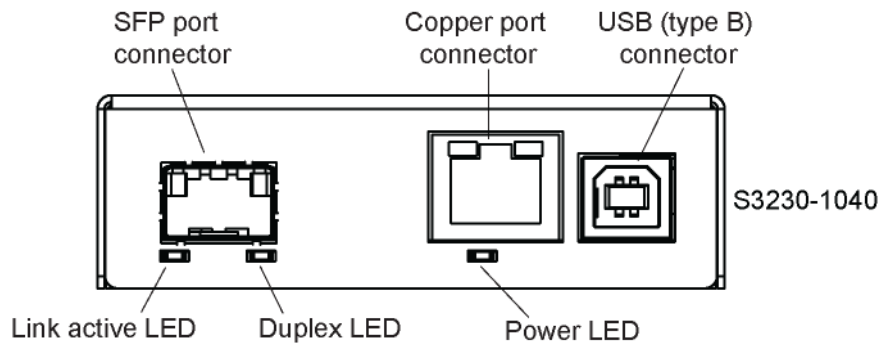


Figure 16: Model S3230-1040 Connectors and LEDs

Section 2: Installation and System Setup

The x3230-1040 connectors and LEDs are described in the table below.

Table 7: Model x3230-1040 Connectors and LED Descriptions

Connector/LED	Description
SFP port connector	Allows you to install a Small Form-Factor Pluggable (SFP) device of your choice in order to make a fiber connection.
USB connector	Used to connect the NID to a PC for a direct serial interface. Through this connection, a system administrator can access and control the NID using CLI commands.
10/100/1000 (Copper port) connector	One connector for Ethernet 10/100/1000 Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either remote Telnet session or the Web interface.
PWR (Power) LED	When lit, indicates that there is power to the NID.
LACT (Link active) LED	Yellow – operation is 10 MBps (10Base-T). Green – operation is 100 MBps, 100Base-T.
DUP (Duplex) LED	When lit, indicates duplex mode: <ul style="list-style-type: none"> • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Model x3231-1040

The x3230-1040 connectors and LEDs are shown in the two figures below, and described in Table 7.

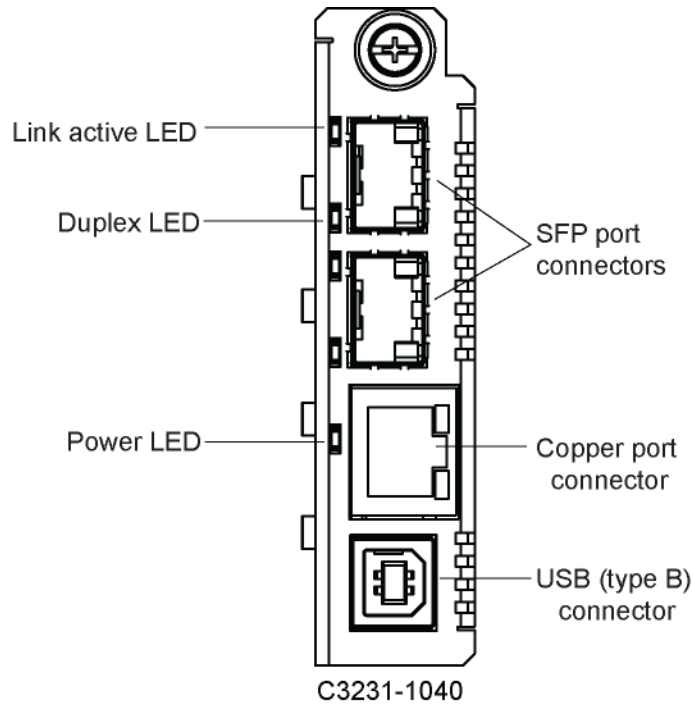


Figure 17: Model C3231-1040 Connectors and LEDs

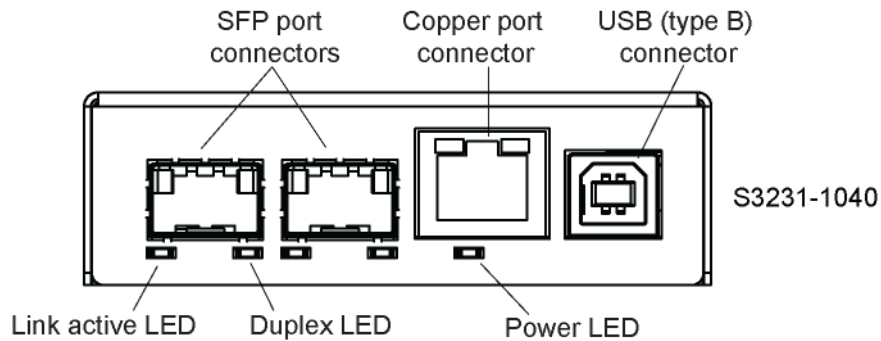


Figure 18: Model S3231-1040 Connectors and LEDs

Section 2: Installation and System Setup

The x3231-1040 connectors and LEDs are described in the table below.

Table 8: Model x3231-1040 Connectors and LED Descriptions

Connector/LED	Description
SFP port connectors	Allows you to install Small Form-Factor Pluggable (SFP) device(s) of your choice in order to make a fiber connection.
USB connector	Used to connect the NID to a PC for a direct serial interface. This connection lets a system administrator access and control the NID using CLI commands.
10/100/1000 (Copper port) Network connectors	One connector for Ethernet 10/100Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either remote Telnet session or the Web interface.
PWR (Power) LED	When lit, indicates that there is power to the NID.
LACT (Link active) LED	Yellow – operation is 10 MBps, 10Base-T. Green – operation is 100 MBps, 100Base-T.
DUP (Duplex) LED	When lit, indicates duplex mode: <ul style="list-style-type: none"> • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Model x3230-10xx

The x3230-1040 connectors and LEDs are shown in the two figures below and described in Table 8.

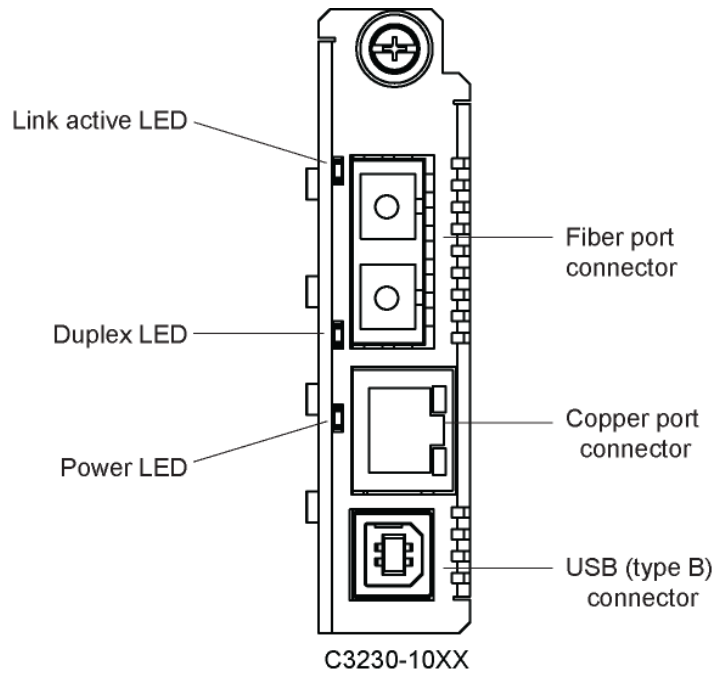


Figure 19: Model C3230-10xx Connectors and LEDs

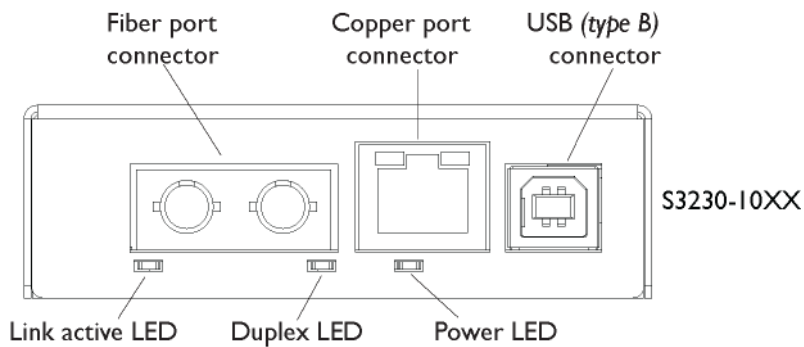


Figure 20: Model S3230-10xx Connectors and LEDs

Section 2: Installation and System Setup

The x3230-10xx connectors and LEDs are described in the table below.

Table 9: Model x3230-10xx Connectors and LED Descriptions

Connector/LED	Description
Fiber port connector	Used to connect the NID to a device (switch, router, NID, etc.).
USB connector	Used to connect the NID to a PC for a direct serial interface. Through this connection a system administrator can access and control the NID using CLI commands.
10/100/1000 (Copper port) Network connectors	One connector for Ethernet 10/100Base-T. The RJ-45 connectors allow the network administrator to manage the chassis through a remote computer using either a remote Telnet session or the Web interface.
PWR (Power) LED	When lit, indicates that there is power to the NID.
LACT (Link active) LED	Yellow – operation is 10 MBps, 10Base-T. Green – operation is 100 MBps, 100Base-T.
DUP (Duplex) LED	When lit, indicates duplex mode: <ul style="list-style-type: none"> • Yellow – half-duplex • Green – full duplex Blinking indicates link activity.

Operating Systems Supported

The following USB drivers are provided with the ION system on a CD, and are also available at <http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>:

Windows [®] 7	Windows 7 x64	Windows XP [®] 32 bit
Windows 2000	Windows 2003 32 bit	Windows Vista [®]
Windows Vista x64	Windows XP 64 bit	

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

The x323x provides a USB Type B connector that can be used as a virtual COM port for accessing the x323x command line interface (CLI).

Installing the USB Driver (Windows XP)

IMPORTANT

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

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

1. Extract the driver (from the provided CD or from the [website](#)) and place it in an accessible folder on the local drive of the PC.
2. Connect the NID to the USB port on the PC.

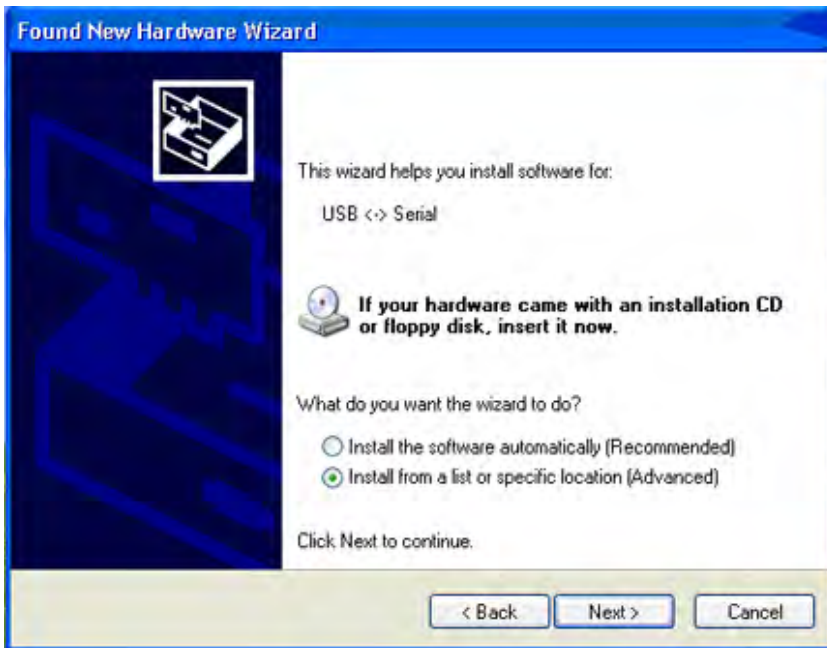
Note: for slide-in modules installed in an ION Chassis, the USB connection will be made to the ION Management Module (IONMM) if one is installed in the chassis.

The *Welcome to the Found New Hardware Wizard* window displays.



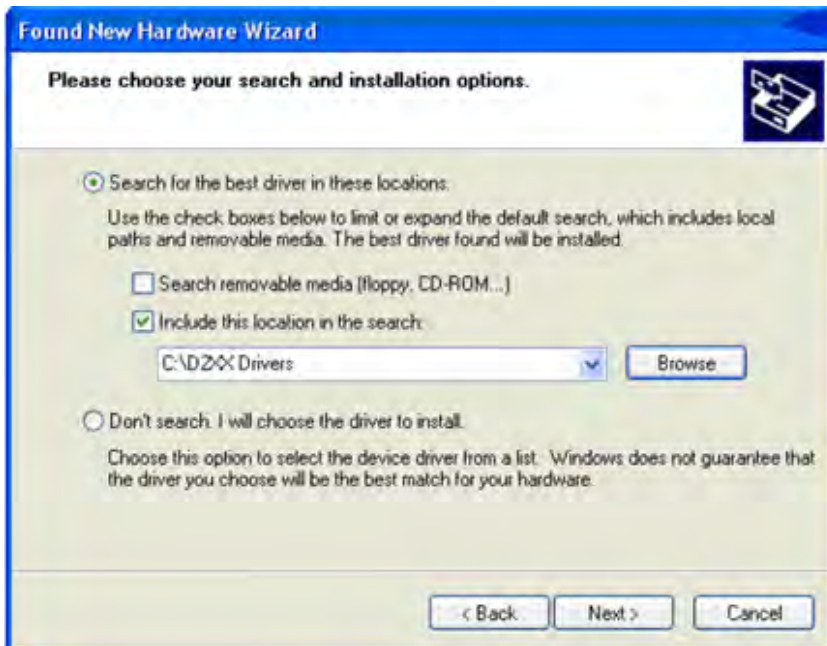
3. Select **No, not this time**.
4. Click **Next**.

The installation options window displays.



5. Select **Install from a list or specific location (Advanced)**.
6. Click **Next**.

The driver search installation options window displays.



7. Click **Browse**.

Section 2: Installation and System Setup

8. Locate and select the USB driver downloaded in step 1 above.
9. Click **Next**.

Driver installation begins.

10. When the finished installing screen displays, click **Finish**.

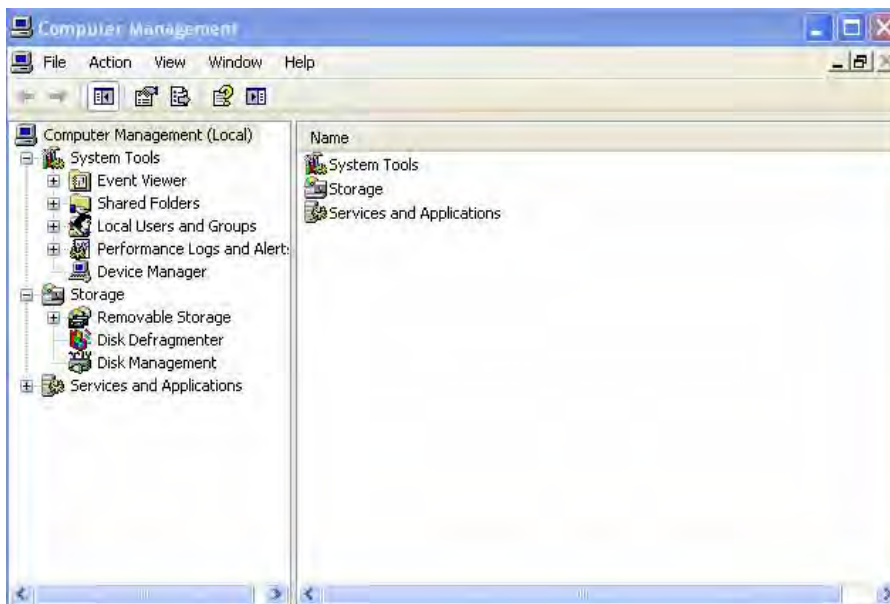
The USB driver installation is complete. You must now configure the COM port to be used by the terminal emulator.

Configuring HyperTerminal

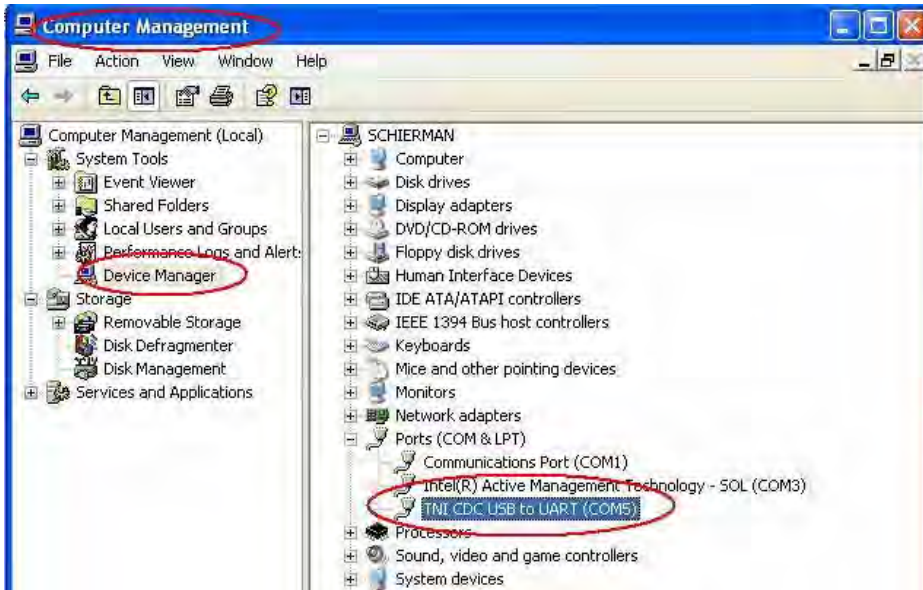
After the USB driver has been installed, you must set up the terminal emulator software (e.g., HyperTerminal) to use the USB COM port.

1. On the desktop, right-click on **My Computer**.
2. Select **Manage**.

The **Computer Management** window displays.



3. Click on **Device Manager** to open the Device Manager panel. (If a Device Manager message displays, click **OK** and continue.)



4. In the right panel, expand the list for **Ports (COM & LPT)**.

Write down the USB COM port number for the “*TNI CDC USB to UART*” listing (**COM5** in the example above). You will need to provide this COM port number in step 8 below.

5. Launch the HyperTerminal software.
 - a) Click **Start**.
 - b) Select: **All Programs > Accessories > Communications**
 - c) Click **HyperTerminal**.

The Connection Description window displays.



Section 2: Installation and System Setup

6. Type in a name and select an icon that will be used for this connection.
7. Click **OK**.

The **Connect To** window displays.



8. From the drop-down list in the **Connect using** field, select the COM port noted in step 4.
9. Click **OK**.

The **Port Settings** window displays.

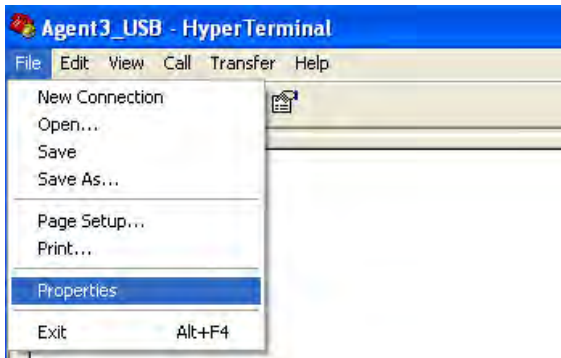


10. Set the COM port properties as follows:

- Bits per second: **115200**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**
- Flow control: **None**

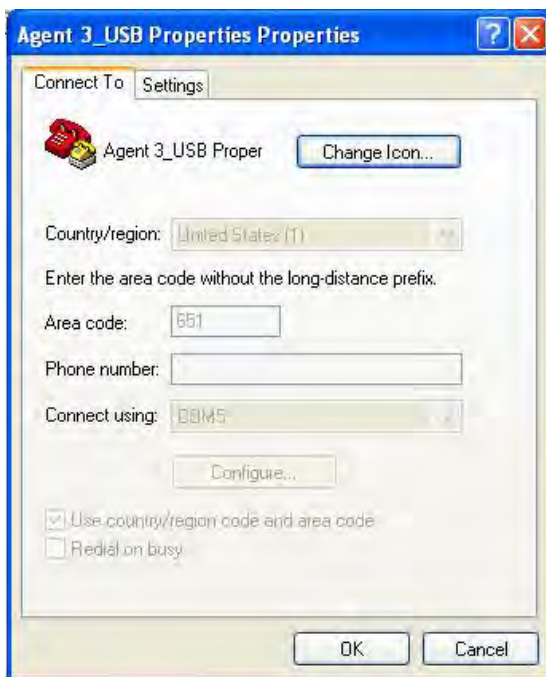
11. Click **OK**.

A blank HyperTerm window displays.



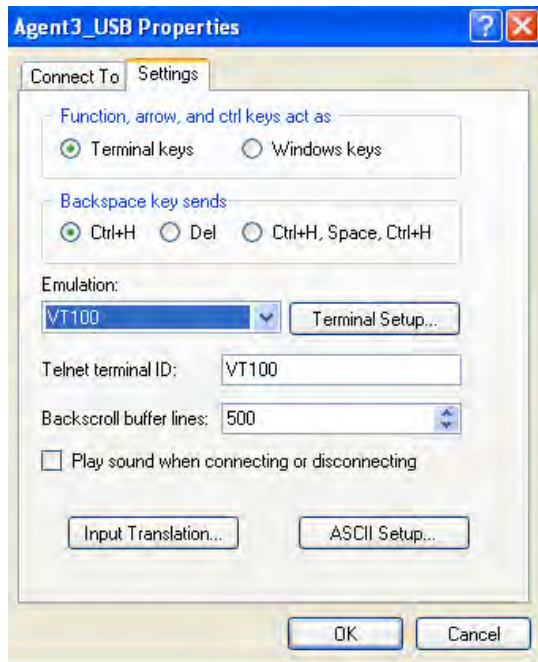
12. In the HyperTerm window, select **File > Properties**.

The Properties window displays the **Connect To** tab.



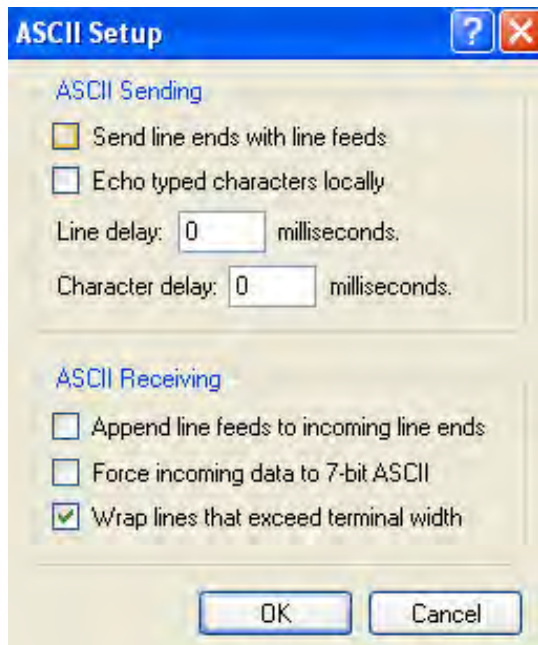
Section 2: Installation and System Setup

13. Click the **Settings** tab.



14. In the **Emulation** field, select **VT100**.

15. Click the **ASCII Setup...** button.



16. Verify that **Wrap lines that exceed terminal width** is selected.

17. Click:

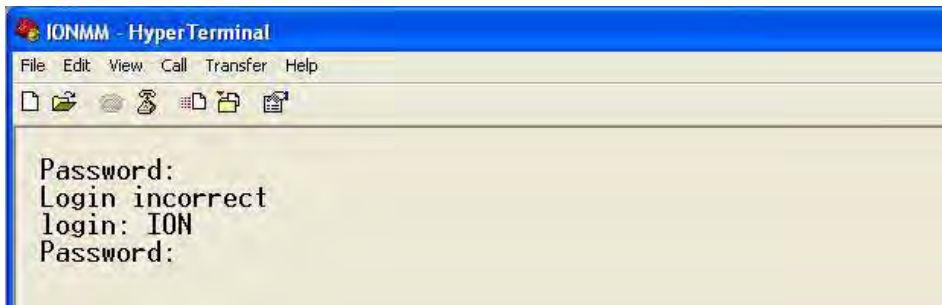
- **OK**
- **OK**

18. Login (see [Starting a USB Session](#) below).

Starting a USB Session in HyperTerminal

The procedure below describes how to access the x323x via a USB connection. The x323x can be controlled from a remote management station via a HyperTerminal session over an Ethernet connection. The x323x is controlled and configured through CLI commands. Use the following procedure to connect to and access the x323x via a HyperTerminal (HT) session.

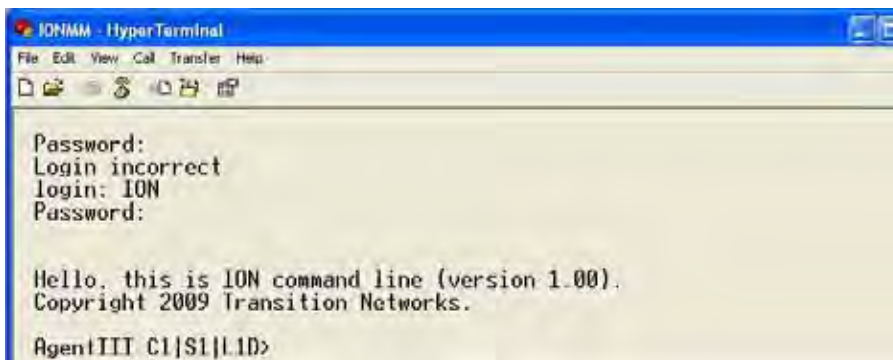
1. Click Windows **Start**.
2. Select **All Programs > Accessories > Communications > HyperTerminal**.
3. Create a new HT connection (select **File > New**) or select an existing connection (**File > Open**).
4. Press the **Enter** key. The Password prompt displays. If “*Login incorrect*” displays, ignore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



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

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

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



Section 2: Installation and System Setup

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

Agent III C1|S1|L1D>
```

7. Continue by entering ION CLI commands to the right of the > symbol. Press the **Enter** key after each command.
8. If the NID controlled by the IONMM, go to step 9. Otherwise continue with step 10.
9. Enter a **go** command to change the location for the command prompt. The **go** command format is:
go[c=<1-16>][s=<1-32>][l1ap=<1-15>][l2ap=<1-15>](l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
 (for a slide in card), or
go[c=<0-16>][s=<0-32>][l1ap=<1-15>][l2ap=<1-15>](l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
 (for a standalone card).
10. Enter commands to set up the various configurations for the NID. For configuration information, see “[Section 4: Configuration](#)” on page 87. For a description of all available CLI commands see the *ION Systems CLI Reference Manual, 33461*.

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

Terminating a USB Connection from HyperTerminal

To terminate the USB connection, do the following.

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

Access via an Ethernet Network

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

IMPORTANT

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

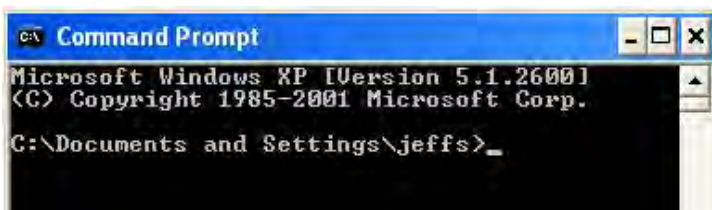
Otherwise, in order to communicate with the NID across the network for the first time, you must change the network settings (IP address, subnet mask and default gateway address) of your PC to coincide with the defaults of the NID (see “[Appendix B: Factory Defaults](#)” on page 179).

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

Starting a Telnet Session

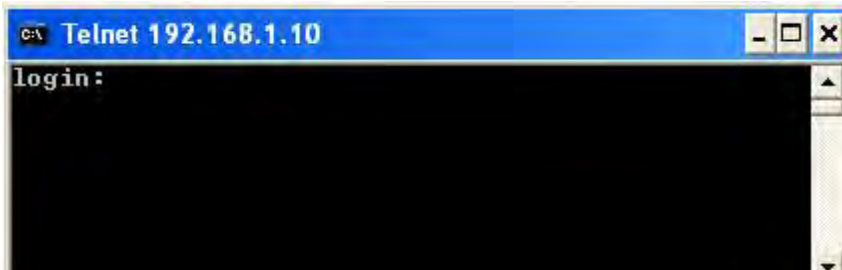
The NID can be controlled from a remote management station via a Telnet session over an Ethernet connection. The NID is controlled and configured through CLI commands. Use the following procedure to connect to and access the NID via a Telnet session.

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



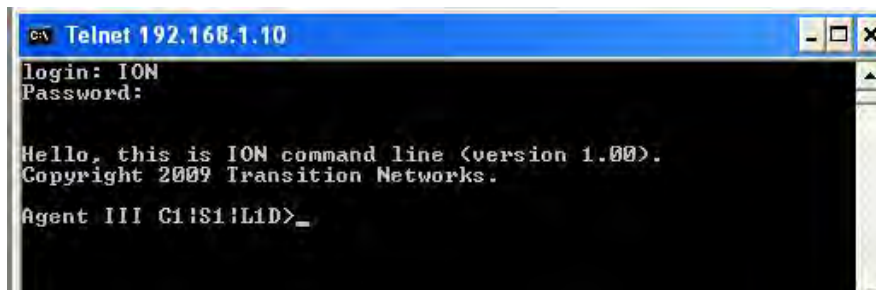
4. At the command line type: **telnet <xx>**
 where:
 xx = the IP address of the NID (e.g., 192.168.1.10).
5. Press **Enter**. The login prompt displays.

Section 2: Installation and System Setup



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

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



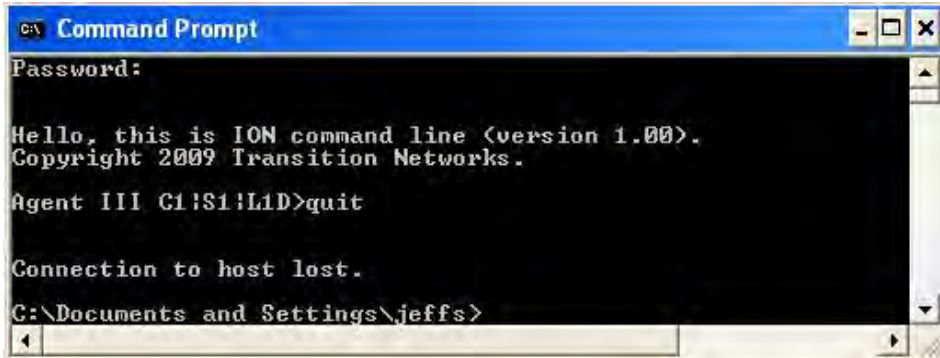
10. If the NID is controlled by the IONMM, go to step 11.
If the NID is not controlled by the IONMM, go to step 12.
11. Enter a **go** command to change the location for the command prompt. The **go** command format is:
go [c=<1-16>][s=<1-32>][l1ap=<1-15>][l2ap=<1-15>](l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
(for a slide in card), or
go [c=<0-16>][s=<0-32>][l1ap=<1-15>][l2ap=<1-15>](l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
(for a standalone card).
12. Enter commands to set up the various configurations for the NID. For configuration information, see [Section 4: “Configuration”](#) on page 55. For a description of all available CLI commands see the *ION Systems CLI Reference Manual, 33461*.

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

Terminating a Telnet Session

To terminate the Telnet session:

1. Type **quit** (or just “q”).
2. Press the **Enter** key.



The message “Connection to host lost.” displays and the command prompt displays.

Initial Setup with a Static IP Address via the CLI

The x323x supports IPv4-based application protocols. The x323x can be assigned IP address statically or dynamically using DHCP. The x323x supports DNS, which lets you assign it a hostname instead of an IP address. The static IP address assignment is part of the initial x323x 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 x323x 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).

The following procedure is for setting a static IP address for the x323x NID. When this procedure is completed, you can then communicate with the x323x across the network via either a Telnet session or the Web interface.

1. Start a USB session (see “Starting a USB Session” on page 48).
2. At the command prompt type: **set ip type=ipv4 addr=<xx> subnet-mask =<yy>** where:
 - xx = IP address of the NID
 - yy = subnet mask
3. Press **Enter**.

Section 2: Installation and System Setup

4. Set the IP address mode. Type **set ip address mode=<xx>** where:
xx = the IP addressing mode (bootp, dhcp, or static).
5. Press **Enter**.
6. Type: **set gateway type=ipv4 addr=<xx>** where:
xx = default gateway address (note that only one default gateway can be set)
7. Press **Enter**.
8. Set the IP Address Mode. Type **set ip address mode={bootp}dhcp|static}** and press **Enter**.
The default is **static**.
9. Verify the configuration has been set. Type: **show ip-mgmt config** and press **Enter**. The current configuration displays. For example:

```

Agent III C1|S9|L1D>set ip type=ipv4 addr=192.168.1.10 subnet-
mask=255.255.255.0
Agent III C1|S9|L1D>set ip address mode=static
Agent III C1|S9|L1D>set gateway type=ipv4 addr=192.168.0.1
Agent III C1|S9|L1D>show ip-mgmt config
IPv4 management configuration:
-----
IP management state:          enable
IP address:                   192.168.1.10
IP subnet mask:              255.255.255.0
Gateway IP address:          192.168.0.1
IP address mode :            Static

IPv6 management configuration:
-----
Management State:            disable
Link Local Address:          fe80::2c0:f2ff:fe21:177
Global Address Mode:         static
Global Address:              ::
Management Prefix:          0
Duplicate Address Detect:    false
Gateway Mode:                static
Gateway Address:             ::

server index  addr_type  address
-----
DNS server1   ipv4       192.168.1.30
DNS server2   ipv4       0.0.0.0
DNS server3   ipv4       0.0.0.0
DNS server4   ipv6       ::
DNS server5   ipv6       ::
DNS server6   ipv6       ::
Agent III C1|S9|L1D>

```

For more information about IP configurations see “[Setting the IP Addressing](#)” on page 92.

Accessing the NIDs

The x323x NIDs can be accessed through either a local serial interface via a USB connection or through an Ethernet network connection. The network connection can be done via a Telnet session or a Web graphical user interface (GUI).

Access via Local Serial Interface (USB)

The x323x NIDs can be connected to a local management station (PC) through a serial interface using a USB connection. The NID is controlled by entering command line interface (CLI) commands at the local management station. To use the serial interface (USB) the following is required:

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

IMPORTANT

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

Web Browsers Supported

The ION system supports the following web browsers.

- Firefox (Mozilla Firefox) 3 - 6
- Internet Explorer (IE) 6 - 9
- Google Chrome 3 - 13

Section 2: Installation and System Setup

Starting the Web Interface

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

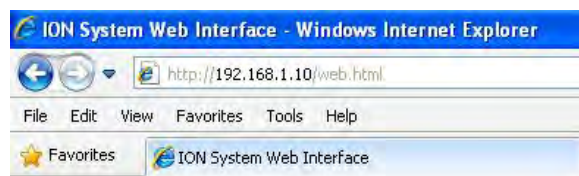
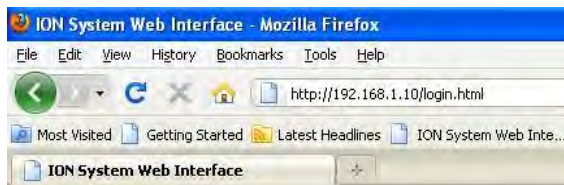
A Web session can be used to connect to and set up the NID.

IMPORTANT

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

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

1. Open a supported web browser.
2. In the address (URL) block, type the IP address of the NID (the default address is 192.168.1.10).



3. Click **Go** or press **Enter**.

The ION System sign in screen displays.



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

4. Type the User Name (the default is **ION**). **Note:** the User Name is case sensitive - all upper case.
5. Type the Password (the default is **private**). **Note:** the password is case sensitive - all lower case.

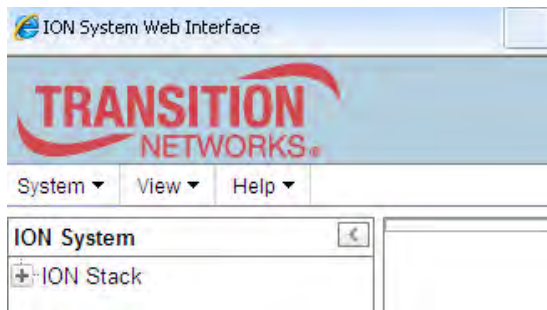
Sign in to ION System Web Interface

User Name:

Password:

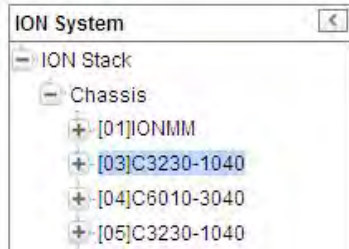
6. Click the **Sign in** button or press the **Enter** key.

The opening screen displays with the **ION Stack** in the upper-left corner.



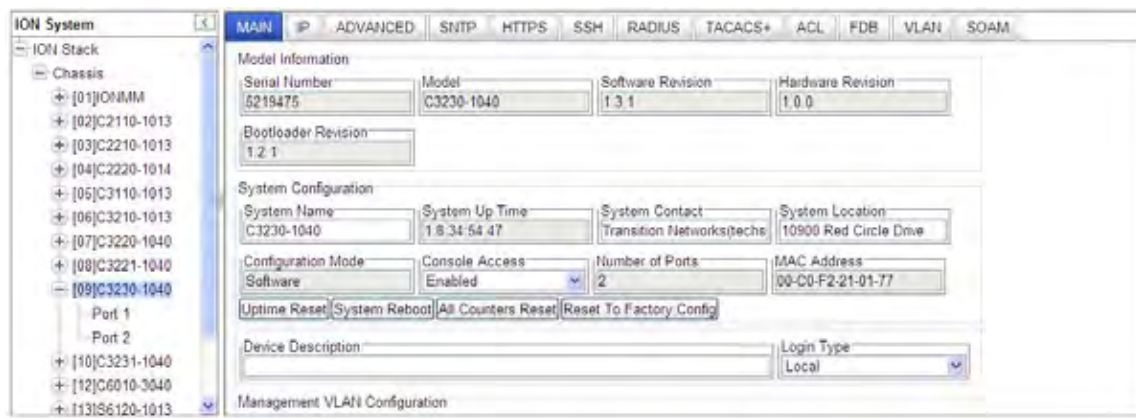
7. Click the plus sign [+] next to **ION Stack**. This unfolds "ION Stack" node in the left tree view and refreshes device status.
8. Click the plus sign [+] next to **Chassis** to unfold the chassis devices.

Section 2: Installation and System Setup

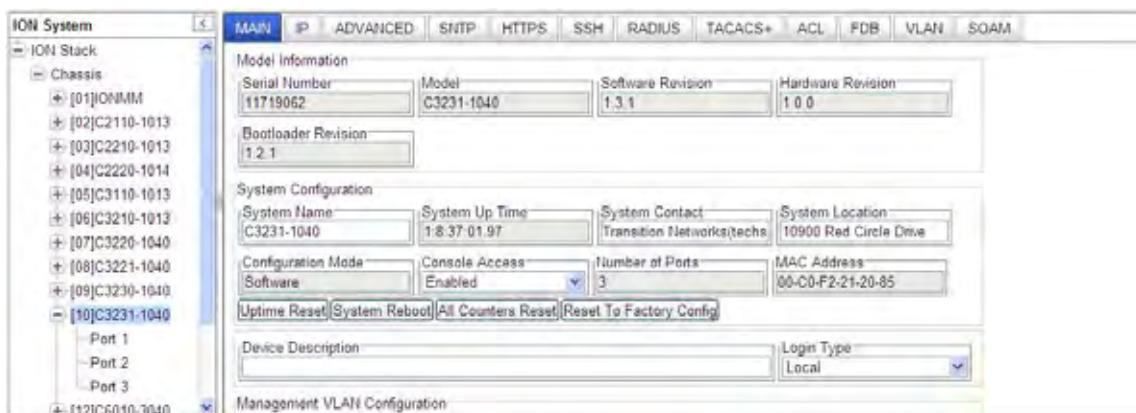


9. Select the appropriate NID. The **MAIN** screen displays for the selected NID.
10. Click the plus sign [+] next to the device to unfold the device ports.

A Model C3230 (with 2 ports expanded) is shown below:



A Model C3231 (with 3 ports expanded) is shown below:

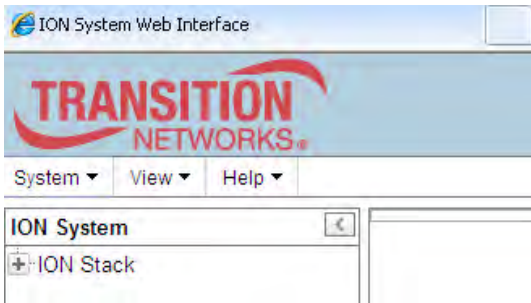


11. Use the various tabs to configure the system, devices and ports. For configuration information, see “[Section 4: Configuration](#)” on page 95.

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

Terminating the Web Interface (Sign Out)

To sign out from the Web interface, in the upper left:



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



The Sign in screen displays.

Note: The x323x does not automatically sign out upon exit or after a timeout period, which could leave it vulnerable if left unattended. Follow your organizational policy on when to sign out from the ION System via the Web interface.

Changing Switch Mode (Local / Remote)

Management and configuration control can be switched between local management control (via CLI, Telnet or Web) or remote management control (via the IONMM). By default, the x323x is managed by 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 (default mode): the device can only be managed and configured via the IONMM.

Setting the switch mode to remote indicates that the device is managed through the IONMM.

The device cannot perform any IP management when in ‘remote’ mode.

Local Mode: the device can only be configured and managed directly via CLI, Telnet or Web. Setting the mode to **local** indicates that the device is managed through either a direct USB connection or a direct network connection via Telnet or the Web interface (i.e., the device is no longer managed by the IONMM).

Note: The x323x NIDs are shipped with switch mode set to “remote.”

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

1. Start a USB session (see “[Starting a USB Session](#)” on page 48).
2. At the command prompt type **set switch mode=local**.
3. Press the **Enter** key.
4. Reboot the card for the changes to take effect. At the command prompt type **reboot**.



Doing a reboot, restart or upgrade of the IONMM, a power restart of the chassis, or a reset to factory remove temporary files (e.g. configuration backup files, Syslog file).

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

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

Section 3: Management Methods

General

The x323x NIDs are managed either directly or through the IONMM. Whether the NID is managed directly or indirectly, management is accomplished through one of the following methods.

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

The x323x NIDs can be remotely managed directly (i.e., not through IONMM). This enables administrators to monitor and configure remote stand-alone x323x NIDs straight from the Network Management Station (NMS) without leaving the office.

IONMM Managed NIDs

NIDS that are managed through the IONMM are either chassis resident (C323x) or standalone modules that are connected as remotes to chassis resident modules. Communications between the IONMM and the NIDs is through the ION Chassis backplane.

Managing Slide-In and Remote Modules Using CLI Commands

You can manage modules other than the IONMM by entering CLI commands through either the local USB serial interface or a remote Telnet session. CLI commands can operate at the device level or port level, as indicated by the status of the command prompt's preamble.

For example: `C1 | S1 | L1D>`

or with the IONMM system name: `Agent III C1 | S1 | L1D>`

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

Section 3: Management Methods

The ION system hierarchy is shown in the figure below.

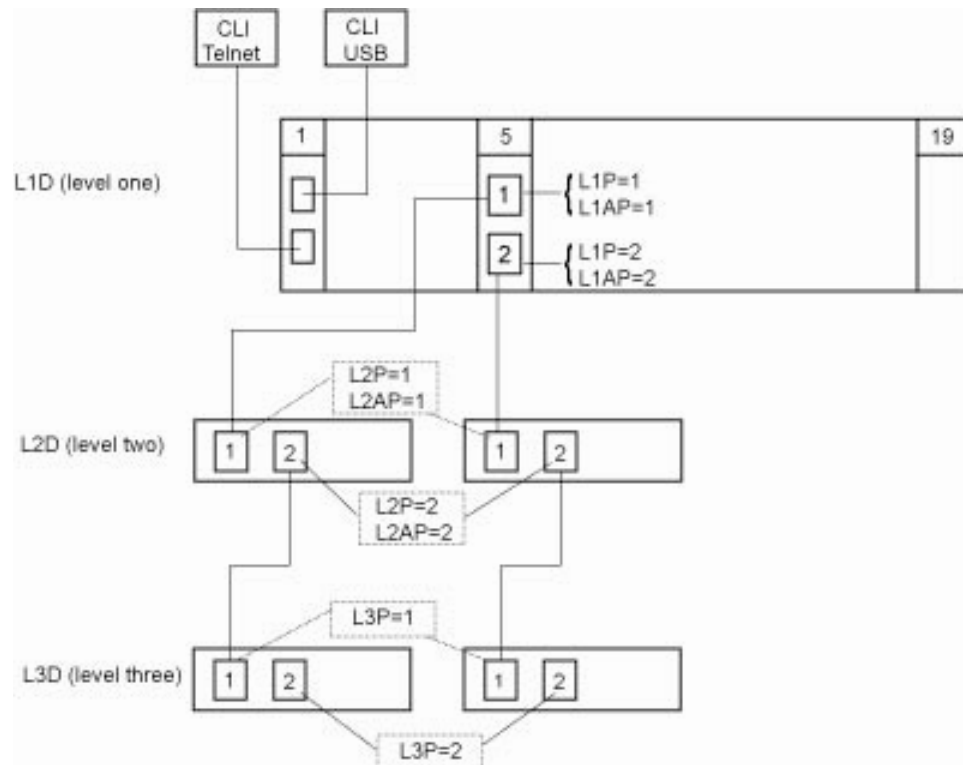


Figure 21: CLI Location Hierarchy

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

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

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

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

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

Example 1:

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

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

The resulting command line prompt would be:

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

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

Example 2:

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

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

The resulting command line prompt would be:

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

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

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

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

Use the **go** command to change the operational location to the device/port to be managed. The **go** command format is:

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

(for a slide in card), or

```
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

(for a standalone card).

2. Configure the NID using the appropriate commands. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
3. To return the location to the IONMM, type **home** and press **Enter**.

Example 3:

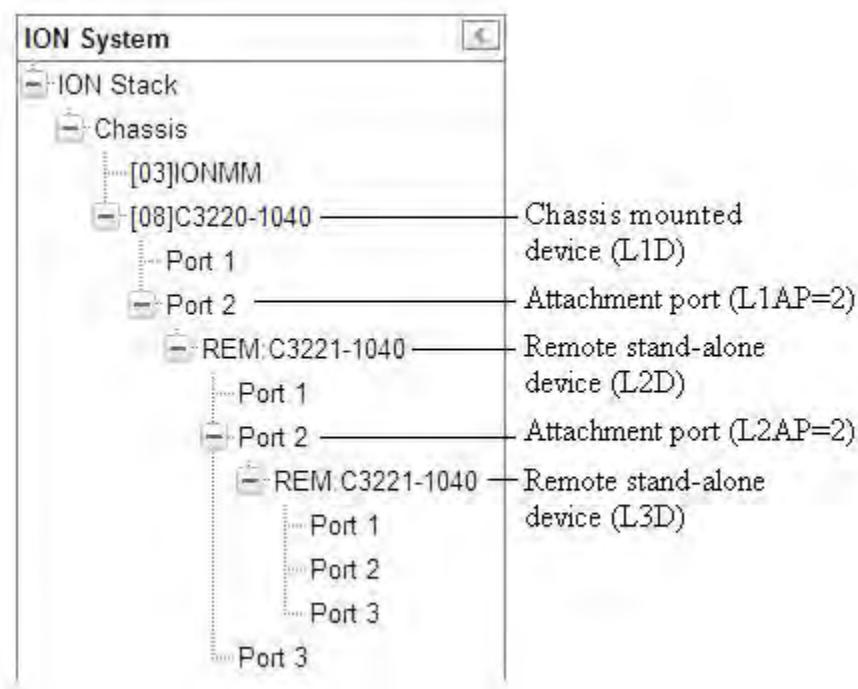
The CLI prompt (>) displays an editable name prefix based on the “System Name” field. You can add or modify the System Name via the CLI. For example if the name was “lab”, the IONMM “System Name” is carried through to every prompt/card that you are logged into (e.g., lab C1|S3|L1D>, lab C1|S5|L1D>, lab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

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

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

Managing Slide-In and Remote Modules via the Web Interface

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



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

Direct Managed NIDs

Direct management is for standalone NIDs (S323x) that are not connected to a module that is managed through the IONMM. In direct management the network and/or USB cable is connected directly to the module to be managed.

Managing Standalone Modules Using CLI Commands

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

For example:

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

or

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

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

The **go** command format is:

```
go [c=<1-16>] [s=<1-32>] [[1ap=<1-15>] [2ap=<1-15>] (1p=<1-5>|2p=<1-15>|3p=<1-15>|1d|2d|3d)
```

(for a slide in card), or

```
go [c=<0-16>] [s=<0-32>] [[1ap=<1-15>] [2ap=<1-15>] (1p=<1-5>|2p=<1-15>|3p=<1-15>|1d|2d|3d)
```

(for a standalone card).

Example

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

```
C0 | S0 | L1D>go 11p=1
```

The resulting command line prompt would be:

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

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

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

```
C0 | S0 | L1P1>go 11d
```

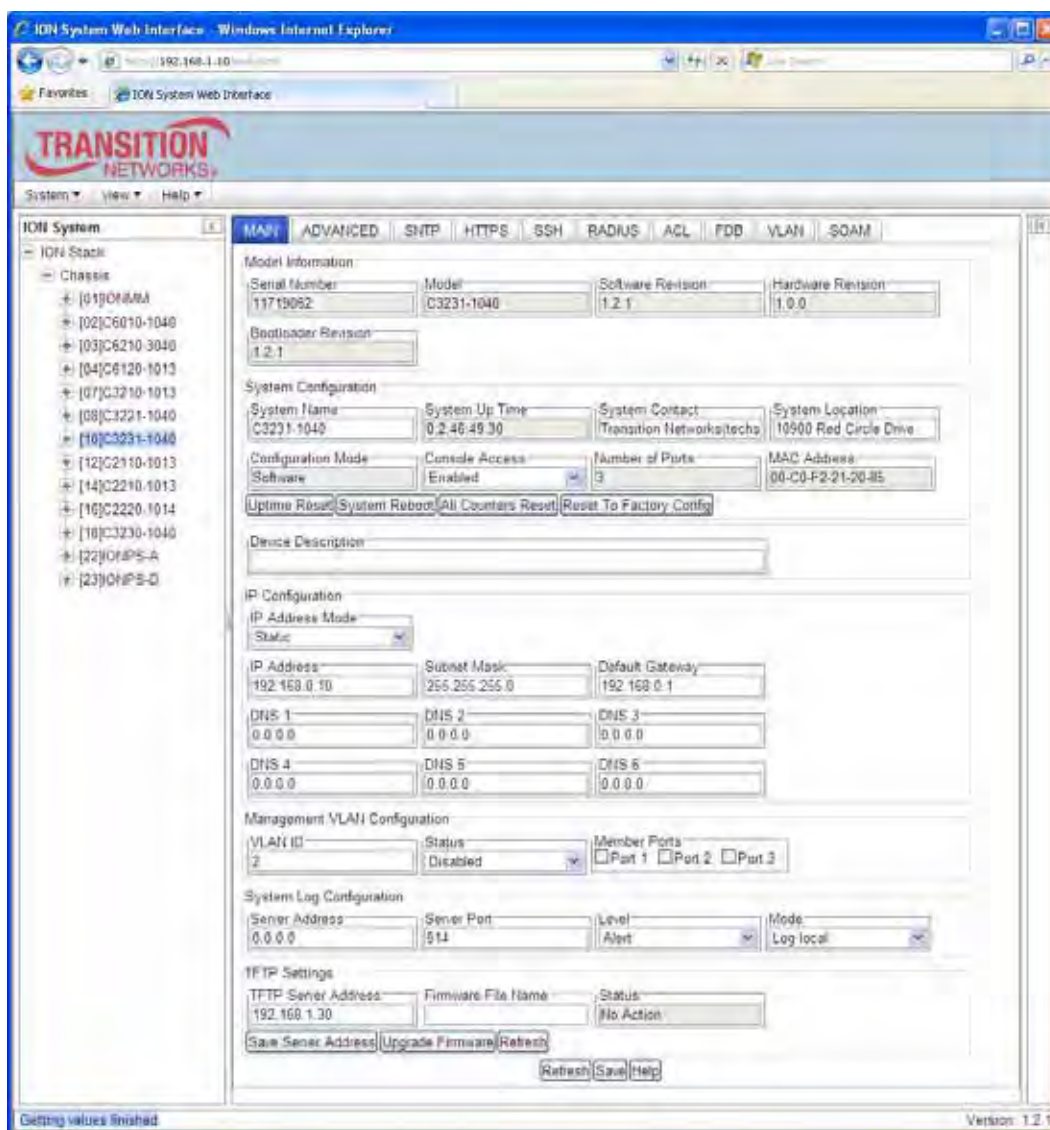
The resulting command line prompt would be:

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

Managing a Standalone Module via the IONMM Web Interface

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

1. Access the NID via the Web interface (see “Starting the Web Interface” on page 45).
2. Click the plus sign [+] next to **ION Stack** to unfold the "ION Stack" node in the left tree view if not already done.
3. Click the plus sign [+] next to **Chassis** and click the plus sign [+] next to a module.
4. Click on the module or port to be managed (e.g., C3231-1040 in slot 10 shown below).

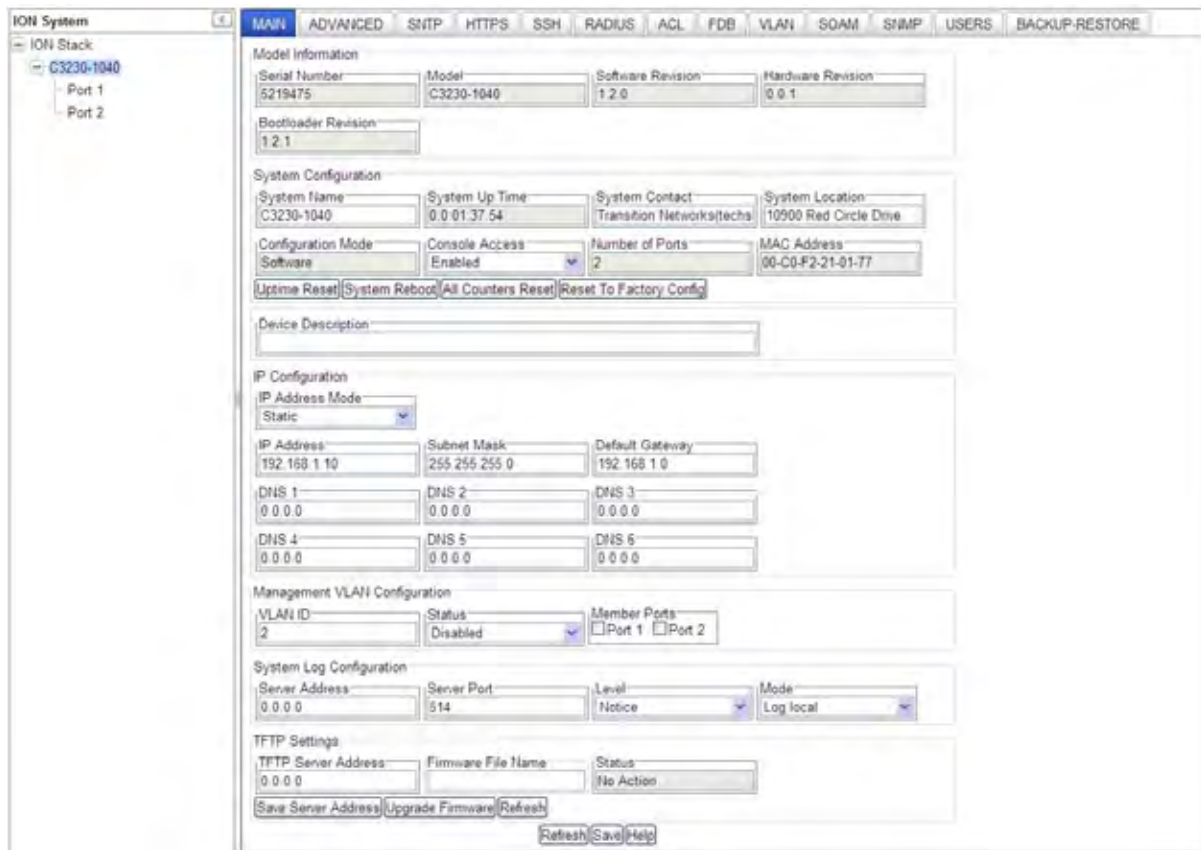


5. Select the various tabs to perform the applicable operations.

Managing a Standalone Module via the Web Interface

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

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



4. Click on the module or port to be managed (e.g., C3230-1040 on the screen above).
5. Select the various tabs to perform the applicable operations.

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

Menu System Descriptions

The table below describes the x323x interface in terms of its system-level pane, dropdowns, tabs and sub-tabs. Note that menus and tabs vary slightly by model.

Table 10: System-Level Menu Description

Dropdown / Tab	Description
ION System pane	<p>ION Stack - consists of one chassis or one standalone. The Stack Members table lists the Stack's chassis and its type.</p> <p>Chassis - the ION System family of products. The Chassis view shows a summary view of one chassis. Model Information includes:</p> <ul style="list-style-type: none"> * Serial Number - The serial number of the chassis itself. Individual NIDs also have their own serial numbers. * Model Name - The exact model name of this device. When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number. * Software Revision, Hardware Revision, and Bootloader Revision. * Chassis Members table - lists local physical components in slots 1 to 19. <p>Device – provides tabs and sub-tabs for the IONMM and NIDs in the ION system.</p> <p>Port - provides tabs and sub-tabs for a selected NID port.</p>
System dropdown	Sign out.
View dropdown	Refresh.
Help dropdown	Online Help, ION Product Home Page, About ION System Web Interface.
MAIN tab	Model Information, System Configuration, Device Description, Management VLAN Configuration, System Log Configuration, and TFTP Settings sections.
IP Tab	<p><u>Sections</u>: IPv4, IPv6, and DNS Configuration.</p> <p><u>Buttons</u>: Refresh, Save Help.</p>
ADVANCED tab	FDB Aging Time, MAC Address Learning, Link Pass Through (LPT), IEEE Priority Class, and IP Traffic Class sections.

SNTP tab	SNTP Configuration, Daylight Saving Time Configuration, and SNTP Servers sections.
HTTPS tab	HTTPS Status, HTTPS Port, Certificate Type, and Copy HTTPS Certification functions.
SSH tab	SSH Server Status, Version, SSH Auth Timeout, SSH Auth Retries, Host Public-Key Settings, and User Public-Key Settings.
RADIUS tab	RADIUS Client and RADIUS Servers configuration.
TACACS+ Tab	<u>Sections:</u> TACACS+ Client and TACACS Server 1 - TACACS Server 6 sections. <u>Buttons:</u> Refresh, Save, Help.
ACL tab	Set ACL Status and Chain Policy, View/Add/Edit Rules, and View/Add/Edit Conditions for Rules. Set Priority, Policy and Trap Rate for Rules. Define Type, Source or Destination, Operation, and Value Conditions for Rules.
FDB tab	Add, Edit or Delete MACs table data (MAC Address, Port, Priority, and Entry Type) and Flush FDBs.
VLAN tab	Add, Edit or Delete VLANs table data (VLAN ID, FDB ID, Priority Override, Priority, Member Tag Port 1, and Member Tag Port 2) and Flush VLANs.
SOAM tab	Main Configuration sub-tab (Sender ID and Port ID information); MD sub-tab (Add, Edit, Delete MDs); MA/MEG sub-tab (Configure MA or MEG); MEP sub-tab (Add/Edit/Delete MEPs, Display statistics; Configuration, CC Monitoring, Loopback, Linktrace, ETH-MCC, ETH-TEST, DM, FLM, AIS sub tabs); MIP sub-tab (Add/Edit/Delete MEPs; Display statistics); and Configuration Error List sub-tab.
SNMP tab	<u>Sub-tabs:</u> General, Users, Groups, Views, Trap Hosts, Remote Users. <u>Fields:</u> Community String, Access Mode, SNMP V3 Engine ID. <u>Buttons:</u> Add, Delete, Refresh, Save, Help buttons.
USERS tab	<u>Fields:</u> User Name, Password, Confirm Password, Level fields. <u>Buttons:</u> Refresh, Add, Edit, Delete, Help buttons.

Section 3: Management Methods

BACKUP / RESTORE tab*	<p><u>Sub-tabs</u>: Backup and Restore. TFTP Server Address and Status fields.</p> <p><i>Backup</i> - lets you select modules from a list to Back Up (you must download config files after backing up is done).</p> <p>Buttons: Download, Refresh, Back Up, Help.</p> <p><i>Restore</i> - lets you select modules to Restore (you must upload config files before restoring is started).</p> <p>Buttons: Upload, Refresh, Restore, Help.</p>
---------------------------------	--

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

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

Table 11: Port-Level Menu Description

Tab	Description
MAIN tab	<p>Sections: Circuit ID, Port Configuration, Auto Negotiation Settings, Control Frames Management / Capabilities Advertised, Port Forward Management, L2CP Disposition, TN Topology Discovery Protocol TX, and Virtual Cable Test (VCT).</p> <p>Buttons: <i>Virtual Cable Test</i>, <i>Refresh</i>, <i>Save</i>, and <i>Help</i>.</p>
ADVANCED tab	<p>Sections: Bandwidth Allocation, MAC Security, VLAN Forwarding Rules, Priority Forwarding Rules, VLAN Tag Management, User Priority, and Egress Queue Mode.</p>
COUNTERS tab	<p>Sections: RMON Counters, RX Counter, TX Counter, Dot3 Statistics, and MAC Control Frames sections.</p> <p>Buttons: <i>Reset Counters</i>, <i>Refresh</i>, and <i>Help</i> buttons.</p>
LOAM tab	<p>Sub-tabs: Main (LOAM Configuration, LOAM Peer Information, Loopback Management), Counters, Event Configuration, and Event Log sub-tabs.</p>

<p>DMI tab (Port 2 only)</p>	<p>Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length.</p> <p>The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See “DMI (Diagnostic Maintenance Interface) Parameters” on page 248 for more information.</p> <p>Note: not all NID or SFP models support DMI. Transition Networks NIDs that support DMI have a “D” at the end of the model number. If you click the DMI tab on a NID model that does not support DMI, the message “<i>The DMI feature is not supported on current port.</i>”</p>
---	---

Reboot, Reset, and Power Off Function Notes

Certain functions such as a System Reboot, Reset to Factory Configuration, Reset Power to a Slot, and Power Off a Slot) cause the system to delete certain stored files. **Caution:** In some circumstances, these stored files are lost unless you first perform a System Backup. See the “[Backup and Restore Operations](#)” section starting on page 286 for information on how to save the stored files from deletion.

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

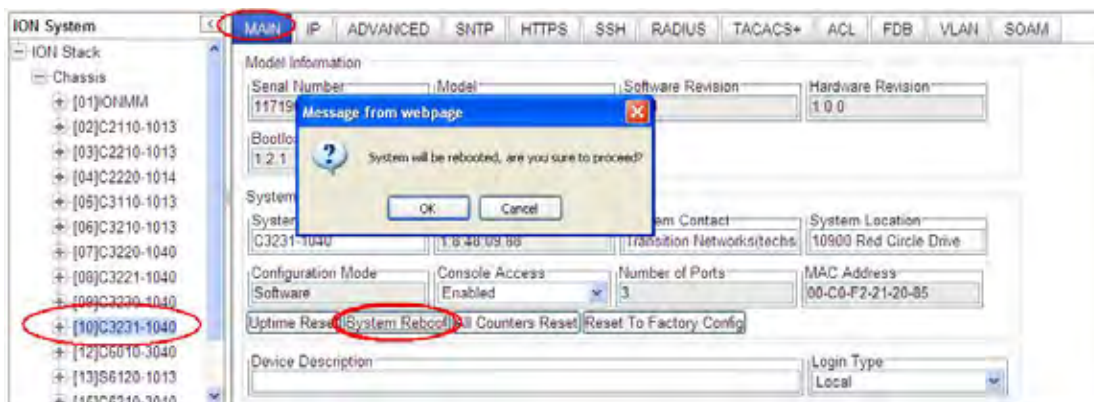
- Table 17. [Back Up and Restore File Content and Location](#) on page 286
- Table 18. [File Status after a Reset to Factory Defaults](#) on page 291
- Table 19. [File Content and Location after a System Reboot](#) on page 295
- Table 20. [File Content and Location after a Firmware Upgrade](#) on page 309



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

System Reboot

Clicking the **System Reboot** button resets all system states and reinitializes the system; all configuration data is saved during a restart. The message “*Loading, please wait...*” displays.



Press the **Cancel** button if you are not sure you want a system reboot to occur.

Press the **OK** button to clear the webpage message and begin the reboot process.

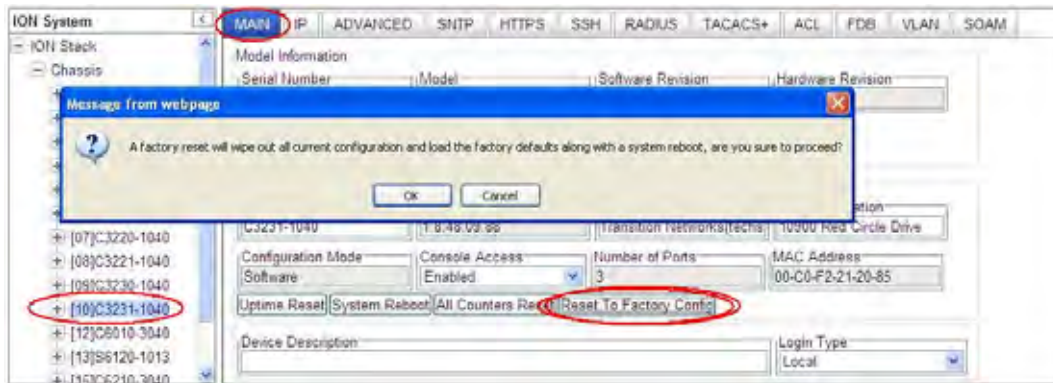
The message “*Loading, please wait...*” displays.

Note that a System Reboot can take several minutes.

Reset To Factory Config

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

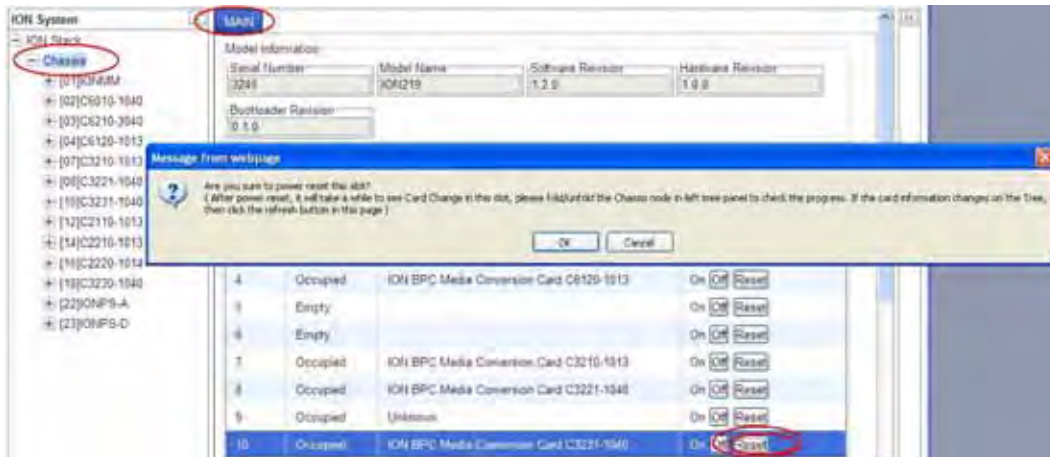
The message “A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?” displays.



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

Reset Power to a Slot

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



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

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

Section 3: Management Methods

Power Off a Slot

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



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

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

Section 4: Configuration

General

After the x323x has been installed and access has been established, the device and its ports must be configured to operate within your network. The configuration establishes operating characteristics of the x323x device and associated ports. Configurations can be done either by entering CLI commands (USB / Telnet) or through a Web interface. For complete descriptions of all CLI commands, see the *ION System CLI Reference Manual, 33461*.

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

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

Section 4: Configuration

Note: Transition Networks recommends as a “best practice” to back up each SIC card’s configuration after it is fully configured so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored.

Setting the IPv4 Addressing

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

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

- The BootP (Bootstrap Protocol) network protocol used by a network client to obtain an IP address from a configuration server. A BootP configuration server assigns an IP address to each client from a pool of addresses. BOOTP uses the User Datagram Protocol (UDP) as a transport on IPv4 networks only. The Bootp protocol lets a network user be automatically configured (receive an IP address) and have an OS booted without user involvement. The BootP server automatically assigns the IP address from a pool of addresses for a certain duration of time. BootP uses UDP port number 67 for the server and UDP port number 68 for the BootP client.
- A DHCP server can assign a dynamic (temporary) IP address. The DHCP server contains a list of IP address that can be used, and assigns one when a requesting device wants to communicate. The address is assigned to the device for that session only.
- A static IP address is one that is permanently assigned to the NID. The static IP address, subnet mask and default gateway address can be configured in the NID using either the CLI or Web method.

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

IMPORTANT

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

Otherwise, in order to communicate with the NID across the network for the first time, you must change the network settings (IP address, subnet mask and default gateway address) of your PC to coincide with the defaults of the NID (see “[Appendix B: Factory Defaults](#)” on page 339).

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

The factory default settings are:

IP Address = 192.168.1.10
Subnet Mask = 255.255.255.0
Default Gateway addr = 192.168.1.0
IP Type = IPv4
IP Addr = 192.168.1.10
Subnet-mask = 255.255.255.0
IP Address mode = Static

IPv4 Address Config – CLI Method

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

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

2. Define the IP address and subnet mask for the NID. Type:

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

where:

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

yy = subnet mask (e.g., 255.255.255.1 in the example)

3. Press **Enter**.
4. Set the IP addressing mode. Type **set ip address mode=<bootp|dhcp|static>** and press **Enter**.
5. Define the default gateway address. Type: **set gateway type=ipv4 addr=<xx>**, where:
xx = default gateway address (e.g., 192.168.1.2 in the example)
6. Press **Enter**.
7. Verify the configuration has been set. Type **show ip-management config** and press **Enter**.
The current configuration displays. For example:

```
Agent III C1|S9|L1D>set ip type=ipv4 addr=192.168.1.10
Agent III C1|S9|L1D>set ip address mode=static
Agent III C1|S9|L1D>set gateway type=ipv4 addr=192.168.1.0
Agent III C1|S9|L1D>show ip- config
IPv4 management configuration:
-----
IP management state:          enable
IP address:                   192.168.0.10
IP subnet mask:               255.255.255.0
Gateway IP address:           192.168.0.1
IP address mode :             Static

IPv6 management configuration:
-----
Management State:             disable
Link Local Address:           fe80::2c0:f2ff:fe21:177
```

Section 4: Configuration

```

Global Address Mode:      static
Global Address:          ::
Management Prefix:      0
Duplicate Address Detect: false
Gateway Mode:           static
Gateway Address:        ::

```

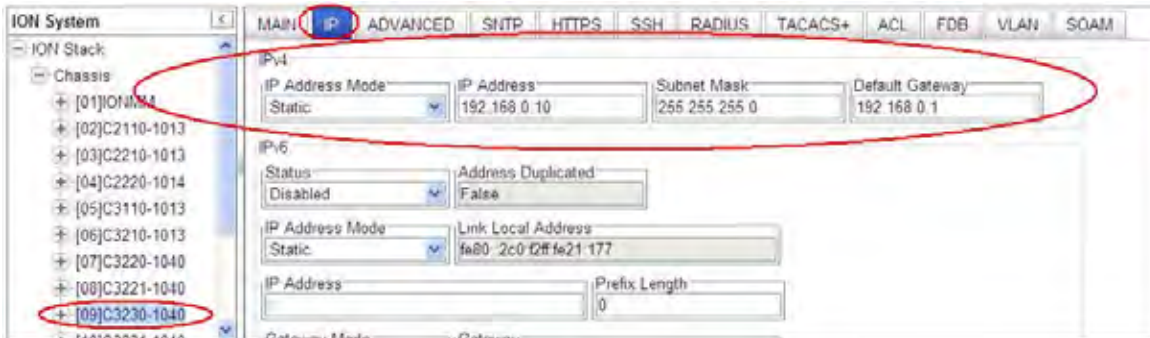
server index	addr_type	address
DNS server1	ipv4	0.0.0.0
DNS server2	ipv4	0.0.0.0
DNS server3	ipv4	0.0.0.0
DNS server4	ipv6	::
DNS server5	ipv6	::
DNS server6	ipv6	::

Agent III C1|S9|L1D>

IPv4 Address Mode Config – Web Method

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

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



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

BootP Addressing Configuration

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

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

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

Defining Domain Name System (DNS) Servers

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

DNS Lookups over IPv6 Transport

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

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

DNS ‘3 vs. 3’ Rule (‘Up to 3’ Rule)

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

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

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

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

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

DHCPv6 DNS Server Configuration

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

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

Section 4: Configuration

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

Static DNS Server Configuration

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

Assigning a Dynamic IPv4 Address via DHCP

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

Note:

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

A dynamic IP address can be configured in the x323x using either the CLI method.

IPv4 Dynamic Config – CLI Method

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

```
set dhcp state=enable
```

3. Press **Enter**.

Defining DNS Servers

A Domain Name System (DNS) is a database that correlates names of devices and domains on the network to IP addresses. Every device and domain in a network is assigned an IP address. They may also have names assigned. It is the responsibility of the DNS server to translate the name assigned to a device to the actual IP address of the device. Every domain has a DNS server that handles its requests, translating names to IP addresses.

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

DNS Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the command prompt type: **set dns-svr=<xx> type=<yy> addr=<zz>** where:
xx = the number (1–6) of the DNS server being defined. Up to six DNS servers can be defined.
yy = the type of addressing; select **dns** (domain name address format).
zz = the IP address of the DNS server.
3. Press **Enter**.
4. Repeat Steps 2 and 3 for each DNS server to be defined. For example:

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

5. Verify the DNS server(s) defined. Type **show ip config** and press **Enter**. For 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:

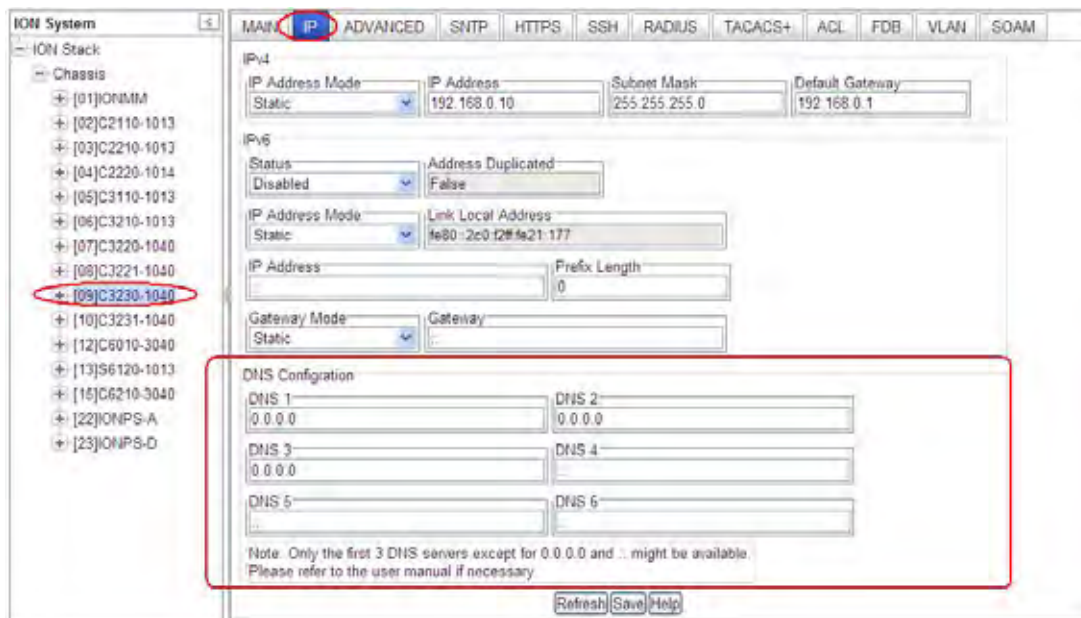
warning: server1 to server3 is just used for ipv4!

warning: server4 to server6 is just used for ipv6!

DNS Config – Web Method

The DNS 1 through DNS 6 entries can be in IPv4 or IPv6 format, or both (a combination of up to 3 of each). DNS servers 1-3 are for IPv4; DNS servers 4-6 are for IPv6. See “DNS ‘3 vs. 3’ Rule (‘Up to 3’ Rule)’ on page 101.

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

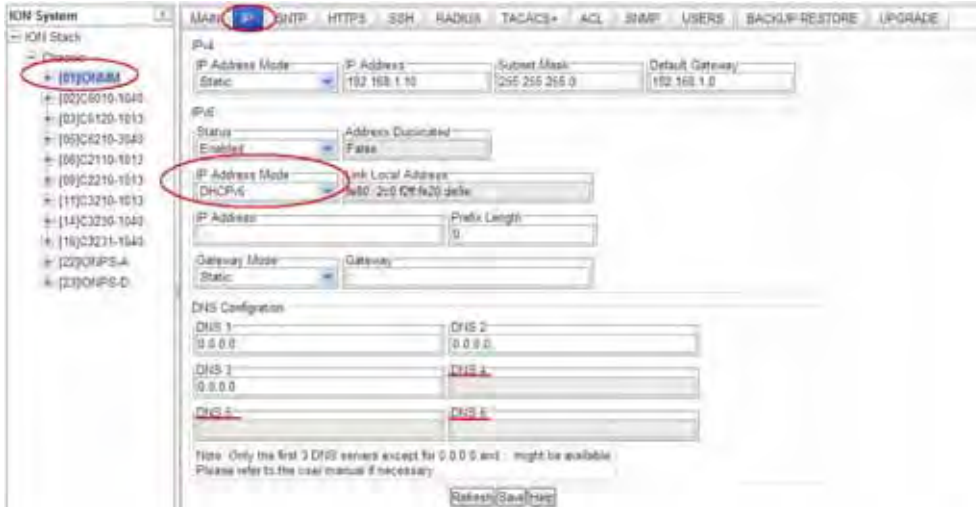


Note: Only the first 3 DNS servers except for 0.0.0.0 and :: might be available.

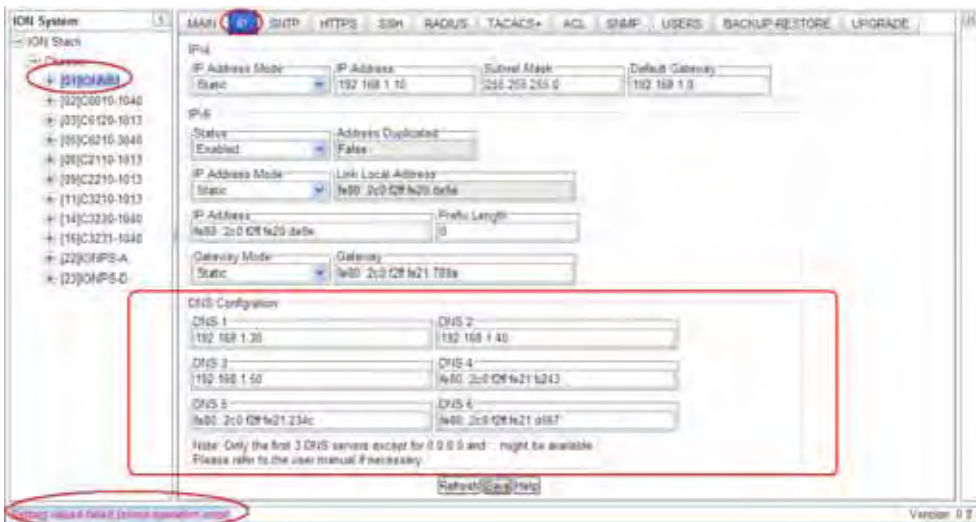
4. In the DNS 1- DNS 3 fields, enter a valid IPv4 IP address (not applicable if DHCP is selected for IPv4 Address Mode).
5. In the DNS 4- DNS 6 fields, enter a valid IPv6 IP address (not applicable if DHCP v6 is selected for IPv6 Address Mode).
6. Scroll down and click **Save** when done.

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

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



The figure below shows an invalid configuration:



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

IPv6 Description

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

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

Note: The IPv6 version of ICMP is required by all IPv6 implementations.

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

Differences between IPv4 and IPv6

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

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

IPv6 Features

The ION system provides the following IPv6 features.

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

These features are described in the following sections.

ION IPv6 Function Descriptions

IPv6 Dual Protocol Stacks and Multiple Server Support

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

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

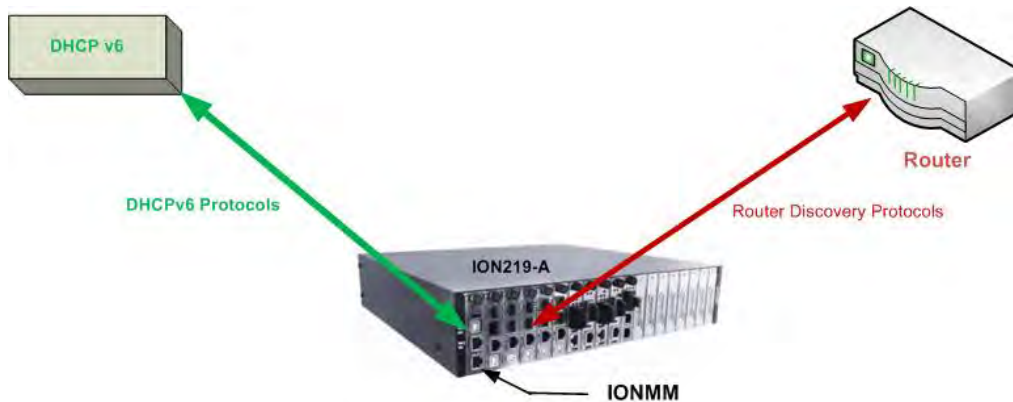


Figure x. Multiple Routers - One DHCPv6 server and One Router

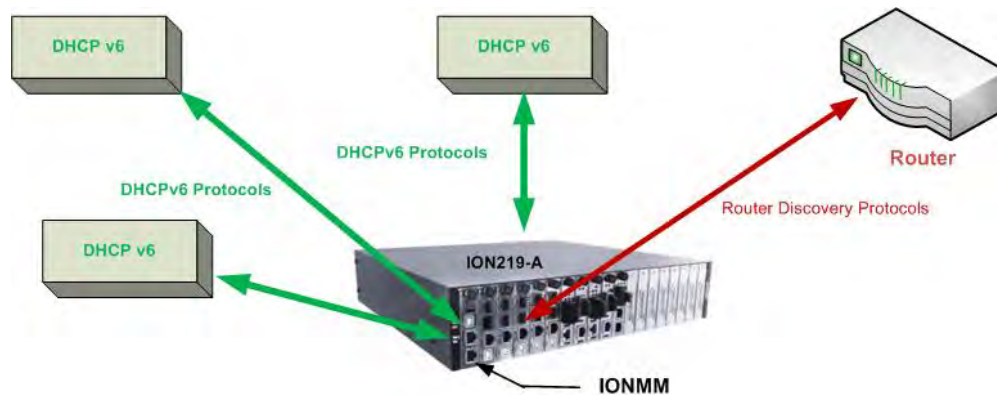


Figure x. Multiple DHCPv6 servers and One Router

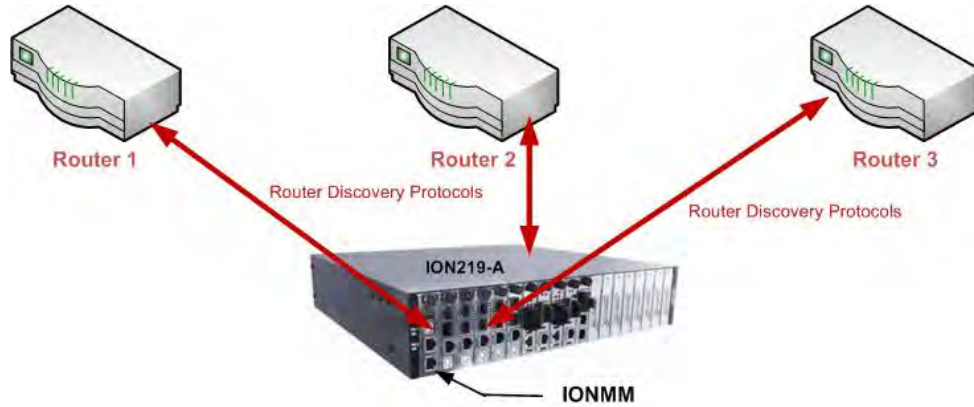


Figure x. Multiple Routers

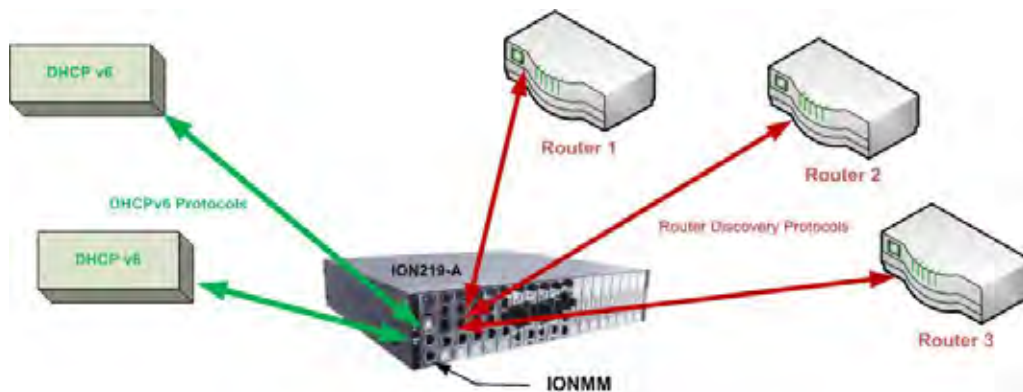


Figure x. Multiple DHCPv6 Servers and Routers

IPv6 Management Functions

IPv6 Address Formats

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

IPv6 Unicast Addresses

ION IPv6 Unicast Address support includes:

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

Section 4: Configuration

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

IPv6 Multicast Addresses

ION IPv6 multicast support includes:

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

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

ICMP v6 (Internet Control Message Protocol for IPv6)

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

IPv6 Neighbor Discovery Protocol

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

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

The Neighbor Discovery protocol uses the following messages:

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

IPv6 DAD (Duplicate Address Detection)

IPv6 DAD is an IPv6 component to check the duplicated address. The function is always enabled on ION. When a new IPv6 address is configured on ION, this device will first check duplicated address on the link.

If the S3280 finds the new address has existed on the link, this new address can not be used. If the IP address is duplicated with another node, the ION Web/CLI will show the DAD attribute if the duplicated address is detected.

IPv6 Auto Configuration per IETF RFC 2462

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

IPv6 supports the following types of auto-configuration:

- Stateless auto-configuration
- Stateful auto-configuration

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

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

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

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

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

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

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

Section 4: Configuration

IPv6 Stateless Auto-configuration

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

Stateless autoconfiguration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. In the absence of routers, a host can only generate link-local addresses. However, link-local addresses are sufficient for allowing communication among nodes attached to the same link.

Stateless auto-configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address.

The stateless approach is used when a site is not particularly concerned with the exact addresses hosts use, so long as they are unique and properly routable. Stateless auto-configuration is suitable for small organizations and individuals. In this case, each host determines its addresses from the contents of received router advertisements. Using the IEEE EUI-64 standard to define the network ID portion of the address, it is reasonable to assume the uniqueness of the host address on the link.

IPv6 Stateful Auto-configuration with DHCPv6 Support

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

Stateful autoconfiguration has hosts obtain interface addresses and/or configuration information and parameters from a server. Servers maintain a database that keeps track of which addresses have been assigned to which hosts. The stateful autoconfiguration protocol allows hosts to obtain addresses, other configuration information or both from a server. Stateful auto-configuration requires a certain level of human intervention because it needs a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server for the installation and administration of the nodes. The DHCPv6 server keeps a list of nodes to which it supplies configuration information. It also maintains state information so the server knows how long each address is in use, and when it might be available for reassignment.

The stateful approach is used when a site requires tighter control over exact address assignments. Both stateful and stateless address autoconfiguration may be used simultaneously.

Stateful auto-configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator.

IPv6 Static Configuration

As in IPv4, the host address can be statically defined in the case where the IPv6 address, mask, and the gateway address are all manually defined on the host. Using static configuration causes all of the Auto-configuration features provided by IPv6 to be lost.

When IPv6 mode is switched from DHCPv6 and Stateless to static, all IPv6 address and prefix and IPv6 DNS values will be set back to the default value of all zero. When IPv4 mode is switched from DHCP/BootP to static, IP address and Mask and Gateway and DNS values will be set back to default values (192.168.0.10 and 255.255.255.0 and 192.168.0.1 and all zeros).

When IPv6 mode is switched from DHCP to Static, the IPv6 address and DNS will be set to ":::" by the web interface, and IPv4 will be set to the default of 192.168.0.10 and DNS will be set to 0.0.0.0.

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

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

IPv6 MTU (Maximum Transmission Unit) Path Discovery

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

IPv6 Route

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

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

ION IPv6 Configuration Considerations

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

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

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

IPv4 and IPv6 Initialization Defaults

The IPv4/IPv6 factory default configuration settings are:

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

The IPv6 default configuration includes:

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

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

IP Address Mode Notes

1. When you switch IPv6 address mode from DHCPv6 to Static, the defaults become:
 - a. IPv6 address (::)
 - b. IPv6 prefix (0)
 - c. IPv6 DNS (::)
2. When you switch IPv6 address mode from Stateless to static, the defaults become:
 - a. IPv6 address (::)
 - b. IPv6 prefix (0)
3. When you switch IP address mode from DHCP to static or from static to DHCP, the defaults become:
 - a. IP address (192.168.0.10)
 - b. Network Mask (255.255.255.0)
 - c. Gateway (192.168.0.1)
 - d. DNS (0.0.0.0)

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

Telnet IPv4 and IPv6 Connections

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

The ION system supports up to 16 Telnet sessions.

TFTP IPv4 and IPv6 Connections

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

IPv6 Address Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Check the current IP addressing configuration. Type **show ipv6 interface** and press **Enter**.
3. Define the IPv6 Gateway Mode. Type **set ipv6 gateway mode=<routerDisc|static>** and press **Enter**.
4. Define the IPv6 Address. Type **set ip type=TYPE addr=ipaddr-type (subnet-mask|prefix)=A** and press **Enter**.
5. Verify the IP configuration. Type **show ip-mgmt config** and press **Enter**. For example:

```

Agent III C1|S1|L1D>set ipv6 address mode ?
  dhcpv6
  stateless
  static
Agent III C1|S1|L1D>set ipv6 address mode=static
Agent III C1|S1|L1D>set ipv6 gateway mode=<routerDisc|static>
Agent III C1|S1|L1D>set ip type=TYPE addr=ipaddr-type (subnet-mask|prefix)=A
Agent III C1|S1|L1D>show ip-mgmt config
IPv4 management configuration:
-----
IP management state:          enable
IP address:                   192.168.1.10
IP subnet mask:               255.255.255.0
Gateway IP address:          192.168.1.0
IP address mode :             Static

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

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

```

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

Example:

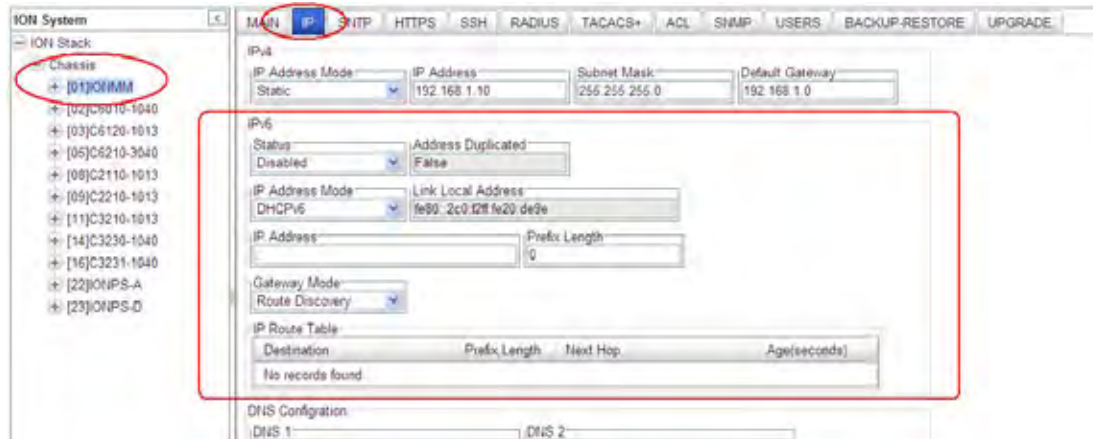
```

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

```


IPv6 Address Config – Web Method

1. Access the NID via the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **IP** tab.
3. Locate the **IPv6** section.

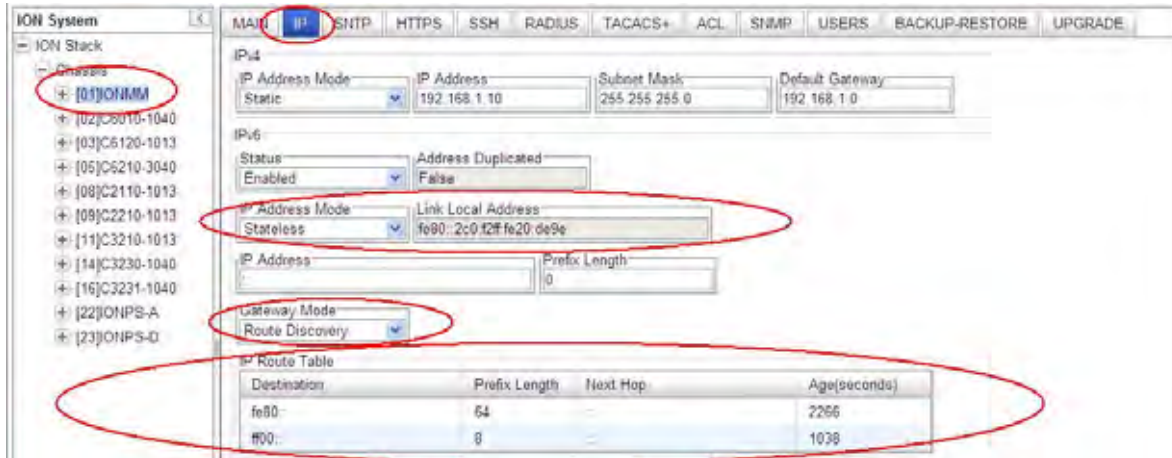


4. At the IPv6 **Status** dropdown, select **Enabled**. The default is **Disabled**. When enabled, the IP Route Table populates after a **Save**.
5. In the **Address Duplicated** field, verify False or True is displayed. The default is False (read-only field). Note that it will take up to three seconds for the **Address Duplicated** field to display TRUE when a new address is being verified. This field displays the status of IPv6 address for the device, where:
 - True**: duplicate address detected.
 - False**: no duplicate address detected.
6. At the **IP Address Mode** dropdown, select **Static**, **DHCPv6**, or **Stateless**, where:
 - Static**: selects static IPv6 addressing.
 - DHCPv6**: selects DHCP v6 addressing and disables (grays out) the DNS 4 -DNS 6 fields.
 - Stateless**: selects IPv6 stateless addressing.
7. In the **Link Local Address** field, verify the displayed address (e.g., fe80::2c0:f2ff:fe20:de9e).
8. In the **IP Address** field, enter a valid IPv6 address to be used (e.g., fe80::2c0:f2ff:fe21:b243).
9. In the **Prefix Length** field enter a value of 0-127 as the IPv6 prefix length.
10. At the **Gateway Mode** dropdown, select **Static** or **Route Discovery**, where:
 - Static**: selects Static gateway operation, displays the **Gateway** entry field, and hides the IP Route Table. In the **Gateway** field, enter a valid IPv6 address.

Section 4: Configuration

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

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

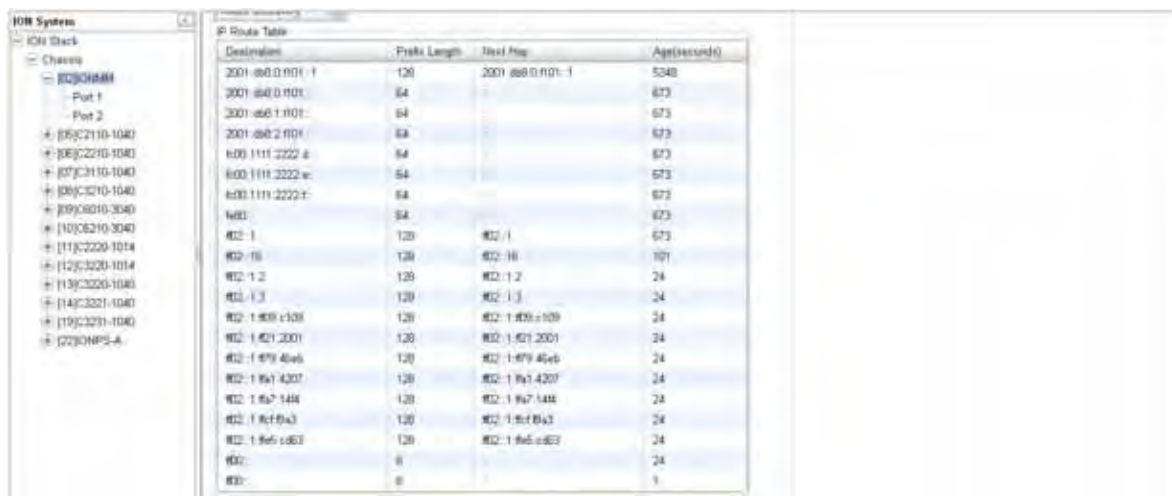


The screen above shows an **IONMM > IP** tab with **IP Addr Mode = Stateless** and **Gateway Mode = Route Discovery**. The IP Route table holds a maximum of 16 entries.

IP Route Table Parameters

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

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



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

Destination: The destination IP address of this route (i.e., a valid IPv6 address).

Prefix Length: The number of leading one bits that form the mask to be logical-ANDed with the destination address before being compared to the value in the ipv6DynRouteDest field (e.g., 8, or 64, etc.) The valid range is 0 - 127.

Next Hop: On remote routes, the address of the next system en route. For non-remote routes, a zero length string.

Age: The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of 'too old' can be implied, except through knowledge of the routing protocol by which the route was learned.

System Configuration

The system configuration defines:

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

The entry for the system contact, system location, and system name must be a text string with no spaces between characters. Note that numbers, upper/lower case characters, and special characters (~!@#%&*(*)_+)" are allowed.

The system configuration can be defined via the CLI or the Web interface.

System Configuration – CLI Method

The system information can be alphabetic, numeric or a combination.

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the command prompt type **set system contact=CONTACT**, where CONTACT is the new contact person or entity, and press **Enter**.
3. Type **set system location=LOC**, where LOC is the new location description, and press **Enter**.
4. Type **set system name=NAME**, where NAME is the new system name, and press **Enter**.

For example:

```
C1|S5|L1D>set system contact=support
C1|S5|L1D>set system location=headquarters
C1|S5|L1D>set system name=C3240-1040
```

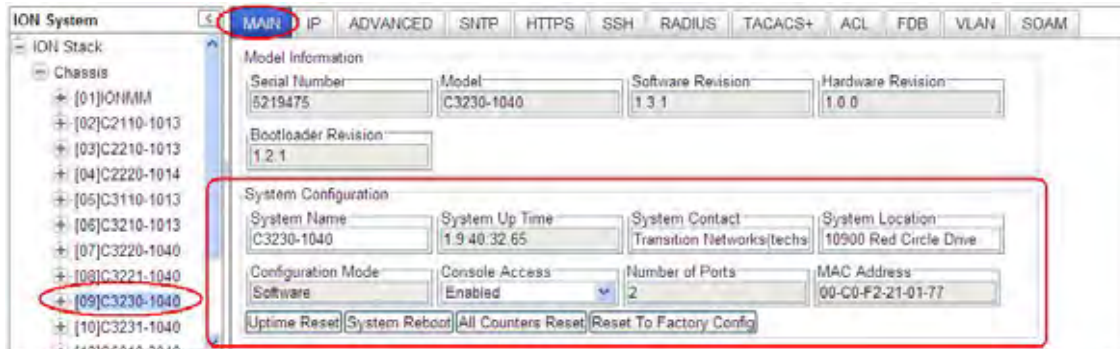
5. Verify the new system Configuration. Type **show system info** and press **Enter**. For example:

```
C1|S5|L1D>show system info
system descr:           The C3230-1040 of the Transition networks
                        ION (Chassis Generation III) platform products
system objectID:       1.3.6.1.4.1.868.2.5.1802661751
system uptime:         1 day, 04:56:04
system contact:        support
system name:           C3230-1040
system location:       headquarters
C1|S5|L1D>
```

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

System Configuration – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. At the **MAIN** tab, locate the **System Configuration** section.



3. In the **System Name** field, enter the name and for the x323x device. The name can be alphabetic, numeric or a combination. Do not enter spaces between System Name characters.
4. In the **System Contact** field, enter the name and information of the person to contact if there is a problem with the system. The name and information can be alphabetic, numeric or a combination.
5. In the **System Location** field, enter the information describing the physical location of where the system is located (e.g., room 110, IT lab, etc.). The information can be alphabetic, numeric or a combination.
6. In the **Console Access** field, select:
 - **Enabled** – allows communications through the USB serial interface (usually to a PC for entering CLI commands).
 - **Disabled** – communications through the USB serial interface is not allowed (CLI commands can only be entered through a Telnet session).
7. Verify the value displayed in the **Configuration Mode** field. The NID has a jumper that disables software management of the NID. When the **Configuration Mode** field displays **Hardware**, the NID takes some of its configuration from DIP switches or jumpers on the NID. In **Software** mode, all configuration parameters are controlled by management. Refer to the “[Jumper Settings](#)” section on page 450 for details on **Hardware** mode configuration.
8. When done, scroll to the bottom and click **Save**.

Device Description Configuration

The x323x supports a Device Description at the device level and a Circuit ID at the port level.

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

The Device Description can be configured in the x323x using either the CLI or Web method.

Device Description– CLI Method

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

2. At the device’s command prompt type: **set device description=<xx> where:**

xx = the Device Description to be used for this device or port.

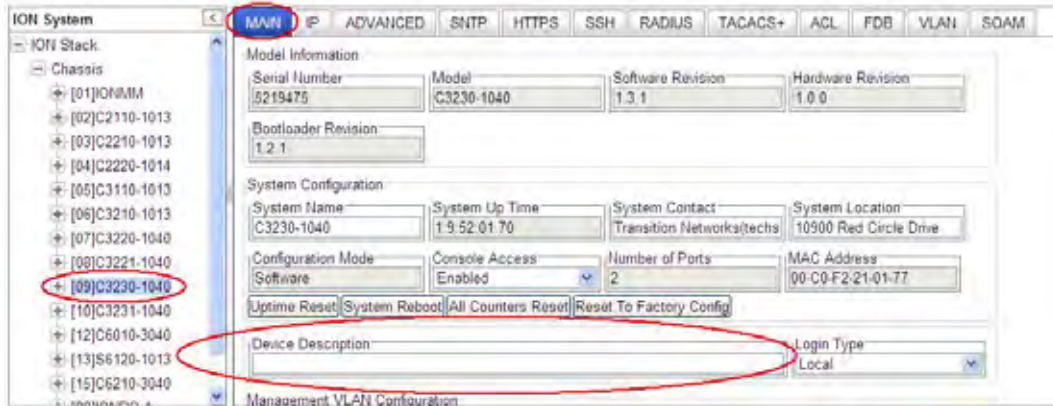
3. Press **Enter**.

4. Verify the Device Description setting. Type **show device description** and press **Enter**. Note that the dash (“-”) is required, and the letters “ID” must be upper-case. The Device Description information displays. For example:

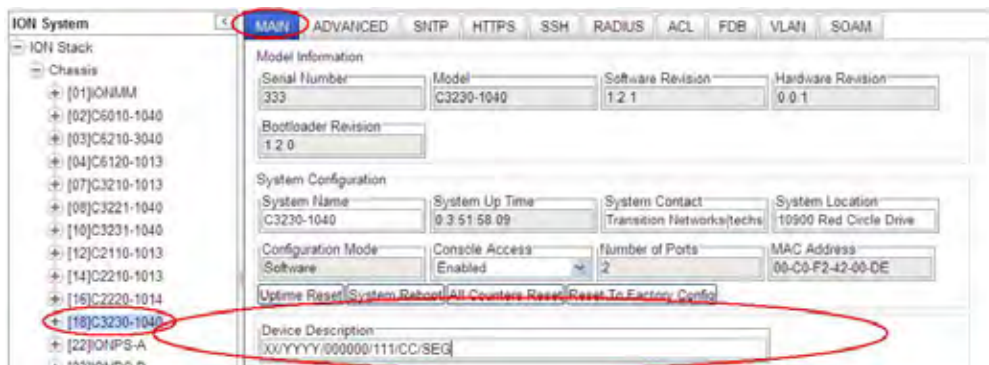
```
Agent III C1|S9|L1P1>set device description zzzzzzz
Error: this command should be executed on a device!
Agent III C1|S9|L1P1>go l1d
Agent III C1|S9|L1D>set device description zzzzzzz
Agent III C1|S9|L1D>show device description
Device description: zzzzzzz
Agent III C1|S9|L1D>
```

Device Description Config – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. At the x323x **MAIN** tab, locate the **Device Description** section.



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



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

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

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

Circuit ID Configuration

The x323x supports a Device Description at the device level and a Circuit ID at the port level.

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

The Circuit ID can be configured in the x323x using either the CLI or Web method.

Circuit ID Config – CLI Method

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

2. At the device’s command prompt type: **set circuit-ID=<xx> where:**

xx = the Circuit ID to be used for this device or port.

3. Press **Enter**.

4. Verify the Circuit ID setting. Type **show circuit-ID** and press **Enter**. Note that the dash (“-”) is required, and the letters “ID” must be upper-case. The Circuit ID information displays. For example:

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

5. At the each of the device port’s command prompts, enter the Circuit ID as in step 2 and 3.

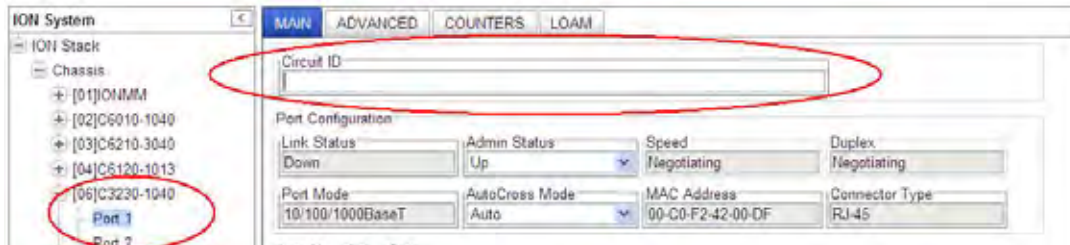
6. At the each of the device port’s command prompts, verify the Circuit ID setting as in step 4. For example:

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

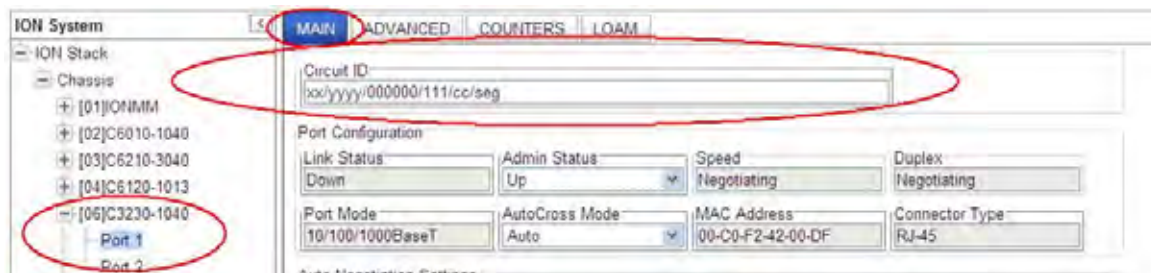
C1|S16|L1P1>go llp=2
C1|S16|L1P2>set circuit XX/YYYY/000000/111/CC/SEG
C1|S16|L1P2>show circuit-ID
Circuit-ID:          XX/YYYY/000000/111/CC/SEG
C1|S16|L1P2>
```

Circuit ID Config – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port and locate the **Circuit ID** field.



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



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

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

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

Login Type Configuration (Local / RADIUS / TACACS+)

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

You can configure the ION user login method via either the CLI or Web method. See the “[ION IPv6 Configuration Considerations](#)” section on page 116.

Login Type Config – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Check the current Login Type configuration. Type **show tacplus config** and press **Enter**.
3. Set the desired login method. If more than just “local” login is required, sets the login sequence (order of login validation). Type **set login method=type**, where:
type = (local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal), and:

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

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

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

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

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

4. Verify the TACACS+ and/or RADIUS configuration. For example:

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

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



```

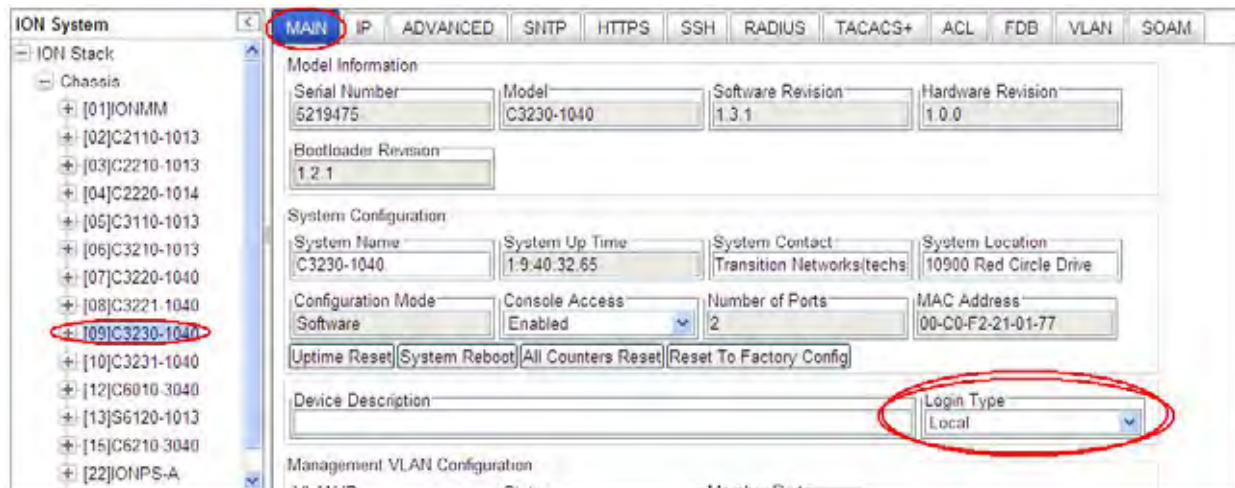
Agent III C1|S1|L1P1>set tacplus ?
  client
  svr
Agent III C1|S1|L1P1>set tacplus client state ?
  disable
  enable
Agent III C1|S1|L1P1>set tacplus svr 1 ?
  retry
  secret
  timeout
  type
Agent III C1|S1|L1D>set tacplus svr 1 retry 3
Agent III C1|S1|L1D>set tacplus svr 1 secret Buffrey1
Agent III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

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

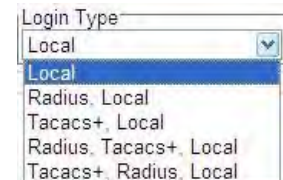
```

Login Type Config – Web Method

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



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



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

3. Verify your selection and continue configuration.

Ports Configuration

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

Configuring AutoCross

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

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

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

The x323x *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection, making the distinction between a straight through cable and a crossover cable unimportant.

Note:

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

The Auto Cross feature can be configured in the x323x using either the CLI or Web method.

AutoCross Config – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).

2. At the device port’s command line, type: **set ether autocross=xx** where:

xx = cable type. Valid choices are:

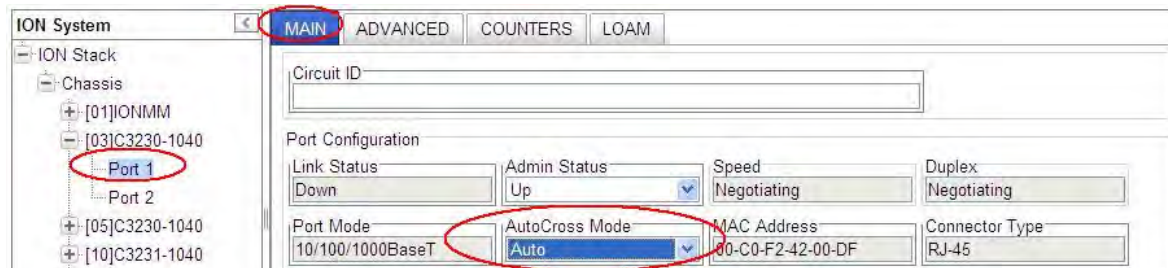
- **Auto** – hardware will automatically correct errors in cable selection.
- **MDI** – transmit pair on one end of the cable is connected to the receive pair on the other end.
- **MDIX** – cross over cable is used.

3. Press **Enter**.

Section 4: Configuration

AutoCross Config – Web Method

1. Access the x323x via the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port.



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

Configuring Auto Negotiation

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

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

- speed
- duplex
- pause capability (whether Pause frames are supported)

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

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

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

10/100/1000BaseT Port – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).

2. At the command line, type: **set ether autoneg state=xx**

where:

xx = **enable** or **disable**

3. Press **Enter**.

Section 4: Configuration

4. Is auto negotiation enabled or disabled?

Enabled	Disabled
Go to Step 5.	Go to Step 9.

5. Set the advertised speed/duplex capabilities; type:

set ether adv-cap

where:

xx = advertised speed capability; valid choices are:

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

To specify more than one capability use a plus sign (+) between entries (e.g., adv-cap=10TFD+100TFD+1000THD)

6. Press **Enter**.

7. Set the advertised pause frame capability; type: **set ether pause=xx**

where:

xx = advertised pause capability; valid choices are:

- **nopause** (the port will advertise that it 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)

8. Press **Enter**.

9. Set the speed of this port; type: **set ether speed=xx**

where:

xx = speed setting; valid choices are:

- **10M**
- **100M**
- **1000M**

10. Press **Enter**.

11. Set the duplex of this port; type: **set ether duplex=xx**

where:

xx = duplex setting; valid choices are:

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

12. Press **Enter**.

13. Verify the configuration has been set. Type: **show ether config**

14. Press **Enter**. The Ethernet configuration displays:

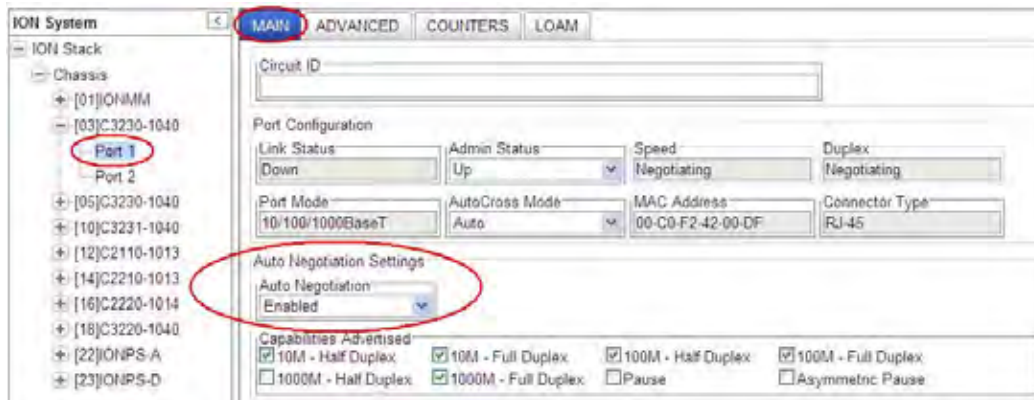
```
Agent III C1|S9|L1P1>show ether config
Port-11040
TP port:
-----
Link operation status:      down
Admin status:              up
Port mode:                 RJ-45
PHY operation mode:        phy10-100-1000BaseT
Speed:                     Negotiating
Duplex:                    Negotiating
Autocross:                 auto
PHY mode change cap:      false

AutoNeg admin state:      enable
Advertisement:
Capability:                10THD+10TFD+100THD+100TFD+1000TFD
Pause:                     nopause
Agent III C1|S9|L1P1>
```

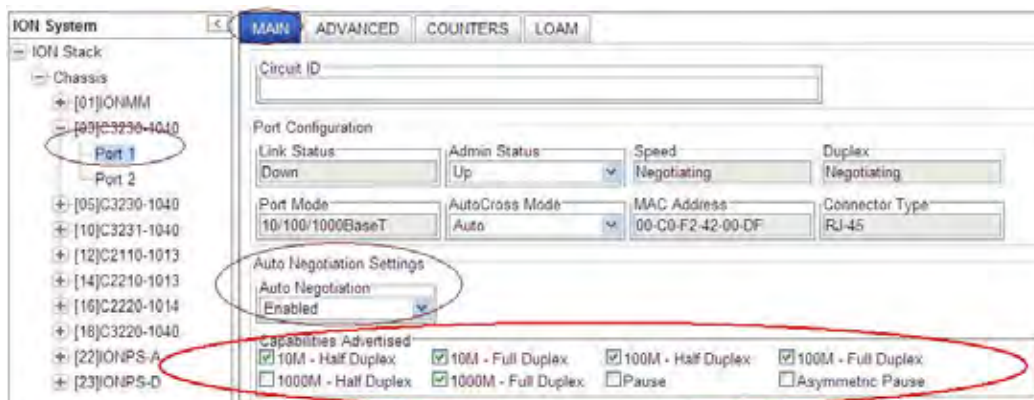
Section 4: Configuration

10/100/1000BaseT Port – Web Method

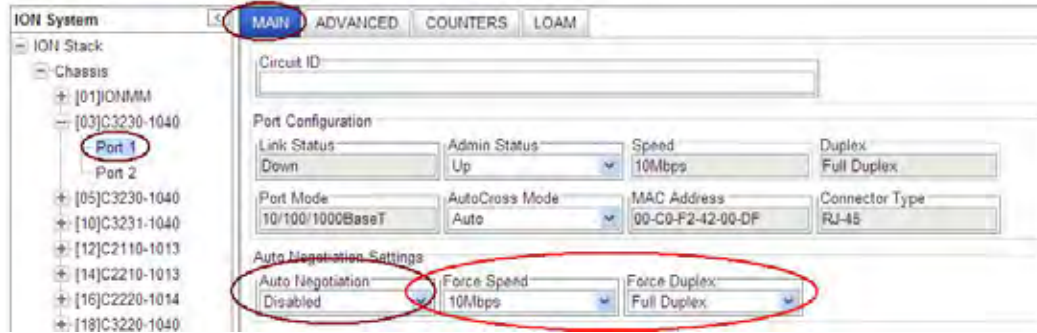
1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port. Select the port’s **MAIN** tab if not already displayed.
3. Locate the **Auto Negotiation Settings** section.



4. In the **Auto Negotiation** field, select whether this feature is enabled or disabled.



5. If **Auto Negotiation** is set to **Enabled** (as shown above), in the **Capabilities Advised** field, select:
 - the speed and duplex settings to be advertised to other devices,
 - the type of pause frames supported on this port (**Pause** and/or **Asymmetric Pause**).



6. To select Auto Negotiation disabled, select **Disabled** from the drop down and then click **Save**. The **Force Speed** and **Force Duplex** fields display (as shown above).
7. With **Auto Negotiation** set to **Disabled**, select:
 - the port's operating speed (10Mbps or 100Mbps) in the **Force Speed** field,
 - the port's duplex mode of operation (Half Duplex or Full Duplex) in the **Force Duplex** field.
8. Click **Save** when done.

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

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

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

A port's Ethernet port speed and Duplex mode can be configured in the x323x using either the CLI or Web method.

Set Ethernet Port Speed / Duplex Mode – CLI Method

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

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

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the command line, type: **set ether autoneg state disable** and press **Enter**.
3. Set the speed of this port; type: **set ether speed=xx** where:
 - xx** = speed setting; valid choices are:
 - **10M**
 - **100M**
 - **1000M**
4. Press **Enter**.
5. Set the Duplex mode for this port; type: **set ether duplex=xx** where:
 - xx** = duplex setting; valid choices are:
 - **full**
 - **half**
6. Press **Enter**.
7. Verify the configuration has been set. Type: **show ether config**
8. Press **Enter**. The Ethernet configuration displays.

The first example below show a TP port, the second example shows a Fiber Port:

```

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>

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>

```

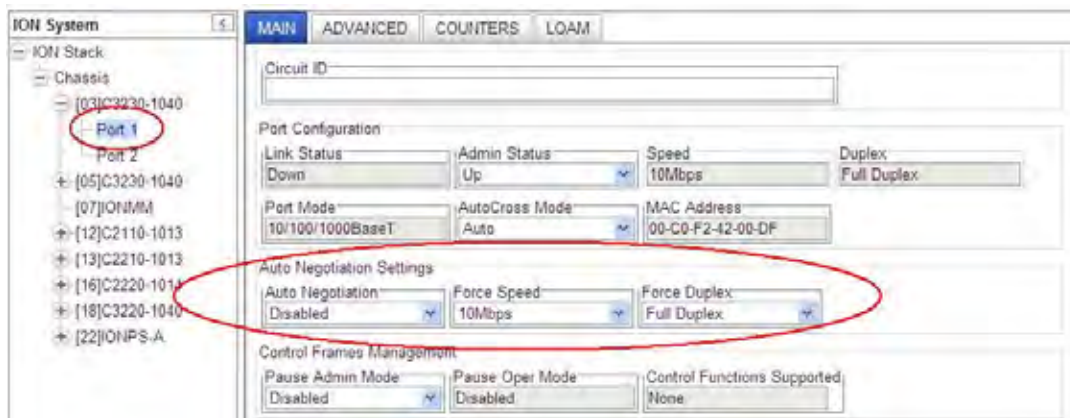
Section 4: Configuration

Set Ethernet Port Speed / Duplex Mode – Web Method

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

Note: This function only applies to a copper port.

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



4. Set **Auto Negotiation** to **Disabled** and then click **Save**. The **Force Speed** and **Force Duplex** sections display.
5. Select the copper port’s Ethernet operating speed (e.g., 10M | 100M | 1000M, or 10M | 100M). The default is 10 M bps.
6. Select the port’s Duplex mode of operation (Half Duplex | Full Duplex). The default is Full Duplex.
7. Click **Save** when done.

Set Port Admin Mode (Ethernet PHY Mode)

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

The C3220-1040 and C3221-1040 NIDs support SGMII with 10/100/1000BASE-T copper SFPs. The C3221-1040 NID has 10/100/1000BASE-T (RJ-45) [100 m] to two 100/1000Base-X open SFP slots. The C3231-1040 provides 10/100/1000BASE-T (RJ-45) [100 m] to two 100/1000Base-X open SFP slots. The SGMII (Serial Gigabit Media Independent Interface) provides network data and port speed information between a 10/100/1000 PHY and a MAC, operating in both half duplex and full duplex at all port speeds. If SGMII is configured, the auto negotiation feature is disabled.

A port’s Ethernet PHY mode can be configured in the x323x using either the CLI or Web method.

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

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

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the command line, type **set ether phymode=xx** and press **Enter**, where:
 - xx = port admin mode setting (SGMII|100BaseFX|1000BaseX – case sensitive); the valid choices are:
 - phySGMII
 - phy100BaseFX
 - phy1000BaseX
3. Verify the configuration has been set. Type **show ether config** and press **Enter**. The Ethernet configuration displays.

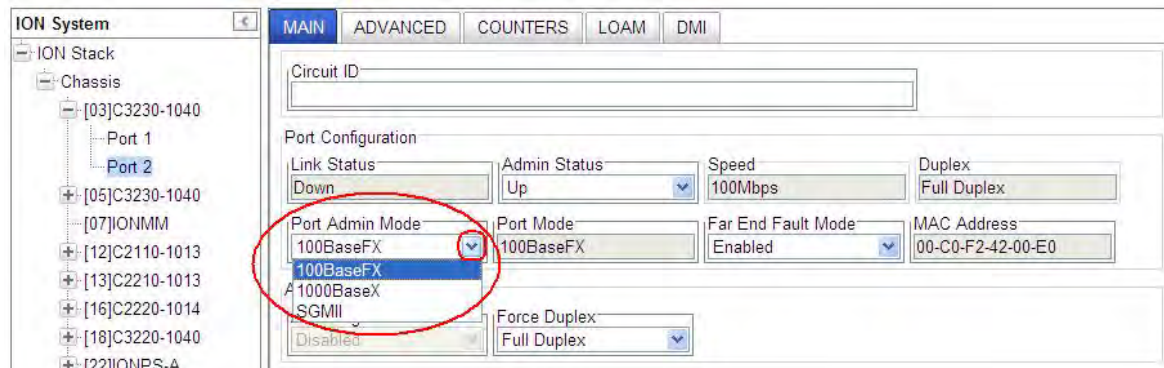
```
C1|S3|L1P1>set ether phymode ?
  phy1000BaseX
  phy100BaseFX
  phySGMII
C1|S3|L1P1>set ether phymode phySGMII
Cannot set PHY mode on this port!
C1|S3|L1P1>go l1p=2
C1|S3|L1P2>set ether phymode phySGMII
Agent III C1|S9|L1P2>show ether config
Port-21040
FIBER port:
-----
Link operation status:      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>
```

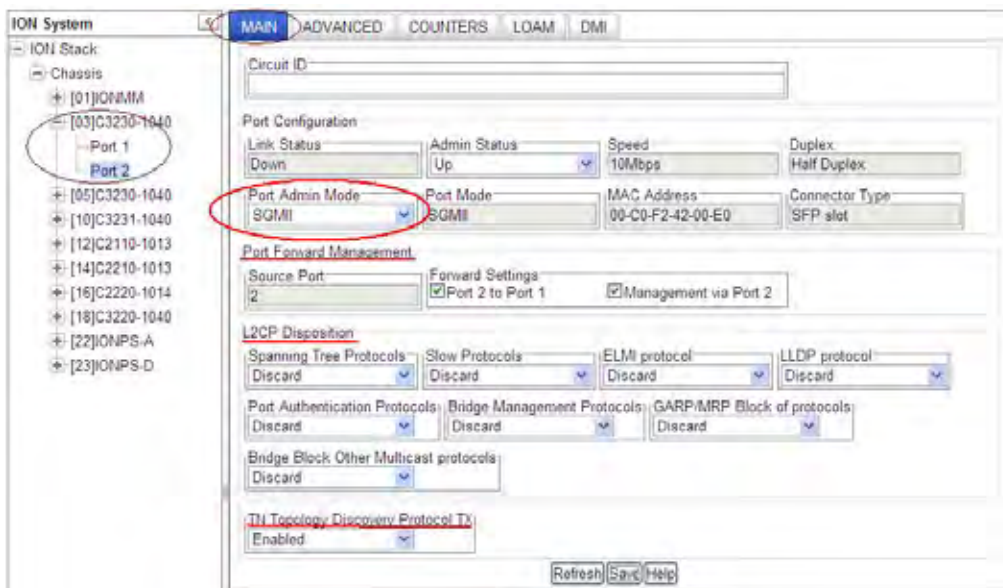
Section 4: Configuration

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

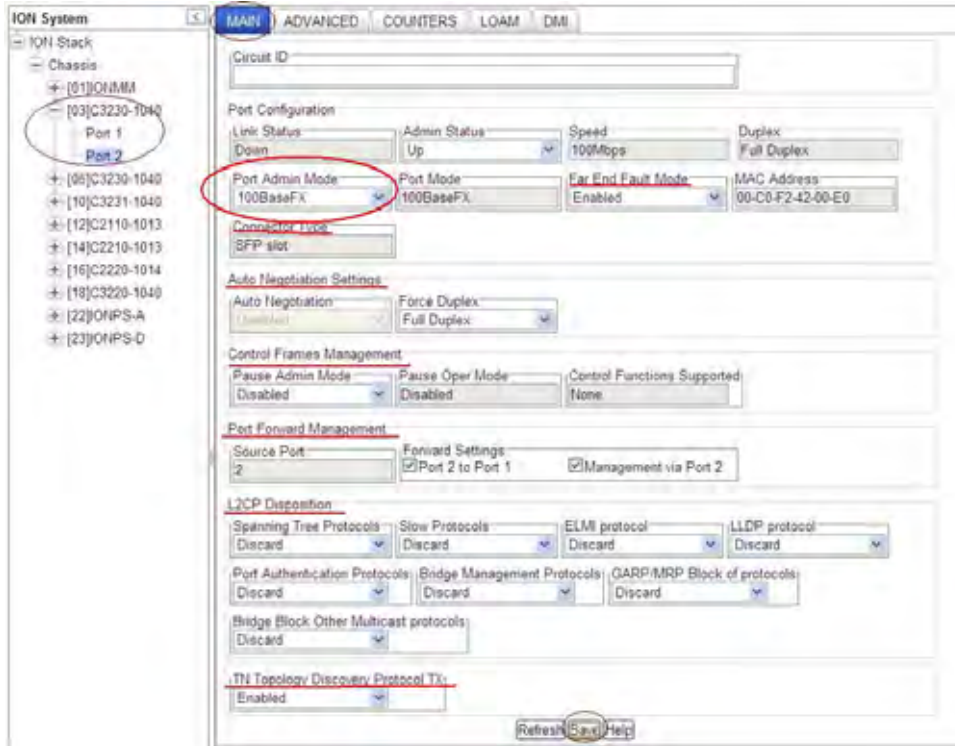
1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Locate the **Port Admin Mode** field on the Port 2 **MAIN** tab.



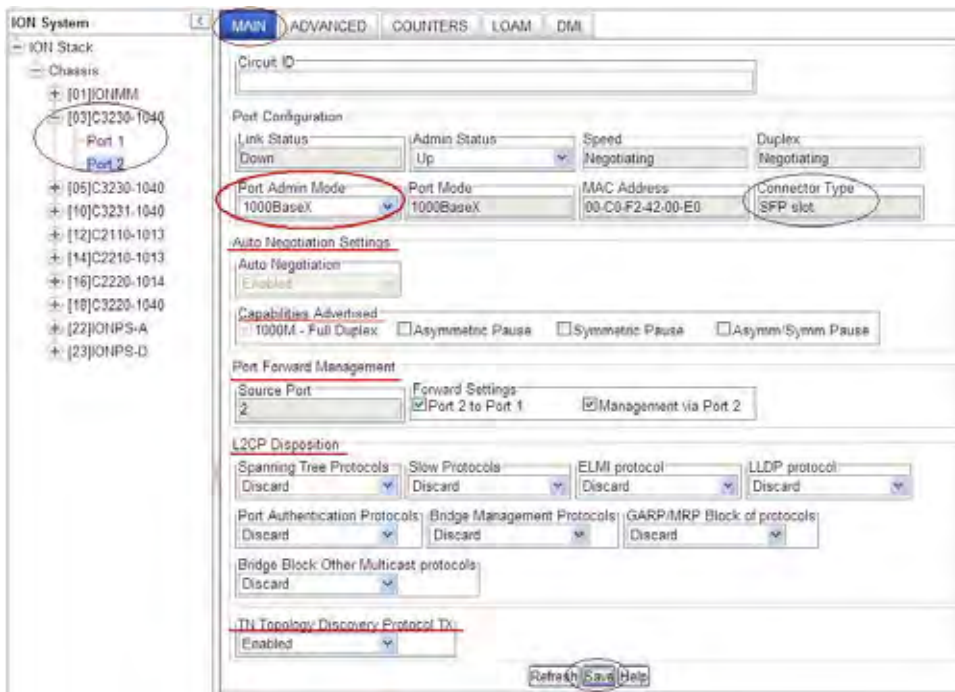
3. Select either **1000BaseX**, **1000BaseFX**, or **SGMII** for the port’s Ethernet PHY mode.
4. Click **Save**. The displayed function set changes based on the Port Admin Mode selected in step 3:



With **SGMII** selected (see above), the **Port Forward Management** and **L2CP Disposition** sections display. The **Connector Type** field displays **SFP slot**. The **Far End Fault** and **Control Frames Management** sections do not display with **SGMII** selected.



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



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

Far End Fault Mode Configuration

With Far End Fault (FEF) mode enabled, the x323x can track and report FEF capabilities and setting information.

The Far End Fault (FEF) mode can be configured on a 100M fiber port in the x323x using either the CLI or Web method. Note that the Far End Fault mode can not be enabled with SGMII selected as the Port Admin Mode (see the preceding section).

Far End Fault Mode Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the device’s command prompt type **set ether fef=xx** where:
 xx = {enable | disable}
3. Press **Enter**.
4. Use the **show ether config** command to verify the FEF mode capability and mode settings (e.g., Far End Fault cap: true, Far End Fault mode: enable). For example:

```
C1|S16|L1D>set ether fef=disable
C1|S16|L1D>go l1p=2
C1|S16|L1P2>show ether config
Port-21014
FIBER port:
-----
Link operation status:  down
Speed:                 Negotiating
Duplex:                Negotiating
Far End Fault cap:    true
Far End Fault mode:   enable
PHY mode change cap:  false
PHY operation mode:   phy100BaseFX

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

Note: Only a 100M fiber port can be set for Far End Fault enabled.

Set Bandwidth Allocation / Rate Limiting

The x323x Bandwidth Allocation (Rate Limiting) can be configured to limit both Ingress bandwidth and Egress bandwidth. If so configured, traffic at rates higher than this CIR (Committed Information Rate) is discarded. Note that these limits cannot be set faster than the port speed.

Bandwidth Allocation / Rate Limiting can be configured in the x323x NID using either the CLI or Web method.

Set Bandwidth Allocation / Rate Limiting – CLI Method

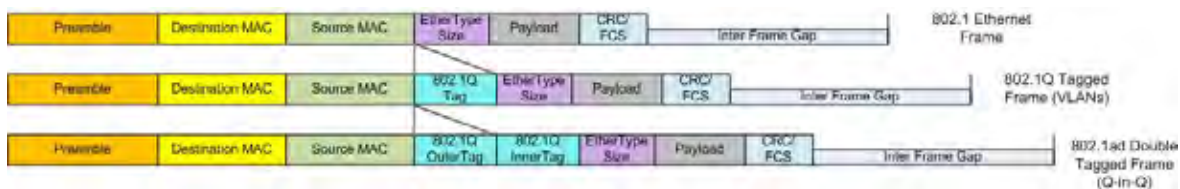
1. Access the x323x through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. At the command line, define which transmission layer is to be counted when determining the rate limit. Type `set bw alloc-type={countAllLayer1 | countAllLayer2 | countAllLayer3}`.

The default is **countAll Layer1** bytes.

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

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



3. Press **Enter**.

4. Define the ingress and egress rate limits of the port. Type `set irate=<xx> erate=<yy>`, where:

xx= In-rate: Ingress rate in bps.

yy = Egress-rate: Egress rate in bps.

5. Press **Enter**.

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

Section 4: Configuration

```

For example: C1 | S5 | L1P1 > set irate=rate1M erate=rate1M
C1 | S5 | L1P1 > show bandwidth allocation
Bandwidth allocation type:    countAllLayer2
Ingress rate:                 rate1M
Egress rate:                  rate1M
C1 | S5 | L1P1 > set irate=unLimit erate=unLimit
C1 | S5 | L1P1 > show bandwidth allocation
Bandwidth allocation type:    countAllLayer2
Ingress rate:                 unLimit
Egress rate:                  unLimit
C1 | S5 | L1P1 >

```

Note: The rate parameters are case-sensitive.

Rate Limits Summary

You can set ingress rate and egress rate of a port with increased granularity of Ingress/Egress Rate Limiting per MEF 11: 1 Mbps steps up to 10 Mbps, 5 Mbps steps beyond 10 Mbps and up to 100 Mbps, and 50 Mbps steps beyond 100 Mbps and up to 1 Gbps.

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.

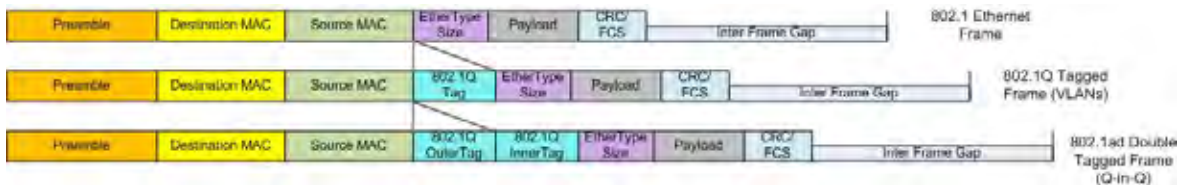
Set Bandwidth Allocation / Rate Limiting – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port’s **ADVANCED** tab.
3. Locate the **Bandwidth Allocation** section.



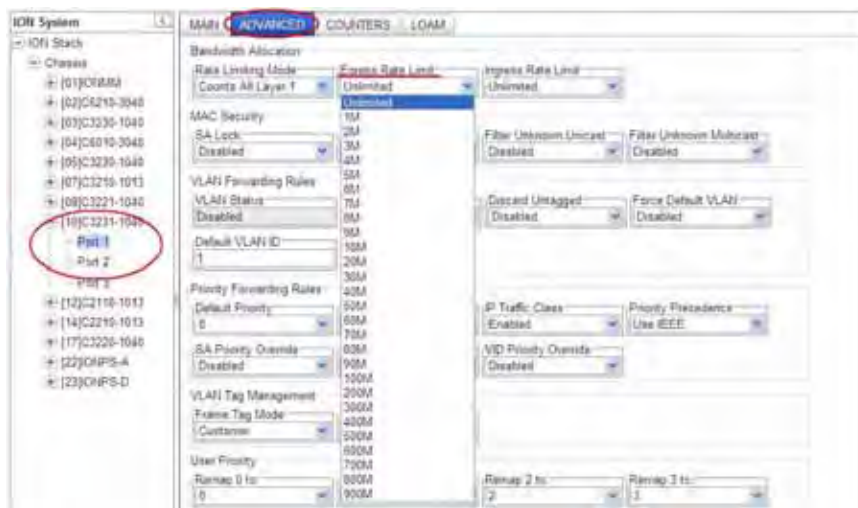
4. In the **Rate Limiting Mode** field, select which bytes in a frame are to be counted in determining the rate limit:
 - **Counts All Layer 1:** (the default): in determining the rate limit, this selection counts the following bytes in a frame: Preamble (8 Bytes) + DA to CRC + Inter Frame Gap (12 bytes).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

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

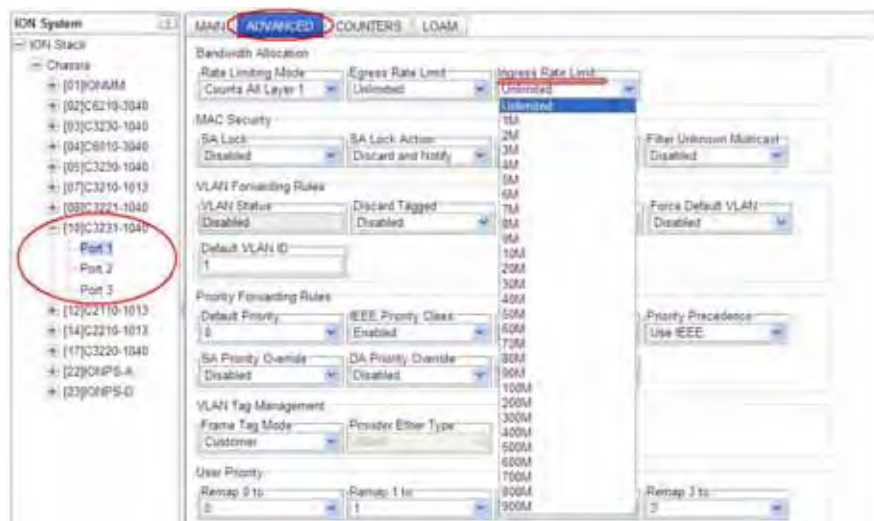


Section 4: Configuration

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



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



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

Rate Limits Summary

You can set ingress rate and egress rate of a port with increased granularity of Ingress/Egress Rate Limiting per MEF 11: 1 Mbps steps up to 10 Mbps, 5 Mbps steps beyond 10 Mbps and up to 100 Mbps, and 50 Mbps steps beyond 100 Mbps and up to 1 Gbps.

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.

Configuring Priority Queuing

The x323x lets you configure the Egress Queue mode to either “Weighted Round Robin (WRR)” or “Strict” via either the CLI or the Web interface.

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

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

Priority Queuing Config – CLI Method

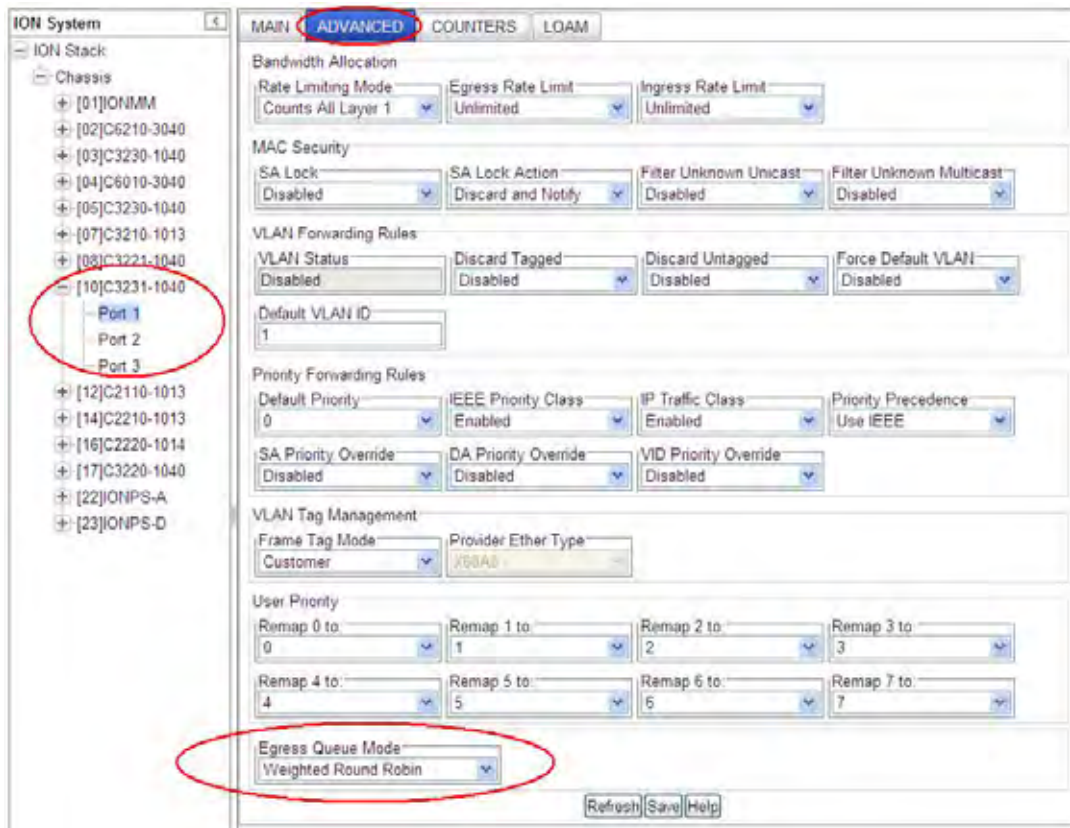
1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the command line, use the **go** command to switch to port 1.
3. Define the port queuing method. Type `set port queuingmethod=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

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

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

Priority Queuing Config – Web Method

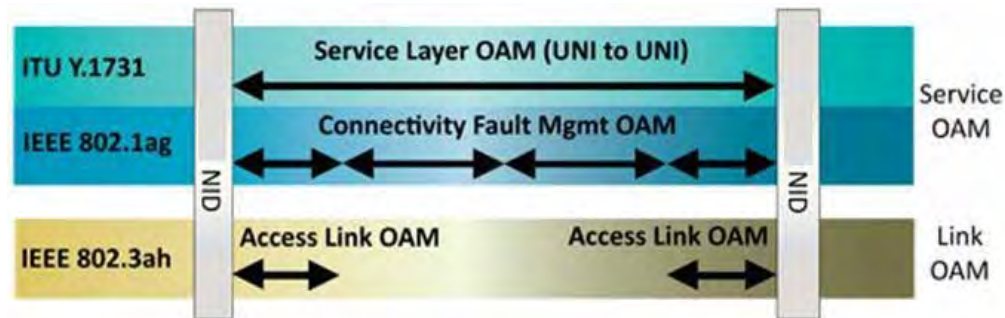
1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the Port 1 **ADVANCED** tab.
3. Locate the **Egress Queue Mode** field.



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

Configuring Ethernet OAM

Ethernet Operations, Administration and Maintenance (OAM) protocol is used for monitoring and troubleshooting Ethernet networks. Ethernet Service Operations, Administration and Maintenance (SOAM) standards from the IEEE, ITU-T and MEF provide end-to-end connectivity fault management and performance monitoring across multiple operator networks.



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

LOAM (Link OAM) Configuration

The x323x NID supports the Link OAM standard IEEE 802.3–2005 Clause 57 which defines mechanisms for monitoring and troubleshooting Ethernet access links. Specifically it defines tools for discovery, remote failure indication, remote and local loopback, and status and performance monitoring.

LOAM Configuration Prerequisites and Restrictions

For the latest feature information and caveats, see the release notes for your particular device/system and software release. The prerequisites and restrictions below apply to C3230, C3231, S3230, and S3231 models unless otherwise noted.

The x323x products implement LOAM on both the fiber and twisted pair interfaces. The LOAM enabled port is user selectable. By default, the fiber port is the default LOAM enabled port. With dual fiber ports, Port 2 is the default.

LOAM Configuration Prerequisites

1. Network topology and network administration have been reviewed.
2. Business and service policies have been established.
3. In a typical application, you connect a cable from the Active local device (chassis) to the Passive remote device. The Active local device manages its Passive remote peer. The relationship between the Active local device and its Passive remote peer is established via **LOAM** functionality.
4. To change any of the IP parameters through the CLI interface, the management state must be enabled (see “[Performing Initial System Setup](#)” on page 71).
5. To remotely manage specific OAM critical events, set up SNMP trap host managers in the IONMM (see “[Configuring SNMP](#)” on page 227 for set-up instructions).

6. The x323x supports both private and public MIBs for SNMP management including RFC 4878 (Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM)). See “[Supported MIBs](#)” on page 29 for more information.
7. Provisioning a standalone S323x for remote operation without IONMM management requires a change to the switch mode. By default, the S323x is managed by the ION MM. Setting the switch mode to local indicates that the device is not managed by the IONMM, but by either a direct USB connection or a direct network connection via Telnet or the Web interface. Setting the mode to remote indicates that the device is managed through the IONMM. Use the **set switch mode=** command to change management mode between local and remote. To change any of the IP parameters through the CLI interface, the management state must be enabled.

LOAM Configuration Restrictions

1. The x323x NIDs do not support variable retrieval nor unidirectional link. They support loopback and event notifications only.
2. LOAM on Ethernet interfaces may be in 'Active' mode or 'Passive' mode. These two modes differ in that Active mode provides additional capabilities to initiate monitoring activities with the remote LOAM peer entity, while Passive mode generally waits for the peer to initiate LOAM actions with it. For example, an active LOAM entity can put the remote LOAM entity in a loopback state, where a passive OA entity cannot.

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

LOAM can be configured in the x323x using either the CLI or Web method.

LOAM Config – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).

Go to the port where LOAM is to operate (use the **go** command). The **go** command format is:

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

(for a slide in card), or

```
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

(for a standalone card).

2. Enable LOAM for the port. Type: **set loam admin state=enable** and press **Enter**.
3. Set the OAM operating mode. Type:

```
set loam mode=<xx>
```

where:

xx = operating mode:

- **active** –the x323x sends out discovery frames (OAM Information PDUs). It can initiate OAM Loopback to its remote peer.

Section 4: Configuration

- **passive** – the x323x can receive and respond to discovery messages (LOAM Information PDUs). It can not initiate LOAM Loopback but can process loopback requests from a LOAM Peer in active mode.
4. Enable or disable Event notifications and define the values associated with the events. The table below describes the various events and the commands associated with them.

Table 12: LOAM Events

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

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

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

<p>Window Value</p>	<p>The threshold window in which the threshold value must occur before an event notification is sent.</p> <p>set loam esp window high=<xx> low=<yy></p> <p>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.</p> <p>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.</p>
---------------------	--

For example:

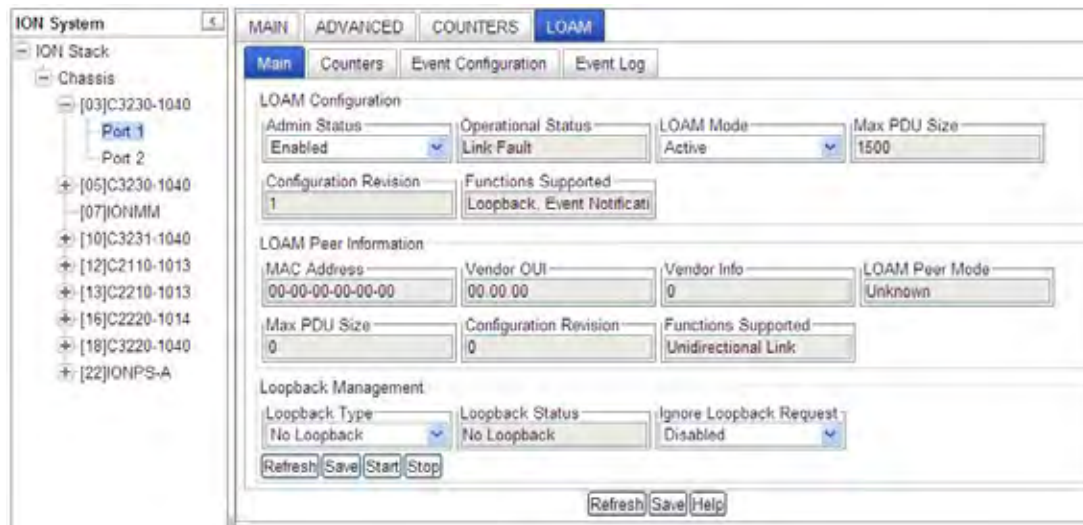
```

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

```

LOAM Config – Web Method

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

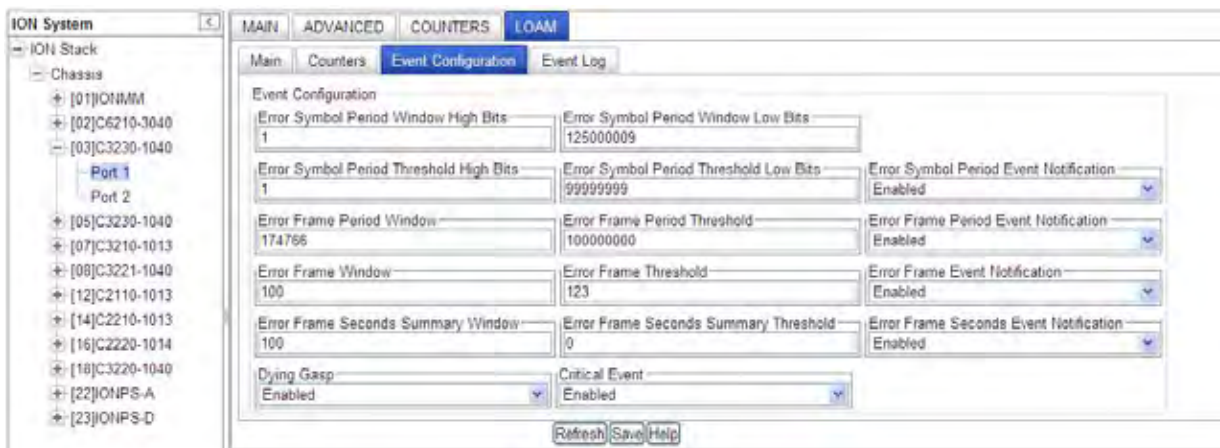


4. In the **Admin Status** field, select **Enabled**.
5. In the **LOAM Mode** field, select the operating mode:
 - **Active** – the NID can initiate LOAM communications and can issue queries and commands to a peer device. When in Active mode, the NID sends out discovery frames (OAM Information PDU).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

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

6. Locate the **Loopback Management** section.

7. In the **Loopback Type** field, select the operating mode:
 - **No Loopback** – disables LOAM loopback testing.
 - **Remote Peer**- prevents that port from forwarding data frames to other ports when it goes into “loopback” mode. (AKA “intrusive loopback”).
 - **Alternate** – allows the data frames to be forwarded to other ports, while doing the loopback with its peer.
8. The **Loopback Status** field displays the loopback status for this interface when enabled. The only two possible values for a SET operation are *initiateLoopback(2)* and *terminateLoopback(3)*. All other values are read-only to show the status of the loopback operation (No Loopback, Local in Loopback, Remote in Loopback).
9. In the **Ignore Loopback Request** field, select:
 - **Enabled** – causes the LOAM enabled x323x NID to ignore all Loopback requests (i.e., not respond to remote loopback requests from peers).
 - **Disabled** – causes the LOAM enabled x323x NID to respond to all remote loopback requests from peers.
10. Click **Save** to perform the loopback action. Click **Start** to begin the loopback request; click **Stop** to end the loopback request.
11. Select the **Event Configuration** sub-tab.



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

Section 4: Configuration

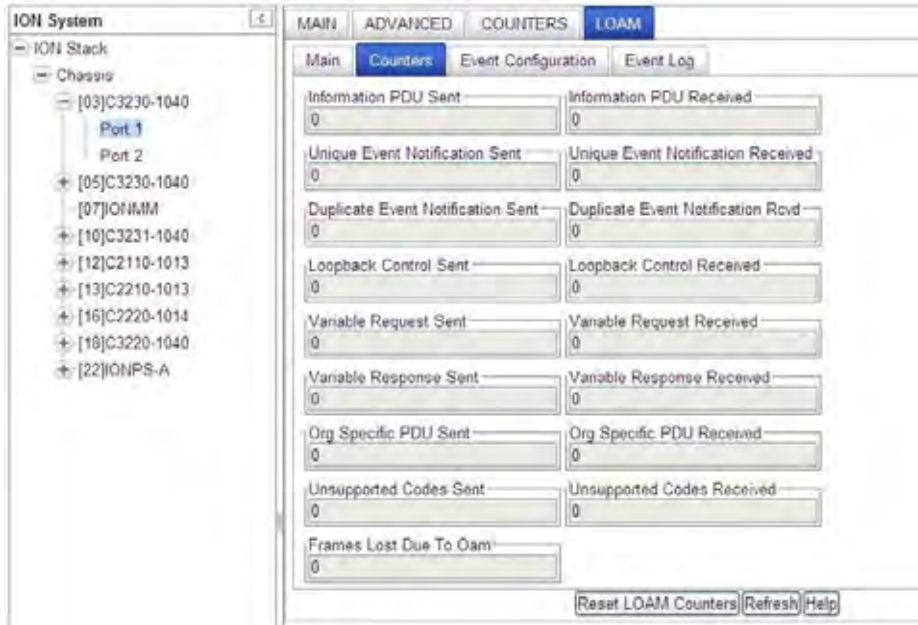
13. For the Event Notifications enabled in step 12, enter the appropriate values for the related window and threshold fields (defaults are shown in parenthesis):

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

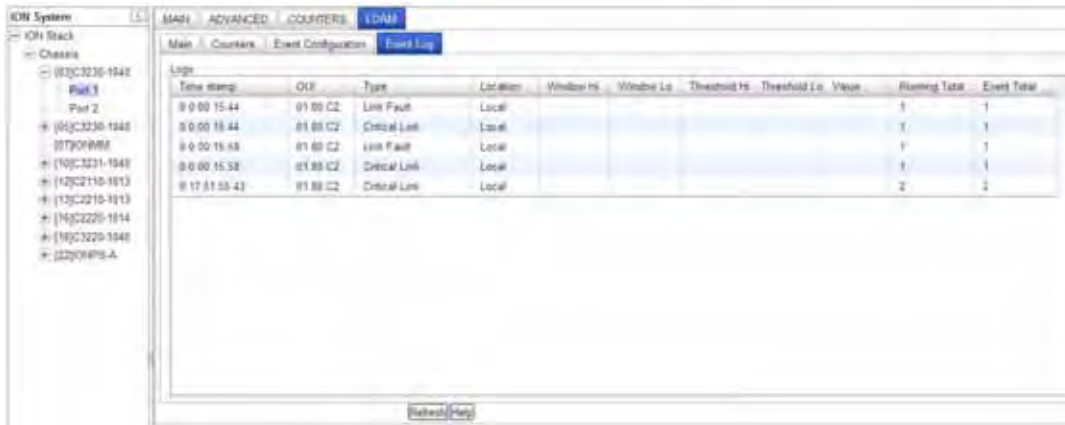
Threshold Value: The number of frame errors that must occur within the defined window before notification of this event is made.

Window Value: The amount of time (in 100ms increments) in which the threshold value must occur before an event notification is sent.

14. Enable or disable the **Dying Gasp** function as needed. The default is **Enabled** (OAM notification is done for a loss of power condition).
15. Enable or Disable the **Critical Event** function as needed. The default is **Enabled** (OAM notification is performed for critical events).
16. Click the **Save** button.
17. Select the **Counters** sub-tab.



18. To update Counters information, click the **Refresh** button.
To reset Counters to zero, click the **Reset LOAM Counters** button.
19. Select the **Event Log** sub-tab.
20. Click the **Refresh** button. Updated Event Log information displays.



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

Section 4: Configuration

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

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

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

22. The **Location** column identifies whether the event report was for a local or remote device.

23. When the **OUI** (Organizationally Unique Identifier) column displays something other than **01.80.C2**, then an organization other than IEEE 802.3 has defined the event space. When the **OUI** column displays **01.80.C2** (the IEEE 802.3 OUI), the following event types are defined:

- **Errored Symbol Event** – a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of symbol errors exceeds a threshold within a given window by a number of symbols (e.g., 1,000 symbols out of 1,000,000 had errors).
- **Errored Frame Period Event** - a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of frame errors exceeds a threshold within a given window defined by a number of frames (e.g., 10 frames out of 1000 had errors).
- **Errored Frame Event** - a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of frame errors exceeds a threshold within a given window defined by a period of time (e.g., 10 frames in 1 second had errors).
- **Errored Frame Seconds Event** - a threshold crossing event, generated when a metric exceeds a given value within a specified window. Generated when the number of errored frame seconds exceeds a threshold within a given time period (e.g., 10 errored frame seconds

within the last 100 seconds). An errored frame second is defined as a 1 second interval which had more than 0 frame errors.

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

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

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

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

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

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

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

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

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

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

Section 4: Configuration

Event Notification (for example, 51 when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset).

LOAM Operational Status

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

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

Disabled - This value is always Disabled(1) if LOAM is disabled on this interface via the 'Admin Status'.

LinkFault - If the link has detected a fault and is transmitting OAMPDUs with a link fault indication, the value is LinkFault(2). Also, if the interface is not operational ('Link Status' is not Up(1)), LinkFault(2) is returned. Note that the object 'Link Status' may not be Up(1) as a result of link failure or administrative action (ifAdminState being Down(2) or Testing(3)).

PassiveWait - The PassiveWait(3) state is returned only by LOAM entities in passive mode ('LOAM Mode') and reflects the state in which the LOAM entity is waiting to see if the peer device is OA capable.

Active Send Local - The Active Send Local(4) value is used by active mode devices ('LOAM Mode') and reflects the LOAM entity actively trying to discover whether the peer has LOAM capability but has not yet made that determination.

SendLocalAndRemote - The state SendLocalAndRemote(5) reflects that the local OA entity has discovered the peer but has not yet accepted or rejected the configuration of the peer. The local device can, for whatever reason, decide that the peer device is unacceptable and decline LOAM peering.

SendLocalAndRemoteOk - If the LOAM peering is allowed by the local device, the state moves to SendLocalAndRemoteOk(6).

OamPeeringLocallyRejected - If the local LOAM entity rejects the peer LOAM entity, the state becomes OamPeeringLocallyRejected(7). Note that both the SendLocalAndRemote(5) and OamPeeringLocallyRejected(7) states fall within the state SEND_LOCAL_REMOTE of the Discovery state diagram [see 802.3ah, Figure 57-5], with the difference being whether the local LOAM client has actively rejected the peering or has just not indicated any decision yet. Whether a peering decision has been made is indicated via the local flags field in the OAMPDU (reflected in the aOAMLocalFlagsField of 30.3.6.1.10).

OamPeeringRemotelyRejected - If the remote LOAM entity rejects the peering, the state becomes OamPeeringRemotelyRejected(8). Note that both the SendLocalAndRemoteOk(6) and OamPeeringRemotelyRejected(8) states fall within the state SEND_LOCAL_REMOTE_OK of the Discovery state diagram [802.3ah, Figure 57-5], with the difference being whether the remote LOAM client has rejected the peering or has just not yet decided. This is indicated via the remote flags field in the OAMPDU (reflected in the aOAMRemoteFlagsField of 30.3.6.1.11).

Operational - When the local LOAM entity learns that both it and the remote LOAM entity have accepted the peering, the state moves to Operational(9) corresponding to the SEND_ANY state of the Discovery state diagram [802.3ah, Figure 57-5].

NonOperHalfDuplex - Since Ethernet LOAM functions are not designed to work completely over half-duplex interfaces, the value NonOperHalfDuplex(10) is returned whenever Ethernet LOAM is enabled ('Admin Status' is Enabled(1)), but the interface is in half-duplex operation.

LOAM Peer Information Fields

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

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

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

Vendor Info – e.g., 0 or 1.

LOAM Peer Mode – e.g., Active, Passive, Unknown. This object configures the mode of LOAM operation for this Ethernet-like interface. LOAM on Ethernet interfaces may be in 'Active' mode or 'Passive' mode. These two modes differ in that active mode provides additional capabilities to initiate monitoring activities with the remote LOAM peer entity, while passive mode generally waits for the peer to initiate OA actions with it. As an example, an active LOAM entity can put the remote LOAM entity in a loopback state, where a passive OA entity cannot. The default value of *dot3OamMode* is dependent on the type of system on which this Ethernet-like interface resides. The value should be 'Active(2)' unless it is known that this system should take on a subservient role to the other device connected over this interface. Changing this value results in incrementing the configuration revision field of locally generated OAMPDUs and potentially re-doing the LOAM discovery process if the 'Operational Status' was already Operational.

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

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

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

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

Section 4: Configuration

- 'Variable Request and Response(3)' indicates that the LOAM entity can send and receive Variable Request and Response OAMPDUs.

The default value of "**LOAM Configuration > Functions Supported**" is "Loopback, Event Notification". Note that the x323x NIDs do not support variable retrieval nor unidirectional link.

LOAM Event Configuration Default Values and Valid Ranges

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

802.3 LOAM Event	Default Value	Low Limit	High Limit
ErrSymPeriodWindowHi	0	0	0x0FFFFFFF
ErrSymPeriodWindowLo	0x07735940	1	0x0FFFFFFF
ErrSymPeriodThreshold Hi	0	0	0x0FFFFFFF
ErrSymPeriodThresholdLo	1	0	0x0FFFFFFF
ErrFramePeriodWindow	0x1AAAAA	1	0x63FFFFD8
ErrFramePeriodThreshold	1	0	0x0FFFFFFF
ErrFrameWindow	10	10	600
ErrFrameThreshold	1	0	0x0FFFFFFF
ErrFrameSecsSummaryWindow	100	100	9000
ErrFrameSecsSummaryThreshold	1	0	9000

Last Gasp / Dying Gasp Management

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

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

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

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

Copper Port Loopback Procedure

The procedure below is for performing a copper Port Loopback via direct link between a C3230 and an S3230. In this procedure, the S3230 Port1 is connected to a switch, and a Management PC is also connected this switch so the Management PC can reach the S3230 or C3230. There are no other devices between C3230 and S3230; if you connect a device between S3230 and C3230, make sure this device can forward LOAM messages.

In this example, the LOAM settings of port 1 of the C3230 and port 1 of S3230:

C3230 Port 1 LOAM Mode = Active, **Admin Status** = Enabled

S3230 Port 1 LOAM Mode = Passive, **Admin Status** = Enabled

You can inter-change LOAM Active/Passive modes between the C3230 and S3230 (be sure one is **Active** the other is **Passive**).

This procedure has an ION chassis with a C3230 and a stand-alone S3230 when using the web interface method:

1. Make sure the copper ports on both sides show **Links Status = Up** when you run the loopback test from one of the copper sides (local or remote side). See Figure 1 for this sample Loopback Configuration.
2. For all S3230 and C3230 copper and fiber ports, set LOAM **Admin Mode** to **Enabled** (at **x323x > Port 1 > LOAM > Main > Admin Status = Enabled**).
3. One side of copper port can be LOAM **Admin Status = Active** and other can be **Passive**; or both can be **Active**.
4. One of the Fiber ports LOAM **Admin Status** must be **Active** for the MAC address to display.
5. At both the C3230 and the S3230, at the **Loopback Type** dropdown, select **Remote Peer**.
6. From the Active side, click the **Start** button to begin the loopback test; you may have to wait a minute or more for the loopback test to start.
7. Verify the **Operational Status** on both sides (**Operational** or **Passive Wait**). Click Refresh if necessary.
8. Verify the **Loopback Status** (**Remote in Loopback** on the local side, **Local in Loopback** on the remote side).
9. At both the C3230 and the S3230 **Port 1 > LOAM > Main > Counters** tab, compare the counters data (e.g., Information PDU Sent, Information PDU Received, Unique Event Notification Sent, Unique Event Notification Received, Loopback Control Sent, Loopback Control Received, etc.). See Figure 2 for sample Loopback Counters information.
10. Click the **Refresh** button to update the **Counters** data as desired.
11. When done click the **Stop** button on the Active side. The Loopback Status changes to **No Loopback**.
12. When the test results are completed as required, click the **Reset LOAM Counters** on both sides. (You may have to click the Reset LOAM Counters button twice, or click Reset LOAM Counters and then click Refresh to clear the counters.) The counters will begin incrementing again immediately.

Each time you change the loopback configuration and run a loopback test, the **Configuration Revision** field increments by one on both sides.

Note that there is a field in the GUI for the MAC address, but you cannot add a MAC peer address to the GUI or via the CLI.

If the cable between the C3230 and the S3230 is disconnected, the remote S3230 fields display in red boxes (at both the device level and at the port level). To recover, plug the cable back in and on the remote S3230 at **Port 1 > LOAM > Main**, click both of the **Refresh** buttons.

Section 4: Configuration

Local C3230 > Port 1 > LOAM > Main > Active > Remote In Loopback Status:

The screenshot displays the configuration page for LOAM on a Local C3230 device. The left sidebar shows the device hierarchy with 'Port 1' selected. The main panel has tabs for MAIN, ADVANCED, COUNTERS, and LOAM. The LOAM Configuration section includes:

- Admin Status: Enabled
- Operational Status: Operational
- LOAM Mode: Active
- Max PDU Size: 1500
- Configuration Revision: 3
- Functions Supported: Loopback, Event Notificats

 The LOAM Peer Information section includes:

- MAC Address: 00-C0-F2-21-09-6C
- Vendor OUI: 00 C0 F2
- Vendor Info: 2123
- LOAM Peer Mode: Passive
- Max PDU Size: 1500
- Configuration Revision: 2
- Functions Supported: Loopback, Event Notificati

 The Loopback Management section includes:

- Loopback Type: Remote Peer
- Loopback Status: Remote In Loopback
- Ignore Loopback Request: Enabled

 Buttons for Refresh, Save, Start, Stop, and Help are visible at the bottom.

Remote S3230 > Port 1 > LOAM > Main > Passive > Local In Loopback Status:

The screenshot displays the configuration page for LOAM on a Remote S3230 device. The left sidebar shows the device hierarchy with 'Port 1' selected. The main panel has tabs for MAIN, ADVANCED, COUNTERS, and LOAM. The LOAM Configuration section includes:

- Admin Status: Enabled
- Operational Status: Operational
- LOAM Mode: Passive
- Max PDU Size: 1500
- Configuration Revision: 2
- Functions Supported: Loopback, Event Notificati

 The LOAM Peer Information section includes:

- MAC Address: 00-C0-F2-21-01-77
- Vendor OUI: 00 C0 F2
- Vendor Info: 2123
- LOAM Peer Mode: Active
- Max PDU Size: 1500
- Configuration Revision: 3
- Functions Supported: Loopback, Event Notificati

 The Loopback Management section includes:

- Loopback Type: Remote Peer
- Loopback Status: Local In Loopback
- Ignore Loopback Request: Disabled

 Buttons for Refresh, Save, Start, Stop, and Help are visible at the bottom.

Figure 20: Sample Loopback Configuration

C3230 - Port 1 - LOAM - Counters tab:

The screenshot shows the ION System configuration interface. On the left, a tree view shows the hierarchy: ION Stack > Chassis > [14]C3230-1040 > Port 1. The main panel has tabs for MAIN, ADVANCED, COUNTERS, and LOAM. The LOAM tab is active, and the Counters sub-tab is selected. The following table represents the data shown in the counters panel:

Information PDU Sent	118394	Information PDU Received	115851
Unique Event Notification Sent	5229	Unique Event Notification Received	0
Duplicate Event Notification Sent	0	Duplicate Event Notification Rcvd	0
Loopback Control Sent	1	Loopback Control Received	0
Variable Request Sent	0	Variable Request Received	0
Variable Response Sent	0	Variable Response Received	0
Org Specific PDU Sent	0	Org Specific PDU Received	0
Unsupported Codes Sent	0	Unsupported Codes Received	0
Frames Lost Due To Oam	0		

S3230 - Port 1 - LOAM - Counters tab:

The screenshot shows the ION System configuration interface for S3230-1040. On the left, a tree view shows the hierarchy: ION Stack > Chassis > [14]S3230-1040 > Port 1. The main panel has tabs for MAIN, ADVANCED, COUNTERS, and LOAM. The LOAM tab is active, and the Counters sub-tab is selected. The following table represents the data shown in the counters panel:

Information PDU Sent	116192	Information PDU Received	118742
Unique Event Notification Sent	0	Unique Event Notification Received	5246
Duplicate Event Notification Sent	0	Duplicate Event Notification Rcvd	0
Loopback Control Sent	0	Loopback Control Received	1
Variable Request Sent	0	Variable Request Received	0
Variable Response Sent	0	Variable Response Received	0
Org Specific PDU Sent	0	Org Specific PDU Received	0
Unsupported Codes Sent	0	Unsupported Codes Received	0
Frames Lost Due To Oam	0		

Figure 21: Sample Loopback Counters Information

SOAM (Service OAM) Configuration

SOAM Configuration Prerequisites and Restrictions

Your software release may not support all the features documented for this module. For the latest feature information and caveats, see the release notes for your particular device/system and software release. The prerequisites and restrictions below apply to both ITU-T Y.1731 and IEEE 802.1ag unless noted otherwise.

Prerequisites for Configuring SOAM Functions

1. Network topology and network administration have been reviewed.
2. Business and service policies have been established.
3. A MIP or a MEP must be configured.
 - a. A MEP needs MD or MEG setup first; also, peer MEPs must be set up before SOAM can be operational for fault management.
 - b. A MIP must be configured for AIS messages to be generated on the interface which has this MIP configured. AIS can only be configured if the MIP is set up for Y.1731. AIS messages are generated by a Server MEP; the MIP just propagates to the higher layer if configured as an AIS client.
4. CFM is configured and enabled for either Y.1731 Fault Management support or for 802.1ag Fault Management support. CFM 802.1ag and Y.1731 are two different protocols for SOAM and they operate independently. A CFM 802.1ag MEP/MIP cannot do Y.1731 fault management; you need a Y.1731 MEP/MIP for doing Y.1731 fault management.
5. If you create an up MEP with primary VID 100, and VID 100 does not exist in the VLAN table, the MEP status should be 'failed'. However, the SOAM protocol does not check if a MEP's VID is actually configured in the device. It always sends the CCM for the MEP with configured C/S-VLAN tags. On the x323x, the Rx CCM frames are not subjected to VLAN checking. Hence, the SOAM stack would report the CCM status as "OK", but the port status would be "Failed", indicating the device does not have the VLAN setup yet. On the x323x, the ingress SOAM frames are not subjected to VLAN filtering; egress SOAM frames are validated only for port status and not for VLAN filtering. For S323x devices, SOAM traffic is not filtered based on VLAN, and *MACDefect* is used to indicate any VLAN rule violation.

Restrictions for Configuring SOAM Functions

1. There is a maximum limit on the number of MEG and MEPs that the ION system can support (up to 16 VLANs per port and 8 levels on each VLAN).
2. SOAM is only supported on Port 3 of the x3231 NID in regards to redundancy. The x3231 does not function as a 3-port switch in regards to SOAM, but rather allows for fiber redundancy, including SOAM. SOAM views Port 3 as a redundant port, so a SOAM MEP or MIP can not be created on Port 3. This restriction applies whether the "Redundancy" feature is enabled or disabled.

SOAM can coexist with all other features. All operating modes are supported.

See "[Appendix D: SOAM Configuration Example](#)" on page 419 for SOAM configuration examples via the CLI Method and the Web Method.

SOAM CLI Commands

There are numerous CLI commands that let you define and display SOAM configuration information. For a complete description of these and other CLI commands see the *ION System CLI Reference Manual, 33461*.

SOAM Menu System

SOAM configuration, statistics, and related menu functions are shown in the figure below.

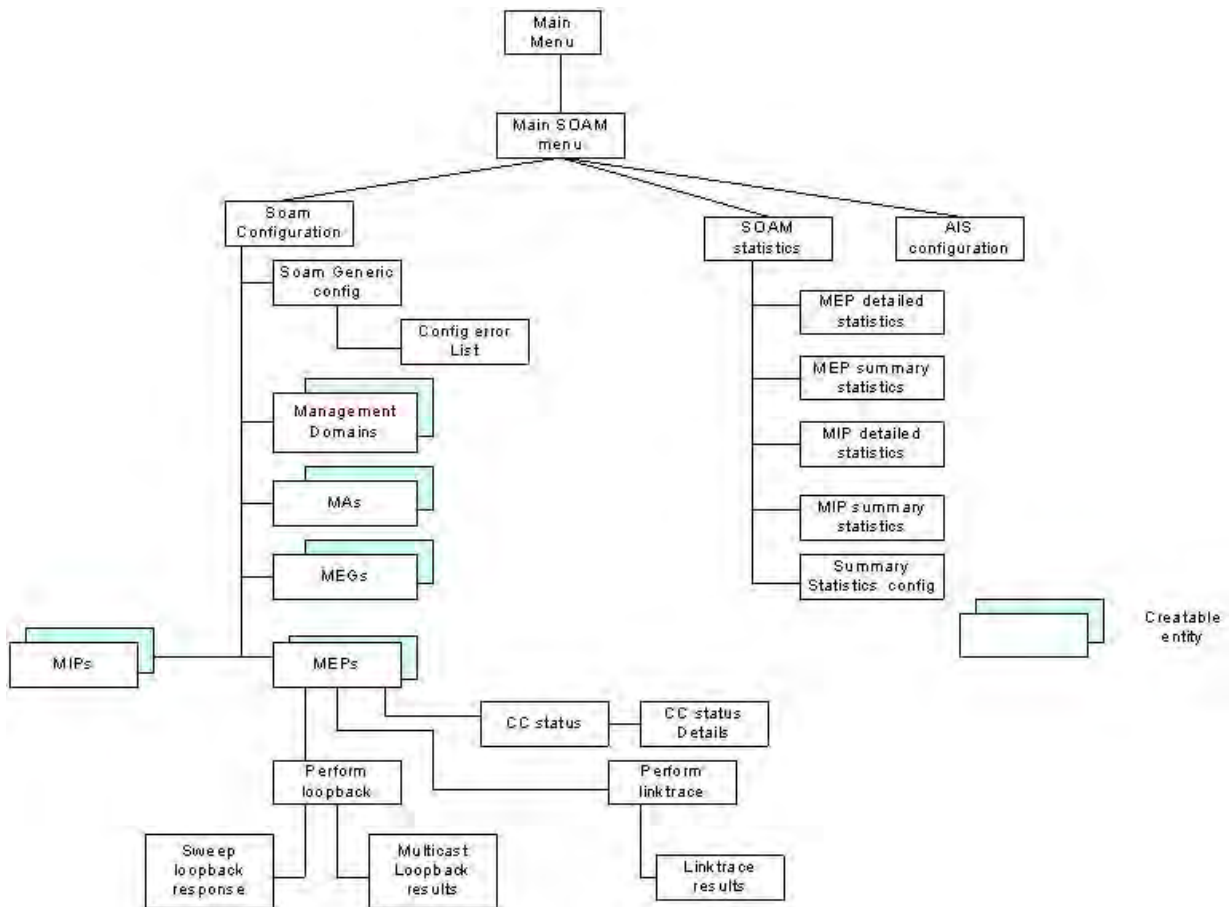


Figure 22: SOAM Menu System

SOAM can be configured in the NID per 802.1AG or Y.1731 using either the CLI or Web method. The SOAM configurable functions – MD/MA, MEG, MEP, and MIP – are documented in the following sections.

Configuring a SOAM MD/MA

SOAM 802.1AG MD/MA Config – CLI Method

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

2. Define a maintenance domain (MD). Type:

```
add soam md local-md-id=<xx> md-name=<yy> md-level=<zz>
```

where:

xx = maintenance domain identifier (1–4294967295)

yy = maintenance domain name or **none**. The name can be a maximum of 43 characters.

zz = level (0–7) assigned to the maintenance domain

3. Press **Enter**.

4. Define sender permissions associated with the MD. Type:

```
set soam md local-md-id=<xx> permission-id=<yy>
```

where:

xx = maintenance domain identifier (1–4294967295)

yy = fields of the Sender ID that are to be sent; valid choices are:

- **none**
- **chassis**
- **mgmtaddr**
- **chassismgmtaddr**

5. Press **Enter**.

6. Repeat steps 2-5 for each maintenance domain to be defined.

7. Define a maintenance association (MA) for the MD. Type:

```
add soam ma local-ma-id=<uu> local-md-id=<vv> ma-name=<ww> vlan-type=<xx>
[vlan-id-list=<yy>] [s-vid=<zz>]
```

where:

uu = maintenance association identifier (1–4294967295)

vv = maintenance domain identifier (1–4294967295)
 ww = maintenance association name (maximum of 44 characters)
 xx = VLAN type of VLAN ID list to associate with the MA; valid choices are:

- none
- ctype
- stype
- doubletag

Note: If **doubletag** is selected, then **s-vid=** must be specified.

yy = optional; a list of one or more VLAN IDs. Omit this parameter if **vlan-type=none** is specified.

zz = conditional; the ID of the S-VLAN. This parameter must be specified if **vlan-type=doubletag** is entered.

8. Press **Enter**.
9. Define/modify the MA attributes. Type:

set soam ma local-ma-id=<xx> attr_name=<yy> attr_value=<zz>

where:

xx = maintenance association identifier (1–4294967295)
 yy = name of the attribute to be defined/changed (see Table 13 below).
 zz = value to be associated with attribute yy (see Table 13 below).

Table 13: SOAM MA Attributes

If yy equals:	Then zz can be:
<p>permission</p> <p>Determines which fields of the maintenance domain are to be sent.</p>	<ul style="list-style-type: none"> • none • chassis • mgmtaddr • chassismgmtaddr • defined (defer)

Section 4: Configuration

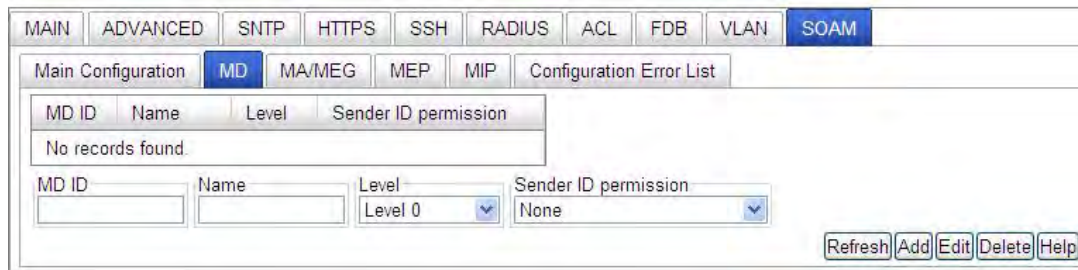
<p>ccmininterval</p> <p>The interval at which CC messages are transmitted.</p>	<ul style="list-style-type: none"> • 3.3ms • 10ms • 100ms • cci1s • cci10s • cci1min • cci10min
<p>mepid-add</p> <p>Configure local and remote MEPs belonging to this MA.</p>	<p>ID (1–8191) of the MEP to be configured.</p>
<p>mepid-remove</p> <p>Remove local and remote MEPs belonging to this MA.</p>	<p>ID (1–8191) of the MEP to be deleted.</p>
<p>vlan-add</p> <p>Add a VLAN to this MA.</p>	<p>ID of the VLAN to be added.</p>
<p>vlan-remove</p> <p>Remove a VLAN from this MA.</p>	<p>ID of the VLAN to be removed.</p>
<p>primary-vlan</p> <p>The primary VID used for all CFM frames belonging to this MA.</p>	<p>VLAN ID (2 – 4094)</p>
<p>autodetection-timeout</p> <p>The amount of time before a remote peer MEP is removed from the CCM Database on loss of CCMs from the remote MEP.</p>	<p>Number of milliseconds.</p>

<p>autodetectrmp</p> <p>Whether MEPs are discovered automatically based on received CCM messages.</p>	<ul style="list-style-type: none"> • enable • disable
--	---

10. Press **Enter**.
11. Repeat steps 9 and 10 to define/modify the MA attributes for each attribute to be added or modified.
12. Define the associated MEPs and/or MIPs. See “[SOAM MEP Config – CLI Method](#)” on page 87 and “[SOAM MIP Config – CLI Method](#)” on page 92.

SOAM 802.1AG MD/MA Config – Web Method

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



3. Select the **MD** sub-tab if not already selected.
4. Define a maintenance domain (MD). In the **MD ID** field, enter an ID number (1–4294967295) for the maintenance domain being defined.
5. Optional: in the **Name** field, enter a name for this maintenance domain.
6. In the **Level** field, select the level this maintenance domain is associated with (**Level 0 – Level 7**) for the MD being defined.
7. In the **Sender ID permission** field, select the permission that will be sent with each transmission. This indicates what, if anything, is to be included in the Sender ID TLV transmitted by MEPs configured in this MD (Maintenance Domain). Valid selections are **None**, **Chassis ID**, **Manage**, and **Chassis ID and Manage**. The default value is **None** (name).
 - **None**: The Sender ID TLV is not to be sent.
 - **Chassis ID**: The Chassis ID Length, Chassis ID Subtype, and Chassis ID fields of the Sender ID TLV are to be sent.
 - **Manage**: The Management Address Length and Management Address of the Sender ID TLV are to be sent.
 - **Chassis ID and Manage**: The Chassis ID Length, Chassis ID Subtype, Chassis ID, Management Address Length and Management Address fields are all to be sent.
8. Click **Add**.

- Repeat steps 3-8 for each maintenance domain being defined and verify your entries.

The screenshot shows the SOAM configuration page with the MD tab selected. A table lists maintenance domains:

MD ID	Name	Level	Sender ID permission
1	UNlabMD	Level 0	None
6	ProviderMD	Level 0	None
111	UINcdMD	Level 0	None

Below the table, there are input fields for MD ID (111), Name (UINcdMD), Level (Level 0), and Sender ID permission (None). Buttons for Refresh, Add, Edit, Delete, and Help are visible at the bottom right.

- Define a maintenance association (MA) for the MD. Select the MA/MEG tab. Select the MA Configuration sub-tab if not already selected.

The screenshot shows the MA Configuration page. The MA ID field is set to 1. The CC interval is set to 1 sec. The RMEP auto detection is set to Disabled and the RMEP auto detection timeout is set to 4000. The Sender ID permission is set to MD defer. Below the configuration fields, there are sections for VLAN ID list and MEP ID list, both showing no records found.

- In the **Parent MD ID** field, select the MD to which this MA will be associated.
- In the **MA ID** field, enter an ID number (1–4294967295) for the maintenance association.
- In the **Name** field, enter a name for this maintenance association. This is the Short Maintenance Association name; it must be unique within a maintenance domain.
- In the **CC interval** field, select the interval at which Continuity Check Messages (CCM) will be sent. This is the interval between CCM transmissions to be used by all MEPs in the MA. The valid selections are **3.3ms**, **10ms**, **100ms**, **1s**, **10s**, **1min**, and **10min**. The default is **1 second**.

Section 4: Configuration

15. Is this MA associated with a VLAN?

Yes	No
<p>a) In the VLAN type field, select the type of VLAN, where:</p> <ul style="list-style-type: none"> ○ none specifies an untagged VLAN. Used typically for level 0 domains. ○ ctype specifies that the VLAN indication associated with this MA/MEG refers to a C-Tagged VLAN. ○ stype specifies that the VLAN indication associated with this MA/MEG refers to a S-Tagged VLAN. ○ doubletag specifies that the VLAN indication associated with this MA/MEG refers to the inner VLAN tag. <p>b) In the Primary VID field, enter the primary VLAN ID. The Primary VLAN ID with which the MEG is associated, or 0 if the MA is not attached to any VID. If the MA is associated with more than one VID, the VLAN table lists them. The valid range is 2 - 4094.</p> <p>c) In the S-VID field, enter the VLAN ID of the secondary VID. S-VID is available only for the double-tagged or 802.1D tagged MEPs. The S-VID will be used in the Provider tag. This is the Outer tag where the VLAN type is doubletagged.</p> <p>d) Continue with Step 16.</p>	<p>Continue with Step 16.</p>

16. In the **RMEP auto detection** field, select whether RMEPs (Remote MEPS) will be detected automatically or whether they will be explicitly defined. This specifies whether the MEP Autodiscovery feature is enabled for this particular MA.

- **Enabled** – remote MEPs will be detected automatically.
- **Disabled** – remote MEPs must be explicitly defined.

17. In the **RMEP auto detection timeout** field, enter the number of milliseconds (required only if **RMEP auto detection** is set to **Enabled**). This specifies the timeout value for removal of peer MEPs added through autodetection if no CCM frames are received from that peer MEP.

18. In the **Sender ID permission** field, select the permission that will be sent with each transmission. The valid selections are **None**, **Chassis ID**, **Manage**, **Chassis ID and Manage**, and **MD Defer**. The default is **MD Defer**.

This selection indicates what, if anything, is to be included in the Sender ID TLV transmitted by MPs configured in this MA. The values indicate:

- **None** - The Sender ID TLV is not to be sent.
- **Chassis ID** - The Chassis ID Length, Chassis ID Subtype, and Chassis ID fields of the Sender ID TLV are to be sent.
- **Manage** - The Management Address Length and Management Address of the Sender ID TLV are to be sent.
- **Chassis ID and Manage** - The Chassis ID Length, Chassis ID Subtype, Chassis ID, Management Address Length, and Management Address fields are all to be sent.
- **MD defer** - the contents of the Sender ID TLV are determined by the corresponding Maintenance Domain permission variable (*dot1agCfmMaCompldPermission*).

Note: The permission can be set in the MD and/or at the MA level. If the MA has a permission ID set then that is used. Otherwise, by default, the permissions from parent MD are used. Since MDs can have multiple MAs, each MA can use its or the MDs permission ID.

19. Click **Add**.

20. Will this MA operate in additional VLANs (if the MA is associated with other VLANs)?

Yes	No
a) In the VLAN ID field (VLAN ID list tab), enter the VID. b) Click Add . c) Add as many VIDs as required via sub-steps a) and b) above. d) Continue with Step 21 below.	Continue with Step 21.

21. Will MEPs be associated with this MA?

Yes	No

Section 4: Configuration

- a) At the bottom left, select the **MEP ID list** tab.
- b) In the **Parent MA/MEG ID** field, select the MA the MEPs will be associated with.
- c) In the **MEP ID** field, enter the ID number of a MEP.
- d) Click **Add**.
- e) Add as many MEPs as required for this MA via sub-steps a) - d) above.
- f) Continue with step 22.

Continue with Step 22.

22. Repeat [Define a maintenance association \(MA\) for the MD](#) (steps 10-14 or steps 9-21) for each MA to be defined.
23. Define the associated MEPs and/or MIPs. See [“SOAM MEP Config – Web Method”](#) on page 90 and [“SOAM MIP Config – Web Method”](#) on page 93.
24. Verify your selections.

The screenshot shows the MA Configuration web interface. At the top, there are tabs for Generic configuration, MD, MA/MEG, MEP, MIP, and Configuration Error List. The MA/MEG tab is selected, and the MA Configuration sub-tab is active. Below the tabs is a table with the following data:

MA ID	Name	CC interval	VLAN type	Primary VID	S-VID	RMEP auto-detection	RMEP auto-detection timeout	Sender ID permission
3	OperatorSta	1 sec	styp	100	0	Disabled	0	MD defer
6	ProviderCTa	1 sec	ctyp	200	0	Disabled	0	MD defer
11	UNlbcUntag	1 sec	none	0	0	Disabled	0	MD defer
111	UNlbcUntag	1 sec	none	0	0	Disabled	0	MD defer

Below the table are form fields for adding a new MA:

- Parent MD ID: 3
- MA ID: (empty)
- Name: (empty)
- CC interval: 1 sec
- VLAN type: none
- Primary VID: 0
- S-VID: 0
- RMEP auto-detection: Disabled
- RMEP auto-detection timeout: 4000
- Sender ID permission: MD defined

Buttons: Refresh, Add, Edit, Delete, Help

Below the form fields are two tabs: VLAN ID list and MEP ID list. The MEP ID list tab is active, showing a table with the following data:

Primary VLAN ID	VLAN ID
No records found	
MA PVID: 100	0

Buttons: Refresh, Add, Delete, Help

Configuring a SOAM MEG

SOAM Y.1731 MEG Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Define a maintenance entity group (MEG). Type:

```
add soam meg local-meg-id=<uu> meg-name=<vv> meg-level=<ww> vlan-type=<xx>  
[vlan-id-list=<yy>] [s-vid=<zz>]
```

where:

uu = maintenance entity group identifier (1–4294967295)

vv = maintenance entity group name (maximum of 13 characters)

ww = level (0–7) assigned to the added maintenance entity group (MEG)

xx = type of VLAN ID list to associate with the MA; valid choices are:

- none
- ctype
- stype
- doubletag

NOTE: If **doubletag** is selected, then **s-vid=** must be specified.

yy = optional; a list of one or more VLAN IDs. Omit this parameter if **vlan-type=none** is specified.

zz = conditional; the ID of the S-VLAN. This parameter must be specified if **vlan-type=doubletag** is entered.

3. Press **Enter**.
4. Define/modify the MEG attributes. Type:

```
set soam meg local-meg-id=<xx> attr_name=<yy> attr_value=<zz>
```

where:

xx = maintenance entity group identifier (1–4294967295)

yy = name of the attribute to be defined/changed (see table below).

Section 4: Configuration

zz = value to be associated with attribute yy (see table below).

Table 14: SOAM MEG Attributes

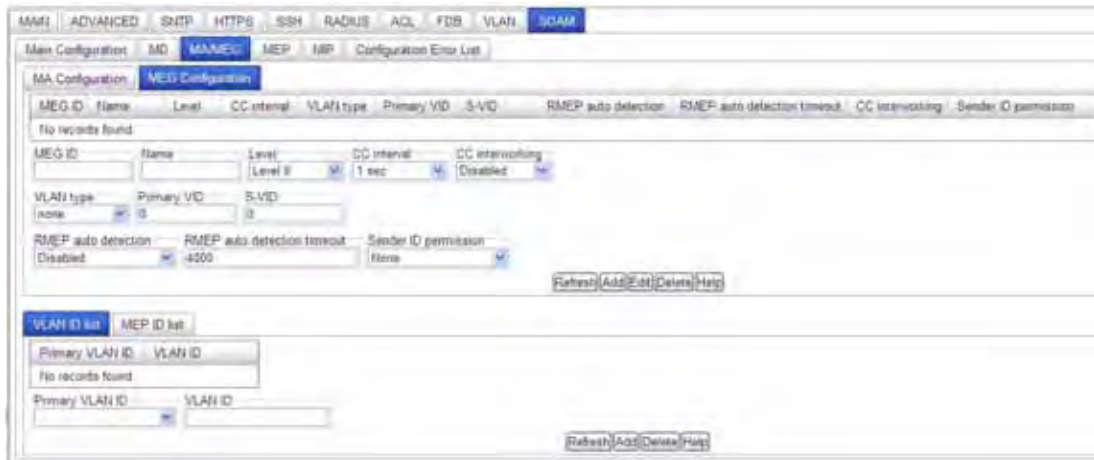
If yy equals:	Then zz can be:
<p>permission</p> <p>Determines which fields of the sender ID are to be sent.</p>	<ul style="list-style-type: none"> • chassis • chassismgmtaddr • disable • enable • mgmtaddr • none
<p>ccmininterval</p> <p>The interval at which CC messages are transmitted.</p>	<ul style="list-style-type: none"> • 3.3ms • 10ms • 100ms • cci1s • cci10s • cci1min • cci10min
<p>mepid-add</p> <p>Configure local and remote MEPs.</p>	<p>ID (1–8191) of the MEP to be configured.</p>
<p>mepid-remove</p> <p>Remove local and remote MEPs.</p>	<p>ID (1–8191) of the MEP to be deleted.</p>
<p>vlan-add</p> <p>Add a VLAN to this MEG.</p>	<p>ID of the VLAN to be added.</p>
<p>vlan-remove</p> <p>Remove a VLAN from this MEG.</p>	<p>ID of the VLAN to be removed.</p>

<p>primary-vlan</p> <p>The primary VID used for all CFM frames belonging to this MEG.</p>	<p>VLAN ID.</p>
<p>autodetection-timeout</p> <p>The amount of time before a remote peer MEP is removed from the CCM Database on loss of CCMs from the remote MEP.</p>	<p>Number of milliseconds.</p>
<p>autodetectrmep</p> <p>Whether MEPs are discovered automatically based on received CCM messages.</p>	<ul style="list-style-type: none"> • enable • disable
<p>y.1731-802.lag-interop</p> <p>Status of the interoperability mode.</p>	<ul style="list-style-type: none"> • enable • disable

5. Press **Enter**.
6. Repeat steps 4 and 5 to define or modify the MEG attributes for each MEG to be defined or modified.
7. Repeat steps 2-3 (Define a maintenance entity group (MEG) and repeat steps 4-5 (Define/modify the MEG attributes) for each MEG to be defined.
8. Define the associated MEPs and/or MIPs. See “[SOAM MEP Config – CLI Method](#)” on page 87 and “[SOAM MIP Config – CLI Method](#)” on page 92.

SOAM Y.1731 MEG Config – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MA/MEG** sub-tab > **MEG Configuration** sub-tab.



3. In the **MEG ID** field, enter an ID number (1–4294967295) for this maintenance entity group (MEG).
4. In the **Name** field, enter a name for this maintenance entity group (maximum of 13 characters). If CCI interoperability mode is set, then the format must be ASCII text.
5. In the **Level** field, select the domain level for the MEG (**Level 0 – Level 7**). This specifies the domain level for the MEG being defined.
6. In the **CC interval** field, select the interval at which continuity check messages (CCM) will be sent. This is the interval between CCM transmissions to be used by all MEPs in the MEG.
7. In the **CC interworking** field, select **Enabled** only if there will be interworking (compatibility mode) between IEEE 802.1ag and ITU-T Y.1731. The default is **Disabled**.

8. Is this MEG associated with a VLAN?

Yes	No
<ul style="list-style-type: none"> • In the VLAN type field, select the type of VLAN, where: <ol style="list-style-type: none"> 1. none specifies an untagged VLAN. Used typically for level 0 domains. 2. ctype specifies that the VLAN indication associated with this MA/MEG refers to a C-Tagged VLAN. 3. stype specifies that the VLAN indication associated with this MA/MEG refers to a S-Tagged VLAN. 4. doubletag specifies that the VLAN indication associated with this MA/MEG refers to the inner VLAN tag. <p>All VLANs associated with an MEG are of the same type.</p> • In the Primary VID field, enter the primary VLAN ID. The Primary VLAN ID with which the MEG is associated, or 0 if the MEG is not attached to any VID. If the MEG is associated with more than one VID, the on-screen table lists them. The valid range is 2 - 4094. • In the S-VID field, enter the VLAN ID of the secondary VID. S-VID is available only for the double-tagged or 802.1ad tagged MEPs. The S-VID will be used in the provider tag. • Continue with step 9 below. 	<p>Continue with step 10.</p>

9. In the **RMEP auto detection** field, select whether [remote](#) MEPs will be detected automatically or whether they will be explicitly defined.

- **Enabled** – remote MEPs will be detected automatically.
- **Disabled** – remote MEPs must be explicitly defined.

10. In the **RMEP auto detection timeout** field, enter the number of milliseconds (required only if **RMEP auto detection** is **Enabled**). Specifies the timeout value for removal of peer MEPs added through autodetection if no CCM frames are received from that peer MEP. The default is 4000 milliseconds (4 seconds).

11. In the **Sender ID permission** field, select the permission that will be sent with each transmission. The valid selections are **None**, **Chassis ID**, **Manage**, and **Chassis ID and Manage**. The default is **None**.

Section 4: Configuration

This selection indicates what, if anything, is to be included in the Sender ID TLV transmitted by MPs configured in this MA. The values indicate:

- **None** - The Sender ID TLV is not to be sent.
- **Chassis ID** - The Chassis ID Length, Chassis ID Subtype, and Chassis ID fields of the Sender ID TLV are to be sent.
- **Manage** - The Management Address Length and Management Address of the Sender ID TLV are to be sent.
- **Chassis ID and Manage** - The Chassis ID Length, Chassis ID Subtype, Chassis ID, Management Address Length and Management Address fields are all to be sent.

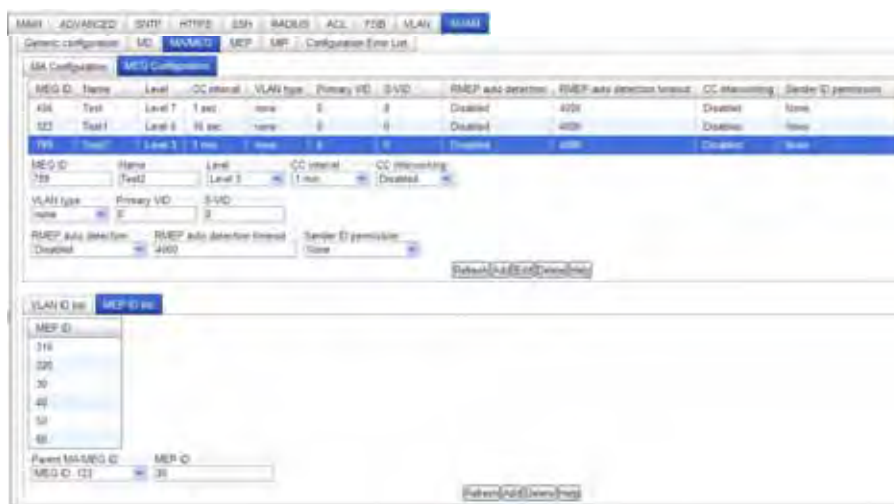
Note: The Sender ID Permission can be set at the MD and/or at the MA level. If the MA has permission ID set, then that is used. Otherwise, by default, the permissions from the parent MD are used. Since MDs can have multiple MAs, each MA can use its own or the MDs permission ID.

12. Click **Save**.

13. Repeat steps 2-12 for each MEG to be defined.

14. Define the associated MEPs/MIPs. See “[SOAM MEP Config – Web Method](#)” on page 90 and “[SOAM MIP Config – Web Method](#)” on page 93.

15. Verify your SOAM selections displayed in the table.



16. To edit an existing MEG, select the MEG ID from the table and click the **Edit** button. (The MEG ID, Name and Level cannot be edited.) Click **Add** when done editing.
To delete an existing MEG, select the MEG ID from the table and click the **Delete** button.

Configuring a SOAM MEP

SOAM MEP Config – CLI Method

NOTE: You must define either an MD/MA combination or a MEG before defining a MEP.

1. Add a new MEP to the SOAM engine. Type:

```
add soam mep mep-id=<ww> local-parent-id=<xx> direction=<yy> port=<zz>
```

where:

ww = MEP identifier (1–8191)

xx = ID of the local MA or MEG the MEP is associated with (parent ID)

yy = direction the traffic is monitored:

- **up** – upstream traffic is monitored ('Up' MEP - a MEP that transmits CFM PDUs towards, and receives them from, the direction of the Bridge Relay Entity).
- **down** – downstream traffic is monitored ('Down' MEP – a MEP that receives CFM PDUs from, and transmits them towards, the direction of the LAN).

zz = number of the port the MEP will be associated with

2. Press **Enter**.
3. Define/modify the MEP attributes. Type:

```
set soam mep config mep-id=<ww> local-parent-id=<xx> attr_name=<yy> attr_value=<zz>
```

where:

ww = MEP identifier (1–8191)

xx = ID of the local MA or MEG associated with the MEP.

yy = name of the attribute to be defined/changed (see Table 15 below).

zz = value to be associated with attribute yy (see Table 15 below).

Table 15: SOAM MEP Attributes

If yy equals:	Then zz can be:
<p>admin Admin status of the MEP.</p>	<ul style="list-style-type: none"> • enable • disable
<p>cci CCM generation status.</p>	<ul style="list-style-type: none"> • enable • disable
<p>primary-vid ID of the primary VLAN for the MEP.</p>	<p>VLAN ID (2 – 4094)</p>
<p>ccmltmpriority Priority of the CCM and LTM.</p>	<p>0–7</p>
<p>faultalarmdetect The number of milliseconds that defects must be present before an alarm is issued.</p>	<p>2500–10000</p>
<p>faultalarmreset The number of milliseconds that defects must be absent before an alarm is reset.</p>	<p>2500–10000</p>

<p>lowestprilevel</p> <p>The lowest priority defect that is allowed to generate an alarm.</p>	<ul style="list-style-type: none"> • alldf – generate an alarm for all defects. • macremerrxcon – generate an alarm only for MAC, not receiving CCM, erroneous CCM, and cross-connect defects • remerrxconn – generate an alarm only for not receiving CCM, erroneous CCM, and cross-connect defects • errrxconn – generate an alarm only for erroneous CCM and cross-connect defects • xconn – generate an alarm only for cross-connect defects • noxcon – do not generate an alarm for any defect.
<p>aisclient–add</p> <p>List of AIS clients to be added (Y.1731 only).</p>	<p>client list (e.g., MEP153 MIP4, etc.)</p>
<p>aisclient–remove</p> <p>List of AIS clients to be deleted (Y.1731 only).</p>	<p>client list (e.g., MEP153 MIP4, etc.)</p>
<p>aistransmit</p> <p>Status of the AIS transmission (Y.1731 only).</p>	<ul style="list-style-type: none"> • enable • disable
<p>aisinterval</p> <p>The AIS transmission interval (Y.1731 only).</p>	<ul style="list-style-type: none"> • 1min • 1s
<p>aisnotifyup</p> <p>The AIS notify up status (Y.1731 only).</p>	<ul style="list-style-type: none"> • enable • disable

Section 4: Configuration

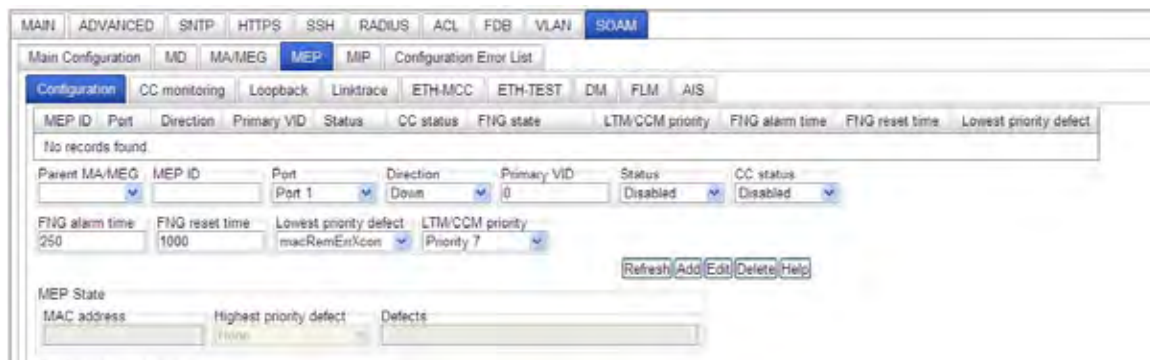
<p>aisprocess</p> <p>The AIS process to perform (Y.1731 only).</p>	<ul style="list-style-type: none"> • .. • 1min / 1s • alldf / disable / enable / errxconn / macremerrxcon / noxcon / remerrxconn / xconn
<p>aisframepriority</p> <p>The AIS frame priority (Y.1731 only).</p>	<p>0-7</p>

4. Press **Enter**.
5. Repeat steps 3 and 4 for each MEP attribute to be defined or modified.

SOAM MEP Config – Web Method

NOTE: You must define either an MD/MA combination or a MEG before defining a MEP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab.



3. Select the **Configuration** sub-tab if not already displayed.
4. In the **Parent MA/MEG** field, select the MA or MEG that this MEP will be associated with.
5. In the **MEP ID** field, enter the ID number (1–8191) for this MEP.
6. In the **Port** field, select the device port that this MEP is associated with (**Port 1** or **Port 2**; and **Port 3** on x3231 models).
7. In the **Direction** field, select whether monitoring is to be done upstream (**Up**) or downstream (**Down**) from the MEP. (Where an ‘Up’ MEP transmits CFM PDUs towards, and receives them from, the direction of the Bridge Relay Entity, and a ‘Down’ MEP receives CFM PDUs from, and transmits them towards, the direction of the LAN).
8. In the **Primary VID** field, enter the VLAN ID of the primary VLAN the MEP is associated with. This must be the same as the Primary VID specified for the parent MA/MEG. The valid range is 2 - 4094.
9. In the **Status** field, select **Enabled**.
10. In the **CC status** field, select **Enabled**.
11. In the **FNG alarm time** field, enter the number of milliseconds that defects must be present before a fault alarm is issued. This is the Fault Notification Generation (FNG) alarm that is generated whenever a CCM (Continuity Check Message) is lost. The default is 250 milliseconds (0.25 seconds). The valid range is 250–1000 milliseconds.

Section 4: Configuration

12. In the **FNG reset time** field, enter the number of milliseconds that defects must be absent before a fault alarm is reset. The Fault Notification Generation (FNG) alarm is generated whenever a CCM (Continuity Check Message) is lost. The default is 1000 milliseconds (10 seconds). The valid range is 250–1000 milliseconds.
13. In the **Lowest priority defect** field, select the lowest priority defect that is allowed to generate an alarm. The default is **macRemErrXcon**. The valid selections are:
 - **allDef** – generate an alarm for all defects.
 - **macRemErrXcon** – generate an alarm only for MAC, not receiving CCM, erroneous CCM, and cross-connect defects.
 - **remErrXcon** – generate an alarm only for not receiving CCM, erroneous CCM, and cross-connect defects (the default).
 - **errXcon** – generate an alarm only for erroneous CCM and cross-connect defects.
 - **xcon** – generate an alarm only for cross-connect defects.
 - **noXcon** – do not generate an alarm for any defect.
14. In the **LTM/CCM priority** field, select the priority for the Link Trace Message / Continuity Check Messages. This field defines the priority value for LTM/CCM frames transmitted by the MEP, in the range of 0 – 7, where 0 is the lowest priority and 7 is the highest priority.
15. Click the **Add** button.
16. Repeat steps 3-15 for each MEP to be defined.

17. Verify your SOAM MEP configuration selections.

The screenshot displays the SOAM MEP configuration page. At the top, there are tabs for 'Configuration', 'CC monitoring', 'Loopback', 'Linktrace', 'ETHMCC', 'ETH TEST', 'DM', 'FLM', and 'AIS'. The 'Configuration' tab is active. Below the tabs is a table with the following columns: MEP ID, Port, Direction, Primary VID, Status, CC status, FTG state, LTM/CCM priority, FTG alarm time, FTG reset time, and Lowest priority defect.

MEP ID	Port	Direction	Primary VID	Status	CC status	FTG state	LTM/CCM priority	FTG alarm time	FTG reset time	Lowest priority defect
339	Port 2	Up	0	Enabled	Enabled	Defect reported	7	250	1000	macRemEnr/low
40	Port 1	Down	0	Enabled	Enabled	Defect reported	7	250	1000	macRemEnr/low
50	Port 2	Down	0	Enabled	Enabled	Defect reported	7	250	1000	macRemEnr/low

Below the table, there are configuration fields for the selected MEP (MEP ID: 50):

- Parent MA/MEG: MA ID 111
- MEP ID: 50
- Port: Port 2
- Direction: Down
- Primary VID: 0
- Status: Enabled
- CC status: Enabled
- FTG alarm time: 250
- FTG reset time: 1000
- Lowest priority defect: macRemEnr/low
- LTM/CCM priority: Priority 7

Buttons for 'Refresh', 'Add', 'Edit', 'Delete', and 'Help' are visible. Below the configuration fields are several statistics sections:

- MEP State:** MAC address: 00-C9-F2-42-08-E0; Highest priority defect: CC; Defects: RemoteCCM
- Continuity Check Statistics:** CCMs sent: 70200; CCMs with RDI bit sent: 70296; CCMs received: 0; CCMs with RDI bit received: 0; CCMs discarded due to SenderID TLV invalid: 0; CCMs discarded due to Port Status TLV invalid: 0; CCMs discarded due to Interface Status TLV invalid: 0; CCMs with sequence errors received: 0
- Loopback Statistics:** In order LBRs received: 0; Out of order LBRs received: 0; LBRs with bad mode received: 0; LBRs sent: 0
- Linktrace Statistics:** LTRs received: 0; LTRs received: 0; LTRs sent: 0; LTRs with bad dest MAC discarded: 0
- AIS Statistics:** AIS frames transmitted: 0; AIS frames received: 0; AIS sent true up notifications: 0; AIS sent false up notifications: 0; AIS received true up notifications: 0; AIS received false up notifications: 0
- MCC Statistics:** MCC packets sent: 0; MCC packets received: 0

17. To edit an existing MEP, select the MEP ID from the table and click the **Edit** button. (The Parent MA/MEG, MEP ID, and Port cannot be edited.) Click **Add** when done editing. To delete an existing MEP, select the MEP ID from the table and click the **Delete** button.

Configuring a SOAM MIP

SOAM MIP Config – CLI Method

NOTE: You must define either an MD/MA combination or a MEG before defining a MIP.

1. Add a new MIP to the SOAM engine. Type:

```
add soam mip mip-type=<ww> local-mip-id=<xx> local-parent-id=<yy> port=<zz>
```

where:

ww = MIP type; valid choices are:

- **y.1731**
- **802.1ag**

xx = MIP identifier (1–4294967295)

yy = ID of the local MA or MEG associated with the MEP

zz = number of the port the MIP will be associated with

2. Press **Enter**.

3. Define/modify the MIP attributes. Type:

```
set soam mip local-mip-id=<xx> attr-name=<yy> attr-val=<zz>
```

where:

xx = MIP identifier (1–4294967295)

yy = name of the attribute to be changed (see the table below).

zz = value to be associated with attribute yy (see the table below).

Table 16: SOAM MIP Attributes

If yy equals:	Then zz can be:
admin Admin state of the MIP.	<ul style="list-style-type: none"> • up • down

<p>aistransmit</p> <p>Status of the AIS transmission (Y.1731 only).</p>	<ul style="list-style-type: none"> • enable • disable
<p>aisinterval</p> <p>The AIS transmission interval (Y.1731 only).</p>	<ul style="list-style-type: none"> • 1min • 1s
<p>aisframepriority</p> <p>The AIS frame priority (Y.1731 only).</p>	<p>0-7</p>

4. Press **Enter**.
5. Repeat [steps 3-4](#) for each MIP attribute to be defined or modified.

SOAM MIP Config – Web Method

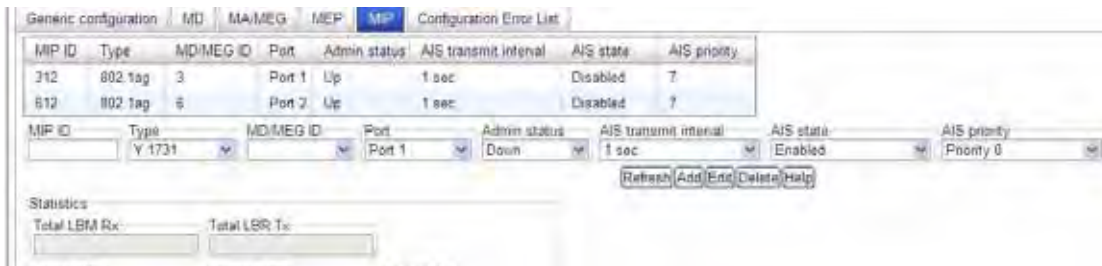
NOTE: You must define either an MD/MA combination or a MEG before defining a MIP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MIP** sub-tab.

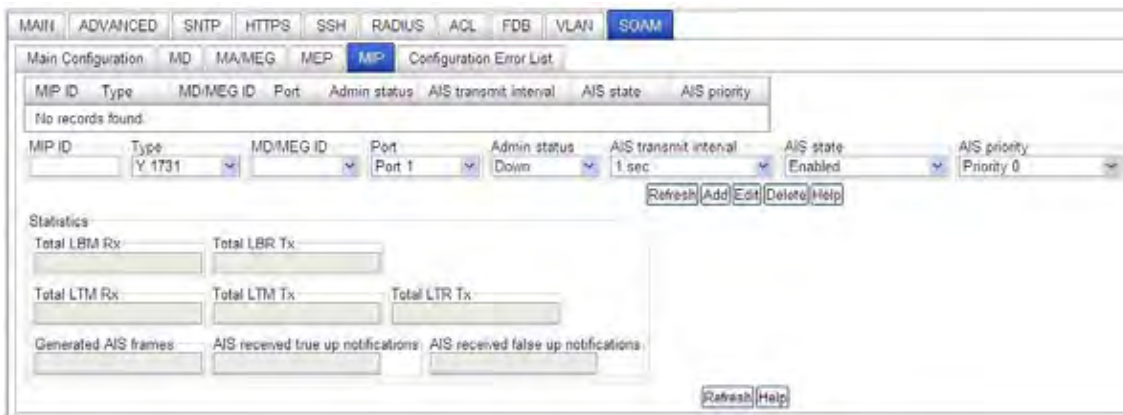


3. In the **MIP ID** field, enter a unique ID number (1–4294967295) for this MIP.
4. In the **Type** field, select the type of configuration this MIP is associated with (**Y.1731** or **802.1ag**).
5. In the **MD/MEG ID** field, enter the ID of the MD or MEG this MIP is to be associated with. **Note:** if the **Type** field is **802.1ag**, you must enter an MD ID. If Type is **Y.1731** you must enter a MEG ID.
6. In the **Port** field, select the number of the device port this MIP is associated with (the port on which the MIP is attached).
7. In the **Admin status** field, select **Up**. This is the Administrative state of the MIP.
8. In the **AIS transmit interval** field, select the desired interval between AIS transmissions. Valid selections are **1 second** and **1 minute**. The default is **1 second**. AIS operates in Y.1731 mode only; this field is not configurable for a MIP Type of 802.1ag as the fields are uneditable.
9. In the **AIS state** field, select whether to enable or disable transmission of AIS frames. The default is **Enabled**. AIS operates in Y.1731 mode only; this field is not configurable for a MIP Type of 802.1ag as the fields are uneditable.
10. In the **AIS priority** field, select the desired priority value for AIS frames transmitted by the MIP. The valid range is 0 – 7, where 0 is the lowest priority and 7 is the highest priority. The default is **Priority 0**. AIS operates in Y.1731 mode only; this field is not configurable for a MIP Type of 802.1ag as the fields are uneditable.
11. Click the **Add** button.

12. Repeat steps 3-11 for each MIP to be defined.
13. Verify your SOAM MIP selections.



14. Refresh the **Statistics** section and examine the SOAM MIP Statistics.



The SOAM MIP Statistics include:

- Total LBM Rx* - the number of LBMs received by this MIP.
- Total LBR Tx* - the number of LBRs sent by this MIP.
- Total LTM Rx* - the number of LTMs received by this MIP.
- Total LTM Tx* - the number of LTM messages forwarded by MIP.
- Total LTR Tx* - the number of LTR responses sent by this MIP.
- Generated AIS frames* – the total number of AIS frames generated by this MIP
- AIS received true up notifications* – the number of AIS ‘true’ up frames received by this MIP
- AIS received false up notifications* - the number of AIS ‘false’ up frames received by this MIP

15. To edit an existing SOAM MIP, select the desired MIP ID line and click the **Edit** button. (The MIP ID, Type and MD/MEG ID cannot be edited.) Click **Add** when done editing.

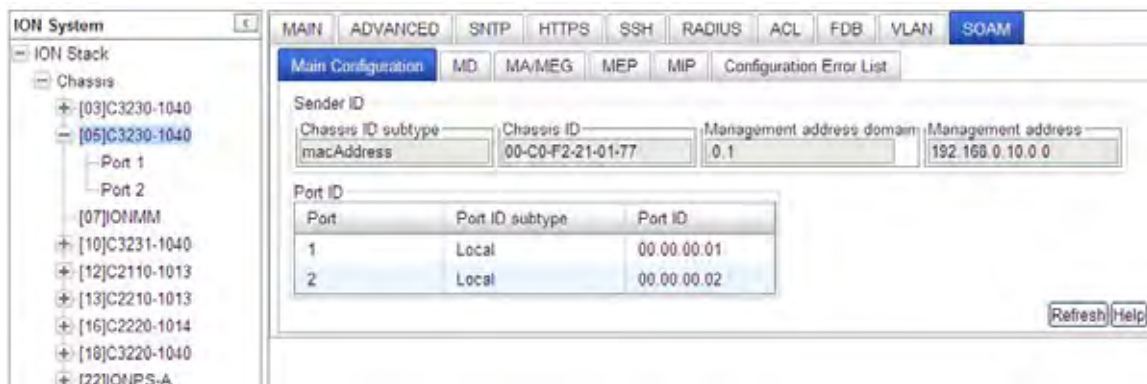
To delete an existing MIP, select the MIP ID from the table and click the **Delete** button.

See “[Appendix D: SOAM Configuration Example](#)” on page 419 for SOAM configuration examples via the CLI Method and the Web Method.

Verifying the SOAM Main Configuration

The **Main Configuration** sub-tab on the **SOAM** tab displays basic device configuration information.

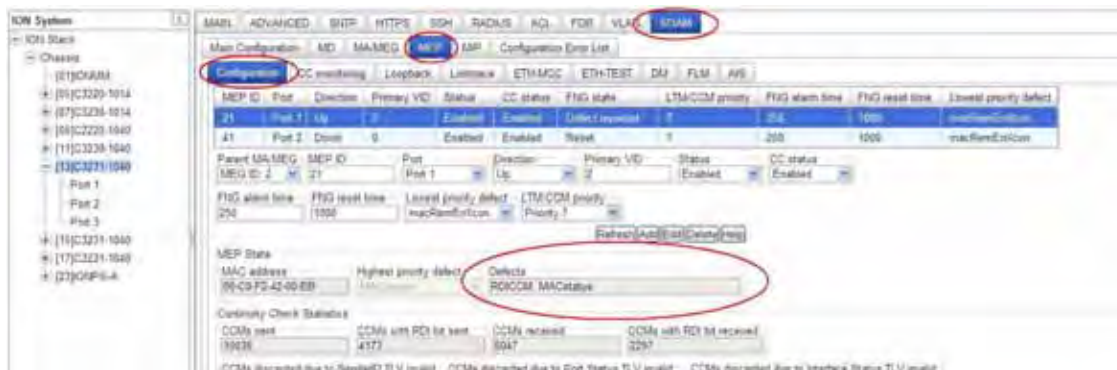
1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **Main Configuration** sub-tab.



3. Verify the **Sender ID** section information:
 - **Chassis ID subtype** (1. Chassis Component, 2. Interface Alias, 3. Port Component, 4. MAC Address, 5. Network Address, 6. Interface Name, or 7. Local).
 - **Chassis ID** (e.g., e.g., 00-C0-F2-21-01-77 in the sample screen above).
 - **Management address domain** (the TDomain that identifies the type and format of the related Sender ID TLV Man Address, used to access the SNMP agent of the system).
 - **Management address** (the TAddress that can be used to access the SNMP agent of the system, as it is sent in the SenderID TLV).
4. Verify the **Port ID** section information:
 - **Port** (the interface index for the port which Port ID should be configured).
 - **Port ID subtype** (1. Interface Alias, 2. Port Component, 3. MAC Address, 4. Network Address, 5. Interface Name, 6. Agent Circuit ID, or 7. Local).
 - **Port ID** (the Port ID value. The format is determined by the value of the TLV Port Subtype (e.g., 00.00.00.01 and 00.00.00.02).
5. Press the **Refresh** button to update the information at any time.

Viewing SOAM MEP Defects

The **SOAM > MEP > Configuration** sub-tab displays any MEP defects detected since the last refresh.



A MEP can detect and report a number of defects, and multiple defects can be present at the same time. The SOAM MEP defects reported are (in order of priority):

RDICCM - A remote MEP reported the RDI (Remote Defect Indication) bit in the last received CCM (Connectivity Check Message).

MACstatus - Either some remote MEP is reporting its Interface Status TLV as not Up, or all remote MEPs are reporting a Port Status TLV with a value other than psUp (Down, Testing, Unknown, Dormant, Not Present, Lower Layer Down).

RemoteCCM - The MEP is not receiving valid CCMs from at least one of the remote MEPs.

ErrorCCM - The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.

XconCCM - The MEP has received at least one CCM from either another MAID, or from a lower MD Level whose CCM Interval has not yet timed out.

Defects are separated from Fault Alarms. The loss of CCMs or the reception of a cross connected CCM are defects. A Fault Alarm is a Management operation (e.g., an unsolicited announcement by a Bridge).

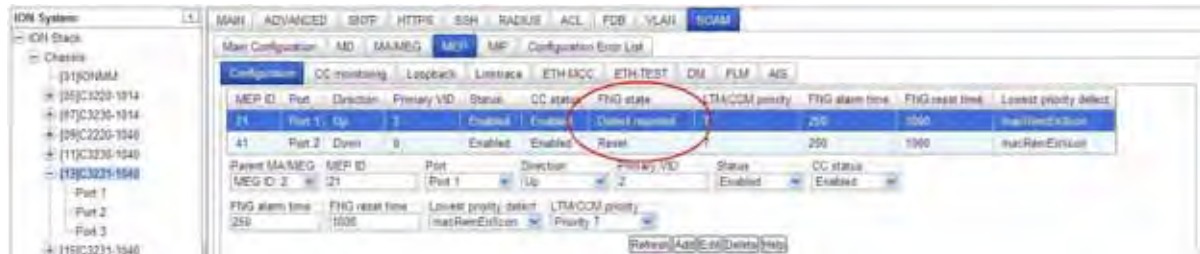
When a Fault Alarm is received, the normal operator procedure is to inspect the reporting MEP's managed objects, diagnose the fault, correct the fault, examine the MEP's managed objects to see whether the MEP Fault Notification Generator has reset, and then repeat those steps until the Fault Alarm has cleared.

The separate defects maintained by a MEP, listed above, are ranked by priority. So if a higher priority defect occurs after a lower priority defect has triggered a Fault Alarm, but before the Fault Alarm has reset, then the MEP will immediately issue another Fault Alarm. This lets the operator reliably prioritize Fault Alarms (e.g., cross connect errors are typically more concerning than loss of connectivity errors).

Section 4: Configuration

Viewing SOAM FNG (Fault Notification Generation) States

The **SOAM > MEP > Configuration** sub-tab displays FNG states. In the MEP ID table, the FNG state column shows the MEP Fault Notification Generation (FNG) status.

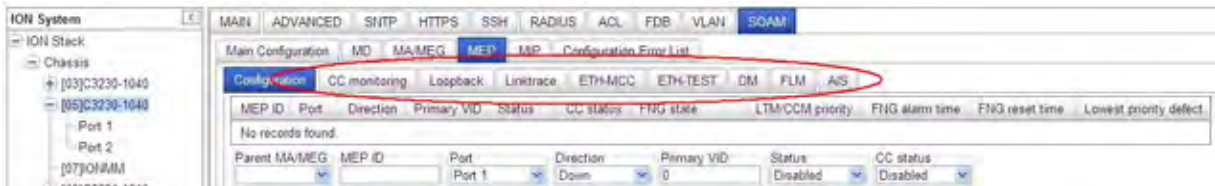


The MEP Fault Notification Generation (FNG) statuses are described below.

<u>Status</u>	<u>Description</u>
Reset	No defect has been present since the FNG Reset Time timer expired, or since the state machine was last reset.
Defect	A defect is present, but not for a long enough time to be reported (FNG Alarm Time).
Report Defect	A momentary state during which the defect is reported by sending a Fault Alarm notification, if that action is enabled.
Defect Reported	A defect is present, and a defect has been reported.
Defect Clearing	No defect is present, but the FNG Reset Time timer has not yet expired.

SOAM MEP Tests

The **MEP** sub-tab on the **SOAM** tab provides access to the Service level OAM (SOAM) tests.

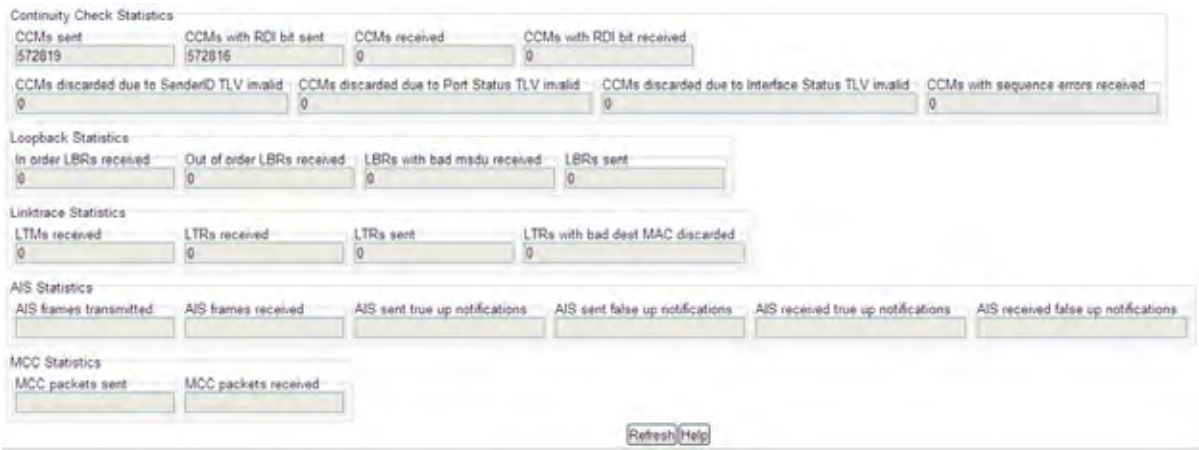


You can configure the following checks and tests from the **MEP** sub-tab on the **SOAM** tab.

- **CC Monitoring** (Continuity Checks Monitoring) on page 167
- **Loopback** (LB) on page 173
- **Linktrace** (LTR) on page 178
- **ETH-MCC** (Ethernet Maintenance Communication Channel) on page 184
- **ETH-TEST** on page 188
- **DM** (Frame Delay Measurement) on page 193
- **FLM** (Frame Loss Measurement) and **LM** (Periodic Loss Measurement) on page 198
- **AIS** (Ethernet Alarm Indication Signal) on page 204
- **RDI** (Ethernet Remote Defect Indication) on page 209

These checks and tests require that the SOAM MD/MA, MEG, MEP, and MIP are properly configured per the previous sections.

The **SOAM > MEP > Configuration** sub-tab also displays the current Service level OAM test results.



These SOAM test results include:

Continuity Check (CCM) Statistics: CCMs sent and received, with and without RDI bit set, discarded CCMs, and errored CCMs.

Section 4: Configuration

Loopback (LB) Statistics: LBRs received in and out of order, LBRs received with bad MDSU, and LBRs sent.

Linktrace Statistics: LTMs received, LTRs received and sent, and LTRs with bad destination MAC discarded.

AIS Statistics: AIS frames transmitted and received, and AIS frames transmitted and received with true up and false up notifications.

MCC Statistics: MCC packets sent and received.

Note: run one SOAM MEP test request at a time for a given MEP.

The SOAM MEP tests vary slightly between the IEEE 902.1ag and ITU-T 1731 standards. The differences are noted below.

Function	Feature	802.1ag	Y.1731
Connectivity Fault Management	Continuity Check	Yes	Yes
	Loopback	Yes	Yes
	Link Trace	Yes	Yes
	AIS	Not applicable	Yes
	RDI	Yes	Yes
Performance Monitoring	ETH-TST	Not applicable	Yes
	Loss Measurement	Not applicable	Yes
	Delay Measurement and Delay Variation Measurement	Not applicable	Yes

The SOAM MEP tests and checks are described in the following sub-sections.

CC Monitoring (Continuity Checks Monitoring)

Fault detection uses the Continuity Check protocol to detect both connectivity failures and unintended connectivity between service instances. Each MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA, and tracks the CCMs received from the other MEPs. All connectivity faults that can misdirect a CCM show up as differences between the CCMs received and the MEP's configured expectations. The state of the tracked CCMs can be displayed.

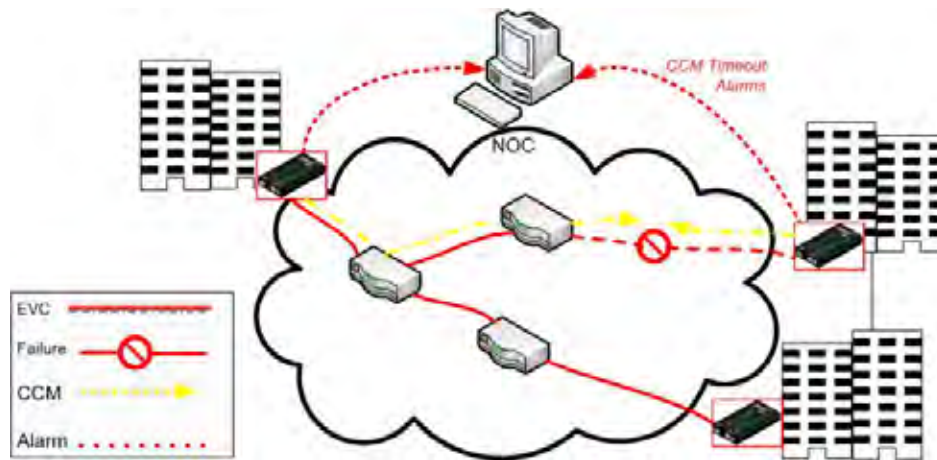


Figure 23: Continuity Checks (CC)

Each Continuity Check Message (CCM) is a multicast CFM PDU transmitted periodically by a MEP to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM. CCMs use addresses from the Continuity Check Message Group Destination MAC Address table. The CCM can be sent away from or towards the MAC Relay Entity.

The Continuity Check Message (CCM) provides a means to detect connectivity failures in an MA. Each MEP can be configured to periodically transmit a CCM. A connectivity failure is defined as either:

1. Inability of a MEP to receive three consecutive CCMs from any one of the other MEPs in its MA, indicating either a MEP failure or a network failure,
2. Reception by a MEP of a CCM with an incorrect transmission interval, indicating a configuration error,
3. Reception by a MEP of a CCM with an incorrect MEPID or MAID, indicating a configuration error or a cross connect error,
4. Reception by a MEP of a CCM with an MD Level lower than that of the MEP, indicating a configuration error or a cross connect error; or
5. Reception by a MEP of a CCM containing a Port Status TLV or Interface Status TLV, indicating a failed Bridge Port or aggregated port.

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

Section 4: Configuration

Note: run one SOAM MEP test request at a time for a given MEP.

CC Monitoring can be configured in the system using either the CLI or Web method.

CC Monitoring Config – CLI Method

This procedure displays the Continuity Check (CC) database for a given MEP via SOAM CLI command.

1. To configure the CCM and LTM priority, enter the set soam mep config command. Type:

```
set soam mep config mep-id=<1-8191> local-parent-id=<1-4095>
attr_name=(admin|cci|primaryvid|ccmltmpriority|faultalarmdetect|faultalarmreset|low
estprilevel|aisclient-add|aisclient-
remove|aistransmit|aisinterval|aisnotifyup|aisprocess|aisframepriority)
attr_value=(on|off|enable|disable|alldef|macremerrxcon|remerrxconn|errxconn|xconn|n
oxcon|1s|1min|...)
```

where:

ccmltmpriority={0-7} (the CCM and LTM priority)

all other parameters are as required.

2. To view the Continuity Check (CC) database, enter the **show soam mep cc** command.

Type: **show soam mep cc mep-id=<xx> local-parent-id=<yy>**

where:

xx= *mep-id* (the MEP ID of the MEP for which CC information is required (from 1-8191))

yy= *local-parent-id* (the MA/MEG identifier from 1- 4095)

3. Press the **Enter** key. The CC database displays for the specified MEP. For example:

```
C1|S13|L0D/>show soam mep cc mep-id=2 local-parent-id=2
MEP ID                : 2
MEG Local ID          : 0
MEG level              : 2
MEG name               : MEG1

Remote MEP ID         : 1
State                  : Failed
TimeStamp              : 5.9 sec
MAC                    : FF:FF:FF:FF:FF:FF
RDI BIT                : False
Port Status            : No Port State
Interface Status       : No Interface Status
Chassis id subtype    : None
Chassis id             :
Manage address domain : 0.0 (None)
Manage address         :
Autodetected           : No
```

The CC database parameters are described below:

<u>Parameter</u>	<u>Example</u>	<u>Range</u>
State:	Failed	CCM Test Passed or Failed;
Timestamp:	5.9 sec	A time in seconds;
RDI Bit:	False	True if Remote Defect indication enabled.
Port Status:	No Port State	None or active state of the port.
Interface Status:	No Interface Status	None or status of the link.
Chassis id / subtype:	None	Chassis information as available.
Manage address domain:	0.0 (None)	The management's domain.
Autodetected:	No	Yes if Autodetected, otherwise No.

- To view the SOAM MEP statistics, type:

```
show soam mep stats [mep-id=<1-8191> local-parent-id=<1-4095>]
```

where:

mep-id: (optional) The MEP identifier. If not present, the default is to display a list of all configured MEPs.

local-parent-id: MA/MEG identifier. Mandatory only if mep-id is specified.

- Press **Enter**. MEP CCM (and other) data displays.

- To view the SOAM MEP configuration, type:

```
show soam mep config [mep-id=<1-8191> local-parent-id=<1-4095>]
```

where:

mep-id: (optional) The MEP identifier. If not present, the default is to display a list of all configured MEPs.

local-parent-id: MA/MEG identifier. Mandatory only if mep-id is specified.

- Press **Enter**. MEP CCM (and other) data displays.

Note: The CLI commands to create a MA / MEG / MEP include parameters to define CC Monitoring parameters. These commands include:

```
set soam ma local-ma-id=  
set soam meg local-meg-id=  
set soam mep config mep-id=
```

See “[Configuring SOAM MEP](#)” on page 124. For a complete list of all CLI commands for CCM operations see the *ION System CLI Reference Manual*, 33461.

CC Monitoring Config – Web Method

Use this procedure to display Continuity Check (CC) information for a given MEP via the web interface.

Note: run one SOAM MEP test request at a time for a given MEP.

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. At **SOAM > MEP > Configuration**, select the line in the MEP ID table for the test.
3. Select the **SOAM** tab > **MEP** sub-tab > **CC monitoring** sub tab.



4. Click the **Refresh** button to update the fields. The **CC monitoring** fields are described below:

Local MEP ID - Identifier of local MEP.

Remote MEP ID - MA/MEG End Point Identifier of a remote MEP.

State – the operational state of the remote MEP. This lists the reception of valid CCMs from a remote MEP with a specific MEPID. It uses a timer that expires in 3.5 times the length of time indicated by the CCM Interval setting. The values are:

- *Idle* - Momentary state during reset.
- *Start* - The timer has not expired since the state machine was reset, and no valid CCM has yet been received.
- *Failed* - The timer has expired, both since the state machine was reset, and since a valid CCM was received.
- *Ok* - The timer has not expired since a valid CCM was received.

Timestamp - the time (SysUpTime) at which the Remote MEP last entered either the *Failed* or *Ok* state.

MAC address - The MAC address of the remote MEP.

RDI bit – the state of the RDI (Remote Defect Indication) bit in the last received CCM: *True* for RDI=1, or *False* if no RDI bit was received.

Port status – a value from the Port Status TLV from the last CCM received from the last MEP. It indicates the ability of the Bridge Port on which the transmitting MEP resides to pass ordinary data, regardless of the status of the MAC. The values are:

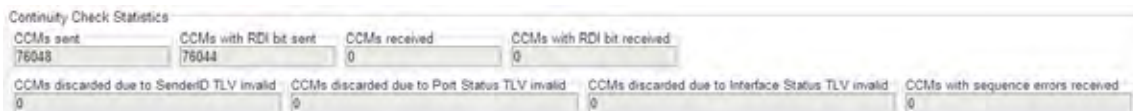
- *No Port State* - indicates either that no CCM has been received or that no port status TLV was present in the last CCM received.
- *Blocked* - indicates ordinary data cannot pass freely through the port on which the remote MEP resides.
- *Up* - Ordinary data can pass freely through the port on which the remote MEP resides.

Interface status - a value from the Interface Status TLV from the last **CCM** received from the last MEP. It indicates the status of the Interface within which the MEP transmitting the CCM is configured, or the next lower Interface in the Interface Stack, if the MEP is not configured within an Interface.

- *No Interface Status* - indicates either that no CCM has been received or that no interface status TLV was present in the last CCM received. The values are:
 - *Up* - the interface is ready to pass packets.
 - *Down* - the interface cannot pass packets
 - *Testing* - the interface is in some test mode.
 - *Unknown* - the interface status cannot be determined for some reason.
 - *Dormant* - the interface is not in a state to pass packets but is in a pending state, waiting for some external event.
 - *Not Present* - some component of the interface is missing.
 - *Lower Layer Down* - the interface is down due to state of the lower layer interfaces.

Auto added - *True*, if this remote MEP has been auto added, otherwise *False*.

5. At **SOAM > MEP > Configuration**, view the **Continuity Check Statistics** section.



Continuity Check Statistics			
CCMs sent	CCMs with RDI bit sent	CCMs received	CCMs with RDI bit received
76048	76044	0	0
CCMs discarded due to SenderID TLV invalid	CCMs discarded due to Port Status TLV invalid	CCMs discarded due to Interface Status TLV invalid	CCMs with sequence errors received
0	0	0	0

The **Continuity Check Statistics** fields are:

CCMs sent - the total number of Continuity Check messages transmitted.

CCMs with RDI bit sent - the total number of sent CCMs with RDI bit set.

CCMs Received – the total number of CCMs received from all remote MEPs.

CCMs with RDI bit received - the total number of CCMs with RDI bit set received from all remote MEPs.

CCMs discarded due to SenderID TLV invalid - the total number of CCMs with invalid Sender ID TLV received from all remote MEPs.

CCMs discarded due to Port Status TLV invalid - the total number of CCMs with invalid Port Status TLV received from all remote MEPs.

Section 4: Configuration

CCMs discarded due to Interface Status TLV invalid - the total number of CCMs with invalid Interface Status TLV received from all remote MEPs.

CCMs with sequence errors received - the total number of out-of-sequence CCMs received from all remote MEPs.

Loopback (LB)

The Loopback protocol is used to perform fault verification. A MEP can be ordered to transmit a unicast Loopback Message (LBM) to a MEP or MIP in the MA, whose MAC address can be discovered from CCMs (MEPs only) or LTMs/LTRs (MEPs or MIPs). The receiving MP responds by transforming the LBM into a unicast Loopback Reply (LBR) sent back to the originating MEP. That MEP records the responses for examination by the administrator.

Each Loopback Message (LBM) is a unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR. Each Loopback Reply (LBR) is the unicast CFM PDU transmitted by an MP to a MEP, in response to an LBM received from that MEP. The purpose of transmitting Loopback messages is to signal to the MEP to transmit some number of LBMs.

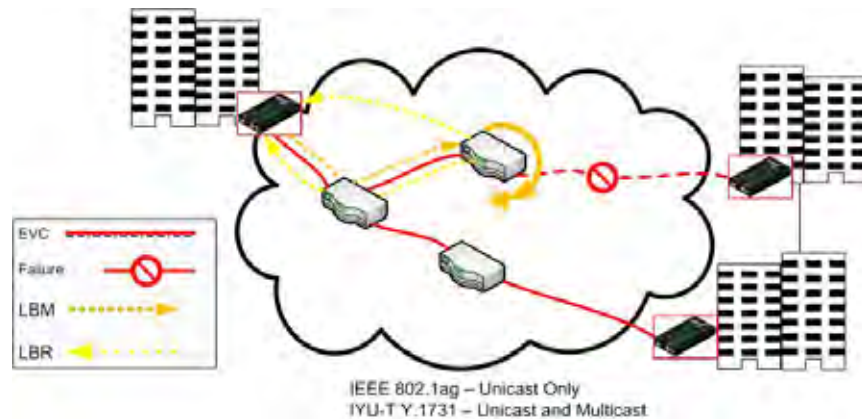


Figure 24: Loopbacks (LB)

LBM outputs can include:

1. An indication of whether the command was accepted by the MEP, either:
 - a. Operation rejected due to nonexistent MEP;
 - b. Operation rejected due to invalid number of LBMs to be transmitted;
 - c. Operation rejected due to too much data to be transmitted;
 - d. Operation rejected due to invalid priority or drop-eligible parameters to be transmitted;
 - e. The LBM(s) will be (or have been) sent; or
 - f. The LBM(s) will not be sent (e.g., because the Bridge is busy with another LBM transmit; and
 - g. Operational status.
2. The Loopback Transaction Identifier of the first LBM to be sent. The value returned is undefined if the Transmit Loopback Messages command was not accepted.

Note: IEEE 802.1ag supports Unicast only, while ITU-T Y.1731 supports Unicast and Multicast.

Section 4: Configuration

A unicast Loopback Message (LBM) is used for Fault verification and isolation. To verify the connectivity between MEPs and MIPs, a MEP can be instructed by a system administrator to issue one or more LBMs.

The LBM is initiated by a MEP with specified `destination_address`, `priority`, and `drop_eligible` parameters, the `destination_address` being the Individual MAC address of another MP within the same Maintenance Association as the transmitting MEP. The receiving MP responds to the LBM with a unicast Loopback Reply (LBR).

When an LBM is received by an MP Loopback Responder, it may be examined for validity and discarded if invalid. Whether or not the LBM is examined for validity, it will be discarded if the `source_address` is a Group and not an Individual MAC address.

Note: run one SOAM MEP test request at a time for a given MEP.

Loopback (LB) can be configured in the system using either the CLI or Web method.

Loopback (LB) Config – CLI Method

This procedure initiates a loopback (LB) request and then displays the status of that loopback request for the specified MEP via SOAM CLI commands.

1. To initiate a Loopback request, enter the **send soam mep loopback mep-id** command.

Type: **send soam mep loopback mep-id=<uu> local-parent-id=<vv> dest=DEST amount-frames=<ww> [data=DATA-TLV]**

Where:

vv = mep-id (the MEP ID of the MEP to initiate the loopback - from 1-8191)

ww = local-parent-id (the MA/MEG identifier - from 1-4095)

xx = dest (the type of destination - either a single destination (MAC address or remote MEP ID) or multicast)

yy = amount-frames (the number of packets to send -for a multicast destination, enter a 1)

zz = data (optional; the data to be transmitted in loopback message)

2. Press the **Enter** key. This initiates a Loopback request for the specified MEP. Example:

```
C1|S13|L0D/> send soam mep loopback mep-id=2 local-parent-id=2 dest=00-01-02-03-04-05 amount-frames=1 data=123
```

3. To display the status of the Loopback request for the specified MEP, enter the command **show soam mep loopback mep-id**.

Type: **show soam mep loopback mep-id=<xx> local-parent-id=<yy> dest=(zz)**

Where:

xx = the mep-id (the MEP ID of the MEP for which loopback information is requested (from 1-8191))

yy = the local-parent-id (the MA/MEG identifier from 1-4095)

zz = the destination statistics type (either **unicast** or **multicast**)

4. Press the **Enter** key. The status of the Loopback request displays. For example:

```
C1|S13|L0D/>show soam mep loopback mep-id=2 local-parent-id=2
dest=unicast
First sent LBM sequence number : 3
Destination MAC address       : 00-00-00-00-00-01
LBMs sent                     : 1
LBRs received                 : 0
Status                        : Failed

First sent LBM sequence number : 4
Destination MAC address       : 00-01-02-03-04-05
LBMs sent                     : 1
LBRs received                 : 0
Status                        : Failed
```

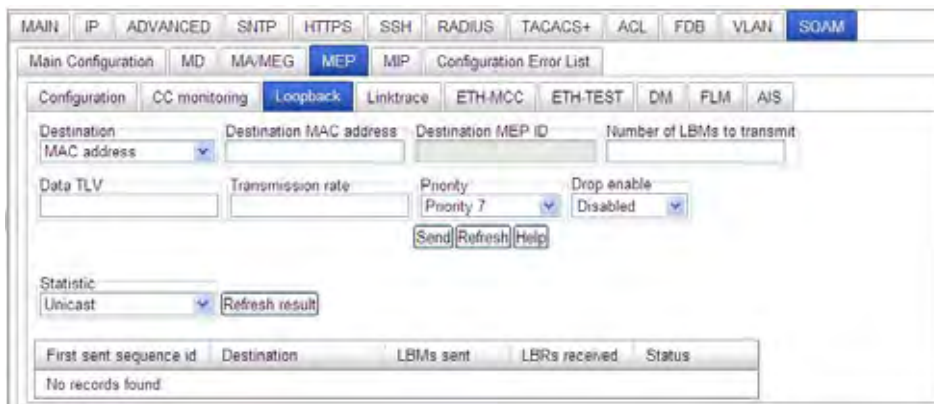
The Loopback parameters are described below:

<u>Parameter</u>	<u>Example</u>	<u>Range</u>
First sent LBM sequence number:	3, 4, 5	An ID number in sequence.
Destination MAC address:	00-00-00-00-00-01	A valid MAC address.
LBMs sent:	1	A number greater than 0;.
LBRs received:	0	A number 0 or greater.
Status:	Failed	LB Passed or Failed.

Loopback (LB) Config – Web Method

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP. **Note:** run one SOAM MEP test request at a time for a given MEP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. At **SOAM > MEP > Configuration**, select the line in the MEP ID table for the test.
3. Select the **SOAM** tab > **MEP** sub-tab > **Loopback** sub tab.



4. In the **Destination** field, select **Mac address**, **MEP ID**, or **Multicast**.
 - *MAC address* indicates that unicast destination MAC address of the target MEP is used for Loopback transmission.
 - *MEP ID* indicates that MEPID of the target MEP is used for Loopback transmission.
 - *Multicast* indicates that multicast loopback should be used. The remaining fields are grayed out and cannot accept entries.
5. In the **Destination MAC address** field, enter the target MAC Address to be transmitted toward (a unicast destination MAC address). This field is active if the **Destination** field has **MAC address** selected.
6. In the **Destination MEP ID** field, enter the MA/MEG End Point Identifier of another MEP in the same MA/MEG to which the LBM is to be sent. This field is active if the **Destination** field has **MEP ID** selected. The valid range is 1 – 8191.
7. In the **Number of LBMs to transmit** field, enter the number of Loopback messages to be transmitted. The valid range is 1 – 1024 LBMs.
8. In the **Data TLV** field, enter the amount of data to be included in the Data TLV, if the Data TLV is selected to be sent.
9. In the **Transmission rate** field, enter the number of loopback messages sent per second. The valid range is 1 – 80 LBMs per second.
10. At the **Priority** dropdown, select a Priority from **1** (lowest) to **7** (highest).
11. At the **Drop enable** dropdown, select Drop enable (**Enabled** or **Disabled**).
12. In the **Statistic** field, select either **Unicast** or **Multicast**. The default is **Unicast**.

13. Click the **Send** button. A table displays the test results.

The Unicast Loopback test result fields are:

First sent sequence id – the Loopback Transaction Identifier of the first LBM sent.

Destination – the MAC Address of the destination MP.

LBMs sent – the number of Loopback Messages that were sent.

LBRs received – the number of Loopback Replies that were received.

Status – specifies the state of the current Loopback request:

- *None* – no LB test currently in process.
- *In Progress* – a LB test is being executed.
- *Failed* – a LB test was executed but was not successful.
- *Succeeded* – the LB test executed successfully.

The Multicast Loopback test result fields are:

ID - the index of the multicast loopback result.

Remote MAC address – the MAC address for the received reply.

14. At **SOAM > MEP > Configuration**, view the **Loopback Statistics** section.

Loopback Statistics			
In order LBRs received	Out of order LBRs received	LBRs with bad msdu received	LBRs sent
0	0	0	0

The **Loopback Statistics** fields are:

In order LBRs received - the total number of valid, in-order Loopback Replies received.

Out of order LBRs received - the total number of valid, out-of-order Loopback Replies received.

LBRs with bad msdu received - the total number of LBRs received whose MAC Service Data Unit did not match (except for the OpCode) that of the corresponding LBM.

LBRs sent - the total number of Loopback Replies transmitted.

Linktrace

Link Trace messages are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP. Each receiving MEP sends a Linktrace Reply (LTR) directly to the Originating MEP, and regenerates the Linktrace Message.

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

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

Linktrace Replies (LTRs) are carried in unicast frames. Linktrace Messages (LTMs) use addresses from the Linktrace Message Group Destination MAC Addresses table.

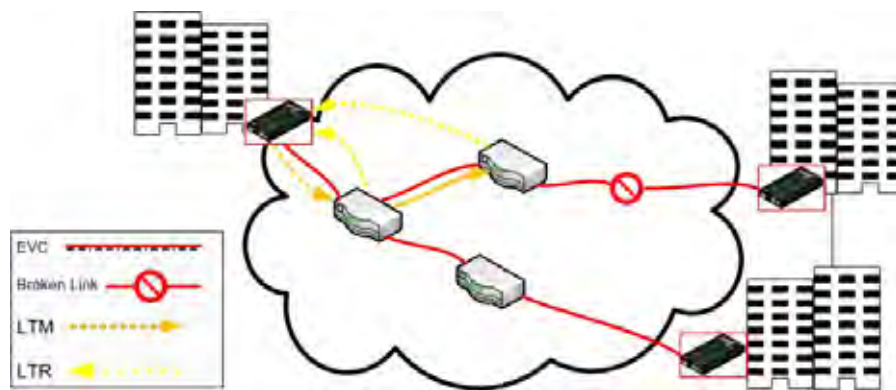


Figure 25: Link Trace (LT)

An LTM is used to signal to the MEP to transmit an LTM and to create an LTM entry in the MEP's Linktrace Database. The MA End Point can then be examined to determine whether or not the corresponding LTRs have been received by the MEP.

Outputs provide an indication of whether the command was accepted by the MEP, either:

1. Operation rejected due to nonexistent MEP;
2. Operation rejected due to invalid Flags field to be transmitted;
3. Operation rejected due to invalid Target MAC Address to be transmitted;
4. Operation rejected due to invalid LTM TTL field to be transmitted;
5. Command accepted and the LTM has (or will be) transmitted; or
6. Command was rejected and no LTM will be sent (e.g., because of another LTM transmit operation).

The MEP's Linktrace database stores the LTM entry for a previously transmitted LTM with a specific LTM Transaction Identifier. An LTM entry consists of a list of LTR entries, each corresponding to a Linktrace Reply (LTR) PDU received in response to that LTM.

LT outputs include an indication of whether the command was accepted by the MEP, either:

1. Operation rejected due to nonexistent MEP;
2. Operation rejected due remote MEPID not configured in MA; or
3. Operation accepted.

Note: run one SOAM MEP test request at a time for a given MEP.

Linktrace (LT) can be configured in the NID using either the CLI or Web method.

Linktrace (LT) Config – CLI Method

This procedure initiates a Linktrace (LT) request and then displays the status of that Linktrace request for the specified MEP via SOAM CLI commands.

1. To initiate a Linktrace request for a given MEP, enter the **send soam mep linktrace mep-id** command.

Type: **send soam mep linktrace mep-id=<vv> local-parent-id=<ww> dest=xx use-fdb-only=(yy) ttl=<zz>**

Where:

vv = mep-id (the MEP ID of the MEP to initiate the linktrace, from 1-8191)

ww = local-parent-id (the MA/MEG identifier, from 1-4095)

xx = dest (the type of destination; either a MEPID or a MAC address)

yy = use-fdb-only (determines if the Linktrace relies only on the forwarding database; *true* or *false*)

zz = ttl (the time to live value for the initial LTM request, from 0-255)

2. Press the **Enter** key.
3. To display the status of a Linktrace request for a given MEP, enter the **show soam mep linktrace mep-id** command.

Type: **show soam mep linktrace mep-id=<xx> local-parent-id=<yy> tid=<zz>**

Where:

xx = mep-id (the MEP id of the MEP for which linktrace info is required, from 1-8191)

yy = the local-parent-id (the MA/MEG identifier, from 1-4095)

zz = tid (the Transaction ID of the initiated link trace to display, from 0-4294967295)

4. Press the **Enter** key. The Linktrace information displays. For example:

Section 4: Configuration

```

C1|S13|L0D/>send soam mep linktrace mep-id=2 local-parent-id=2 dest=00-
01-02-03-04-05 use-fdb-only=true ttl=10
C1|S13|L0D/>show soam mep linktrace mep-id=2 local-parent-id=2 tid=1

TTL                                     : 9
Responder MAC address                   : 00-a1-b0-a1-69-5e
LTM was forwarded                       : Yes
Terminal MEP was reached                 : No
Relay Action                            : RlyUndefined
Egress Action                           : OK
Egress Address                          : 00-a1-b0-a1-69-5e

TTL                                     : 8
Responder MAC address                   : 00-a1-b0-a1-59-48
LTM was forwarded                       : Yes
Terminal MEP was reached                 : No
Relay Action                            : RlyUndefined
Ingress Action                          : OK
Ingress Address                         : 00-a1-b0-a1-59-48

```

5. Press the **Enter** key.

The Linktrace **show** command parameters are described below:

<u>Parameter</u>	<u>Example</u>	<u>Range / Comment</u>
TTL:	8	0 - 255
Responder MAC address:	00-a1-b0-a1-59-48	A valid MAC address
LTM was forwarded:	Yes	Yes (relies on LT) or No
Terminal MEP was reached:	No	Yes if successful; otherwise No.
Relay Action:	RlyUndefined	RlyUndefined or RlyDefined
Ingress Action:	OK	OK or failed.
Ingress Address:	00-a1-b0-a1-59-48	A valid MAC address.

Note: The CLI commands to create a MA / MEG / MEP include parameters to define Linktrace parameters. These commands include:

```

send soam mep linktrace mep-id=
show soam mep linktrace mep-id=

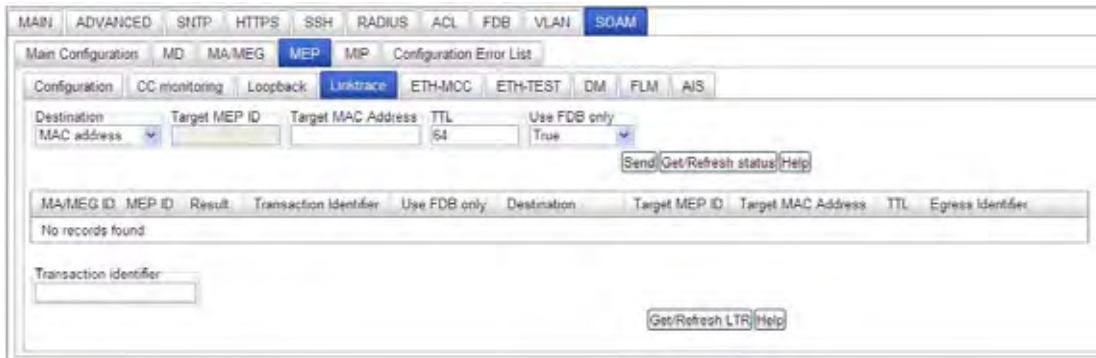
```

See “[Configuring SOAM MEP](#)” on page 124. For a complete list of CLI commands for all operations, see the *ION System CLI Reference Manual*, 33461.

Linktrace (LT) Config – Web Method

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP. **Note:** run one SOAM MEP test request at a time for a given MEP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab > **Linktrace** sub-tab.



3. In the **Destination** field, select either **Mac address** or **MEP ID**. This is the target of the Linktrace; either a) the unicast destination MAC address of the target MEP is used for Linktrace transmission, or b) the MEPID of the target MEP is used for Linktrace transmission.
4. In the **Target MEP ID** field, enter the MEP ID of the desired Linktrace target. This is the MA/MEG End Point Identifier of another MEP in the same MA/MEG. This address is used if **MEP ID** was selected in the **Destination** field.
5. In the **Target MAC Address** field, enter a unicast destination MAC address. This is the Target MAC Address Field of the Linktrace transmission. This address is used if **Mac address** was selected in the **Destination** field.
6. In the **TTL** field, enter the LTM TTL. The **TTL** entry defines the number of hops remaining to the LTM. The number is decremented by 1 by each Linktrace Responder that handles the LTM. The value returned in the LTR is one less than the value received in the LTM. If the LTM TTL is 0 or 1, the LTM is not forwarded to the next hop, and if 0, no LTR is generated. The default is 64 hops.
7. In the **Use FDB only** field, enter **True** or **False**. This is the flags field for LTMs transmitted by the MEP.
8. Click the **Send** button.
9. Select a line in the MEP Linktrace transactions table.

Section 4: Configuration

10. Select the **Get/Refresh LTR** button. The MA/MEG ID information displays in the MEP Linktrace transactions table.

MA/MEG ID	MEP ID	Result	Transaction Identifier	Use FDB only	Destination	Target MEP ID	Target MAC Address	TTL	Egress Identifier
3	320	True	1	False	MAC address	40	00-00-00-00-00-00	64	00-00-00-C0-F2-42-00-E0
11	40	True	0	False	MAC address	0	00-00-00-00-00-00	64	00-00-00-00-00-00-00-00
111	50	True	0	False	MAC address	0	00-00-00-00-00-00	64	00-00-00-00-00-00-00-00

Transaction identifier
0

Get/Refresh LTR Help

The MEP Linktrace transactions table values are:

Result - Indicates the result of the operation, either:

- True - The Linktrace Message will be (or has been) sent.
- False - The Linktrace Message will not be sent.

Transaction identifier – The LTM Transaction Identifier of the LTM sent.

TTL – TTL (Time to live) field value for a returned LTR. The default TTL for ION software is 64 transmissions sent/received without errors.

Egress identifier - identifies the MEP Linktrace Initiator that is originating, or the Linktrace Responder that is forwarding, this LTM. Contains an IEEE MAC address unique to the system in which the MEP Linktrace Initiator or Linktrace Responder resides. The value is sufficient to uniquely identify the MEP Linktrace Initiator or Linktrace Responder within the system.

11. Select the **Get/Refresh LTR** button. The SOAM Linktrace results display at the bottom of the screen.

Receive order	TTL	LTM was forwarded	Sender MAC address	Terminal MEP was reached	Last egress identifier	Next egress identifier	Relay action
1	63	True	00-C0-F2-42-00-DF	False	00-00-00-C0-F2-42-00-E0	00-00-00-C0-F2-42-00-DF	Down

The SOAM Linktrace results fields are:

Receive order – the order in which LTR results are returned, starting with 1.

TTL – the TTL (Time to live) field value for the returned LTR.

Sender MAC Address – the MAC address of LTR transmission.

Terminal MEP was reached – a value (*True* or *False*) stating whether the forwarded LTM reached a MEP enclosing its MA/MEG, as returned to the Terminal MEP.

Last egress identifier – the Last Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Last Egress Identifier identifies the MEP Linktrace Initiator that originated, or the Linktrace Responder that forwarded, the LTM to which this LTR is the response. This is the same value as the Egress Identifier TLV of that LTM.

Next egress identifier – the Next Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Next Egress Identifier Identifies the Linktrace Responder that transmitted this LTR, and can forward the LTM to the next hop. This is the same value as the Egress Identifier TLV of the forwarded LTM, if any.

Relay action – the value returned in the Relay Action field; either:

- Hit: the Link trace has reached the MEP/MIP that was targeted with the LTM.
- Fdb: the Egress port was determined using the FDB table - the Forwarding Database ID number for this VLAN.
- Mpdb: the egress port was determined using the CCM database.
- Down: the selected MEP is unreachable (status=disabled, or FNG state= Defect reported).

12. At **SOAM > MEP > Configuration**, view the **Linktrace Statistics** section.

Linktrace Statistics			
LTM's received	LTRs received	LTRs sent	LTRs with bad dest MAC discarded
0	0	0	0

The **Linktrace Statistics** fields are:

LTM's received - the total number of LTMs received for this test.

LTRs received - the total number of LTRs received for this test.

LTRs sent - the total number of LTRs sent for this test.

LTRs with bad dest MAC discarded - the total number of LTRs with an unknown or undefined destination MAC address received for this test.

ETH-MCC (Ethernet Maintenance Communication Channel)

The Ethernet Maintenance Communication Channel (ETH-MCC) function provides a channel for maintenance communication between a pair of MEPs. ETH-MCC is used to perform remote management.

A MEP can send a frame with ETH-MCC information to its peer MEP with a remote maintenance request, remote maintenance reply, notification, etc.

The specific configuration information required by a MEP to support ETH-MCC includes:

- MEG level – MEG level at which the MEP exists.
- Unicast MAC address of the remote MEP for which ETH-MCC is intended.
- OUI – Organizationally Unique Identifier used to identify the organization defining a specific format and meaning of ETH-MCC.
- Data – Additional information that may be needed which is dependent on the specific application of ETH-MCC.
- Priority – Identifies the priority of frames with ETH-MCC information. This information is configurable for each operation.
- Drop Eligibility – Frames with ETH-MCC information are always marked as drop ineligible (this information is not necessarily configured).

A remote MEP, upon receiving a frame with ETH-MCC information and with a correct MEG level, passes the ETH-MCC information to the management agent, which may also respond.

A MIP is transparent to the frames with ETH-MCC information and therefore does not require any configuration information to support ETH-MCC functionality. The PDU used for ETH-MCC information is MCC. Frames carrying the MCC PDU are called MCC frames.

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP. **Note:** run one SOAM MEP test request at a time for a given MEP.

ETH-MCC can be configured in the system using either the CLI or Web method.

ETH-MCC Config – CLI Method

This procedure sends a Y.1731 Ethernet Maintenance Communication Channel (ETH-MCC) request from a local MEP towards a given destination and then displays the configuration error list for the given port and VLAN via SOAM CLI commands.

1. To initiate a Y.1731 ETH-MCC request for a given MEP, enter the **send soam mep mcc mep-id** command. This command provides a maintenance communication channel between a pair of MEPs.

Type: **send soam mep mcc mep-id=<vv> local-parent-id=<ww> dest=xx oui=yy data=zz**

where:

vv = mep-id (the MEP ID of the MEP which is to be configured for ETH MCC, from 1-8191)

ww = local-parent-id (the MEG identifier, from 1-4095)

xx = dest (the destination for which the message is destined - either a MEPID or a MAC address)

yy = oui (3 bytes in hex for the Organizationally Unique Identifier of the organization defining the format of MCC Data)

zz = data (the data to send to the destination)

2. Press the **Enter** key.
3. To show the Configuration Error List for the given port and VLAN, enter the **show soam conferror vid** command.

Type: **show soam conferror vid=<2-4095> port=<1-2>**

where:

yy = vid (the VLAN ID, from 2-4095)

zz = port (the Port number, either 1 or 2)

4. Press the **Enter** key. For example:

```
C1 | S5 | L1D > send soam mep mcc mep-id=2 local-parent-id=2 dest=00-01-02-03-04-05
oui=123 data=123445
C1 | S5 | L1D > show soam conferror vid 1 port 2
No config errors.
C1 | S5 | L1D >
```

Note: The CLI commands to create a MA / MEG / MEP include parameters to define ETH-MCC parameters. These commands include:

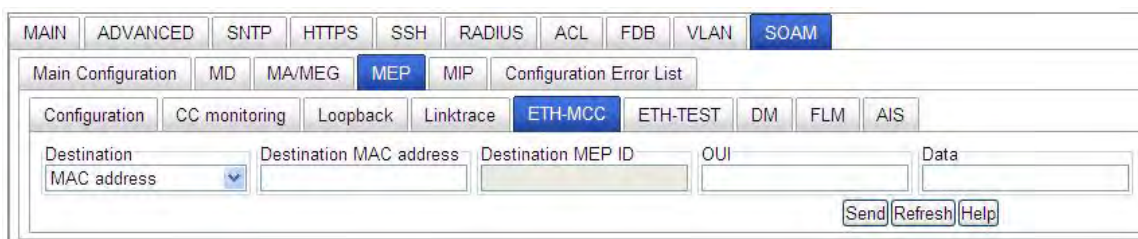
send soam mep mcc mep-id=

See “[Configuring SOAM MEP](#)” on page 124. For a complete list of CLI commands for all operations, see the *ION System CLI Reference Manual*, 33461.

ETH-MCC Config – Web Method

This procedure sends a Y.1731 Ethernet Maintenance Communication Channel (ETH-MCC) request from a local MEP towards a given destination and then displays the configuration error list for the given port and VLAN via the Web interface.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab > **ETH-MCC** sub tab.



3. In the **Destination** field, select either **MAC address** or **MEP ID**. This is the type of target MEP to be used for MCC transmission. Selecting **MAC address** indicates that the unicast destination MAC address of the target MEP will be used for MCC transmission. Selecting **MEP ID** indicates that the MEPID of the target MEP will be used for MCC transmission.
4. In the **Destination MAC address** field, enter the target MAC Address to be transmitted to. This is the unicast destination MAC address. This address is used if **MAC address** was selected in the **Destination** field in the previous step.
5. In the **Destination MEP ID** field, enter the MEP ID of the remote MEP to which the MCC is to be sent. This address is used if **MEP ID** was selected in the **Destination** field in step 3 above. The valid range is 1- 8191.
6. In the **OUI** field, enter an Organizationally Unique Identifier (OUI) of the organization defining the format of MCC Data. The OUI is issued by IEEE, and each company is assigned its own unique OUI (a 3 byte value from 00:00:00 to FF:FF:FF defined by IEEE).
7. In the **Data** field, enter data to send to the destination for this MCC test. The MCC test returns a ‘Failed’ status if no data is specified.
8. Click the **Send** button to send a Y.1731 ETH-MCC request from a local MEP towards the specified destination and then display the configuration error list for the given port and VLAN.

- At **SOAM > MEP > Configuration** locate the MCC Statistics section and view the MCC Statistics for the desired MEP ID.



The MCC Statistics are:

MCC packets sent - the total number of sent MCCs with this test since the last refresh.

MCC packets received - the total number of received MCCs with this test since the last refresh.

- At **SOAM > Configuration Error List**, view the set of configuration errors generated.



If necessary, click **Refresh** to update the information.

The IEEE802.1ag standard lists the possible Configuration errors (CFM Leak, Conflicting VIDs, Excessive Levels, and Overlapped Levels). If error free, displays “*No config errors.*”

CFM leak: MAX is associated with a specific VID list, one or more of the VIDs in MAX can pass through the Bridge Port, no Down MEP is configured on any Bridge Port for MAX, and some other MAY, at a higher MD Level than MAX, and associated with at least one of the VID(s) also in MAX, does have a MEP configured on the Bridge Port.

Conflicting VIDs: MAX is associated with a specific VID list, an Up MEP is configured on MAX on the Bridge Port, and some other MAY, associated with at least one of the VID(s) also in MAX, also has an Up MEP configured on some Bridge Port.

Excessive Levels: The number of different MD Levels at which MIPs are to be created on this port exceeds the Bridge's capabilities.

Overlapped Levels: A MEP is created for one VID at one MD Level, but a MEP is configured on another VID at that MD Level or higher, exceeding the Bridge's capabilities.

- Click the **Refresh** button to generate updated information.

ETH-TEST

The Ethernet test signal function (ETH-Test) is used to perform one-way on-demand in-service or out-of-service diagnostics tests. This includes verifying bandwidth, throughput, frame loss, bit errors, etc.

When configured to perform ETH-Test, a MEP inserts frames with ETH-Test information with specified throughput, frame size and transmission patterns.

When an out-of-service ETH-Test is performed, client data traffic is disrupted in the diagnosed entity. The MEP configured for the out-of-service test transmits LCK frames in the immediate client (sub-) layer.

When an in-service ETH-Test is performed, data traffic is not disrupted and the frames with ETH-Test information are transmitted in such a manner that a limited part of the service bandwidth is utilized. This rate of transmission for frames with ETH-Test information is pre-determined for in-service ETH-Test function.

Specific configuration information required by a MEP to support ETH-Test includes:

- MEG level – MEG level at which the MEP exists.
- Unicast MAC address of the peer MEP for which ETH-Test is intended. This information is configurable per operation.
- Data – Optional element whose length and contents are configurable at the MEP. The contents can be a test pattern and an optional checksum (e.g., pseudo-random bit sequence (PRBS), all '0' pattern, etc.). At the transmitting MEP and receiving MEP, configuration is required for a test signal generator associated with the MEP.
- Priority – Identifies the priority of frames with ETH-Test information (this information is configurable per operation).
- Drop Eligibility – Identifies the eligibility of frames with ETH-Test information to be dropped when congestion conditions are encountered.

A MIP is transparent to the frames with ETH-Test information and therefore does not require any configuration information to support ETH-Test functionality.

A MEP inserts frames with ETH-Test information towards a targeted peer MEP. The receiving MEP detects these frames with ETH-Test information and makes the intended measurements.

The PDU used for ETH-Test information is TST; Frames carrying the TST PDU are called TST frames.

A test signal generator associated with a MEP can transmit TST frames as often as the test signal generator configuration. Each TST frame is transmitted with a specific sequence number. A different sequence number must be used for every TST frame, and no sequence number from the same MEP may be repeated within one minute.

When a MEP is configured for an out-of-service test, the MEP also generates LCK frames at the immediate client MEG level in the same direction where TST frames are transmitted.

When a MEP receives TST frames, it examines them to ensure that the MEG level corresponds to its own configured MEG level. If the receiving MEP is configured for ETH-TST function, the test signal detector

associated with the MEP detects bit errors from the pseudo-random bit sequence of the received TST frames and reports such errors. When a receiving MEP is configured for an out-of-service test, it also generates LCK frames at the client MEG level in the direction in which the TST frames are received.

Note: run one SOAM MEP test request at a time for a given MEP.

ETH-TEST can be configured in the system using either the CLI or Web method.

ETH-TEST Config – CLI Method

These ETH-TST procedures are applicable only for MEPs configured in Y.1731 mode. All ETH-TST procedures are uni-directional. One MEP is designated as originator, and the far end MEP is the receiver. A test request is generated at the originator, while the result of the procedure is checked at the receiver.

1. To send a Y.1731 ETH-TST request from a local MEP towards a given destination, enter the command **send soam mep test mep-id**. Note that this command will fail if another request is still in progress.

Type:

```
send soam mep test mep-id=<uu> local-parent-id=<vv> dest=ww pattern=(xx)
size=<yy> frame-num=<zz>
```

Where:

uu = mep-id (the MEP ID of the MEP which is to be configured for ETH-TST, from 1-8191)

vv = local-parent-id (the MEG identifier, from 1-4095)

ww = dest (the destination for which the delay is to be measured; either a MEPID or a MAC address)

xx = pattern (the Pattern to be used in the message; either **nullnocrc**, **nullcrc**, **prbs231nocrc**, or **prbs231crc**)

yy = size (the pattern size, excluding CRC; from 0-1467 bytes)

zz = frame-num (the number of packets to be sent, from 1-32)

For example: C1|S13|L0D/> **send soam mep test mep-id=2 local-parent-id=2 dest=00-01-02-03-04-05 pattern=prbs231crc size=30 frame-num=2**

2. Press the **Enter** key.
3. To monitor the status of the Y.1731ETH-TST requests, enter the command **show soam mep test**. This displays the status and statistics information regarding the ETH-TST procedures which have been executed on the specified MEP.

Type: **show soam mep test mep-id=<1-8191> local-parent-id=<1-4095>**

Where:

Section 4: Configuration

yy = the test mep-id (the MEP ID of the MEP which will display its ETH TST statistics, from 1-8191)

zz = the local-parent-id (the MEG identifier, from 1-4095)

4. Press the **Enter** key. The test results display. For example:

```
C1|S13|L0D/> show soam mep test mep-id=2 local-parent-id=2
ETH-TEST status for MEP          : 2
Transmit status
  Last Transmitted Sequence Number : 4
  Transmit Request State           : Completed
  Transmitted Requests             : 4
Received status
  Last Received Sequence Number    : 0
  Missed Sequence Numbers         : 0
  Valid ETH-TEST frames received  : 0
  Invalid ETH-TEST frames received : 0
  Discarded ETH-TEST frames       : 0
```

The ETH-TEST parameters are described below:

<u>Parameter</u>	<u>Example</u>	<u>Range / Comment</u>
ETH-TEST status for MEP:	2	Transmit status number from 1 to x.
Last Transmitted Sequence Number:	4	A Transmit sequence number, 1- x.
Transmit Request State:	Completed	Completed or Incomplete.
Transmitted Requests:	4	A Transmit request number, 1- x.
Received status		
Last Received Sequence Number:	0	A number 0 to <Last Trans. Seq. No.>
Missed Sequence Numbers:	0	A number from 0 to x; a low # is good.
Valid ETH-TEST frames received:	0	The number (0 - x) of good frames rcvd.
Invalid ETH-TEST frames received:	0	The number (0 - x) of bad frames rcvd.
Discarded ETH-TEST frames:	0	The number of frames rcvd. & dumped.

Note: The CLI commands to create a MA / MEG / MEP include parameters to define SOAM parameters. These commands include:

set soam ma local-ma-id=

set soam meg local-meg-id=

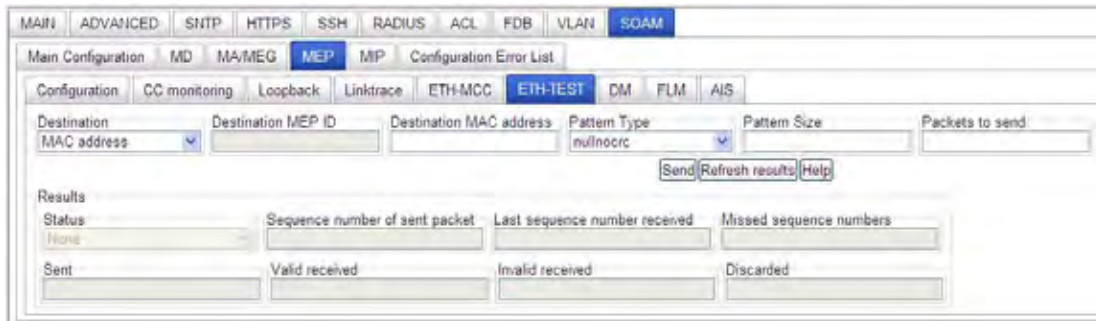
set soam mep config mep-id=

See “[Configuring SOAM MEP](#)” on page 124. For a complete list of all CLI commands for CCM operations see the *ION System CLI Reference Manual*, 33461.

ETH-TEST Config – Web Method

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP. **Note:** run one SOAM MEP test request at a time for a given MEP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab > **ETH-TEST** sub-tab.



3. In the **Destination** field, select either **MAC address** or **MEP ID**. This selects the type of target addressing. Selecting **MAC address** indicates that the unicast destination MAC address of the target MEP will be used for ETH-Test transmission. Selecting **MEP ID** indicates that the MEPID of the target MEP will be used for ETH-Test transmission.
4. In the **Destination MAC address** field, enter the target MAC Address to be transmitted to. This is the unicast destination MAC address. This address is used if **MAC address** was selected in the **Destination** field in the previous step.
5. In the **Destination MEP ID** field, enter the MEP ID of the remote MEP to which the MCC is to be sent. This address is used if **MEP ID** was selected in the **Destination** field in step 3 above. The valid range is 1- 8191.
6. In the **Pattern Type** field, select the type of pattern to be used in this ETH-TEST message, either:
 - nullnocrc** – Null pattern, with no CRC checking.
 - nullcrc** – Null pattern, with CRC checking.
 - prbsnocrc** - pseudo-random bit sequence, with no CRC checking.
 - prbscrc** - pseudo-random bit sequence, with CRC checking.
7. In the **Pattern Size** field, enter the size of the pattern, excluding the CRC. The valid range is from 1-1467.
8. In the **Packets to send** field, enter the number of ETH-TEST messages to be transmitted. The valid range is from 1-32.
9. Click the **Send** button to send an ETH-TEST message.
10. Click the **Refresh results** button. The test results are displayed. The ETH-TEST results fields are:
 - Status** - the state of the current on Test request:
 - *None* – no status to display.
 - *In Progress* – an ETH-TEST is in process.
 - *Completed* – an ETH-TEST is done.
 - *Proceed* - a new request is triggered.
 - Sequence number of sent packet** – the Last Transmitted sequence number.

Section 4: Configuration

Last sequence number received – the Last Received sequence number.

Missed sequence numbers - missed sequence numbers.

Sent – the total number of transmitted requests.

Valid received - the number of valid ETH-TEST packets received since the last Refresh.

Invalid received - the number of invalid ETH-TEST packets received since the last Refresh.

Discarded - the number of discarded ETH-TEST packets since the last Refresh.

DM (Frame Delay Measurement)

ITU-T ETH-DM can be used for on-demand OAM to measure frame delay and frame delay variation. Frame delay and frame delay variation measurements are performed by sending periodic frames with ETH-DM information to the peer MEP and receiving frames with ETH-DM information from the peer MEP during the diagnostic interval. Each MEP may perform frame delay and frame delay variation measurement.

When a MEP is enabled to generate frames with ETH-DM information, it periodically sends frames with ETH-DM information to its peer MEP in the same ME. When a MEP is enabled to generate frames with ETH-DM information, it also expects to receive frames with ETH-DM information from its peer MEP in the same ME.

Specific configuration information required by a MEP to support ETH-DM includes:

- MEG level – MEG level at which the MEP exists.
- Priority – Identifies the priority of the frames with ETH-DM information. This information is configurable per operation.
- Drop Eligibility – Frames with ETH-DM information are always marked as drop ineligible (this information is not necessarily configured).

A MIP is transparent to the frames with ETH-DM information and therefore does not require any information to support ETH-DM functionality.

A MEP transmits frames with ETH-DM information with the following information element:

- **TxTimeStamp**: Timestamp at the transmission time of ETH-DM frame.

ETH-DM can be performed in two ways:

- One-way ETH-DM
- Two-way ETH-DM

The receiving MEP can compare this value with the RxTime_f, the time at the reception of ETH-DM frame and calculate the one-way frame delay as:

$$\text{Frame delay} = \text{RxTime}_f - \text{TxTimeStamp}_f$$

However, one-way frame delay measurement requires that the clocks at the transmitting MEP and the receiving MEPs are synchronized.

The frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with ETH-DM request information with the TxTimeStamp_f, and the receiving MEP responds with a frame with ETH-DM reply information with TxTimeStamp_f copied from the ETH-DM request information. The MEP receiving the frame with ETH-DM reply information compares the TxTimeStamp_f with the RxTime_b, which is the time at the reception of frame with ETH-DM reply information and calculates the two-way frame delay as:

$$\text{Frame delay} = \text{RxTime}_b - \text{TxTimeStamp}_f$$

Section 4: Configuration

The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

To allow a more precise two-way frame delay measurement, the MEP replying to a frame with ETH-DM request information can also include two additional timestamps in the ETH-DM reply information:

- *RxTimeStampf* (timestamp at the time of receiving a frame with ETH-DM request information)
- *TxTimeStampb* (timestamp at the time of transmitting a frame with ETH-DM reply information)

Frame loss measurement commands include Periodic Loss Measurement (LM) and Frame Delay Measurement (DM) functions. Frame loss measurement is a MEP-to-MEP function. It is performed as part of Continuity Check messages. This feature is only supported for MEPs which have a VLAN type of none.

Note that Frame Loss measurements (LM or DM) can be enabled only for point-to-point MEGs (i.e., MEGs with only one peer MEP).

Note: run one SOAM MEP test request at a time for a given MEP.

ETH-DM can be configured in the system using either the CLI or Web method.

DM Config – CLI Method

Frame delay measurement and frame delay variation measurement are executed on demand for a given MEP-to-MEP pair. Note that Delay measurement can be enabled only for point-to-point MEGs (i.e., MEGs with only one peer MEP).

1. To initiate a Delay Measurement request for a specified MEP, use the **send** command.

Note: enter just one DM request at a time for a specified MEP.

Type:

```
send soam mep dm mep-id=<1-8191> local-parent-id=<1-4294967295> dest=(MAC|MEPID)
period=(1s|10s) frame-num=<3-32>
```

Where:

vv = the mep-id (the MEP ID of the MEP to initiate the delay measurement, from 1-8191)

ww = the local-parent-id (the MEG identifier, from 1-4294967295)

xx = the dest (the destination for which the delay is to be measured; either a MEPID or a MAC address)

yy = the period (the period of the delay measurement, either 1 second or 10 seconds)

zz = the frame-num (the number of frames to be transmitted periodically, from 3-32)

2. Press the **Enter** key.
3. To show the Delay Measurement results for a specified MEP, enter the **show soam mep dm status** command.

Type: **show soam mep dm status mep-id=<1-8191> local-parent-id=<1-4294967295>**

Type: **show soam mep dm status mep-id=<1-8191> local-parent-id=<1-4095>**

Where:

yy = the mep-id (the MEP ID of the MEP to display delay measurement results, from 1-8191)

zz = the local-parent-id (the MEG identifier, from 1-4095)

For example: **C1|S13|L0D/>show soam mep dm status mep-id=2 local-parent-id=2**

4. Press the **Enter** key. The DM status displays for the specified MEP. For example:

```
C1|S13|L0D/>show soam mep dm status mep-id=2 local-parent-id=2
Local MEP id                : 2
Remote MEP mac address      : 00-01-02-03-04-05
Status                      : completed
Far end processing          : Not included
Average round trip delay    : 12.500000 ms
Minimum round trip delay    : 11.100000 ms
Maximum round trip delay    : 9.200000 ms
Average far end processing  : 0.200000 ms
Minimum far end processing  : 0.100000 ms
Maximum far end processing  : 0.300000 ms
Average round trip delay variation : 0.100000 ms
Minimum round trip delay variation : 0.000000 ms
Maximum round trip delay variation : 0.200000 ms
Total DMM frames transmitted : 182
Total DMR frames received   : 172
```

The DM parameters are described below:

<u>Parameter</u>	<u>Example</u>	<u>Range / Comment</u>
Local MEP id:	2	A valid MEP ID.
Remote MEP mac address:	00-01-02-03-04-05	A valid MAC address.
Status:	completed	Completed or incomplete.
Far end processing:	Not included	Included or Not included.
Average round trip delay:	12.500000 ms	A number in ms; a low number is good.
Minimum round trip delay:	11.100000 ms	A number (x.yyy) in milliseconds.
Maximum round trip delay:	9.200000 ms	A number (x.yyy) in milliseconds.
Average far end processing:	0.200000 ms	Avg. FEP time (x.yyy) in milliseconds.
Minimum far end processing:	0.100000 ms	Min. FEP time (x.yyy) in milliseconds.
Maximum far end processing:	0.300000 ms	Max. FEP time (x.yyy) in milliseconds.
Avg. round trip delay variation:	0.100000 ms	Avg. RT Delay (x.yyy) in milliseconds.
Min. round trip delay variation:	0.000000 ms	Min. RT Delay (x.yyy) in milliseconds.
Maximum round trip delay variation:	0.200000 ms	Max. RT Delay (x.yyy) in milliseconds.
Total DMM frames transmitted:	182	Number (xxx) of Delay Measurement Message frames sent.

Section 4: Configuration

Total DMR frames received:	172	Number (xxx) of Delay Measurement Message frames received.
----------------------------	-----	--

Note: The CLI commands to create a MA / MEG / MEP include parameters to define SOAM parameters. These commands include:

set soam md local-md-id=

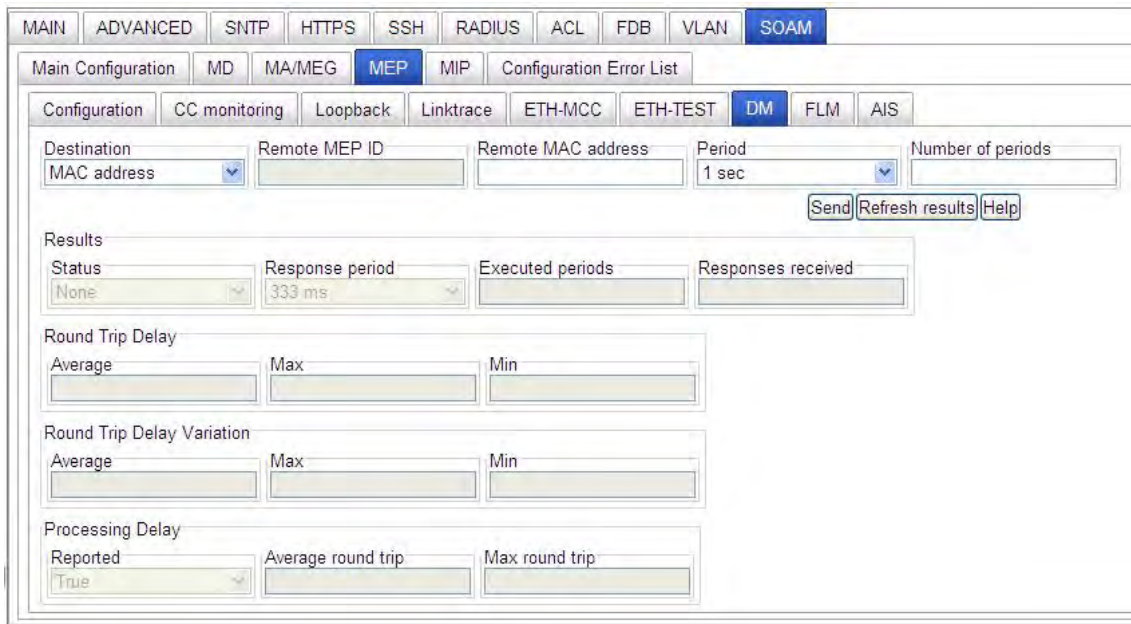
set soam mep config mep-id=

See “[Configuring SOAM MEP](#)” on page 124. For a complete list of CLI commands for all operations, see the *ION System CLI Reference Manual*, 33461.

DM Config – Web Method

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP. **Note:** run one SOAM MEP test request at a time for a given MEP.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab > **DM** sub-tab.



3. In the **Destination** field, select **MAC address** or **MEP ID**. Selecting **MEP ID** indicates that the MEP ID of the target MEP will be used for DM transmission. Selecting **MAC address** indicates that the unicast destination MAC address of the target MEP will be used for DM transmission.
4. In the **Remote MAC address** field, enter the target MAC Address to be transmitted. This is the unicast destination MAC address. This address will be used if **MAC address** was selected in step 3 above.
5. In the **Remote MEP ID** field, enter the MEP ID of the remote MEP to which the DM is to be sent. This address will be used if **MEP ID** was selected in step 3 above. The valid **MEP ID** range is 1-8191.
6. In the **Period** field, select either **1 second** or **10 seconds**. This specifies the delay between two consecutive DM messages.
7. In the **Number of Periods** field, enter the number of Periods (defined in step 6 above) to execute for this ETH-DM test. This specifies the number of periods for which the DM is being executed. The valid **Number of Periods** range is 3-32.
8. Select the MEP to test from the MEP Configuration table at **SOAM > MEP > Configuration**.
9. Click the **Send** button. The message “Loading, please wait ...” displays momentarily.

Section 4: Configuration

10. Click the **Refresh results** button. The DM results display in a table.

Results			
Status	Response period	Executed periods	Responses received
Round Trip Delay			
Average	Max	Min	
Round Trip Delay Variation			
Average	Max	Min	
Processing Delay			
Reported	Average round trip	Max round trip	

The DM test results fields are:

Status - the state of the current DM request. A new request is triggered when *Proceed* is the result.

- *None* – no status to display.
- *Initiated* – started but not yet completed.
- *In Progress* – a DM test is in process.
- *Failed* – DM test started but could not complete.
- *Completed* - DM test finished successfully.
- *Proceed* - a new request is triggered.

Response period - the expected response time for each DM message; either:

- 333 Msec (0.333 seconds)
- 3 Seconds

Executed periods – the number of transmitted DM packets within this session.

Responses received – the number of received DMR packets within this session.

Average Round Trip Delay – the average round trip delay for the session, expressed in 1/100th of a millisecond.

Max Round Trip Delay - the maximum round trip delay for the session, expressed in 1/100th of a millisecond.

Min Round Trip Delay - the minimum round trip delay for the session, expressed in 1/100th of a millisecond.

Average Round Trip Delay Variation - the average round trip delay variation for the session, expressed in 1/100th of milliseconds.

Max Round Trip Delay Variation - the maximum round trip delay variation for the session, expressed in 1/100^{ths} of a millisecond.

Min Round Trip Delay Variation - the minimum round trip delay variation for the session, expressed in 1/100^{ths} of a millisecond.

Reported - indicates if the processing delay is included in the far end report.

Average round trip - the average processing delay for the session, expressed in 1/100^{ths} of a millisecond.

Max round trip - the maximum round trip delay variation for the session, expressed in 1/100^{ths} of a millisecond.

11. Click the **Refresh** button to update the fields.

FLM (Frame Loss Measurement)

ITU-T ETH-LM is used to collect counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.

ETH-LM is performed by sending frames with ETH-LM information to a peer MEP and similarly receiving frames with ETH-LM information from the peer MEP. Each MEP performs frame loss measurements which contribute to unavailable time. Since a bidirectional service is defined as unavailable if either of the two directions is deemed unavailable, ETH-LM must facilitate each MEP to perform near-end and far-end frame loss measurements.

For a MEP, near-end frame loss refers to frame loss associated with ingress data frames, and far-end frame loss refers to frame loss associated with egress data frames. Both near-end and far-end frame loss measurements contribute to near-end severely errored seconds (near-end SES) and far-end severely errored seconds (far-end SES) respectively which together contribute to unavailable time.

A MEP maintains two local counters for each peer MEP and for each priority class being monitored in a point-to-point ME for which loss measurements are to be performed:

- TxFCI: Counter for in-profile data frames transmitted towards the peer MEP.
- RxFCI: Counter for in-profile data frames received from the peer MEP.

TxFCl and RxFCI counters do not count the OAM frames transmitted or received by the MEP at the MEP's MEG level in some conditions. However, the counters do count OAM frames from the higher MEG levels that pass through the MEPs in a manner similar to the data frames.

The method of loss measurement involving pairs of consecutive frames with ETH-LM information alleviates lack of synchronization across the initial counter values at the transmitting and receiving MEPs. Further, when a MEP detects a loss-of-continuity defect condition, it ignores loss measurements during the defect condition and assumes 100% losses.

Specific configuration information required by a MEP to support ETH-LM includes:

- MEG level – MEG level at which the MEP exists.
- ETH-LM transmission period – Default transmission period is 100 ms (i.e., a transmission rate of 10 frames/second).
- Priority – Identifies the priority of the frames with ETH-LM information (this information is configurable per operation).
- Drop Eligibility – Frames with ETH-LM information are always marked as drop ineligible (this information is not necessarily configured).

A MIP is transparent to frames with ETH-LM information and therefore does not require any information to support ETH-LM functionality.

ETH-LM can be performed in two ways: a) Dual-ended ETH-LM, or b) Single-ended ETH-LM.

Note: run just one SOAM MEP test request at a time for a given MEP.

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

LM (Periodic Loss Measurement) Config – CLI Method

Frame loss measurement commands include Periodic Loss Measurement (LM) and Frame Delay Measurement (DM) functions. Frame loss measurement is a MEP-to-MEP function. Frame loss measurement is performed as part of Continuity Check messages. This feature is only supported for MEPs which have a VLAN Type of **none**.

Note that Frame Loss measurements (LM or DM) can be enabled only for point-to-point MEGs (i.e., MEGs with only one peer MEP).

LM Config – CLI Method

1. To initiate a Periodic Loss Measurement request for a specified MEP, use the command **send soam mep dm mep-id**. This configures the periodic loss measurement for a given MEP with a VLAN type of **none**. Note that the periodic LM function cannot be enabled on a MEP which has the CC function (Continuity Checks Monitoring) disabled.

Type: **set soam mep lmpersistent mep-id=<xx> local-parent-id=<yy> state=(zz)**

Where:

xx = the mep-id (the MEPid of the MEP to initiate the loss measurement, from 1-8191)

yy = the local-parent-id (the MEG identifier, from 1-4095)

zz = the state (the status of the periodic loss measurement; either **enable**, **disable**, or **clear counters**). Selecting **clear counters** resets the accumulated results for a port, and can be applied only if the LM periodic mode is enabled.

For example: **C1|S13|L0D/> set soam mep lmpersistent mep-id=2 local-parent-id=2 state=enable**

2. Press the **Enter** key.
3. To display Periodic Loss Measurement information for a specified MEP, use the command **show soam mep lmpersistent mep-id**.

Type:

show soam mep lmpersistent mep-id=<1-8191> local-parent-id=<1-4095> far-end-mep-id=<1-8191>

Where:

xx = the mep-id (the MEP ID of the MEP to display the periodic loss measurement results, from 1-8191)

yy = the local-parent-id (the MEG identifier, from 1-4095)

zz = the far-end-mep-id (the remote MEP ID, from 1-8191)

Section 4: Configuration

4. Press the **Enter** key. The Periodic Loss Measurement information for the specified MEP displays. For example:

```
C1|S13|L0D/>show soam mep lperiodic mep-id=2 local-parent-id=2 far-
end-mep-id=1

Local MEP id           : 2
Periodic LM            : enabled
Remote MEP id          : 1
Statistics state        : Valid
Near end frame loss     : 0
Far end frame loss     : 0
Near end frame loss ratio : 100%
Far end frame loss ratio : 100%
```

The periodic LM parameters are described below:

<u>Parameter</u>	<u>Example</u>	<u>Range / Comment</u>
Local MEP id:	2	A valid MEP ID
Periodic LM:	enabled	Enabled or disabled
Remote MEP id:	1	A valid MEP ID
Statistics state:	Valid	Valid or Invalid; if Invalid, retry operation.
Near end frame loss:	0	A reported number; a low number is good.
Far end frame loss:	0	A reported number; a low number is good.
Near end frame loss ratio:	100%	A reported FLR; a high number is good.
Far end frame loss ratio:	100%	A reported FLR; a high number is good.

These LM results are described below.

Far end frame loss – the number of frames lost at the far end.

Far end frame loss ratio – the Frame loss ratio at the far end, in 1/100th of a percent (0.01%). A value of 100 means a 1% far end frame loss.

Near end frame loss – the number of frames lost at the near end.

Near end frame loss ratio – the Frame loss ratio at the near end, in 1/100th of a percent (0.01%) increments. A value of 100 means a 1% near end frame loss.

Note: The SOAM CLI commands to configure LM are:

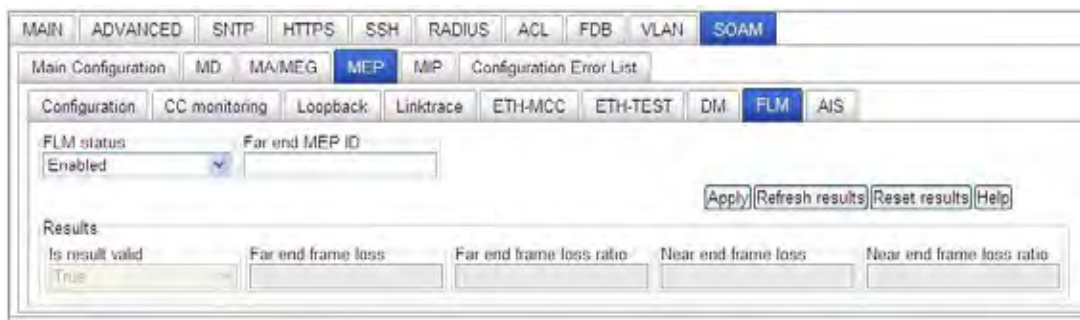
```
set soam mep lperiodic mep-id=<1-8191> local-parent-id=<1-4294967295> state=(enable|disable|clearcounters)
show soam mep lperiodic mep-id=<1-8191> local-parent-id=<1-4294967295> far-end-mep-id=<1-8191>
```

See “[Configuring SOAM MEP](#)” on page 124. For a complete list of CLI commands for all operations, see the *ION System CLI Reference Manual*, 33461.

FLM Config – Web Method

Note: You must have already defined either an MD/MA combination or a MEG, and then defined a MEP.

1. Access the NID via the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab > **FLM** sub-tab.



3. In the **FLM status** field, select **Enabled**. This selection enables or disables periodic FLM (frame loss measurement) processes.
4. In the **Far end MEP ID** field, enter the MEP ID for the far end MEP for each the periodic FLM is being enabled. The valid range is 1-8191.
5. Click the **Apply** button. The message “Loading, please wait ...” displays momentarily.
6. When the message “Getting values finished” displays, select the **Refresh results** button. The Results table displays the FLM test results. For example:

Results				
Is result valid	Far end frame loss	Far end frame loss ratio	Near end frame loss	Near end frame loss ratio
True	0	100	0	100

The **Results** table fields are described below.

Is result valid – displays *True* if FLM test results displayed are valid. Displays *False* if FLM test results displayed are invalid. This result specifies if the **values** read in the following counters are valid.

Far end frame loss – the number of frames lost at the far end.

Far end frame loss ratio – the Frame loss ratio at the far end, in 1/100th of a percent (0.01%). A value of 100 means a 1% far end frame loss.

Near end frame loss – the number of frames lost at the near end.

Near end frame loss ratio – the Frame loss ratio at the near end, in 1/100th of a percent (0.01%) increments. A value of 100 means a 1% near end frame loss.

7. Click the **Refresh results** button to display new FLM Test results.
8. Click the **Reset results** button to reset (zero out) the displayed FLM Test results.

Ethernet Alarm Indication Signal (AIS)

ETH-AIS allows alarm suppression when defects to be detected at the server layer. You can enable or disable frames transmission with ETH-AIS information on an MEP or on a server MEP. You can also issue frames with ETH-AIS information at the client maintenance level by a MEP, including a server MEP, on detecting defect conditions. Defect conditions can include signal fail conditions with ETH-CC enabled, and AIS condition with ETH-CC disabled.

Only a MEP or Server MEP is configured to issue frames with ETH-AIS information. When a MEP detects a defect condition, it immediately starts transmitting periodic frames with ETH-AIS information at a configured client maintenance level. The MEP continues to transmit periodic frames with ETH-AIS information until the defect condition is resolved. On receiving a frame with ETH-AIS information, a MEP detects the AIS condition and suppresses loss of continuity alarms with all of its peer MEPs. The MEP resumes loss of continuity alarm generation on detecting loss of continuity conditions in place of the AIS condition.

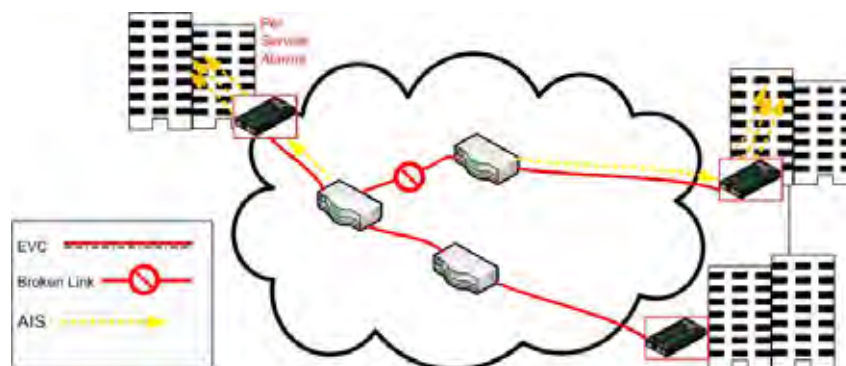


Figure 26: Alarm Indication Signal (AIS)

Transmission of frames with ETH-AIS information can be enabled or disabled on a MEP (or on a server MEP). Frames with ETH-AIS information can be issued at the client MEG level by a MEP, including a server MEP, upon detecting defect conditions.

Defect conditions may include:

- Signal fail conditions when ETH-CC is enabled, or
- AIS condition or LCK condition if ETH-CC is disabled.

The configuration information required by a MEP to support ETH-AIS transmission includes:

- Client MEG level – MEG level at which the most immediate client layer MIPs and MEPs exist.
- ETH-AIS transmission period – Determines transmission periodicity of frames with ETH-AIS information.
- Priority – Identifies the priority of frames with ETH-AIS information.
- Drop Eligibility – Frames with ETH-AIS information are always marked as drop ineligible (this information is not necessarily configured).

The configuration information required by a MEP to support ETH-AIS reception includes:

- Local MEG level – MEG level at which the MEP operates.

A MIP is transparent to frames with ETH-AIS information and therefore does not require any information to support ETH-AIS functionality.

Upon detecting a defect condition, a MEP can transmit AIS frames in a direction opposite to its peer MEP(s). The periodicity of AIS frames transmission is based on the AIS transmission period. An AIS transmission period of 1 second is typical; an AIS transmission period of 1 minute is also supported. The first AIS frame must always be transmitted immediately following the detection of a defect condition.

On receiving an AIS frame, the MEP tries to detect an AIS defect condition. If an AIS defect condition is detected, if no AIS frames are received within an interval of 3.5 times the AIS transmission period indicated in the AIS frames received before, the MEP clears the AIS defect condition.

Note: run one SOAM MEP test request at a time for a given MEP.

ETH-AIS can be configured in the system using either the CLI or Web method.

ETH-AIS Config – CLI Method

AIS statistics are available as a part of “**show soam mep stats**” command; there are no trap results, just counters. The AIS configuration is set by ‘**set soam mep**’ and ‘**set soam mip**’ commands.

1. To display MEP statistics for a specified MEP, use the command **send soam mep dm mep-id**. Type: **show soam mep stats [mep-id=<xx> local-parent-id=<yy>]**

where:

xx = optional; MEP identifier (1–8191). If omitted, the statistics of all configured MEPs is displayed.

yy = conditional; ID of the local MA or MEG to be associated with the MEP. This parameter must be specified if mep-id= is entered.

2. Press **Enter**. The AIS statistics of the specified SOAM MEP display.

Section 4: Configuration

Example:

```
C1|S3|L1D>show soam mep stats
MEP id : 320
CCMs sent : 80232
CCMs with RDI bit sent : 80229
CCMs received : 0
CCMs discarded due to SenderID TLV invalid : 0
CCMs discarded due to Port Status TLV invalid : 0
CCMs discarded due to Interface Status TLV invalid : 0
CCMs with sequence errors received : 0
CCMs with RDI bit received : 0
In order LBRs received : 0
Out of order LBRs received : 0
LBRs with bad msdu received : 0
LBRs sent : 0
LTMs received : 0
LTRs received : 0
LTRs sent : 0
LTRs with bad dest MAC discarded : 0
AIS frames transmitted : 0
AIS frames received : 0
AIS sent true up notifications : 0
AIS sent false up notifications : 0
AIS received true up notifications : 0
AIS received false up notifications : 0
```

Note: The SOAM CLI commands to configure ETH-AIS are:

```
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|1s|1min|...)
```

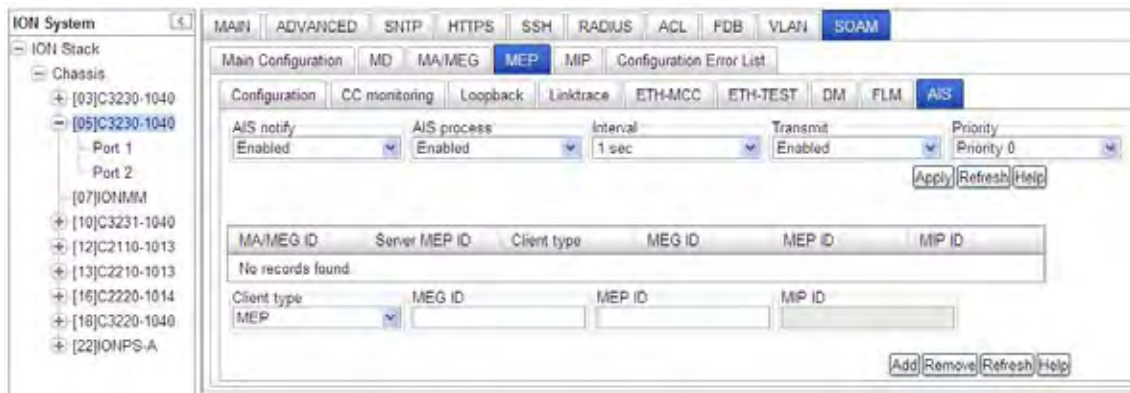
```
set soam mip local-mip-id=<1-4294967295> attr-name=(admin|aistransmit|aisinterval|aisframepriority) attr-
val=(enable|disable|1s|1min|...)
```

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

ETH-AIS Config – Web Method

Note: You must have previously defined either an MD/MA combination or a MEG, and then defined a MEP. **Note:** run one SOAM MEP test request at a time for a given MEP.

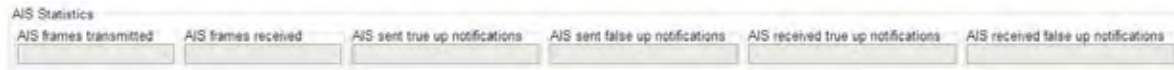
1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **SOAM** tab > **MEP** sub-tab > **AIS** sub-tab.



3. In the **AIS notify** field, select **Enabled**. This selection enables or disables defect notifications to upper layers for AIS transmission.
4. In the **AIS process** field, select **Enabled**. This selection enables or disables AIS frames processing.
5. In the **Interval** field, select either **1 second** or **1 minute** as the AIS transmission interval.
6. In the **Transmit** field, select **Enabled**. This selection enables or disables transmission of AIS frames.
7. In the **Priority** field, select Priority 0 - Priority 7, where Priority 7 is the highest and Priority 0 is the lowest. This selection sets the priority value for AIS frames transmitted by the MEP.
8. Click the **Apply** button.
9. In the **Client type** field, specify if the client is a **MEP** or a **MIP**.
10. If **MEP** was selected in step 9, in the **MEG ID** field, enter an **MA Index** for an IEEE 802.1ag MEP client or a **MEG index** for an ITU-T Y.1731 MEP. The valid range of entries is 1-4294967295.
11. If **MEP** was selected in step 9, in the **MEP ID** field, enter a MEP index for an IEEE 802.1ag or ITU-T Y.1731 MEP client.
12. If **MIP** was selected in step 9, in the **MIP ID** field, enter a local MIP ID for a MIP client. The valid range of entries is 1 – 4294967295.

Section 4: Configuration

13. Click the **Add** button.
14. Click the **Apply** button. The AIS statistics table displays. The AIS statistics table fields are **MA/MEG ID**, **Server MEP ID**, **Client type**, **MEG ID**, **MEP ID**, and **MIP ID**, as specified in steps 9-12 above.
15. Select **SOAM > MEP > Configuration** to examine the AIS statistics.



16. The AIS statistics fields are:

AIS frames transmitted – the number of AIS frames transmitted by the MEP.

AIS frames received – the number of AIS frames received by the MEP.

AIS sent true up notifications – the number of AIS true up notifications sent.

AIS sent false up notifications – the number of AIS false up notifications sent.

AIS received true up notifications – the number of AIS true up notifications received.

AIS received false up notifications – the number of AIS false up notifications received.

17. To delete an entry, click (highlight) a table entry and click the **Remove** button.
18. To refresh (clear) the table entries click the **Refresh results** button.

Ethernet Remote Defect Indication (RDI)

The IEEE Remote Defect Indication (RDI) is a single bit carried by the CCM. The absence of RDI in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.

A MEP can use ITU-T ETH-RDI to notify its peer MEPs that it detects a defect condition. ETH-RDI is used only if ETH-CC transmission is enabled. ETH-RDI is used in single-ended fault management and in contributing to far-end performance monitoring. A MEP in a defect condition transmits frames with ETH-RDI information. When a MEP receives frames with ETH-RDI information it determines that its peer MEP has encountered a defect condition

ETH-RDI has these two applications:

- Single-ended fault management: The receiving MEP detects an RDI defect condition, which gets correlated with other defect conditions in this MEP and may become a fault cause. The absence of received ETH-RDI information in a single MEP indicates the absence of defects in the entire MEG.
- Contribution to far-end performance monitoring: It reflects that there was a defect condition in the far-end which is used as an input to the performance monitoring process.

A MEP that is in a defect condition transmits frames with ETH-RDI information. A MEP, on receiving frames with ETH-RDI information, determines that its peer MEP has encountered a defect condition.

Specific configuration information required by a MEP to support ETH-RDI function includes:

- MEG level – MEG level at which the MEP exists.
- ETH-RDI transmission period – Application-dependent and is configured to be the same as ETH-CC transmission period.
- Priority – Identifies the priority of frames with ETH-RDI information. The priority is the same as ETH-CC priority.
- Drop Eligibility – Frames with ETH-RDI information are always marked as drop ineligible (this information is not necessarily configured).

A MIP is transparent to frames with ETH-RDI information and therefore does not require any configuration information to support ETH-RDI functionality. The PDU used to carry ETH-RDI information is CCM.

A MEP, on detecting a defect condition with its peer MEP, sets the RDI field in the CCM frames for the duration of the defect condition. CCM frames are transmitted periodically based on the CCM transmission period when the MEP is enabled for CCM frames transmission. When the defect condition clears, the MEP clears the RDI field in the CCM frames in subsequent transmissions.

Section 4: Configuration

On receiving a CCM frame, a MEP examines it to ensure that its MEG level corresponds to its configured MEG level, and detects RDI condition if the RDI field is set. For a point-to-point ETH connection, a MEP can clear the RDI condition when it receives the first CCM frame from its peer MEP with the RDI field cleared. For multipoint ETH connectivity, a MEP can clear the RDI condition when it receives the CCM frames from its entire list of peer MEPs with the RDI field cleared.

RDI is an error condition and is reflected by the MEP status. The RDI configuration is set by 'set soam mep' and 'set soam mip' commands.

1. To show MEP statistics for a specified MEP, use the command **send soam mep dm mep-id**.

Type: **show soam mep stats [mep-id=<xx> local-parent-id=<yy>]**

where:

xx = optional; MEP identifier (1–8191). If omitted, the statistics of all configured MEPs is displayed.

yy = conditional; ID of the local MA or MEG to be associated with the MEP. This parameter must be specified if mep-id= is entered.

2. Press **Enter**. The statistics of a MEP of the SOAM engine display:

```
C1|S3|L1D> C1|S13|L0D/>show soam mep stats
MEP id                               : 320
CCMs sent                             : 80232
CCMs with RDI bit sent                 : 80229
CCMs received                         : 0
CCMs discarded due to SenderID TLV invalid : 0
CCMs discarded due to Port Status TLV invalid : 0
CCMs discarded due to Interface Status TLV invalid : 0
CCMs with sequence errors received    : 0
CCMs with RDI bit received            : 0
```

The RDI parameters returned are:

CcmRdiSent: The total number of sent CCMs with RDI bit set (e.g., 80229 in the example above). This number will be equal to or less than the total number of sent CCMs (e.g., 80232 in the example above).

CcmRdiReceived: The total number of CCMs with RDI bit set received from all remote MEPs. This number will be equal to or less than the number of sent CCMs with RDI bit set (e.g., 0 in the example above).

SOAM MEP Test Summary

The SOAM MEP tests used for checking connectivity between MEPs are summarized below in terms of the Web interface tabs and the CLI **send** and **show** commands used.

Web I/F Test	Send command	Show command
1. CC Monitoring (Continuity Check Monitoring)	set soam mep config	show soam mep cc show soam mep config show soam mep stats
2. Loopback (LB)	send soam mep loopback	show soam mep loopback
3. Linktrace (LTR)	send soam mep linktrace	show soam mep linktrace
4. ETH-MCC	send soam mep mcc	show soam mep stats
5. ETH-TEST	send soam mep test	show soam mep test
6. DM (Frame Delay Measurement)	send soam mep dm	show soam mep dm status
7. FLM (Frame Loss Measurement) and LM (Periodic Loss Measurement)	set soam mep lmp	show soam mep lmp
8. AIS (Ethernet Alarm Indication Signal)	set soam mep and set soam mip	show soam mep stats
* 9. RDI (Remote Defect Indication) – no web interface tab	(an error state; no command needed to configure RDI)	(an error state; no command needed to configure RDI)

SOAM Terminology Differences between IEEE, ITU-T, and MEF

The SOAM standards are similar, with minor differences, in the terminology used for the concepts of maintenance association, maintenance entity group, maintenance identifier, maintenance domain, etc.

IEEE 802.1ag	ITU-T Y.1731	MEF 20
MA	MEG	MEG
MAID	MEG ID	MAID
MD Level	MEG Level	MEG Level

Configuring Selective and Transparent Link Pass Through

Selective and Transparent Link Pass Through are troubleshooting features that allow the NID to monitor both the fiber and copper RX ports for loss of signal. In the event of a loss of RX signal on one media port, the NID will automatically disable the TX signal of the other media port, thus passing through the link loss. Note that both TLPT and SLPT can be enabled at the same time, and both can be operational together.

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

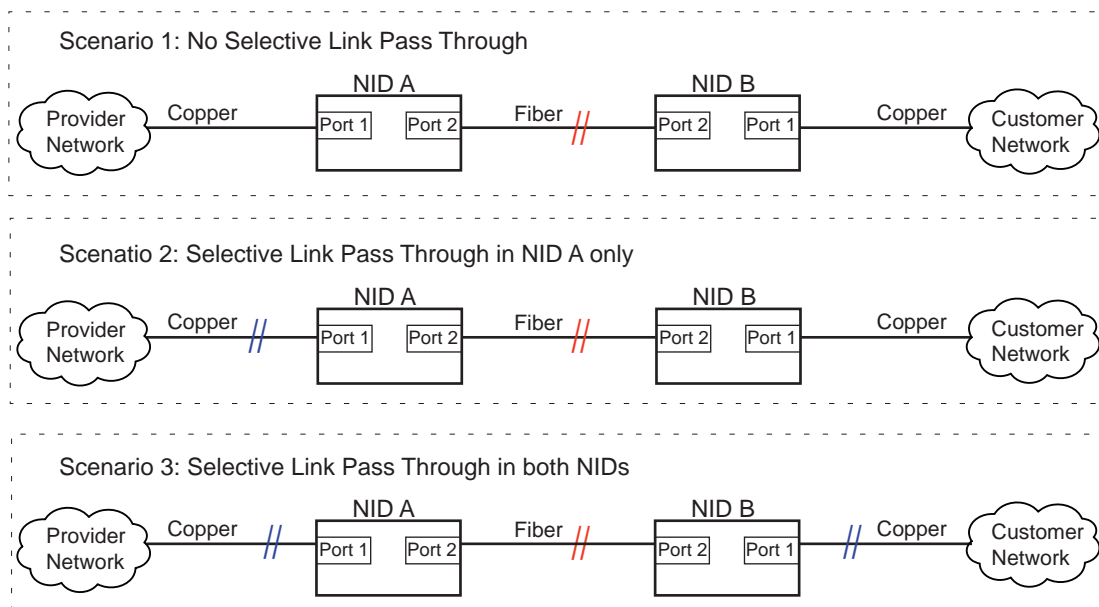


Figure 27: Selective Link Pass Through (SLPT)

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

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

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

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

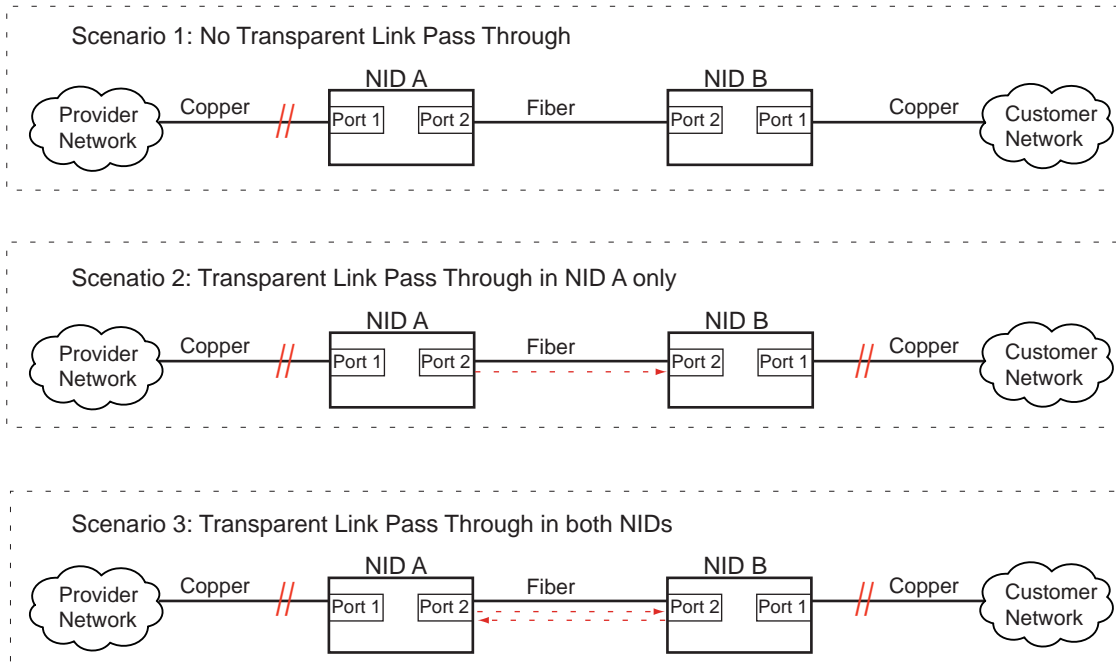


Figure 28: Transparent Link Pass Through (TLPT)

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

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

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

Link Pass Through Config – CLI Method

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

3. Define the port to be monitored. Type:

set lpt monitor-port=<xx>

where:

xx = the port to be monitored. **Note:** this should always be the port that the fiber cable is connected to.

4. Was Transparent Link Pass Through enabled?

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

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

go l<x>p=<y>

where:

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

y = the port number. **Note:** it is recommended that this be the port that the fiber cable is connected to.

6. Check whether LOAM is enabled and active. Type: **show loam config** and press **Enter**.

7. Is the LOAM admin state enabled?

Yes	No
------------	-----------

Continue with step 8 .	a) Type: set loam admin state=enable b) Press Enter . c) Continue with step 8 .
--	---

8. Is the LOAM mode active?

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

9. Verify the configuration has been set.

- a) Type: **show loam config**
- b) Press **Enter**.
- c) Go to the device level.
- d) Type: **show lpt config**
- d) Press **Enter**. Examples of related LOAM and LPT commands and displays are shown below:

```

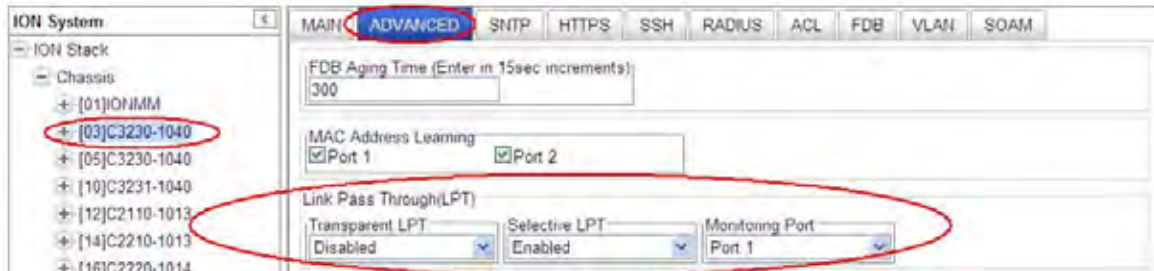
C1|S3|L1D>set selective lpt state=enable
C1|S3|L1D>set transparent lpt state=enable
C1|S3|L1D>set lpt monitor-port=2
C1|S3|L1D>go llp=2
C1|S3|L1P2>show loam config
Link OAM configuration:
-----
Link OAM admin state:          enable
Link link OAM operation status:linkFault
Link OAM mode:                 active
Link OAM maxium PDU size:     1500
Link OAM configuration revision:0
Link OAM function supported:  loopbackSupport+eventSupport
C1|S3|L1D>go llp=2
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

```

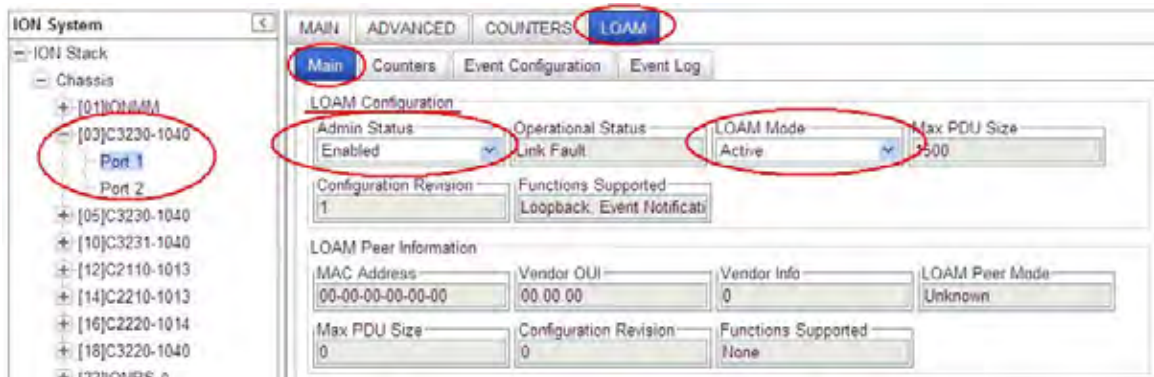
Section 4: Configuration

Link Pass Through Config – Web Method

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



3. In the **Transparent LPT** field, select **Enabled**.
4. In the **Selective LPT** field, select **Enabled**.
5. In the **Monitoring Port** field, select the port to be monitored. **Note:** it is recommended that this be the port that the fiber cable is connected to.
6. Click **Save**.
7. In the ION Stack tree, select the port that was set as the monitoring port (Port 1 in this example).



8. Select the **LOAM** tab, select the **Main** sub-tab, and locate the **LOAM Configuration** section.
9. Is **Admin Status** set to **Enabled**?

Yes	No
Go to step 10 below.	<ol style="list-style-type: none"> a) Set the Admin Status field to Enabled. b) Click Save.

	c) Go to step 10 below.
--	-------------------------

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

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

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

Configure Forwarding Learning (FDB) Aging Time

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

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

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

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

While the x323x can learn up to 8192 entries, there is a limit of 1000 entries that it can manage via the Web/CLI/FP interfaces. So even if the NID learns more than 1000 entries, only 1000 entries (including static entries) can be displayed/managed through the x323x interface (as limited by x323x memory space and CPU capability).

Forwarding Learning (FDB) Aging Time Config – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).

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

where:

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

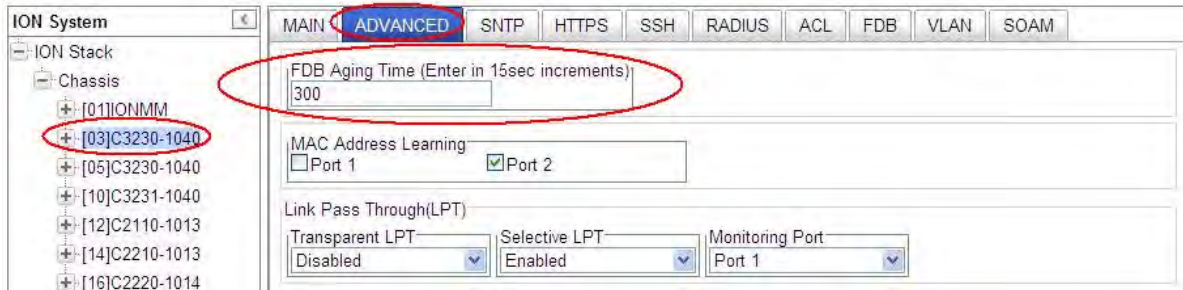
3. Press **Enter**. The dot1 bridge aging time is set.
4. Verify the dot1 bridge aging time setting. Type **show dot1bridge aging-time** and press **Enter**. The current dot1 bridge aging time setting is displayed. For example:

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

FDB Aging Time Config – Web Method

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

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



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

Configuring SNTP

IMPORTANT

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

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

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

The x323x supports only client implementations of SNTP. You can use the client implementation of SNTP to synchronize the clock on the x323x with up to six SNTP servers.

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

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

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

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

SNTP Config – CLI Method

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

2. Enable SNTP. Type:

```
set sntp state=enable
```

3. Press **Enter**.

4. Set the current time. Type:

```
set curr-time=<“xx”>
```

where:

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

5. Press **Enter**.

6. Set your timezone. Type:

```
set sntp timezone=<xx>
```

where:

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

Table 17: 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

Section 4: Configuration

10	(GMT -06:00) Saskatchewan
11	(GMT -05:00) Bogota, Lima, Quito
12	(GMT -05:00) Eastern, Time, US, and, Canada
13	(GMT -05:00) Indiana, East
14	(GMT -04:00) Atlantic, Time, Canada
15	(GMT -04:00) Caracas, La, Paz
16	(GMT -04:00) Santiago
17	(GMT -03:30) Newfoundland
18	(GMT -03:00) Brasilia
19	(GMT -03:00) Buenos, Aires, Georgetown
20	(GMT -02:00) Mid-Atlantic
21	(GMT -01:00) Azores, Cape, Verde, Is
22	(GMT) Casablanca, Monrovia
23	(GMT) Greenwich, Mean, Time, Dublin, Edinburgh, Lisbon, London
24	(GMT +01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
25	(GMT +01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
26	(GMT +01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius
27	(GMT +01:00) Sarajevo, Skopje, Sofija, Warsaw, Zagreb
28	(GMT +02:00) Athens, Istanbul, Minsk
29	(GMT +02:00) Bucharest
30	(GMT +02:00) Cairo
31	(GMT +02:00) Harare, Pretoria
32	(GMT +02:00) Helsinki, Riga, Tallinn
33	(GMT +02:00) Jerusalem
34	(GMT +03:00) Baghdad, Kuwait, Riyadh
35	(GMT +03:00) Moscow, St, Petersburg, Volgograd
36	(GMT +03:00) Nairobi
37	(GMT +03:30) Tehran
38	(GMT +04:00) Abu, Dhabi, Muscat
39	(GMT +04:00) Baku, Tbilisi

40	(GMT +04:30) Kabul
41	(GMT +05:00) Ekaterinburg
42	(GMT +05:00) Islamabad, Karachi, Tashkent
43	(GMT +05:30) Bombay, Calcutta, Madras, New, Delhi
44	(GMT +06:00) Astana, Almaty, Dhaka
45	(GMT +06:00) Colombo
46	(GMT +07:00) Bangkok, Hanoi, Jakarta
47	(GMT +08:00) Beijing, Chongqing, Hong, Kong, Urumqi
48	(GMT +08:00) Perth
49	(GMT +08:00) Singapore
50	(GMT +08:00) Taipei
51	(GMT +09:00) Osaka, Sapporo, Tokyo
52	(GMT +09:00) Seoul
53	(GMT +09:00) Yakutsk
54	(GMT +09:30) Adelaide
55	(GMT +09:30) Darwin
56	(GMT +10:00) Brisbane
57	(GMT +10:00) Canberra, Melbourne, Sydney
58	(GMT +10:00) Guam, Port, Moresby
59	(GMT +10:00) Hobart
60	(GMT +10:00) Vladivostok
61	(GMT +11:00) Magadan, Solomon, Is, New, Caledonia
62	(GMT +12:00) Auckland, Wllington
63	(GMT +12:00) Fiji, Kamchatka, Marshall, Islands

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

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

Section 4: Configuration

8. Enable DST. Type:

```
set sntp dst-state=enable
```

9. Press **Enter**.

10. Set the date and time that DST is to start. Type:

```
set sntp dst-start=<"xx">
```

where:

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

11. Press **Enter**.

12. Set the date and time that DST is to end. Type:

```
set sntp dst-end=<"xx">
```

where:

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

13. Press **Enter**.

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

```
set sntp dst-offset=<xx>
```

where:

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

15. Press **Enter**.

16. Define the IP address of the SNTP server. Type:

```
set sntp-svr svr=<xx> type=<yy> addr=<zz>
```

where:

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

yy = IP address format; valid choices are:

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

zz = IP address of the server

17. Press **Enter**.

18. Verify the configuration has been set. Type:

show sntp config

19. Press **Enter**. The SNTP Configuration displays:

```

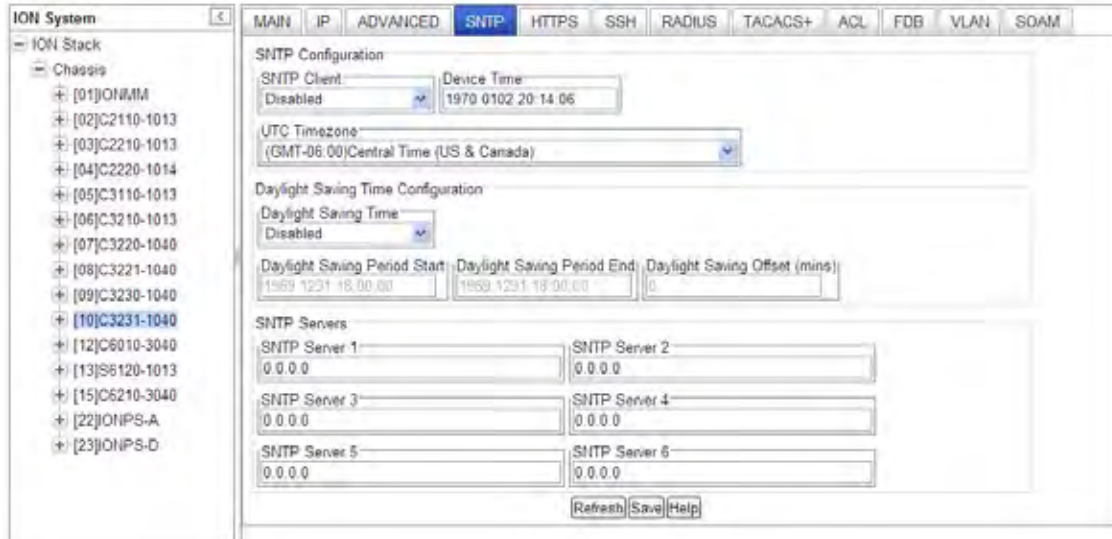
C1|S3|L1D>set sntp state=enable
C1|S3|L1D>set curr-time="20100106 13:15:30"
C1|S3|L1D>set sntp timezone=8
C1|S3|L1D>set sntp dst-state=enable
C1|S3|L1D>set sntp dst-start="20100307 02:00:00"
C1|S3|L1D>set sntp dst-end="20101107 02:00:00"
C1|S3|L1D>set sntp dst-offset=60
C1|S3|L1D>set sntp-svr svr=1 type=ipv4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

Sntp server:
index          addr-type          address
-----
1              ipv4                192.168.1.30
2              dns                 0.0.0.0
3              dns                 0.0.0.0
4              dns                 0.0.0.0
5              dns                 0.0.0.0
6              dns                 0.0.0.0

```

SNTP Config – Web Method

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



3. In the **SNTP Client** field select **Enabled**.
4. In the **Device Time** field, enter the current time in the format `yyymmdd hh:mm:ss`.
5. In the **UTC Timezone** field, select your timezone.
6. If you want to set daylight savings time (DST), continue with step 7 below.
If you do not want to set daylight savings time (DST), continue with step 11 below.
7. In the **Daylight Saving Time** field select **Enabled**.
8. In the **Daylight Saving Period Start** field, enter the DST start date and time in the format `yyymmdd hh:mm:ss`.
9. In the **Daylight Saving Period End** field, enter the DST end date and time in the format `yyymmdd hh:mm:ss`.
10. In the **Daylight Saving Offset (mins)** field, enter the DST offset in minutes (1–720). This is usually set to 60 minutes. When SNTP Client and DST are Enabled and current time at Daylight Saving Period, the current time of the switch will be offset by the entry here
11. Enter the IP address of each SNTP Server - the IPv4 or IPv6 address of one or more DNS servers.
12. Click the **Save** button when done.

Configuring System Login Users

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

Table 18: User Level Rights via Web / CLI

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

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

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

Note Regarding SNMPv3 Users vs. Web/CLI Login Users

Note: do not confuse SNMPv3 users with the Web/CLI login users. SNMPv3 user configuration has nothing to do with the WEB/CLI login users. These two type users are different and have different functionalities. The SNMPv3 users are used for SNMPv3 access (for example MGSoft). The Web/CLI login users are used for Web/CLI login when users try to use the ION Web interface or CLI to access the ION system. SNMPv3 users can not use their SNMP login credentials to log in to the ION Web/CLI (and vice-versa). See “[Configuring SNMP Users](#)” on page 104 for information on configuring Web/CLI login users.

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

Configuring System Login Users - CLI Method

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

1. Access the x323x via either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).

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

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

where:

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

level = <**administrator**, **read-write**, or **read-only**>

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

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

4. Press the **Enter** key.

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

where:

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

level = the user’s new access level; either **administrator**, **read-write**, or **read-only**.

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

where:

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

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

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

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

For example:

```

S3230-1040 C0|S0|L1D>show sysuser
name                level                password
ION                 admin                *****
S3230-1040 C0|S0|L1D>add sysuser name AndersonT level read-only pass ***** confirmpass
*****
S3230-1040 C0|S0|L1D>add sysuser name BensonJ level read-only pass ***** confirmpass
*****
S3230-1040 C0|S0|L1D>add sysuser name CarlsonAnn level read-only pass ***** confirmpass
*****
S3230-1040 C0|S0|L1D>add sysuser name CarlsonAndy level read-only pass ***** confirmpass
*****
S3230-1040 C0|S0|L1D>add sysuser name Fitz level read-only pass ***** confirmpass
*****

S3230-1040 C0|S0|L1D>show sysuser
name                level                password
ION                 admin                *****
ion                 admin                *****
AndersonT           read-only            *****
BensonJ             read-only            *****
CarlsonAnn          read-only            *****
CarlsonAndy         read-only            *****
Fitz                read-only            *****
S3230-1040 C0|S0|L1D>

```

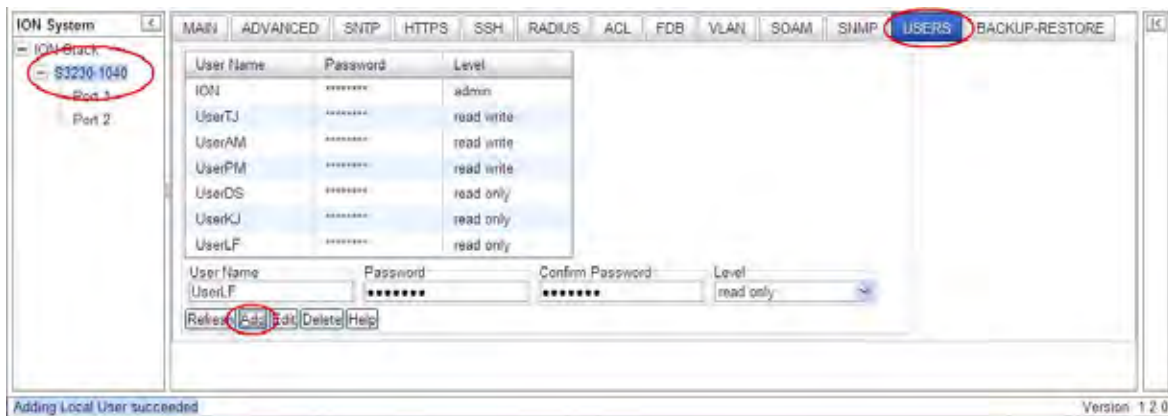
8. Backup the configuration. See “[Backup and Restore Operations \(Provisioning\)](#)” on page 161.

Configuring System / Login Users - Web Method

1. Access the x through the Web interface (see “Starting the Web Interface” on page 45).
2. At the **USERS** tab, locate the Users table.



3. In the **User Name** field, enter this user’s name (1-64 alphanumeric characters with no spaces between characters).
4. In the **Password** field, enter this user’s password.
5. In the **Confirm Password** field, re-enter the password as entered in step 4. If the two password entries do not match, the message *”ERROR: The two passwords are not the same, please check!”* displays and you must enter matching passwords.
6. At the **Level** dropdown, select this user’s access level (**admin**, **read write**, or **read only**).
7. Click the **Add** button. The new user is added to the User s table.



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

Changes to Existing ION Applications with IPv4 / IPv6

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

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

Dynamic Table Entry Limits

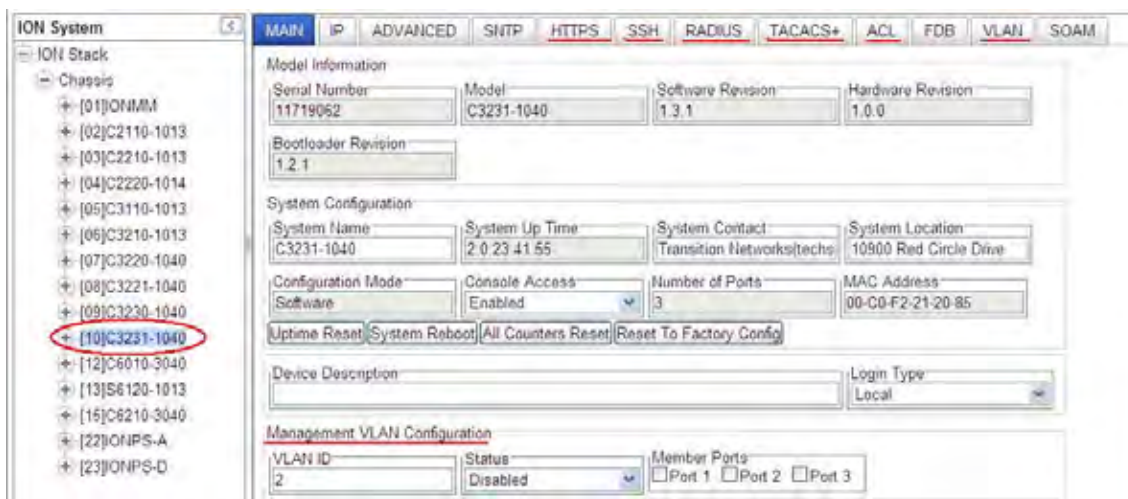
These IPv6 changes bring the entry limitations for several dynamic tables shown below.

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

Configuring Security Features

One or more of the following can be defined for the x323x NID:

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



Configuring these features is discussed in the following sections.

Configuring an ACL

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

IMPORTANT

- If the NID is managed by the ION Management Module (IONMM), configuring ACL should be done at the IONMM and not at the NID.
- An ACL does not control access to the NID through a serial interface (USB connection).
- The ION system supports the configuration of the INPUT chain of the filter table of Linux iptables; all rules being added belong to the INPUT chain of the filter table.
- At least one condition is needed for a rule before the rule can work. After you create a rule, you also need to create at least one condition for it.
- Multiple conditions can be assigned to one rule; only when all conditions of the rule are matched for an input packet, the policy of the rule can be applied to it.
- If multiple rules are matched to an input packet, the rule with the highest priority will be applied.
- You can add/modify/delete a rule or a condition whether the ACL is enabled or disabled.
- Since only the configuration for INPUT chain of the filter table is supported, there is no option to select the table-type and chain-type. They are fixed values: table is filter and chain is INPUT. This table and chain meets most, if not all, ACL functionality requirements.
- The x323x NIDs do not support two ACL conditions with the same condition type.

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

A chain is a table that contains a set of rules, usually for a particular function, such as input or output. The chain also defines a default policy that will be used if a policy is not determined by the end of processing for all rules. The only chain that can be specified for the x323x NID is INPUT. This chain contains the rules and conditions for accessing the NID through an Ethernet connection (via Telnet session or Web interface).

The rules of an ACL define the policy to be followed for certain defined conditions. There are three different policies (rules) that can be defined for the x323x NID:

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

Section 4: Configuration

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.

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

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

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

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

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

For IPv6:

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

For IPv4:

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

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

ACL Config (IPv4) – CLI Method

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

1. Access the IONMM through either a USB connection (see “Starting a USB Session” on page 23) or a Telnet session (see “Starting a Telnet Session” on page 24).
2. Enable ACL. Type: **set acl state=enable** and press **Enter**.
3. Define the default chain policy. **Note:** the defaults are set to **table=filter** and **chain=input** and cannot be changed. Type:

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

where:

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

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

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

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

where:

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

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

xx = restriction stream; valid choices are:

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

yy = operation type; valid choices are:

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

Section 4: Configuration

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

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

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

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

where:

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

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

xx = ACL policy type; valid choices are:

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

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

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

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

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

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

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

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

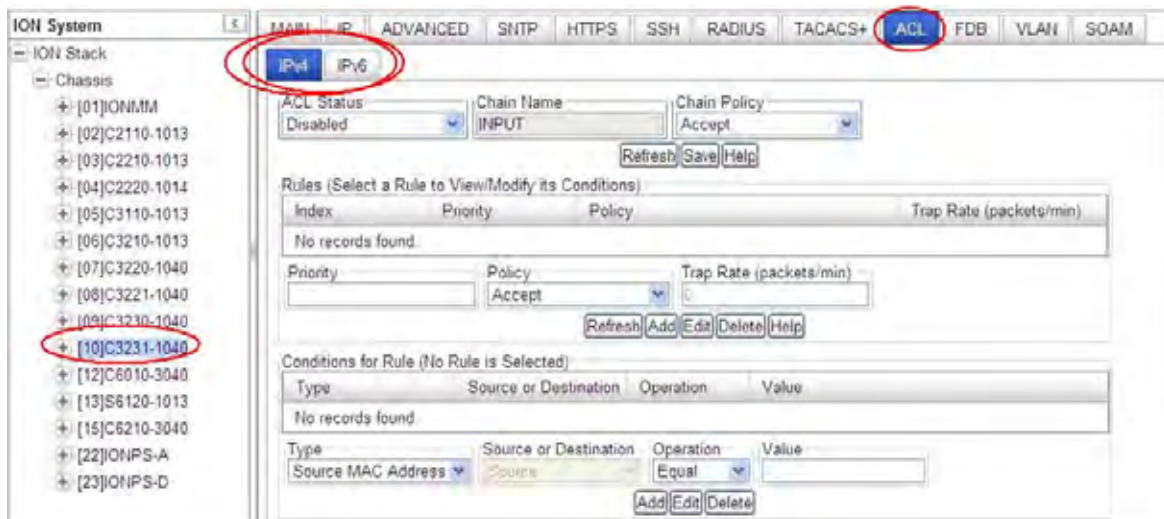
```
C1|S7|L1D>set acl state=enable
C1|S7|L1D>set acl table=filter chain=input policy=accept
C1|S7|L1D>add acl condition type=ipv4addr srcdst=src oper=equal value=192.168.1.30
C1|S7|L1D>add acl condition type=ipv4addr srcdst=src oper=notequal value=192.168.1.30
C1|S7|L1D>add acl rule position=head table=filter chain=input policy=accept condition=1
  condlist=1
C1|S7|L1D>add acl rule position=tail table=filter chain=input policy=trap condition=2
  condlist=2
C1|S7|L1D>show acl rule
```

index	table-type	chain-type	priority	policy	traprate(packets/min)	conditions
1	filter	input	1	trap	1500	2

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

ACL Config (IPv4) – Web Method

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



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

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

- The policy selected is **Trap**.
- A trap server is defined on the **MAIN** tab.
- A trap server is in the network and available.

d) Click **Add**.

7. Define additional rules as needed.

8. Define a condition for the Rule:

a) Select a rule by clicking its index number.

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

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

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

e) If the **Type** field selection was *ICMP Type*, then in the **Value** field, specify the MAC address, IP Address, Port number, or type associated with the selection in the **Type** field. There are 36 **ICMP Type** values selectable:

1. ICMP-ECHO-REPLY, 2. ICMP-DESTINATION-UNREACHABLE, 3. ICMP-NETWORK-UNREACHABLE, 4. ICMP-HOST-UNREACHABLE, 5. ICMP-PROTOCOL-UNREACHABLE, 6. ICMP-PORT-UNREACHABLE, 7. ICMP-FRAGMENTATION-NEEDED, 8. ICMP-SOURCE-ROUTE-FAILED, 9. ICMP-NETWORK-UNKNOWN, 10. ICMP-HOST-UNKNOWN, 11. ICMP-NETWORK-PROHIBITED, 12. ICMP-HOST-PROHIBITED, 13. ICMP-TOS-NETWORK-UNREACHABLE, 14. ICMP-TOS-HOST-UNREACHABLE, 15. ICMP-COMMUNICATION-PROHIBITED, 16. ICMP-HOST-PRECEDENCE-VIOLATION, 17. ICMP-PRECEDENCE-CUTOFF, 18. ICMP-SOURCE-QUENCH, 19. ICMP-REDIRECT, 20. ICMP-NETWORK-REDIRECT, 21. ICMP-HOST-REDIRECT, 22. ICMP-TOS-NETWORK-REDIRECT, 23. ICMP-TOS-HOST-REDIRECT, 24. ICMP-ECHO-REQUEST, 25. ICMP-ROUTER-ADVERTISEMENT, 26. ICMP-ROUTER-SOLICITATION, 27. ICMP-TIME-EXCEEDED, 28. ICMP-TTL-ZERO-DURING-TRANSIT, 29. ICMP-TTL-ZERO-DURING-REASSEMBLY, 30. ICMP-PARAMETER-PROBLEM, 31. ICMP-IP-HEADER-BAD, 32. ICMP-REQUIRED-OPTION-MISSING, 33. ICMP-TIMESTAMP-REQUEST, 34. ICMP-TIMESTAMP-REPLY, 35. ICMP-ADDRESS-MASK-REQUEST, and 36. ICMP-ADDRESS-MASK-REPLY.

f) Click **Add**.

Section 4: Configuration

9. Define additional conditions as needed following step 8 above.
10. To change an existing Rule, select the Rule in the table, click the **Edit** button, and make changes per steps 5-6 above.
11. Verify the newly-defined Rules and Conditions.

ACL Status:
 Chain Name:
 Chain Policy:

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

Index	Priority	Policy	Trap Rate (packets/min)
1	3334	Trap	10
2	3444	Trap	100

Priority:
 Policy:
 Trap Rate (packets/min):

Conditions for Rule 1

Type	Source or Destination	Operation	Value
IPv4 Address	Source	Not Equal	192.168.2.20
IPv4 Network	Source	Not Equal	192.168.2.0:255.255.255.0
IPv4 Address Range	Destination	Equal	192.168.2.20-192.168.2.90

Type:
 Source or Destination:
 Operation:
 Value: -

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

ACL under IPv6

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

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

ACL Config (IPv6) – CLI Method

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

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

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

9. Verify the ACL rules have been defined and associated. Type: **show ip6tables acl rule** and press **Enter**.

The current ACL Rule information table displays. For example:

```
Agent III C1|S9|L1D>set ip6tables acl state=enable
Agent III C1|S9|L1D>set ip6tables acl table=filter chain=input policy=accept
Agent III C1|S1|L1D>add ip6tables acl rule position=head table=filter
chain=input policy=1 trap=444
Agent III C1|S1|L1D>add ip6tables acl rule index=2 table=filter
chain=input prio=2 policy=trap traprate=100
Agent III C1|S1|L1D>set ip6tables acl condition=1 rule_index=1
```

Section 4: Configuration

```

Agent III C1|S1|L1D>add ip6tables acl condition type= ipv6addr srcdst=src
oper=equal value=VAL
Agent III C1|S1|L1D>show ip6tables acl rule
index      table-type  chain-type  priority  policy  traprate(pkts/min)  condi-
tion
-----
--
2          filter    input      1         trap    0                    no
1          filter    input      2         trap    0                    no
Agent III C1|S1|L1D>

```

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

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

```

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

```

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

```

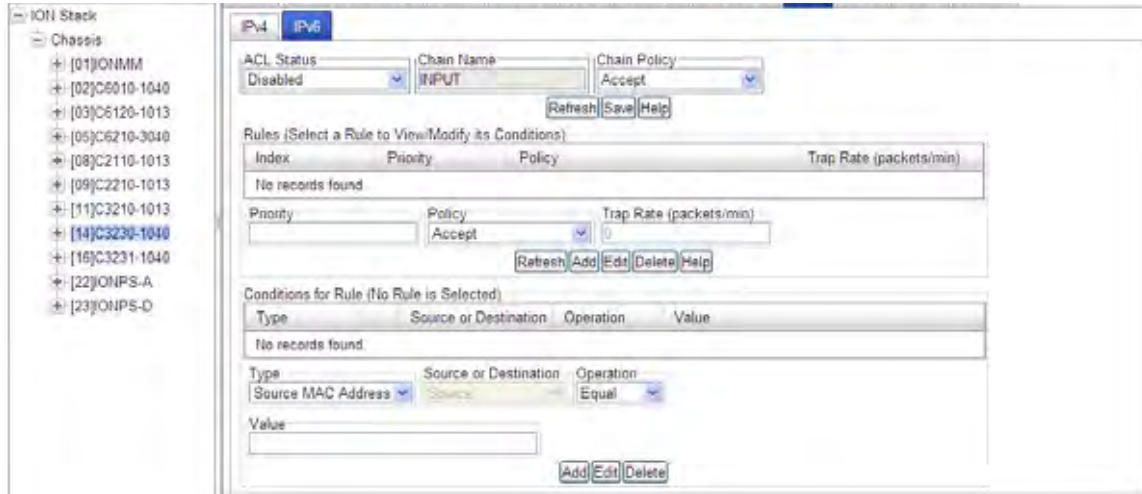
Agent III C1|S1|L1D>show ip6tables acl chain
table-type  contain-type  chain-name  default-policy
-----
filter      input        INPUT       accept
C1|S3|L1D>

```

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

ACL Config (IPv6) – Web Method

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



3. At the **ACL Status** dropdown, select **Enabled**.
4. At the **Chain Policy** dropdown, select **Accept** or **Drop**.
5. In the **Rules - Priority** field, enter a priority of 1-65,535.
6. At the **Policy** dropdown, select **Accept** or **Drop** or **Trap**.
7. In the **Trap Rate** (packets/min) field, enter the desired rate for trapping (if selected). The valid range is 1-65,535. The trap sent rate is 2 packet/sec (two packets/second (2 pps)). The matched packets number in one minute. If over this rate matched, a trap will be sent.
8. Click the **Add** button to add this Rule.
9. At the **Conditions - Type** dropdown, select the basis for conditions for this rule. The IPv6 options are:
 - Source MAC Address** (default)
 - IPv6 Address**
 - IPv6 Network**
 - TCP Port**
 - TCP Port Range**
 - UDP Port**
 - UDP Port Range**
 - ICMP Type**
4. Enter a **“Value”** (a valid IPv6 address / a number from 0-128 or an IP address such as ffff:00:00:00:00:00:00).

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

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

Section 4: Configuration

IPv6 Condition Type Values

Source MAC address: first 6 bytes for mac address.

IPv6 address: the first 16 bytes for IPv6 address.

)IPv6 network: address[/mask], the first 16 bytes for IPv6 address, the followed bytes can be either of two cases.

Case 1: the 17th byte is a plain number, specifying the number of 1's at the left side of the network mask.

Case 2: bytes 17-32 are the value for network mask.

TCP port: the first two bytes for TCP port number.

TCP port range: the first 4 bytes(0-1 byte for the start TCP port number, 2-3 byte for the end TCP port number).

UDP port: the first two bytes for UDP port number.

UDP port range: the first 4 bytes(0-1 byte for the start UDP port number, 2-3 byte for the end UDP port number).

ICMP type: the first two bytes for ICMP type. For ICMP type, the following values are supported:

ICMP_DESTINATION-UNREACHABLE = 0x3ff,
 ICMP_NO-ROUTE = 0x0301,
 ICMP_COMMUNICATION-PROHIBITED = 0x0302,
 ICMP_ADDRESS-UNREACHABLE = 0x0303,
 ICMP_PORT-UNREACHABLE = 0x0304,
 ICMP_PACKET-TOO-BIG = 0x04ff,
 ICMP_TIME-EXCEEDED = 0x05ff,
 ICMP_TTL-ZERO-DURING-TRANSIT = 0x0501,
 ICMP_TTL-ZERO-DURING-REASSEMBLY = 0x0502,
 ICMP_PARAMETER-PROBLEM = 0x06ff,
 ICMP_BAD-HEADER = 0x0601,
 ICMP_UNKNOWN-HEADER-TYPE = 0x0602,
 ICMP_UNKNOWN-OPTION = 0x0603,
 ICMP_ECHO-REQUEST = 0x07ff,
 ICMP_ECHO-REPLY = 0x08ff,
 ICMP_ROUTER-SOLICITATION = 0x09ff,
 ICMP_ROUTER-ADVERTISEMENT = 0x0aff,
 ICMP_NEIGHBOUR-SOLICITATION = 0x0bff,
 ICMP_NEIGHBOUR-ADVERTISEMENT = 0x0cff,
 ICMP_REDIRECT = 0x0dff, Use this OID to set the value of the corresponding condition type.

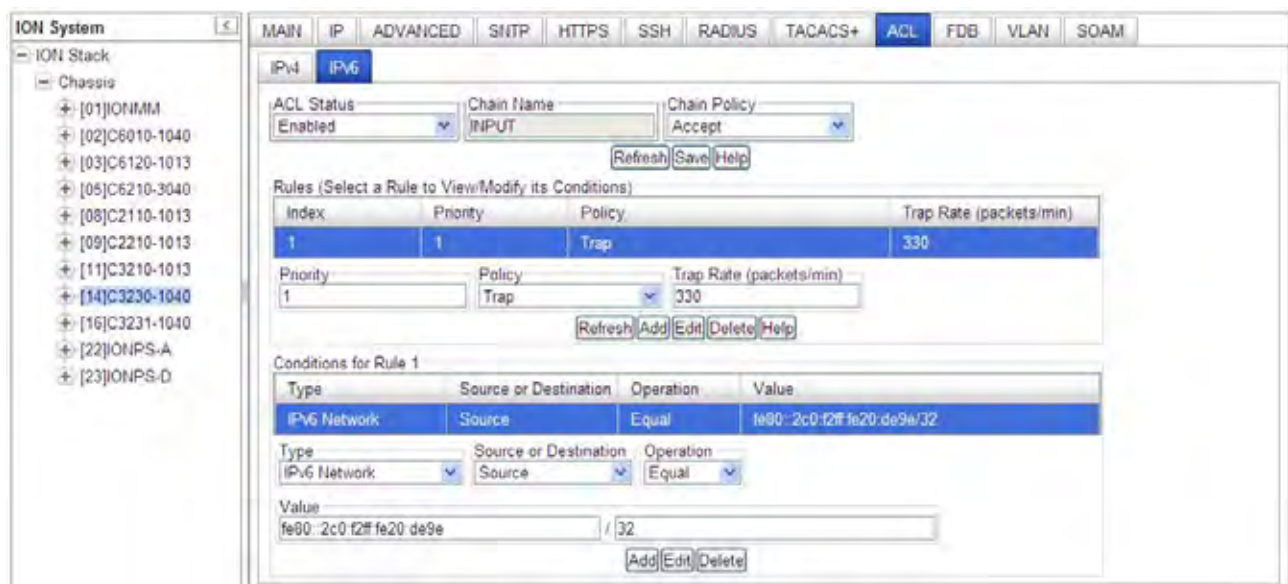
Notifications: `ionDevSysIPv6AclIdsEvt` (`entPhysicalIndex`, `ip6tablesGRuleIndex`)

A `ionDevSysIPv6AclIdsEvt` event is sent if an `ip6tables IDS` (Intrusion Detection Systems) is detected.

`entPhysicalIndex` indicates in which SIC the IDS is detected.

`entPhysicalIndex/ip6tablesGRuleIndex` indicates which `ip6tables ACL` rule is matched for this IDS.

For example, shown below is a C3230 NID with IPv6 ACL configured with one Rule and one Condition.



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

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

Configuring HTTPS

HTTPS is a secure version of the Hyper Text Transfer Protocol (HTTP), and is used as a security option when accessing the IONMM through the Web interface.

IMPORTANT

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

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

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

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

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

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

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

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

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

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

HTTPS Config – CLI Method

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

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Enable HTTPS. Type **set https state=enable** and press **Enter**.
3. Set the port number to be used. Type **set https port=<x>** and press **Enter**. The default is 443.
4. Define whether the certificate is from a certificate authority or is self-generated. Type:

```
set https certificate-type=<xx>
```

where:

xx = certificate authority; valid choices are:

- **authorized**
- **self-certificate**

5. Press **Enter**.
6. Specify the name of the certificate file. Type:

```
set https certificate-file=<xx>
```

where:

xx = name of the file

7. Press **Enter**.
8. Specify the name of the private key file. Type:

```
set https private-key file=<xx>
```

Section 4: Configuration

where:

xx = the name of the file

9. Press **Enter**.
10. Define the password to be used for the private key file. Type **set https private-key password=xxxx** and press **Enter**. The message *“Please input password:”* displays.
11. Type the password then press **Enter**. The message *“Please input password again:”* displays.
12. Type the password again then press **Enter**.
13. Verify the configuration has been set. Type **show https config** and press **Enter**. The current HTTPS configuration table displays. For example:

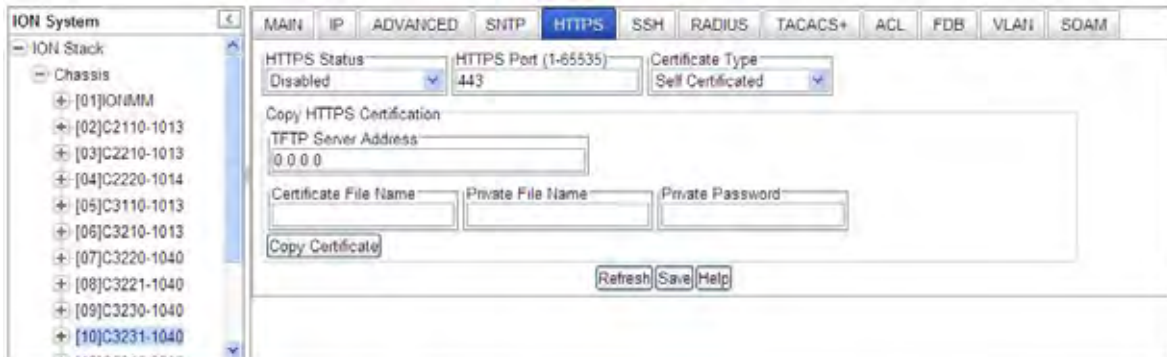
```
C1|S8|L1D>set https state=enable
C1|S8|L1D>set https port=443
C1|S8|L1D>set https certificate-type=authorized
C1|S8|L1D>set https certificate-file-name=name.cer
C1|S8|L1D>set https private-key file-name=name.key
C1|S8|L1D>set https private-key password
Please input password:

Please input password again:

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

HTTPS Config – Web Method

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



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

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

4. In the **HTTPS Port** field, enter the port number for HTTPS operations. The valid range is from 1-65535. The default is port 443.
5. In the **Certificate Type** field select **Self Certified** or **Authorized**.
6. In the **TFTP Server Address** field, enter the IP address of your remote TFTP server (or client). This entry must be an IP address or a domain name.
7. In the **Certificate File Name** field, enter the name of the file with the authentication certificate.



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

8. In the **Private File Name** field, enter the name of the private key file.
9. In the **Private Password** field, enter the private key password. This is the password to access the private key file.
10. Click the **Copy Certificate** button. The message “*The certificate file(s) is being copied, please wait...*” displays momentarily.
11. Click the **Save** button. A re-login occurs immediately; and the ION login prompt displays.

Section 4: Configuration

12. The ION System Web Interface is now an HTTPS (secure) address. In your web browser, click **Tools**, click *Internet Options*, click **Advanced**, and make sure the **SSL** and **TLS** protocols are enabled under the security section.
13. For subsequent logins, use **https** instead of **http** as the URL prefix (eg., <https://192.168.1.10/web.html>).
14. Enter the ION system *User Name* and *Password*.
15. Click the **Sign In** button. The **MAIN** tab displays.

If the message *Invalid user name or password!* displays, see the [Troubleshooting](#) section of this document.

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

Configuring MAC Address Filtering

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

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

MAC Address Filtering – CLI Method

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

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

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

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

static - a Valid entry that does not age.

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

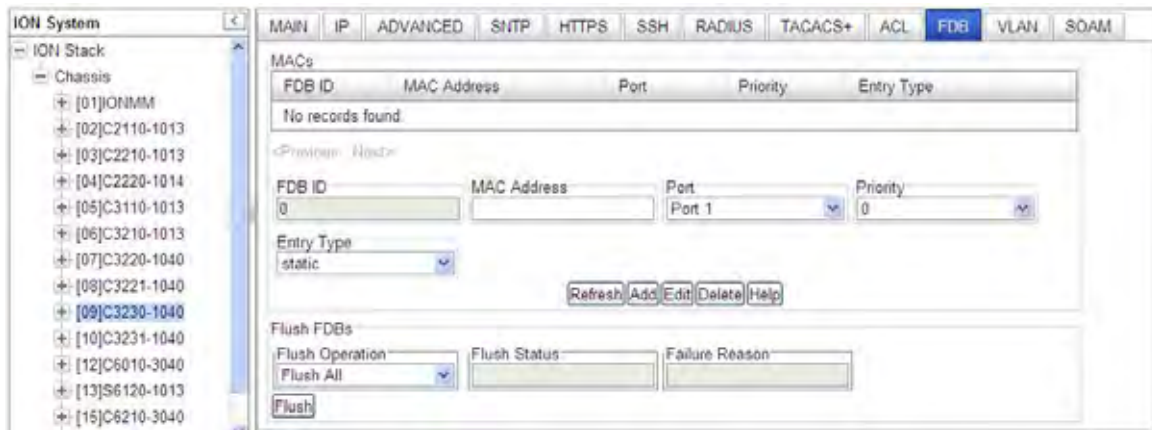
staticPA - a static entry that has priority override enabled.

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

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

MAC Address Filtering – Web Method

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



3. In the **MAC Address** field, enter the MAC address to be filtered. This is the unicast or multicast MAC address associated with this entry.
4. In the **Port** field, select the port to be filtered (Port 1 or Port 2 on the x3230, or Port 1, 2 or 3 on the x3231). This is the logical port to which this Address is connected.
5. In the **Priority** field, select the priority to be assigned (0-7, where 0 is the lowest priority). The priority specified here is used when Priority Override is enabled.

In the **Entry Type** field, select the type of entry / MAC address database. This is used to define the entry state, depending on whether it is a unicast or a multicast address in the entry. The selections are “static”, “staticNRL” “staticPA” or “dynamic”.

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

For Unicast frames:

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

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

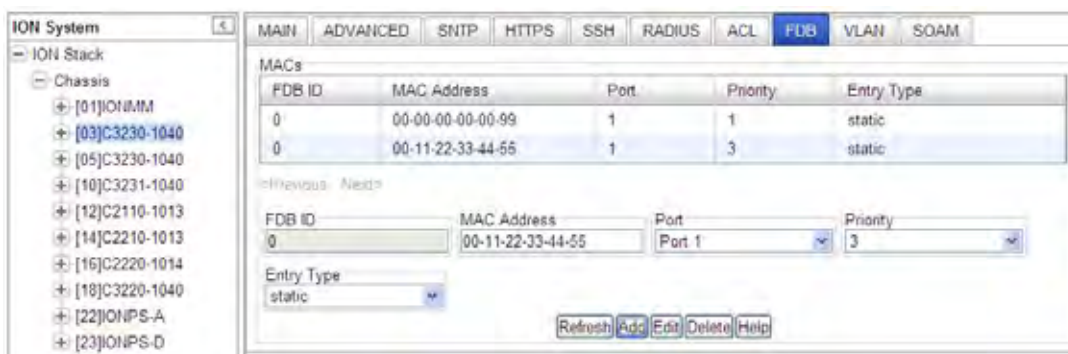
For Multicast frames:

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

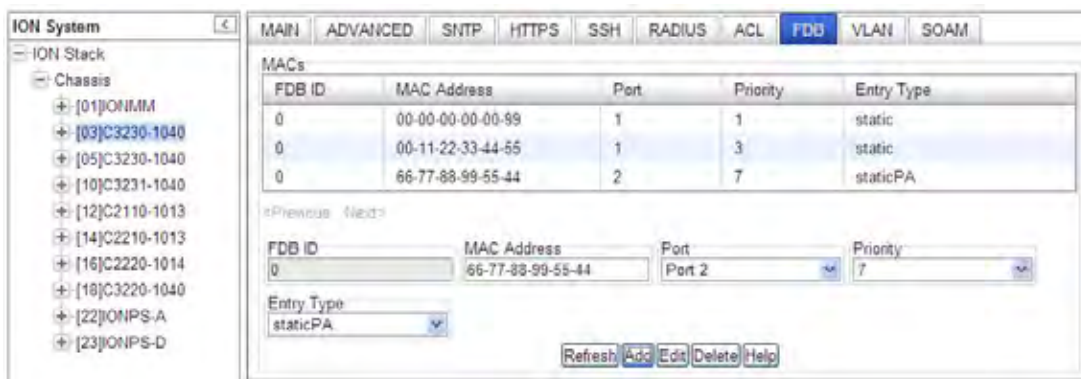
staticPA (static with priority override): this is a static entry not aged and the priority (sC3231100FwdPriority) indicates the priority to use for this frame's source/destination address.

dynamic - A valid entry with no special attributes which ages and is ultimately removed from the forwarding database (not selectable; read-only value only).

- Click the **Add** button. The message “Adding MAC succeeded” displays and the entry is added to the MACs table.



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



Note:

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

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

Configuring MAC Address Blocking

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

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

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

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

MAC Address Blocking – CLI Method

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

where:

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

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

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

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

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

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

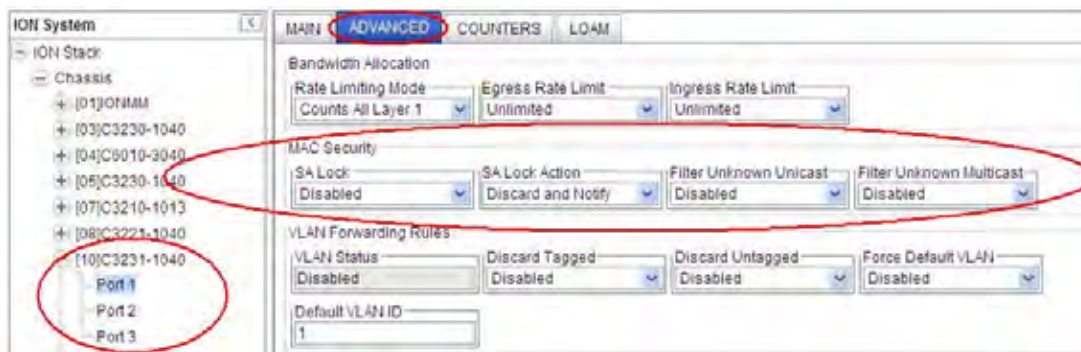
5. Press **Enter**.

6. Verify the port security configuration. Type **show ether security config** and press **Enter**.
The Ethernet Port Security configuration table displays. For example:

```
C1|S13|L1P1>set ether src-addr-lock=enable
C1|S13|L1P1>set ether src-addr-lock action=discardandnotify
C1|S1|L1D>go s=13 llp=1
C1|S13|L1P1>show ether security config
Ethernet port security configuration:
-----
Source MAC address lock:          enable
Source MAC address lock action:   discard
Filter unknown dest unicast:     enable
Filter unknown dest multicast:   disable
```

MAC Address Blocking – Web Method

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



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

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

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

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

Shutdown: This will shutdown the interface on receiving the frame.

All: All the above actions take place. The frame is discarded, a trap is sent and the port is shutdown to prevent intrusion attack.

7. In the **Filter Unknown Unicast** field, select **Enabled** to filter all unicast frames with an unknown destination address from egressing this Port.
8. In the **Filter Unknown Multicast** field, select **Enabled** to filter all multicast frames with unknown destination address from egressing this Port.
9. Locate the **VLAN Forwarding Rules** section.

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

Configuring Port Forward Management / IP Access Blocking

Any management of the system via IP can be locked at the system level, or only on certain ports. For example, management can occur via web/SNMP only on Port 1, so that access via other ports can be blocked. For each port, define the set of ports that frames ingressing this Source port can be forwarded to, and define the port that will perform its management functions.

Port Forward Management / IP Access Blocking can be configured in the NID using either the CLI or Web method.

Port Forward Management / IP Access Blocking – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Access the desired port.
3. Set the forwarding port list. Type: **set fwd portlist=y**
where: y=port number{1, 2, 3}
4. Press **Enter**.
5. Enable port management access. Type **set port mgmtaccess=z**
where: z=enable or disable
6. Press **Enter**.
7. View the port list. Type **show fwd portlist** and press **Enter**. The FWD Portlist table displays:

```

C1|S1|L1D>go s=13 llp=1
C1|S13|L1P1>set fwd portlist 2
C1|S13|L1P1>show fwd portlist
port-id          fwd portlist      mgmt access
-----
1                2                disable

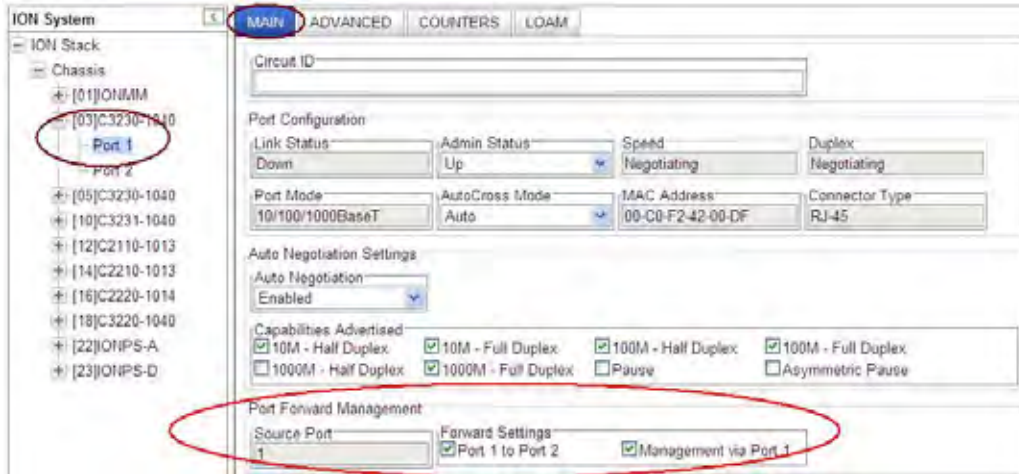
C1|S13|L1P1>set port mgmtaccess enable
C1|S13|L1P1>show fwd portlist
port-id          fwd portlist      mgmt access
-----
1                2                enable

C1|S13|L1P1>set fwd portlist 2,3
C1|S13|L1P1>show fwd portlist
port-id          fwd portlist      mgmt access
-----
1                2,3              enable

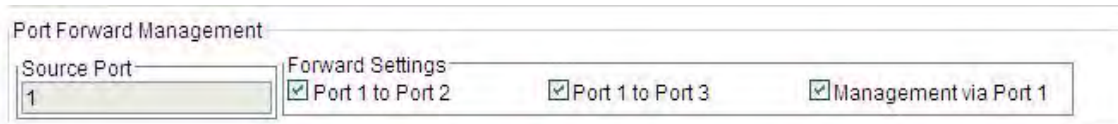
```


Port Forward Management / IP Access Blocking – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port. Select the port’s **MAIN** tab if not already displayed.
3. Locate the **Port Forward Management** section.



(Model C3230 – Port 1 shown above, Model x3231 – Port 3 shown below.)



4. In the **Forward Settings** fields, check the checkbox for the set of ports to which frames ingressing this Source port can be forwarded.
5. Check the checkbox for the **Management via Port x** as required for this port.
6. Click the **Save** button when done.

Configuring RADIUS

IMPORTANT

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

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

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

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

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

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

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

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

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

IMPORTANT

After configuring the NID for RADIUS, a re-login occurs immediately; you must then enter the RADIUS defined username and password in order to re-connect to the ION system. This procedure will end your current session, and you must then log in using your RADIUS log in and password.

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

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

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

RADIUS Config – CLI Method



Note before performing this configuration: After configuring the x323x for RADIUS, you will be required to enter the RADIUS defined username and password when connecting to the IONMM.

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Enable RADIUS. Type **set radius client state=enable** and press **Enter**.
3. Define a single RADIUS server. Type:

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

where:

vv = RADIUS server number (1–6)

ww = IP address format; the valid choices are:

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

xx = RADIUS server IP address

yy = optional; number of times the access request will be re-sent to the RADIUS server before being discarded or re-directed to another server. The default is 3.

zz = optional; number of seconds to wait for a response from the RADIUS server before re-sending the request. The default is 30.

4. Define a secret. Type:

```
set radius svr=<xx> secret=<yy>
```

Section 4: Configuration

where:

xx = server number (enter the same as entered in Step 4).

yy = an alphanumeric text string used to validate communications. Maximum length of the secret is 128 characters.

5. Press **Enter**.
6. Repeat Steps 3–5 for each server to be defined. Up to six RADIUS servers can be defined in the system.
7. Verify that the configuration has been set. Type:

show radius config

8. Press **Enter**. The RADIUS Configuration table information displays. For example:

```
C1|S3|L1D>set radius svr=1 type=ipv4 addr=192.168.1.30 retry=2 timeout=15
C1|S3|L1D>set radius svr=1 secret=private
C1|S3|L1D>set radius client state=enable
C1|S3|L1D>show radius config
RADIUS client state:          disable

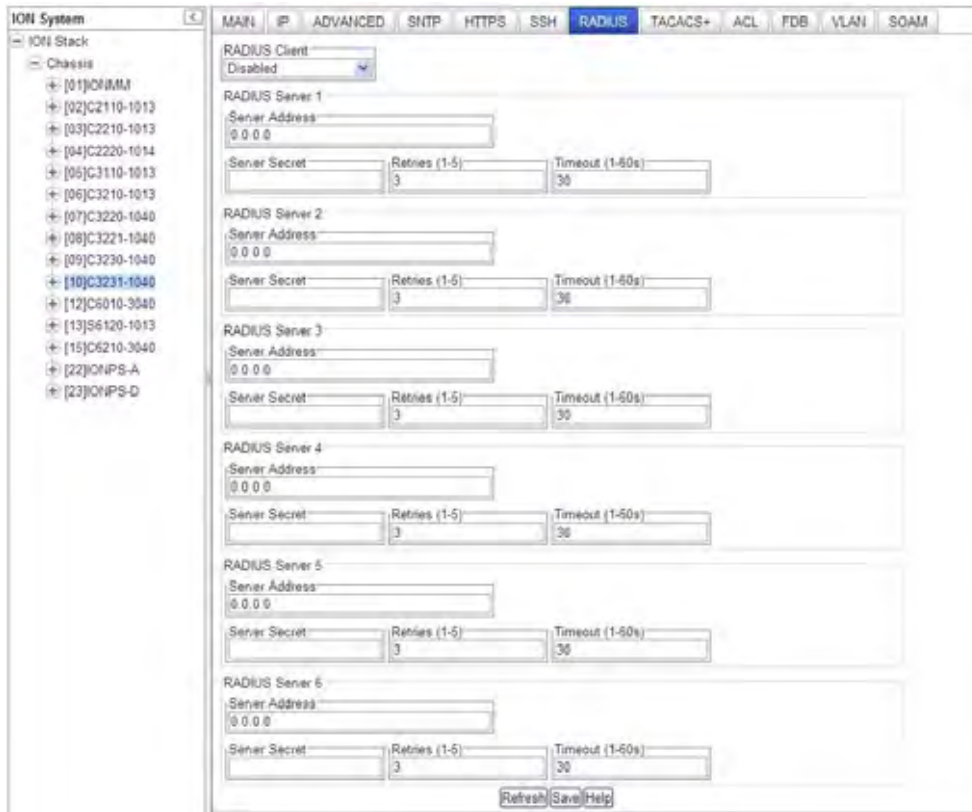
RADIUS authentication server:
index      addr-type      addr          retry      timeout
-----
1          ipv4           192.168.1.30  2          15
2          dns            0.0.0.0      3          30
3          dns            0.0.0.0      3          30
4          dns            0.0.0.0      3          30
5          dns            0.0.0.0      3          30
6          dns            0.0.0.0      3          30
```

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

RADIUS Config – Web Method

Note before performing this configuration: After configuring the x323x for RADIUS, you will be required to enter the RADIUS defined username and password when connecting to the IONMM.

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



3. In the **Radius Client** field, select **Enabled**. The default is **Disabled**.
4. Configure the RADIUS Server.
 - In the **Server Address x** field, enter the IP address of the RADIUS server. This is the IPv4 or IPv6 address of a RADIUS server.
 - In the **Server Secret x** field, enter the secret. It can be written but displays only a series of dots (e.g., ●●●●●).
 - In the **Retries x** field, enter the number of times the access request will be re-sent to the RADIUS server before being discarded or re-directed to another server. This is the maximum number of RADIUS Access-Request packets sent to this server before it times out or receives a response. The factory default is 3. The valid range of entries is from 1-5 retries.

Section 4: Configuration

- In the **Timeouts x** field enter the number of seconds to wait for a response from the RADIUS server before re-sending the request. This is the second number of authentication timeouts to this server. After a timeout, the client may retry to the same server, send to a different server, or give up. The default is 30 seconds. The valid range of entries is from 1-60 seconds.
5. Repeat Step 4 for each RADIUS Server to be defined (up to 6).
 6. When all of the RADIUS Servers have been defined, click **Save**.
The message “*The RADIUS settings have been changed and a re-login will be performed right now.*” displays.
 7. Click the **OK** button.
 8. The new sign in message displays: “*Sign in to ION System Web Interface (RADIUS)*”.
 9. Enter the new User Name and Password and then click the **Sign in** button.
 10. If your web browser displays a Certificate Error, follow the on-screen instructions. See the [Troubleshooting](#) section starting on page 269 for specific error messages.

Configuring TACACS+

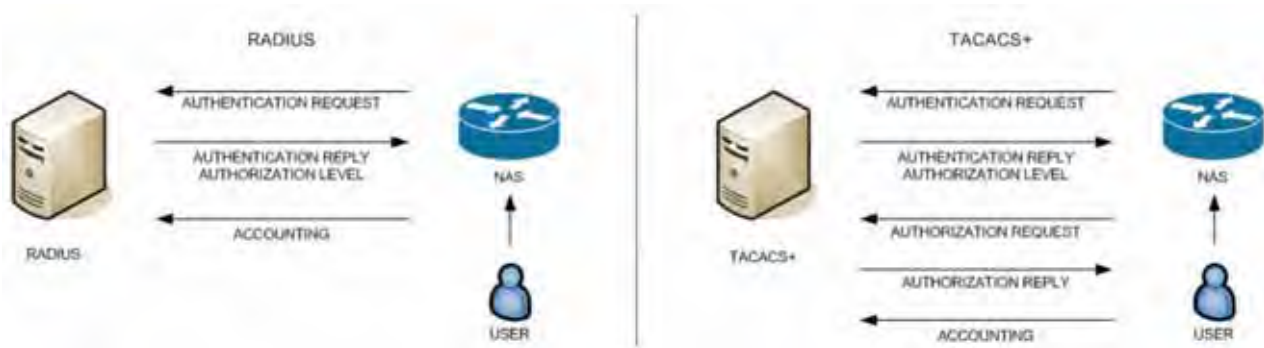
TACACS+ (Terminal Access Controller Access Control System) provides routers and access servers with authentication, authorization and accounting services. TACACS+ is used along with or as a replacement for RADIUS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram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

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

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

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

By default, Tacplus listens on TCP port 49 and provides network devices with authentication, authorization and accounting services (AAA).



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

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

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

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

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

Section 4: Configuration

The privilege level (`priv_lvl`) indicates what the user is authenticating as. Privilege levels are values from 0 to 15 with each level representing a privilege level that is a superset of the next lower value.

The type of authentication (`authen_type`) indicates what is being performed. Values can include ASCII, PAP, CHAP, ARAP, and MSCHAP.

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

The `authen_method` indicates the authentication method used by the client to acquire the user information.

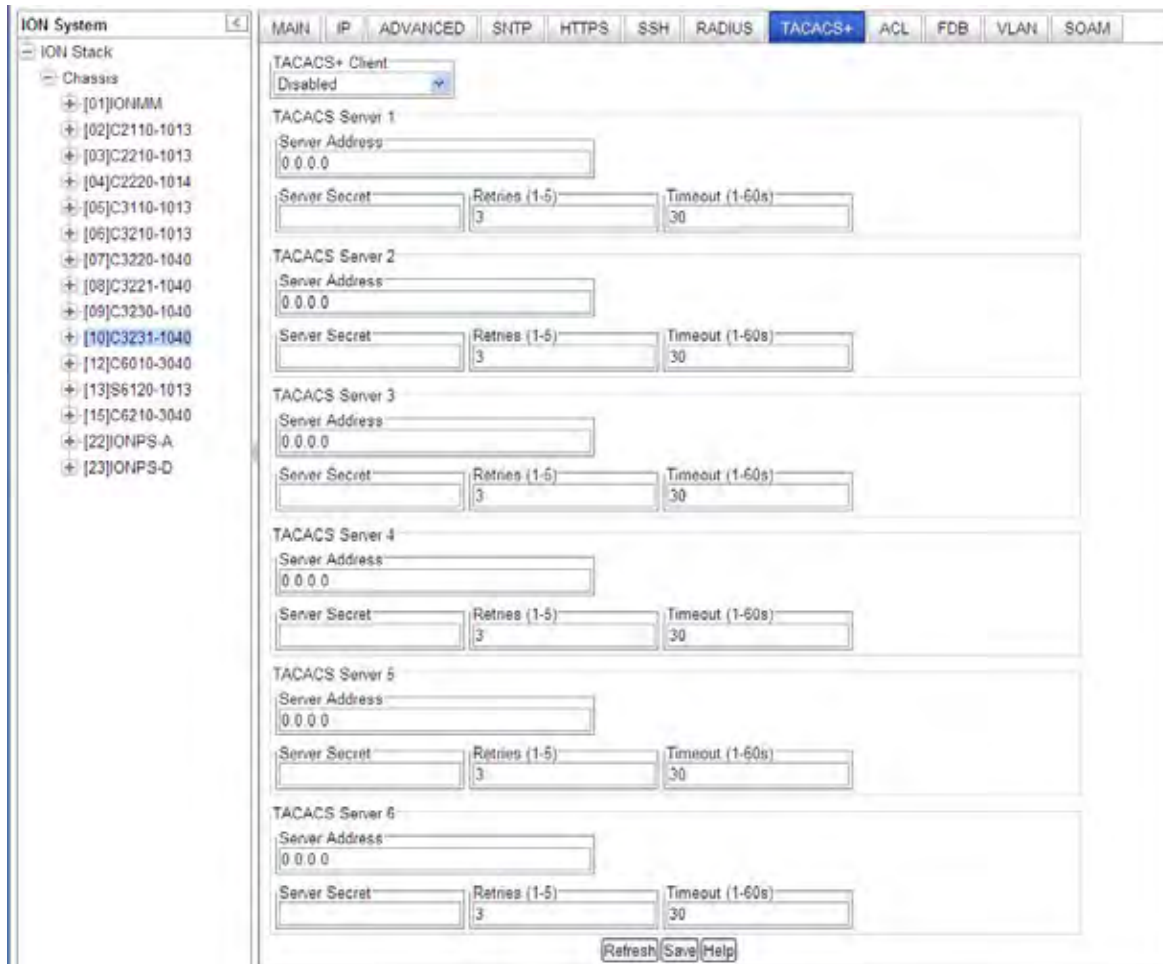
These methods can include NOT_SET, NONE, KRB5, LINE, ENABLE, LOCAL, TACACSPLUS, GUEST, RADIUS, KRB4, and RCMD.

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

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

TACACS+ Config - Web Method

1. From the or x323x card, navigate to the TACACS+ tab.



2. At the **TACACS+ Client** dropdown, select **Enabled**. The default is **Disabled**.
3. At the **TACACS Server 1** Server Address, enter a valid IPv4 or IPv6 address. For this TACACS+ server, enter:
 - Server Secret:** enter a server secret (password); the entry displays as a series of ●●●● characters. This is a string well known to both client and server and is used to validate and/or encrypt data, transmitted between them.
 - Retries (1-5):** enter the number of connection attempts before quitting further attempts.
 - Timeout (1-60s):** The number of seconds to wait for a response from the TACACS+ server before re-sending the request. After a timeout, the TACACS+ client may retry to the same TACACS+ server, send to a different server, or give up. The default is 30 seconds. The valid range of entries is from 1-60 seconds.
4. At the **TACACS Server 2-6** Server Address, enter valid IPv4 or IPv6 address(es). For each TACACS+ server, enter **Server Secret**, **Retries (1-5)**, and **Timeout (1-60s)** values. Configure up to six TACACS Servers per steps 1-2 above.
5. Click the **Save** button when done.

TACACS+ Config - CLI Method

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

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 23) or a Telnet session (see “[Starting a Telnet Session](#)” on page 24).
2. Enable TACACS+. Type **set tacplus client state=enable** and press **Enter**.
3. Set the TACACS+ server type. Type **set tacplus svr 1 type= ipv4|ipv6|dns** and press **Enter**.
4. Set the number of retry attempts to be made before quitting. Type: **set tacplus svr 1 retry=<1-5>** and press **Enter**.
5. Define the TACACS+ secret (password) to be used. Type **set tacplus svr 1 secret= SECRET** and press **Enter**.
6. Set the number of timeouts to be included. Type: **set tacplus svr 1 timeout=<1-60>** and press **Enter**.
7. Verify the TACACS+ settings. Type **show tacplus config** and press **Enter**.
8. Set the user login levels. Type: **set login method=(local|radiuslocal|tacpluslocal|radiustacpluslocal|tacplusradiuslocal)** and press **Enter**. This is the order in which the user attempts logins.
9. Verify the settings. Type **show tacplus config** and press Enter. For example:

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

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

TACACS+ Messages

Message:

Error: The parameter is wrong!
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!"
Fail to get system user name!
Fail to set TACPLUS client state!
Fail to set Tacplus server address type!
Fail to set TACPLUS server address!
Fail to set TACPLUS server retry
Fail to set TACPLUS server time out!
Fail to set TACPLUS server row status!
Fail to set TACPLUS server time out!
Getting TACPLUS server fail
Invalid TACPLUS server address!
Please input a digital number to specify radius server index!
Please input a digital number to specify RADIUS server retry!
Please input a digital number to specify tacplus server time out!
Please input a digital number to specify TACPLUS server retry!
Please input a digital number to specify TACPLUS server time out!
Please input a digital number to specify tacplus server index!
Please input a digital number to specify TACPLUS server index!
Please input a number to specify the TACPLUS server index!
Set TACPLUS server secret
TACPLUS authentication server index is out of range!
TACPLUS server retry is out of range!
TACPLUS server time out is out of range!
The ipv6 address is multicast address
The TACPLUS authentication server specified does not exist!
Wrong parameter number!

Meaning: You entered a TACACS+ (Tacplus) command, but the command was unsuccessful.

Recovery:

1. Make sure you enter the TACACS+ command on an IONMM or a standalone SIC at the device level.
2. Make sure the TACACS+ client is enabled and that the TACACS+ server is correctly configured and running.
3. Make sure you enter the command parameters within the valid ranges and in the proper syntax. See “[TACACS+ Commands](#)” on page 111.
4. Check the RADIUS configuration.
5. Retry the command. See the related manual or section.
6. Check your third party TACACS+ server documentation and helps (e.g., [ClearBox Server](#), etc.).
7. If the problem persists, contact TN Technical Support.

Message: *The TACACS+ settings have been changed and a re-login will be performed right now.*

Meaning: When you hit **Save** after any TACACS+ re-config a re-login is required.

Recovery:

1. Log back in to the system. See “[TACACS+ Commands](#)” on page 111.
2. Enter the **show tacplus config** command and verify the TACACS+ configuration settings.

Section 4: Configuration

TACACS+ Syslog Messages

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

```

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

```

Configuring SSH

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

IMPORTANT

- If the NID is managed by the ION Management Module (IONMM), configuring SSH should be done at the IONMM and not at the NID.
- SSH has no affect when accessing the IONMM through either the USB or the Web interface.

SSH is widely used by network administrators to control servers remotely (i.e., a Web server). SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secured in several ways. Both ends of the client/server connection are authenticated using a digital certificate provided by the administrator and passwords are encrypted to prevent interception. Once a password is given and verified, a session will be created and SSH will issue a unique digital signature (or private key) associated with that session. To make a secure connection, SSH must be installed, activated, and certificates must be given to both the source machine and the NID.

For the SSH implementation, the NID can support and will generate both the Rivest-Shamir-Adleman (RSA) and Digital Signature Algorithm (DSA) for public key cryptography for both connection and authentication.

Notes:

- The ION system provides a temporary certificate and key, but they must be updated with a permanent version for production use (e.g., from Verisign, DigiCert, Thawte, etc.).
- You must install an SSH client on the management station (PC) to access the IONMM for management via the SSH protocol.
- SSH has no affect when accessing the IONMM through either the USB or the Web interface.
- On ION systems, SSH can be configured for either Login/Password authentication or for Public/Private key and Certificate authentication.
- For Login/Password, you must establish the SSH login and password in the SSH client. When logging in to the IONMM, you will be required to first enter the SSH login and password and then will be prompted for the ION System password.
- After an upgrade from v1.0.3 to v0.5.12, the User Public-Key is not saved. In ION v1.0.3, the user-public key is binding with the Linux root user and is stored in the root file system (/root/.ssh/). This file system is replaced after this version upgrade, so this key will be lost. You can still log in through SSH, but you must upload the public key again in order to use it. This missing key problem will occur only if you upgrade from 0.5.14 to a later release. In ION versions after 0.5.14, the user-public key is saved after an upgrade.

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

SSH Config – CLI Method

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

2. Enable SSH. Type **set ssh server state=enable** and press **Enter**.

3. Set the timeout value. Type:

```
set ssh client timeout=<xx>
```

where:

xx = number, 1–120, of seconds to wait for a response before timing out

4. Press **Enter**.

5. Set the retry limit. Type:

```
set ssh auth-retry=<xx>
```

where:

xx = the number (1–5) of retries that will be attempted before dropping the connection.

6. Generate the host public key. Type:

```
generate ssh host-key=<xx>
```

where:

xx = type of key to be generated; the valid choices are:

- **rsa**
- **dsa**
- **both**

7. Obtain the public key file using the TFTP **get** command.

8. Associate the public key with a user. Type:

```
set ssh public-key user=<xx> type=<yy> file=<zz>
```

where:

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

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

- **rsa**
- **dsa**

zz = name of the file that contains the public key

9. Press **Enter**.

10. Verify the configuration has been set. Type:

```
show ssh config
```

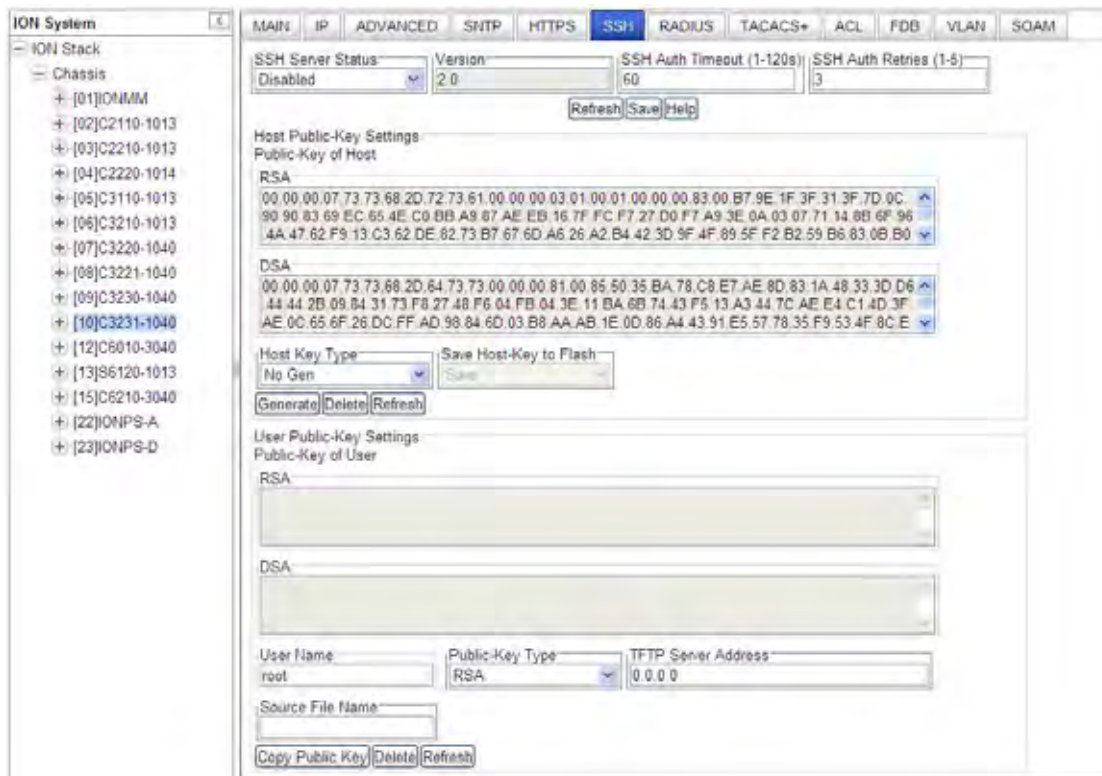
11. Press **Enter**. The Secure Shell (SSH) configuration table displays. For example:

```
C1|S3|L1D>set ssh server state=enable
C1|S3|L1D>set ssh client timeout=15
C1|S3|L1D>set ssh auth-retry=3
C1|S3|L1D>generate ssh host-key=both
Processing...
Processing...
Host-key generated!
C1|S3|L1D>set ssh public-key user=agent type=dsa file=id_dsa.pub
C1|S3|L1D>show ssh config
Secure Shell configuration:
-----
Secure shell server state:                               enable
Secure shell major version:                             2
Secure shell minor version:                             0
Secure shell time out:                                  15
Secure shell authentication retries:                     3
```

Section 4: Configuration

SSH Config – Web Method


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



The screenshot shows the ION System web interface with the SSH configuration page selected. The interface includes a navigation menu on the left and a main configuration area on the right. The SSH Server Status is set to Disabled. The Host Public-Key Settings section shows RSA and DSA key generation options. The User Public-Key Settings section shows RSA key generation options.

3. In the **SSH Server Status** field, select **Enabled**. The default is **Disabled**.
4. If SSH is being configured for Login/Password authentication, go to step 17.
If SSH is being configured for Public/Private key and Certificate, continue with step 5 below.
5. In the **SSH Auth Timeout** field, enter the number of seconds that the IONMM will wait for a response before dropping the connection. This is the time period, in seconds, that the router waits for the SSH client to respond. The valid range is 1-120 seconds. The default is 60 seconds.
6. In the **SSH AUTH Retries** field, enter the number of times that communication will be attempted before the connection is dropped. This is the number of attempts after which the interface is reset. The valid range is 1-5. The default is 3 retries.
7. In the **Host Key Type** field, select the type of host key to be generated; valid choices are:
 - **No Gen** – no key will be generated (disables SSH function)
 - **RSA** – generate an RSA key (the generated key will display in the RSA block)
 - **DSA** – generate a DSA key (the generated key will display in the DSA block)
 - **Both** – generate both an RSA key and a DSA key

8. Leave the default setting in the **Save Host-Key to Flash** field (for future use).
9. Click the **Generate** button. The message “*The host key is being generated, please wait...*” displays while the host key(s) are generated.
10. Scroll down to the **User Public-Key Settings** section.



11. In the **User Name** field, enter the name of the user to be associated with the user public key.
 12. In the **Public-Key Type** field, select the type of user's public key to be copied or deleted, either:
 - **RSA** (an RSA public key is generated)
 - **DSA** (a DSA public key is generated)
 13. In the **TFTP Server Address** field, enter the IP address of your TFTP server.
 14. In the **Source File Name** field, enter the name of the file for the user public key.
 15. Click the **Copy Public Key** button.
 16. At the top of the screen, click **Save** to set the configuration.
- You can click the **Delete** button to delete the chosen host key.
- You can click the **Refresh** button to refresh the RSA / DSA host key.

Configuring SSH and RADIUS

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

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

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

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

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

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

Configuring SNMP

Simple Network Management Protocol (SNMP) is a request-response protocol that defines network communication between a managed device and a network management station (NMS).

The following terms will help in understanding SNMP:

- **Managed Device or Agent** – A hardware device with embedded firmware connected to a network with SNMP management capabilities. An example of a managed device/agent is the ION Management Module.
- **Network Management Station (NMS)** – A high-end workstation or computer used by the network administrator to work with and manage various agents around the network.
- **Management Information Base (MIB)** – A set of variables used to monitor and control a managed device.
- **Managed Object or MIB variable** – The individual variables that make up the MIB. These variables are the individual features of the managed device. The administrator can use these variables to monitor and configure the managed device. For example, a slide-in module can have up to 20 or more managed objects (MIB variables) associated with it. Some examples are:
 - Power ON/OFF the card
 - Enable the *AutoCross* feature
 - Display activity on the fiber link, etc.
- **Trap** – A one-way notification from the IONMM to the NMS. Its purpose is to alert the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the Agent rather than the NMS. In order for a management system to understand a trap sent to it by the IONMM, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

See “[Supported MIBs](#)” on page 11 for more information. A more detailed explanation of SNMP is at: <http://www.transition.com/pshelp/snmp.html>.

For information on the traps that the IONMM supports, see “[Appendix G: SNMP Traps Supported](#)” on page 543.

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

Note Regarding SNMPv3 Users vs. Web/CLI Login Users

Note: do not confuse SNMPv3 users with the Web/CLI login users. SNMPv3 user configuration has nothing to do with the WEB/CLI login users. These two type users are different and have different functionalities. The SNMPv3 users are used for SNMPv3 access (for example MGSoft). The Web/CLI login users are used for Web/CLI login when users try to use the ION Web interface or CLI to access the ION system. SNMPv3 users can not use their SNMP login credentials to log in to the ION Web/CLI (and vice-versa). See “Configuring System / Login Users” on page 104 for information on configuring Web/CLI login users.

SNMP Definition and Description

Simple Network Management Protocol (SNMP) is a request-response protocol that defines network communication between a managed device and a network management station (NMS).

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more." It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

An SNMP-managed network consists of three key components:

1. Managed device(s),
2. Agent - software which runs on the managed devices, and
3. Network management system (NMS) - software which runs on the manager.

The following terms will help in understanding SNMP:

- Managed Device or Agent – A hardware device with embedded firmware connected to a network with SNMP management capabilities. An example of a managed device/agent is the NID.
- Network Management Station (NMS) – A high-end workstation or computer used by a network administrator to work with and manage various agents around the network.
- Management Information Base (MIB) – A set of variables used to monitor and control a managed device.
- Managed Object or MIB variable – The individual variables that make up the MIB. These variables are the individual features of the managed device. The administrator can use these variables to monitor and configure the managed device. For example, a slide-in module can have up to 20 or more managed objects (MIB variables) associated with it. Some examples are:
 - Power ON/OFF the card,
 - Enable the *AutoCross* feature,
 - Display activity on the fiber link, etc.

- Trap – A one-way notification from the NID to the NMS. Its purpose is to alert the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the Agent rather than the NMS. In order for a management system to understand a trap sent to it by the NID, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

For a detailed explanation of SNMP see <http://www.transition.com/pshelp/snmp.html>.

An ION NID can act as an agent in an SNMP environment, enabling the NID to notify the management station (PC) of significant events within the network. Notification is accomplished through traps, which are unsolicited messages sent to the management station in response to certain events that have taken place (e.g., cold start, etc.).

Management Information Base (MIB)

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

MIBs use the notation defined by ASN.1; for example:

1.3.6.1.4.1.868 Transition Network private MIB root OID

A MIB Example - ionDevSysCfgTable

A sample MIB tree is shown below.

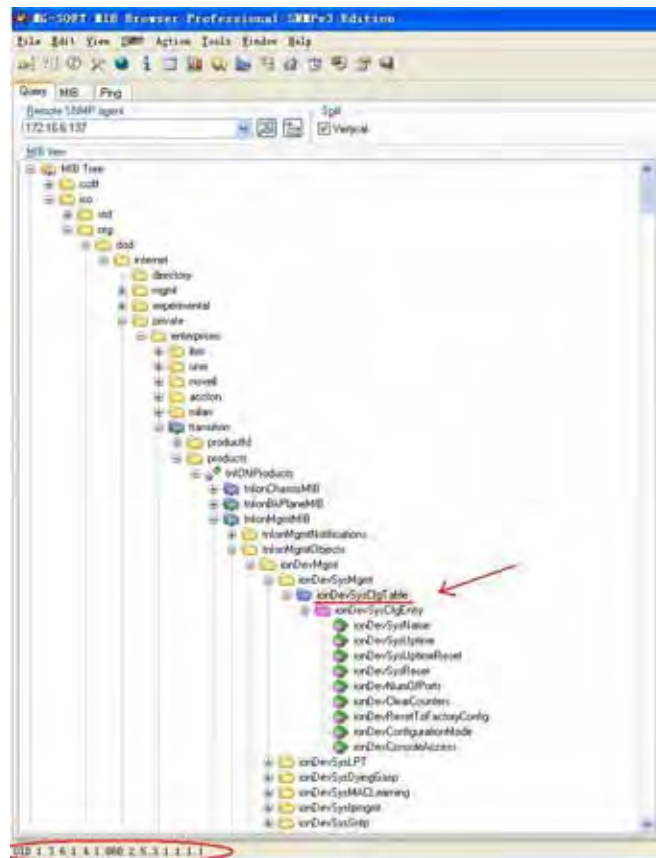


Figure 29. MIB Example

SNMP PDUs

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The SNMP agent may generate notifications from any available port.

SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs, GetBulkRequest and InformRequest were added in SNMPv2 and carried over to SNMPv3.

SNMP PDUs are constructed as follows:

IP header	UDP header	version	community	PDU-type	request-id	error-status	error-index	variable bindings
-----------	------------	---------	-----------	----------	------------	--------------	-------------	-------------------

Figure 30. SNMP PDU Format

The seven SNMP protocol data units (PDUs) are:

- GetRequest
- SetRequest
- GetNextRequest
- GetBulkRequest (Only v2 and v3)
- Response
- Trap
- InformRequest (SNMP v2 and v3 only)

Each of the seven SNMP PDUs is described below.

GetRequest: A manager-to-agent request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A Response with current values is returned.

SetRequest: A manager-to-agent request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A Response with (current) new values for the variables is returned.

GetNextRequest: A manager-to-agent request to discover available variables and their values. Returns a Response with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of GetNextRequest starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

GetBulkRequest: Optimized version of GetNextRequest. A manager-to-agent request for multiple iterations of GetNextRequest. Returns a Response with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific non-repeaters and max-repetitions fields are used to control response behavior. GetBulkRequest was introduced in SNMPv2.

Response: Returns variable bindings and acknowledgement from agent to manager for GetRequest, SetRequest, GetNextRequest, GetBulkRequest and InformRequest. Error reporting is provided by error-status and error-index fields. Although it was used as a response to both gets and sets, this PDU was called GetResponse in SNMPv1.

Trap: Asynchronous notification from agent to manager. Includes current sysUpTime value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.

InformRequest: An acknowledged asynchronous notification from manager to manager. This PDU uses the same format as the SNMPv2 version of Trap. Manager-to-manager notifications were already possible in SNMPv1 (using a Trap), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a Trap was not guaranteed. InformRequest fixes this by sending back an acknowledgement on receipt. Receiver replies with Response parroting all information in the InformRequest. This PDU was introduced in SNMPv2.

SNMP Version v1, v2c, v3 Considerations

1. SNMPv3 provides secure access to the ION system by a combination of authenticating and encrypting packets over the network. With the SNMPv3 feature, users can enable SNMPv1/v2c or SNMPv3 access to ION system as follows:

SNMP Access	How To Configure	Description
SNMP v1/v2c only	<ul style="list-style-type: none"> • Add SNMPv1/v2c community strings. • Remove all SNMPv3 users. 	Only allow SNMPv1/v2c access to ION system though community strings.
SNMPv3 only	<ul style="list-style-type: none"> • Remove all SNMPv1/v2c community strings. • Add SNMPv3 users, assign the users to groups, enable the groups to have access to views, add views to have access to MIBs. 	Only allow SNMPv3 access to ION system though SNMPv3 users.
SNMPv1/v2c/v3	<ul style="list-style-type: none"> • Add SNMPv1/v2c community strings • Add SNMPv3 users, assign the users to groups, enable the groups to have access to views, add views to have access to MIBs. 	Allow SNMPv1/v2 access to ION system though community strings. Also allow SNMPv3 access to ION system though SNMPv3 users.

2. You can configure the SNMPv1/v2c write community string and read only community string. SNMPv1 and v2c share the same community strings.
3. You can set the local SNMPv3 engine ID in the **SNMP > GENERAL** tab. An SNMPv3 engine is an independent SNMP agent that resides on the IONMM. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

A local engine ID is automatically generated that is unique to the IONMM. The input engine ID is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users are cleared, and you must reconfigure all existing users.

A new engine ID can be specified by entering 9 to 64 hexadecimal characters. An engineID can not be empty. At default the SNMPv3 engine ID string of an IONMM is “80 00 03 64 03 00 c0 f2 xx xx xx” (“03 64” is the enterprise number of Transition Networks; “00 c0 f2 xx xx xx” is the MAC address of an ION device). In other words, the default IONMM SNMPv3 engine ID string is: *the MAC address of the IONMM + 'Transition Networks'*.

The engine ID is specified by hexadecimal characters. Each two input characters correspond to one octet character. For engine ID “80 00 03 64 03 00 c0 f2 00 01 02”, the first two characters ‘80’ correspond to the first octet character ‘\128’ with ASCII value of 128 (8*16 + 0 = 128).

The second two characters “00” correspond to the second octet character ‘\0’ with ASCII value of 0 (0*16 + 0 = 0).

SNMP v1, v2c, v3 Descriptions

Each SNMP version is described below.

SNMPv1

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used and is the de facto network-management protocol in the Internet community.

The first RFCs for SNMP, now known as SNMPv1, appeared in 1988: RFC 1065, RFC 1066, and RFC 1067. These protocols were obsoleted by SNMPv1: RFC 1155, RFC 1156 and RFC 1157. After a short time, RFC 1156 (MIB-1) was replaced by more often used

RFC 1213 - Version 2 of management information base (MIB-2) for network management of TCP/IP-based internets

SNMPv1 was criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext. The '80s design of SNMP V1 was done by a group of collaborators who viewed the officially sponsored OSI/IETF/NSF (National Science Foundation) effort (HEMS/CMIS/CMIP) as both unimplementable in the computing platforms of the time as well as potentially unworkable. SNMP was approved based on the belief that it was an interim protocol needed for taking steps towards large scale deployment of the Internet and its commercialization. In that time period Internet-standard authentication/security was considered a dream and was discouraged by focused protocol design groups.

SNMPv2 and v2c

SNMPv2 (RFC 1441–RFC 1452) revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced GetBulkRequest, an alternative to iterative GetNextRequests for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMPv2, viewed by many as overly complex, was not widely accepted.

Community-Based Simple Network Management Protocol version 2, or SNMPv2c, is defined in RFC 1901–RFC 1908. In its initial stages, this was also informally known as SNMPv1.5. SNMPv2c comprises SNMPv2 without the controversial new SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1. While officially only a "Draft Standard", this is widely considered the de facto SNMPv2 standard.

User-Based Simple Network Management Protocol version 2, or SNMPv2u, is defined in RFC 1909–RFC 1910. This is a compromise that attempts to offer greater security than SNMPv1, but without incurring the high complexity of SNMPv2. A variant of this was commercialized as SNMP v2*, and the mechanism was eventually adopted as one of two security frameworks in SNMP v3.

Section 4: Configuration

SNMPv3

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.

SNMPv3 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.

Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.

Authentication - to verify that the message is from a valid source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combined security model / security level determines which security mechanism is used when handling an SNMP packet. Three security models are available: SNMPv1, v2c, and v3. The table below shows the combinations of security models / levels.

Table 19. SNMPv3 Private MIB Levels / Auth / Encryption

Model	Level	Authentication	Encryption	Results
v1	noAuthNoPriv	Community String	None	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	None	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	None	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	None	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES/AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES/AES encryption in addition to authentication based on the DES/AES standard.

SNMPv3 Summary and Key Features

SNMPv3 includes the following key features:

- SNMPv3 EngineID
- SNMPv3 USM
- SNMP VACM
- SNMP Trap/Inform (v1/v2c/v3 trap, v2c/v3 inform)

SNMPv3 Services Provided

The SNMPv3 function supports these services:

- SNMP v3 user management, authentication and encryption.
- SNMP VACM management.
- SNMP v1/v2c/v3 selection.
- SNMP notification (v1/v2c/v3 trap, v2c/v3 inform) functionality.

SNMPv3 features can be configured via the Web interface, CLI, Telnet, or SSH. The SNMPv3 configuration can be backed up and restored. These services are further detailed below.

Table 20: SNMPv3 Services

No.	Function	Description	Reference
1	SNMP v3 USM	SNMP v3 User-based Security Model.	RFC 3414
2	SNMP VACM	SNMP View-based Access Control Model.	RFC 3415
3	SNMP v1/v2c/v3 version selection	SNMP v1/v2c/v3 version selection	Private MIB
4	SNMP v1/v2c/v3 Trap	SNMP v1/v2c/v3 Trap functionality	Private MIB
5	SNMP v1/v2c/v3 Inform	SNMP v1/v2c/v3 Inform functionality	Private MIB
6	Web for SNMP v3	Configure SNMP v3 via Web	None
7	CLI for SNMP v3	Configure SNMP v3 via CLI	None
8	Backup/Restore for SNMP v3	Backup/Restore SNMP v3 configuration.	None

SNMPv3 Public MIBs

Table 21. SNMPv3 Private MIBs

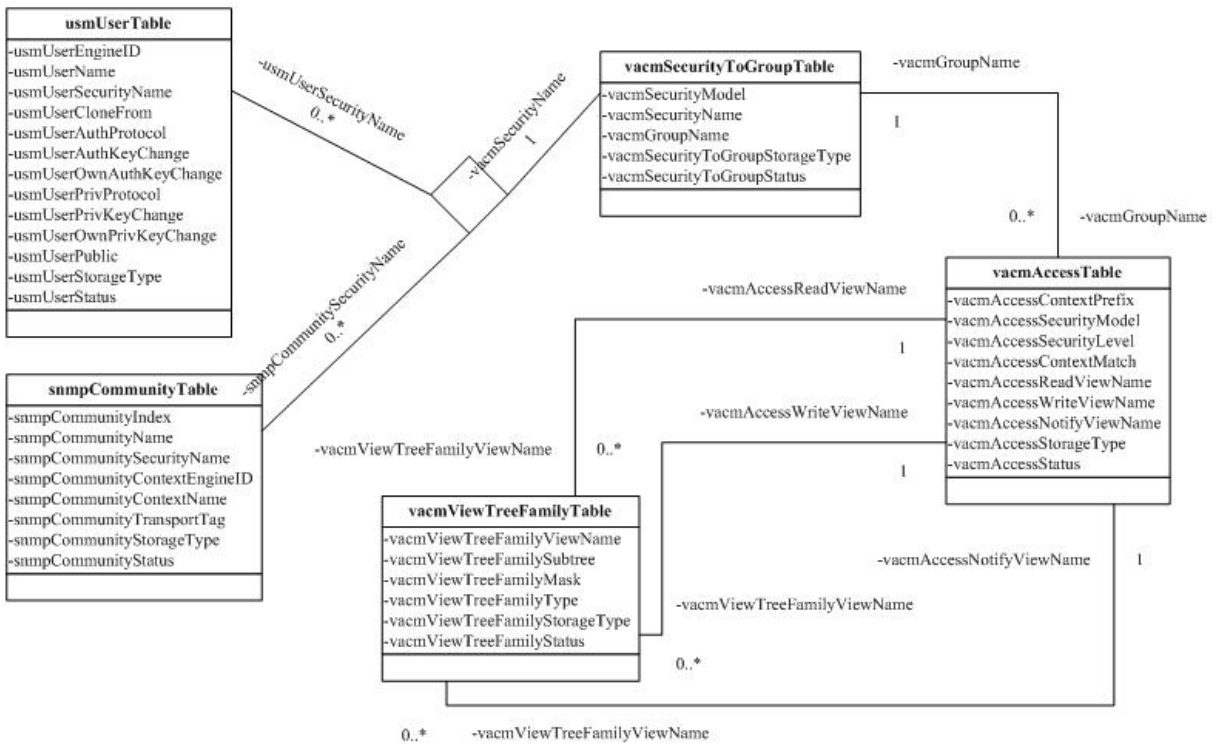
MIB	MIB tables or variables	Function
snmpFrameworkMIB (RFC 3411)	snmpEngine	local SNMPv3 engine information
snmpTargetMIB (RFC 3413)	snmpTargetSpinLock	Lock for modifying the snmpTargetAddrTagList of snmpTargetAddrTable
	snmpTargetAddrTable	SNMP v1/v2c/v3 trap(v2c/v3 inform) host address, udp port number, v2c/v3 inform timeout and retries
	snmpTargetParamsTable	SNMP v1/v2c/v3 trap(v2c/v3 inform) version selection, trap security level, trap community or security name
snmpNotificationMIB (RFC 3413)	snmpNotifyTable	SNMP v2c/v3 trap/inform selection
	snmpNotifyFilterProfileTable	Relate snmpTargetParamsTable with snmpNotifyFilterTable
	snmpNotifyFilterTable	Trap/inform view filtering
snmpUsmMIB (RFC 3414)	usmStats	USM user access error statistic
	usmUserSpinLock	Lock for altering the secrets of usmUserTable
	usmUserTable	USM user management table
snmpVacmMIB (RFC 3415)	vacmContextTable	The table of locally available contexts
	vacmSecurityToGroupTable	Mapping USM user or v1/v2c community string to group
	vacmAccessTable	Group access rights to view
	vacmViewSpinLock	Lock for creating and modifying views
	vacmViewTreeFamilyTable	View to OID tree management table
snmpCommunityMIB (RFC 3584)	snmpCommunityTable	Multiple v1/v2c community string management table

SNMPv3 Private MIBs

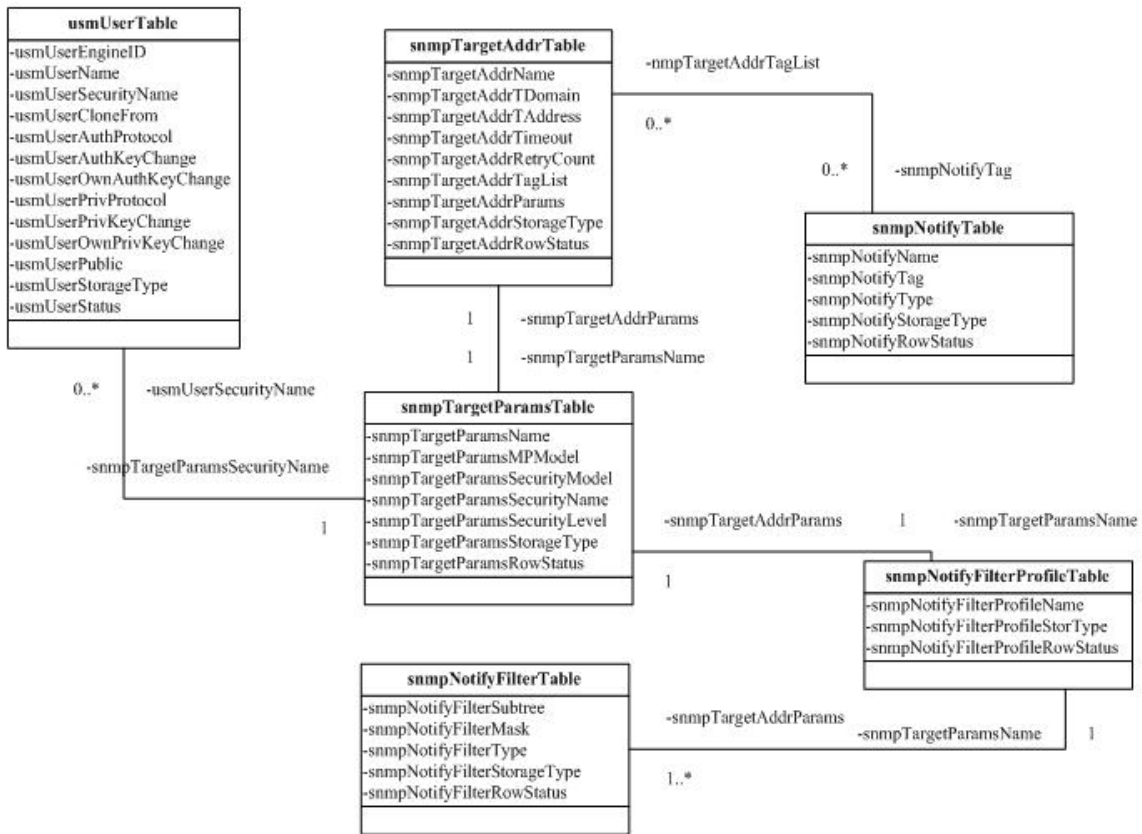
Table 22. SNMPv3 Private MIBs

MIB	MIB tables or variables	Function
ionDevSysSnmprgmt	ionDevSysSnmplocal	Modify the local engineID
	ionDevSysSnmprmgmtTrapManagerTable	Maintain the mapping from SNMPv3 trap hosts to their engine IDs.

SNMP v3 MIB Relationships



Section 4: Configuration



Examples of SNMP v3 private MIB objects trees are shown in the figures below.



Figure 31. SNMP v3 MIBs



Figure 32. SNMP v3 Trap-Inform MIBs

SNMP v3 EngineID Concept

An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity which contains it. The SNMP v3 engine contains:

- a Dispatcher
- a Message Processing Subsystem
- a Security Subsystem, and
- an Access Control Subsystem.

Within an administrative domain, an snmpEngineID is the unique and unambiguous identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, it also uniquely and unambiguously identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for snmpEngineID. Federation of administrative domains may necessitate assignment of new values.

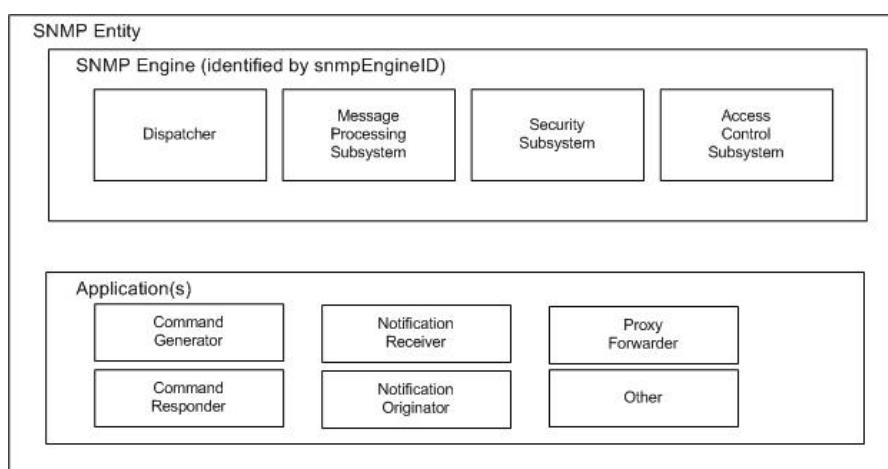


Figure 33. SNMP v3 Entity / Engine / Applications

Local engineID:

- The engineID for the local SNMP engine.
- The engineID for the SNMP engine residing in the managed IONMM or standalone S2x2x/S3x2x/S3240.

Remote engineID:

- The engineID for a remote SNMP engine.
- In the ION system, the remote engineID is only used to configure the engineID of the remote SNMPv3 inform receipt server.

RFC standard: RFC 3411.

SNMPv3 EngineID MIBs

Public MIB for engineID: snmpEngine

- OID is 1.3.6.1.6.3.10.2.1
- For local engineID
- Read-only

Private MIB for local engineID:

- OID is 1.3.6.1.4.1.868.2.5.3.1.1.14.3.1
- Read-write
- Used to modify the local engineID.
- When modifying the local engineID, all the local SNMPv3 USM users will be deleted.

Private MIB for remote engineID:

- OID is 1.3.6.1.4.1.868.2.5.3.1.1.14.4.1
- Read-write
- The combination of *ionDevSysSnmpTrapManagerAddrTDomain* and *ionDevSysSnmpTrapManagerAddrTAddress* must be unique.
- The engineID in this table must be unique (it can not be the same as the local engineID).
- Used to add/delete remote engineIDs.
- When deleting a remote engineID, all the SNMPv3 USM users belonging to the SNMP engine will be deleted.

You must add a remote engine before you can add remote users for this engine.

SNMPv3 USM (User-Based Security Model)

The ION SNMP v3 implementation uses the traditional concept of a user (identified by a *userName*) with associated security information. This is a key SNMPv3 security feature implemented per RFC 3414.

SNMP v3 USM Service: USM provides the following security service:

- Data Integrity is the provision of the property that data has not been altered or destroyed in an unauthorized manner, nor have data sequences been altered to an extent greater than can occur non-maliciously.
- Data Origin Authentication is the provision of the property that the claimed identity of the user on whose behalf received data was originated is corroborated.
- Data Confidentiality is the provision of the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Message timeliness and limited replay protection is the provision of the property that a message whose generation time is outside of a specified time window is not accepted. Note that message reordering is not dealt with and can occur in normal conditions too.

SNMP v3USM User: Management operations using this Security Model make use of a defined set of user identities. For any user on whose behalf management operations are authorized at a particular SNMP engine, that SNMP engine must have knowledge of that user. An SNMP engine that wishes to communicate with another SNMP engine must also have knowledge of a user known to that engine, including knowledge of the applicable attributes of that user.

SNMPv3 USM User and SNMP Engine

- A USM user must belong to a SNMP engine.
- You must add a remote engine before you can add remote users for this engine.
- If a user belongs to the local SNMP engine, it is called a local USM user.
- If a user belongs to a remote SNMP engine, it is called a remote USM user.
- If an engineID of a SNMP engine is changed or deleted, its USM users are deleted.

Section 4: Configuration

SNMPv3 USM MIB

Public MIB for USM: usmUser

- OID is 1.3.6.1.6.3.15.1.2
- Used to add/modify/delete USM users
- Store information for both local USM users and remote USM users

SNMPv3 VACM (View-based Access Control Model)

The View-based Access Control Model defines a set of services that an application (such as a Command Responder or a Notification Originator application) can use for checking access rights.

Access Control occurs (either implicitly or explicitly) in an SNMP entity when processing SNMP retrieval or modification request messages from an SNMP entity.

Access Control also occurs in an SNMP entity when an SNMP notification message is generated (by a Notification Originator application).

VACM includes these elements:

- Groups
- SecurityLevel
- Contexts
- MIB Views and View Families
- Access Policy

SNMPv3 USM – VACM MIBs

Public MIB for VACM: snmpVacmMIB

- OID is 1.3.6.1.6.3.16
- Used to manage VACM configurations including the mapping from user to groups, groups access, view table.
- RFC 3415

Table 23: SNMP v3 Default Values

snmpVacmMIB (RFC 3415)	vacmContextTable	The table of locally available contexts.
	vacmSecurityToGroup Table	Mapping USM user or v1/v2c community string to Group.
	vacmAccess Table	Group access right to View
	vacmViewSpinLock	Lock for creating and modifying Views.
	vacmViewTree Family Table	View to OID tree management table.

SNMPv3 VACM – Groups

A Group is a set of zero or more *<securityModel, securityName>* tuples on whose behalf SNMP management objects can be accessed. A Group defines the access rights afforded to all securityNames which belong to that group. The combination of a *securityModel* and a securityName maps to at most one Group. A Group is identified by a *groupName*.

The Access Control module assumes that the *securityName* has already been authenticated as needed and provides no further authentication of its own.

The View-based Access Control Model uses the *securityModel* and the *securityName* as inputs to the Access Control module when called to check for access rights. It determines the *groupName* as a function of *securityModel* and *securityName*.

Note that when the security model is v1 or v2c, the groups "public" and "private" can not be removed, but when the security model is v3 the groups "public" and "private" can be removed.

SNMPv3 VACM – Views

Views are used to restrict the access rights of some groups to only a subset of the management information in the management domain.

A view subtree is the set of all MIB object instances which have a common ASN.1 OBJECT IDENTIFIER prefix to their names.

A family of view subtrees is a pairing of an OBJECT IDENTIFIER value (called the family name) with a bit string value (called the family mask). The family mask indicates which sub-identifiers of the associated family name are significant to the family's definition.

SNMPv3 Traps and Informs

A **Trap** is an SNMP message sent from one application to another (which is typically on a remote host). Their purpose is merely to notify the other application that something has happened, has been noticed, etc. The big problem with Traps is that they're unacknowledged, so you don't actually know if the remote application received your -important message. The trap is available for SNMP v1, v2c and v3.

An **Inform** is an acknowledged Trap. When the remote application receives an inform it sends back an acknowledgement message. Inform is available for SNMP v2c and v3. For SNMP v3, an inform must be sent to a specific remote USM user resided in the inform receiver.

SNMPv3 Trap/Inform MIBs

- Public MIB for trap/inform: *snmpTargetMIB* and *snmpNotificationMIB*
- OIDs are 1.3.6.1.6.3.12 and 1.3.6.1.6.3.13
- Used to manage trap/inform server configuration.
- RFC 3413

Table 24: SNMP v3 Trap and Inform MIBs

snmpTargetMIB (RFC 3413)	snmpTargetSpinLock	Lock for modifying the snmpTargetAddr TagList of snmpTargetAddrTable.
	snmpTargetAddrTable	SNMP v1/v2c/v3 trap(v1/v2c/v3 inform) host address, udp port #, v2c/v3 inform timeout & retries.
	snmpTargetParamsTable	SNMP v1/v2c/v3 trap(v1/v2c/v3 inform) version selection, trap security level, trap community or security name.
snmpNotificationMIB (RFC 3413)	snmpNotifyTable	SNMP v2c/v3 trap/inform selection.
	snmpNotifyFilterProfileTable	Relate snmpTargetParamsTable with snmpNotifyFilterTable.
	snmpNotifyFilterTable	Trap/inform view filtering.

The MIB tables used for each tab are shown in the table below. Some MIB tables are used in several tabs.

Table 25: Web Interface Tabs to MIB Tables Mapping

Tab	sub-tab	Used MIB tables
SNMP	General	snmpCommunityTable vacmSecurityToGroupTable ionDevSysSnmpLocal(private)
	Users	usmUserSpinLock usmUserTable vacmSecurityToGroupTable vacmAccessTable
	Groups	vacmAccessTable vacmViewTreeFamilyTable
	Views	vacmViewSpinLock vacmViewTreeFamilyTable
	Trap hosts	snmpTargetSpinLock snmpTargetAddrTable snmpTargetParamsTable snmpNotifyTable
	Remote Users	ionDevSysSnmpTrapManagerTable(private) usmUserSpinLock usmUserTable
USERS		ionDevSysUserTable

ION System SNMP Support

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

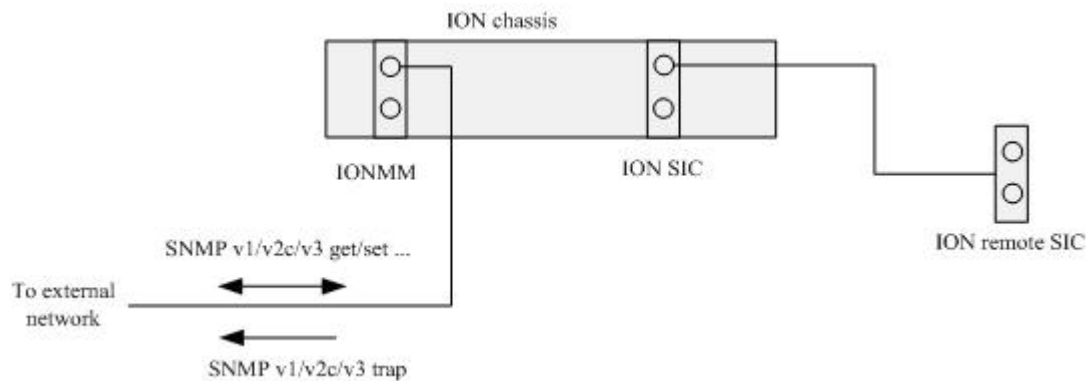


Figure 34: ION System Managed via SNMP

The ION system provides several interfaces (Web /CLI/Telnet/SSH) to configure the SNMPv3 features for the IONMM. The IONMM can backup and restore SNMPv3 configurations for the IONMM when doing a backup or restore operation.

SNMP Command Line Interface (CLI) Support

The SNMP Command Line Interface (CLI) is implemented with device-level and port-level CLI commands.

SNMP v3 Users, Groups, and Views Configuration

SNMP v3 configuration involves setting up SNMP v3 Users, Groups, and Views, with the caveats discussed below.

With SNMPv3, you can define SNMP users, groups, and views to provide access control to SNMP devices, and restrict certain users so they can only access the parts of the MIB that they have been given access rights to. The SNMP views, groups and users are described below.

Note: the concept of SNMP communities that was introduced in SNMPv2 is not relevant to SNMPv3, and has been replaced by SNMP groups/users. However, you can configure an ION system NID to respond to both SNMPv2 and SNMPv3 commands. If both SNMPv2 and SNMPv3 are to be used, you must configure SNMP communities and SNMP groups and users. To use SNMPv1/v2c, all you need to do is add a Community at **IONMM > SNMP > General** tab; no thing else needs to be configured. You can add or delete any Communities including the default communities.

SNMP Users have a specified username, authentication password, privacy password, (if required) and authentication and privacy algorithms assigned. The authentication algorithm options are none, MD5, or

SHA. The privacy algorithm options are none, AES, or DES. When a new User is created, it is associated with an SNMP group. (MD5 is Message Digest Algorithm version 5, SHA is the Secure Hash Algorithm, DES is the Data Encryption Standard, and AES is the Advanced Encryption Standard.)

SNMP Groups are basically access control policies to which users can be added. Each SNMP Group is configured with a security level, and is associated with an SNMP View. These parameters specify the type of authentication and privacy a user within the SNMP group will use, and also which objects in the MIB the User can access. Each SNMP Group name and security level pair must be unique within the device.

SNMP MIB Views are defined lists of objects within a MIB that can be used to control which parts of a MIB can be accessed by Users belonging to the SNMP Group associated with that particular View. Objects in the View may be from anywhere in the MIB, and are not required to be in the same MIB subtree. When you have defined your Views, you must configure for your SNMP Groups the type of access Users will have to those Views. There are three possible types of access configurable, and at least one must be configured in order for Users in that SNMP Group to have access to an SNMP View.

The three types of access that you can configure are 1. ReadView specifies the SNMP View to which the Group has read access, 2. WriteView specifies the SNMP View to which the group has write access, and 3. NotifyView specifies the SNMP View for which the group will receive notifications. **Views:** one default View (defaultview) exists which can not be modified or deleted. You can configure an SNMP v3 Group with read access to one SNMP View, and write access to a different SNMP View.

Summary: You can create multiple Views. You can then create multiple Groups, and associate them with a View. You can configure multiple Groups (each with a different Group name and security level) and associate them with a particular View. You can also configure more than one View associated with a Group (e.g., a Group with read access to the entire MIB tree, but with only write access to certain objects). You could then create multiple Users, and associate them with a Group (you can associate multiple Users with a particular Group).

With SNMPv3 you can define SNMP views, groups and users to provide access control to SNMP devices, as shown below.

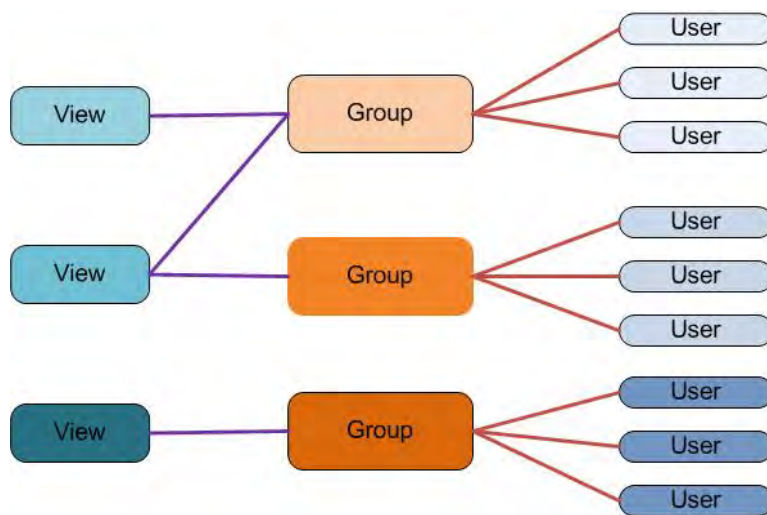


Figure 35 .SNMP v3 Users, Groups, and Views

Section 4: Configuration

You can create multiple Views. You can then create multiple Groups, and associate them with a View. You can configure multiple Groups (each with a different Group name and security level) and associate them with a particular View. You can also configure more than one View associated with a Group (e.g., a Group with read access to the entire MIB tree, but with only write access to certain objects). You could then create multiple Users, and associate them with a Group (you can associate multiple Users with a particular Group).

Configuring SNMP v3 Users

With the introduction of USM and SNMP VACM in SNMPv3 comes the ability to manage the SNMPv3 users. SNMPv3 users are configured as follows:

- The user levels (admin/read-write/read-only) which is described in the USERS tab section are used for Web/CLI login user. There is no level definition for SNMPv3 users. At default there are no SNMPv3 users.
- SNMPv3 users can not log in to the ION system via Web/CLI. Users must log in via the Web/CLI USERS path, not the SNMPv3 Users path.
- If the RADIUS client is enabled, all login is through the RADIUS server (via the Web interface or the CLI). Any user that logs in successfully via RADIUS is treated as a super user.

Configuring SNMP v3 Groups

With the introduction of SNMPv3 users comes the ability to manage groups of SNMP v3 users. An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read, write, and notify views.

An SNMPv3 user must belong to a SNMPv3 group. There are four default groups. The default group is defined for the super 'ION' user. The Public group and the Private group are used by SNMP v1/v2c community strings.

The four default group entries are:

Public Group:

- Public v1: this entry has SNMPv1 read access to the default view.
- Public v2c: this entry has SNMPv2c read access to the default view.

Private Group:

- Private v1: this entry has SNMPv1 read and write access to the default view.
- Private v2c: this entry has SNMPv2c read and write access to the default view.

These groups can not be deleted or modified.

Configuring SNMP v3 Views

With the introduction of SNMPv3 users and groups comes the ability to manage SNMP v3 users' views.

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The default view includes access to the entire MIB tree. This default view can not be deleted or modified.

SNMP v3 Limitations

No Space Characters Allowed: The Community string, Local user name, Group name, View name, Remote user name, Authentication password, and Privacy password can include any combination of characters except the "space" characters. If you enter a "space" character in these fields (via CLI or Web interface) the messages *"It can be set to any characters combination except the character space."* and "this.pattern is required: /^[\\S]*{1,256}\$/" display. You must then re-enter the command or field without any "space" characters.

Other ION system SNMP v3 limitations are:

- Changing the engine ID will delete all previously configured USM users.
- Changing the remote engine ID will delete all remote users belonged to this engine.
- Trap filtering can only be configured through SNMP interface (not via Web interface or CLI).
- Mapping from SNMPv1/v2c communities to group can only be configured via the SNMP interface; Web interface / CLI only supports configuring two types of SNMP v1/v2c communities: read-only and read-write. These two types of communities will be mapped to the default groups automatically.
- Supports a maximum of six trap hosts.
- Only one local Engine ID can be configured.
- Up to 255 remote Engine IDs can be configured.
- The length range of an Engine ID is from 8 to 64 characters (no space characters).
- Up to 255 SNMPv3 users can be configured
- Up to 255 SNMPv3 remote users can be configured
- Up to 255 SNMPv3 groups can be configured
- Up to 255 SNMPv3 views can be configured
- Up to 255 Communities can be configured.
- The length range of each Community name is from 1 to 32 characters (no space characters).

SNMP and IPv6

With IPv6 support, ION SNMP support includes the following IPv6 functions:

- If IPv6 is enabled, the SNMPv1/v2c communities can be used to do get/set operations though either the IPv4 address or the IPv6 global address of a device. Up to 16 SNMP communities are supported on one device.
- If IPv6 is enabled, the SNMPv3 USM local users can be used to do get/set operations though either the IPv4 address or the IPv6 global address of a device. The SNMPv3 USM remote users can be configured for either an IPv4 trap host or an IPv6 trap host. Up to 255 USM users (local and remote) are supported on one device.
- The trap host can be either an IPv4 address or an IPv6 address. If IPv6 is enabled and one trap (or inform) is generated, this trap (or inform) can be sent to all the trap servers. If IPv6 is disabled, the traps can not be sent to any IPv6 trap host. Up to 6 trap servers can be supported on one device.

Section 4: Configuration

The maximum number of SNMP group/view/community/local user entries is 255. An error message displays if more than 255 entries are attempted.

The SNMP Community String entry can be any ASCII printable characters except :: and @; otherwise the message "Its value must be ASCII printable characters except \"::\" and \"@\"." displays.

Configuring SNMP

The x323x can act as an agent in an SNMP environment, enabling the IONMM to notify the management station of significant events within the network. Notification is done with traps, which are unsolicited messages sent to the management station in response to certain events that have taken place (e.g., warm start, etc.).

A full SNMP configuration can include:

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

Note:

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

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

SNMP Config – CLI Method

This procedure is for a full SNMP configuration via CLI commands. Not all user applications will require all of the steps below. For a full description of the individual commands see “[SNMP v3 Commands](#)” on page 46.

1. Access the IONMM through either a USB connection (see “[Starting a USB Session](#)” on page 23) or a Telnet session (see “[Starting a Telnet Session](#)” on page 24).

2. Define the General configuration. For example, type:

```
S3230-1040 C0|S0|L1D>add snmp community name xxxxxxxx
    access_mode={read_only|read_write}
S3230-1040 C0|S0|L1D>add snmp remote engine addrtype=ipv4 addr=xx port=xx
    engine_id=xx
S3230-1040 C0|S0|L1D>set snmp local engine=xx
```

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

```
S3230-1040 C0|S0|L1D>add snmp local user name=STR_USR_NAME security-
    level={noAuthNoPriv|authNoPriv|authPriv}
    [auth-protocol={md5|sha} password=STR_AUTH_PASS] [priv-protocol={des|aes}
    password=STR_PRIV_PASS] [group=STR_GRP_NAME]
S3230-1040 C0|S0|L1D>set snmp local user name=xxxx group=xxxx
```

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

```
S3230-1040 C0|S0|L1D>set snmp local user group=xxx
```

5. Define one or more Views. Type **set snmp view name= STR_SNMP_VIEW** and press **Enter**.

6. Define one or more Trap Hosts.

Type **add snmp traphost version=v3 type=ipv4 addr=STR_SVR_ADDR** and press **Enter**.

7. Define one or more Remote Engines. Type **add snmp remote engine addrtype=ipv4 addr=192.168.1.30 port=xx engine_id=xxxxx** and press **Enter**.

8. Define one or more Remote Users by address type. For example, type:

```
S3230-1040 C0|S0|L1D>add snmp remote user name=STR_USR_NAME addrtype=ipv4
    addr=192.168.1.30 port=55 security-level={noAuthNoPriv|authNoPriv|authPriv} auth-
    protocol={md5|sha} password=xxxxxxx priv-protocol={des|aes} password=STR_PRIV_PASS
```

9. Press **Enter**.

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

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

11. Press **Enter**.

Section 4: Configuration

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

```
S3230-1040 C0|S0|L1D>show snmp ?
community
group
local
remote
traphost
view
```

```
S3230-1040 C0|S0|L1D>show snmp community
Community string          Access mode
-----
comm1                     read_write
public                   read_write
private                  read_only
xxxxxxx                  read_only
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|L1D>show snmp group
Name      Security Model  Security Level  Read View  Write View  Notify View
-----
public    v1               noAuthNoPriv   defaultView
public    v2c              noAuthNoPriv   defaultView
private   v1               noAuthNoPriv   defaultView defaultView
private   v2c              noAuthNoPriv   defaultView defaultView
```

```
S3230-1040 C0|S0|L1D>show snmp local engine
Local engine ID:      80.00.03.64.03.00.c0.f2.20.de.9e (hex)
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|L1D>show snmp local user
User Name  Group Name  Security Model  Security Level  Auth Protocol  Privacy Protocol
-----
BobB      private    v3              authPriv        MD5             DES
TedT      private    v3              noAuthNoPriv
JeffS     private    v3              authPriv        SHA             AES
CarolC    private    v3              authPriv        SHA             AES
GomesD    private    v3              authPriv        SHA             AES
AndersonT private    v3              authNoPriv      SHA
```

```
S3230-1040 C0|S0|L1D>show snmp remote engine
Remote Address      Remote port  Remote Engine ID
192.168.1.20       162         800003640300c0f2209ede
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|L1D>show snmp remote user
User Name  Engine ID  Security Model  Security Level  Auth Protocol  Privacy Protocol
-----
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|L1D>show snmp traphost
Trap version  IP          Port Community/Security name  Security level  Trap/inform Timeout  Retry times
-----
v3            192.168.1.30    162 TrpHstA6                    authPriv       trap
v3            192.168.1.40    162 private                      authNoPriv     trap
v3            192.168.1.50    162 public                       authPriv       trap
v2c           192.168.1.10    162 public                       noAuthNoPriv  inform        1500        3
v1            192.168.1.20    162 public                       noAuthNoPriv  trap
S3230-1040 C0|S0|L1D>
```

```
S3230-1040 C0|S0|L1D>show snmp view
name          OID Sub Tree      type
-----
defaultView   0                    include
defaultView   1                    include
defaultView   2                    include
S3230-1040 C0|S0|L1D>
```

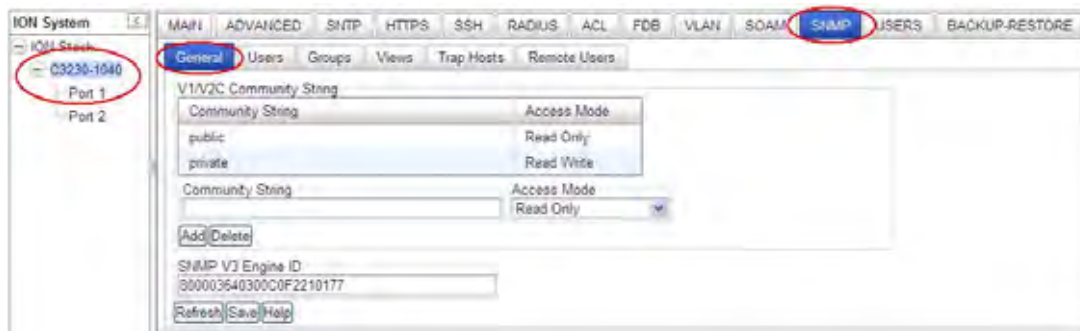
8. Backup the configuration. See “[Backup and Restore Operations \(Provisioning\)](#)” on page 161.

Section 4: Configuration

SNMP Config – Web Method

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

1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 26).
2. Select the **SNMP** tab.
3. Select the **General** sub-tab if not already displayed.



4. Add a new community string as required:

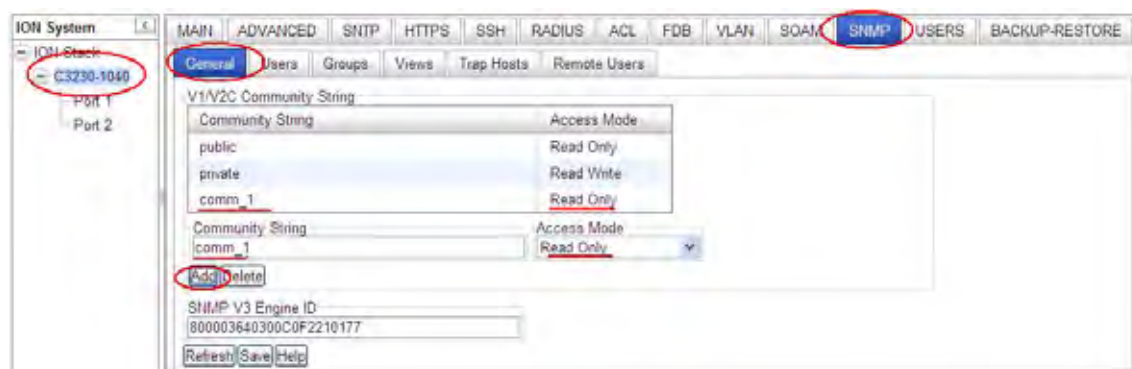
Community String: enter the string to be added (e.g., **comm_1**) from 1-32 alphanumeric characters (no space characters).

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

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

Enter 18-128 characters using the characters a-f, 0-9, and A-F. The total length must be a dual from 18-128.

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



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

7. Select the **Users** sub-tab.



8. Enter the fields as required:

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

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

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

Security Level: The security level used for the user:

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

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

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

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

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

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

Section 4: Configuration

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

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



User Name	Group Name	Security Model	Security Level	Authentication Protocol	Privacy Protocol
Adam	G1V3AuthPrivMD5I	V3	AuthPriv	MD5	DES
JeffS	private2	V3	NoAuthNoPriv	None	None

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



Group Name	Security Model	Security Level	Read View	Write View	Notify View
public	V1	NoAuthNoPriv	defaultView		
public	V2C	NoAuthNoPriv	defaultView		
private	V1	NoAuthNoPriv	defaultView	defaultView	
private	V2C	NoAuthNoPriv	defaultView	defaultView	

- Add and Edit the fields as required:

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

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

Security Level: The security level used for the group:

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

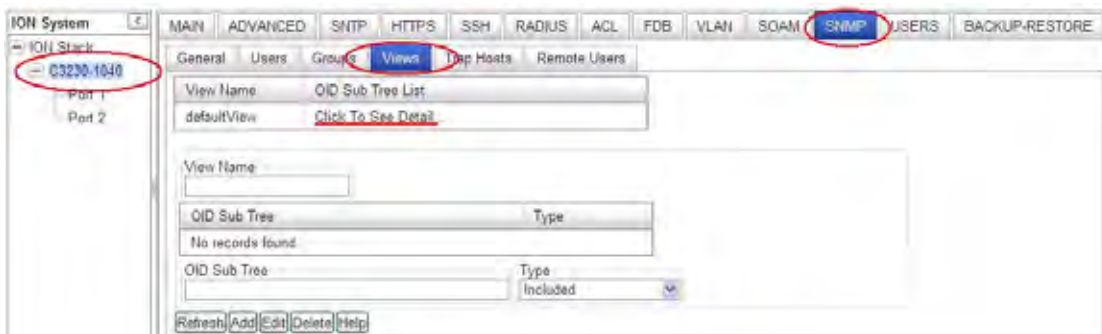
The Group Security Level is the minimum level of security required in order to gain the access rights to the views (read/write/notify). If the User Security Level is less than the Group Security Level, this user will have no access rights to the views. A Security Level of *noAuthNoPriv* is less than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

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

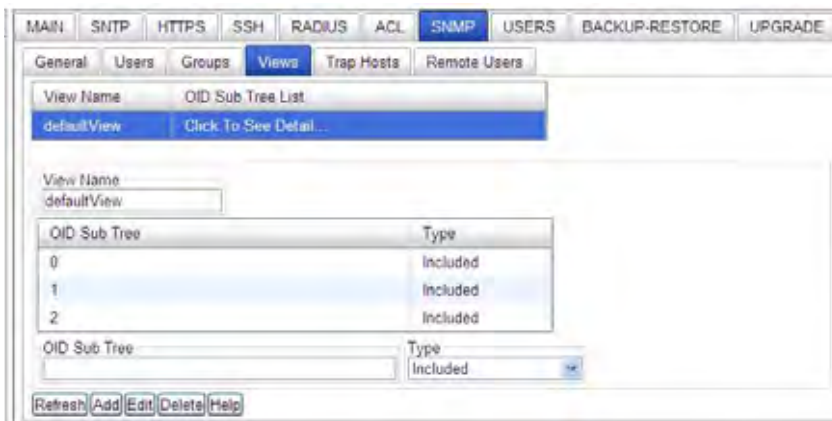
Write View: The configured view for write access. You can leave this view blank (none), or enter a specific view name (1-64 characters, no space characters), or select the **defaultView** radio button. **Note** that an entry here does not mean this view already exists in the view table.

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

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



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



Section 4: Configuration

14. Add / Edit the fields as required:

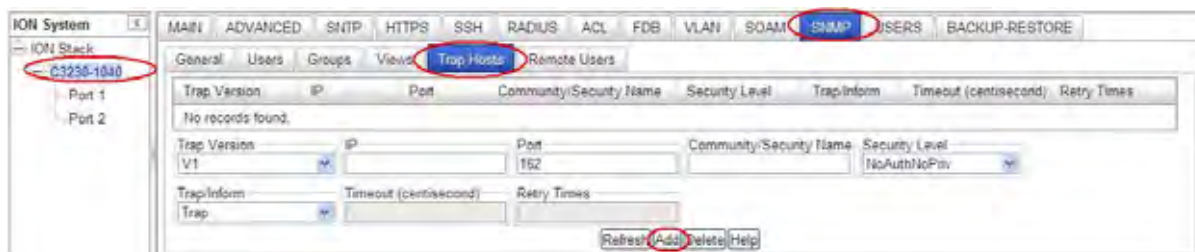
View Name: enter a name (1-64 characters) for this SNMP view (e.g., *Default View*, *Test View* above).

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

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

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

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



16. Add / Edit the fields as required.

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

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

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

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

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

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

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

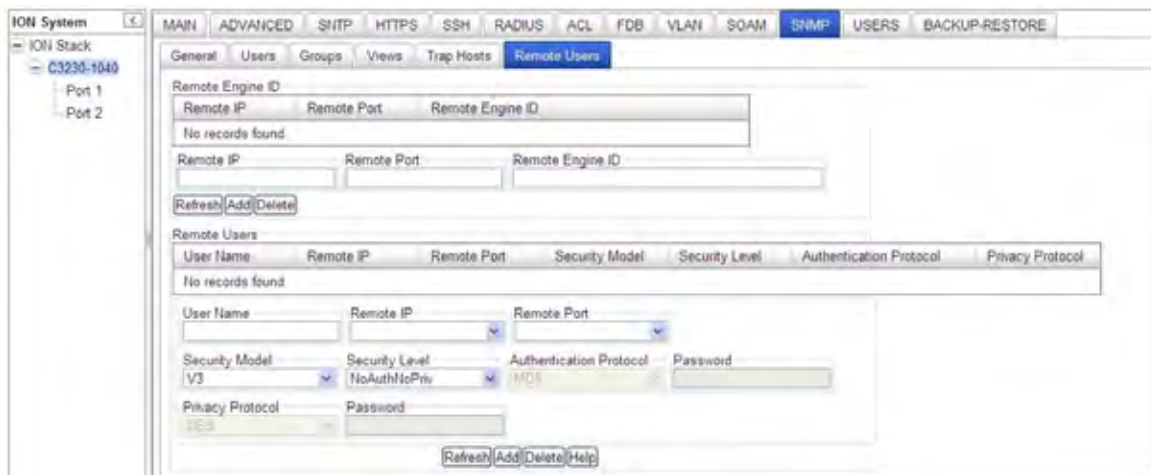
Trap/Inform: When the “Trap Version” of a trap host is “v2c” or “v3”, this field can be used to specify whether notifications are sent either by Trap or by Inform messages.

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

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

17. Verify the table selections and click the **Add** button when done.

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



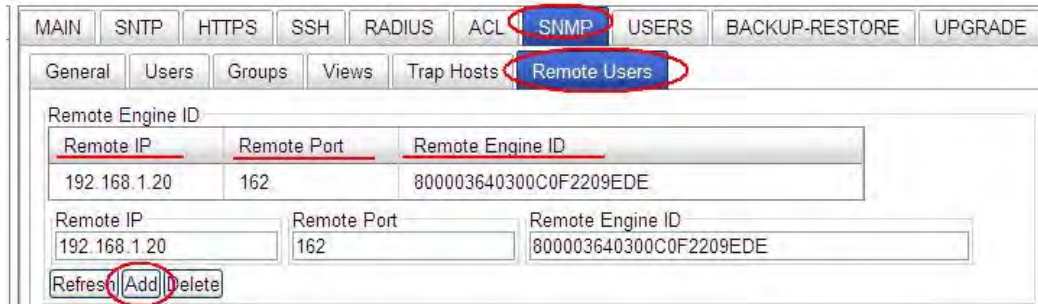
19. Add / Edit the **Remote Engine ID** section fields as required.

Remote IP: enter the trap host IP address of a remote management station to receive notification messages.

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

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

Section 4: Configuration



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

General | Users | Groups | Views | Trap Hosts | **Remote Users**

Remote Engine ID

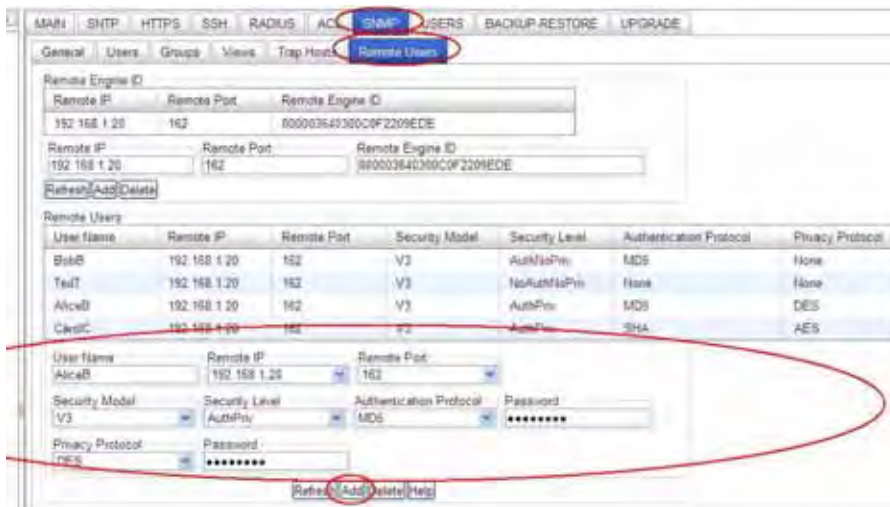
Remote IP	Remote Port	Remote Engine ID
192.168.1.20	162	800003640300C0F2209EDE

Remote IP: 192.168.1.20 | Remote Port: 162 | Remote Engine ID: 800003640300C0F2209EDE

Refresh | **Add** | Delete

20. Click the **Add** button when done.

21. Add / Edit the **Remote Users** section fields as required.



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

General | Users | Groups | Views | Trap Hosts | **Remote Users**

Remote Engine ID

Remote IP	Remote Port	Remote Engine ID
192.168.1.20	162	800003640300C0F2209EDE

Remote IP: 192.168.1.20 | Remote Port: 162 | Remote Engine ID: 800003640300C0F2209EDE

Refresh | Add | Delete

Remote Users

User Name	Remote IP	Remote Port	Security Model	Security Level	Authentication Protocol	Privacy Protocol
BobB	192.168.1.20	162	V3	AuthNoPriv	MD5	None
TedT	192.168.1.20	162	V3	NoAuthNoPriv	None	None
AliceA	192.168.1.20	162	V3	AuthPriv	MD5	DES
CarolC	192.168.1.20	162	V3	AuthPriv	SHA	AES

User Name: AliceB | Remote IP: 192.168.1.20 | Remote Port: 162

Security Model: V3 | Security Level: AuthPriv | Authentication Protocol: MD5 | Password: *****

Privacy Protocol: DES | Password: *****

Refresh | **Add** | Delete | Help

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

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

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

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

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

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

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

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

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

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

22. Verify the Remote Users table selections and click the **Add** button when done.
23. Backup the configuration. See “[Backup and Restore Operations \(Provisioning\)](#)” on page 161.

Section 4: Configuration

Change a SNMP User's Group - Web Method

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

1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 26).
2. Select the **SNMP** tab.
3. In the **Users** sub-tab, select (highlight) an existing user in the table.
4. Enter the new Group name in the **Group Name** field.
5. Click the **Change Group** button.

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

User Name: AndersonT
 Group Name: private
 Security Model: V3
 Security Level: AuthNoPriv
 Authentication Protocol: SHA
 Privacy Protocol: Password

Buttons: Refresh, Add, Delete, Change Group, Help

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

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

User Name: AndersonT
 Group Name: private
 Security Model: V3
 Security Level: AuthNoPriv
 Authentication Protocol: SHA
 Privacy Protocol: Password

Buttons: Refresh, Add, Delete, Change Group, Help

In this example, user “AndersonT” is moved from the Group “comm_1” to the Group “private”.

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

SNMP v3 Default Values

SNMPv3 initializes with the following default values.

Table 26: SNMP v3 Initialization (Default) Values

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

Notes for SNMPv1 and SNMPv2c Users

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

Table 27: SNMP v3 Web Interface Default Values

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

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

SNMP v3 Commands

Command Categories

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

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

SNMP v3 Commands - Alphabetical List

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

Web Interface-to-CLI Command Cross Reference

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

Table 28: Web Interface to CLI Command Cross Reference

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

Section 4: Configuration

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

SNMP CLI Messages

Message:

At most 255 SNMP views can be created!
At most 255 SNMP communities can be created!
At most 255 SNMP groups can be created!
Fail to create SNMP community!
Fail to create SNMP group!
Fail to create SNMP view!

Meaning: You exceeded the SNMP configuration maximum of 255 Communities, Groups, or Views.

Recovery:

1. Verify the limit of 255 SNMP Users, Groups, and Views entries has not been reached.
2. Verify the SNMP Trap hosts and Remote Users tabs parameter settings.
3. See the “[SNMP Web Interface](#)” section on page 27 for more information.

Syslog Messages

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

SNMP Engine ID Length

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

Message:

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

SNMP Web Interface Messages

Message:

community name too long
Couldn't allocate enough memory
example config COMMUNITY not properly configured
example config NETWORK not properly configured
getnameinfo failed
missing CONTEXT_NAME parameter
missing NAME parameter
missing SOURCE parameter
missing COMMUNITY parameter
no IPv6 source address in PDU?
security name too long

Meaning: A problem occurred during SNMP configuration.

Recovery:

1. Verify the SNMP Users, Groups, and Views tabs parameter settings.
2. Verify the SNMP Trap hosts and Remote Users tabs parameter settings.
3. See the “[SNMP Web Interface](#)” section on page 27 for more information.

Configuring VLANs, VLAN Management, and VLAN Tunneling

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Ports on a switch can be grouped into VLANs in order to limit traffic flooding since it is limited to ports belonging to that VLAN and its trunk ports. Any switch port can belong to a VLAN. Packets are forwarded and flooded only to stations in the same VLAN. Each VLAN is a logical network, and packets destined for stations that do not belong to the same VLAN must be forwarded through a routing device. Each VLAN can also run a separate instance of the spanning-tree protocol (STP).

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

Virtual LANs are essentially Layer 2 constructs, whereas IP subnets are Layer 3 constructs. In a campus LAN employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs. Virtual LANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to one another and this correspondence is useful during the network design process.

A virtual LAN (VLAN) is a collection of network nodes that share the same broadcast domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers. This allows users to share information and resources as though located on the same LAN. VLANs also allow a single physical LAN to be divided into multiple logical LANs.

This section covers VLAN and Management VLAN configurations including:

- [Management VLAN Config](#) on page 311
- [VLAN Config – Network Port](#) on page 315
- [VLAN Config – Provider Port](#) on page 319
- [VLAN Config – Customer Port](#) on page 324
- [Configuring VLAN Tunneling \(802.1q Tunneling\)](#) on page 328

Note that the VLAN config and Management VLAN config can be configured together or separately.

Configuring Management VLAN

The Management VLAN is used to separate management traffic from other network traffic to and from the x323x. The Management VLAN is designed to help ensure the security of management control by making sure that equipment not belonging to the Management VLAN does not have access to the management traffic.

When configuring Management VLAN for the x323x, you specify a VLAN ID which is to be used for all management traffic to and from the device. The management station that belongs to that VLAN is the only one able to manage the x323x. This VLAN ID is given to untagged frames on ingress into the x323x. By default it is disabled or zero. When the value is non-zero, the management traffic is expected to be tagged with the management VLAN ID configured when Management VLAN is enabled.

Also when configuring x323x Management VLAN, you can specify whether one or several or all of the ports on the x323x are part of the Management VLAN. Note that you must create the Management VLAN before you create any other VLANs.



Note before performing this configuration: When you specify a Management VLAN, your Web and Telnet interfaces to the x323x are lost, unless the management station (PC) is on the same VLAN. Only management stations in the same VLAN can communicate with the x323x through the network. Enabling a Management VLAN does not disable a USB serial interface to the x323x.

IMPORTANT

- 1) When you specify a Management VLAN, your Web and Telnet interfaces to the x323x are lost, unless the management station is on the same VLAN. Only management stations in the same VLAN will be allowed to communicate with the x323x through the network. If a remote x323x is configured, make sure that the management station/PC is part of the same VLAN as the x323x.
 - 2) A series of messages display after you enable Management VLAN either via the x323x Web interface or the CLI. In both cases, management control is given to the Management VLAN that you enabled. To regain control, turn off Management VLAN via the CLI (**set mgmt vlan state=enable**) or via the Web interface (x323x **MAIN > Management VLAN Configuration > Status = Enabled**).
 - 3) Enabling a Management VLAN does not disable a USB serial interface to the x323x.
 - 4) See [Appendix B](#) for VLAN tab factory default settings.
-

Section 4: Configuration

The following configuration restrictions apply to the x323x Management VLAN feature:

- 1) Management VLAN: a VLAN ID of 2-4094 is valid.
- 2) Management VLAN status can not be changed to “Enabled” when no port members are selected.
- 3) Management VLAN Status “Disabled” means that Management access is allowed on all the ports; the values in Management VLAN ID and port members are ignored (at **Device > Port > ADVANCED** tab > **VLAN Forwarding Rules** section > **VLAN Status** field).
- 4) Management VLAN can be enabled in "Network" mode or "Provider" mode. Before adding the ports for Management VLAN, set the Frame Tag mode of that port to “Network”. When Provider tagging is required in that port, then set the Frame Tag mode to "Provider".
- 5) Port members cannot be checked without first enabling “Network/Provider” mode on those ports (at **Device > Port > ADVANCED** tab > **VLAN Tag Management** section > **Frame Tag Mode** field).
- 6) The card must be in “Network” mode (**Port 1 > Advanced > Frame Tag Mode**) to set the VLAN ID. If it is not set to “Network”, an SNMP error will occur.
- 7) A port with its Frame Tag mode set to "Customer" (default) can not be added to Member Ports for Management VLAN.

The Management VLAN default values for x323x NIDs are:

- VLAN ID: 2
- Port members checked: none
- Status: Disabled

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

Management VLAN Config –CLI Method

1. Access the x323x via either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Check the current Management VLAN configuration. Type `show mgmt vlan config` and press **Enter**.

Note: In the following steps to enable Management VLAN, the first is at the port level, the other steps are at the device level. These steps must be performed in the order shown.

3. Change the Management port from default “Customer” mode to “Network” mode. Type `set port vlan tag mode=network` and press **Enter**.
4. Set this port as Management port. Enter the ports to be associated with this VLAN ID (VID). This sets the device ports which are to be members of this Management VLAN. This is for security, to make some ports non-members, which blocks all management access from this port. If multiple ports are specified, they must be separated by commas with no spaces between the numbers (i.e., `port=1,2,3`).
5. Enable Management VLAN mode. Type `set mgmt vlan state=enable` and press **Enter**.
6. Change the Management VID. Type `set mgmt vlan vid=10` and press **Enter**. This is the VLAN ID number (2–4094). The default is **2**. This sets the VLAN ID which is to be used for all management traffic to and from the device. The management station that belongs to this VLAN is the only one able to manage the x323x. By default the VLAN ID is set to 1 (Management VLAN 1 enabled). When the Management VLAN ID value is not 0 or 1, the Management traffic is expected to be tagged with the Management VLAN ID configured when Management VLAN is enabled.
7. Add a VLAN. Type `add vlan vid=10` and press **Enter**.

Other Management VLAN or Port VLAN attributes could be changed without strict order. For example:

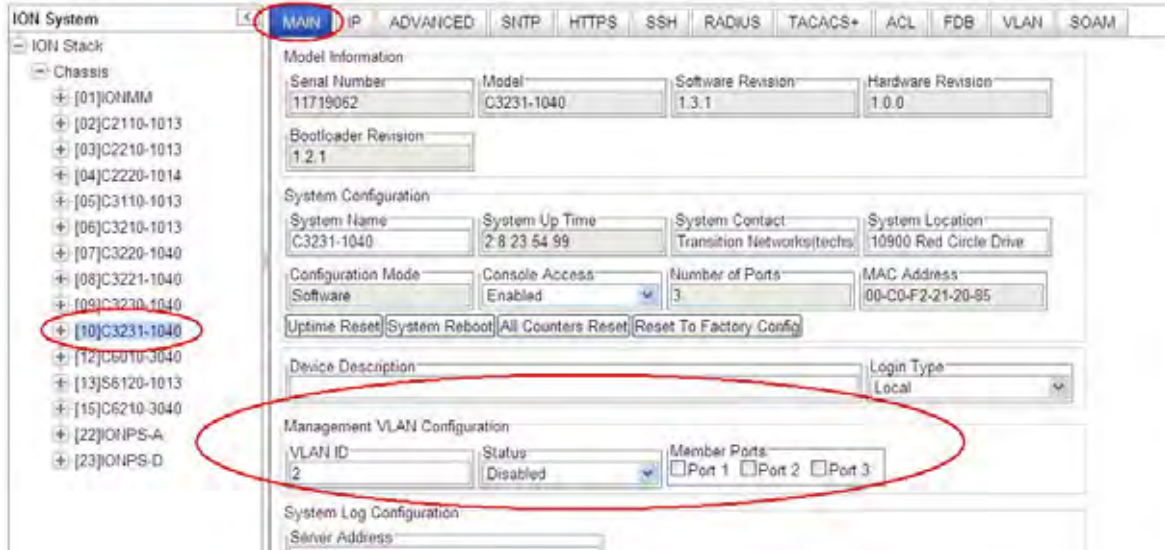
```
C1|S3|L1P1>set port vlan tag mode=network
C1|S3|L1P1>home
C1|S3|L1D>set mgmt vlan port=1
C1|S3|L1D>set mgmt vlan state=enable
C1|S3|L1D>set mgmt vlan vid=10      << to change the Mgmt VID>>
C1|S3|L1D>show mgmt vlan config    <<to verify the port VLAN configuration>>
  vlan id  vlan state      vlan portlist
-----
  2        enable        1
C1|S3|L1D>set port vlan tag mode=network
C1|S3|L1D>set mgmt vlan port=2
C1|S3|L1D>set mgmt vlan state=enable
C1|S3|L1D>set mgmt vlan vid=10
C1|S3|L1D>add vlan vid=10
C1|S3|L1D>show mgmt vlan config
  vlan id  vlan state      vlan portlist
-----
  3        enable        1
C1|S3|L1D>go l1p=1
C1|S3|L1P1>set port default-vid or set port force-default-vid
C1|S3|L1P1>set port=discard-tagged or set port=discard-untagged
```


Section 4: Configuration

```
C1|S3|L1P1>set port mgmtaccess=enable    <<to configure port vlan>>
C1|S3|L1P1>show port vlan config        <<to verify the port VLAN configuration>>
C1|S3|L1P1> go llp=2
C1|S3|L1P1>show port vlan config
Dot1q state:                             vlanEnabled
Discard-tagged:                           false
Discard-untagged:                         false
Default VLAN id:                          5
Force use default VLAN id:                true
C1|S3|L1P1>
```

Management VLAN Config –Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. At the device’s **MAIN** tab, locate the **Management VLAN Configuration** section.



3. In the **VLAN ID** field, enter the **VLAN ID** number. The valid range is from 2–4094. This sets the VLAN ID which is to be used for all management traffic to and from the device.
The management station that belongs to this VLAN is the only one able to manage the x323x. By default the VLAN ID is set to 2. When the value is not 0 or 1, the Management traffic is expected to be tagged with the Management VLAN ID configured when Management VLAN is enabled.
4. In the **Status** field, select **Enabled**. This enables a secure channel for all associated management traffic. The default Status is Disabled.
5. In the **Member Ports** field, select the ports to be associated with this VLAN ID (VID). This sets the ports on this device which are to be members of this Management VLAN. This is for security, as some ports can be made non-members, which blocks all management access from this port. Check the checkbox for ports that you want to be VLAN member ports. The default is all Ports unchecked (not associated with this VID).
6. Click the **Save** button.

Configuring VLANs – Network / Provider / Customer Mode

The following sections document how to configure VLAN network, provider and customer modes via the CLI and Web interface.

VLAN Config – Network Port - CLI Method

Network mode is the normal network operating mode. It can take untagged and 802.3ac tagged frames. In this mode, Management VLAN can be enabled on the interface. Frames with an ethertype of 0x8100 are considered as tagged.

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Check the current VLAN configuration. Type `show vlan config` and press **Enter**.
3. Define VLAN VID 10 port 2 tagging.
Type `set vlan vid=10 port=2 memetag=<noMod|notMember|tag|unTag>` and press **Enter**.
4. Enable or disable VLAN VID 10 Priority Override as desired.
Type `set vlan vid 10 pri-override=<enable|disable>` and press **Enter**.
5. Set the Priority level for VLAN VID 10. Type `set vlan vid 10 priority 2` and press **Enter**.
6. Enable and configure Management VLAN as required; see previous section.
7. Switch to the applicable port. Type `go llp=1` and press **Enter**.
8. Set the port’s VLAN tagging mode to **Network**. Type `set port vlan tag mode=network` and press **Enter**.
9. Verify the VLAN configuration. Type `show vlan config` and press **Enter**.

Configure the x323x and each of the ports as required. An example is provided on the next page.

Example (VLAN Config – Network Port - CLI Method):

The following command sequence places the NID in VLAN 10, creates a Network port, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

```
C1|S3|L1D>set vlan vid 10 port 2 memetag<noMod|notMember|tag|unTag>
C1|S3|L1D>set vlan vid 10 pri-override<enable|disable>
C1|S3|L1D>set vlan vid 10 priority 2
C1|S3|L1D>go llp=1
C1|S3|L1P1>set port vlan tag mode<network>
C1|S3|L1P1>show vlan config
vid:10          fid:0          priority:2      priv_override:disable
port1:         noMod  port2:         Tag
C1|S3|L1P1
```

Enable and configure Management VLAN as required; see previous section.

This procedure places the NID in the VLAN specified, creates a Network port, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

VLAN Config – Network Port - Web Method

Network mode is the normal network operating mode. It can take untagged and 802.3ac tagged frames. In this mode, 802.1q can be enabled on the interface. Frames with an ethertype of 0x8100 are considered as tagged.

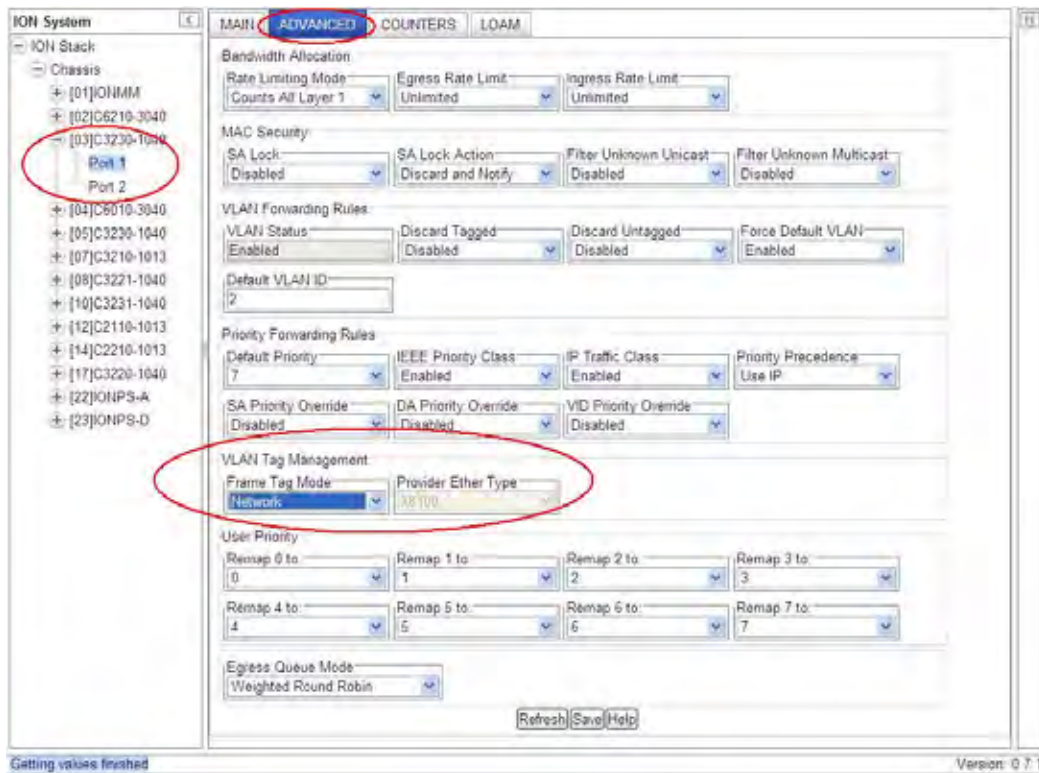
1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Click the **Save** button.
3. Select the desired port’s **ADVANCED** tab.
4. Locate the **VLAN Forwarding Rules** section.



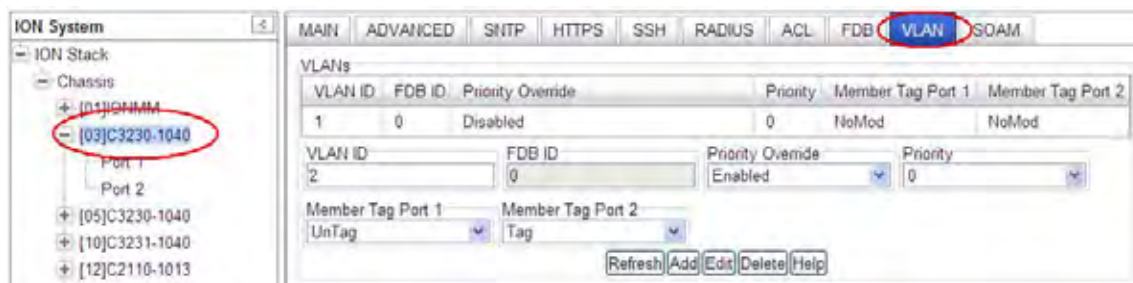
5. For each Port, at the **ADVANCED** tab in the **VLAN Forwarding Rules** section:
 - a) Set **Discard Tagged** to Enabled or Disabled (the default is Disabled).
 - b) Set **Discard Untagged** to Enabled or Disabled (the default is Disabled).
 - c) Set **Force Default VLAN** to Enabled or Disabled (the default is Disabled).
 - d) Set the **Default VLAN ID** to <2-4094>. The default is VID 2.
6. Locate the **VLAN Tag Management** section.

Section 4: Configuration

- For each port, at the **Frame Tag Mode** field, select **Network**.



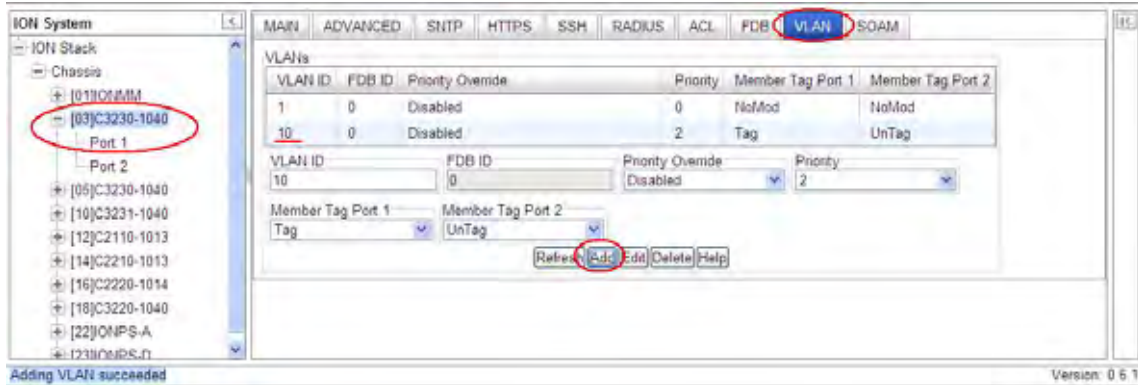
- Note:** Leave the **Provider Ether Type** field at the default setting. The **Provider Ether Type** value has no effect when the port is in **Network** Frame Tag Mode.
- If required, enable and configure **Management VLAN**; see the previous section.
- Select the x323x **VLAN** tab.



- Create VLAN VID 10:
 - In the **VLAN ID** field, enter **10**.
 - At the **Priority Override** dropdown, select **Disabled**.
 - At the **Priority** dropdown, select **2**.

- d) At the **Member Tag Port x** dropdowns, select **NoMod**, **NotMember**, **Tag**, or **UnTag** as the membership / action for this VID. Set each of the ports as not a member of the VLAN, or to either not modify, or add a tag to, or remove the tag from management traffic.

12. Click the **Add** button to add the new VLAN to the VLANs table.



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

Enable and configure Management VLAN as required; see the previous section.

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

VLAN Config – Provider Port – CLI Method

In a VLAN enabled network, you can assign a VLAN as a Management VLAN. The VLAN ID will be used in all management frames. This separates the management traffic from the data.

In Provider mode, frames are considered provider tagged if it matches the 'ProviderEtherType' setting. Frames which are ingress with a provider tag, are stripped of their provider tag on egressing this interface. If the frame's EtherType doesn't match the 'ProviderEtherType' setting, it is considered as untagged.

Use the following steps to configure Management VLAN over S-tag for a Provider port.

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Check the current VLAN configuration. Type `show vlan config` and press **Enter**.
3. Define VLAN VID 10 port 2 tagging.
Type `set vlan vid=10 port=2 memetag=<noMod|notMember|tag|unTag>` and press **Enter**.
4. Enable or disable VLAN VID 10 Priority Override as desired.
Type `set vlan vid 10 pri-override=<enable|disable>` and press **Enter**.
5. Set the Priority level for VLAN VID 10. Type `set vlan vid 10 priority 2` and press **Enter**.
6. Enable Management VLAN. Type `set mgmt vlan state=enable` and press **Enter**.
7. Switch to the applicable port. Type `go 11p=1` and press **Enter**.
8. Set the port's VLAN tagging mode to **Network**. Type `set port vlan tag mode=provider` and press **Enter**.
9. Set the provider port's VLAN tag EtherType.
Type `set port vlan tag provider ethtype=<x8100|x88a8|x9100>` and press **Enter**.
10. Verify the VLAN configuration. Type `show vlan config` and press **Enter**.

Configure the x323x and each of the ports as required. An example is provided on the next page.

Example (VLAN Config – Provider Port - CLI Method):

The following command sequence places the NID in VLAN 10, creates a Provider port, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

```
C1|S3|L1D>set vlan vid 10 port 2 memetag<noMod|notMember|tag|unTag>
C1|S3|L1D>set vlan vid 10 pri-override<enable|disable>
C1|S3|L1D>set vlan vid 10 priority 2
C1|S3|L1D>go llp=1
C1|S3|L1P1>set port vlan tag mode=provider
C1|S3|L1P1>set port vlan tag provider ethtype=<x8100|x88a8|x9100>
C1|S3|L1P1>show vlan config
vid:10      fid:0      priority:2      priv_override:disable
port1:      noMod    port2:         Tag
C1|S3|L1P1>
```

Enable and configure Management VLAN as required; see the previous section.

This procedure places the NID in the VLAN specified, creates a Provider port, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

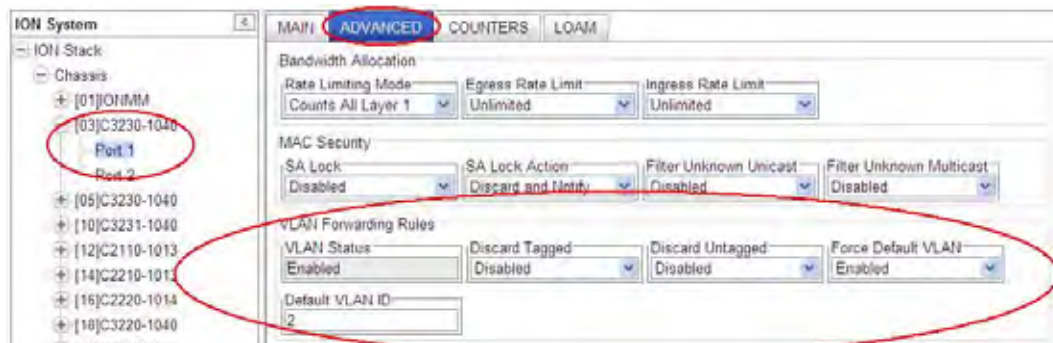
Section 4: Configuration

VLAN Config – Provider Port – Web Method

In a VLAN enabled network, you can assign a VLAN as a Management VLAN. The VLAN ID will be used in all management frames. This separates the management traffic from the data.

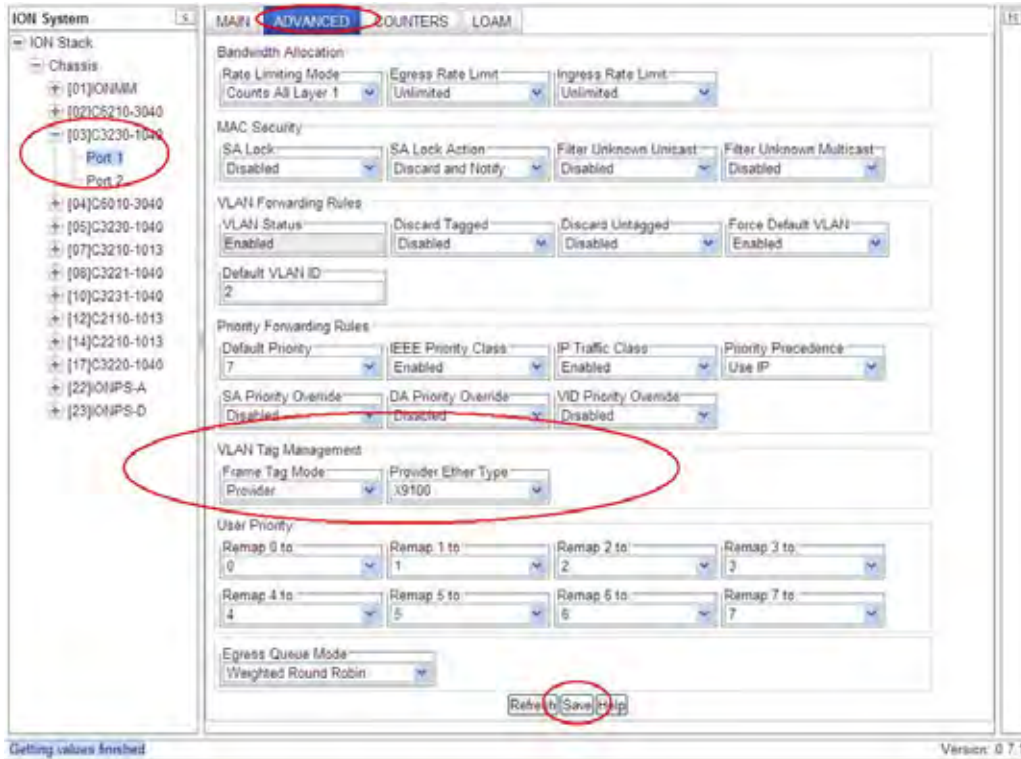
Use the following steps to configure Management VLAN over S-tag.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port’s **ADVANCED** tab.
3. Locate the **VLAN Forwarding Rules** section.



4. For each Port, at the **ADVANCED** tab in the **VLAN Forwarding Rules** section:
 - a) Set **Discard Tagged** to Enabled or Disabled (the default is Disabled).
 - b) Set **Discard Untagged** to Enabled or Disabled (the default is Disabled).
 - c) Set **Force Default VLAN** to Enabled or Disabled (the default is Disabled).
 - d) Set the **Default VLAN ID** to <2-4094>. The default is VID 2.
5. Locate the **VLAN Tag Management** section.

6. At the **Frame Tag Mode** field, select **Provider**.

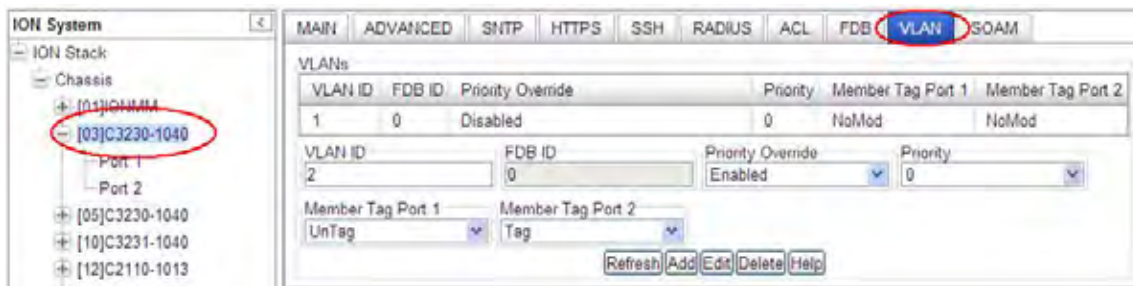


7. Click the **Save** button.

8. At the **Provider Ether Type** field, select **X8100**, or **X9100**, or **X88A8**. In Provider mode, a frame is considered Provider tagged if it matches the 'Provider Ether Type'. Frames that are ingress with a Provider tag are stripped of their Provider tag on egressing this interface. If the frame's Ethertype doesn't match the **Provider Ether Type** it is considered as untagged. The default **x88a8**.

9. Click the **Save** button.

10. Select the x323x **VLAN** tab.

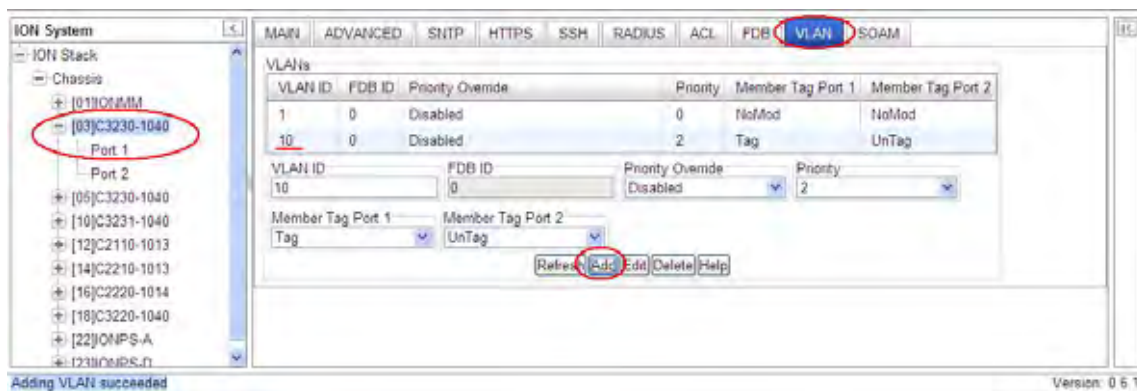


Section 4: Configuration

11. Create VLAN VID 10:

- a) In the **VLAN ID** field, enter **10**.
- b) At the **Priority Override** dropdown, select **Disabled**.
- c) At the **Priority** dropdown, select **2**.
- d) At the **Member Tag Port x** dropdowns, select **NoMod**, **NotMember**, **Tag**, or **UnTag** as the membership / action for this VID. Set each of the ports as not a member of the VLAN, or to either not modify, or add a tag to, or remove the tag from management traffic.

12. Click the **Add** button to add the new VLAN to the VLANs table.



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

This procedure places the x323x in the VLAN specified, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

Enable and configure Management VLAN as required; see previous section.

Use the **Flush Operation** functions as needed; see the [“Flush VLAN Databases Config”](#) section on page 198.

VLAN Config – Customer Port – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Check the current VLAN configuration. Type **show vlan config** and press **Enter**.
3. Define VLAN VID 10 port 2 tagging.
Type **set vlan vid=10 port=2 memetag=<noMod|notMember|tag|unTag>** and press **Enter**.
4. Enable or disable VLAN VID 10 Priority Override as desired.
Type **set vlan vid 10 pri-override=<enable|disable>** and press **Enter**.
5. Set the Priority level for VLAN VID 10. Type **set vlan vid 10 priority 2** and press **Enter**.
6. Switch to the applicable port. Type **go llp=2** and press **Enter**.
7. Set the port’s VLAN tagging mode to **Network**. Type **set port vlan tag mode=customer** and press **Enter**.
8. Verify the Management VLAN configuration. Type **show mgmt vlan config** and press **Enter**.
9. Verify the VLAN configuration. Type **show vlan config** and press **Enter**.

Enable and configure Management VLAN as required; see previous section.

Configure the x323x and each of the ports as required. An example is provided on the next page.

Example (VLAN Config – Customer Port - CLI Method):

The following command sequence places the NID in VLAN 10, creates a Customer port, allowing both ports (Ethernet connections) to receive management traffic only from devices that are also in VLAN 10.

```
C1|S3|L1D>set vlan vid 10 port 2 memetag<noMod|notMember|tag|unTag>
C1|S3|L1D>set vlan vid 10 pri-override<enable|disable>
C1|S3|L1D>set vlan vid 10 priority 2
C1|S3|L1D>go llp=1
C1|S3|L1P1>set port vlan tag mode<customer>
C1|S3|L1P1>show vlan config
vid:10          fid:0          priority:2          priv_override:disable
port1:         noMod  port2:         Tag
C1|S3|L1P1>
```

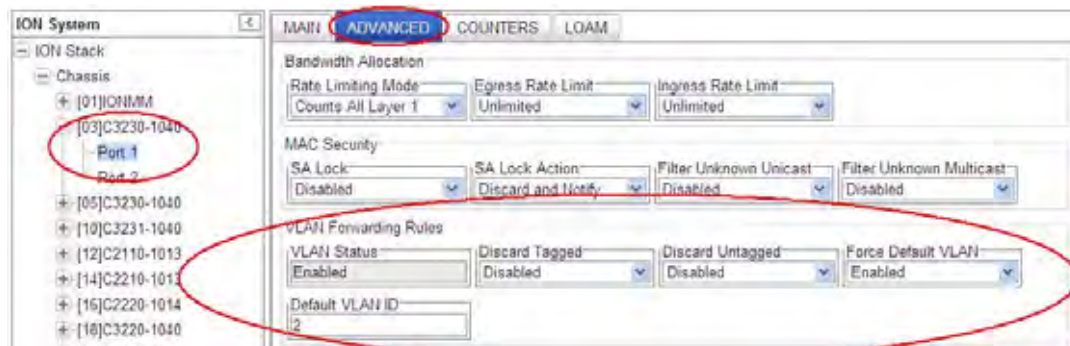
Enable and configure Management VLAN as required; see previous section.

This procedure places the NID in the VLAN specified, creates a Customer port, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

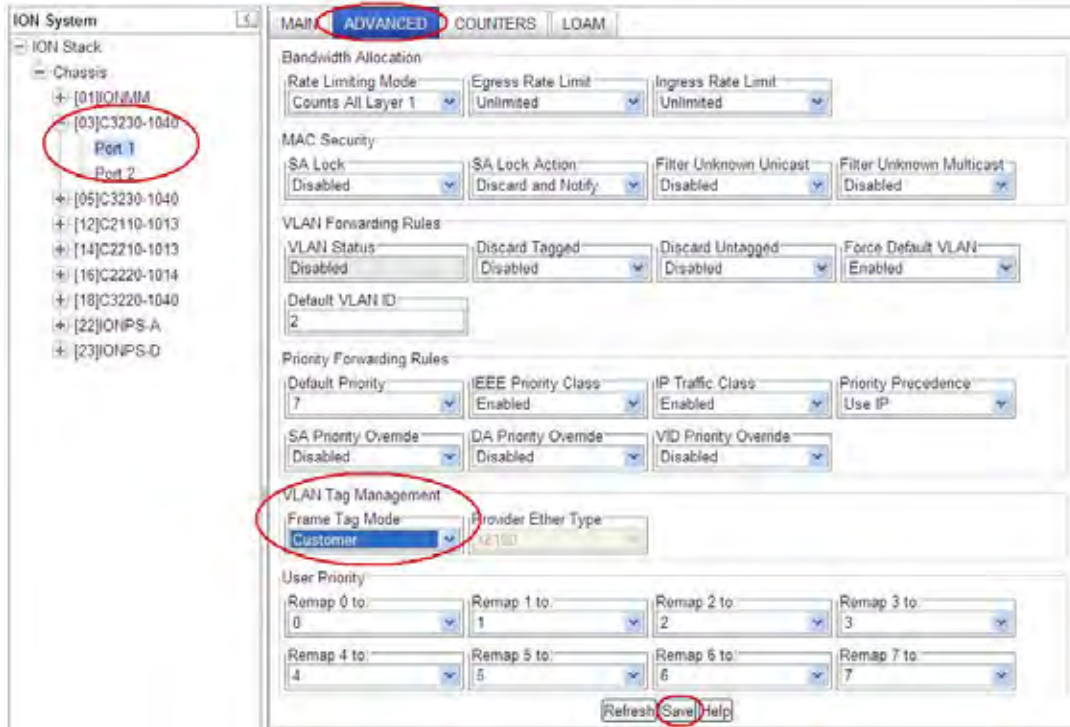
Section 4: Configuration

VLAN Config – Customer Port - Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port’s **ADVANCED** tab.
3. Locate the **VLAN Forwarding Rules** section.

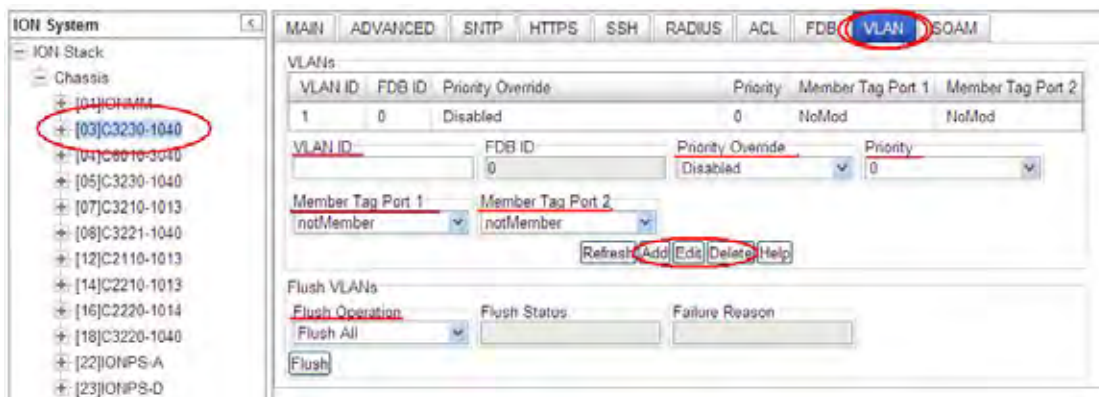


4. For each Port, at the **ADVANCED** tab in the **VLAN Forwarding Rules** section:
 - a) Set **Discard Tagged** to Enabled or Disabled (the default is Disabled).
 - b) Set **Discard Untagged** to Enabled or Disabled (the default is Disabled).
 - c) Set **Force Default VLAN** to Enabled or Disabled (the default is Disabled).
 - d) Set the **Default VLAN ID** to <2-4094>. The default is VID 2.
5. Locate the **VLAN Tag Management** section.
6. For each port, at the **Frame Tag Mode** field, select **Customer**.



Note: Leave the **Provider Ether Type** field at the default setting. The **Provider Ether Type** value has no affect when the port is in **Customer Frame Tag Mode**.

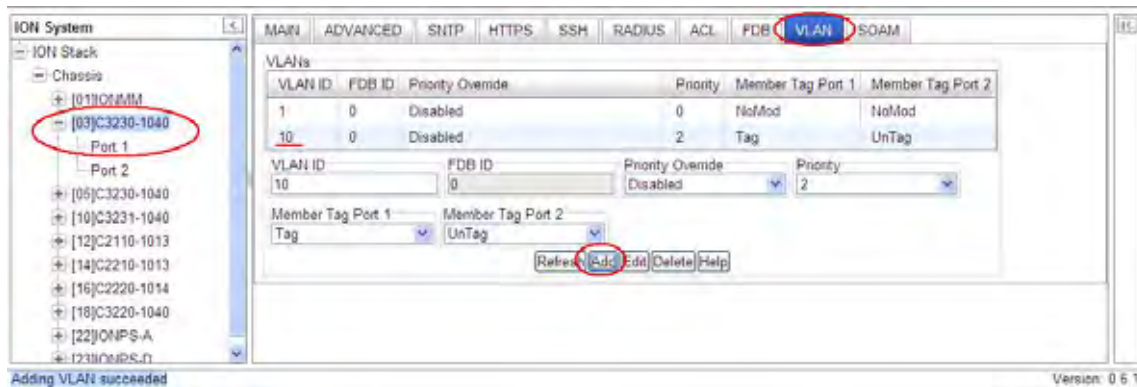
7. Select the x323x VLAN tab.



8. Create VLAN VID 10:
 - a) In the **VLAN ID** field, enter **10**.
 - b) At the **Priority Override** dropdown, select **Disabled**.
 - c) At the **Priority** dropdown, select **2**.
 - d) At the **Member Tag Port x** dropdowns, select **NoMod**, **NotMember**, **Tag**, or **UnTag** as the membership / action for this VID. Set each of the ports as not a member of the VLAN, or to either not modify, or add a tag to, or remove the tag from management traffic.

Section 4: Configuration

9. Click the **Add** button to add the new VLAN to the VLANs table.



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

This procedure places the x323x in the VLAN specified, allowing the member ports (Ethernet connections) selected to receive management traffic only from devices that are also in the specified VLAN.

Enable and configure Management VLAN as required; see previous section.

Use the **Flush Operation** functions as needed; see the “[Flush VLAN Databases Config](#)” section below.

Flush VLAN Databases Config

You can delete (flush) the VLAN FID DB and the VLAN DB entries via the x323x CLI or the Web interface.

Flush FID DB – CLI Method

The **flush fiddb type** command is a port level command to clear the dynamic entries or all of the entries in the VLAN forwarding information database. **Note:** The **flush fiddb type=dynamic** command only deletes the dynamic entries; it does not affect the static, staticNRL, or staticPA Entry Types. The **flush fiddb type=all** command deletes all of the Entry Types (static, staticNRL, staticPA, and dynamic).

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Enter the CLI command to Flush the VLAN FID. Type **flush fiddb type=<all|dynamic>** and press **Enter**. The message “*Flushing fiddb is in progress!*” displays momentarily. If the Flush FID DB process completes successfully, the message “*Flush VLANdb succeeded!*” displays.

For example:

```
C1|S1|L1D>flush fiddb type ?
  all
  dynamic
C1|S1|L1D>flush fiddb type dynamic
Cannot flush vlandb on this card!
C1|S1|L1D>go c=1 s=3 l1d
C1|S3|L1D>flush fiddb type dynamic
Flushing fiddb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>flush fiddb type all
Flushing fiddb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>
```

FID Db Flush Operation Status

The current FID database flush operation status displays, either:

unknown: no flush operation has been performed.

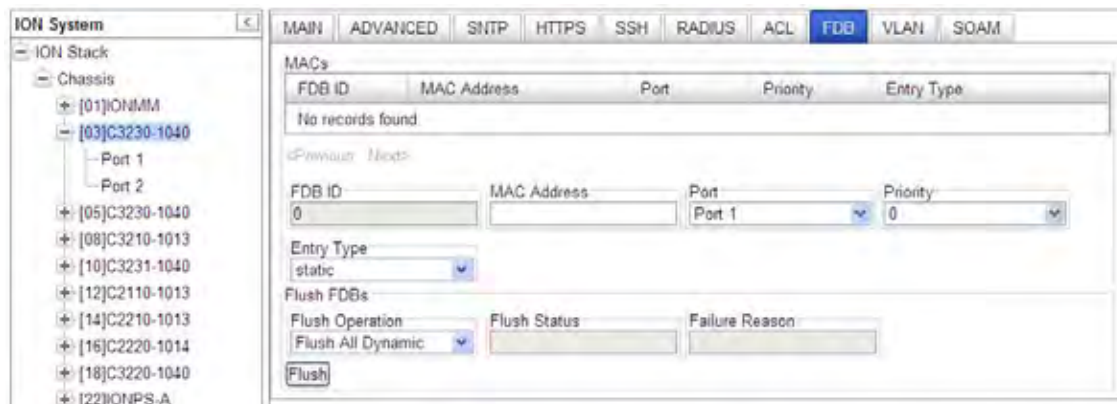
success: the last flush operation was finished successfully.

failure: indicates the last flush operation failed.

inProgress: a FID Db flush operation is currently in progress. Wait for ‘success’ before starting another FID DB flush process.

Flush FID DB – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the device’s **FDB** tab.



3. In the **Flush VLANs** section at the **Flush Operation** dropdown, select **Flush All** or **Flush All Dynamic** and click the **Flush** button. The webpage message “Are you sure to flush all?” displays. If this is the operation that you want, click the **OK** button. The “Flush is being processed” message displays momentarily.

If the Flush was successful, the **Flush Status** field displays “*Success*”.

If the Flush was unsuccessful, the **Failure** field displays the reason for the Flush failure.

See the Troubleshooting section for the set of Failure Reason codes that may be displayed.

Note: The **Flush All Dynamic** selection only deletes the dynamic entries; it does not affect the static, staticNRL, or staticPA Entry Types. The **Flush All** selection deletes all of the Entry Type entries (static, staticNRL, staticPA, and dynamic).

Flush VLAN DB – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Enter the CLI command to flush the VLAN FID. Type **flush vlandb=all** and press **Enter**. This is a port level command to erase all VLAN database entries except for the default VLAN database entry (which cannot be deleted).
3. The message “*Flushing VLANdb is in progress!*” displays momentarily. If the Flush FID DB process completes successfully, the message “*Flush VLANdb succeeded!*” displays.

```
For example: C1|S1|L1D>flush vlandb ?
              all
C1|S3|L1D>flush vlandb all
Flushing VLANdb is in progress!
Flush VLANdb succeeded!
C1|S3|L1D>
```

The VLAN database flush operation status displays **failure** to indicate the last flush operation failed.

Note: if a FID Db flush operation is currently in progress, wait for the “*Flush VLANdb succeeded!*” message before starting another FID DB flush process.

VLAN Db Flush Operation Status

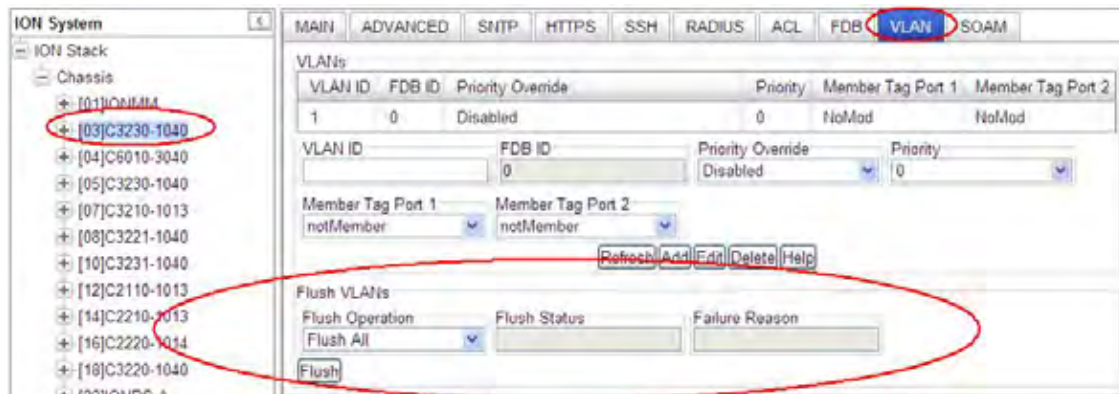
The current VLAN database flush operation status; either:

- unknown:** no flush operation has been performed.
- success:** the last flush operation was finished successfully.
- failure:** indicates the last flush operation failed.
- inProgress:** a flush operation is currently in progress.

Section 4: Configuration

Flush VLAN DB – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the device’s VLAN tab.



3. In the **Flush VLANs** section at the **Flush Operation** dropdown, select **Flush All** and click the **Flush** button. The web page message “Are you sure to flush all?” displays. If this is the operation that you want, click the OK button. The “Flush is being processed” message displays momentarily.

If the Flush was successful, the **Flush Status** field displays “Success”.

If the Flush was unsuccessful, the **Failure** field displays the reason for the Flush failure.

See “Section 6: Troubleshooting” on page 271 for the set of **Failure Reason** codes that may be displayed.

Configuring VLAN Tunneling (802.1q Tunneling)

How VLAN Tunneling Works

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

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

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

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

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

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

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

Section 4: Configuration

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same S-tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the S-tag is not added when it is sent out the tunnel port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

A QinQ tunnel port may receive either tagged or untagged packets. Note that no matter how many tags the incoming packet has, it is treated as-tagged packet.

The ingress process performs source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet.

Packets entering a Q-in-Q tunnel port are processed as follows:

1. New S-tags are added to all incoming packets, no matter how many tags they already have. The ingress process creates and inserts the outer tag (S-tag) into the packet, based on the default VID and the tag's ether-type). The outer tag is used for learning and switching packets. The priority of the inner tag is copied to the outer tag if it is a tagged or priority-tagged packet.
2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an S-tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is-tagged, the outer tag is an S-tag, and the inner tag is a C-tag.
3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).
4. The switch sends the packet to the proper egress port.
5. If the egress port is an untagged member of the SVLAN, the outer tag is stripped. If egress port is a tagged member, the outgoing packets will have two tags.

An uplink port receives one of the following packets:

- Untagged
- One tag (ctype or stype)
- Double tag (ctype and stype)

The ingress process performs source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a Q-in-Q uplink port are processed as follows:

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double-tagged) is not equal to the ether type of the uplink port, the VLAN tag is determined to be a Customer VLAN C-tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The ether type must be configured on a per-port basis, and the

verification cannot be disabled.

3. If the ether-type of an incoming packet (single or double tagged) is equal to the ether type of the up-link port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookup, the packet is double tagged. The switch uses the ether type of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port ether type and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its ether type, and port ether type is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.
5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The switch sends the packet to the proper egress port.
8. If the egress port is an untagged member of the SP VLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

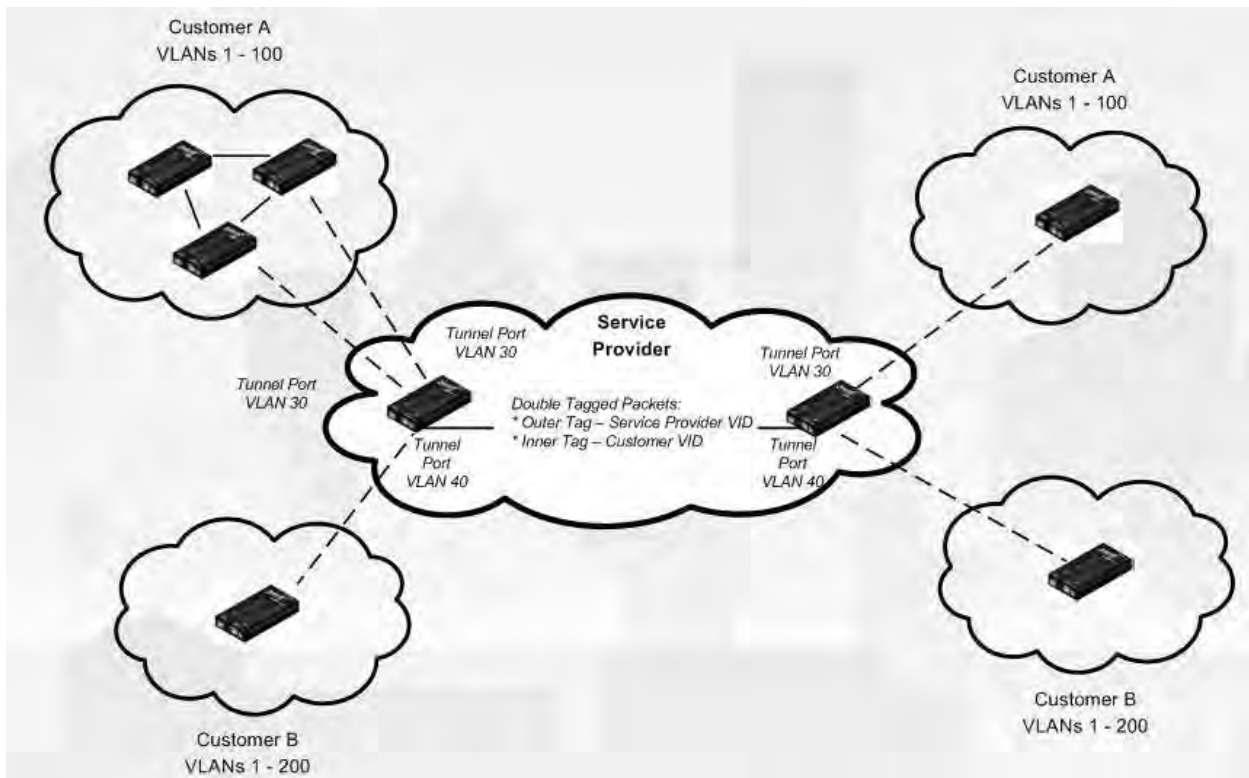


Figure 36: VLAN Tunneling Example

Section 4: Configuration

VLAN Tunneling (802.1Q Tunneling) Summary

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

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

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

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

Prerequisites for VLAN Tunneling Functions

1. Network topology and network administration have been reviewed.
2. Business and service policies have been established.
3. A Maintenance End Point (MEP) is configured.
4. Maintenance Intermediate Point (MIP) is configured.

Restrictions for Configuring VLAN Tunneling Functions

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

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

For specific procedures on configuring VLAN Tunneling via the CLI or Web method, see "[Appendix F: VLAN Tunneling Configuration Examples](#)" on page 532.

Configuring QoS

QoS (Quality of Service) can be set up on the NIDs either:

- At the Layer 2 level using CoS (Class of Service) bits per IEEE 802.1p, or
- At the Layer 3 level based on DSCP/ToS (Differentiated Services Code Point/Type of Service).

QoS (Quality of Service) can be set up on ION modules that support the layer-2 switch QoS functions of priority classification, queuing and remarking. The x323x NIDs provide QoS at the Layer 2 level using CoS bits per IEEE 802.1p. The priority bits in the 802.3ac tag can be remapped as frames ingress the device based on Ingress port, Source MAC address, Destination MAC address, or VLAN ID in the 802.1q tag, or on the basis of remapping to a user-defined priority on a per-port basis.

The x323x NIDs also provide QoS based on DSCP/ToS bits in the IP header. Three precedence bits have a value from 0 to 7 and are used to indicate the importance of a datagram. The default is 0 (higher indicates more importance). Bits 3, 4, and 5 represent the following:

D: requests low delay

T: requests high throughput

R: requests high reliability

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

QoS Config – CLI Method

QoS (Quality of Service) allows the bandwidth, error rates and latency to be monitored, sampled and possibly improved. QoS also delivers tools to help deliver data efficiently by reducing the impact of delay during peak times when networks are approaching full capacity. QoS does not add capacity, nor does it multiplex the signals like WDM. QoS simply tries to manage data traffic better so that top priority traffic will not be compromised. QoS helps manage the use of bandwidth by applying a set of tools like priority scheme, so certain packets (mission critical must go packets) are forwarded first.

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

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Select the desired device port.
3. Set the Default Priority for the Port. Type **set qos default-priority={0-7}** and press **Enter**.
Example: C1|S7|L1D>**set qos default-priority 7**.

Section 4: Configuration

4. Set a Frame Priority for the Port. Select either:
 - **Destination MAC Address** is Used {enable | disable}
 - **IEEE Tag** is Used {enable | disable}
 - **IP Tag** is Used {enable | disable}
 - **Source MAC Address** is Used {enable | disable}
 - **VLAN ID is Used** {enable | disable}
5. If selected in step 4, set IEEE Priority Remapping. Type **set dot1dbridge ieee-tag-priority={0-3} remap-priority={0-7}** and press **Enter**.
6. Set the Ingress Priority Remapping. Type **set qos ingress-priority {0-7} {0-7}** and press **Enter**.
7. Define the priority remapping for IP traffic. Type **set dot1dbridge ip-priority-index={0 – 63} remap-priority={0 – 3}**
8. Set the tag type (IEEE or IP) to be used to decide frame priority type of a port if both tags are available. Type **set qos priority tag-type={useIEEE | useIP}** and press **Enter**.
9. Show the Priority Remapping to verify the selected configuration. Type **show qos priority remapping** and press **Enter**. The QoS Priority Remapping configuration displays:

```
C1|S10|L1P1>show qos priority remapping
ingress-priority          remapping-priority
-----
0                          0
1                          1
2                          2
3                          3
4                          4
5                          5
6                          6
7                          7
```

10. Show the QoS Configuration of the port to verify the selected configuration. Type **show qos config** and press **Enter**. The QoS configuration information displays:

```
C1|S5|L1P1>show qos config
Default priority:          0
Use IEEE tag for priority: enable
Use IP tag for priority:  enable
Tag type for priority if both tag available: useIEEE
Use source MAC address for priority:  disable
Use destination MAC address for priority:  disable
Use VLAN id for priority:  disable
```

QoS Config – Web Method

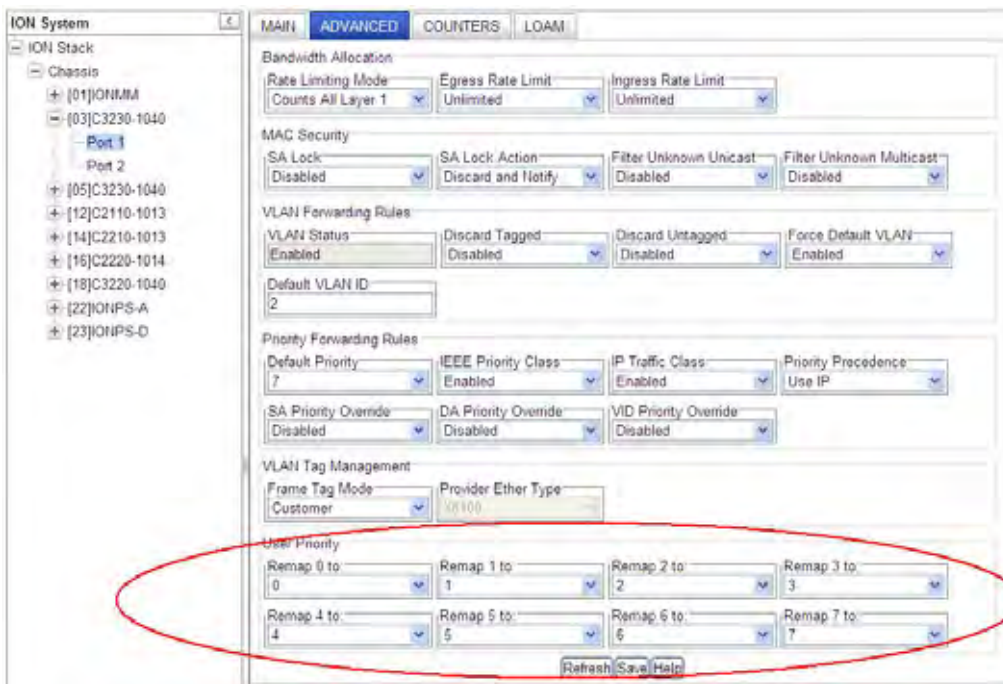
1. **Port Priority Queues:** Each port contains four different classes of output priority queues.

Priority Queue	Frame Type	Weight
0	Best Effort	1
1	Background	2
2	Excellent Effort	4
3	Critical Applications	8

Packets will be transmitted from these queues in weighted round-robin fashion with the weights of 8:4:2:1 for class queues 3, 2, 1 and 0.

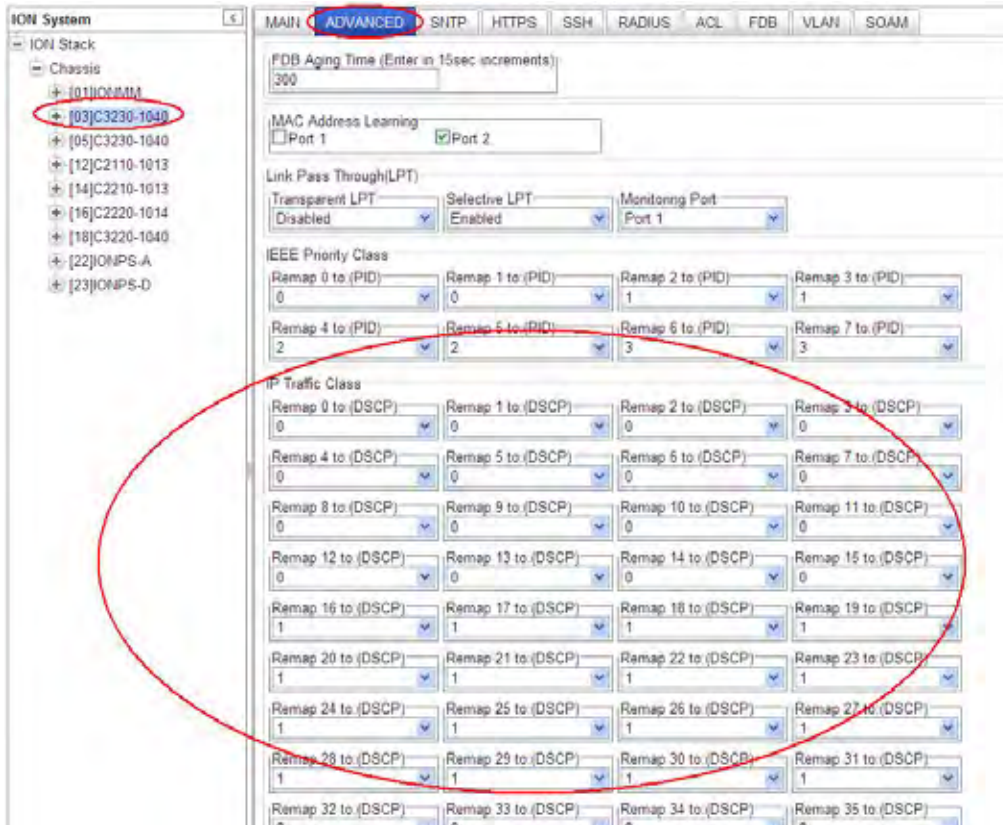
2. **Classification:** Incoming Packets to a port can be classified based on L2 CoS (IEEE 802.1p) or L3 IP DiffServ (IPv4/IPv6) priority field or port default priority. See the [Priority Override](#) section for details on how port/L2/L3 classification can be configured per port.

IEEE priority re-mapping: When a packet is classified by L2 CoS priority, it will be re-mapped to another L2 priority value as defined in the per-port priority re-mapping table.



Section 4: Configuration

IP Traffic Class priority re-mapping: When a packet is classified by IP priority, it will be re-mapped by the global IP remapping table.

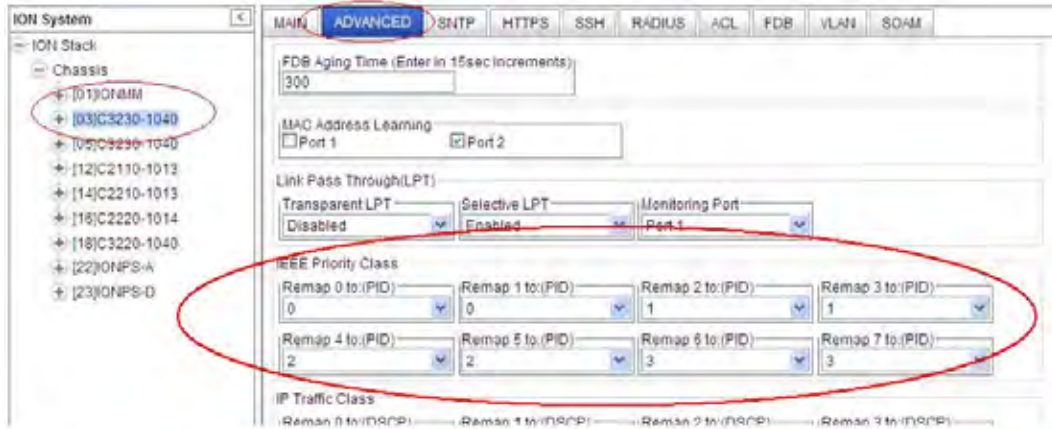


The re-mapped 2-bit priority value would be used for two purposes:

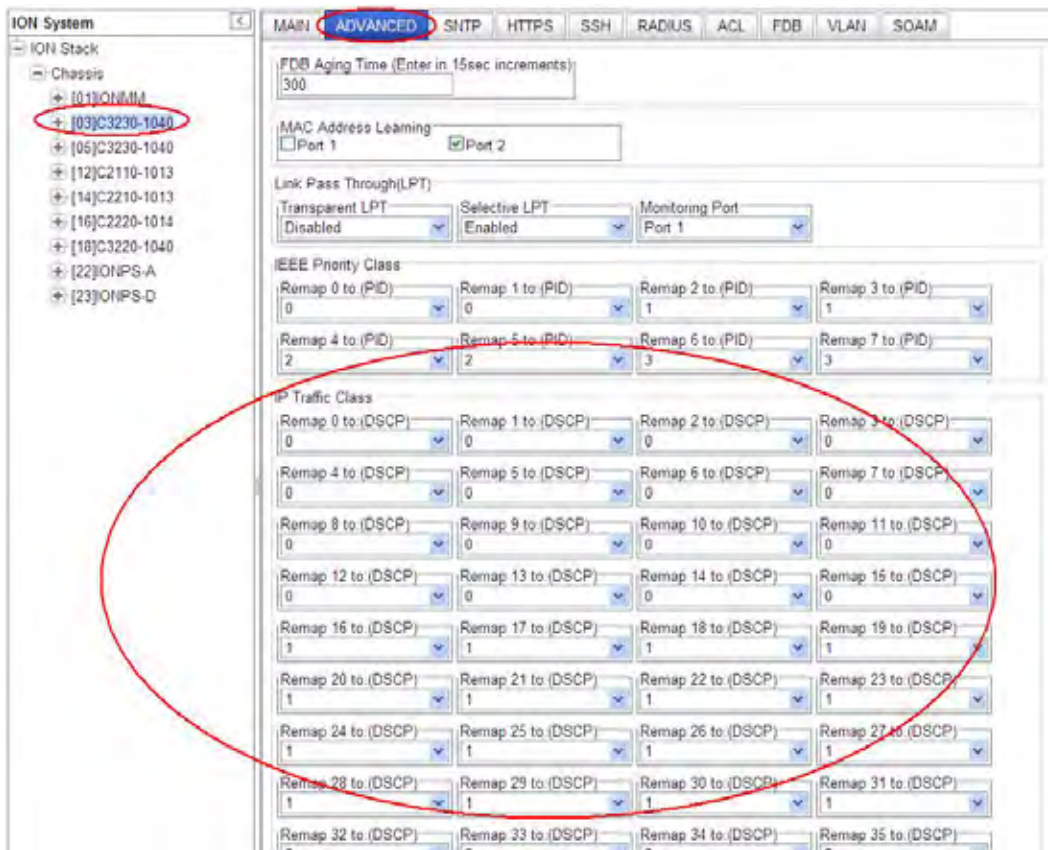
- 1) These 2-bit class values would directly map to the output queue of the egress port.
- 2) Egress priority re-marking of the frame. When the packet is eligible for remarking, it would be scaled-up to 3 bits, by borrowing the least significant bit of the port default priority.

3. Queuing: Once the incoming packet is classified/re-mapped based on port/L2/L3 priority, the packet is queued to the egress port queue based on the global system queue remapping table.

a) L2 Priority Queuing: Packet classified by port L2 default or frame L2 priority will be queued based on the “IEEE Priority Class” re-mapping.

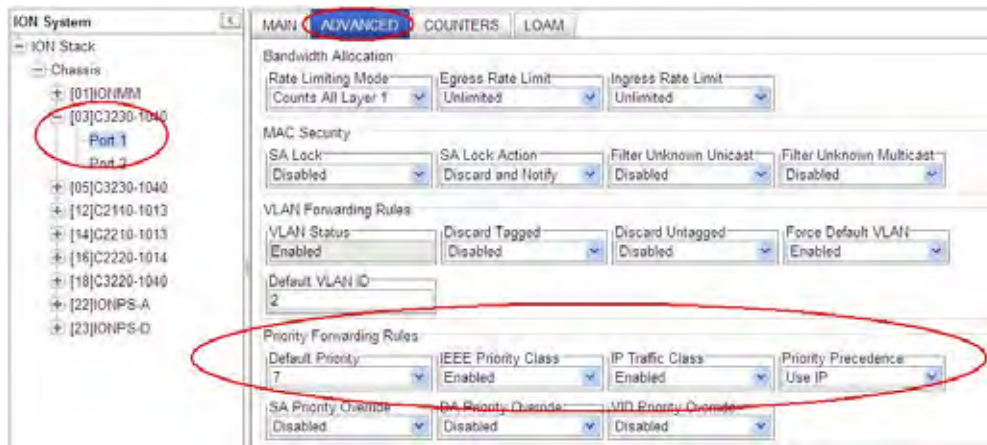


b) IP Priority Queuing: Packet classified by IP priority will be queued based on the “IP Traffic Class” remapping table.



Section 4: Configuration

4. Classification and Queuing configuration options: The following classification/queuing options are available and can be configured per port at the port's **ADVANCED** tab > **Priority Forwarding Rules** section.



a) Port default priority: This can be enabled per port by disabling “IEEE Priority Class” and “IP Traffic Class”. All frames will be assigned to the port Default Priority. In the following example, port Default Priority has been set to “4”.



b) IEEE priority only: This can be configured per port by enabling “IEEE Priority Class” and disabling “IP Traffic Class”. All untagged frames (including IP) will be assigned to the port Default Priority.

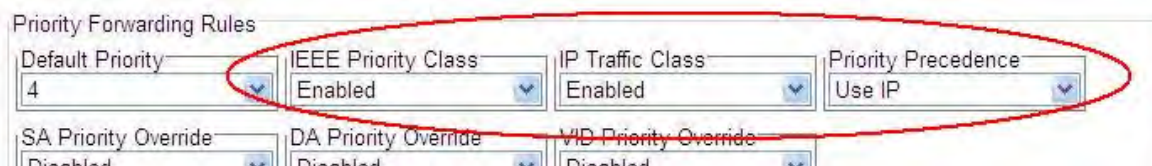


c) IP priority only: This can be configured per port by enabling “IP Traffic Class” and disabling “IEEE Priority Class”. Tagged and non-IP frames will be assigned to the port Default Priority.



d) IP and IEEE priority with the precedence of IP: This can be configured per port by enabling both “IEEE Priority Class” and “IP Traffic Class” and “Priority Precedence” set to “Use IP”.

Note: The Tagged IP packet would get queued to one of the egress port priority queues per the global IP-remapping table. However, the remapped IEEE priority value will be used for re-marking the packet.



e) **IP and IEEE priority with the precedence of IEEE:** This can be configured per port by enabling both “IEEE Priority Class” and “IP Traffic Class” and “Priority Precedence” set to “Use IEEE.”

Note: Tagged IP packet would get queued on the egress port as per the global IEEE remapping table.



The last two options (“IP and IEEE priority with the precedence of IP” and “IP and IEEE priority with the precedence of IEEE”) differ only in how a packet gets queued. The frame re-marking priority works the same way for both options.

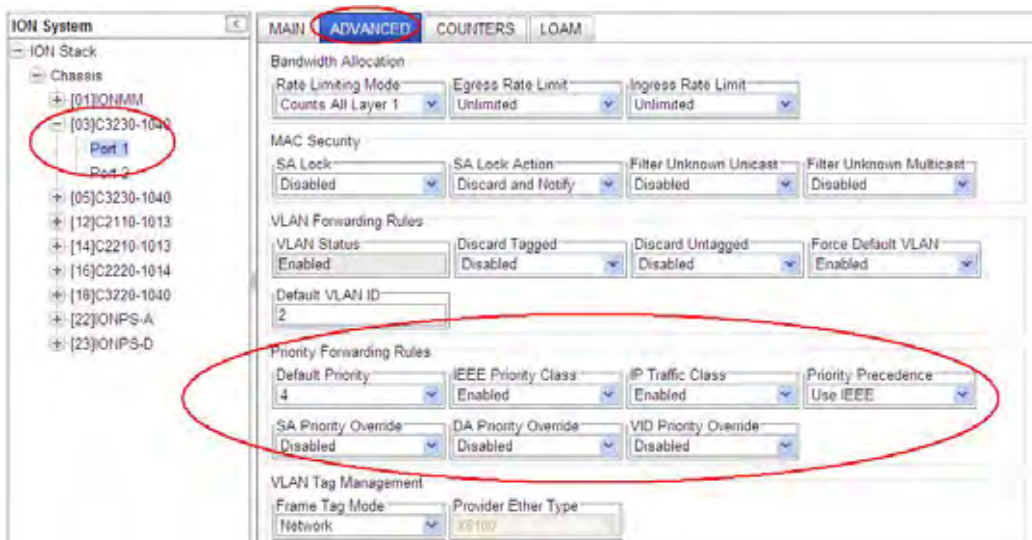
5. Priority Override: The initial re-mapped priority value can be further over-ridden by VLAN or per frame SA/DA.

One or more of the following overrides can be enabled per port. Should more than one override match, the following order of priority is applied (i.e., DA would override all others):

- 1) VID Priority Override (VLAN ID priority overrides)
- 2) SA Priority Override (Source Address priority overrides)
- 3) DA Priority Override (Device Address priority overrides all others)

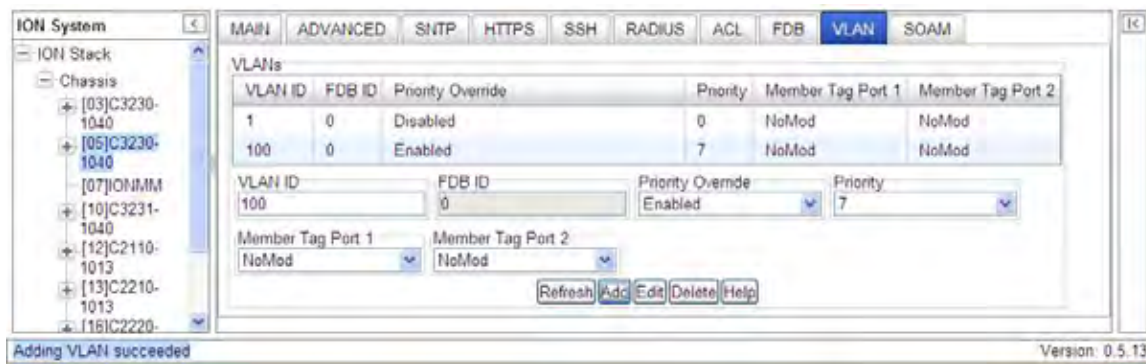
The higher order 2 bits of the VID/MAC priority will be used as the queue re-mapped priority.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port’s **ADVANCED** tab.
3. Locate the **Priority Forwarding Rules** section.



Section 4: Configuration

a) VID Priority Override: This requires the VLAN entry to be configured with the desired priority in the VLAN database.

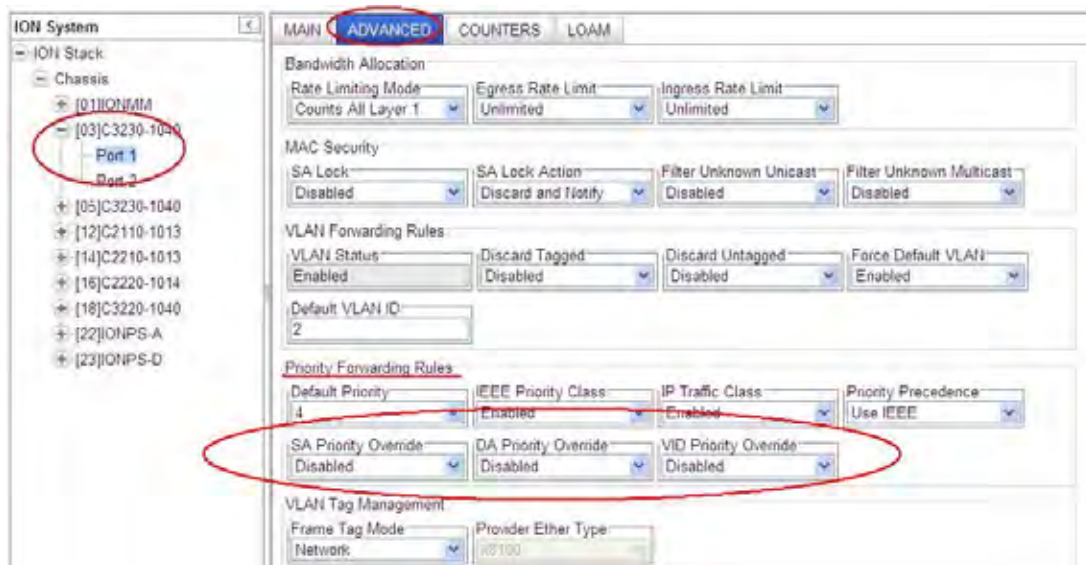


In the above example, the VLAN 100 packets egress on port with the priority marked/restricted to priority “7”. The higher 2 bits of the VID priority (0x7) will be used as the queue priority. Hence, the packets will get queued to the output queue “3”.

b) SA/DA Priority Override: Add Priority Override for SA/DA to the MACs table as a static Entry Type with the desired priority.

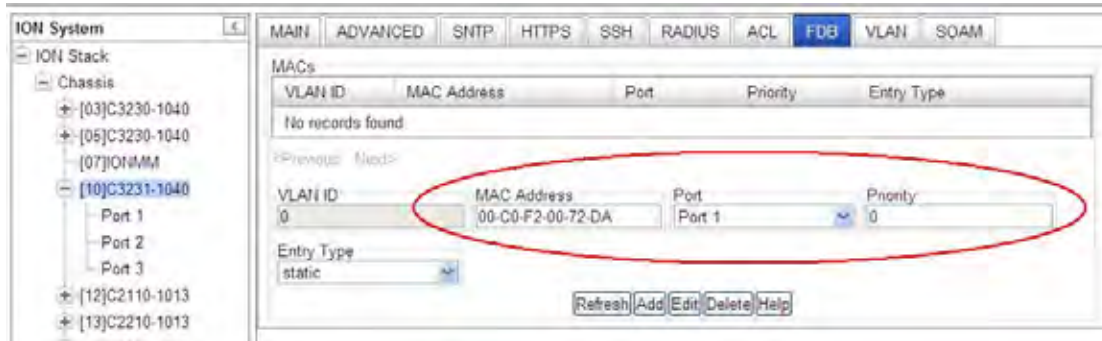


Locate the device port **ADVANCED** tab's **Priority Forwarding Rules** section.



With **SA Priority Override** set to **Enabled**, a frame's Source MAC address (SA) decides the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.

With **DA Priority Override** set to **Enabled**, a frame's Destination MAC address (DA) decides the priority of the frame. The new priority value is assigned based on the priority assigned to that MAC address in the MAC forwarding database.



6. Remapping: Packet IEEE priority could be re-marked with the value assigned during the ingress classification/priority override. This would require proper VLAN configuration with the egress port defined as “Tag” in the VLAN DB. See the “[Configuring VLANs](#)” section on page 281 for VLAN configuration application example details.

Configuring Fiber Port Redundancy

The Port Redundancy state can be set to enable or disable on a NID with 2 or more fiber ports.

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

The Fiber Redundancy feature adds a form of automatic protection switching using a LOS mechanism that triggers the switch to the surviving line. The ION system uses 1:1 protection, with a modified form of bi-directional switching. TLPT and SLPT are operational with fiber redundancy enabled or disabled.

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

Note: On the x3231, LPT is operational in non-redundant mode.

Fiber Port Redundancy Use Cases

For a 3-port card used as a converter, assuming ports 2 and 3 are in a group as one side, port 1 as one side; provides the following use cases:

- Case 1 (disabled): no LPT
- Case 2 (Monitoring Port = 1): port 1 down, cause port 2 down, port 3 unchanged.
- Case 3 (monitor port = 2 or 3): port 2 or 3 down, cause port 1 down.
- Case 4 (monitor port = a special number like 100, means all copper ports): all copper ports down causes all fiber ports down.
- Case 5 (monitor port = a special number like 101, means all fiber ports): all fiber ports down causes all copper ports down.

If used as a 3-ports switch, another case could be:

- Case 6 (add a target port in the MIB; like monitor port = port 2, target port = 3): user can use any specific port to do the LPT case any other specific port link up/down.

On a 3-port card, the Customer Port is Port 1, Primary Port is Port 2, Secondary Port is Port 3, and the 'Active Port' is the Port that on which the Redundancy function is active.

Fiber Port Redundancy can be configured in the NID using either the CLI or Web method.

Redundancy Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Set the Redundancy state to enable. Type: **set redundancy state=<state>**

Where:

state = enable or disable

3. Press **Enter**.
4. Verify the configuration has been set. Type: **show redundancy info**
5. Press **Enter**. The port’s redundancy state displays. For example:

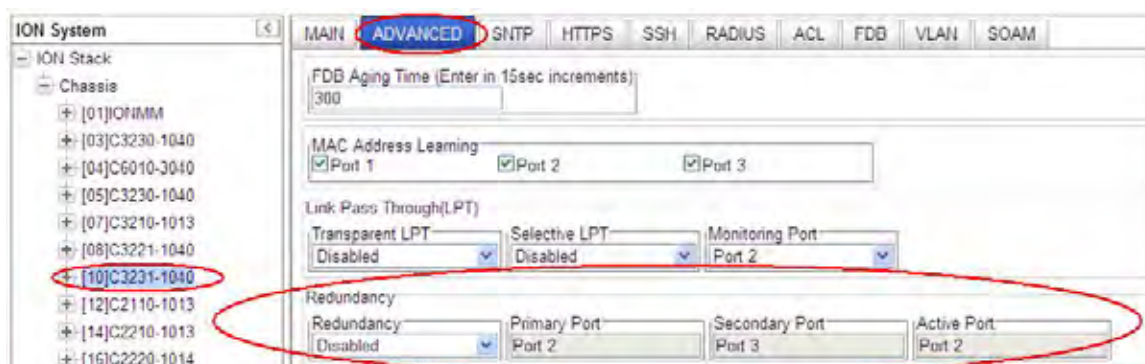
```
AgentIII C1|S10|L1P3>set redundancy state ?
  disable
  enable
AgentIII C1|S10|L1P3>set redundancy state enable
Error: this command should be executed on a device!
AgentIII C1|S10|L1P3>go l1d
AgentIII C1|S10|L1D>set redundancy state enable
AgentIII C1|S10|L1D>show redundancy info
Redundancy information:
-----
Port redundancy state:           enable
Primary port:                   2
Secondary port:                 3
Active port:                    2
AgentIII C1|S10|L1D>
```

Section 4: Configuration

Redundancy Config – Web Method

Note: With the port Redundancy state set to enabled, a Primary Port, Secondary Port, and/or Active Port may still display with the field grayed out.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **ADVANCED** tab.
3. Locate the **Redundancy** section.
4. Set the Primary Port and Secondary Port redundancy (failover) port numbers. The default configuration is Redundancy = Disabled, Primary Port = 2, Secondary Port = 3, and Active Port = N/A.



5. Select Redundancy **Enabled**.
6. Click **Save** and then click **Refresh**.
7. Verify the Redundancy configuration. For example, the Redundancy configuration below shows Redundancy = **Enabled**, Primary Port = **Port 2**, Secondary Port = **Port 3**, and Active Port = **Port 2**.



Configuring L2CP

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

Layer 2 Control protocols are designed to interact with various entities and peer-entities for the proper flow of Layer-2 traffic through the network. Depending on the customer's network configuration or the operator's service offering, this traffic is handled in one of three ways:

1. **Pass** 'as-is' between network-side and customer-side ports. "Peer" (pass) means that the MEN will actively participate with the Customer Equipment (CE). This is the default setting (pass to an EVC for tunneling).
2. **Discard** so that no specified L2CP traffic is ingressed, as this may lead to network instability. "Discard" means that the MEN will discard ingress L2CP frames of a given protocol, and will not generate that protocol on egress from the MEN.
3. **Tunnel** encapsulated traffic to another x323x to allow a network operator to offer a transparent Ethernet service. "Tunnel" means that frames associated with a given protocol are transparently passed to a given EVC for transport across the MEN to the destination UNI.

The MEF (Metro Ethernet Forum) introduced the L2CP attribute for Ethernet services and UNI in MEF 6. L2CP processing for both the EPL and EVPL is discussed in the following sections.

L2CP Protocol Descriptions

The following L2CP protocols are supported:

- STP Protocols
- Slow Protocols
- ELMI Protocol
- LLDP Protocol
- Port Authentication Protocols
- Bridge Management Protocols
- **GARP/GMRP Block of Protocols**
- Bridge Block Other Multicasts

Most Layer 2 control protocols use untagged frames; the exception being certain SOAM (802.1ag) protocols that use VLAN tags.

The L2CP protocols are described in the following sections. The x323x handling syntax for each protocol is 1) **discard** (discard frames at the UNI) or 2) **pass** (pass frames to an EVC for tunneling). The default for each protocol is **pass**.

STP Protocols Fwd

Spanning Tree Protocols (STP) disposition – handling of 802.1D Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP, per IEEE 802.1w. Any STP/RSTP/MSTP protocol frames with destination address of 01-80-C2-00-00-00 are discarded at this port or passed.

Section 4: Configuration

Slow Protocols Fwd

Slow Protocols disposition – handling of Slow Protocols, one of two distinct classes of protocols used to control various operating aspects of IEEE 802.3 devices; protocols such as LACP, with less stringent frequency and latency requirements.

Any LACP/LAMP protocol frames with destination address of 01-80-C2-00-00-02 is discarded at this port or passed. Since this device pairs link OAM frames, these frames will not be forwarded or discarded.

Port Auth Protocol Fwd

Port Authentication Protocols disposition – handling of RADIUS, CHAP, EAP, PEAP, FCPAP, and/or other port authenticating protocols. Port authentication protocol frames with a destination address of 01-80-C2-00-00-03 are discarded at this port or passed.

ELMI Protocol Fwd

ELMI protocol disposition – handling of Ethernet Local Management Interface (ELMI), a MEF 16 protocol between the service provider network and the customer equipment that lets the customer equipment communicate its status and service characteristics to the service provider network for faster and easier deployment and troubleshooting.

E-LMI protocol frames with destination address of 01-80-C2-00-00-07 is discarded at this port or passed.

ELMI Support Prerequisites and Restrictions

ELMI relies on Ethernet CFM for the status of an EVC, the remote EVC's UNI identifier, and the remote UNI status; therefore:

1. Ethernet LOAM (e.g., CFM) must be implemented and operational on the service provider's network.
2. LOAM must be enabled on the NID. See "[SOAM Configuration Prerequisites and Restrictions](#)" on page 133.
3. ELMI can coexist with all other features. All operating modes are supported.

LLDP Protocol Fwd

LLDP protocol disposition – handling of Link Layer Discovery Protocol (LLDP), a Layer 2 protocol defined by IEEE Standard 802.1AB-2005.

LLDP protocol frames with destination address of 01-80-C2-00-00-0E which are not TN discovery LLDP frames are discarded at this port or passed.

Bridge Mgmt Protocols Fwd

Bridge Management Protocols disposition – handling of one of several protocols standardized by IEEE 802, including Bridge Group Address (STP), IEEE Std. 802.3x Full Duplex PAUSE operation, Bridge Management Group Address, GMRP and GVRP.

Bridge Management protocol frames with destination address of 01-80-C2-00-00-10 is discarded at this port or passed.

GARP/GMRP Block of Protocols Fwd

GARP/ GMRP Block of protocols disposition – handling of GARP (Generic Attribute Registration Protocol) and GMRP (GARP Multicast Registration Protocol) per IEEE 802.1ak. GARP/GMRP traffic with destination address of 01-80-C2-00-00-20 to 01-80-C2-00-00-2F is discarded at this port or passed.

Select ‘Pass’ (pass to an EVC for tunneling) or ‘Discard’ (discard at the UNI). The default is ‘Pass’.

Bridge Block Other Multicasts Fwd

Bridge Block Other Multicast protocols disposition – Passes or discards all of the IEEE multicast frames in the bridge block of addresses [01-80-C2-00-00-04 to 01-80-C2-00-00-0F]. This applies to all addresses in this block that are not covered by the other mib variables in the table (i.e., this is not applicable for STP, slow protocols, etc.).

L2CP can be configured in the NID using either the CLI or Web method.

L2CP Config – CLI Method

Note that the default setting for each protocol is “pass” (pass frames to an EVC for tunneling).

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Set the L2CP protocol parameters. Change the default “pass” setting to “discard” for Spanning Tree Protocol, Slow Protocols, Port Authentication Protocols, ELMI Protocols, LLDP Protocols, Bridge Mgmt Protocols, GARP/MRP Block of Protocols, and/or Bridge Block Other Multicast Protocols.

Type **set l2cp proto=xx process={pass/discard}** for each L2CP protocol, select **pass** (pass to an EVC for tunneling) or **discard** (discard at the UNI).and press **Enter**. For example:

```
C1|S10|L1P2>set l2cp proto ?
spanningTree
slow
portAuthentication
elmi
lldp
bridgeMgmt
garpmrpBlock
bridgeBlockOtherMulticast
C1|S10|L1P2>set l2cp proto=elmi process=discard
C1|S10|L1P2>set l2cp proto=elmi process=discard
C1|S10|L1P2>set l2cp proto=elmi process=discard
```

3. Verify the L2CP configuration. Type **show l2cp config** and press **Enter**.

The L2CP configuration parameter settings display:

```
C1|S10|L1P2>show l2cp config
Parameter                               Value
-----
Spanning Tree Protocols                  pass
Slow Protocols                           pass
```

Section 4: Configuration

```

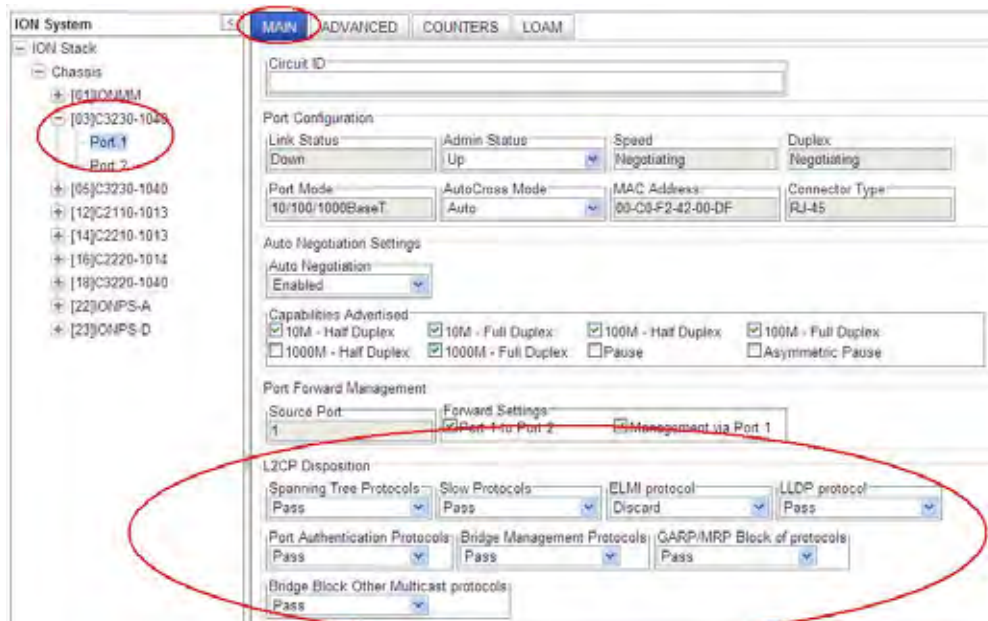
Port Authentication Protocols          pass
ELMI Protocols                        discard
LLDP Protocols                        discard
Bridge Mgmt Protocols                 discard
GARP/MRP Block of Protocols           pass
Bridge Block Other Multicast Protocols pass
C1|S10|L1P2>

```

L2CP Config – Web Method

Note that the default setting for each protocol is “Pass” (pass frames to an EVC for tunneling).

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port.
3. Locate the **L2CP Disposition** section.



4. Set the L2CP protocol forward disposition parameters. For each field, select **Pass** (pass frames to an EVC for tunneling) or **Discard** (discard frames at the UNI).

The default setting for each protocol is **Pass** (pass frames to an EVC for tunneling).

5. Click **Save** when done configuring L2CP for this port.
6. Repeat steps 2-5 for each device port.
7. Click **Save** when done configuring L2CP for all ports on the device.

TNDP (TN Topology Discovery Protocol) Disable/Enable

TNDP (TN Topology Discovery Protocol) is the 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.

If using the NID with a switch or router, the NID continues to send out LLDP-based information (TN proprietary - sent once every second). While this does not impact the data traffic seen, it drops for unrecognized upper-level protocols in the switch / router. Disabling TNDP can help eliminate invalid errors and make troubleshooting simpler. This ability to enable or disable MAC learning is supported via the Web interface and the CLI).

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

TNDP Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Enable or disable the TN Topology Discovery Protocol. Type **set tndp=<enable|disable>** and press **Enter**. This is a Port level command to enable or disable the TN topology discovery protocol (TN’s LLDP implementation) on a port. When set to Enabled, the device entering this command will not be discovered by the IONMM if it is remotely managed through this port. If enabled, TN Topology Discovery Data will be sent out from this interface. If disabled, TN Topology Discovery Data will not be sent out from this interface. The default is enabled.

```
For example: C1 | S3 | L1P2>set tndp tx state=enable
             C1 | S3 | L1P2>
```

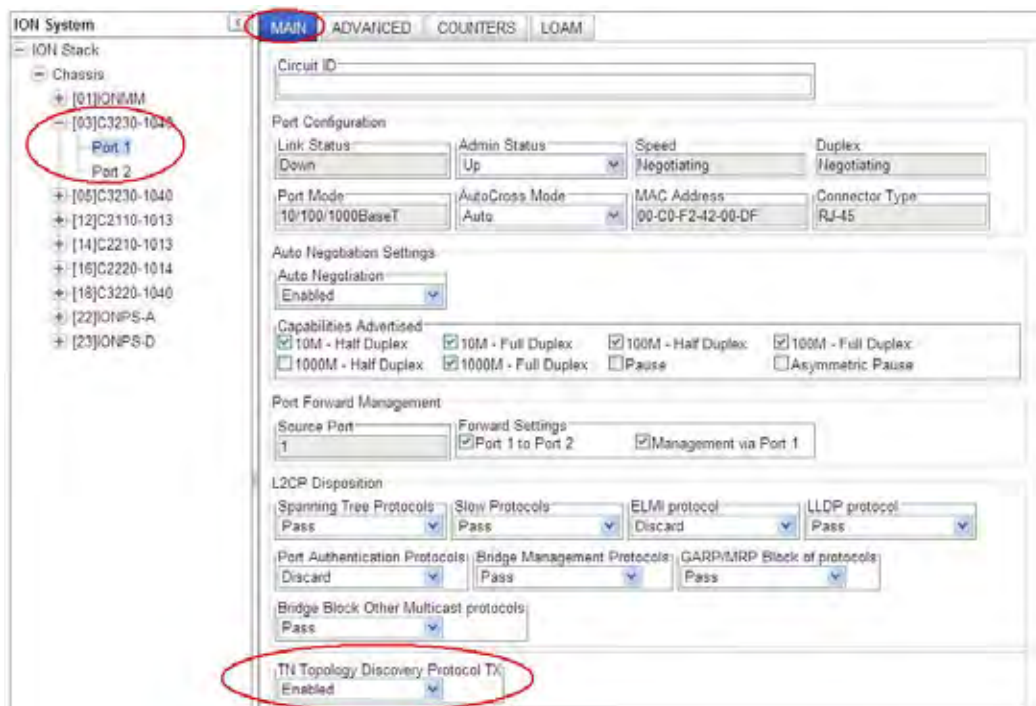
3. Verify the entry. Type **show tndp tx state** and press **Enter**. This displays the current setting (Enabled or Disabled) of the TN topology discovery protocol on a port. When Enabled, the device is not being discovered by the IONMM if the device is remotely managed through this port.

```
For example: C1 | S10 | L1P1>show tndp tx state
             TNDP Tx state:                enable
             C1 | S10 | L1P1>
```

Section 4: Configuration

TNDP Config – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port.
3. Locate the **TN Topology Discovery Protocol TX** section.



4. Set TN Topology Discovery Protocol TX to enabled or disabled. The default setting is Enabled. If **Enabled**, TN Topology Discovery Data will be sent out from this interface. If **Disabled**, TN Topology Discovery Data will not be sent out from this interface.
5. Click the **Save** button when done.

Configuring Loopback

You can define the x323x Loopback type and operation at the port level.

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

Loopback Config – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Select the desired port.
3. If desired, check the port’s loopback capabilities. Type **show ether loopback cap** and press **Enter**. This displays the current loopback functionality that has been set for the port specified in the command. The loopback capabilities that can display are "nolooopback", "phyLayer", "macLayer", "alternate", or "remotePeer".
4. Set the Loopback Type of the selected TDM Port. At the device’s command prompt type **set ether loopback type={nolooopback|phylayer}** and press **Enter**.
5. Set the TDM Loopback operation. Type **set ether loopback oper={init|stop}** and press **Enter**. This alternately initiates or stops the loopback test.
6. Check the TDM Loopback state. Type **show ether loopback state** and press **Enter**. This displays the current loopback operating state for the port entering the command. The loopback capabilities that can display are ""noLoopback", "intiateLoopback", "terminateLoopback", "inProcess", "localInLoopback", or "remoteInLoopback".

For example:

```
C1|S3|L1P1>set ether loopback ?
oper
type
C1|S3|L1P1>set ether loopback oper ?
init
stop
C1|S3|L1P1>set ether loopback oper init
Fail to set Ethernet port loopback operation, please check if Link OAM
admin state of remote peer port is enabled, link status and other is-
sues.
C1|S3|L1P1>set ether loopback oper stop
C1|S3|L1P1>set ether loopback type ?
alternate
maclayer
nolooopback
phylayer
remote
C1|S3|L1P1>set ether loopback type phylayer
Set Ethernet port loopback type failed.
C1|S3|L1P1>set ether loopback type alternate
C1|S3|L1P1>show ether loopback ?
```

Section 4: Configuration

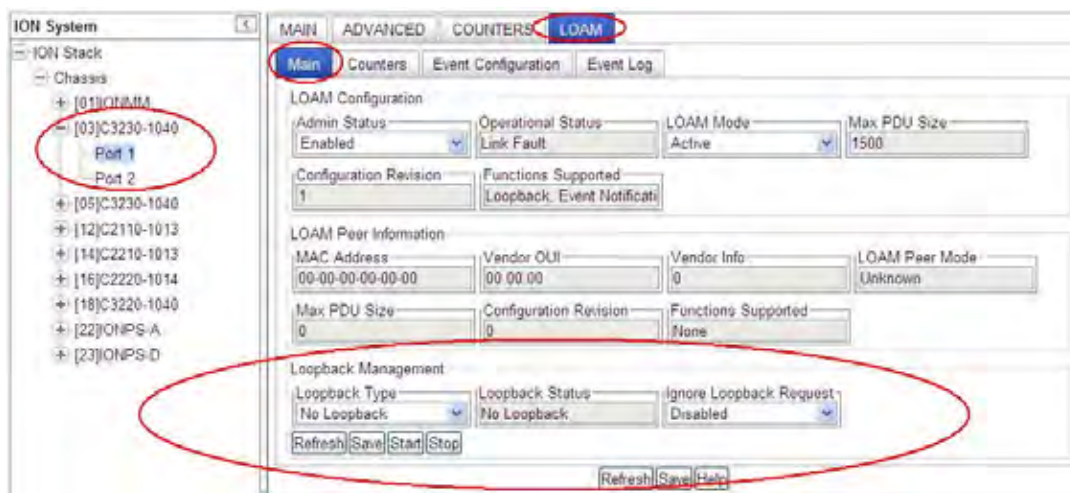
```

capability
state
C1|S3|L1P1>show ether loopback state
Loopback type: alternate
Loopback state: noLoopback
C1|S3|L1P1>show ether loopback capability
Loopback capability: alternate remotePeer
C1|S3|L1P1>set ether loopback type alternate
C1|S3|L1P1>

```

Loopback Config – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port.
3. Locate the **Loopback Management** section.



4. At the **Loopback Type** dropdown, select **No Loopback**, **Alternate**, or **Remote Peer**.
5. At the **Ignore Loopback Request** dropdown, select **Enabled** or **Disabled**.
Enabled causes the LOAM enabled x323x to ignore all Loopback requests (i.e., not respond to remote loopback requests from peers).
Disabled causes the LOAM enabled x323x to respond to all remote loopback requests from peers.
6. Click the **Save** button when done.
7. Click the **Start** button to initiate the selected loopback test type.
8. Click the **Stop** button to end the loopback test.
9. Check the **Loopback Status** field for results. This field displays the loopback status for this interface when enabled. The values are read-only to show the status of the loopback operation (*No Loopback*, *Local in Loopback*, or *Remote in Loopback*).

Configuring System Logging (Syslog)

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

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

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

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

Table 29: Syslog Severity Levels

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

Messages used to enable debugging or software testing are assigned Severity 7. Severity 0 is reserved for messages of very high importance (e.g., serious hardware failures or imminent power failure). Refer to your organizations policy administrator for this level of severity. Note that the syslog protocol does not

Section 4: Configuration

provide for acknowledgment of message delivery. See “[Syslog Messages and Sys.log Output](#)” on page 193 for more information.

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

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

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

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

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

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

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

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

Syslog Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the device’s command prompt type the following set of five CLI commands to define Syslog operations (the Syslog server address and port, and Syslog level and mode). Press the **Enter** key after each command:

```

set syslog svr port=<1-65535> <cr>
set syslog mode=<local/localAndRemote/off/remote> <cr>
set syslog level=<alert/crit/debug/emerg/err/info/notice/warning> <cr>
set syslog svr type=<ipv4|dns> addr=<SYSLOG_SVR_ADDR> <cr>
set syslog svr port=<1-65535>

```

3. Verify the Syslog configuration using the **show syslog config** command. For example:

```

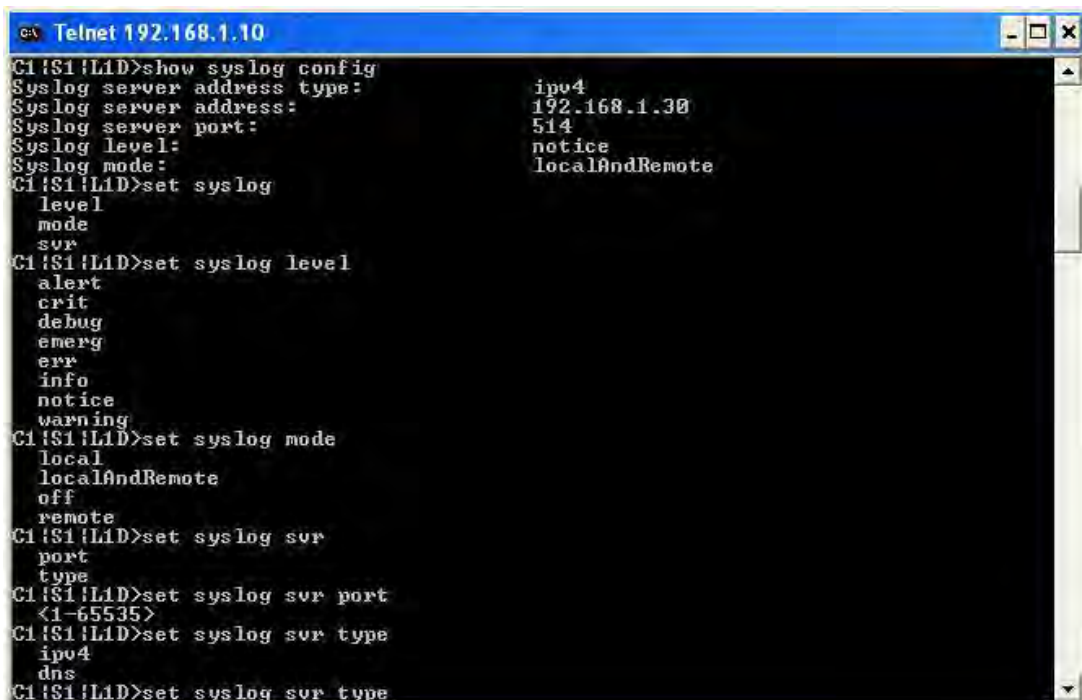
C0|S10|L1D>show syslog config
Syslog server address type:          ipv4
Syslog server address:              192.168.0.2
Syslog server port:                 514
Syslog level:                       info
Syslog mode:                         local
C0|S10|L1D>

```

See [Table 9](#) above for complete descriptions of the Syslog severity levels.

You can use the `clear syslog` command to erase all existing records on the configured Syslog server.

Telnet Example:



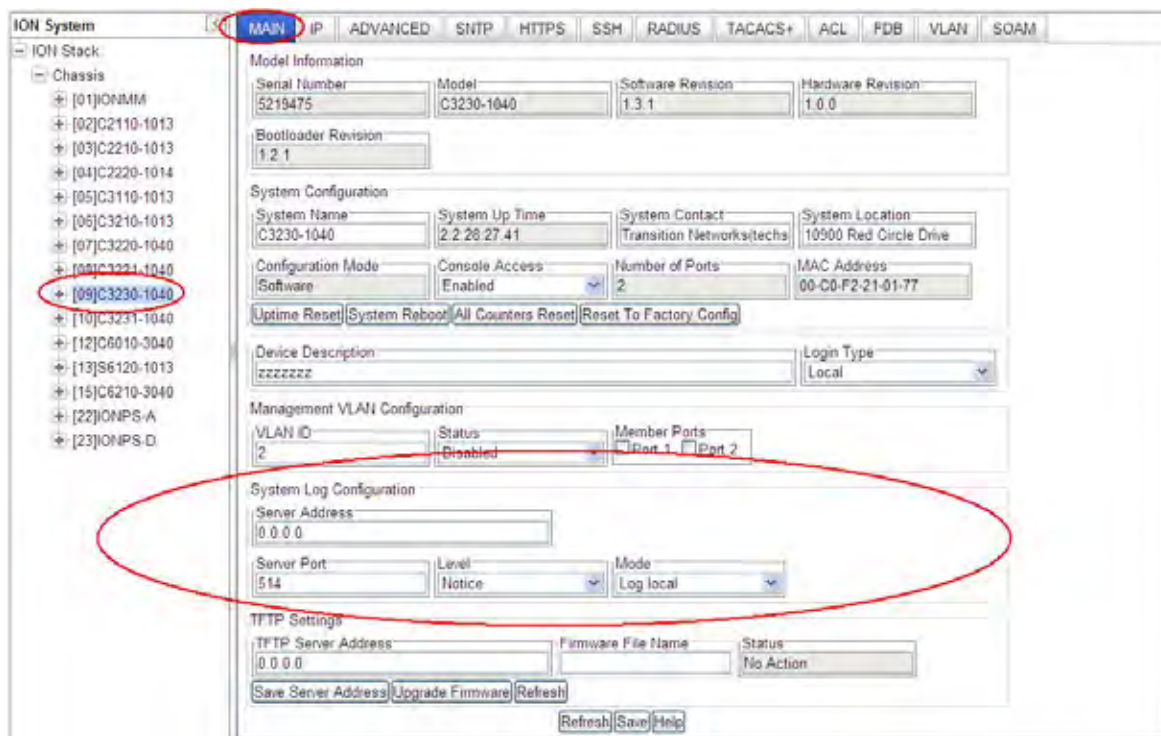
```

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

```


Syslog Config – Web Method

1. Access the IONMM or NID through the Web interface (see “Starting the Web Interface” on page 45).
2. At the IONMM MAIN tab, locate the **System Log Configuration** section.



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

System Log Configuration			
Server Address	Server Port	Level	Mode
192.168.0.2	514	Notice	Log local

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.

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

See [Table 9](#) above for full Syslog severity level descriptions

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

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

4. Verify the Syslog configuration.

System Log Configuration

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

Server Port: 2 Level: Warning Mode: Log local and remote

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

See “[Syslog Messages and Sys.log Output](#)” on page 193 for more Syslog information.

Configuring MAC Address Learning

MAC address learning can be disabled on a per-port basis for security purposes. If MAC address learning is disabled, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port. When enabled, sets the port state to allow learning (the other port states - Flooding, Filtering and Forwarding – are disabled). This function lets you disable MAC learning on the device, but still allow user traffic (data) to pass. This ability to enable or disable MAC learning is supported in all interfaces (Web interface, CLI, SNMP, etc.).

The MAC Learning function can be disabled via the CLI or the Web interface.

MAC Address Learning Portlist Config – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the device’s command prompt type **set mac enable portlist=x**
where x=1, 2 or 3 (port 1, port 2, and/or port 3)

disable learning ports <portlist> Disables MAC address learning on one or more ports for security purposes. If MAC address learning is disabled, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port. The default setting is enabled.

enable learning ports <portlist> Enables MAC address learning on one or more ports. The default setting is enabled. Sets the port state to Learning (the other port states - Flooding, Filtering and Forwarding – are disabled).

```
C1|S1|L1D>set mac enable portlist ?
STR_MAC_LEARNING_PORT_LIST
C1|S1|L1D>set mac enable portlist
C0|S0|L1D>set mac_learning enable portlist=1,3
C0|S0|L1D>
```

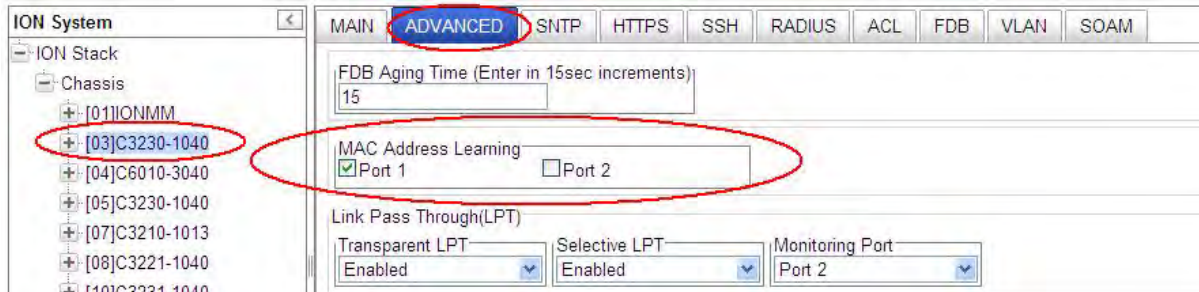
3. Verify the MAC Learning Portlist configuration. Type **show port mac state** and press **Enter**.

For example:

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

MAC Address Learning Portlist Config – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. At the device’s **ADVANCED** tab, locate the **MAC Address Learning** section.



3. Check (enable) or uncheck (disable) the Port checkboxes as desired.
Disabled: with MAC address learning **Disabled**, only certain traffic (broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number) are forwarded to the port.
Enabled: with MAC address learning **Enabled**, sets the port state to allow learning. The other port states (Flooding, Filtering and Forwarding) are disabled.
4. Click the **Save** button when done. The message “Setting values succeeded” displays in the lower left corner of the screen when successfully saved.

Section 5: Operations

General

This section describes the non-configuration operations that can be performed for the x323x NID.

Backup and Restore Operations (Provisioning)

Through the Web interface you can back up and restore the configuration information for the IONMM and any or all of the NIDs in the ION system.

A **Backup** is used to get the SIC card running configuration, convert it to CLI commands, and save those CLI commands into the backup file. The backup file is stored in the IONMM.

Note: Transition Networks recommends as a “best practice” to back up each SIC card’s configuration after it is fully configured, so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored.

A **Restore** is used to send the CLI commands in the configuration file to a SIC after removing the current SIC running configuration. If a problem causes the SIC card configuration restoration to stop (e.g., due to a lost network connection between the PC host and Agent card) the SIC card will use the previous configuration to run the traffic. If the IONMM card is downloading the restore configuration data to the SIC card, and the SIC card is physically removed from the chassis, the SIC card will use the factory default configuration setting when it is re-inserted into the chassis.

Transition Networks recommends that you to enter a “**show card info**” CLI command to view the NID’s current configuration before a backup/restore operation to verify the desired configuration settings. There are several CLI **show** commands that allow you to display (show) information about a SIC card’s configuration. For a complete description of these and other CLI commands see the *ION System CLI Reference Manual, 33461*.

Note: Disable the DHCP client for each device that you backup/restore.

IMPORTANT



Doing a reboot, a restart or upgrade of the NID, 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.

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

- Table 18. [Back Up and Restore File Content and Location](#) on page 308
- Table 19. [File Status after a Reset to Factory Defaults](#) on page 312
- Table 20. [File Content and Location after a System Reboot](#) on page 316
- Table 21. [File Content and Location after a Firmware Upgrade](#) on page 332

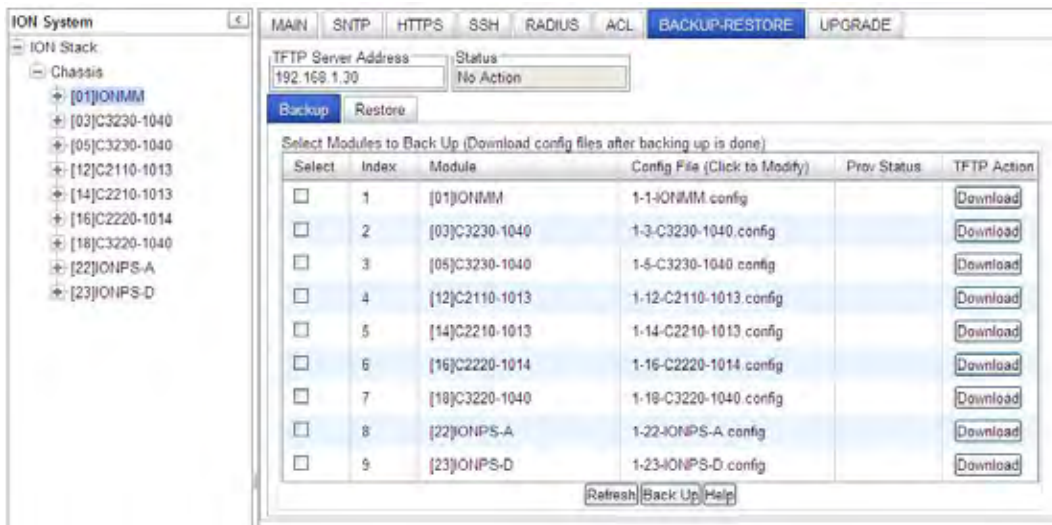
Backing Up Slide-In and Remote Module Configuration

The following procedure describes how to back up the configuration of one or more slide-in or remote modules in the ION system. The backup file is stored in x323x NID memory. Note that a backup/restore operation of a NID with full configuration (maximum entries for all dynamic tables) may take a long time (approximately 50 minutes).

When you execute a backup/restore, the status will change to ‘Success’ approximately one second after you start the backup/restore, but actually it is still ongoing in the background. A message displays saying that action is ongoing; after the action is finished, then the status will change to ‘Success’.

If you add 255 VLAN entries via script, then perform a backup and restore, the backed up config file list totals 255 VLAN entries (less the default VLAN). When you perform the restore, it fails, due to adding the 255th VLAN entry. See “[Dynamic Table Entry Limits](#)” on page 267.

1. Access the IONMM through the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select the **BACKUP-RESTORE** tab. Select the **Backup** sub-tab if not already displayed.



3. Verify that the TFTP Server address shown is correct, that the TFTP Server is running and configured, and that the file to be downloaded is located correctly (e.g., at *C:\TFTP-Root*).
4. Verify that the card list shown in the table is correct; if not correct, fold and then unfold the "ION Stack" node in the left tree view to refresh.
5. Note the **Status** field message (Wrong Firmware, No Action, etc.).
6. In the **Select** column, check the checkbox of each module to be backed up.

Section 5: Operations

7. Do you want to rename the backup file?

Yes	No
a) In the Config File column, click the file name. b) Type a new name for the backup file. Note: the file name must be 1–63 characters long and must end with .config . c) Continue with step 8 below.	Continue with step 8 below.

8. Click the **Download** button. When completed, the message “*File has successfully transferred via TFTP*” displays.

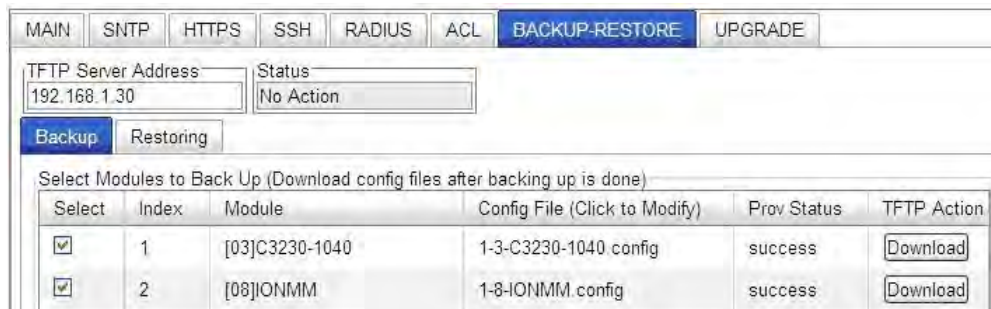
9. Click the **OK** button to clear the web page message.

10. Click the **Back Up** button. The message “*Backup is being processed ...*” displays. The Back Up operation can take several minutes.

11. At the confirmation message, click **OK**. The message “*Backup is being processed ...*” displays. The Back Up operation can take several minutes.

12. When the confirmation window displays, click **OK**. The backup file is saved in the IONMM.


The **Prov Status** column displays the provision operation result (*ongoing, success, or fail*).

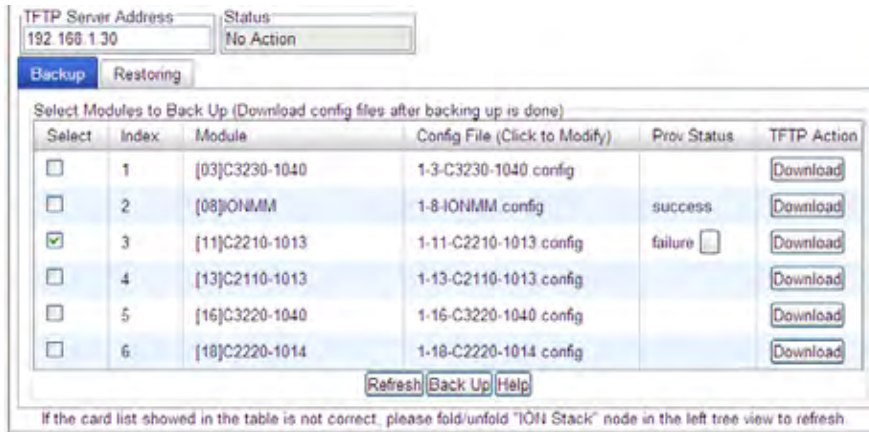


13. If the Back Up operation fails, go to step 15 below.

14. To send a copy of the backup file to the TFTP Server:

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

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



The error (.ERR) log file is downloaded to the TFTP server address specified, in TFTP-Root with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad. See “[The Config Error Log \(config.err\) File](#)” section on page 397 for error messages and possible recovery procedures.

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

- [Editing the Config File \(Optional\)](#) on page 370
- [Restoring Slide-In and Remote Modules](#) on page 371
- [Restoring Standalone Modules](#) on page 373

Backing Up Standalone Modules

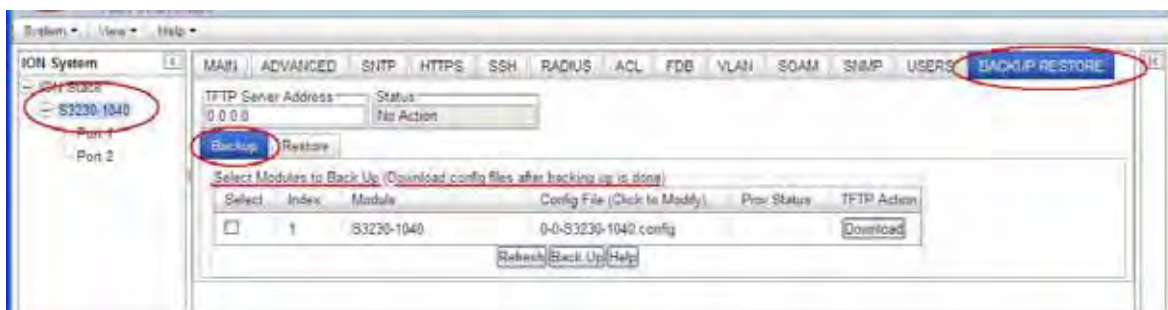
The following procedure describes how to back up the configuration of a standalone S3230 module. Note that a TFTP Server must be configured and running.

IMPORTANT



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

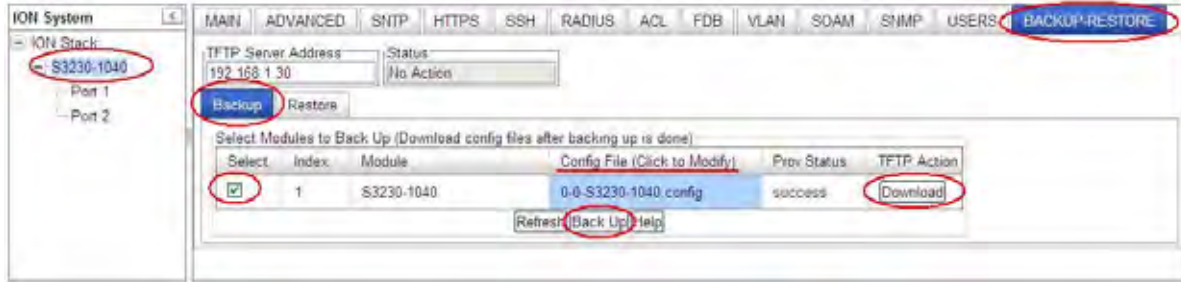
1. Access the S323x module through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **BACKUP-RESTORE** tab.



3. In the **TFTP Server Address** field enter the address of the TFTP Server.
4. In the **Select** column, check the checkbox of the module to be backed up.
5. Do you want to rename the backup file?

Yes	No
a) In the Config File column, click the file name. b) Type a new name for the backup file. Note: the file name must be from 1–63 characters in length and must end with .config . c) Continue with step 6 .	Continue with step 6 .

6. Click the **Back Up** button.



7. When the message “Backup following modules: S3230-1040, are you sure to proceed?” displays, click **OK**.

The message “Backup is being processed.” displays as the backup file is saved in the IONMM module. When the Backup is successfully completed, the message “success” displays in the Prov Status column.

8. Click the **Download** button. When completed, the message “File has successfully transferred via TFTP” displays.

9. Click the **OK** button to clear the webpage message. The config file (e.g., 0-0-S3230-1040) is saved to the C:\TFTP-Root folder.

To send a copy of the backup file to the TFTP server, be sure to:

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

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

- [Editing the Config File \(Optional\)](#) on page 370
- [Restoring Slide-In and Remote Modules](#) on page 371
- [Restoring Standalone Modules](#) on page 372

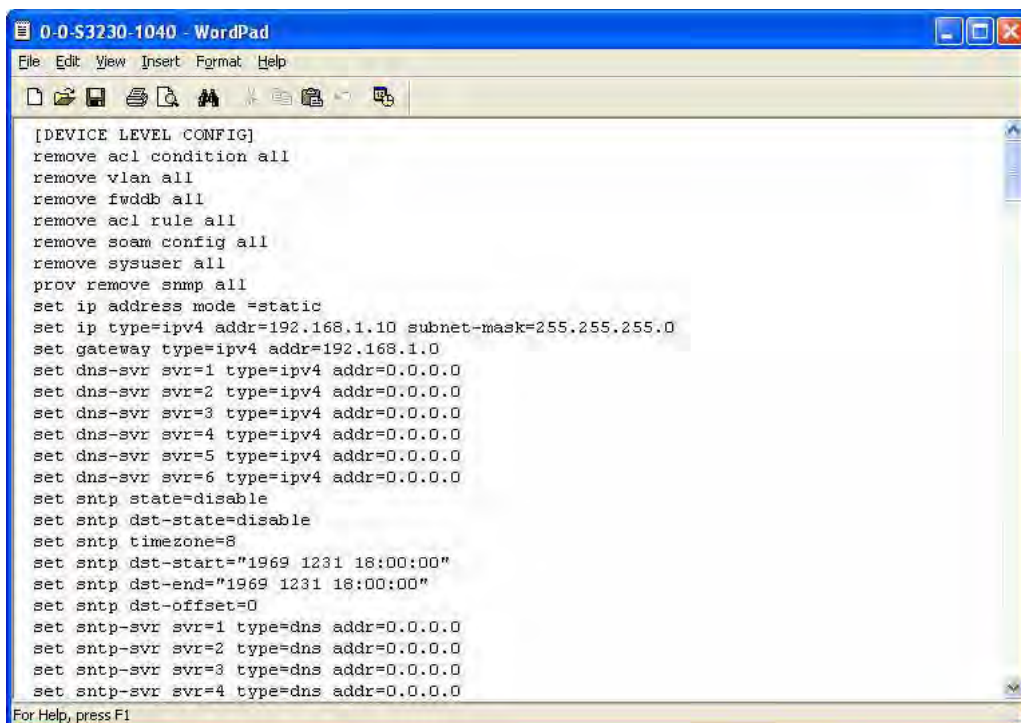
Editing the Config File (Optional)

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

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

1. Complete the applicable Backup procedure from the previous section.
2. Open the Config file (in Notepad, WordPad, Word, OpenOffice Writer, etc.) from the TFTP server location (e.g., *C:\TFTP-Root\1-9-C3231-1040.config*).
3. Edit the Config file sections. Each Config file contains a DEVICE LEVEL CONFIG section and two PORT x CONFIG sections (three PORT x CONFIG sections for the x323x).
4. Save the edited Config file back to the TFTP server location (e.g., *C:\TFTP-Root\1-9-C3231-1040.config*).
5. Continue with the applicable Restore procedure from the following section using the edited Config file.

A sample portion of a typical Config file is shown below in WordPad.



```
[DEVICE LEVEL CONFIG]
remove acl condition all
remove vlan all
remove fwddb all
remove acl rule all
remove soam config all
remove sysuser all
prov remove snmp all
set ip address mode =static
set ip type=ipv4 addr=192.168.1.10 subnet-mask=255.255.255.0
set gateway type=ipv4 addr=192.168.1.0
set dns-svr svr=1 type=ipv4 addr=0.0.0.0
set dns-svr svr=2 type=ipv4 addr=0.0.0.0
set dns-svr svr=3 type=ipv4 addr=0.0.0.0
set dns-svr svr=4 type=ipv4 addr=0.0.0.0
set dns-svr svr=5 type=ipv4 addr=0.0.0.0
set dns-svr svr=6 type=ipv4 addr=0.0.0.0
set sntp state=disable
set sntp dst-state=disable
set sntp timezone=8
set sntp dst-start="1969 1231 18:00:00"
set sntp dst-end="1969 1231 18:00:00"
set sntp dst-offset=0
set sntp-svr svr=1 type=dns addr=0.0.0.0
set sntp-svr svr=2 type=dns addr=0.0.0.0
set sntp-svr svr=3 type=dns addr=0.0.0.0
set sntp-svr svr=4 type=dns addr=0.0.0.0
```

For Help, press F1

Restoring Slide-In and Remote Modules' Configuration

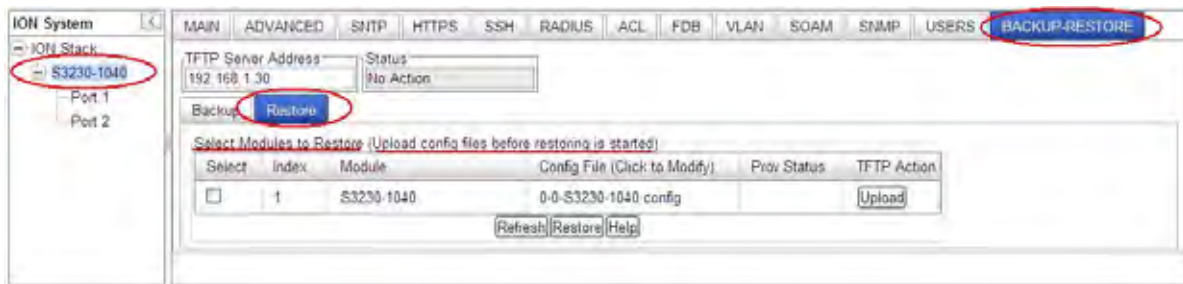
The following procedure describes how to restore the configuration of one or more slide-in or remote modules in the ION system.

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

IMPORTANT

A restore operation can only be performed for a module that had its configuration file backed up (see [Backing Up Standalone Modules](#) on page 252).

1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 45).
2. At the **BACKUP-RESTORE** tab, select the **Restore** sub-tab. The “Select Modules to Restore” table displays.



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

Section 5: Operations

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

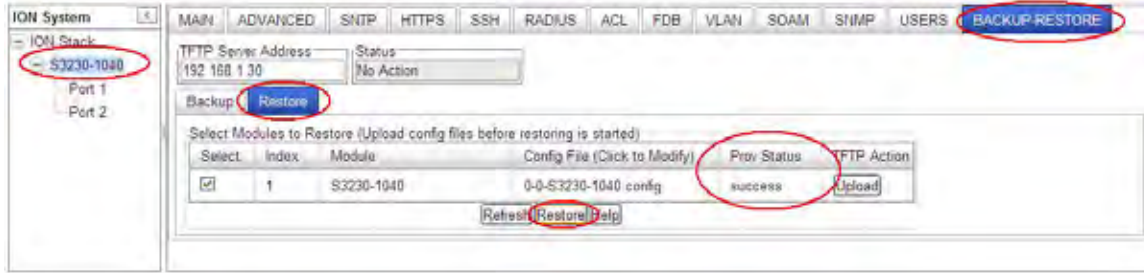
Yes	No
a) In the Config File column, click the file name. b) Type the name of the backup file to be restored. Note: the file name must end with .config . c) Continue with step 6 .	Continue with step 7 .


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

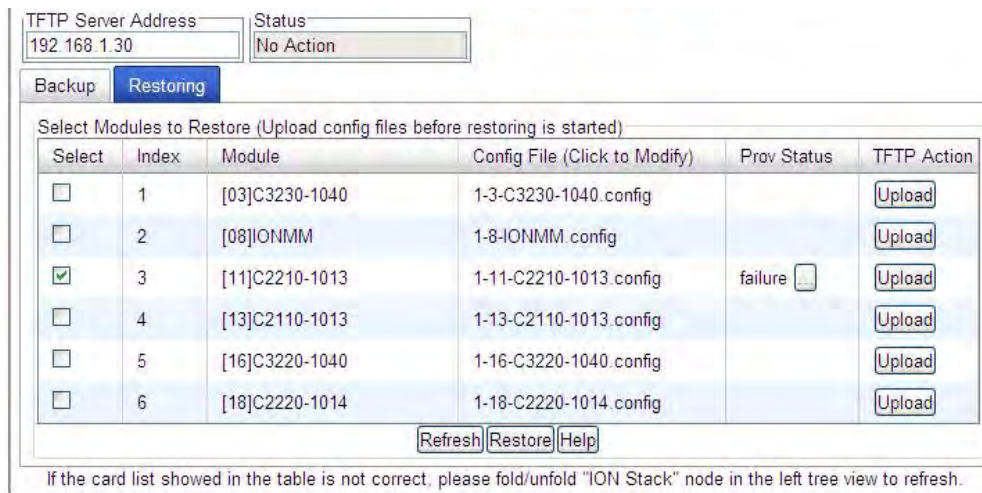
Yes	No
a) In the TFTP Server Address field, enter the IP address of the server. b) Click Upload . c) When the successful transfer message displays, click OK . d) Continue with step 7 .	Continue with step 8 .

8. Click the **Upload** button. The config file is uploaded via the TFTP server. When done, the message “*File has been successfully transferred via TFTP.*”
9. Click the **OK** button to clear the webpage message.
10. Click the **Restore** button.
11. When the “*Restore following modules: S3230-1040, are you sure to proceed?*” message displays, click **OK**.

The configuration will be restored from the specified file. During the Restore operation the message “*Restoring is being processed ...*” displays, and the **Prov Status** column displays “ongoing”. When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.



12. If the **Restore** operation fails, the **Prov Status** column displays **failure**  click the box to download an error log from the device.



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

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

Section 5: Operations

```

1-3-C3230-1040.config - WordPad
File Edit View Insert Format Help

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

```

See “[The Config Error Log \(config.err\) File](#)” section on page 397 for error messages and possible recovery procedures.

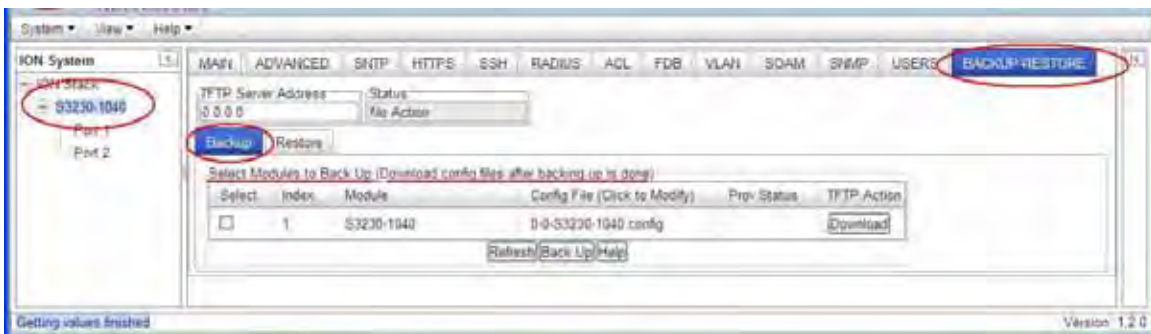
Restoring Standalone Modules

The following procedure describes how to restore the configuration of a standalone module.

IMPORTANT

A restore operation can only be performed for a module that had its configuration file backed up (see [Backing Up Standalone Modules](#) on page 152).

1. Access the IONMM module through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **BACKUP-RESTORE** tab.
3. Select the **Restore** sub-tab. The “Modules to Restore” table displays.



4. In the **Select** column, check the checkbox of the module to be restored.
5. Is the configuration file to be restored different than the one shown in the **Config File** column?

Yes	No
<p>a) In the Config File column, click the file name.</p> <p>b) Type the name of the backup file to be restored. Note: the file name must end with .config.</p> <p>c) Continue with step 5.</p>	<p>Continue with step 5.</p>

Section 5: Operations

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

Yes	No
a) In the TFTP Server Address field, enter the IP address of the server. b) Click Upload . c) When the successful transfer message displays, click OK . d) Continue with step 6.	Continue with step 6.

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

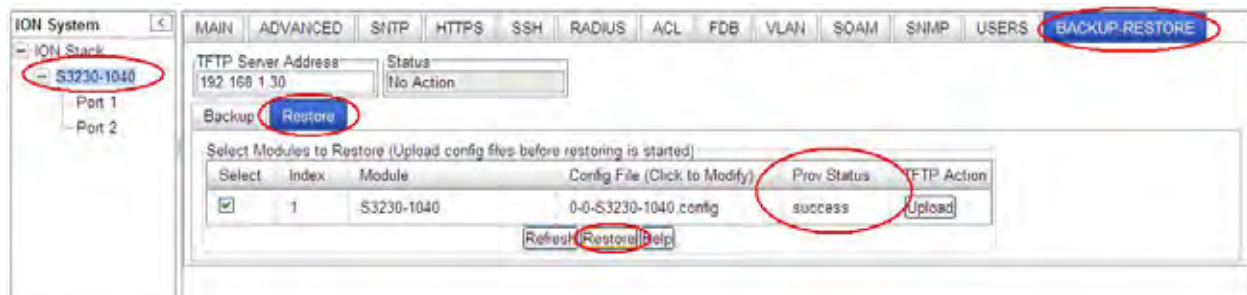
8. Click the **OK** button to clear the Webpage message.


9. Click the **Restore** button.

10. When the confirmation window displays, click **OK**.

The configuration will be restored from the specified file. During the Restore operation the message “*Restoring is being processed ...*” displays, and the **Prov Status** column displays “ongoing”.

When the Restore operation is successfully completed, *success* displays in the **Prov Status** column.



11. If the **Restore** operation fails, the **Prov Status** column displays *failure* . Click the checkbox to download an error log from the device.

TFTP Server Address: 192.168.1.30 Status: No Action

Backup **Restoring**

Select Modules to Restore (Upload config files before restoring is started)

Select	Index	Module	Config File (Click to Modify)	Prov Status	TFTP Action
<input type="checkbox"/>	1	[03]C3230-1040	1-3-C3230-1040.config		<input type="button" value="Upload"/>
<input type="checkbox"/>	2	[08]IONMM	1-8-IONMM.config		<input type="button" value="Upload"/>
<input checked="" type="checkbox"/>	3	[11]C2210-1013	1-11-C2210-1013.config	failure <input type="button" value="..."/>	<input type="button" value="Upload"/>
<input type="checkbox"/>	4	[13]C2110-1013	1-13-C2110-1013.config		<input type="button" value="Upload"/>
<input type="checkbox"/>	5	[16]C3220-1040	1-16-C3220-1040.config		<input type="button" value="Upload"/>
<input type="checkbox"/>	6	[18]C2220-1014	1-18-C2220-1014.config		<input type="button" value="Upload"/>

If the card list showed in the table is not correct, please fold/unfold "ION Stack" node in the left tree view to refresh.

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

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

```

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

See “[The Config Error Log \(config.err\) File](#)” on page 353 for message descriptions.

Back Up and Restore File Content and Location

The IONMM card stores all configuration backup files, HTTPS certification file, SSH key file, and Syslog file.

Note: Doing a reboot, restart, an upgrade or a reset to factory settings may cause some configuration backup files, HTTPS certification file, SSH key file, and Syslog files to be lost.

The Back Up operation backs up all of the SNMP settings (the same as what can be set via the Web interface / CLI) for one SIC into a file containing a list of CLI commands. This file can be downloaded from IONMM. When restoring for one SIC, you can upload a provisioning backup file (this file must have been made via the Backup operation and must be for the same SIC type) to the IONMM and do a Restore. See the IONMM **BACKUP-RESTORE** (provisioning) tab description. Currently, the Backup content includes configuration files, HTTPS certification file, SSH key file, the Syslog file, and certain other files, as outlined in the table below.

Table 30: Back Up and Restore File Content and Location

File Type	Filename	File Description	Stored Directory	Backed up? (Y/N)	Changed after Restore? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes - these files are created during Backup operation	No
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	No - not needed; the configurations included in this file are backed up by SNMP set operations.	Yes
HTTPS configuration file*	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No - not needed; the configurations included in this file are backed up by SNMP set operations	Yes
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No	No
SOAM backup files	_____	SOAM config files	_____	Yes	_____
SSH host key**	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No (see Note 1)	No
SSH user key file**	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	No (see Note 2)	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No	Always changes

File Type	Filename	File Description	Stored Directory	Backed up? (Y/N)	Changed after Restore? (Y/N)
MIB configuration files	e.g., 'agent3.conf', 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No - not needed; the configurations included in this file are backed up by SNMP set operations	Yes

Back Up and Restore Notes:

1. The HTTPS certificate is stored in '/agent3/conf/lighttpd', and is retained over power cycle and upgrades. For SSH, the host keys (RSA and DSA) are stored in '/agent3/conf/dropbear', and are also retained over power cycle and upgrades.
2. For the SSH user key, there is a 'root' user and the user key for 'root' is stored in '/root/.ssh'. This key is retained for power cycle but not upgrades. The Dropbear SSH2 server uses the Linux users as the users and it maintains the user keys with the Linux users.

Backup / Restore (Provisioning) - CLI Method

These commands can only be executed on an IONMM or a standalone SIC.

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the command prompt, check the current provisioning status. Type **show prov modules** and press **Enter**.
3. Specify a backup index item number and a config file name.
Type **set backup module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.
4. Specify a restore index item number and a config file name.
Type **set restore module-index=<1-256> config-file=STR_CFG_FILE** and press **Enter**.
5. Specify 1-10 provision modules to be backed up. Type **backup module-list=xx** and press **Enter**.
6. Specify 1-10 provision modules to be restored. Type **restore module-list=xx** and press **Enter**.
7. Verify the configuration. Type **show prov modules** and press **Enter**. For example:

```
C1|S1|L1D>show prov modules
Index      Module                               Config File                            Prov Status
-----
1          [01]IONMM                            1-1-IONMM.config
2          [02]C6210-3040                       1-2-1-C6210-3040.config
3          [02:L2]REM:S6210-3040                1-2-2-S6210-3040.config
4          [03]C3230-1040                       1-3-1-C3230-1040.config
5          [04]C6010-3040                       1-4-1-C6010-3040.config
C1|S1|L1D>set backup module-index 1 config-file xxxxx
C1|S1|L1D>set restore module-index 1 config-file 1
C1|S1|L1D>backup module-list 1
Processing...
Processing...
Backup finished
C1|S1|L1D>restore module-list 1
Processing...
Restore finished
C1|S1|L1D> C1|S1|L1D>show prov modules
Index      Module                               Config File                            Prov Status
-----
1          [01]IONMM                            1-1-IONMM.config                      success
2          [02]C6210-3040                       1-2-1-C6210-3040.config
3          [02:L2]REM:S6210-3040                1-2-2-S6210-3040.config
4          [03]C3230-1040                       1-3-1-C3230-1040.config
5          [04]C6010-3040                       1-4-1-C6010-3040.config
C1|S1|L1D>
```


An example of the backup / restore of a standalone C2230 is shown below.

```
C2230-1014 C0|S0|L1D>set backup module-index 1 config-file 0-0-S3230-1040
C2230-1014 C0|S0|L1D>set restore module-index 1 config-file 1
C2230-1014 C0|S0|L1D>backup module-list 1
Processing.....
Buckup finished
C2230-1014 C0|S0|L1D>
```

You can change the name of the “Config File” that displays when using the ‘**show provision modules**’ command. Use the **refresh provision configure filename** command to change the name of the “Config File” displayed.

Backup/Restore Status:

- No backup/restore operations are processed.*
- This card is a remote remote x2x2x/x3x2x/x3x3x SIC and now is doing backup.*
- This card is a remote remote x2x2x/x3x2x/x3x3x SIC and now is doing restore.*
- This card is an IONMM or standalone x2x2x/x3x2x/x3x3x SIC and now is doing backup.*
- This card is an IONMM or standalone x2x2x/x3x2x/x3x3x SIC and now is doing restore.*

Messages:

- Error: this command should be executed on a remote mode x2x2x/x3x2x/x3x3x SIC!*
- Fail to set backup/restore operation!*
- Fail to set physical index!*
- Fail to set provisioning status!*

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

Meaning: You entered an invalid Backup module list parameter.

Example:

```
Agent III C1|S1|L1D>backup module-list dddd
Invalid backup module-list, please give the parameter like module-
list=1,4,13 Agent III C1|S1|L1D>backup module-list 3333
(The session will be forced to quit after you input "3333" similar characters.)
Agent III C1|S1|L1D>backup module-list 1
The specified module does not exist!
Agent III C1|S1|L1D>backup module-list 1
Processing...

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

Recovery:

1. Enter a valid backup module-list input parameter
2. Retry the Backup operation. See the related section of the manual.
3. Contact TN Tech Support if the problem persists.

Disabling USB Console Access to the x323x

Console access to the x323x through the USB serial interface can be disabled as a security precaution. When Console access is disabled, the x323x will not respond to CLI commands entered by a local management station via the USB serial interface. The only access to the x323x will then be through either a Telnet session or the Web interface.

Note: Access via the USB serial Console interface can be disabled using either the CLI or Web method.

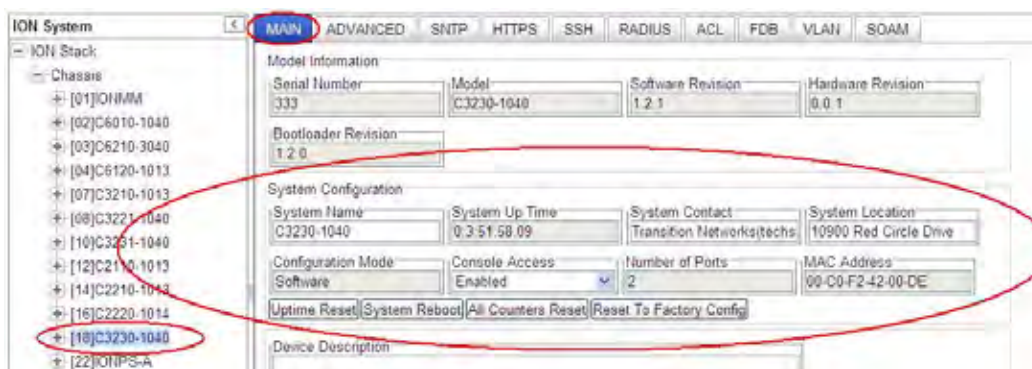
Disabling Console Access – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Set the status of the device’s USB connection to disabled. At the command prompt, type **set usb state=disable** and press **Enter**.
3. Verify the status of the device’s USB connection is disabled. Type **show usb state** and press **Enter**. The USB state displays:

```
C1 | S3 | L1D>set usb state=enable
C1 | S3 | L1D>show usb-port state
USB port state:                               enable
C1 | S3 | L1D>show usb state
USB port state:                               enable
C1 | S3 | L1D>
```

Disabling Console Access – Web Method

1. Access the x323x NID through the Web interface (see “Starting the Web Interface” on page 45).
2. At the **MAIN** tab locate the **System Configuration** section.



3. In the **Console Access** field, select **Disabled**. The default is **Enabled**.
4. Scroll to the bottom and click **Save**. With the x323x USB connection disabled, the x323x will no longer respond to CLI commands entered by a local management station (console) via the USB serial interface. The only access to the x323x will now be through either a Telnet session or the Web interface.

Displaying Information

There are several CLI commands that allow you to display (show) information about the NID configuration. For a complete description of these and other CLI commands see the *ION System CLI Reference Manual, 33461*.

Reset to Factory Defaults

If need be, you can reset all configurations in the IONMM back to their original factory defaults. This operation can be accomplished through either the CLI or Web method.

IMPORTANT



This operation deletes **all** configuration information that was saved in the IONMM, including the IP address you assigned to the IONMM.

Resetting Defaults – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the command prompt type: **reset factory** and press **Enter**. The following displays:

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

All configuration parameters will be reset to their factory values. For a list of all factory defaults, see “[Appendix B: Factory Defaults](#)” on page 399).

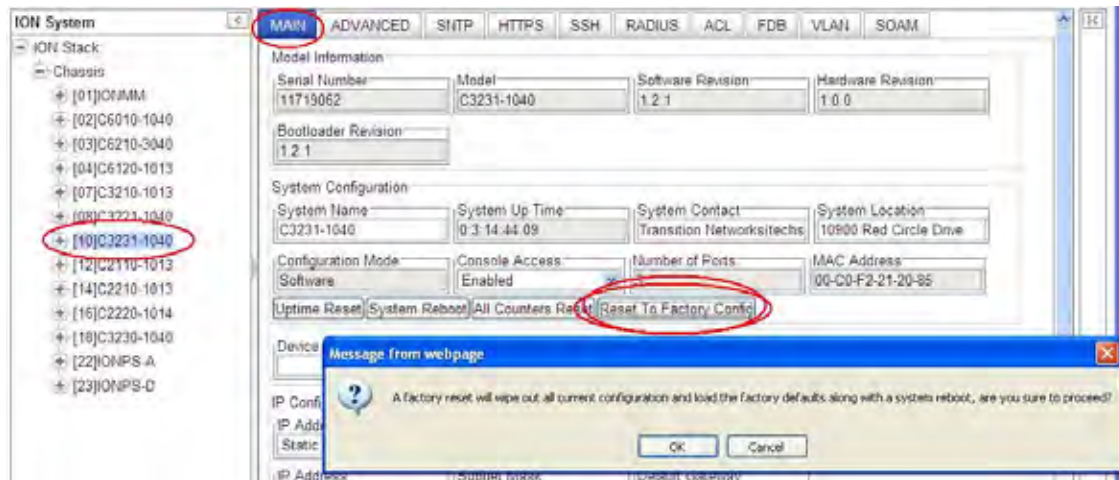
Note: Your USB and/or Telnet session will be disconnected.

3. Set the IP configuration (see “[Doing the Initial System Setup](#)” on page 48).

Resetting Defaults – Web Method

Caution: This operation deletes all configuration information that was saved in the x323x, including the IP address you assigned to the x323x.

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



4. Click the **Reset to Factory Config** button. The message “A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?” displays.
5. Click **Cancel** if you are sure you want to proceed with the Reboot. Click **OK** only if you wish to reboot.

All configuration parameters will be reset to their factory values. For a list of all factory defaults, see “Appendix B: Factory Defaults” on page 379).

Note: Your Web session will be discontinued.

6. Set the IP configuration (see “Doing the Initial System Setup” on page 48).

File Status after Reset to Factory Defaults

The table below shows the status of various [system](#) files after a reset to factory defaults.

Table 31: File Status after a Reset to Factory Defaults

File Type	Filename	File Description	Stored Directory	Status after Reset to Factory Default
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Lost
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	Restored to factory configuration
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	Restored to factory configuration
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	Restored to factory configuration
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	Restored to factory configuration
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	Restored to factory configuration (lost)
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	Lost
SOAM backup files	_____	SOAM config files	_____	Yes
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	Restored to factory configuration (lost)

Resetting Uptime

The ION system uptime field displays the amount of time that the ION system has been in operation.

The System Up Time is displayed in the format days:hours:minutes:seconds.milliseconds. For example, a **System Up Time** field display of **9:8:15:18.26** indicates the ION system has been running for 9 days, 8 hours, 15 minutes, 18 seconds, and 26 milliseconds.

The ION **System Up Time** counter can be reset via the CLI method or Web method.

Reset System Uptime – CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. At the command prompt type: **reset uptime** and press **Enter**. The System Up Time field resets to zero, and immediately begins to increment. For example:

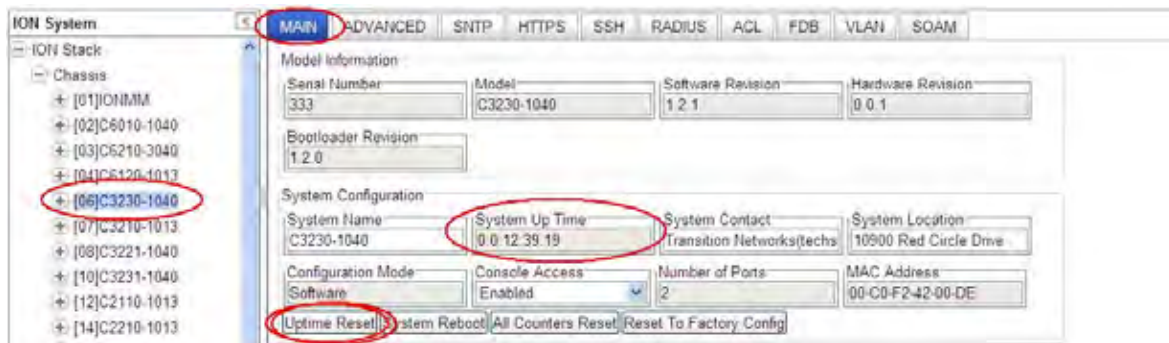
```
C3230-1014 C0|S0|L1D>reset uptime
C3230-1014 C0|S0|L1D>
```

Use the **show system information** command to display the current system uptime.

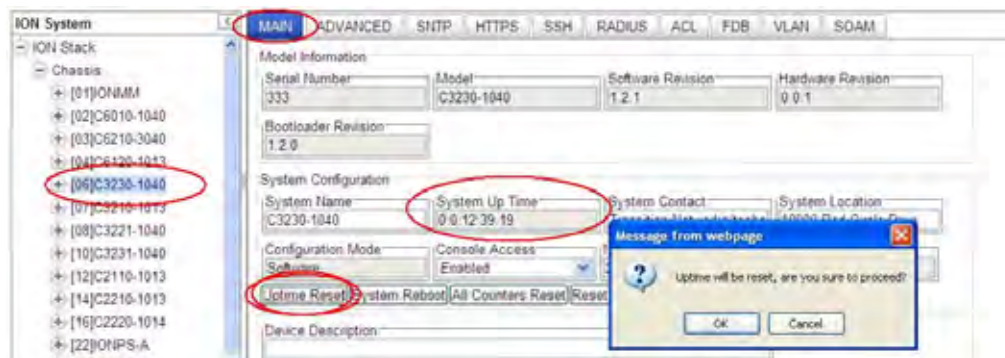
Note: The **reset uptime** command is not available for all ION devices.

Reset System Uptime – Web Method

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 26).
2. At the **MAIN** tab, locate the **System Configuration** section.



3. If desired, observe and record the **System Up Time** field count.
4. Click the **Uptime Reset** button. The message “Uptime reset, are you sure” window displays.



5. Click **OK** to reset the system up time. The message “Setting values succeeded” displays at the bottom left of the screen when the Uptime reset is done.
6. Click the **Refresh** button at the bottom of the screen. The **System Up Time** field resets to zero and immediately begins to increment.

Resetting Counters

Before running certain diagnostics / tests, you may want to reset (zero out) all or some x323x device and/or port counters.

The x323x counters can be reset via the CLI method or Web method.

Reset All Ports Counters – CLI Method

This is a device-level command to reset all of the x323x ports counters.

1. Access the x323x through either a USB connection (see “[Start a USB Session in HyperTerminal and Log In](#)” on page 70) or a Telnet session (see “[Starting a Telnet Session](#)” on page 72).
2. At the command prompt type: **reset all ports counters** and press **Enter**. For example:

```
C1|S3|L1P1>reset ?
  all
  factory
  uptime
C1|S3|L1P1>reset all ports counters
Error: this command should be executed on a device!
C1|S3|L1P1>go l1d
C1|S3|L1D>reset all ports counters
C1|S3|L1D>
```

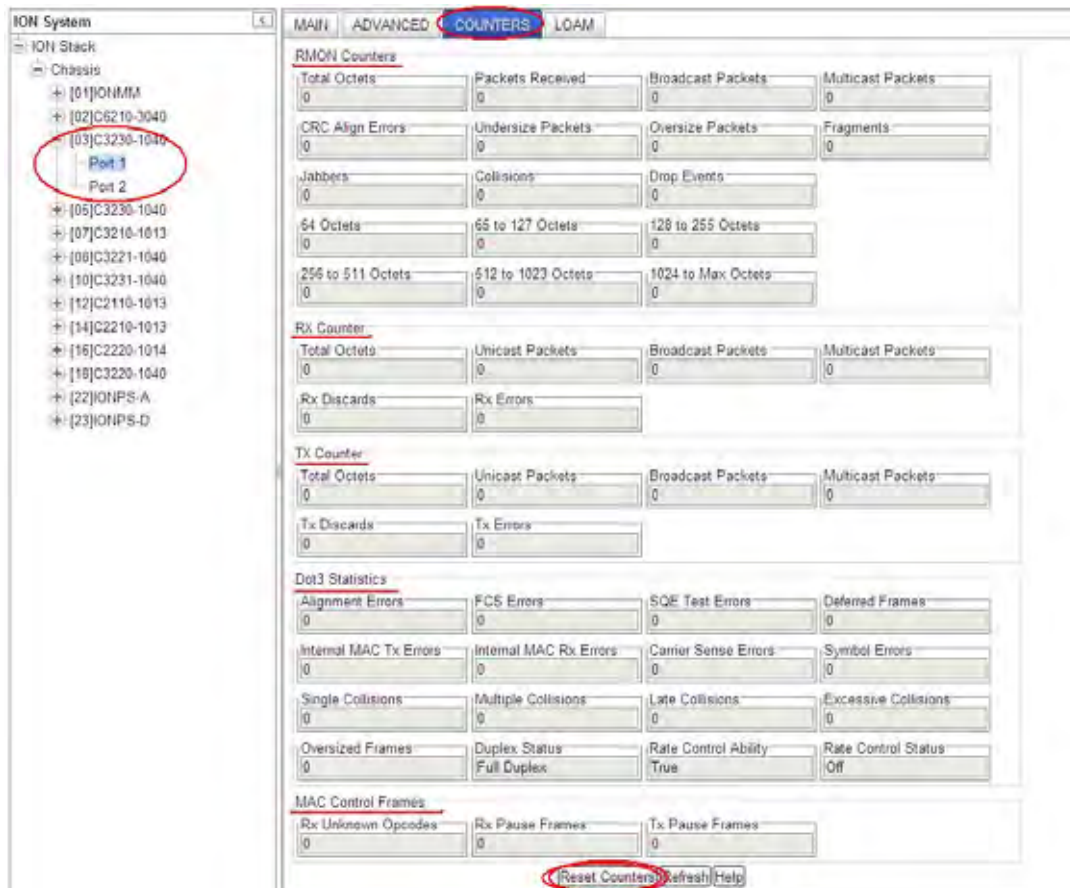
Use the **show ether statistics** command to display Port Counters Received, Port Counters Sent, and related information.

The counters that are reset include all Port Counters, Port LOAM Counters, Port LOAM Event Configuration, Port LOAM Event Log, and Port DMI.

Reset Port Counters– Web Method

This is a port-level function used to reset all of an x323x port’s counters.

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 26).
2. Select the desired x323x port.
3. Select the **COUNTERS** tab.



4. If desired, click the **Refresh** button and observe and record the various counter field counts for later comparison.
5. Click the **Reset Counters** button. The x323x port-level counters are reset to zero and begin incrementing immediately. The counters that are reset include:
 - RMON Counters
 - Rx Counter
 - Tx Counter
 - Dot3 Statistics
 - MAC Control Frames

Section 5: Operations

Clear All Ethernet Port Counters – CLI Method

This is a port-level command to reset all of an x323x port's Ethernet counters.

1. Access the x323x through either a USB connection (see “[Start a USB Session in HyperTerminal and Log In](#)” on page 70) or a Telnet session (see “[Starting a Telnet Session](#)” on page 72).
2. Select the desired x323x port.
3. At the command prompt type **clear ether all counters** and press **Enter**. For example:

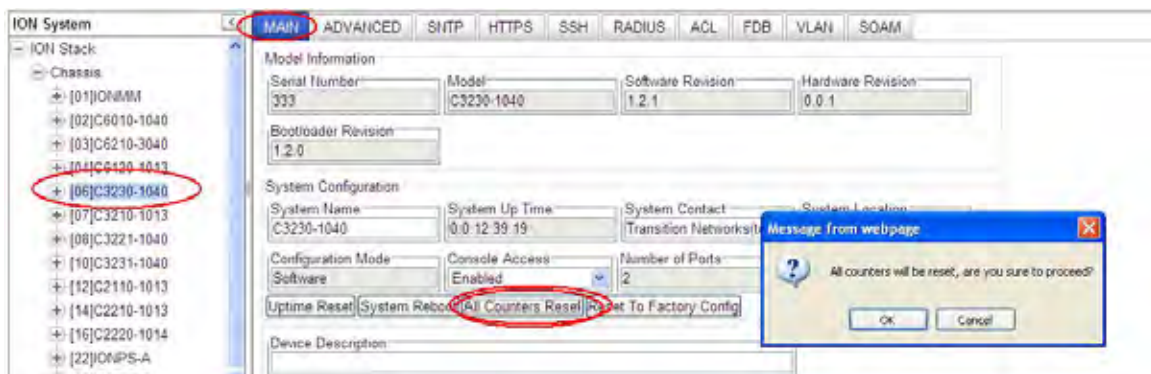
```
C1|S3|L1D>clear ether all counters
Error: this command should be executed on a port!
C1|S3|L1D>go llp=1
C1|S3|L1P1>clear ether all counters
C1|S3|L1P1>
```

The counters that are reset include all Port Counters, Port LOAM Counters, Port LOAM Event Configuration, Port LOAM Event Log, and Port DMI.

All Counters Reset – Web Method

This is a device-level function to reset all of the x323x counters.

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 26).
2. At the **MAIN** tab, locate the **System Configuration** section.
3. If desired, observe and record the various counter field counts for later comparison.
4. Click the **All Counters Reset** button. The message “All counters will be reset, are you sure to proceed?” displays.



5. Click the **OK** button to proceed. The x323x device counters are reset to zero and begin incrementing immediately. These counters are reset:
 - SOAM > MEP > Configuration (MEP Defects and various Statistics)
 - SOAM > MEP > Loopback (LBMs sent and LBRs received)
 - SOAM > MEP > ETH-TEST > Results
 - SOAM > MEP > DM > Results
 - SOAM > MEP > FLM > Results
 - SOAM > MIP > Statistics
 - Port > COUNTERS
 - Port > LOAM > Counters
 - Port > LOAM > Event Configuration
 - Port > LOAM > Event Log
 - Port > DMI >

Reboot

At times you may have to reboot (restart) the ION system. This operation can be accomplished by either the CLI or Web method.

Note: this operation can take several minutes. The amount of time for the reboot to complete depends on the ION system configuration. When the reboot is finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The 'red box' condition occurs while the devices are resetting; this condition can continue several minutes after the reboot.

See Table 19 in this section for file content and location after a System Reboot.

IMPORTANT



Doing a system reboot, restart, upgrade, or a reset to factory settings may cause some configuration backup files, HTTPS certification file, SSH key file, or Syslog file to be deleted.

Rebooting – CLI Method

After a reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console PC to become accessible again.

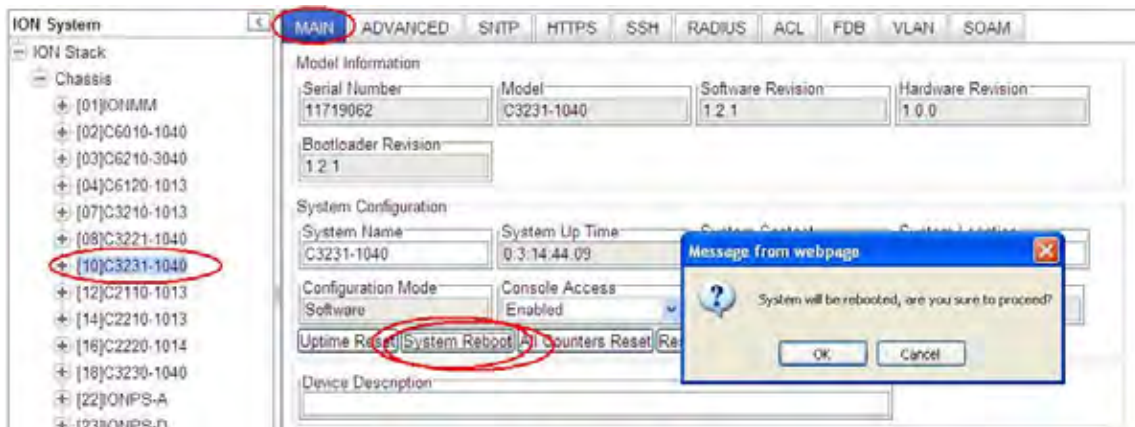
1. Access the NID through either a USB connection (see [“Starting a USB Session”](#) on page 41) or a Telnet session (see [“Starting a Telnet Session”](#) on page 43).
2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login again!* The ION system reboots. If this operation is performed on a standalone module, the connection / session is terminated.
3. To reestablish the connection / session, wait about one minute, and then:
 - For a USB connection:
 - a) Select **Call>Disconnect**.
 - b) Select **File>Exit**.
 - c) Disconnect then reconnect one end of the USB cable.
 - d) Start a USB session (see [“Starting a USB Session”](#) on page 41).
 - For a Telnet session:
 - a) Press **Enter**.
 - b) Start a Telnet session (see [“Starting a Telnet Session”](#) on page 43).

Rebooting – Web Method

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

Note: If you have a USB or Telnet session established, terminate the session before doing the reboot.

1. Access the x323x through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.
4. Click the **System Reboot** button. The confirmation message “System will be rebooted, are you sure to proceed?” displays.



5. At the confirmation window, click the **OK** button to start the reboot, or click **Cancel** to quit the reboot.

The x323x will restart and will be available for operations after about one minute.

Reboot File Content and Location

The table below shows file content and location resulting from a system re-boot.

Table 32: File Content and Location after a System Reboot

File Type	Filename	File Description	Stored Directory	Lost after Reboot? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes
Net-SNMP configuration file	snmpd.conf	This a configuration file for Net-SNMP	/agent3/conf/snmp	No
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No
SOAM backup files	_____	SOAM config files	_____	Yes
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

Upgrade the IONMM and/or NID Firmware

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

Note: Transition Networks recommends that before completing any steps on an install that you verify that the IONMM and NIDs have the latest firmware version installed and running. The latest firmware version is at:

<http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>. Ideally, all the cards in a chassis will be upgraded to the latest versions at the same time; running devices with a mix of old and new firmware can cause a “red box” condition. See “Section 6: Troubleshooting” on page 332.

Note: You can not upgrade a module with multiple BIN files.



Upgrading a NID may cause some of its configuration backup files to be lost.

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

Upgrading IONMM and/or NID Firmware – CLI Method

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

1. Access the IONMM through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Display the current version of the IONMM firmware. Type **show card info** and press **Enter**.
3. Determine the current TFTP server address using the **prov** command and press **Enter**.
For example:

```
prov get tftp svr addr
prov set tftp svr type=(ipv4|dns) addr=ADDR
```

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

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

Section 5: Operations

8. Unzip the file. Type **update firmware-db file=FILENAME** and press **Enter**.
9. Verify the Update results. Type **show firmware-db update result** and press **Enter**.
10. Upgrade the module. Type **upgrade module** and press **Enter**.
11. A table of available modules displays with upgrade instructions.

```
C1|S7|L1D>upgrade module
Available modules:

index      module                                     loc
-----
1          ION219                                    c=1 s=0 11d
2          C3230-1040                               c=1 s=3 11d
3          C3230-1040                               c=1 s=5 11d
4          S3230-1040                               c=1 s=5 llap=2 l2d
5          IONMM                                      c=1 s=7 11d
6          C3231-1040                               c=1 s=10 11d
7          C2110-1013                               c=1 s=12 11d
8          C2210-1013                               c=1 s=13 11d
9          C2220-1014                               c=1 s=16 11d
10         C3220-1040                               c=1 s=18 11d
11         IONPS-A                                   c=1 s=22 11d

Choose the module you want to upgrade: (eg. 1,3,16; at most 8 modules to
  upgrade, press 'q' to exit upgrade)
1,2,3,4,5,6,10,11

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

12. Choose the module(s) to upgrade (# **1-6,10,11** in the example above) and press **Enter**. If you need to exit the upgrade, press the **q** key and the press **Enter** to return to the command prompt.
13. Verify the Upgrade results. Type **show firmware upgrade result** and press **Enter**. The firmware upgrade results are displayed in a table. If the firmware upgrade was successful, the *time started* and *time completed* display.

```
C1|S7|L1D>show firmware upgrade result
index      module                                     status   reason   time started   time completed
-----
1          card registering...                       success                                     00:21:23       00:21:32
2          C3230-1040 c=1 s=3 11d                   inProgress                               00:21:23       00:00:00
3          C3230-1040 c=1 s=5 11d                   inProgress                               00:21:24       00:00:00
4          S3230-1040 c=1 s=5 llap=2 l2d            inProgress                               00:21:24       00:00:00
5          IONMM c=1 s=7 11d                         success                                     00:21:24       00:21:47
6          C3231-1040 c=1 s=10 11d                  inProgress                               00:21:26       00:00:00
7          C3220-1040 c=1 s=18 11d                 inProgress                               00:21:26       00:00:00
8          IONPS-A c=1 s=22 11d                    success                                     00:21:29       00:21:40
C1|S7|L1D>
```

If a module upgrade was unsuccessful, the reason for the failure displays in the “reason” column of the table (e.g., *invalid input file*, *protocol timeout*). See “[Section 5 – Troubleshooting](#)” on page 401 for error messages and recovery procedures.

Upgrading IONMM and/or NID Firmware – Web Method

The following describes the procedure for upgrading the firmware in the IONMM through the Web Interface. If the IONMM is to be upgraded at the same time as other modules in the ION Chassis, see [Upgrading Slide-In and Remote Modules](#).

Note: Doing an IONMM / x323x firmware upgrade will cause all configuration backup files to be lost.

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

A. Verify the Current IONMM / NID Firmware Version

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

1. Access the IONMM via the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select the **MAIN** tab and locate the **Software Revision** area in the **Model Information** section. (You can also use the **Help** dropdown and select **About ION System Web Interface** to determine the current firmware version.)
3. Note the current version of the x323x or IONMM firmware for use in steps D1 and D2 below.

B. Locate the New IONMM / NID Firmware Version

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

1. Go to the Transition Networks Software Upgrades web page at <http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.
2. Locate the “**Agent Firmware**” section and examine the link in the right hand column (e.g., “**Download x323x_1.0.5_AP.bin**”).
3. Compare the IONMM / NID version displayed in the **MAIN** tab **Software Revision** area with the version number on the web site, and continue if the web site version is newer than the current (running) version.
4. Click the link located in step 1 above to download the new firmware file.

C. Run TFTP Server

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

1. Install, run and configure the TFTP Server.
2. Copy the file downloaded in step 4 above to the required TFTP Server location.
Note: the upgrade file must be resident in the default directory on the TFTP server (normally *C:TFTP-Root*).
3. Note the location of the downloaded file and its filename for use in steps D1 and D2 below.

Section 5: Operations

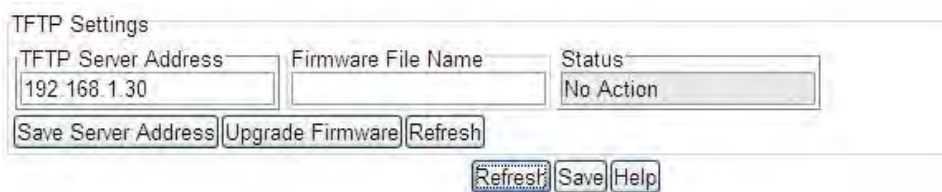
D. Upgrade the IONMM / NID Firmware

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

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

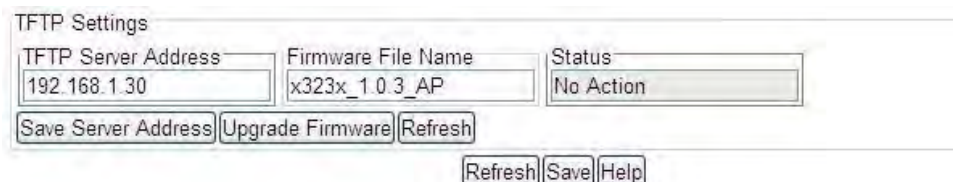
D1. Upgrade IONMM / NID Firmware from the **MAIN** tab.

1. Access the IONMM card through the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select the **MAIN** tab.
3. Locate the **TFTP Settings** section at the bottom of the screen.



TFTP Settings		
TFTP Server Address 192.168.1.30	Firmware File Name 	Status No Action
Save Server Address	Upgrade Firmware	Refresh
Refresh Save Help		

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



TFTP Settings		
TFTP Server Address 192.168.1.30	Firmware File Name x323x_1.0.3_AP	Status No Action
Save Server Address	Upgrade Firmware	Refresh
Refresh Save Help		

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

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

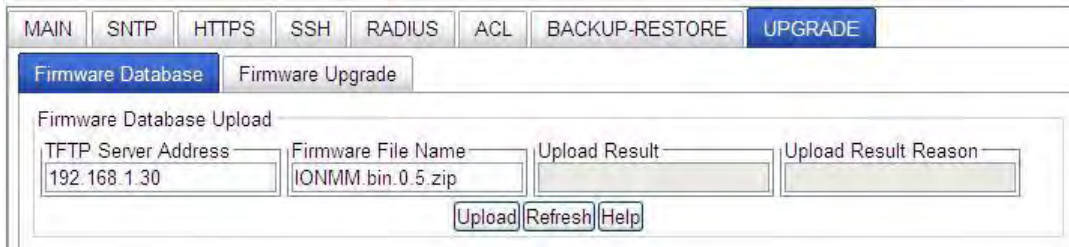
7. Click **OK**.

The file is downloaded and the x323x and/or IONMM reboots. When the reboot is complete, the message “[xx]IONMM rebooting finished” displays.

8. Click the **Refresh** button. The **Software Revision** area is updated from the old version number to the new version number (e.g., from 1.0.3 to 1.0.5).
9. If you will be using the same TFTP Server Address for future upgrades, click the **Save Server Address** button.

D2. Upgrade IONMM / NID Firmware from the UPGRADE Tab

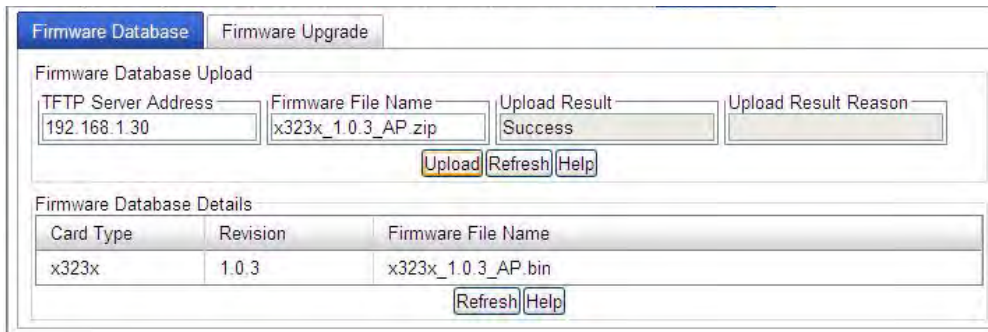
1. Access the IONMM card through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **UPGRADE** tab.
3. Select the **Firmware Database** sub-tab if not already selected.
4. Locate the **Firmware Database Upload** section.



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

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

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



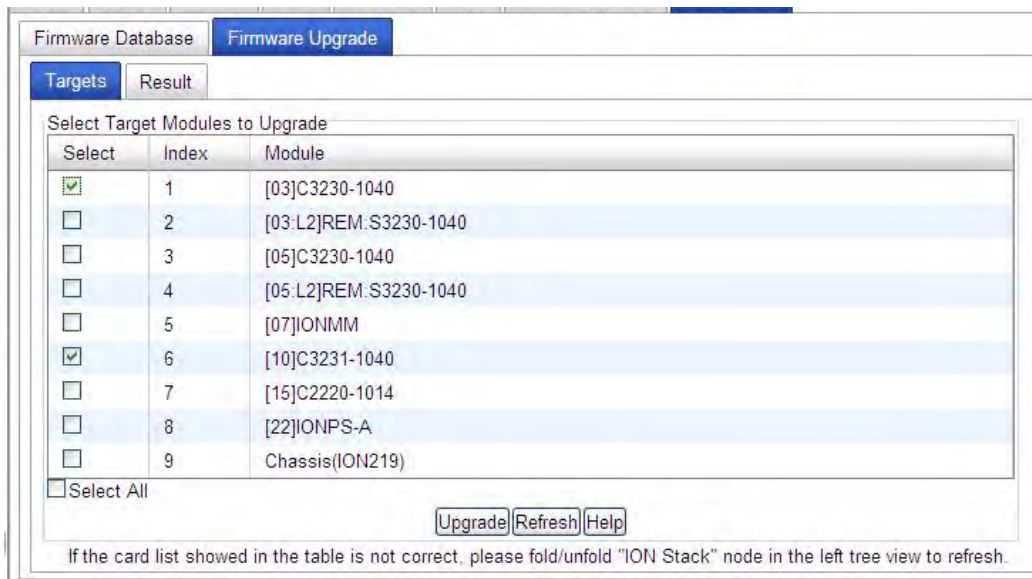
Card Type	Revision	Firmware File Name
x323x	1.0.3	x323x_1.0.3_AP.bin

8. If the firmware upload operation failed, the **Upload Result** area displays either:
 - **None**: no operation was performed, or
 - **Failure**: the specified operation has failed.

Section 5: Operations

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

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



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

Firmware Database		Firmware Upgrade			
Targets		Result			
Result of Upgrade					
Index	Module	Status	Reason	Time Started	Time Completed
1	[03]C3230-1040	in progress		0:2:55:27.00	0:0:00:00.00
2	[10]C3231-1040	in progress		0:2:55:27.00	0:0:00:00.00
3				0:0:00:00.00	0:0:00:00.00
4				0:0:00:00.00	0:0:00:00.00
5				0:0:00:00.00	0:0:00:00.00
6				0:0:00:00.00	0:0:00:00.00
7				0:0:00:00.00	0:0:00:00.00
8				0:0:00:00.00	0:0:00:00.00

Refresh Help

15. Click the **Refresh** button.

Firmware Database		Firmware Upgrade			
Targets		Result			
Result of Upgrade					
Index	Module	Status	Reason	Time Started	Time Completed
1	[03]C3230-1040	in progress		0:2:55:27.00	0:0:00:00.00
2	[10]C3231-1040	success		0:2:55:27.00	0:2:58:36.00

16. If upgrading more than one device, you may have to click **Refresh** again.

Firmware Database		Firmware Upgrade			
Targets		Result			
Result of Upgrade					
Index	Module	Status	Reason	Time Started	Time Completed
1	[03]C3230-1040	success		0:2:55:27.00	0:2:59:42.00
2	[10]C3231-1040	success		0:2:55:27.00	0:2:58:36.00
3				0:0:00:00.00	0:0:00:00.00
4				0:0:00:00.00	0:0:00:00.00
5				0:0:00:00.00	0:0:00:00.00
6				0:0:00:00.00	0:0:00:00.00
7				0:0:00:00.00	0:0:00:00.00
8				0:0:00:00.00	0:0:00:00.00

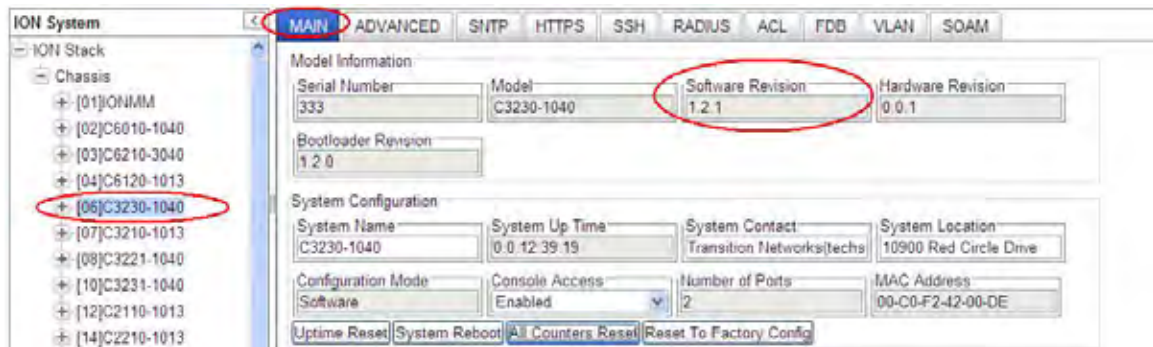
Refresh Help

Note: the upgrade will take one or more minutes to complete. The exact amount of time for the upgrade depends on the number of modules being upgraded.

17. After the upgrade has successfully completed, “*success*” displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See “[Section 5 – Troubleshooting](#)” on page 301 for error messages and recovery procedures.

Section 5: Operations

18. Check the **MAIN** tab for each upgraded module to ensure that the correct revision level is displayed in the **Software Revision** field.



The sample screen above shows the C3230 **MAIN** tab with the Software Revision field indicating a successful firmware upgrade to version **1.2.1**.

Upgrading Slide-In and Remote Modules Firmware via TFTP

This procedure is used to upgrade one or more of the slide-in modules installed in the ION Chassis or a remote module connected to a slide-in module.

Before you can upgrade the firmware in the ION system modules you must do the following:

- Have the upgrade files resident in the default directory on the TFTP Server (normally *C:/TFTP-Root*). To find the latest version of the firmware, go to:
<http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.
- Create the Database Index and Archive Files (below).
- Perform the Module Firmware Upgrade (page 299).

Creating the Database Index and Archive Files

The database index file is a listing of the modules that can be upgraded and the firmware file that will be used to upgrade each module. The index file must be named **db.idx**. The archive file is a zip file containing the index file and the firmware upgrade files. The archive file must be named **db.zip** in Windows XP. If using Windows 7, name the index file just “**db**”.

The following describes the procedure for creating the firmware database index and archive files.

1. Launch the program that will be used to create the index file (**db.idx**).

Note: a program such as Notepad can be used to create the file.

2. Make an entry for each firmware file to be used for the upgrade in the following format:

model rev file

where:

model = name of the module

rev = revision level of the firmware upgrade file

file = name of the firmware upgrade file

Note: Each of the three fields must be separated by a single space or a single tab.

EXAMPLE

Below is a sample **db.idx** file for a system that has three chassis-resident modules (IONMM, C3220-1040, and C3231-1040), and no second level remotes.

IONMM	1.1.0	IONMM.bin.1.1.0_AP
C3220-1040	1.1.0	x222x_x322x.bin. 1.1.0_AP
C3231-1040	1.0.5	x323x.bin. 1.1.0_AP

3. Save the file as **db.idx**.

Section 5: Operations

Note: if you used a program, such as Notepad, that does not allow you to save the file as .idx, then save it as a text file and rename it (i.e., change *db.txt* to *db.idx*).

4. Create a zip file that contains each of the upgrade files and the index file. Save the .zip file to the TFTP Server root directory (e.g., filename of **x323x.bin.1.0.5.zip**).

For example, using the files listed in the EXAMPLE above, the db.zip file would contain the following four files:

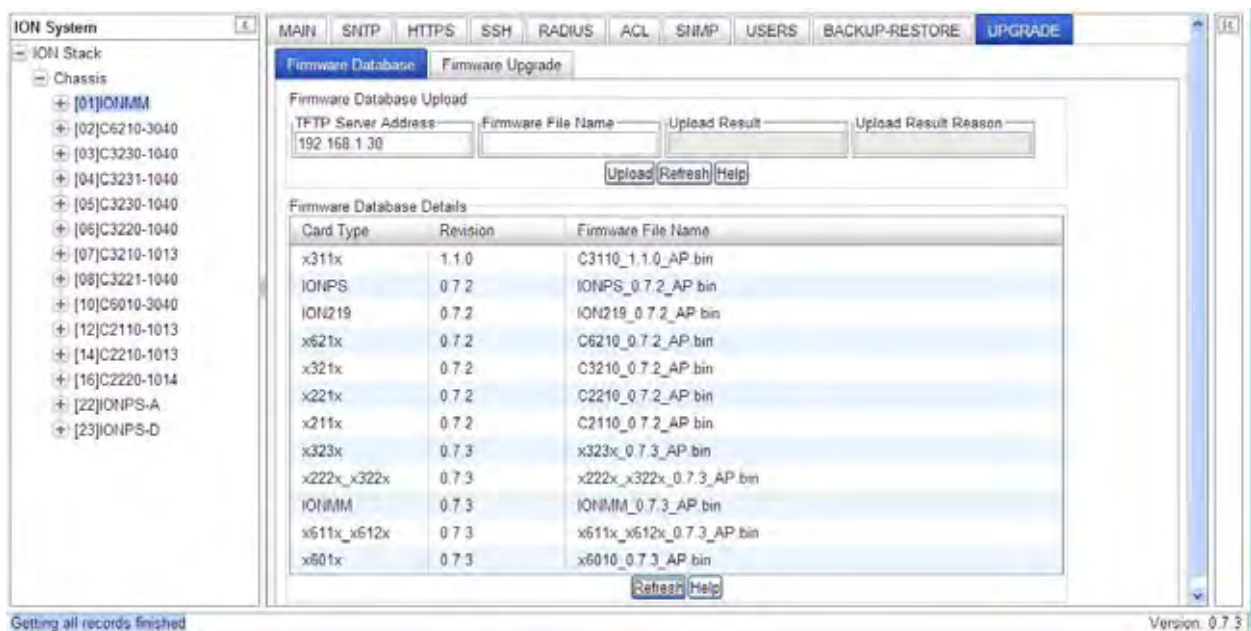
- db.idx
- IONMM.bin.1.1.0_AP
- x222x_x322x.bin. 1.1.0_AP
- x323x.bin. 1.1.0_AP

5. Perform the upgrade (see [Performing the Module Firmware Upgrade](#) below).

Performing the Module Firmware Upgrade

The upgrade consists of two parts: uploading the archive file to the IONMM, and then loading the upgrade file into the appropriate modules. The following procedure is for upgrading the ION family modules. This procedure assumes that the TFTP server is running and is configured to send and receive transmissions, and that it contains the .zip file created on the previous page.

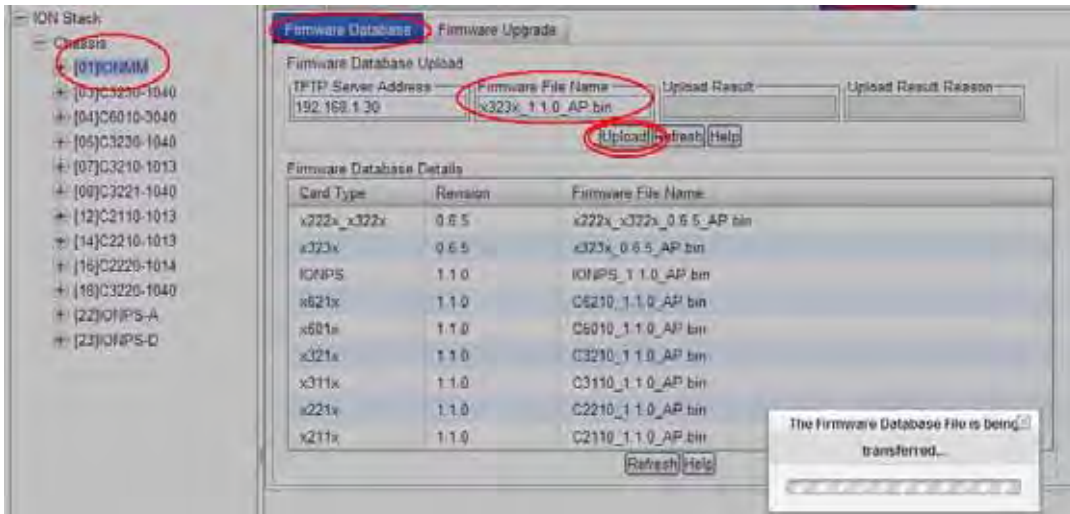
1. Access the IONMM through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **Upgrade** tab. The **Firmware Database** sub-tab displays.



3. In the **TFTP Server Address** field, enter the IP address of the TFTP Server where the upgrade (.bin) file is located.

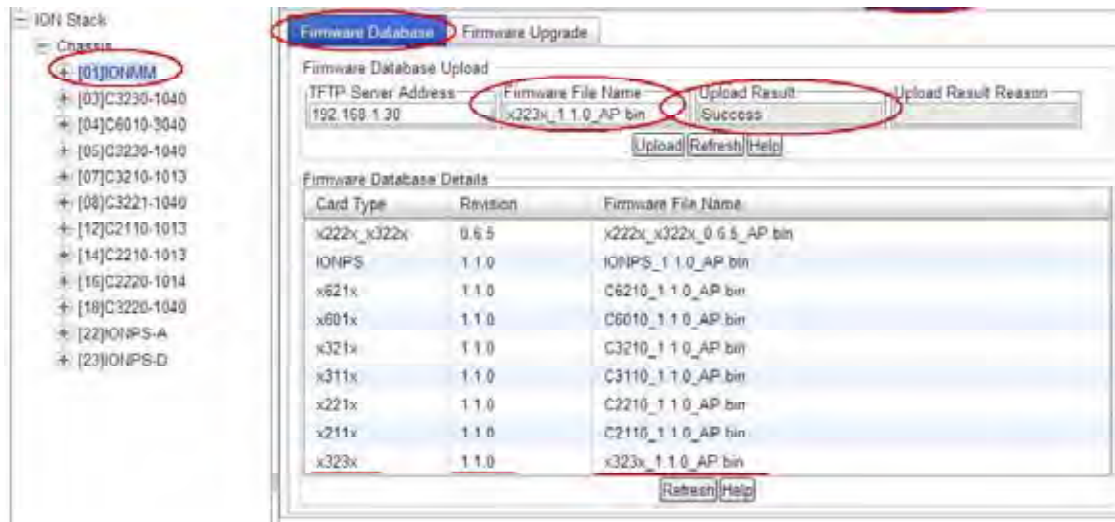
- In the **Firmware File Name** field, enter the name of the file you created (e.g., **x323x_1.1.0_AP.bin**).
Note: Be sure to include the .bin extension in the filename.
- Click the **Upload** button.

The firmware file is uploaded from the TFTP server. **Note:** this operation can take several minutes. The amount of time for the upload to complete depends on the size of the file. The messages “*Getting values in progress*” and “*Getting values finished*” display during the upload process.



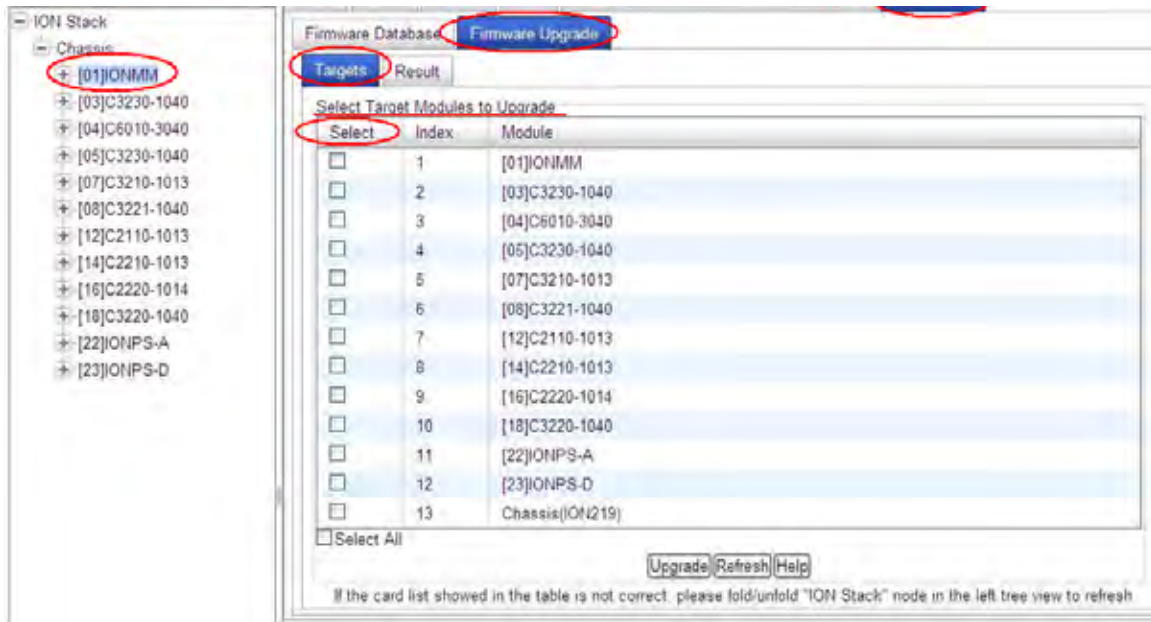
- Wait for the file to successfully upload. The messages “*The Firmware Database File is being transferred...*” and “*Getting all records finished*” display during the upload process.

The message “*Success*” displays in the **Upload Result** field and the modules listed in the **db.idx** file will be listed in the **Firmware Database Details** table.



- Select the **Firmware Upgrade** sub-tab. The **Targets** sub-tab displays.

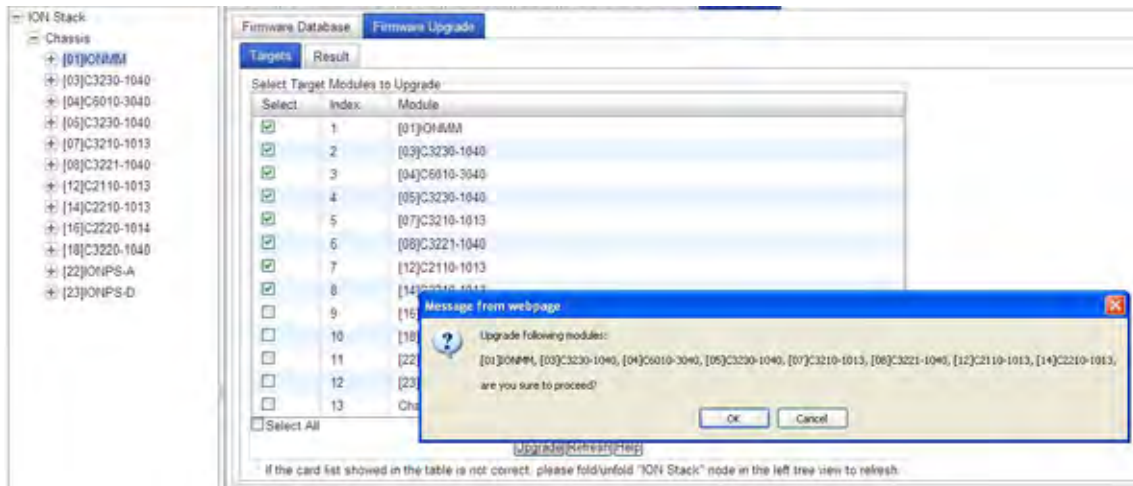
Section 5: Operations



8. In the **Select** column, check the checkbox of each module to be upgraded.

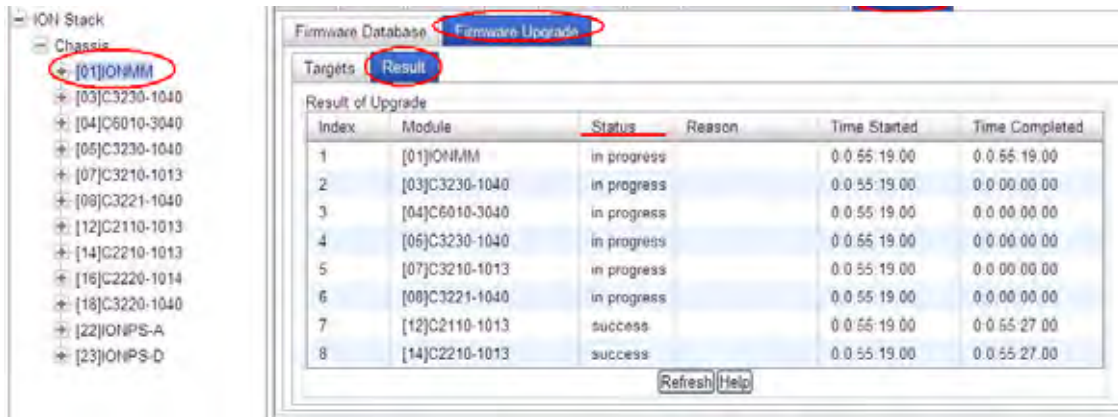
Note: You **CAN NOT** upgrade a module and a remote module connected to it at the same time. In order to upgrade both, you must first do one and then the other.

9. Click the **Upgrade** button.

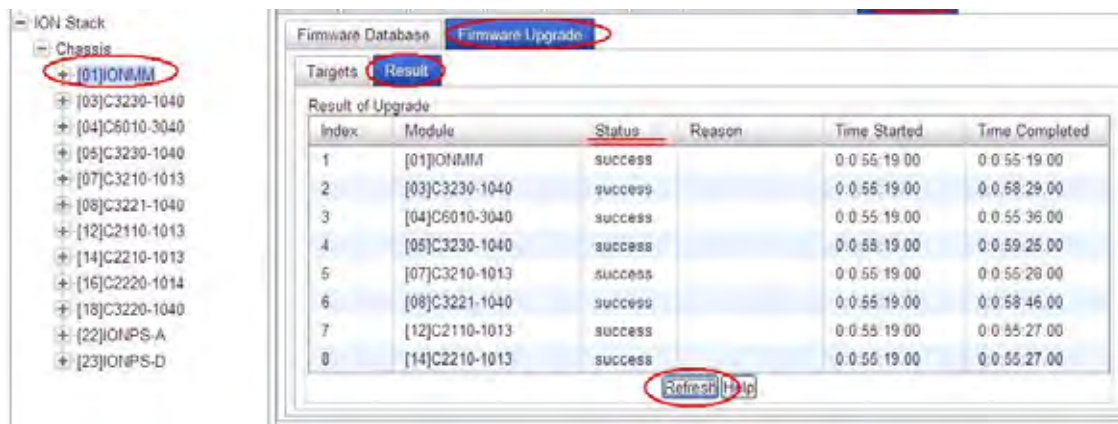


10. When the confirmation window displays, click **OK**.

11. To monitor the progress, select the **Result** sub-tab and click **Refresh**.



If the Status *in progress* displays, click Refresh again; the Status *success* displays.



Note: the upgrade will take one or more minutes to complete. The exact amount of time for the upgrade depends on the number and model of modules being upgraded.

After the upgrade has successfully completed, “*success*” displays in the **Status** column of the Result sub-tab window. If the upgrade fails, the **Reason** column displays a failure code. See “Section 5 – Troubleshooting” on page 261 for error messages and recovery procedures.

- Check the **MAIN** tab for each module to ensure that the correct revision level is displayed in the **Software Revision** field.



The sample screen above shows the C3230 **MAIN** tab with the **Software Revision** field indicating a successful firmware upgrade to version **1.2.1**.

Section 5: Operations

Upgrading Standalone Module Firmware via TFTP Server

This procedure is used to upgrade a remote stand-alone S323x NID, a local stand-alone C323x module installed in the ION Chassis, or a remote x323x module connected to a slide-in module.

Before you can upgrade the firmware in the ION system modules you must do the following:

- Have the TFTP Server configured and running.
- Have the upgrade files resident in the default directory on the TFTP Server (normally TFTP-Root).

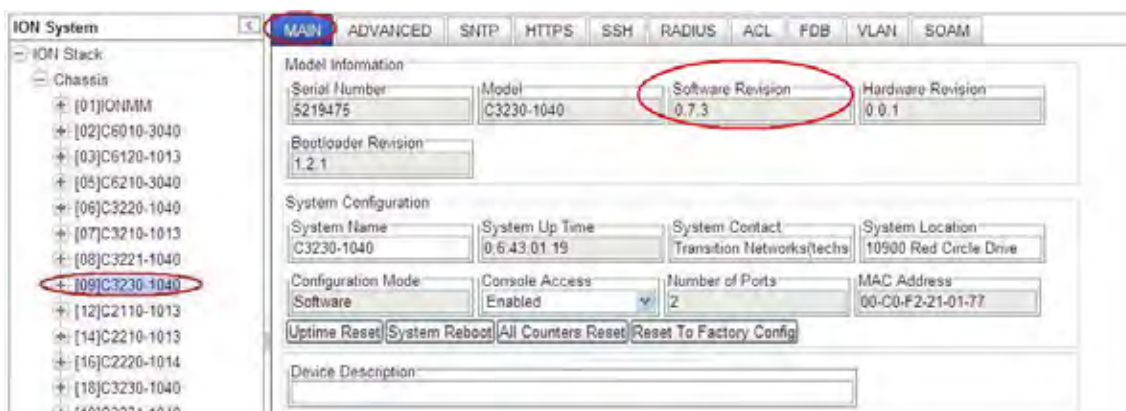
To find the latest version of the firmware, go to:

<http://www.transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>.

- Verify that the standalone module is in the correct Switch Mode (local / remote mode). See “[Changing Switch Mode \(Local / Remote\)](#)” on page 69.

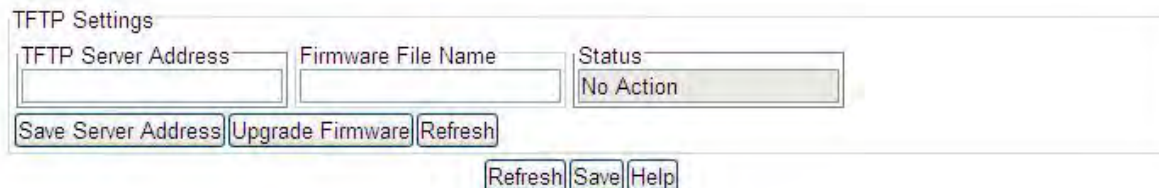
Use the procedure below for upgrading the firmware for a standalone module.

1. Access the NID through the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select the **MAIN** tab. Check the **Software Revision** field in the **Model Information** section (**0.5.1** in the sample screen below).



The screenshot shows the ION System web interface. The 'MAIN' tab is selected. In the 'Model Information' section, the 'Software Revision' field is circled in red and contains the value '0.7.3'. The '09]C3230-1040' module is highlighted in the left-hand tree view.

3. Locate the **TFTP Settings** section at the bottom of the screen.



The screenshot shows the TFTP Settings section. It includes fields for 'TFTP Server Address', 'Firmware File Name', and 'Status'. The 'Status' field contains 'No Action'. There are buttons for 'Save Server Address', 'Upgrade Firmware', 'Refresh', 'Refresh', 'Save', and 'Help'.

4. In the **TFTP Server Address** field, enter the IP address of the TFTP server that has the upgrade file (e.g., **192.168.1.30** in the sample screen below).

TFTP Settings

TFTP Server Address	Firmware File Name	Status
192.168.1.30	x222x_x322x.bin.0.5.4	No Action

Buttons: Save Server Address, Upgrade Firmware, Refresh, Refresh, Save, Help

- In the **Firmware File Name** field, enter the name of the upgrade file (*x222x_x322x.bin.0.5.4* in the sample screen above).
- Click the **Upgrade Firmware** button.
- When the confirmation window displays, click the **OK** button.

The upgrade begins. The message “*The firmware is being upgraded ...*” displays. Note that this will take one or more minutes to complete. The exact amount of time for the upgrade depends on the module being upgraded.

On successful firmware upgrade completion, the message “*S3230-1040 rebooting finished*” displays at the bottom of the screen, and the **MAIN** screen **TFTP Settings** section **Status** field displays “**Success**”.

TFTP Settings

TFTP Server Address	Firmware File Name	Status
192.168.1.30	x323x.bin.0.5.4	Success

Buttons: Save Server Address, Upgrade Firmware, Refresh, Refresh, Save, Help

If the upgrade fails, see “[Section 5 – Troubleshooting](#)” on page 326 for error messages and recovery procedures.

- You can click the **Save Server Address** button to retain the TFTP Server address entered in step 4.
- Check the module’s **MAIN** tab to ensure that the correct revision level is displayed in the **Software Revision** field (e.g., successful x323x firmware upgrade to revision *1.2.1* in the sample screens above and below).

ION System

Model Information:

Serial Number	Model	Software Revision	Hardware Revision
333	C3230-1040	1.2.1	0.0.1

Bootloader Revision: 1.2.0

System Configuration:

System Name	System Up Time	System Contact	System Location
C3230-1040	0:0:12:39:19	Transition Networks\techs	10900 Red Circle Drive

Configuration Mode: Software, Console Access: Enabled, Number of Ports: 2, MAC Address: 00-C0-F2-42-00-DE

- After the upgrade has successfully completed, continue with [Section 4: Configuration](#) procedures on page 82 or [Section 5: Operations](#) on page 242.

Firmware Upgrade File Content and Location

The table below shows file content and location resulting from a firmware upgrade.

Table 33: File Content and Location after a Firmware Upgrade

File Type	Filename	File Description	Stored Directory	Lost after Firmware Upgrade? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	No
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No
SSH user key file	authorized_keys	Currently one 'root' user provided; this file is the user key file for 'root'	/agent3/conf/root/.ssh	Yes (1)
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	Yes
SOAM backup files	_____	SOAM config files	_____	Yes
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

(1) Exception: after Upgrade from v1.0.3 to v0.5.12, the User Public-Key is missing. In ION v1.0.3, the user-public key is binding with the Linux root user and is stored in the root file system (/root/.ssh/). This file system will be replaced after this version upgrade, so this key will be lost. You can still log in through SSH, but you must upload the public key again in order to use it. In v 0.5.14, the stored key was moved from the root file system to the application flash area (/agent3/conf). This missing key problem will occur only if you upgrade from 0.5.14 to a later release. In ION versions after 0.5.14, the user-public key is saved after an upgrade.

Additional Upgrade Procedures

Additional upgrade procedures are available for the ION system. Refer to the *IONMM User Guide* for these IONMM upgrade procedures:

- Upgrade the IONMM and/or NID Firmware.
- Upgrade Slide-In and Remote Modules Firmware via TFTP. This procedure is used to upgrade one or more of the slide-in modules installed in the ION Chassis or a remote module connected to a slide-in module. Requires you to 1) Create Database Index and Archive Files, and 2) Perform the Module Firmware Upgrade.
- Perform the Module Firmware Upgrade - the upgrade consists of two parts: uploading the archive file to the IONMM, and then loading the upgrade file into the appropriate modules. This procedure is for upgrading the ION family modules.

Transfer Files via Serial Protocol (X/Y/Zmodem) - CLI Method

Use the **serial** (**get|put|upgrade**) **protocol**=(**xmodem|xmodem-1k|ymodem|zmodem**) commands to transfer a file over the USB serial line. These commands can only be entered at the device level (e.g., when the command line prompt is **C1|S8|L1P1>** or similar). These commands function similar to the TFTP download function; technical support can download configuration files and firmware files through the x323x USB port by entering the corresponding CLI commands.

General Usage: **serial** (**get|put|upgrade**) **protocol**=(**xmodem|xmodem-1k|ymodem|zmodem**) **file**=FILE%s

Perform this procedure to upgrade the C3210 firmware from the CLI.

1. Access the IONMM through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Sends a request to the server / local file system to download content for a subsequent **put** command. Type **serial get protocol zmodem file=xxxx** and press **Enter**.
3. Send a request to the server / local file system to upload content. Type **serial put protocol zmodem file=xxxx** and press **Enter**.
4. Perform a firmware upgrade over the selected serial line. Type **serial upgrade protocol zmodem file=xxxx** and press **Enter**.

For example:

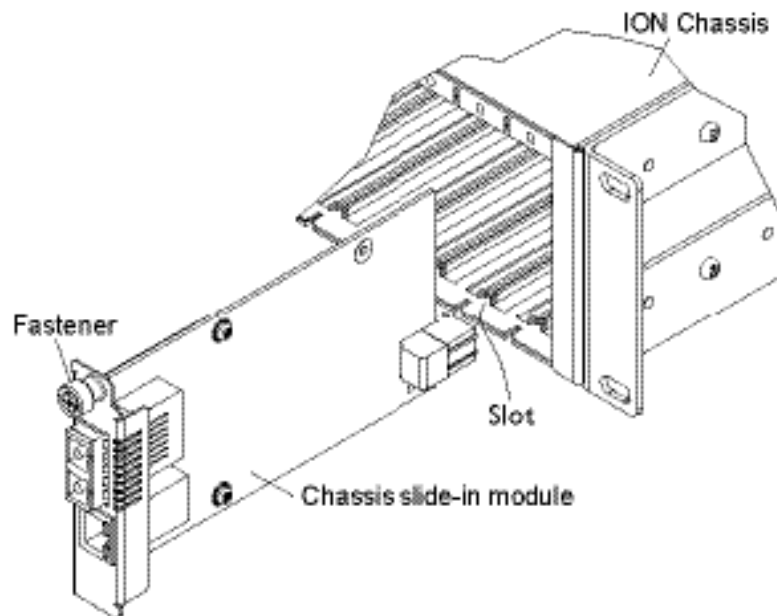
```
C1|S1|L1D>serial ?
  get
  put
  upgrade
C1|S1|L1D>serial get protocol zmodem file=xxxx
Warning: the input file name will be ignored when using ymodem/zmodem
to retrieve file!
now start to transfer the file ...
$ CCCCCCCCCC B B0 B B0 B B0 B B0 B B0 B B0 B B0 B B0
  B B0 B B0 B B0 B B0 B B0
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file ...
$ 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!
C1|S1|L1D>serial upgrade protocol zmodem file=xxxx
now start to transfer the file ...
**B000000063f694ceive.**B000000063f694
CCCCCCCCCCCCBB0BBBB0BBBB0BBBB0BB0BB0BB0BB0
file transfer failed!
C1|S1|L1D>
```

If the serial file transfer causes HyperTerminal (HT) to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT.

Replacing a Chassis Resident NID

The NID is a “hot swappable” device; it can be removed and installed while the chassis is powered on. Use this procedure to replace a chassis resident NID.

1. Backup the configuration (see [Backing Up Slide-In and Remote Modules](#) on page 150).
2. Disconnect any cables attached to the NID.



3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the NID from the Chassis.
5. Carefully slide the new NID fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the NID to the chassis.
7. Connect the appropriate cables to the NID.
8. Load (restore) the configuration into the new NID (see [Restoring Slide-In and Remote Modules](#) on page 234).

Section 6: Troubleshooting

General

This section provides basic and specific problem determination processes, and a description of problem conditions that may occur or messages that may be displayed. This section also documents ION system tests, x323x jumpers, and describes where and how to get technical support.

IMPORTANT

For each procedure described in this section, do each step sequentially as indicated. If the result of a step causes the problem to be corrected, **do not** continue with the other steps in the procedure.

Basic ION System Troubleshooting

This basic process is intended to provide some high-level techniques that have been found useful in isolating ION problems. This process is not a comprehensive guide to troubleshooting the ION system. The intent here is to 1) avoid missing any important information, 2) simplify analysis of captured information, and 3) improve accuracy in finding and explaining problem causes and solutions.

This basic process applies to these ION system and related components:

- ION Chassis
- ION NIDs (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web Interface or ION command line interface - CLI).
- ION power supply
- ION Options (ION SFPs, ION LG Kit, etc.)
- Data cables, electrical cables, and electrical outlets
- Third party network equipment (circuit protection equipment, battery backup, 3rd party client or server software – RADIUS or TFTP, etc.)

When troubleshooting an ION system / network problem on site:

1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the most simple and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the NIDs are seated properly, view the CLI **show** command output, check the Syslog file, verify IP addresses and Gateway IP address, check Windows Event Viewer, ping the interface, run the various SOAM tests if functional, etc.).
6. Write down your initial 2-3 guesses as to the cause of the problem.

Section 6: Troubleshooting

7. Verify that the TN product supports the function you are attempting to perform. Your particular TN product or firmware version may not support all the features documented for this module. For the latest feature information and caveats, see the release notes for your particular device/system and firmware release.
8. Use the Web interface or command line interface (CLI) to obtain all possible operating status information (log files, test results, **show** command outputs, counters, etc.)
9. If SOAM or LOAM is configured, check the LOAM Event Log table parameters, SOAM Configuration Error List, etc. Print the output if possible.
10. Use the ION system manual procedure to retry the failed function or operation.
11. For the failed function or operation, verify that you entered valid parameters using the cursor-over-help (COH) and/or the ION system manual.
12. Based on the symptoms recorded, work back through each step in the process or operation to recall a point at which the problem occurred, and examine for a possible failure point and fix for each.
13. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
14. Isolate the 1-2 most likely main causes of what went wrong, and gain as much information as you can to prove the suspected cause(s).
15. If you find a sequence of actions that causes the problem to recur, replicate the full sequence several times and document it if possible.
16. Review your logged information and add any other comments that occur to you about what has taken place in terms of system behavior and suspected problem causes and solutions.
17. Review the “[Recording Model Information and System Information](#)” section on page 438 before calling TN for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED fault and activity displays ([page 462](#))
- Problem Conditions ([page 464](#))
- CLI Messages ([page 481](#))
- Web Interface Messages ([page 496](#))
- Syslog Messages ([page 512](#))
- Webpage Messages ([page 534](#))
- Config Error Log (config.err File) Messages ([page 559](#))
- SOAM Configuration Error Messages ([page 569](#))
- Third Party Tool Messages (HyperTerminal, Ping, and Telnet Messages) ([page 537](#))

These message types and their recommended recovery procedures are covered in the following subsections.

LED Fault and Activity Displays

Refer to this section if the LEDs indicate a problem. For any LED problem indication, review the “[Front Panel Connections and LEDs](#)” section on page 54, and then perform the following steps.

1. Check the power cord connections and power outlet.
2. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
3. Make sure the USB cable is properly connected.
4. Check the power supply voltages (see related documentation).
5. Verify that the ION system devices have the latest firmware versions. Download the latest firmware version and upgrade as necessary.
6. Check if other network devices are working properly.
7. Run the SOAM tests and checks:
 - CC Monitoring (Continuity Checks Monitoring) on page [158](#)
 - Loopback (LB) on page [164](#)
 - Linktrace on page [169](#)
 - ETH-MCC (Ethernet Maintenance Communication Channel) on page [175](#)
 - ETH-TEST on page [179](#)
 - DM (Frame Delay Measurement) on page [184](#)
 - FLM (Frame Loss Measurement) on page [191](#)
 - Ethernet Alarm Indication Signal (AIS) on page [195](#)
 - Ethernet Remote Defect Indication (RDI) on page [200](#)

Power (PWR) LED is off (not lit):

1. Check for a loose power cord.
2. Check for a power supply failure. Replace power supply if failed.
3. Make sure all circuit protection and connection equipment and devices are working.
4. Verify that the ION system power supply is within operating range.
5. Remove the card from the chassis and re-insert it. Replace if failed.
6. Make sure the mode displayed matches the hardware setting on the device. See the “[Jumper Settings](#)” section on page [512](#).

LACT (Link Activity) LED off (not lit):

1. Check the data cables for obvious problems, incorrect type, incorrect wiring, etc.
2. See if the administrator has manually disabled the console device (PC) via the Web interface.
3. Check if other network devices are working properly.
4. Remove the suspect card from the chassis and re-insert it.
5. Check Auto-Negotiation setting.
6. See if the port transmission mode / speed (full or half-duplex, etc.) match those of the attached device.
7. Verify that the ION system devices have the latest firmware versions (see “[Upgrade the IONMM and/or NID Firmware](#)” on page [312](#)). Download the latest firmware version and upgrade as necessary.

Section 6: Troubleshooting

Fault LED is lit:

1. Check for a problem with the IONMM or NID hardware, software, or configuration.
2. Make sure all circuit protection and connection equipment and devices are working.
3. Verify that the ION system power supply is within operating range.
4. Remove the card from the chassis and re-insert it.
5. Make sure the USB cable is properly connected.
6. Reset the IONMM.

TX or RX LED off (not flashing):

1. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
2. Check if other network devices are working properly.
3. Verify that the ION system devices have the latest firmware versions.
4. Download the latest firmware version and upgrade as necessary.
5. Remove the card from the chassis and re-insert it.

Troubleshooting Auto-negotiation Mismatches

The IEEE 802.3ab Auto-negotiation protocol manages the switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, causing a mismatch and reducing performance. A mismatch can occur when:

1. A manually set speed or duplex parameter is different than the manually set speed or duplex parameter on the connected port.
2. A port is set to auto-negotiate, and the connected port is set to full duplex with no AutoNegotiation.

To maximize performance and ensure a link, follow one of these two guidelines when changing the settings for duplex and speed:

1. Set both ports to auto-negotiate both speed and duplex, or
2. Manually set the speed and duplex parameters for the ports on both ends of the connection.

IPv6 Troubleshooting

Start by using these third party resources when performing general IPv6 problem solving:

- The standard Windows 7 command-line tools with full IPv6 functionality (Ping, Ipconfig, Pathping, Tracert, Netstat, and Route all support IPv6).
- The IPv6-specific tools in the Netsh command.

Address Resolution in Windows 7

In unicast global IPv6 (equal to IPv4 Public) addresses, the 64-bit host portion of the address is derived from the MAC address of the network adapter. The Neighbor Discovery (ND) protocol resolves IPv6 addresses to MAC addresses. The resolution of host names to IPv6 addresses is done by DNS with the exception of link-local (equivalent to IPv4 APIPA) addresses, which resolve automatically. DNS handles records for IPv6 host names similar to IPv4 and also uses pointer (PTR) records to perform reverse lookups. Where DNS is not implemented (e.g., peer-to-peer environments) the Peer Name Resolution Protocol (PNRP) provides dynamic name registration and name resolution.

Verify IPv6 Configuration in Windows 7

The main tool is Ipconfig. The command **ipconfig /all** displays both IPv4 and IPv6 configuration. To display the configuration of only the IPv6 interfaces use netsh. The **netsh interface ipv6 show address** command displays each interface IPv6 address including the interface ID after the % character (the configuration can be accessed via the GUI).

Verify IPv6 Connectivity

Try to **ping** the local address. Note that if pinging link-local addresses from one host to another, you must include the destination adapter interface ID (e.g., ping fe80::38e7:3df1:f5ff:fd0%13). When pinging site-local (equal to IPv4 Private) addresses you can add the interface ID to ensure that the address is configured on the desired interface. You must add an 'allow' rule for ICMPv6 traffic to pass through each computer's firewall.

Command examples - third party CLI commands for IPv6:

```
ipconfig /all
netsh interface ipv6 show address
ping fe80::38e7:3df1:f5ff:fd0%13)
netsh interface ipv6 delete neighbors
netsh interface ipv6 show neighbors
netsh interface ipv6 delete destinationcache
netsh interface ipv6 show destinationcache
netsh interface ipv6 show route
route print
tracert -d <destination IPv6 address>
pathping -d <destination IPv6 address>
```

For Additional Information

IPv6 Forum at <http://www.ipv6forum.com/>

ARIN (American Registry for Internet Numbers) at

https://www.arin.net/knowledge/ipv6_info_center.html

or ARIN wiki at http://www.getipv6.info/index.php/Main_Page

Cisco: <http://www.ciscopress.com/articles/article.asp?p=777892&seqNum=7>

Troubleshooting IPv6 on Windows 7: <http://itexpertvoice.com/home/troubleshooting-ipv6-on-windows-7-and-why-its-worth-the-bother/>

Troubleshooting IPv6 on Windows Servers (Microsoft TechNet): [http://technet.microsoft.com/en-us/library/cc780623\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc780623(ws.10).aspx)

Test IPv6 Connectivity Using the ping6 Command (Windows XP)

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_pro_diag_ping6_conn.mspx?mfr=true

IPv6 Auto Config Troubleshooting

Determine whether your particular computer will require reconfiguration. For example, for Microsoft .NET Framework version 2.0 and later, IPv6 is enabled by default. For .NET Framework version 1.1 and earlier, IPv6 is disabled by default. For more information see the MSDN article at <http://msdn.microsoft.com/en-us/library/8db2058t.aspx>. Windows Server 2008 provides complete support for IPv6 and all of its features, and does not need additional installation or configuration.

For Windows 7 see <http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx>.

For Windows XP see <http://support.microsoft.com/kb/2478747>.

For Windows Vista see <http://ipv6.com/articles/general/IPv6-Microsoft-Vista.htm>.

For Linux / BSD, see <http://ipv6.com/articles/applications/Linux-and-BSD.htm> or

http://tldp.org/HOWTO/html_single/Linux+IPv6-HOWTO/ or your distribution documentation and/or website.

Problem Conditions

Cannot access the NID via USB port

1. If you can access the IONMM, continue with step 2 below. If you can not access the IONMM, see the IONMM User Guide.
2. Check that the syntax for the go command is correct. The **go** command format is:

```
go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

 (for a slide in card), or

```
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

 (for a standalone card).
3. Make sure that SSH Server, RADIUS client and HTTPS state are all set to disable. The related SSH, RADIUS, and HTTPS information is below:
 - Use the **set ssh service state / show ssh config** commands. See "[Configuring SSH](#)" on page 258.
 - Use the **set https state / show https config** commands. See "[Configuring HTTPS](#)" on page 234.
 - Use the **set radius client state / show radius config** commands. See "[Configuring RADIUS](#)" on page 248.
4. Power cycle the NID.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot access the NID via Telnet

1. If you can access the IONMM, continue with step 2 below. If you can not access the IONMM, see the IONMM User Guide.
 Check that the syntax used for the **go** command is correct. The **go** command syntax is:

```
go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

 (for a slide in card), or

```
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

 (for a standalone card).
2. Make sure that SSH Server, RADIUS client and HTTPS state are all set to disable. The related SSH, RADIUS, and HTTPS information is below:
 - Use the **set ssh service state / show ssh config** commands. See "[Configuring SSH](#)" on page 258.
 - Use the **set https state / show https config** commands. See "[Configuring HTTPS](#)" on page 234.

- Use the **set radius client state** / **show radius config** commands. See "[Configuring RADIUS](#)" on page 248.
3. Power cycle the NID.
 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot access the NID via the Web

1. If you can access the IONMM, continue with step 2 below. If you can not access the IONMM, see the IONMM User Guide.
2. Make sure that SSH Server, RADIUS client and HTTPS state are all set to disabled.
3. Power cycle the NID.
4. If the NID is a remote, power cycle the local NID.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot activate IP-based management

1. Verify that the IP, gateway, and subnet mask are configured correctly.
2. With DHCP enabled, DHCP could have failed leaving the system with the old static IP configuration. Check the configuration via the USB port.
 - a) Access the IONMM through a USB connection (see "[Starting a USB Session](#)" on page 41).
 - b) At the command prompt, type: **show ip-mgmt config**.
 - c) Press **Enter**.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot upgrade modules

See [Upgrade fails](#) on page 177.

Cannot upload upgrade files

See [Upload fails](#) on page 177.

Section 6: Troubleshooting

Telnet connection is lost after a CLI command is executed

1. If you can connect to the IONMM through the Web interface (see “[Starting the Web Interface](#)” on page 45), go to step 3 below. If you cannot connect to the IONMM through the Web interface, continue with step 2 below.
2. Check the following:
 - the IONMM is seated properly in the chassis
 - the IONMM is powered up
 - the network cable is seated
 - the network is operational
3. For all modules (slide-in and remote) check the following:
 - module is properly seated/connected
 - module is powered up
4. Cycle power for the module in question. **Note:** for slide-in cards, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Trap Server does not record traps

1. Ensure the Trap Server application is running.
2. SNMP traps may be blocked by a router or firewall. Consult your Network administrator to determine if this is the case.
3. Check that the correct SNMP trap manager IP address has been defined for the module.
 - For Web Interface – go to the **SNMP Configuration** section on the **MAIN** tab.
 - For CLI – at the device level, type: **show snmp config**.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Upgrade fails

1. Check the following:
 - The correct module(s) has been selected.
 - The module selected is listed in the **Card Type** column on the **Firmware Database** sub-tab.
 - A hierarchy conflict does not exist (i.e., trying to upgrade a level 2 module and its level 1 module at the same time).
 - The modules are powered on.
2. Wait two minutes, and then retry the operation. If the operation still fails, continue with step 3 below.
3. Reboot the IONMM and all modules in the upgrade stream.
4. Retry the operation. **Note:** you will have to do another upload of the upgrade files.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Upload fails

1. Check the following:
 - The IONMM is powered on.
 - The IP address of the TFTP server is correct.
 - The TFTP server is online and available.
 - The correct file name, **db.zip**, is specified (including the .zip extension for Windows XP). If using Windows 7, name the file just “**db**”.
 - The **db.zip** file is in the default directory on the TFTP server.
 - The **db.zip** (or **db**) file contains the db.idx file and the upgrade files.
 - The **db.idx** file is formatted correctly (“[Creating the Database Index and Archive Files](#)” on page 148).
2. Wait three minutes then retry the operation. If the operation still fails, continue with step 3.
3. Reboot the IONMM.
4. Retry the upload operation.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

USB connection resets after a CLI command is executed

1. If you can connect to the IONMM through the Web interface (see “[Starting the Web Interface](#)” on page 45), go to step 4 of “[Telnet connection is lost after a CLI command is executed](#)” on page 168. If you can not connect to the IONMM through the Web interface, continue with step 2 below.
2. Check the following:
 - the IONMM is seated properly in the chassis
 - the IONMM is powered up
 - the network cable is seated
 - the network is operational
3. For all modules (slide-in and remote) check the following:
 - the module is properly seated/connected
 - the module is powered up
4. Cycle power for the module in question.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Configuration Mode Mismatch

On the device **MAIN** tab, in the **System Configuration** section in the **Configuration Mode** box, the mode displayed does not match the hardware setting on the device.

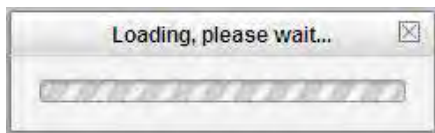
The device may have a jumper or switch that disables software management of the device. When Configuration Mode is **Hardware**, the devices take some of the configurations from DIP switches or jumpers on the device. In **Software** mode, configuration is controlled by management.

1. Collapse the "Chassis" node in the left tree view and then expand it after the newly inserted card is totally initialized.
2. Refer to the “[Jumper Settings](#)” section on page 312 for details on hardware mode configuration.
3. 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.

Ethernet connection works, but at a very low speed

1. Check if the **Auto Negotiate** feature is enabled.
2. If **Auto Negotiate** is enabled, check if one device is using full duplex while the other one is using half-duplex (a duplex mismatch condition). The usual effect of this mismatch is that the connection works but at a very low speed.
3. Change Ethernet connection settings; see "[Configuring Auto Negotiation](#)" on page 77.

loading, please wait ... Displays continuously



1. Wait for one or more minutes for discovery to complete.
2. Click the icon to close the message.
3. Check the parameter entries and retry the operation.
4. Click the **Refresh** button and try the operation again.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

No ACL condition now!

You entered a **show acl condition** CLI command, but you have not yet defined an ACL Condition.

1. Define an ACL condition. See "[Configuring an ACL](#)" on page 211.
2. Re-enter the **show acl condition** command.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

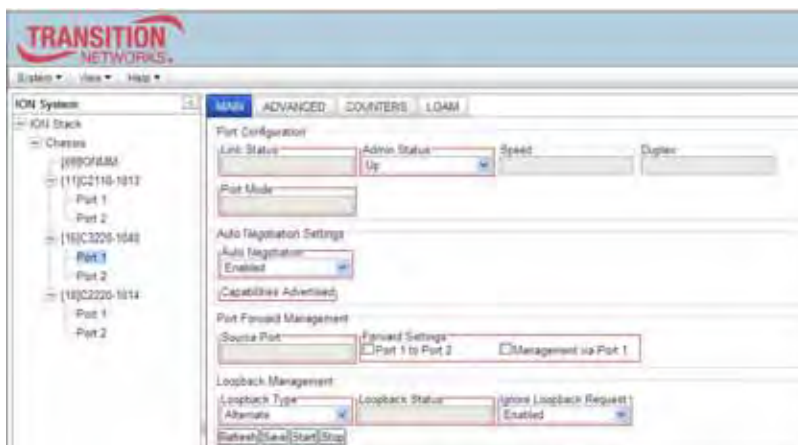
Section 6: Troubleshooting

No ACL rule now!

When doing a backup of the IONMM and several other modules, an error was detected when the IONMM was initially backed up (AGENT PM ERROR: CLI command show acl rule failed).

1. Execute a System Reboot on the IONMM.
2. Execute a backup on the IONMM alone.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



1. Check if the device is physically connected and powered on.
2. If the “*Getting values failed*” message also displays, refresh the device by clicking the **Refresh** key.
3. Collapse and then expand the ION System tree (i.e., fold and then unfold the "ION Stack" node in the left tree view) to refresh.
4. Cycle power for the device in question.
5. Reboot the device by clicking the **Reboot** key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
6. Upgrade the device(s) to the latest software version.
7. Reboot the ION System using the **System Reboot** button. See the [Reboot](#) section on page 285.
8. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Red Box Condition

When certain operations (e.g., a reboot) are finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The 'red box' condition occurs while the devices are resetting; this condition can continue several minutes after the reboot. Until the system is ready to be fully managed, certain fields may display within "red boxes". The "red boxes" will disappear when the system is ready to be fully managed.

1. Wait a couple of minutes for the current operation to complete, and then continue operation.
2. Check the devices' firmware versions. For example, a C2220 has only certain items 'red boxed'. The IONMM in this case is at latest version and shows certain new functions on the GUI, while the C2220 is at an older version and shows the newer functions as 'red boxed'. Since the older version of C2220 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as 'red boxed'. Upgrade the devices to the latest software version.
3. Reboot the system. See the "Reboot" section on page 285 for more information.
4. Contact 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.

TFTP Server Address is empty or invalid!

1. On a device MAIN tab, in the **TFTP Settings** section, you clicked the **Save Server Address** button with no TFTP Server Address entered, or with an invalid TFTP Server Address entered.
2. Enter a valid **TFTP Server Address** and click the **Save Server Address** button.

Windows XP Cannot Find Drivers For My Device

This error can occur if the information programmed into the device EEPROM do not match those listed in the INF files for the driver. If they do not match, the driver cannot be installed for that device without either reprogramming the device EEPROM or modifying the INF files.

1. Contact 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.

Section 6: Troubleshooting

Windows XP Forces a Reboot after Installing a Device

This problem can occur if an application is accessing a file while the New Hardware Wizard is trying to copy it. This usually occurs with the FTD2XX.DLL file.

1. Select not to restart the computer and then unplug and re-plug the device. This may allow the device to function properly without restarting.
2. Restart the computer to allow the device to work correctly.
3. Contact 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.

Driver Installation Fails and Windows XP Gives Error Code 10

Windows error code 10 indicates a hardware error or failed driver installation. This error may appear if a device has insufficient power to operate correctly (e.g. plugged into a bus powered hub with other devices), or may indicate a more serious hardware problem. Also, it may be indicative of USB root hub drivers being incorrectly installed.

1. Contact 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.

Windows XP Displays an Error and then Terminates Installation

If the following screen is displayed with this message, Windows XP has been configured to block the installation of any drivers that are not WHQL certified.



To successfully install the device, you must change the driver signing options to either warn or ignore to allow the installation to complete.

1. To change the current driver signing setting, in Windows XP, go to "Control Panel\System", click on the "Hardware" tab and then click "Driver Signing".
2. Select the desired signing option.

For other USB Driver / OS Messages (Win2K, Vista, Windows 7, Linux, Mac) refer to the separate document with Driver / OS install, uninstall and troubleshooting information.

Cannot find new IP address

DHCP issued address is not being displayed

IP Address Wrong

If the DHCP client is enabled on the IONMM Main page, there is no easy way to determine the new IP address. If DHCP client status set to "enable", the value of "ip address" shows the last IP address, not the current dynamic allocation IP address.

When a "**show ip-mgmt config**" command is entered on the CLI, the previous "fixed" IP address is still returned. If a Fully Qualified Domain Name is used on any of the IONMM pages to access other devices (TFTP,SNTP or Radius), or to ping another PC, they will fail because of an internal sync problem when getting the IP settings from the ION system when the DHCP client is enabled.

1. Disable the DHCP client and set the DNS server; the problem resolves. (If you enable the DHCP client and then set the DNS servers via the Web interface, this issue may occur due to the internal sync problem noted above).
2. Contact 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.

L2CP: LLDP packets will not forward when the "LLDP protocol" set to "Pass"

All the LLDP packets received are forwarded internally, as the ION system uses it to do topology discovery. The ION system checks the LLDP packets to find out whether it is an ION system LLDP packet.

If it is a Transition Network's LLDP packet (xxDP) the ION system handles it separately.

If it is not a Transition Network's LLDP packet, it may be handled in one of two ways, based on the packet verification result: if it is a valid LLDP message, the ION system will forward it to the specific port based on the port's L2CP configuration; if the packet is invalid, it is immediately discarded.

The L2CP MIB definition for xxDP forwarding states that "LLDP protocol frames with a destination address of 01-80-C2-00-00-0E which are not TN discovery LLDP frames are either discarded or passed at this port".

Little indication of an IONPS-D Power Supply failure in Web interface

Meaning: If a power supply is powered down or loses input power, the only indication on the web interface is a Power reading of 0.0. The "Power Status OK" means that the Power Sensor is operating normally, not that the input power is OK.

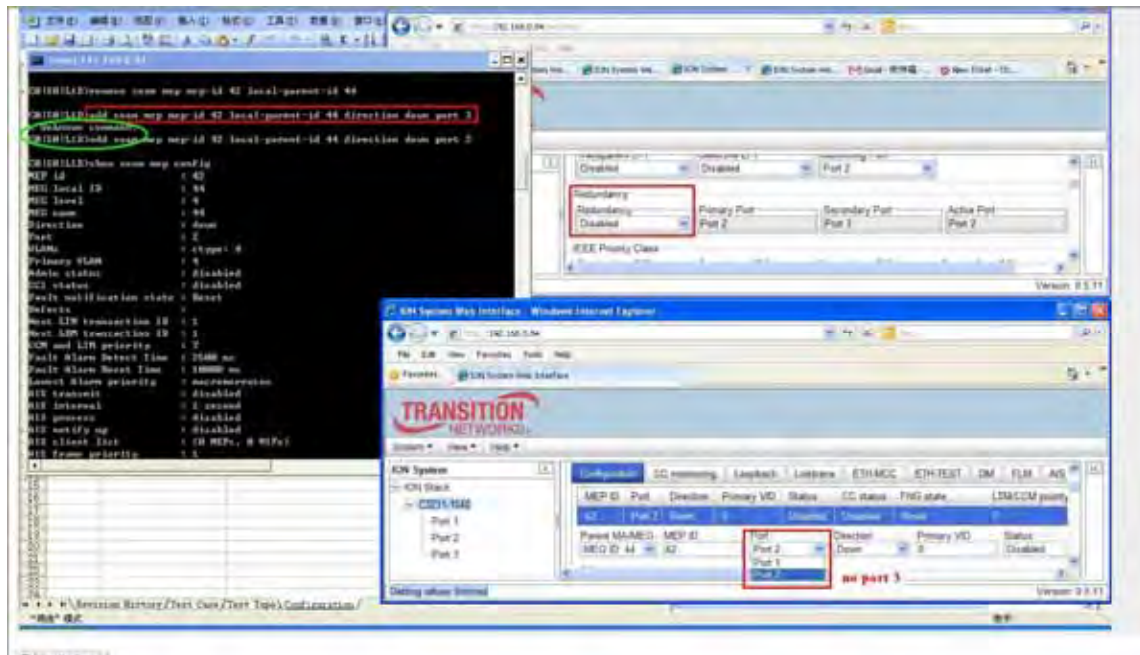
Recovery: To check the loss of power, check at **IONPS-A > MAIN tab > Sensor and Fan(s) section > Power** value field. See [Appendix H](#) on page 653 for more information.

Section 6: Troubleshooting

Problem: Can't add a MEP on Port 3 either via the Web interface or the CLI.

Meaning: 1) In Web interface, there is no "Port 3" option in the port table list at Device > **ADVANCED** tab in the **Redundancy** section / field.

2) On the CLI, if you enter the **add soam mep** command, the message "*Unknown command.*" displays.



Recovery:

1. See “[SOAM Configuration Prerequisites and Restrictions](#)” on page 133.
2. Retry the operation using a different port (i.e., Port 1 or Port 2).
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: SOAM 802.1ag MIP can't be deleted via Web or CLI.

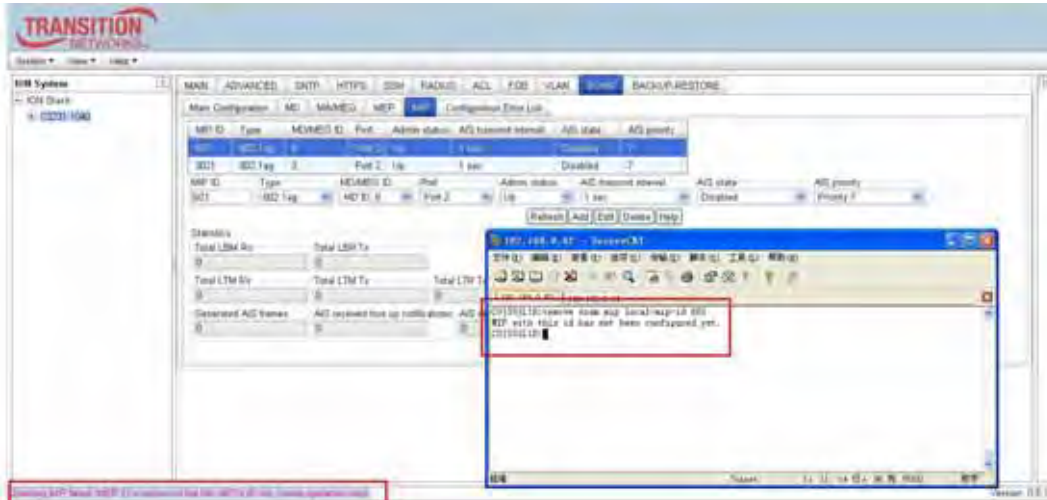
Problem: SOAM MIP vanishes after a reboot.

Problem: Cannot configure AIS on SOAM 802.1ag MIP.

Message: Deleting MIP failed. MEP ID is absent in the MA MEP's ID list. (snmp operation error) (Web interface message)

Message: MIP with this ID has not been configured yet. (CLI message)

Message: Add SOAM MIP failed. MEP on such port, VLAN(s) and higher/same level already configured. (CLI message)



Meaning: 802.1ag SOAM does not support AIS. This manifests in several ways, including:

1. AIS attributes can not be created if MIP type is 802.1ag.
2. AIS attributes do not display in table if MIP type is 802.1ag.
3. Adding a new MIP apparently fails.
4. Deleting an existing MIP apparently fails.
5. An existing MIP apparently ceases to exist after a reboot.

The add new MIP issue occurs when you either try to create an 802.1ag type MIP via the Web interface, or you enter an invalid configuration for the MIP, such as trying to create two MIPs on the same port with same level.

Trying to add two 802.1ag type MIPs on ports 1 and 2 fails, with the “Add SOAM MIP failed.” Web interface message displayed on the bottom left of the screen. This fails because when an 802.1ag MIP is created via the Web interface, AIS attributes are also sent with the create request. Since AIS attributes are invalid under 802.1ag, the MIP creation fails in the SOAM stack. However, in spite of the failure when a refresh is done on the web, the entries for the MIPs are shown on the Web as if they actually were created in the system. Because the MIP creation actually did not succeed, the entries are not saved in flash, so when a card power cycles or reboot is done, these entries are lost from RAM and not shown at all on the Web interface.

If you try to create a new MIP ID on a same port using the same MEG ID, the CLI displays the “Add SOAM MIP failed.” message indicating that the MIP was not successfully created. But when a refresh is done via CLI or Web, the new MIP entry is displayed. In this case, the MIP is not actually created in the SOAM stack and hence not saved in flash, so after a reset the MIP entry is lost. The reason that MIP creation is not allowed is because only one MIP is allowed per MEG level and per port.

Section 6: Troubleshooting

For example:

```
C1|S6|L1D>add soam mip mip-type y.1731 local-mip-id 1 local-parent-id 1 port 2
Add SOAM MIP failed. MEP on such port, VLAN(s) and higher/same level already configured.
C1|S6|L1D>show soam mip config
MIP id : 1
MEG local ID : 1
MEG level : 3
MEG name : Test
MEG VLANs : ctype: 500
Port : 2
Admin status : disabled
AIS transmit : disabled
AIS interval : 1s
AIS frame priority : 7
C1|S6|L1D>
```

An issue can occur if you try to delete an existing MIP, but deleting the MIP fails. For example:

```
C1|S6|L1D>remove soam mip local-mip-id 6
MIP with this id has not been configured yet.
C1|S6|L1D>show soam mip config
MIP id          : 6
MD local ID     : 7
MD level        : 7
MD name         : Level7MD
VLANs           : ctype: 500
Port            : 2
Admin status    : enabled
C1|S6|L1D>
```

Recovery:

1. Make sure this is the function you want. See "[SOAM \(Service OAM\) Configuration](#)" on page 133.
2. Review the "[SOAM Configuration Prerequisites and Restrictions](#)" on page 133 and read the Notes information below.
3. Use the CLI to create either an 802.1ag MIP or Y.1731 MIP. See "[SOAM MIP Config – CLI Method](#)" on page 157.
4. Use Y.1731 for SOAM operations via the web interface. See "[ITU-T Y.1731 Configuration](#)" on page 528. Via the Web interface, create one or more Y.1731 MIPs.
5. Reboot and retry the SOAM MIP operation.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Notes:

1. AIS is not recommended for environments utilizing STP (spanning tree protocol), since STP provides its own restore capability. Due to AIS' STP (and other) limitations, the IEEE decided not to support AIS in 802.1ag.
2. For point-to-point S-VLANs/Ethernet connections, there is just one remote peer MEP that cannot be reached. But for multipoint S-LANs/Ethernet connections, a client layer MEP, on receiving an AIS, cannot determine which of its remote peers have lost connectivity. It is recommended that for multipoint, the client layer MEP should suppress alarms for all peer MEPs.

Problem: *User Public-Key Missing after Upgrade from v1.0.3 to v0.5.12*

Meaning: In ION v1.0.3, the user-public key is binding with the Linux root user and is stored in the root file system (*/root/.ssh/*). This file system will be replaced after this version upgrade, so this key will be lost.

Recovery: This missing key problem will occur only if you upgrade from 0.5.14 to a later release. In ION versions after 0.5.14, the user-public key is saved after an upgrade. You can still log in through SSH, but you must upload the public key again in order to use it. In v 0.5.14, the stored key was moved from the root file system to the application flash area (*/agent3/conf*).

Problem: "Unknown command." message displays when entering system name/contact/location.

Problem: The **System Name** can not be restored when the system name contains special character "space" in the middle.

Meaning: The "Unknown command." message displays when the system name/contact/location contains a "space" character within the text using the CLI command "**set system name**" or "**set system contact**" or "**set system location**" is entered. The entry for the system contact, system location, and system name must be a text string with no spaces between characters. Note that numbers, upper/lower case characters, and special characters (~!@#%&*()_+)" are allowed.

Recovery: From the Web interface, at the device's **MAIN** tab in the **System Configuration** section, re-enter the "**System Name**" or "**System Contact**" or "**System Location**", making sure there are no spaces between the text characters.

From the CLI, re-enter the "**set system name**" or "**set system contact**" or "**set system location**" CLI command, making sure there are no spaces between the text characters. For example:

```
C1 | S1 | L1D > set system ?
  contact
  location
  name
C1 | S1 | L1D > set system name=123abcABC ~!@#%&*( )_+"
% Unknown command.
C1 | S1 | L1D > set system name=123abcABC ~!@#%&*(
% Unknown command.
C1 | S1 | L1D > set system name=123abcABC ~!@#%
% Unknown command.
C1 | S1 | L1D > set system name=123abcABC
C1 | S1 | L1D > set system name=123abcABC
C1 | S1 | L1D > set system name=123abcABC!@#%
C1 | S1 | L1D > set system name=aa bb
% Unknown command.
C1 | S1 | L1D > set system name=%^^&*
C1 | S1 | L1D > set system contact=Rob Roy
% Unknown command.
C1 | S1 | L1D > set system contact=RobRoy
C1 | S1 | L1D > set system location=12345 West 6th
% Unknown command.
C1 | S1 | L1D > set system location=12345West6th
C1 | S1 | L1D > set system name=123abcABC
C1 | S1 | L1D >
```

Section 6: Troubleshooting

Problem: Bandwidth Ingress fault

Meaning: With rate set at 100Mbps with Full Duplex and Frame Size = 9216 a bandwidth Ingress fault occurs. When Ingress rate limiting is set at or below 512Kbps, the S322x will pass approximately 1 Mbps of traffic. At 768kbps and above rate limiting is working. This problem only happens on Ingress (not Egress) and only happens when connected at 100Mbps Full Duplex. Packets of 1518k or less work fine. This is a known hardware component limitation that only occurs when using very large Jumbo Frame (>5k) and very low bandwidth ($\leq 512k$).

Recovery: Change the rate, duplex mode, frame size, packet size, or Ingress Rate Limit. See the related section of this manual for details.

CLI Messages

The following are messages that may appear during CLI (Command Line Interface) operations.

Add ACL rule failed.

This message indicates that the rule could not be added.

1. Verify the CLI command syntax.
2. Retry the operation.
3. If the problem persists, contact Technical Support. 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.
3. See the *ION System CLI Reference Manual, 33461*.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Bad advertisement capability!

This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability command are not valid choices.

1. Verify the command syntax.
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33461.
3. If the problem persists, contact Technical Support. 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. For example:

```
C1|S7|L1D>show lpt config
Cannot get link pass through information on this card!
C1|S7|L1D>
```

1. Use the **go** command to change from the IONMM to the specific slide-in module. The **go** command format is:
go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
 (for a slide in card), or
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
 (for a standalone card).
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot get LOAM configuration on this port!

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the **go** command to change location of where the command operates. The **go** command format is:
`go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)`
 (for a slide in card), or
`go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)`
 (for a standalone card).
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33461.
3. If the problem persists, contact Technical Support. 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)`
 (for a slide in card), or
`go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)`
 (for a standalone card).
2. Retry the operation. For a complete list of the available commands, see the ION System CLI Reference Manual, 33461.
3. If the problem persists, contact Technical Support. 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. Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. 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)

(for a slide in card), or

go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)

(for a standalone card).

2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. 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)

(for a slide in card), or

go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)

(for a standalone card).

2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Fail to get MAC address!

This message indicates that communications to the module can not be established.

1. Verify that the correct hierarchy has been specified in the command (see “[Managing Slide-In and Remote Modules Using CLI Commands](#)” on page 49).
2. For all modules (slide-in and remote) check the following:
 - module is properly seated/connected
 - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
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. For a complete list of the available commands, 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.

Failed to set DHCP client state!

This message indicates a problem in the DHCP setup / configuration.

1. Verify the operation in the “[Assigning a Dynamic IP Address](#)” section on page 91.
2. Retry the operation. See the related DHCP command in *the ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Failed to set current time
Failed to set SNTP state!
Failed to set SNTP daylight savings time state!
Failed to set timezone!
Failed to set SNTP server
Failed to set SNTP server!
Failed to set system contact
Failed to set system name
Failed to set system location!

These messages indicate a problem in the SNTP setup / configuration.

1. Verify the operation in the “[Configuring SNTP](#)” section on page 203.
2. Retry the operation. See the related SNTP command in *the ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Incomplete location command!
Incomplete location parameters, lack of level1 attachment port!

This message indicates that one or more parameters for the **go** command are missing. The **go** command was entered to set location parameters, but the module, slot and/or port value(s) were not included in the command string.

The **go** command can operate on a local or remote card/port, and you must give the last parameter to specify the target is a port or device. For example, the input `go c=1 s=14` does not include the port parameter, so the CLI module displays “Incomplete location parameters”.

1. Verify the command syntax.
2. Re-enter the **go** command and be sure to include all of the location parameters:
3. Use the **go** command to change location of where the command operates. The **go** command format is:

```
go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

(for a slide in card), or

```
go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

(for a standalone card).
4. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

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 is not valid.

1. Verify the value being input; it must match with the value input for type=.
2. Retry the operation.
3. If the problem persists, contact Technical Support. 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.

Section 6: Troubleshooting

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 will have 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"!

This message indicates that you entered an unsupported ACL table or chain parameter value.

For example:

```
C1 | S7 | L1D>set acl table {raw|nat|mangle}
C1 | S7 | L1D>set acl table raw chain {prerouting|input|forward|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 ACL parameters table=filter and chain=input.
2. See “[Configuring an ACL](#)” on page 211.
3. Retry the operation.
4. If the problem persists, contact Technical Support. 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.
 - 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 **Ports (COM & LPT)**.

3. Is the COM port in the list?

Yes	No
Continue with step 4 .	Restart the Management station (PC).

4. In the HyperTerminal window, select **File>Properties**.
5. Check that the correct port is listed in the **Connect using** field.
6. Restart the Management station (PC).
7. Reboot the IONMM.
8. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

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.

1. Enter the **go** command and be sure to include all of the location parameters. The **go** command format is:

```
go[c=<1-16>][s=<1-32>][l1ap=<1-15>][l2ap=<1-15>](l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

(for a slide in card), or

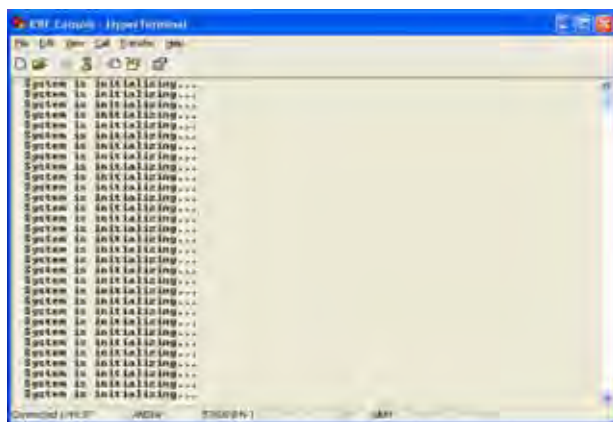
```
go[c=<0-16>][s=<0-32>][l1ap=<1-15>][l2ap=<1-15>](l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d)
```

(for a standalone card).

2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.

System is initializing...

CLI is receiving continuous error message "system is initializing..."



1. Wait for a few minutes for the message to clear.
2. Cycle power to the IONMM.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 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!

1. Verify the command entered is the one you want.
2. Verify that the device for the command entered can support the function of the command (e.g., SOAM functions / commands are only supported by NID models S323x / C323x NIDs).
3. Retry the operation (e.g., type **show soam port** and press **Enter**).
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 the *ION System CLI Reference Manual, 33461*.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

There is no matched command.

The command you entered is not supported, or you entered the wrong command format / syntax.

1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error location parameter number!

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).

2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.

Fail to set link pass through state!

You tried to set the LPT state to an unacceptable state. For example, you typed:

```
C1|S3|L1D>set lpt state=enable
```

and then pressed **Enter**.

1. Verify the CLI command syntax.
2. Check the **set lpt monitor-port** and **set selective lpt state** command settings.
3. Enter the **show lpt config** command and in the Link Pass Through configuration, check if the Link pass through state is set to **notSupported** or if the **Remote fault detect state** is set to **notSupported**.

If either is set to **notSupported**, change the setting to enable (e.g., type **set rfd state enable** and press **Enter**).

4. Retry the operation.
5. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.

6. If the problem persists, contact Technical Support. 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 in 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.

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.

TFTP transfer failed!

The attempted firmware upgrade via the tftp upgrade command was unsuccessful.

1. Verify the CLI command syntax.
2. Verify the firmware version.
3. Be sure the TFTP server is configured and running.
4. Check that the remotefile is in the proper location (e.g., the file *x323x.bin.1.0.5* is at *C:\TFTP-Root*).
5. Retry the operation. See the tftp upgrade command in “[Section 6: Command Line Interface \(CLI\) Reference](#)” on page 124.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Fail to transfer the file!

tftp get: set address type failed.

tftp put failed.

The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., tftp get or tftp put or tftp transfer). For example:

```
C1|S4|L1D>tftp get iptype ipv4 ipaddr 192.168.1.30 remotefile xxxx
tftp get: set address type failed.
C1|S4|L1D>tftp put iptype ipv4 ipaddr 192.168.1.30 localfile xxxx
tftp put failed.
C1|S4|L1D>tftp upgrade iptype ipv4 ipaddr 192.168.1.30 remotefile xxxx
tftp get: set address type failed.
```

1. Check the command syntax. See “[TFTP Commands](#)” page on page [157](#).
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

TFTP transfer failed!

1. The attempted firmware upgrade via the **tftp upgrade** command was unsuccessful.
2. Verify the CLI command syntax.
3. Verify the firmware version.
4. Be sure the TFTP server is configured and running.
5. Check that the remotefile is in the proper location (e.g., the file *x323x.bin.0.5.4* is at *C:\TFTP-Root*).
6. Retry the operation. See the **tftp upgrade** command in the *ION System CLI Reference Manual, 33461*.
7. 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: C1|S7|L1D>set rfd state enable

1. Verify that the card you entered the command on supports this function. See [Set RFD State](#) on page [190](#).
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot set service translation type on this card!

The attempted command was rejected. For example, you entered:

```
C1|S7|L1D>set dot1bridge service
```

1. Verify that the card you entered the command on supports this function.
2. Retry the operation. See the **dot1bridge** commands section command in 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.

Cannot set service vid for tag on this card!

The attempted **set dot1bridge vid** command was rejected (e.g., C1|S7|L1D>set dot1bridge vid 2).

4. Verify that the card you entered the command on supports this function.
5. Retry the operation. See the **dot1bridge aging-time** command.
6. If the problem persists, contact Technical Support. 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 in 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.

Get aging time failed!

The attempted show dot1bridge aging-time command failed to complete.

1. Verify the **dot1bridge aging-time** command syntax. See [Configure Forwarding Learning Aging Time](#) on page 191.
2. Retry the operation. See the **dot1bridge aging-time** command in the *ION System CLI Reference Manual, 33461*.

Section 6: Troubleshooting

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

CLI command `remove fwddb all` failed

The attempted C3220-1040 Backup/Restore failed during the restore; the restore displays "ongoing" status, and will not succeed.

The dynamic MAC address should not be backed up or restored - only static entries should be backed-up and restored.

1. Retry the operation. See “[Backup/Restore Operations](#)” on page 256.
2. See the *ION System CLI Reference Manual, 33461*.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

The format of Ethtype value should like `0x8810`, `0x88a8` etc.

The attempted CLI command entry failed (e.g., `set dot1bridge`).

1. Retry the operation with the correct parameter entry.
2. See the *ION System CLI Reference Manual, 33461* for the full set of available command parameters.
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 NID 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.

The MD with this id has been configured already.

The MD that you tried to create has already been defined. For example, you entered the command: **add soam md local-md-id 1 md-name none md-level 7**, but that local-md-id already exists.

1. Verify that the local-md-id you entered is the one you want.
2. Retry the operation with a unique MD ID. See the “Add Maintenance Domain” command on page 118.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

MA/MEG with this id has been configured already.

The MA or MEG that you tried to create has already been defined. For example, you entered the command: **add soam ma local-ma-id=1 local-maid=1 ma-name=maid1 vlan-type=ctype**, but that local-ma-id already exists.

1. Verify that the local-ma-id you entered is the one you want.
2. Retry the operation with a unique MA or MEG. See the “Add Maintenance Association” command on page 120.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

MD cannot be deleted. There are MAs configured on this MD.

The MD that you tried to delete has MAs defined for it. For example, you entered the command: **remove soam md local-md-id=1**, but an MA has been defined for and associated with it.

1. Verify that the local-md-id you entered is the one you want.
2. Delete the associated MA(s).
3. Try again to delete the MD. See the “Remove Maintenance Domain” command section on page 118.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

MA with this id has not been configured yet.
MD with this id hasn't been configured yet.
MEG with this id isn't configured.
MEP with this id not been configured yet.
MIP with this id not been configured yet.

You entered a command to show or set MEP or MIP configuration information, but you have not yet defined the MEP (or MIP). For example, you entered the command **show soam mep cc mep-id=1 local-parent-id=10**, but that MEP ID does not yet exist.

1. Verify that the local-mep-id you entered is the one you want.
2. Create a unique MEP. See the “Add a MEP” command on page 130.
3. Retry the operation with the unique MEP (or MIP).
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Send SOAM Unicast Loopback failed.

Can't read last soam error description

You entered the command **send soam mep loopback**, but the last soam error description was unreadable. For example, you entered the command:

```
send soam mep loopback mep-id=10 local-parent-id=1 dest=10 amount-frames=1.
```

1. Make sure the SOAM port is configured and enabled.
2. See the “[Initiate a Loopback Request](#)” command on page 136.
3. Enter the **show soam conferror vid=x port=y** to verify there are “No config errors”.

An error has been occurred during LTM sending.

A problem occurred when performing a Linktrace function. For example, you entered the command:

```
send soam mep linktrace mep-id=10 local-parent-id=1 dest=10 use-fdb-only=false ttl=1.
```

1. Verify that the parameters were entered correctly.
2. Verify the forwarding database is configured and enabled.
3. Enter the **show soam conferror vid=x port=y** to verify there are “No config errors”.
4. Retry the operation.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Add SOAM MIP failed.

Can't read last soam error description

You entered the command **add soam mip mip-type**, but the last soam error description was unreadable. For example, you entered the command:

```
send soam mep loopback mep-id=10 local-parent-id=1 dest=10 amount-frames=1.
```

1. Make sure the SOAM port is configured and enabled.
2. See the “[Add SOAM MIP](#)” command on page 139.
3. Enter the **show soam conferror vid=x port=y** to verify there are “No config errors”.
4. Retry the operation.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Get SOAM MIP stats no such object.

You entered the command **show soam mip stats**, but that object does not yet exist.

1. Make sure the SOAM MIP is configured and enabled.
2. Verify the command parameters. See the “[show mip statistics](#)” command on page 151.
3. Retry the operation.
4. 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 transfer the file!

The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., **tftp get** or **tftp put** or **tftp transfer**).

1. Check the command syntax. See “[TFTP Commands](#)” page on page 157.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set management VLAN id!
Fail to set management VLAN FDB ID!
Fail to set management VLAN state!

You entered the command **set mgmt vlan state** or **set mgmt vlan port** or **set mgmt vlan vid** to enable or configure Management VLAN, but the operation failed.

1. Verify the VLAN Management configuration using the **show vlan** command and the **show vlan service** command.
2. Review the set mgmt vlan command syntax for the port / state / vid. See the “[VLAN Commands](#)” on page 159.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Upgrade is only supported on IONMM card!

You entered a firmware *upgrade* or firmware *update* command from a device other than the IONMM. For example:

```
C1|S3|L1D>show firmware upgrade result
C1|S3|L1D>show firmware-db update result
C1|S3|L1D>show upgrade firmware file
C1|S3|L1D>update firmware-db file cert
C1|S3|L1D>upgrade module
```

1. Make sure of the command you want to enter. See “[Firmware Upgrade Commands](#)” on page 167.
2. Use the **home** command to go to the IONMM device.
3. Re-enter the firmware upgrade command from the IONMM.
4. If the problem persists, contact Technical Support. 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 noLimit erate noLimit
Cannot set ingress and egress rate on this card!
```

1. Verify if the card supports rate limiting. Try the syntax **set irate=unLimit erate=unLimit**.
2. Use the **go** command to switch to a different card and switch to the port level.
3. Verify the command entry. See “[Bandwidth Commands](#)” on page 53.
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!**

You entered a command (e.g., **clear loopback counters**) for a function not supported on the card or port.

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.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

No Time-domain reflectometer support on this card!

Cannot get port security configuration on this port!

Fail to get MAC control frames statistics!

Fail to get auto-negotiation state!

Cannot show forwarding port list on this card!

Cannot show slot info on this card!

Cannot show USB port state on this card!

Cannot show USB port configure on this card!

Cannot show TP port cable length on this card!

Cannot set management VLAN on this card!

Cannot set PHY mode on this port!

Cannot clear counters on this port!

Cannot reset all ports' counters on this cards!

Cannot set aging time on this card!

Cannot show aging time on this card!

You entered a command 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 may 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.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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.

Fail to get system name!

You entered a command for system information, but the information on the card was not available. For example:

```
C1|S10|L1D>show card info
Fail to get system name!
```

1. Try entering the **show cardtype** command.
2. Select the **MAIN** tab > **System Configuration** section > **System Name** field, and verify the name and for the device.
3. Use the **set system name** command to enter the **System Name** information (e.g., **set system name=NAME**). Do not enter any spaces between the text characters in the system name.
4. Remove and reset the card.
5. Try the operation again.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Set system name timeout.

You entered a command to define system information, but it was not accepted. For example:

```
C1|S10|L1D>set system name C3231
Set system name timeout.
```

1. Use the **set system name** command to enter the System Name information (e.g., **set system name=NAME**) without any special characters (e.g., without the ! or # or % or & characters).
2. Remove and reseal the card.
3. Try the operation again.
4. Select the **MAIN** tab > **System Configuration** section > **System Name** field, and verify the name and for the device.

Section 6: Troubleshooting

5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

System is busy, please retry this command later!

You entered a **show** or **set** command, but the command was not accepted by the system. For example:

```
C1|S10|L1D>show https config
System is busy, please retry this command later!
C1|S10|L1D>
```

1. Wait 1-2 minutes and then retry the command.
2. Reboot the system and then retry the command.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Get HTTPS state no such object.

Get management VLAN state no such object.

IP management state no such object.

You entered a **show** or **get** command, but the command was not accepted by the system. For example:

```
C1|S10|L1D>show https config
HTTPS configuration:
-----
Get HTTPS state no such object.

C1|S10|L1D>show mgmt vlan config
vlan id    vlan state      vlan portlist
-----
Get management VLAN state no such object.

C1|S10|L1D>show ip-mgmt config
IP management configuration:
-----
IP management state no such object.
```

1. Wait 1-2 minutes and then retry the command.
2. Try the command again.
3. Reboot the system and then retry the command.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Warning: this command will restart system, connection will be lost and please login again!
Warm start failed.

You entered a **reboot** command, but the reboot was unsuccessful.

1. Wait 1-2 minutes and then retry the command.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

4 packets transmitted, 0 packets received, 100% packet loss

The attempted ping command failed. For example:

```
PING 192.168.1.10 (192.168.1.10): 56 data bytes
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

1. Verify the IP address.
2. Check the cable connection.
3. Refer to the **Ping** command section.
4. Retry the command.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Ping command can only be used on management card!

The attempted ping command was not accepted by the system. For example:

```
C1|S5|L1D>ping 192.168.1.30
Ping command can only be used on management card!
```

1. Use the **go** command to switch to the IONMM card.
2. Refer to the **Ping** command section.
3. Retry the command.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Admin state of Link OAM of this port is disable, please enable it first!

The attempted **loopback** command was not accepted by the system. For example:

```
C1|S16|L1P1>set oam loopback oper=stop
Admin state of Link OAM of this port is disable, please enable it first!
```

1. Use the **set ether admin state=up** command to enable the Ethernet port for use.
2. Use the **set loam admin state=enable** command to enable OAM administration.

Section 6: Troubleshooting

3. Use the **show oam loopback** commands and **show loam config** commands to verify the configuration.
4. Re-enter the **loopback** command.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Only 100M fiber port can set far end fault!

The attempted far end fault command was not accepted by the system. For example:

```
C1|S16|L1P1>set ether fef enable
Only 100M fiber port can set far end fault!
```

1. Use the **go** command to switch to the 100M fiber port.
2. Re-enter the **fef** command.
3. Use an alternate Ethernet test command in place of the **fef** command.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Can not set 1000M speed for this card!

You tried to use the **set ether speed** command to set the device's speed to 1000 Mbps (1 Gbps), but the card you entered the command on does not support this speed. For example:

```
C1|S16|L1P1>set ether speed=1000M
Can not set 1000M speed for this card!
C1|S16|L1P1>
```

1. Use the **set ether speed ?** command to determine the card's speed capabilities.
2. Re-enter the **set ether speed= command** with a speed supported by the card.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to set Ethernet port speed!

You tried to use the **set ether speed** command to set the device's speed, but the command was not accepted. For example:

```
C1|S16|L1P1>set ether speed 1000
Fail to set Ethernet port speed!
C1|S16|L1P1>
```

1. Verify the command syntax; for example make sure you entered "10M" or "100M", etc.
2. Use the **set ether speed ?** command to display the card's speed capabilities.
3. Re-enter the **set ether speed= command** with a speed supported by the card.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid pause value!

You tried to use the **set ether pause** command to set the device's pause mode / value, but the value was not accepted. For example:

```
C1|S16|L1P1>set ether pause=bpause
Invalid pause value!
```

1. Use the **set ether pause ?** command to display the card's Pause capabilities.
2. Configure the device for full duplex mode; only stations configured for full duplex operation can send pause frames.
3. Select another pause type – nopause, apause (asymmetric), bpause (asym/sym), pause (the port will advertise it has pause capability), or spause (symmetric).
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Set Ethernet port loopback type failed.

You tried to use the **set oam loopback type** command to set the device's type of loopback support, but the command was not accepted. For example:

```
C1|S16|L1P1>set oam loopback type=phylayer
Set Ethernet port loopback type failed.
C1|S16|L1P1>
```

1. Verify the command syntax.
2. Use the **set oam loopback type** command to set the device's type of loopback support (alternate, noloopback, or remote).
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Please input a number to specify threshold!

Please input a number to specify fdbid!

You entered a number to specify (for example) 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 efthreshold 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.

Section 6: Troubleshooting

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 x323x 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.

Fail to set management VLAN id!

You tried to set the Management VLAN ID, but the VLAN ID was not accepted. For example:

```
C1|S18|L1D>set mgmt vlan port=2
Fail to set management VLAN id!
```

1. Verify the Management VLAN state setting (**set mgmt vlan state** command).
2. Verify the Management VLAN port setting (**set mgmt vlan port** command).
3. Try setting the Management VLAN ID again.
4. If the problem persists, contact Technical Support. 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)

Invalid forward port list!
```

1. Re-enter the command, wait for the prompt, and then enter a response in the correct syntax. Do not enter any space in the command string. Do not enter more than 8 modules.
2. See the [upgrade module](#) command section of this manual for more information.
3. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.
4. If the problem persists, contact Technical Support. 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.

Section 6: Troubleshooting

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.

Please reboot the card for the changes to take effect!

You made a change that requires a system reboot in order for the change to take affect. For example:

```
C1|S5|L1D>set snmp traphost svr 1 type ipv4 addr 192.168.1.30
Please reboot the card for the changes to take effect!
C1|S5|L1D>
```

1. Reboot the card. See the “[Reboot](#)” section on page 292.
2. Continue the operation.
3. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Get DMI identifier no such object.

You entered the CLI command to display DMI information, but it was not available. For example:

```
C1|S3|L1P2>show dmi info
Get DMI identifier no such object.
C1|S3|L1P2>
```

1. Make sure this is the command / function that you wanted.
2. Try entering the command again. See “[DMI \(Diagnostic Maintenance Interface\) Parameters](#)” on page 395.
3. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Get SNMP version no such object.

You entered the CLI command to display SNMP configuration information, but it was not available. For example:

```
C1|S3|L1D>show snmp config
SNMP configuration:
-----
Get SNMP version no such object.
C1|S3|L1D>
```

1. Make sure this is the command / function that you wanted.
2. Verify the command syntax. See “[Configuring SNMP](#)” on page 245.
3. For complete command descriptions, see the *ION System CLI Reference Manual*, 33461.
4. Try entering the command again. See “[DMI \(Diagnostic Maintenance Interface\) Parameters](#)” on page 395.
5. If a 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 oam loopback oper init
Fail to set Ethernet port loopback operation, please check if Link OAM
admin state of remote peer port is enabled, link status and other issues.
C1|S5|L1P2>
```

1. Make sure the LOAM admin state of remote peer port is enabled (see “[set loam admin state](#)” command).
2. Verify the command syntax.
3. Use the **set oam loopback ?** command to display the card’s loopback capabilities. For example:

```
C1:S7:L1P1>set oam loopback type ?
alternate
noloopback
remote
```

4. Re-enter the **set oam loopback=** command with a loopback capability supported by the card (alternate, or remote or noloopback).
5. Verify the loopback capability with the **show oam loopback capability** command. For example:

```
C1|S5|L1P2>show oam loopback capability
Loopback capability: alternate remotePeer
C1|S5|L1P2>
```

6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Fail to remove ACL condition!

Fail to remove ACL rule!

You tried to delete an ACL rule or condition, but the operation failed.

1. Make sure ACL Status is enabled.
2. Verify the command syntax. See “[Configuring an ACL](#)” on page 219.
3. For complete command descriptions, see the *ION System CLI Reference Manual*, 33461.
4. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to get cable length

You initiated a VCT test (Web I/F) or **show cable length** CLI command, but the Time Domain Reflector (TDR) test failed. For example, you entered **start ether tdr test** and pressed **Enter**.

1. Make sure the NID supports the VCT Test or **show cable length** command (only for x2110).
2. Make sure you enter the Time Domain Reflector (TDR) test on an Ethernet copper port.
3. Verify the command syntax. See “[Virtual Cable Test \(VCT\)](#)” on page 409.
4. Type **show ether tdr config** to show the Ethernet port TDR Test configuration.
5. If the problem persists, contact Technical Support. 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!

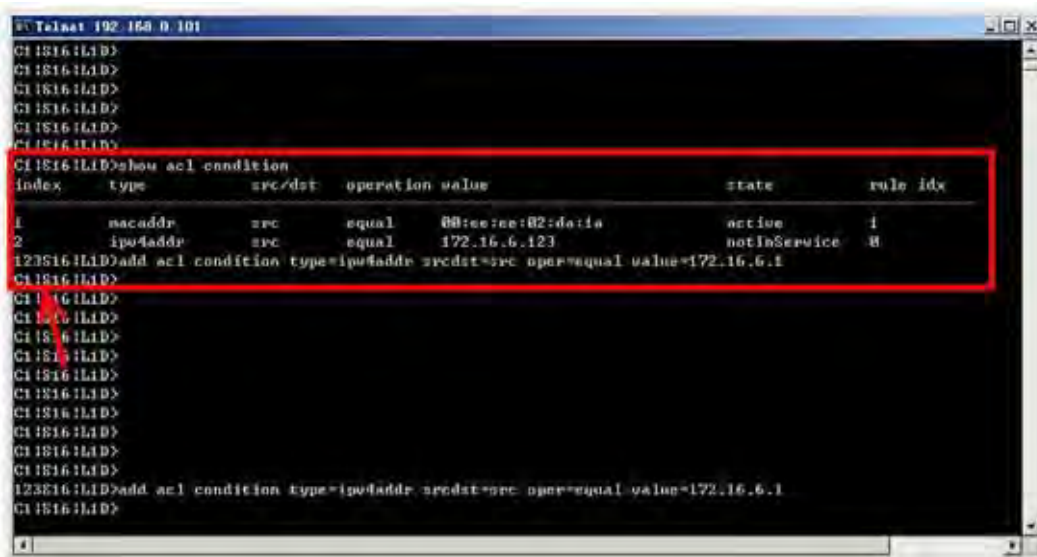
This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability (set ether adv-cap) command are not valid choices. For example:

```
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 the *ION System CLI Reference Manual*, 33461.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Long Command Causes Cursor Wrap to Same Line

When the input command reaches the input max length, the cursor does not return to the next line, but goes back to the beginning of the same line, overwriting the original data.



1. Press the **Enter** key towards the end of the command string and continue entering command text.
2. Try using HyperTerminal or the Web interface, at least temporarily.
3. Contact 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.

Section 6: Troubleshooting

Please change to power supply slot first before showing its configure!

You entered the show power config command from a device other than the power supply. For example:

```
C1|S16|L1D>show power config
Please change to power supply slot first before showing its configure!
C1|S16|L1D>
```

1. Make sure this is the command you want.
2. Verify the command syntax.
3. Use the go command to switch to the slot containing the power supply (typically slot 22 and/or 23).
4. Contact 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.

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 1 - 268435455!

Error frame period window is out of range, its range is 1 - 104857560!

Error frame period threshold is out of range, its range is 0 - 268435455!

Error frame window is out of range, its range is 10 - 600!

Error frame threshold is out of range, its range is 0 - 268435455!

Error frame seconds summary window is out of range, its range is 100 - 9000!

Error frame seconds summary threshold is out of range, its range is 0 - 268435455!

A parameter entered in the "Event Configuration" has exceeded the range limitation.

1. Enter a parameter within the valid range displayed. See [“LOAM Event Configuration Default Values and Valid Ranges”](#) on page 130.
2. Use the **show loam event config** command to verify the setting.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

No data in VLAN forward database table now!

You entered the command to display FWDDDB 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 FWDDDB entry but the effort failed. For example:

```
C1|S16|L1D>add fwddb mac 00-c0-f2-21-02-b3 conn-port=1 priority=7 type=static
set forward database connection port failed.
C1|S16|L1D>
```

1. Make sure this is the function that you want.
2. Use the [Forwarding Database Commands](#) on page 92 to create the VLAN FDB entry.
3. If the problem persists, contact Technical Support. 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](#)” on page 234 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.

Show SOAM FLM Error!

You tried to display SOAM MEP FLM (Frame Loss Measurement) results, but the information was not available. For example:

```
C1 | S5 | L1D>show soam mep lmpersistent
Show SOAM FLM Error!
C1 | S5 | L1D>
```

1. Make sure this is the function that you want.
2. Review the “[MEP Frame Loss Measurement Commands](#)” on page 166.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

primary-vlan is Invalid

You tried to add a new Maintenance Association (MA) to the SOAM configuration, but it was not accepted.

1. Make sure this is the function that you want.
2. See "[Configuring SOAM MD/MA](#)" on page 133.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error: Can not remove AIS config!

Error: Can not remove dot1agCfmMepTable config!

Error: Can not remove ionSoamExtMipTable config!

Error: Can not remove CfmMaMepListTable config!

Error: Can not remove ExtMegTable config!

Error: Can not remove MaCompTabl config!

Error: Can not remove dot1agCfmMaNetTable config!

Error: Can not remove dot1agCfmMdTable config!

You tried to perform a SOAM configuration, but it was not accepted (e.g., remove soam ma, remove soam md / meg / mep / mip, etc.).

1. Make sure this is the function that you want.
2. See "[Configuring SOAM MD/MA](#)" on page 133.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Error: location parameter should be digital number!

You entered a letter or special character as part of the **go** command. For example:

```
C1|S7|L1P2>go c=s s=5 l1d
Error: location parameter should be digital number!
C1|S7|L1P2>
```

1. Re-enter the **go** command with the correct syntax (e.g., change the letter **s** to a number in the example above).
2. Retry the operation. For a complete list of the available commands, see the *ION System CLI Reference Manual*, 33461.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Fail to find first row of acl rules!

You tried to configure a condition for an ACL rule, but the rule has not yet been created.

1. Make sure ACL Status is enabled.
2. Verify the command syntax. See “[Configuring an ACL](#)” on page 219.
3. For complete command descriptions, see the *ION System CLI Reference Manual*, 33461.
4. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error: parameter out of range, chassis-id range is (1 .. 16)!

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)

Error: parameter out of range, level1 port-id range is (1 .. 15)!

Error: parameter out of range, level2 port-id range is (1 .. 16)!

Error: parameter out of range, level3 port-id range is (1 .. 16)!

Error: parameter out of range, level1 attachment port-id range is (1 .. 16)!

Error: parameter out of range, level2 attachment port-id range is (1 .. 16)!

You used the **go** command to move to a port, but the command was not accepted. For example:

```
C1 S7 L1D>go l1p=0
Error: parameter out of range, level1 port-id range is (1 .. 15)!
C1 S7 L1D>
```

1. Make sure this is the port that you want. See “[Managing Device and Port Hierarchy Using CLI Commands](#)” on page 83.
2. Re-enter the **go** command.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Please input a number to specify fdbid!

Please input a number to specify the connection port!

Please input a number to specify the priority!

Please input static or staticNRL or staticPA or dynamic to specify the type!

1. Make sure this is the function that you want.
2. See the [Forwarding Database Commands](#) on page 92 for the FDB entry.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot create forward database on this card!

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.

Invalid dot1dbridge MAC address!

Invalid MAC address!

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.

Please input a number to specify fdbid!

Please input a number to specify the connection port!

Please input a number to specify the priority!

Please input static or staticNRL or staticPA or dynamic to specify the type!

1. Make sure this is the function that you want.
2. See the “[Forwarding Database Commands](#)” on page 92 for the FDB entry.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot create forward database on this card!

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.

Invalid dot1dbridge MAC address!

Invalid MAC address!

The specified MAC address has been existed!

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.

Section 6: Troubleshooting

Fail to set forward database row status!

set forward database connection port

set forward database priority

set forward database entry type

1. Make sure this is the function that you want.
2. See the [Forwarding Database Commands](#) on page 92 for the FDB entry.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Adding MA failed

Adding MA Comp add failed

Adding MA add failed

At the devices' **SOAM > MD** tab you tried to add an MA that was already defined.

1. Press **OK** to clear the message, then enter a unique MA ID number.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Delete SSH public key failed

You tried to remove the SSH public key, but the operation failed.

1. Make sure you entered the correct User Name.
2. See the "[Remove SSH Public Key From a User](#)" command on page 174.
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:

```
C1|S3|L1D>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.
C1|S3|L1D>
```

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.

Section 6: Troubleshooting

Fail to set errored frame period window!

Fail to set errored symbol period window low!

You entered an EFP Window parameter or ESP Window parameter that was outside the valid range. For example, you entered:

```
C0|S0|L1P2>set loam efp window 300
Fail to set errored frame period window!
C0|S0|L1P2>
```

1. Verify the valid range. See “[LOAM Event Configuration Default Values and Valid Ranges](#)” on page 133.
2. Re-enter the command.
3. Use the **show loam event config** command to verify the setting.
4. If the problem persists, contact Technical Support. 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. 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.

- IP management is not supported on this card!**
- No tdm loopback supported on this card!**
- Syslog is not supported on this card!**
- TAOS status setting is not supported on this card!**
- TNDP is not supported on this card!**

You entered a command for a function that is not supported on the x323x. For example:

```
C1|S15|L1D>set dhcp state disable
IP management is not supported on this card!
C1|S15|L1D>
```

1. Try another command on the x323x.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support. 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.

Section 6: Troubleshooting

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 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.

Cannot get port VLAN configuration on this card!

Cannot get VLAN tag management configuration on this port!

Cannot set discard tagged frame on this card!

You entered a VLAN command on a device or port that does not support this function.

1. Try another command on the x323x.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support. 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!

You tried to enter the **set tndp** command but either the function is not supported or you entered it at the device level or you are being asked to verify the command entry.

1. Verify that this is the function you want.
2. Use the **go** command to switch to a port.
3. Use the ION Web interface to perform the function.
4. Use the **go** command to switch to a device that supports this function.
5. Refer to the “[TNDP Disable/Enable](#)” section on page 416.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

No loopback supported on this card!

Error: this command should be executed on a port!

No TDM loopback supported on this card!

Fail to set Ethernet port loopback operation, please check if Link OAM admin state of remote peer port is enabled, link status and other issues.

Fail to get loopback type!

You tried to enter the **set tdm** command but either the function is not supported or you entered it at the device level or you are being asked to verify the command entry.

1. Verify that this is the function you want.
2. Use the **go** command to switch to a port.
3. Use the ION Web interface to perform the function.
4. Use the **go** command to switch to a device that supports this function.
5. Verify that the Link OAM admin state of the remote peer port is enabled, the link status is Up, and other prerequisites are met. Refer to the “[Configuring TDM Loopback](#)” section on page 418.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

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 x323x device (i.e., you cannot enter the command in the example above (`set mac_learning enable portlist 1,2,3`) on a 2-port device such as the x3230.
3. Refer to the “[Configuring MAC Address Learning](#)” section 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 FWDDDB 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.

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:
xxxxxxx
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!

Backup finished

Error: this command should be executed on a device!

Error: this command should be executed on IONMM or a standalone SIC!

Fail to set card entity index!

Processing...

The MAX provision configure file name is 64!

The specified module does not exist!

You entered a “**backup**” or “**restore**” command to do a backup or restore function, but a problem was encountered or the process is not yet finished. You entered a “**prov**” command to do a backup or restore function, but a problem was encountered or the process is not yet finished.

1. Wait a few moments for the command to complete and the *Restore finished* or *Backup finished* message to display.
2. Retry the backup or restore operation with 10 or fewer devices listed.
3. Use the **go** command to switch to a device that supports this feature (IONMM or a standalone SIC).

Section 6: Troubleshooting

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 103.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

```

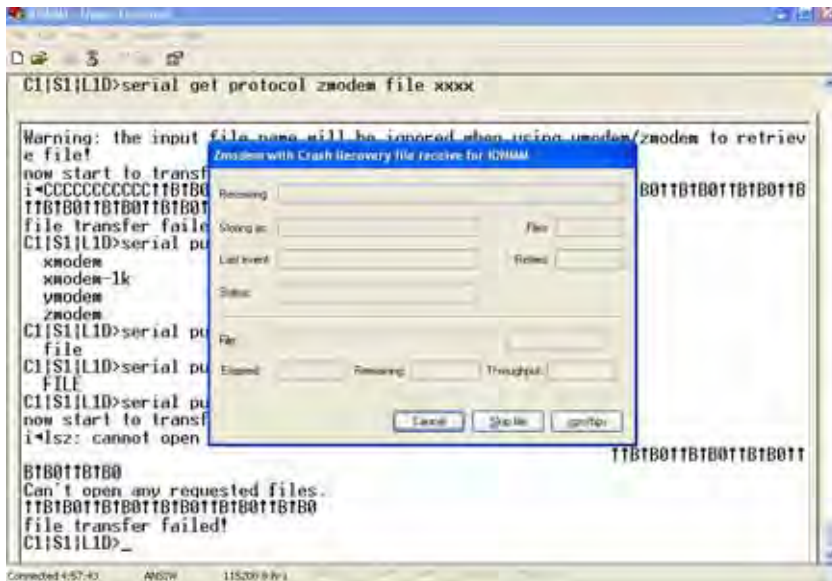
Can't open any requested files.
cannot open /tftpboot/xxxx: No such file or directory
now start to transfer the file ...
file transfer failed!
file transfer succeeded!
now start to upgrade the system ...
/usr/local/bin/flash_firmware /tftpboot/
upgrade failed!
upgrade failed due to wrong file %s!
upgrade 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.
2. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

File Transfer Failed - ZModem Crash Recovery dialog box:



You entered a Serial File Transfer command, but the operation failed.

1. Either enter the requested information and click **cps/bps**, or click **Skip file**, or click **Cancel**.
2. See the HyperTerminal Helps or the [Hilgraeve web site](#) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.

Section 6: Troubleshooting

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.

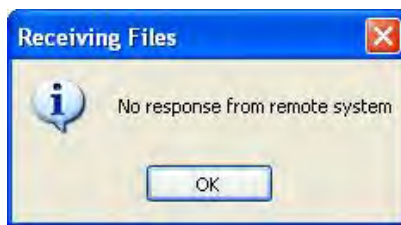
5. If the problem persists, contact Microsoft or Hilgraeve Technical Support:

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 if you need a more powerful HyperTerminal alternative. For questions call (734)-243-0576 ext. 1# or see <http://www.hilgraeve.com/support/>.

Receiving Files - No response from remote system



You entered a Serial File Transfer command, but the ZModem file transfer failed.

1. Click the **OK** button to clear the message dialog box.
2. See the HyperTerminal Helps or the [Hilgraeve web site](#) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Technical Support. 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!**Software version of this card is too old, please upgrade it!**

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. You performed a reboot, but the ION card’s firmware version was checked and found to be too old to support this newer function.

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.
3. Retry the operation.
4. 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!**Get chassis slot state fail****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.

Section 6: Troubleshooting

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 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 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!

Backup finished

Error: this command should be executed on a device!

Error: this command should be executed on IONMM or a standalone SIC!

Fail to set card entity index!

Processing...

The MAX provision configure file name is 64!

The specified module does not exist!

Section 6: Troubleshooting

You entered a “**backup**” or “**restore**” command to do a backup or restore function, but a problem was encountered or the process is not yet finished.

1. Wait a few moments for the command to complete and the *Restore finished* or *Backup finished* message to display.
2. Retry the backup or restore operation with 10 or fewer devices listed.
3. Use the **go** command to switch to a device that supports this feature (IONMM or a standalone SIC).
4. Enter a config filename with less than 64 characters. See the “[Configuring Backup / Restore](#)” section 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 103.

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!

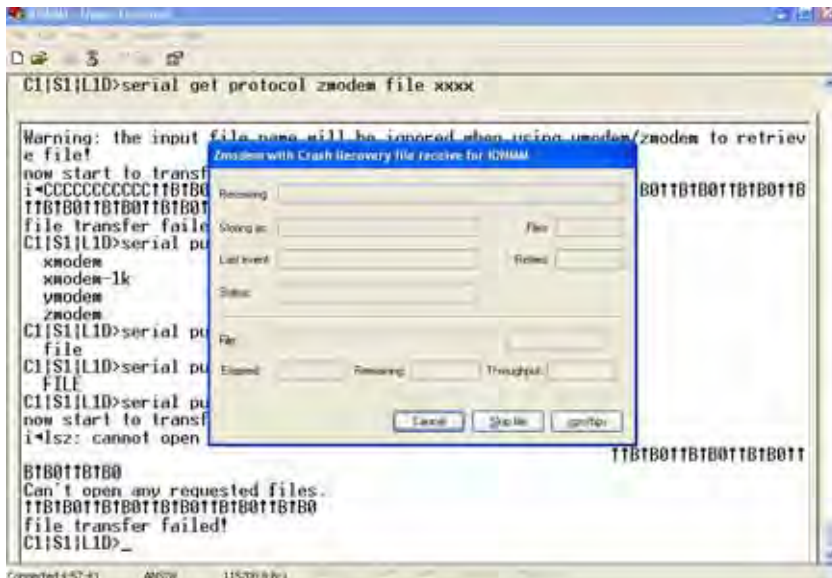
Warning: xmodem/xmodem-1k protocol might append some garbage at the end of the file!

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 103.
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:



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**.

Section 6: Troubleshooting

2. See the HyperTerminal Helps or the [Hilgraeve web site](#) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Microsoft or Hilgraeve Technical Support:

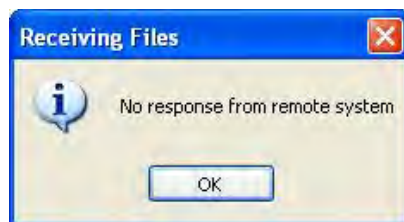
HyperTerminal Support

HyperTerminal is part of certain Microsoft Windows versions and is supported by Microsoft with 24-hour worldwide responsibility for Windows communications components. Contact Microsoft Windows Support at (425) 635-7000, or contact your computer manufacturer. See the Microsoft Support knowledge base for articles regarding your topic: <http://support.microsoft.com/directory/> and do a key word search using your issue keywords.

HyperACCESS Support

Certain other Microsoft Windows versions do not include HyperTerminal support. HyperACCESS is the official, full powered Hilgraeve version of HyperTerminal Private Edition. If you need a more powerful HyperTerminal alternative, HyperACCESS is available. For questions call (734)-243-0576 ext. 1# or see <http://www.hilgraeve.com/support/>.

Receiving Files - No response from remote system



You entered a Serial File Transfer command, but the ZModem file transfer failed.

1. Click the **OK** button to clear the message.
2. See the HyperTerminal Helps or the [Hilgraeve web site](#) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “[Transfer Files via Serial Protocol \(X/Y/Zmodem\)](#)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Technical Support. 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.

5. Check the card’s current firmware version using the “**show card info**” command.
6. Upgrade the card firmware. See "[Upgrade the Firmware](#)" on page 129.
7. Retry the operation.
8. 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 "[Upgrade the Firmware](#)" on page 129.
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.

4. Enter another (supported) show command on this card, or use the "**go**" command to switch to the IONMM.
5. Retry the operation.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

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.

4. Verify the command syntax ("add sysuser name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR").
5. Retry the operation, making sure the "pass" and "confirmpass" entries match.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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). Verify the command syntax ("add sysuser name=NAMESTR level=(admin|read-write|read-only) pass=PASSSTR confirmpass=PASSSTR").
4. See the "[Configuring System / Login Users](#)" section 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 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+)*\$;/;

Set IP address type failed.

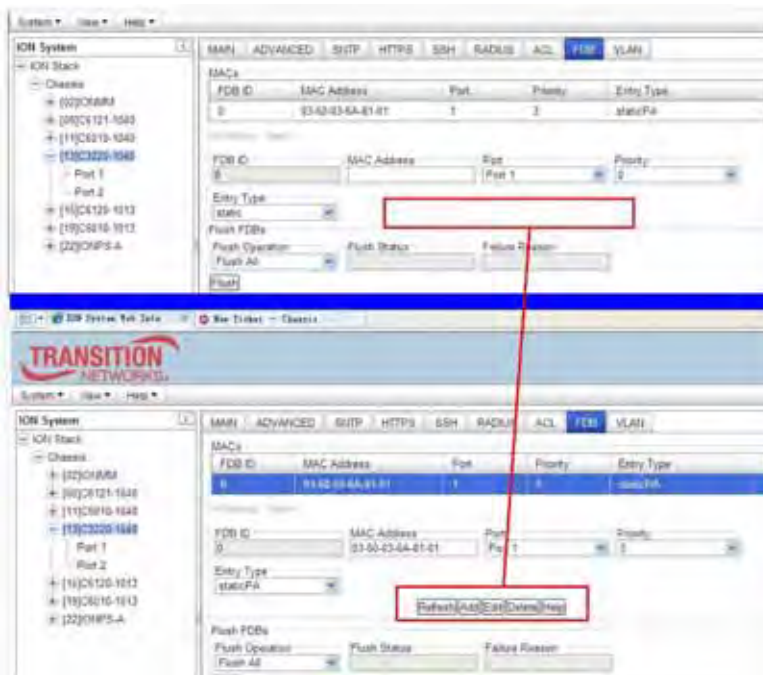
You tried to change the IP address type (mode), but the operation failed. For example:

```
C1|S5|L1D>set ip type=bootp addr=192.168.1.30 subnet-mask=255.255.255.0
Set IP address type failed.
```

1. Enter another (supported) command on this card, or use the "go" command to switch to the IONMM.
2. Make sure the DHCP or BootP server is correctly configured and running.
3. Retry the operation. See “[Setting Up the IP Configuration](#)” on page 42 for the “set ip mode” command.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

In IE8, at C3220 > FDB, the ‘Refresh’, ‘Add’, ‘Edit’, ‘Delete’, ‘Help’ buttons of FDB do not display.



1. Select IE8 **Tools > Compatibility Mode** to use the IE8 ‘Compatibility View’. The message “*Compatibility View - 192.168.1.10 is now running in Compatibility View.*” displays.

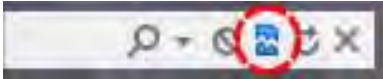


2. Log in to the ION system again.
3. Select the **FDB** tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
4. Click one existing MAC address in the MAC address list.

Website displays incorrectly in Internet Explorer 8 or 9

Websites that were designed for earlier versions of Internet Explorer might not display correctly in the current version. However, you can often improve how a website will look in Internet Explorer by using the new 'Compatibility View' feature. When you turn on Compatibility View, the webpage displayed (and any other webpages within the website's domain) will display as if you were using an earlier version of Internet Explorer.

1. In IE8, click the **Stop** button on the right side of the Address bar.
2. If the page has stopped loading, click the **Refresh** button to try again.
3. Click the **Tools** button, and then click **Compatibility View**.



If Internet Explorer recognizes a webpage that is not compatible, the **Compatibility View** button displays on the Address bar. To turn Compatibility View on, click the **Compatibility View** button. From now on, whenever you visit this website, it will be displayed in Compatibility View. However, if the website receives updates to display correctly in the current version of Internet Explorer, Compatibility View will automatically turn off. Note that not all website display problems are caused by browser incompatibility. Interrupted Internet connections, heavy traffic, or website bugs can also affect how a webpage is displayed. To go back to browsing with Internet Explorer 8 on that site, click the **Compatibility View** button again.

4. Check your ION firmware version and upgrade to the latest if outdated. See the “[Upgrade](#)” section on page 266.
5. Check the Microsoft Support Online website <http://support.microsoft.com/ph/807/en-us/#tab0> for more information.
6. See also: <http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx>
<http://support.microsoft.com/kb/960321>
<http://blogs.msdn.com/b/ie/archive/2008/08/27/introducing-compatibility-view.aspx>
7. In IE9, click the **Compatibility View** toolbar button on the Address bar to display the website as if you were using an earlier version of Internet Explorer. See the Microsoft Support website Article ID: 956197 at <http://support.microsoft.com/kb/956197>.

Section 6: Troubleshooting

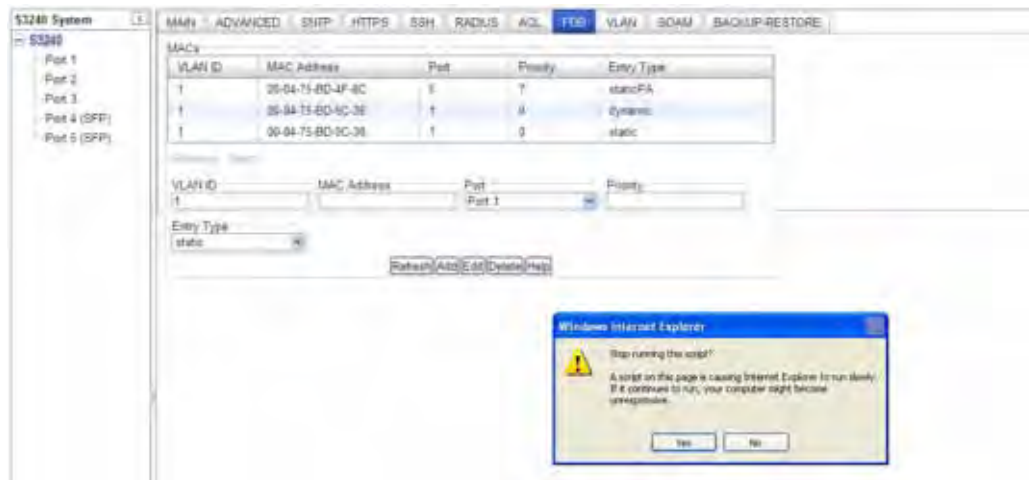
Script error message received.

Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No

Error: Object doesn't support this property or method.

A Runtime Error has occurred. Do you wish to Debug?

Done, but with errors on page.



1. Click the **Yes** button to stop the script.
2. Click **Show Details** to display error details.
3. Disable script debugging.
4. Test a Web page from another user account, another browser, and another computer.
5. Verify that Active Scripting, ActiveX, and Java are not being blocked by Internet Explorer.
6. Remove all the temporary Internet-related files.
7. Install the latest Internet Explorer service pack and software updates.
8. For more advanced troubleshooting, see the Microsoft Support Article ID 308260 at <http://support.microsoft.com/kb/308260>.

Message:

4_T1 port display name enhanced/Remote card version checking with stand alone card.

Cannot find software version of this card!

Error: Set egress/ingress rate failed!

IONMM card version is 1.3, and ARM-based card is 1.2, the SIC needs upgrade

Software version of this card (" + cardVersion + ") is not supported, please upgrade to the same version as the Standalone Card

Software version of this card (" + cardVersion + ") is not supported, please upgrade to the same version as the IONMM

Various FP and ION web interface and CLI compatibility messages.

Meaning: An ION NID compatibility issue occurred. There is a mismatch between a NID and the IONMM firmware versions. For example, you selected 5M/7M/9M/90M at the "Egress Rate Limit" or "Ingress Rate Limit" dropdown, clicked **Save**, and the message displayed.

Recovery:

1. Verify your configuration using the information below.

- ION version 1.2.2 is released for these AVR-based SIC cards with some bug fixes: C3110, C3210, C2110, C2210, C611x, C612x, C6210, BPC and Power Supply.
- ION version 1.3.0 is released for these ARM-based SIC cards with fixes and powerful new features: IONMM, C/S222x, C/S322x, and C/S323x.
- IONMM v1.3 supports the v1.2 AVR-based SIC cards. IONMM v1.3 does not support the v1.2 ARM-base SIC cards.

ARM-based SIC; IONMM revision	1.1	1.2	1.3
1.1	Y	N	N
1.2	N*	Y	N
1.3	N*	N*	Y

Note 1: ARM-base SIC cards include IONMM, C/S222x, C/S322x, and C/S323x.

Note 2: N* means an error interface will display to remind you to upgrade the SIC firmware to the same revision of IONMM.

AVR-based SIC; IONMM revision	1.1	1.2	
1.1	Y	N	
1.2	N*	Y	
1.3	N*	Y	

Note 1: AVR-base SIC cards include C3110, C3210, C2110, C2210, C611x, C612x, C6210, BPC, and Power Supply.

1. Check the firmware versions of the NID and IONMM and upgrade as needed.
2. Check the Release Notes for possible installation scenarios.
3. Re-try the operation.
4. Contact TN Tech Support if the problem persists.

Section 6: Troubleshooting

Problem: S3231 port 1 link is down and the S3231 can't be managed anymore.

Meaning: The S3231 port 1 and attached switch ports should all have link up and S3231 should be able to be managed. If the Management VLAN config has not changed, the S3231 should be manageable all the time.

For example, after the S3231 has run for about two days under Management VLAN, you performed some get and set operations on this card during this time, but made no changes to the Management VLAN configuration. You reboot S3231 to try to recover the Management but it doesn't work.

Recovery: Verify if MAC security is enabled; if so, the port is closed when more than one MAC address arrives at this port (normal operation)

Message:

warning: server1 to server3 is just used for ipv4!

warning: server4 to server6 is just used for ipv6!

Meaning: The DNS 1 through DNS 6 entries can be in IPv4 or IPv6 format, or both (a combination of up to three of each). DNS servers 1-3 are for IPv4; DNS servers 4-6 are for IPv6.

Recovery:

1. Change the DNS server settings to make them valid.
2. See “DNS ‘3 vs. 3’ Rule (‘Up to 3’ Rule)” on page 101.

Web Interface Messages

IMPORTANT

For each procedure described below, do each step sequentially as indicated. If performing the step fixes the problem, **do not** continue with the other steps in the procedure.

Cannot Ping IONMM Device

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails. The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic. The PC can then ping to the NID again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Cannot Ping IONMM Device

1. With the "Management VLAN" state set to "enabled", the PC can not ping the IONMM device. The reason is enabling the Management VLAN function gives management control to the Management VLAN that you enabled.
2. Enter the CLI command **set mgmt vlan state disable** and press **Enter**. The PC can ping to S2220-1013 success again, and the Web interface can be managed again.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Getting values failed (snmp operation timeout)

This message indicates that you entered an invalid parameter value.

1. Click the **Refresh** button to clear the message.
2. Verify the recent parameter entries. Refer to the related CoH (cursor-over-help) and then revise parameter entries as needed.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Failed to start Virtual Cable Test.

This message indicates that the VCT test could not be started.

1. Check the following:
 - Module has power.
 - Cable is properly connected to the port.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Firmware DB operation failed, unzip failed.

This message indicates that the upload of the upgrade file failed.

1. Check that the **db.zip** file was specified in the **Database File Name** field for Windows XP; for Windows 7, specify just “**db**”.
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 input file

This message displays in the “**Upload Result Reason**” field at **IONMM > Upgrade tab > Firmware database** sub-tab if the “Firmware File Name” entered had an incorrect filename format.

1. Verify the parameter value entered; see “[Upgrading IONMM Firmware – Web Method](#)” on page 250 for valid input information.
2. Retry the operation with a valid firmware file name (e.g., *IONMM.bin.1.0.5*, or *x323x.bin.1.0.5*).
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid input found!

This message indicates that you entered a parameter outside the valid range (e.g, VLAN ID = 0).

1. Verify the parameter value to be entered; check the online Help for valid input information.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid password!

This message indicates that the password entered during sign on is not valid.

1. Sign in using the correct password. The default password is **private**.

Note: the password is case sensitive. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Failed to retrieve DMI info on current port.

You clicked the Device port's DMI tab, but the device does not support DMI. Not all NID models support DMI. The NIDs that support DMI have a "D" at the end of the model number.

1. Verify that the NID supports DMI.
2. See "[DMI \(Diagnostic Maintenance Interface\) Parameters](#)" on page 248 for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Admin Status: Down (or Testing)

In the device's port, at the **MAIN** tab in the **Port Configuration** section, the Admin Status field displays "Down". Typically, if 'Admin Status' is Down, then 'Link Status' is also Down.

The status here is the desired state of the interface. The "Testing" status indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with 'Admin Status' in the Down state. As a result of either explicit management action or per configuration information retained by the managed system, 'Admin Status' is then changed to either the Up or Testing states, or remains in the Down state.

Section 6: Troubleshooting

1. Verify the initialization process; see “[Section 2: Installation and System Setup](#)” on page 40.
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization and discovery to take place.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Link Status: Down (or Testing or Dormant, or NotPresent)

This is the current operational state of the interface.

The 'Link Status' Testing state indicates that no operational packets can be passed.

If 'Admin Status' is Down then 'Link Status' likely will be Down.

If 'Admin Status' is changed to Up, then 'Link Status' should change to Up if the interface is ready to transmit and receive network traffic.

'Link Status' should change to Dormant if the interface is waiting for external actions (such as a serial line waiting for an incoming connection);

'Link Status' should remain in the Down state if and only if there is a fault that prevents it from going to the Up state;

'Link Status' should remain in the NotPresent state if the interface has missing (typically, hardware) components.

Link Status: Down: The ION system interface is not ready to transmit and receive network traffic due a fault.

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see “[Section 2: Installation and System Setup](#)“ on page 40.
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization and discovery to take place.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Link Status: Dormant: The ION system interface is waiting for external actions (such as a serial line waiting for an incoming connection).

1. Wait several minutes for initialization and discovery to take place, and then retry the operation.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Link Status: NotPresent: the interface has missing components (typically hardware).

1. Verify the ION system installation; see “[Section 2: Installation and System Setup](#)“ on page 40.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Link Status: *Testing*: The ION system interface can not pass operational packets.

1. Verify that diagnostic tests were run properly and completed successfully.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Setting values failed (http server error)*

This message indicates a configuration entry error (e.g., https).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See “[Configuring HTTPS](#)” on page 208.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Setting values failed (snmp operation error)*

This message indicates that the SNMP Configuration entered had an invalid SNMP entry (e.g., an unrecognized Trap Manager address entry).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See “[Configuring SNMP](#)” on page 226.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *TFTP file transferring failed!*

This message indicates that a TFTP operation could not be completed.

TFTP for Backup download operation:

1. Verify that:
 - a. The correct module(s) has been selected.
 - b. The IP address of the TFTP server is correct.
 - c. The TFTP server is online and available.
2. Perform a backup of the module(s) for which the download operation was intended. Make sure that the status of the backup operation for each module is “*Success*”.
3. Retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

TFTP for Restore upload operation:

1. Check:
 - The IP address of the TFTP server is correct.
 - The TFTP server is online and available.
 - The file to be uploaded is in the default directory on the server.
 - The correct module(s) has been selected.
2. Retry the operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *TFTP operation failed!*

This message indicates that the upload portion of an upgrade operation failed.

1. Check:
 - The IP address of the TFTP server is correct.
 - The TFTP server is online and available.
 - The correct file name is specified (“**db.zip**” for Windows XP or “**db**” for Windows 7).
 - The **db.zip** (or **db**) file is in the default directory on the TFTP server.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *There is a problem with this website's security certificate.*

This message indicates that the security certificate presented by this website was changed.

1. Click the [Continue to this website...](#) selection.
2. See the “[Configuring HTTPS](#)” section on page [192](#).
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Web UI Management connection Lost*

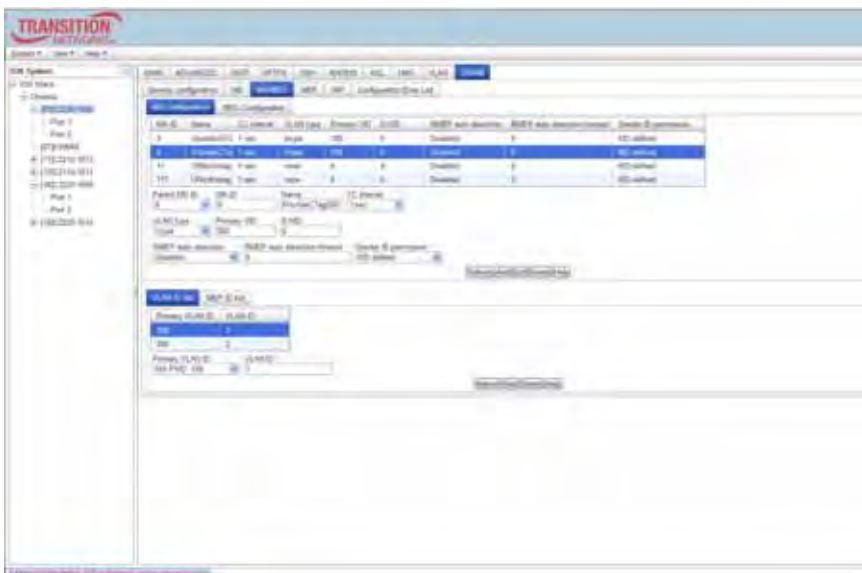
1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails.
The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic.
The PC can ping to S2220-1013 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Adding MA Net failed: AIS is disabled. (snmp operation error)*

Meaning: At **SOAM > MA/MEG > MA Configuration** you selected an existing MA ID and then clicked the **Add** button.

Recovery: At **SOAM > MA/MEG > MA Configuration** select the **Refresh** button.

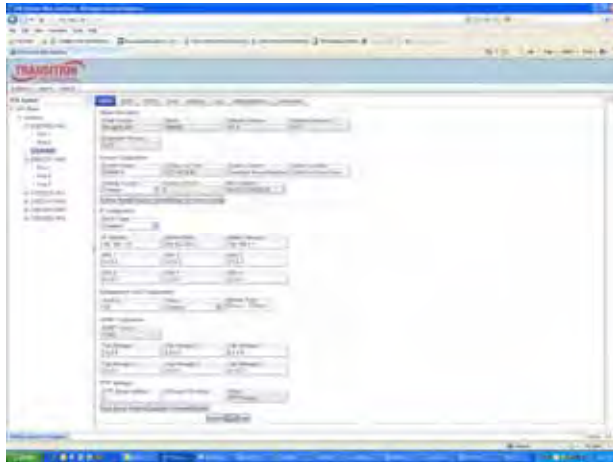
1. Perform the intended operation; either:
 1. Select an existing MA ID and then click the **Edit** button, or
 2. Enter new MA ID information and then click the **Add** button.



Section 6: Troubleshooting

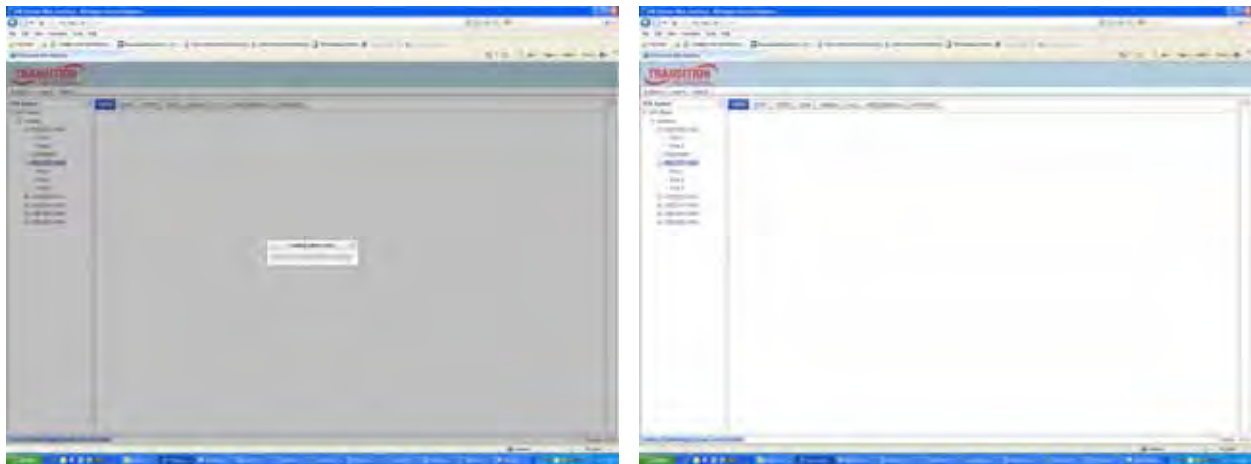
Message: “Setting values in progress ...” displays continuously

The message “Setting values in progress ...” displays for over 10 minutes after you set up a VLAN 100, then set Management VLAN to Enabled and clicked Save.



Getting values failed (http server error) then displays.

Loading Template agent_main_view.htm failed displays:



MAIN tab displayed is blank after you close the **Loading ...** dialog box.

Meaning: These messages display after you turn on the Management VLAN function either via the ION Web interface or the CLI. (The CLI command is **set mgmt vlan state=enable**, and the Web interface is from the IONMM MAIN screen in the **Management VLAN Configuration** section, where the **Status** field is set to **Enabled**. In both cases, management control is given to the Management VLAN that you enabled.

Recovery: The recovery (re-gaining control from the CLI or Web interface) is to turn off Management VLAN via the CLI (**set mgmt vlan state=enable**) or via the Web interface (**IONMM MAIN > Management VLAN Configuration > Status > Enabled**).

Message: *The DMI feature is not supported on current port*

Meaning: Not all NID models support DMI. Transition Networks NIDs that support DMI have a “D” at the end of the model number. If you click the DMI tab on a NID model that does not support DMI, the message “*The DMI feature is not supported on current port.*”

The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.

Recovery: 1. Verify that the device and port support DMI. See “[DMI \(Diagnostic Maintenance Interface\) Parameters](#)” on page 248 for more information.

2. Switch to a NID / port that supports the DMI feature.
3. Retry the operation.

Message: *priority is empty or invalid*

Meaning: Can't change ACL status to enable, message box show "priority is empty or invalid"

Recovery: 1. Review the ACL entries. See “[Configuring an ACL](#)” on page 201.

2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Loading template config file succeeded* displays but the ION Stack node won't expand.

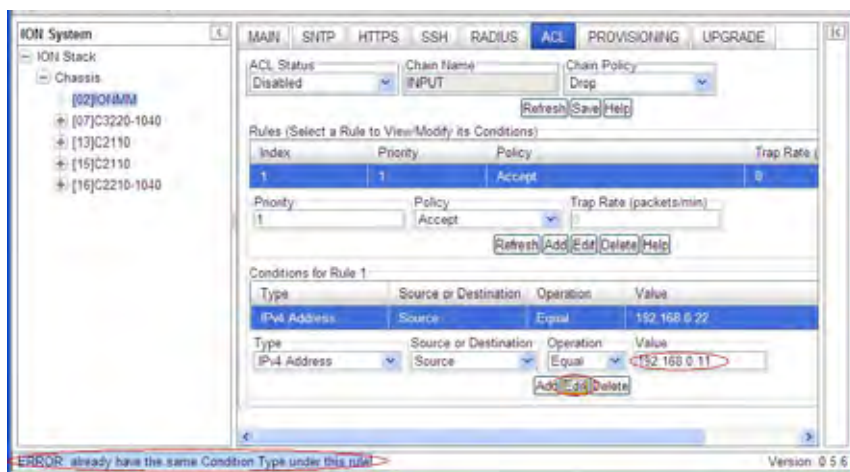
Meaning: Either the loading or the discovery process may be hung up.

Recovery: 1. Click the checkbox to close the “*Loading, please wait ...*” dialog box (if displayed).

2. Contract and expand the ION Stack node again.
3. If the message “*Discovering succeeded*” displays, but the ION Stack node won't expand:
 - a) Sign out and sign back in to the ION system
 - b) Cycle power to the ION system.
 - c) Disconnect and then re-connect the USB cable at the IONMM.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Error - already have the same Condition Type under this rule*



Meaning: At IONMM > ACL tab, when you try to edit or add a Condition to an IP address, the error message displays.

Recovery: 1. Select a different Condition Type, and then change back the original type condition. The Type selections are Source, MAC Address, IPv4 Address, IPv4 Address Range, IPv4 Network, TCP Port, TCP Port Range, UDP Port, UDP Port Range, and ICMP Type.

2. See “[Configuring an ACL](#)” on page 55.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Getting Records failed (snmp operation timeout)*

Message: *Getting records failed (http server error)*

Meaning: The NID could not find the records associated with the operation attempted.

Recovery: 1. Verify the attempted operation was performed correctly (e.g., Policy/ Rule type drop down on the ACL page).

2. Retry the operation. See the applicable section (e.g., “[Upgrade](#)” section on page 321 or page 327, or “[Backup and Restore Operations \(Provisioning\)](#)” on page 296.

3. Reboot the NID. See “[Reboot](#)” on page 317.

3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *System initializing or SNMP service busy, please wait...*

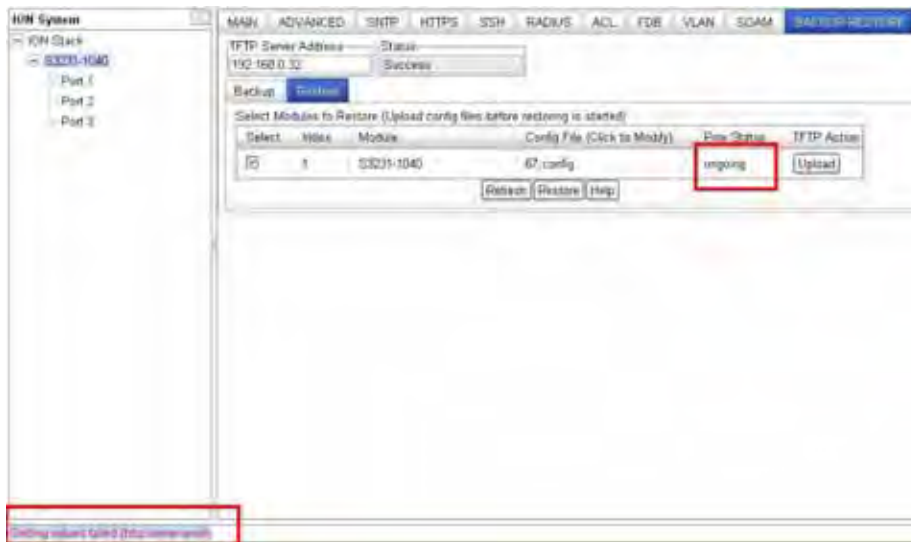
Meaning: The system password was accepted, but the system cannot recognize or process it.

Recovery: Sign in using the correct password. The default password is private. Note that the password is case sensitive.

1. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. Verify the SNMP configuration.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Getting values failed (http server error)* and "ongoing" Prov Status

Meaning: When performing a Restore operation (BACKUP-RESTORE tab) with SOAM configured, the message "Getting values failed (http server error)" displays and the Prov Status column displays "ongoing" after wait message box disappears.



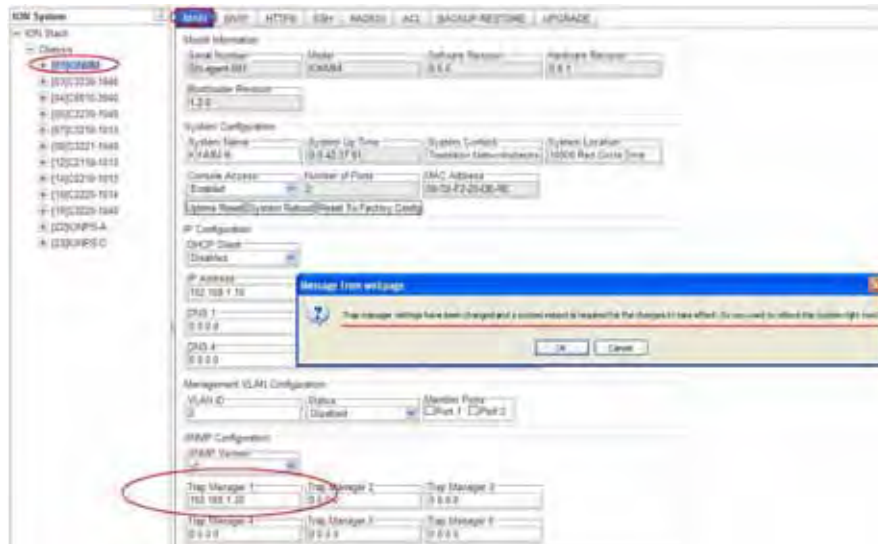
During the card Restore operation, the HTTP/HTTPS server must restart in order to activate the new configuration. At that time, the Web interface momentarily loses connection with the Web server, but when you click the **Refresh** button, the status display and other web operations work normally.

Recovery:

1. Click the **Refresh** button.
2. Verify the Restore configuration and continue operation.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Trap manager settings changed and a system reboot is required for the changes to take effect.*
– Do you want to reboot the system right now?

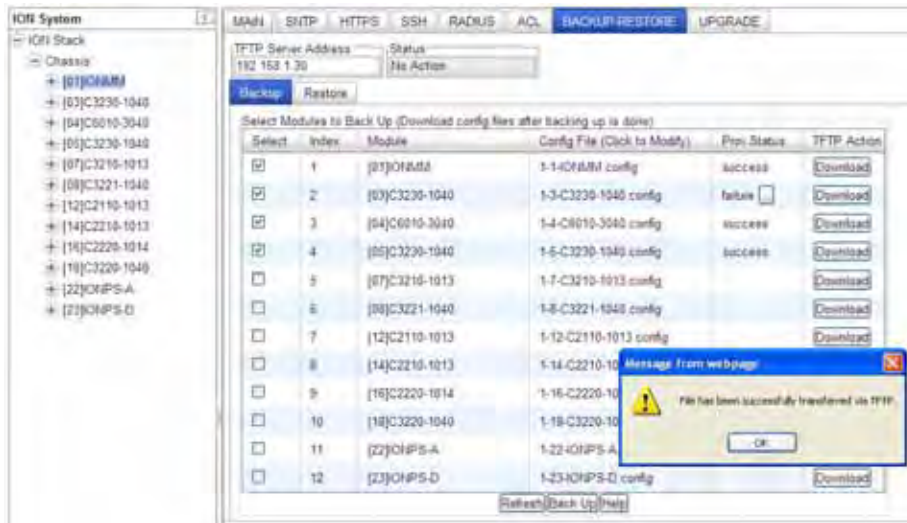


Meaning: Information only. At IONMM > MAIN > SNMP Configuration > Trap Manager x you entered an IP address for a trap server.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Verify the Trap Manager setting and continue operation.
3. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *File has been successfully transferred via TFTP.”* but the Prov. status column displays failure [...].

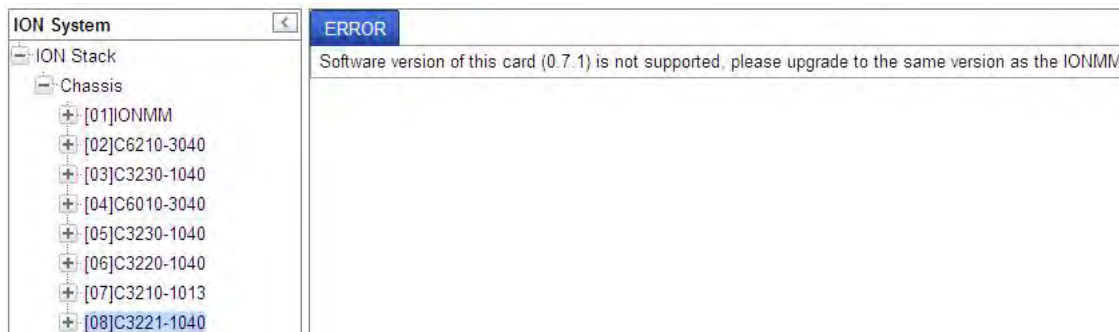


Meaning: At IONMM > BACKUP-RESTORE > Backup you selected a module to back up, the “successful transfer” message displays, but the Prov. Status column displays failure [...].

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Click the [...] box after the word “failure” in the Prov Status column.
3. Open the config.ERR file at *C:\TFTP-Root*.
4. Fix any config commands and then retry the operation.
5. Verify the Backup and continue operation.
6. If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *ERROR: Software version of this card (0.7.1) is not supported, please upgrade to the same version as the IONMM*



Meaning: You selected a device in the tree, but its firmware version is not compatible with the IONMM.

Recovery: 1) Select the IONMM device. 2) Select the UPGRADE tab. 3) Perform a firmware upgrade to this card (and others that may have outdated firmware). See the “Upgrade” section on page 347.

2) If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Failed to retrieve DMI info on current port*



Meaning: You selected **C3230 > Port 2 > DMI** but the DMI information does not display.

Recovery: 1) Click **Refresh**. 2) Expand and contract the tree. 3) If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Current power status of this slot is off, please turn it on before you reset it!*

Meaning: The reset function only works when the slot power is in the On position for the unit to re-boot/reset.

Recovery: 1) At **Chassis > MAIN > Chassis Members** click the "On" button in the **Power Status** column of the device before you click the "Reset" button. 2) If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: Setting the VLANID failed with an SNMP operation error message:

Message: *Setting values failed (snmp operation error) or Adding VLAN failed (snmp operation error)*

Meaning: You tried to add or edit a VLAN ID but the effort failed.

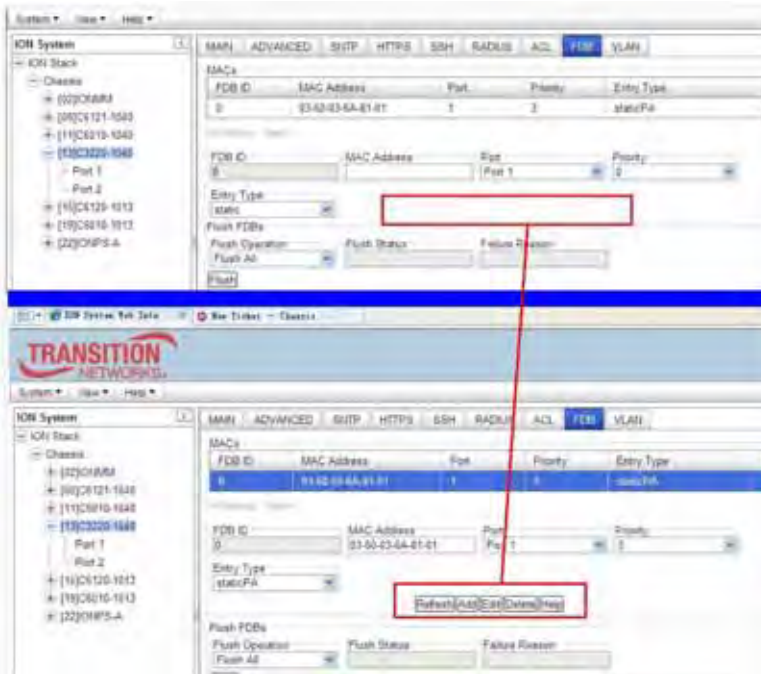
Recovery: The card must be in "Network" mode (at Port 1 > Advanced > Frame Tag Mode) to set the VLAN ID. If it is not set to "Network", an SNMP error will occur. Before adding the ports for Management VLAN, set the Frame Tag Mode of that port to "Network". When Provider tagging is required for that port, then set the Frame Tag Mode to "Provider". A port with the Frame Tag Mode set to the default setting "Customer" can not be added to Member Ports for Management VLAN.

Message: *The value of MD ID must be an integer!*

Meaning: The valid range is from 1 to 21xxxxxxx; if it is larger than the maximum, Focal Point displays "The value of MD ID must be an integer!".

Recovery: 1) Change the setting with a MD ID max of 4294967295. 2) If a problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

In IE8, at C3220 > FDB, the ‘Refresh’, ‘Add’, ‘Edit’, ‘Delete’, ‘Help’ buttons of FDB do not display.



1. Select IE8 **Tools > Compatibility Mode** to use the IE8 ‘Compatibility View’. The message “*Compatibility View - 192.168.1.10 is now running in Compatibility View.*” displays.



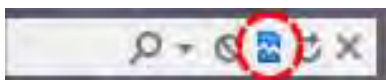
2. Log in to the ION system again.
3. Select the **FDB** tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
4. Click one existing MAC address in the MAC address list.

Section 6: Troubleshooting

Website displays incorrectly in Internet Explorer 8 or 9

Websites that were designed for earlier versions of Internet Explorer might not display correctly in the current version. However, you can often improve how a website will look in Internet Explorer by using the new 'Compatibility View' feature. When you turn on Compatibility View, the webpage displayed (and any other webpages within the website's domain) will display as if you were using an earlier version of Internet Explorer.

1. In IE8, click the **Stop** button on the right side of the Address bar.
2. If the page has stopped loading, click the **Refresh** button to try again.
3. Click the **Tools** button, and then click **Compatibility View**.



If Internet Explorer recognizes a webpage that is not compatible, the **Compatibility View** button displays on the Address bar. To turn Compatibility View on, click the **Compatibility View** button. From now on, whenever you visit this website, it will be displayed in Compatibility View. However, if the website receives updates to display correctly in the current version of Internet Explorer, Compatibility View will automatically turn off. Note that not all website display problems are caused by browser incompatibility. Interrupted Internet connections, heavy traffic, or website bugs can also affect how a webpage is displayed. To go back to browsing with Internet Explorer 8 on that site, click the **Compatibility View** button again.

4. Check your ION firmware version and upgrade to the latest if outdated. See the “[Upgrade](#)” section on page 266.
5. Check the Microsoft Support Online website <http://support.microsoft.com/ph/807/en-us/#tab0> for more information.
6. See also: <http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx>
<http://support.microsoft.com/kb/960321>
<http://blogs.msdn.com/b/ie/archive/2008/08/27/introducing-compatibility-view.aspx>
7. In IE9, click the **Compatibility View** toolbar button on the Address bar to display the website as if you were using an earlier version of Internet Explorer. See the Microsoft Support website Article ID: 956197 at <http://support.microsoft.com/kb/956197>.

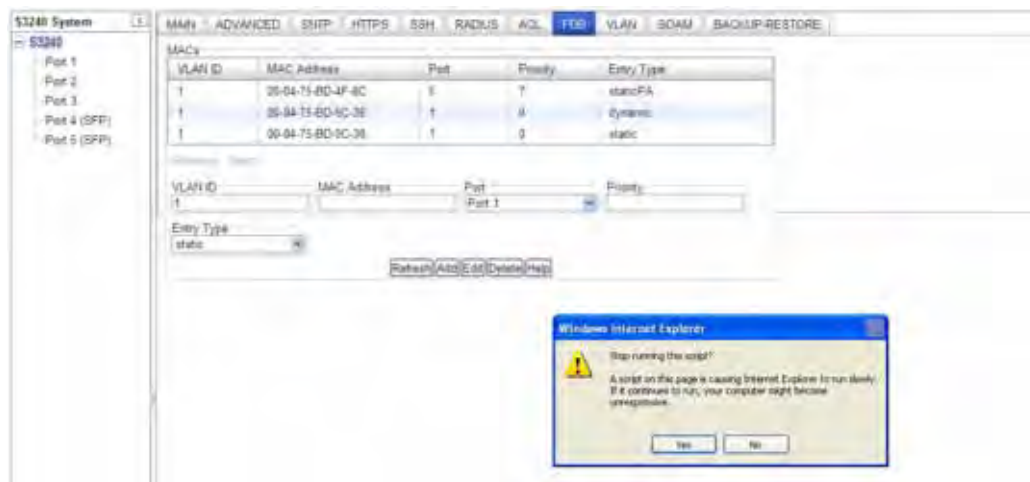
Script error message received.

Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No

Error: Object doesn't support this property or method.

A Runtime Error has occurred. Do you wish to Debug?

Done, but with errors on page.



1. Click the **Yes** button to stop the script.
2. Click **Show Details** to display error details.
3. Disable script debugging.
4. Test a Web page from another user account, another browser, and another computer.
5. Verify that Active Scripting, ActiveX, and Java are not being blocked by Internet Explorer.
6. Remove all the temporary Internet-related files.
7. Install the latest Internet Explorer service pack and software updates.
8. For more advanced troubleshooting, see the Microsoft Support Article ID 308260 at <http://support.microsoft.com/kb/308260>.

Problem: OAM loopback can be enabled and is working on the fiber ports, but not on the copper ports.

Meaning: The documented loopback procedure does not work on copper ports.

Recovery:

1. You must first enable OAM on the fiber ports to be able to establish OAM on the copper side. The OAM PDU's can only be received from copper ports if the fiber ports are also OAM enabled. The fiber port is the network connection between the two devices, and this is the path that the copper ports send their OAM PDU's between remote peer devices.
2. Follow the procedure in the section "[Copper Port Loopback Procedure](#)" on page 144.
3. To determine if the loopback was successful, the LOAM counters show "loopback sent" and "loopback received".

SNMP Messages

For any error condition, you can check the [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 engineIDType, forcing IPv4

Meaning: You entered an SNMP v3 command, but the command failed due to an unrecognized entry.

Recovery: 1) Make sure this is the command you want. Use the Help (?) command for details. 2) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 3) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 4) Try using the ION Web interface to perform the function. 5) If the problem persists, contact 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.

Section 6: Troubleshooting

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.

Section 6: Troubleshooting

Message:

Resetting local Engine ID will delete all exist local users, continue?(y: yes, n: no)

Meaning: You entered an SNMP v3 command, but a confirmation message displayed.

Recovery: 1) Make sure this is the command you want. Use the Help (?) command for details. 2) Enter **n** if you are not sure you want to reset the local Engine ID, or enter **y** to continue to reset the local Engine ID and delete all existing local users.

Message:

ERROR: Adding sub oid tree to defaultView is prohibited!

ERROR: defaultView can not be deleted!

ERROR: Modifying defaultView is prohibited!

ERROR: Please do not modify the View Name or the OID Sub Tree!

ERROR: Sub oid tree in defaultView can not be deleted!

ERROR: This group can not be deleted!

Meaning: You entered an SNMP v3 command, but the add/delete/modify command failed.

Recovery: 1) Wait for a few moments for the operation to complete. 2) Make sure this is the command you want. Use the Help (?) command for details. 3) Make sure this device / port supports the command/function attempted. Use the **go** command to switch locations. 4) Verify the command syntax and re-enter the command. See the related section of the manual for specifics. 5) Try using the ION Web interface to perform the function. 6) If the problem persists, contact 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.

Section 6: Troubleshooting

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.

Section 6: Troubleshooting

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 timeout value!*

Meaning: You set an unsupported SNMP trap timeout boundary value.

Recovery: 1) In the "**add snmp traphost**" command, specify a valid timeout (-15s%-16s%-5u%-30s%-16s%-12s%-12u%-12u%s (change from 8u to 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](http://www.transition.com/techsupport); fax: +1 952-941-2322; Email: techsupport@transition.com.

Section 6: Troubleshooting

Message: *Invalid group parameter for user!*

No group name is specified!

Too many options follow \"group name\"!

Meaning: You entered the CLI command for adding a local snmpv3 user, but the entry failed.

Recovery: 1) Verify the "**add snmp local user name**" syntax. 2) Check if the ION firmware is the latest and upgrade if possible. 3) If the problem persists, contact TN Tech Support.

Message:

Following \"authentication password\" should be either \"group\" option or no option!

Following \"noAuthNoPriv\" should be either \"group\" option or no option!

Following \"privacy password\" should be \"group\" option or no option!

Meaning: You entered an invalid group parameter while creating an SNMP v3 user

Recovery: 1) Verify the "add snmp local user" syntax. 2) Check if the ION firmware is the latest and upgrade if possible. 3) If the problem persists, contact 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:

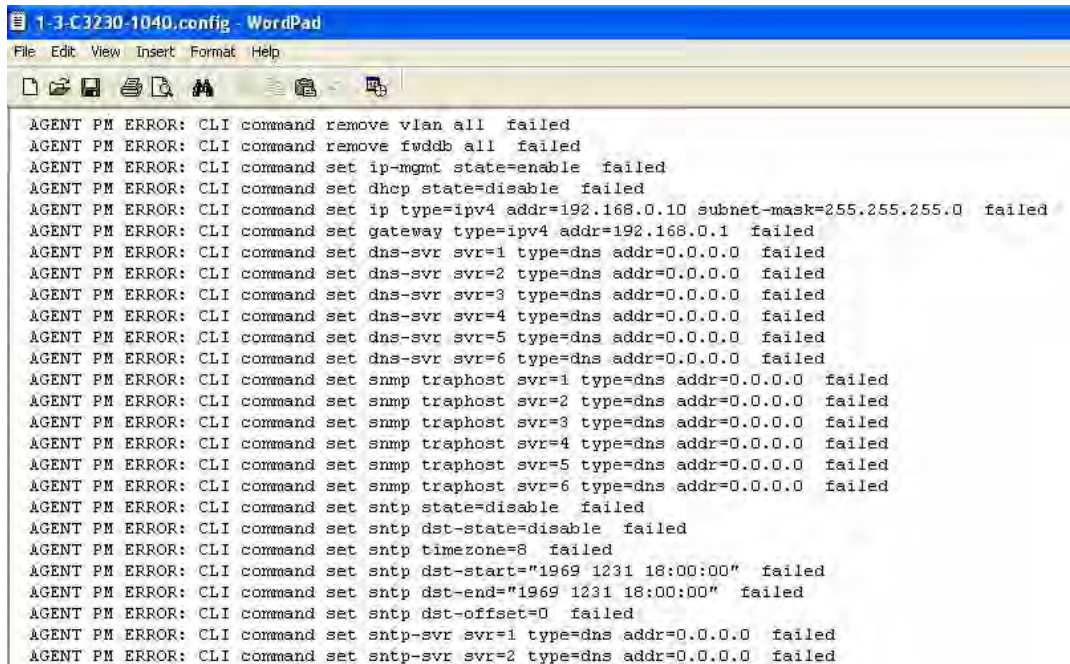
```
S3230-1040 C0|S0|L1D>show snmp group name
Name          Security Model      Security Level   Read View   Write View   Notify View
-----
login: ION
Password:
```

Recovery: 1. Log in to the ION system again. 2. Configure the SNMPv3 Local or Remote Engine ID before you configure the Local or Remote Users for this engine. See "[Configuring SNMP](#)" on page 27. Retry the operation.

The Config Error Log (config.err) File

The error log file (.ERR file) is downloaded to the TFTP server address specified, in TFTP-Root, with a filename such as *1-11-C2210-1013.config*. You can open the file in WordPad or a text editor. The config.err messages are failed web interface functions that were attempted, translated into CLI commands.

A sample portion of an error log file (.ERR file) is shown below.



```

AGENT PM ERROR: CLI command remove vlan all failed
AGENT PM ERROR: CLI command remove fwddb all failed
AGENT PM ERROR: CLI command set ip-mgmt state=enable failed
AGENT PM ERROR: CLI command set dhcp state=disable failed
AGENT PM ERROR: CLI command set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed
AGENT PM ERROR: CLI command set gateway type=ipv4 addr=192.168.0.1 failed
AGENT PM ERROR: CLI command set dns-svr svr=1 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=2 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=3 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=4 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=5 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set dns-svr svr=6 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=1 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=2 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=3 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=4 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=5 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp traphost svr=6 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp state=disable failed
AGENT PM ERROR: CLI command set snmp dst-state=disable failed
AGENT PM ERROR: CLI command set snmp timezone=8 failed
AGENT PM ERROR: CLI command set snmp dst-start="1969 1231 18:00:00" failed
AGENT PM ERROR: CLI command set snmp dst-end="1969 1231 18:00:00" failed
AGENT PM ERROR: CLI command set snmp dst-offset=0 failed
AGENT PM ERROR: CLI command set snmp-svr svr=1 type=dns addr=0.0.0.0 failed
AGENT PM ERROR: CLI command set snmp-svr svr=2 type=dns addr=0.0.0.0 failed
  
```

These messages show a translation of failed web interface functions that were attempted, translated into their equivalent CLI commands.

The config.err files are saved in the TFTP server location specified (typically *C:\TFTP-Root*) with a file name something like: *1-2-2-C3220-1040_20100608.config.err*. Each message is prefixed by the words “AGENT PM ERROR: CLI command”. The remaining words and phrases are explained below:

1. The first word in the message (e.g., *add*, *set*, *remove*) shows the type of action attempted.
2. The second word or phrase in the message (e.g., *dhcp state*, *fwddb*, *gateway type*, *vlan-db vid*, etc.) lists the general function attempted. This is the part of the message immediately preceding the = sign.
3. The next word or phrase in the message is the specific function attempted that immediately follows the = sign or the second word of the message (e.g., *all*, *=enable*, *=disable*, *=8*, *=dns addr=0.0.0.0*, etc.). This part of the error message may include several segments with = signs (e.g., *=0.0.0.0 retry=3 timeout=30*).
4. The final word in the message line is the word “failed”.

Section 6: Troubleshooting

config.err Messages

Sample config.err file information is provided below.

1-2-2-C3220-1040_20100608.config.err

Line

```

1 AGENT PM ERROR- CLI command remove vlan all failed
2 AGENT PM ERROR- CLI command remove fwddb all failed
3 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed
4 AGENT PM ERROR- CLI command remove vlan all failed
5 AGENT PM ERROR- CLI command remove fwddb all failed
6 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-02 conn-port=1 priority=1 type=staticNRL failed
7 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-03 conn-port=1 priority=1 type=staticNRL failed
8 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-04 conn-port=1 priority=1 type=staticNRL failed
9 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-05 conn-port=1 priority=1 type=staticNRL failed
10 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-06 conn-port=1 priority=1 type=staticNRL failed
11 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-07 conn-port=1 priority=1 type=staticNRL failed
12 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-08 conn-port=1 priority=1 type=staticNRL failed
13 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-09 conn-port=1 priority=1 type=staticNRL failed
14 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed
15 AGENT PM ERROR- CLI command remove vlan all failed
16 AGENT PM ERROR- CLI command remove fwddb all failed
17 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-02 conn-port=1 priority=1 type=staticNRL failed
18 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-03 conn-port=1 priority=1 type=staticNRL failed
19 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-04 conn-port=1 priority=1 type=staticNRL failed
20 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-05 conn-port=1 priority=1 type=staticNRL failed
21 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-06 conn-port=1 priority=1 type=staticNRL failed
22 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-07 conn-port=1 priority=1 type=staticNRL failed
23 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-08 conn-port=1 priority=1 type=staticNRL failed
24 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-09 conn-port=1 priority=1 type=staticNRL failed
25 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed
26 AGENT PM ERROR- CLI command remove vlan all failed
27 AGENT PM ERROR- CLI command remove fwddb all failed
28 AGENT PM ERROR- CLI command add fwddb mac=01-00-00-00-00-10 conn-port=1 priority=1 type=staticNRL failed

```

config.err Message Responses

Some typical error log file messages and the recommended responses are provided below (without the prefix of “AGENT PM ERROR: CLI command”).

Message: remove vlan all failed

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: remove fwddb all failed

Response: 1. Check if this is a recurring problem. 2. Verify the Forwarding Database (FWDB) operation in the related section of this manual. Retry the FWDB operation. 3. See the related FWDB command in *the ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set dhcp state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the DHCP operation in the related section of this manual. Retry the DHCP operation. 3. See the related DHCP command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set gateway type=ipv4 addr=192.168.0.1 failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set dns-svr svr=1 type=dns addr=0.0.0.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the DNS Server operation in the related section of this manual. Retry the operation. 3. See the related DNS server command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set snmp traphost svr=1 type=dns addr=0.0.0.0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set snmp state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set snmp dst-state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set snmp timezone=8 failed

Response: 1. Check if this is a recurring problem. 2. Verify the SNMP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNMP command in the *ION System CLI*

Section 6: Troubleshooting

Reference Manual, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set snmp dst-start="1969 1231 18:00:00" failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set snmp dst-end="1969 1231 18:00:00" failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set snmp dst-offset=0 failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set snmp-svr svr=1 type=dns addr=0.0.0.0 failed`

Response: 1. Check if this is a recurring problem. 2. Verify the SNTP operation in the related section of this manual. Retry the SNMP operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set radius client state=disable failed`

Response: 1. Check if this is a recurring problem. 2. Verify the RADIUS operation in the related section of this manual. Retry the RADIUS operation. 3. See the related RADIUS command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `set radius svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30 failed`

Response: 1. Check the RADIUS server setup, configuration and documentation. 2. Verify the RADIUS operation in the related section of this manual. Retry the RADIUS operation. 3. See the related SNTP command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: `add vlan-db vid=100 priority=0 pri-override=disable failed`

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in *the ION System CLI Reference Manual, 33461*. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: add vlan-db vid=200 priority=0 pri-override=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set acl state=disable failed

Response: 1. Check if this is a recurring problem. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set acl table=filter chain=input policy=accept failed

Response: 1. Check if this is a recurring problem. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: set dot1dbridge ip-priority-index=0 remap-priority=0 failed

Response: 1. Check if this is a recurring problem. 2. Verify the operation in the related section of this manual. Retry the operation. 3. See the related dot1dbridge command in the *ION System CLI Reference Manual*, 33461. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: AGENT PM ERROR: CLI command show dot1dbridge ip-tc priority remapping failed

Response: 1. Check if this is a recurring problem with ACL Rules and Conditions. 2. Verify the ACL operation in the related section of this manual. Retry the ACL operation. 3. See the related ACL command in the *ION System CLI Reference Manual*, 33461. 4. If the message was the result of recent backup/restore, retry the operations. 5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: DHCP failed, please restart system to recover.

Response:

1. Retry the operation.
2. If the problem recurs:
 - a. Make sure a DHCP server is on the network, available and running.
 - b. Make sure the DHCP client is enabled.
 - c. Verify the DHCP IP address assignment procedure in "[Assigning a Dynamic IP Address via DHCP](#)" on page 92.
3. Restart the system.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: AGENT PM ERROR: CLI command set lpt state=configuration. failed

Response:

1. Make sure the LPT (Link Pass Through) is enabled.
2. Retry the operation.
3. Verify the procedure in "[Configuring Selective and Transparent Link Pass Through](#)" on page 204.
4. Restart the system.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: AGENT PM ERROR: CLI command set rfd state=configuration. failed

Response:

1. Make sure the RFD (Remote Fault Detect) is enabled.
2. Retry the operation.
3. Verify the procedure in "[Configuring Selective and Transparent Link Pass Through](#)" on page 204.
4. Restart the system.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

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...

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.

Section 6: Troubleshooting

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.
- 5.

System initializing or SNMP service busy, please wait..." : "Invalid password!

Meaning: possible internal error.

Recovery:

1. Wait for several seconds for the message to clear.
2. Verify the Syslog configuration. See “[Configuring System Logging \(Syslog\)](#)” 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.

Syslog Warning: A defined IDS is detected.

Meaning: The Upgrade file failed, the Web interface reports an error, the system can't login and keeps initializing. For example:

```
Line 1 Jan 1 19:33:01 (none) user.warn subagent[818]: A defined IDS is detected.
```

At the ACL tab, you selected rule 1 and edited policy to "Trap", Trap Rate to "4", selected Condition 1, and then edited the Condition 1 value to the local host's IP address. Then uploaded upgrade file by TFTP server tried to upgrade the system. The upgrade file failed, the Web interface reported an error, and the system can't login and keeps initializing. After enabling the ACL trap for the same source IP as the TFTP server and doing tftp operation to the TFTP server, a large amount of packets with the source TFTP server IP are received by the IONMM and each packet is looked at as an IDS packet which caused the subagent and snmpd to become overburdened.

Recovery: None; this issue appears as something like a manual IDS attack to the ION system, which may not be an issue for most users.

Section 6: Troubleshooting

Sample Sys.log Output

A typical Syslog output is shown below.

```

Line
1 00|80|L1D>cat sys.log
2 Dec 31 18:00:07 (none) local5.notice bpd_linux[716]: BFD Started.
3 Dec 31 18:00:08 (none) local5.notice loam[715]: LOAM started
4 Dec 31 18:00:12 (none) user.notice subAgent2[726]: subAgent Started.
5 Dec 31 18:00:16 (none) daemon.notice ION-EM[742]: Entity Manager running in Mast
6 er Mode
7 Dec 31 18:00:17 (none) daemon.notice ION-EM[742]: Discovered a card in slot-[0],
8 relpos=[1]
9 Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=1
10 Dec 31 18:00:19 (none) user.notice subAgent2[726]: create contextID=2
11 Dec 31 18:00:19 (none) user.notice subAgent2[726]: subAgent session connected.
12 Dec 31 18:00:19 (none) user.notice subAgent2[726]: Standalone mode, Send the col
13 dStart trap.
14 Dec 31 18:00:21 (none) daemon.err snmpd[719]: ion-ns/logical: session from local
15 subAgent2_end_point_name [/var/agentx/master]
16 Dec 31 18:28:58 (none) local5.err bpd_linux[716]: BFD ERROR: SAP(3) closed for a
17 ppPduFrameLen == 0 when recyMsgFromAppSAP
18 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
19 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
20 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
21 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
22 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
23 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
24 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
25 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
26 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
27 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
28 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
29 Dec 31 18:29:08 (none) user.err subAgent2[822]: agentx_send: Broken pipe
30 Dec 31 18:29:08 (none) daemon.warn ION-EM[742]: AgentX master agent failed to re
31 spond to ping. Attempting to re-register.

```

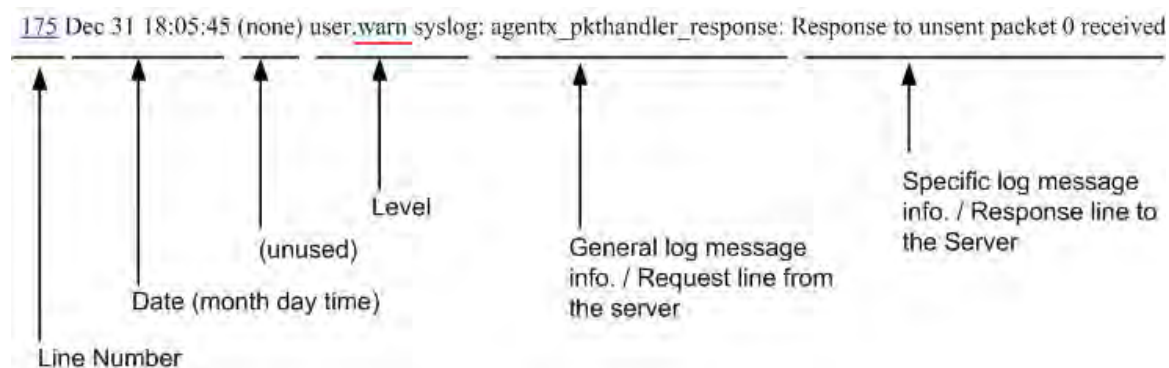
A typical syslog message is shown below.

```

175 Dec 31 18:05:45 (none) user.warn syslog: agentx_pkthandler_response: Response to unsent
packet 0 received

```

The Syslog format is shown below.



Syslog messages, their meanings, and suggested responses are provided below.

Message: local5.err bpd_linux[716]: BPD ERROR: SAP(8) closed for a ppPduFrameLen == 0 when recvMsgFromAppSAP

Meaning: Level 3 Error (err) severity; received a frame with a frame length of 0.

Recovery: 1. Refer to your organizations policy for this level of severity. 2. Retry the operation. 3. If the problem persists, contact Technical Support. 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 which descript as "user.err upgrade-Manager", that 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.

Section 6: Troubleshooting

Sys.log sample - A typical Syslog output is shown below (Telnet screen)

```

telnet 192.168.0.10
logshow -l 4.1 (2011-03-01 14:39:04) C13 Serial-0 in shell (ach3)
Enter 'help' for a list of built-in commands.

T # cd /var/log
/var/log # cat sgs.log
Jan 1 00:00:18 (snmp) snmp-notification: attach platform info in closed memory at 0x00000000
Jan 1 00:00:19 (snmp) snmp-err upgradeManager(17191): upgradeManager starts...
Jan 1 00:00:19 (snmp) snmp-err upgradeManager(17201): upgradeManager covers both lanes...
Jan 1 00:00:21 (snmp) local5.notice hpd_11mc(17311): SPD Started...
Jan 1 00:00:22 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 11 is released already.
Jan 1 00:00:22 (snmp) dsmon.notice 100-DM(17231): attach platform info in shared memory at 0x00000000
Jan 1 00:00:23 (snmp) dsmon.notice 100-DM(17231): Backup Manager running in Backup Mode
Jan 1 00:00:26 (snmp) snmp-notice subagent(17411): subagent Started...
Jan 1 00:00:27 (snmp) snmp-notice subagent(17411): attach platform info in shared memory at 0x00000000
Jan 1 00:00:27 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 7 is released already.
Jan 1 00:00:28 (snmp) dsmon.notice 100-DM(17231): Discovered Character 1
Jan 1 00:00:28 (snmp) snmp-err upgradeManager(17201): location = 13421728
Jan 1 00:00:28 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:28 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 15 is released already.
Jan 1 00:00:28 (snmp) dsmon.notice 100-DM(17231): Discovered a card in slot-141, rslpwr-111
Jan 1 00:00:29 (snmp) snmp-err upgradeManager(17201): location = 152047520
Jan 1 00:00:29 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:29 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 11 is released already.
Jan 1 00:00:29 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 13 is released already.
Jan 1 00:00:29 (snmp) dsmon.notice 100-DM(17231): Discovered a card in slot-1221, rslpwr-111
Jan 1 00:00:29 (snmp) snmp-err upgradeManager(17201): location = 222540992
Jan 1 00:00:29 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:29 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 14 is released already.
Jan 1 00:00:30 (snmp) dsmon.notice 100-DM(17231): Discovered a card in slot-141, rslpwr-111
Jan 1 00:00:30 (snmp) snmp-err upgradeManager(17201): location = 137986560
Jan 1 00:00:30 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:30 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 18 is released already.
Jan 1 00:00:30 (snmp) dsmon.notice 100-DM(17231): Discovered a card in slot-161, rslpwr-111
Jan 1 00:00:30 (snmp) snmp-err upgradeManager(17201): location = 160947120
Jan 1 00:00:30 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:30 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:31 (snmp) snmp-err upgradeManager(17201): location = 179406080
Jan 1 00:00:31 (snmp) snmp-err upgradeManager(17201): It is 8GEN0 hard disk!!
Jan 1 00:00:31 (snmp) snmp-err upgradeManager(17201): Just reply OK ...
Jan 1 00:00:31 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 15 is released already.
Jan 1 00:00:31 (snmp) dsmon-err snmp(17301): [snmp-logical]: session from local subagent2 and print_snm /var/log/snmp/err
snmp1
Jan 1 00:00:34 (snmp) dsmon-err snmp(17301): [snmp-logical]: session from local subagent2 and print_snm /var/log/snmp/err
snmp1
Jan 1 00:00:34 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 13 is released already.
Jan 1 00:00:34 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 14 is released already.
Jan 1 00:00:34 (snmp) local5.err hpd_11mc(17311): SPD ERROR: the application dsap 15 is released already.
/var/log #

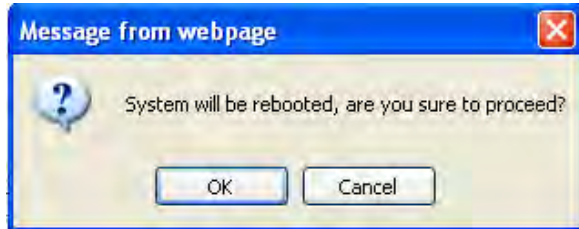
```

Webpage Messages

Certain menu operations will display a webpage verification message to verify that you want to proceed. These messages also provide information on the effect that the operation will have if you continue. These messages display for operations such as **Reset to Factory Config**, **Reboot the System**, or other operational confirmation messages.

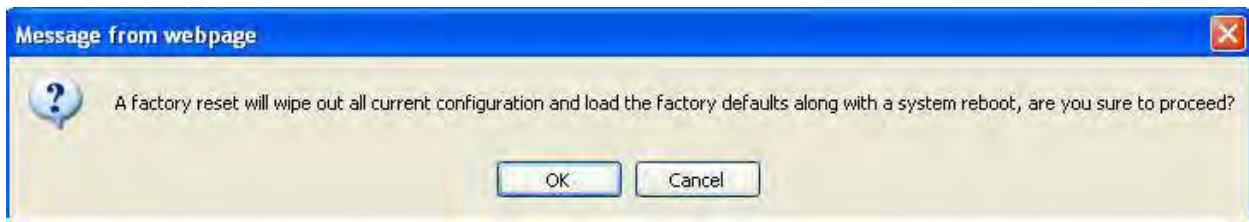
See [Menu System Notes](#) on page 79 for more information.

Message: *System will be rebooted, are you sure to proceed?*



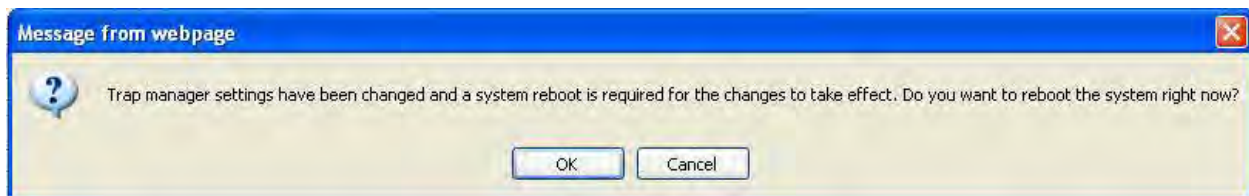
Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

Message: *A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*



Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

Message: *Trap manager settings have been changed and a system reboot is required for the changes to take effect. Do you want to reboot the system right now?*

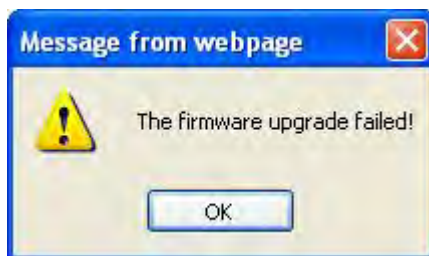


Meaning: At the device's **MAIN > SNMP Configuration** tab you clicked Save to create a new SNMP trap server location.

Response: Click **OK** only if you wish to reboot the system right now. Otherwise click **Cancel**. See [SNMP Configuration](#) on page 229.

Section 6: Troubleshooting

Message: *The firmware upgrade failed!*



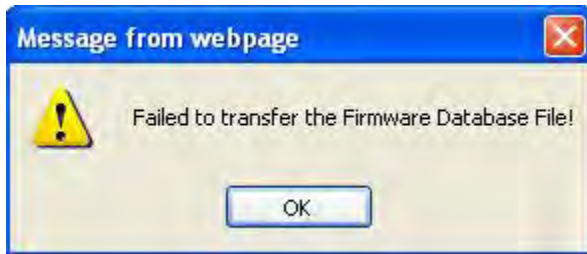
The **MAIN** tab > **TFTP Settings** section **Status** area displays “*TFTP Failure*”.

Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the [Upgrade the IONMM Firmware](#) section on page 205.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Transition Networks web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.1.0.5**).
6. Check the log status in the TFTP Server package; when successful, it should show something like “*Sent IONMM.bin.1.0.5 to (192.168.1.30), 9876543 bytes*”. The **TFTP Settings** section **Status** area should display “*Success*” when done.
7. Make sure that the Management VLAN function is disabled.
8. Reset the device. The **TFTP Settings** section **Status** area should display “*Success*” when done.
9. Check the “[TFTP Server Messages](#)” sub-section in the “[Third Party Tool Messages](#)” section on page 415.
10. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Failed to Transfer the Firmware Database File!*



Meaning: While performing a Firmware Upgrade from the **MAIN** tab > **TFTP Settings** section, a problem was detected. See the [Upgrade the IONMM Firmware](#) section on page 205.

Recovery:

1. Click **OK**.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Transition Networks web site.
4. Verify the **TFTP Server Address** entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the **Firmware File Name** that you entered is the one you intended, and that it is in the proper filename format (e.g., **IONMM.bin.1.0.5**).
6. Check the log status in the TFTP Server package; when successful, it should show something like “Sent IONMM.bin.1.0.5 to (192.168.1.30), 9876543 bytes”. The **TFTP Settings** section **Status** area should display “Success” when done.
7. Reset the device. The **TFTP Settings** section **Status** area should display “Success” when done.
8. Check the “[TFTP Server Messages](#)” sub-section in the “[Third Party Tool Messages](#)” section on page 415.
9. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *MEG/MD ID: value isn't a number.*



Meaning: An error was detected at the **SOAM > MIP > MD/MEG ID** entry.

Recovery:

1. Select a valid (defined) MD ID or MEG ID.
2. Click the **OK** button.
3. See the “[SOAM MIP Config – Web Method](#)” section on page 126.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *No LTRs has been received.*



Meaning: An error was detected at the **SOAM > MEP > Linktrace** entry.

Recovery: See “[Configuring Linktrace \(LT\)](#)” on page 152.

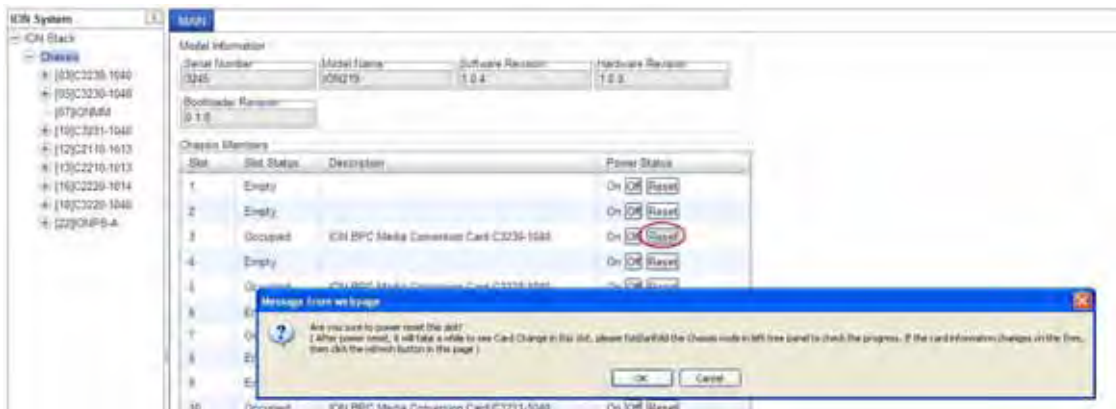
Message: *You should select a MEP from the MEP configuration table.*



Meaning: An error was detected at the **SOAM > MEP > DM** entry.

Recovery: See “[Configuring DM \(Frame Delay Measurement\)](#)” on page 152.

Message: *Are you sure to power reset this slot? (After power reset, it will take a while to see card change in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page.)*



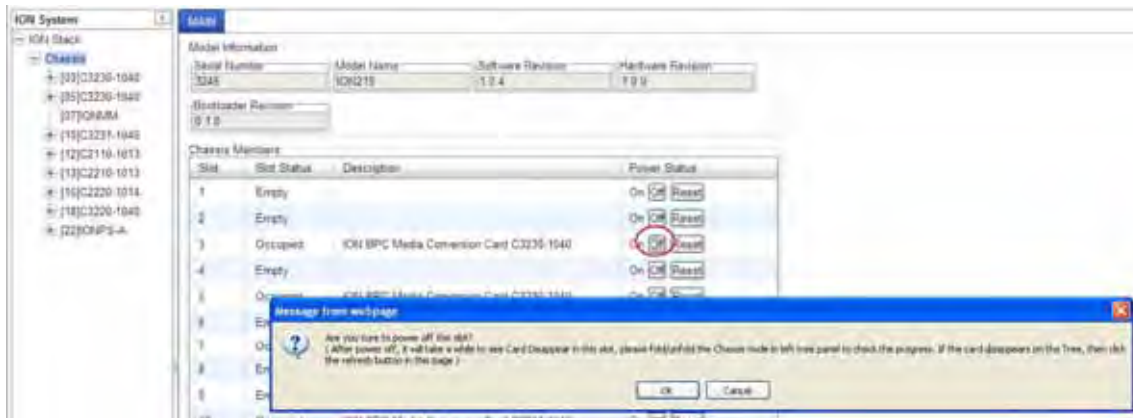
Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Reset** button for a particular slot.

Recovery:

1. If you are not sure that you want to reset this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to reset this chassis, click the **OK** button to clear the message and reset power to the slot.
3. At the **Chassis > MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See the “[Menu System Notes](#)” section on page 77.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Are you sure you want to power off this slot? (After power off, it will take a while to see Card Disappear in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page.)*

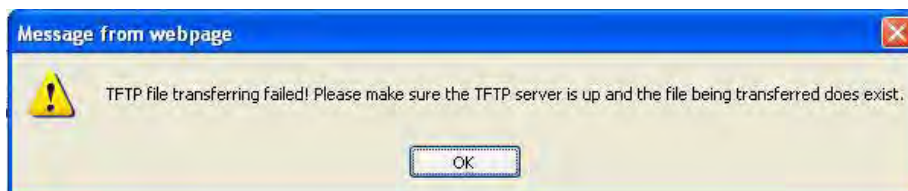


Meaning: A caution message generated at the **Chassis > MAIN** tab. You clicked the **Off** button for a particular slot.

Recovery:

1. If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to power off this slot, click the **OK** button to clear the message and remove power to the slot.
3. At the **Chassis > MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See the “[Menu System Notes](#)” section on page 77.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *TFTP file transferring failed!*



Meaning: Either the TFTP Server is not running, or the filename entered was incorrect or not found. See the “[Backup/Restore Operations](#)” section on page 218.

Recovery: 1. Start the TFTP Server and verify the name and location of the file to be transferred. If the file does not exist (e.g., at *C:\TFTP-Root*), then download the file from the TN website at <http://transition.com/TransitionNetworks/TechSupport/Downloads/Software.aspx>. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *HTTPS settings have been changed and a re-login will be performed right now.*

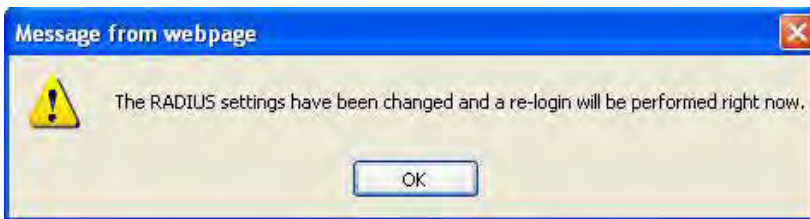


Meaning: You performed a Copy Certificate function for the IONMM in the HTTPS tab.

Recovery:

1. Click **OK** to clear the message.
2. See “[Configuring HTTPS](#)” on page 192.
3. If a message displays regarding a problem with the website's security certificate, select “Continue to this website”.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *The RADIUS settings have been changed and a re-login will be performed right now.*



Meaning: You performed a Copy Certificate function for the IONMM in the RADIUS tab.

Recovery:

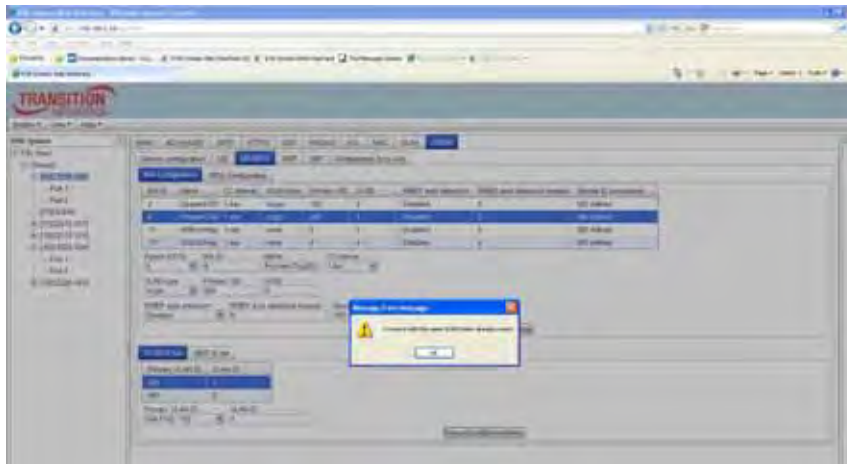
1. Click **OK** to clear the message.
2. Sign in to ION System Web Interface (RADIUS). See “[Configuring RADIUS](#)” on page 192.
3. If a message displays regarding a problem with the website's security certificate, select “Continue to this website”.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *A record with the same VLAN index already exists!*



Meaning: At **SOAM > MA/MEG > MA Configuration** you selected a VLAN from the table and clicked the **Add** button.



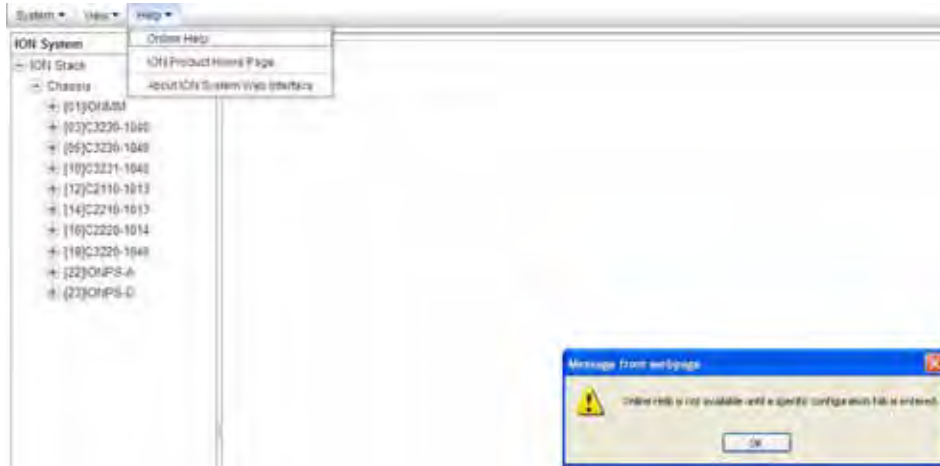
Recovery:

1. Click the **OK** button to clear the error message.
2. Click the **Refresh** button
3. To add a new VLAN record, enter new information and click the **OK** button.
To edit an existing VLAN record, select a VLAN ID from the list and click the **Edit** button.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Online Help is not available until a specific configuration is entered.*



Meaning: You clicked on **Online Help** from the **Help** dropdown without first selecting a device.



Recovery:

1. Click the **OK** button to close the webpage message.
2. Select an ION device.
3. Click on **Help > Online Help** again.

Section 6: Troubleshooting

Message: *The Connection was Reset*



Meaning: The FireFox web browser connection failed to load the page.

Recovery:

1. Verify the URL (e.g., *http://* versus *https://*).
2. Check if the applicable server is running (TFTP, Syslog, HTTPS server) in the expected location.
3. Click the **Try again** button to retry the operation.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *This Connection is Untrusted*

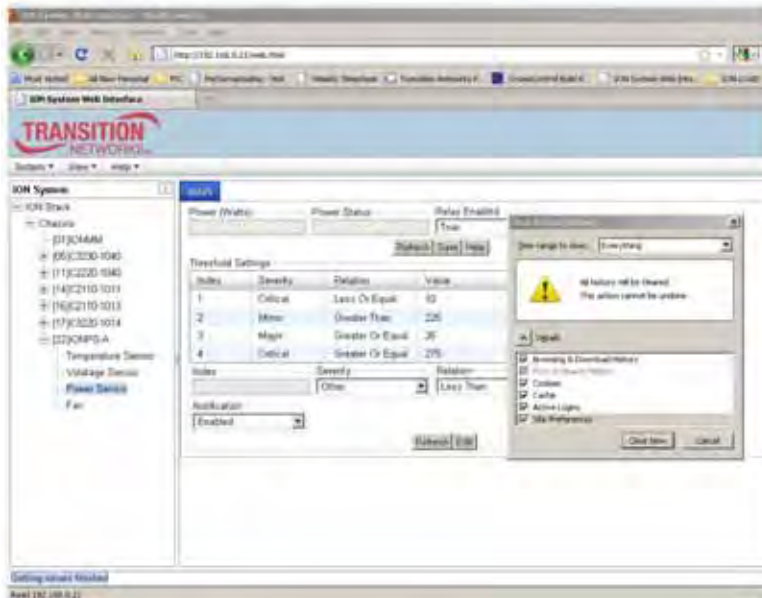


Meaning: You tried to connect via FireFox to a URL, but the FireFox web browser did not find a trusted certificate for that site.

Recovery: 1. Click **Technical Details** for details, or click **I Understand the Risks** to continue operation.

2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Clear Recent History*



Meaning: You tried to display the Power Supply’s temperature, fan, voltage or power sensor sub-menu in the Mozilla Firefox browser.

Recovery:

1. Click **Cancel** / Click **Clear Now** to clear the error dialog.
2. Make sure the latest firmware is running. See “[Upgrade the IONMM and/or NID Firmware](#)” on page 310. Upgrade the firmware version if needed.
3. Expand and contract the ION Stack.
4. Retry the operation.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Static Non Rate Limit entry must have a multiple cast MAC address!*



Meaning: When setting up MAC filtering, you entered a unicast MAC address and selected a Static NRL (Non Rate Limit) Entry Type.

Recovery:

1. Click **OK** to clear the message.
2. Either enter a multicast MAC Address, or select another Entry Type.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Adding MD failed: Maintenance Domain already exists. (snmp operation error)*

Meaning: At the devices' **SOAM > MD** tab you tried to add an MD that was already defined.

Recovery: 1. Press **OK** to clear the message, then enter a unique MD ID number. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Adding MA Net failed: Maintenance Domain already exists. (snmp operation error)*

Meaning: At the devices' **SOAM > MA/MEG > MA Configuration** tab you tried to add an MA ID that was already defined.

Recovery: 1. Press **OK** to clear the message, then enter a unique MD ID number. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: A record with the same MD Index already exists!



Meaning: At the devices' **SOAM > MD** tab you tried to add an MD that was already defined.

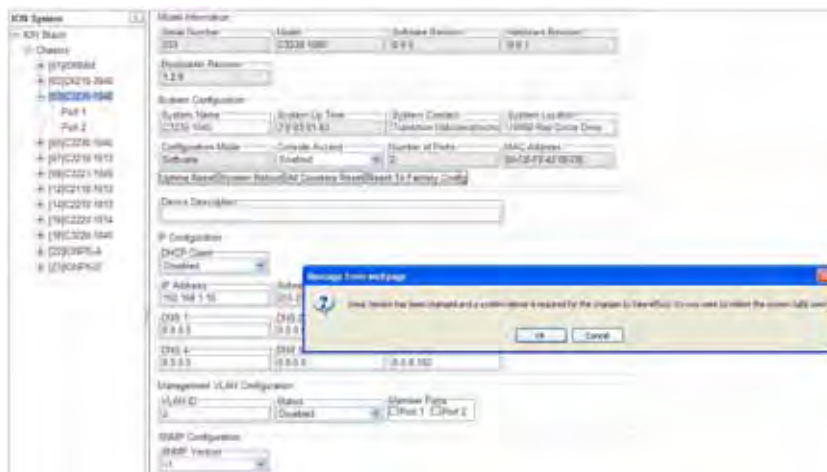
Recovery: 1. Press **OK** to clear the message, and then enter a unique MD ID number. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: xxxxxx is out of range, its range is yyyyyy
 Error symbol period window low is out of range, its range is 125000000 - 268435455!
 Error frame period window is out of range, its range is 174762 - 104857560!
 Error frame period threshold is out of range, its range is 0 - 268435455!
 Error frame window is out of range, its range is 10 - 600!
 Error frame threshold is out of range, its range is 0 - 268435455!
 Error frame seconds summary window is out of range, its range is 100 - 9000!
 Error frame seconds summary threshold is out of range, its range is 0 - 268435455!

Meaning: A parameter entered in the "Event Configuration" has exceeded the range limitation.

Recovery: 1. Enter a parameter within the valid range displayed for the parameter. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: Snmp version has been changed and a system reboot is required for the changes to take effect. Do you want to reboot the system right now?



Meaning: At **Device > MAIN** tab > **SNMP Configuration** section you made a change to the SNMP configuration and then pressed **Save**.

Recovery: 1. Select **OK** to continue with the required reboot, or select **Cancel** to leave the SNMP version unchanged. 2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Local Area Connection x – A network cable is unplugged*

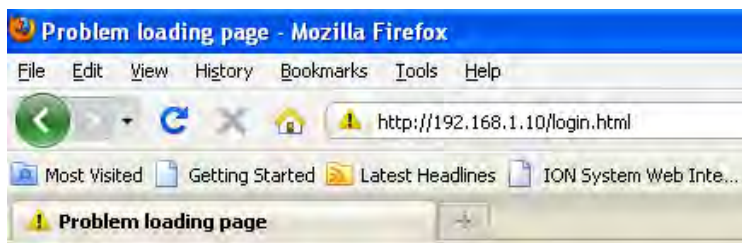


Meaning: You unplugged the USB cable at the NID or IONMM, or the NID or IONMM was unplugged from the ION chassis, or you pressed the **RESET** button on the IONMM.

Recovery:

1. If you pressed the **RESET** button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM's **USB-DEVICE** connector, or plug the USB cable back into the NID's **USB** connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Problem loading page – Mozilla Firefox*

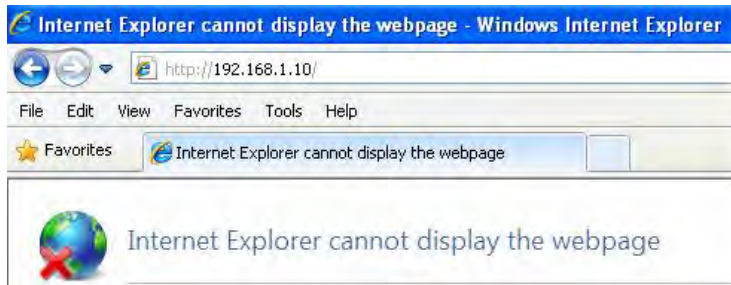


Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See “[Web Browsers Supported](#)” on page 72.
2. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)” on page 59.
3. Verify NID access. See “[Accessing the NIDs](#)” on page 60.
4. Verify the IP address setting. See “[Setting the IP Addressing](#)” on page 89.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Internet Explorer cannot display webpage*

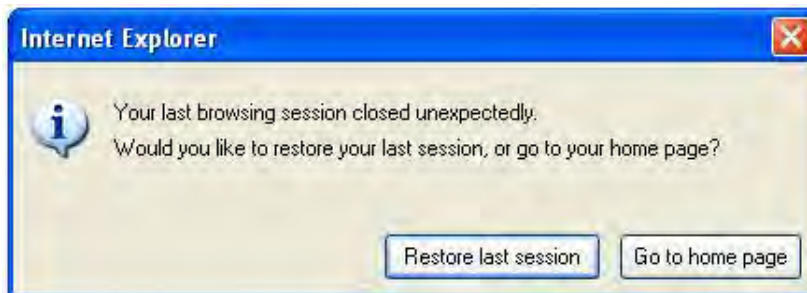


Meaning: You tried to log in to the ION system from IE, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See “[Web Browsers Supported](#)” on page 72.
2. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)” on page 59.
3. Verify NID access. See “[Accessing the NIDs](#)” on page 60.
4. Verify the IP address setting. See “[Setting the IP Addressing](#)” on page 89.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *IE - Your last browsing session closed unexpectedly*



Meaning: The IE web browser crashed.

Recovery: Click the **Restore last session** button. The **Sign in to ION System Web Interface** screen displays. Enter your Password and click the **Sign In** button.

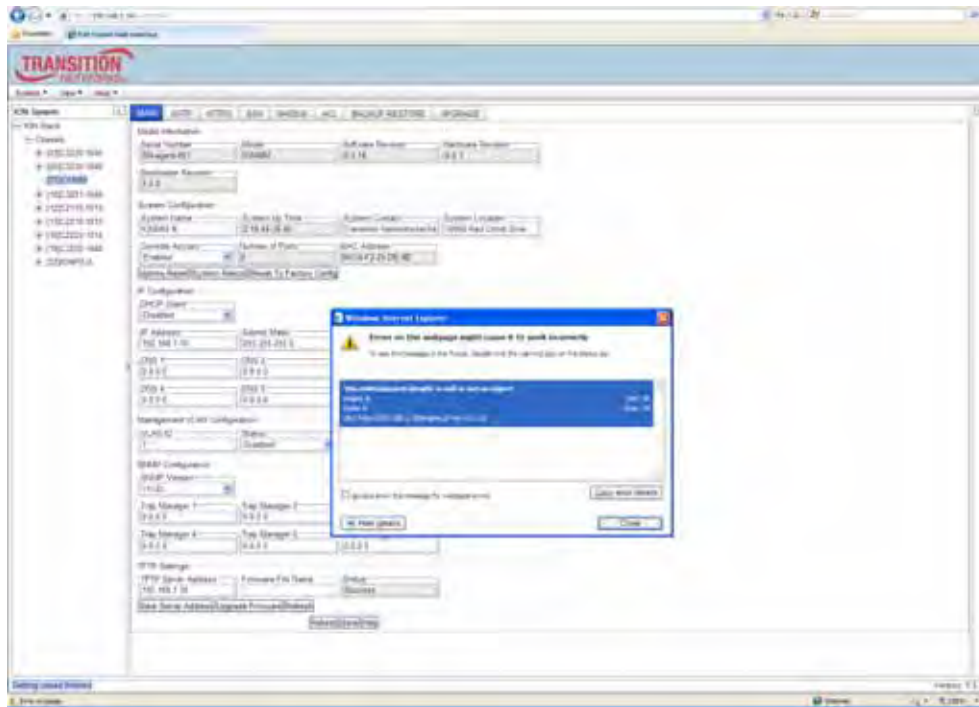
Section 6: Troubleshooting

Message: *Error on page.*

Message: *Errors on this webpage might cause it to work incorrectly.*

Message: *'this.mibValuesList.length' is null or not an object*

Meaning: In Windows IE, the message displays after some amount of inactivity.



Recovery:

1. On the Windows IE error dialog, click the “**Show details button**”.
2. Click the “**Copy error details**” button”.
3. Click the “**Webpage error details**” button. Additional error information is copied (like doing a **Ctl-C** keyboard command)
4. Paste the error details text (use **Ctl-V** command) into a text file in Notepad, Wordpad, MS Word, etc., and then save the newly created file. For example:

```
User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Timestamp: Mon, 6 Dec 2010 14:20:17 UTC
```

```
Message: 'this.mibValuesList.length' is null or not an object
Line: 30
Char: 24
Code: 0
URI: http://192.168.1.10/engine.js?ver=0.5.16
```

5. Click the **Close** button to close the Windows IE error dialog.
6. Click the ION system **Refresh** button.
7. Retry the operation.
8. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *The webpage cannot be found*

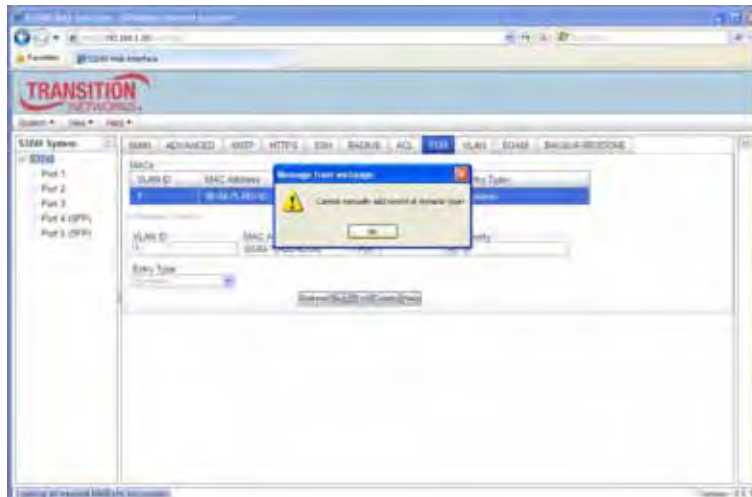
Message: *HTTP 404 Not Found – Windows Internet Explorer*

Meaning: There might be a typing error in the address, or the link you clicked on may be out of date.

Recovery:

1. Retype the address.
2. Go back to the previous page.
3. Make sure the web browser / version you are using is supported. See “[Web Browsers Supported](#)” on page 72.
4. Verify the URL entered. See “[Initial Setup with a Static IP Address via the CLI](#)” on page 59.
5. Verify NID access. See “[Accessing the NIDs](#)” on page 60.
6. Verify the IP address setting. See “[Setting the IP Addressing](#)” on page 89.
7. Verify the URL (e.g., [http://](#) versus [https://](#)).
8. Log in to the x323x again.
9. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Cannot manually add record of the dynamic type!*



Meaning: At the **FDB** tab, you tried to create a MACs table entry with an **Entry Type** of *dynamic*.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Try entering a different MAC address for the MACs table entry.
3. Select another Entry Type (**static**, **staticPA**, or **staticNRL**).
4. Continue with other MACs table entries and press the **Add** button.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

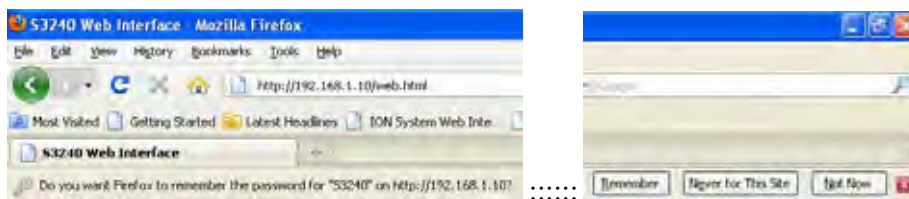
Message: *Transmission rate: value is out of range 1-80*



Meaning: You entered an invalid LBM transmission rate at x323x **SOAM** > **MEP** > **Loopback**.

Recovery: 1. Click **OK** to clear the webpage message. 2. In the **Transmission rate** field, enter the number of loopback messages (LBMs) to be sent per second. The valid range is 1 – 80 LBMs per second. 3. Continue operation; see “[Loopback \(LB\) Config – Web Method](#)” on page 185. 4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

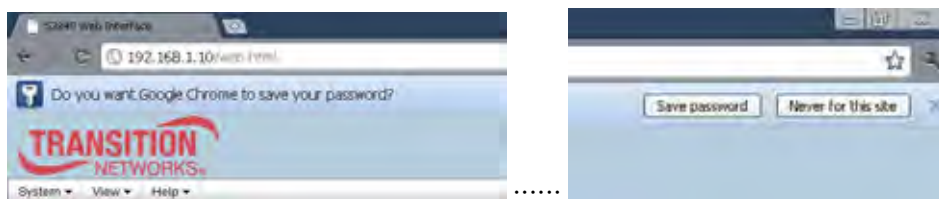
Message: *Do you want Firefox to remember the password for “x323x” on http://192.168.1.10?*



Meaning: The Mozilla Firefox login security option screen.

Recovery: Select one of the three options as desired or according to your organization’s security policy. Select **Remember** to avoid entering the password at the next login, or select **Never for this site** to eliminate this option at future logins, or select **Not Now** to avoid password entry at the next login but keep the option available for future logins.

Message: *Do you want Google Chrome to save your password?*



Meaning: The Google Chrome login security option screen.

Recovery: Select one of the two options as desired or according to your organization’s security policy. Select **Save password** to avoid entering the password at the next login, or select **Never for this site** to eliminate this option at future logins.

SOAM Configuration Error List

The x323x NIDs can display a set of SOAM Configuration errors while making the MIP creation evaluation described in IEEE 802.1ag clause 22.2.3, that the management entity (IONMM) encounters as errors in the configuration. The CFM Configuration Error List table provides a list of Interfaces and VIDs that are incorrectly configured.

While making the MIP creation evaluation described in 802.1ag clause 22.2.3, the management entity can encounter errors in the configuration. The SOAM Configuration errors that can be encountered are:

- CFM leak
- Conflicting VIDs
- Excessive Levels
- Overlapped Levels

The SOAM Configuration Error List can be accessed via the CLI or the Web interface.

SOAM Configuration Error List - CLI Method

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).

2. Enter the **show soam conferror** command. Type:

```
show soam conferror vid=x port=y
```

where:

vid is the VLAN ID

port is the device’s port number (1 or 2 for x3230; 1, 2, or 3 for x3231)

3. Press Enter. The configuration error information displays. For example:

```
C1 | S13 | L0D /> show soam conferror vid=12 port=1  
List: CFMleak
```

See “[SOAM Configuration Error Messages](#)” below for message descriptions and recommended recovery procedures.

SOAM Configuration Error List - Web Method

1. Access the NID through the Web interface (see “[Starting the Web Interface](#)” on page 45).
2. Select **SOAM** tab > **Configuration Error List** sub-tab.



3. Click the **Refresh** button to update the table.

See “[SOAM Configuration Error Messages](#)” below for message descriptions and recommended recovery procedures.

SOAM Configuration Error Messages

The IEEE802.1ag standard lists the possible errors (CFM Leak, Conflicting VIDs, Excessive Levels, and Overlapped Levels). If error free, “*No config errors.*” displays.

These SOAM Configuration errors are discussed below.

Message: *CFM Leak*

Meaning: MAX is associated with a specific VID list, one or more of the VIDs in MAX can pass through the Bridge Port, no Down MEP is configured on any Bridge Port for MAX, and some other MAY, at a higher MD Level than MAX, and associated with at least one of the VID(s) also in MAX, does have a MEP configured on the Bridge Port.

Recovery:

1. Verify the **SOAM** configuration (Main configuration, MD, MA/MEG, MEP and MIP tabs).
2. Make any configuration changes required (see the specific SOAM tab sections in this manual).
3. Click the **Refresh** button on the changed tabs.
4. At the **Configuration Error List** tab, click the **Refresh** button to generate a new Configuration Error List.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Conflicting VIDs*

Meaning: MA_x is associated with a specific VID list, an Up MEP is configured on MA_x on the Bridge Port, and some other MA_y, associated with at least one of the VID(s) also in MA_x, also has an Up MEP configured on some Bridge Port.

Recovery:

1. Verify the **SOAM** configuration (Main configuration, MD, MA/MEG, MEP and MIP tabs).
2. Make any configuration changes required (see the specific SOAM tab section in this manual).
3. Click the **Refresh** button on the changed tabs.
4. At the **Configuration Error List** tab, click the **Refresh** button to generate a new Configuration Error List.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Excessive Levels*

Meaning: The number of different MD Levels at which MIPs are to be created on this port exceeds the Bridge's capabilities. See IEEE 802.1ag clause 22.2.3 for more information.

Recovery:

1. Verify the **SOAM** configuration (Main configuration, MD, MA/MEG, MEP and MIP tabs).
2. Make any configuration changes required (see the specific SOAM tab section in this manual).
3. Click the **Refresh** button on the changed tabs.
4. At the **Configuration Error List** tab, click the **Refresh** button to generate a new Configuration Error List.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Overlapped Levels*

Meaning: A MEP is created for one VID at one MD Level, but a MEP is configured on another VID at that MD Level or higher, exceeding the Bridge's capabilities.

Recovery:

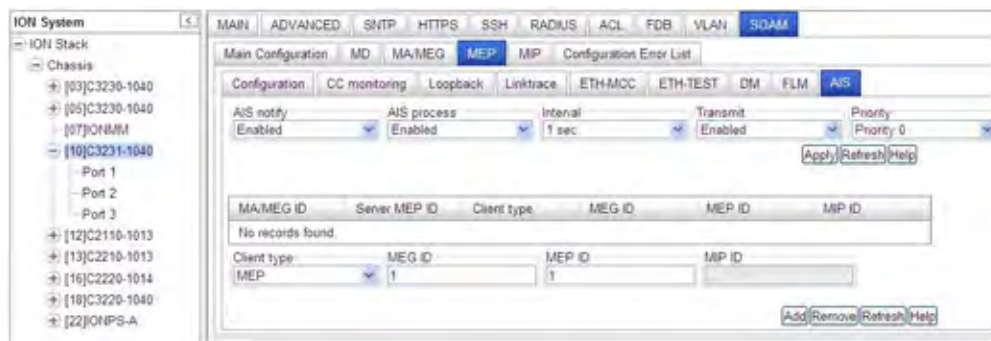
1. Verify the **SOAM** configuration (Main configuration, MD, MA/MEG, MEP and MIP tabs).
2. Make any configuration changes required (see the specific **SOAM** tab section in this manual).
3. Click the **Refresh** button on the changed tabs.
4. At the **Configuration Error List** tab, click the **Refresh** button to generate a new Configuration Error List.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Error at adding MEP AIS client*

Meaning: An error was detected at the **SOAM > MEP > AIS** entry.

Recovery: See “[Ethernet Alarm Indication Signal \(AIS\)](#)” on page 176.



Message: *MEP AIS client deleting failed, error status*

Meaning: You tried to delete a new MEP from the device configuration, but the operation failed.

Recovery: Delete the MA, and then delete the MEP.

Message: *MEP AIS client deleting failed*

Meaning: You tried to delete a new MEP from the device configuration, but the operation failed.

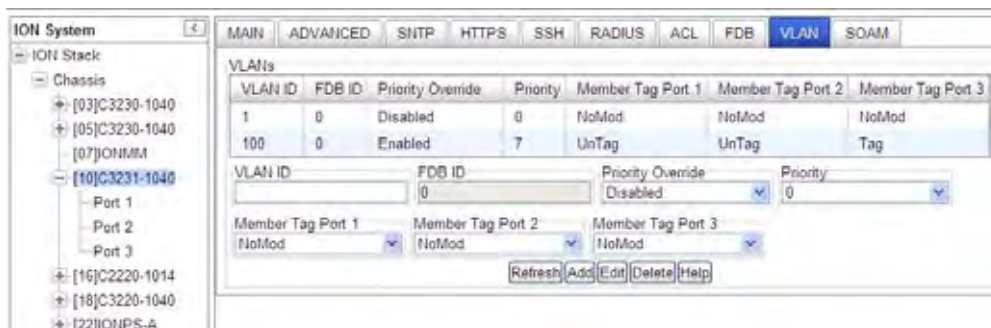
Recovery: Delete the MA, and then delete the MEP.

Message: *Adding VLAN failed (http server error)*

Meaning: You tried to add a new VLAN to the device configuration, but the operation failed.

Recovery:

1. At the device **VLAN** tab, in the **VLAN ID** field, enter a valid VLAN ID (0 is not valid), select the desired **Priority Override** and **Priority**, select **Member Tag Ports 1** and **2** as required (and **Member Tag Port 3** on x3231 models), and click the **Add** button. See “[Configuring VLANs](#)” on page 219.
2. At **SOAM > MA/MEG > MA Configuration > VLAN ID List**, make sure that Primary VLAN ID and the VLAN ID are properly displayed.



7. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *VLAN ID is empty or invalid!*

Meaning: You tried to add a new VLAN to the device configuration, but the operation failed.

Recovery:

1. At the device **VLAN** tab, in the **VLAN ID** field, enter a valid VLAN ID (2 - 4094.), select the desired **Priority Override** and **Priority**, select **Member Tag Ports 1 and 2** required (and **Member Tag Port 3** on x3231 models) as required, and click the **Add** button. See “Configuring VLANs” on page 219.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *MA/MEG with this id has not been configured yet.*

Meaning: You entered the command **show soam mep cc mep-id=** for an undefined MA or MEG. For example, you typed:

```
C1|S3|L1D>show soam mep cc mep-id=320 local-parent-id=11
```

and pressed **Enter**.

Recovery:

1. Verify the SOAM MEP command parameters and re-enter the command.
2. If necessary, define a new MA/MEG.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *MEP with this id not been configured yet.*

Meaning: You entered the command **show soam mep cc mep-id=** for an undefined MEP. For example, you typed:

```
C1|S3|L1D>show soam mep cc mep-id=3 local-parent-id=3
```

and pressed **Enter**.

Recovery:

1. Verify the SOAM MEP command parameters and re-enter the command.
2. If necessary, define a new MEP.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Message: *Send SOAM Unicast Loopback failed.*

Meaning: You entered the command **send soam mep loopback mep-id=** with one or more unrecognized parameters. For example, you typed:

```
C1|S3|L1D>send soam mep loopback mep-id=320 local-parent-id=3 dest=40 amount-frames=1  
and pressed Enter.
```

Recovery:

1. Verify the SOAM MEP command parameters and re-enter the command.
2. Note that only one SOAM MEP test request is supported at a time for a given MEP.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *The multicast loopback request is available only in ITU-T Y.1731 mode.*

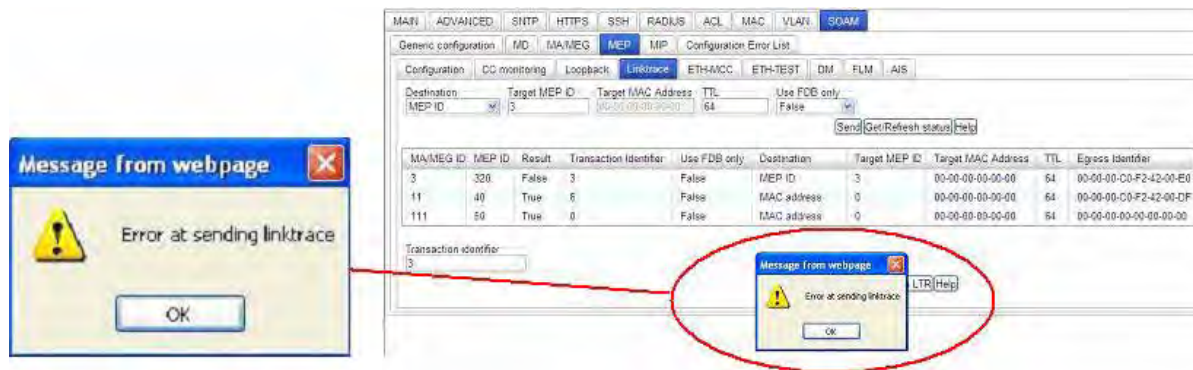
Meaning: You entered the command **send soam mep loopback mep-id=** while in IEEE 802.3 mode. For example, you typed:

```
C1|S3|L1D>send soam mep loopback mep-id=320 local-parent-id=3 dest=multicast amount-frames=1  
and pressed Enter.
```

Recovery:

1. Verify the SOAM MEP command parameters and re-enter the command.
2. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Error at sending linktrace*



Meaning: At **SOAM > MEP > Linktrace** you tried to send a Linktrace to a Target MEP ID on a different MA/MEG (the two MEP ID levels are different).

Recovery:

1. Click **OK** to clear the message.
2. Select a MEP from the MEP Configuration table (at **SOAM > MEP > Configuration**).
3. Select the remaining Linktrace parameters.
4. Click **Send**. See [Linktrace \(LT\) Config – Web Method](#) on page 158.

Message: *Deleting MA Comp failed: MEP ID is absent in the MA MEPs ID list. (snmp operation error)*

Meaning: You tried to delete an MA before deleting its MEP. For example:

1. Created a MD: ID=2
2. Created a MA: ID=2, Parent MD ID=2
3. Created MEP ID list: 2010 and 2020, Parent MA ID=2
4. Created a MEP: ID 2010, Parent MA/MEG=2
5. Then when you try to delete the parent node (which includes children node MA=2), the MA cannot be deleted, and the error message displays.

Recovery: Delete MEP and MEP ID list first, and then delete the related MA.

Section 6: Troubleshooting

Message: Please delete MEP and MEP ID list first

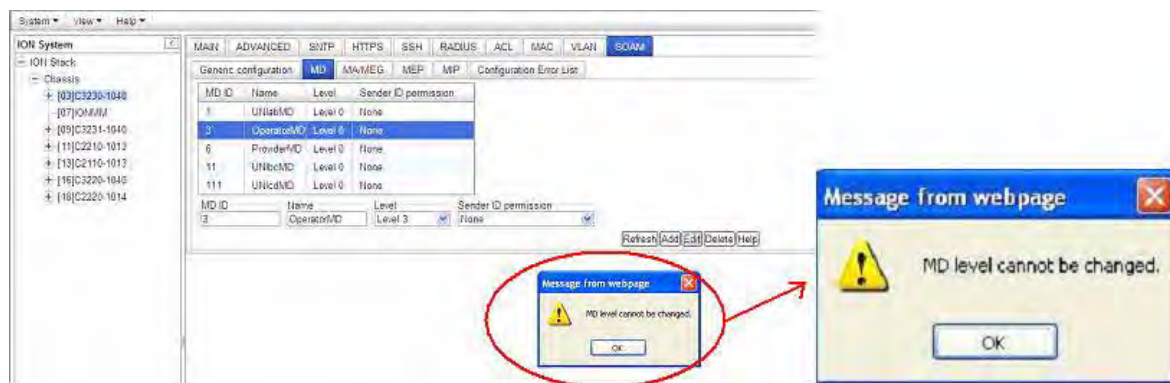
Meaning:

You tried to delete an MA before deleting its MEP. For example:

1. Created a MD: ID=2
2. Created a MA: ID=2, Parent MD ID=2
3. Created MEP ID list: 2010 and 2020, Parent MA ID=2
4. Created a MEP: ID 2010, Parent MA/MEG=2
5. Then when you try to delete the parent node (which includes children node MA=2), the MA cannot be deleted, and the error message displays.

Recovery: Delete MEP and MEP ID list first, and then delete the related MA.

Message: MD level cannot be changed.



Meaning: At **SOAM > MEP** you tried to edit an existing MD after it was saved.

Recovery: Delete the MD and re-define it. See “[Configuring SOAM MD/MA](#)” on page 111.

Message: Adding MEP failed: MEP ID is absent in the MA MEPs ID list. (snmp operation error)

Meaning: At the device’s **SOAM > MEP > Configuration** sub-tab, you tried to add a MEP before adding its Parent MA/MEG.

Recovery: Create a parent MEG, and then create the child MEP.

Message: Adding MEP failed: Operation rejected due to the existence of a MEP in the same direction, level, VIDs (no VID), port. (snmp operation error)

Meaning: At the device’s **SOAM > MEP > Configuration** sub-tab, you tried to create a MEP with the same MEP characteristics.

Recovery: Create a MEP with different MEP characteristics and continue operation.

Message: Adding MEP failed: VLAN ID doesn't exist in anchor VLAN list. (snmp operation error)

Meaning: You tried to add a MEP within a related VLAN without first creating the VLAN.

Recovery: Create a VLAN in the VLAN List, and then add the associated MEP.

Message: Adding MIP failed: Operation rejected due to the existence of a MEP in the same direction, level, VIDs (no VID), port. (snmp operation error)

Meaning: At the device's **SOAM > MIP** sub-tab, you tried to create a MIP with the same MIP characteristics.

Recovery: Create a MIP with different MIP characteristics and continue operation.

Message: Adding MIP failed: LBM discarded - dest MAC address not equal to MAC addr of MIP or dest group MAC addr not equal to MP MD/MEG Level. (snmp operation error)

Meaning: At the device's **SOAM > MIP** sub-tab, you created two 802.1ag MEPs with status of OK, then added a MIP between these two MEPs, and checked the result, but the "Adding MIP failed.." message displays.

Recovery: 1. Click the **Refresh** button, verify that the MIP has been added, and continue operation.
2. A MIP with the type 802.1ag can not be configured with AIS (AIS is disabled when the type is 802.1ag). Configure the MIP as a type y.1731 MIP. See "Configuring a SOAM MIP" on page 155.

AIS can only be configured if the MIP is set up for Y.1731. See "SOAM (Service OAM) Configuration" on page 131.

Message: Deleting MA Comp failed: MEG with such a name already exists. (snmp operation error)

Meaning: You tried to delete an MA before deleting its child MEG(s).

When you try to delete the parent node (which includes children node MA=2), the MA cannot be deleted, and the error message displays.

Recovery: Delete MEG and MEP ID list first, and then delete the related MA.

Message: Deleting MD failed: Operation rejected due to the existence of a MEP in the same direction, level, VIDs (no VID), port. (snmp operation error)

Meaning: You tried to delete an MD before deleting its MEP.

Recovery: Create a similar related MEP if desired. Delete the MEP, and then delete the MD.

Message: Deleting MIP failed - MEP ID is absent in the MA MEPs ID list. (snmp operation error)

Meaning: You tried to delete a MIP but the MEP does not exist in the MA MEP's table.

Section 6: Troubleshooting

Recovery: 1. Verify that the local-mep-id you entered is the one you want. 2. Create a unique MEP (see “Add a MEP” on page 130). 3. Retry the operation with the unique MEP (or MIP).

Message:

Error at sending loopback: Remote MEP CCM db entry is not initialized. (snmp operation error)
 Error at sending MCC: Remote MEP CCM db entry is not initialized. (snmp operation error)
 Error at sending ETH test: Remote MEP CCM db entry is not initialized. (snmp operation error)
 Error at sending MEP DM: Remote MEP CCM db entry is not initialized. (snmp operation error)
 Apply MEP FLM failed: Remote MEP CCM db entry is not initialized. (snmp operation error)

Meaning: An attempted SOAM MEP test failed.

Recovery:

1. Verify the SOAM MEP test parameters and re-enter the command.
2. Refer to “Service OAM (SOAM) Configuration” on page 109.
3. Retry the specific test (loopback, MCC, DM, etc.). Refer to the appropriate section of this manual.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *The SOAM Port table is empty.
 The SOAM Port ID table is empty.
 The MDs table is empty.
 The MAs table is empty.
 Add a new maintenance entity group to the SOAM engine.
 Primary VLAN ID is incorrect.
 The primary parameter should be a number.
 The MEGs table is empty.
 The MEPs table is empty.
 Set SOAM FLM Far end MEP ID*

Meaning: The attempted SOAM configuration entry was incorrect or incomplete.

Recovery:

1. Verify the SOAM parameters and re-enter the command.
2. Refer to “Service OAM (SOAM) Configuration” on page 109.
3. Retry the specific function (MA entry, MEG entry, test, etc.). Refer to the appropriate section of this manual.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: Data is empty.

Meaning: The SOAM ETH-MCC data can not be empty.

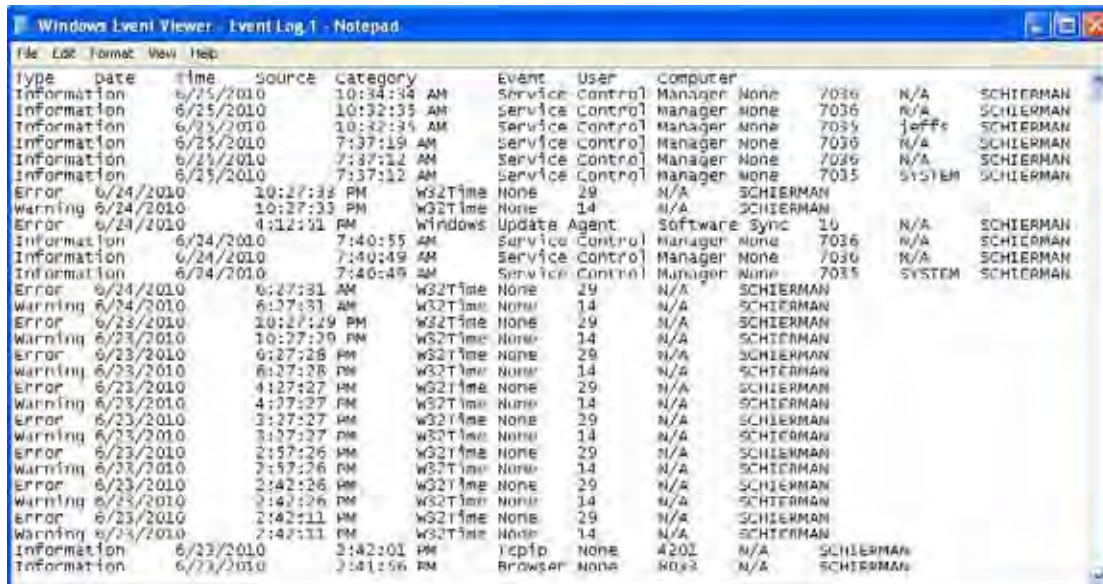
1. Verify the SOAM ETH-MCC test parameters and re-enter the command.
2. Refer to “[ETH-MCC \(Ethernet Maintenance Communication Channel\)](#)” on page 180.
3. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Section 6: Troubleshooting

Windows Event Viewer Messages

A sample Event Log file is shown below.

Windows Event Viewer - Event Log 1:



Type	Date	Time	Source	Category	Event	User	Computer				
Information	6/25/2010	10:34:34 AM	Service Control Manager	None	7036	N/A	SCHIERMAN				
Information	6/25/2010	10:32:35 AM	Service Control Manager	None	7036	N/A	SCHIERMAN				
Information	6/25/2010	10:32:35 AM	Service Control Manager	None	7036	jeffs	SCHIERMAN				
Information	6/25/2010	7:37:19 AM	Service Control Manager	None	7036	N/A	SCHIERMAN				
Information	6/25/2010	7:37:12 AM	Service Control Manager	None	7036	N/A	SCHIERMAN				
Information	6/25/2010	7:37:12 AM	Service Control Manager	None	7035	SYSTEM	SCHIERMAN				
Error	6/24/2010	10:27:33 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/24/2010	10:27:33 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/24/2010	4:12:51 PM	Windows Update Agent	Software Sync	16	N/A	SCHIERMAN				
Information	6/24/2010	7:40:55 AM	Service Control Manager	None	7036	N/A	SCHIERMAN				
Information	6/24/2010	7:40:49 AM	Service Control Manager	None	7036	N/A	SCHIERMAN				
Information	6/24/2010	7:40:45 AM	Service Control Manager	None	7035	SYSTEM	SCHIERMAN				
Error	6/24/2010	6:27:31 AM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/24/2010	6:27:31 AM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	10:27:29 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	10:27:29 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	6:27:28 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	6:27:28 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	4:27:27 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	4:27:27 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	3:27:27 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	3:27:27 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	2:57:26 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	2:57:26 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	2:42:26 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	2:42:26 PM	W32Time	None	14	N/A	SCHIERMAN				
Error	6/23/2010	2:42:11 PM	W32Time	None	29	N/A	SCHIERMAN				
Warning	6/23/2010	2:42:11 PM	W32Time	None	14	N/A	SCHIERMAN				
Information	6/23/2010	3:42:01 PM	tcpip	None	4201	N/A	SCHIERMAN				
Information	6/23/2010	3:41:56 PM	Browser	None	8032	N/A	SCHIERMAN				

Message: Information 6/25/2010 7:37:12 AM Service Control Manager None 7035 SYSTEM

Meaning: Information message regarding SCM.

Recovery: No action required.

Message: Error 6/24/2010 10:27:33 PM W32Time None 29 N/A SYSTEM

Meaning: Error level message regarding W32Time.

Recovery: Open the file, examine the number of messages like this, and the potential problem level.

Message: Warning 6/24/2010 10:27:33 PM W32Time None 14 N/A SYSTEM

Meaning: Warning level message regarding W32Time.

Recovery: Check the other system logs for related messages. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

ION System Tests

This section describes the x323x system level tests, DMI functions, and related test functions.

Virtual Cable Test (VCT)

The VCT feature uses TDR (Time Domain Reflectometry) to determine the quality of cables, connectors, and terminations. Problems that can be determined include opens, shorts, cable impedance mismatches, failed connectors, and termination mismatches.

The VCT runs the cable diagnostic by transmitting a signal of known amplitude sequentially along each of the TX and RX pairs of an attached cable. The transmitted signal continues along the cable until it is reflected from a cable imperfection, and that distance is displayed. If the test status returned is Normal, the distance displayed is the actual cable length. The VCT test is intrusive, as the tested port's link is brought down during the test.

When the VCT is activated, a pre-defined amount of time elapses before a VCT test pulse is transmitted. This ensures that the link partner loses link, so that it stops sending 100BASE-TX idles or 10 Mbps data packets. The VCT can be performed either when there is no link partner, or when the link partner is Auto-Negotiating or sending 10 Mbps idle link pulses.

Use the VCT test to determine if cabling is at fault when you cannot establish a link. Problems can include opens, shorts, cable impedance mismatches, failed connectors, and termination mismatches, bad magnetics.

Note: Do not change the port configuration while the TDR test is running.

Due to cable characteristics, run the TDR test several times to get accurate results.

Do not change port status (e.g., remove the cable at the near or far end) as the results may be inaccurate.

The VCT test can be configured via the CLI method or the Web method.

VCT Test – CLI Method

Use the VCT test to determine if cabling is at fault when you cannot establish a link for an x323x copper port.

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Start the VCT Test from the command line. Type **start ether tdr test** and press **Enter**. The Time Domain Reflector (TDR) test starts on the specified Ethernet copper port.
3. Show the Ethernet port TDR Test configuration. Type **show ether tdr config** and press **Enter**. The Time Domain Reflectometry (TDR) test configuration displays for the Ethernet copper port. For example:

```
C1|S16|L1P1>show ether tdr config
Time-domain reflectometer configuration:
-----
TDR test state:                success
TDR test init time:           22:39:18
TDR test result valid:        true
C1|S16|L1P1>
```

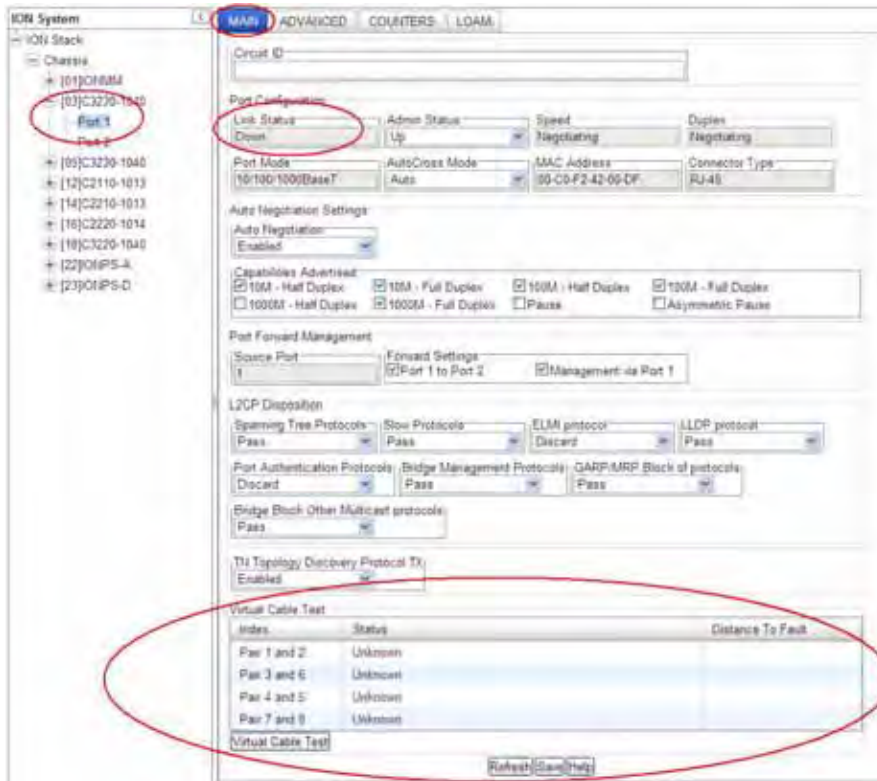
4. Show the Ethernet port TDR Test results. Type **show ether tdr test result** and press **Enter**. The results of an Ethernet port TDR test display for the copper port. For example:

```
C1|S5|L1P1>show ether tdr test result
Cable pair :
index          distance to fault(unit)    status
-----
pair1and2      0(meter)                  open
pair3and6      0(meter)                  open
pair4and5      0(meter)                  open
pair7and8      1(meter)                  open
C1|S5|L1P1>
```


5. Run the TDR test several times to ensure accurate results. Do not change port status (e.g., remove the cable at the near end or far end) as this may cause inaccurate results.

VCT Test – Web Method

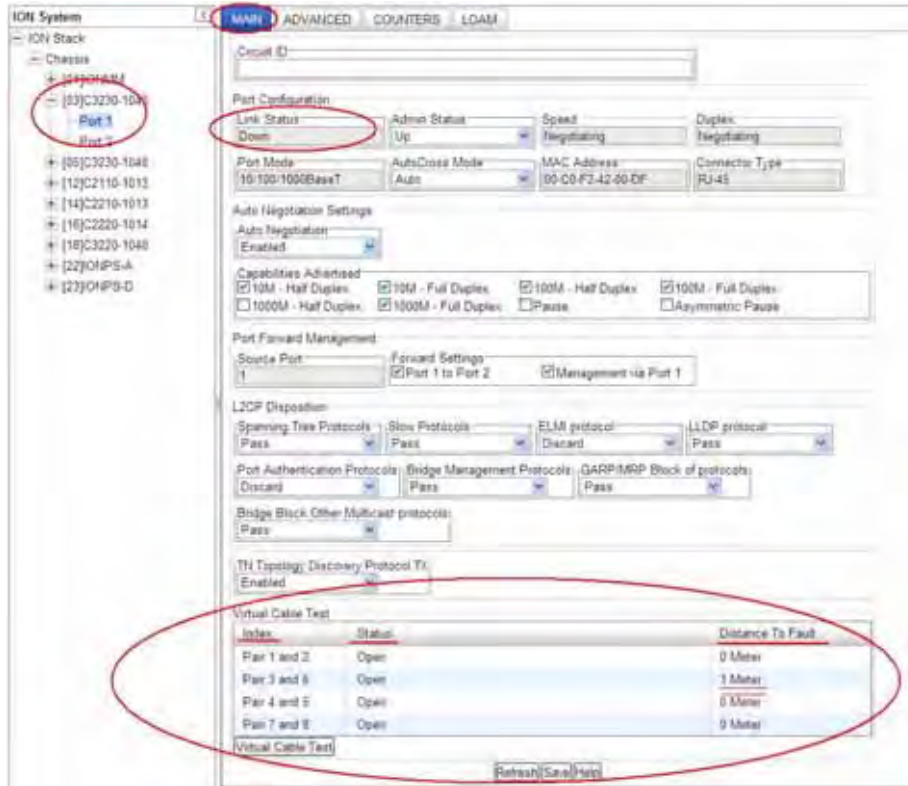
1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired port.
3. At the port-level **MAIN** tab, check the information displayed in the **Link Status** and **Virtual Cable Test** areas.



4. Click the **Virtual Cable Test** button.

The VCT test runs, the  message displays momentarily, and then test information displays.

Section 6: Troubleshooting



5. Check the information displayed in the **Link Status** (*Up or Down*) and **Virtual Cable Test** sections.

Virtual Cable Test		
Index	Status	Distance To Fault
Pair 1 and 2	Open	0 Meter
Pair 3 and 6	Open	1 Meter
Pair 4 and 5	Open	0 Meter
Pair 7 and 8	Open	0 Meter

Virtual Cable Test

Refresh Save Help

The possible VCT Test parameter values and states are described in the table below.

Parameter	Fault State	Meaning
Link Status Down		VCT Test failed due to lost link.
Link Status Up		VCT Test passed; link is up. No action needed.
Index - Pair x and y		There are four pairs of standard category 5 cable. Each pair (e.g., Pair 1 and 2) displays one of these states: Open, Broken, Shorted, Terminated, Impedance Mismatch, or Unknown.
Status – Normal		The pair is properly terminated at the remote end (not a fault state). The 'Distance To Fault' is blank.

Parameter	Fault State	Meaning
Status – Open	X	Open (not connected) connection failure status. Cable impedance is <u>greater</u> than 333 ohms.
Status – Broken	X	Broken connection failure status.
Status – Shorted	X	Shorted connection failure status. Cable impedance is <u>less</u> than 333 ohms.
Status – Terminated		Connection terminated status (non-fault state).
Status – Impedance Mismatch	X	The impedance of the pair is mismatched.
Status – Unknown	X	None of the above (i.e., not Normal, Open, Shorted, Terminated, Impedance Mismatch, or Unknown).
Distance To Fault - 0 Meter		The overall distance to the fault in Meters (Open or no fault found).
Distance To Fault > 0 Meter		The overall distance to the fault in Meters.

DMI (Diagnostic Maintenance Interface) Parameters

The DMI (Diagnostic Maintenance Interface) function displays NID diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. **Note:** only certain NID models support DMI. Transition Networks NIDs that support DMI have a “D” at the end of the model number.

Note: If the message “ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.” displays, follow your organization’s policy and procedure for intrusion detection.

DMI can be configured in the NID using either the CLI or Web method.

DMI Config – CLI Method

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. Set the Diagnostic Monitoring Interface receive preset power level for a fiber port. Type:

```
set dmi rx-power-preset-level=xx
```

where:

xx is a preset level for Rx Power on the Fiber port, in the range of 1 to 10.

3. Press **Enter**. For example: **set dmi preset-power-level=10**.

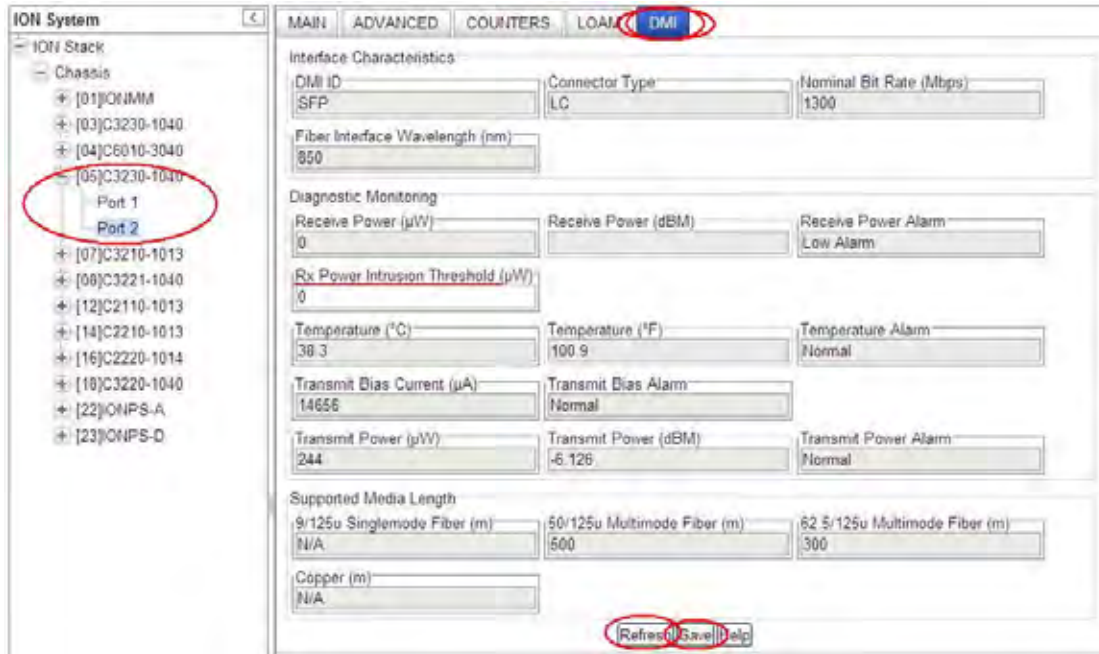
4. Display the DMI information. Type: **show dmi info** and press **Enter**. For example:

```
C1|S5|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:                   37.7*C
DMI temperature:                   99.9*F
DMI temperature alarm:             normal
DMI transmit bias current:         14672*uA
DMI transmit bais alarm:          normal
DMI Transmit power:                241*uW
DMI Transmit power:                -6.180*dBM
DMI Transmit power alarm:         normal
DMI Receive power:                 0*uW
DMI Receive power alarm:          lowAlarm
DMI Receive power intrusion threshold: 0*uW
C1|S5|L1P2>
```

The DMI tab parameters are described in Table 22 later in this section.

DMI Config – Web Method

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the desired device and port.
3. Select the **DMI** tab.



The Interface Characteristics, Diagnostic Monitoring, and Supported Media Length information sections display. See the table below for individual field / parameter descriptions.

4. Change the “**Rx Power Intrusion Threshold**” setting as desired. The default is 0 uW. The valid range is 0 - 65,535 uW (microwatts).
5. You can click the **Refresh** button to update the information displayed.
6. Click the **Save** button to save the updated information.

Section 6: Troubleshooting

The **DMI** tab parameters are described in the table below.

Table 34: DMI Parameters

Parameter	Possible Parameters	Description
DMI ID	Unknown, GBIC, soldered to motherboard, SFP, Reserved, vendor-specific	Specifies the physical device from SFF-8472 Rev 9.5 Standard: 00h Unknown or unspecified 01h GBIC 02h Module/connector soldered to motherboard 03h SFP 04-7Fh Reserved 80-FFh Vendor specific
Connector Type	LC, MT-RJ LC, SC, ST, RJ-45, or VF-45, or unknown	The external optical or electrical cable connector provided as the interface. * MT-RJ: Media Termination - Recommended Jack for Duplex multimode connections. * LC: Lucent Connector or Local Connector for High-density connections, SFP transceivers. * SC: Subscriber Connector for Datacomm and Telecomm. * ST: BFOC Straight Tip / Bayonet Fiber Optic Connector for Multimode - rarely Singlemode (APC not possible). * VF-45: Snap connector for Datacom uses. See " Connector Types " section below.
Nominal Bit Rate (Mbps)	(measured rate)	Transmission rate in units of Mbps (the sample screen above shows 1300, or 1.3 Gbps).
Fiber Interface Wavelength (nm)	(measured wavelength)	The Nominal transmitter output wavelength at room temperature. The unit of measure is nanometers (the sample screen above shows 850 nm).
Receive Power (uW)	(measured power measurement)	Receive power on local fiber measured in microwatts (the sample screen above shows 240 uW). If the link is down, the "DMI Rx power" reports the last measured value.
Receive Power (dBm)	(measured signal strength)	Receive power on local fiber measured in dBm (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -6.198 dBm. If the link is down, the "DMI Rx power" reports the last measured value.
Receive Power Alarm	Normal - 1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for receive power on local fiber (alarm first, warning second).
Rx Power Intrusion Threshold (uW)	0-10	A preset level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated.
Temperature (°C)	(measured temp.)	Temperature of fiber transceiver in tenths of degrees C (Celsius). The sample screen above shows 46.1°C.
Temperature (°F)	(measured temp.)	Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). The sample screen above shows 115.2°F.

Temperature Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for temperature of fiber transceiver. An <i>ionDMITemperatureEvt</i> event is sent when there is a warning or alarm on DMI temperature (alarm first, warning second).
Transmit Bias Current (uA)	(measured current)	Transmit bias current on local fiber interface, in uA (microamperes). The sample screen above shows 15440 uA (microamps).
Transmit Bias Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for transmit bias current on local fiber interface (alarm first, warning second).
Transmit Power (uW)	(measured power)	Transmit power on local fiber measured in microwatts. The sample screen above shows 244 uW (microwatts).
Transmit Power (dBm)	(measured power)	Transmit power on local fiber measured in dBm (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -6.126 dBm.
Transmit Power Alarm	Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7	Alarm status for transmit power on local fiber (alarm first, warning second).
Supported Media Length	9/125u Singlemode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). The sample screen above shows N/A, indicating the media is not applicable.
Supported Media Length	50/125u Multimode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 500 meters as the supported media length.
Supported Media Length	62.5/125u MM Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 300 meters as the supported media length.
Supported Media Length	Copper (m)	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters. The sample screen above shows N/A, indicating the media is not applicable.

Connector Types

The DMI **Connector Type** field indicates the external optical or electrical cable connector provided as the interface. The information below is from SFF 8472 Rev 9.5.

Value	Description of connector
00h	Unknown or unspecified
01h	SC
02h	Fibre Channel Style 1 copper connector
03h	Fibre Channel Style 2 copper connector
04h	BNC/TNC
05h	Fibre Channel coaxial headers
06h	FiberJack
07h	LC
08h	MT-RJ
09h	MU
0Ah	SG
0Bh	Optical pigtail
0C-1Fh	Reserved
20h	HSSDC II
21h	Copper Pigtail
22h-7Fh	Reserved
80-FFh	Vendor specific

The LC, MT-RJ LC, SC, ST, or VF-45 connector types (jacks) are shown below.



ST



SC



LC



MT-RJ



VF-45

Set Debug Level

You can use the CLI method to define the system debug level.

1. Access the NID through either a USB connection (see “[Starting a USB Session](#)” on page 41) or a Telnet session (see “[Starting a Telnet Session](#)” on page 43).
2. Set the desired debug level. Type:

```
set dbg level=<0-2>
```

where:

0=debug Severity level 0 (Emergency: system is unusable - e.g., serious hardware failure or imminent power failure).

1=debug Severity level 1 (Alert: action must be taken immediately).

2=debug Severity level 2 (Critical condition).

3. Press **Enter**. For example:

```
C1|S3|L1D>set dbg level 0
C1|S3|L1D>set dbg level 1
C1|S3|L1D>set dbg level 2
C1|S3|L1D>set dbg level 3
% Parameter value is out of range.
C1|S3|L1D>
```

Show Ethernet Statistics Counter Descriptions

In a situation where performance, particularly rate or error counts, is suspect, you can use the **show ether statistics** command to display Ether-like counters and If-MIB counters for a copper or fiber port.

These counters are described below.

Total Octets: The total number of octets transmitted out of the interface, including framing characters. (Displayed for “Port Counters Received” and “Port Counters Sent”.)

Unicast Packets: The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. (Displayed for “Port Counters Received” and “Port Counters Sent”.)

Broadcast Packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.

Multicast Packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. (Displayed for “Port Counters Received” and “Port Counters Sent”.)

Rx Discards: The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. (Displayed for “Port Counters Received” and “Port Counters Sent”.)

Rx Errors: For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. (Displayed for “Port Counters Received” and “Port Counters Sent”.)

Alignment Errors: A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.

FCS Errors: A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.

SQE Test Errors: A count of times that the SQE TEST ERROR is received on a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6. This counter does not increment on interfaces operating at speeds greater than 10 Mb/s, or on interfaces operating in full-duplex mode.

Deferred Frames: A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. This counter does not increment when the interface is operating in full-duplex mode.

Internal MAC Tx Errors: A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the *dot3StatsLateCollisions* object, the *dot3StatsExcessiveCollisions* object, or the *dot3StatsCarrierSenseErrors* object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Internal MAC Rx Errors: A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the *dot3StatsFrameTooLongs* object, the *dot3StatsAlignmentErrors* object, or the *dot3StatsFCSErrors* object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.

Carrier Sense Errors: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. This counter does not increment when the interface is operating in full-duplex mode.

Symbol Errors: For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the

receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. This counter does not increment when the interface is operating at 10 Mb/s.

Single Collisions: A count of frames that are involved in a single collision, and are subsequently transmitted successfully. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the 'Unicast Packets', 'Multicast Packets', or 'Broadcast Packets' (Port Counters Sent), and is not counted by the corresponding instance of the 'Multiple Collisions' object. This counter does not increment when the interface is operating in full-duplex mode.

Multiple Collisions: A count of frames that are involved in more than one collision and are subsequently transmitted successfully. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the *ifOutUcastPkts*, *ifOutMulticastPkts*, or *ifOutBroadcastPkts*, and is not counted by the corresponding instance of the 'Single Collisions' object. This counter does not increment when the interface is operating in full-duplex mode.

Late Collisions: The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. This counter does not increment when the interface is operating in full-duplex mode.

Excessive Collisions: A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.

Oversized Frames: A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the *frameTooLong* status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Duplex Status: The current mode of operation of the MAC entity. 'Unknown' indicates that the current duplex mode could not be determined.

Rate Control Ability: 'True' for interfaces operating at speeds above 1000 Mb/s that support Rate Control through lowering the average data rate of the MAC sublayer, with frame granularity, and 'False' otherwise.

Rate Control Status: The current Rate Control mode of operation of the MAC sublayer of this interface (Rate Control either *on* or *off*).

Rx Unknown Opcodes: A count of MAC Control frames received on this interface that contain an opcode that is not supported by this device.

Rx Pause Frames: A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Tx Pause Frames: A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Jumper Settings

The x323x NID has on-board components that can be used to configure device operation, typically at the direction of a TN technical support specialist. In most cases, the factory default settings provide optimal configuration settings; however, jumper setting changes may be required for operating mode changes or troubleshooting purposes.

PCB Identification

This section covers the following PCBs (printed circuit boards):

5. **C3230** NID - PCB: 11320a Rev. A (this information is silkscreened on the top right corner of the PCB).
6. **C3231** NID - PCB: 11320b Rev. A (this information is silkscreened on the top right corner of the PCB).

Note: Do not change the configurable items except at the direction of a TN technical support specialist.

C3230 NID

PCB: 11320a Rev. A (information is silkscreened on the top right corner of the PCB).



J11 (Reset Unit to Factory Defaults)

J11 is a 3-position jumper that can be used to force a factory reset of all configuration values.



Doing a **Reset To Factory Config** resets the NID configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the system configuration with the factory default settings. See “[Reset To Factory Config](#)” on page 80 for more information.



Jumper

Pin #s

1-2 (N)

2-3 (F)

Function

Normal operation (default setting).

Reset device to **F**actory Defaults.

J8 / J9 /J12 (Not Used)

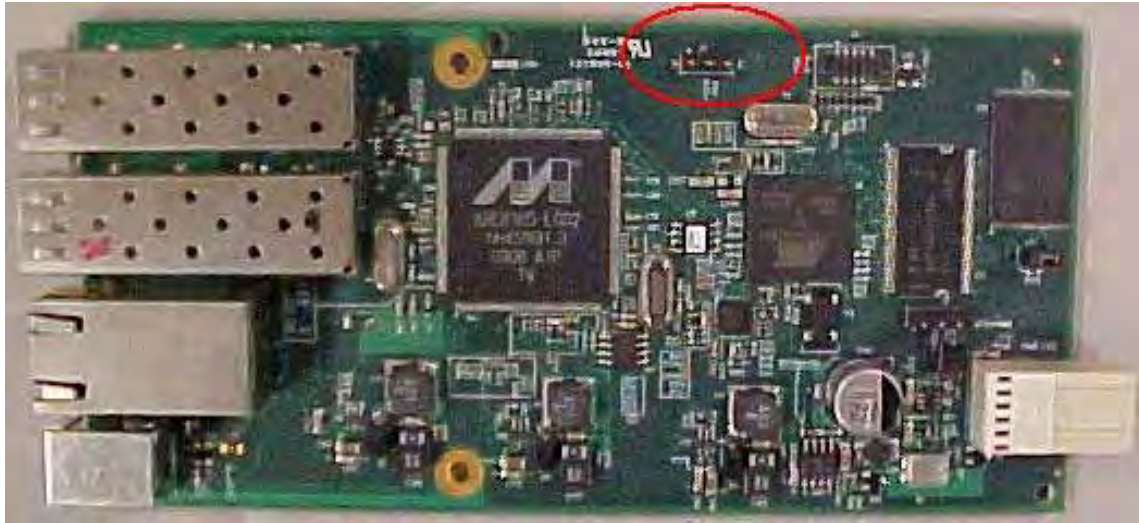
Do not use. Jumpers J8, J9 and J12 are used for manufacturing / debug purposes only.

Section 6: Troubleshooting

C3231 NID

PCB: 11320b Rev. A (this information is silkscreened on the top left corner on the back of the PCB).

PCB: 11320 Rev. 05 (this information is silkscreened on the top left corner on the back of the PCB).



D13 (Yellow Diode / LED)

When lit, indicates that the processor has a link with the main switch.

J11 (Reset Unit to Factory Defaults)

J11 is a 3-position jumper that can be used to force a factory reset of all configuration values.



Doing a **Reset To Factory Config** resets the NID configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the system configuration with the factory default settings. See “[Reset To Factory Config](#)” on page 80 for more information.



Jumper

Pin #s

1-2 (N)

2-3 (F)

Function

Normal operation (default setting).

Reset device to **F**actory Defaults.

J8 / J9 / J12 (Not Used)

Do not use. Jumpers J8, J9 and J12 are used for manufacturing / debug purposes only.

Third Party Troubleshooting Tools

This section provides information on third party troubleshooting tools for Windows, Linux, etc. Note that this section may provide links to third party web sites. Transition Networks is not responsible for any third party web site content or application. These web sites' information was accurate at the time of publication, but may have changed in the interim.

- Ipconfig and ifconfig
- Windows Network Connections
- Ping
- Telnet
- PuTTY
- Tracert (Traceroute)
- Netstat
- Winipcfg
- Nslookup
- Dr. Watson
- SNMPc
- HPOV (HP OpenView)
- US-CERT

Note: IETF RFC 2151 is a good source for information on Internet and TCP/IP tools at <ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt>.

Ipconfig

Ipconfig (Windows Vista): Use the procedure below to find your IP address, MAC (hardware) address, DHCP server, DNS server and other useful information under Windows Vista.

1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway display. If your IP address is 192.168.x.x, 10.x.x.x, or 172.16.x.x, then you are receiving an internal IP address from a router or other device.
4. For more detailed information, type **ipconfig /all** at the prompt. Here you can get the same information as **ipconfig** plus your MAC (hardware) address, DNS and DHCP server addresses, IP lease information, etc.

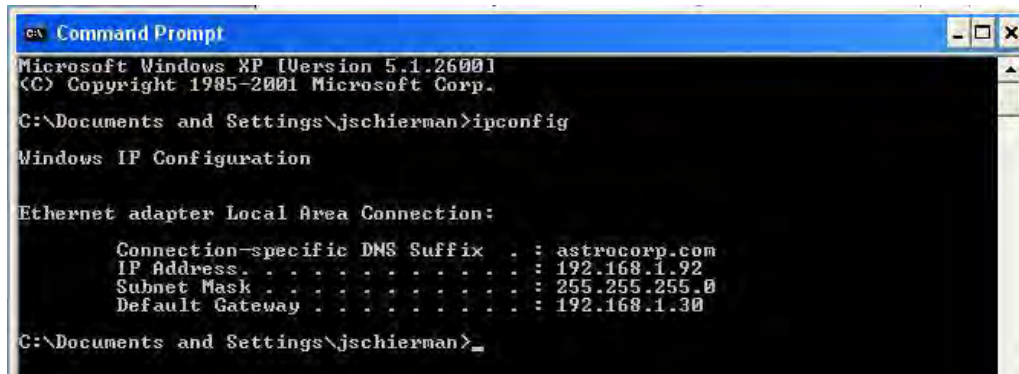
Note: If you are receiving a 169.254.x.x address, this is a Windows address that generally means your network connection is not working properly.

Section 6: Troubleshooting

Ipconfig (Windows XP): ipconfig (Internet Protocol Configuration) in Windows is a console application that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.

Use the **ipconfig** command to quickly obtain the TCP/IP configuration of a computer.

1. Open a Command Prompt. Click Start, point to Programs, point to Accessories, and then click Command Prompt.
2. Type **ipconfig** and press Enter. The Windows IP Configuration displays:



```

C:\Documents and Settings\jschierman>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : astrocorp.com
    IP Address . . . . . : 192.168.1.92
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.30

C:\Documents and Settings\jschierman>

```

3. Make sure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
4. For more information, use the /all parameter (type **ipconfig /all** and press **Enter**).

The **ipconfig** command is the command-line equivalent to the **winipcfg** command, which is available in Windows ME, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the **winipcfg** command; however, you can get the equivalent functionality for viewing and renewing an IP address using Windows' Network Connections (see below).

ifconfig

1. Verify that the machine's interfaces are up and have an IP address using the **ifconfig** command:

```
[root@sleipnir root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:6E:0A:3D:26
          inet addr:192.168.168.11  Bcast:192.168.168.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13647 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12020 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:7513605 (7.1 Mb)  TX bytes:1535512 (1.4 Mb)
          Interrupt:10

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:892258 (871.3 Kb)  TX bytes:892258 (871.3 Kb)
```

The above machine is running normally. The first line of output shows that the Ethernet interface eth0 has a layer 2 (MAC or hardware) address of 00:0C:6E:0A:3D:26. This confirms that the device driver is able to connect to the card, as it has read the Ethernet address burned into the network card's ROM. The next line shows that the interface has an IP address of 192.168.168.11, and the subnet mask and broadcast address are consistent with the machine being on network 192.168.168.0.

Section 6: Troubleshooting

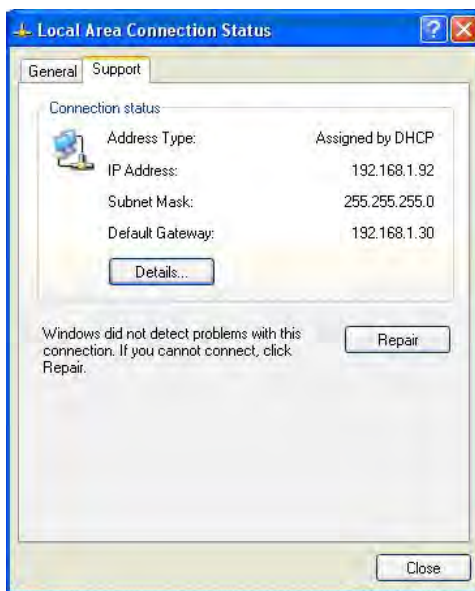
Windows Network Connections

In Windows XP you can view and renew an IP address using Windows Network Connections.

1. Open Network Connections from **Start** → **Settings** → **Network Connections**.



2. Right-click a network connection.
3. Click **Status**.
4. Click the **Support** tab. Your connection status information displays.

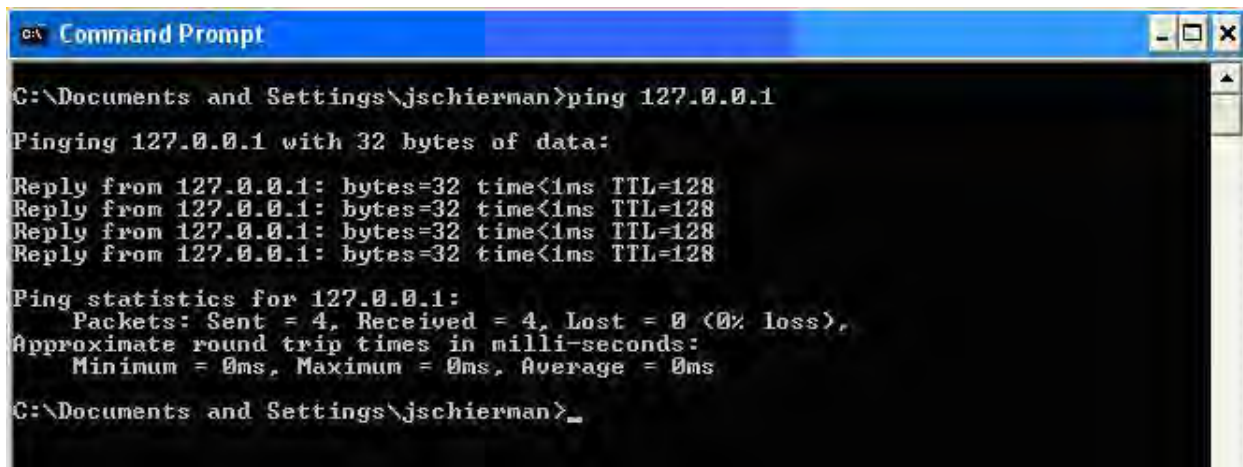


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

Ping

Use the **ping** command to test a TCP/IP configuration by using the ping command (in Windows XP Professional in this example). Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

1. Open a Command Prompt. To open a command prompt, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, ping the loopback address by typing **ping 127.0.0.1**.



```

C:\Documents and Settings\jschierman>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\jschierman>_
    
```

3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the **ping** command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host on a different subnet). If the **ping** command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server. If the **ping** command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

If the **ping** command is not found or the command fails, you can use Event Viewer to check the System Log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.

The **ping** command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

Telnet

Telnet is a simple, text-based program that lets you connect to another computer via the Internet. If you've been granted the right to connect to that computer by that computer's owner or administrator, Telnet will let you enter commands used to access programs and services that are on the remote computer, as if you were sitting right in front of it.

The Telnet command prompt tool is included with the Windows Server 2003 and Windows XP operating systems. See the related OS documentation and helps for more information. Note that if you are only using computers running Windows, it may be easier to use the Windows Remote Desktop feature. For more information about Remote Desktop, see the related OS documentation and helps.

Telnet Client

By default, Telnet is not installed with Windows Vista or Windows 7, but you can install it by following the steps below.

To install Telnet Client:

1. Click the **Start** button, click **Control Panel**, click **Programs**, and then select **Turn Windows features on or off**. If prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In the **Windows Features** dialog box, check the **Telnet Client** checkbox.
3. Click **OK**. The installation might take several minutes.

After Telnet Client is installed, open it by following the steps below.

To open the Telnet Client:

1. Clicking the **Start** button, type **Telnet** in the Search box, and then click **OK**.
2. To see the available telnet commands, type a question mark (?) and then press **Enter**.

Telnet Server

In Windows Server 2003 for most Telnet Server functions, you do not need to configure Telnet Server options to connect a Telnet client to the Windows Server 2003-based Telnet Server. However, in Windows Server 2003 you must configure Telnet Server options to be able to do certain functions.

For example, the following command uses the credentials of the user who is currently logged on to the client to create a Telnet connection on port 23 with a host named server01.

```
telnet server01
```

The following example creates the same Telnet connection and enables client-side logging to a log file named c:\telnet_logfile.

```
telnet -f c:\telnet_logfile server01
```

The connection with the host remains active until you exit the Telnet session (by using the **Exit** command), or you use the Telnet Server administration tool to terminate the Telnet session on the host.

For more information, see the Windows Server TechCenter at [http://technet.microsoft.com/en-us/library/cc787407\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc787407(W.S.10).aspx).

1. If you try to enable and install Telnet in Windows 7, and the message “An error has occurred. Not all of the features were successfully changed” displays, one workaround is to use a third party Telnet client, such as PuTTY, which also supports recommended SSH client.

PuTTY

PuTTY is a simple, free, but excellent SSH and Telnet replacement for Windows.

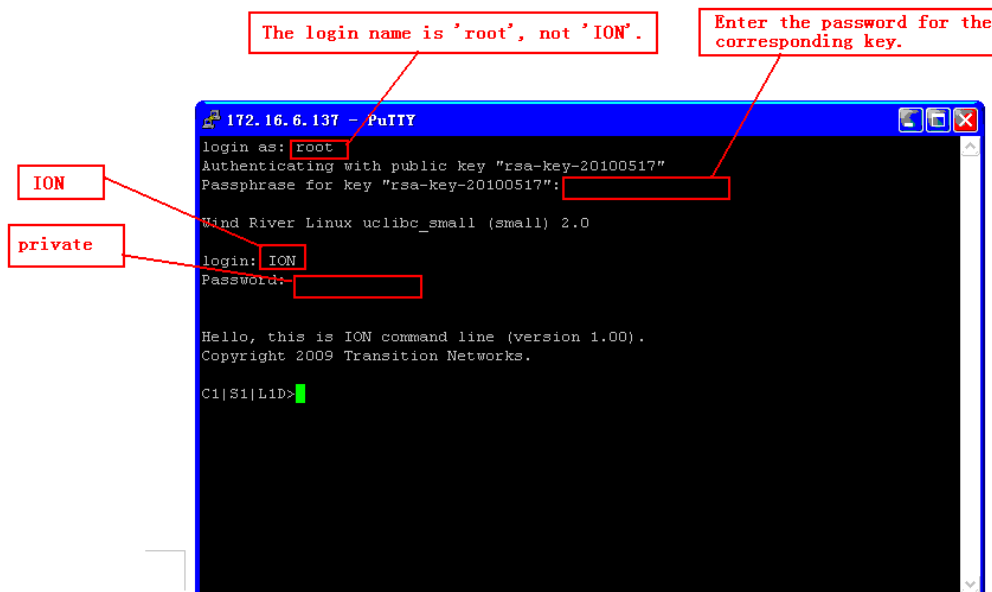
The PuTTY SSH and telnet client was developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is developed and supported by a group of volunteers. PuTTY has been ported to various other operating systems. Official versions exist for some Unix-like platforms, with on-going ports to Mac OS and Mac OS X.

The PuTTY terminal emulator application also works as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols.

For PuTTY legal and technical details, see the PuTTY download page at <http://putty.org/> or at <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

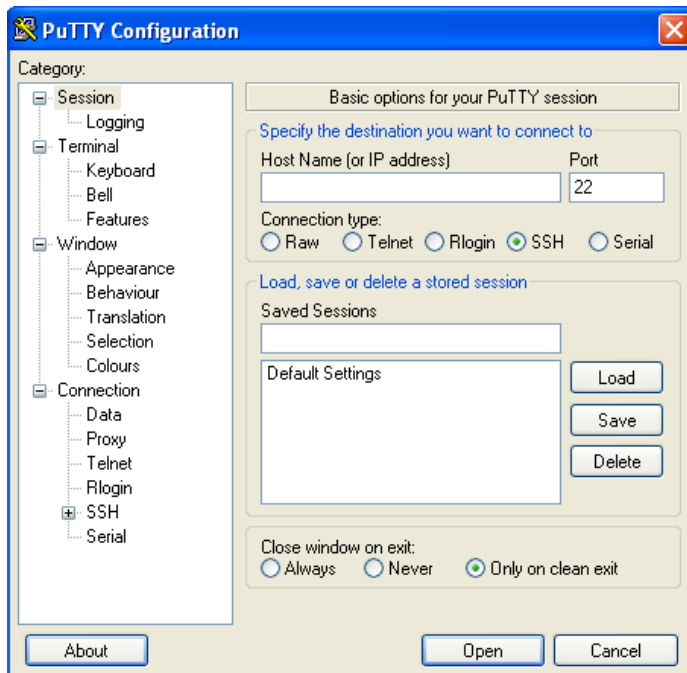
Note:

- 1) When the user-public key is loaded into the IONMM successfully, the key will take effect immediately; you do not need to restart the SSH server.
- 2) The ION system supports SSH2 keys only; SSH1 keys are not supported. When generating using puttyGen.exe, do not select the SSH1 keys.
- 3) The ION system currently supports one default user named 'root' with public key authentication.

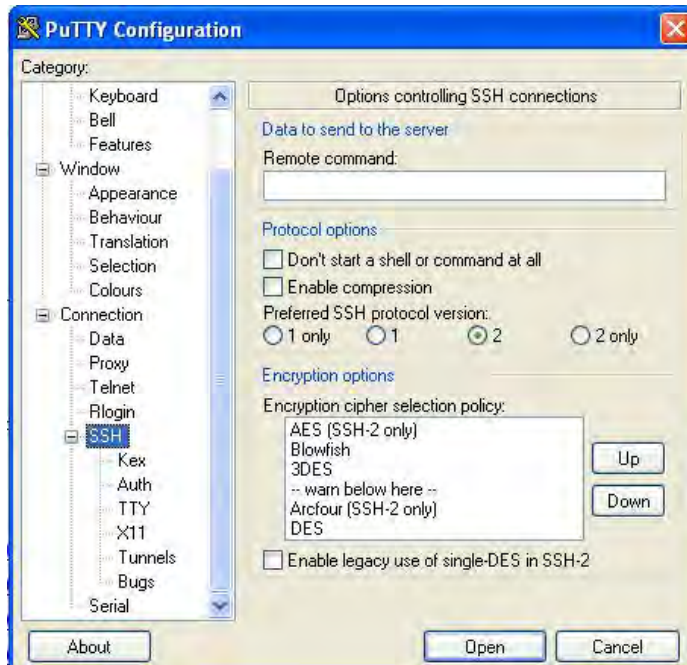


Section 6: Troubleshooting

PuTTY Basic Options:



PuTTY SSH Options:



Tracert (Traceroute)

Traceroute is a computer network tool used to determine the route taken by packets across an IP network. "Tracert" (pronounced "traceroute") sends a test network message from a computer to a designated remote host and tracks the path taken by that message.

Tracert is a Windows based tool that allows you to help test your network infrastructure. In this article we will look at how to use tracert while trying to troubleshoot real world problems. This will help to reinforce the tool's usefulness and show you ways in which to use it when working on your own networks.

The traceroute tool is available on practically all Unix-like operating systems. Variants with similar functionality are also available, such as tracepath on modern Linux installations and tracert on Microsoft Windows operating systems. Windows NT-based operating systems also provide **pathping**, which provides similar functionality.

The tracert TCP/IP utility allows you to determine the route packets take through a network to reach a particular host that you specify. Tracert works by increasing the "time to live" (TTL) value of each successive packet sent. When a packet passes through a host, the host decrements the TTL value by one and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded. Tracert, if used properly, can help you find points in your network that are either routed incorrectly or are not existent at all.

The Tracert Windows based command-line tool lets you trace the path that an IP packet takes to its destination from a source. Tracert determines the path taken to a destination by sending ICMP (Internet Control Message Protocol) Echo Request messages to the destination. When sending traffic to the destination, it incrementally increases the TTL (Time to Live) field values to help find the path taken to that destination address.

Tracert options include:

- ? which displays help at the command prompt.
- d which prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names (this speeds up the display of tracert results). Using the **-d** option helps when you want to remove DNS resolution. Name servers are helpful, but if not available, incorrectly set, or if you just want the IP address of the host, use the **-d** option.

Netstat

Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on UNIX, Unix-like, and Windows NT-based operating systems.

The **netstat** tool is used for finding network problems and determining the amount of traffic on the network as a performance measurement. It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, **netstat** displays active TCP connections.

Note: parameters used with this command must be prefixed with a hyphen (-) and NOT a slash (/):

- a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- b Displays the binary (executable) program's name involved in creating each connection or listening port. (Windows XP, 2003 Server only - not Microsoft Windows 2000 or other non-Windows operating systems).
- e Displays Ethernet statistics, such as the number of bytes and packets sent and received.
- f Displays fully qualified domain names (FQDN) for foreign addresses.(not available under Windows)
- i Displays network interfaces and their statistics (not available under Windows).
- o Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).
- p (Windows): Protocol : Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- p (Linux) Process : Show which processes are using which sockets (you must be root to do this).

Winipcfg

The **winipcfg** command is available in Windows ME, Windows 98, and Windows 95 to review your current TCP/IP network protocol settings. Follow these steps to view your current TCP/IP settings using **winipcfg**:

1. Click the Start button and then click Run.
2. Type **winipcfg** in the Open box, and then click OK. Your current TCP/IP settings are displayed.
3. To view additional information, click **More Info**.

Note: The Winipcfg display is not updated dynamically. To view changes, quit **winipcfg** and then run it again. If your IP address was dynamically allocated by a DHCP server, you can use the Release and Renew buttons to release and renew the IP address.

The following information is displayed by the **winipcfg** tool.

Adapter Address: This string of hexadecimal numbers represents the hard-coded identification number assigned to the network adapter when it was manufactured. When you are viewing the IP configuration for a PPP connection using Dial-Up Networking, the number is set to a default, meaningless value (because modems are not hard-coded with this type of address).

IP Address: This is the actual IP networking address that the computer is set to. It is either dynamically assigned to the computer upon connection to the network, or a static value that is manually entered in TCP/IP properties.

Subnet Mask: The subnet mask is used to "mask" a portion of an IP address so that TCP/IP can determine whether any given IP address is on a local or remote network. Each computer configured with TCP/IP must have a subnet mask defined.

Default Gateway: This specifies the IP address of the host on the local subnet that provides the physical connection to remote networks, and is used by default when TCP/IP needs to communicate with computers on other subnets.

Click **More Info** to display the following settings:

DHCP Server: This specifies the IP address of the DHCP server. The DHCP server provides the computer with a dynamically assigned IP address upon connection to the network. Clicking the Release and Renew buttons releases the IP address to the DHCP server and requests a new IP address from the DHCP server.

Primary and Secondary WINS Server: These settings specify the IP address of the Primary and Secondary WINS servers (if available on the network). WINS servers provide a service translating NetBIOS names (the alphanumeric computer names seen in the user interface) to their corresponding IP address.

Lease Obtained and Lease Expires: These values show when the current IP address was obtained, and when the current IP address is due to expire. You can use the Release and Renew buttons to release and renew the current IP address, but this is not necessary because the DHCP client automatically attempts to renew the lease when 50 % of the lease time has expired.

Section 6: Troubleshooting

Nslookup

nslookup is a computer program used in Windows and Unix to query DNS (Domain Name System) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The name nslookup means "name server lookup". A common version of the program is included as part of the BIND package.

Microsoft Windows 2000 Server, Windows 2000 Advanced Server, and Windows NT Server 4.0 Standard Edition provide the **nslookup** tool.

Windows' nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through the Control Panel.

Nslookup.exe can be run in two modes: interactive and noninteractive. Noninteractive mode is used when just a single piece of data is needed.

1. The syntax for noninteractive mode is:

nslookup [-option] [hostname] [server]

2. To start Nslookup.exe in interactive mode, simply type "**nslookup**" at the command prompt:

C:\> nslookup

Default Server: nameserver1.domain.com

Address: 10.0.0.1

3. Type "**help**" or "?" at the command prompt to generate a list of available commands.

Notes:

- The TCP/IP protocol must be installed on the computer running Nslookup.exe.
- At least one DNS server must be specified when you run the IPCONFIG /ALL command from a command prompt.
- Nslookup will always devolve the name from the current context. If you fail to fully qualify a name query (i.e., use a trailing dot), the query will be appended to the current context. For example, if the current DNS settings are att.com and a query is performed on www.microsoft.com; the first query will go out as www.microsoft.com.att.com because of the query being unqualified. This behavior may be inconsistent with other vendor's versions of Nslookup.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by DHCP clients (devices) to obtain configuration information for operation in an Internet Protocol network. DHCP reduces system administration workload, allowing devices to be added to the network with little or no manual intervention.

DHCP was initially defined in RFC 1531 as a standard-track protocol in October 1993, succeeding the BOOTP. The next update was RFC 2131, which is the current DHCP definition for IPv4 networks.

DHCP automates network parameter assignment to network devices from one or more fault-tolerant DHCP servers. DHCP is useful even in small networks, because it makes it easy to add new machines to the network.

DHCP is also recommended for servers whose addresses rarely change, so that if a server needs to be readdressed (RFC 2071), changes need be made in as few places as possible. For devices such as routers and firewalls that should not use DHCP, it can be useful to put SSH servers on the same host that runs DHCP, which serves to centralize administration.

DHCP is an Internet-standard protocol by which a computer can be connected to a local network, ask to be given configuration information, and receive from a server enough information to configure itself as a member of that network. ISC DHCP is open source software that implements the Dynamic Host Configuration Protocols for connection to a local network. It is a reference implementation of those protocols, but it is also production-grade software, suitable for use in high-volume and high-reliability applications. ISC's DHCP software is the most widely used open source DHCP implementation on the Internet. See <http://www.isc.org/software/dhcp>.

Section 6: Troubleshooting

Dr. Watson

Dr. Watson detects information about Windows system and program failures and records the information in a log file. Dr. Watson starts automatically at the event of a program error. To start Dr. Watson, click **Start**, click **Run**, and then type **drwtsn32**. To start Dr. Watson from a command prompt, change to the root directory, and then type **drwtsn32**.

When a program error occurs, Dr. Watson creates a log file (Drwtsn32.log) which contains:

- The line *Application exception occurred:*.
- Program error information.
- System information about the user and the computer on which the program error occurred.
- The list of tasks that were running on the system at the time that the program error occurred.
- The list of modules that the program loaded.
- The state dump for the thread ID that is listed.
- The state dump's register dump.
- The state dump's instruction disassembly.
- The state dump's stack back trace.
- The state dump's raw stack dump.
- The symbol table.

The default log file path is:

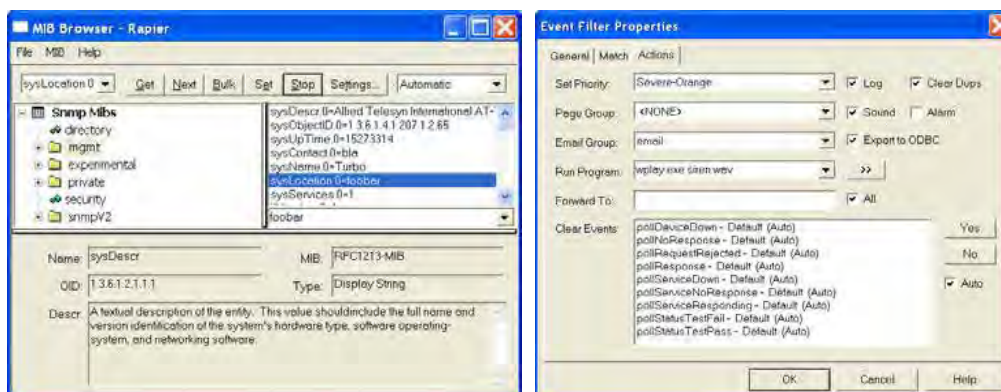
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson.

The default Crash Dump path is:

C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp.

SNMPC

SNMPC is a secure distributed network management system that can monitor an entire network infrastructure. It lets you visualize, monitor and pro-actively manage your network. The SNMPC MIB Browser screen and the SNMPC Event Filter screen are shown below.



See the Castel Rock Computing Knowledge Base, How To Guides, and FAQs at <http://www.castlerock.com/support/default.htm> for more information.

HPOV (HP OpenView)

HP OpenView was the former name for a Hewlett Packard product family that consisted of network and systems management products. The main OpenView product was Network Node Manager (NNM), a network monitoring application based on SNMP. In 2007, along with integrated Mercury Interactive, Peregrine Systems and Opware products, HP OpenView products were rebranded into HP Software & Solutions, and "OpenView" and "Mercury" names were eliminated. The HP OpenCall product remains a part of the HP Software & Solutions business. The HP Network Management Center support web site is at https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-119_4000_100.

You can access patches from the HP Software Support Online system, search for the products of interest, find Release Notes, and refer to the NNM Documentation List using your HP passport credentials at

[https://ovrd.external.hp.com/rd/sign-in?TYPE=33554433&REALMOID=06-000dbac2-dc02-1680-9aa0-a14d91440000&GUID=1&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=\\$SM\\$i%2bVqGd4Zrg0nzFPTAbCG%2fQrn0f2UZowYfT2RitHvQEb1t1qIFq3Rt65IHxgfcRnD&TARGET=\\$SM\\$http%3a%2f%2fsupport%2eopenview%2ehp%2ecom%2fselfsolve%2fmanuals](https://ovrd.external.hp.com/rd/sign-in?TYPE=33554433&REALMOID=06-000dbac2-dc02-1680-9aa0-a14d91440000&GUID=1&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SMi%2bVqGd4Zrg0nzFPTAbCG%2fQrn0f2UZowYfT2RitHvQEb1t1qIFq3Rt65IHxgfcRnD&TARGET=SMhttp%3a%2f%2fsupport%2eopenview%2ehp%2ecom%2fselfsolve%2fmanuals).

US-CERT

The National Cyber Alert System is America's first cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. Managed by the US-CERT, the system relays computer security update and warning information to all users. It provides all citizens—from computer security professionals to home computer users with basic skills—with free, timely, actionable information to better secure their computer systems. The National Cyber Alert System provides valuable cyber security information in the form of Technical Cyber Security Alerts, Cyber Security Alerts, Cyber Security Tips, and Cyber Security Bulletins.

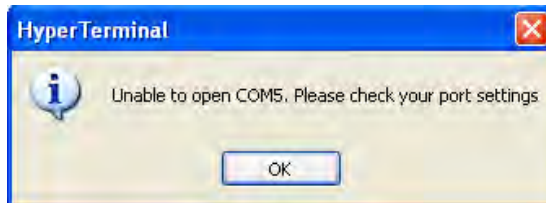
You can sign up to receive this information via email at <https://forms.us-cert.gov/maillists/>. An example of a recent alert is at <http://www.us-cert.gov/cas/techalerts/TA08-162A.html>.

Third Party Tool Messages

This section discusses messages generated by HyperTerminal, Ping, and Telnet during ION system installation, operation and configuration.

HyperTerminal Messages

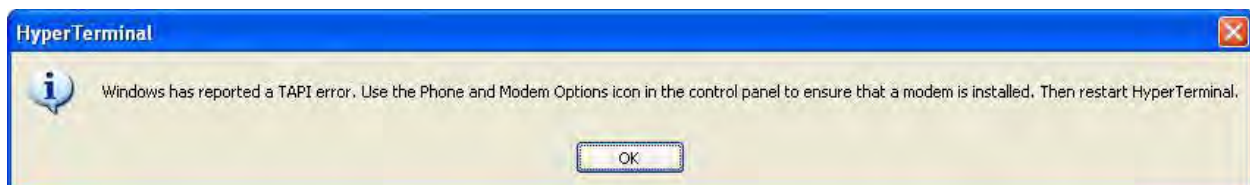
Message: *Unable to open COM x. Please check your port settings.*



Response:

1. Verify your computer's **Ports (COM & LPT)** setting. See “[Configuring HyperTerminal](#)” on page 53.
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

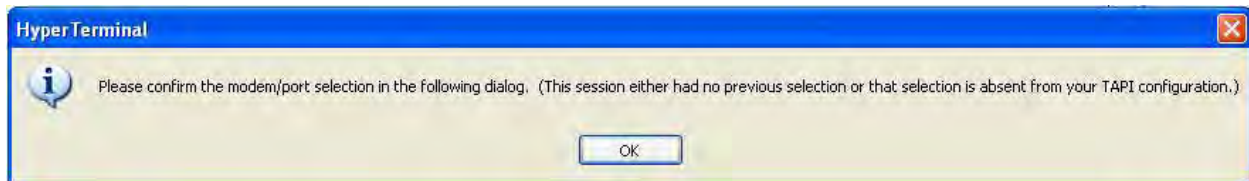
Message: *Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal.*



Response:

1. Click **OK** to close the HyperTerminal error dialog box.
2. Try opening an existing HyperTerminal connection (**File > Open**).
3. Verify your computer's **Ports (COM & LPT)** setting. See “[Configuring HyperTerminal](#)” on page 53.
4. Use the **Computer Management > Device Manager > Troubleshooter** button on the **General** tab in **Properties**.
5. Unplug and re-plug the USB connector on the IONMM card.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: Please confirm the modem/port selection in the following dialog. (This session either had no previous selection or that selection is absent from your TAPI configuration.)



Response:

1. Verify the HyperTerminal configuration. See “[Configuring HyperTerminal](#) “ on page 65 (e.g., verify your **computer’s Ports (COM & LPT)** setting).
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the NID.
4. Retry the operation. See “[Start a USB Session in HyperTerminal and Log In](#) “ on page 72.
5. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: HT Overtyping Problem - You tried to edit a typo in a CLI command, and the new data is stored, but the old data is appended to it.

Meaning: HyperTerminal (HT) is a terminal emulation program developed by Hillgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a text entry. Overtyping an entry should automatically replace the previous characters. This is a HyperTerminal problem that the ION CLI stack cannot resolve.

Response:

1. Upgrade to the latest version (a free download from www.hilgreave.com). The more current product seems to run more smoothly and has text editing features not found in earlier versions.
2. In HT, turn off local echo - refer to the HT helps and documentation for the command to use.
3. Make sure the keyboard Insert mode is turned off.
4. Download and use PuTTY or TeraTerm to use as a replacement for HT.

Section 6: Troubleshooting

5. Message: *USB Device Not Recognized*

One of the USB devices attached to this computer has malfunctioned, and Windows does not recognize it. For assistance in solving this problem, click this message.



Response:

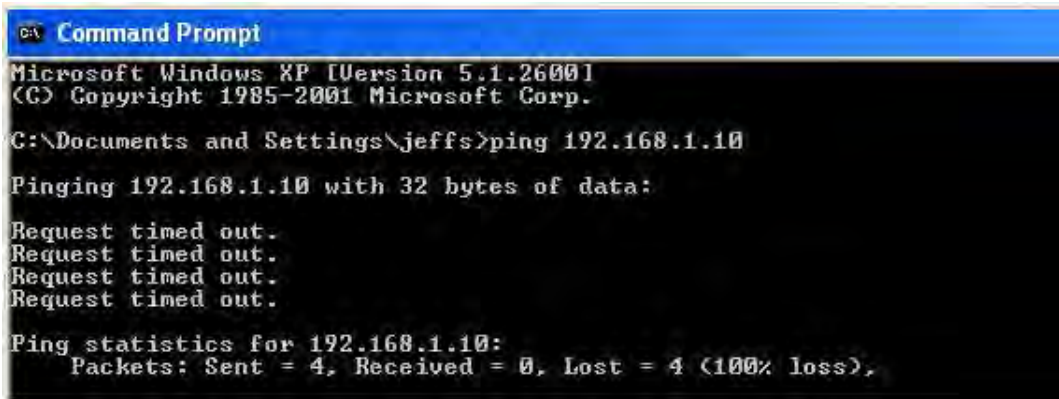
1. Click message icon in the tray. A Windows recommendation dialog displays.



2. Click **Close** to close the dialog.
3. Try reconnecting the device to the same USB port on the console device (PC).
4. Try reconnecting the device to a different USB port on the console device (PC) if available.

Ping Command Messages

Message: *Request timed out.*



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jeffs>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

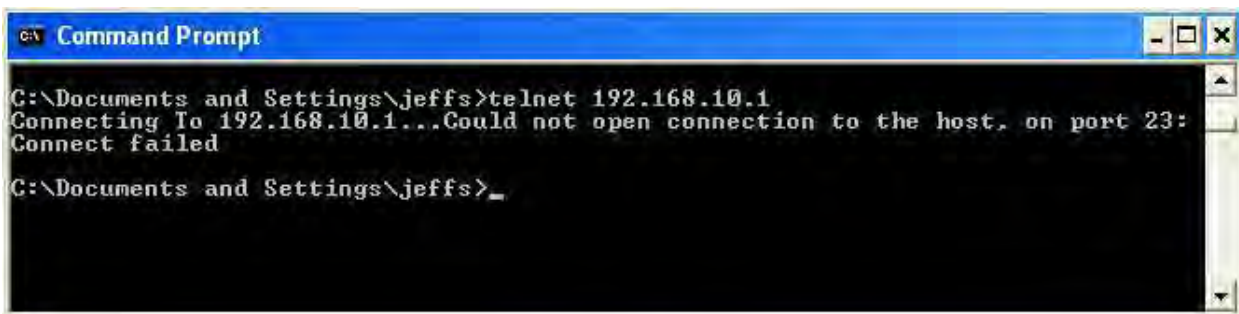
Meaning: The Ping command failed.

Recovery:

1. Verify the connection, verify correct IP address entry, and retry the operation.
2. Verify if the default IP address has changed using the Ipconfig (or similar) command.

Telnet Messages

Message: *Could not open connection to the host, on port 23: Connect failed.*



```

C:\ Command Prompt

C:\Documents and Settings\jeffs>telnet 192.168.10.1
Connecting To 192.168.10.1...Could not open connection to the host, on port 23:
Connect failed

C:\Documents and Settings\jeffs>_
  
```

Meaning: The attempted Telnet connection failed.

Recovery:

1. Verify the physical connection, verify correct IP address entry, and retry the operation.
2. Check if the default IP address has changed using the Ipconfig (or similar) command.

Section 6: Troubleshooting

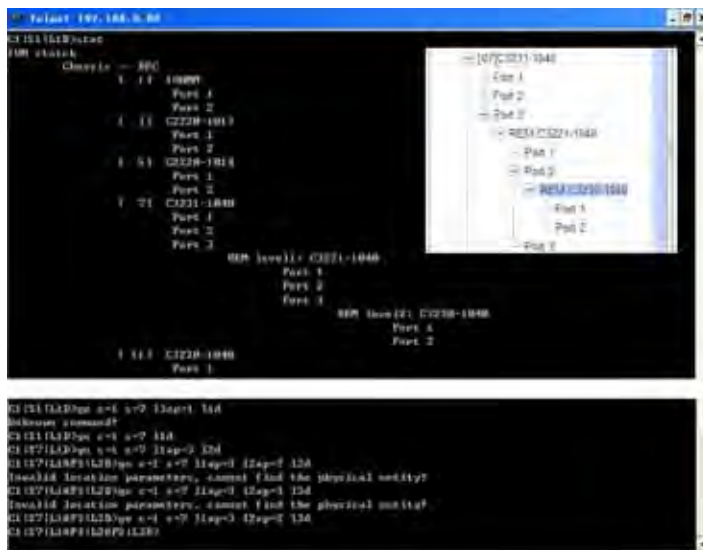
Message: *Invalid location parameters, cannot find the physical entity!*

```
C1!S7!L1AP3!L2D>go c=1 s=7 l1ap=3 l2ap=3 l3d
Invalid location parameters, cannot find the physical entity!
```

Meaning: 1) The **go** command you entered includes a location that does not exist or that you entered incorrectly. 2) The NID is in the process of a reset operation; wait one minute and then re-try the function.

Recovery:

1. Run the **stat** command to verify your configuration.
2. Click the plus sign [+] next to **ION Stack** to unfold the "ION Stack" node in the left tree view to refresh device status.
3. Click the plus sign [+] next to **Chassis** to unfold the chassis devices.



4. Compare the **stat** command results to the Web interface tree view configuration information.
5. Re-run the **stat** command with the correct location parameters.
6. Ping the device in question.
7. Unplug and re-plug the USB connector on the IONMM card.
8. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Message: *Unknown command!*

```
C1!S1!L1D>go c=1 s=7 l3ap=1 l1d
Unknown command!
```

Meaning: The command you entered is not supported, or you entered the wrong command format / syntax.

Recovery:

1. Verify the CLI command syntax.
2. For a complete list of the available commands, see the *ION System CLI Reference Manual, 33461*.

TFTP Server Messages

Messages like the ones below may display during TFTP Server operation, depending on the TFTP Server package that you selected.

Message: *File does not exist*

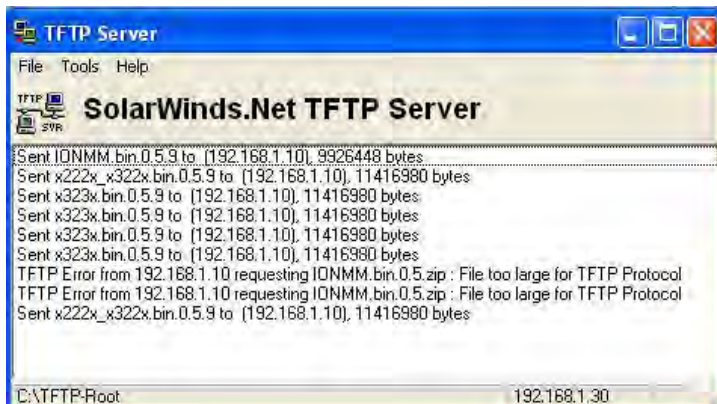


Meaning: A TFTP Server error - the TFTP Server Address that you specified does not contain the Firmware File Name specified.

Recovery:

- 1) Verify the TFTP server's correct file location (e.g., local disk at *C:\TFTP-Root*).
- 2) Verify the filename / extension.
- 3) Check the TFTP Server's online helps for suggestions.

Message: *File too large for TFTP Protocol*



Meaning: A TFTP Server error - you tried to upload a file (e.g., IONMM.bin.0.5 – 50Mb) but the TFTP server failed. The file you tried to upload via the TFTP server exceeded the file size capability.

Recovery:

- 1) Check if some extra files ended up in the zip folder – some repeated – 6 FW files total.
- 2) Remove some of the files from the zip folder and try the upload again.
- 3) Send the remaining files in a separate file.
- 4) Check the TFTP Server's online helps for suggestions.

PuTTY Messages

Messages like the ones below may display during PuTTY (or similar package) operation, depending on the package that you selected.

Message: *Server refused key*

Meaning: You can connect to a secure telnet session using password authentication, but when you try to connect using public key authentication, you receive a "*Server refused our key*" message on the client (PuTTY) session. For example, you generated a public/private key (using Puttygen) and saved them, loaded the client public key into the IONMM via TFTP, and enabled SSH. The PuTTY SSH Authentication pointed to the saved private key. You set the auto-log on user name to root as suggested, but when you activated PuTTY, after 20-30 seconds, the refusal message displayed and PuTTY reverted back to password authentication (the default).

Recovery:

1. When generating using *puttyGen.exe*, select the SSH2 keys - do not select the SSH1 keys.
2. Log in to PuTTY as '*root*' with the public key authentication.
3. Use the online helps and documentation to set up Putty as suggested.
4. See the "[PuTTY](#)" section notes on page [408](#).

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

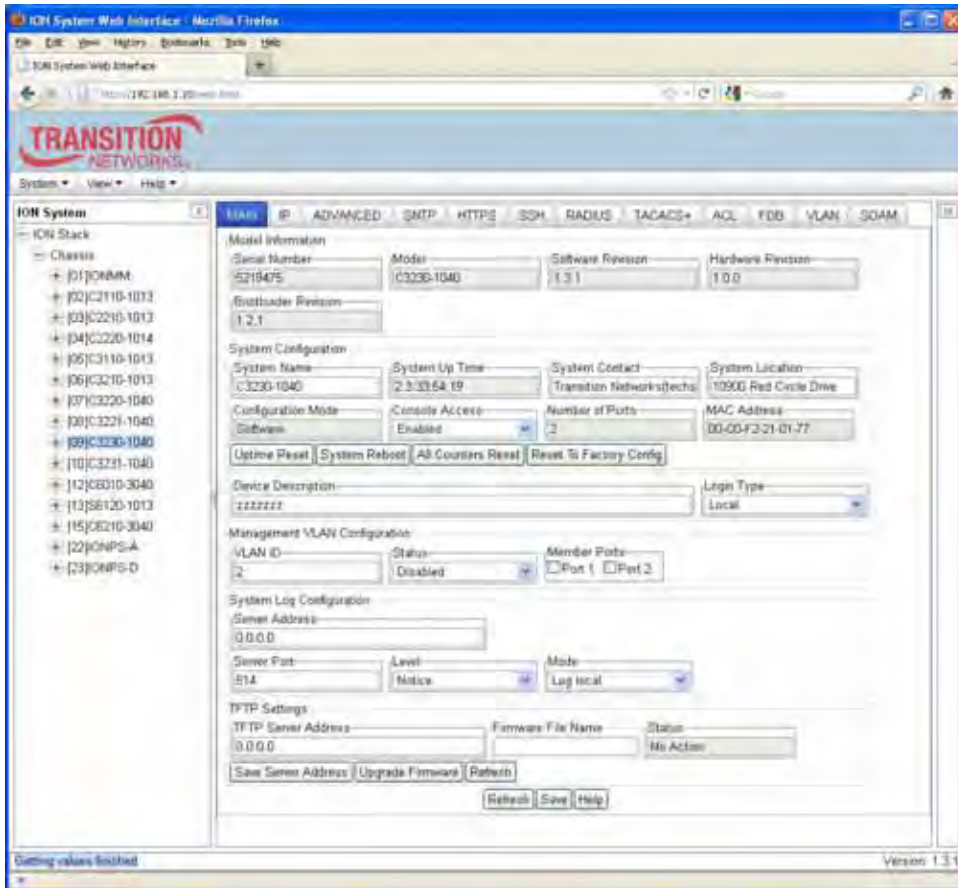
Address

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 to help the TN Technical Support Specialist.

1. From the ION system Web interface, select the x323x device **MAIN** tab. (From the CLI, use the **show** commands to gather the information requested below. This could include commands such as **show card info**, **show slot info**, **show system info**, **show ether config**, **show ip-mgmt config**, **show loam config**, or others as request by the TN Support Specialist.



2. Record the **Model Information** for your device.

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: _____ MAC Address: _____
 Number of Ports: _____ Device Description: _____

4. Provide additional Model and System information to your Technical Support Specialist. See “[Basic ION System Troubleshooting](#)” on page 301.

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 # of each involved Transition Networks product in the network:

A description of your network environment (layout, cable type, etc.): _____

Network load and frame size at the time of trouble (if known): _____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

Any previous Return Material Authorization (RMA) numbers: _____

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: Warranty and Compliance Information

Warranty

This warranty is your only remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Transition Networks is not liable for any special, indirect, incidental or consequential damages or losses, including loss of data, arising from any cause or theory. Authorized resellers are not authorized to extend any different warranty on transition networks' behalf.

Limited Lifetime Warranty

Effective for products shipped May 1, 1999 and after. Every Transition Networks' labeled product purchased after May 1, 1999 will be free from defects in material and workmanship for its lifetime. This warranty covers the original user only and is not transferable.

What the Warranty Does Not Cover

This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside the product's specified rating, or normal wear and tear of mechanical components. If the user is unsure of the proper means of installing or using the equipment, contact Transition Networks' free technical support services.

Establishing Original Ownership

To establish original ownership and provide date of purchase, please complete and return the registration card accompanying the product or register the product on-line on our product registration page.

Transition Networks will at its option:

- Repair the defective product to functional specifications at no charge
- Replace the product with an equivalent functional product
- Refund the purchase price of a defective product

Who to Contact for Returns

To return a defective product for warranty coverage, contact Transition Networks' technical support department for a return authorization number. Transition's technical support department can be reached through any of the following means:

Service Hours

Mon thru Fri 7 AM - 6 PM CST:

Contact Tech Support via telephone at 800-260-1312 or 952-941-7600

Fax 952-941-2322

Email techsupport@transition.com

Live web chat: [Transition Now](#)

Any Other Time

Voice Mail 800-260-1312 x 579 or 952-941-7600 x 579

How and Where to Send Returns

Send the defective product postage and insurance prepaid to the following address:

Transition Networks, Inc.

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Attn: RETURNS DEPT: CRA/RMA # _____

Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number.

CRA's are valid for 60 days from the date of issuance. An invoice will be generated for payment on any unit(s) not returned within 60 days.

Upon completion of a demo/ evaluation test period, units must be returned or purchased within 30 days. An invoice will be generated for payment on any unit(s) not returned within 30 days after the demo/ evaluation period has expired.

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

Before making any non-warranty repair, Transition Networks requires a \$200.00 charge plus actual shipping costs to and from the customer. If the

Appendix A: Warranty and Compliance Information

repair is greater than \$200.00, an estimate is issued to the customer for authorization of repair. If no authorization is obtained, or the product is deemed 'not repairable', Transition Networks will retain the \$200.00 service charge and return the product to the customer not repaired. Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. TRANSITION NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY. AUTHORIZED RESELLERS ARE NOT AUTHORIZED TO EXTEND ANY DIFFERENT WARRANTY ON TRANSITION NETWORKS'S BEHALF.

Customer Pays Non-Compliant Return Costs

The customer must pay the non-compliant product(s) return transportation cost to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for shipping the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

Non-Warranty Repair Costs



Before making any non-warranty repair, Transition Networks requires a \$200 charge, plus actual shipping costs to and from the customer. If the repair is greater than \$200, an estimate is issued to the customer for authorization before making the repair. If no authorization is obtained, or the product is deemed not repairable, Transition Networks will retain the \$200 service charge and return the product to the customer not repaired.

Repaired Non-Warranty Products

Non-warranted products repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

Compliance Information

Standards	CISPR22/EN55022 Class A, CE Mark
FCC Regulations	 This equipment has been tested and found to comply with the limits for class A devices, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and radiates radio frequency energy; therefore, if not installed and used in accordance with the instructions in this document, the device could cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference; all customers will be required to correct the interference problem at their expense.
CE Marking	This is a Class A product. In a domestic environment, this product could cause radio interference; as a result, the customer may be required to take adequate preventative measures.
UL Recognized	 Tested and recognized by the Underwriters Laboratories, Inc.
Canadian Regulations	<p>This digital apparatus does not exceed the Class A limits for radio noise from digital apparatus set out on the radio interference regulations of the Canadian Department of Communications.</p> <p>Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la Class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.</p>

European Regulations

WARNING:

This is a Class A product. In a domestic environment, this product could cause radio interference in which case the user may be required to take adequate measures.

Achtung !

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fall ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention !

Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.





In accordance with European Union Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, Transition Networks will accept post usage returns of this product for proper disposal. The contact information for this activity can be found in the 'Contact Us' portion of this document.



CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK.
Failure to observe this caution could result in damage to the public telephone network.

Der Anschluss dieses Gerätes an ein öffentliches Telekommunikationsnetz in den EG-Mitgliedstaaten verstößt gegen die jeweiligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Declaration of Conformity

	Declaration of Conformity
Name of Mfg:	Transition Networks 10900 Red Circle Drive, Minnetonka MN 55343 U.S.A.
Model number(s):	C3230-10 xx, C3231-10xx, C3220-10xx, C3221-10xx S3230-10 xx, S3231-10xx, S3220-10xx, S3221-10xx
ION x222x & x32xx multi-port NIDs conform to the following directive(s) and standard(s):	
EMC Directive 2004/108/EC; EN 55022:2006+A1:2007 Class A; EN55024:1998+A1:2001+A2:2003; EN6100-2-3; EN6100-3-3; CFR Title 47 Part 15 Subpart B Class A. Low Voltage Directive: 2006/95/EC; IEC 60950-1:2005; CFR Title 21 Section 1040.10 Class I; CE Mark.	
I, the undersigned, hereby declare that the model numbers listed in this declaration of conformity conform to the Directive(s) and Standard(s) herein.	
 Stephen Anderson, Vice-President of Engineering	<u>June 2010</u> Date

MEF Certifications

Transition Networks has received MEF 9, 14, and 21 certification for the x2220, x3220, x3230 and S3240 products at the time of this publication. The MEF Carrier Ethernet Certification Program is designed to ensure that global equipment and services comply with MEF standards and pave the way for interoperability. The latest list of MEF certified TN products, and the MEF certificates and test reports are available on the TN website at <http://www.transition.com>.

Electrical Safety Warnings

Electrical Safety

IMPORTANT: This equipment must be installed in accordance with safety precautions.

Elektrische Sicherheit

WICHTIG: Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

Elektrisk sikkerhed

VIGTIGT: Dette udstyr skal installeres i overensstemmelse med sikkerhedsadvarslerne.

Elektrische veiligheid

BELANGRIJK: Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

Sécurité électrique

IMPORTANT : Cet équipement doit être utilisé conformément aux instructions de sécurité.

Sähköturvallisuus

TÄRKEÄÄ : Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

IMPORTANTE: questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal installeres i samsvar med sikkerhetsregler.

Segurança eléctrica

IMPORTANTE: Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

Seguridad eléctrica

IMPORTANTE: La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

Elsäkerhet

OBS! Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.

Appendix B: Factory Defaults

The x323x NID *Device* Level Factory Defaults are shown in Table 23 below.

The x323x NID *Port* Level Factory Defaults are shown in Table 24.

Device-Level Factory Defaults

Note: The default settings shown are as seen in the tabs/fields of the Web interface.

Table 35: Device-Level Factory Defaults

Item/Field	Default Setting
Web Access Password	private
Telnet/USB Login	ION
Telnet/USB Password	private
MAIN tab	
Model Information	Serial Number: device dependent (e.g., 1234567) Model: device dependent (e.g., C3230-1040) Software Revision: FW vs. dependent (e.g., 1.1.0) Hardware Revision: HW vs. dependent (e.g., 0.0.1) Bootloader Revision: BL vs. dependent (e.g., 1.2.0)
System Configuration	System Name: C3230-1040 System Contact: Transition Networks (techsupport@transition.com) System Location: 10900 Red Circle Drive
Configuration Mode Console Access Number of Ports MAC Address	Software Enabled 2 (x3230) or 3 (x3231) PC-specific (e.g., 00-C0-F2-42-00-DE)
Device Description	blank
VLAN ID	2
Status	Disabled

Member Ports	none checked
System Log Configuration (Syslog)	Server Address: 192.168.0.2 Server Port: 514 Level: Notice Mode: Log local
TFTP Settings	TFTP Server Address: 0.0.0.0 Firmware File Name: blank Status: blank
IP tab	
IPv4	IP Address Mode: Static IP Address: 192.168.0.10 Subnet Mask: 192.168.1. 0 Default Gateway: 192.168.0.1
IPv6	Status: Enabled IP Address Mode: Static IP Address: 2001:1234::1 Prefix Length: 64 Gateway Mode: Route Discovery
DNS Configuration	DNS 1-6: 0.0.0.0
ADVANCED tab	
FDB Aging Time	300
MAC Address Learning	Port 1 and Port 2 unchecked
Link Pass Through(LPT)	Transparent LPT: Disabled Selective LPT: Disabled Monitoring Port: Port 2
Redundancy (x3231 only) Primary Port Secondary Port Active Port	Enabled Port 2 Port 3 Port 2

Appendix B: Factory Defaults

IEEE Priority Class	<table border="1"> <thead> <tr> <th><u>Remap</u></th> <th><u>To</u></th> </tr> </thead> <tbody> <tr><td>0</td><td>PID 0</td></tr> <tr><td>1</td><td>PID 0</td></tr> <tr><td>2</td><td>PID 1</td></tr> <tr><td>3</td><td>PID 1</td></tr> <tr><td>4</td><td>PID 2</td></tr> <tr><td>5</td><td>PID 2</td></tr> <tr><td>6</td><td>PID 3</td></tr> <tr><td>7</td><td>PID 3</td></tr> </tbody> </table>	<u>Remap</u>	<u>To</u>	0	PID 0	1	PID 0	2	PID 1	3	PID 1	4	PID 2	5	PID 2	6	PID 3	7	PID 3
<u>Remap</u>	<u>To</u>																		
0	PID 0																		
1	PID 0																		
2	PID 1																		
3	PID 1																		
4	PID 2																		
5	PID 2																		
6	PID 3																		
7	PID 3																		
IP Traffic Class	<table border="1"> <thead> <tr> <th><u>Remap</u></th> <th><u>To</u></th> </tr> </thead> <tbody> <tr><td>0 – 15</td><td>0</td></tr> <tr><td>16 – 31</td><td>1</td></tr> <tr><td>32 – 47</td><td>2</td></tr> <tr><td>48 – 63</td><td>3</td></tr> </tbody> </table>	<u>Remap</u>	<u>To</u>	0 – 15	0	16 – 31	1	32 – 47	2	48 – 63	3								
<u>Remap</u>	<u>To</u>																		
0 – 15	0																		
16 – 31	1																		
32 – 47	2																		
48 – 63	3																		
SNTP tab																			
SNTP Client Device Time	Disabled 1970 0102 20:46:50																		
UTC Timezone	(GMT-06:00)Central Time (US & Canada)																		
Daylight Saving Time	Disabled																		
SNTP Server x	0.0.0.0																		
HTTPS tab																			
HTTPS Status	Disabled																		
HTTPS Port	443																		
Certificate Type	Self Certificated																		
TFTP Server Address	0.0.0.0																		
Certificate File Name	blank																		

Private File Name	blank
Private Password	blank
SSH tab	
SSH Server Status	Disabled
Version	2.0
SSH Auth Timeout	60
SSH Auth Retries	3
Public-Key of Host	RSA: 00.00.00.07. ... B0.44.AB.F0.79 DSA: 00.00.00.07. ... 3C.00.4A.1F.89
Host Key Type	No Gen
Save Host-Key to Flash	Save (not configurable)
Public-Key of User	RSA: blank DSA: blank
User Name	blank
Public-Key Type	RSA
TFTP Server Address	0.0.0.0
Source File Name	blank

Appendix B: Factory Defaults

RADIUS tab	
RADIUS Client	Disabled
Server Address x	0.0.0.0
Server Secret x	blank
Retries x	3
Timeout x	30
TACACS+ tab	
TACACS+ Client	Enabled
TACACS Server 1-6	Server Address: 0.0.0.0 Server Secret: blank Retries (1-5): 3 Timeout (1-60s): 30
ACL tab	
ACL Status	Disabled
Chain Name	INPUT
Chain Policy	Accept
Rules table	No records found.
Priority	blank
Policy	Accept
Trap Rate	0

Conditions table	No records found.
Type	Source MAC Address
Source or Destination	Source
Operation	Equal
Value	blank
FDB tab	
FDB ID	0
MAC Address	blank
Port	Port 1
Priority	blank
Entry Type	static
Flush Operation Flush Status Failure Reason	Flush All blank blank
VLAN tab	
VLAN ID	blank
FDB ID	0
Priority Override	Disabled
Priority	0
Member Tag Port 1	NoMod
Member Tag Port 2	NoMod

Appendix B: Factory Defaults

Member Tag Port 3*	NoMod
Flush Operation Flush Status Failure Reason	Flush All blank blank
SOAM tab	
SOAM: Main Configuration sub-tab	
Chassis ID sub-type Chassis ID Management address domain Management address Port ID table : Port Port ID subtype Port ID	macAddress XX-XX-XX-XX-XX-XX .0.1 192.168.0.10.0.0 1 and 2 Local 00.00.00.01 and 00.00.00.02
SOAM: MD sub-tab	
MD table	No records found.
MD ID	blank
Name	blank
Level	Level 0
Sender ID permission	None
SOAM : MA/MEG sub-tab – MA Configuration	
Parent MD ID	blank
MA ID	blank
Name	blank
CC interval	1 sec

VLAN type	none
Primary VID	0
S-VID	0
RMEP auto detection	Disabled
RMEP auto detection timeout	4000
Sender ID permission	MD defer
VLAN ID list: Primary VLAN ID	blank
VLAN ID list: VLAN ID	0
MEP ID list: Parent MA/MEG ID	blank
MEP ID list: MEP ID	blank
SOAM: MA/MEG sub-tab – MEG Configuration	
MEG ID	blank
Name	blank
Level	Level 0
CC interval	1 sec
CC interworking	Disabled
VLAN type	none
Primary VID	0
S-VID	0

Appendix B: Factory Defaults

RMEP auto detection	Disabled
RMEP auto detection timeout	4000
Sender ID permission	None
VLAN ID list: Primary VLAN ID	blank
VLAN ID list: VLAN ID	0
MEP ID list: Parent MA/MEG ID	blank
MEP ID list: MEP ID	blank
SOAM: MEP sub-tab – Configuration	
Parent MA/MEG	blank
MEP ID	blank
Port	Port 1
Direction	Down
Primary VID	0
Status	Disabled
Cc status	Disabled
FNG alarm time	250
FNG reset time	1000
Lowest priority defect	macRemErrXcon
LTM/CCM priority	Priority 7

SOAM: MEP sub-tab – CC monitoring	
Local MEP ID table	No records found.
SOAM: MEP sub-tab – Loopback	
Destination	MAC address
Destination MAC address	blank
Destination MEP ID	blank
Number of LBMs to transmit	blank
Data TLV	blank
Transmission rate	blank
Priority	Priority 7
Drop enable	Disabled
Statistic	Unicast
First sent sequence id table	No records found.
SOAM: MEP sub-tab – Linktrace	
Destination	MAC address
Target MEP ID	blank
Target MAC Address	blank
TTL	64
Use FDB only	True

Appendix B: Factory Defaults

MA/MEG ID table	No records found.
Transaction Identifier	blank
SOAM: MEP sub-tab – ETH-MCC	
Destination	MAC address
Destination MAC address	blank
Destination MEP ID	blank
OUI	blank
Data	blank
SOAM: MEP sub-tab – ETH-TEST	
Destination	MAC address
Destination MEP ID	blank
Destination MAC address	blank
Pattern Type	nullnocrc
Pattern Size	blank
Packets to send	blank
SOAM: MEP sub-tab – DM	
Destination	MAC address
Remote MEP ID	blank
Remote MAC address	blank

Period	1 sec
Number of periods	blank
SOAM: MEP sub-tab – FLM	
FLM status	Enabled
Far end MEP ID	blank
SOAM: MEP sub-tab – AIS	
AIS notify	Enabled
AIS process	Enabled
Interval	1 sec
Transmit	Enabled
Priority	Priority 0
MA/MEG ID table	No records found.
Client type	MEP
MEG ID	blank
MEP ID	blank
MIP ID	blank
SOAM: MIP sub-tab	
MIP table	No records found.
MIP ID	blank

Appendix B: Factory Defaults

Type	Y.1731
MD/MEG ID	blank
Port	Port 1
Admin status	Down
AIS transmit interval	1 sec
AIS state	Enabled
AIS priority	Priority 0
SOAM: Configuration Error List sub-tab	
VLAN ID table	No records found.

SNMP tab	
General sub-tab	Community String: blank Access Mode: Read Only SNMP V3 Engine ID: 800003640300C0F2209EDE
Users sub-tab	User Name: blank Group Name: blank Security Model: V3 Security Level: NoAuthNoPriv Authentication Protocol: grayed out Password: grayed out Privacy Protocol: grayed out Password: grayed out
Groups sub-tab	Group Name: blank Security Model: V1 Security Level: NoAuthNoPriv Read View: blank Write View: blank Notify View: blank
Views sub-tab	View Name: blank OID Sub Tree: blank Type: Included
Trap Hosts sub-tab	Trap Version: V1 IP: blank Port: 162 Community/Security Name: blank Security Level: NoAuthNoPriv Trap/Inform: Trap Timeout (centisecond): grayed out Retry Times: grayed out
Remote Users sub-tab	Remote IP: blank Remote Port: blank Remote Engine ID: blank User Name: blank Security Model: V3

Appendix B: Factory Defaults

	Security Level: NoAuthNoPriv Authentication Protocol: grayed out Password: grayed out Privacy Protocol: grayed out Password: grayed out
	USERS tab
User table	User Name: ION Password: ***** Level: admin
User entry field	User Name: blank Password: blank Confirm Password: blank Level: admin

Port-Level Factory Defaults

Note: The default settings shown are as seen in the tabs/fields of the Web interface.

The x323x *Device* Level Factory Defaults are shown in Table 23 above.

The x323x *Port* Level Factory Defaults are shown in Table 24 below.

Table 36: Port-Level Factory Defaults

Item/Field	Default Setting
MAIN tab	
Circuit ID	blank
Link Status	Down
Admin Status	Up
Speed Duplex	Negotiating Negotiating
Port Mode (Port 1)	1000BaseX
Port Admin Mode (Port 2)	100BaseFX
AutoCross Mode	Auto
MAC Address	00-C0-F2-42-00-E0
Connector Type	RJ-45 (Port 1) SFP slot (ports 2 and 3)
Auto Negotiation	Enabled
Force Speed Force Duplex	100Mbps Full Duplex
Capabilities Advertised	<ul style="list-style-type: none"> • All speed/duplex boxes checked • All Pause boxes unchecked

Appendix B: Factory Defaults

Pause Admin Mode (Port 2) Pause Oper Mode Control Functions Supported	Disabled Disabled None
Source Port Forward Settings	2 All boxes checked
L2CP Disposition	All set to "Pass"
TN Topology Discovery Protocol TX	Enabled
Virtual Cable Test table	No records found
ADVANCED tab	
Rate Limiting Mode	Counts All Layer 1
Egress Rate Limit	Unlimited
Ingress Rate Limit	Unlimited
SA Lock	Disabled
SA Lock Action	Discard and Notify
Filter Unknown Unicast	Disabled
Filter Unknown Multicast	Disabled
VLAN Status	Disabled
Discard Tagged	Disabled
Discard Untagged	Disabled
Force Default VLAN	Disabled
Default VLAN ID	2
Default Priority	0

IEEE Priority Class	Enabled																		
IP Traffic Class	Enabled																		
Priority Precedence	Use IEEE																		
SA Priority Override	Disabled																		
DA Priority Override	Disabled																		
VID Priority Override	Disabled																		
Frame Tag Mode	Customer																		
Provider Ether Type	X88A8																		
User Priority	<table border="1"> <thead> <tr> <th><u>Remap</u></th> <th><u>To</u></th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td></tr> <tr><td>1</td><td>1</td></tr> <tr><td>2</td><td>2</td></tr> <tr><td>3</td><td>3</td></tr> <tr><td>4</td><td>4</td></tr> <tr><td>5</td><td>5</td></tr> <tr><td>6</td><td>6</td></tr> <tr><td>7</td><td>7</td></tr> </tbody> </table>	<u>Remap</u>	<u>To</u>	0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7
<u>Remap</u>	<u>To</u>																		
0	0																		
1	1																		
2	2																		
3	3																		
4	4																		
5	5																		
6	6																		
7	7																		
LOAM tab																			
Main sub-tab																			
Admin Status	Disabled																		
Operational Status	Link Fault																		
LOAM Mode	Passive																		
Max PDU Size	1500																		
Configuration Revision	1																		

Appendix B: Factory Defaults

Functions Supported	None / Loopback, Event Notification
LOAM Peer Information	MAC Address: 00-00-00-00-00-00 Vendor OUI: 00:00:00 Vendor Info: 0 LOAM Peer Mode: Unknown Max PDU Size: 0 Configuration Revision: 0 Functions Supported: None
Loopback Type	Alternate
Loopback Status	No Loopback
Ignore Loopback Request	Disabled

Event Configuration sub-tab	
Error Symbol Period Window High Bits	0
Error Symbol Period Window Low Bits	125000000
Error Symbol Period Threshold High Bits	0
Error Symbol Period Threshold Low Bits	0
Error Symbol Period Event Notification	Enabled
Error Frame Period Window	0
Error Frame Period Threshold	0
Error Frame Period Event Notification	Enabled
Error Frame Window	0

Error Frame Threshold	0
Error Frame Event Notification	Enabled
Error Frame Seconds Summary Window	0
Error Frame Seconds Summary Threshold	0
Error Frame Seconds Event Notification	Enabled
Dying Gasp	Enabled
Critical Event	Enabled
Event Log sub-tab	
Event Log table	No record found.

Switch Mode Default: By default, the S323x is managed by the IONMM. Setting the mode to local indicates that the device is not managed by the IONMM but either a direct USB connection or a direct network connection via Telnet or the Web interface. Setting the mode to remote indicates that the device is managed through the IONMM. See the **switch mode** command for details.

Appendix C: Configuration Quick Reference – CLI

IPv4 Configuration

1. Define IP address and subnet mask.

```
set ip type={ ipv4 | dns } addr=<ipaddr> subnet-mask =<subnet>
```

2. Define the IP address mode.

```
set ip address mode={ bootp|dhcp|static }
```

2. Define default gateway.

```
set gateway type={ ipv4 | dns } addr=<gway>
```

3. Define DNS servers.

```
set dns-server svr=<index> type=<format> addr=<ipaddr>
```

IPv6 Configuration

1. Set the IPv6 Mode.

```
set ipv6 address mode=<static|dhcpv6|stateless>
```

2. If 'Stateless Auto configuration' is selected, then enable Route Discovery (step 4).

3. Enable IPv6 Management state.

```
set ipv6-mgmt state=enable
```

4. Configure the IPv6 gateway method.

```
set ipv6 gateway mode=<static|routerdisc>
```

ACL Configuration (IPv4)

1. Enable ACL.

```
set acl state=enable
```

2. Define default chain policy.

```
set acl table=filter chain=input policy=<ptype>
```

3. Define one or more conditions.

```
add acl condition type=<xx> srcdst={src | dst} oper={equal | notequal} value=<yy>
```

4. Define one or more rules.

```
add acl rule index=<inum>position={head | tail} table=filter chain=input policy={accept | drop | trap} traprate=<rate> condition=<list>
```

ACL Configuration (IPv6)

1. Enable ACL.

```
set ip6tables acl state
```

2. Define the default chain policy.

```
set ip6tables acl table=filter chain=input policy=accept
```

3. Define condition(s) to be associated with a rule.

```
set ip6tables acl condition=1 rule_index=1
```

4. Define rule(s) to be associated with the chain.

```
add ip6tables acl rule position=head table=filter chain=input policy=1 trap=444
```

5. Verify that ACL has been enabled.

```
show ip6tables acl state
```

6. Verify the ACL rules have been defined and associated.

```
show ip6tables acl rule
```


Backup and Restore

1. Show provision modules.
show prov modules
2. Set Backup Module Configuration.
set backup module-index=<1-256>
3. Set Restore Module Configuration.
set restore module-index=<1-256>
4. Backup module list.
backup module-list=<1-10>
5. Restore module list.
restore module-list=<1-10>
6. Show provision modules.

HTTPS Configuration

1. Enable HTTPS.
set https state=enable
2. Define the certificate type.
set https certificate-type={authorized | self-certificate}
3. Define the certificate file.
set https certificate-file=<name>
4. Define the private key file.
set https private-key file=<name>
5. Define the password.
set https private-key password

Management VLAN Configuration

1. Access the x323x via either a USB connection or a Telnet session.
2. Check the current Management VLAN configuration. Type **show mgmt vlan config** and press **Enter**.

Note: In the following steps to enable Management VLAN, the first is at the port level, the other steps are at the device level. These steps must be performed in the order shown.
3. Change the Management port from the default “Customer” mode to “Network” mode. Type **set port vlan tag mode=network** and press **Enter**.
4. Set this port as Management port; enter the ports to be associated with this VLAN ID (VID). Type **set mgmt vlan port=2** and press **Enter**.
5. Enable Management VLAN mode. Type **set mgmt vlan state=enable** and press **Enter**.
6. Change the Management VID. Type **set mgmt vlan vid=10** and press **Enter**.
7. Add a VLAN. Type **add vlan vid=10** and press **Enter**.
8. Other Management VLAN or Port VLAN attributes can be changed without strict order. See “[Configuring Management VLAN](#)” on page 268.

RADIUS Configuration

1. Define the RADIUS server.

set radius svr=<index> type={ipv4 |ipv6|dns} addr=<ipaddr> [retry=<limit>] [timeout=<secs>]
2. Define the RADIUS server secret.

set radius svr=<index> secret=<secret>
3. Enable RADIUS.

set radius client state=enable

Create a User with RADIUS and SSH Enabled

1. Launch the SSH client.
2. Enter 'ION' – 'private' to log in to SSH (the first time).
3. Enter the RADIUS user and password to log in to RADIUS.
4. Add the 'TEST' (user name) – 'TEST111' (password) user.
5. Close the SSH client.
6. Launch the SSH client again
7. Enter 'TEST' – 'TEST111' to log in to SSH.
8. Enter the RADIUS user and password to log in to RADIUS.

Create a User with SSH Enabled (RADIUS Disabled)

1. Launch the SSH client.
2. Enter 'ION' – 'private' to login to SSH (the first time).
3. Add 'TEST' (user name) – 'TEST111' (password) user (see Note below).
4. Close the SSH client.
5. Launch the SSH client again.
6. Enter 'TEST' – 'TEST111' to login via SSH.

TACACS+ Configuration

1. Enable the TACACS+ client.

set tacplus client state=enable

2. Configure the TACACS + server retry attempts.

set tacplus svr 1 retry=<1-5>

3. Configure the TACACS + server (password).

set tacplus svr 1secret=SECRET

4. Configure the TACACS + server timeout period.

set tacplus svr 1 timeout=<1-60>

5. Configure the TACACS + server type.

set tacplus svr 1 type=<ipv4 / ipv6 / dns>

SNTP Configuration

1. Enable SNTP.

```
set sntp state=enable
```

2. Set the current time.

```
set curr-time=<“time”>
```

3. Define your timezone.

```
set sntp timezone=<zone>
```

4. Enable daylight savings time (DST).

```
set sntp dst-state=enable
```

5. Define DFST start time.

```
set sntp dst-start=<“time”>
```

6. Define DST end time.

```
set sntp dst-end=<“time”>
```

7. Define DST offset.

```
set sntp dst-offset=<value>
```

8. Define SNTP server.

```
set sntp-svr svr=<index> type={ipv4 | dns} addr=<ipaddr>
```

SSH Configuration

1. Enable SSH.

```
set ssh server state=enable
```

2. Define the timeout value.

```
set ssh client timeout=<seconds>
```

3. Define the retry limit.

```
set ssh auth-retry=<limit>
```

4. Generate the host key.

```
generate ssh host-key={rsa | dsa | both}
```

5. Define the public key user.

```
set ssh public-key user=<name> type={rsa | dsa} file=<file>
```

Fiber Port Redundancy Configuration

1. Set the Redundancy state to enable.

```
set redundancy state=[enable|disable]
```

2. Verify the configuration has been set.

```
show redundancy info
```

Syslog Configuration

1. Define the Syslog server port.

```
set syslog svr port=<1-65535>
```

2. Set the Syslog operating mode.

```
set syslog mode=<local|remote|localAndRemote|off>
```

3. Set the level of Syslog reporting.

```
set syslog level=<emerg|alert|crit|err|warning|notice|info|debug>
```

4. Set the Syslog server type and address.

```
set syslog svr type=<ipv4|ipv6|dns> addr=<ipaddr>
```

System (Login) User Configuration

1. Create a new system user.

```
add sysuser name=NAMESTR level=<admin|read-write|read-only> pass=PASSSTR  
confirmpass=PASSSTR
```

2. Edit an existing user's access level.

```
set sysuser name=NAMESTR level=<admin|read-write|read-only>
```

3. Set a new password for an existing ION system user.

```
set sysuser name=NAMESTR pass=PASSSTR confirmpass=PASSSTR
```

4. Remove an existing system user.

```
remove sysuser name=NAMESTR
```

Transfer Files via Serial Protocol (X/Y/Zmodem)

1. Send a request to servers / local file system to download content for a subsequent put command.

```
serial get protocol={ xmodem|xmodem-1k|ymodem|zmodem }
```

2. Send a request to servers / local file system to upload content.

```
serial put protocol=zmodem file=xxxx
```

3. Perform a firmware upgrade over the selected serial line.

```
serial upgrade protocol=<xmodem|xmodem-1k|ymodem|zmodem file=xxxx
```


SNMP Configuration

1. Access the IONMM through either a USB connection or a Telnet session.
2. Define the General configuration. Type:


```
add snmp community name=xxxxxxx access_mode={read_only|read_write}
add snmp remote engine addrtype=ipv4 addr=xx port=xx engine_id=xx
set snmp local engine=xx
```
3. Define one or more Local Users. Type:


```
add snmp local user name=STR_USR_NAME group=STR_GRP_NAME security-
level=(noAuthNoPriv|authNoPriv|authPriv) [auth-protocol=(md5|sha) pass-
word=STR_AUTH_PASS] [priv-protocol=(des|aes) password=STR_PRIV_PASS]

set snmp local user name=xxxx group=xxxx
```
4. Define one or more Groups. Type:


```
set snmp group name=STR_SNMP_GRP
set snmp local user group=xxx
```
5. Define one or more Views. Type **set snmp view name= STR_SNMP_VIEW**.
6. Define one or more Trap Hosts.
 Type **add snmp traphost version=v3 type=ipv4 addr=STR_SVR_ADDR**.
7. Define one or more Remote Engines. Type
 add snmp remote engine addrtype=ipv4 addr=192.168.1.30 port=xx engine_id=xxxxxx.
8. Define one or more Remote Users by address type. Type:
 **add snmp remote user name=STR_USR_NAME addrtype=ipv4 addr=192.168.1.30 port=55 se-
curity-level={noAuthNoPriv|authNoPriv|authPriv} auth-protocol={md5|sha} password=xxxxxxx**
 priv-protocol={des|aes} password=STR_PRIV_PASS
9. Define one or more Remote Users by the remote engine. Type:
 **add snmp remote user name=STR_USR_NAME engine=STR_ENGINES security-
level=authPriv auth-protocol=md5 password=STR_AUTH_PASS priv-protocol=des**
 password=STR_PRIV_PASS
10. Verify the configuration has been set. Type **show snmp config**.

Appendix D: SOAM Configuration Example – Web Method

This appendix provides a sample SOAM configuration set up via the Web interface.

SOAM Sample Configuration – Web Method

This sample configuration sets up SOAM between two subscriber sites: CPE1 and CPE2 (for illustrative purposes it is managed in the same chassis.) This configuration will allow testing of Y.1731 (UP- MEPs, DOWN-MEPs, MIP, AIS, etc) and 802.1ag (UP- MEPs, DOWN-MEPs and MIPs) and also will help verify nesting rules of Management Domains. This is a typical customer network configuration of devices.

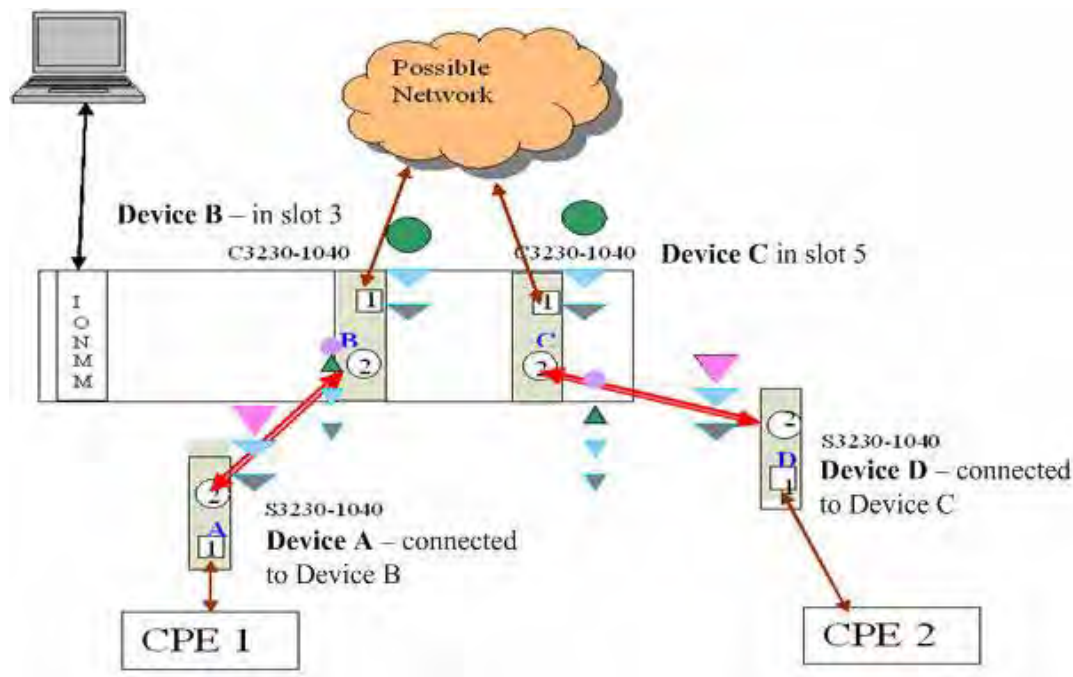


Figure D-1: SOAM Configuration

This sample configuration includes an ION219 chassis, two C3230 NIDs, two S3230 NIDs, an IONMM card, four SFP-SX devices, MMF-6.2/125 optical fiber cable, a CAT.5E patch cable, and a high-speed shielded USB 2.0 cable. The configuration includes:

- 1) Two C3230-S3230 pairs used for SOAM configuration and testing.
- 2) A total of 3 MEG levels configured as specified in this document. Two MEGs will be C-tagged MEGs and one an untagged MEG.
- 3) Devices A and D (S3230s) will have the MEPs at Level 7, devices B and C will have MIPs at Level 4.
- 4) Devices B and C (C3230s) have MEPs and MIPs for operator MEG at Level 3.
- 5) UNI MEG will be configured between A-B, B-C, and C-D.

This sample SOAM configuration assumes that the chassis and devices are installed and cabling is completed.

The MEG level layouts are shown below:

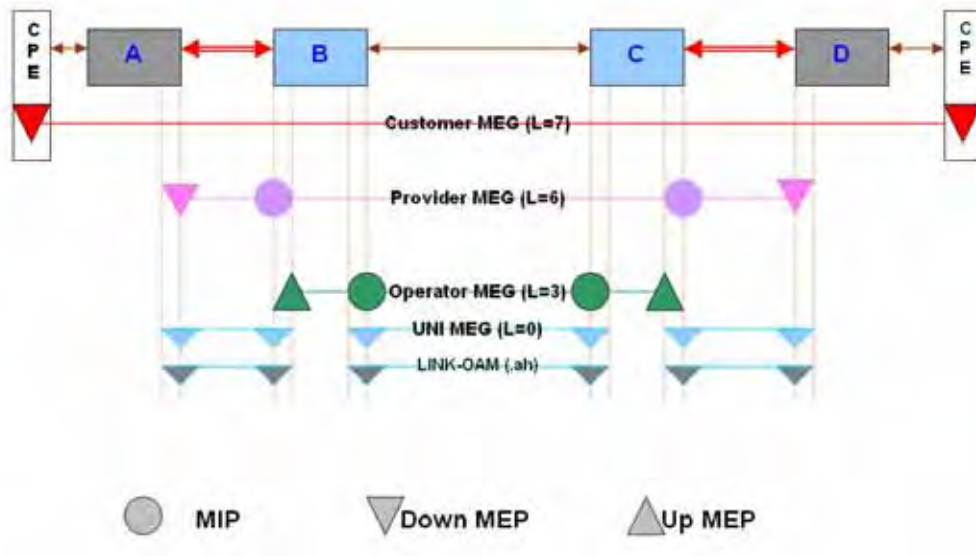


Figure D-2: MEG Level Layouts

IEEE 802.1ag Configuration

The sample configuration using IEEE 802.1ag is shown below.

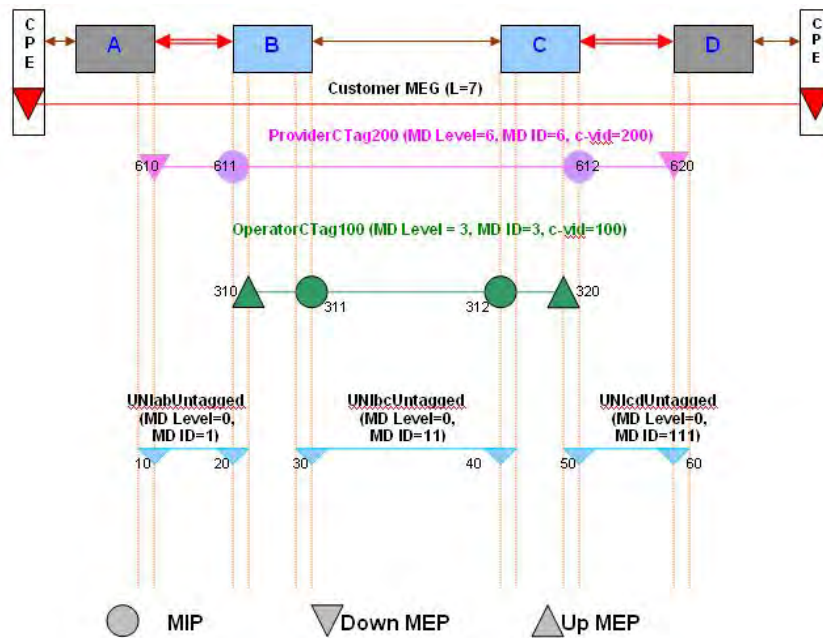


Figure D-3: IEEE 802.1ag Test Configuration

The ION system configuration is shown below.

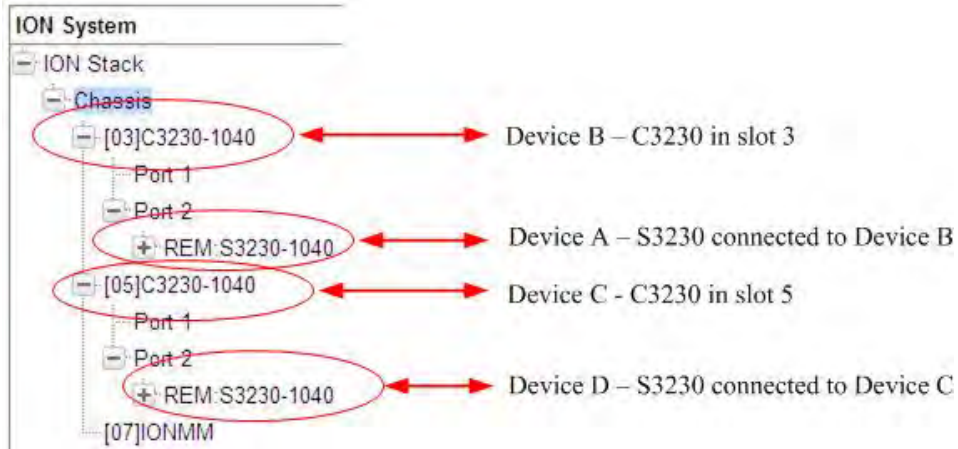


Figure D-4: ION Chassis / Device Configuration

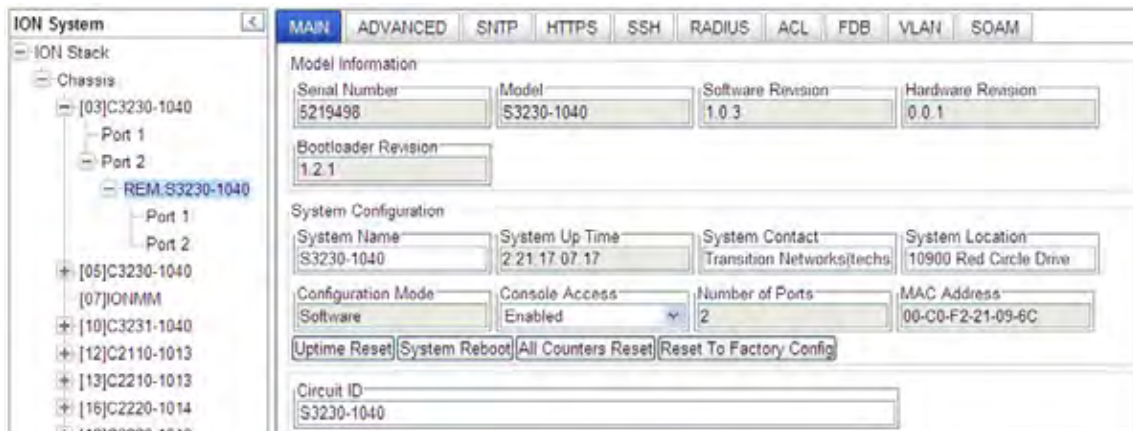
The following sections document the configuration of SOAM MD/MAs, MEGs, MEPs, and MIPs for Devices A, B, C, and D via the Web method. Sample procedures are provided for configurations based on both the IEEE 802.1ag standard and the ITU-T Y.1731 standard.

SOAM Web Config - IEEE 802.1ag Standard – Device A

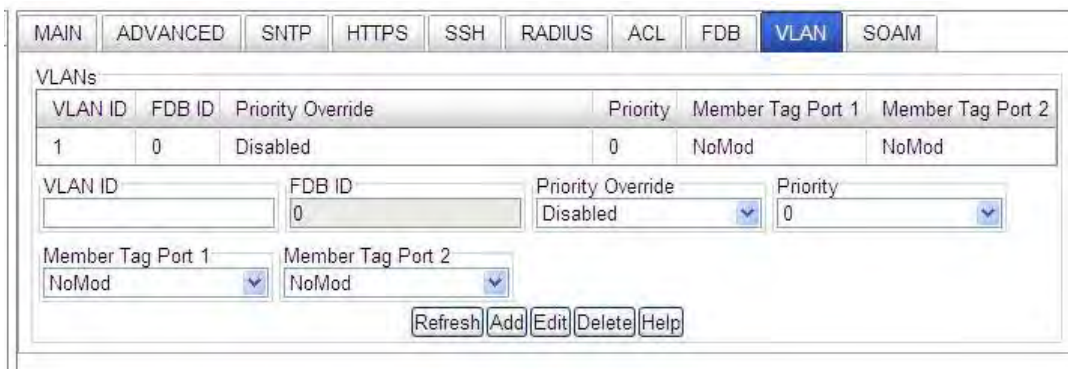
This procedure configures Device A (S3230-1040 at CPE 1):

Device A	Level 0 UNI	Level 6 Provider MD
MA ID	1	6
MD ID	1	6
MD Name	UNIabMD	ProviderMD
MA Name	UNIabUntagged	ProviderCTag200
VLAN Type	none	ctype 200
Level	0	6
MEP ID	10, 20	610, 620
Direction	Down Port 2	Down Port 2
CCI	enabled	enabled

1. Access Device A (C3230 at CPE 1) through the Web interface (see “Starting the Web Interface” on page 45 of the x323x NID User Guide). The **MAIN** tab displays.



2. Select the **VLAN** tab.



3. In the **VLAN ID** field enter **200**. At **Priority Override** select **Disabled**. At **Priority** select **0**. At **Member Tag Port 1** select **Tag**. At **Member Tag Port 2** select **UnTag**. Click **Add**. Click **Refresh** and verify the VLANs table for Device A:

MAIN	ADVANCED	SNTP	HTTPS	SSH	RADIUS	ACL	FDB	VLAN	SOAM
------	----------	------	-------	-----	--------	-----	-----	-------------	------

VLANs

VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2
1	0	Disabled	0	NoMod	NoMod
200	0	Disabled	0	Tag	Tag

VLAN ID: FDB ID: Priority Override: Priority:

Member Tag Port 1: Member Tag Port 2:

4. Select the **SOAM** tab.

5. At the **MD** sub-tab, define the first maintenance domain (MD) for Device A:

- a. In the **MD ID** field, enter *1* as the ID number for the first MD being defined.
- b. In the **Name** field, enter *UNlabMD* as the name for this maintenance domain.
- c. In the **Level** field, select *0* for the level this maintenance domain is associated with.
- d. In the **Sender ID permission** field, select *None* for the permission that will be sent with each transmission. This indicates what, if anything, is to be included in the Sender ID TLV transmitted by MPs configured in this MD. Valid selections are **None**, **Chassis ID**, **Manage**, and **Chassis ID and Manage**. For this example, leave the setting at the default value (**None** - the Sender ID TLV is not to be sent).
- e. Click **Add**. The first MD is defined in the table (shown below).

MAIN	ADVANCED	SNTP	HTTPS	SSH	RADIUS	ACL	FDB	VLAN	SOAM
------	----------	------	-------	-----	--------	-----	-----	------	-------------

Main Configuration **MD** MA/MEG MEP MIP Configuration Error List

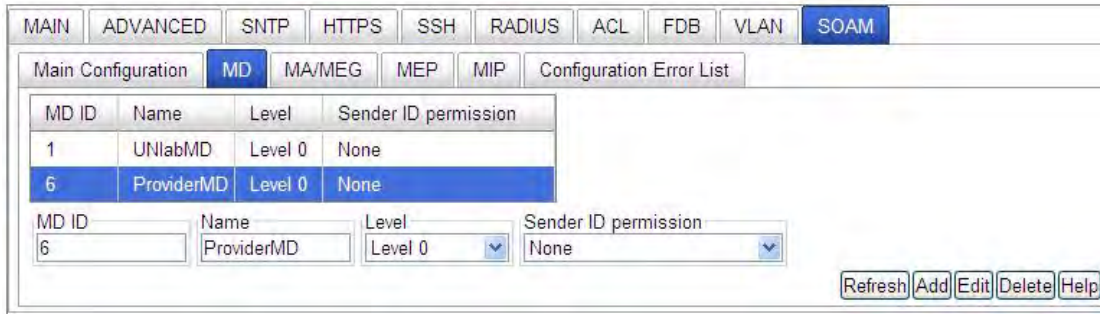
MD ID	Name	Level	Sender ID permission
1	UNlabMD	Level 0	None

MD ID: Name: Level: Sender ID permission:

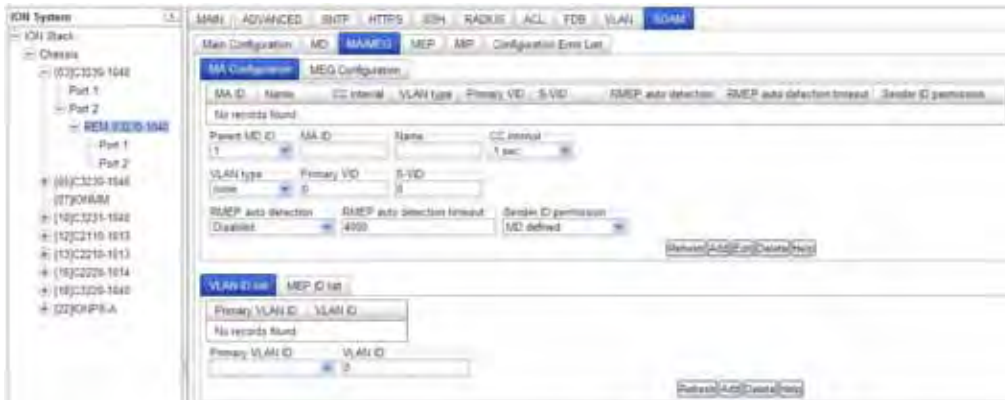
6. At the **MD** sub-tab, define a second MD:

- a. In the **MD ID** field, enter *6* as the ID number.
- b. In the **Name** field, enter *ProviderMD*.
- c. In the **Level** field, select *0*.
- d. In the **Sender ID permission** field, leave the setting at the default value (**None** - the Sender ID TLV is not to be sent).

- e. Click **Add**. The **second** MD is defined.
- 7. Click **Refresh** and verify the MD ID table:

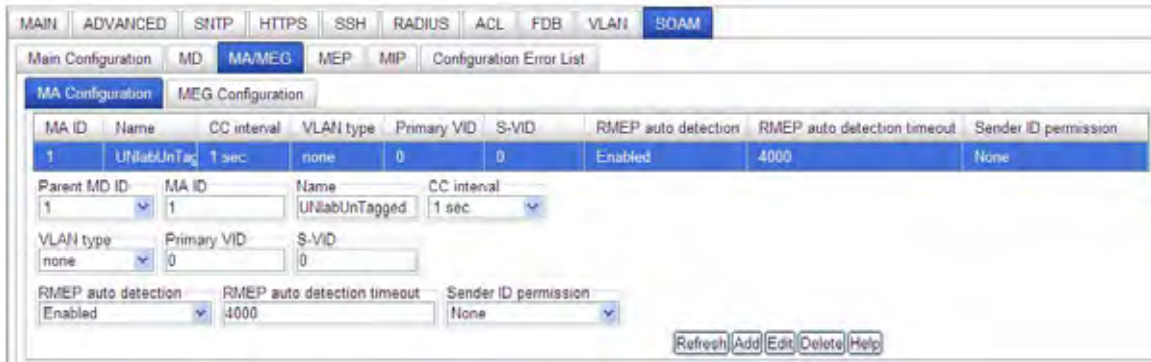


- 8. At the **MA/MEG** tab's **MA Configuration** sub-tab, define a maintenance association (MA ID 1) for MD ID 1 for Device A:

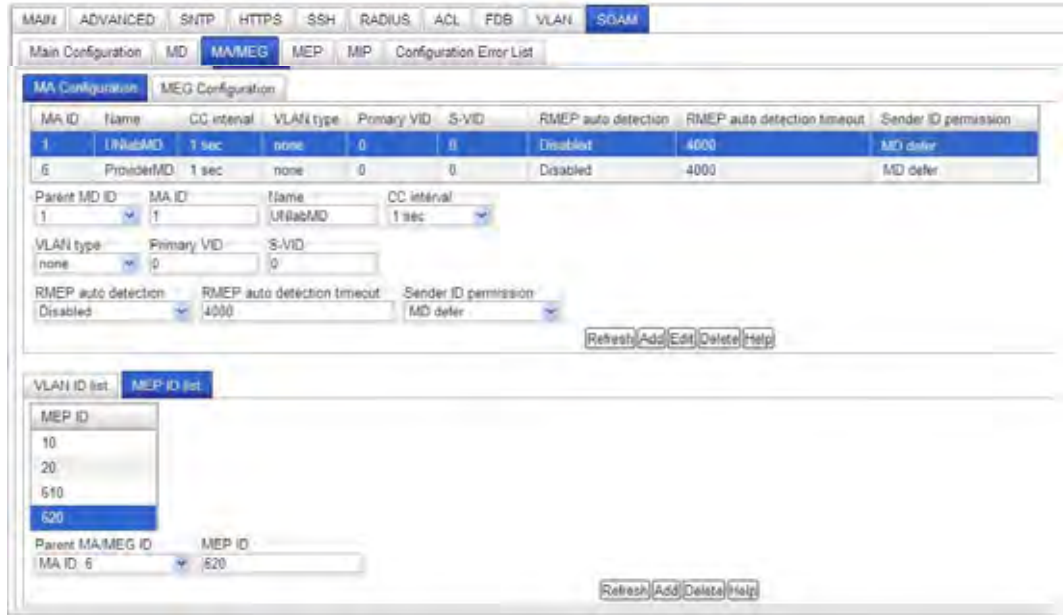


- 9. In the **Parent MD ID** field, select 1 as the MD to which this MA will be associated.
- 10. In the **MA ID** field, enter an ID number of **1** for this MA.
- 11. In the **Name** field, enter a name for this MA. This is the Short Maintenance Association name; it must be unique within a maintenance domain. Enter **UNlabUntagged**.
- 12. In the **CC interval** field, select the interval at which Continuity Check Messages (CCMs) will be sent. This is the interval between CCM transmissions to be used by all MEPs in the MA. The valid selections are **3.3ms, 10ms, 100ms, 1s, 10s, 1min, and 10min**. The default is **1 second**. For this example, leave the setting at the default value (**1 second**).
- 13. In the **VLAN type** field, select **None** to specify no VLAN.
- 14. In the **Primary VID** and **S-VID** fields, leave at the default settings (**0**).
- 15. In the **RMEP auto detection** field, select **Enabled** if **remote** MEPs will be detected automatically, or select **Disabled** if **remote** MEPs are to be explicitly defined.
- 16. In the **RMEP auto detection timeout** field, leave at the default setting (**4000**).

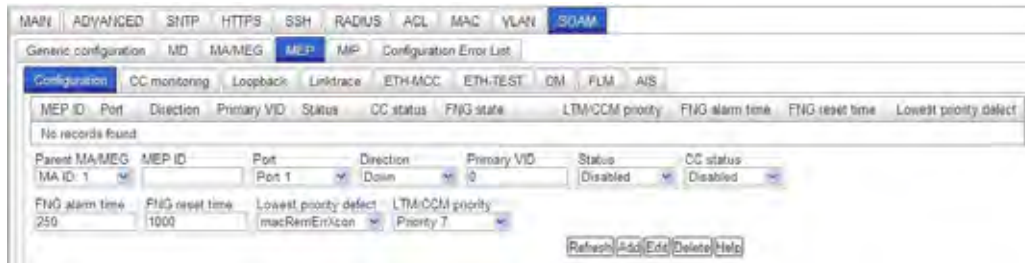
17. In the **Sender ID permission** field, leave the setting at the default value (**None** - the Sender ID TLV is not to be sent).
18. Leave the **Primary VLAN ID** field and **VLAN ID** field at the default settings (**blank** and **0**).
19. Click **Add**. The first MA is added for Device A:



20. At the **MA/MEG** tab, define MA ID 6 for MD ID 6 for Device A:
 - a. In the **Parent MD ID** field, select **6**.
 - b. In the **MA ID** field, enter **6**.
 - c. In the **Name** field, enter **ProviderCTag200**.
 - d. In the **CC interval** field, leave the setting at the default value (**1 second**).
 - e. In the **VLAN type** field, select **ctype**.
 - f. In the **Primary VID** field, enter **200**.
 - g. In the **S-VID** field, leave at the default settings (**0**) and then click **Add**.
21. At the **VLAN ID list** tab, at **Primary VLAN ID** select **MA PVID 100**. At **VLAN ID** enter **100**. Click **Add**.
22. At **Primary VLAN ID** select **MA PVID 200**. At **VLAN ID** enter **200**. Click **Add**.
23. Select the **MEP ID list** sub-tab.
 - a. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **VLAN ID** field enter **610** and click **Add**.
 - b. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **VLAN ID** field enter **620** and click **Add**.
 - c. In the **Parent MA/MEG ID** field select **MA ID: 1**. In the **VLAN ID** field enter **10** and click **Add**.
 - d. In the **Parent MA/MEG ID** field select **MA ID: 1**. In the **VLAN ID** field enter **20** and click **Add**.
24. Verify the **SOAM > MA/MEG > MA Configuration** for Device A:



25. Select the **SOAM > MEP > Configuration** sub-tab.



26. Define MEP ID 610 and 620 for Device A:

- a. Define MEP ID 610 for MA ID 6. At the bottom left, select the **MEP ID** list tab, and enter: **Parent MA/MEG = MA ID 1, MEP ID = 610, Port = 2, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Disabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.
- b. Define MEP ID 620 for MA ID 6: **Parent MA/MEG = MA ID 1, MEP ID = 620, Port = 2, Direction = Down, Primary VID = none, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.
- c. Define MEP ID 10 for MA ID 1. At the bottom left, select the **MEP ID** list tab, and enter: **Parent MA/MEG = MA ID 1, MEP ID = 10, Port = 2, Direction = Down, Primary VID = 200, Status = Enabled, CC status = Disabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.

Appendix D: SOAM Configuration Example – CLI Method

- d. Define MEP ID 20 for MA ID 1: **Parent MA/MEG = MA ID 1, MEP ID = 20, Port = 2, Direction = Down, Primary VID = 200, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.

27. Verify your **SOAM MEP Configuration** selections for Device A.

MEP ID	Port	Direction	Primary VID	Status	CC status	FNG state	LTM/CCM priority	FNG alarm time	FNG reset time	Lowest priority defect
10	Port 2	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrXcon
20	Port 1	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrXcon

Parent MA/MEG	MEP ID	Port	Direction	Primary VID	Status	CC status
MA ID: 6	610	Port 2	Down	200	Enabled	Enabled

FNG alarm time	FNG reset time	Lowest priority defect	LTM/CCM priority
250	1000	macRemErrXcon	Priority 0

Refresh Add Edit Delete Help

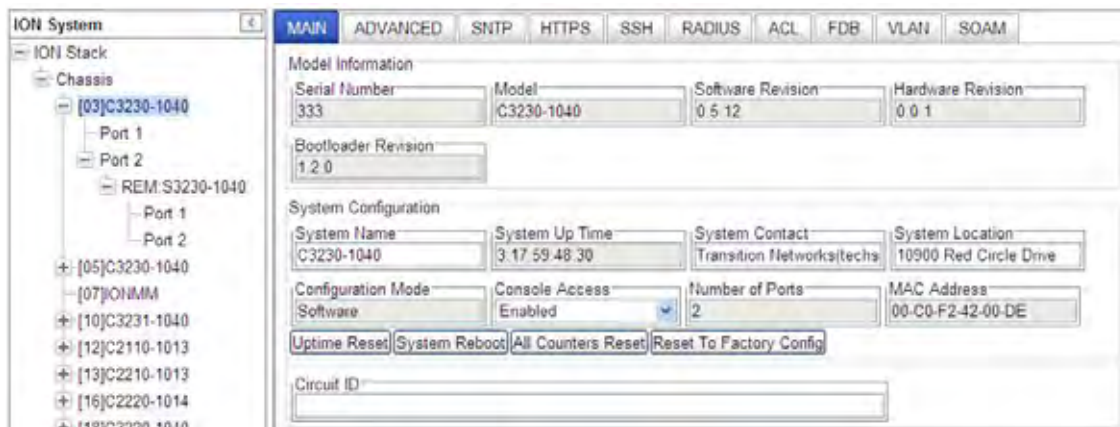
Device A is configured; continue with Device B configuration below.

SOAM Web Config - IEEE 802.1ag Standard – Device B

This procedure configures Device B (C3230-1040 in ION Chassis slot 3):

Device B	Level 0 UNI	Level 0 UNI	Level 3 OperatorMD	Level 6 ProviderMD
MA ID	1	11	3	6
MD ID	1	11	3	6
MD Name	UNIabMD	UNIbcMD	OperatorMD	ProviderMD
MA Name	UNIabUntagged	UNIbcUntagged	OperatorCTag100	ProviderCTag200
VLAN Type	none	none	ctype 100	ctype 200
Level	0	6	3	6
MEP ID	10, 20	30	310, 320	
Direction	Down Port 2	Down Port 1	Up Port 2	
CCI	enabled	enabled	enabled	
MEP Local Parent ID	11		3	6 – port 2
MIP Type			802.1ag	802.1ag
MIP ID			312	612
MIP Local Parent ID - Port			3 – port 1	6 – port 2

1. Access Device B (C3230 in ION Chassis slot 3) through the Web interface. The **MAIN** tab displays.



2. Select the **VLAN** tab. In the **VLAN ID** field enter **100**. At **Priority Override** select **Disabled**. At **Priority** select **0**. At **Member Tag Port 1** select **Tag**. Click **Add**.
3. At **Member Tag Port 2** select **UnTag**. Click **Add**. Click **Refresh** and verify the VLANs table:

MAIN	ADVANCED	SNTF	HTTPS	SSH	RADIUS	ACL	FDB	VLAN	SOAM
------	----------	------	-------	-----	--------	-----	-----	-------------	------

VLANs

VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2
1	0	Disabled	0	NoMod	NoMod
100	0	Disabled	0	Tag	UnTag
200	0	Disabled	0	Tag	UnTag

VLAN ID: 200 FDB ID: 0 Priority Override: Disabled Priority: 0

Member Tag Port 1: Tag Member Tag Port 2: UnTag

Refresh Add Edit Delete Help

4. Select the **SOAM** tab.

MAIN	ADVANCED	SNTF	HTTPS	SSH	RADIUS	ACL	FDB	VLAN	SOAM
------	----------	------	-------	-----	--------	-----	-----	------	-------------

Main Configuration **MD** MA/MEG MEP MIP Configuration Error List

MD ID	Name	Level	Sender ID permission
No records found.			

MD ID: Name: Level: Level 0 Sender ID permission: None

Refresh Add Edit Delete Help

5. At the **MD** sub-tab, define the first maintenance domain (MD) for Device B:

- In the **MD ID** field, enter **1** as the ID number for the first MD being defined.
- In the **Name** field, enter **UNlabMD** as the name for this maintenance domain.
- In the **Level** field, select 0 for the level this maintenance domain is associated with.
- In the **Sender ID permission** field, leave the setting at the default value (**None** - the Sender ID TLV is not to be sent).
- Click **Add**. The first MD is defined in the table (shown below).

MAIN	ADVANCED	SNTF	HTTPS	SSH	RADIUS	ACL	FDB	VLAN	SOAM
------	----------	------	-------	-----	--------	-----	-----	------	-------------

Main Configuration **MD** MA/MEG MEP MIP Configuration Error List

MD ID	Name	Level	Sender ID permission
1	UNlabMD	Level 0	None

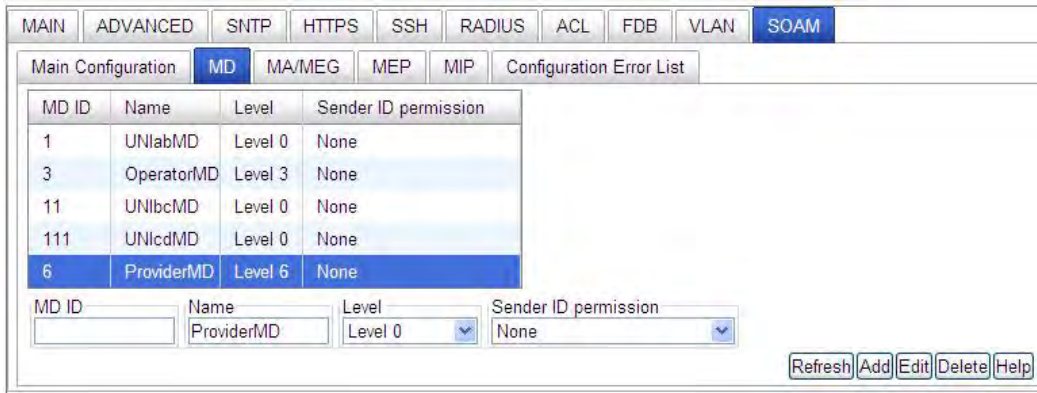
MD ID: 1 Name: UNlabMD Level: Level 0 Sender ID permission: None

Refresh Add Edit Delete Help

6. At the **MD** sub-tab, define a second MD:

- In the **MD ID** field, enter **6** as the ID number.
- In the **Name** field, enter **ProviderMD**.
- In the **Level** field, select **6**.

- d. In the **Sender ID permission** field, leave the setting at the default value (*None* - the Sender ID TLV is not to be sent).
- e. Click **Add**. The second MD is defined.
7. Define a third MD: Enter **MD ID = 11**, **Name = UNIbcMD**, **Level = 0**, **SenderID permission = 0** and click **Add**.
8. Define a fourth MD: Enter **MD ID = 3**, **MD = OperatorMD**, **Level = 3**, **SenderID permission = 0** and click **Add**.
9. Click **Refresh** and verify the MD ID table:

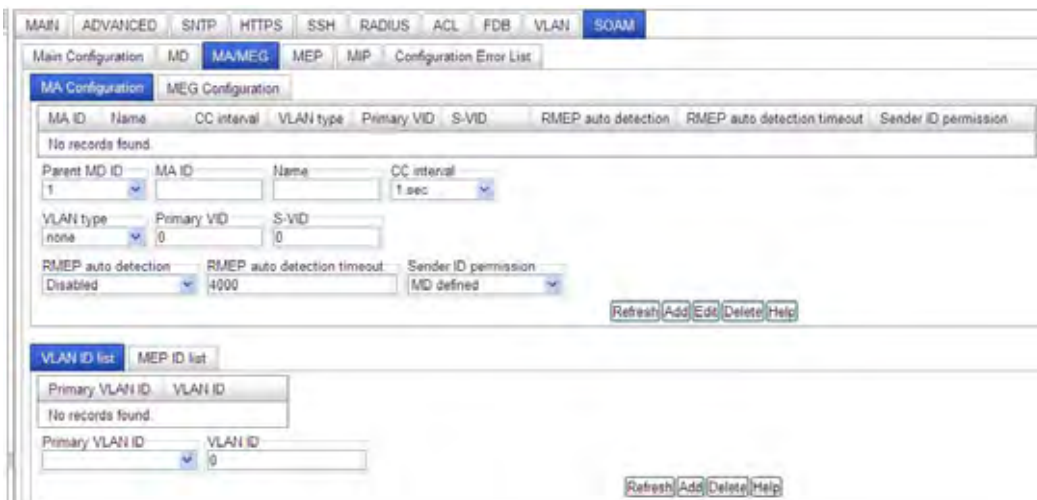


The screenshot shows the SOAM configuration page with the MD ID table. The table has the following data:

MD ID	Name	Level	Sender ID permission
1	UNlabMD	Level 0	None
3	OperatorMD	Level 3	None
11	UNIbcMD	Level 0	None
111	UNlcdMD	Level 0	None
6	ProviderMD	Level 6	None

Below the table, there are input fields for MD ID, Name (ProviderMD), Level (Level 0), and Sender ID permission (None). Buttons for Refresh, Add, Edit, Delete, and Help are visible at the bottom right.

10. At the **MA/MEG** tab's **MA Configuration** sub-tab, define a maintenance association (MA ID 1) for MD ID 1 for Device B.



The screenshot shows the MA Configuration sub-tab. The MA ID field is set to 1. The Parent MD ID field is set to 1. The Name field is set to UNlabUntagged. The CC interval is set to 1 sec. The RMEP auto detection is set to Disabled, and the RMEP auto detection timeout is set to 4000. The Sender ID permission is set to MD defined. Buttons for Refresh, Add, Edit, Delete, and Help are visible at the bottom right.

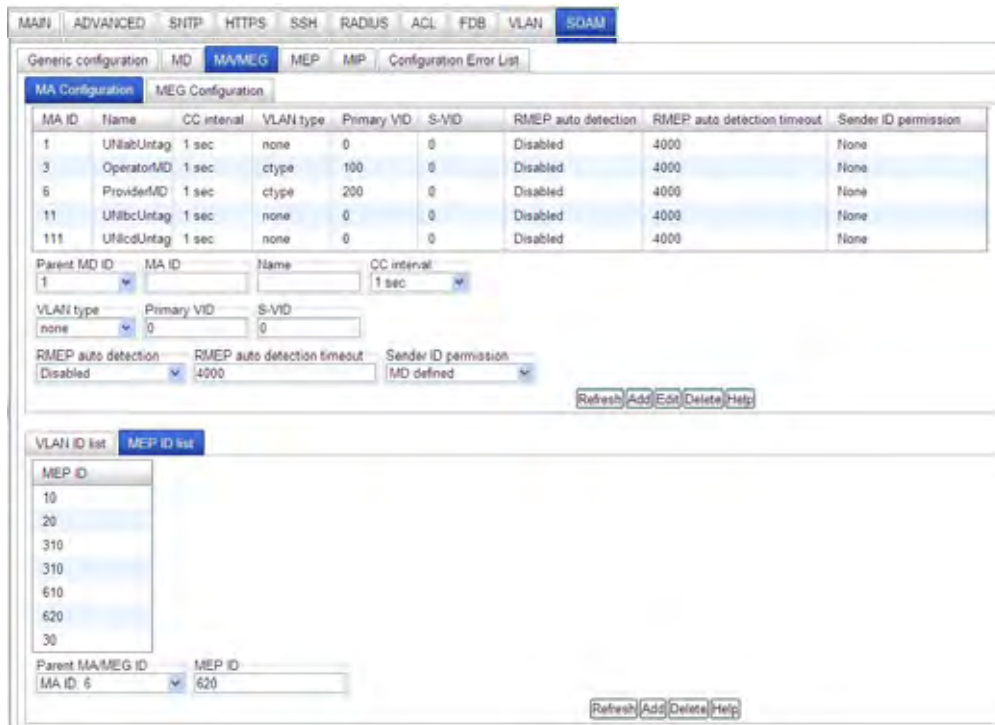
11. In the **Parent MD ID** field, select 1 as the MD to which this MA will be associated.
12. In the **MA ID** field, enter an ID number of *1* for this MA.
13. In the **Name** field, enter a name for this maintenance association. This is the Short Maintenance Association name; it must be unique within a maintenance domain. Enter *UNlabUntagged*.

14. In the **CC interval** field, leave the setting at the default value (**1 second**).
15. In the **VLAN type** field, select **None** to specify no VLAN.
16. In the **Primary VID** and **S-VID** fields, leave at the default settings (**None** and **0**).
17. In the **RMEP auto detection** field, select **Enabled** if remote MEPs will be detected automatically, or select **Disabled** if remote MEPs must be explicitly defined.
18. In the **RMEP auto detection timeout** field, leave at the default setting (**4000**).
19. In the **Sender ID permission** field, leave the setting at the default value (**None** - the Sender ID TLV is not to be sent).
20. Leave the **Primary VLAN ID** field and **VLAN ID** field at the default settings (**blank** and **0**).
21. Click **Add**. The first MA is added for Device B.



22. At the **MA/MEG** tab, define MA ID 6 for MD ID 6 for Device B:
 - a. In the **Parent MD ID** field, select **6**.
 - b. In the **MA ID** field, enter **6**.
 - c. In the **Name** field, enter **ProviderCTag200**.
 - d. In the **CC interval** field, leave the setting at the default value (**1 second**).
 - e. In the **VLAN type** field, select **ctype**.
 - f. In the **Primary VID** field, enter **200**.
 - g. In the **S-VID** field, leave at the default settings (**0**) and then click **Add**.
23. At the **MA/MEG** tab, define MA ID 3 for MD ID 3: **Parent MD ID = 3, MA ID =3, Name = OperatorMD, CC interval = 1 sec, VLAN type = ctype, Primary VID = 100, and S-VID = 0**. Click **Add**. The MA is added.
24. At the **MA/MEG** tab, define MA ID 1 for MD ID 1: **Parent MD ID = 1, MA ID = 1, Name = UNlabUntagged, CC interval = 1 sec, VLAN type = none, Primary VID = 0, and S-VID = 0**. Click **Add**. The MA is added.

25. At the **MA/MEG** tab, define MA ID 11 for MD ID 11: **Parent MD ID = 11, MA ID = 11, Name = UNIbcUntagged, CC interval = 1 sec, VLAN type = none, Primary VID = 0, and S-VID = 0.** Click **Add**. The MA is added.
26. At the **VLAN ID list** tab, at **Primary VLAN ID** select **MA PVID 100**. At **VLAN ID** enter **100**. Click **Add**.
27. At **Primary VLAN ID** select **MA PVID 200**. At **VLAN ID** enter **200**. Click **Add**.
28. Select the **MEP ID list** sub-tab.
 - a. In the **Parent MA/MEG ID** field select **MA ID: 1**. In the **VLAN ID** field enter **10** and click **Add**.
 - b. In the **Parent MA/MEG ID** field select **MA ID: 1**. In the **VLAN ID** field enter **20** and click **Add**.
 - c. In the **Parent MA/MEG ID** field select **MA ID: 3**. In the **VLAN ID** field enter **310** and click **Add**.
 - d. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **VLAN ID** field enter **610** and click **Add**.
 - e. In the **Parent MA/MEG ID** field select **MA ID: 11**. In the **VLAN ID** field enter **30** and click **Add**.
29. Verify the **SOAM > MA/MEG > MA Configuration** for Device B.



30. Select the **SOAM > MEP > Configuration** sub-tab.



31. Define MEP ID 10, 20, 30, 310 and 320 for Device B:

- e. Define MEP ID 10 for MA ID 1. At the bottom left, select the **MEP ID** list tab, define MEP ID 10 for MA ID 1: **Parent MA/MEG = MA ID 1, MEP ID = 10, Port = 1, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Disabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.
- f. Define MEP ID 20 for MA ID 1: **Parent MA/MEG = MA ID 1, MEP ID = 20, Port = 2, Direction = Down, Primary VID = none, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.
- g. Define MEP ID 30 for MA ID 11: **Parent MA/MEG = MA ID 11, MEP ID = 30, Port = 1, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.
- h. Define MEP ID 310 for MA ID 3: **Parent MA/MEG = MA ID 3, MEP ID = 310, Port = 2, Direction = Up, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.
- i. Define MEP ID 320 for MA ID 3: **Parent MA/MEG = 3, MEP ID = 320, Port = 2, Direction = Up, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click **Add**.

32. Verify your **SOAM MEP Configuration** selections for Device B.

MEP ID	Port	Direction	Primary VID	Status	CC status	FNG state	LTM/CCM priority	FNG alarm time	FNG reset time	Lowest priority defect
10	Port 1	Down	0	Enabled	Disabled	Defect reported	0	250	1000	macRemEnXcon
20	Port 2	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemEnXcon
310	Port 2	Up	0	Enabled	Enabled	Reset	0	250	1000	macRemEnXcon

33. At **SOAM > MIP** add new MIPs to the Device B configuration.

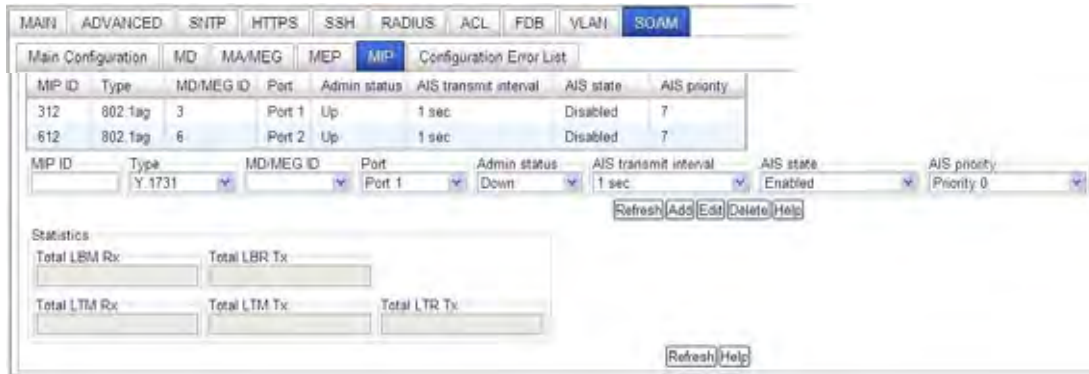
MIP ID	Type	MD/MEG ID	Port	Admin status	AIS transmit interval	AIS state	AIS priority
No records found.							

- a. In the **MIP ID** field, enter ID **311** for this MIP.
 In the **Type** field, select 802.1ag.
 In the **MD/MEG ID** field, enter **3** for the MD ID.
 In the **Port** field, enter **1**.
 In the **Admin status** field, select **Up** as the Administrative state of the MIP.
 Leave the **AIS transmit interval** field, the **AIS state** field, and the **AIS priority** field at the defaults.

- b. In the **MIP ID** field, enter ID **611** for this MIP.
 In the **Type** field, select 802.1ag.
 In the **MD/MEG ID** field, enter **6** for the ID of the MD.
 In the **Port** field, enter **2**.
 In the **Admin status** field, select **Up** as the Administrative state of the MIP.
 Leave the **AIS transmit interval** field, the **AIS state** field, and the **AIS priority** field at the defaults.

- c. Click **Add**.

- d. Click **Refresh**. Verify your SOAM MIP selections for Device C.



Device B is configured; continue with Device C configuration below.

SOAM Web Config - IEEE 802.1ag Standard – Device C

This procedure configures Device C (C3230-1040 in ION Chassis slot 5):

Device C	Level 0 UNI	Level 0 UNI	Level 3 OperatorMD	Level 6 ProviderMD
MA ID	11	111	3	6
MD ID	11	11	3	6
MD Name	UNIbcMD	UNIdcMD	OperatorMD	ProviderMD
MA Name	UNIbcUntagged	UNIdcUntagged	OperatorCTag100	ProviderCTag200
VLAN Type	none	none	Ctype 100	ctype 200
Level	0	6	0	6
MEP ID	30, 40	50, 60	310, 320	
Direction	Down Port 1	Down Port 2	Up Port 2	
CCI	enabled	enabled	enabled	
MEP Local Parent ID	11	111	3	
MIP Type			802.1ag	802.1ag
MIP ID			311, 312	612
MIP Local Parent ID - Port			3 – port 1	6 – port 2

1. Access Device C (C3230 in ION Chassis slot 5) through the Web interface. The **MAIN** tab displays.
2. Select the **VLAN** tab.

In the **VLAN ID** field enter *100*. At **Priority Override** select *Disabled*. At **Priority** select *0*. At **Member Tag Port 1** select *Tag*. At **Member Tag Port 2** select *UnTag*. Click **Add**. VLAN ID 100 is added.

In the **VLAN ID** field enter *200*. At **Priority Override** select *Disabled*. At **Priority** select *0*. At **Member Tag Port 1** select *Tag*. At **Member Tag Port 2** select *UnTag*. Click **Add**. VLAN ID 200 is added.

Click **Refresh** and verify the VLANs table:



3. Select the **SOAM** tab. At the **MD** sub-tab, define MD ID 3, 6, 11, and 111 for Device C:
 Enter **MD ID = 3**, Name = OperatorMD, Level = 0, SenderID permission = 0 and click **Add**.
 Enter **MD ID = 6**, Name = ProviderMD, Level = 0, SenderID permission = 0 and click **Add**.
 Enter **MD ID = 11**, Name = UNIbcMD, Level = 0, SenderID permission = 0 and click **Add**.
 Enter **MD ID = 111**, Name = UNIcdMD, Level = 0, SenderID permission = 0 and click **Add**.
4. Click **Refresh** and verify the MD ID table for Device C:

MD ID	Name	Level	Sender ID permission
3	OperatorMD	Level 0	None
6	ProviderMD	Level 0	None
11	UNIbcMD	Level 0	None
111	UNIcdMD	Level 0	None

MD ID: 111, Name: UNIcdMD, Level: Level 0, Sender ID permission: None

Buttons: Refresh, Add, Edit, Delete, Help

5. At the **MA/MEG** tab's **MA Configuration** sub-tab, define MA ID 3, 6, 11, and 111 for Device C:

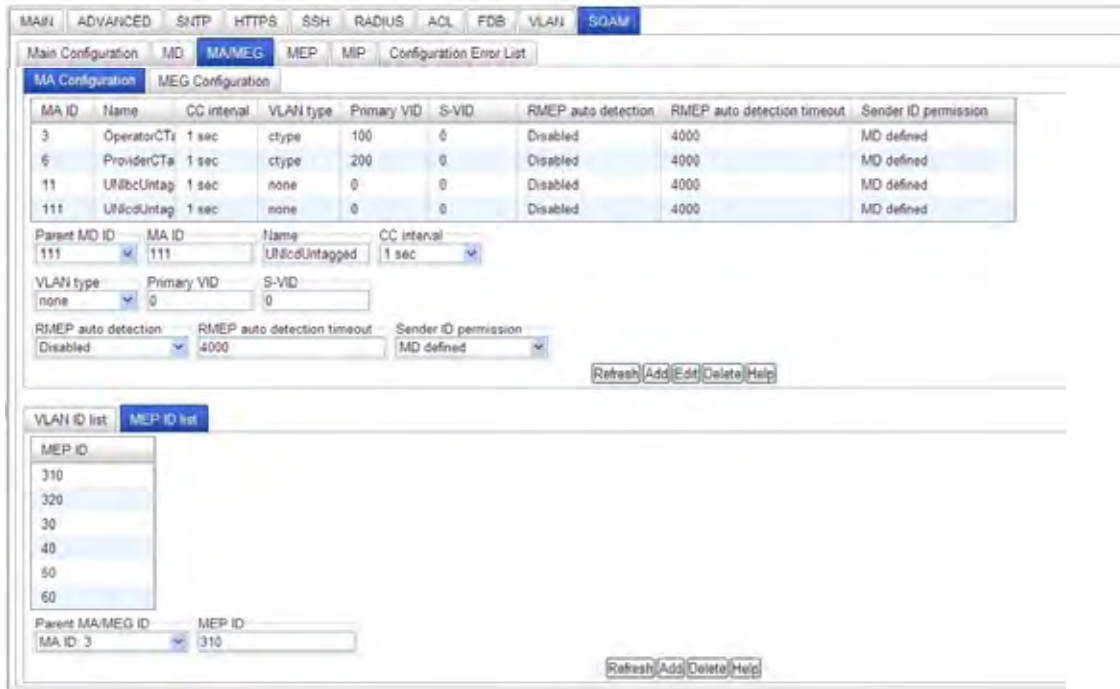
 For MA ID 3, enter: **Parent MD ID = 3**, **MA ID = 3**, **Name = OperatorCTag100**, **CC interval = 1 sec**, **VLAN type = ctype**, **Primary VID = 100**, and **S-VID = 0**. Click **Add**. The MA is added.

 For MA ID 6, enter: **Parent MD ID = 6**, **MA ID = 6**, **Name = ProviderCTag200**, **CC interval = 1 sec**, **VLAN type = ctype**, **Primary VID = 200**, and **S-VID = 0**. Click **Add**. The MA is added.

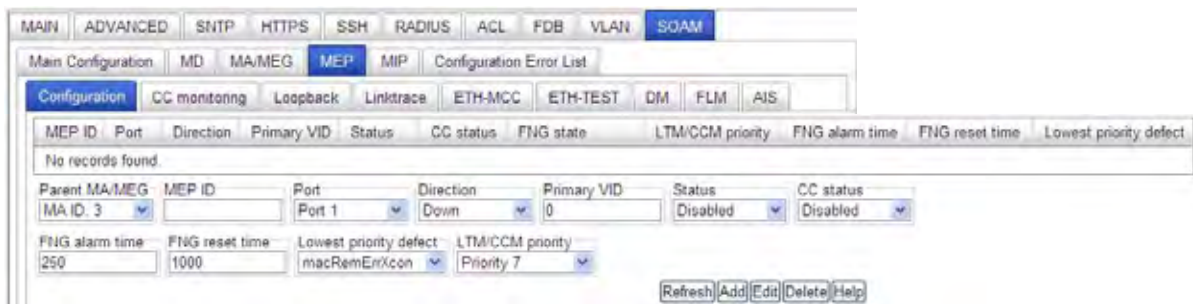
 For MA ID 11, enter: **Parent MD ID = 11**, **MA ID = 11**, **Name = UNIbcUntagged**, **CC interval = 1 sec**, **VLAN type = none**, **Primary VID = 0**, and **S-VID = 0**. Click **Add**. The MA is added.

 For MA ID 111, enter: **Parent MD ID = 111**, **MA ID = 111**, **Name = UNIcdUntagged**, **CC interval = 1 sec**, **VLAN type = none**, **Primary VID = 0**, and **S-VID = 0**. Click **Add**. The MA is added.
6. At the **VLAN ID list** tab, at **Primary VLAN ID** select **MA PVID 100**. At **VLAN ID** enter **100**. Click **Add**.
7. At **Primary VLAN ID** select **MA PVID 200**. At **VLAN ID** enter **200**. Click **Add**.
8. Select the **MEP ID list** sub-tab.
 - a. In the **Parent MA/MEG ID** field select **MA ID: 3**. In the **MEP ID** field enter **320** and click **Add**.
 - b. In the **Parent MA/MEG ID** field select **MA ID: 3**. In the **MEP ID** field enter **310** and click **Add**.
 - c. In the **Parent MA/MEG ID** field select **MA ID: 11**. In the **MEP ID** field enter **30** and click **Add**.

- d. In the **Parent MA/MEG ID** field select *MA ID: 11*. In the **MEP ID** field enter *40* and click **Add**.
 - e. In the **Parent MA/MEG ID** field select *MA ID: 111*. In the **MEP ID** field enter *50* and click **Add**.
 - f. In the **Parent MA/MEG ID** field select *MA ID: 111*. In the **MEP ID** field enter *60* and click **Add**.
9. Click **Refresh** and verify the **SOAM > MA/MEG > MA Configuration** for Device C:



10. Select **SOAM > MEP > Configuration** and define MEP ID 30, 40, 50, 60, 310, and 320 for Device C:



Appendix D: SOAM Configuration Example – CLI Method

- a. Define MEP ID 30 for MA ID 11: **Parent MA/MEG = 11, MEP ID = 30, Port = 1, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
- b. Define MEP ID 40 for MA ID 11: **Parent MA/MEG = 11, MEP ID = 40, Port = 1, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
- c. Define MEP ID 50 for MA ID 111: **Parent MA/MEG = 111, MEP ID = 50, Port = 2, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
- d. Define MEP ID 60 for MA ID 111: **Parent MA/MEG = 111, MEP ID = 60, Port = 2, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
- e. Define MEP ID 310 for MA ID 3: **Parent MA/MEG = 3, MEP ID = 50, Port = 2, Direction = Up, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
- f. Define MEP ID 320 for MA ID 3: **Parent MA/MEG = 3, MEP ID = 320, Port = 2, Direction = Up, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.

11. Click **Refresh** and verify **SOAM > MEP > Configuration** for Device C.

MEP ID	Port	Direction	Primary VID	Status	CC status	FNG state	LTM/CCM priority	FNG alarm time	FNG reset time	Lowest priority defect
310	Port 2	Up	0	Enabled	Enabled	Reset	0	250	1000	macRemErrXcon
320	Port 1	Up	100	Enabled	Enabled	Reset	7	250	1000	macRemErrXcon
30	Port 1	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrXcon
50	Port 2	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrXcon

Parent MA/MEG	MEP ID	Port	Direction	Primary VID	Status	CC status
MA ID: 111	60	Port 1	Down	0	Enabled	Enabled
FNG alarm time	FNG reset time	Lowest priority defect	LTM/CCM priority			
250	1000	macRemErrXcon	Priority 7			

Refresh Add Edit Delete Help

Select **SOAM > MIP** and define MIP ID 312 and 612 for Device C:

- a. In the **MIP ID** field, enter **312**. In the **Type** field select **802.lag**. In the **MD/MEG ID** field select **MD ID 3**. In the **Port** field, select **Port 2**. In the **Admin** status field, select **Up**. Leave the remaining fields at the default settings. Click **Add**.
- b. In the **MIP ID** field, enter **612**. In the **Type** field select **802.lag**. In the **MD/MEG ID** field select **MD ID 6**. In the **Port** field, select **Port 2**. In the **Admin** status field, select **Up**. Leave the remaining fields at the default settings. Click **Add**.

12. Click **Refresh** and verify the **SOAM > MIP** configuration for Device C.

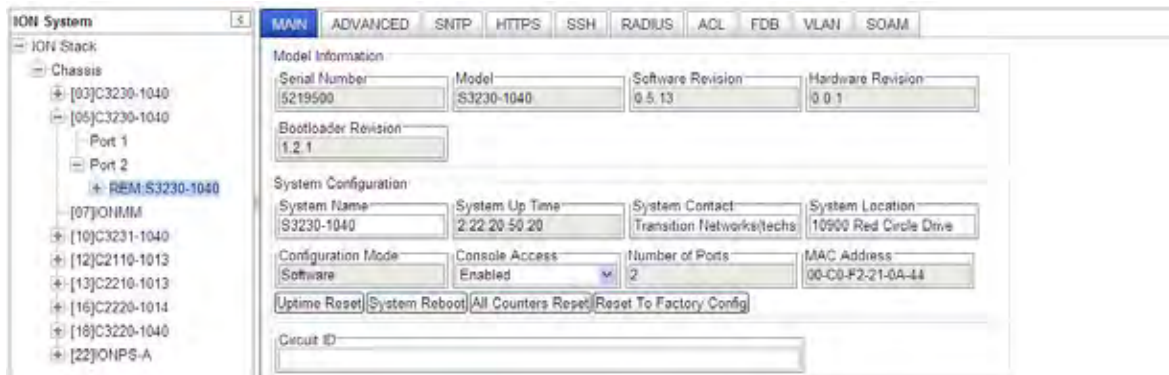
Device C is configured; continue with Device D configuration below.

SOAM Web Config - IEEE 802.1ag Standard – Device D

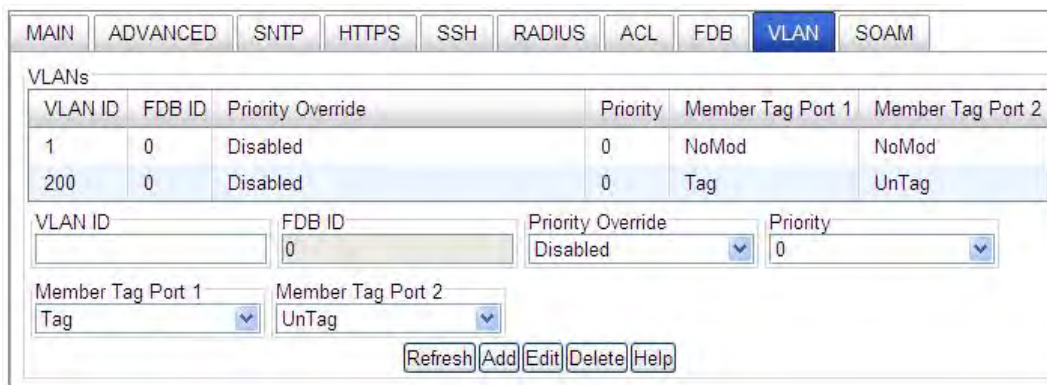
This procedure configures Device D (C3230-1040 at CPE 2):

Device D	Level 0 UNI	Level 6 ProviderMD
MA ID	111	6
MD ID	111	6
MD Name	UNIcdMD	ProviderMD
MA Name	UNIcdUntagged	ProviderCTag200
VLAN Type	none	ctype
Level	0	6
MEP ID	50, 60	610, 620
Direction	Down Port 2	Down Port 2
CCI	enabled	enabled
MEP Local Parent ID	111	6

1. Access Device D (S3230 at CPE 2) through the Web interface. The **MAIN** tab displays.



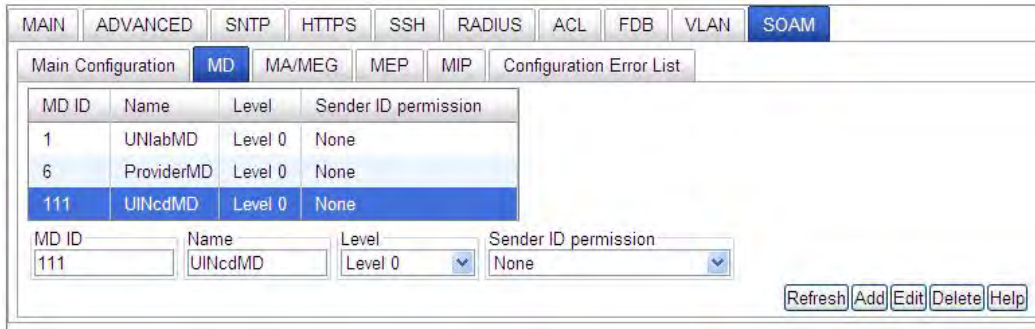
2. At the **VLAN** tab, in the **VLAN ID** field enter **200**. In the **Member Tag Port** field select **Tag**. Click **Add** and verify the **SOAM > VLAN** configuration for Device D.



3. Select the **SOAM** tab. At the **MD** sub-tab, define MD ID 6 and 111 for Device D:
 - a. Enter **MD ID = 6**, **Name = ProviderMD**, **Level = 0**, **SenderID permission = 0** and then click **Add**.

- b. Enter **MD ID = 111**, **Name = UNlCdMD**, **Level = 0**, **SenderID permission = 0** and click **Add**.

- 4. Click **Refresh** and verify the MD ID table for Device C:



The screenshot shows the SOAM configuration page with the MD ID table and configuration fields. The table contains the following data:

MD ID	Name	Level	Sender ID permission
1	UNlabMD	Level 0	None
6	ProviderMD	Level 0	None
111	UNlCdMD	Level 0	None

Below the table, the configuration fields are set as follows:

- MD ID: 111
- Name: UNlCdMD
- Level: Level 0
- Sender ID permission: None

Buttons: Refresh, Add, Edit, Delete, Help

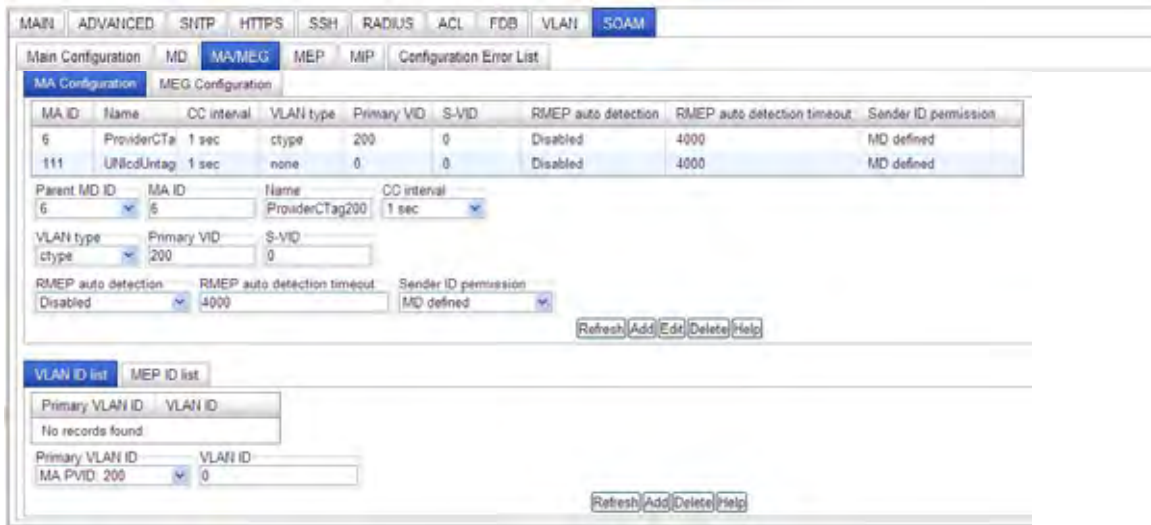
- 5. At the **MA/MEG** tab's **MA Configuration** sub-tab, define MA ID 6 and 111 for Device C:

For MA ID 6, enter: **Parent MD ID = 6**, **MA ID = 6**, **Name = ProviderCTag200**, **CC interval = 1 sec**, **VLAN type = ctype**, **Primary VID = 200**, and **S-VID = 0**. Click **Add**. The MA is added.

For MA ID 111, enter: **Parent MD ID = 111**, **MA ID = 111**, **Name = UNlCdUntagged**, **CC interval = 1 sec**, **VLAN type = none**, **Primary VID = 0**, and **S-VID = 0**. Click **Add**. The MA is added.

- 6. At the **VLAN ID list** tab, at **Primary VLAN ID** select **MA PVID 100**. At **VLAN ID** enter **100**. Click **Add**.
- 7. At **Primary VLAN ID** select **MA PVID 200**. At **VLAN ID** enter **200**. Click **Add**.
- 8. Select the **MEP ID list** sub-tab.
 - a. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **MEP ID** field, enter **610** and click **Add**.
 - b. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **MEP ID** field, enter **620** and click **Add**.
 - c. In the **Parent MA/MEG ID** field select **MA ID: 111**. In the **MEP ID** field, enter **50** and click **Add**.
 - d. In the **Parent MA/MEG ID** field select **MA ID: 111**. In the **MEP ID** field enter **60** and click **Add**.

9. Click **Refresh** and verify the **SOAM > MA/MEG > MA Configuration** for Device D:

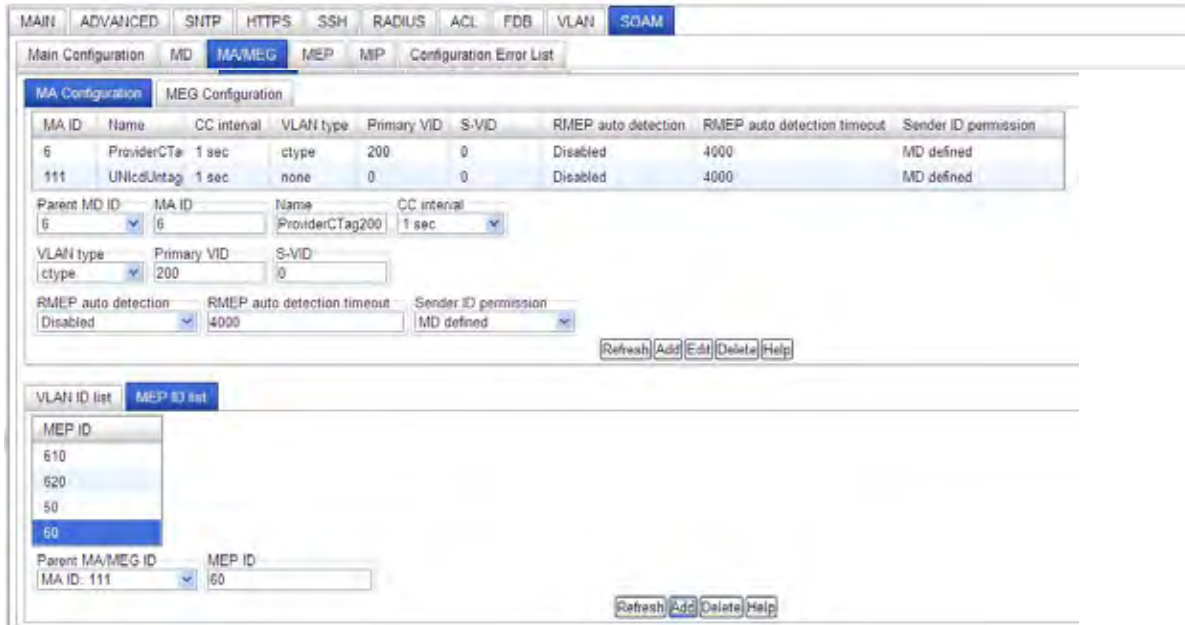


10. At the **VLAN ID list** tab, at **Primary VLAN ID** select **MA PVID 200**. At **VLAN ID** enter **100**. Click **Add**.

11. Select the **MEP ID list** sub-tab.

- a. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **MEP ID** field enter **610** and click **Add**.
- b. In the **Parent MA/MEG ID** field select **MA ID: 6**. In the **MEP ID** field enter **620** and click **Add**.
- c. In the **Parent MA/MEG ID** field select **MA ID: 111**. In the **MEP ID** field enter **50** and click **Add**.
- d. In the **Parent MA/MEG ID** field select **MA ID: 111**. In the **MEP ID** field enter **60** and click **Add**.

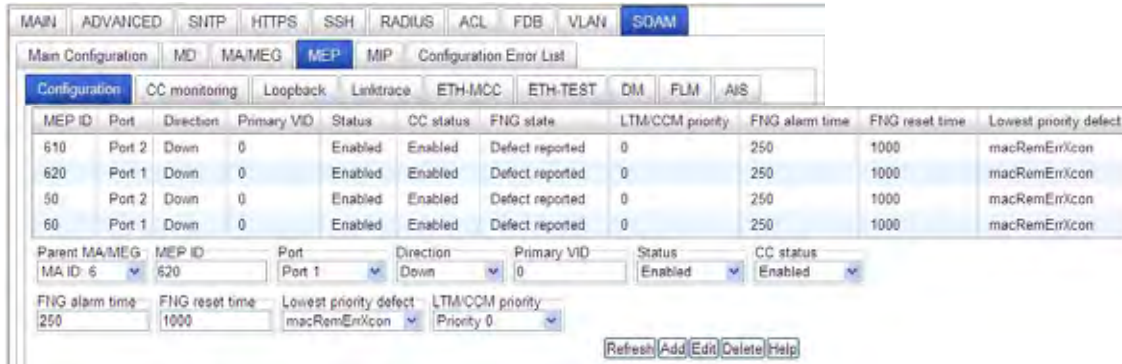
12. Click **Refresh** and verify the **SOAM > MA/MEG > MA Configuration** for Device D:



13. Select **SOAM > MEP > Configuration** and define MEP ID 50, 60, 610, and 620 for Device D:
 - a. Define MEP ID 50 for MA ID 111: **Parent MA/MEG = 111, MEP ID = 50, Port = 2, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
 - b. Define MEP ID 60 for MA ID 111: **Parent MA/MEG = 111, MEP ID = 60, Port = 2, Direction = Down, Primary VID = 0, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
 - c. Define MEP ID 610 for MA ID 6: **Parent MA/MEG = 6, MEP ID = 610, Port = 2, Direction = Down, Primary VID = 200, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.
 - d. Define MEP ID 620 for MA ID 6: **Parent MA/MEG = 6, MEP ID = 620, Port = 2, Direction = Up, Primary VID = 200, Status = Enabled, CC status = Enabled, FNG alarm time = 250, FNG reset time = 1000, Lowest priority defect = macRemErrXcon, LTM/CCM priority = Priority 0.** Click Add.

Appendix D: SOAM Configuration Example – CLI Method

13. Click **Refresh** and verify **SOAM > MEP > Configuration** for Device D.



MEP ID	Port	Direction	Primary VID	Status	CC status	FNG state	LTM/CCM priority	FNG alarm time	FNG reset time	Lowest priority defect
610	Port 2	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrIcon
620	Port 1	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrIcon
50	Port 2	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrIcon
60	Port 1	Down	0	Enabled	Enabled	Defect reported	0	250	1000	macRemErrIcon

Parent MA/MEG:	MEP ID:	Port:	Direction:	Primary VID:	Status:	CC status:
MA ID: 6	620	Port 1	Down	0	Enabled	Enabled
FNG alarm time:	FNG reset time:	Lowest priority defect:	LTM/CCM priority:			
250	1000	macRemErrIcon	Priority 0			

Refresh Add Edit Delete Help

14. Devices A, B, C, and D are configured for SOAM per the IEEE 802.1ag Standard.

Note: Transition Networks recommends as a ‘best practice’ to backup each SIC card configuration after it is fully configured so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored. See “[Backing Up Slide-In and Remote Modules](#)” in section 5 of the *ION System x3230 Remotely Managed NID User Guide*, 33342.

ITU-T Y.1731 Configuration

The sample configuration using ITU-T Y.1731 is shown below.

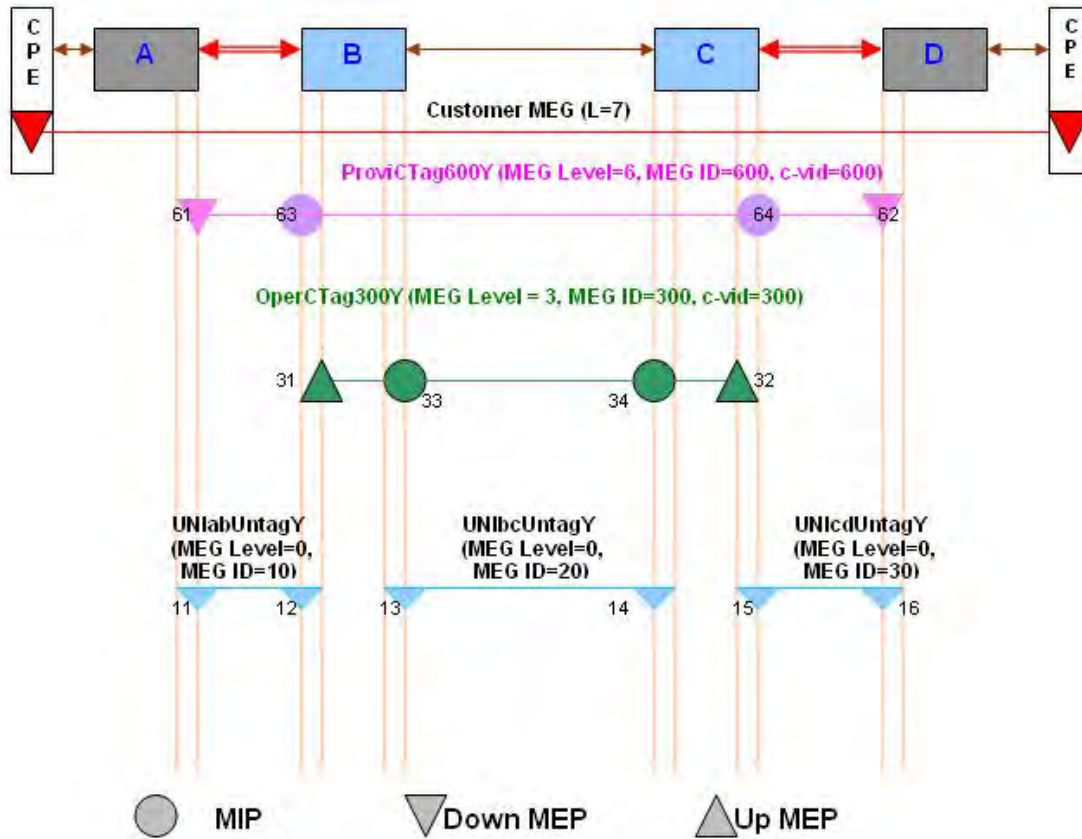


Figure D-5: ITU-T Y.1731 Configuration Example

The ION system (ION Stack) configuration is shown below.

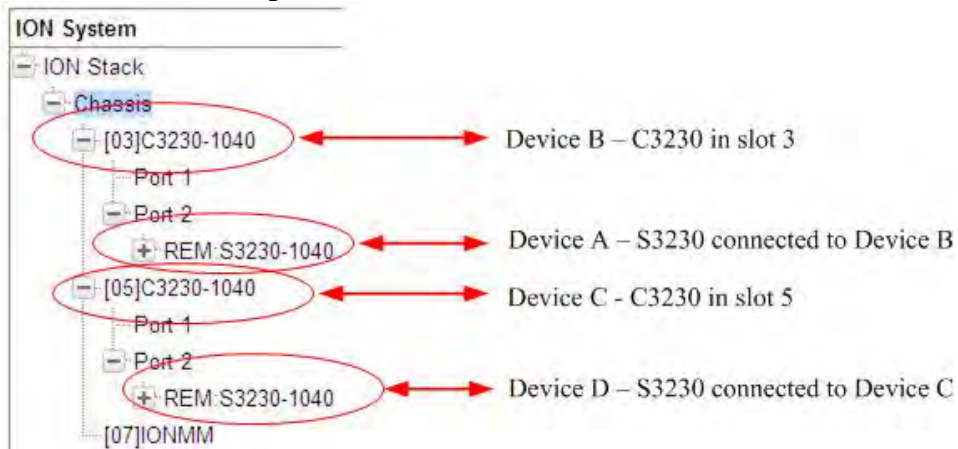


Figure D-6: ION Chassis / Device Configuration

Appendix D: SOAM Configuration Example – CLI Method

Configuration of SOAM MD/MAs, MEGs, MEPs, and MIPs for Devices A, B, C, and D via the Web method is documented in the following sections. The sample procedure below is provided for configurations based on the ITU-T Y.1731 standard.

SOAM Web Config - ITU-T Y.1731 Standard – Device A

This procedure configures Device A (S3230-1040 at CPE 1):

Device A	Level 0 UNI	Level 6 Provider MD
Local MEG ID	10	600
MEG Name	UNlabUntagY	ProvCTag600Y
MEG level	0	6
VLAN Type	none	ctype 600
MEP IDs	11, 12	61, 62
Direction	Down port 2	Down port 2
Admin	Enabled	Enabled
CCI	Enabled	Enabled
AIS Process		Enabled

1. Access Device A (C3230 at CPE 1) through the Web interface (see “Starting the Web Interface” on page 45 of the *x323x NID User Guide*). The **MAIN** tab displays for Device A.

The screenshot shows the ION System web interface. The left sidebar shows a tree view of the ION Stack with 'REM S3230-1040' selected. The main content area is the 'MAIN' tab, which includes the following sections:

- Model Information:** Serial Number (5219498), Model (S3230-1040), Software Revision (1.0.3), Hardware Revision (0.0.1), and Bootloader Revision (1.2.1).
- System Configuration:** System Name (S3230-1040), System Up Time (2-21-17 07:17), System Contact (Transition Networks(techs), System Location (10900 Red Circle Drive), Configuration Mode (Software), Console Access (Enabled), Number of Ports (2), and MAC Address (00-C0-F2-21-09-6C).
- Buttons:** Uptime Reset, System Reboot, All Counters Reset, and Reset To Factory Config.
- Circuit ID:** S3230-1040.

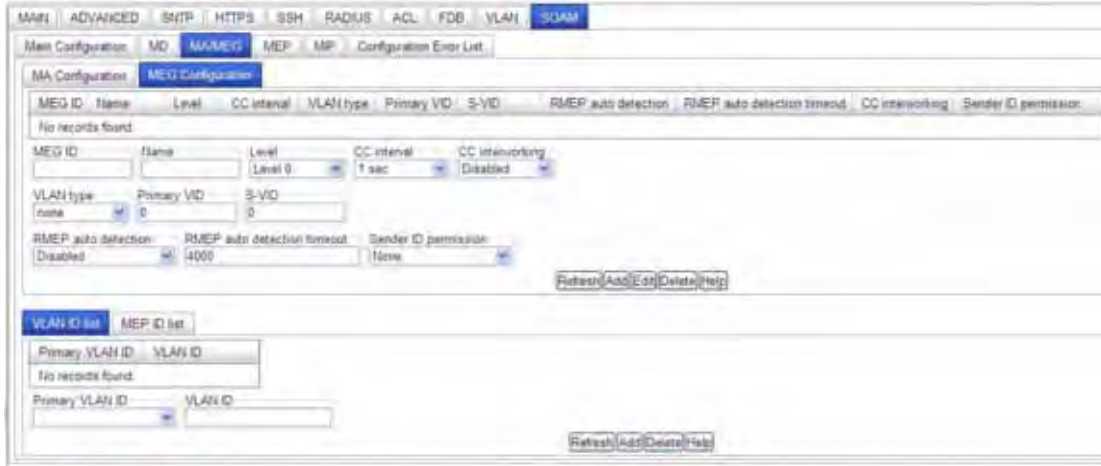
2. Select the **VLAN** tab. In the **VLAN ID** field, enter **600**. Leave the **Priority Override** field at the default setting of **Disabled**. At the **Priority** field select **3**. At **Member Tag Port 1** select **NoMod**. At **Member Tag Port 2** select **UnTag**. Click **Add**. Verify the VLAN ID table for Device A:

The screenshot shows the VLAN configuration page. The 'VLANs' section contains a table with the following data:

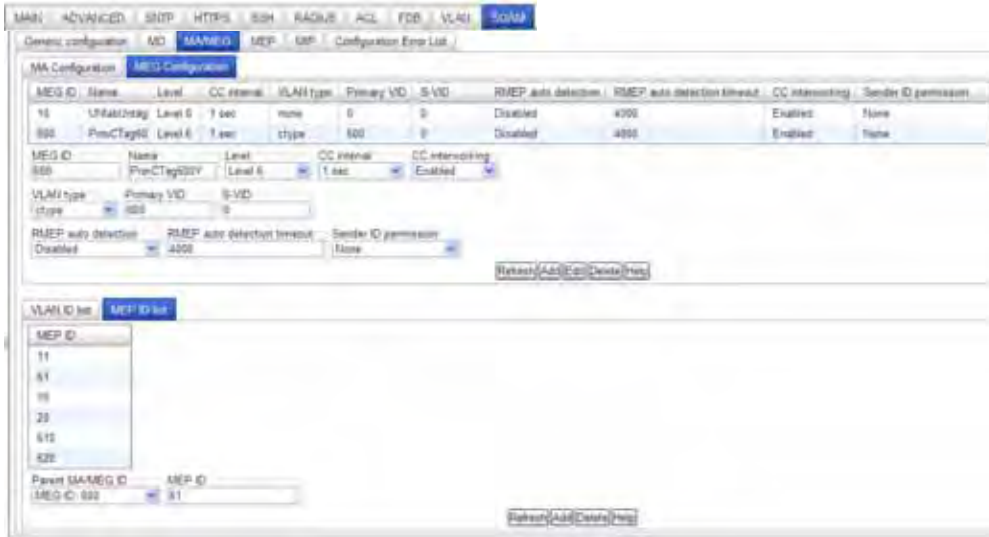
VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2
1	0	Disabled	0	NoMod	NoMod
600	0	Disabled	3	NoMod	UnTag

Below the table, the configuration fields are shown: VLAN ID (600), FDB ID (0), Priority Override (Disabled), Priority (3), Member Tag Port 1 (NoMod), and Member Tag Port 2 (UnTag). Buttons for Refresh, Add, Edit, Delete, and Help are visible at the bottom.

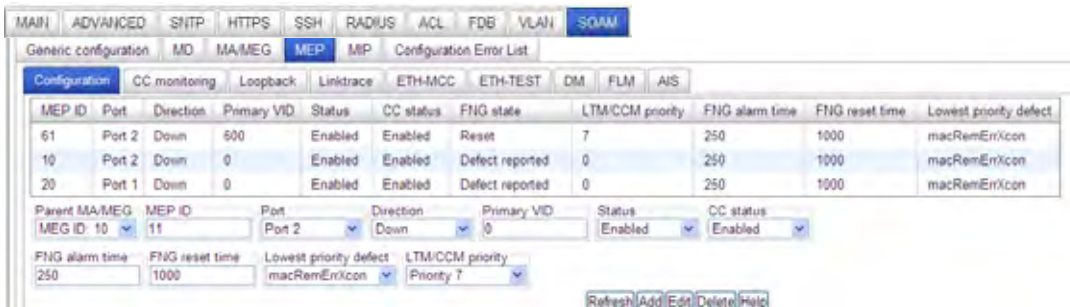
3. Select the **SOAM** tab > **MA/MEG** sub-tab > **MEG Configuration**.



4. In the **MEG ID** field, enter **10**. In the **Name** field, enter **UNIabUntagY**. In the **Level** field select **Level 3**.
In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **none**. Leave the **Primary VID** and **S-VID** fields at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**. Verify the MEG ID table entries.
5. In the **MEG ID** field, enter **600**. In the **Name** field, enter **ProvCTag600Y**. In the **Level** field select **Level 6**. In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **ctype**. In the **Primary VID** field, enter **600**. Leave the **S-VID** field at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**. Verify the MEG ID table entries.
6. At the **VLAN ID list** tab, select **MEG PVID: 600**. In the **VLAN ID** field, enter **600**.
7. Select the **MEP ID list** tab. In the **Parent MA/MEG ID** field, select **MEG ID: 10**. In the **MEP ID** field enter **11**. Click **Add**. Click **Refresh**.
8. In the **Parent MA/MEG ID** field, select **MEG ID: 600**. In the **MEP ID** field enter **61**. Click **Add**. Click **Refresh**. Verify the MEG ID table entries for Device A:



9. Select **SOAM > MEP > Configuration**. In the **Parent MA/MEG** field enter **MEG ID: 600**. In the **MEP ID** field enter **61**. In the **Port** field select **Port 2**. In the **Direction** field select **Down**. In the **Primary VID** field enter **600**. In the **Status** field select **Enabled**. In the **CC status** field select **Enabled**. Leave the other selections at the default settings. Click **Add**. Click **Refresh**. Verify the MEP ID table selections for Device A:



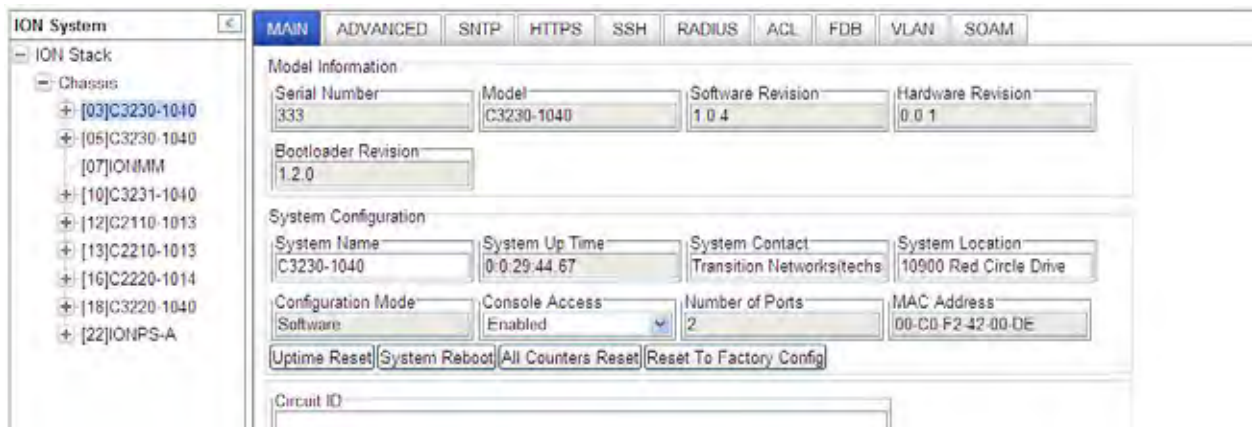
10. Device A is configured; continue with Device B configuration below.

SOAM Web Config - ITU-T Y.1731 Standard – Device B

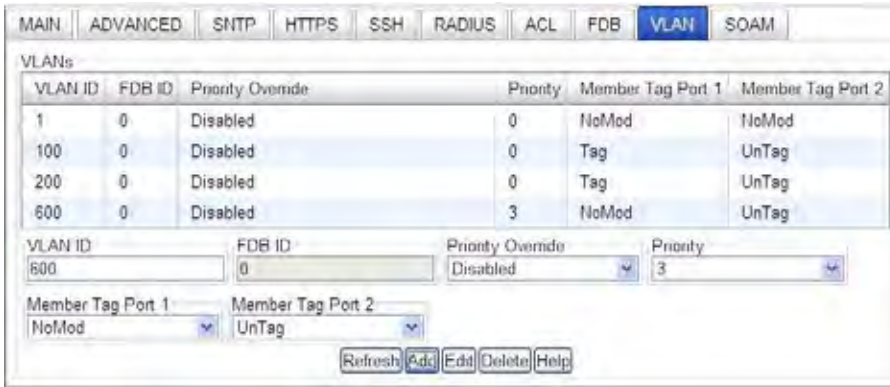
This procedure configures Device B (C3230 in slot 3):

Device B	Level 0 UNI	Level 0 UNI	Level 3 OperatorMD	Level 6 ProviderMD
Local MEG ID	10	20	300	600
MEG Name	UNIabUntagY	UNIbcUntagY	OperCTag300Y	ProvCTag600Y
MEG level	0	0	3	6
VLAN Type	none	none	ctype 300	ctype 600
MEP IDs	11, 12	13, 14	31, 32	
Direction	Down port 2	Down port 1	Up port 2	
Admin	Enabled	Enabled	Enabled	Enabled
CCI	Enabled	Enabled	Enabled	Enabled
AIS Process		Enabled	Enabled	
AIS Notify Up		Enabled	Enabled	Enabled
AIS Transmit		Enabled	Enabled	
AIS Client		MIP33	MIP63	
MIP Type			Y.1731	Y.1731
Local MIP ID			33	63
Local Parent ID			300 port 1	600 port 2
MIP Admin			Enabled	Enabled
MIP AIS Transmit			Enabled	Enabled

1. Access Device B (C3230 in slot 3) through the Web interface. The Device B **MAIN** tab displays.



2. Select the **VLAN** tab. In the **VLAN ID** field, enter **600**. Leave the **Priority Override** field at the default setting of **Disabled**. At the **Priority** field select **3**. At **Member Tag Port 1** select **NoMod**. At **Member Tag Port 2** select **UnTag**. Click **Add**. Verify the VLAN ID table for Device B.



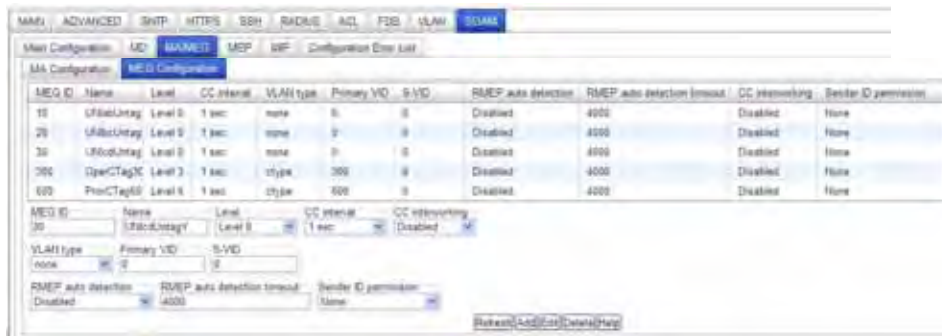
3. Select the **SOAM** tab > **MA/MEG** sub-tab > **MEG Configuration** for Device B.



4. In the **MEG ID** field, enter **10**. In the **Name** field, enter **UNIabUntagY**. In the **Level** field select **Level 0**.
 In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **none**. Leave the **Primary VID** and **S-VID** fields at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**. Verify the MEG ID table entries.
5. In the **MEG ID** field, enter **20**. In the **Name** field, enter **UNIbcUntagY**. In the **Level** field select **Level 0**.
 In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **none**. Leave the **Primary VID** and **S-VID** fields at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.
6. In the **MEG ID** field, enter **30**. In the **Name** field, enter **UNIcdUntagY**. In the **Level** field select **Level 0**.
 In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **none**. Leave the **Primary VID** and **S-VID** fields at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.
7. In the **MEG ID** field, enter **300**. In the **Name** field, enter **OperCTag300Y**. In the **Level** field select **Level 0**. In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the

VLAN type field select *none*. Leave the **Primary VID** and **S-VID** fields at *0*. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.

8. In the **MEG ID** field, enter *600*. In the **Name** field, enter *ProvCTag600Y*. In the **Level** field select *Level 6*. In the **CC interval** field select *Isec*. In the **CC interworking** field select *Enabled*. In the **VLAN type** field select *ctype*. In the **Primary VID** field, enter *600*. Leave the **S-VID** field at *0*. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**. Verify the MEG ID table entries for Device B.



MEG ID	Name	Level	CC interval	VLAN type	Primary VID	S-VID	RMEP auto detection	RMEP auto detection timeout	CC interworking	Sender ID permission
10	UflicUnTag	Level 0	1 sec	none	0	0	Disabled	4000	Disabled	None
20	UflicUnTag	Level 0	1 sec	none	0	0	Disabled	4000	Disabled	None
30	UflicUnTag	Level 0	1 sec	none	0	0	Disabled	4000	Disabled	None
300	OperCTagC	Level 3	1 sec	ctype	300	0	Disabled	4000	Disabled	None
600	ProvCTagY	Level 6	1 sec	ctype	600	0	Disabled	4000	Disabled	None

MEG ID: Name: Level: CC interval: CC interworking: Enabled

VLAN type: Primary VID: S-VID:

RMEP auto detection: RMEP auto detection timeout: Sender ID permission:

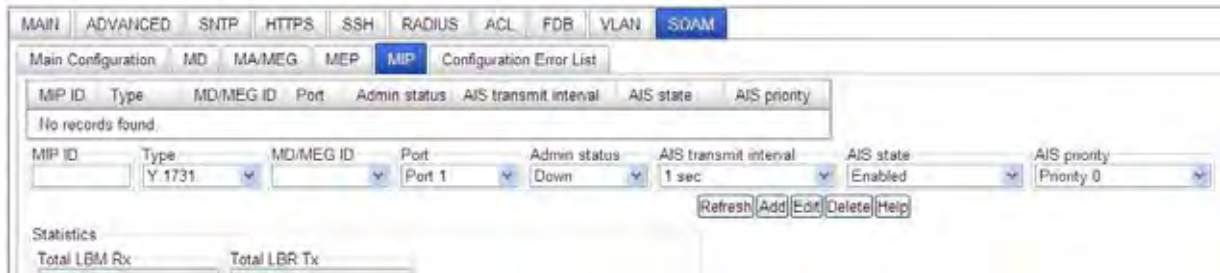
9. At the **VLAN ID list** tab, in the **Primary VLAN ID** field, select *MEG PVID: 300*. In the **VLAN ID** field, enter *300*.
10. At the **VLAN ID list** tab, in the **Primary VLAN ID** field, select *MEG PVID: 600*. In the **VLAN ID** field, enter *600*.
11. Select the **MEP ID list** tab. In the **Parent MA/MEG ID** field, select *MEG ID: 20*. In the **MEP ID** field enter *13*. Click **Add**. Click **Refresh**.
12. In the **Parent MA/MEG ID** field, select *MEG ID: 20*. In the **MEP ID** field enter *14*. Click **Add**. Click **Refresh**.
13. In the **Parent MA/MEG ID** field, select *MEG ID: 30*. In the **MEP ID** field enter *15*. Click **Add**. Click **Refresh**.
14. In the **Parent MA/MEG ID** field, select *MEG ID: 30*. In the **MEP ID** field enter *16*. Click **Add**. Click **Refresh**.
15. In the **Parent MA/MEG ID** field, select *MEG ID: 300*. In the **MEP ID** field enter *31*. Click **Add**. Click **Refresh**.

16. In the **Parent MA/MEG ID** field, select *MEG ID: 300*. In the **MEP ID** field enter **32**. Click **Add**. Click **Refresh**. Verify the MEP ID list entries for Device B:



15. Select **SOAM > MEP > Configuration** and define MEP IDs 11, 12, 13, 14, 31 and 32 for Device B.
16. In the **Parent MA/MEG** field enter *MEG ID: 10*. In the **MEP ID** field enter **11**. In the **Port** field select *Port 2*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
17. In the **Parent MA/MEG** field enter *MEG ID: 10*. In the **MEP ID** field enter **12**. In the **Port** field select *Port 2*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
18. In the **Parent MA/MEG** field enter *MEG ID: 20*. In the **MEP ID** field enter **13**. In the **Port** field select *Port 1*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
19. In the **Parent MA/MEG** field enter *MEG ID: 20*. In the **MEP ID** field enter **14**. In the **Port** field select *Port 1*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
20. In the **Parent MA/MEG** field enter *MEG ID: 300*. In the **MEP ID** field enter **31**. In the **Port** field select *Port 2*. In the **Direction** field select *Up*. In the **Primary VID** field enter **300**. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings.
Click **Add**. Click **Refresh**.
21. In the **Parent MA/MEG** field enter *MEG ID: 30*. In the **MEP ID** field enter **32**. In the **Port** field select *Port 2*. In the **Direction** field select *Up*. In the **Primary VID** field enter **300**. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings.
Click **Add**. Click **Refresh**.
22. Verify the MEP ID table selections for Device B.

23. Select **SOAM** > **MIP** and define MIP ID 33 and 63 for Device B:



24. In the **MIP ID** field, enter **33**. In the **Type** field select **Y.1731**. In the **MD/MEG ID** field select **MD ID 33**. In the **Port** field, select **Port 1**. In the **Admin** status field, select **Down**. Leave the remaining fields at the default settings. Click **Add**.

25. In the **MIP ID** field, enter **63**. In the **Type** field select **Y.1731**. In the **MD/MEG ID** field select **MD ID 63**. In the **Port** field, select **Port 1**. In the **Admin** status field, select **Down**. Leave the remaining fields at the default settings. Click **Add**. Click **Refresh** and verify the **SOAM** > **MIP** configuration for Device B.



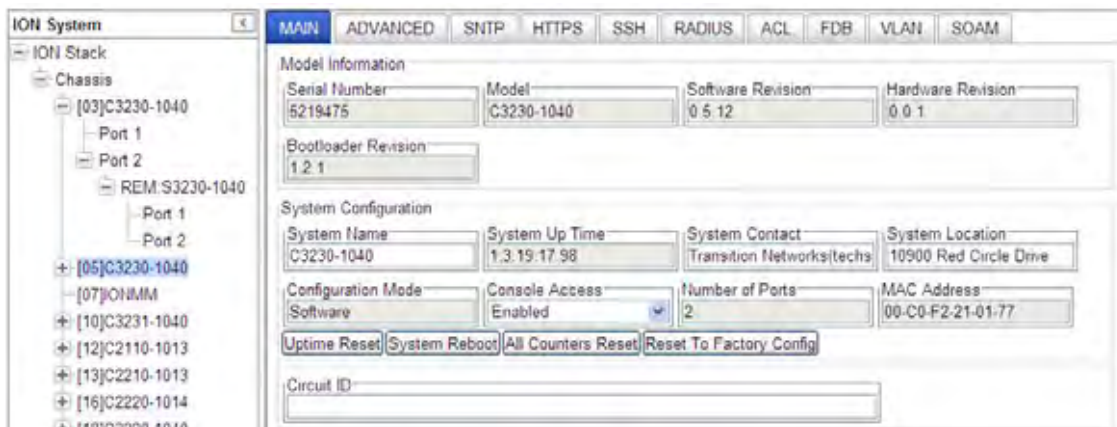
Device B is configured; continue with Device C configuration below.

SOAM Web Config - ITU-T Y.1731 Standard – Device C

This procedure configures Device C (C3230 in slot 5):

Device C	Level 0 UNI	Level 0 UNI	Level 3 OperatorMD	Level 6 ProviderMD
Local MEG ID	20	30	300	600
MEG Name	UNIbcUntagY	UNIcdUntagY	OperCTag300Y	ProvCTag600Y
MEG level	0	0	3	6
VLAN Type	none	none	ctype 300	ctype 600
MEP IDs	13, 14	15, 16	31, 32	
Direction	Down port 1	Down port 2	Up port 2	
Admin	Enabled	Enabled	Enabled	
CCI	Enabled	Enabled	Enabled	
AIS Process	Enabled		Enabled	
AIS Notify Up	Enabled		Enabled	
AIS Transmit	Enabled		Enabled	
AIS Client	MIP34		MIP64	
MIP Type			Y.1731	Y.1731
Local MIP ID			34	64
Local Parent ID			300 port 1	600 port 2
MIP Admin			Enabled	Enabled
MIP AIS Transmit			Enabled	Enabled

1. Access Device C (C3230 in slot 5) through the Web interface. The **MAIN** tab displays for Device C.



2. Select the **VLAN** tab. In the **VLAN ID** field, enter **300**. Leave the **Priority Override** field at the default setting of **Disabled**. At the **Priority** field select **0**. At **Member Tag Port 1** select **Tag**. At **Member Tag Port 2** select **UnTag**. Click **Add**.
3. At the **VLAN** tab. In the **VLAN ID** field, enter **600**. Leave the **Priority Override** field at the default setting of **Disabled**. At the **Priority** field select **0**. At **Member Tag Port 1** select **Tag**. At **Member Tag Port 2** select **UnTag**. Click **Add**. Verify the VLAN ID table for Device C.

MAIN ADVANCED SNTP HTTPS SSH RADIUS ACL FDB VLAN SOAM						
VLANs						
VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2	
1	0	Disabled	0	NoMod	NoMod	
100	0	Disabled	0	Tag	UnTag	
200	0	Disabled	0	Tag	UnTag	
300	0	Disabled	0	Tag	NoMod	
600	0	Disabled	0	UnTag	Tag	

VLAN ID	FDB ID	Priority Override	Priority
600	0	Disabled	0
Member Tag Port 1	Member Tag Port 2		
UnTag	Tag		

Refresh Add Edit Delete Help

- Select the **SOAM** tab > **MA/MEG** sub-tab > **MEG Configuration** for Device C.
- In the **MEG ID** field, enter **20**. In the **Name** field, enter **UNIbcUntagY**. In the **Level** field select **Level 0**.
In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **none**. Leave the **Primary VID** and **S-VID** fields at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.
- In the **MEG ID** field, enter **30**. In the **Name** field, enter **UNIcdUntagY**. In the **Level** field select **Level 0**.
In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **none**. Leave the **Primary VID** and **S-VID** fields at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.
- In the **MEG ID** field, enter **300**. In the **Name** field, enter **OperCTag300Y**. In the **Level** field select **Level 3**. In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **ctype**. In the **Primary VID** field enter **300**. Leave the **S-VID** field at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.
- In the **MEG ID** field, enter **600**. In the **Name** field, enter **ProvCTag600Y**. In the **Level** field select **Level 6**. In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type** field select **ctype**. In the **Primary VID** field, enter **600**. Leave the **S-VID** field at **0**. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**. Verify the MEG ID table entries for Device C.

MAIN ADVANCED SNTP HTTPS SSH RADIUS ACL FDB VLAN SOAM										
Main Configuration MD MA/MEG MEP MIP Configuration Error List										
MA Configuration MEG Configuration										
MEG ID	Name	Level	CC interval	VLAN type	Primary VID	S-VID	RMEP auto detection	RMEP auto detection timeout	CC interworking	Sender ID permission
20	UNIbcUntag	Level 0	1 sec	none	0	0	Disabled	4000	Enabled	None
30	UNIcdUntag	Level 0	1 sec	none	0	0	Disabled	4000	Enabled	None
60	ProvCTag60	Level 6	1 sec	ctype	600	0	Disabled	4000	Enabled	None
300	OperCTag300	Level 3	1 sec	ctype	300	0	Disabled	4000	Enabled	None

- At the **VLAN ID list** tab, in the **Primary VLAN ID** field, select **MEG PVID: 300**. In the **VLAN ID** field, enter **300**.

Appendix D: SOAM Configuration Example – CLI Method

10. In the **Primary VLAN ID** field, select **MEG PVID: 600**. In the **VLAN ID** field, enter **600**. Verify the VLAN ID list table entries for Device C.

Primary VLAN ID	VLAN ID
200	100
100	200
300	300
600	600

Primary VLAN ID: 600
VLAN ID: 600

Refresh Add Delete Help

17. Select the **MEP ID list** tab. In the **Parent MA/MEG ID** field, select **MEG ID: 20**. In the **MEP ID** field enter **13**. Click **Add**. Click **Refresh**.
18. In the **Parent MA/MEG ID** field, select **MEG ID: 20**. In the **MEP ID** field enter **14**. Click **Add**. Click **Refresh**.
19. In the **Parent MA/MEG ID** field, select **MEG ID: 30**. In the **MEP ID** field enter **15**. Click **Add**. Click **Refresh**.
20. In the **Parent MA/MEG ID** field, select **MEG ID: 30**. In the **MEP ID** field enter **16**. Click **Add**. Click **Refresh**.
21. In the **Parent MA/MEG ID** field, select **MEG ID: 300**. In the **MEP ID** field enter **31**. Click **Add**. Click **Refresh**.
22. In the **Parent MA/MEG ID** field, select **MEG ID: 300**. In the **MEP ID** field enter **32**. Click **Add**. Click **Refresh**. Verify the **SOAM > MA/MEG > MEG Configuration** for Device C:

MEG ID	Name	Level	OC interval	VLAN type	Primary VID	S-VID	RMEP auto detection	RMEP auto detection timeout	OC interworking	Sender ID permission
20	UMInUtag	Level 0	1 sec	none	0	0	Disabled	4000	Enabled	None
30	UMInUtag	Level 0	1 sec	none	0	0	Disabled	4000	Enabled	None
30	ProCTag30	Level 3	1 sec	stype	600	0	Disabled	4000	Enabled	None
300	OpenCTag30	Level 3	1 sec	ctype	300	0	Disabled	4000	Enabled	None

MEP ID list

MEP ID: 13, 14, 15, 16, 31, 32, 310, 300, 30, 40, 50, 60

Parent MA/MEG ID: 300
MEP ID: 13

Refresh Add Delete Help

26. Select **SOAM > MEP > Configuration** and define MEP ID 13, 14, 15, 16, 31 and 32 for Device C.
27. In the **Parent MA/MEG** field enter *MEG ID: 20*. In the **MEP ID** field enter *13*. In the **Port** field select *Port 1*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
28. In the **Parent MA/MEG** field enter *MEG ID: 20*. In the **MEP ID** field enter *14*. In the **Port** field select *Port 1*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
29. In the **Parent MA/MEG** field enter *MEG ID: 30*. In the **MEP ID** field enter *15*. In the **Port** field select *Port 2*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
30. In the **Parent MA/MEG** field enter *MEG ID: 30*. In the **MEP ID** field enter *16*. In the **Port** field select *Port 2*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
31. In the **Parent MA/MEG** field enter *MEG ID: 300*. In the **MEP ID** field enter *31*. In the **Port** field select *Port 2*. In the **Direction** field select *Up*. In the **Primary VID** field enter *300*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings.
Click **Add**. Click **Refresh**.
32. In the **Parent MA/MEG** field enter *MEG ID: 300*. In the **MEP ID** field enter *32*. In the **Port** field select *Port 2*. In the **Direction** field select *Up*. In the **Primary VID** field enter *300*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings.
Click **Add**. Click **Refresh**.
33. Verify the **SOAM > MA/MEG > MEG Configuration** for Device C.
34. Select **SOAM > MIP** and define MIP ID 34 and 64 for Device C:



35. In the **MIP ID** field, enter *34*. In the **Type** field select *Y.1731*. In the **MD/MEG ID** field select *MD ID 34*. In the **Port** field, select *Port 1*. In the **Admin** status field, select *Down*. Leave the remaining fields at the default settings. Click **Add**.

Appendix D: SOAM Configuration Example – CLI Method

36. In the **MIP ID** field, enter *64*. In the **Type** field select *Y.1731*. In the **MD/MEG ID** field select *MD ID 64*. In the **Port** field, select *Port 1*. In the **Admin** status field, select *Down*. Leave the remaining fields at the default settings. Click **Add**. Click **Refresh** and verify the **SOAM > MIP** configuration for Device B.

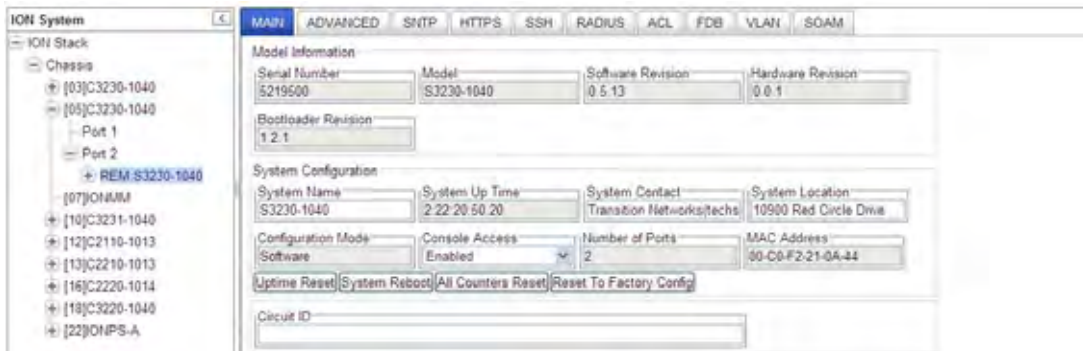
Device C is configured; continue with Device D configuration below.

SOAM Web Config - ITU-T Y.1731 Standard – Device D

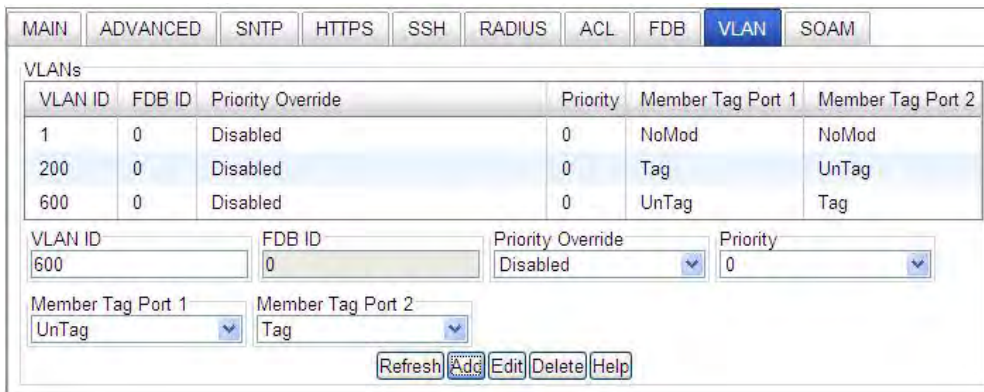
This procedure configures Device D (S3230-1040 at CPE 1):

Device D	Level 0 UNI	Level 6 Provider MD
Local MEG ID	30	600
MEG Name	UNIcdUntagY	ProvCTag600Y
MEG level	0	6
MEP IDs	15, 16	61, 62
VLAN Type	none	ctype 600
Direction	Down port 2	Down port 2
Admin	Enabled	Enabled
CCI	Enabled	Enabled
AIS Process	Enabled	Enabled

1. Access Device D (S3230 at CPE 2) through the Web interface. The **MAIN** tab displays.



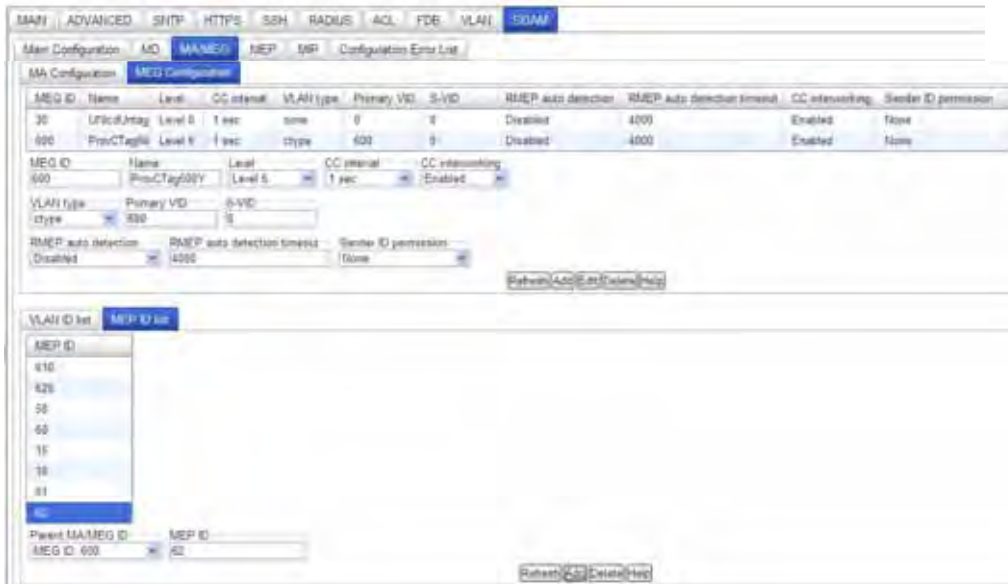
2. Select the **VLAN** tab. In the **VLAN ID** field, enter **600**. Leave the **Priority Override** field at the default setting of **Disabled**. At the **Priority** field select **0**. At **Member Tag Port 1** select **Tag**. At **Member Tag Port 2** select **UnTag**. Click **Add**. Click **Refresh**. Verify the VLAN ID table for Device D.



3. Go to **SOAM > MA/MEG > MEG Configuration** for Device D.
4. In the **MEG ID** field, enter **30**. In the **Name** field, enter **UNIcdUntagY**. In the **Level** field select **Level 0**.
In the **CC interval** field select **Isec**. In the **CC interworking** field select **Enabled**. In the **VLAN type**

field select *none*. Leave the **Primary VID** and **S-VID** fields at *0*. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.

5. In the **MEG ID** field, enter *600*. In the **Name** field, enter *ProvCTag600Y*. In the **Level** field select *Level 0*. In the **CC interval** field select *Isec*. In the **CC interworking** field select *Enabled*. In the **VLAN type** field select *none*. Leave the **Primary VID** and **S-VID** fields at *0*. Leave both **RMEP** fields and the **Sender ID permission** fields at the default settings. Click **Add**. Click **Refresh**.
6. At the **VLAN ID list** tab, in the **Parent VLAN ID** field, select *MEG PVID: 600*. In the **VLAN ID** field, enter *600*.
7. Select the **MEP ID list** tab. In the **Parent MA/MEG ID** field, select *MEG ID: 600*. In the **MEP ID** field enter *61*. Click **Add**. Click **Refresh**.
8. In the **Parent MA/MEG ID** field, select *MEG ID: 600*. In the **MEP ID** field enter *62*. Click **Add**. Click **Refresh**.
9. In the **Parent MA/MEG ID** field, select *MEG ID: 30*. In the **MEP ID** field enter *15*. Click **Add**. Click **Refresh**.
10. In the **Parent MA/MEG ID** field, select *MEG ID: 30*. In the **MEP ID** field enter *16*. Click **Add**. Click **Refresh**. Verify the **SOAM > MA/MEG > MEG Configuration** for Device D.



11. Select **SOAM > MEP > Configuration** and define MEP IDs 15, 16, 61 and 62 for Device D.
12. In the **Parent MA/MEG** field enter *MEG ID: 30*. In the **MEP ID** field enter *15*. In the **Port** field select *Port 2*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status** field select *Enabled*. In the **CC status** field select *Enabled*. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.
13. In the **Parent MA/MEG** field enter *MEG ID: 30*. In the **MEP ID** field enter *16*. In the **Port** field select *Port 2*. In the **Direction** field select *Down*. In the **Primary VID** field enter *none*. In the **Status**

field select **Enabled**. In the **CC status** field select **Enabled**. Leave the other selections at the default settings. Click **Add**. Click **Refresh**.

14. In the **Parent MA/MEG** field enter **MEG ID: 600**. In the **MEP ID** field enter **61**. In the **Port** field select **Port 2**. In the **Direction** field select **Down**. In the **Primary VID** field enter **600**. In the **Status** field select **Enabled**. In the **CC status** field select **Enabled**. Leave the other selections at the default settings.

Click **Add**. Click **Refresh**.

15. In the **Parent MA/MEG** field enter **MEG ID: 600**. In the **MEP ID** field enter **62**. In the **Port** field select **Port 2**. In the **Direction** field select **Down**. In the **Primary VID** field enter **600**. In the **Status** field select **Enabled**. In the **CC status** field select **Enabled**. Leave the other selections at the default settings.

Click **Add**. Click **Refresh**. Verify the **SOAM > MEP > Configuration** for Device D.

16. Devices A, B, C, and D are configured for SOAM per the ITU-T Y.1731 Standard.

Note: Transition Networks recommends as a ‘best practice’ to backup SIC card configuration after it is fully configured so that in the event of an error or hardware failure, the configuration can be easily and rapidly restored. See “[Backing Up Slide-In and Remote Modules](#)” in section 5 of the *ION System x323x Remotely Managed NID User Guide*, 33342.

For the set of SOAM Configuration errors that the x323x NID can display see “[Section 6 – Troubleshooting](#)” on page 308.

Appendix E: SOAM Configuration Example – CLI Method

This appendix provides a sample SOAM configuration set up via the Command Line Interface (CLI) method.

SOAM Sample Configuration – CLI Method

This sample configuration sets up SOAM between two subscriber sites: CPE1 and CPE2 (for illustrative purposes it is managed in the same chassis.) This configuration will allow testing of Y.1731 (UP- MEPs, DOWN-MEPs, MIP, AIS, etc) and 802.1ag (UP- MEPs, DOWN-MEPs and MIPs) and also will help verify nesting rules of Management Domains. This is a typical customer network configuration of devices.

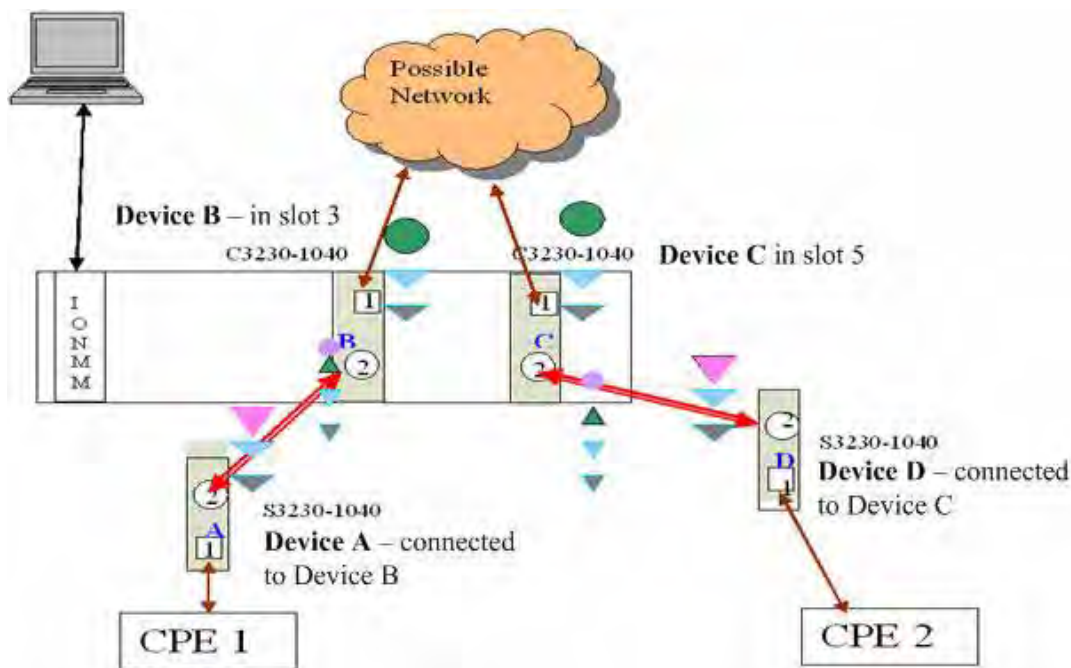


Figure E-1: SOAM Configuration

This sample configuration includes an ION219 chassis, two C3230 NIDs, two S3230 NIDs, an IONMM card, four SFP-SX devices, MMF-6.2/125 optical fiber cable, a CAT.5E patch cable, and a high-speed shielded USB 2.0 cable. The configuration includes:

- 6) Two C3230-S3230 pairs used for SOAM configuration and testing.
- 7) A total of 3 MEG levels configured as specified in this document. Two MEGs will be C-tagged MEGs and one an untagged MEG.
- 8) Devices A and D (S3230s) will have the MEPs at Level 7, devices B and C will have MIPs at Level 4.
- 9) Devices B and C (C3230s) have MEPs and MIPs for operator MEG at Level 3.
- 10) UNI MEG will be configured between A-B, B-C, and C-D.

This sample SOAM configuration assumes that the chassis and devices are installed and cabling is completed. The MEG level layouts are shown below:

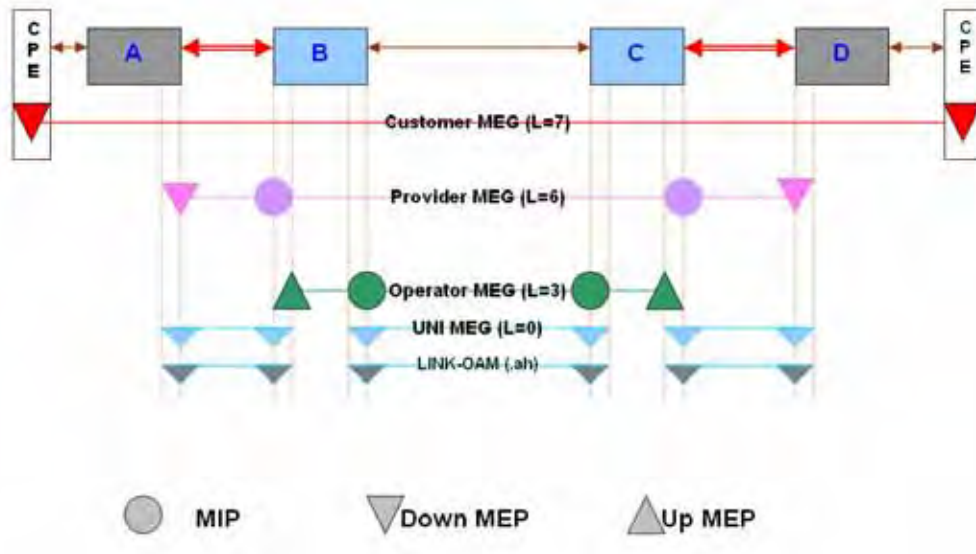


Figure E-2: MEG Level Layouts

IEEE 802.1ag Configuration

The sample configuration using IEEE 802.1ag is shown below.

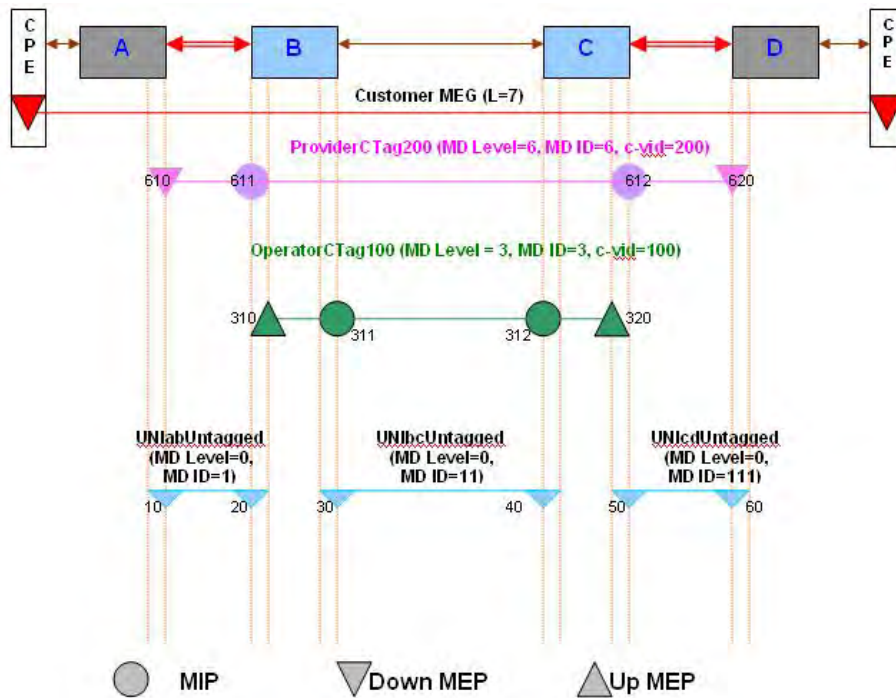


Figure E-3: IEEE 802.1ag Configuration

The ION system configuration is shown below.

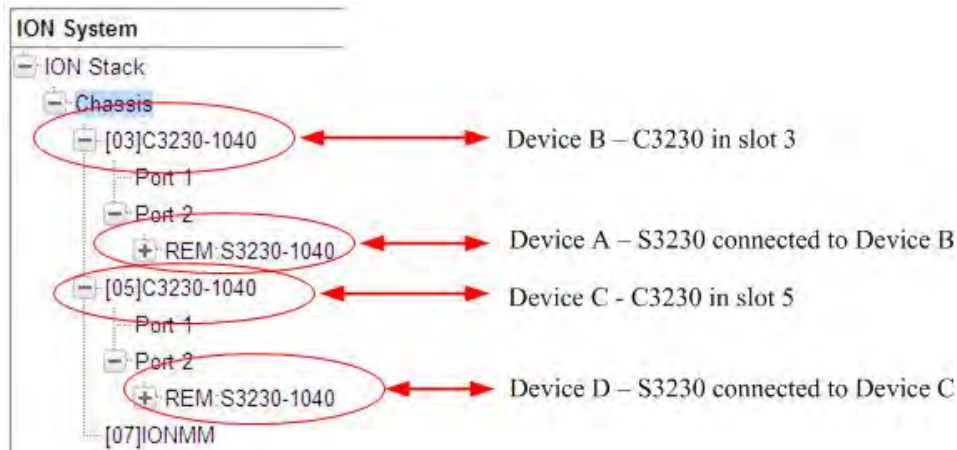


Figure E-4: ION Chassis / Device Configuration

The following sections document the configuration of SOAM MD/MAs, MEGs, MEPs, and MIPs for Devices A, B, C, and D via the CLI method. Sample procedures are provided for configurations based on both the IEEE 802.1ag standard and the ITU-T Y.1731 standard.

IEEE 802.1ag Configuration Example (Devices A, B, C, D)

A sample configuration using IEEE 802.1ag is provided below.

```
*****
* 802.1ag (All MAs on different CTAGs) *
*****

## Device A #####

## Level 0 UNI ##
add soam md local-md-id 1 md-name UNIabMD md-level 0
add soam ma local-ma-id 1 local-md-id 1 ma-name UNIabUntagged vlan-type none
set soam ma local-ma-id 1 attr_name mepid-add attr_value 10
set soam ma local-ma-id 1 attr_name mepid-add attr_value 20
add soam mep mep-id 10 local-parent-id 1 direction down port 2
set soam mep config mep-id 10 local-parent-id 1 attr_name admin attr_value enable
set soam mep config mep-id 10 local-parent-id 1 attr_name cci attr_value enable

## Level 6 Provider MD ##
add soam md local-md-id 6 md-name ProviderMD md-level 6
add soam ma local-ma-id 6 local-md-id 6 ma-name ProviderCTag200 vlan-type ctype 200
set soam ma local-ma-id 6 attr_name mepid-add attr_value 610
set soam ma local-ma-id 6 attr_name mepid-add attr_value 620
add soam mep mep-id 610 local-parent-id 6 direction down port 2
set soam mep config mep-id 610 local-parent-id 6 attr_name admin attr_value enable
set soam mep config mep-id 610 local-parent-id 6 attr_name cci attr_value enable
```

```

## Device B #####
## Level 0 UNI ##
add soam md local-md-id 1 md-name UNIAbMD md-level 0
add soam ma local-ma-id 1 local-md-id 1 ma-name UNIAbUntagged vlan-type none
set soam ma local-ma-id 1 attr_name mepid-add attr_value 10
set soam ma local-ma-id 1 attr_name mepid-add attr_value 20
add soam mep mep-id 20 local-parent-id 1 direction down port 2
set soam mep config mep-id 20 local-parent-id 1 attr_name admin attr_value enable
set soam mep config mep-id 20 local-parent-id 1 attr_name cci attr_value enable

## Level 0 UNI ##
add soam md local-md-id 11 md-name UNIBcMD md-level 0
add soam ma local-ma-id 11 local-md-id 11 ma-name UNIBcUntagged vlan-type none
set soam ma local-ma-id 11 attr_name mepid-add attr_value 30
set soam ma local-ma-id 11 attr_name mepid-add attr_value 40
add soam mep mep-id 30 local-parent-id 11 direction down port 1
set soam mep config mep-id 30 local-parent-id 11 attr_name admin attr_value enable
set soam mep config mep-id 30 local-parent-id 11 attr_name cci attr_value enable

## Level 3 Operator MD ##
add soam md local-md-id 3 md-name OperatorMD md-level 3
add soam ma local-ma-id 3 local-md-id 3 ma-name OperatorCTag100 vlan-type ctype 100
set soam ma local-ma-id 3 attr_name mepid-add attr_value 310
set soam ma local-ma-id 3 attr_name mepid-add attr_value 320
add soam mep mep-id 310 local-parent-id 3 direction up port 2
set soam mep config mep-id 310 local-parent-id 3 attr_name admin attr_value enable
set soam mep config mep-id 310 local-parent-id 3 attr_name cci attr_value enable
add soam mip mip-type 802.lag local-mip-id 311 local-parent-id 3 port 1
set soam mip local-mip-id 311 attr-name admin attr-val enable

## Level 6 Provider MD ##
add soam md local-md-id 6 md-name ProviderMD md-level 6
add soam ma local-ma-id 6 local-md-id 6 ma-name ProviderCTag200 vlan-type ctype 200
add soam mip mip-type 802.lag local-mip-id 611 local-parent-id 6 port 2
set soam mip local-mip-id 611 attr-name admin attr-val enable

```

Appendix E: SOAM Configuration Example – CLI Method

```

## Device C #####
## Level 0 UNI ##
add soam md local-md-id 11 md-name UNIBCMD md-level 0
add soam ma local-ma-id 11 local-md-id 11 ma-name UNIBCUntagged vlan-type none
set soam ma local-ma-id 11 attr_name mepid-add attr_value 30
set soam ma local-ma-id 11 attr_name mepid-add attr_value 40
add soam mep mep-id 40 local-parent-id 11 direction down port 1
set soam mep config mep-id 40 local-parent-id 11 attr_name admin attr_value enable
set soam mep config mep-id 40 local-parent-id 11 attr_name cci attr_value enable

## Level 0 UNI ##
add soam md local-md-id 111 md-name UNICdMD md-level 0
add soam ma local-ma-id 111 local-md-id 111 ma-name UNICdUntagged vlan-type none
set soam ma local-ma-id 111 attr_name mepid-add attr_value 50
set soam ma local-ma-id 111 attr_name mepid-add attr_value 60
add soam mep mep-id 50 local-parent-id 111 direction down port 2
set soam mep config mep-id 50 local-parent-id 111 attr_name admin attr_value enable
set soam mep config mep-id 50 local-parent-id 111 attr_name cci attr_value enable

## Level 3 Operator MD ##
add soam md local-md-id 3 md-name OperatorMD md-level 3
add soam ma local-ma-id 3 local-md-id 3 ma-name OperatorCTag100 vlan-type ctype 100
set soam ma local-ma-id 3 attr_name mepid-add attr_value 310
set soam ma local-ma-id 3 attr_name mepid-add attr_value 320
add soam mep mep-id 320 local-parent-id 3 direction up port 2
set soam mep config mep-id 320 local-parent-id 3 attr_name admin attr_value enable
set soam mep config mep-id 320 local-parent-id 3 attr_name cci attr_value enable
add soam mip mip-type 802.1ag local-mip-id 312 local-parent-id 3 port 1
set soam mip local-mip-id 312 attr-name admin attr-val enable

## Level 6 Provider MD ##
add soam md local-md-id 6 md-name ProviderMD md-level 6
add soam ma local-ma-id 6 local-md-id 6 ma-name ProviderCTag200 vlan-type ctype 200
add soam mip mip-type 802.1ag local-mip-id 612 local-parent-id 6 port 2
set soam mip local-mip-id 612 attr-name admin attr-val enable

```



```
## Device D #####
## Level 0 UNI ##
add soam md local-md-id 111 md-name UNICdMD md-level 0
add soam ma local-ma-id 111 local-md-id 111 ma-name UNICdUntagged vlan-type none
set soam ma local-ma-id 111 attr_name mepid-add attr_value 50
set soam ma local-ma-id 111 attr_name mepid-add attr_value 60
add soam mep mep-id 60 local-parent-id 111 direction down port 2
set soam mep config mep-id 60 local-parent-id 111 attr_name admin attr_value enable
set soam mep config mep-id 60 local-parent-id 111 attr_name cci attr_value enable

## Level 6 Provider MD ##
add soam md local-md-id 6 md-name ProviderMD md-level 6
add soam ma local-ma-id 6 local-md-id 6 ma-name ProviderCTag200 vlan-type ctype 200
set soam ma local-ma-id 6 attr_name mepid-add attr_value 610
set soam ma local-ma-id 6 attr_name mepid-add attr_value 620
add soam mep mep-id 620 local-parent-id 6 direction down port 2
set soam mep config mep-id 620 local-parent-id 6 attr_name admin attr_value enable
set soam mep config mep-id 620 local-parent-id 6 attr_name cci attr_value enable
```

Configuring Device A – CLI Method

```
C1|S12|L1AP2|L2D>#### DEVICE A ###
```

```
C1|S12|L1AP2|L2D>show soam md
```

Local MD ID	Name	Level	MAs	MIPs	Permission
1	UNIabMD	0	1	0	none
6	ProviderMD	6	1	0	none

```
C1|S12|L1AP2|L2D>show soam ma
```

```
MA index          : 1
MD index          : 1
MD level          : 0
MD name           : UNIabMD
MA name           : UNIabUntagged
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 10 20
Permission        : defer
VLAN ID list      : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 6
MD index          : 6
MD level          : 6
MD name           : ProviderMD
MA name           : ProviderCTag200
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 610 620
Permission        : defer
VLAN ID list      : ctype: 200
Primary VLAN ID   : 200
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
C1|S12|L1AP2|L2D>show soam mip config
```

```
The MIPs table is empty.
```

```
C1|S12|L1AP2|L2D>show soam mep config
```

```
MEP id           : 10
MD local ID      : 1
MD level         : 0
MD name          : UNIabMD
MA local ID      : 1
MA name          : UNIabUntagged
Direction        : down
Port             : 2
VLANs            : none
Primary VLAN     : 0
Admin status     : enabled
CCI status       : enabled
Fault notification state : Reset
Defects          :
```

```

Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time  : 10000 ms
Lowest Alarm priority   : macremerrxcon

```

```

MEP id                  : 610
MD local ID             : 6
MD level                : 6
MD name                 : ProviderMD
MA local ID             : 6
MA name                 : ProviderCTag200
Direction               : down
Port                    : 2
VLANs                   : ctype: 200
Primary VLAN            : 200
Admin status            : enabled
CCI status              : enabled
Fault notification state : Reset
Defects                 :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time  : 10000 ms
Lowest Alarm priority   : macremerrxcon

```

```

C1|S12|L1AP2|L2D>show soam mep cc mep-id 10 local-parent-id 1
MEP ID                  : 10
MD Local ID             : 1
MD level                : 0
MD name                 : UNIabMD

```

```

Remote MEP ID          : 20
State                  : OK
TimeStamp               : 233.98 sec
MAC                    : 00-C0-F2-20-E2-18
RDI BIT                : False
Port Status            : No Port State
Interface Status       : No Interface Status
Chassis id subtype     : None
Chassis id             :
Manage address domain  : 0.0
Manage address         :
Autodetected           : No

```

```

C1|S12|L1AP2|L2D>show soam mep cc mep-id 610 local-parent-id 6
MEP ID                  : 610
MD Local ID             : 6
MD level                : 6
MD name                 : ProviderMD

```

```

Remote MEP ID          : 620
State                  : OK
TimeStamp               : 5569.85 sec
MAC                    : 00-C0-F2-42-01-8E

```

Appendix E: SOAM Configuration Example – CLI Method

```
RDI BIT           : False
Port Status       : No Port State
Interface Status  : No Interface Status
Chassis id subtype : None
Chassis id        :
Manage address domain : 0.0
Manage address    :
Autodetected      : No
```

Configuring Device B – CLI Method

```
C1|S12|L1D>#### DEVICE B ###
```

```
C1|S12|L1D>show soam md
```

Local MD ID	Name	Level	MAs	MIPs	Permission
1	UNIabMD	0	1	0	none
3	OperatorMD	3	1	1	none
6	ProviderMD	6	1	1	none
11	UNIbcMD	0	1	0	none

```
C1|S12|L1D>show soam ma
```

```
MA index          : 1
MD index          : 1
MD level          : 0
MD name           : UNIabMD
MA name           : UNIabUntagged
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 10 20
Permission        : defer
VLAN ID list      : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 3
MD index          : 3
MD level          : 3
MD name           : OperatorMD
MA name           : OperatorCTag100
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 310 320
Permission        : defer
VLAN ID list      : ctype: 100
Primary VLAN ID   : 100
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 6
MD index          : 6
MD level          : 6
MD name           : ProviderMD
MA name           : ProviderCTag200
CCM interval      : 1s
MEPs              : 0
MEP ID list       : (0 MepIds)
Permission        : defer
VLAN ID list      : ctype: 200
Primary VLAN ID   : 200
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 11
MD index          : 11
```

Appendix E: SOAM Configuration Example – CLI Method

```
MD level           : 0
MD name           : UNIbcMD
MA name           : UNIbcUntagged
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 30 40
Permission        : defer
VLAN ID list      : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
C1|S12|L1D>show soam mip config
```

```
MIP id            : 311
MD local ID       : 3
MD level          : 3
MD name           : OperatorMD
VLANs             : ctype: 100
Port              : 1
Admin status      : enabled
```

```
MIP id            : 611
MD local ID       : 6
MD level          : 6
MD name           : ProviderMD
VLANs             : ctype: 200
Port              : 2
Admin status      : enabled
```

```
C1|S12|L1D>show soam mep config
```

```
MEP id            : 20
MD local ID       : 1
MD level          : 0
MD name           : UNIabMD
MA local ID       : 1
MA name           : UNIabUntagged
Direction         : down
Port              : 2
VLANs             : none
Primary VLAN      : 0
Admin status      : enabled
CCI status        : enabled
Fault notification state : Reset
Defects           :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon
```

```
MEP id            : 310
MD local ID       : 3
MD level          : 3
MD name           : OperatorMD
MA local ID       : 3
MA name           : OperatorCTag100
Direction         : up
```

```

Port                : 2
VLANs               : ctype: 100
Primary VLAN       : 100
Admin status       : enabled
CCI status         : enabled
Fault notification state : Reset
Defects            :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon

```

```

MEP id              : 30
MD local ID        : 11
MD level           : 0
MD name            : UNIbcMD
MA local ID        : 11
MA name            : UNIbcUntagged
Direction          : down
Port               : 1
VLANs              : none
Primary VLAN       : 0
Admin status       : enabled
CCI status         : enabled
Fault notification state : Reset
Defects            :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon

```

C1|S12|L1D>

C1|S12|L1D>show soam mep cc mep-id 20 local-parent-id 1

```

MEP ID              : 20
MD Local ID        : 1
MD level           : 0
MD name            : UNIabMD

Remote MEP ID      : 10
State              : OK
TimeStamp          : 73229.15 sec
MAC                : 00-C0-F2-42-01-16
RDI BIT           : False
Port Status        : No Port State
Interface Status   : No Interface Status
Chassis id subtype : None
Chassis id         :
Manage address domain : 0.0
Manage address     :
Autodetected       : No

```


Appendix E: SOAM Configuration Example – CLI Method

```
C1|S12|L1D>show soam mep cc mep-id 310 local-parent-id 3
MEP ID           : 310
MD Local ID      : 3
MD level         : 3
MD name          : OperatorMD
```

```
Remote MEP ID    : 320
State            : OK
TimeStamp        : 77828.94 sec
MAC              : 00-C0-F2-42-00-E0
RDI BIT         : False
Port Status      : No Port State
Interface Status : No Interface Status
Chassis id subtype : None
Chassis id       :
Manage address domain : 0.0
Manage address   :
Autodetected     : No
```

```
C1|S12|L1D>show soam mep cc mep-id 30 local-parent-id 11
MEP ID           : 30
MD Local ID      : 11
MD level         : 0
MD name          : UNIbcMD
```

```
Remote MEP ID    : 40
State            : OK
TimeStamp        : 75890.96 sec
MAC              : 00-C0-F2-42-00-DF
RDI BIT         : False
Port Status      : No Port State
Interface Status : No Interface Status
Chassis id subtype : None
Chassis id       :
Manage address domain : 0.0
Manage address   :
Autodetected     : No
```

```
C1|S12|L1D>
```

Configuring Device C – CLI Method

```
C1|S6|L1D>### DEVICE C ###
```

```
C1|S6|L1D>show soam md
```

Local MD ID	Name	Level	MAs	MIPs	Permission
3	OperatorMD	3	1	1	none
6	ProviderMD	6	1	1	none
11	UNIbcMD	0	1	0	none
111	UNIcdMD	0	1	0	none

```
C1|S6|L1D>show soam ma
```

```
MA index          : 3
MD index          : 3
MD level          : 3
MD name           : OperatorMD
MA name           : OperatorCTag100
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 310 320
Permission        : defer
VLAN ID list      : ctype: 100
Primary VLAN ID   : 100
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 6
MD index          : 6
MD level          : 6
MD name           : ProviderMD
MA name           : ProviderCTag200
CCM interval      : 1s
MEPs              : 0
MEP ID list       : (0 MepIds)
Permission        : defer
VLAN ID list      : ctype: 200
Primary VLAN ID   : 200
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 11
MD index          : 11
MD level          : 0
MD name           : UNIbcMD
MA name           : UNIbcUntagged
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 30 40
Permission        : defer
VLAN ID list      : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 111
MD index          : 111
```

Appendix E: SOAM Configuration Example – CLI Method

```

MD level           : 0
MD name           : UNICdMD
MA name           : UNICdUntagged
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 50 60
Permission        : defer
VLAN ID list      : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled

```

C1|S6|L1D>show soam mip config

```

MIP id            : 312
MD local ID       : 3
MD level          : 3
MD name           : OperatorMD
VLANs             : ctype: 100
Port              : 1
Admin status      : enabled

```

```

MIP id            : 612
MD local ID       : 6
MD level          : 6
MD name           : ProviderMD
VLANs             : ctype: 200
Port              : 2
Admin status      : enabled

```

C1|S6|L1D>show soam mep config

```

MEP id            : 320
MD local ID       : 3
MD level          : 3
MD name           : OperatorMD
MA local ID       : 3
MA name           : OperatorCTag100
Direction         : up
Port              : 2
VLANs             : ctype: 100
Primary VLAN      : 100
Admin status      : enabled
CCI status        : enabled
Fault notification state : Reset
Defects           :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon

```

```

MEP id            : 40
MD local ID       : 11
MD level          : 0
MD name           : UNIbcMD
MA local ID       : 11
MA name           : UNIbcUntagged
Direction         : down

```

```

Port                : 1
VLANs               : none
Primary VLAN       : 0
Admin status       : enabled
CCI status         : enabled
Fault notification state : Reset
Defects            :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon

```

```

MEP id             : 50
MD local ID       : 111
MD level          : 0
MD name           : UNICdMD
MA local ID       : 111
MA name           : UNICdUntagged
Direction         : down
Port              : 2
VLANs             : none
Primary VLAN      : 0
Admin status      : enabled
CCI status        : enabled
Fault notification state : Reset
Defects           :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon

```

C1|S6|L1D>

C1|S6|L1D>show soam mep cc mep-id 320 local-parent-id 3

```

MEP ID              : 320
MD Local ID        : 3
MD level           : 3
MD name            : OperatorMD

Remote MEP ID      : 310
State              : OK
TimeStamp          : 69334.5 sec
MAC               : 00-C0-F2-20-E2-18
RDI BIT           : False
Port Status       : No Port State
Interface Status  : No Interface Status
Chassis id subtype : None
Chassis id        :
Manage address domain : 0.0
Manage address    :
Autodetected     : No

```

Appendix E: SOAM Configuration Example – CLI Method

```
C1|S6|L1D>show soam mep cc mep-id 40 local-parent-id 11
MEP ID           : 40
MD Local ID      : 11
MD level         : 0
MD name          : UNIbcMD
```

```
Remote MEP ID    : 30
State            : OK
TimeStamp        : 67397.50 sec
MAC              : 00-C0-F2-20-E2-17
RDI BIT          : False
Port Status      : No Port State
Interface Status : No Interface Status
Chassis id subtype : None
Chassis id       :
Manage address domain : 0.0
Manage address    :
Autodetected     : No
```

```
C1|S6|L1D>show soam mep cc mep-id 50 local-parent-id 111
MEP ID           : 50
MD Local ID      : 111
MD level         : 0
MD name          : UNIdMD
```

```
C1|S6|L1D>
```

Configuring Device D – CLI Method

```
C1|S6|L1AP2|L2D>#### DEVICE D ###
```

```
C1|S6|L1AP2|L2D>show soam md
```

Local MD ID	Name	Level	MAs	MIPs	Permission
6	ProviderMD	6	1	0	none
111	UNICdMD	0	1	0	none

```
C1|S6|L1AP2|L2D>show soam ma
```

```
MA index          : 6
MD index          : 6
MD level          : 6
MD name           : ProviderMD
MA name           : ProviderCTag200
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 610 620
Permission        : defer
VLAN ID list      : ctype: 200
Primary VLAN ID   : 200
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
MA index          : 111
MD index          : 111
MD level          : 0
MD name           : UNICdMD
MA name           : UNICdUntagged
CCM interval      : 1s
MEPs              : 1
MEP ID list       : (2 MepIds) 50 60
Permission        : defer
VLAN ID list      : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
```

```
C1|S6|L1AP2|L2D>show soam mip config
```

The MIPs table is empty.

```
C1|S6|L1AP2|L2D>show soam mep config
```

```
MEP id            : 620
MD local ID       : 6
MD level          : 6
MD name           : ProviderMD
MA local ID       : 6
MA name           : ProviderCTag200
Direction         : down
Port              : 2
VLANs             : ctype: 200
Primary VLAN      : 200
Admin status      : enabled
CCI status        : enabled
Fault notification state : Reset
Defects           :
```

Appendix E: SOAM Configuration Example – CLI Method

```

Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority    : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time  : 10000 ms
Lowest Alarm priority   : macremerrxcon

```

```

MEP id                  : 60
MD local ID            : 111
MD level               : 0
MD name                : UNICdMD
MA local ID           : 111
MA name                : UNICdUntagged
Direction              : down
Port                   : 2
VLANs                  : none
Primary VLAN           : 0
Admin status           : enabled
CCI status             : enabled
Fault notification state : Reset
Defects                :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority    : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time  : 10000 ms
Lowest Alarm priority   : macremerrxcon

```

```
C1|S6|L1AP2|L2D>
```

```
C1|S6|L1AP2|L2D>
```

```
C1|S6|L1AP2|L2D>show soam mep cc mep-id 620 local-parent-id 6
```

```

MEP ID                  : 620
MD Local ID            : 6
MD level               : 6
MD name                : ProviderMD

Remote MEP ID          : 610
State                  : OK
TimeStamp              : 7054.16 sec
MAC                    : 00-C0-F2-42-01-16
RDI BIT                : False
Port Status            : No Port State
Interface Status       : No Interface Status
Chassis id subtype    : None
Chassis id             :
Manage address domain  : 0.0
Manage address         :
Autodetected           : No

```



```
C1|S6|L1AP2|L2D>show soam mep cc mep-id 60 local-parent-id 111
MEP ID : 60
MD Local ID : 111
MD level : 0
MD name : UNICdMD

Remote MEP ID : 50
State : OK
TimeStamp : 3853.31 sec
MAC : 00-C0-F2-42-00-E0
RDI BIT : False
Port Status : No Port State
Interface Status : No Interface Status
Chassis id subtype : None
Chassis id :
Manage address domain : 0.0
Manage address :
Autodetected : No

C1|S6|L1AP2|L2D>
```

Y.1731 Configuration Example

A sample configuration using ITU-T Y.1731 is shown below.

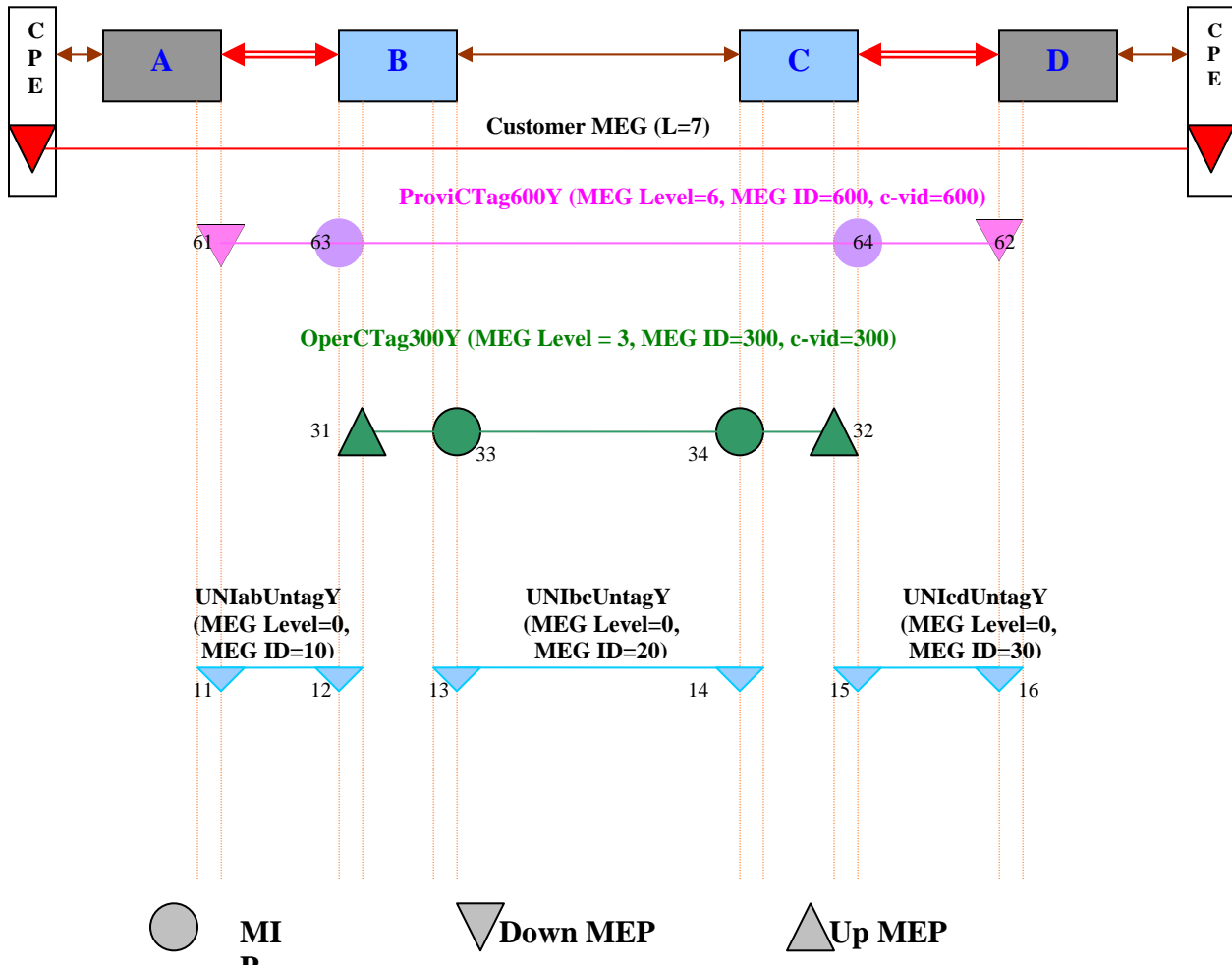


Figure E-5: ITU-T Y.1731 Configuration Example

ITU-T Y.1731 Configuration Example (Devices A, B, C, D)

A sample configuration using ITU-T Y.1731 is provided below.

```
*****
* Y.1731 (All MEGs on different CTAGs) *
*****

## Device A #####
## Level 0 UNI ##
add soam meg local-meg-id 10 meg-name UNIabUntagY meg-level 0 vlan-type none
set soam meg local-meg-id 10 attr_name mepid-add attr_value 11
set soam meg local-meg-id 10 attr_name mepid-add attr_value 12
add soam mep mep-id 11 local-parent-id 10 direction down port 2
set soam mep config mep-id 11 local-parent-id 10 attr_name admin attr_value enable
set soam mep config mep-id 11 local-parent-id 10 attr_name cci attr_value enable

## Level 6 Provider MD ##
add soam meg local-meg-id 600 meg-name ProvCTag600Y meg-level 6 vlan-type ctype 600
set soam meg local-meg-id 600 attr_name mepid-add attr_value 61
set soam meg local-meg-id 600 attr_name mepid-add attr_value 62
add soam mep mep-id 61 local-parent-id 600 direction down port 2
set soam mep config mep-id 61 local-parent-id 600 attr_name admin attr_value enable
set soam mep config mep-id 61 local-parent-id 600 attr_name cci attr_value enable
set soam mep config mep-id 61 local-parent-id 600 attr_name aisprocess attr_value enable

## Device B #####

## Level 0 UNI ##
add soam meg local-meg-id 10 meg-name UNIabUntagY meg-level 0 vlan-type none
set soam meg local-meg-id 10 attr_name mepid-add attr_value 11
set soam meg local-meg-id 10 attr_name mepid-add attr_value 12
add soam mep mep-id 12 local-parent-id 10 direction down port 2
set soam mep config mep-id 12 local-parent-id 10 attr_name admin attr_value enable
set soam mep config mep-id 12 local-parent-id 10 attr_name cci attr_value enable

## Level 0 UNI ##
add soam meg local-meg-id 20 meg-name UNIbcUntagY meg-level 0 vlan-type none
set soam meg local-meg-id 20 attr_name mepid-add attr_value 13
set soam meg local-meg-id 20 attr_name mepid-add attr_value 14
add soam mep mep-id 13 local-parent-id 20 direction down port 1
set soam mep config mep-id 13 local-parent-id 20 attr_name admin attr_value enable
set soam mep config mep-id 13 local-parent-id 20 attr_name cci attr_value enable
set soam mep config mep-id 13 local-parent-id 20 attr_name aisprocess attr_value enable
set soam mep config mep-id 13 local-parent-id 20 attr_name aisnotifyup attr_value enable
set soam mep config mep-id 13 local-parent-id 20 attr_name aistransmit attr_value enable
set soam mep config mep-id 13 local-parent-id 20 attr_name aisclient-add attr_value MIP33
```

Appendix E: SOAM Configuration Example – CLI Method

Level 3 Operator MD

```
add soam meg local-meg-id 300 meg-name OperCTag300Y meg-level 3 vlan-type ctype 300
set soam meg local-meg-id 300 attr_name mepid-add attr_value 31
set soam meg local-meg-id 300 attr_name mepid-add attr_value 32
add soam mep mep-id 31 local-parent-id 300 direction up port 2
set soam mep config mep-id 31 local-parent-id 300 attr_name admin attr_value enable
set soam mep config mep-id 31 local-parent-id 300 attr_name cci attr_value enable
set soam mep config mep-id 31 local-parent-id 300 attr_name aisprocess attr_value enable
set soam mep config mep-id 31 local-parent-id 300 attr_name aisnotifyup attr_value enable
set soam mep config mep-id 31 local-parent-id 300 attr_name aistransmit attr_value enable
set soam mep config mep-id 31 local-parent-id 300 attr_name aisclient-add attr_value MIP63
add soam mip mip-type y.1731 local-mip-id 33 local-parent-id 300 port 1
set soam mip local-mip-id 33 attr-name admin attr-val enable
set soam mip local-mip-id 33 attr-name aistransmit attr-val enable
```

Level 6 Provider MD

```
add soam meg local-meg-id 600 meg-name ProvCTag600Y meg-level 6 vlan-type ctype 600
add soam mip mip-type y.1731 local-mip-id 63 local-parent-id 600 port 2
set soam mip local-mip-id 63 attr-name admin attr-val enable
set soam mip local-mip-id 63 attr-name aistransmit attr-val enable
```

```

## Device C #####
## Level 0 UNI ##
add soam meg local-meg-id 20 meg-name UNIBCUntagY meg-level 0 vlan-type none
set soam meg local-meg-id 20 attr_name mepid-add attr_value 13
set soam meg local-meg-id 20 attr_name mepid-add attr_value 14
add soam mep mep-id 14 local-parent-id 20 direction down port 1
set soam mep config mep-id 14 local-parent-id 20 attr_name admin attr_value enable
set soam mep config mep-id 14 local-parent-id 20 attr_name cci attr_value enable
set soam mep config mep-id 14 local-parent-id 20 attr_name aisprocess attr_value enable
set soam mep config mep-id 14 local-parent-id 20 attr_name aisnotifyup attr_value enable
set soam mep config mep-id 14 local-parent-id 20 attr_name aistransmit attr_value enable
set soam mep config mep-id 14 local-parent-id 20 attr_name aisclient-add attr_value MIP34

## Level 0 UNI ##
add soam meg local-meg-id 30 meg-name UNICdUntagY meg-level 0 vlan-type none
set soam meg local-meg-id 30 attr_name mepid-add attr_value 15
set soam meg local-meg-id 30 attr_name mepid-add attr_value 16
add soam mep mep-id 15 local-parent-id 30 direction down port 2
set soam mep config mep-id 15 local-parent-id 30 attr_name admin attr_value enable
set soam mep config mep-id 15 local-parent-id 30 attr_name cci attr_value enable

## Level 3 Operator MD ##
add soam meg local-meg-id 300 meg-name OperCTag300Y meg-level 3 vlan-type ctype 300
set soam meg local-meg-id 300 attr_name mepid-add attr_value 31
set soam meg local-meg-id 300 attr_name mepid-add attr_value 32
add soam mep mep-id 32 local-parent-id 300 direction up port 2
set soam mep config mep-id 32 local-parent-id 300 attr_name admin attr_value enable
set soam mep config mep-id 32 local-parent-id 300 attr_name cci attr_value enable
set soam mep config mep-id 32 local-parent-id 300 attr_name aisprocess attr_value enable
set soam mep config mep-id 32 local-parent-id 300 attr_name aisprocess attr_value enable
set soam mep config mep-id 32 local-parent-id 300 attr_name aisnotifyup attr_value enable
set soam mep config mep-id 32 local-parent-id 300 attr_name aistransmit attr_value enable
set soam mep config mep-id 32 local-parent-id 300 attr_name aisclient-add attr_value MIP64
add soam mip mip-type y.1731 local-mip-id 34 local-parent-id 300 port 1
set soam mip local-mip-id 34 attr-name admin attr-val enable
set soam mip local-mip-id 34 attr-name aistransmit attr-val enable

## Level 6 Provider MD ##
add soam meg local-meg-id 600 meg-name ProvCTag600Y meg-level 6 vlan-type ctype 600
add soam mip mip-type y.1731 local-mip-id 64 local-parent-id 600 port 2
set soam mip local-mip-id 64 attr-name admin attr-val enable
set soam mip local-mip-id 64 attr-name aistransmit attr-val enable

## Device D #####
## Level 0 UNI ##
add soam meg local-meg-id 30 meg-name UNICdUntagY meg-level 0 vlan-type none
set soam meg local-meg-id 30 attr_name mepid-add attr_value 15
set soam meg local-meg-id 30 attr_name mepid-add attr_value 16
add soam mep mep-id 16 local-parent-id 30 direction down port 2
set soam mep config mep-id 16 local-parent-id 30 attr_name admin
attr_value enable
set soam mep config mep-id 16 local-parent-id 30 attr_name cci attr_value enable

```

Appendix E: SOAM Configuration Example – CLI Method

Level 6 Provider MD

```
add soam meg local-meg-id 600 meg-name ProvCTag600Y meg-level 6 vlan-type ctype 600
set soam meg local-meg-id 600 attr_name mepid-add attr_value 61
set soam meg local-meg-id 600 attr_name mepid-add attr_value 62
add soam mep mep-id 62 local-parent-id 600 direction down port 2
set soam mep config mep-id 62 local-parent-id 600 attr_name admin
attr_value enable
set soam mep config mep-id 62 local-parent-id 600 attr_name cci attr_value enable
set soam mep config mep-id 62 local-parent-id 600 attr_name aisprocess attr_value enable
```

Configuring Device A – CLI Method

```

C1|S12|L1AP2|L2D>### DEVICE A ####
C1|S12|L1AP2|L2D>show soam meg
MEG index           : 10
MEG level           : 0
MEG name            : UNIabUntagY
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 11 12
Permission          : none
VLAN ID list        : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 600
MEG level           : 6
MEG name            : ProvCTag600Y
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 61 62
Permission          : none
VLAN ID list        : ctype: 600
Primary VLAN ID     : 600
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

C1|S12|L1AP2|L2D>show soam mep config
MEP id              : 11
MEG local ID        : 10
MEG level           : 0
MEG name            : UNIabUntagY
Direction           : down
Port                : 2
VLANs               : none
Primary VLAN        : 0
Admin status        : enabled
CCI status          : enabled
Fault notification state : Reset
Defects             :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon
AIS transmit        : disabled
AIS interval        : 1 second
AIS process         : disabled
AIS notify up       : disabled
AIS client list     : (0 MEPs, 0 MIPs)

```


Appendix E: SOAM Configuration Example – CLI Method

```

AIS frame priority      : 1

MEP id                 : 61
MEG local ID          : 600
MEG level              : 6
MEG name               : ProvCTag600Y
Direction              : down
Port                   : 2
VLANs                  : ctype: 600
Primary VLAN           : 600
Admin status           : enabled
CCI status             : enabled
Fault notification state : Reset
Defects                :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority   : macremerrxcon
AIS transmit           : disabled
AIS interval           : 1 second
AIS process            : enabled
AIS notify up          : disabled
AIS client list        : (0 MEPs, 0 MIPs)
AIS frame priority     : 1

```

```
C1|S12|L1AP2|L2D>show soam mip config
```

The MIPs table is empty.

```
C1|S12|L1AP2|L2D>
```

```
C1|S12|L1AP2|L2D>show soam mep cc mep-id 11 local-parent-id 10
```

```

MEP ID                 : 11
MEG Local ID           : 0
MEG level              : 0
MEG name               : UNIabUntagY

Remote MEP ID         : 12
State                  : OK
TimeStamp              : 238.98 sec
MAC                    : 00-C0-F2-20-E2-18
RDI BIT                : False
Port Status            : No Port State
Interface Status       : No Interface Status
Chassis id subtype    : None
Chassis id             :
Manage address domain : 0.0
Manage address         :
Autodetected           : No

```

```
C1|S12|L1AP2|L2D>show soam mep cc mep-id 61 local-parent-id 600
```

```

MEP ID                 : 61
MEG Local ID           : 0
MEG level              : 6
MEG name               : ProvCTag600Y

Remote MEP ID         : 62
State                  : OK

```

```
TimeStamp          : 3644.96 sec
MAC                : 00-C0-F2-42-01-8E
RDI BIT           : False
Port Status        : No Port State
Interface Status   : No Interface Status
Chassis id subtype : None
Chassis id         :
Manage address domain : 0.0
Manage address     :
Autodetected       : No
```

Configuring Device B – CLI Method

```
C1|S12|L1D>### DEVICE B ###
C1|S12|L1D>
C1|S12|L1D>show soam meg
MEG index           : 10
MEG level           : 0
MEG name            : UNIabUntagY
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 11 12
Permission          : none
VLAN ID list        : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 20
MEG level           : 0
MEG name            : UNIbcUntagY
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 13 14
Permission          : none
VLAN ID list        : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 300
MEG level           : 3
MEG name            : OperCTag300Y
CCM interval        : 1s
MEPs                : 1
MIPs                : 1
MEP ID list         : (2 MepIds) 31 32
Permission          : none
VLAN ID list        : ctype: 300
Primary VLAN ID     : 300
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 600
MEG level           : 6
MEG name            : ProvCTag600Y
CCM interval        : 1s
MEPs                : 0
MIPs                : 1
MEP ID list         : (0 MepIds)
Permission          : none
VLAN ID list        : ctype: 600
Primary VLAN ID     : 600
```

```
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking      : disabled
```

```
C1|S12|L1D>show soam mep config
MEP id                : 12
MEG local ID          : 10
MEG level              : 0
MEG name               : UNIabUntagY
Direction             : down
Port                  : 2
VLANs                 : none
Primary VLAN          : 0
Admin status          : enabled
CCI status             : enabled
Fault notification state : Reset
Defects               :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority  : macremerrxcon
AIS transmit          : disabled
AIS interval          : 1 second
AIS process            : disabled
AIS notify up         : disabled
AIS client list       : (0 MEPs, 0 MIPs)
AIS frame priority    : 1
```

```
MEP id                : 13
MEG local ID          : 20
MEG level              : 0
MEG name               : UNIbcUntagY
Direction             : down
Port                  : 1
VLANs                 : none
Primary VLAN          : 0
Admin status          : enabled
CCI status             : enabled
Fault notification state : Reset
Defects               :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority  : macremerrxcon
AIS transmit          : enabled
AIS interval          : 1 second
AIS process            : enabled
AIS notify up         : enabled
AIS client list       : (0 MEPs, 1 MIPs) MIP33
AIS frame priority    : 1
```

```
MEP id                : 31
MEG local ID          : 300
```

Appendix E: SOAM Configuration Example – CLI Method

```

MEG level           : 3
MEG name            : OperCTag300Y
Direction           : up
Port                : 2
VLANs               : ctype: 300
Primary VLAN        : 300
Admin status        : enabled
CCI status          : enabled
Fault notification state : Reset
Defects             :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon
AIS transmit        : enabled
AIS interval        : 1 second
AIS process         : enabled
AIS notify up       : enabled
AIS client list     : (0 MEPs, 1 MIPs) MIP63
AIS frame priority  : 1

```

```
C1|S12|L1D>show soam mip config
```

```

MIP id              : 33
MEG local ID        : 300
MEG level           : 3
MEG name            : OperCTag300Y
VLANs               : ctype: 300
Port                : 1
Admin status        : enabled
AIS transmit        : enabled
AIS interval        : 1 second
AIS frame priority  : 7

```

```

MIP id              : 63
MEG local ID        : 600
MEG level           : 6
MEG name            : ProvCTag600Y
VLANs               : ctype: 600
Port                : 2
Admin status        : enabled
AIS transmit        : enabled
AIS interval        : 1 second
AIS frame priority  : 7

```

```
C1|S12|L1D>show soam mep cc mep-id 31 local-parent-id 300
```

```

MEP ID              : 31
MEG Local ID        : 0
MEG level           : 3
MEG name            : OperCTag300Y

```

```

Remote MEP ID       : 32
State                : OK
TimeStamp            : 3408.97 sec
MAC                  : 00-C0-F2-42-00-E0
RDI BIT              : False

```

```

Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype    : None
Chassis id            :
Manage address domain : 0.0
Manage address        :
Autodetected          : No

C1|S12|L1D>show soam mep cc mep-id 12 local-parent-id 10
MEP ID                : 12
MEG Local ID          : 0
MEG level              : 0
MEG name               : UNIabUntagY

Remote MEP ID         : 11
State                  : OK
TimeStamp              : 3.48 sec
MAC                    : 00-C0-F2-42-01-16
RDI BIT                : False
Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype    : None
Chassis id            :
Manage address domain : 0.0
Manage address        :
Autodetected          : No

C1|S12|L1D>show soam mep cc mep-id 13 local-parent-id 20
MEP ID                : 13
MEG Local ID          : 0
MEG level              : 0
MEG name               : UNIbcUntagY

Remote MEP ID         : 14
State                  : OK
TimeStamp              : 399543.9 sec
MAC                    : 00-C0-F2-42-00-DF
RDI BIT                : False
Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype    : None
Chassis id            :
Manage address domain : 0.0
Manage address        :
Autodetected          : No

C1|S12|L1D>

```

Configuring Device C – CLI Method

```
C1|S6|L1D>### DEVICE C ####
C1|S6|L1D>
C1|S6|L1D>show soam meg
MEG index           : 20
MEG level           : 0
MEG name            : UNIbcUntagY
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 13 14
Permission          : none
VLAN ID list        : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 30
MEG level           : 0
MEG name            : UNIcdUntagY
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 15 16
Permission          : none
VLAN ID list        : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 300
MEG level           : 3
MEG name            : OperCTag300Y
CCM interval        : 1s
MEPs                : 1
MIPs                : 1
MEP ID list         : (2 MepIds) 31 32
Permission          : none
VLAN ID list        : ctype: 300
Primary VLAN ID     : 300
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 600
MEG level           : 6
MEG name            : ProvCTag600Y
CCM interval        : 1s
MEPs                : 0
MIPs                : 1
MEP ID list         : (0 MepIds)
Permission          : none
VLAN ID list        : ctype: 600
Primary VLAN ID     : 600
```



```
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking      : disabled
```

```
C1|S6|L1D>show soam mep config
```

```
MEP id          : 14
MEG local ID    : 20
MEG level       : 0
MEG name        : UNIbcUntagY
Direction      : down
Port           : 1
VLANs          : none
Primary VLAN    : 0
Admin status    : enabled
CCI status      : enabled
Fault notification state : Reset
Defects        :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority  : macremerrxcon
AIS transmit         : enabled
AIS interval         : 1 second
AIS process          : enabled
AIS notify up        : enabled
AIS client list      : (0 MEPs, 1 MIPs) MIP34
AIS frame priority   : 1
```

```
MEP id          : 15
MEG local ID    : 30
MEG level       : 0
MEG name        : UNIcdUntagY
Direction      : down
Port           : 2
VLANs          : none
Primary VLAN    : 0
Admin status    : enabled
CCI status      : enabled
Fault notification state : Reset
Defects        :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority   : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority  : macremerrxcon
AIS transmit         : disabled
AIS interval         : 1 second
AIS process          : disabled
AIS notify up        : disabled
AIS client list      : (0 MEPs, 0 MIPs)
AIS frame priority   : 1
```

```
MEP id          : 32
MEG local ID    : 300
```

Appendix E: SOAM Configuration Example – CLI Method

```

MEG level           : 3
MEG name            : OperCTag300Y
Direction           : up
Port                : 2
VLANs               : ctype: 300
Primary VLAN        : 300
Admin status        : enabled
CCI status          : enabled
Fault notification state : Reset
Defects             :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon
AIS transmit        : enabled
AIS interval        : 1 second
AIS process         : enabled
AIS notify up       : enabled
AIS client list     : (0 MEPs, 1 MIPs) MIP64
AIS frame priority  : 1

```

```
C1|S6|L1D>show soam mip config
```

```

MIP id              : 34
MEG local ID        : 300
MEG level           : 3
MEG name            : OperCTag300Y
VLANs               : ctype: 300
Port                : 1
Admin status        : enabled
AIS transmit        : enabled
AIS interval        : 1 second
AIS frame priority  : 7

```

```

MIP id              : 64
MEG local ID        : 600
MEG level           : 6
MEG name            : ProvCTag600Y
VLANs               : ctype: 600
Port                : 2
Admin status        : enabled
AIS transmit        : enabled
AIS interval        : 1 second
AIS frame priority  : 7

```

```
C1|S6|L1D>show soam mep cc mep-id 32 local-parent-id 300
```

```

MEP ID              : 32
MEG Local ID        : 0
MEG level           : 3
MEG name            : OperCTag300Y

```

```

Remote MEP ID       : 31
State                : OK
TimeStamp           : 258076.32 sec
MAC                 : 00-C0-F2-20-E2-18
RDI BIT             : False

```

```

Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype   : None
Chassis id           :
Manage address domain : 0.0
Manage address       :
Autodetected         : No

C1|S6|L1D>show soam mep cc mep-id 14 local-parent-id 20
MEP ID                : 14
MEG Local ID         : 0
MEG level             : 0
MEG name              : UNIbcUntagY

Remote MEP ID        : 13
State                 : OK
TimeStamp             : 653995.52 sec
MAC                   : 00-C0-F2-20-E2-17
RDI BIT               : False
Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype   : None
Chassis id           :
Manage address domain : 0.0
Manage address       :
Autodetected         : No

C1|S6|L1D>show soam mep cc mep-id 15 local-parent-id 30
MEP ID                : 15
MEG Local ID         : 0
MEG level             : 0
MEG name              : UNIcdUntagY

Remote MEP ID        : 16
State                 : OK
TimeStamp             : 172726.51 sec
MAC                   : 00-C0-F2-42-01-8E
RDI BIT               : False
Port Status           : No Port State
Interface Status      : No Interface Status
Chassis id subtype   : None
Chassis id           :
Manage address domain : 0.0
Manage address       :
Autodetected         : No

C1|S6|L1D>

```

Configuring Device D – CLI Method

```
C1|S6|L1AP2|L2D>### DEVICE D ###
C1|S6|L1AP2|L2D>
C1|S6|L1AP2|L2D>show soam meg
MEG index           : 30
MEG level           : 0
MEG name            : UNICdUntagY
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 15 16
Permission          : none
VLAN ID list        : none
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

MEG index           : 600
MEG level           : 6
MEG name            : ProvCTag600Y
CCM interval        : 1s
MEPs                : 1
MIPs                : 0
MEP ID list         : (2 MepIds) 61 62
Permission          : none
VLAN ID list        : ctype: 600
Primary VLAN ID     : 600
Auto detection timeout : 4000
Auto detect remote MEP : disabled
CCI interworking    : disabled

C1|S6|L1AP2|L2D>show soam mep config
MEP id              : 16
MEG local ID        : 30
MEG level           : 0
MEG name            : UNICdUntagY
Direction           : down
Port                : 2
VLANs               : none
Primary VLAN        : 0
Admin status        : enabled
CCI status          : enabled
Fault notification state : Reset
Defects             :
Next LTM transaction ID : 1
Next LBM transaction ID : 1
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon
AIS transmit        : disabled
AIS interval        : 1 second
AIS process         : disabled
AIS notify up       : disabled
```

```

AIS client list      : (0 MEPs, 0 MIPs)
AIS frame priority  : 1

MEP id              : 62
MEG local ID       : 600
MEG level          : 6
MEG name           : ProvCTag600Y
Direction         : down
Port               : 2
VLANs              : ctype: 600
Primary VLAN       : 600
Admin status       : enabled
CCI status         : enabled
Fault notification state : Reset
Defects            :
Next LTM transaction ID : 2
Next LBM transaction ID : 2
CCM and LTM priority : 7
Fault Alarm Detect Time : 2500 ms
Fault Alarm Reset Time : 10000 ms
Lowest Alarm priority : macremerrxcon
AIS transmit       : disabled
AIS interval       : 1 second
AIS process        : enabled
AIS notify up      : disabled
AIS client list    : (0 MEPs, 0 MIPs)
AIS frame priority : 1

```

```
C1|S6|L1AP2|L2D>show soam mip config
```

The MIPs table is empty.

```
C1|S6|L1AP2|L2D>
```

```
C1|S6|L1AP2|L2D>show soam mep cc mep-id 62 local-parent-id 600
```

```

MEP ID              : 62
MEG Local ID       : 0
MEG level          : 6
MEG name           : ProvCTag600Y

Remote MEP ID      : 61
State              : OK
TimeStamp          : 105380.75 sec
MAC                : 00-C0-F2-42-01-16
RDI BIT            : False
Port Status        : No Port State
Interface Status   : No Interface Status
Chassis id subtype : None
Chassis id         :
Manage address domain : 0.0
Manage address     :
Autodetected       : No

```

```
C1|S6|L1AP2|L2D>show soam mep cc mep-id 16 local-parent-id 30
```

```

MEP ID              : 16
MEG Local ID       : 0
MEG level          : 0
MEG name           : UNICdUntagY

Remote MEP ID      : 15

```

Appendix E: SOAM Configuration Example – CLI Method

```
State : OK
TimeStamp : 20030.83 sec
MAC : 00-C0-F2-42-00-E0
RDI BIT : False
Port Status : No Port State
Interface Status : No Interface Status
Chassis id subtype : None
Chassis id :
Manage address domain : 0.0
Manage address :
Autodetected : No
```

For More Information

Transition Networks has designed their full-featured products to include the most advanced features on the market today. Please utilize the following resources to learn more about this or other advanced features from Transition Networks, Inc.

- Documentation on the ION system CD.
- x323x Remotely Managed NID User Guide (PN 33432)
- ION Systems Command Line Interface (CLI) Reference Manual (PN 33461)
- Advanced Product Features literature available at the Transition Networks web site at www.transition.com
- Transition Networks Learning Center: <http://www.transition.com/TransitionNetworks/Learning/Seminar/Description.aspx>
- Transition Networks Tech Support: <http://www.transition.com/TransitionNetworks/TechSupport/Contact.aspx>
- ITU-T - [Recommendations](#) page.
- IEEE 802 [Standards](#) page
- Metro Ethernet Forum – MEF [Specifications](#) page.
- IETF - Request for Comments (RFC) <http://www.ietf.org/rfc.html> page.

To contact Transition Networks directly, call us at 800-526-9267 or +1-952-941-7600.

Appendix F: VLAN Tunneling Configuration Examples

This appendix provides sample VLAN configurations using both the CLI method and the Web method.

There are four different VLAN properties for a port configured in a VLAN entry at the ION System Level in the VLAN database:

- 1) **NoMod**: the frame maps to this VLAN egress unmodified out on this port (frame maps to a VLAN id when it ingresses a port, the VLAN id is mapped based on either the existing VID if it is already tagged or the port default VLAN ID if untagged).
- 2) **Tag**: the frame maps to this VLAN egress tagged out on this port.
- 3) **UnTag**: the frame maps to this VLAN egress untagged out on this port.
- 4) **notMember**: frame maps to this VLAN will not be forwarded out on this port.

The ports can be configured in one of three Frame Tag modes:

- 1) **Customer**: this is VLAN unaware mode. This means that if a VLAN entry has this port member property as Tag or UnTag.
- 2) **Network**: enables Dot1.Q Mode. Whenever tagging/untagging is required, all of the participating ports must be configured as Network. This includes the port that is facing the untagged traffic as well.
- 3) **Provider**: (Provider EtherTypes X8100, X9100, X88A8) - this mode will ensure that the frame egressing this port will always have the S-Tag added, regardless of whether the ingress frame was already C-Tagged (Case E) or plain untagged (Case B).

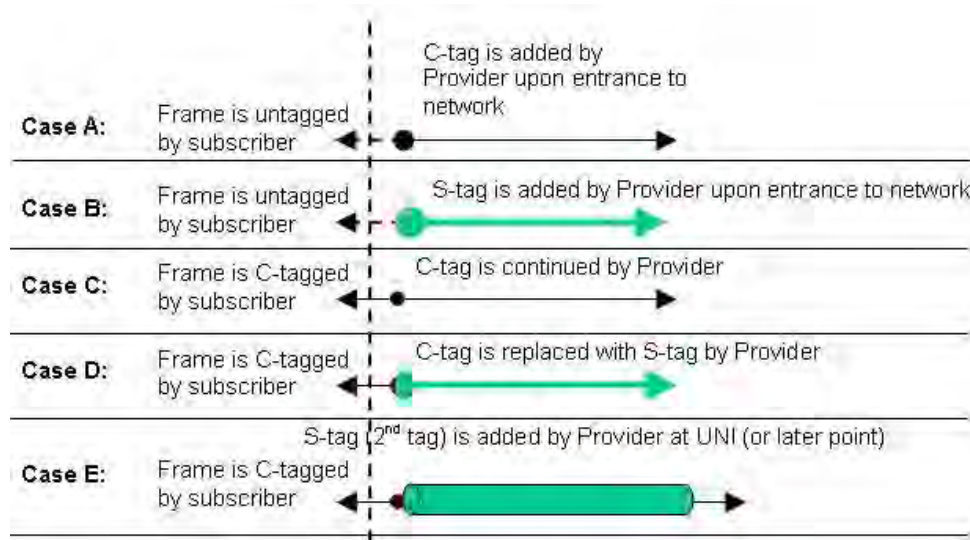


Figure F-1: VLAN Tagging Example

VLAN Tunneling can be configured using either the CLI or Web method.

VLAN Tunneling Config – CLI Method

See the “*ION Systems CLI Reference Manual – 33461*” for the various VLAN commands (Management VLAN, Device-level, and Port-level VLAN commands). Certain commands can only be entered when the last part of the command line prompt indicates the location is a device (L1D, L2D or L3D). Not all of the steps (CLI commands) below are required for each possible VLAN configuration.

Note: VLAN 1 is the default VLAN and you cannot Edit or Delete it.

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Add a VLAN Database Entry. This adds a new VLAN to the device. By default, VLAN ID one (VID 1) is defined for internal use. Type:

add vlan-db vid=<xx> [priority=<yy>] [pri-override={enable | disable}]

where:

xx = ID (2–4094) of the VLAN to which the device is to become a member

yy = optional; priority for frames

3. Set the VLAN Database Member/Egress Tagging. This sets the priority of a row of the VLAN forwarding database. Type:

set vlan-db vid=<xx> port=<yy> memetag=<zz>

set vlan-db vid= <xx> fid=<yy> pri-override=<aa> priority=<bb>

Where:

ww =

xx = number that identifies the VLAN (2–4094)

yy = logical port index or fid

zz = valid memetag choices are:

- noMod
- unTag
- tag
- notMember

aa = pri-override={enable | disable}

bb = priority = {0-7}

4. Press **Enter**.
5. Set the Management VLAN admin state to enable. Type:

set mgmt vlan state=enable

6. Press **Enter**.

7. Select the management VLAN ports. Type:

set mgmt vlan port=port-list

Where:

Port-list = a management VLAN port (1-19)

Example: C1 | S13 | 10d /> **set mgmt vlan port=1,2**

8. Press **Enter**.

9. Set the port discard untagged non-management frames option to true if untagged non-management frames are to be discarded for this port. Type:

set port discard-untagged=truth-val

Where:

Truth-val = true or false

Example: C1 | S13 | 10ap1 | 11p2 /> **set port discard-untagged=true**

10. Press **Enter**.

11. Set the port discard tagged non-management frames option to true if the tagged non-management frames for this port are to be discarded. Type:
set port discard-tagged=truth-val
 Where:
 Truth-val = true or false
 Example: C1 | S13 | 10ap1 | 11p2 /> **set port discard-tagged=true**
12. Press **Enter**.
13. Set the port default VLAN-ID for this port. Type:
set port default-vid=vid
 Where:
 vid = 2 - 4094
 Example: C1 | S13 | 10ap1 | 11p2 /> **set port default-vid=2**
14. Press **Enter**.
15. Set if force port to use default VLAN-ID. If set to true, this forces all untagged and 802.1Q tagged frames to assume the default VLAN-ID. Type:
set port force-default-vid=truth-val
 Where:
 Truth-val = true or false
 Example: C1 | S13 | 10ap1 | 11p2 /> **set port force-default-vid=true**
16. Press **Enter**.
17. Set the port VLAN tag mode of a port interface. Type:
set port vlan tag mode=tagmode
 Where:
 tagmode = **network, provider, or customer**
 Example: C1 | S13 | 10ap1 | 11p2 /> **set port vlan tag mode=provider**
18. Press **Enter**.
19. Set Ethernet type if the VLAN tagging mode was set to *provider* in step 17.
 Type:
set port vlan tag provider ethtype=type
 Where:
 ethtype = x8100, x88a8, or x9100
 Example: C1 | S13 | 10ap1 | 11p2 /> **set port vlan tag provider ethtype=x8100**
20. Add a new row in the VLAN forwarding database. Type:
add vlan-db vid=vlan-id [priority=prio] [pri-override=override]
 Where:
 vlan-id = 1-4094
 prio = the priority for frames (0-7)
 pri-override = enable or disable
 Example:
 C1 | S13 | 10ap1 | 11p2 /> **add vlan-db vid=3 priority=1 pri-override=enable**
21. Press **Enter**.
22. Set the priority override of a VLAN forwarding database row. This sets the override priority on frames associated with this VID of the VLAN forwarding database. Type:
set vlan-db vid=vlan-id fid=fid pri-override=override
 Where:
 vlan-id = 1-4094
 fid = 0
 override = enable or disable (specify if override priority on frames enabled in step 18)
 Example:
 C1 | S13 | 10ap1 | 11p2 /> **set vlan-db vid=3 fid=0 pri-override=enable**
23. Press **Enter**.

Appendix F: VLAN Tunneling Configuration Examples

24. Set the priority of a VLAN forwarding database row. Type:

```
set vlan-db vid=vlan-id fid=fid priority=prio
```

Where:

vlan-id = 2-4094

fid = 0

Prio = priority for frames (0-8)

Example: C1|S13|10ap1|11p2/>**set vlan-db vid=3 fid=0 priority=2**

25. Press **Enter**.

26. Set the member and egress tagging of a VLAN forwarding database row. Type:

```
set vlan-db vid=vlan-id port=port-id memetag=memetag_mode
```

Where:

vlan-id = 1-4094

port-id = logical port index

Memetag_mode = noMod, notMember, tag, unTag

Example:

C1|S13|10ap1|11p2/>**set vlan-db vid=3 port=2 memetag=tag**

27. Press **Enter**.

28. Use the CLI commands to verify your VLAN configuration(s).

- Show all existing VLAN(s) on the NID. Type **show vlan config** and press **Enter**.

For example:

```
C1|S13|L0D/>show vlan config
```

vid	fid	priority	p-override	port1	port2	port3
1	0	0	disable	NoMod	NoMod	notApp

- Show the Management VLAN configuration. Type **show mgmt vlan config** and press **Enter** to show the management VLAN configuration on a device. Example:

```
C1|S13|10d/>show mgmt vlan config
```

vlan id	vlan state	vlan portlist
0	enable	none

- Show the VLAN Service configuration on a device. Type **show vlan service** and press **Enter**. Example:

```
C1|S13|10d/> show vlan service
```

```
VLAN service connection type:      customerProvider
VLAN service VID for tag:          8
VLAN service Ethernet Type for tag: 0x8100
VLAN translation type:             untagged to untagged
```

- Show the Port VLAN configuration. Type **show port vlan config** and press **Enter**. For example:

```
C1|S13|10ap1|11p2/>show port vlan config
```

```
Dot1q state:          vlanEnabled
Discard-tagged:       false
Discard-untagged:    false
Default VLAN id:     22
Force use default VLAN id: false
```

- Show the Port VLAN Tag configuration. Type **show port vlan tag config** and press **Enter**. For example:

```
C1|S13|10ap1|11p2/>show port vlan tag config
Tagging mode:          network
Network tagging:      addTag
```

- Show the VLAN forwarding database configuration for the device. Type **show vlan-db config** and press **Enter**. For example:

```
C1|S13|11d>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
```

29. Click the **Add** button to add the newly-defined VLAN.

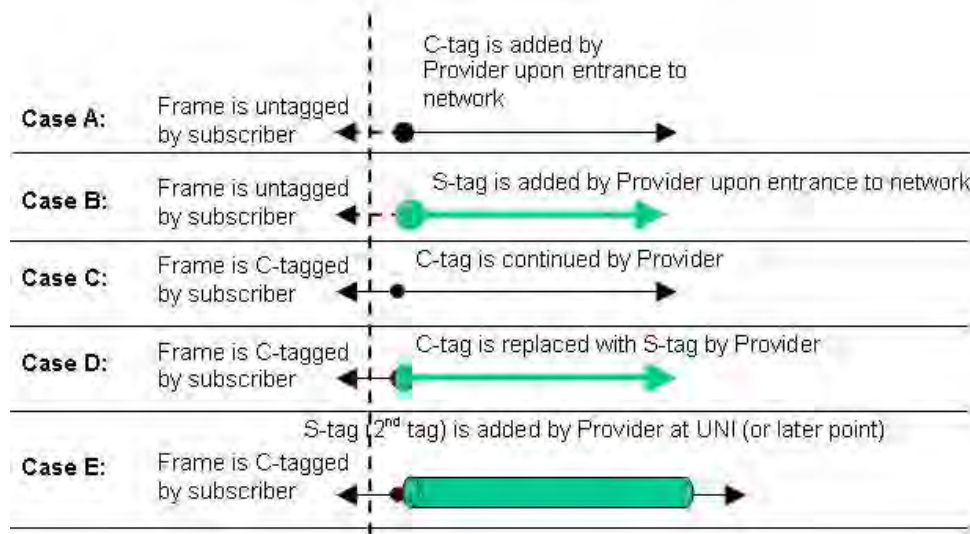
30. Verify the SOAM configuration. Type **show soam conferror vid=xx port=<xx>** and press **Enter**. For example:

```
C1|S10|L1D>show soam conferror vid 1 port 1
No config errors.
```

VLAN Tunneling Config – Web Method

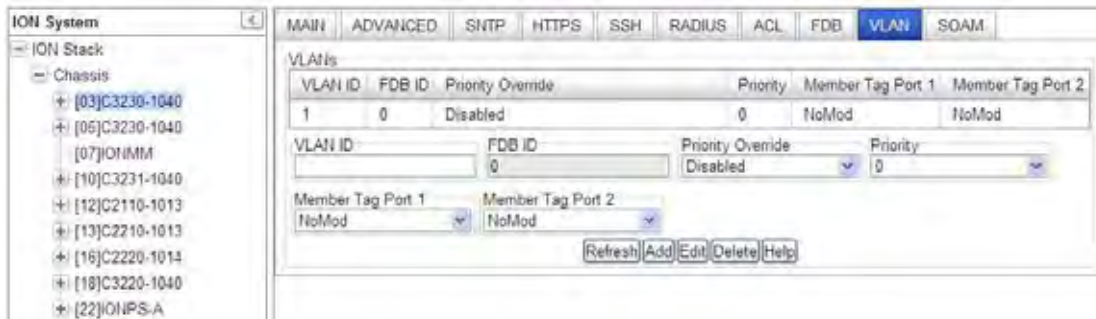
Configuring VLAN 100 with Provider S-Tag

This procedure is used to configure an untagged customer VLAN (e.g., VLAN 100) on C322x and S323x models and how to add an S-Tag (x88A8) by the Provider once the packet enters the network, based on Case B in the graphic below.



Not all of the steps below are required for each possible VLAN configuration. **Note:** VLAN 1 is the default VLAN and you cannot Edit or Delete it.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the **VLAN** tab.



3. Enter the **VLAN ID** (e.g., **VLAN 100**) into the VLAN ID field.
4. Set **Member Tag Port 1** to *UnTag* and set **Member Tag Port 2** for *Tag*. (On the S3231 model, set **Member Tag Port 3** to *Tag*.)
5. In the **Priority Override** field, select **Enabled** or **Disabled**.

- In the **Priority** field, select **0 – 7**. The frame's priority is remapped to this value. Frames that egress tagged will have this remapped priority. Priority 0 is the lowest priority selection.

VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2
1	0	Disabled	0	NoMod	NoMod

VLAN ID: FDB ID: Priority Override: Priority:

Member Tag Port 1: Member Tag Port 2:

Buttons: Refresh Add Edit Delete Help

- Click the **Add** button. The new VLAN ID (100) is added.

VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2
1	0	Disabled	0	NoMod	NoMod
100	0	Disabled	0	UnTag	Tag

VLAN ID: FDB ID: Priority Override: Priority:

Member Tag Port 1: Member Tag Port 2:

Buttons: Refresh Add Edit Delete Help

- Select the **MAIN** tab and locate the **Management VLAN Configuration** section.

ION System

Model Information

Serial Number: 333 Model: C3230-1040 Software Revision: 1.1.0 Hardware Revision: 0.0.1

Bootloader Revision: 1.2.0

System Configuration

System Name: C3230-1040 System Up Time: 0 1 13 42 84 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-F2-42-00-DE

Uptime Reset System Reboot All Counters Reset Reset To Factory Config

Device Description:

IP Configuration

DHCP Client: Disabled

IP Address: 192.168.1.10 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.0.1

DNS 1: 0.0.0.0 DNS 2: 0.0.0.0 DNS 3: 0.0.0.0

DNS 4: 0.0.0.0 DNS 5: 0.0.0.0 DNS 6: 0.0.0.192

Management VLAN Configuration

VLAN ID: 2 Status: Disabled Member Ports: Port 1 Port 2

- In the **VLAN ID** field enter **100**. In the **Status** dropdown, select **Enabled**.

Appendix F: VLAN Tunneling Configuration Examples

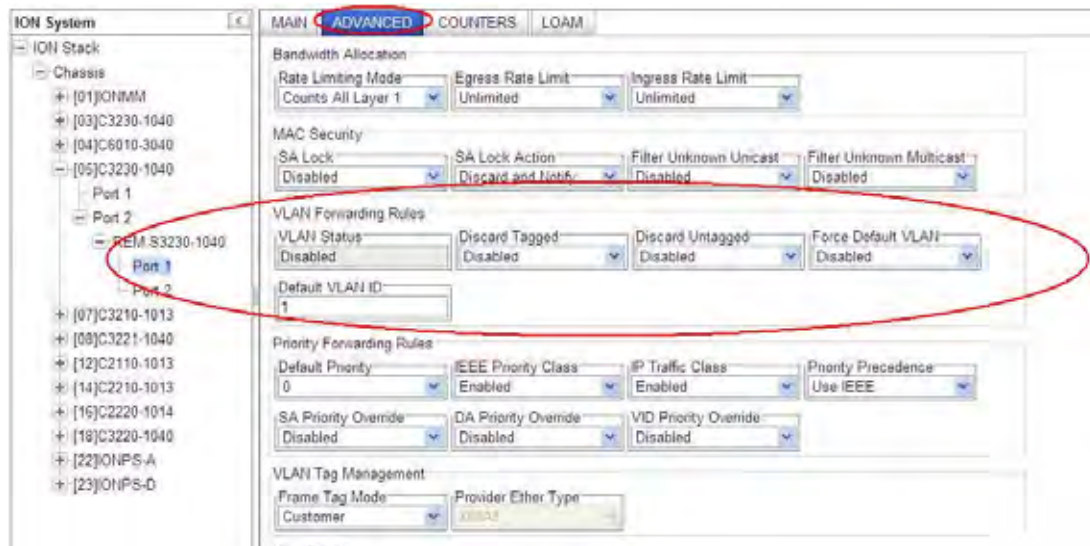
10. In the **Member Ports** section, check the **Port 1** and **Port 2** checkboxes. (On the S3231 model, check the **Port 3** checkbox.)
11. Repeat steps 1 - 10 above for the C322x NID, if applicable, and then click the **Add** button. The message “Adding VLAN succeeded” displays, and the new VLAN 100 is added to the VLANs table.

MAIN	ADVANCED	SNTP	HTTPS	SSH	RADIUS	ACL	FDB	VLAN	SOAM
VLANs									
VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2				
1	0	Disabled	0	NoMod	NoMod				
100	0	Disabled	0	UnTag	Tag				
VLAN ID	FDB ID	Priority Override	Priority						
100	0	Disabled	0						
Member Tag Port 1	Member Tag Port 2								
UnTag	Tag								
<input type="button" value="Refresh"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>									

12. Go to REM S3230-1040 NID, select **Port 1**, and click on the **ADVANCED** tab.

MAIN	ADVANCED	COUNTERS	LOAM
ION System			
<div style="display: flex;"> <div style="flex: 1;"> <ul style="list-style-type: none"> ION Stack Chassis [01]IONMM [03]C3230-1040 [04]C6010-3040 [05]C3230-1040 <ul style="list-style-type: none"> Port 1 Port 2 REM S3230-1040 <ul style="list-style-type: none"> Port 1 Port 2 [07]C3210-1013 [08]C3221-1040 [12]C2110-1013 [14]C2210-1013 [16]C2220-1014 [18]C3220-1040 [22]IONPS-A [23]IONPS-D </div> <div style="flex: 2;"> <div style="border-bottom: 1px solid gray; padding-bottom: 5px;"> Bandwidth Allocation </div> <div style="display: flex; justify-content: space-between;"> <div>Rate Limiting Mode</div> <div>Egress Rate Limit</div> <div>Ingress Rate Limit</div> </div> <div style="display: flex; justify-content: space-between;"> <div>Counts All Layer 1</div> <div>Unlimited</div> <div>Unlimited</div> </div> <div style="border-bottom: 1px solid gray; padding-bottom: 5px;"> MAC Security </div> <div style="display: flex; justify-content: space-between;"> <div>SA Lock</div> <div>SA Lock Action</div> <div>Filter Unknown Unicast</div> <div>Filter Unknown Multicast</div> </div> <div style="display: flex; justify-content: space-between;"> <div>Disabled</div> <div>Discard and Notify</div> <div>Disabled</div> <div>Disabled</div> </div> <div style="border-bottom: 1px solid gray; padding-bottom: 5px;"> VLAN Forwarding Rules </div> <div style="display: flex; justify-content: space-between;"> <div>VLAN Status</div> <div>Discard Tagged</div> <div>Discard Untagged</div> <div>Force Default VLAN</div> </div> <div style="display: flex; justify-content: space-between;"> <div>Disabled</div> <div>Disabled</div> <div>Disabled</div> <div>Disabled</div> </div> <div>Default VLAN ID</div> <div>1</div> <div style="border-bottom: 1px solid gray; padding-bottom: 5px;"> Priority Forwarding Rules </div> <div style="display: flex; justify-content: space-between;"> <div>Default Priority</div> <div>IEEE Priority Class</div> <div>IP Traffic Class</div> <div>Priority Precedence</div> </div> <div style="display: flex; justify-content: space-between;"> <div>0</div> <div>Enabled</div> <div>Enabled</div> <div>Use IEEE</div> </div> <div style="display: flex; justify-content: space-between;"> <div>SA Priority Override</div> <div>DA Priority Override</div> <div>VID Priority Override</div> </div> <div style="display: flex; justify-content: space-between;"> <div>Disabled</div> <div>Disabled</div> <div>Disabled</div> </div> <div style="border-bottom: 1px solid gray; padding-bottom: 5px;"> VLAN Tag Management </div> <div style="display: flex; justify-content: space-between;"> <div>Frame Tag Mode</div> <div>Provider Ether Type</div> </div> <div style="display: flex; justify-content: space-between;"> <div>Customer</div> <div>802.1Q</div> </div> </div> </div>			

- In the **VLAN Tag Management** section, set **Frame Tag Mode** to *Network*, set **EtherType** to *X88A8*, enter the default **VLAN ID (100)**, and then click the **Save** button.



- In the **VLAN Forwarding Rules** section, set **Discard Tagged**, **Discard Untagged** and **Force Default VLAN** to **Enabled** or **Disabled**.

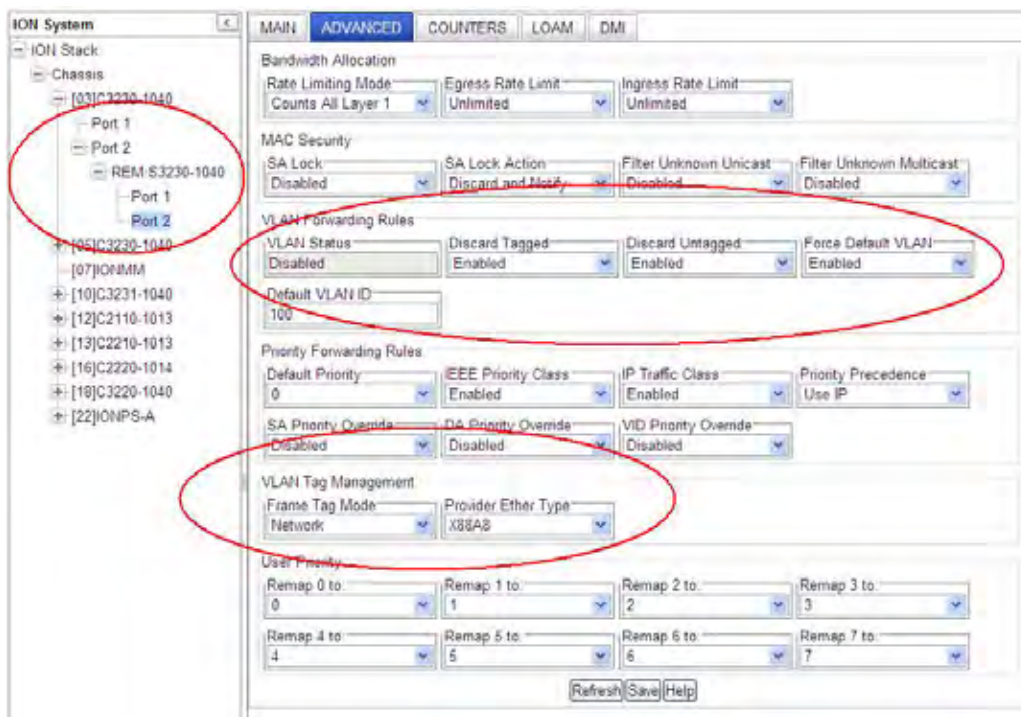
Discard Tagged filters all tagged non-management frames ingressing this port. All untagged and priority tagged frames are processed as normal frames.

Discard Untagged filters all untagged and priority tagged non-management frames ingressing this port. All 802.1Q tagged frames are processed as normal frames.

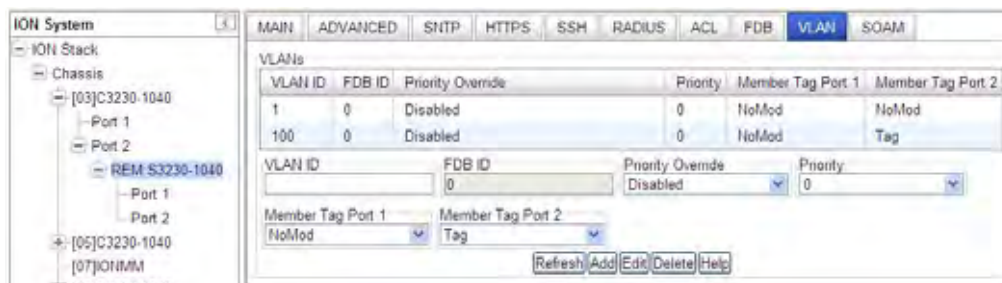
Force Default VLAN forces all untagged and (802.1Q) tagged frames to take up the interface's Default VLAN ID.

- Go to Port 2 of REM x323x and select the **ADVANCED** tab.

- In the **VLAN Tag Management** section, set **Frame Tag Mode** to *Network*, set **EtherType** to *x88A8*, and then click the **Save** button.



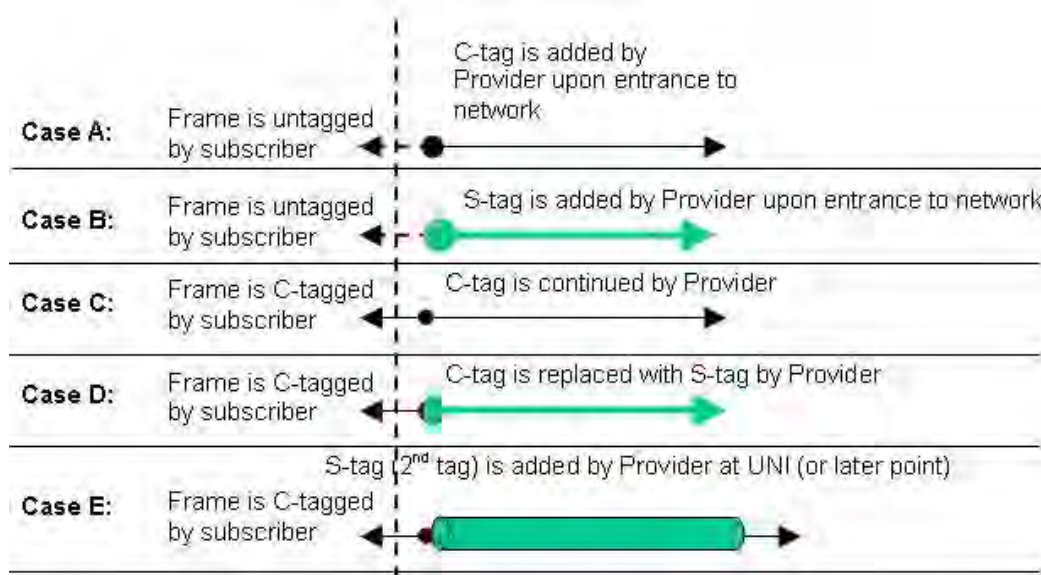
17. Repeat Steps 2 through 16 above on the C322x NID, if applicable.
18. Verify that VLAN 100 is correctly set up in the VLAN Database with **Port 1** set to “*UnTag*” and **Port 2** set to “*Tag*”. (On the S3231 model, set **Port 3** for **NoMod**.)



19. When VLAN 100 is correctly set up, click the **Save** button.
20. You can use the **Refresh** button to clear the current entry data.
21. To make changes to an existing VLAN table entry, select the VLAN in the table to highlight it, and then click the **Edit** button. **Note:** VLAN 1 is the default VLAN and you cannot Edit or Delete it.
22. To remove an existing VLAN table entry, select the VLAN in the table to highlight it, and then click the **Delete** button. The selected VLAN entry is deleted.

Configuring a VLAN with C-Tags and S-Tags

This procedure is used to configure customer and service provider tags (EtherType x88A8) using case studies B and E below simultaneously.



The procedure below is used to configure VLAN C-Tags and S-Tags.

1. Select the REM-S323x device and then select the **VLAN** tab.



2. Add a new **VLAN ID** in the **VLANs** section:
 - a. Enter **VLAN ID =100**.
 - b. Set **Member Tag Port 1** to *NoMod*.
 - c. Set **Member Tag Port 2** to *NoMod*.
 - d. Set **Member Tag Port 3** to *NoMod* (x3231 model only).
 - e. Click the **Add** button.

The new VLAN ID 100 displays in the VLANs table:

MAIN ADVANCED SNTP HTTPS SSH RADIUS ACL FDB VLAN SOAM					
VLANs					
VLAN ID	FDB ID	Priority Override	Priority	Member Tag Port 1	Member Tag Port 2
1	0	Disabled	0	NoMod	NoMod
100	0	Disabled	0	UnTag	Tag

VLAN ID	FDB ID	Priority Override	Priority
100	0	Disabled	0

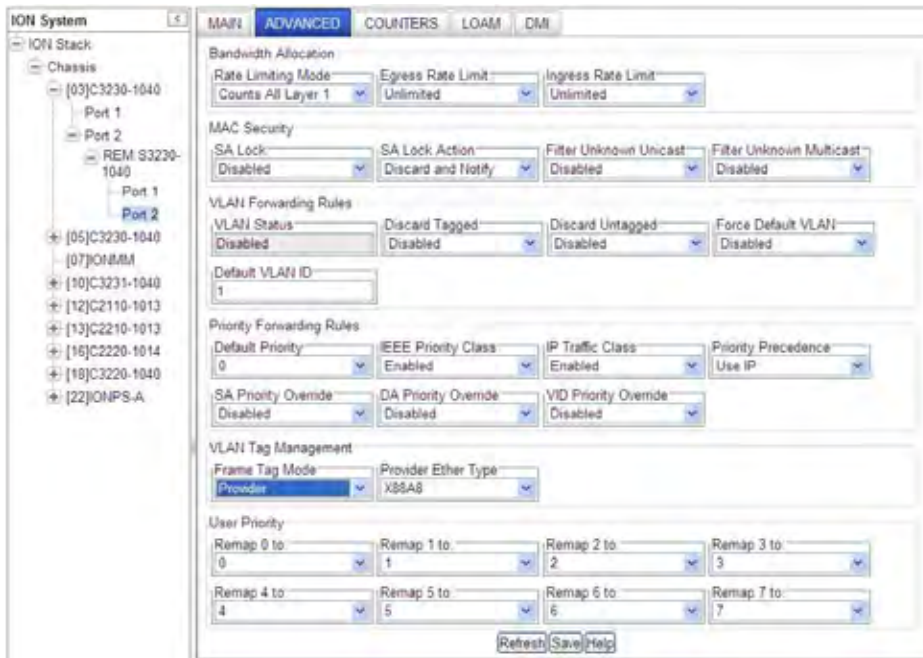
Member Tag Port 1	Member Tag Port 2
UnTag	Tag

Refresh Add Edit Delete Help

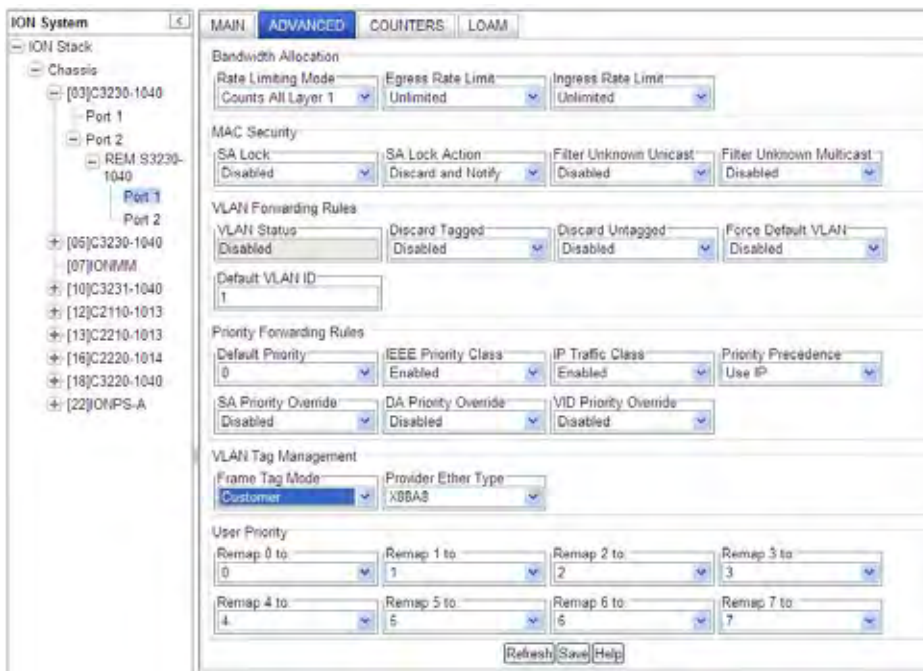
- Go to REM S3230-1040, Port 2 and click on the **ADVANCED** tab, and configure the “Provider Port” under port level config in the **VLAN Tag Management** section.

The screenshot shows the configuration page for port REM S3230-1040 Port 2. The 'ADVANCED' tab is selected. The 'VLAN Forwarding Rules' section shows 'VLAN Status' set to 'Disabled' and 'Default VLAN ID' set to '100'. The 'VLAN Tag Management' section shows 'Frame Tag Mode' set to 'Provider' and 'Provider Ether Type' set to 'x88A8'. The 'Use Priority' section shows remapping options for ports 0 through 7.

- Set the **Frame Tag Mode** to *Provider*, set the **EtherType** as *x88A8*, and click the **Save** button.

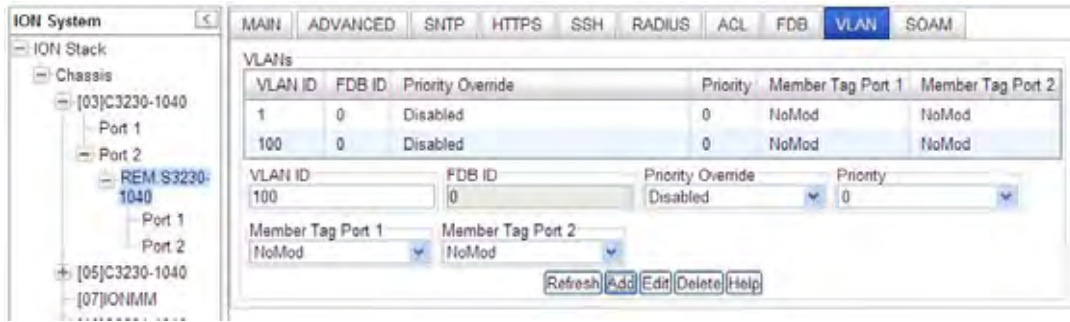


- Go to REM S3230-1040, Port 1 and click on the **ADVANCED** tab.



- Configure the “Customer Port” under port-level configuration. In the **VLAN Tag Management** section in the **Frame Tag Mode** field, select *Customer*.
- In the **Provider Ether Type** field, select *x88A8*.

8. Select REM-C323x, select the **VLAN** tab, and verify the VLAN database configuration.



Verify:

- a. **VLAN ID =100.**
- b. **Member Tag Port 1** set to *NoMod*.
- c. **Member Tag Port 2** set to *NoMod*.
- d. **Member Tag Port 3** for *NoMod* (S3231 model only).

Configuring Q-in-Q (Provider Tagging)

The x323x NID supports Q-in-Q service, where a frame may contain one or more tags. Complete IEEE802.1ad support is not supported, but provider tags can be added or stripped on a per-port basis. There are different cases for VLAN service translation, providing options for dealing with C-Tags and S-Tags. Using IEEE 802.1Q-in-Q frames is an effective way to construct Layer 2 tunnels, apply QoS policies, etc.

The figure below illustrates tagging options that exist for using C-Tags and S-Tags.

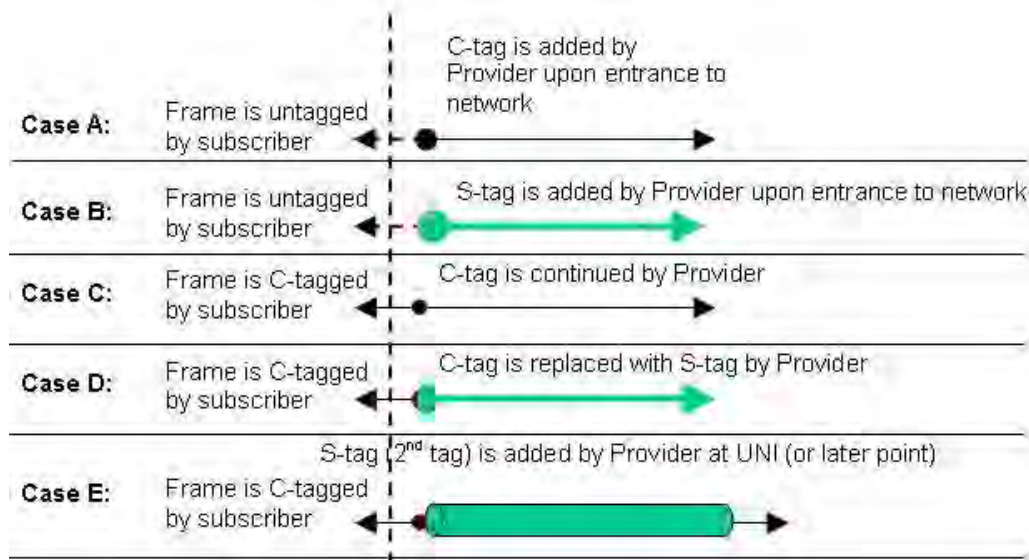


Figure F-2: Q-in-Q (Provider Tagging)

Case B and Case E above are more widely used by providers when subscriber's traffic enters and leaves the provider network at the UNI.

Q-in-Q implies a C-Tag followed by an S-Tag or another C-Tag.

Note: VLAN 1 is the default VLAN and you cannot Edit or Delete it.

Q-in-Q service can be configured in the NID using either the CLI or the Web method.

Q-in-Q Config – CLI Method

This procedure configures Q-in-Q using **ethtype = 0x9100**.

1. Access the NID through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Add a VLAN Database Entry. This adds a new VLAN to the device. By default, VLAN ID one (VID 1) is defined for internal use. Type:

```
add vlan-db vid=<xx> [priority=<yy>] [pri-override={enable | disable}]
```

where:

xx = ID (2–4094) of the VLAN to which the device is to become a member

yy = optional; priority for frames

3. Set the VLAN Database Member/Egress Tagging. This sets the priority of a row of the VLAN forwarding database. Type:

```
set vlan-db vid=<xx> port=<yy> memetag=<zz>
```

```
set vlan-db vid=<xx> fid=<yy> pri-override=<aa> priority=<bb>
```

where:

ww =

xx = number that identifies the VLAN (2–4094)

yy = logical port index or fid

zz = valid memetag choices are **noMod**, **notMember**, **tag**, and **unTag**.

aa = pri-override={enable | disable}

bb = priority = {0-7}

4. Press **Enter**.
5. Set the Management VLAN admin state to enable. Type:

```
set mgmt vlan state=enable
```

6. Press **Enter**.
7. Select the management VLAN ports. Type:

```
set mgmt vlan port=port-list
```

where:

Port-list = a management VLAN port (1-19)

Example: C1 | S13 | 10d />**set mgmt vlan port=2,3**

8. Press **Enter**.
9. Set the port discard untagged non-management frames option to true if untagged non-management frames are to be discarded for this port. Type:

```
set port discard-untagged=truth-val
```

where:

Truth-val = true or false

Example: C1 | S13 | 10ap1 | 11p2 />**set port discard-untagged=true**

10. Press **Enter**.
11. Set the port discard tagged non-management frames option to true if the tagged non-management frames for this port are to be discarded. Type:

```
set port discard-tagged=truth-val
```

where:

Truth-val = true or false

Example: C1 | S13 | 10ap1 | 11p2 />**set port discard-tagged=true**

12. Press **Enter**.

13. Set the port default VLAN-ID for this port. Type:

set port default-vid=vid

where:

vid = 2 - 4094

Example: C1|S13|10ap1|11p2/>**set port default-vid=2**

14. Press **Enter**.

15. Set if force port to use default VLAN-ID. If set to true, this forces all untagged and 802.1Q tagged frames to assume the default VLAN-ID. Type:

set port force-default-vid=truth-val

where:

Truth-val = true or false

Example: C1|S13|10ap1|11p2/>**set port force-default-vid=true**

16. Press **Enter**.

17. Set the port VLAN tag mode of a port interface. Type:

set port vlan tag mode= provider

Example: C1|S13|10ap1|11p2/>**set port vlan tag mode=provider**

18. Press **Enter**.

19. Set the Ethernet type for the VLAN tagging mode that was set to *provider* in step 17.

Type:

set port vlan tag provider ethtype= x9100

Example: C1|S13|10ap1|11p2/>**set port vlan tag provider ethtype=x9100**

20. Press **Enter**.

21. Add a new row in the VLAN forwarding database. Type:

add vlan-db vid=vlan-id [priority=prio] [pri-override=override]

where:

vlan-id = 1-4094

prio = the priority for frames (0-7)

pri-override = enable or disable

Example:

C1|S13|10ap1|11p2/>**add vlan-db vid=3 pri-override=enable priority=1**

22. Press **Enter**.

23. Set the priority override of a VLAN forwarding database row. This sets the override priority on frames associated with this VID of the VLAN forwarding database. Type:

set vlan-db vid=vlan-id fid=fid pri-override=override

where:

vlan-id =1-4094

fid = 0

override = enable or disable (specify if override priority on frames enabled in step 18)

Example:

C1|S13|10ap1|11p2/>**set vlan-db vid=3 fid=0 pri-override=enable**

24. Press **Enter**.

Appendix F: VLAN Tunneling Configuration Examples

25. Set the priority of a VLAN forwarding database row. Type:

```
set vlan-db vid=vlan-id fid=fid priority=prio
```

Where:

vlan-id = 2-4094

fid = 0

Prio = priority for frames (0-8)

Example: C1|S13|10ap1|11p2/>**set vlan-db vid=3 fid=0 priority=2**

26. Press **Enter**.

27. Set the member and egress tagging of a VLAN forwarding database row. Type:

```
set vlan-db vid=vlan-id port=port-id memetag=memetag_mode
```

Where:

vlan-id = 1-4094

port-id = logical port index

Memetag_mode = noMod, notMember, tag, and unTag.

Example:

C1|S13|10ap1|11p2/>**set vlan-db vid=3 port=2 memetag=memETag**

28. Press **Enter**.

29. Use CLI commands to verify your VLAN configuration(s).

- Show all existing VLAN(s) on the NID. Type **show vlan** and press **Enter**. For example:

```
C1|S13|L0D/>show vlan
```

vid	fid	priority	p-override	port1	port2	port3
1	0	0	disable	NoMod	NoMod	notApp

- Show the Management VLAN configuration. Type **show mgmt vlan config** and press **Enter** to show the management VLAN configuration on a device. Example:

```
C1|S13|10d/>show mgmt vlan config
```

vlan id	vlan state	vlan portlist
0	enable	none

- Show the Port VLAN configuration. Type **show port vlan config** and press **Enter**. For example:

```
C1|S13|10ap1|11p2/>show port vlan config
```

```
Dot1q state:          vlanEnabled
Discard-tagged:      false
Discard-untagged:    false
Default VLAN id:     22
Force use default VLAN id: false
```

- Show the Port VLAN Tag configuration. Type **show port vlan tag config** and press **Enter**. For example:

```
C1|S13|10ap1|11p2/>show port vlan tag config
```

```
Tagging mode:        provider
Network tagging:     addTag
```

- Show the VLAN forwarding database configuration for the device. Type **show vlan-db config** and press **Enter**. For example:

```
C1|S13|l1d>show vlan-db config
vid:1      fid:0      priority:0      priv_override:disable
port1:     NoMod    port2: NoMod
vid:100    fid:0      priority:0      priv_override:disable
port1:     notMember port2: notMember
```

30. Click the **Add** button to add the newly-defined VLAN.

31. Verify the SOAM configuration. Type **show soam conferror vid=xx port=<xx>** and press **Enter**.

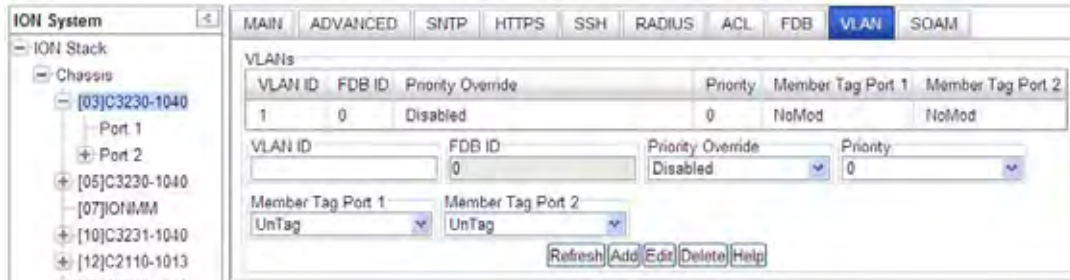
For example:

```
C1|S10|L1D>show soam conferror vid 1 port 1
No config errors.
```

Q-in-Q Config – Web Method

This procedure configures Q-in-Q using **ethtype = 0x9100**.

1. Access the NID through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the REM-S323x device and then select the **VLAN** tab.

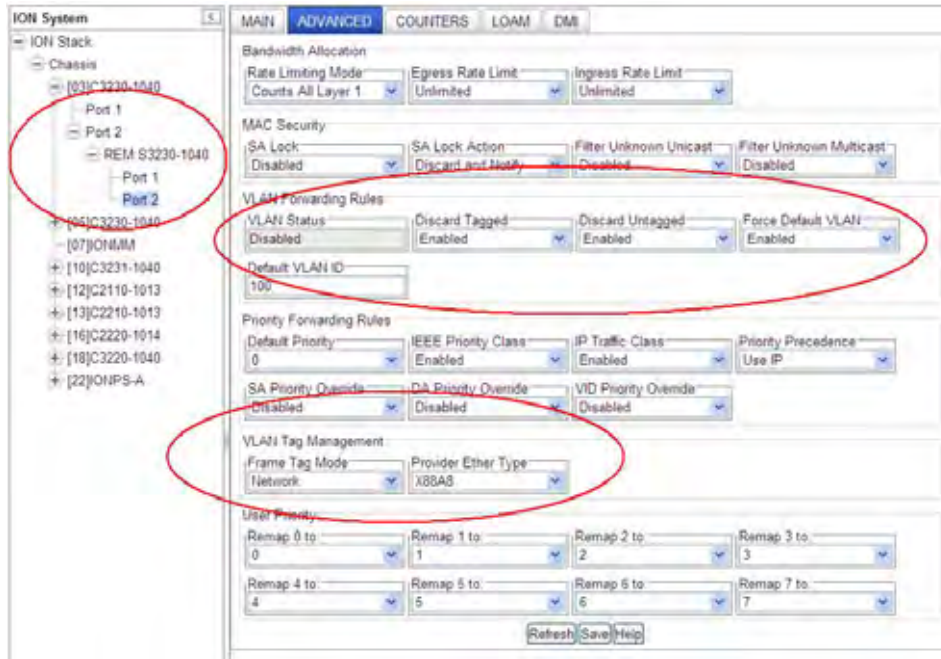


3. Add a new **VLAN ID** in the **VLANs** section:
 - a. Enter **VLAN ID =100**.
 - b. Set **Member Tag Port 1** to *NoMod*.
 - c. Set **Member Tag Port 2** to *NoMod*.
 - d. Set **Member Tag Port 3** to *NoMod* (x3231 model only).
 - e. Click the **Add** button.

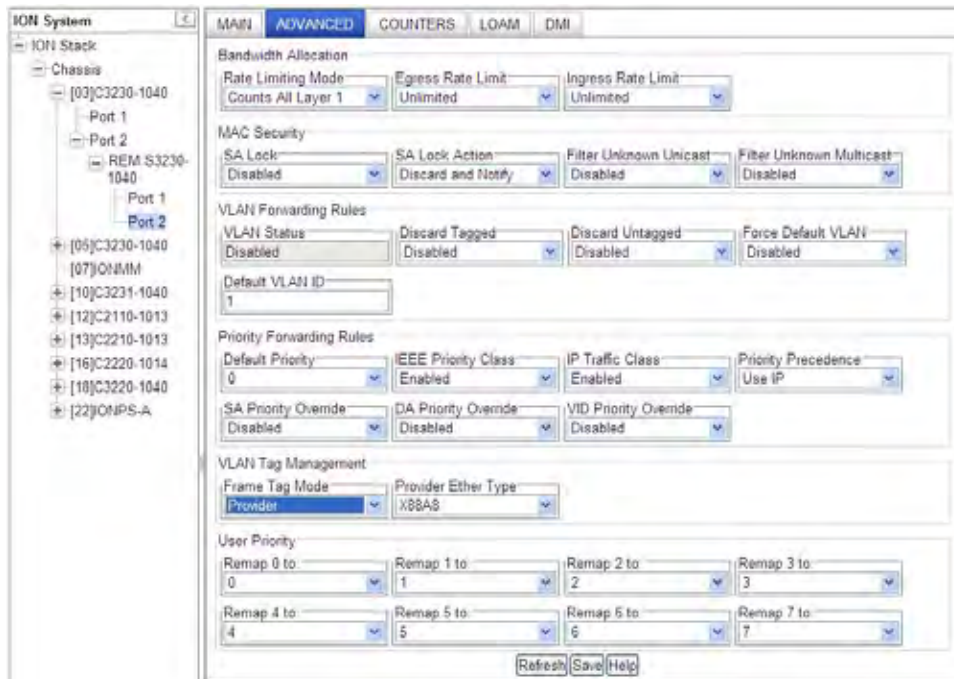
The new VLAN ID 100 displays in the VLANs table:



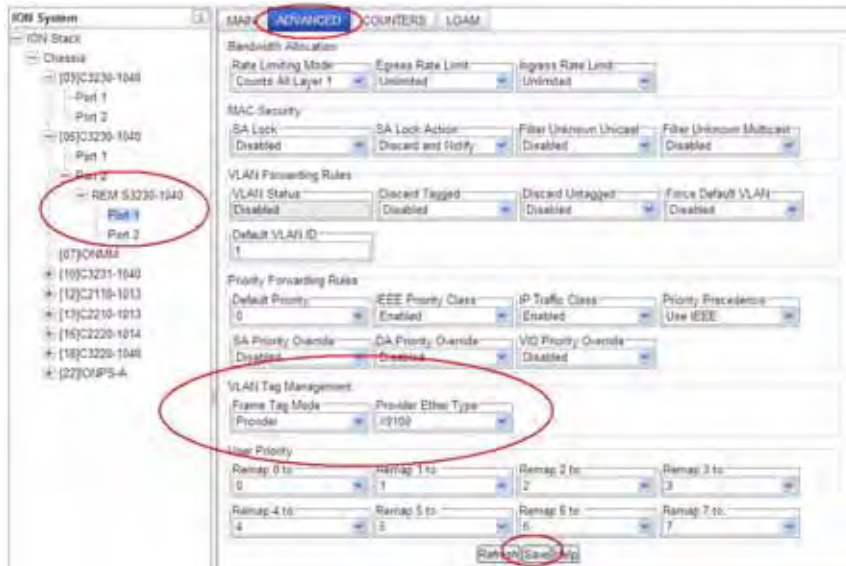
4. Go to REM S3230-1040, Port 2 and click on the **ADVANCED** tab, and configure the “Provider Port” under port level config in the **VLAN Tag Management** section.



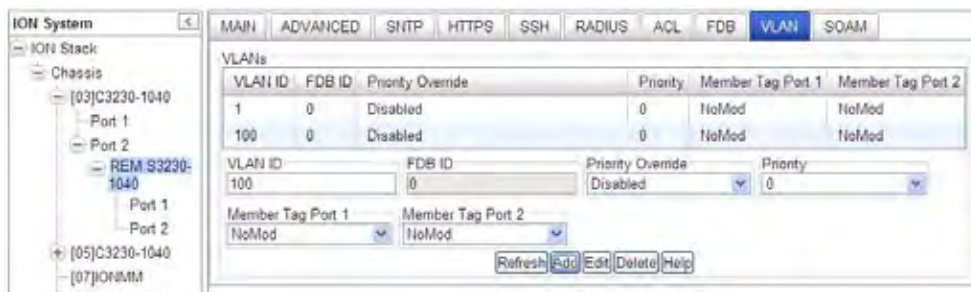
5. Set the **Frame Tag Mode** to *Provider*, set the **EtherType** as *x88A8*, and click the **Save** button.



6. Go to REM S3230-1040, Port 1 and click on the **ADVANCED** tab.



7. Configure the “*Provider* Port” under port-level configuration. In the **VLAN Tag Management** section in the **Frame Tag Mode** field, select *Provider*.
8. In the **Provider Ether Type** field, select **0x9100**.
9. Select REM-C323x, select the **VLAN** tab, and verify the VLAN database for correct set-up.



Verify the desired **Priority** and **Priority Override** settings and verify these settings:

- a. **VLAN ID =100**.
- b. **Member Tag Port 1** set to *NoMod*.
- c. **Member Tag Port 2** set to *NoMod*.
- d. **Member Tag Port 3** for *NoMod* (S3231 model only).

Appendix G: SNMP Traps Supported

This appendix provides information on SNMP traps supported on the IONMM, including when a trap is generated and what information is in each trap.

All ION system critical events are reported via SNMP Traps. The ION system uses only SNMPv2 traps, with the definition of NOTIFICATION-TYPE in the MIB (Management Information Base).

See the “[Supported MIBs](#)” section on page 32 for information on support for public (standard) and private MIBs. For information on “[Configuring SNMP](#)” see page 234. See the *ION Management Module (IONMM) User Guide* manual for SNMP traps supported on the IONMM.

Traps are generated when a condition has been met on the SNMP agent. These conditions are defined in the Management Information Base (MIB). The administrator then defines thresholds, or limits to the conditions, that are to generate a trap. Conditions range from preset thresholds to a restart.

All of the values that SNMP reports are dynamic. The information needed to get the specified values that SNMP reports is stored in the MIB. This information includes Object IDs (OIDs), Protocol Data Units (PDUs), etc. The MIBs must be located at both the agent and the manager to work effectively.

Traps List

ionSlotStatusChangeEvt	ionSoamRemoteMepRemoveTrap
ionChassisDiscoveredEvt	dot1agCfmFaultAlarm
ionChassisRemovedEvt	newroot
entSensorThresholdNotification	topologyChange
ionDMIRxIntrusionEvt	dot3OamThresholdEvent
ionDMIRxPowerEvt	linkDown
ionDMITxPowerEvt	linkUp
ionDMITxBiasEvt	risingAlarm
ionDMITemperatureEvt	fallingAlarm
ionSysDyingGaspTrap	ionIfSourceAddrChangeEvt
ionSoamCCMDefectTrap	ionDevSysAcIldsEvt
ionSoamRemoteMepAddTrap	

Appendix G: SNMP Traps Supported

SNMP v1 Traps

Most SNMPv1 messages follow a model where a client (Network Management System) makes a request and a server (agent) responds to that request. Traps are the exception. An SNMP agent will transmit a trap to the NMS when it has a condition to report that is deemed too important to wait until asked. A common example of this is the failure of a communications link.

With most traps, the agent will include something called "'Interesting' variable bindings," which are the OID(s) and value(s) of MIB variable(s) that provide more information about the condition. So, for example, when a communications channel fails, the agent will send a pSError trap, which will have the OID of the "Link" or "Signal Detect" variable for that channel, and the value "down." Newer versions of Management Module firmware will also include bindings for the BIA (Cabinet serial number), slot, and (if applicable) subdevice of the entity in question. This information is always embedded in the first binding (as above), but are repeated separately for more convenient viewing under certain NMS packages.

SNMP v2c Traps

All ION system SNMP Trap messages conform to SNMPv2 MIB RFC-2573.

See the [“Supported MIBs”](#) section on page 32 for information on the x323x NIDs support for public (standard) and private MIBs.

For information on [“Configuring SNMP”](#) see page 234, see the *ION Management Module (IONMM) User Guide* manual for SNMP traps supported on the IONMM.

A sample SNMP Message sequence is shown below.

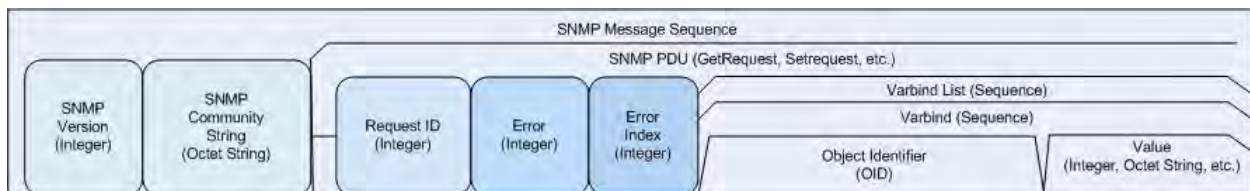


Figure G-1: SNMP Message Sequence

SNMP v3 Traps

SNMP v3 traps are mainly SNMPv2 traps with added authentication and privacy capabilities. SNMPv3 Traps use the engineID of the local application sending the trap rather than the engineID of the remote application. This means that you must create users in your remote user database and create one for each engineID you wish to send traps from.

MIB Traps Summary

The ION system MIB Traps are summarized in the table below in terms of related MIB and varbinds.

Table 37: MIB Traps Summary		
MIB (linked to section)	TRAP (linked to section)	VARBINDS
TN-ION-BPC-MIB	ionSlotStatusChangeEvt	entPhysicalIndex, ionChassisSlotNumber ionChassisSlotStatus
TN-ION-Chassis-MIB	ionChassisDiscoveredEvt	entPhysicalIndex ionChassisStackSerialNo
	ionChassisRemovedEvt	entPhysicalIndex ionChassisStackSerialNo
TN-ION-ENTITY-SENSOR-MIB	entSensorThresholdNotification	entSensorThresholdValue entSensorValue
TN-ION-MGMT-MIB	ionDMIRxIntrusionEvt	ifIndex ionDMIRxPwrLvlPreset ionDMIRxPowerLevel
	ionDMIRxPowerEvt	ifIndex ionDMIRxPowerAlarm ionDMIRxPowerLevel
	ionDMITxPowerEvt	ifIndex ionDMITxPowerAlarm ionDMITxPowerLevel
	ionDMITxBiasEvt	ifIndex, ionDMITxBiasAlarm, ionDMITxBiasCurrent
	ionDMITemperatureEvt	ifIndex ionDMITempAlarm ionDMITemperature
	ionSysDyingGaspTrap rxPwrThreshold	
TN-ION-SOAM-EXT-MIB	ionSoamCCMDefectTrap	dot1agCfmMdIndex, dot1agCfmMaIndex, dot1agCfmMepIdentifier dot1agCfmMepDefects
	ionSoamRemoteMepAddTrap	dot1agCfmMdIndex, dot1agCfmMaIndex, dot1agCfmMepIdentifier dot1agCfmMepDbRMepIdentifier

Table 37: MIB Traps Summary		
MIB (linked to section)	TRAP (linked to section)	VARBINDS
	ionSoamRemoteMepRemoveTrap	dot1agCfmMdIndex, dot1agCfmMaIndex, dot1agCfmMepIdentifier dot1agCfmMepDbRMepIdentifier
IEEE8021-CFM-MIB	dot1agCfmFaultAlarm	dot1agCfmMepHighestPrDefect
BRIDGE-MIB	newroot	
	topologyChange	
DOT3-OAM-MIB	dot3OamThresholdEvent	dot3OamEventLogTimestamp, dot3OamEventLogOui, dot3OamEventLogType, dot3OamEventLogLocation, dot3OamEventLogWindowHi, dot3OamEventLogWindowLo, dot3OamEventLogThresholdHi, dot3OamEventLogThresholdLo, dot3OamEventLogValue, dot3OamEventLogRunningTotal, dot3OamEventLogEventTotal
IF-MIB	linkDown	ifIndex, ifAdminStatus, ifOperStatus
	linkUp	ifIndex, ifAdminStatus, ifOperStatus
RMON	risingAlarm	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmFallingThreshold
	fallingAlarm	alarmIndex, alarmVariable, alarmSam- pleType, alarmValue, alarmFallingThreshold
ION-DEV-SYS-ACL-MIB	ionDevSysAcldsEvt	
TN-ION-VLAN-MGMT-MIB	ionIfSourceAddrChangeEvt	

TN-ION-MGMT-MIB.smi

```

ionDevSysMgmt      OBJECT IDENTIFIER ::= { ionDevMgmt 1 }
ionDevSysLPT       OBJECT IDENTIFIER ::= { ionDevMgmt 2 }
ionDevSysDyingGasp OBJECT IDENTIFIER ::= { ionDevMgmt 3 }

ionDevSysCfgTable OBJECT-TYPE
    ::= { ionDevSysLPTEnt 5 }

--
-- Dying Gasp management
--
ionDevSysDyingGaspTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IonDevSysDyingGaspEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table supplements the ENTITY-MIB for 2-port devices managed by this Agent."
    ::= { ionDevSysDyingGasp 1 }

ionDevSysDyingGaspEntry OBJECT-TYPE
    SYNTAX      IonDevSysDyingGaspEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A entry in the table contains additional information related to a device."
    INDEX       { entPhysicalIndex }
    ::= { ionDevSysDyingGaspTable 1 }

IonDevSysDyingGaspEntry ::= SEQUENCE
{
    ionSysDyingGaspTrap  INTEGER
}

ionSysDyingGaspTrap OBJECT-TYPE
    SYNTAX      INTEGER { enabled(1), disabled(2), notSupported(3) }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Devices which support this feature allow write for enabling or disabling the feature.

```

When a device detects the power is going to be lost, a system dying gasp procedure will be triggered internally.

If this ionSysDyingGaspTrap is set to enabled, a ionDyingGaspEvt will be sent out. Other events may also be sent out in this procedure, e.g. LOAM event.

The LOAM event (enabled by dot3OamDyingGaspEnable) and this Trap event will be processed at the same time if both enabled.

If LOAM is enabled in multiple ports, the LOAM event will be sent out one port at a time, beginning from the smaller port number (e.g. smallest is copper port, port 1)

If multiple trap servers are enabled, the trap will be sent out server by server, beginning from the server 1.

Depends on different hardware, the dying gasp's power may be not enough for sending out all the LOAM event and Traps.

Appendix G: SNMP Traps Supported

So, it is suggested that users should keep as few targets as possible."
 ::= { ionDevSysDyingGaspEntry 1 }

--

--ION Ethernet Interface management

... ..

::= { tnIonMgmtNotifications 6 }

ionDyingGaspEvt NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"when the device lost power, this dying gasp trap will be sent out."

::= { tnIonMgmtNotifications 7 }

Agent_III_Private MIBS

ION-DEV-SYS-ACL-MIB

The `ionDevSysAclIdsEvt` event is included in 'ION-DEV-SYS-ACL-MIB.my'. This event is related to 'iptableRulesTable' which is also defined in 'ION-DEV-SYS-ACL-MIB.my'.

```
ionDevSysAclIdsEvt  NOTIFICATION-TYPE
    OBJECTS {
        entPhysicalIndex, gRuleIndex
    }
```

STATUS current

DESCRIPTION

"An `ionDevSysAclIdsEvt` event is sent if an IDS (Intrusion Detection Systems) is detected.

The `entPhysicalIndex` event indicates in which SIC the IDS is detected.

The `entPhysicalIndex/gRuleIndex` indicates which ACL rule is matched for this IDS."

```
::= { tnIonMgmtNotifications 16 }
```

ION-DEV-SYS-HTTPS-MIB

None

ION-DEV-SYS-IPMGMT-MIB

None

ION-DEV-SYS-RADIUS-MIB

None

ION-DEV-SYS-SNMPMGMT-MIB

None

ION-DEV-SYS-SNTP-MIB

None

ION-DEV-SYS-SSH-MIB

None

ION-DEV-SYS-TFTP-MIB

None

TN-ION-VLAN-MGMT-MIB.mib

The **ionIfSourceAddrChangeEvt** event is included 'TN-ION-VLAN-MGMT-MIB.mib'.
The 'ionIfSourceAddrChangeEvt' event is related to 'ionIfMACSecurityTable' which is defined in 'TN-ION-MGMT-MIB.smi'.

```
ionIfSourceAddrChangeEvt  NOTIFICATION-TYPE
    OBJECTS {
        ionFIDDbMacAddress, ionFIDDbConnPort
    }
STATUS current
DESCRIPTION
"An ionIfSourceAddrChangeEvt event is sent when the ionIfSourceAddrLock is set to 'true',
the ionIfSourceAddrLockAction is set to 'discardAndNotify' or 'all' and there is an intrusion/SA change
on this port."
::= { tnIonVlanQoSManagementNotifications 1 }
```

TN_ION Private MIBS

TN-ION-BPC-MIB

ionSlotStatusChangeEvt

An ionSlotStatusChangeEvt event is sent when a new module is inserted in this slot or when it is removed. The chassis is identified by its entPhysicalIndex.

Varbinds

entPhysicalIndex

SYNTAX INTEGER

DESCRIPTION

"The entPhysicalIndex in this chassis."

ionChassisSlotNumber,

SYNTAX INTEGER

DESCRIPTION

"The slot number in this chassis."

ionChassisSlotStatus

SYNTAX INTEGER { empty(1), occupied(2) }

DESCRIPTION

"The status of the slot, whether occupied or empty."

OID

MIB Description

ionSlotStatusChangeEvt NOTIFICATION-TYPE

OBJECTS {

 entPhysicalIndex,
 ionChassisSlotNumber,
 ionChassisSlotStatus

}

STATUS current

DESCRIPTION

"An ionSlotStatusChangeEvt event is sent when a new module is inserted in this slot or when it is removed. The chassis is identified by its entPhysicalIndex."

::= { tnIonBkPlaneNotifications 1 }

TN-IONCHASSIS-MIB

ionChassisDiscoveredEvt

An ionChassisDiscoveredEvt event is sent when a new chassis is discovered.

Varbinds

entPhysicalIndex

SYNTAX INTEGER

DESCRIPTION

"The entPhysicalIndex in this chassis."

ionChassisStackSerialNo

SYNTAX OCTET STRING

DESCRIPTION

"The chassis serial number, this is unique to each chassis."

OID

MIB Definition

ionChassisDiscoveredEvt NOTIFICATION-TYPE

```
OBJECTS {
    entPhysicalIndex,
    ionChassisStackSerialNo
}
```

STATUS current

DESCRIPTION

"An ionChassisDiscoveredEvt event is sent when a new chassis is discovered."

```
::= { tnIonChassisNotifications 1 }
```

ionChassisRemovedEvt

An ionChassisRemovedEvt event is sent when a managed chassis is removed.

Varbinds***entPhysicalIndex***

SYNTAX INTEGER

DESCRIPTION

"The entPhysicalIndex in this chassis."

ionChassisStackSerialNo

SYNTAX OCTET STRING

DESCRIPTION

"The chassis serial number, this is unique to each chassis."

OID**MIB Description**

ionChassisRemovedEvt NOTIFICATION-TYPE

OBJECTS {

```
    entPhysicalIndex,  
    ionChassisStackSerialNo
```

}

STATUS current

DESCRIPTION

"An ionChassisRemovedEvt event is sent when a managed chassis is removed."

```
::= { tnIonChassisNotifications 2 }
```

TN-ION-ENTITY-SENSOR-MIB

entSensorThresholdNotification

The sensor value crossed the threshold listed in entSensorThresholdTable.

This notification is generated once each time the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification.

Varbinds

entSensorThresholdValue

SYNTAX SensorValue

DESCRIPTION

"This variable indicates the value of the threshold.

To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision.

However, you can directly compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."

entSensorValue

SYNTAX SensorValue

DESCRIPTION

"This variable reports the most recent measurement seen by the sensor.

To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision.

However, you can compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."

SensorValue TEXTUAL-CONVENTION

SensorValue ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"For sensors that measure volts AC, volts DC, amperes, watts, hertz, Celsius, or cmm, this item is a fixed point number ranging from -999,999,999 to +999,999,999. Use the value -1000000000 to indicate underflow. Use the value +1000000000 to indicate overflow. Use SensorPrecision to indicate how many fractional digits the SensorValue has.

For sensors that measure percentRH, this item is a number ranging from 0 to 100.

For sensors that measure rpm, this item can take only nonnegative values, 0..999999999.

For sensors of type truthvalue, this item can take only two values: true(1), false(2).

For sensors of type specialEnum, this item can take any value in the range (-1000000000..1000000000), but the meaning of each value is specific to the sensor.

For sensors of type other and unknown, this item can take any value in the range (-1000000000..1000000000), but the meaning of the values are specific to the sensor.

Use Entity-MIB entPhysicalTable.entPhysicalVendorType to learn about the sensor type."
SYNTAX INTEGER (-1000000000..1000000000)

OID

MIB Description

```
entSensorThresholdNotification NOTIFICATION-TYPE  
OBJECTS { entSensorThresholdValue, entSensorValue }  
STATUS current  
DESCRIPTION
```

"The sensor value crossed the threshold listed in entSensorThresholdTable.

This notification is generated once each time the sensor value crosses the threshold.

The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification."

```
::= { entitySensorMIBNotifications 1 }
```

TN-ION-LOAM-EXT-MIB

None

TN-ION-MGMT-MIB**ionDMIRxIntrusionEvt**

An ionDMIRxIntrusionEvt event is sent if the ionDMIRxPowerLevel falls below the ionDMIRxPwrLvlPreset indicating an intrusion on the fiber.

Varbinds***ifIndex***

SYNTAX INTEGER32 ()
DESCRIPTION
"IF-MIB Index of the port this was relevant to."

ionDMIRxPwrLvlPreset

SYNTAX INTEGER (0 . . 65535)
DESCRIPTION
"A preset level for Rx Power on the Fiber port, if the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated."

ionDMIRxPowerLevel

SYNTAX INTEGER
DESCRIPTION
"DMI: Diagnostic Monitoring Interface for fiber transceivers. Receive power on local fiber measured in microwatts."

OID**MIB Description**

```
ionDMIRxIntrusionEvt NOTIFICATION-TYPE
OBJECTS {
    ifIndex, ionDMIRxPwrLvlPreset, ionDMIRxPowerLevel
}
STATUS current
DESCRIPTION
"An ionDMIRxIntrusionEvt event is sent if the ionDMIRxPowerLevel falls below the ionDMIRxPwrLvlPreset indicating an intrusion on the fiber."
 ::= { tnIonMgmtNotifications 1 }
```


ionDMIRxPowerEvt

An ionDMIRxPowerEvt event is sent when there is a warning or alarm on Rx Power.

Varbinds

ifIndex

ionDMIRxPowerAlarm

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),
lowAlarm(6), highAlarm(7) }
```

```
DESCRIPTION "."
```

ionDMIRxPowerLevel

```
SYNTAX INTEGER
```

```
DESCRIPTION
```

```
"DMI: Diagnostic Monitoring Interface for fiber transceivers. Receive power on local fiber, measured in microwatts."
```

OID

MIB Description

```
ionDMIRxPowerEvt NOTIFICATION-TYPE
```

```
OBJECTS {
    ifIndex, ionDMIRxPowerAlarm, ionDMIRxPowerLevel
}
```

```
STATUS current
```

```
DESCRIPTION
```

```
"An ionDMIRxPowerEvt event is sent when there is a warning or alarm on Rx Power."
```

```
::= { tnIonMgmtNotifications 2 }
```

ionDMITxPowerEvt

An ionDMITxPowerEvt event is sent when there is a warning or alarm on Tx Power.

Varbinds

ifIndex

ionDMITxPowerAlarm

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),  
lowAlarm(6), highAlarm(7) }  
DESCRIPTION "."
```

ionDMITxPowerLevel

```
SYNTAX INTEGER  
DESCRIPTION "DMI: Diagnostic Monitoring Interface for fiber transceiv-  
ers. Transmit power on local fiber measured in microwatts."
```

OID

MIB Definition

```
ionDMITxPowerEvt NOTIFICATION-TYPE  
OBJECTS {  
    ifIndex, ionDMITxPowerAlarm, ionDMITxPowerLevel  
}  
STATUS current  
DESCRIPTION  
"An ionDMITxPowerEvt event is sent when there is a warning or alarm on Tx Power."  
::= { tnIonMgmtNotifications 3 }
```

ionDMITxBiasEvt

An ionDMITxBiasEvt event is sent when there is a warning or alarm on Tx Bias current,

Varbinds

ifIndex

ionDMITxBiasAlarm

```
SYNTAX INTEGER { normal(1), notSupported(2), lowWarn(3), highWarn(4),
lowAlarm(6), highAlarm(7) }
```

```
DESCRIPTION ". "
```

ionDMITxBiasCurrent

```
SYNTAX INTEGER
```

```
DESCRIPTION
```

```
"Transmit bias current on local fiber interface, in microamperes."
```

OID

MIB Description

```
ionDMITxBiasEvt NOTIFICATION-TYPE
```

```
OBJECTS {
    ifIndex, ionDMITxBiasAlarm, ionDMITxBiasCurrent
}
```

```
STATUS current
```

```
DESCRIPTION
```

```
"An ionDMITxBiasEvt event is sent when there is a warning or alarm on Tx Bias current."
```

```
::= { tnIonMgmtNotifications 4 }
```

ionDMITemperatureEvt

Varbinds

ifIndex

ionDMITempAlarm

SYNTAX INTEGER
DESCRIPTION ""

ionDMITemperature

SYNTAX INTEGER
STATUS current
DESCRIPTION
"Temperature of fiber transceiver in tenths of degrees C."

OID

MIB Description

```
ionDMITemperatureEvt NOTIFICATION-TYPE
OBJECTS {
    ifIndex, ionDMITempAlarm, ionDMITemperature
}
STATUS current
DESCRIPTION
"An ionDMITemperatureEvt event is sent when there is a warning or alarm on DMI temperature."
 ::= { tnIonMgmtNotifications 5 }
```

TN-ION-SOAM-EXT-MIB

ionSoamCCMDefectTrap

This trap is issued whenever a MEP records a change in its defect status.

Varbinds

dot1agCfmMdIndex

SYNTAX Unsigned32(1..4294967295)

DESCRIPTION

"The index to the Maintenance Domain table. dot1agCfmMdTableNextIndex needs to be inspected to find an available index for row-creation.

Referential integrity is required, i.e., the index needs to be persistent upon a reboot or restart of a device. The index can never be reused for other Maintenance Domain. The index value should keep increasing up to the time that they wrap around. This is to facilitate access control based on OID.

dot1agCfmMaIndex

SYNTAX Unsigned32(1..4294967295)

DESCRIPTION

"Index of the MA table dot1agCfmMdMaNextIndex needs to be inspected to find an available index for row-creation."

dot1agCfmMepIdentifier

SYNTAX Dot1agCfmMepId

DESCRIPTION

"Integer that is unique among all the MEPs in the same MA. Other definition is: a small integer, unique over a given Maintenance Association, identifying a specific Maintenance Association End Point (3.18).

The MEP Identifier is also known as the MEPID."

REFERENCE

"802.1ag clauses 3.18, 19.2 and 12.14.7"

Dot1agCfmMepDefects ::= TEXTUAL-CONVENTION

DESCRIPTION

"A MEP can detect and report a number of defects, and multiple defects can be present at the same time. These defects are:

bDefRDICCM(0) A remote MEP is reported the RDI bit in its last CCM.

bDefMAStatus(1) Either some remote MEP is reporting its Interface Status TLV as not isUp, or all remote MEPs are reporting a Port Status TLV that contains some value other than psUp.

bDefRemoteCCM(2) The MEP is not receiving valid CCMs from at least one of the remote MEPs.

bDefErrorCCM(3) The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.

bDefXconCCM(4) The MEP has received at least one CCM from either another MAID or a lower MD Level whose CCM Interval has not yet timed out. "

REFERENCE

"802.1ag clauses 12.14.7.1.3:o, 12.14.7.1.3:p, 12.14.7.1.3:q, 12.14.7.1.3:r, and 12.14.7.1.3:s."

SYNTAX BITS {

```

    bDefRDICCM(0),
    bDefMACstatus(1),
    bDefRemoteCCM(2),
    bDefErrorCCM(3),
    bDefXconCCM(4)
  }
```

DotlagCfmMepId ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

DESCRIPTION

"Maintenance association End Point Identifier (MEPID): A small integer, unique over a given Maintenance Association, identifying a specific MEP. "

REFERENCE

"802.1ag clauses 3.18 and 19.2.1"

SYNTAX Unsigned32 (1..8191)

OID**MIB Definition**

ionSoamCCMDefectTrap NOTIFICATION-TYPE

```

OBJECTS { dotlagCfmMdIndex,
          dotlagCfmMaIndex,
          dotlagCfmMepIdentifier,
          dotlagCfmMepDefects }
```

STATUS current

DESCRIPTION

"This trap is issued whenever a MEP records a change in its defect status"

```
 ::= { ionSoamExtTraps 1 }
```

ionSoamRemoteMepAddTrap**Varbinds*****dotlagCfmMdIndex***

SYNTAX Unsigned32(1..4294967295)

DESCRIPTION

"The index to the Maintenance Domain table. dotlagCfmMdTableNextIndex needs to be inspected to find an available index for row-creation.

Referential integrity is required, i.e., the index needs to be persistent upon a reboot or restart of a device. The index can never be reused for other Maintenance Domain. The index value should keep increasing up to the time that they wrap around. This is to facilitate access control based on OID.

dotlagCfmMaIndex

SYNTAX Unsigned32(1..4294967295)

DESCRIPTION

"Index of the MA table dot1agCfmMdMaNextIndex needs to be inspected to find an available index for row-creation."

dot1agCfmMepIdentifier

SYNTAX Dot1agCfmMepId

DESCRIPTION

"Integer that is unique among all the MEPs in the same MA. Other definition is: a small integer, unique over a given Maintenance Association, identifying a specific Maintenance association End Point (3.18). MEP Identifier is also known as the MEPID. "

REFERENCE

"802.1ag clauses 3.18, 19.2 and 12.14.7"

dot1agCfmMepDbRMepIdentifier

SYNTAX Dot1agCfmMepId

DESCRIPTION

"Maintenance association End Point Identifier of a remote MEP whose information from the MEP Database is to be returned. "

REFERENCE

"802.1ag clause 12.14.7.6.2:b"

Dot1agCfmMepId ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

DESCRIPTION

"Maintenance association End Point Identifier (MEPID): A small integer, unique over a given Maintenance Association, identifying a specific MEP. "

REFERENCE

"802.1ag clauses 3.18 and 19.2.1"

SYNTAX Unsigned32 (1..8191)

OID

MIB Description

ionSoamRemoteMepAddTrap NOTIFICATION-TYPE

OBJECTS { dot1agCfmMdIndex,
dot1agCfmMaIndex,
dot1agCfmMepIdentifier,
dot1agCfmMepDbRMepIdentifier }

STATUS current

DESCRIPTION

"This trap is issued whenever a far end MEP is added to the CCM database via auto-detection"

::= { ionSoamExtTraps 2 }

ionSoamRemoteMepRemoveTrap

Varbind

dot1agCfmMdIndex

SYNTAX Unsigned32(1..4294967295)

DESCRIPTION

"The index to the Maintenance Domain table.

dot1agCfmMdTableNextIndex needs to be inspected to find an available index for row-creation.

Referential integrity is required, i.e., the index needs to be persistent upon a reboot or restart of a device. The index can never be reused for other Maintenance Domain. The index value should keep increasing up to the time that they wrap around. This is to facilitate access control based on OID.

dot1agCfmMaIndex

SYNTAX Unsigned32(1..4294967295)

DESCRIPTION

"Index of the MA table dot1agCfmMdMaNextIndex needs to be inspected to find an available index for row-creation."

dot1agCfmMepIdentifier

SYNTAX Dot1agCfmMepId

DESCRIPTION

"Integer that is unique among all the MEPs in the same MA. Other definition is: a small integer, unique over a given Maintenance Association, identifying a specific Maintenance association End Point (3.18). MEP Identifier is also known as the MEPID. "

REFERENCE

"802.1ag clauses 3.18, 19.2 and 12.14.7"

dot1agCfmMepDbRMepIdentifier

SYNTAX Dot1agCfmMepId

DESCRIPTION

"Maintenance association End Point Identifier of a remote MEP whose information from the MEP Database is to be returned. "

REFERENCE

"802.1ag clause 12.14.7.6.2:b"

Dot1agCfmMepId ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

DESCRIPTION

"Maintenance association End Point Identifier (MEPID): A small integer, unique over a given Maintenance Association, identifying a specific MEP."

REFERENCE

"802.1ag clauses 3.18 and 19.2.1"

SYNTAX Unsigned32 (1..8191)

OID**MIB Definition**

ionSoamRemoteMepRemoveTrap NOTIFICATION-TYPE

OBJECTS { dotlagCfmMdIndex,
dotlagCfmMaIndex,
dotlagCfmMepIdentifier,
dotlagCfmMepDbRMepIdentifier }

STATUS current

DESCRIPTION

"This trap is issued whenever a far end MEP is removed from the CCM database via auto-detection"

::= { ionSoamExtTraps 3 }

TN-ION-SOAM-IDX-MIB

None

TN-PROVBRIDGE-MIB

None

ION Public MIBS

IEEE8021-CFM-MIB

dot1agCfmFaultAlarm

"A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.

Whenever a MEP has a persistent defect, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm.

If a defect with a higher priority is raised after a Fault Alarm has been issued, another Fault Alarm is issued.

The management entity receiving the notification can identify the system from the network source address of the notification, and can identify the MEP reporting the defect by the indices in the OID of the dot1agCfmMepHighestPrDefect variable in the notification:

dot1agCfmMdIndex - Also the index of the MEP's Maintenance Domain table entry (dot1agCfmMdTable).

dot1agCfmMaIndex - Also an index (with the MD table index) of the MEP's Maintenance Association network table entry (dot1agCfmMaNetTable), and (with the MD table index and component ID) of the MEP's MA component table entry (dot1agCfmMaCompTable).

dot1agCfmMepIdentifier - MEP Identifier and final index into the MEP table (dot1agCfmMepTable).

VarBinds

dot1agCfmMepHighestPrDefect

OBJECT-TYPE

SYNTAX Dot1agCfmHighestDefectPri

DESCRIPTION

"The highest priority defect that has been present since the MEPs Fault Notification Generator State Machine was last in the FNG_RESET state. "

REFERENCE

"802.1ag clause 12.14.7.1.3:n 20.33.9 and Table 21-1"

Dot1agCfmHighestDefectPri ::= TEXTUAL-CONVENTION

DESCRIPTION

"An enumerated value, equal to the contents of the variable highestDefect (20.33.9 and Table 20-1), indicating the highest-priority defect that has been present since the MEP Fault Notification Generator State Machine was last in the FNG_RESET state, either:

 none(0) no defects since FNG_RESET

```
defRDICCM(1)   DefRDICCM
defMACstatus(2) DefMACstatus
defRemoteCCM(3) DefRemoteCCM
defErrorCCM(4) DefErrorCCM
defXconCCM(5) DefXconCCM
```

The value 0 is used for no defects so that additional higher priority values can be added, if needed, at a later time, and so that these values correspond with those in Dot1agCfmLowestAlarmPri. "

REFERENCE

"802.1ag clause 20.1.2, 12.14.7.7.2:c and 20.33.9"

```
SYNTAX   INTEGER {
    none          (0),
    defRDICCM     (1),
    defMACstatus  (2),
    defRemoteCCM  (3),
    defErrorCCM   (4),
    defXconCCM    (5)
}
```

OID

MIB Description

```
-- *****
-- NOTIFICATIONS (TRAPS)
-- These notifications will be sent to the management entity
-- whenever a MEP loses/restores contact with one or more other MEPs.
-- *****
```

```
dot1agCfmFaultAlarm
NOTIFICATION-TYPE
OBJECTS   { dot1agCfmMepHighestPrDefect
}
STATUS    current
DESCRIPTION
```

"A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.

Whenever a MEP has a persistent defect, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm.

If a defect with a higher priority is raised after a Fault Alarm has been issued, another Fault Alarm is issued.

The management entity receiving the notification can identify the system from the network source address of the notification, and can identify the MEP reporting the defect by the indices in the OID of the dot1agCfmMepHighestPrDefect variable in the notification:

dot1agCfmMdIndex - Also the index of the MEP's

Maintenance Domain table entry
(dot1agCfmMdTable).
dot1agCfmMaIndex - Also an index (with the MD table index)
of the MEP's Maintenance Association
network table entry
(dot1agCfmMaNetTable), and (with the MD
table index and component ID) of the
MEP's MA component table entry
(dot1agCfmMaCompTable).
dot1agCfmMepIdentifier - MEP Identifier and final index
into the MEP table (dot1agCfmMepTable).

"

REFERENCE

"802.1ag clause 12.14.7.7"
::= { dot1agNotifications 1 }

BRIDGE-MIB

newRoot

The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.

Varbinds

None

OID

MIB Description

```
newRoot NOTIFICATION-TYPE
```

```
-- OBJECTS      { }
```

```
STATUS          current
```

```
DESCRIPTION
```

"The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional."

```
::= { dot1dNotifications 1 }
```

topologyChange

A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newroot trap is sent for the same transition. Implementation of this trap is optional.

Varbinds

None

OID

MIB Description

```
topologyChange NOTIFICATION-TYPE
-- OBJECTS      { }
STATUS         current
DESCRIPTION
```

"A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newroot trap is sent for the same transition. Implementation of this trap is optional."

```
::= { dot1dNotifications 2 }
```


DOT3-OAM-MIB

dot3OamThresholdEvent

A dot3OamThresholdEvent notification is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event.

This notification should not be sent more than once per second.

The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance in the dot3OamEventLogTable.

The management entity should periodically check dot3OamEventLogTable to detect any missed events.

Varbinds

dot3OamEventLogTimestamp

SYNTAX TimeStamp

DESCRIPTION

"The value of sysUpTime at the time of the logged event. For locally generated events, the time of the event can be accurately retrieved from sysUpTime. For remotely generated events, the time of the event is indicated by the reception of the Event Notification OAMPDU indicating that the event occurred on the peer. A system may attempt to adjust the timestamp value to more accurately reflect the time of the event at the peer OAM entity by using other information, such as that found in the timestamp found of the Event Notification TLVs, which provides an indication of the relative time between events at the peer entity. "

dot3OamEventLogOui

SYNTAX EightOTwoOui

DESCRIPTION

"The OUI of the entity defining the object type. All IEEE 802.3 defined events (as appearing in [802.3ah] except for the Organizationally Unique Event TLVs) use the IEEE 802.3 OUI of 0x0180C2. Organizations defining their own Event Notification TLVs include their OUI in the Event Notification TLV that gets reflected here. "

dot3OamEventLogType

SYNTAX Unsigned32

DESCRIPTION

"The type of event that generated this entry in the event log. When the OUI is the IEEE 802.3 OUI of 0x0180C2, the following event types are defined:

- erroredSymbolEvent(1),
- erroredFramePeriodEvent(2),
- erroredFrameEvent(3),
- erroredFrameSecondsEvent(4),
- linkFault(256),

dyingGaspEvent(257),
criticalLinkEvent(258)

The first four are considered threshold crossing events, as they are generated when a metric exceeds a given value within a specified window. The other three are not threshold crossing events.

When the OUI is not 71874 (0x0180C2 in hex), then some other organization has defined the event space. If event subtyping is known to the implementation, it may be reflected here.

Otherwise, this value should return all F's (2³² - 1). "

REFERENCE "[802.3ah], 30.3.6.1.10 and 57.5.3."

dot3OamEventLogLocation

SYNTAX INTEGER { local(1), remote(2) }

DESCRIPTION

"Whether this event occurred locally (local(1)), or was received from the OAM peer via Ethernet OAM (remote(2)).

"

dot3OamEventLogWindowHi

SYNTAX Unsigned32

DESCRIPTION

"If the event represents a threshold crossing event, the two objects dot3OamEventWindowHi and dot3OamEventWindowLo, form an unsigned 64-bit integer yielding the window over which the value was measured for the threshold crossing event (for example, 5, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

$dot3OamEventLogWindow = ((2^{32}) * dot3OamEventLogWindowHi) + dot3OamEventLogWindowLo$.

Otherwise, this value is returned as all F's (2³² - 1) and adds no useful information.

"

REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogWindowLo

SYNTAX Unsigned32

DESCRIPTION

"If the event represents a threshold crossing event, the two objects dot3OamEventWindowHi and dot3OamEventWindowLo form an unsigned 64-bit integer yielding the window over which the value was measured for the threshold crossing event (for example, 5, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

$dot3OamEventLogWindow = ((2^{32}) * dot3OamEventLogWindowHi) + dot3OamEventLogWindowLo$

Otherwise, this value is returned as all F's (2³² - 1) and adds no useful information. "

REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogThresholdHi

SYNTAX Unsigned32

DESCRIPTION

"If the event represents a threshold crossing event, the two objects dot3OamEventThresholdHi and dot3OamEventThresholdLo form an unsigned 64-bit integer yielding the value that was

crossed for the threshold crossing event (for example, 10, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

$$\text{dot3OamEventLogThreshold} = ((2^{32}) * \text{dot3OamEventLogThresholdHi}) + \text{dot3OamEventLogThresholdLo}$$

Otherwise, this value is returned as all F's ($2^{32} - 1$) and adds no useful information. "
 REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogThresholdLo

SYNTAX Unsigned32

DESCRIPTION

"If the event represents a threshold crossing event, the two objects dot3OamEventThresholdHi and dot3OamEventThresholdLo form an unsigned 64-bit integer yielding the value that was crossed for the threshold crossing event (for example, 10, when 11 occurrences happened in 5 seconds while the threshold was 10). The two objects are combined as:

$$\text{dot3OamEventLogThreshold} = ((2^{32}) * \text{dot3OamEventLogThresholdHi}) + \text{dot3OamEventLogThresholdLo}$$

Otherwise, this value is returned as all F's ($2^{32} - 1$) and adds no useful information. "
 REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogValue

SYNTAX CounterBasedGauge64

DESCRIPTION

"If the event represents a threshold crossing event, this value indicates the value of the parameter within the given window that generated this event (for example, 11, when 11 occurrences happened in 5 seconds while the threshold was 10).

Otherwise, this value is returned as all F's ($2^{64} - 1$) and adds no useful information. "
 REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogRunningTotal

SYNTAX CounterBasedGauge64

DESCRIPTION

"Each Event Notification TLV contains a running total of the number of times an event has occurred, as well as the number of times an Event Notification for the event has been transmitted. For non-threshold crossing events, the number of events (dot3OamLogRunningTotal) and the number of resultant Event Notifications (dot3OamLogEventTotal) should be identical.

For threshold crossing events, since multiple occurrences may be required to cross the threshold, these values are likely different. This value represents the total number of times this event has happened since the last reset (for example, 3253, when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset). "

REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

dot3OamEventLogEventTotal

SYNTAX Unsigned32

DESCRIPTION

"Each Event Notification TLV contains a running total of the number of times an event has occurred, as well as the number of times an Event Notification for the event has been transmitted. For non-threshold crossing events, the number of events (dot3OamLogRunningTotal) and the number of resultant Event Notifications (dot3OamLogEventTotal) should be identical.

For threshold crossing events, since multiple occurrences may be required to cross the threshold, these values are likely different. This value represents the total number of times one or more of these occurrences have resulted in an Event Notification (for example, 51 when 3253 symbol errors have occurred since the last reset, which has resulted in 51 symbol error threshold crossing events since the last reset).

"

REFERENCE "[802.3ah], 30.3.6.1.37 and 57.5.3.2."

OID

MIB Description

dot3OamThresholdEvent NOTIFICATION-TYPE

```
OBJECTS { dot3OamEventLogTimestamp,
          dot3OamEventLogOui,
          dot3OamEventLogType,
          dot3OamEventLogLocation,
          dot3OamEventLogWindowHi,
          dot3OamEventLogWindowLo,
          dot3OamEventLogThresholdHi,
          dot3OamEventLogThresholdLo,
          dot3OamEventLogValue,
          dot3OamEventLogRunningTotal,
          dot3OamEventLogEventTotal
        }
```

STATUS current

DESCRIPTION

"A dot3OamThresholdEvent notification is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event.

This notification should not be sent more than once per second.

The OAM entity can be derived from extracting the ifIndex from the variable bindings.

The objects in the notification correspond to the values in a row instance in the dot3OamEventLogTable.

The management entity should periodically check dot3OamEventLogTable to detect any missed events."

```
::= { dot3OamNotifications 1 }
```

dot3OamNonThresholdEvent NOTIFICATION-TYPE

```
OBJECTS { dot3OamEventLogTimestamp,
          dot3OamEventLogOui,
          dot3OamEventLogType,
```

```

dot3OamEventLogLocation,
dot3OamEventLogEventTotal
}
STATUS current

```

DESCRIPTION

"A dot3OamNonThresholdEvent notification is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event.

This notification should not be sent more than once per second.

The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance of the dot3OamEventLogTable.

The management entity should periodically check dot3OamEventLogTable to detect any missed events."
::= { dot3OamNotifications 2 }

ENTITY-MIB

```
entConfigChange NOTIFICATION-TYPE
```

```
STATUS current
```

DESCRIPTION

"An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.

An agent should not generate more than one entConfigChange 'notification-event' in a given time interval (five seconds is the suggested default). A 'notification-event' is the transmission of a single trap or informs PDU to a list of notification destinations.

If additional configuration changes occur within the throttling period, then notification-events for these changes should be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event should be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started right away.

An NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events, e.g., due to throttling or transmission loss."

```
::= { entityMIBTrapPrefix 1 }
```

EtherLike-MIB

None

IANA-MAU-MIB

None

IEEE8021-CFM-V2-MIB

None

IEEE8021-TC-MIB

None

IF-MIB**linkDown****varbinds*****ifIndex***

SYNTAX InterfaceIndex

DESCRIPTION

"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

ifAdminStatus

```
SYNTAX INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3)     -- in some test mode
}
```

DESCRIPTION

"The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state)."

ifOperStatus

```
SYNTAX INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3),    -- in some test mode
    unknown(4),   -- status can not be determined
                  -- for some reason.
    dormant(5),
    notPresent(6), -- some component is missing
    lowerLayerDown(7) -- down due to state of
                    -- lower-layer interface(s)
}
```

DESCRIPTION

"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive

network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

InterfaceIndex ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

DESCRIPTION

"A unique value, greater than zero, for each interface or interface sub-layer in the managed system. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

SYNTAX Integer32 (1..2147483647)

OID

MIB Description

linkDown NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }

STATUS current

DESCRIPTION

"A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 3 }

linkUp

varbinds

ifIndex

SYNTAX InterfaceIndex

DESCRIPTION

"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

ifAdminStatus

```
SYNTAX INTEGER {
    up(1),           -- ready to pass packets
    down(2),
    testing(3)      -- in some test mode
}
```

DESCRIPTION

Appendix G: SNMP Traps Supported

"The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state)."

ifOperStatus

```
SYNTAX INTEGER {
    up(1),          -- ready to pass packets
    down(2),
    testing(3),     -- in some test mode
    unknown(4),    -- status can not be determined -- for some reason.
    dormant(5),
    notPresent(6), -- some component is missing
    lowerLayerDown(7) -- down due to state of -- lower-layer interface(s)
}
```

DESCRIPTION

"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

InterfaceIndex ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

DESCRIPTION

"A unique value, greater than zero, for each interface or interface sub-layer in the managed system. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

SYNTAX Integer32 (1..2147483647)

OID

MIB Description

linkUp NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }

STATUS current

DESCRIPTION

"A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 4 }

LLDP-MIB

None

NOTIFICATION-LOG-MIB

None

P-BRIDGE-MIB

None

Q-BRIDGE-MIB

None

RFC1213-MIB

None

RMON-MIB (RFC 2819)

risingAlarm

SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP.

Varbinds

alarmIndex

SYNTAX Integer32 (1..65535)

DESCRIPTION

"An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device."

alarmVariable

SYNTAX OBJECT IDENTIFIER

DESCRIPTION

"The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.

Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

During a set operation, if the supplied variable name is not available in the selected MIB view, a bad-Value error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

alarmSampleType

```
SYNTAX INTEGER {
    absoluteValue(1),
    deltaValue(2)
}
```

DESCRIPTION

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

This object may not be modified if the associated alarmStatus object is equal to valid(1).

alarmValue

SYNTAX Integer32

DESCRIPTION

"The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds.

The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes."

alarmRisingThreshold

SYNTAX Integer32

DESCRIPTION

"A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.

A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3).

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

OID

MIB Description

risingAlarm NOTIFICATION-TYPE

OBJECTS { alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmRisingThreshold }

STATUS current

DESCRIPTION

"The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps."

::= { rmonEventsV2 1 }

fallingAlarm

The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Varbinds

alarmIndex

SYNTAX Integer32 (1..65535)

DESCRIPTION

"An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device."

alarmVariable

SYNTAX OBJECT IDENTIFIER

DESCRIPTION

"The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.

Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe.

During a set operation, if the supplied variable name is not available in the selected MIB view, a bad-Value error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4).

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

alarmSampleType

```
SYNTAX INTEGER {  
    absoluteValue(1),  
    deltaValue(2)  
}
```

DESCRIPTION

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

This object may not be modified if the associated alarmStatus object is equal to valid(1).

alarmValue

SYNTAX Integer32

DESCRIPTION

"The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds.

The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes."

alarmRisingThreshold

SYNTAX Integer32

DESCRIPTION

"A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3).

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.

This object may not be modified if the associated alarmStatus object is equal to valid(1)."

MIB Description

fallingAlarm NOTIFICATION-TYPE

OBJECTS { alarmIndex, alarmVariable, alarmSampleType,
alarmValue, alarmFallingThreshold }

STATUS current

DESCRIPTION

"The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps."

::= { rmonEventsV2 2 }

RMON2-MIB

None

SNMP-COMMUNITY-MIB

None

SNMP-NOTIFICATION-MIB

None

SNMP-TARGET-MIB

None

Trap Server Log

The Trap Server log file contains information presented to the trap server by ION devices.

A sample part of a trap server log file is shown below.

```
Line
1
2
3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
12
13 E=
14 Ebig=
15 IP=192.251.144.220
16 com=trap
17 GT=Notification
18 ST=
19 TS=Thu May 13 10:06:42 2010
20 VB-Count=3
21 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266790) 326 days, 15:37:47.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
22
23 E=
24 Ebig=
25 IP=192.251.144.220
26 com=trap
27 GT=Notification
28 ST=
29 TS=Thu May 13 10:10:17 2010
30 VB-Count=3
31 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288348) 326 days, 15:41:23.48 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 |
iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
32
33 E=
34 Ebig=
35 IP=192.251.144.220
36 com=trap
37 GT=Notification
38 ST=
39 TS=Thu May 13 10:10:18 2010
40 VB-Count=5
41 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288428) 326 days, 15:41:24.28 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.4.1.868.2.5.2.0.1 |
iso.3.6.1.2.1.47.1.1.1.1.1.134217728 = 134217728 | iso.3.6.1.4.1.868.2.5.2.1.1.1.1.134217728.6 = 6 | iso.3.6.1.4.1.868.2.5.2.1.1.2.134217728.6
= 1
```


The trap server log file lines are described below.

```

3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 =

```

Table 38: Trap Server Log File Description

Category	Example	Meaning
E=		Endian
Ebig=		bigEndian
IP=	192.251.144.220	IP address
com=	trap	
GT=	Notification	
ST=		
TS=	Thu May 13 10:06:37 2010	Timestamp – the log date that the file was recorded
VB-Count=	3	
Vars=	iso.3.6.1.2.1.1.3.0 =	Varbinds (Variable bindings) - the variable number of values that are included in an SNMP packet. Each varbind has an OID, type, and value (the value for/from that Object ID).
Timeticks:	(2822266290) 326 days, 15:37:42.90	
iso.3.6.1.6.3.1.1.4.1.0 =	iso.3.6.1.2.1.47.2.0.1	
iso.3.6.1.6.3.1.1.4.3.0 =	iso.3.6.1.2.1.47.2	

For Additional SNMP MIB Trap Information

For information on Network Management for Microsoft Networks Using SNMP, see <http://technet.microsoft.com/en-us/library/cc723469.aspx> or the [MSDN Library](#).

The notification MIB is described in section 4.2 and section 7.2 of RFC 2573, available from the IETF web site at <http://www.ietf.org/rfc/rfc2573.txt>.

Appendix H: ION Power Supply / DCR / ADP / LG Configuration

This appendix provides information on various options and Power Supply modules for the ION chassis:

- IONDCR (Dry Contact Relay) Module
- IONADP (Point System™-to-ION Adapter)
- IONLG (ION Last Gasp) Kit
- ION Power Supply Temperature, Voltage, Power, and Fan sensors
- IONPS-A Redundant AC Power Supply for 19-Slot ION Chassis
- IONPS-D Redundant -48VDC Power Supply Module for 19-Slot ION Chassis

The ION chassis can support up to two power supply modules which mount in the rear of the chassis. A single power supply can be used to power all the devices installed in the chassis; however the system can be made redundant with the use of a second power supply. In this configuration, the power supplies operate in an instant-fail-over mode.

The ION Power Supply (IONPS-A or IONPS-D) can be configured using either the CLI or Web method.

Power Supply Config – CLI Method

1. Access the Power Supply through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. To turn slot power on or off, or reset (reboot) a slot, type **set slot xx power yy** and press **Enter** (where xx = the PS slot number – 22 or 23, and yy = the function to perform – off, on, or reset).
3. To enable the Power Supply’s Power Relay, type **set power relay state=enable** and press **Enter**.
4. Set the Power Supply or Fan’s Sensor Notification / Relation / Severity / Value. For example:

```
C1|S5|L1P2>set slot 22 power ?
  off
  on
  reset
C1|S5|L1P2>set slot 22 power=on
C1|S22|L1D>set sensor stid=9 notif= enable
C1|S22|L1D>set sensor stid=9 relation=lessThan
C1|S22|L1D>set sensor stid=9 severity=major
C1|S22|L1D>set sensor stid=9 value=9
```

5. Press **Enter**.

Note: Use the **stat** command to view the chassis slot assignments. Power Supplies are assigned slot 22 and slot 23 by default. The ION chassis has **PS 1 ON** and **PS 2 ON** LEDs to indicate power supply presence and function.

Note: Use the **show power config** command to view the existing power supply configuration. For example:

```
C1|S22|L1D>show power config
Power supply sensors information:
```

Temperature Sensor:

```
Type:          celsius
Scale:         units
Precision:     0
Value:        26
Operation status: ok
Units display: The data units displayed for temperature is units(9)
```

Threshold information:

index	severity	relation	value	evaluation	notifEnable
1	other	lessThan	0	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:         milli
Precision:     0
Value:        12624
Operation status: ok
Units display: The data units displayed for volts is milli(8)
```

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:     0
Value:        26
Operation status: ok
Units display: The data units displayed for watts is in units(9)
```

Threshold information:

index	severity	relation	value	evaluation	notifEnable
1	critical	lessOrEqual	10	false	true
2	minor	greaterThan	225	false	false
3	major	greaterOrEqual	250	false	false
4	critical	greaterOrEqual	275	false	true

Relay:

```
Type:          other
Scale:         units
Precision:     0
Value:        2
Operation status: ok
Units display: The data units displayed for Relay is in units(9)
```

```
Installed:     false
State:         disable
Module type:   acModule
Oper mode:    master
```

Appendix G: SNMP Traps Supported

Fan-1:

```
Type: rpm
Scale: units
Precision: 0
Value: 2685
Operation status: ok
Units display: The data units displayed for Fan 1 in RPM is in units(9)
```

Threshold information:

index	severity	relation	value	evaluation	notifEnable
1	critical	equalTo	0	false	true
2	minor	greaterThan	9000	false	false
3	major	greaterOrEqual	9500	false	false
4	critical	greaterOrEqual	9900	false	true

Fan-2:

```
Type: rpm
Scale: units
Precision: 0
Value: 2760
Operation status: ok
Units display: The data units displayed for Fan 2 in RPM is in units(9)
```

Threshold information:

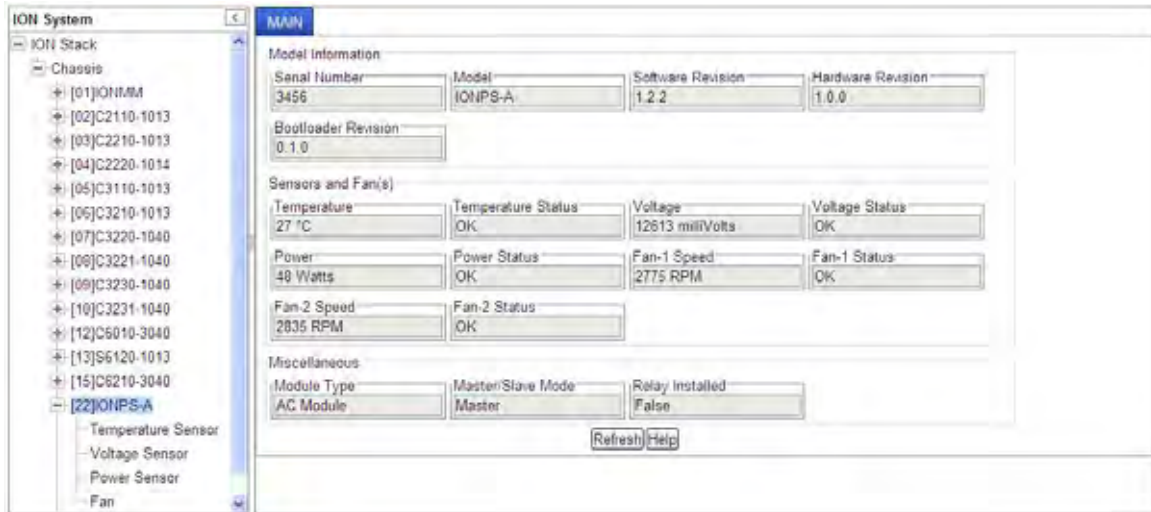
index	severity	relation	value	evaluation	notifEnable
1	critical	equalTo	0	false	true
2	minor	greaterThan	9000	false	false
3	major	greaterOrEqual	9500	false	false
4	critical	greaterOrEqual	9900	false	true

C1|S22|L1D>

Power Supply Config – Web Method

The ION Web interface allows configuration of the IONPS-A Power Supply’s Temperature Sensor, Voltage Sensor, Power Sensor, and Fan.

1. Select the IONPS-A or IONPS-D Power Supply. The Power Supply **MAIN** tab displays the current power supply information.

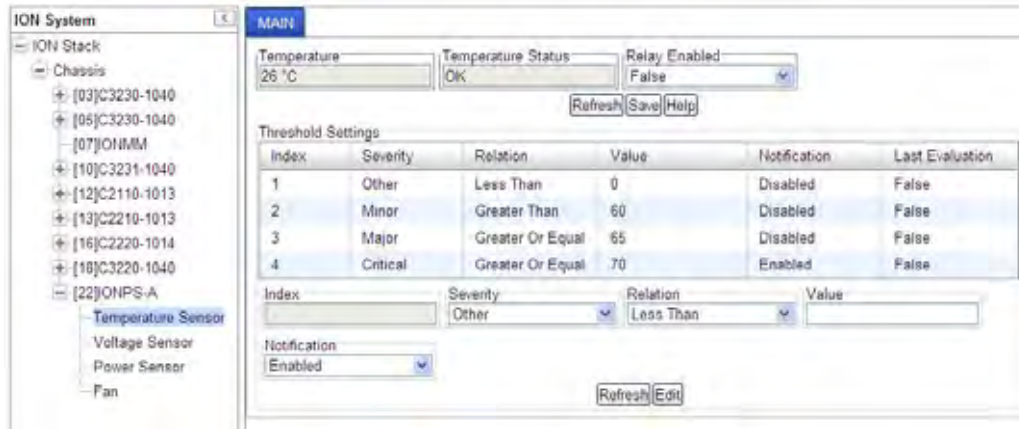


The **MAIN** tab displays an overview of power supply model information, data on the sensor and fan(s), and Miscellaneous information. The **MAIN** tab’s **Miscellaneous** section includes:

- **Module Type:** AC or DC voltage.
 - **Master/Slave Mode:** if a redundant module exists, this value indicates whether this is the Master power supply or the Slave power supply. The Slave power supply is the fail-over or redundant (backup) power supply.
 - **Relay Installed:** tells whether the dry contact relay (DCR) is installed (ExtRelayInstalled) in the power supply.
 - **Relay Enabled:** this setting enables or disables the relay contact if it is installed (SensorExtRelayInstalled) in the power supply. This relay contact is used to trigger an event to the user by attaching an external indicator. Displays only if the **Relay Installed** field displays **True**.
2. From the Power Supply’s **MAIN** tab, expand / select the Temperature Sensor, Voltage Sensor, Power Sensor, or Fan for configuration and status information.

Temperature Sensor Configuration

The Threshold Settings table lists the threshold severity, relation, and comparison value for a sensor listed in the Entity-MIB Physical Table.



Index	Severity	Relation	Value	Notification	Last Evaluation
1	Other	Less Than	0	Disabled	False
2	Minor	Greater Than	60	Disabled	False
3	Major	Greater Or Equal	65	Disabled	False
4	Critical	Greater Or Equal	70	Enabled	False

- **Temperature:** displays the most recent temperature measurement obtained by the agent for this sensor.
- **Temperature Status:** displays the operational status of the physical sensor.
 - **OK** - indicates that the agent can obtain the sensor value.
 - **Unavailable** - indicates that the agent presently cannot obtain the sensor value.
 - **Nonoperational** - indicates that the agent believes the sensor is broken. The sensor could have a hard failure (disconnected wire), or a soft failure (e.g., out-of-range, jittery, or wildly fluctuating readings).
- **Relay Enabled:** select **False** to disable DCR (Dry Contact Relay) operation or select **True** to enable it. This selection enables or disables the relay contact if it is installed (ExtRelayInstalled) in the power supply.
- **Index:** select an index line / number that uniquely identifies an entry in the Threshold Table. The index permits the same sensor to have several different threshold values set.
- **Severity:** select **Minor**, **Major**, **Critical** or **Other**. Critical is the most severe, Major is the next most severe, and Minor is the least severe. The system might shut down the sensor associated FRU automatically if the sensor value reaches the Critical problem threshold.
- **Relation:** Less Than (<), Less Or Equal (\geq), Greater Than (>), Greater Or Equal (\geq), Equal To (=), or Not Equal To (\neq).
 - LessThan: if the sensor value is less than the threshold value.
 - LessOrEqual: if the sensor value is less than or equal to the threshold value.
 - GreaterThan: if the sensor value is greater than the threshold value.
 - GreaterOrEqual: if the sensor value is greater than or equal to the threshold value.
 - EqualTo: if the sensor value is equal to the threshold value.
 - NotEqualTo: if the sensor value is not equal to the threshold value.

Indicates the relation between sensor value (entSensorValue) and threshold value (ionEntSensorThresholdValue), required to trigger the alarm.

When evaluating the relation, entSensorValue is on the left of SensorThresholdRelation, and SensorThresholdValue is on the right (e.g., entSensorValue \geq SensorThresholdValue).

- **Value:** defines the value of the threshold (e.g., for a Major threshold severity selection, set a relation of Greater than or equal to 65 as the requirement for notification). To correctly display or interpret this variable's value, you must also know the SensorType, SensorScale, and SensorPrecision. However, you can directly compare SensorValue with the threshold values given in the SensorThresholdTable without any semantic knowledge.
- **Notification:** select **Enabled** to be informed of Temperature Sensor events, or select **Disabled** to not receive notification of Temperature Sensor events. If this value is **Disabled**, then no SensorThresholdNotification will be generated on this device. If this value is **Enabled**, then whether a SensorThresholdNotification for a threshold will be generated or not depends on the instance value of SensorThresholdNotificationEnable for that threshold.
- **Last Evaluation:** displays **True** if parameters were included in the most recent measurement, otherwise displays **False**. This value indicates the result of the most recent evaluation of the threshold. If the threshold condition is True, then SensorThresholdEvaluation is True. If the threshold condition is False, then SensorThresholdEvaluation is False. Thresholds are evaluated at the rate indicated by the SensorValueUpdateRate (e.g., 0= on demand (when polled), when the sensor value changes (event-driven), or the agent does not know the update rate).

3. Click the **Save** button when finished with Temperature Sensor configuration.

Voltage Sensor Configuration



Index	Severity	Relation	Value	Notification	Last Evaluation
1	Critical	Less Than	11220	Enabled	False
2	Minor	Greater Than	13000	Disabled	False
3	Major	Greater Or Equal	14000	Disabled	False
4	Critical	Greater Or Equal	14673	Enabled	False

- **Voltage:** displays the most recent voltage measurement obtained by the agent for this sensor.
- **Voltage Status:** displays the operational voltage status of the sensor.
 - **OK** - indicates that the agent can obtain the sensor value.
 - **Unavailable** - indicates that the agent presently cannot obtain the sensor value.
 - **Nonoperational** - indicates that the agent believes the sensor is broken. The sensor could have a hard failure (disconnected wire), or a soft failure (e.g., out-of-range, jittery, or wildly fluctuating readings).
- **Relay Enabled:** select **False** to disable DCR (Dry Contact Relay) operation or select **True** to enable it. This selection enables or disables the relay contact if it is installed (ExtRelayInstalled) in the power supply.
- **Index:** select an index line / number that uniquely identifies an entry in the Threshold Table. The index permits the same sensor to have several different threshold values set.
- **Severity:** select **Other**, **Minor**, **Major**, or **Critical**. Critical is the most severe, Major is the next most severe, and Minor is the least severe. The system might shut down the sensor associated FRU automatically if the sensor value reaches the Critical problem threshold.
- **Relation:** Less Than (<), Less Or Equal (\geq), Greater Than (>), Greater Or Equal (\geq), Equal To (=), or Not Equal To (\neq).
 - LessThan: if the sensor value is less than the threshold value.
 - LessOrEqual: if the sensor value is less than or equal to the threshold value.
 - GreaterThan: if the sensor value is greater than the threshold value.
 - GreaterOrEqual: if the sensor value is greater than or equal to the threshold value.
 - EqualTo: if the sensor value is equal to the threshold value.
 - NotEqualTo: if the sensor value is not equal to the threshold value.

Indicates the relation between sensor value (SensorValue) and threshold value (SensorThresholdValue), required to trigger the alarm.

When evaluating the relation, SensorValue is on the left of SensorThresholdRelation, and SensorThresholdValue is on the right (e.g., SensorValue \geq SensorThresholdValue).

- **Value:** defines the value of the threshold (e.g., for a Major threshold severity selection, set a relation of Greater than or equal to 14000 as the requirement for notification). To correctly display or interpret this variable's value, you must also know the SensorType, SensorScale, and SensorPrecision. However, you can directly compare SensorValue with the threshold values given in the SensorThresholdTable without any semantic knowledge.
 - **Notification:** select Enabled to be informed of Temperature Sensor events, or select Disabled to not receive notification of Temperature Sensor events. If this value is **Disabled**, then no SensorThresholdNotification will be generated on this device. If this value is **Enabled**, then whether a SensorThresholdNotification for a threshold will be generated or not depends on the instance value of SensorThresholdNotificationEnable for that threshold.
 - **Last Evaluation:** displays **True** if parameters were included in the most recent measurement, otherwise displays **False**. This value indicates the result of the most recent evaluation of the threshold. If the threshold condition is True, then SensorThresholdEvaluation is True. If the threshold condition is False, then SensorThresholdEvaluation is False. Thresholds are evaluated at the rate indicated by the SensorValueUpdateRate (e.g., 0= on demand (when polled), when the sensor value changes (event-driven), or the agent does not know the update rate).
4. Click the **Save** button when finished with Voltage Sensor configuration.

Power Sensor Configuration



The screenshot shows the 'ION System' configuration window. On the left is a tree view of the 'ION Stack' with 'Power Sensor' selected under 'ONPS-A'. The main area shows the following configuration:

- Power:** 31 Watts
- Power Status:** OK
- Relay Enabled:** False

Buttons: Refresh, Save, Help

Threshold Settings Table:

Index	Severity	Relation	Value	Notification	Last Evaluation
1	Critical	Less Or Equal	10	Enabled	False
2	Minor	Greater Than	225	Disabled	False
3	Major	Greater Or Equal	250	Disabled	False
4	Critical	Greater Or Equal	275	Enabled	False

Below the table are input fields for Index, Severity (Other), Relation (Less Than), and Value. A Notification dropdown is set to 'Enabled'. Buttons: Refresh, Edit

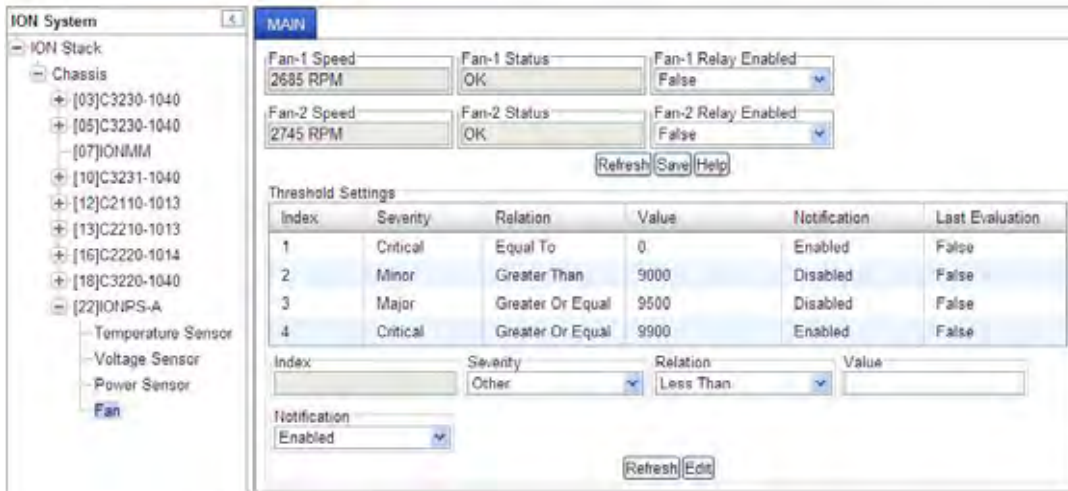
- **Power:** displays the most recent power measurement obtained by the agent for this sensor.
- **Power Status:** displays the operational power status of the sensor.
 - **OK** - indicates that the agent can obtain the sensor value.
 - **Unavailable** - indicates that the agent presently cannot obtain the sensor value.
 - **Nonoperational** - indicates that the agent believes the sensor is broken. The sensor could have a hard failure (disconnected wire), or a soft failure (e.g., out-of-range, jittery, or wildly fluctuating readings).
- **Relay Enabled:** select **False** to disable DCR (Dry Contact Relay) operation or select **True** to enable it. This selection enables or disables the relay contact if it is installed (ExtRelayInstalled) in the power supply.
- **Index:** select an index line / number that uniquely identifies an entry in the Threshold Table. The index permits the same sensor to have several different threshold values set.
- **Severity:** select **Other**, **Minor**, **Major**, or **Critical**. Critical is the most severe, Major is the next most severe, and Minor is the least severe. The system might shut down the sensor associated FRU automatically if the sensor value reaches the Critical problem threshold.
- **Relation:** Less Than (<), Less Or Equal (\geq), Greater Than (>), Greater Or Equal (\geq), Equal To (=), or Not Equal To (\neq).
 - LessThan: if the sensor value is less than the threshold value.
 - LessOrEqual: if the sensor value is less than or equal to the threshold value.
 - GreaterThan: if the sensor value is greater than the threshold value.
 - GreaterOrEqual: if the sensor value is greater than or equal to the threshold value.
 - EqualTo: if the sensor value is equal to the threshold value.
 - NotEqualTo: if the sensor value is not equal to the threshold value.

Indicates the relation between sensor value (entSensorValue) and threshold value (ionEntSensorThresholdValue), required to trigger the alarm.

When evaluating the relation, entSensorValue is on the left of SensorThresholdRelation, and SensorThresholdValue is on the right (e.g., entSensorValue \geq SensorThresholdValue).

- **Value:** defines the value of the threshold (e.g., for a Major threshold severity selection, set a relation of Greater than or equal to 14000 as the requirement for notification). To correctly display or interpret this variable's value, you must also know the SensorType, SensorScale, and SensorPrecision. However, you can directly compare SensorValue with the threshold values given in the SensorThresholdTable without any semantic knowledge.
 - **Notification:** select Enabled to be informed of Temperature Sensor events, or select Disabled to not receive notification of Temperature Sensor events. If this value is **Disabled**, then no SensorThresholdNotification will be generated on this device. If this value is **Enabled**, then whether a SensorThresholdNotification for a threshold will be generated or not depends on the instance value of SensorThresholdNotificationEnable for that threshold.
 - **Last Evaluation:** displays **True** if parameters were included in the most recent measurement, otherwise displays **False**. This value indicates the result of the most recent evaluation of the threshold. If the threshold condition is True, then SensorThresholdEvaluation is True. If the threshold condition is False, then SensorThresholdEvaluation is False. Thresholds are evaluated at the rate indicated by the SensorValueUpdateRate (e.g., 0= on demand (when polled), when the sensor value changes (event-driven), or the agent does not know the update rate).
5. Click the **Save** button when finished with Power Sensor configuration.

Fan Configuration



The screenshot shows the 'ION System' configuration window. On the left is a tree view of the 'ION Stack' with components like Chassis, IONMM, and IONPS-A. The main area is titled 'MAIN' and contains fields for Fan-1 and Fan-2 Speed, Status, and Relay Enabled. Below this is a 'Threshold Settings' table with columns for Index, Severity, Relation, Value, Notification, and Last Evaluation. At the bottom, there are input fields for Index, Severity, Relation, Value, and Notification, along with 'Refresh' and 'Edit' buttons.

Index	Severity	Relation	Value	Notification	Last Evaluation
1	Critical	Equal To	0	Enabled	False
2	Minor	Greater Than	9000	Disabled	False
3	Major	Greater Or Equal	9500	Disabled	False
4	Critical	Greater Or Equal	9900	Enabled	False

- **Fan-x Speed:** displays the most recent fan speed measurement obtained by the agent for this fan in RPM (e.g., 2730 revolutions-per-minute).
- **Fan-x Status:** displays the fan's operational status.
 - **OK** - indicates that the agent can obtain the sensor value.
 - **Unavailable** - indicates that the agent presently cannot obtain the sensor value.
 - **Nonoperational** - indicates that the agent believes the sensor is broken. The sensor could have a hard failure (disconnected wire), or a soft failure (e.g., out-of-range, jittery, or wildly fluctuating readings).
- **Fan-x Relay Enabled:** select **False** to disable the related Fan Relay operation or select **True** to enable it.
- **Index:** select an index line that uniquely identifies an entry in the Threshold Table. The index permits the same sensor to have several different threshold values set.
- **Severity:** select **Other**, **Minor**, **Major**, or **Critical**. Critical is the most severe, Major is the next most severe, and Minor is the least severe. The system might shut down the sensor associated FRU automatically if the sensor value reaches the Critical problem threshold.
- **Relation:** Less Than (<), Less Or Equal (≤), Greater Than (>), Greater Or Equal (≥), Equal To (=), or Not Equal To (≠).
 - **Less Than:** if the sensor value is less than the threshold value.
 - **Less Or Equal:** if the sensor value is less than or equal to the threshold value.
 - **Greater Than:** if the sensor value is greater than the threshold value.
 - **Greater Or Equal:** if the sensor value is greater than or equal to the threshold value.
 - **Equal To:** if the sensor value is equal to the threshold value.
 - **Not Equal To:** if the sensor value is not equal to the threshold value.

Indicates the relation between sensor value and sensor threshold value, required to trigger the alarm.

When evaluating the relation, SensorValue is on the left of SensorThresholdRelation, and SensorThresholdValue is on the right (e.g., SensorValue \geq SensorThresholdRelation \geq SensorThresholdValue).

- **Value:** defines the value of the threshold (e.g., for a Major threshold severity selection, set a relation of Greater than or equal to 14000 as the requirement for notification). To correctly display or interpret this variable's value, you must also know the SensorType, SensorScale, and SensorPrecision. However, you can directly compare SensorValue with the threshold values given in the SensorThresholdTable without any semantic knowledge.
- **Notification:** select Enabled to be informed of Temperature Sensor events, or select Disabled to not receive notification of Temperature Sensor events. If this value is **Disabled**, then no SensorThresholdNotification will be generated on this device. If this value is **Enabled**, then whether a SensorThresholdNotification for a threshold will be generated or not depends on the instance value of SensorThresholdNotificationEnable for that threshold.
- **Last Evaluation:** displays **True** if parameters were included in the most recent measurement, otherwise displays **False**. This value indicates the result of the most recent evaluation of the threshold. If the threshold condition is True, then SensorThresholdEvaluation is True. If the threshold condition is False, then SensorThresholdEvaluation is False. Thresholds are evaluated at the rate indicated by the SensorValueUpdateRate (e.g., 0= on demand (when polled), when the sensor value changes (event-driven), or the agent does not know the update rate).

5. Click the **Save** button when finished with Fan configuration.

IONDCR (Dry Contact Relay) Module

The IONDCR is a field installable dry contact relay option module for the IONPS-A (AC) and IONPS-D (DC) power supplies.

The IONDCR module mounts in the lower right-hand corner of the IONPS face-plate, allowing the power supply to be tied into a separate alarm circuit. Contacts will be activated on the loss of power, enabling an external visual or audible alarm (third party power management alarm systems).



Figure H-1: The IONDCR Module

Applications for this type of fault alarm output would include enterprise networks as well as in industrial applications. The DCR module provides another layer of fault indicators, complementing network management software by providing a signal to either a local or remote alarm system.

The IONDCR can be installed in either the IONPS-A (AC) or the IONPS-D (DC) power supply.

IONDCR with IONPS-A (AC) Power Supply

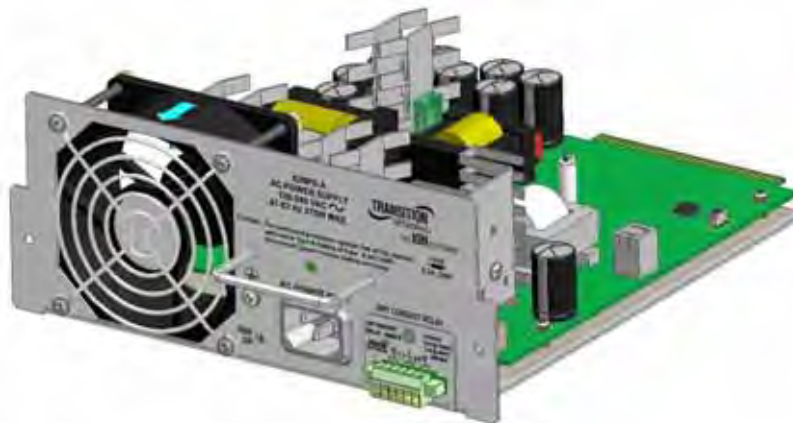


Figure H-2: IONDCR Installed in IONPS-A Power Supply

The IONDCR can be configured in either the IONPS-A or the IONPS-D via the CLI or Web interface.

IONDCR with IONPS-D (DC) Power Supply

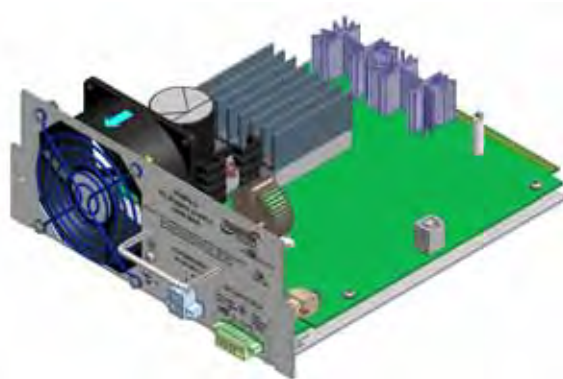


Figure H-3: IONDCR Installed in IONPS-D (DC) Power Supply

With a relay is installed in the IONPS, and a sensor set to Relay Enabled (the threshold evaluation is *true* and the corresponding threshold notification is *enabled*) then a physical alarm will be generated to warn that maintenance is required.

The IONDCR can be configured in either the IONPS-A or in the IONPS-D via the CLI or Web interface.

IONDCR Config –CLI Method

1. Access the Power Supply through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. To turn slot power on or off, or reset (reboot) a slot, type **set slot=xx power=yy** and press **Enter** (where xx = the PS slot number – 22 or 23, and yy = the function to perform – off, on, or reset).
3. Use the **go** command to switch to the Relay.
4. To enable the Power Supply’s Power Relay, type **set power relay state=enable** and press **Enter**.
5. Set the Power Supply or Fan’s Sensor Notification / Relation / Severity / Value. For example:

```

C1|S5|L1P2>set slot 22 power ?
  off
  on
  reset
C1|S5|L1P2>set slot 22 power=on
C1|S22|L1D>set sensor stid 9 ?
  notif
  relation
  severity
  value
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
    
```


Appendix G: SNMP Traps Supported

Note: Use the **stat** command to view the chassis slot assignments. Power Supplies are assigned slot 22 and slot 23 by default. The ION chassis has **PS 1 ON** and **PS 2 ON** LEDs to indicate power supply presence and function.

Note: Use the **show power config** command to view the existing power supply configuration.

IONDCR Config –Web Method

1. At the IONPS-A's MAIN screen, locate the **Relay Installed** field.

The screenshot shows the ION System web interface. On the left, a tree view shows the ION Stack with Chassis slots. Slot [22] IONPS-A is selected and circled in red. The main content area shows the MAIN screen for IONPS-A. The 'Relay Installed' field is circled in red. The 'Relay Installed' field is currently set to 'False'.

1. Under the IONPS-A, select the desired sensor's MAIN screen.
2. At the **Relay Enabled** dropdown, select **True**.
3. Click the **Save** button.
4. In the **Threshold Settings** table, select the desired **Index** number (line item).
5. Click the **Refresh** button.

The screenshot shows the ION System web interface. On the left, a tree view shows the ION Stack with Chassis slots. Slot [22] IONPS-A is selected. The main content area shows the MAIN screen for IONPS-A. The 'Relay Enabled' dropdown is set to 'True' and circled in red. The 'Threshold Settings' table is shown below, with the first row (Index 1) highlighted in blue. The 'Notification' column for Index 1 is 'Enabled' and the 'Last Evaluation' column is 'True'.

Index	Severity	Relation	Value	Notification	Last Evaluation
1	Minor	Less Than	28	Enabled	True
2	Minor	Greater Than	60	Disabled	False
3	Major	Greater Than	65	Disabled	False
4	Critical	Greater Or Equal	70	Enabled	False

6. Verify that the line item's **Notification** column shows **Enabled**, and the **Last Evaluation** column shows **True**.

IONADP (Point System™ -to-ION Adapter)

The IONADP is an adapter card that allows the ION chassis to be backwards compatible with Point System™ media converter modules. This adapter is designed to sit between a Point System module and the backplane of the ION chassis. The purpose of the IONADP is to lengthen the Point System module so it can be securely mounted in an ION chassis while also connecting to the backplane allowing the ION chassis to power the Point System module.

SNMP management of the Point System modules installed in the ION chassis is possible by using a Point System management module along with the IONADP.

The ION modules and the Point System modules are managed independently by their own respective management modules. The ION management module and the Point System management module would each require a unique IP address assigned to them, while Focal Point can be used to access the management information from each management module simultaneously.

The IONADP allows the ION platform to be backwards compatible with Point System slide-in-modules. Essentially, an ION chassis can be used as a Point System chassis. The IONADP kit includes adapter card, bracket, and four screws. Refer to the *IONADP Install Guide*, 33421 for more information.



Figure H-4: The IONADP Module

IONADP Config – CLI Method

1. *Information to be provided.*

IONADP Config – Web Method

1. *Information to be provided.*

IONLG (ION Last Gasp) Kit

The Last Gasp 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. This notification of an impending power loss before it happens allows for quicker resolution of the power loss. **Note:** the IONLG has last gasp hardware, but the last gasp trap in is not implemented in the current ION release.

The IONLG uses an external wall mount 12V 1.5A power supply. Refer to the *IONLG (ION Last Gasp Kit) Install Guide*, 33421 for more information.

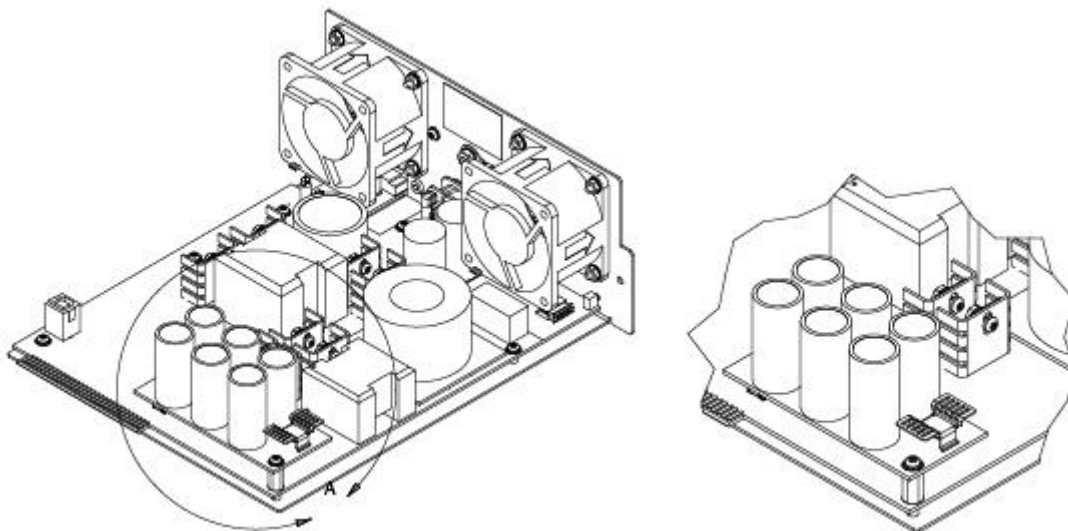


Figure H-5: The IONLG Module

IONLG Config – CLI Method

1. The x323x Dying Gasp function is configured via the CLI using the **set loam dg-evt-notif=enable** command.
2. Use the **show loam event config** command to display the current Link OAM event configuration.

IONLG Config – Web Method

1. The x323x Dying Gasp function is configured via the Web interface at Port > **LOAM** > **Event Configuration** > **Dying Gasp** Enabled/Disabled.

Glossary

This section describes many of the terms and mnemonics used in this manual. Note that the use of or description of a term does not in any way imply support of that feature or of any related function(s).

100BASE-FX

100BASE-FX is a version of Fast Ethernet over optical fiber. It uses a 1300 nm near-infrared (NIR) light wavelength transmitted via two strands of optical fiber, one for receive (RX) and the other for transmit (TX). Maximum length is 400 meters (1,310 ft) for half-duplex connections (to ensure collisions are detected), 2 kilometers (6,600 ft) for full-duplex over multimode optical fiber, or 10,000 meters (32,808 feet) for full-duplex single mode optical fiber. 100BASE-FX uses the same 4B5B encoding and NRZI line code that 100BASE-TX does. 100BASE-FX should use SC, ST, or MIC connectors with SC being the preferred option. 100BASE-FX is not compatible with 10BASE-FL, the 10 MBit/s version over optical fiber.

1000BASE-X

Refers to gigabit Ethernet transmission over fiber, where options include 1000BASE-CX, 1000BASE-LX, and 1000BASE-SX, 1000BASE-LX10, 1000BASE-BX10 or the non-standard -ZX implementations.

802.1

The IEEE standard for port-based Network Access Control.

802.1ad

IEEE 802.1ad (Provider Bridges) is an amendment to IEEE standard IEEE 802.1Q-1998 (aka QinQ or Stacked VLANs), intended to develop an architecture and bridge protocols to provide separate instances of the MAC services to multiple independent users of a Bridged LAN in a manner that does not require cooperation among the users, and requires a minimum of cooperation between the users and the provider of the MAC service.

802.1ag

The IEEE standard for Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management, 2007. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3-2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to LOAM.

802.1ah

IEEE 802.1ah-2008 is a set of architecture and protocols for routing of a customer network over a provider network, allowing interconnection of multiple Provider Bridge Networks without losing each customer's individually defined VLANs. The final standard was approved by the IEEE in June 2008.

802.1p

The IEEE standard for QoS packet classification.

802.1p Prioritization

The ability to send traffic to various prioritization queues based on the 802.1q VLAN Tag priority field. (AKA, CoS. Standard: IEEE 802.1p.)

802.1q

IEEE 802.1Q, or VLAN Tagging, is a networking standard allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks. IEEE 802.1Q (aka, dot1q) is commonly refers to the encapsulation protocol used to implement this mechanism over Ethernet networks. IEEE 802.1Q defines the meaning of a VLAN with respect to the specific conceptual model for bridging at the MAC layer and to the IEEE 802.1D spanning tree protocol.

802.1Q VLAN

802.1Q is a standardized way of segmenting and distributing VLAN information. Switches that support 802.1Q can recognize and forward, a tag packet upon egress. See also VID, dot1Q, IEEE 802.1Q. Contrast "PVLAN".)

802.3

The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to LOAM.

ACL

(Access Control List) A set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute.

Address

An IPv6-layer identifier for an interface or a set of interfaces.

Anycast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocol's measure of distance).

AES

(Advanced Encryption Standard) A privacy protocol; one of two encryption algorithms used for ION system data privacy. AES is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES ciphers were analyzed extensively and are now used worldwide (as was its predecessor, DES). AES was announced by NIST as U.S. FIPS PUB 197 (FIPS 197) in 2001 after a 5-year standardization process. AES was implemented as a Federal government standard in 2002 after approval by the U.S. Secretary of Commerce. AES is available in many different encryption packages. See also "DES".

Alarm Terminology - RFC 3877

The IETF's definitions of Alarms and other terms related to alarm management:

Error: A deviation of a system from normal operation.

Fault: A lasting error or warning condition.

Event: Something that happens which may be of interest (e.g., fault, a change in status, crossing a threshold, or an external input to the system).

Notification: Unsolicited transmission of management information.

Alarm: Persistent indication of a fault.

Alarm State: A condition or stage in the existence of an alarm. At a minimum, alarms states are raise and clear. They could also include severity information such as defined by perceived severity in the ITU model M.3100 (cleared, indeterminate, critical, major, minor and warning).

Alarm Raise: The initial detection of the fault indicated by an alarm or any number of alarm states later entered, except clear.

Alarm Clear: The detection that the fault indicated by an alarm no longer exists.

Active Alarm: An alarm which has an alarm state that has been raised, but not cleared.

Alarm Detection Point: The entity that detected the alarm.

Perceived Severity: The severity of the alarm as determined by the alarm detection point using the information it has available.

ANSI

(American National Standards Institute) A private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide.

ARAP

(AppleTalk Remote Access Protocol) the protocol used for accessing AppleTalk networks remotely. ARAP was introduced in conjunction with AppleTalk Remote Access in 1991. ARAP is an open protocol, and specifications are available for third-party developers. In its latest versions of the Apple Remote Access product family, the AppleTalk Remote Access Protocol has been enhanced to provide superior performance and configuration flexibility. ARAP slowly disappeared in the late 1990s when TCP/IP took over the vast majority of networking needs, notably remote access. In Mac OS X, ARAP is no longer required, as Apple has migrated their networking software to IP, and includes free remote access software.

AV pairs

(Attribute Value Pairs) AV-pairs are strings of text in the form attribute=value, sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

ARP

(Address Resolution Protocol) A protocol for mapping an IP address to a physical machine address that is recognized in the local network

Auto-Negotiation

With Auto-Negotiation in place, Ethernet can determine the common set of options supported between a pair of "link partners." Twisted-pair link partners can use Auto-Negotiation to figure out the highest speed that they each support as well as automatically setting full-duplex operation if both ends support that mode. (AKA, N-WAY Protocol. Standard: IEEE 802.3u.)

Auto MDI / MDIX

Auto MDI/MDIX automatically detects the MDI or MDIX setting on a connecting device in order to obtain a link. This means installers can use either a straight through or crossover cable and when connecting to any device, the feature is pretty self explanatory.

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.

Authentication

The process of ensuring message integrity and protection against message replays. Authentication includes both data integrity and data origin authentication.

Authoritative SNMP engine

SNMPv3 introduced the concept of an authoritative SNMP engine that lets you create authorized users for specific SNMPv3 agents. One of the SNMP copies involved in network communication designated as the allowed SNMP engine to protect against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (e.g., get exact, get next, set request), the receiver of these messages is authoritative. When an SNMP message does not expect a response, the sender is authoritative.

Bandwidth Profile Traffic Parameters

A Bandwidth profile associated with an Ethernet service consists of four traffic parameters: CIR, CBS, EIR, and EBS. A service frame is also associated with a Color Mode (CM); together, these five parameters specify the bandwidth profile for a particular service (i.e., Bandwidth Profile = CIR, CBS, EIR, EBS, CM).

Big Endian

Bit ordering within a byte where bits are sent serially starting with the MSB (most significant byte) and ending with the LSB (least significant byte). Contrast "Little Endian".

BPC

(Back Plane Controller) the ION chassis component that provides communication between the SIC cards and the IONMM. The BPC is an active device with a microprocessor and management software used to interconnect IONMM and SIC cards via the Ethernet management plane. The BPC has knowledge of the cards that are present in the system, and is responsible for managing the Ethernet switch that interconnects all the chassis slots.

BPDU

(Bridge Protocol Data Unit) Data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go.

Bridge

A device that connects one local area network (LAN) to another LAN.

CAT 1 – CAT 7 Cabling

ANSI/EIA Standard 568 is one of several standards that specify "categories" (each a "CAT") of twisted pair cabling systems. Assigned by the American National Standards Institute/Electronic Industries Association, these standards categories include CAT 1 – CAT 7, as shown below.

Category	Max Data Rate	Typical Application
CAT 1	Up to 1 Mbps (1 MHz)	Analog voice (POTS), ISDN BRI
CAT 2	4 Mbps	IBM Token Ring network cabling systems
CAT 3	16 Mbps	Voice (analog mainly); 10BASE-T Ethernet
CAT 4	20 Mbps	Used in 16 Mbps Token Ring, but not much else.
CAT 5	100 MHz	100 Mbps TPDDI. 155 Mbps ATM. No longer supported; replaced by 5E. 10/100BASE-T.
CAT 5E	100 MHz	100 Mbps TPDDI, 155 Mbps ATM, Gigabit Ethernet. Offers better near-end crosstalk than CAT 5.
CAT 6	Up to 250 MHz	Minimum cabling required for data centers in TIA-942. Quickly replacing CAT 5e.
CAT 6E	Up to 500 MHz	Field-tested to 500 MHz. Supports 10 Gigabit Ethernet (10GBASE-T). May be either shielded (STP, ScTP, S/FTP) or unshielded (UTP). Standard published in Feb. 2008. The minimum requirement for Data Centers in the ISO Data Center standard.
CAT 7 (ISO Class F)	600 MHz, 1.2 GHz in pairs with Siemon connector	Full-motion video, Teleradiology, Government and manufacturing environments. Fully Shielded (S/FTP) system using non-RJ45 connectors but backwards compatible with hybrid cords. Standard published in 2002. Until Feb. 2008, the only standard to support 10GBASE-T for a full 100m.

CAT 7A/Class FA and Category 6A/Class EA specifications were published in February, 2008.

CE

A mandatory conformity mark on many products placed on the single market in the European Economic Area (EEA). The CE marking certifies that a product has met EU consumer safety, health or environmental requirements.

Certificate

A public key certificate - an electronic document which incorporates a digital signature to bind together a public key with an identity (information such as the name of a person or an organization, their address, etc.). The certificate can be used to verify that a public key belongs to an individual without exchanging secret keys. The signatures on a certificate are of a certificate authority (CA) and attest that the identity information and the public key belong together.

CHAP

(Point-to-Point Protocol authentication via Challenge/Handshake Authentication Protocol).

CHAP is used to periodically verify the identity of the peer using a 3-way handshake. CHAP provides protection against playback attack through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges. CHAP authentication depends on a "secret" known only to the authenticator and that peer. The secret is not sent over the link. This method is most likely used where the same secret is easily accessed from both ends of the link.

The CHAP process for connecting to a system includes:

1. After a link is made, the server sends a 'challenge' message to the connection requestor.
2. The requestor responds with a value obtained by using a one-way hash function.
3. The server checks the response by comparing it its own calculation of the expected hash value.
4. If the values match, the authentication is acknowledged; otherwise the connection is typically terminated.

At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP. Compared to PAP, CHAP has a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string). IETF RFC 1334 defines both CHAP and PAP.

CFM

The IEEE 802.1ag standard for Connectivity Fault Management (CFM) divides a network into maintenance domains in the form of hierarchy levels. The levels are allocated to users, service providers, and operators. CFM assigns Maintenance End Points (MEPs) to the edges of each domain, and Maintenance Intermediate Points (MIPs) to ports within domains. This helps define the relationships between all entities from a maintenance perspective, letting each entity monitor the layers under its responsibility and more easily localize problems.

CIR

(Committed Information Rate) The average rate up to which service frames are delivered according to performance objectives (e.g., delay, loss, etc.) associated with the service; the CIR value is always less than or equal to the UNI speed.

Circuit ID

A company-specific identifier assigned to a data or voice network between two locations. This circuit is then leased to a customer by that ID. If a subscriber has a problem with the circuit, the subscriber contacts the telecommunications provider to provide this circuit id for action on the designated circuit.

Several Circuit ID formats exist (Telephone Number Format, Serial Number Format, Carrier Facility Format and Message Trunk Format). Telecom Circuit ID formats (LEC circuit IDs) provide service codes for DSL, HDSL, ADSL, Digital data, SST Network Trunk, Switched Access, E1, Switched Access, Basic Data and Voice, LAN, SONET, Ethernet, Video, Voice, Digital Transmission, and others. [Contrast "Device Description"](#).

CLI

(Command-Line Interface) A mechanism for interacting with a computer operating system or software by typing commands to perform specific tasks. The CLI allows users to set up switch configurations by using simple command phrases through a console / telnet session.

Communication

In IPv6, any packet exchange among nodes that requires that the address of each node used in the exchange remain the same for the duration of the packet exchange. Examples are a TCP connection or a UDP request- response.

Community

Two levels of ION system access privileges are password protected:

- Read access (Read ONLY) - a Community Name with a particular set of privileges to monitor the network without the right to change any of its configuration.
- Read/Write (Read and make changes) - a Community Name with an extended set of privileges to monitor the network as well as actively change any of its configuration.

Community string

A text string used to authenticate messages between a management station and an SNMP v1/v2c engine.

A Community string is used as the name of the community; it acts as a password by controlling access to the SNMP community.

CoS

(Class of Service) a 3-bit field within an Ethernet frame header when using 802.1Q tagging. The field specifies a priority value from 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines

to differentiate traffic. While CoS operates only on Ethernet at the data link layer, other QoS mechanisms (such as DiffServ) operate at the network layer and higher. Others operate on other physical layer. See also ToS and QoS. In MEF terms, CoS is a set of Service Frames that have a commitment from the Service Provider to receive a particular level of performance. See also "QoS".

QoS provides a 'guaranteed' level of service, while CoS provides no explicit guarantee, just a higher level of service at each higher priority.

CoS Queues

Class of Service allows traffic to be directed into different priority levels or "internal queues" in the switch on a particular network transaction. When network traffic congestion occurs, the data assigned to a higher queue will get through first. (Standard: IEEE 802.1p.)

CSA

(Canadian Standards Association) A not-for-profit membership-based association serving business, industry, government and consumers in Canada and the global marketplace.

C-Tag

(Customer Tag) When the 0x8100 tag is added twice, the outer tag is called the Provider tag and the inner one is called the Customer IEEE 802.1Q tag. The inner VLAN tag is referred to as the customer VLAN tag (C-Tag) because the customer assigns it. Contrast S-Tag. Before the standardization, some vendors used 0x8100 and 0x9100 for outer Provider tagging. The 0x88A8 tag was adapted by the IEEE later.

The C-Tag is one of several ION system VLAN tagging options. The ION system can provide QinQ service where a frame may contain one or more tags by adding or stripping provider tags on a per-port basis. There are different cases for VLAN service translation options that are possible in the ION system for dealing with C-Tags and S-Tags. Contrast with S-Tag. See also Provider tag.

DAD

(Duplicate Address Detection) - part of the NDP protocol that lets nodes check if an address is already in use.

daemon

A program which services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.

dBm

(DeciBels below 1 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.

DCE

(Data Circuit-terminating Equipment) A device that sits between the data terminal equipment (DTE) and a data transmission circuit. Also called data communications equipment and data carrier equipment.

Deprecated address

In IPv6, an address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection).

DES

(Data Encryption Standard) A privacy protocol; one of two encryption algorithms used for ION system data privacy. DES is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official FIPS standard for the US in 1976 and has since enjoyed widespread use internationally. DES is based on a symmetric-key algorithm that uses a 56-bit key. Despite criticism, DES was approved as a federal standard in 1976, and published in 1977 as FIPS PUB 46, authorized for use on all unclassified data. DES was confirmed as the standard in 1983, 1988 (revised as FIPS-46-1), 1993 (FIPS-46-2), and in 1999 (FIPS-46-3, as "Triple DES"). See also "AES".

DHCP

(Dynamic Host Configuration Protocol) A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

DHCP lets a network administrator supervise and distribute IP addresses from a central point, and automatically sends a new address when a computer is plugged into a different place in the network. (Standard: RFC 2131.)

DiffDerv

In terms of traffic classification, DiffDerv lets a network perform differentiated service treatments.

Discovering / Discovery

Discovery allows a Service OAM capable NID to learn sufficient information (e.g. MAC addresses etc.) regarding other SOAM capable NIDs so that OAM frames can be exchanged with those discovered NIDs.

Down MEP

A MEP residing in a Bridge that receives CFM PDUs from, and transmits them towards, the direction of the LAN. See also Up MEP.

DMI

(Diagnostic Monitoring Interface) Adds parametric monitoring to SFP devices.

DMM / DMR

(Delay Measurement Message / Delay Measurement Response) DMM/DMR is used to measure single-ended (aka, two-way) Frame Delay (FD) and Frame Delay Variation (FDV, aka, Jitter).

DNS

(Domain Name System) An internet service that translates domain names into IP addresses. DNS allows you to use friendly names, such as www.transition.com, to easily locate computers and other resources on a TCP/IP-based network.

DNS is a standard technology for managing the names of Web sites and other Internet domains. DNS lets you type a name into your web browser (e.g., transition.com/TransitionNetworks/Learning/Seminar) to automatically find that address on the Internet.

DNS server

(Domain Name System server) any computer registered to join the Domain Name System. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts.

DoSAP

(Domain Service Access Point) A member of a set of SAPs at which a Maintenance Domain is capable of offering connectivity to systems outside the Maintenance Domain. Each DoSAP provides access to an instance either of the EISS or of the ISS.

Dr. Watson

Dr. Watson for Windows is a program error debugger. The information obtained and logged by Dr. Watson is used by technical support groups to diagnose a program error for a computer running Windows. A text file (Drwtsn32.log) is created whenever an error is detected, and can be delivered to support personnel by the method they prefer. There is an option to create a crash dump file, which is a binary file that a programmer can load into a debugger.

DSCP

DiffServ (Differentiated Services) Prioritization provides the ability to prioritize traffic internally based on the DSCP field in the IP header of a packet. (AKA, DiffServ Modification DSCP / DiffServ. Standard: RFC 3290.)

DST

(Daylight Savings Time) Advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring (March) and are adjusted backward in autumn (November).

DTE

(Data Terminal Equipment) The RS-232C interface that a computer uses to exchange data with a modem or other serial device. An end instrument that converts user information into signals or reconverts received signals (e.g., a terminal).

dual-stack name server

A name server that is configured to run both IPv4 and IPv6 protocols. IETF RFC 3901 describes a means to maintain name space continuity using administrative policies, for operating DNS where queries and responses are carried in a mixed environment of IPv4 and IPv6 networks.

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.

Dynamic IP addressing

"Dynamic" means moving or changing. A dynamic IP address is an address that is used for the current session only; when the session is terminated, the IP address is returned to the list of available addresses.

If a network uses dynamic addressing, it means that when a network interface asks to join the network, it is randomly allocated an IP address from a pool of available addresses within that network. Thus, under dynamic addressing, a computer may possess over time (e.g. across reboots) a variety of different IP addresses. Dynamic addressing is often used in scenarios where end-user computers are intermittently connected to the network.

The DHCP protocol provides a means to dynamically allocate IP addresses to computers on a network. A system administrator assigns a range of IP addresses to a DHCP server, and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server, which can grant the request. The request and grant process uses a lease concept with a controllable time period.

EEA

(European Economic Area) Established on 1 January 1994 following an agreement between member states of the European Free Trade Association, the European Community, and all member states of the European Union (EU). It allows these EFTA countries to participate in the European single market without joining the EU.

Egress Frame

A service frame sent from the Service Provider network to the CE. Contrast Ingress Frame.

Egress rules

Egress rules determine which frames can be transmitted out of a port, based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether the frames will be transmitted as tagged or untagged frames.

EIR

(Excess Information Rate) The max rate over the CIR. The EIR specifies the average rate (greater than or equal to the CIR) up to which service frames are admitted into the Service Provider network. EIR frames are considered EIR-conformant. EIR frames are delivered with no performance guarantees, and are not CIR-conformant (however, service frames that are not EIR-conformant are discarded).

ELMI Protocols

Enhanced Link Management Interface (ELMI or E-LMI) is the Ethernet Local Management Interface, based on MEF 16. In the ION system, ELMI Protocol disposition (pass or discard) is defined in the L2CP Disposition section of the device port's MAIN tab and at the CLI with the **set l2cp state** command.

ESD

(Electrostatic Discharge) A sudden and momentary electric current that flows between two objects.

EtherType

One of two types of protocol identifier parameters that can occur in Ethernet frames after the initial MAC-48 destination and source identifiers. Ethertypes are 16-bit identifiers appearing as the initial two octets after the MAC destination and source (or after a tag).

Implies use of the IEEE Assigned EtherType Field with IEEE Std 802.3, 1998 Edition Local and Metropolitan Area Networks. The EtherType Field provides a context for interpretation of the data field of the frame (protocol identification). Several well-known protocols already have an EtherType Field.

The IEEE 802.3, 1998 Length/EtherType Field, originally known as EtherType, is a two-octet field. When the value of this field is greater than or equal to 1536 decimal (0600 hexadecimal) the EtherType Field indicates the nature of the MAC client protocol (EtherType interpretation). The length and EtherType interpretations of this field are mutually exclusive.

The ION system **Ether Type** parameters are set at the ION device port's **ADVANCED** tab in the **VLAN Tag Management** section.

ETH-CC

(Ethernet Continuity Check) – the function used for proactive OAM. It detects loss of continuity (LOC) between any pair of MEPs in a MEG. ETH-CC also allows detection of unintended connectivity between two MEGs (Mismerge), unintended connectivity within the MEG with an unexpected MEP (Unexpected MEP), and other defect conditions (e.g., Unexpected MEG level, Unexpected period, etc.). ETH-CC is used for fault management, performance monitoring, or protection switching.

A MEP must always report reception of frames with unexpected ETH-CC information. ETH-CC transmission may be enabled or disabled in a MEG. When ETH-CC transmission is enabled in a MEG, all MEPs are enabled to periodically transmit frames with ETH-CC information to all other MEPs in the MEG. The ETH-CC transmission period is the same for all MEPs in the MEG. When a MEP is enabled to generate frames with ETH-CC information, it is also enabled to receive frames with ETH-CC information from its peer MEPs in the MEG.

When ETH-CC transmission is disabled in a MEG, all MEPs are unable to transmit frames with ETH-CC information. A MIP is transparent to the ETH-CC information and thus does not require any configuration information to support ETH-CC. When a MEP does not receive ETH-CC information from a peer MEP, in the list of peer MEPs, within an interval of 3.5 times the ETH-CC transmission period, it detects loss of continuity to that peer MEP. The interval is equivalent to a loss of 3 consecutive frames carrying ETH-CC information from the peer MEP. The OAM PDU used for ETH-CC information is CCM. Frames that carry the CCM PDU are called CCM frames.

ETH-LB

(Ethernet Loopback) - the function used to verify connectivity of a MEP with a MIP or with peer MEP(s). There are two ETH-LB types: Unicast ETH-LB and Multicast ETH-LB.

- Unicast ETH-LB is an on-demand OAM function that can be used to 1) verify bidirectional connectivity of a MEP with a MIP or a peer MEP; or 2) perform a bidirectional in-service or out-of-service diagnostics test between a pair of peer MEPs (bandwidth throughput, detecting bit errors, etc.). Unicast ETH-LB can be used to perform only one of the two applications at any time.

Specific configuration information is required by a MEP to support Unicast ETH-LB. Specific configuration information is required by a MIP to support Unicast ETH-LB

- Multicast ETH-LB is an on-demand OAM function used to verify the bidirectional connectivity of a MEP with its peer MEPs. When a Multicast ETH-LB function is invoked on a MEP, the MEP returns to the initiator of Multicast ETH-LB a list of its peer MEPs with whom the bidirectional connectivity is detected. When Multicast ETH-LB is invoked on a MEP, a Multicast frame with ETH-LB request information is sent from a MEP to other peer MEPs in the same MEG. The MEP expects to receive Unicast frames with ETH-LB reply information from its peer MEPs within a specified period of time. Upon reception of a Multicast frame with ETH-LB request information, the receiving MEPs validate the Multicast frame with ETH-LB request information and transmit a Unicast frame with ETH-LB reply information after a randomized delay in the range of 0 to 1 seconds.

ETH-LT

(Ethernet Link Trace) - an on-demand OAM function that can be used 1) to retrieve adjacency relationship between a MEP and a remote MEP or MIP, and 2) for Fault localization – when a fault (e.g., a link and/or a device failure) occurs, the sequence of MIPs and/or MEP will likely differ from the expected sequence. These differences provide information about the fault location.

ETH-LT request information is initiated in a MEP on an on-demand basis. After transmitting a frame with ETH-LT request information, the MEP expects to receive frames with ETH-LT reply information within a specified period of time. Network elements containing MIPs or MEPs and receiving the frame with ETH-LT request information respond selectively with frames containing ETH-LT reply information.

EUI-64

The 64-bit Extended Unique Identifier (EUI-64) in IPv6.

Event log

Records events such as port link down, configuration changes, etc. in a database.

FCC

(Federal Communications Commission) An independent United States government agency established by the Communications Act of 1934 that is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

FDB

The Forwarding Database for an ION system VLAN, identified by a unique FDB ID and kept for a specified aging time.

FDX

(Full Duplex) Communication in both directions simultaneously.

FEF

(Far End Fault) A troubleshooting feature usually used in conjunction with Link Pass Through to notify both end devices of a loss of link.

FID

(Forwarding Information Database) The address database in the switch; may be the same as the V-LAN ID (VID) or different, depending on the device.

Filtering Database

When a bridge receives data, it determines to which VLAN the data belongs either by implicit or explicit tagging. In explicit tagging, a tag header is added to the data. The bridge also keeps track of VLAN members in a filtering database which it uses to determine where the data is to be sent. Membership information for a VLAN is stored in a filtering database. The filtering database consists of two types of entries:

- *Static Entries:* Static information is added, modified, and deleted by management only. Entries are not automatically removed after some time (ageing), but must be explicitly removed by management.
- *Dynamic Entries:* Dynamic entries are “learned” by the bridge and cannot be created or updated by management. The learning process observes the port from which a frame with a given source addresses and VLAN ID (VID) is received, and updates the filtering database. The entry is updated only if a) this port allows learning, b) the source address is a workstation address and not a group address, and c) there is space available in the database.

Entries are removed from the filtering database by the aging process where, after a certain amount of time specified by management, entries allow automatic reconfiguration of the filtering database if the topology of the network changes.

Firmware

Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Flow Control

Prevents congestion and overloading when a sending port is transmitting more data than a receiving port can receive. (Standard: IEEE 802.3X.)

FNG alarm

A Fault Notification Generation (FNG) alarm is generated whenever a CCM (Continuity Check Message) is lost.

FNG state

A MEP Fault Notification Generation (FNG) status, either **FNG Reset**, **FNG Defect**, **FNG Report Defect**, **FNG Defect Reported**, or **FNG Defect Clearing**.

Frame

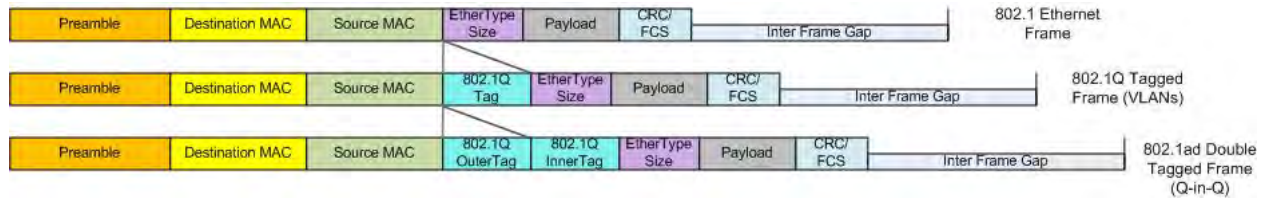
A unit of data that is transmitted between network points on an Ethernet network. An Ethernet frame has explicit minimum and maximum lengths and a set of required data that must appear within it. Each frame on an IEEE 802 LAN MAC conveys a protocol data unit (PDU) between MAC Service users. There are three types of frame; untagged, VLAN-tagged, and priority-tagged.

Frame Format

In Ethernet, a frame is a way of arranging sections of data for transfer over a computer network. The frame is a key element of an Ethernet system. A typical Ethernet frame is made up of three elements: a pair of addresses, the data itself, and an error checking field.

Frame Formats for 802.1, 802.1Q and 802.1ad are illustrated below.

Glossary



Frame Loss Ratio

Frame loss ratio is the number of service frames not delivered divided by the total number of service frames during time interval T, where the number of service frames not delivered is the difference between the number of service frames arriving at the ingress ETH flow point and the number of service frames delivered at the egress ETH flow point in a point-to-point ETH connection.

Frame Delay

Frame delay is the round-trip delay for a frame, defined as the time elapsed from the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the loopbacked frame by the same source node, when the loopback is performed at the frame's destination node.

FTP

(File Transfer Protocol) A standard network protocol used to exchange and manipulate files over a TCP/IP based network, such as the Internet. See also TFTP.

GBIC

(Gigabit Interface Converter) A transceiver that converts serial electrical signals to serial optical signals and vice versa. In networking, a GBIC is used to interface a fiber optic system with an Ethernet system, such as Fibre Channel and Gigabit Ethernet.

Gbps

(Gigabits Per Second) Data transfer speeds as measured in gigabits.

Global address

In IPv6, an address with unlimited scope.

Group

A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive.

Group Views

The ION system supports three SNMP v3 Views: notifview, readview, and writeview.

GUI

(Graphical User Interface) A type of user interface item that allows people to interact with programs in more ways than typing. A GUI offers graphical icons, and visual indicators, as opposed to text-based interfaces, typed command labels or text navigation to fully represent the information and actions available to a user. The actions are usually performed through direct manipulation of the graphical elements.

Host

In IPv6, any node that is not a router.

HSCP

(High-Security Console Password)

HTML

(HyperText Markup Language) The predominant markup language for web pages. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists etc as well as for links, quotes, and other items.

HTTPS

(Hypertext Transfer Protocol Secure) A combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server.

ICMP

(Internet Control Message Protocol) Part of the internet protocol suite that is used by networked computers to send error, control and informational messages indicating, for instance, that a requested service is not available or that a host or router could not be reached.

ICMPv6

(Internet Control Message Protocol version 6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6) defined in RFC 4443.[1] ICMPv6 is an integral part of IPv6 and performs error reporting, diagnostic functions (e.g., ping), and a framework for extensions to implement future changes. Several extensions are published to define new ICMPv6 message types and options for existing ICMPv6 message types. The Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 that replaces and enhances functions of ARP. Secure Neighbor Discovery Protocol (SEND) is an extension of NDP with extra security. Multicast Router Discovery (MRD) allows discovery of multicast routers.

IEC

(International Electrotechnical Commission) The world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

IEEE

(Institute of Electrical and Electronics Engineers) An international non-profit, professional organization for the advancement of technology related to electricity.

IGMP

(Internet Group Management Protocol) A communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

IGMP snooping

Internet Group Multicast Protocol snooping allows a switch to "listen in" on the IGMP conversation between hosts and routers. Based on the query and reports being passed through the switch, a forwarding database for multicast is created.

Informs

One of two types of SNMP notifications that can be sent. See also "traps". An SNMP notification can be sent as a 'trap' or an 'inform'. Traps are less reliable since the trap receiver does not send acknowledgments when it receives traps. The trap sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, making informs more likely to reach their intended destination. However, informs use more agent and network resources. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received, otherwise the request times out. Also, a trap is sent only once, while an inform may be retried several times.

The ION SNMPv3 feature provides users SNMP v1/v2c/v3 access to manage the ION system through the IONMM. Any ION defined traps can be sent to the configured trap servers in v1 or v2c or v3 format through the IONMM. If the IONMM sends out v2c/v3 informs, the trap servers will send responses.

Ingress

The direction from the CE into the Service Provider network. Contrast Egress.

Ingress rules

A means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame.

Interface

In IPv6, a node's attachment to a link.

Interface identifier - in IPv6, a link-dependent identifier for an interface that is (at least) unique per link. Stateless address autoconfiguration combines an interface identifier with a prefix to form an address. In address autoconfiguration, an interface identifier is a bit string of known length. The exact length of an interface identifier and the way it is created is defined in a separate link-type specific document that covers issues related to the transmission of IP over a particular link type. In many cases, the identifier will be the same as the interface's link-layer address.

Invalid address

In IPv6, an address that is not assigned to any interface. A valid address becomes invalid when its valid lifetime expires. Invalid addresses should not appear as the destination or source address of a packet. In the former case, the internet routing system will be unable to deliver the packet, in the later case the recipient of the packet will be unable to respond to it.

IP

(Internet Protocol) One of the core protocols of the Internet Protocol Suite. IP is one of the two original components of the suite (the other being TCP), so the entire suite is commonly referred to as TCP/IP. IP is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IPv6

(Internet Protocol version 6) - The Version 6 IP protocol for Next Generation (IPng).

IPv6 Header

The IPv6 Header format is shown below - from RFC 2460 - IPv6 Specification (Dec. 1998):

The IPv6 header fields are:

- Version: The 4-bit Internet Protocol version number (6).
- Traffic Class: An 8-bit traffic class field.
- Flow Label: A 20-bit flow label.
- Payload Length: the 16-bit unsigned integer. The Length of the IPv6 payload (i.e., the rest of the packet following this IPv6 header, in octets. Note that any extension headers present are considered part of the payload (i.e., included in the length count).
- Next Header: An 8-bit selector that identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.
- Hop Limit: An 8-bit unsigned integer decremented by 1 by each node that forwards the packet. The packet is discarded if the Hop Limit is decremented to zero.
- Source Address: The 128-bit address of the originator of the packet.
- Destination Address: The 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

A full IPv6 implementation also includes these six extension headers: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, and Encapsulating Security Payload headers. Unlike IPv4, IPv6 nodes are not required to enforce a maximum packet lifetime, which is why the IPv4 "Time to Live" field was renamed "Hop Limit" in IPv6.

IPC

(Interprocess Communications) The exchange of data between one program and another either within the same computer or over a network. It implies a protocol that guarantees a response to a request.

IP Stacking

The capability to stack multiple switches together and manage them under one IP address.

IPToS

(IP Type of Service) Prioritization - The ability to prioritize traffic internally based on the IPToS field in the IP header of a packet.

IPv4

(Internet Protocol version 4) the primary Internet protocol used today. An IPv4 address has 32 bits.

ITU

ITU is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services. For nearly 145 years, ITU has coordinated the shared global use of the radio spectrum, worked to improve telecommunication infrastructure in the developing world, and established worldwide standards that foster seamless interconnection of a vast range of communications systems. See <http://www.itu.int/net/about/itu-t.aspx>.

ITU-T OAM Performance Monitoring

OAM functions for performance monitoring allow measurement of different performance parameters. The performance parameters are defined for point-to-point ETH connections. This covers Frame Loss Ratio and Frame Delay parameters. An additional performance parameter, Throughput, is identified per RFC 2544.

Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size, which is 1518 bytes (1522 if VLAN-tagged). Though this is not a standard, more vendors are adding support for jumbo frames. An initiative to increase the maximum size of the MAC Client Data field from 1500-bytes to 9000-bytes. The initiative was not adopted by the IEEE 802.3 Working Group, but it was endorsed by a number of other companies. Larger frames would provide a more efficient use of the network bandwidth while reducing the number of frames that have to be processed. The Jumbo Frame proposal restricts the use of Jumbo Frames to full-duplex Ethernet links, and defines a "link negotiation" protocol that allows a station to determine if the station on the other end of the segment is capable of supporting Jumbo Frames.

Kbps

(Kilobits Per Second) Data transfer speeds as measured in kilobits.

L2/L3/L4 Access Control List Port Based ACLs

ACLs allow administrators to create permit and deny lists based on various traffic characteristics such as Source MAC, Destination MAC, Source IP, Destination IP, and UDP/TCP ports.

L2CP

(Layer 2 Control Protocol) – a network control protocol standardized by the IETF, IEEE and MEF.

The IETF, in an Internet-Draft, defined a framework for a Layer 2 Control Protocol (L2CP) mechanism between a service-oriented layer 3 edge device and a layer 2 Access Node in a multi-service architecture. This mechanism allows QoS-related, service-related, and subscriber-related operations.

The MEF and IEEE 802.1 terms are related as follows:

<u>MEF Term</u>	<u>IEEE 802.1 Term</u>
Peer	Participate
Tunnel	Forward (relay)
Discard	Not forward, Not participate

LAN

(Local Area Network) A group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building).

L2CP Service Frame

A Service Frame that is used for Layer 2 control (e.g., Spanning Tree Protocol).

L2CP Service Frame Delivery

The process by which a Layer 2 Control Protocol Service Frame is passed through the Service Provider network switches without being processed by those switches and delivered to the proper UNI(s).

L2CP Tunneling

The process by which a Layer 2 Control protocol Service Frame is passed through the Service Provider network without being processed and delivered unchanged to the proper UNI(s).

LA

(Link Aggregation) Allows one or more links to be aggregated together to form a Link Aggregation Group, so a MAC Client can treat the Link Aggregation Group as if it were a single link. LA specifies the establishment of data terminal equipment (DTE) to DTE logical links, consisting of n parallel instances of

full duplex, point-to-point links operating at the same data rate. The IEEE standard defines the MAC independent Link Aggregation capability, and general information relevant to specific MAC types that support Link Aggregation. Link Aggregation allows full duplex point-to-point links that have a higher aggregate bandwidth than the individual links that form the aggregation. This provides improved utilization of available links in a bridged LAN environment, plus improved resilience in handling individual link failures. Link aggregation, at times referred to as 'trunking', 'muxing' or 'bonding', increases the capacity and availability of a channel between devices using existing hardware.

LACP

(Link Aggregation Control Protocol) A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.

LACP lets you bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. (Standard: IEEE 802.3ad.)

LAN

(Local Area Network) A group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building).

Last Gasp

This feature enables the device to store a small amount of power to enable it to send out an SNMP trap to alert the management console in the event of a power failure. The notification of an impending power loss before it happens allows for quicker resolution of the power loss.

Layer 2 Switch

A network device that functions as multi-port switch.

Layer 3 Switch

A network device that functions as a router and a multi-port switch.

Layer 4 Switch

A switch that makes forwarding decisions taking Layer 4 protocol information into account.

LBM

(Loopback Message) A unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR.

LBR

(Loopback Reply) A unicast CFM PDU transmitted by an MP to a MEP, in response to an LBM received from that MEP.

LED

(Light Emitting Diode) An electronic light source.

Link

In IPv6, a communication facility or medium over which nodes can communicate at the link layer (i.e., the layer immediately below IPv6). Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.

Link MTU

The IPv6 Maximum Transmission Unit - the maximum packet size in octets that can be conveyed over a link.

Link-layer address

In IPv6, a link-layer identifier for an interface. Examples include IEEE 802 addresses for Ethernet links and E.164 addresses for ISDN links.

Link-local address

One of IPv6 addresses for local link usage. In IPv6, an address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address.

In IPv6, the two types of local-use unicast addresses defined are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Reference IETF RFC 2373. See also "Site-Local unicast address".

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present. Routers must not forward any packets with link-local source or destination addresses to other links. All interfaces are required to have at least one link-local unicast address.

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. Globally-connected sites typically use the same subnet IDs for site-local and global prefixes.

Routers must not forward any packets with site-local source or destination addresses outside of the site.

Little Endian

Bit ordering within a byte where bits are sent serially starting with the LSB (least significant byte) and ending with the MSB (most significant byte). Ethernet uses Little Endian bit ordering. Contrast "Big Endian".

LLDP

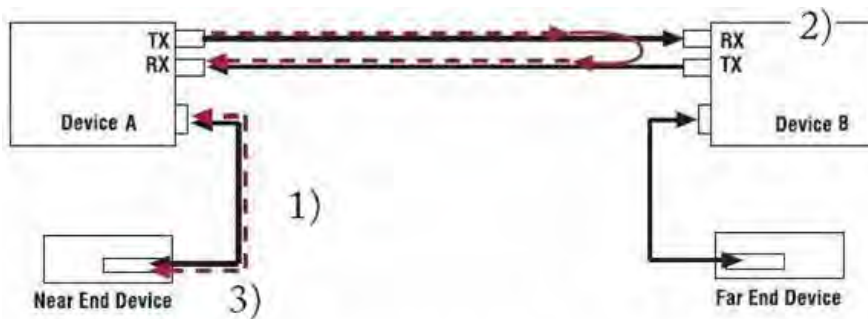
(Link Layer Discovery Protocol) A standard method for Ethernet Network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

LOAM

(Link OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.3ah OAM. The major features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, and Remote Loopback. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to SOAM.

Loopback (LB)

The Loopback feature puts a device in a special mode that enables the device to loop back the signal from the RX port to the TX port on either media for testing and troubleshooting purposes. Test signals can then be inserted into the link and looped back as received by a device to test a particular segment of the link (i.e. copper or fiber). Loopback can be either local or remote depending on the location of the converter in the link.



- 1) Test signal inserted by near end device.
- 2) Device B set to remote loopback on Fiber.
- 3) Returned test signal received by near end device.

LPT

(Link Pass Through) A troubleshooting feature that allows a device to monitor both the fiber and copper RX ports for loss of signal. In the event of a loss of RX signal on one media port, the device will automatically disable the TX signal of the other media port, thus “passing through” the link loss.

LTM

(Linktrace Message) A CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR.

LTR

(Linktrace Reply) A unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP.

MA

(Maintenance Association) A set of MEPs, each configured with the same MAID and MD Level, established to verify the integrity of a single service instance. An MA can also be thought of as a full mesh of Maintenance Entities among a set of MEPs so configured.

MAC

(Media Access Control) An address that is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN.

MAC-based Security

the ability to lock the learning mechanism down on a port. This means that no further MACs will be learned on those ports. (AKA, MAC Lockdown.)

MAC Table Size

the location where switches store learned addresses. The size of the MAC table determines how many unicast streams the switch can support without flooding. (AKA, FDB (Forwarding Data Base) table, CAM table, MAC.)

Mbps

(Megabits per second) Data transfer speed measured in thousands of bits per second.

MD

(Maintenance Domain) The network or the part of the network for which faults in connectivity can be managed. The boundary of a Maintenance Domain is defined by a set of DoSAPs, each of which can become a point of connectivity to a service instance.

MD5

(Message-Digest algorithm 5) An authentication protocol; one of two cryptography methods used for ION system user authentication. MD5 is a widely used cryptographic hash function with a 128-bit hash value. Specified in RFC 1321, MD5 is used in a wide range of security applications, and is also commonly used to check file integrity. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. MD5 was designed by Ron Rivest in 1991 to replace the earlier hash function MD4. See also “SHA”.

MDI

(Medium Dependent Interface) A type of Ethernet port connection using twisted pair cabling. The MDI is the component of the media attachment unit (**Error! Reference source not found.**) that provides the physical and electrical connection to the cabling medium. MDI ports connect to MDIX ports via straight-through twisted pair cabling; both MDI-to-MDI and MDIX-to-MDIX connections use crossover twisted pair cabling. See also MDIX.

The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX). The x323x device's *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection.

MDIX

(MDI Crossover) A version of MDI that enables connection between like devices. The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX).

The x323x device's *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection. See also MDI.

ME

(Maintenance Entity) An entity that requires management and is a relationship between two maintenance entity group (MEG) end points. MEs in Ethernet networks can nest but not overlap.

MEG

(Maintenance Entity Group) A ME Group (MEG) consists of the MEs that belong to the same service inside a common OAM domain.

MEG Level

The MEG Level is used to distinguish between OAM frames belonging to different nested MEs. MEs belonging to the same MEG share a common MEG Level. Eight MEG Levels have been identified for the purposes of Ethernet OAM.

When a Subscriber, Service Providers, and Network Operators share the MEG Levels space, allocation of MEG Levels can be negotiated between the various roles involved. A default allocation of MEG Levels is such that Service OAM frames for a Subscriber ME use MEG Level 7, 6 or 5; Service OAM frames for an EVC ME use MEG Level 3 or 4 as EVC ME belongs to a Service Provider OAM Domain; and Operator MEs use MEG Levels 2, 1, or 0. The MEG Levels used for UNI ME and NNI ME default to 0. Note that this default allocation of MEG Level space between Subscribers, Service Providers and Operators could change based on a mutual agreement between them.

MEP

(Maintenance end point) An inward-facing point at the edge of the domain that defines the boundary and confines CFM messages within these boundaries. Inward facing means that they communicate through

the relay function side, not the wire side (connected to the port).
See also MIP, Down MEP, and Up MEP.

A MEG End Point (MEP) is a provisioned OAM reference point which can initiate and terminate proactive OAM frames. A MEP can also initiate and react to diagnostic OAM frames. A Point-to-Point EVC has two MEPs, one on each end point of the ME. A Multipoint-to-Multipoint EVC of n UNIs has n MEPs, one on each end point.

MHF

(MIP Half Function) A MIP consists of two MIP Half Functions (MHFs) on a single Bridge Port, an Up MHF and a Down MHF. An MHF may maintain a MIP CCM Database, separate from the MEP CCM Databases.

MIB

(Management Information Base) The set of variables that are used to monitor and control a managed device. A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP.

MIBs 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”.

MIP

(Maintenance intermediate point) – A point internal to a domain, not at the boundary, that responds to CFM only when triggered by trace route and loopback messages. MIPs forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level, and forward all CFM frames at a higher level, regardless of whether they are received from the relay or wire side.

A MEG Intermediate Point (MIP) is a provisioned OAM reference point that can react to diagnostic OAM frames initiated by MEPs. A MIP does not initiate proactive or diagnostic OAM frames. See also MEP.

MLD

(Multicast Listener Discovery) - a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link (much as IGMP is used in IPv4). MLD is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3. The MLD protocol is described in RFC 3810 which was updated by RFC 4604. Windows Vista and later support MLDv2. FreeBSD 8 includes support for MLDv2. The Linux kernel has supported MLDv2 since v 2.5.68.

MSA

(Multi-Source Agreement) Common product specifications for pluggable fiber optic transceivers.

MSDU

(MAC Service Data Unit) The service data unit that is received from the logical link control (LLC) sub-layer which lies above the medium access control (MAC) sub-layer in a protocol stack (communications stack).

MT-RJ

(Mechanical Transfer-Registered Jack) A small form-factor fiber optic connector which resembles the RJ-45 connector used in Ethernet networks.

Multicast

One of the four forms of IP addressing, each with its own unique properties, a multicast address is associated with a group of interested receivers. Per RFC 3171, addresses 224.0.0.0 through 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4. The sender sends a single datagram (from the sender's unicast address) to the multicast address, and the intermediary routers take care of making copies and sending them to all receivers that have registered their interest in data from that sender. See also “Unicast”.

Multicast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

Multicast destination

A multicast IP address indicating all hosts and routers that are members of the corresponding group. See also Unicast destination.

Multi-point MEG

A MEG with more than one peer MEP. Contrast Point-to--point MEG.

MVRP

(Multiple VLAN Registration Protocol) a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches. It was defined in the IEEE 802.1ak amendment to 802.1Q-2005 standard. MVRP provides a method to dynamically share VLAN information and configure the needed VLANs within a layer 2 network.

NAS

(Network Access Server), a TN, Cisco, or other device, or any other client which makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets. Servers using RADIUS or TACACS protocol are often called NAS (Network Access Server), not to be confused with NAS (Network Attached Storage).

Native VLAN

The initial VLAN to which a switch port belonged before becoming a trunking port. If the trunking port becomes an access port, in most of the cases, that port will go back to its native VLAN. Traffic coming from the initial VLAN is untagged. To avoid VLAN hopping, do not to use this VLAN for other purposes.

NDP

(Neighbor Discovery Protocol) - a protocol in the Internet Protocol Suite used with IPv6. NDP operates in the Link Layer and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and DNS servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes per IETF RFC 4861.

Neighbors

In IPv6, nodes attached to the same link.

NIC

(Network Interface Card or Network Interface Controller) A computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using wireless communications or cables.

NID

(Network Interface Device) A device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In telecommunications, a NID is a device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In fiber-to-the-premises systems, the signal is transmitted to the customer premises using fiber optic technologies. In general terms, a NID may also be called a Network Interface Unit (NIU), Telephone Network Interface (TNI), Slide-in-card (SIC), or a slide-in-module.

NMS

(Network Management Station) A high-end workstation that, like the Managed Device, is also connected to the network. A station on the network that executes network management applications that monitor and control network elements such as hosts, gateways and terminal servers. See also "SNMP".

Node

In IPv6, a device that implements IPv6.

Non Intrusive test

Ability to troubleshoot a circuit while it is in use.

Notification

An SNMP trap or inform message. See also "traps" and "informs". SNMP notifications can be sent as traps or informs. Traps are less reliable since the receiver does not send an acknowledgment when it receives a trap (the sender cannot tell if the traps were received). However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again (making informs more likely to reach their intended destination). On the other hand, informs use more agent and network resources. While a trap is discarded as soon as it is sent, an inform request is held in memory until a either response is received or the request times out. Note also that traps are sent only once, while an inform may be resent several times. These inform retries increase traffic and contribute to a higher overhead on the network.

Notification host

An SNMP entity to which notifications (traps and informs) are to be sent.

Notifview

An SNMP v3 string of up to 64 characters that is the name of the view that enables you to specify a notify, inform, or trap. The default notifview is 'nothing' (i.e., the null OID). If a view is specified, any notifications in that view that are generated are sent to all users associated with the group (provided an SNMP server host configuration has been created for the user).

Notify view

A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group.

NTP

(Network Time Protocol) A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

OAM

(Operation, Administration and Maintenance) A group of network management functions that provide network fault indications, performance information, data, and diagnosis. Since Ethernet OAM functions are not designed to work completely over half-duplex interfaces, the value NonOperHalfDuplex is returned whenever Ethernet OAM is enabled ('Admin Status' is Enabled) but the interface is in half-duplex operation.

OAM Event

The following OAM event types are defined and logged in the ION system:

- Errored Symbol Event
- Errored Frame Period Event
- Errored Frame Event
- Errored Frame Seconds Event
- Link Fault
- Dying Gasp Event
- Critical Link Event

The first four are considered threshold crossing events, as they are generated when a metric exceeds a given value within a specified window. The other three are not threshold crossing events.

OAMPDU

(Ethernet OAM protocol data unit) The mechanism by which two directly connected Ethernet interfaces exchange OA information.

OID

(Object Identifier) Known as a “MIB object identifier” or “MIB variable” in the SNMP network management protocol, an OID is a number assigned to devices in a network for identification purposes. Each branch of the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an Object ID or OID.

In SNMP, an Object Identifier points to a particular parameter in the SNMP agent.

OSI

(Open Systems Interconnection) A standard description or reference model for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementors so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication.

OUI

(Organizationally Unique Identifier) the Ethernet Vendor Address component. Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits, which specify the interface serial number for that interface vendor. These high-order 3 octets (6 hex digits) are called the Organizationally Unique Identifier or OUI.

Packet

An IPv6 header plus payload.

PAP

(Point-to-Point Protocol authentication via Password Authentication Protocol) provides a simple method for the peer to establish its identity using a 2-way handshake. This is done only after initial link establishment. After link establishment is done, an ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated. PAP is not a strong authentication method. Passwords are sent over the circuit "in the clear", and there is no protection from playback or repeated trial and error attacks. The peer is in control of the frequency and timing of the attempts. PAP works like a standard login procedure; the remote system authenticates itself to the using a static user name and password combination. The password can be encrypted for additional security, but PAP is subject to numerous attacks. In particular, since the information is static, it is subject to password guessing as well as snooping. IETF RFC 1334 defines both PAP and CHAP.

Path MTU

The minimum IPv6 link MTU of all the links in a path between a source node and a destination node.

Pause

The Pause feature (data pacing) uses Pause frames for flow control on full duplex Ethernet connections. If a sending device is transmitting data faster than the receiving device can accept it, the receiving station will send a pause frame to halt the transmission of the sender for a specified period of time.

Pause frames are only used on full duplex Ethernet link segments defined by IEEE 802.3x that use MAC control frames to carry the pause commands. Only stations configured for full duplex operation can send pause frames.

PD

(Powered Device) Modules that are designed to extract power from a conventional twisted pair Category 5 Ethernet cable. All PD modules are IEEE802.3af compatible, with built-in signature chip, output voltage adjustment and class programming.

PDU

(Protocol Data Units) **1.** Information that is delivered as a unit among peer entities of a network and that may contain control information, address information or data. **2.** In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol control information and possibly user data of that layer.

PID

(Priority ID) on the x323x NID, the PID is configured at the ADVANCED tab in the “IEEE Priority Class” section; the selections are Remap 0 to: (PID) 0123.

(Process ID) in Netstat, the -o option displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).

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.

Point-to-point MEG

A MEG with only one peer MEP. Contrast Multi-point MEG.

PON

(Passive Optical Network) A point-to-multipoint fiber to the premises network architecture using unpowered optical splitters. Passive optical networks do not use electrically powered components to split the signal. Instead, the signal is distributed using beam splitters. Each splitter typically splits the signal from a single fiber into 16, 32, or 64 fibers (depending on the manufacturer).

ITU-T G.983 / 984 sub-types include APON (ATM Passive Optical Network), BPON (Broadband PON), IEEE 802.3ah EPON or GEPON (Ethernet PON), and GPON (Gigabit PON).

Port-Based Rate Limiting

The ability to regulate throughput on a per-port basis. (AKA, metering, Rate Limiting.)

Port Labeling

The ability to assign names to ports through the management interface.

Preferred address

In IPv6, an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface.

Preferred lifetime

In IPv6, the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.

Primary VID

The VID, among a list of VIDs associated with a service instance, on which all CFM PDUs generated by MPs except for forwarded LTMs are to be transmitted.

Priority-tagged frame

A tagged frame whose tag header carries priority information, but carries no VLAN identification information. Note: Priority tagged frames, which, by definition, carry no VLAN identification information, are treated the same as untagged frames for the purposes of VLAN identification. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. These frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).

Privacy

An encrypted state of the contents of an SNMP packet where they are prevented from being disclosed on a network. Encryption is performed with algorithms called DES or AES.

Protocol Endpoint

A communication point from which data may be sent or received. It represents communication points at various levels on an Open Systems Interconnection (OSI) structure.

Provider Tag

When the 0x8100 tag is added twice, the outer one is called the Provider tag and the inner one is called the Customer IEEE 802.1Q tag. Before the standardization, some vendors used 0x8100 and 0x9100 for outer Provider tagging. The 0x88A8 tag was adapted by the IEEE later. See also 'Customer tag'.

Provisioning

The process of preparing / equipping a network to allow it to provide one or more new services to its users (i.e., initial system setup). In telecom services, "provisioning" means "initiation" which includes changing the state of an existing service or capability. The provisioning process 1) monitors access rights and privileges to ensure the security of an enterprise's resources and user privacy, 2) ensures compliance and minimizes the vulnerability of systems to penetration and abuse, and 3) reduces the amount of custom configuration and the number of different configurations involved. Provisioning refers only to the setup or startup part of the service operation. In the ION system, the prov xxxx commands are typically used for provisioning the system.

PSE

(Power Sourcing Equipment) In power over Ethernet (PoE), equipment that serves as power injectors to provide output of 48V DC power over the twisted-pair cable plant to terminal units with PoE compliant devices known as powered devices (PDs). For devices not PoE-compliant, splitters inserted into the Ethernet cabling provide 12V or 6V DC output.

PVID

(Port VID) A default VID that is assigned to an access port to designate the virtual LAN segment to which this port is connected. The PVID places the port into the set of ports that are connected under the designated VLAN ID. Also, if a trunk port has not been configured with any VLAN memberships, the virtual switch's PVID becomes the default VLAN ID for the ports connection.

PVLAN

(Private Virtual-LAN) a non-standardized way of segmenting ports into separate groups. (Contrast "802.1Q VLAN".)

Q-in-Q (or "QinQ" or "Q in Q")

(IEEE 802.1Q in 802.1Q) an Ethernet networking standard for Ethernet frame formats (actually, 802.1Q-in-Q is an amendment to IEEE 802.1Q, and not a separate specification). It is also known simply as "QinQ" or "Q in Q". The original 802.1Q specification allows a single VLAN header to be inserted into an Ethernet frame. Q-in-Q allows multiple VLAN headers to be inserted into a single frame. In the

context of an Ethernet frame, a Q-in-Q frame has 2 VLAN 802.1Q headers (i.e., the Q-in-Q frame is 'double-tagged').

QoS

(Quality of Service) A mechanism to allow different classes of services to the customers. The QoS varies on a per customer basis, depending on their Service Level Agreement (SLA) they chose, and the kind of service they want. Customer traffic priorities are assigned based on their SLAs. QoS is standardized at both layer 2 and layer 3.

Service providers offering Layer 2 services can use the IEEE 802.1 Q/p standard for QoS. It allows a service provider to attach special tags, called VLAN IDs, to all incoming frames from a customer. With this, the service provider can have multiple customers using the same circuit, but still maintain separation between them. Each customer's traffic is identified by a different VLAN tag. The method also allows for the addition of a priority value to be associated to the VLAN tag. By using the priority field, service providers can offer various classes of service.

The two current Layer 3 (IP) QoS standards are IETF RFC-791, which defines the ToS, and RFC-2475, which defines DSCP. Both standards use the same field in the IP packet header to identify the level of service for the packet.

The various QoS parameters (either for Layer 2 or 3) are stored as part of the overhead in the transmitted frames. See also CoS and ToS.

RADIUS

(Remote Authentication Dial In User Service) Is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service. The RADIUS protocol does not transmit passwords in cleartext between the NAS and RADIUS server (not even with PAP protocol). Rather, a shared secret is used along with the MD5 hashing algorithm to obfuscate passwords.

RADIUS has been officially assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting by the IANA. However, prior to IANA allocation of ports 1812 and 1813, ports 1645 (authentication) and 1646 (accounting) were unofficial default ports assigned by many RADIUS Client/Server implementations at the time. Ports 1645 and 1646 are still used for backwards compatibility.

Read view

An SNMP View name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the Group.

A Readview is a string of up to 64 characters that is the name of the view that enables you only to view the contents of the agent. The default readview is assumed to be every object belonging to the Internet (1.3.6.1) OID space, unless you use the read option to override this state.

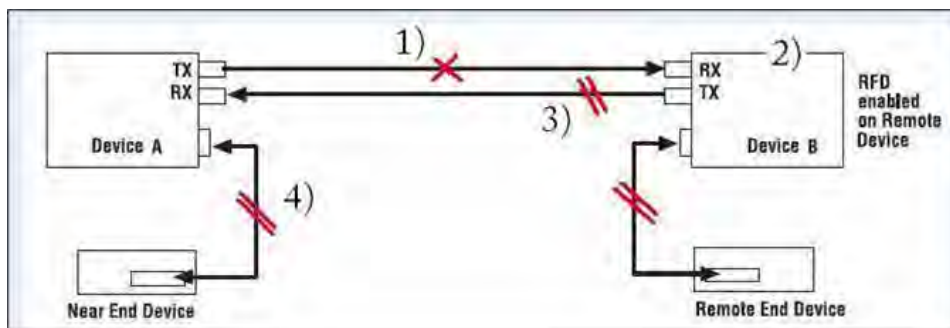
Redundancy

The Fiber Redundancy feature is designed to allow customer traffic and CPU-centric protocols to survive a fault on an uplink port by placing the traffic on a secondary backup port.

On the ION system, the Fiber Redundancy feature adds a form of automatic protection switching using a LOS mechanism that triggers the switch to the surviving line. The ION system uses 1:1 protection, with a modified form of bi-directional switching. TLPT and SLPT are operational with fiber redundancy enabled or disabled. The fault discovery method is LOS at the receiving interface for a set continuous period of time. Traffic rerouting occurs within a minimum period of time after the Primary Port is declared in the fault state. Traffic flow is restored within a minimum set period of time after a fault occurs.

RFD

(Remote Fault Detect) a troubleshooting feature found on Gigabit Ethernet copper-to-fiber media converters and NIDs. By enabling Remote Fault Detect on the remotely located device, the status of the fiber link will be monitored and any link failures will be reported back to the local converter. Should the remote converter lose its fiber RX signal, Remote Fault Detect will force the converter to shut down its fiber TX port. If Link Pass Through is enabled on both ends, then the copper ports will also be shut down to notify both end devices of the link failure. When you enable Remote Fault Detect on the remote device, the local end-device will be notified of remote fiber RX loss.



- 1) Device B loses Fiber link.
- 2) Device A disables its TX copper port via Link Pass Through (LPT) to alert the remote end device (Device A) of link loss.
- 3) Device B disables its Fiber TX port to alert Device A of link loss.
- 4) Device A disables its TX copper port via LPT to alert the Local end device of link loss.

RJ-45

The standard connector utilized on 4-pair (8-wire) UTP (Unshielded Twisted Pair) cable. The RJ-45 connector is the standard connector for Ethernet, T1, and modern digital telephone systems.

RMON

(Remote Network Monitoring) Software that supports the monitoring and protocol analysis of LAN. A part of SNMP, RMON is a network management protocol that gathers remote network information. (Standard: RFC 1271.)

Router

In IPv6, a node that forwards IPv6 packets not explicitly addressed to itself.

RS-232

(Recommended Standard 232) A standard for serial binary data signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

SAP

(Service Access Point) The point at which an Ethernet service is offered.

Security model

The security strategy used by the SNMP agent. Currently, ION supports three security models: SNMPv1 and SNMPv2c.

Self-signed certificate

An identity certificate that is signed by its own creator. That is, the person that created the certificate also signed off on its legitimacy. Such certificates are also called 'root certificates'.

Sender ID

Defined in RFC 4406, Sender ID is a Microsoft protocol derived from SPF (hence the identical syntax), which validates one of a message's address header fields defined by RFC 2822. Which header field it validates is selected according to the PRA (Purported Responsible Address) algorithm per RFC 4407. The PRA algorithm selects the header field with the e-mail address responsible for sending the message. Sender ID can be compared to other RFC 2822 layer protocols like DomainKeys IM (DKIM). The purpose of Sender ID is to help fight spoofing, one of the major deceptive practices used by

spammers. Sender ID works by verifying that each e-mail message did indeed originate from the Internet domain from which it was sent. See <http://www.ietf.org/rfc/rfc4406.txt> and <http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx> and 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). The x323x NIDs have SGMII support for use with 10/100/1000BASE-T copper SFPs. The x323x uses the **set ether phymode=SGMII** CLI command to select SGMII mode.

SHA

(Secure Hash Algorithm) An authentication protocol; one of two cryptography methods used for ION system user authentication. SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. FIPS standard. SHA-1 is part of many widely accepted security applications and protocols (e.g., TLS, SSL, PGP, SSH, S/MIME, and IPsec). See also “MD5”.

Site-Local address

An IPv6 address for a local site only. In IPv6, an address having scope that is limited to the local site.

In IPv6, the two types of local-use unicast addresses defined are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Reference IETF RFC 2373. See also “Link-Local unicast address”.

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present. Routers must not forward any packets with link-local source or destination addresses to other links. All interfaces are required to have at least one link-local unicast address.

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. Globally-connected sites typically use the same subnet IDs for site-local and global prefixes.

Routers must not forward any packets with site-local source or destination addresses outside of the site.

SLA

(Service Level Agreement) In general terms, a part of a service contract where the level of service is formally defined in terms of a contracted delivery time or performance. In Metro Ethernet, the contract between the Subscriber and Service Provider specifying the agreed to service level commitments and related business agreements.

SMAC

(Static MAC) A MAC address that is manually entered in the address table and must be manually removed. It can be a unicast or multicast address. It does not age and is retained when the switch restarts. You can add and remove static addresses and define the forwarding.

SMIv2

RFC 2580 ("Conformance Statements for SMIv2") defines the format for compliance statements which are used for describing requirements for agent implementations and capability statements which can be used to document the characteristics of particular implementations. The term "SMIv2" is somewhat ambiguous because users of the term intend it to have at least two different meanings. Sometimes the term is used to refer to the entire data definition language of RFCs 2578 - 2580 while other times it is used to refer to only the portion of the data definition language defined in RFC 2578. According to the IETF, this ambiguity is unfortunate but is rarely a significant problem in practice. The SMI is divided into three parts (module definitions, object definitions, and notification definitions).

SNMP

(Simple Network Management Protocol) A request-response protocol that defines network communication between a Managed Device and a Network Management Station (NMS). A set of protocols for managing complex IP networks. (Standard: RFC 1157.) A protocol for network management that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. Various SNMP versions exist.

SNMP engine

A copy of SNMP that can reside either on the local or remote device.

SNMP group

A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes defined by the group.

SNMP Message

A sequence representing the entire SNMP message, which consists of the SNMP version, Community String, and SNMP PDU.

SNMP SMI

(SNMP Structure of Management Information) a collection of managed objects, residing in a virtual information store. The SMI is divided into three parts: module definitions, object definitions, and, notification definitions. There are two types of SMI: SMIV1 and SMIV2. For additional information see IETF RFC 1155 v1 and RFC 2578 v2.

SNMP Version

An integer that identifies the version of SNMP (e.g., SNMPv1 = 0).

SNMP Community String

An Octet String that may contain a string used to add security to SNMP devices.

SNMP PDU

An SNMP PDU contains the body of an SNMP message. There are several types of PDUs (e.g., GetRequest, GetResponse, and SetRequest).

SNMP User

A person for which an SNMP management operation is performed. For informs, the user is the person on a remote SNMP engine who receives the informs.

SNMPv1

(SNMP version 1) the original Internet-standard Network Management Framework, as described in RFCs 1155, 1157, and 1212.

SNMPv2

(SNMP version 2) the SNMPv2 Framework as derived from the SNMPv1 Framework. It is described in STD 58, RFCs 2578, 2579, 2580, and RFCs 1905-1907. SNMPv2 has no message definition.

SNMPv2c

(Community-based SNMP version 2) an experimental SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to the SNMPv1 message format. The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

SNMPv2c (SNMPv2 with community-based security) SNMPv2c had the most support within the IETF but had no security and administration whereas both SNMPv2u and SNMPv2* had security but lacked IETF support consensus.

SNMPv3

(SNMP version 3) an extensible SNMP Framework which supplements the SNMPv2 Framework by supporting a new SNMP message format, Security for Messages, Access Control, and Remote configuration of SNMP parameters. The SNMPv3 protocol adds encryption and authentication mechanisms into the SNMP protocol for a secure management protocol where SNMP agents 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.)

SOAM

(Service OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.1AG. Ethernet CFM comprises three protocols that work together to help administrators debug Ethernet networks: continuity check, link trace and loopback protocols. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to LOAM.

Solicited-node multicast address

In IPv6, a multicast address to which Neighbor Solicitation messages are sent. The algorithm for computing the address is given in Discovery.

Stateless auto-configuration

A process to get IPv6 addresses from IPv6 standards.

SSH

(Secure Shell) A network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet. SSH is used to provide a secure Telnet session to the console/command line interface of a network device through an insecure environment. (AKA, Secured Telnet; Standard: SSH RFC 1034).

SSL

(Secure Socket Layer) A protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data; a public key known to everyone and a private or secret key known only to the recipient of the message. SSL is used to manage a network device via its web interface. (AKA, HTTPS, Standard: RFC 2818).

S-Tag

(Service VLAN Tag) The outer VLAN tag is referred to as the Service provider VLAN tag (S-Tag) and it uniquely identifies a given customer within the network of the service provider. It is possible for multiple customer VLANs to be tagged using the same outer or Service provider VLAN tag (S-Tag), thereby trunking multiple VLANs among customer sites.

The S-tag is one of several ION system VLAN tagging options. The ION system can provide QinQ service where a frame may contain one or more tags by adding or stripping provider tags on a per-port

basis. There are different cases for VLAN service translation options that are possible in the ION system for dealing with C-Tags and S-Tags. Contrast with “C-Tag”.

Static IP addressing

"Static" comes from the word stationary, meaning not moving. A static IP address means it never changes. A static IP address is an IP address permanently assigned to a workstation. If a network uses static addressing, it means that each network interface has an assigned IP address that it always uses whenever it is online. With static addressing, the computer has a well-defined IP address which it uses always and which no other computer ever uses.

Static MAC Entry

Static MAC entry support means that users can assign MAC addresses to ports manually that never age out.

STID

(Sensor Transaction Identifier) The STID is used for power supply / sensor / IONDCR configuration via the **set sensor stid** command to define notification, relation, severity, and value parameters. The **show power config** command displays the power supply sensors information. The STID is shown in the Web interface at the **Power Supply** tab > **Temp, Volt, Power**, and **Fan** sub-tabs.

STP

(Spanning-Tree Protocol) A link layer network protocol that ensures a loop-free topology for any bridged LAN. STP prevents loops from being formed when switches are interconnected via multiple paths. STP is a Data Link Layer protocol that was standardized as IEEE 802.1D. STP creates a spanning tree within a mesh network of connected layer-2 bridges (usually Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. With Spanning Tree, a device learns Ethernet (MAC) addresses by inspecting the Ethernet frame and recording the source MAC address in a dynamic table. The device also associates a learned MAC address with a port. The device can then make intelligent forwarding decisions based on the destination MAC address.

The collection of bridges in a LAN can be considered a graph whose nodes are the bridges and the LAN segments (or cables), and whose edges are the interfaces connecting the bridges to the segments. To break loops in the LAN while maintaining access to all LAN segments, the bridges collectively compute a spanning tree (which is not necessarily a minimum cost spanning tree).

The general STP rules describe a way of determining what spanning tree will be computed by the algorithm, but those rules require knowledge of the entire network. The bridges must determine the root bridge and compute the port roles (root, designated, or blocked) with only the information that they have. To ensure that each bridge has enough information, bridges use special data frames called Bridge Protocol Data Units (BPDUs) to exchange information about bridge IDs and root path costs. A bridge sends a

BPDU frame using the unique MAC address of the port itself as a source address, and a destination address of the STP multicast address 01:80:C2:00:00:00. See also “BPDU”. See also “xSTP”.

STP

(Shielded Twisted Pair) A special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground.

S-VLAN

Service VLAN (also referred to as Provider VLAN).

Syslog

(System Logging) a service run mostly on Unix and Linux systems (but also available for other OSes) to track events that occur on the system. Analysis can be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

Can refer to a method of general system logging, a log format, and/or a network log transmission mechanism. The Syslog function is implemented in the ION system via the **set syslog** CLI commands and via the device **MAIN** tab > **System Log Configuration** section parameters.

tacplus

TACACS+ is a protocol for AAA services (Authentication, Authorization, Accounting), very similar to RADIUS. Tacplus is TACACS+ program that provides routers and access servers with authentication, authorization and accounting services. This version is a major rewrite of the original Cisco source code. Key features include NAS specific host keys/prompts/enable passwords, NAS- and ACL-dependent group memberships, Connection multiplexing (multiple concurrent NAS clients per process), Session multiplexing (multiple concurrent sessions per connection, single-connection), IPv4 and IPv6 support, and compliant to latest TACACS+ protocol specification (at the time of publication).

TACACS+ / Tacplus involves:

- A NAS (Network Access Server), such as a TN, Cisco, or other device, or any other client which makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets. Servers using RADIUS or TACACS protocol are often called NAS (Network Access Server), not to be confused with NAS - (Network Attached Storage).
- A daemon - a program which services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.
- AV pairs - strings of text in the form attribute=value, sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

Note: Since a “NAS” is sometimes referred to as a server, and a “daemon” is also often referred to as a server, the term “server” is avoided here in favor of the less ambiguous terms “NAS” and “Daemon”. The Tacplus software provides logs for Authentication (authentication log = log_destination), Authorization (authorization log = log_destination), and Accounting (accounting log = log_destination). Tacplus supports three authentication methods: Clear text, Data Encryption Standard (DES - local and remote), and S/Key.

By default, Tacplus provides authentication services for: 1. VTY login, 2. Point-to-Point Protocol authentication via Password Authentication Protocol (PAP), 3. Point-to-Point Protocol authentication via Challenge/Handshake Authentication Protocol (CHAP), and 4. AppleTalk Remote Access (ARAP).

CHAP and ARAP can only utilize clear text, as required by their protocol definitions. Support for Microsoft CHAP (MSCHAP) is available. Tacplus statuses include: PASS, FAIL, GETDATA, GETUSER, GETPASS, RESTART, ERROR, and FOLLOW.

Tag (IEEE 802.1Q tag)

An IEEE 802.1Q tag, if present, is placed between the Source Address and the EtherType or Length fields. The first two bytes of the 802.1Q tag are the Tag Protocol Identifier (TPID) value of 0x8100. The TPID is located in the same place as the EtherType/Length field in untagged frames, so an EtherType value of 0x8100 means the frame is tagged, and the true EtherType/Length is located after the Q-tag. The TPID is followed by two bytes containing the Tag Control Information (TCI), the IEEE 802.1p priority (QOS) and the VLAN ID. The Q-tag is followed by the rest of the frame.

Tagged frame

A packet that contains a header that carries a VLAN identifier and a priority value. Also called a VLAN tagged packet. A Tagged frame contains a tag header immediately following the Source MAC Address field of the frame or, if the frame contains a Routing Information field, immediately following the Routing Information field. There are two types of tagged frames: VLAN-tagged frames and priority-tagged frames.

Tagging / Tag Header

Sending frames across the network requires a way to indicate to which VLAN the frame belongs, so that the bridge will forward the frames only to those ports that belong to that VLAN, instead of to all output ports. This indication is added to the frame in the form of a tag header. The tag header a) allows user priority information to be specified, b) allows source routing control information to be specified, and c) indicates the format of MAC addresses. Frames in which a tag header has been added are called “tagged” frames. These tagged frames convey the VLAN information throughout the network.

TCP

(Transmission Control Protocol) One of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

TCP/IP

(Transmission Control Protocol/Internet Protocol) The basic communication language or protocol of the Internet and/or a private network (either an intranet or an extranet).

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol (TCP), manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol (IP), handles the address part of each packet so that it gets to the right destination.

TDM

(Time Division Multiplexing) A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing.

TDR

1. (Time Domain Reflectometry) A measurement technique used to determine the characteristics of electrical lines by observing reflected waveforms. **2.** (Time Domain Reflector) An electronic instrument used to characterize and locate faults in metallic cables (for example, twisted wire pairs, coaxial cables). It can also be used to locate discontinuities in a connector, printed circuit board, or any other electrical path.

Telnet

A user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. Telnet is a terminal emulation program for TCP/IP networks that runs on your computer and connects your PC to a switch management. (Standard: RFC 854.)

Tentative address

In IPv6, an address whose uniqueness on a link is being verified, prior to its assignment to an interface.

A tentative address is not considered assigned to an interface in the usual sense. An interface discards received packets addressed to a tentative address, but accepts Neighbor Discovery packets related to Duplicate Address Detection for the tentative address.

TFTP

(Trivial File Transfer Protocol) A file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). Due to its simple design, TFTP can be implemented using a very small amount of memory. Because it uses UDP rather than TCP for transport, TFTP is typically used to transfer firmware upgrades to network equipment.

TFTP Download / Upload

The ability to load firmware, configuration files, etc. through a TFTP server. (AKA, TFTP. Standard: RFC 1350.)

TFTP Root Directory

The location on the console device (PC) where files are placed when received, and where files to be transmitted should be placed (e.g., *C:\TFTP-Root*).

TFTP Server

An application that uses the TFTP file transfer protocol to read and write files from/to a remote server. In TFTP, a transfer begins with a request to read or write a file, which also serves to request a connection. If the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and must be acknowledged by an acknowledgment packet before the next packet can be sent. Examples of available packages include Open TFTP Server, Tftpd32, WinAgents TFTP Server for Windows, SolarWinds free TFTP Server, TFTP Server 1.6 for Linux, and TftpServer 3.3.1, a TFTP server enhancement to the standard Mac OSX distribution.

Threshold crossing event

See “OAM Event”.

Throughput

The maximum rate at which no frame is dropped. This is typically measured under test conditions.

TID

(Transaction Identifier) The TID is entered in the CLI command **show soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> tid=<0-4294967295>**. The TID is shown in the Web interface at the **SOAM** tab > **MEP** sub-tab > **Linktrace** sub-tab.

TLS

(Transport Layer Security) A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

TLV

Type, Length, Value format - LLDP frames are sent by each equipment on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type, length, value (TLV) structures. An LLDP frame should start with mandatory TLVs (e.g., Chassis ID, Port ID, and Time to live). These mandatory TLVs are followed by any number of optional TLVs. The frame should end with a special TLV named end of LLDPDU. The IEEE 802.1ab specification contains a description of all of the TLV types.

TNDP

(TN Topology Discovery Protocol) the 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.

TOS

(Type of Service) The ToS byte in the IPv4 header has had several purposes over time, and has been defined in various ways by IETF RFC 791, RFC 1122, RFC 1349, RFC 2474, and RFC 3168. Currently, the ToS byte is a six-bit Differentiated Services Code Point and a two-bit Explicit Congestion Notification field.

The ToS model described in RFC 2474 uses the Differentiated Services Field (DS field) in the IPv4 Header and IPv6 Header. See also CoS and QoS.

TPID

(Tag Protocol Identifier) a field in a VLAN Tag for which IEEE802.1Q specifies a value of 0x8100.

Trap

In SNMP, a trap is a type of PDU used to report an alert or other asynchronous event about a managed subsystem.

Also, a place in a program for handling unexpected or unallowable conditions - for example, by sending an error message to a log or to a program user. If a return code from another program was being checked by a calling program, a return code value that was unexpected and unplanned for could cause a branch to a trap that recorded the situation, and take other appropriate action.

An ION system trap is a one-way notification (e.g., from the IONMM to the NMS) that alerts the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the IONMM rather than the NMS. For a management system to understand a trap sent to it by the IONMM, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Traps

One of two types of SNMP notifications that can be sent. See also "informs".

A “trap” is a one-way notification from the NID to the NMS. Its purpose is to alert the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the Agent rather than the NMS. In order for a management system to understand a trap sent to it by the NID, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Each Trap is an asynchronous notification from agent to manager. Includes current sysUpTime value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed SNMPv2-Trap.

TCP/UDP Port Prioritization

The ability to prioritize traffic internally based on a TCP or UDP port number. (AKA, Layer 4 Prioritization.)

TTL

(Time to live) an Ethernet counter that records the number of times a transmission is sent/received without errors. TTL specifies how long a datagram is allowed to “live” on the network, in terms of router hops. Each router decrements (reduces by one) the value of the TTL field prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

The default TTL for ION software is 64. This means that a test packet must be successfully sent and received 63 times before a TTL expired message is generated. You can change the TTL value (e.g., a value of 255 is a demanding test because the packet must be sent and received error free 254 times).

Tunnel

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one (as in L2TP and VPN).

Tunneling

Encapsulating one type of packet inside the data field of another packet. This allows transmitting data that is structured in one protocol within the protocol or format of a different protocol. Tunneling can involve most OSI or TCP/IP protocol layers.

UAC

(User Account Control) Technology and security infrastructure of some *Microsoft* operating systems that improve OS security by limiting application software to standard user privileges until an administrator authorizes an increase.

UDP

(User Datagram Protocol) A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

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.

UNI Type 1

In the User-to-Network Interface, a demarcation point defined by MEF 13 defines:

- Service attributes
- Traffic classification and bandwidth profile(s)

The original MEF UNI was called UNI Type 1, which operates in manual configuration mode in which the Service Provider and Customer will have to manually configure the UNI-N and UNI-C for services.

UNI Type 2

In the User-to-Network Interface, a demarcation point defined by MEF 20, exists at version 2.1 or 2.2. UNI Type 2.1 includes Optional and Mandatory Features. The UNI Type 2.1 Mandatory Features include:

- Backward compatibility with UNI Type 1
- Service OAM
- Enhanced UNI attributes
- L2CP Handling

Optional UNI Type 2.1 features include Link OAM, Protection and E-LMI.

UNI Type 2.2 (MEF 20, 25) includes all Mandatory Features:

- Backward compatibility to UNI Type 1
- Service OAM
- Enhanced UNI attributes
- L2CP Handling
- Link OAM
- Protection
- E-LMI

Unicast

One of the four forms of IP addressing, each with its own unique properties. The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient. See also “Multicast”.

Unicast address

In IPv6, an identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

Unspecified Address

In IPv6, the address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.

The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing headers. An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router.

Unicast destination

A host or router that can be identified by a unique unicast IP address. See also “Multicast destination”.

Untagged frame

A frame that does not contain a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or, through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).

Upper layer

In IPv6, a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.

USB

(Universal Serial Bus) A plug-and-play interface between a computer and add-on devices, such as media players, keyboards, telephones, digital cameras, scanners, flash drives, joysticks and printers.

USM

(User-Based Security Model) The SNMPv3 USM lets you implement authentication and privacy in SNMP communication between agents and managers. For example, IETF RFC 2574 defines the User-based Security Model (USM) for SNMPv3.

SNMPv3's security header implements the User Security Model (USM), which provides confidentiality and integrity for network management communications. Confidentiality is provided through the use of Data Encryption Standard (DES). Although this algorithm is notoriously weak (due to its use of a 40-bit encryption key), it provides a marked advantage over plaintext community strings. The SNMPv3 USM also allows for user-based authentication and access control. Rather than using just the two-level "read" and "write" community strings of prior SNMP implementations, administrators can create specific accounts for each SNMP user and grant privileges through those user accounts.

The USM utilizes MD5 and the SHA as keyed hashing algorithms for digest computation to provide data integrity to directly protect against data modification attacks, to indirectly provide data origin authentication, and to defend against masquerade attacks. Contrast with "VACM".

UTC

(Coordinated Universal Time) A time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich.

UTP

(Unshielded Twisted Pair) The most common form of twisted pair wiring, because it is less expensive and easier to work with than STP (Shielded Twisted Pair). UTP is used in Ethernet 10Base-T and 100Base-T networks, as well as in home and office telephone wiring. The twist in UTP helps to reduce crosstalk interference between wire pairs.

VAC

Volts AC (alternating current, as opposed to DC – direct current).

VACM

(View-Based Access Control Model) a new security feature defined by SNMPv3. Like User-based Security Model (USM) it authenticates, encrypts, and decrypts SNMPv3 packets, as specified in RFC 2575. An SNMP entity's Access Control subsystem checks if a specific type of access to a specific managed object is allowed. Access control occurs in the agent when processing SNMP retrieval or modification request messages from a manager, and when a notification message is sent to the manager. VACM concepts are based the problems with SNMPv1 and SNMPv2c community strings. A community string identifies the requesting entity, the location of the requesting entity, and determines access control information and MIB view information. A single community string variable provides low flexibility and functionality. VACM builds on the community string concept with a stricter, and more dynamic, more easily administered access control model. Contrast with "USM".

Valid address

In IPv6, a preferred or deprecated address. A valid address may appear as the source or destination address of a packet, and the internet routing system is expected to deliver packets sent to a valid address to their intended recipients.

Valid lifetime

In IPv6, the length of time an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

Varbind

In SNMP, a Sequence of two fields, an Object ID and the value for/from that Object ID. Varbinds is short for Variable bindings. It's the variable number of values that are included in an SNMP packet. Each varbind is made of an OID, type, and value.

VCP

(Virtual Com Port) A driver that allows a USB device to appear as an additional COM port. The USB device can be accessed by an application in the same manner as a regular COM port.

VDC

Volts DC (direct current, as opposed to AC – alternating current).

VID

(VLAN Identifier) The identification of the VLAN, which is defined by the standard IEEE 802.1Q. VID has 12 bits and allows the identification of 4096 VLANs.

VLAN

(Virtual LAN) Refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

VLAN Endstation Endpoint

A protocol endpoint representing an endstation network port and its VLAN-specific attributes.

VLAN Switch Endpoint

A protocol endpoint representing a switch port and its VLAN-specific attributes.

VLAN-tagged frame

A tagged frame whose tag header carries both VLAN identification and priority information. A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs (i.e., it carries a tag header that carries a non-null VID). A VLAN-tagged frame is classified as belonging to a particular VLAN based on the value of the VID that is included in the tag header. The presence of the tag header carrying a non-null VID means that some other device, either the originator of the frame or a VLAN-aware Bridge, has mapped this frame into a VLAN and has inserted the appropriate VID. Contrast “untagged frame”.

VLAN Tunneling

(Virtual LAN Tunneling) A mechanism that allows service providers to use a single VLAN to support multiple VLANs of customers, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. At the same time, it significantly reduces the number of VLANs required to

support the VPNs. VLAN Tunneling encapsulates the VLANs of the enterprise customers into a VLAN of the service provider. Also called '802.1q Tunneling'.

VOIP

(Voice over Internet Protocol) A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks.

VTY

(Virtual Type Terminal) - A vty interface and password must be created in order to enable Telnet access to an IPv6 router. Also Virtual TTY (VTY) connections are for connecting from a remote location via Telnet or SSH. PuTTY is a vty connection device. A "line" on a router is a physical async serial port (such as a terminal or modem), a virtual network connection, or another type of serial line on the router. A router can have a console line (labeled CTY), an AUX port (labeled AUX), multiple VTY lines, and multiple TTY lines. A Virtual Teletype command line interface is created in a router for a Telnet session. The router is able to generate a VTY dynamically.

Web-based Management

Allows users to manage the switch through a web browser. (AKA, Web GUI, Web interface, Web IF.)

Well Known Ethernet Multicast Addresses

Some common Ethernet multicast MAC addresses are shown below with their related Field Type and typical usage.

Ethernet Multicast Address	Usage
01-00-0C-CC-CC-CC	CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)
01-00-0C-CC-CC-CD	Cisco Shared Spanning Tree Protocol Address
01-80-C2-00-00-00	Spanning Tree Protocol (for bridges) (IEEE 802.1D)
01-80-C2-00-00-01	Ethernet OAM Protocol (IEEE 802.3ah)
01-80-C2-00-00-02	IEEE Std 802.3 Slow Protocols multicast address
01-80-C2-00-00-03	IEEE Std 802.1X PAE address
01-80-C2-00-00-04	IEEE MAC-specific control protocols
01-80-C2-00-00-08	Spanning Tree Protocol (for provider bridges) (IEEE 802.1AD)
01-00-5E-xx-xx-xx	IPv4 Multicast (RFC 1112)
33-33-xx-xx-xx-xx	IPv6 Multicast (RFC 2464)

Well-known IPv6 Multicast Addresses

These well-known multicast addresses are pre-defined. The group IDs defined in this section are defined for explicit scope values. Use of these group IDs for any other scope values, with the T flag equal to 0, is not allowed. These multicast addresses are reserved and can not be assigned to any multicast group.

Reserved Multicast Addresses:

FF00:0:0:0:0:0:0
 FF01:0:0:0:0:0:0
 FF02:0:0:0:0:0:0
 FF03:0:0:0:0:0:0
 FF04:0:0:0:0:0:0
 FF05:0:0:0:0:0:0
 FF06:0:0:0:0:0:0
 FF07:0:0:0:0:0:0
 FF08:0:0:0:0:0:0
 FF09:0:0:0:0:0:0
 FF0A:0:0:0:0:0:0
 FF0B:0:0:0:0:0:0
 FF0C:0:0:0:0:0:0
 FF0D:0:0:0:0:0:0
 FF0E:0:0:0:0:0:0
 FF0F:0:0:0:0:0:0

The following multicast addresses identify the group of all IPv6 nodes, within scope 1 (interface-local) or 2 (link-local).

All Nodes Addresses: FF01:0:0:0:0:0:1
 FF02:0:0:0:0:0:0:1

The following multicast addresses identify the group of all IPv6 routers, within scope 1 (interface-local), 2 (link-local), or 5 (site-local).

All Routers Addresses: FF01:0:0:0:0:0:2
 FF02:0:0:0:0:0:2
 FF05:0:0:0:0:0:2

Solicited-Node Address: FF02:0:0:0:0:1:FFXX:XXXX

Solicited-Node multicast addresses are computed as a function of a node's unicast and anycast addresses. A Solicited-Node multicast address is formed by taking the low-order 24 bits of an address (unicast or anycast) and appending those bits to the prefix FF02:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range FF02:0:0:0:0:1:FF00:0000 to FF02:0:0:0:0:1:FFFF:FFFF.

For example, the Solicited-Node multicast address corresponding to the IPv6 address 4037::01:800:200E:8C6C is FF02::1:FF0E:8C6C. IPv6 addresses that differ only in the high-order bits (e.g., due to multiple high-order prefixes associated with different aggregations) will map to the same Solicited-Node address, thereby reducing the number of multicast addresses a node must join. A node is required to compute and join (on the appropriate interface) the associated Solicited-Node multicast addresses for all unicast and anycast addresses that have been configured for the node's interfaces (manually or automatically).

Well Known Ports

The set of all available port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. The Well Known Ports are those from 0 - 1023. The Registered Ports are those from 1024 - 49151. Registered ports require IANA registration. The Dynamic and/or Private Ports are those from 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.

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 /TCP
161	SNMP /UDP
161	SNMPTRAP /TCP
162	SNMPTRAP /UDP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
546	DHCP Client
547	DHCP Server

Write View

A view name (up to 64 characters) for each SNMP group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group. A “Writeview” is a string of up to 64 characters that is the name of the view that lets you enter data and configure the contents of the agent. The default writeview is 'nothing' (i.e., the null OID). You must configure write access.

xSTP

Spanning Tree Protocol (multiple variations) defined in MEF specification 17. See also “STP”.

XMODEM

a simple file transfer protocol developed in 1977 as the MODEM.ASM terminal program. XMODEM, like most file transfer protocols, breaks up the original data into a series of "packets" that are sent to a receiver, along with information that allows the receiver to tell if the packet was correctly received. It provides single file transfer using 128-byte packets with CRC or checksum error detection.

XMODEM-1K

an expanded version of XMODEM. Like other backward-compatible XMODEM extensions, it was intended that a -1K transfer could be started with any implementation of XMODEM on the other end, backing off features as required.

It provides simple serial file transfer between a server and client across a point-to-point link using fixed-length packets. Each server packet contains 1024 bytes of file data and is individually acknowledged by the receiving client. One file can be sent per transmission, and the transmission must be restarted from the beginning if it fails.

YMODEM

a protocol for file transfers between modems. YMODEM was developed as the successor to XMODEM. The original YMODEM was much the same as XMODEM except that it sent the file name, size, and timestamp in a regular XMODEM block before actually transferring the file. It provides multiple file transfer using 1 Kbyte packets, and is similar to Xmodem in other aspects.

ZMODEM

a file transfer protocol developed in 1986 to improve file transfer performance on an X.25 network. ZMODEM also offers restartable transfers, auto-start by the sender, an expanded 32-bit CRC, control character quoting, and sliding window support. It provides multiple file transfer, sending packets without waiting for acknowledgement, and permits an interrupted transfer to restart.

Y.1731

The ITU-T OAM Recommendation. The x323x NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). See also “SOAM” and 802.1AG.

Index

- AC power, 53
- ACL, 24, 269
 - Conditions, 271, 275
 - Configuring, CLI method, 271, 277
 - Configuring, Web method, 274, 279
 - Default chain policy, 271, 274, 277
 - Rules, 272, 274
 - Trap rate, 272, 274
- [Add Users](#), 263
- Aging Time, 254
- AIS, 240
 - Configuring, CLI method, 241, 243
- Archive file
 - Creating, 449
 - Uploading, 450
- ~~Auto negotiate~~, 133
- AutoCross*, 18, 131
- Automatic link restoration, 23
- Auto-negotiation, 18
- Backing up the configuration, 411, 413, 414
- Backup, 410
- Canadian regulations**, 659
- CCM, 203
- CE marking**, 659
- Certificate authority, 282
- Chassis installation, 49
- Circuit ID, 124, 126
- Circuit ID field, 36
- CLI
 - Configuration quick reference, 684
- CLI error messages, 479
- CLI hierarchy, 82
- COM port
 - Configuring, 64
 - Properties, 67
- Compliance information, 659
- Config File, 416
- Configuration
 - ACL, 269
 - Backing up, 19, 411, 414
 - ETH-MCC, 220
 - FLM, 236
 - HTTPS, 282
 - HyperTerminal, 64
 - IP address, 96
 - IP address, 73
 - Management Redundancy, 392, 397
 - Management VLAN, 204, 210, 215, 225, 230, 241, 358
 - RADIUS, 296
 - Restoring, 417, 421
 - SNMP, 313, 314
 - SNTP, 256
 - SSH, 307
 - System logging, 403
 - TDM Loopback, 401
 - TNDP, 399
- Configuration quick reference, 684
- Configuration:, 777
- Connect AC power, 53
- Connecting by
 - Telnet, 69, 71
 - Web, 76
- Continuity Check Monitoring, 203
- Conventions, documentation, 47
- Critical event, 27
- Database index file, 449
- Daylight savings time, 260, 262
- db.idx file**, 449
- db.zip file**, 449
- Defaults
 - Reset factory settings, 429
- [Delete Users](#), 263
- Device Description field, 36
- DHCP
 - Configuring, 103
 - Server definition, 103
- Disable
 - Serial interface, 428
 - USB access, 428
- Discovery, 27
- DM
 - Configuring, CLI method, 230, 233
- DMI, 620
- DMI
 - Configuring, Web method, 621
- DNS
 - Configuring, CLI method, 104
 - Configuring, Web method, 106
 - Defining a server, 101, 104
- Documentation conventions, 47
- Double tag, 382
- Down MEPs, 694
- Duplex LED
 - Model x3230-1040, 56

- Model x3230-10xx, 60
- Model x3231-1040, 58
- Duplex modes, 56, 58, 60
- Duplex setting, 135, 138
- Dying gasp, 27
- Dynamic IP address, 103
- [Edit Users](#), 263
- Engine ID, 318
- Error messages
 - CLI commands, 479
 - Web interface, 545
- Ethernet connection
 - Telnet CLI, 69, 71
 - Web interface, 76
- Ethernet connector
 - Model x3230-1040, 56
 - Model x3230-10xx, 60
 - Model x3231-1040, 58
- ETH-MCC
 - Configuring, CLI method, 221, 222
- ETH-TST, 224
 - Configuring, CLI method, 225, 227
- European regulations**, 660
- Event notification, 27
- Far end fault, 20
- FCC regulations**, 659
- Features
 - Management module, 16
 - Security, 24
- Firmware
 - Archive file, 449
 - Backing up, 411, 414, 458
 - Database index file (db.idx), 449
 - Upgrading, 441
- FLM, 236
- FocalPoint, 18, 81
- Forward Learning Aging Time, 254
- Frame Delay Measurement, 229
- Full duplex operation, 56, 58, 60
- Gateway address, 74, 97, 99
- GUI, 21, 81
- Half-duplex operation, 56, 58, 60
- HTTPS, 24, 282
 - Certificates, 283, 285
 - Configuring, CLI method, 283
 - Configuring, Web method, 285
 - Port number, 283, 285
 - Private key, 283, 285
 - Public key, 282
- HyperTerminal, configuring, 64
- Hypertext transfer protocol secure, see HTTPS, 24
- IEEE 802.3ah-2004 standards, 27
- Install
 - Chassis model, 49
 - IONMM, 49
 - SFPs, 54
 - Standalone model, 50
 - USB driver, 61
- IP Addr Blocking, 294
- IP address, 96
 - Dynamic configuration, CLI method, 103
 - Static configuration, CLI method, 73, 97
 - Static configuration, Web method, 99
- IP Address modes, 25
- IP configuration, 74
- Jumper settings, 628
- L2CP, 395
- Last gasp, 27
- LB
 - Configuring, CLI method, 212
- LBM, 209
- LBR, 209
- LEDs, 55
- Link active LED
 - Model x3230-1040, 56
 - Model x3230-10xx, 60
 - Model x3231-1040, 58
- Link OAM, 152
 - Configuring, CLI method, 153
 - Configuring, Web method, 158
- Link restoration, 23
- Linktrace, 214
- LM
 - Configuring, CLI method, 237
- Loopbackconfiguration, 209
- LT
 - Configuring, CLI method, 215, 217
- LTM, 214
- LTR, 214
- MAC address
 - Blocking, 25, 290
 - Filtering, 25, 287
- MAC Address Blocking
 - Configuring, CLI method, 292
- MAC Address Filtering, 287
- MAC Address Filtering
 - Configuring, CLI method, 287
- MAC Address Filtering
 - Configuring, CLI method, 288
- MAC Address Learning, 408

- MAC Address Learning, 36
- Maintenance associations (MAs), 172, 176, 697, 703, 711, 716, 722, 725, 730, 735
- Maintenance domains (MDs), 172, 176, 697, 703, 711, 716, 722, 725, 730, 735
- Maintenance end points (MEPs), 31, 187, 191
- Maintenance entity groups (MEGs), 181, 184, 782
- Maintenance intermediate points (MIPs), 31, 194, 196, 206, 212, 217, 220, 227, 233, 243
- Management VLAN, 24, 357, 362
 - Configuring, CLI method, 359, 362
- MDI, 18, 131
- MDIX, 18, 131
- Menuing system, 88
- Mgmt VLAN
 - Configuring, CLI method, 366
 - Configuring, CLI method, 368
- MIB Traps, 801
- MIBs supported, 39
- Network access, 71
 - Telnet session, 69, 71
 - Web interface, 76
- Network management system (NMS), 21, 81, 313, 314
- OAM, 152
 - Communications channel, 27
 - Critical event, 27
 - Discovery, 27
 - Event notification, 27
 - Features, 27
 - Remote loop back, 28
- Operating mode
 - 10 MBps, 56, 58, 60
 - 100 MBps, 56, 58, 60
 - 100Base-TX, 56, 58, 60
 - 10Base-T, 56, 58, 60
 - Full duplex, 56, 58, 60
 - Half-duplex, 56, 58, 60
- OS support, 61
- Pause, 18
- Pause frames, 134
- PHY Mode setting, 141
- ~~Point System~~, 19
- Port
 - Advertised capabilities, 134
 - Duplex setting, 135, 138
 - Pause capability, 134
 - Speed setting, 135, 138
- Port Admin Mode setting, 141
- Port Fwd Mgmt, 294
- Power LED
 - Model x3230-1040, 56
 - Model x3230-10xx, 60
 - Model x3231-1040, 58
- Private key
 - HTTPS, 283, 285
 - SSH, 307
- Problem conditions, 464
- Provisioning, 410
- Provisioning tab, 411, 414, 417, 421
- PS
 - Configuring, CLI method, 842, 845
- Public key
 - HTTPS, 282
- Public key cryptography, 282
- Q-in Q Tunneling, 382
- Q-in-Q Configuration, 791
- QoS, 357, 383
- Rack mount installation, 50
- RADIUS, 24, 296
 - Configuring, CLI method, 290, 297
 - Configuring, Web method, 299
 - Retry limit, 297, 299
 - Secret, 297, 299
 - Server, 296, 297, 299
 - Timeout, 297, 300
- RDI, 245
- Reboot, 438
 - Web method, 439
- Regulations**
 - Canadian**, 659
 - European**, 660
 - FCC**, 659
- Remote loop back, 28
- Reset
 - Factory defaults, 429
 - Uptime, 432
- Restart
 - ION MM, 438
- Restore, 410
- Restoring the configuration, 417, 421
- Returns, product**, 657
- RFC 2544 Benchmarking, 38
- Secure shell, see SSH, 24
- Secure socket layer (SSL), 282
- Security
 - MAC address blocking, 25, 290
 - Security features, 24
 - Selective link pass through, 248
- Serial interface, 56, 58, 60
 - Disable, 428

- Setup, 75
- Service OAM, 28
- Setup
 - Serial interface, 75
 - Telnet, 69, 71
 - USB, 75
 - Web interface, 76
- SFP installation, 54
- SGMII, 141
- Signing in, 76
- Signing out, 79
- Simple network management protocol, see
 - SNMP, 21, 81
- Simple network time protocol, see SNTP, 268
- SLPT, 21
- SNMP, 21, 24, 81, 313, 314
 - Configuring, CLI method, 337
 - Configuring, Web method, 340
- SNMP Group, 334
- SNMP Traps, 799
- SNMP v1, 37
- SNMP v2c, 37
- SNMP v3, 321
- SNMP v3 Groups, 334
- SNMP v3 Traps, 800
- SNMP v3 Users, 334
- SNMP version, 318
- SNMP versions, 37
- SNTP, 256
 - Configuring, CLI method, 257
 - Configuring, Web method, 176, 262
 - Server, 260
- SOAM, 28
 - Configuring DM, Web method, 233
 - Configuring LM, Web method, 239
 - Configuring MDs/MAs, CLI method, 172
 - Configuring MDs/MAs, Web method, 176, 697, 703, 711, 716, 722, 725, 730, 735
 - Configuring MEGs, CLI method, 181
 - Configuring MEGs, Web method, 184, 782
 - Configuring MEPs, CLI method, 187
 - Configuring MEPs, Web method, 191
 - Configuring MIPs, CLI method, 194
 - Configuring MIPs, Web method, 196, 206, 212, 217, 220, 227, 243
 - Configuring, CLI method, 239
 - Configuring, CLI method, 172, 181, 184, 187, 191, 194, 196, 204, 206, 210
 - Configuring, CLI method, 620
- SOAM Config Error List, 603
- SOAM configuration, 170
 - SOAM Configuration, 694
 - SOAM Configuration - CLI, 738
 - SOAM Configuration - Web, 694
 - SOAM description, 26
 - SOAM recommendations, 29
 - SOAM terminology, 247
 - SOAM tests**, 247
 - Speed setting, 135, 138
 - SSH, 24, 307
 - Configuring, CLI method, 308, 361, 363
 - Configuring, Web method, 310
 - Host key, 308, 310
 - Public key, 309, 311
 - Retry limit, 308, 310
 - Timeout value, 308, 310
 - Static IP address, 96
 - Subnet mask, 73, 97, 99
 - Syslog, 403
 - Syslog, 36, 403
 - Tabletop installation, 51
 - TDM Loopback, 401
 - TDM Loopback, 36
 - Tech Support, 653
 - Telnet
 - Default login, 664
 - Default password, 664
 - Ethernet connector, 56, 58, 60
 - Setup, 69, 71
 - Terminate session, 73
 - Terminate
 - Telnet session, 73
 - USB interface, 70
 - TFTP, 19
 - Server address, 285, 311, 450, 454
 - Upgrading firmware, 443, 449, 454
 - Timezones, 257, 262
 - TLPT, 22
 - TN Topology Discovery Protocol, 36
 - TNDP, 399
 - TNDP, 36
 - Transparent link pass through, 23, 248
 - Trap, 315
 - Trap Server Log, 840
 - Traps, 313, 799
 - Troubleshooting, 459
 - UL recognized**, 659
 - Up MEPs, 694
 - Upgrade firmware
 - IONMM, 454
 - Other modules, 449
- USB**

- Configure COM port, 64
- Connection, 69
- Default login, 664
- Default password, 664
- Disable access, 428
- Driver installation, 61, 75
- Model x3230-1040 connectors**, 56
- Model x3230-10xx connectors**, 60
- Model x3231-1040 connectors**, 58
- Setup, 75
- Terminate connection, 70
- User
 - levels, 263, 264, 266
 - login, 263
 - Name, 264, 266
 - Password, 266
- VCT, 615
- Virtual Cable Test, 615
- VLAN, 19
- VLAN Configuration, 356
- VLAN tag, 382
- VLAN Tunneling, 34
- VLAN Tunneling Configuration, 777
- VLANs
 - Configuring, 356
- Wall mount installation, 52
- Warranty, 656
- Web interface
 - Error messages, 545
 - Ethernet connector, 56, 58, 60
 - Signing in, 76
 - Signing out, 79



Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952- 941-7600 or 1-800-526-9267

Fax: 952-941-2322

Copyright © 2010, 2011, 2012 Transition Networks

All rights reserved.

Printed in the U.S.A.

x323x Remotely Managed Network Interface Device (NID)

33432 Rev. E