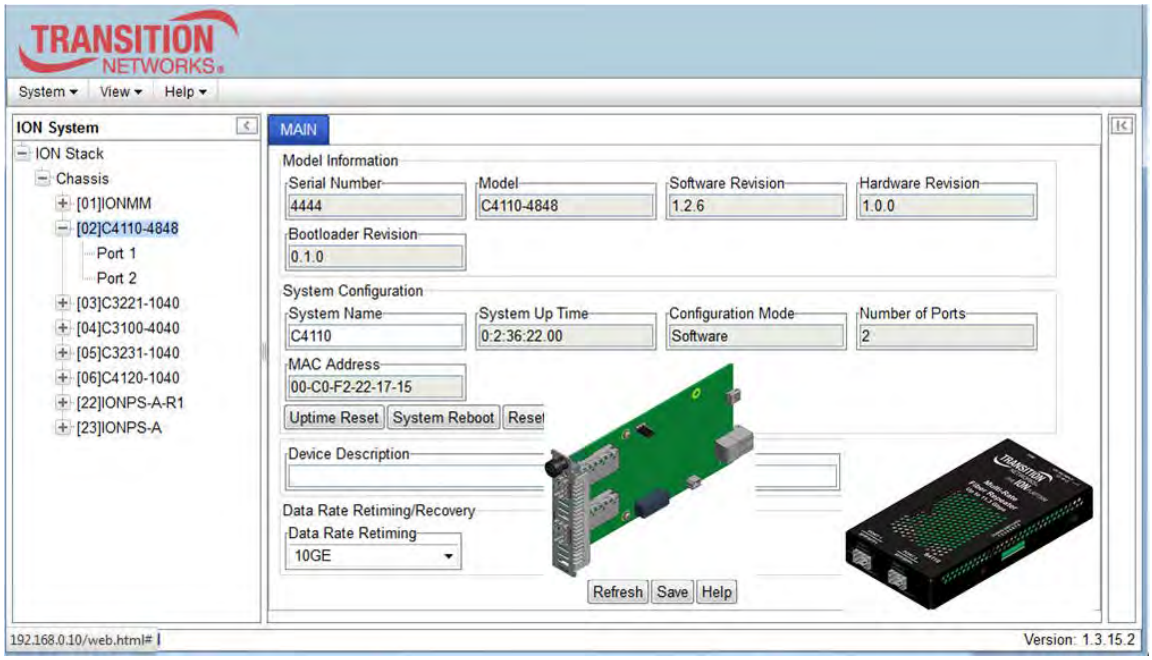
ION System x4110 Series

10 Gbps Fiber-to-Fiber Converter Slide-in-Module and NID



Web User Guide

33574 Rev. B

Trademarks

Copyright Notice/Restrictions

ION System x4110 -- 10 Gbps Fiber-to-Fiber Converter Web User Guide, 33574 Rev. B

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322
sales@transition.com | techsupport@transition.com | customerservice@transition.com

Revision History

Rev	Date	Description
A	3/2/15	Initial release for v 1.2.4.
B	10/17/16	Update for C4110 v1.2.6; add Vendor Specific information to DMI; add C4110 support in Focal Point; update contact information.

Cautions and Warnings

Definitions

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

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

See the related Install Guide manual for Electrical Safety Warnings translated into multiple languages.

Table of Contents

List of Tables

Section 1: Introduction

Document Overview

The purpose of this manual is to provide the user with an understanding of the Transition Networks x4110 Ethernet media converter's web interface. For S4110 and C4110 models, product description, features, applications, manageable features and protocols, see the model-specific *install guide* manual.

Related Manuals and Online Helps

A printed Documentation Postcard is shipped with each x4110. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface. A substantial set of technical documents, white papers, case studies, etc. are available on our web site at https://www.transition.com/.

The ION system and related device manuals are listed below.

1. Product Documentation Postcard, 33504
2. C4110 Install Guide, 33572
3. S4110 Install Guide, 33573
4. x4110 Web User Guide, 33574 (this manual)
5. x4110 CLI Reference, 33575
6. ION Management Module (IONMM) User Guide, 33457
7. FocalPoint 3.0 User Guide, 33293
8. SFP manuals (product specific)
9. Release Notes (software version specific)

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

Documentation Conventions

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

Table 1: Documentation Conventions

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

Section 2: Management Method

General

The x4110s are managed either directly or through the IONMM. Whether the x4110is managed directly or indirectly, management is accomplished through one of the following methods.

- 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 x4110 can be remotely managed directly (i.e., not through IONMM). This enables administrators to monitor and configure remote stand-alone x4110s straight from the Network Management Station (NMS) without leaving the office.

IONMM Managed Devices

IONMM devices that are managed through the IONMM are either chassis resident (x4110) or standalone modules (S32xx or media converters) that are connected as remotes to chassis resident modules. Communications between the IONMM and remote devices is through the ION Chassis backplane. See the *IONMM User Guide* for details.

Managing Slide-In and Remote Modules via the Web Interface

1. Access the x4110 via the Web interface (see "Starting the Web Interface").
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 and Online Helps" section.

Direct Managed Devices

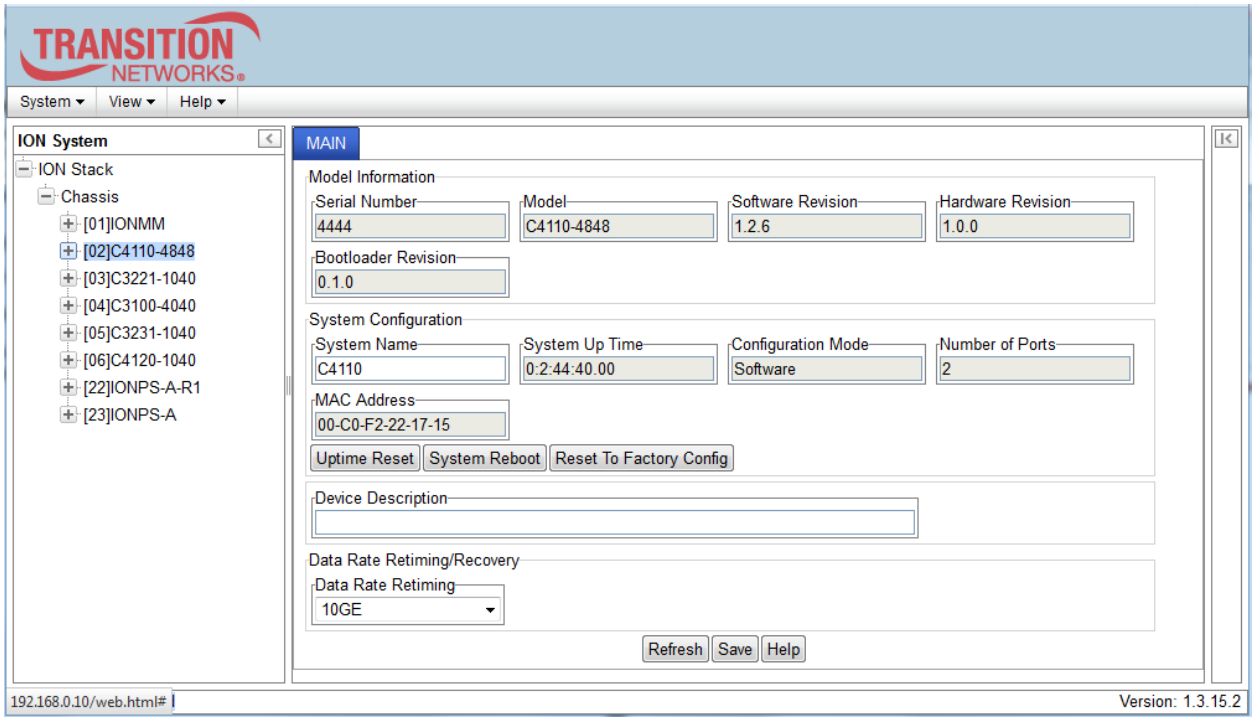
Direct management is for standalone devices that are not connected to a module that is managed through the ION Management Module (IONMM). In direct management, the network and/or USB cable is connected directly to the module to be managed.

Managing Standalone Modules via the IONMM Web Interface

1. Access the x4110through the Web interface (see "Starting the Web Interface").

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 to be managed (e.g., the C4110-4848 module above).

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

Menu System Descriptions

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

Table 2: System-Level Menu Description

Dropdown / Tab	Description
ION System pane	**ION Stack** - consists of one chassis or one standalone device. The Stack Members table lists the Stack's chassis and its type. **Chassis** - the ION System family of products; the Chassis View shows a summary view of one such chassis. Model Information includes: ***** Serial Number - The serial number of the chassis itself. Individual x4110s also have their own serial numbers. ***** Model Name - The exact model name of this device (e.g., ION219). When contacting Technical Support, please be sure to give this name rather than the less specific Catalog number. ***** Software Revision, Hardware Revision, and Bootloader Revision. ***** Chassis Members table - lists local physical components in slots 1 to 19. **Device** – provides tabs and sub-tabs for the IONMM and x4110s in the ION system. **Port** - provides tabs and sub-tabs for a selected x4110 port.
System Dropdown	Sign out.
View Dropdown	Refresh.
Help Dropdown	Online Help, ION Product Home Page, and About ION System Web Interface.
MAIN Tab	Sections: Model Information, System Configuration, Device Description, and Data Rate Timing/Recovery sections. Buttons: Uptime Reset, System Reboot, Reset To Factory Config buttons. Refresh, Save, and Help buttons.

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

Table 3: Port-Level Menu Description

Tab	Description
MAIN Tab	Sections: Circuit ID and Port Configuration. Buttons: *Refresh, Save,* and *Help.*
DMI Tab	Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length, and Vendor Specific Information. The DMI (Diagnostic Maintenance Interface) function displays x4110 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information. **Note**: not all SFP models support DMI. Transition Networks models that support DMI have a "D" at the end of the model number. If you click the DMI tab on a x4110 model that does not support DMI, the message "*The DMI feature is not supported on current port*." Buttons: *Refresh, Save,* and *Help.*

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 for information on how to save the stored files from deletion.

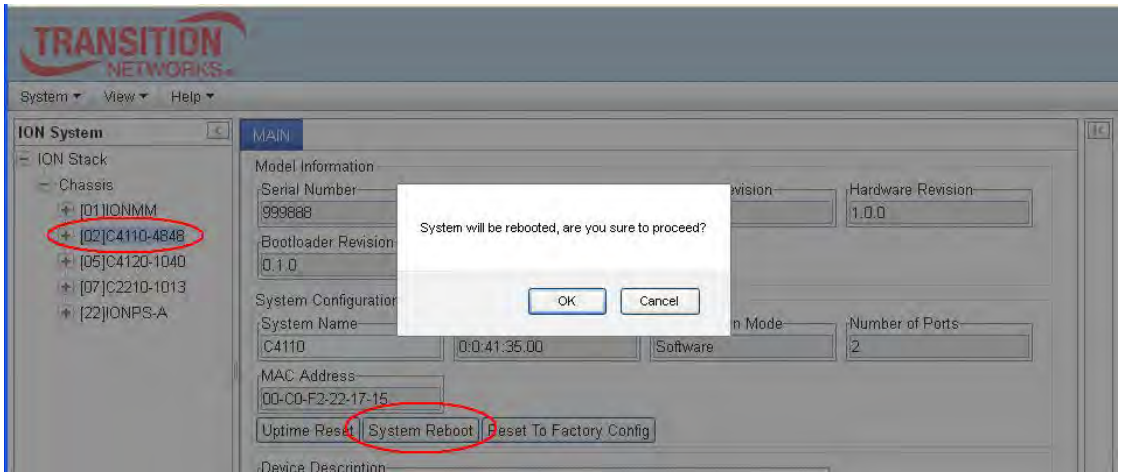
For more information on how the Reboot, Reset, and Power Off functions impact stored files, see:

- Table 5: File Status after a Reset to Factory Defaults on apge 24
- Table 6: File Content and Location after a System Reboot on page 27

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

System Reboot

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



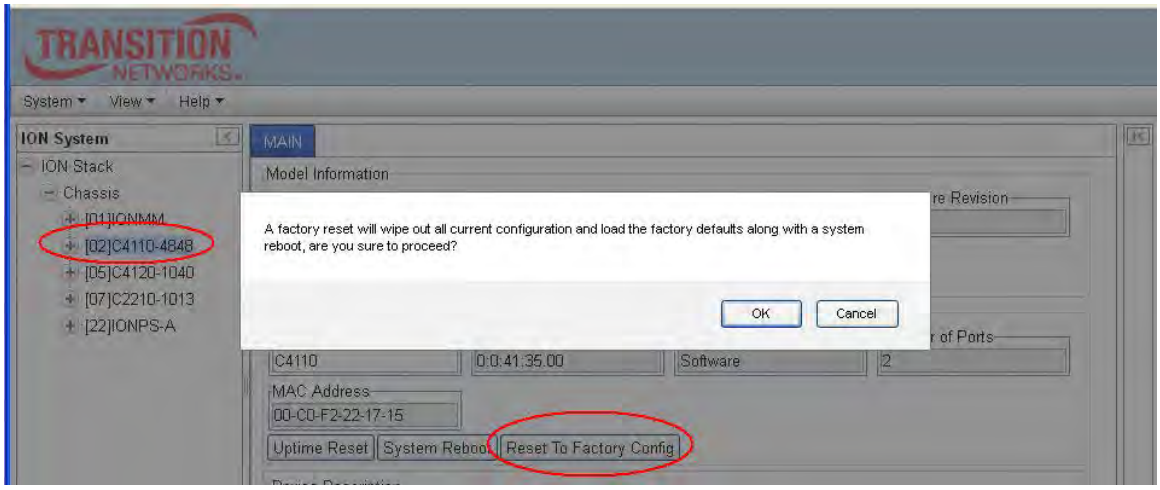
Press the **Cancel** button if you are not sure you want a system reboot to occur.
Press the **OK** button to clear the webpage message and begin the reboot process.

The message *[02]C4110-4848 is rebooting...* displays for a while; when done, the message *[02]C4110-4848 rebooting finished*" displays. You can clcik the **Refresh** button to clear the message.

Note that a System Reboot can take several minutes.

Reset To Factory Config

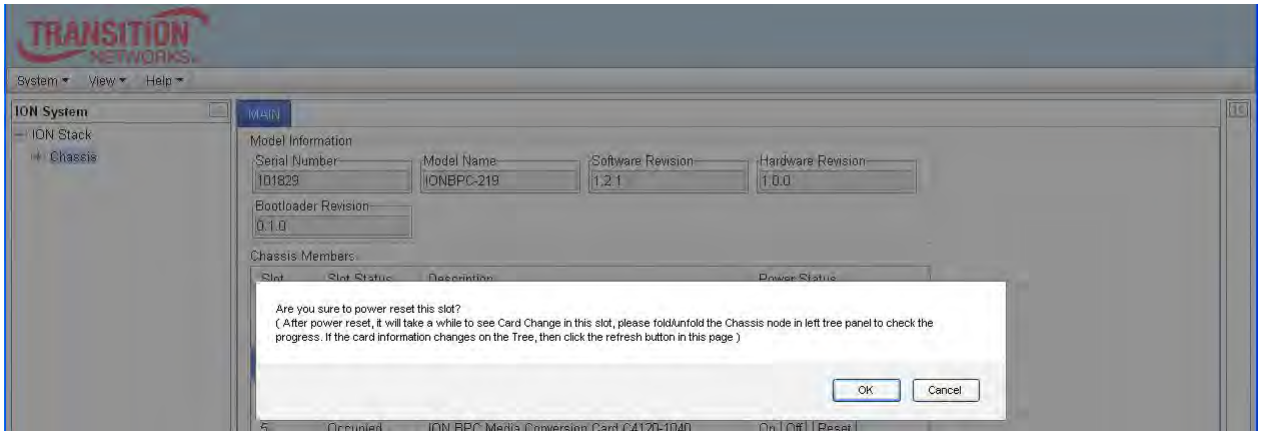
Clicking the **Reset To Factory Config** button resets the entire system configuration to the state it was in when it shipped from the factory. This permanently removes all current configuration details and loads the factory default settings. The message "*A factory reset will wipe out all current configuration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



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

Reset Power to a Slot

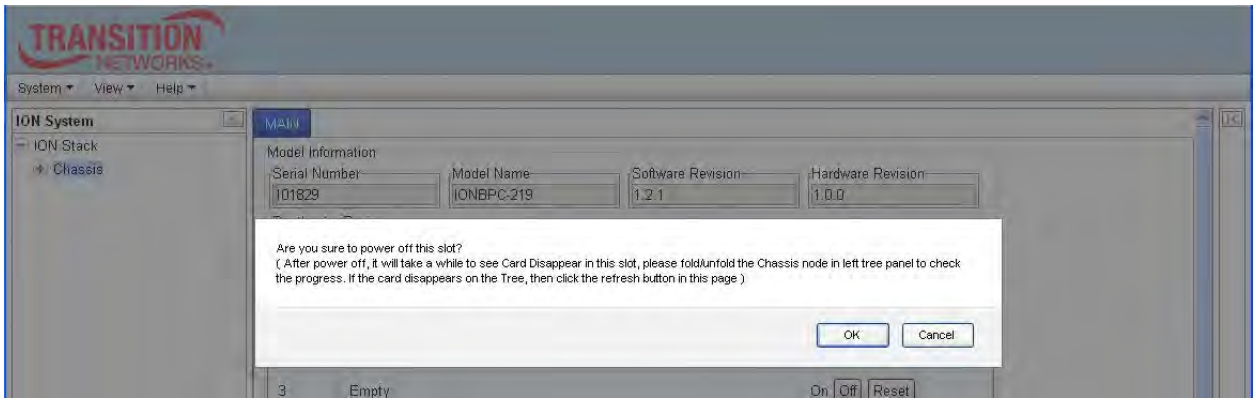
At the **Chassis** > **MAIN** tab, you can click the Reset button to reset power for the selected slot in the chassis. The message "*Are you sure to power reset this slot?*" displays.



After power reset it will take a while to see card change in this slot; fold/unfold the Chassis node in the tree panel to check the progress. If the card information changes on the Tree, then click the **Refresh** button on this page. If you are not sure that you want to reset this chassis, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.

Power Off a Slot

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



If you are 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/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 3: Configuration

General

After the x4110 has been installed and access has been established, the device and its ports must be configured to operate within your network. The configuration establishes operating characteristics of the device and the ports associated with the x4110.

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 *x4110 CLI Reference Manual*.

The operating characteristics that can be defined for the x4110 are:

- System name
- Features
  - Device Description
  - Data Rate Retiming
- Port setup
  - Circuit ID
- DMI (Diagnostic Monitoring Interface)
  - Rx Power Intrusion Threshold (µW)

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.

System Configuration

The system configuration defines:

- a name for the C4110
- a device description (optional)

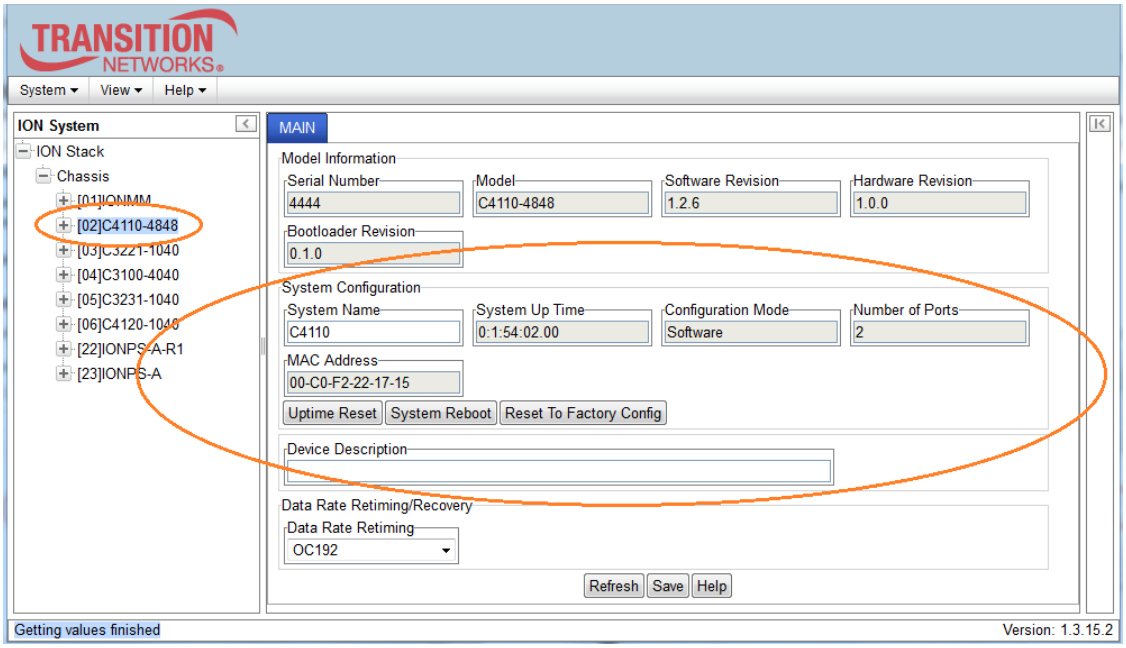
The entry for the system name must be a text string with no spaces between characters. Note that numbers, upper/lower case characters, and special characters (~!@#$%^&*()_+") are allowed.

The system configuration can be defined via the Web interface as described below.

System Configuration – Web Method

1. Access the x4110 via the Web interface.

2. At the device's **MAIN** tab, locate the **System Configuration** section.



3. In the **System Name** field, enter the name and for the x4110. The name can be alphabetic, numeric or a combination, but can not contain any spaces between the characters.

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

Device Description Configuration

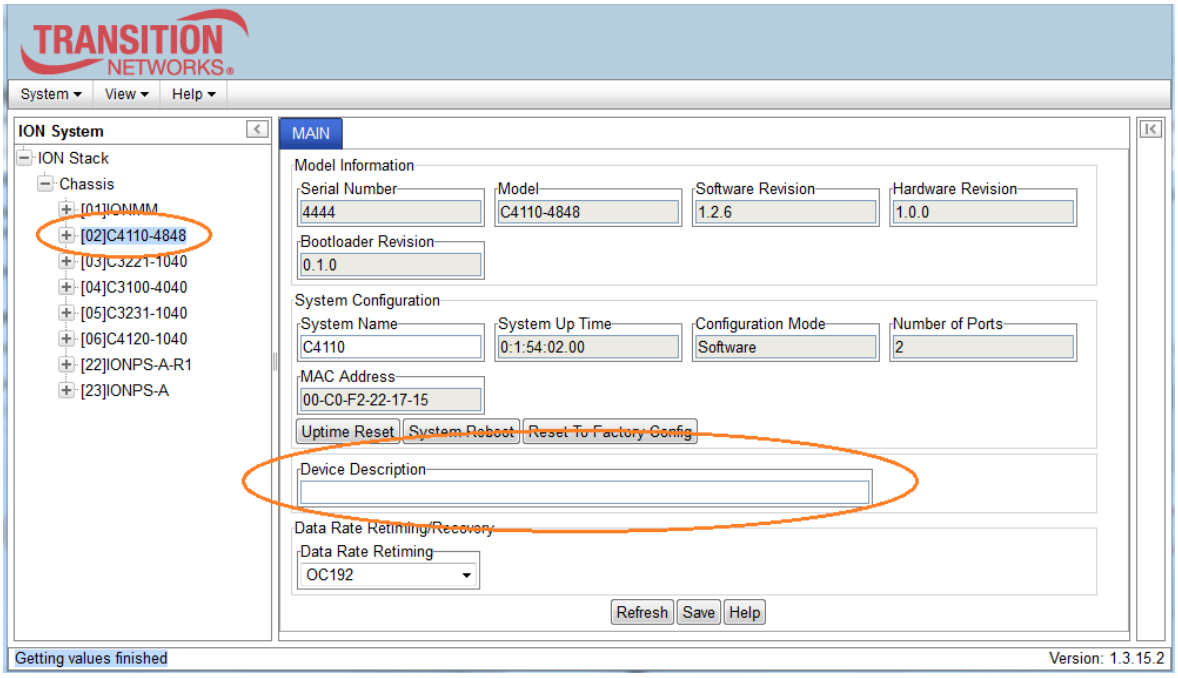
The x4110 supports a Device Description at the device level and a Circuit ID at the port level.

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 x4110 via the Web a follows.

Device Description Config – Web Method

1. Access the x4110 via the Web interface.
2. At the x4110 **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 Device Description 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 Device Description of 64 or fewer characters and click **Save**.
b) The message "*Setting values succeeded*" displays in the lower left corner of the Web interface.

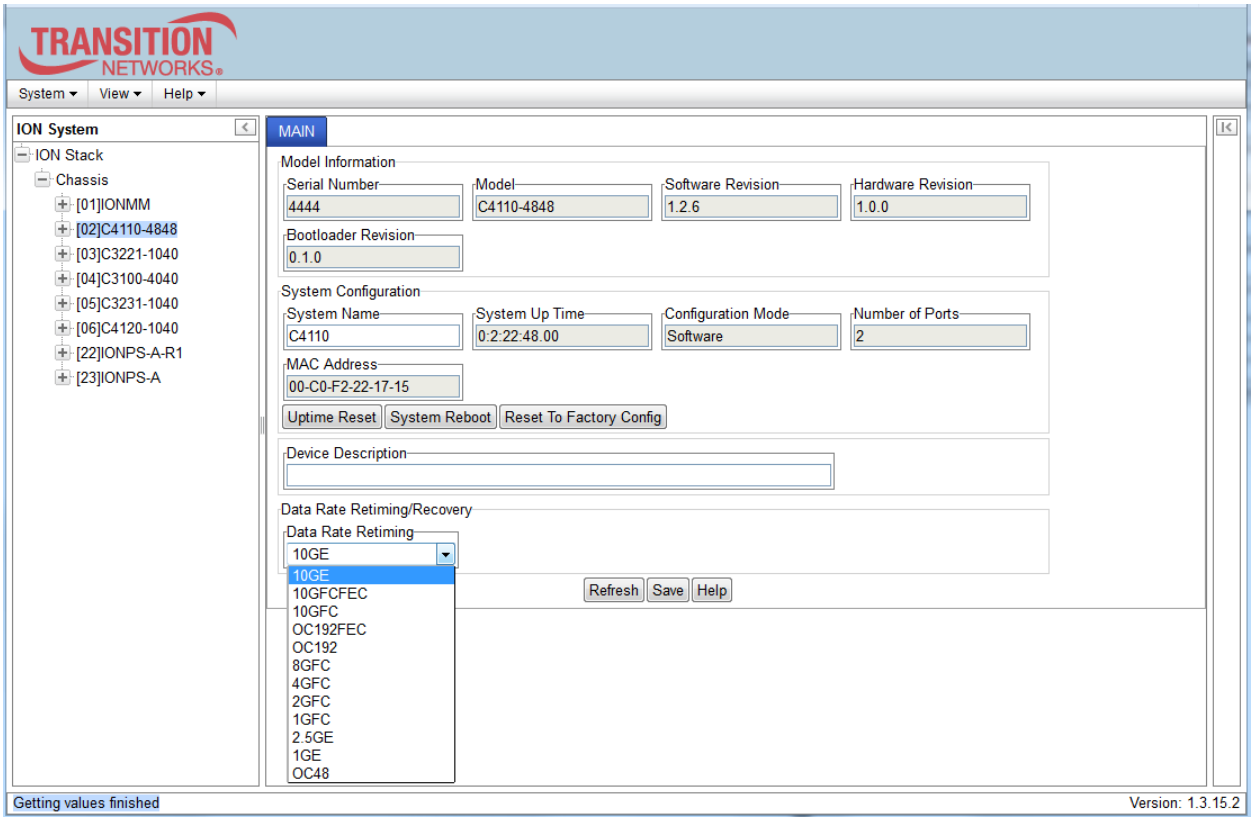
Data Rate Timing/Recovery Configuration

The C4110 can be used in applications where links supporting data rates from 1Gig to 10Gig require fiber extension or where 10Gig links require an interface between two fiber networks. It performs 3R (re-amplify, re-shape, re-time) signal regeneration. The S4110 is protocol 'agnostic', supporting a wide variety of protocols in a network; from 1 to 11.5Gbps, including 10G LAN, 10G WAN, 10G Fiber Channel, SONET OC192, 10G OTN (G.709), 1/2/4/8 Gig Fiber Channel, 1 Gig Ethernet, or Sonet OC-48. The fiber length and type is defined by the SFP+ module inserted.

The OC (Optical Carrier) specifies the speed of fiber optic networks conforming to the SONET standard. The speeds for common OC levels include OC-1 = 51.85 Mbps, OC-3 = 155.52 Mbps, OC-12 = 622.08 Mbps, OC-24 = 1.244 Gbps, OC-48 = 2.488 Gbps, OC-192 = 9.952 Gbps, and OC-255 = 13.21 Gbps.

Device Description Config – Web Method

1. Access the x4110 via the Web interface.
2. At the x4110 **MAIN** tab, locate the **Device Description** section.
3. At the dropdown, select the **Data Rate Retiming** value.



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

The Data Rate Retiming values are described below.

Table 4: Data Rate Retiming Values

Data Rate	Description
10GE	10 gigabit Ethernet (10GbE or 10 GigE) (factory default).
10GFCFEC	10GFC + FEC = 10GbE Fibre Channel with Forward Error Correction.
10GFC	10GbE Fibre Channel.
OC192FEC	WAN/OC-192+FEC = OC-192 network line with transmission speeds up to 9953.28 Mbit/s with Forward Error Correction.
OC192	WAN/OC-192 = OC-192 network line with transmission speeds up to 9953.28 Mbit/s.
8GFC	8G Fiber Channel with 8.5 gigabaud Line rate and 1,600 MBps throughput (at full duplex).
4GFC	4G Fiber Channel with 4.25 gigabaud Line rate and 800 MBps throughput (at full duplex).
2GFC	2G Fiber Channel with 2.125 gigabaud Line rate and 400 MBps throughput (at full duplex).
1GFC	1GbE Fibre Channel.
25GE	2.5 gigabit Ethernet.
1GE	1 gigabit Ethernet.
OC48	Sonet OC-48 network line with transmission speeds to 2488.32 Mbit/s.

Circuit ID Configuration

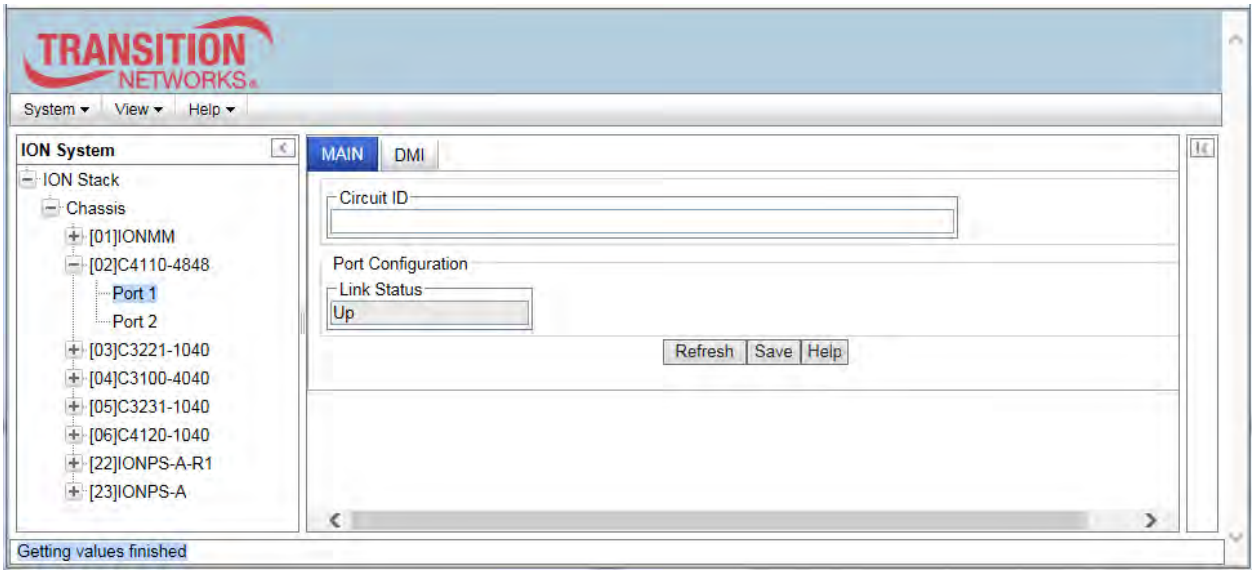
The x4110 supports a Device Description at the device level and a Circuit ID at the port level.

The Circuit ID provides the option to configure an ASCII text string up to 64 bytes and override the default information, which is vlan-module-port in binary format.

The Circuit ID can be configured in the x4110 via the Web as follows.

Circuit ID Config – Web Method

1. Access the x4110 via the Web interface (see "Starting the Web Interface").
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 **Save** 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:

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.

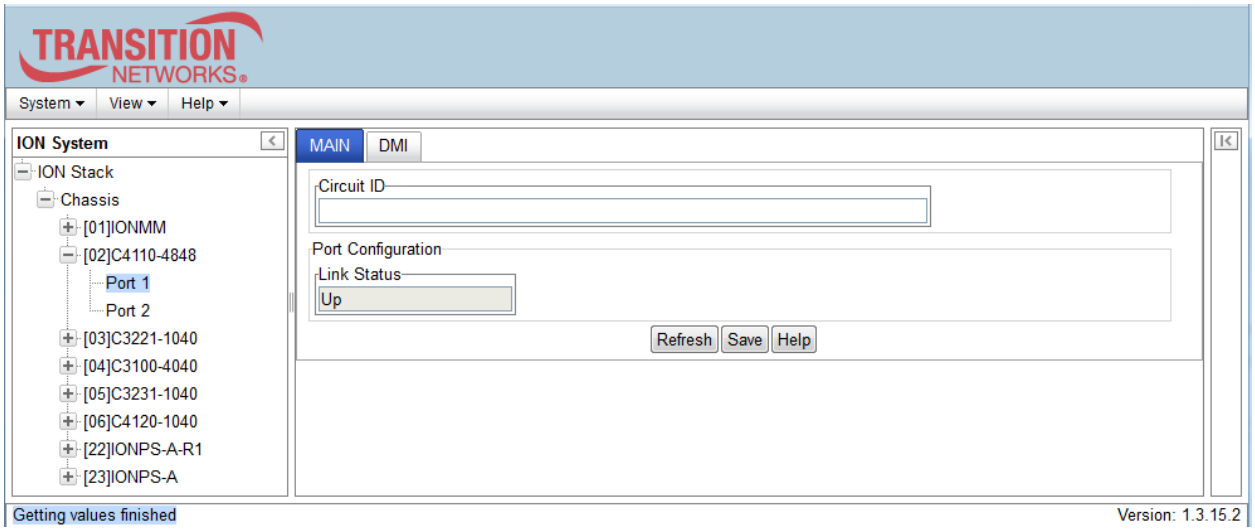
Ethernet Port Configuration

A port's Ethernet port speed and link status can be verified in the x4110 via the Web GUI as follows.

Ethernet Port Config – Web Method

Use this procedure to set the Circuit ID for the Ethernet port and to check the port's link status.

1. Access the x4110 via the Web interface.
2. Select the appropriate port.
3. Locate the **Port Configuration** section on the port's **MAIN** tab.



4. Check the Link Status parameter value (read only) for the current port's link status (**Up** or **Down**).
5. Click the **Refresh** button if necessary.

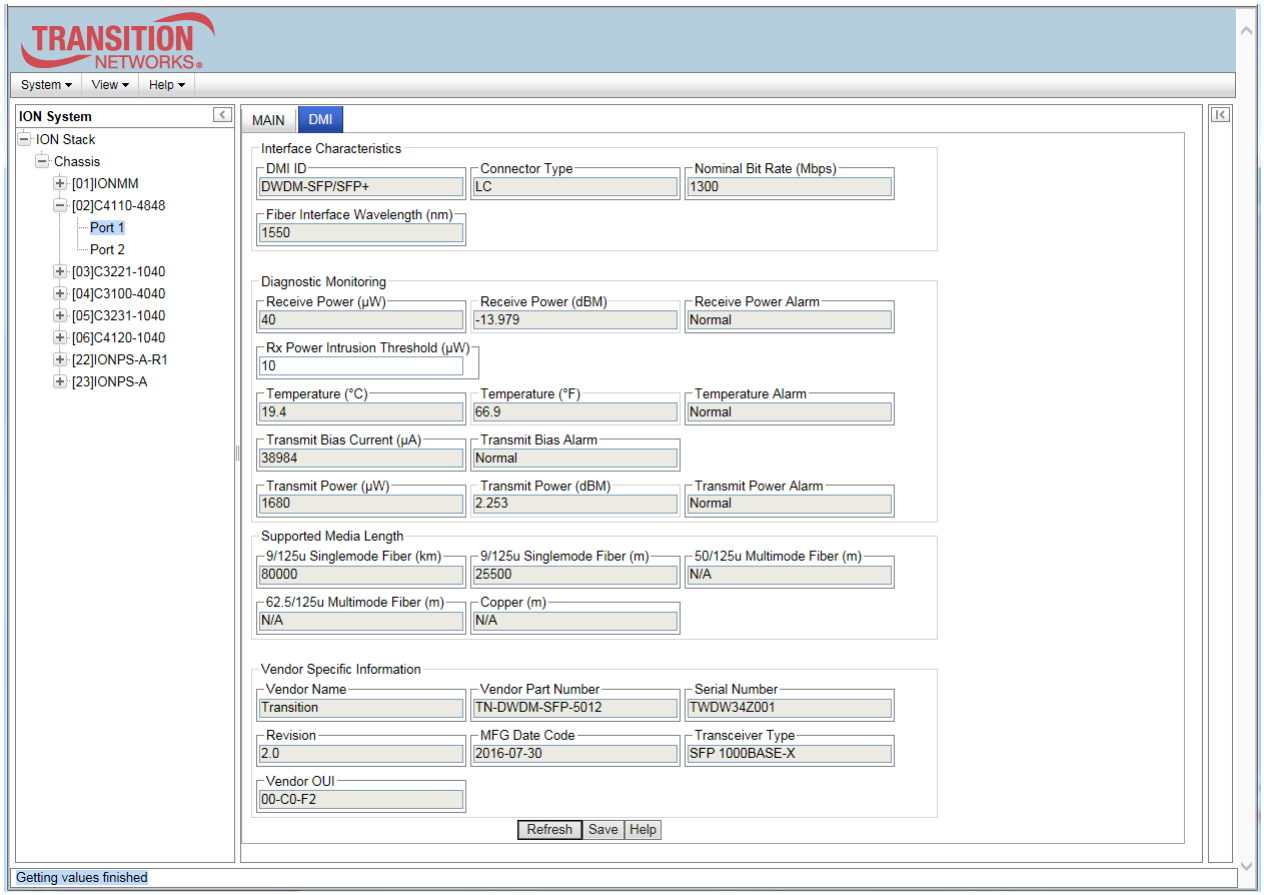
DMI (Diagnostic Maintenance Interface)

The DMI (Diagnostic Maintenance Interface) function displays x4110 SFP/SFP+ diagnostic and maintenance data such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. **Note**: Transition Networks SFPs that support DMI have a "-D" at the end of the model number. For more SFP/XFP information see the Transition Networks SFP product page.

DMI can be configured in the x4110 via the Web GUI as follows.

DMI Config – Web Method

1. Access the x4110 via the Web interface.
2. Select the desired device and port.
3. Select the **DMI** tab.



The Interface Characteristics, Diagnostic Monitoring, Supported Media Length, and Vendor Specific Information sections display. See the table below for parameter descriptions.

4. You can click the **Refresh** button to update the information displayed.
   You can click the **Save** button to save the updated information.

The **DMI** tab parameters are described in the table below.

Table 5: DMI Parameters

Parameter	Description
Interface Characteristics	
DMI ID	Specifies the physical DMI device ID from the standard; for example: SFP/SFP+/SFP28, SG, Optical pigtail, MPO 1x12 (Multifiber Parallel Optic) , MPO 2x16, Module/connector soldered to motherboard, SFP, 300-pin XBI , XENPAK, XFP, XFF, XFP-E, XPAK, X2, DWDM-SFP/SFP+, QSFP, QSFP+, CXP, Shielded Mini Multilane HD 4X or 8X, QSFP28, CXP2, CDFP (Style 1/Style 2), Shielded Mini Multilane HD 4X or 8X Fanout Cable, CDFP (Style 3), microQSFP, QSFP-DD Double Density 8X Pluggable Transceiver, HSSDC II, Copper Pigtail, RJ45 (Registered Jack), No separable connector, or MXC 2x16.
Connector Type	The external optical or electrical cable connector provided as the interface. For example: LC, SC, Dual BNC coax connectors, DB9 for RS232 and RS485, 6 Pos Terminal Block for RS485, RJ-11, unshielded twisted pair, SC fiber, 1550nm 40km, SC fiber, 1 x 9, 125km Gigiabit , ST Single-Fiber 155Mbps, 6-pin RS-485 Terminal Block, DIN 6-Pin for RS232, LC Multimode Fiber, SFP cage, 5 Pos Terminal Block for RS485, Single-Fiber Multimode, SC Multimode (long haul), LC Singlemode (long haul), XFP slot, or SFP+ slot.
Nominal Bit Rate (Mbps)	Bitrate in units of 100Mbps (for example: 10500, or 10.G Gbps) (measured rate).
Fiber Interface Wavelength (nm)	The Nominal transmitter output wavelength at room temperature (measured wavelength). The unit of measure is nanometers (for example: 1550 nm or 850 nm).
Diagnostic Monitoring	
Receive Power (uW)	Receive power (measured power measurement) on local fiber measured in microwatts (for example: 11 uW).
Receive Power (dBM)	Receive power (measured signal strength) on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. For example: -19.586 dBM.
Receive Power Alarm	Alarm status for receive power on local fiber: Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Rx Power Intrusion Threshold (uW)	A preset level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated (0-10). The message displays: *ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress*. See below for alarm recovery.
Temperature (˚C)	Measured temperature of fiber transceiver in tenths of degrees C (Celsius). For example: 30.1˚C.
Temperature (˚F)	Measured Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). For example: 86.2 ˚F.

Parameter	Description
Temperature Alarm	Alarm status for temperature of fiber transceiver. An *ionDMITemperatureEvt* event is sent when there is a warning or alarm on DMI temperature. Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Transmit Bias Current (uA)	Measured transmit bias current on local fiber interface, in uA (microamperes). For example, 5936 uA (microamps).
Transmit Bias Alarm	Alarm status for transmit bias current on local fiber interface. Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Transmit Power (uW)	Measured transmit power on local fiber measured in microwatts.For example, 240 uW (microwatts).
Transmit Power (dBM)	Transmit power on local fiber measured in dBM (decibels relative to one milliwatt) which defines signal strength. For example: -2.291 dBM.
Transmit Power Alarm	Alarm status for transmit power on local fiber. Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6 High Alarm - 7
Supported Media Length	
9/125u Singlemode Fiber (km)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is kilometers (km). For example, 8Km.
9/125u 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). For example, 80m.
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.
62.5/125u Multimode 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.
Copper (m)	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters.

Vendor Specific Information	
Vendor Name	A 16 character field that contains ASCII characters. The full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation. For example: Transition or other.
Vendor Part Number	A 16-byte field that contains ASCII characters, defining the vendor part number or product name. A value of all zeroes in the 16-byte field indicates that the vendor PN is unspecified. For example, TN-SFP-LX1, TN-SFP-BXD, TN-SFP-OC3M, TN-SFP-OC3S, TN-10GSFP-SR or similar. For a DWDM SFP, the xxxx indicates the center wavelength (e.g., for a TN-DWDM-SFP-5012, the 5012 indicates 1550.12 nm center wavelength laser support).
Serial Number	A 16 character field that contains ASCII characters, defining the vendor's serial number for the transceiver. A value of all zeroes in the 16-byte field indicates that the vendor SN is unspecified. For example: TWDW34Z001, 8800022, 102201102, or similar.
Revision	A 4-byte field that contains ASCII characters, defining the vendor product revision number. A value of all zeroes in the 4-byte field indicates that the vendor revision is unspecified. For example, 2.0.
MFG Date Code	An 8-byte field that contains the Vendor's date code in ASCII characters: 84-85 ASCII code, two low order digits of year (00 = 2000). 86-87 ASCII code, digits of month (01 = Jan through 12 = Dec). 88-89 ASCII code, day of month (01-31). 90-91 ASCII code, vendor specific lot code, may be blank. For example 2016-07-30.
Transceiver Type	The SFP transceiver type. For example: None, Not Supported, SFP 100FX, SFP 1000BASE-T, SFP 1000BASE-CX, SFP 1000BASE-SX, SFP 1000BASE-LX, SFP 1000BASE-X, SFP 2G5, SFP 5G, or SFP 10G.
Vendor OUI	The vendor Organizationally Unique Identifier field (Vendor OUI) is a 3-byte field that contains the IEEE Company Identifier for the vendor (e.g., 00-C0-F2). A value of all zeroes in the 3-byte field indicates that the Vendor OUI is unspecified.

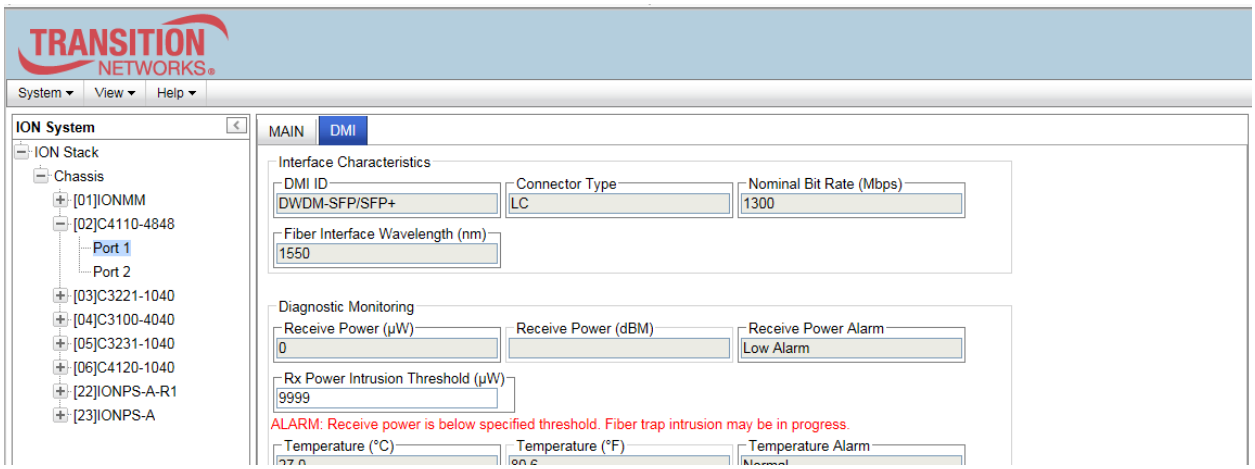
DMI Messages

***Message**: The DMI feature is not supported on current port.*

Meaning: C4110 port 2 DMI is not shown if there is no SFP in port 1. Without an SFP in port 1, the port 2 DMI will display "*The DMI feature is not supported on the current port.*". When an SFP is inserted into port 1, port 2 DMI data displays as expected.

Recovery: Insert an SFP in Port 1 and click the **Refresh** button.

***Message**: ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.*



Meaning: The setting for **Rx Power Intrusion Threshold (µW)** was exceeded. This is a configured 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.
Recovery: Check for an intrusion or change the Rx Power Intrusion Threshold setting to a differrent value. Click the **Save** button and click the **Refresh** button.

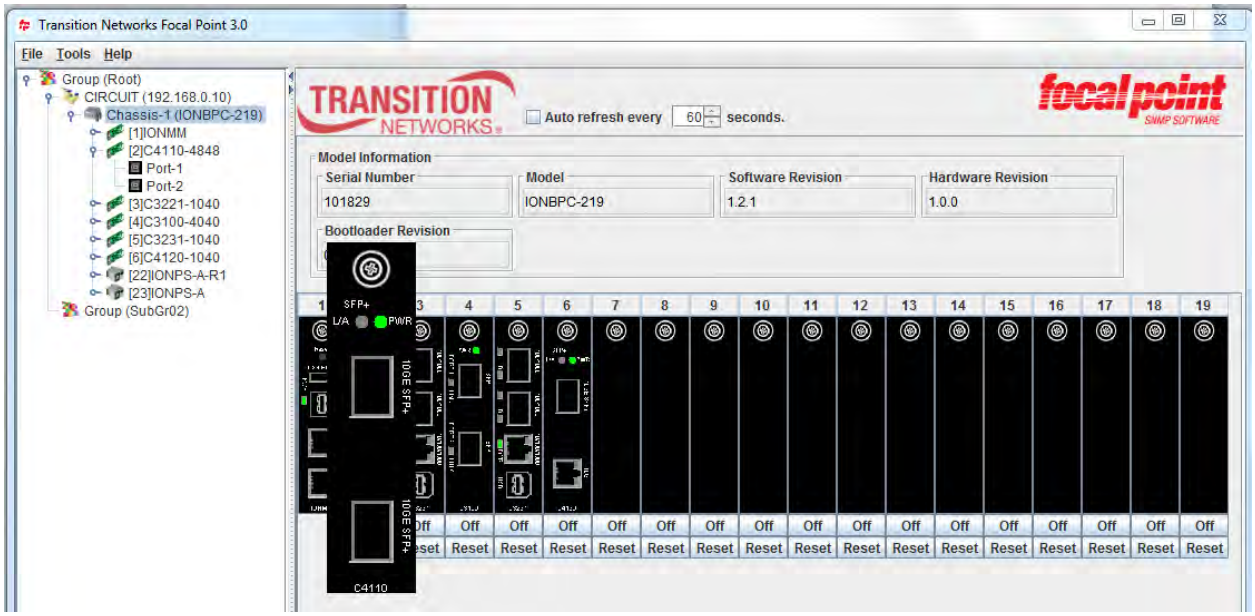
***Message**: Invalid input found!*
Meaning: You entered a parameter value outside of the valid range.
Recovery: Enter a valid parameter and continue operation.

***Message**: No changes to be saved*
Meaning: You clicked the **Save** button without changing any parameter values.
Recovery: Enter a valid parameter, click **Save**, and continue operation.

For More Information on topics such as Fiber Optics Power Measurements, Fiber and Cable Loss, OTDRs, Bandwidth, Reflectance/Optical Return Loss, and Fiber Optic Cleaning Procedures see the The Fiber Optic Association - Tech Topic in the FOA Guide to Optics and Premises Cabling on the FOA website at http://www.thefoa.org/tech/FAQS/FAQ-TEST.HTM#bw.

C4110 Support in Focal Point

C4110 firmware v1.2.6 adds Vendor Specific information to DMI and adds C4110 support in Focal Point, as shown below.



See the FocalPoint User Guide for more information.

Section 4: Operation

General

This section describes the non-configuration operations that can be performed for the x4110.

Backup and Restore Operations (Provisioning)

Using the Web interface you can back up and restore the configuration information for the IONMM and any or all of the x4110s in the ION system. See the *IONMM User Guide* manual for more information.

Displaying Information

There are several CLI commands that allow you to display (show) information about the x4110 configuration. For a complete description of these and other CLI commands see the *x4110 CLI Reference Manual*.

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 via the Web GUI as described below.

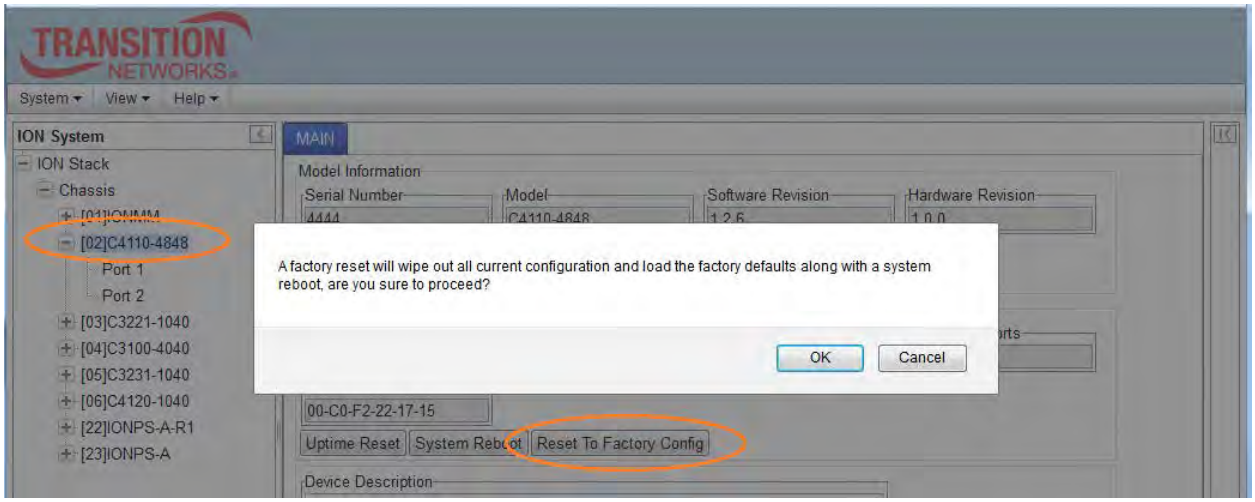
IMPORTANT

This operation deletes **all** configuration information that was saved in the IONMM, including the IP address you assigned to the IONMM.

Resetting Defaults – Web Method

Caution: This operation deletes all configuration information that was saved in the x4110, including the IP address you assigned to the x4110.

1. Access the x4110 via the Web interface.
2. Select the **MAIN** tab.
3. Locate the **System Configuration** section.



4. Click the **Reset to Factory Config** button. The message "*A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?*" displays.
5. Click **Cancel** if you are sure you want to proceed with the Reboot. Click **OK** only if you wish to reboot.

   All configuration parameters will be reset to their factory values. For a list of all factory defaults, see "Appendix B: Factory Defaults").

   Note: Your Web session will be discontinued.
6. Set the IP configuration (see "Doing the Initial System Setup").

File Status after Reset to Factory Defaults

The table below shows the status of x4110 files after a system re-boot.

Table 6: File Status after a Reset to Factory Defaults

File Type	Filename	File Description	Stored Directory	Status after Restore to Factory Default
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Lost
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	Restored to factory configuration
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	Restored to factory configuration
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	Restored to factory configuration
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	Restored to factory configuration
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	Restored to factory configuration (lost)
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	Lost
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	Restored to factory configuration (lost)

Resetting Uptime

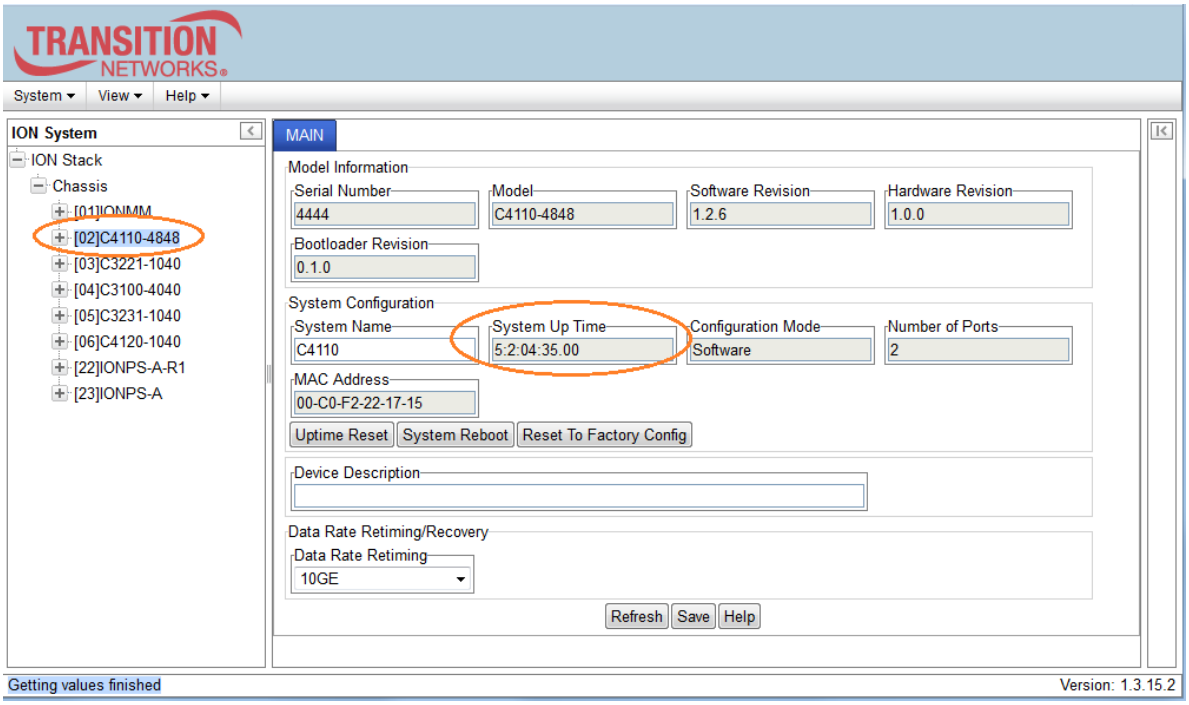
The x4110 system uptime field displays the amount of time that the x4110 has been in operation.

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.

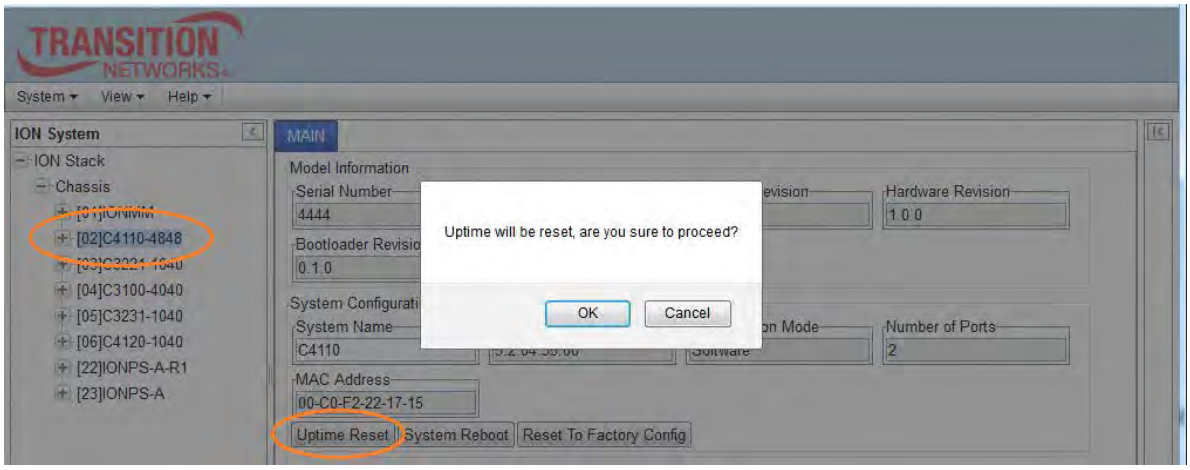
The ION **System Up Time** counter can be reset via the Web GUI as described below.

Reset System Uptime – Web Method

1. Access the x4110 via the Web interface.
2. At the **MAIN** tab, locate the **System Configuration** section.



3. If desired, observe and record the **System Up Time** field count. 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 device has been running for 9 days, 8 hours, 15 minutes, 18 seconds, and 26 milliseconds.
4. Click the **Uptime Reset** button to reset the counter to zero.



5. At the "*Uptime will be reset, are you sure to proceed*" message, click **OK** to reset the system up time.
6. The message "*Setting values succeeded*" displays at the bottom left of the screen when the up time reset is done.
7. Click the **Refresh** button at the bottom of the screen. The **System Up Time** field resets to zero, and immediately begins to increment.

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 11 in this section for file content and location after a System Reboot.

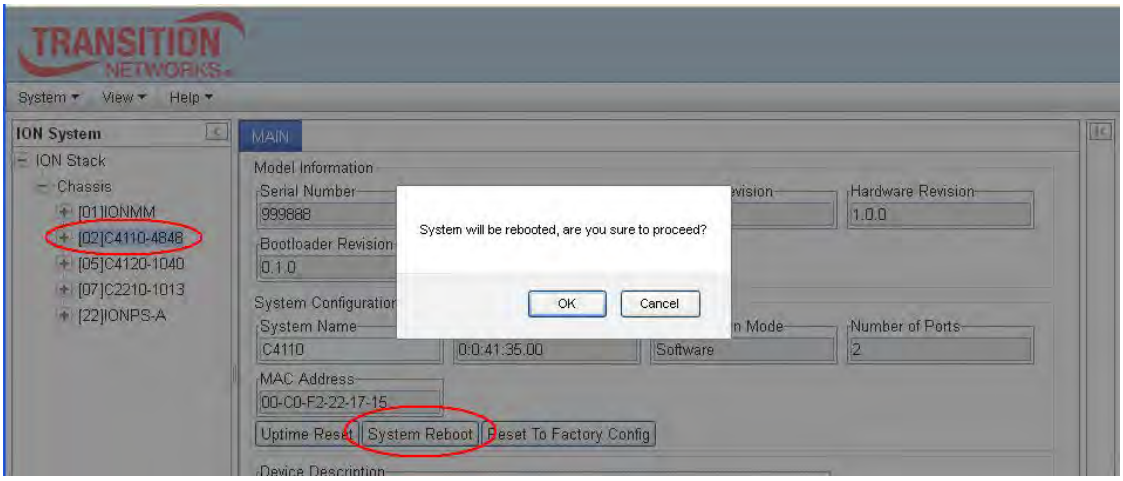
Doing a system reboot, restart, upgrade, or a reset to factory settings will cause all configuration backup files, HTTPS certification file, SSH key file, and Syslog file to be deleted.

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 x4110 via the Web interface.
2. Select the device’s 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 x4110 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 7: File Content and Location after a System Reboot

File Type	Filename	File Description	Stored Directory	Lost after Reboot? (Y/N)
Provisioning backup files	e.g., '1-1-IONMM.config'	These files are only used by provisioning Restore	/tftpboot	Yes
Net-SNMP configuration file	snmpd.conf	This file is a configuration file for Net-SNMP	/agent3/conf/snmp	No
HTTPS configuration file	lighttpd-ssl.conf	This file is a configuration file for HTTPS	/agent3/conf/lighttpd	No
HTTPS certification file	server.pem	HTTPS certificate	/agent3/conf/lighttpd	No
SSH host key	dropbear_rsa_host_key dropbear_dss_host_key	SSH host key files	/agent3/conf/lighttpd	No
SSH user key file	authorized_keys	Currently we have one 'root' user; this file is the user key file for 'root'	/root/.ssh	No
Syslog file	sys.log	The syslog file for IONMM	/tftpboot	No
MIB configuration files	e.g., 'agent3.conf' 'ifMib.conf'	The MIB configuration files for SNMP setting	/agent3/conf	No

Upgrade the IONMM and/or x4110 Firmware

Occasionally changes must be made to the firmware version that is currently stored in IONMM or x4110 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 management module has the latest firmware version installed and running. Keep your products up to date by downloading the latest firmware. You must log in or create an account to download firmware. For further assistance contact us at +1.952.358.3601, 1.800.260.1312, or at techsupport@transition.com.

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 the *IONMM User Guide* for details.

Section 5: Troubleshooting

General

This section provides basic and specific problem determination processes, and a description of problem conditions that may occur or messages that may be displayed. This section also documents ION system tests and x4110 and jumpers, and describes where and how to get technical support.

IMPORTANT

For each procedure described in this section, do each step sequentially as indicated. If the result of a step causes the problem to be corrected, **do not** continue with the other steps in the procedure.

Basic ION System Troubleshooting

This basic process is intended to provide some high-level techniques that have been found useful in isolating ION problems. This process is not a comprehensive guide to troubleshooting the ION system. The intent here is to 1) avoid missing any important information, 2) simplify analysis of captured information, and 3) improve accuracy in finding and explaining problem causes and solutions.

This basic process applies to these ION system and related components:

- ION Chassis
- ION x4110 (SICs, or slide-in-cards)
- IONMM (ION Management Module)
- 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 x4110s are seated properly, view the CLI **show** command output, verify IP addresses and Gateway IP address, check Windows Event Viewer, ping the interface, run the various tests if functional, etc.).
6. Write down your initial 2-3 guesses as to the cause of the problem.
7. Verify that the 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. Use the ION system manual procedure to retry the failed function or operation.
10. For the failed function or operation, verify that you entered valid parameters using the cursor-over-help (COH) and/or the ION system manual.
11. Based on the symptoms recorded, work back through each step in the process or operation to recall a point at which the problem occurred, and examine for a possible failure point and fix for each.
12. Document each suspected problem and attempted resolution; eliminate as many potential causes as possible.
13. Isolate on the 1-2 most likely root causes of what went wrong, and gain as much information as you can to prove the suspected cause(s).
14. If you find a sequence of actions that causes the problem to recur, replicate the full sequence several times and document it if possible.
15. Review your logged information and add any other comments that occur to you about what has taken place in terms of system behavior and suspected problem causes and solutions.
16. Review the "Recording Model Information and System Information" section on page 102 before calling TN for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

These message types and their recommended recovery procedures are covered in the following subsections.

LED Fault and Activity Displays

Refer to this section if the LEDs indicate a problem. For any LED problem indication:

1. Check the power cord connections and power outlet.
2. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
3. Make sure the USB cable is properly connected.
4. Check the power supply voltages (see related documentation).
5. Verify that the ION system devices have the latest firmware versions. Download the latest firmware version and upgrade as necessary.
6. Check if other network devices are working properly.

Power (PWR) LED is off (not lit):

1. Check for a loose power cord.
2. Check for a power supply failure. Replace power supply if failed.
3. Make sure all circuit protection and connection equipment and devices are working.
4. Verify that the ION system power supply is within operating range.
5. Remove the card from the chassis and re-insert it. Replace if failed.
6. Make sure the mode displayed matches the hardware setting on the device. See the "Jumper Settings" section.

L/A SFP+ LED off (not lit):

1. Check the data cables for obvious problems, incorrect type, incorrect wiring, etc.
2. See if the administrator has manually disabled the console device (PC) via the Web interface.
3. Check if other network devices are working properly.
4. Remove the suspect card from the chassis and re-insert it.
5. Check Auto-Negotiation setting.
6. See if the port transmission mode / speed (full or half-duplex, etc.) match those of the attached device.
7. Verify that the ION system devices have the latest firmware versions (see "Upgrade the Firmware" in the IONMM User Guide).
8. Download the latest firmware version and upgrade as necessary.

Problem Conditions

Cannot access the IONMM via Telnet
Cannot access the IONMM via the Web
Cannot access the IONMM via USB port
Management Module does not power on
Telnet connection is lost after a CLI command is executed
Upgrade fails
Upload fails
USB connection resets after a CLI command is executed

1. Verify that the default password has not been changed.
2. Check with your IT department that the network is up and running.
3. Refer to the IONMM User Guide for details.

Cannot access the x4110 via the Web Interface

1. Can you access the IONMM?

Yes	**No**
Continue with Step 2.	See "Cannot access the IONMM via the Web".

2. Power cycle the x4110.
3. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

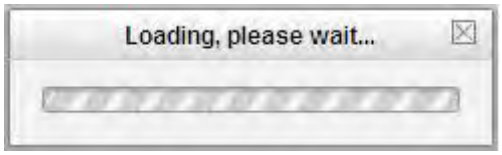
Configuration Mode Mismatch

On the device **MAIN** tab, in the **System Configuration** section in the **Configuration Mode** box, the mode displayed does not match the hardware setting on the device.

The device may have a jumper or switch that disables software management of the device. When Configuration Mode is **hardware**, the devices take some of the configurations from DIP switches or jumpers on the device. In **software** mode, configuration is controlled by management.

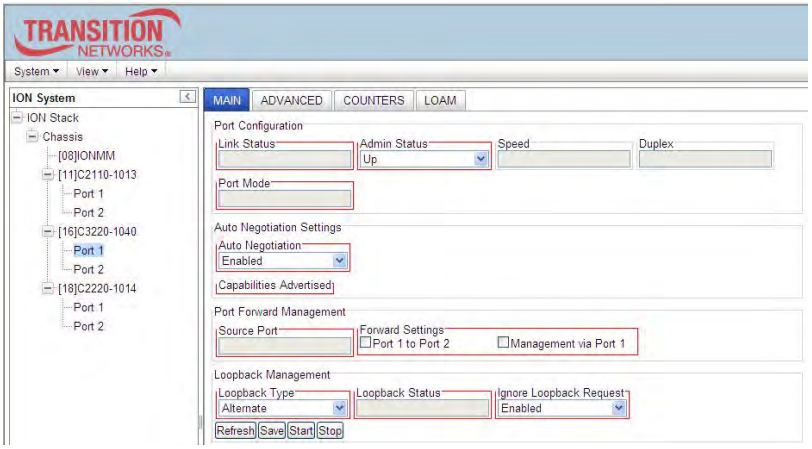
1. Refer to the "Jumper Settings" section of the Install Guide manual for details on hardware mode configuration.
2. Contact Transition Networks for more information. See "Contact Us" on page 80.

***loading, please wait ...* Displays continuously**



1. Wait for one or more minutes for the operation 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. See “Contact Us” on page 80.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



1. Check if the device is physically connected and powered on.
2. Verify the x4110 DIP swtch settings and HW/SW Jumper setting.
3. Refresh the IONMM or x4110 by clicking the **Refresh** button.
4. 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.
5. Cycle power for the module in question.
6. Upgrade the devices to the latest software version.
7. Reboot the device by clicking the **Reboot** key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
8. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Red box Condition after Reboot

When the reboot is finished, some devices (usually remote devices) will show the error condition of a "red box" around items like IP address, Trap Manager IP addresses, and/or DNS Entries. The ‘red box’ condition occurs while the devices are resetting; this condition can continue several minutes after the reboot. Until the system is ready to be fully managed, certain fields may display within "red boxes". The "red boxes" will disappear when the system is ready to be fully managed.

1. Wait a couple of minutes for the current operation to complete, and then continue operation.

2. Check the devices’ firmware versions. For example, a C4110 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 x4110 is at an older version and shows the newer functions as ‘red boxed’. Since the older version of x4110 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as ‘red boxed’. Upgrade the devices to the latest software version.

3. Reboot the system. See the “Reboot” section for more information.

4. Contact Transition Networks for more information. See “Contact Us” on page 80.

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. See “Contact Us” on page 80.

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. See “Contact Us” on page 80.

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. See “Contact Us” on page 80.

Windows XP Displays an Error and then Terminates Installation

If the following screen is displayed with this message, Windows XP has been configured to block the installation of any drivers that are not WHQL certified.

To successfully install the device, you must change the driver signing options to either warn or ignore in order to allow the installation to complete.

1. To change the current driver signing setting, in Windows XP, go to "Control Panel\System", click on the "Hardware" tab and then click "Driver Signing".
2. Select the desired signing option.

For other USB Driver / OS Messages (Win2K, Vista, Windows 7, Linux, Mac) refer to the separate document with Driver / OS install, uninstall and troubleshooting information.

Little indication of an IONPS-D Power Supply failure in Web interface
Meaning: If a power supply is powered down or loses input power, the only indication on the web interface is a Power reading of 0.0. The "Power Status OK" means that the Power Sensor is operating normally, not that the input power is OK.
Recovery: To check the loss of power, check at **IONPS-A** > **MAIN** tab > **Sensor and Fan(s)** section > **Power** value field.

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.

Problem: Bandwidth Ingress fault
Meaning: With rate set at 100Mbps with Full Duplex and Frame Size = 9216 a bandwidth Ingress fault occurs. When Ingress rate limiting is set at or below 512Kbps, the S322x will pass approximately 1 Mbps of traffic. At 768kbps and above rate limiting is working. This problem only happens on Ingress (not Egress) and only happens when connected at 100Mbps Full Duplex. Packets of 1518k or less work fine. This is a known hardware component limitation that only occurs when using very large Jumbo Frame (>5k) and very low bandwidth (≤512k).
Recovery: Change the rate, duplex mode, frame size, packet size, or Ingress Rate Limit. See the related section of this manual for details.

Web Interface Messages

IMPORTANT

For each procedure described below, do each step sequentially as indicated. If the result of a step causes the problem to be corrected, **do not** continue with the other steps in the procedure.

Cannot Ping IONMM Device

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails. The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic. The PC can then ping to the S2220-1013 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support.See “Contact Us” on page 80.

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. See “Contact Us” on page 80.

Getting values failed (snmp operation timeout)

This message indicates that you entered an invalid parameter value.

1. Click the **Refresh** button to clear the message.
2. Verify the recent parameter entries. Refer to the related CoH (cursor-over-help) and revise parameter entries as needed.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Failed to start Virtual Cable Test.

This message indicates that the VCT test could not be started.

1. Check the following:
   - Module has power.
   - Cable is properly connected to the port.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Firmware DB operation failed, unzip failed.

This message indicates that the upload of the upgrade file failed.

1. Check that the **db.zip** file (Windows XP) or **db** file (Windows 7) file was specified in the **Database File Name** field.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

invalid input file

This message displays in the "**Upload Result Reason**" field at **IONMM** > **Upgrade** tab> **Firmware database** sub-tab if the "Firmware File Name" entered had an incorrect filename format.

1. Verify the parameter value entered; see "Upgrading IONMM Firmware – Web Method" for valid input information.
2. Retry the operation with a valid firmware file name (e.g., *IONMM.bin.0.5.4*, or *x222x / x32xx.bin.0.5.4*).
3. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Invalid input found!

This message indicates that you entered a parameter outside the valid range (e.g., VLAN ID = 0).

1. Verify the parameter value to be entered; check the online Help for valid input information.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Invalid password!

This message indicates that the password entered during sign on is not valid.

1. Sign in using the correct password. The default password is **private**.
   Note: the password is case sensitive.
2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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 x4110 supports DMI.
2. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Admin Status: Down (or **Testing)**

In the device's port, at the MAIN tab in the Port Configuration section, the Admin Status field displays "Down". Typically, if 'Admin Status' is Down, then 'Link Status' is also Down.
The status here is the desired state of the interface. The "Testing" status indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with 'Admin Status' in the Down state. As a result of either explicit management action or per configuration information retained by the managed system, 'Admin Status' is then changed to either the Up or Testing states, or remains in the Down state.

1. Verify the initialization process; see "Section 2: Installation and System Setup".
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization to take place.
4. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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

This is the current operational state of the interface.
The 'Link Status' Testing state indicates that no operational packets can be passed.
If 'Admin Status' is Down then 'Link Status' likely will be Down.
If 'Admin Status' is changed to Up, then 'Link Status' should change to Up if the interface is ready to transmit and receive network traffic.
'Link Status' should change to Dormant if the interface is waiting for external actions (such as a serial line waiting for an incoming connection);
'Link Status' should remain in the Down state if and only if there is a fault that prevents it from going to the Up state;
'Link Status' should remain in the NotPresent state if the interface has missing (typically, hardware) components.

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

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see "Section 2: Installation and System Setup".
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization to take place.
5. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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 to take place, and then retry the operation.
2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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

1. Verify the ION system installation; see "Section 2: Installation and System Setup".
2. Wait several minutes for initialization to take place, and then retry the operation.
3. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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 to take place, and then retry the operation.
3. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

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. Try another operation.
3. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: *Web UI Management connection Lost*

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).
2. After reducing the "Egress Rate Limit" to "80m", the ping fails.
   The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.
3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic.
   The PC can ping to S2220-1013 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

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

The message “Setting values in progress ...” displays for over 10 minutes after you set up a VLAN 100, then set Management VLAN to Enabled and clicked Save.

Getting values failed (http server error) then displays.

Loading Template agent_main_view.htm failed displays:

MAIN tab displayed is blank after you close the Loading ... dialog box.

Meaning: These messages display after you turn on the Management VLAN function either via the ION Web interface or the CLI. (The CLI command is **set mgmt vlan state=enable**, and the Web interface is from the IONMM **MAIN** screen in the **Management VLAN Configuration** section, where the **Status** field is set to **Enabled**. In both cases, management control is given to the Management VLAN that you enabled.

The recovery (re-gaining control from the CLI or Web interface) is to turn off Management VLAN via the CLI (**set mgmt vlan state=enable**) or via the Web interface (IONMM **MAIN** > **Management VLAN Configuration** > **Status** > **Enabled**).

Message: Loading Template agent_main_view.htm failed
Loading htm files failed
Loading htm file succeeded
Loading JavaScript file failed
Loading Template Config file failed
Meaning: The status displays at the lower left corner during Port 1 page loading.
Recovery: 1.Wait for the *Loading, please wait...* message to clear. This may take 1 minute or more. 2. See the *Loading, please wait...* message for details. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: *The DMI feature is not supported on current port*

Meaning: Not all x4110 models support DMI. Transition Networks x4110s that support DMI have a "D" at the end of the model number. If you click the DMI tab on a x4110 model that does not support DMI, the message "The DMI feature is not supported on current port."

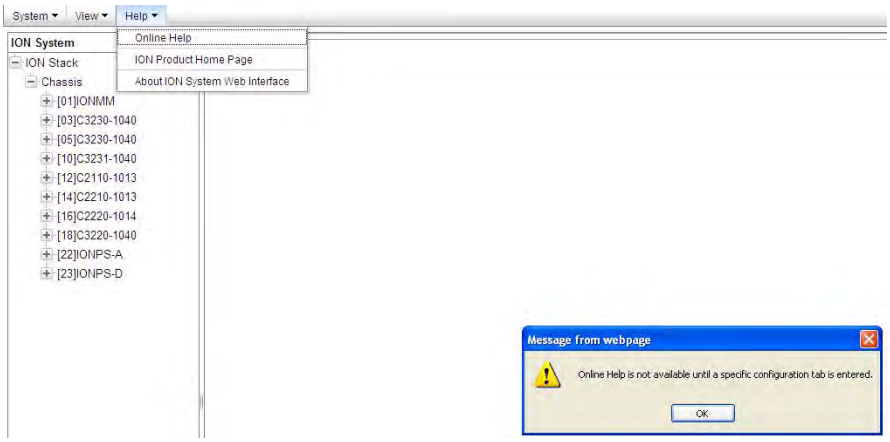
The DMI (Diagnostic Maintenance Interface) function displays x4110 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.

Recovery: 1. Verify that the device and port support DMI. See "DMI (Diagnostic Maintenance Interface) Parameters" for more information.

Message: Loading Template agent_main_view.htm failed
Message: Loading htm files failed
Meaning: The status displays at the lower left corner during Port 1 page loading.
Recovery: 1.Wait for the *Loading, please wait...* message to clear. This may take 1 minute or more. 2. See the *Loading, please wait...* message for details. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: Online Help is not available until a specific configuration is entered.

Meaning: You clicked on **Online Help** from the **Help** dropdown without first selecting a device.



Recovery:

1. Click the **OK** button to close the webpage message.
2. Select an ION device.
3. Click on **Help** > **Online Help** again.

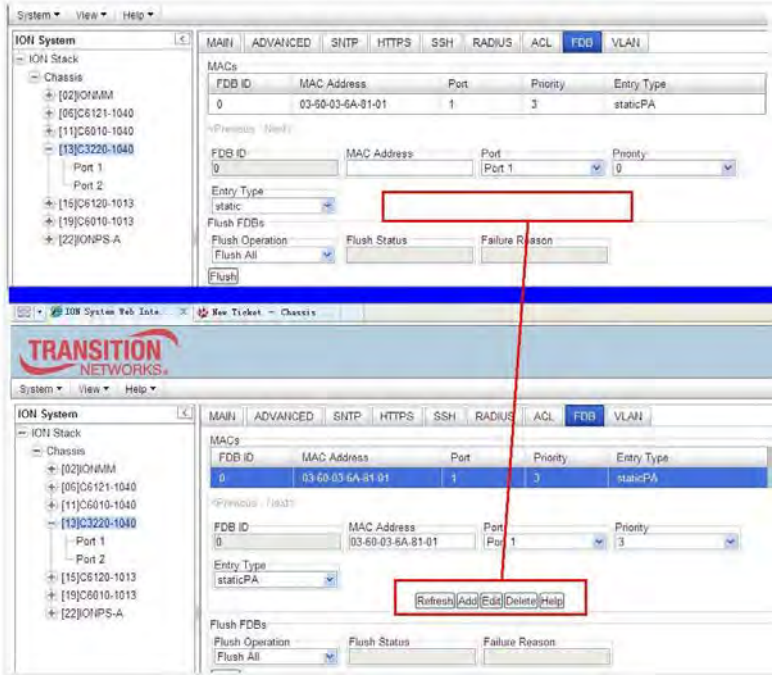
Message: Trap manager settings changed and a system reboot is required for the changes to take effect. – Do you want to reboot the system right now?
Meaning: Information only. At **IONMM > MAIN** > **SNMP Configuration** > **Trap Manager x** you entered an IP address for a trap server.
Recovery:
1. Click the **OK** button to clear the webpage message.
2. Verify the Trap Manager setting and continue operation.
3. If a problem persists, contact Technical Support. See “Contact Us” on page 80.

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. See "Contact Us" on page 80.

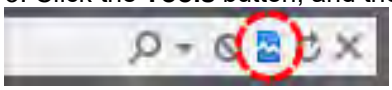
In IE8 or IE9, at C3220 > FDB, the 'Refresh', 'Add', 'Edit', 'Delete', 'Help' buttons of FDB do not display.



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.

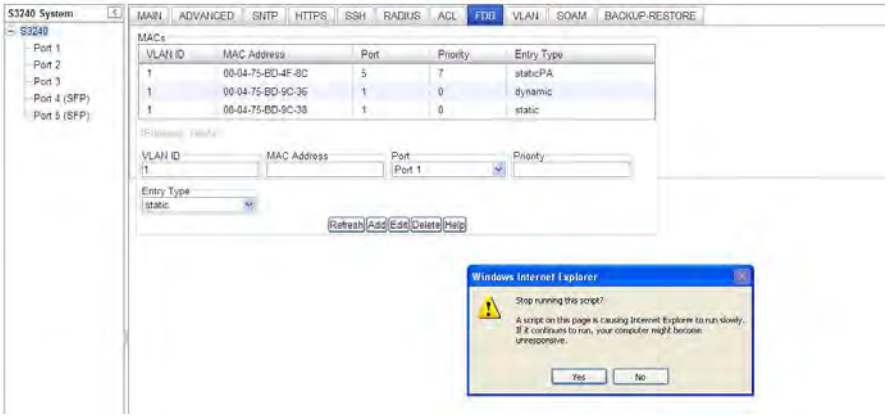
2. Log in to the ION system again.
3. Select the **FDB** tab.
4. Select at least one table of FDB, and then click the web page; the button will display normally.
4. Click one existing MAC address in the MAC address list.

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.
5. Check the Microsoft Support Online website http://support.microsoft.com/ph/807/en-us/#tab0 for more information.
6. See also: http://msdn.microsoft.com/en-us/library/dd567845%28v=vs.85%29.aspx
http://support.microsoft.com/kb/960321
http://blogs.msdn.com/b/ie/archive/2008/08/27/introducing-compatibility-view.aspx
7. In IE9, click the **Compatibility View** toolbar button on the Address bar to display the website as if you were using an earlier version of Internet Explorer. See the Microsoft Support website Article ID: 956197 at http://support.microsoft.com/kb/956197.

Script error message received.
Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No
Error: Object doesn't support this property or method.
A Runtime Error has occured. Do you wish to Debug?
Done, but with errors on page.



1. Click the **Yes** button to stop the script.
2. Click **Show Details** to display error details.
3. Disable script debugging.
4. Test a Web page from another user account, another browser, and another computer.
5. Verify that Active Scripting, ActiveX, and Java are not being blocked by Internet Explorer.

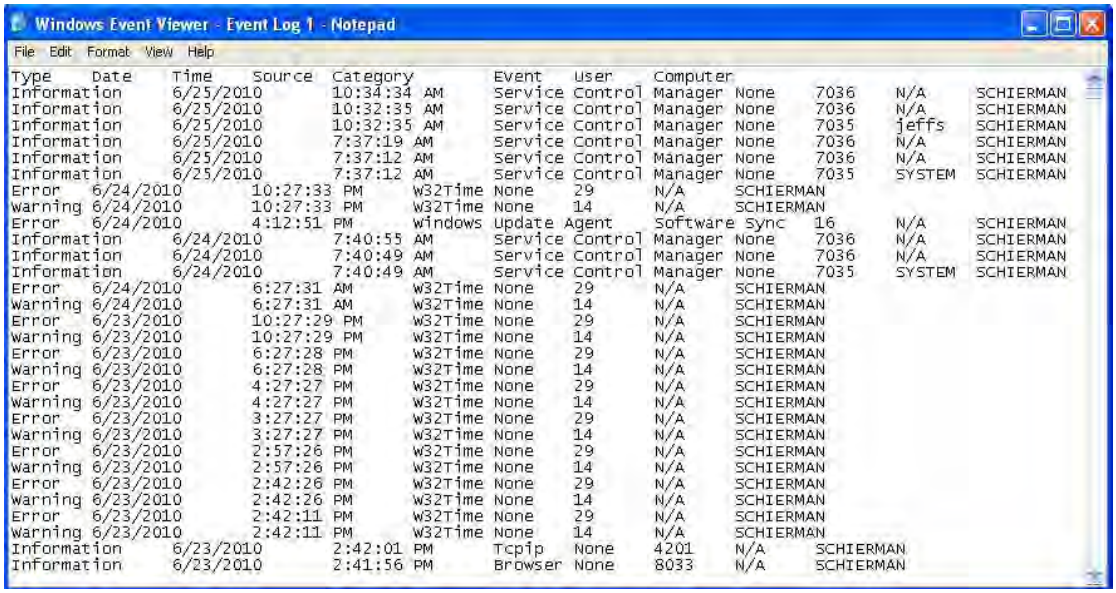
6. Remove all the temporary Internet-related files.
7. Install the latest Internet Explorer service pack and software updates.
8. For more advanced troubleshooting, see the Microsoft Support Article ID 308260 at http://support.microsoft.com/kb/308260.

Message: Getting card hardware mode failed
Meaning: The x4110 is in Hardware mode and you tried to perform a Software operation.
Recovery:

1. Change the mode to Software mode.
2. See the "Field-configurable DIP Switch (SW1) and Jumper (J9)" section of the C4110 Install Guide manual.
3. Contact TN Technical Support. See "Contact Us" on page 80.

Windows Event Viewer Messages

A sample Event Log file is shown below.
Windows Event Viewer - Event Log 1:



Message: `Information 6/25/2010 7:37:12 AM Service Control Manager None 7035 SYSTEM`
Meaning: Information message regarding SCM.
Recovery: No action required.

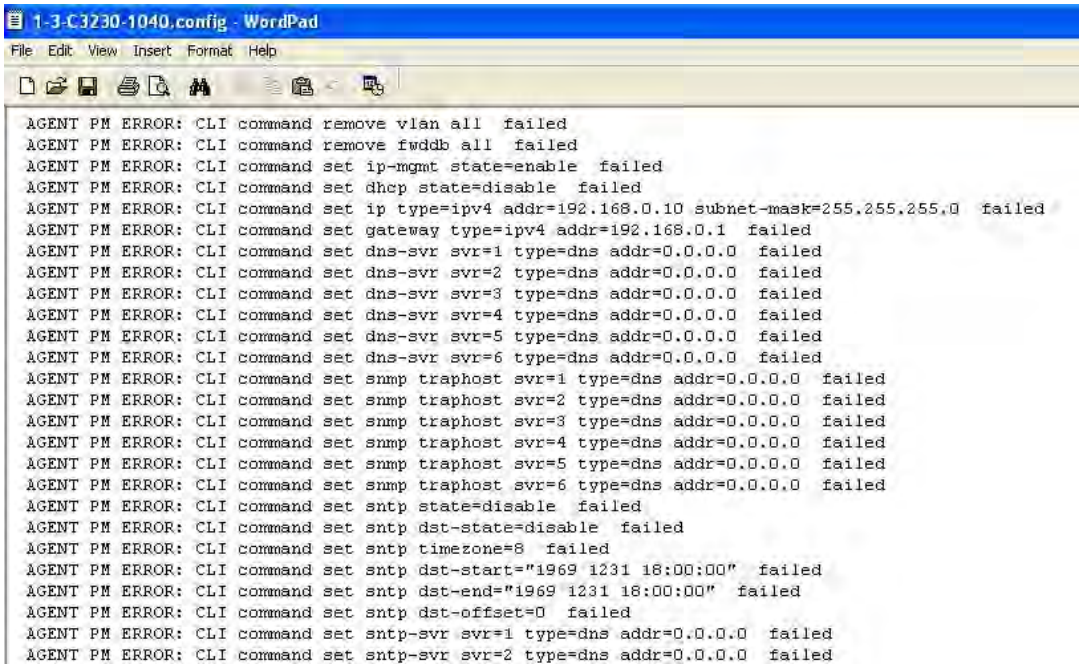
Message: `Error 6/24/2010 10:27:33 PM W32Time None 29 N/A SYSTEM`
Meaning: Error level message regarding W32Time.
Recovery: Open the file, examine the number of messages like this, and the potential problem level.

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. See "Contact Us" on page 80.

The Config Error Log (config.err) File

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

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



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

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

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

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

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

The final word in the message line is the word “failed”.

config.err Messages

Sample config.err file information is provided below.

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

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

config.err Message Responses

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

Message: `remove vlan all  failed`

Response: 1. Check if this is a recurring problem. 2. Verify the VLAN operation in the related section of this manual. Retry the VLAN operation. 3. See the related VLAN command in the *x4110 CLI Reference Manual, 33497*. 4. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `remove fwddb all  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set ip-mgmt state=enable  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set dhcp state=disable  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

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 *x4110 CLI Reference Manual, 33497*. 4. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

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 x4110 CLI Reference Manual, 33497*. 4. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set dns-svr svr=1 type=dns addr=0.0.0.0  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set snmp traphost svr=1 type=dns addr=0.0.0.0  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set sntp state=disable  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set sntp dst-state=disable  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set sntp timezone=8  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set sntp dst-end="1969 1231 18:00:00"  failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

Message: `set sntp dst-offset=0 failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set sntp-svr svr=1 type=dns addr=0.0.0.0 failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set radius client state=disable failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set radius svr=1 type=dns addr=0.0.0.0 retry=3 timeout=30 failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `add vlan-db vid=100 priority=0 pri-override=disable failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `add vlan-db vid=200 priority=0 pri-override=disable failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set acl state=disable failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `set acl table=filter chain=input policy=accept failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: `AGENT PM ERROR: CLI command show dot1dbridge ip-tc priority remapping failed`

Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

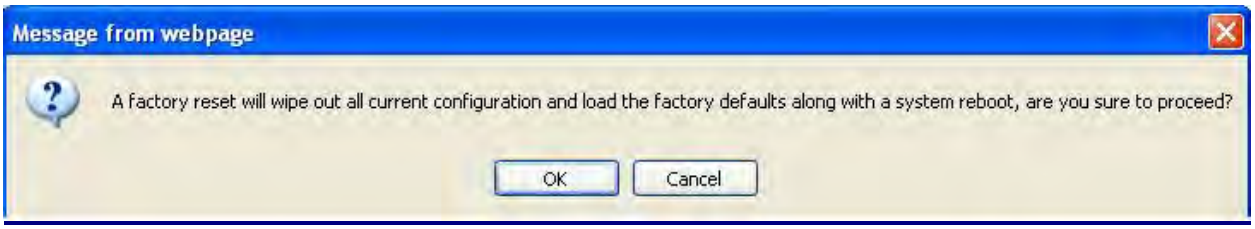
Webpage Messages

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 Descriptions".

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

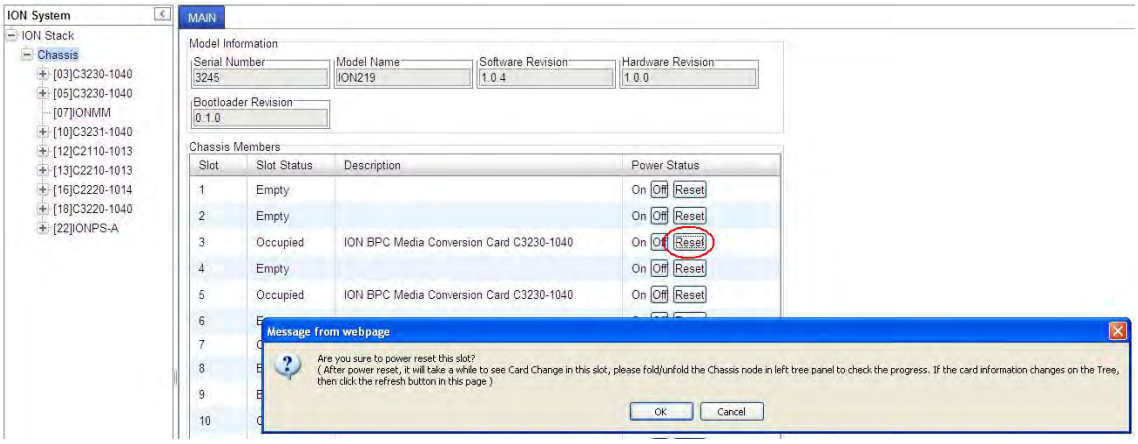
Response: Click **OK** only if you wish to reboot. Otherwise click **Cancel**.

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: *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.*)

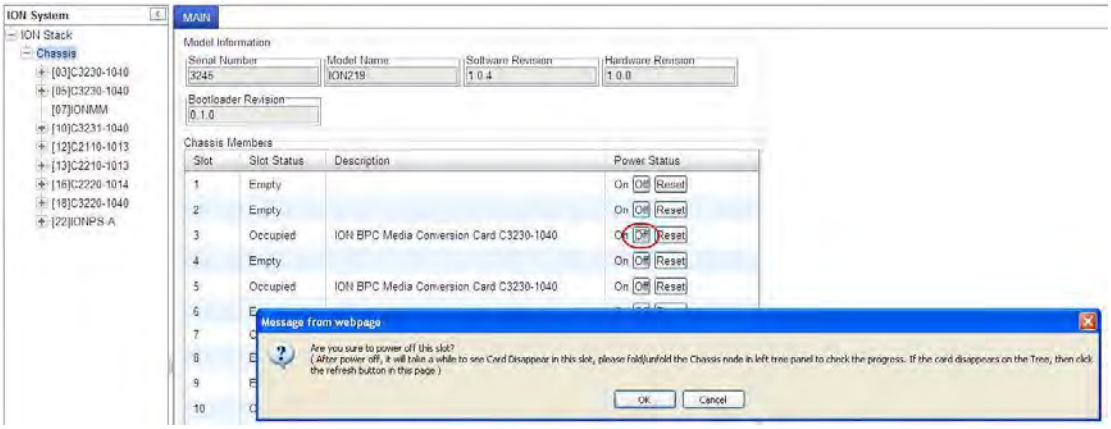


Meaning: A caution message generated at the **Chassis** > **MAIN** tab. You clicked the **Reset** button for a particular slot.

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 "Menu System Descriptions".
6. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: *Are you sure you want to power off this slot? (After power off, it will take a while to see Card Disappear in this slot; please fold/unfold the Chassis node in the left tree panel to check the progress. If the card information changes on the Tree, then click the Refresh button on this page.*)



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

1. **Recovery**: If you are not sure that you want to power off this slot, click the **Cancel** button to clear the message and return to normal operations without resetting power to this slot.
2. If you are sure that you want to power off this slot, click the **OK** button to clear the message and remove power to the slot.
3. At the **Chassis** > **MAIN** tab, fold/unfold the Chassis node in the tree panel to check the progress.
4. If the card information changes on the Tree, then click the **Refresh** button on this page.
5. See "Menu System Descriptions".
6. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

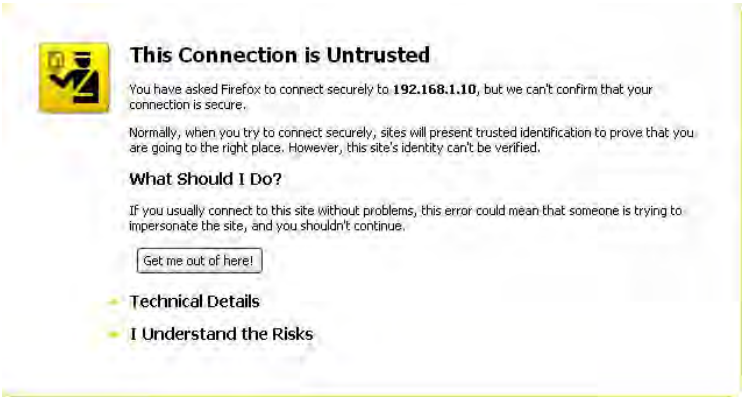
Message: *The Connection was Reset*

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 in the expected location.
3. Click the **Try again** button to retry the operation.

Message: *This Connection is Untrusted*



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

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

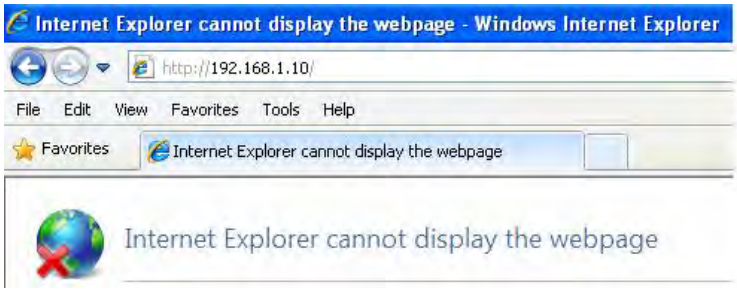
Message: *Local Area Connection x – A network cable is unplugged*

Meaning: You unplugged the USB cable at the x4110 or IONMM, or the x4110 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 x4110's USB connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: *Problem loading page – Mozilla Firefox*

Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.
Recovery:
1. Make sure the web browser you are using is supported. See "Web Browsers Supported".
2. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI".
3. Verify x4110 access. See "Accessing the x4110".
4. Verify the IP address setting. See "Setting the IP Addressing".
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

Message: *Internet Explorer cannot display webpage*



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

1. Make sure the web browser you are using is supported. See "Web Browsers Supported".
2. Verify the URL entered. See "Initial Setup with a Static IP Address via the CLI".
3. Verify NID access. See "Accessing the x4110".
4. Verify the IP address setting. See "Setting the IP Addressing".
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support. See "Contact Us" on page 80.

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. The web site information was accurate at the time of publication, but may have changed in the interim.

- Ipconfig and ifconfig
- Windows Network Connections
- Ping
- Telnet
- PuTTY
- Tracert (Traceroute)
- Netstat
- Winipcfg
- Nslookup
- Dr. Watson

Note: IETF RFC 2151 is a good source for information on Internet and TCP/IP tools at ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt.

Ipconfig

Ipconfig (Windows Vista): Use the procedure below to find your IP address, MAC (hardware) address, DHCP server, DNS server and other useful information under Windows Vista.

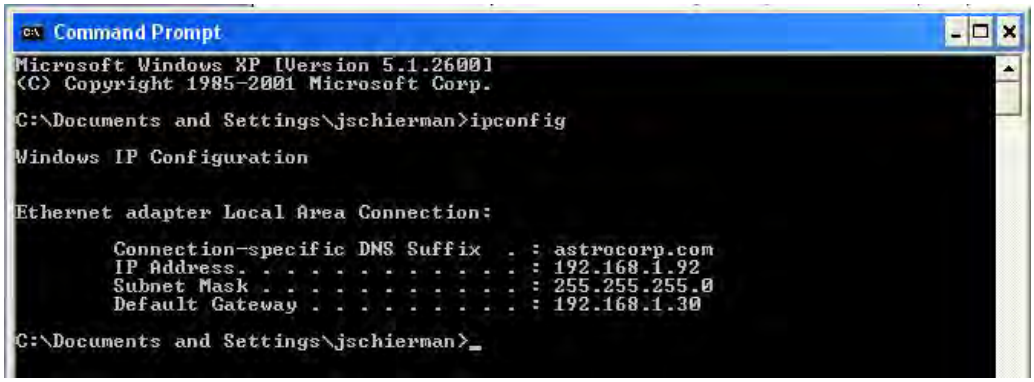
1. Go to the start menu and type **command** in the box.
2. Right-click on Command Prompt and click **Run as administrator**. If a User Account Control window pops up, click **Continue**.
3. At the **C:\>** prompt type **ipconfig** and press **Enter**. Your IP address, subnet mask and default gateway display. If your IP address is 192.168.x.x, 10.x.x.x, or 172.16.x.x, then you are receiving an internal IP address from a router or other device.
4. For more detailed information, type **ipconfig /all** at the prompt. Here you can get the same information as **ipconfig** plus your MAC (hardware) address, DNS and DHCP server addresses, IP lease information, etc.

Note: If you are receiving a 169.254.x.x address, this is a Windows address that generally means your network connection is not working properly.

Ipconfig (Windows XP): **ipconfig** (Internet Protocol Configuration) in Windows is a console application that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.

Use the **ipconfig** command to quickly obtain the TCP/IP configuration of a computer.

1. Open a Command Prompt. Click Start, point to Programs, point to Accessories, and then click Command Prompt.
2. Type **ipconfig** and press Enter. The Windows IP Configuration displays:



3. Make sure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
4. For more information, use the /all parameter (type **ipconfig /all** and press **Enter**).

The **ipconfig** command is the command-line equivalent to the **winipcfg** command, which is available in Windows ME, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the **winipcfg** command; however, you can get the equivalent functionality for viewing and renewing an IP address using Windows' Network Connections (see below).

ifconfig

1. Verify that the machine's interfaces are up and have an IP address using the **ifconfig** command:

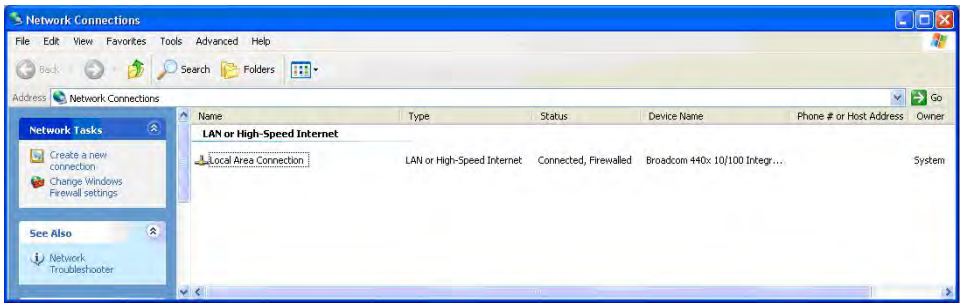
```
[root@sleipnir root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:6E:0A:3D:26
          inet addr:192.168.168.11  Bcast:192.168.168.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13647 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12020 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:7513605 (7.1 Mb)  TX bytes:1535512 (1.4 Mb)
          Interrupt:10

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8744 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:892258 (871.3 Kb)  TX bytes:892258 (871.3 Kb)
```

The above machine is running normally. The first line of output shows that the Ethernet interface eth0 has a layer 2 (MAC or hardware) address of 00:0C:6E:0A:3D:26. This confirms that the device driver is able to connect to the card, as it has read the Ethernet address burned into the network card's ROM. The next line shows that the interface has an IP address of 192.168.168.11, and the subnet mask and broadcast address are consistent with the machine being on network 192.168.168.0.

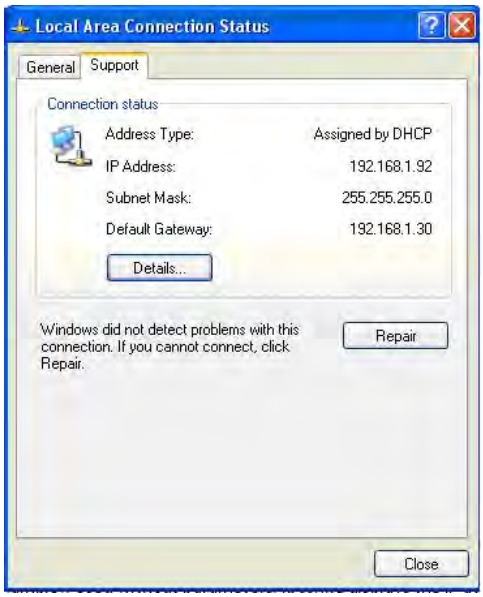
Windows Network Connections

In Windows XP you can view and renew an IP address using Windows Network Connections.

1. Open Network Connections from **Start** → **Settings** → **Network Connections**.



2. Right-click a network connection.
3. Click **Status**.
4. Click the **Support** tab. Your connection status information displays.

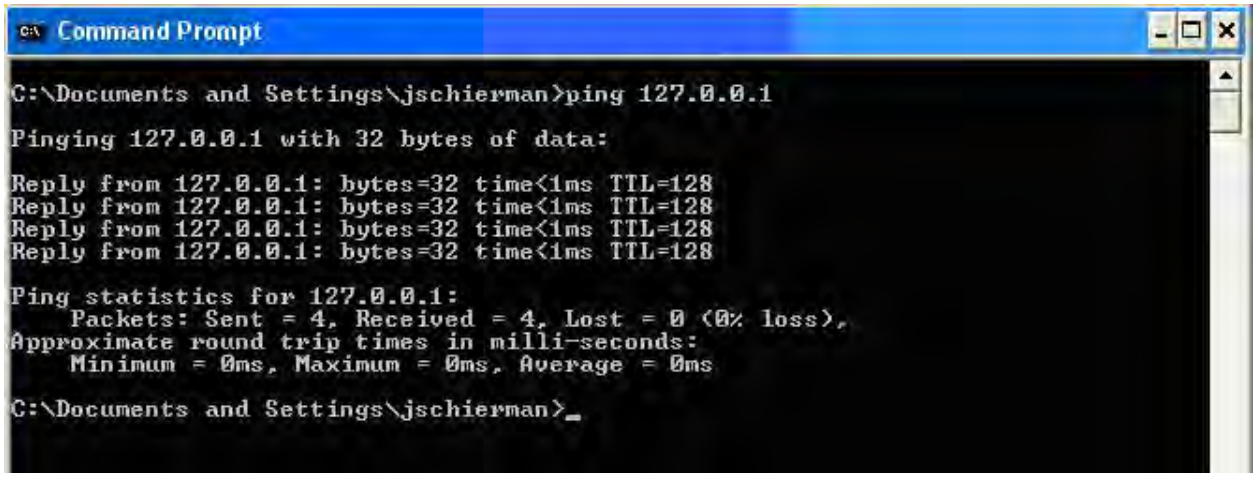


5. Click the **Details** button to display the Physical Address, IP Address, Subnet Mask, Default Gateway, DHCP Server, Lease Obtained, Lease Expires, and DNS Server addresses.

Ping

Use the **ping** command to test a TCP/IP configuration by using the ping command (in Windows XP Professional in this example). Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

1. Open a Command Prompt**.** To open a command prompt, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, ping the loopback address by typing **ping 127.0.0.1**.



3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the **ping** command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host on a different subnet). If the **ping** command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server. If the **ping** command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

If the **ping** command is not found or the command fails, you can use Event Viewer to check the System Log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.

The **ping** command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

Telnet

Telnet is a simple, text-based program that lets you connect to another computer via the Internet. If you've been granted the right to connect to that computer by that computer's owner or administrator, Telnet will let you enter commands used to access programs and services that are on the remote computer, as if you were sitting right in front of it.

The Telnet command prompt tool is included with the Windows Server 2003 and Windows XP operating systems. See the related OS documentation and helps for more information. Note that if you are only using computers running Windows, it may be easier to use the Windows Remote Desktop feature. For more information about Remote Desktop, see the related OS documentation and helps.

Telnet Client

By default, Telnet is not installed with Windows Vista or Windows 7, but you can install it by following the steps below.

To install Telnet Client:

1. Click the **Start** button, click **Control Panel**, click **Programs**, and then select **Turn Windows features on or off**. If prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In the **Windows Features** dialog box, check the **Telnet Client** checkbox.
3. Click **OK**. The installation might take several minutes.

After Telnet Client is installed, open it by following the steps below.

To open the Telnet Client:

1. Clicking the **Start** button, type **Telnet** in the Search box, and then click **OK**.
2. To see the available telnet commands, type a question mark (**?**) and then press **Enter**.

Telnet Server

In Windows Server 2003 for most Telnet Server functions, you do not need to configure Telnet Server options to connect a Telnet client to the Windows Server 2003-based Telnet Server. However, in Windows Server 2003 you must configure Telnet Server options to be able to do certain functions.

For example, the following command uses the credentials of the user who is currently logged on to the client to create a Telnet connection on port 23 with a host named server01.

telnet server01

The following example creates the same Telnet connection and enables client-side logging to a log file named c:\telnet_logfile.

telnet -f c:\telnet_logfile server01

The connection with the host remains active until you exit the Telnet session (by using the **Exit** command), or you use the Telnet Server administration tool to terminate the Telnet session on the host.

For more information, see the Windows Server TechCenter at http://technet.microsoft.com/en-us/library/cc787407(WS.10).aspx.

1. If you try to enable and install Telnet in Windows 7, and the message "*An error has occurred. Not all of the features were successfully changed*" displays, one workaround is to use a third party Telnet client, such as PuTTY, which also supports recommended SSH client.

PuTTY

PuTTY is a simple, free, but excellent SSH and Telnet replacement for Windows 95/98/NT.

The PuTTY SSH and telnet client was developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is developed and supported by a group of volunteers. PuTTY has been ported to various other operating systems. Official versions exist for some Unix-like platforms, with on-going ports to Mac OS and Mac OS X.

The PuTTY terminal emulator application also works as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols.

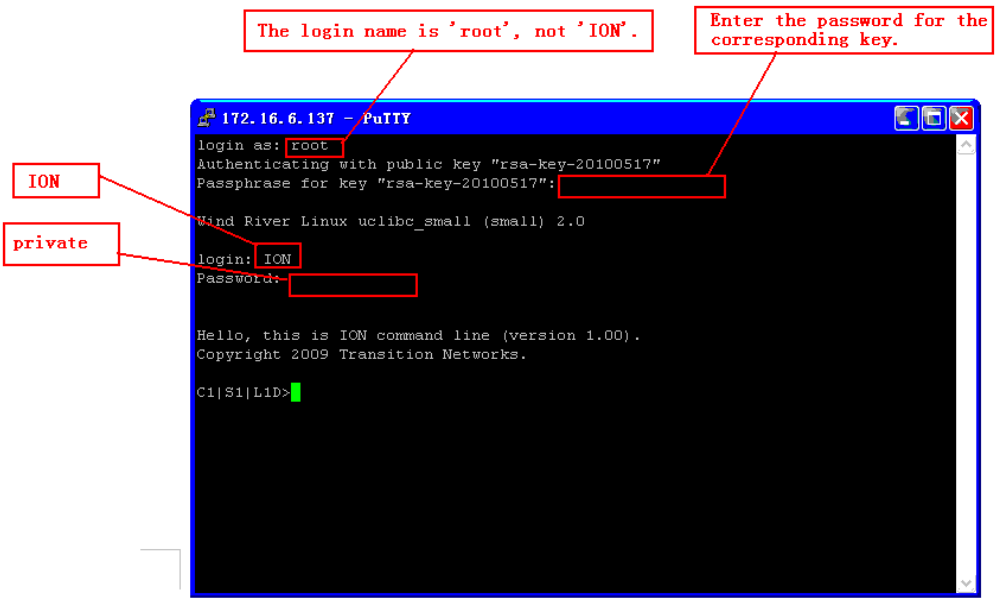
For PuTTY legal and technical details, see the PuTTY download page at http://putty.org/ or at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Note:

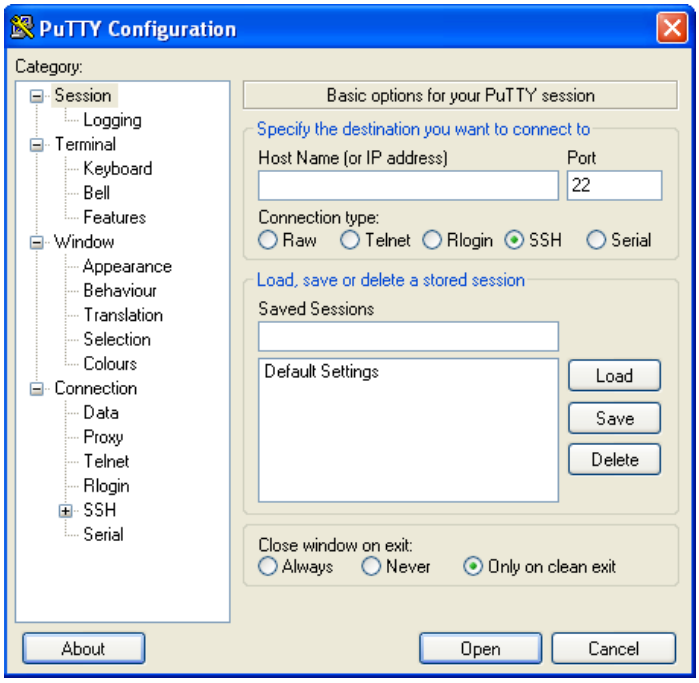
1) When the user-public key is loaded into the IONMM successfully, the key will take effect immediately; you do not need to restart the SSH server.

2) The ION system supports SSH2 keys only; SSH1 keys are not supported. When generating using puttyGen.exe, do not select the SSH1 keys.

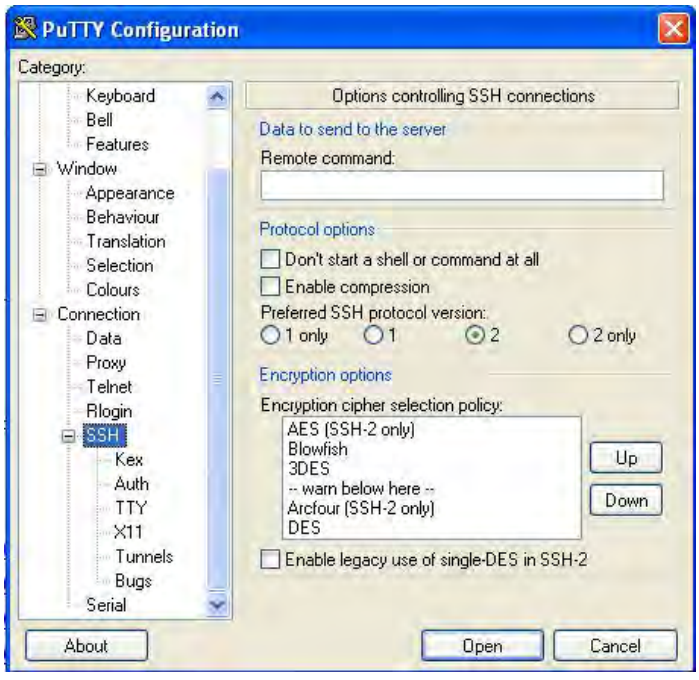
3) The ION system currently supports one user named 'root' with public key authentication.



PuTTY Basic Options:



PuTTY SSH Options:



Tracert (Traceroute)

Traceroute is a computer network tool used to determine the route taken by packets across an IP network. 'Tracert" (pronounced "traceroute") sends a test network message from a computer to a designated remote host and tracks the path taken by that message.

Tracert is a Windows based tool that allows you to help test your network infrastructure. In this article we will look at how to use tracert while trying to troubleshoot real world problems. This will help to reinforce the tool's usefulness and show you ways in which to use it when working on your own networks.

The traceroute tool is available on practically all Unix-like operating systems. Variants with similar functionality are also available, such as tracepath on modern Linux installations and tracert on Microsoft Windows operating systems. Windows NT-based operating systems also provide **pathping**, which provides similar functionality.

The tracert TCP/IP utility allows you to determine the route packets take through a network to reach a particular host that you specify. Tracert works by increasing the "time to live" (TTL) value of each successive packet sent. When a packet passes through a host, the host decrements the TTL value by one and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded. Tracert, if used properly, can help you find points in your network that are either routed incorrectly or are not existent at all.

The Tracert Windows based command-line tool lets you trace the path that an IP packet takes to its destination from a source. Tracert determines the path taken to a destination by sending ICMP (Internet Control Message Protocol) Echo Request messages to the destination. When sending traffic to the destination, it incrementally increases the TTL (Time to Live) field values to help find the path taken to that destination address.

Tracert options include:

-? which displays help at the command prompt.
-d which prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names (this speeds up the display of tracert results). Using the **–d** option helps when you want to remove DNS resolution. Name servers are helpful, but if not available, incorrectly set, or if you just want the IP address of the host, use the **–d** option.

Netstat

Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on UNIX, Unix-like, and Windows NT-based operating systems.

The **netstat** tool is used for finding network problems and determining the amount of traffic on the network as a performance measurement. It displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, **netstat** displays active TCP connections.

Note: parameters used with this command must be prefixed with a hyphen (**-**) and NOT a slash (/):

-a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-b Displays the binary (executable) program's name involved in creating each connection or listening port. (Windows XP, 2003 Server only - not Microsoft Windows 2000 or other non-Windows operating systems).
-e Displays Ethernet statistics, such as the number of bytes and packets sent and received.
-f Displays fully qualified domain names (FQDN) for foreign addresses.(not available under Windows)
-i Displays network interfaces and their statistics (not available under Windows).
-o Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).
-p (Windows): Protocol : Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
-p (Linux) Process : Show which processes are using which sockets (you must be root to do this).

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.

Winipcfg

The **winipcfg** command is available in Windows ME, Windows 98, and Windows 95 to review your current TCP/IP network protocol settings. Follow these steps to view your current TCP/IP settings using **winipcfg**:

1. Click the Start button and then click Run.
2. Type **winipcfg** in the Open box, and then click OK. Your current TCP/IP settings are displayed.
3. To view additional information, click **More Info**.

Note: The Winipcfg display is not updated dynamically. To view changes, quit **winipcfg** and then run it again. If your IP address was dynamically allocated by a DHCP server, you can use the Release and Renew buttons to release and renew the IP address.

The following information is displayed by the **winipcfg** tool.

Adapter Address: This string of hexadecimal numbers represents the hard-coded identification number assigned to the network adapter when it was manufactured. When you are viewing the IP configuration for a PPP connection using Dial-Up Networking, the number is set to a default, meaningless value (because modems are not hard-coded with this type of address).

IP Address: This is the actual IP networking address that the computer is set to. It is either dynamically assigned to the computer upon connection to the network, or a static value that is manually entered in TCP/IP properties.

Subnet Mask: The subnet mask is used to "mask" a portion of an IP address so that TCP/IP can determine whether any given IP address is on a local or remote network. Each computer configured with TCP/IP must have a subnet mask defined.

Default Gateway: This specifies the IP address of the host on the local subnet that provides the physical connection to remote networks, and is used by default when TCP/IP needs to communicate with computers on other subnets.

Click **More Info** to display the following settings:

DHCP Server: This specifies the IP address of the DHCP server. The DHCP server provides the computer with a dynamically assigned IP address upon connection to the network. Clicking the Release and Renew buttons releases the IP address to the DHCP server and requests a new IP address from the DHCP server.

Primary and Secondary WINS Server: These settings specify the IP address of the Primary and Secondary WINS servers (if available on the network). WINS servers provide a service translating NetBIOS names (the alphanumeric computer names seen in the user interface) to their corresponding IP address.

Lease Obtained and Lease Expires: These values show when the current IP address was obtained, and when the current IP address is due to expire. You can use the Release and Renew buttons to release and renew the current IP address, but this is not necessary because the DHCP client automatically attempts to renew the lease when 50 % of the lease time has expired.

Nslookup

nslookup is a computer program used in Windows and Unix to query DNS (Domain Name System) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The name nslookup means "name server lookup". A common version of the program is included as part of the BIND package.

Microsoft Windows 2000 Server, Windows 2000 Advanced Server, and Windows NT Server 4.0 Standard Edition provide the **nslookup** tool.

Windows' nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through the Control Panel.

Nslookup.exe can be run in two modes: interactive and noninteractive. Noninteractive mode is used when just a single piece of data is needed.

1. The syntax for noninteractive mode is:

   nslookup [-option] [hostname] [server]

2. To start Nslookup.exe in interactive mode, simply type "**nslookup**" at the command prompt:

   C:\> nslookup

Default Server: nameserver1.domain.com

Address: 10.0.0.1

>

3. Type "**help**" or "**?**" at the command prompt to generate a list of available commands.

Notes

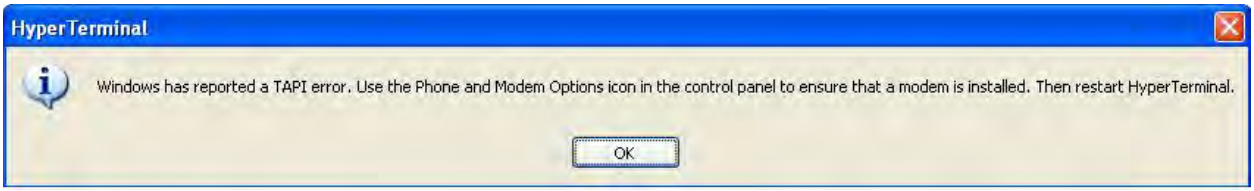
- The TCP/IP protocol must be installed on the computer running Nslookup.exe.
- At least one DNS server must be specified when you run the IPCONFIG /ALL command from a command prompt.
- Nslookup will always devolve the name from the current context. If you fail to fully qualify a name query (i.e., use a trailing dot), the query will be appended to the current context. For example, if the current DNS settings are att.com and a query is performed on www.microsoft.com; the first query will go out as www.microsoft.com.att.com because of the query being unqualified. This behavior may be inconsistent with other vendor's versions of Nslookup.

Third Party Tool Messages

This section discusses messages generated by HyperTerminal, Ping, and Telnet during ION system installation, operation and configuration.

HyperTerminal Messages

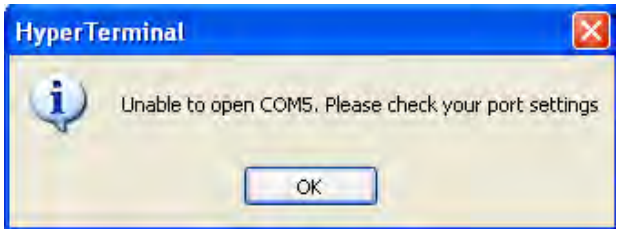
Message: *Windows has reported a TAPI error. Use the Phone and Modem Options icon in the Control Panel to ensure a modem is installed. Then restart HyperTerminal.*



Response:

1. Verify your **computer's Ports (COM)** setting. See "Configuring HyperTerminal".
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. See "Contact Us" on page 80.

Message: *Unable to open COM x. Please check your port settings.*



Response:

1. Verify your **computer's Ports (COM)** setting. See "Configuring HyperTerminal".
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. See "Contact Us" on page 80.

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

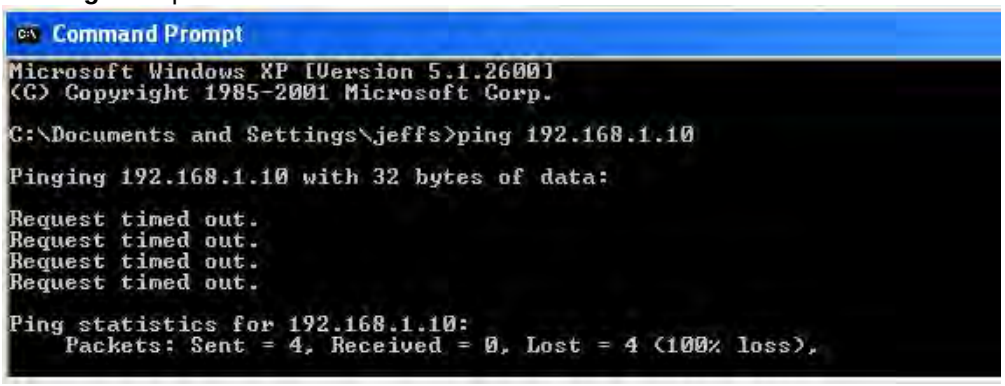
Meaning: HyperTerminal (HT) is a terminal emulation program developed by Hillgraeve, Inc., for Microsoft and supplied with some Windows OSes. In HyperTerminal, use the Enter key to drop to a new line, if required, and use the keyboard's Backspace key or the directional arrows to navigate within a text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

Response:

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

Ping Command Messages

Message: Request timed out.



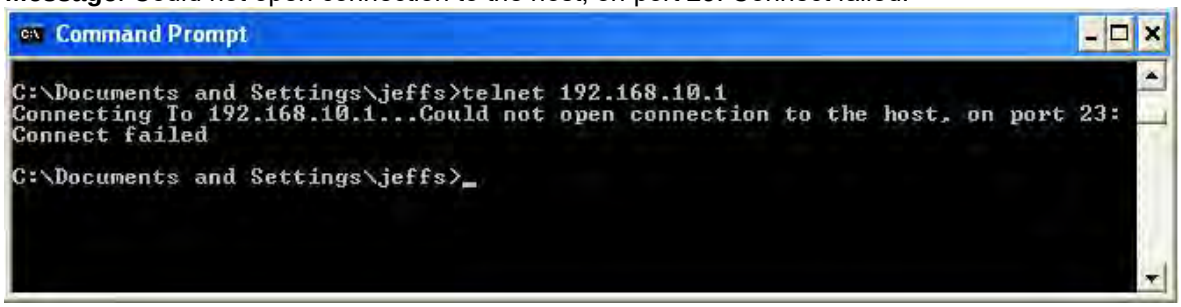
Meaning: The Ping command failed.

Recovery:

1. Verify the connection, verify correct IP address entry, and retry the operation.
2. Verify if the default IP address has changed using the Ipconfig (or similar) command.

Telnet Messages

Message: Could not open connection to the host, on port 23: Connect failed.



Meaning: The attempted Telnet connection failed.

Recovery:

1. Verify the physical connection, verify correct IP address entry, and retry the operation.
2. Check if the default IP address has changed using the Ipconfig (or similar) command.

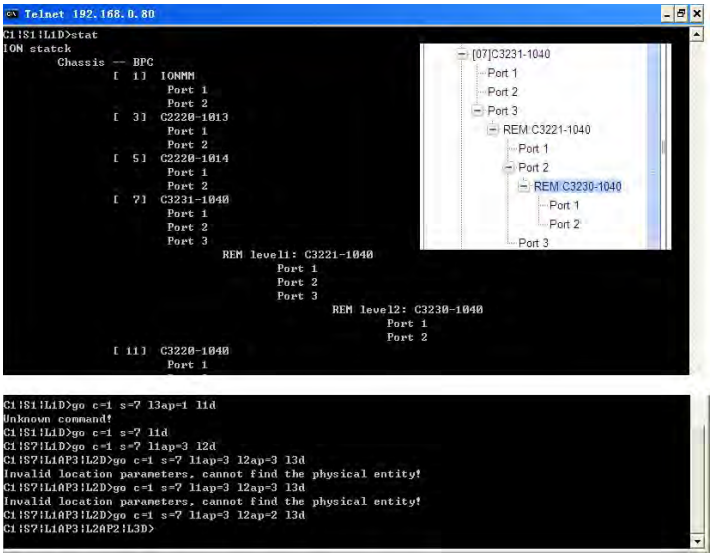
Message: Invalid location parameters, cannot find the physical entity!

```
C1:S7:L1AP3:L2D>go c=1 s=7 l1ap=3 l2ap=3 l3d
Invalid location parameters, cannot find the physical entity!
```

Meaning: The **go** command you entered includes a location that does not exist or that you entered incorrectly.

Recovery:

1. Run the **stat** command to verify your configuration.
2. Click the plus sign [+] next to **ION Stack** to unfold the "ION Stack" node in the left tree view to refresh device status.
3. Click the plus sign [+] next to **Chassis** to unfold the chassis devices.



4. Compare the **stat** command results to the Web interface tree view configuration information.
5. Re-run the **stat** command with the correct location parameters.
6. Ping the device in question.
7. Unplug and re-plug the USB connector on the IONMM card.
8. If the problem persists, contact Technical Support. See “Contact Us” on page 80.

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 *x4110 CLI Reference Manual, 33497*.

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.

Contact Us

Technical Support: Technical support is available 24-hours a day

US and Canada: 1-800-260-1312

International: 00-1-952-941-7600

Main Office

tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322
sales@transition.com | techsupport@transition.com | customerservice@transition.com

Address

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343, U.S.A.

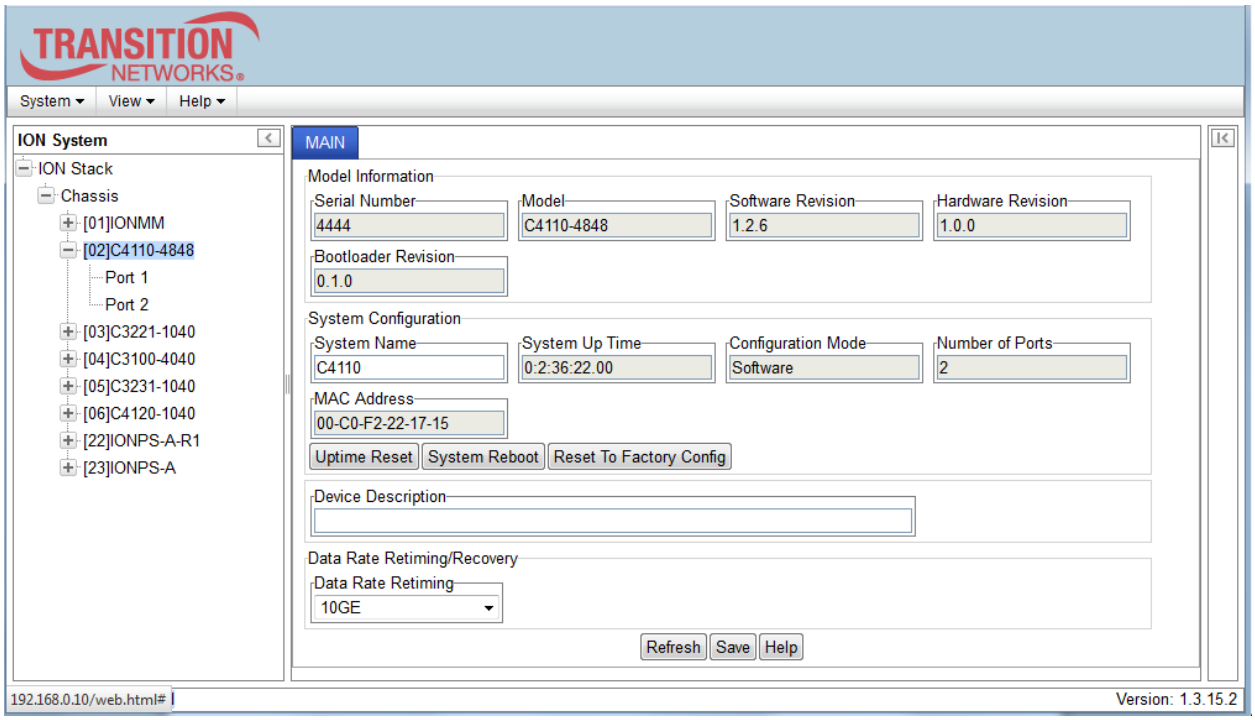
Web: https://www.transition.com

Firmware: Keep your products up to date by downloading the latest firmware. You must log in or create an account to download firmware. For further assistance contact us at +1.952.358.3601, 1.800.260.1312, or at techsupport@transition.com.

Recording Model Information and System Information

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

1. Select the ION system **MAIN** tab. (From the CLI, use the commands needed to gather the information requested below. This could include commands such as **show card info**, **show slot info**, **show system information**, **show ether config**, **show ip-mgmt config**, or others as request by the Support Specialist.



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

   Serial Number: _____ Model: _____

   Software Revision: _____ Hardware Revision: _____

   Bootloader Revision: _____

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

   System Up Time: _____ Configuration Mode: _____

   Number of Ports: _____ MAC Address: _____

   Data Rate Retiming: _____

   LED Status: _____

4. Provide additional Model and System information to your Technical Support Specialist. See "Basic ION System Troubleshooting".

   Your Transition Networks service contract number: _____

   A description of the failure: _____

   _____

   _____

   A description of any action(s) already taken to resolve the problem (e.g., changing switch mode, rebooting, etc.): _____

   _____

   _____

   The serial and revision numbers of all involved Transition Networks products in the network:

   _____

   _____

   A description of your network environment (layout, cable type, etc.): _____

   _____

   _____

   Network load and frame size at the time of trouble (if known): _____

   The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

   _____

   _____

   Any previous Return Material Authorization (RMA) numbers: _____

Appendix A: Warranty and Compliance Information

For Warranty, Returns, Electrical Safety Warnings, and Compliance Information see the related Install Guide manual.

Appendix B: SNMP MIBs and Traps Support

See the *IONMM SNMP User Guide* for information on SNMP traps supported, supported MIBs, private MIB objects tree example, Downloading, Compiling and Integrating MIBs, Trap service and functions, the Trap Server Log, and an example of ION SNMP operation.

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.

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).

10 gigabit Ethernet

(10GE or 10GbE or 10 GigE) refers to various technologies for transmitting Ethernet frames at a rate of 10 gigabits per second (10 billion bits per second), first defined by the IEEE 802.3ae-2002 standard. Like previous versions of Ethernet, 10GbE supports both copper and fiber cabling. However, due to its higher bandwidth requirements, higher-grade copper cables are required: category 6a or Class F/Category 7 cables for links up to 100m. Unlike previous Ethernet standards, 10 gigabit Ethernet only defines full duplex point-to-point links which are generally connected by network switches. Half duplex operation does not exist in 10GbE.
The 10 gigabit Ethernet standard encompasses a number of different physical layer (PHY) standards. A networking device may support different PHY types through pluggable PHY modules, such as those based on SFP+. Over time, market forces will determine the most popular 10GE PHY types. At the time that the 10 gigabit Ethernet standard was developed, interest in 10GbE as a wide area network (WAN) transport led to the introduction of a WAN PHY for 10GbE. The WAN PHY encapsulates Ethernet packets in SONET OC-192c frames and operates at a slightly slower data-rate (9.95328 Gbps) than the local area network (LAN) PHY. Both share the same physical medium-dependent sublayers so can use the same optics. The WAN PHY can support maximum link distances up to 80 km depending on the fiber standard employed.

10GBASE-KX4

Operates over four backplane lanes and uses the same physical layer coding (defined in IEEE 802.3 Clause 48) as 10GBASE-CX4.

10GBASE-KR

Operates over a single backplane lane and uses the same physical layer coding (defined in IEEE 802.3 Clause 49) as 10GBASE-LR/ER/SR.

10GBASE-T

10GBASE-T, or IEEE 802.3an-2006, is a standard released in 2006 to provide 10 Gbit/s connections over unshielded or shielded twisted pair cables, over distances up to 100 meters (330 ft). Although category 6a is required to reach the full 100 meters (330 ft), category 5e is good for up to 45 meters (148 ft) and category 6 will reach 55 meters (180 ft).[22] 10GBASE-T cable infrastructure can also be used for 1000BASE-T allowing a gradual upgrade from 1000BASE-T using autonegotiation to select which speed to use. 10GBASE-T has latency in the range 2 to 4 microseconds compared to 1 to 12 microseconds on 1000BASE-T. As of 2010 10GBASE-T silicon is available from several manufacturers with claimed power dissipation of 3-4 W at structure widths of 40 nm. With 28 nm in development, power will continue to decline.
10GBASE-T uses the IEC 60603-7 8P8C (commonly known as RJ45) connectors already widely used with Ethernet. Transmission characteristics are now specified to 500 MHz. To reach this frequency Category 6A or better balanced twisted pair cables specified in ISO/IEC 11801 amendment 2 or ANSI/TIA-568-C.2 are needed to carry 10GBASE-T up to distances of 100 m. Category 6 cables can carry 10GBASE-T for shorter distances when qualified according to the guidelines in ISO TR 24750 or TIA-155-A.

10GBASE-SR

10GBASE-SR ("short range") is a port type for multi-mode fiber and uses 850 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 52. It delivers serialized data at a line rate of 10.3125 Gbit/s.
Over obsolete FDDI-grade 62.5 micrometers multimode fiber cabling it has a maximum range of 26 meters. Over 62.5 micrometers OM1 it has a range of 33 meters; over 50 micrometers OM2 a range of 82 meters; over OM3 300 meters and over OM4 400 meters. OM3 and OM4 are the preferred choices for structured optical cabling within buildings. MMF has the advantage over SMF of having lower cost connectors because of its wider core.
There is a non-standard lower cost, lower power variant sometimes referred to as 10GBASE-SRL (10GBASE-SR lite). This is inter-operable with 10GBASE-SR but only has a reach of 100 meters.

10GBASE-LR

10GBASE-LR ("long reach") is a port type for single-mode fiber and uses 1310 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 52. It delivers serialized data at a line rate of 10.3125 Gbit/s.
10GBASE-LR has a specified reach of 10 kilometers (6.2 mi), but 10GBASE-LR optical modules can often manage distances of up to 25 kilometers (16 mi) with no data loss.

10GBASE-LRM

10GBASE-LRM, (Long Reach Multimode) originally specified in IEEE 802.3aq is a port type for multi-mode fiber and uses 1310 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 68. It delivers serialized data at a line rate of 10.3125 Gbit/s.
10GBASE-LRM supports distances up to 220 meters (720 ft) on FDDI-grade multimode fiber and the same 220m maximum reach on OM1, OM2 and OM3 fiber types. 10GBASE-LRM reach is not quite as far as the older 10GBASE-LX4 standard.
To ensure that specifications are met over FDDI-grade, OM1 and OM2 fibers, the transmitter should be coupled through a mode conditioning patch cord. No mode conditioning patch cord is required for applications over OM3 or OM4.
Some 10GBASE-LRM transceivers also support distances up to 300 meters (980 ft) on standard single-mode fiber (SMF, G.652), however this is not part of the IEEE or MSA specification. 10GBASE-LRM uses electronic dispersion compensation (EDC) for receive equalization.
10GBASE-LRM has been a failure in the market.

10GBASE-ER

10GBASE-ER ("extended reach") is a port type for single-mode fiber and uses 1550 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 52. It delivers serialized data at a line rate of 10.3125 Gbit/s.
The 10GBASE-ER transmitter is implemented with an externally modulated laser (EML).
10GBASE-ER has a reach of 40 kilometers (25 mi) over engineered links and 30 km over standard links.

10GBASE-ZR

Several manufacturers have introduced 80 km (50 mi) range ER pluggable interfaces under the name 10GBASE-ZR. This 80 km PHY is not specified within the IEEE 802.3ae standard and manufacturers have created their own specifications based upon the 80 km PHY described in the OC-192/STM-64 SDH/SONET specifications. The 802.3 standard will not be amended to cover the ZR PHY.

802.3 Standards for 10GbE

The IEEE 802.3 working group has published several standards relating to 10GbE. These included: 802.3ae-2002 (fiber -SR, -LR, -ER and -LX4 PMDs), 802.3ak-2004 (-CX4 copper twin-ax InfiniBand type cable), 802.3an-2006 (10GBASE-T copper twisted pair), 802.3ap-2007 (copper backplane -KR and -KX4 PMDs) and 802.3aq-2006 (fiber -LRM PMD with enhanced equalization). The 802.3ae-2002 and 802.3ak-2004 amendments were consolidated into the IEEE 802.3-2005 standard. IEEE 802.3-2005 and the other amendments were consolidated into IEEE Std 802.3-2008.

100BASE-FX

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

1000BASE-X

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

802.1

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

802.1ad

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

802.1ah

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

802.1p

The IEEE standard for QoS packet classification.

802.1p Prioritization

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

802.1q

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

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.)

Backplane Ethernet

Backplane - also known by its task force name 802.3ap - is used in backplane applications such as blade servers and routers/switches with upgradable line cards. 802.3ap implementations are required to operate in an environment comprising up to 1 meter (39 in) of copper printed circuit board with two connectors. The standard defines two port types for 10 Gbit/s (10GBASE-KX4 and 10GBASE-KR) and a 1 Gbit/s port type (1000BASE-KX). It also defines an optional layer for FEC, a backplane autonegotiation protocol and link training for 10GBASE-KR where the receiver can set a three tap transmit equalizer. The autonegotiation protocol selects between 1000BASE-KX, 10GBASE-KX4, 10GBASE-KR or 40GBASE-KR4 operation. 40GBASE-KR4 is defined in 802.3ba. New backplane designs use 10GBASE-KR rather than 10GBASE-KX4.

BPC

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

BPDU

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

Bridge

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

Cat 6 (Category 6) Cable

Category 6 cable, commonly referred to as Cat 6, is a standardized cable for Gigabit Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards. Compared to Cat 5 and Cat 5e, Cat 6 provides more stringent specifications for crosstalk and system noise. The Cat 6 cable standard provides performance of up to 250 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), 1000BASE-T/1000BASE-TX (Gigabit Ethernet) and 10GBASE-T (10-Gigabit Ethernet). Category 6 cable has a reduced maximum length when used for 10GBASE-T.
Like most earlier twisted-pair cable, Category 6 cable contains four twisted wire pairs. Attenuation, near end crosstalk (NEXT), and PSNEXT (power sum NEXT) in Cat 6 cable and connectors are all much lower than Cat 5 or Cat 5e, which uses 24 AWG wire. The increase in performance with Cat 6 comes mainly

from increased (22 AWG) wire size. Because the conductor sizes are generally the same, Cat 6 jacks may also be used with Cat 5e cable.
Category 6 cable can be identified by the printing on the side of the cable sheath. Cat 6 patch cables are normally terminated in 8P8C modular connectors. If Cat 6 rated patch cables, jacks, and connectors are not used with Cat 6 wiring, overall performance is degraded to that of the cable or connector.
Connectors use either T568A or T568B pin assignments; although performance is comparable provided both ends of a cable are the same, T568B is a deprecated standard in the US and no longer supported by TIA.

Category 6a Cable (Augmented Category 6)

Category 6a cable, or Augmented Category 6, is characterized to 500 MHz and has improved alien crosstalk characteristics, allowing 10GBASE-T to be run for the same distance as previous protocols.
The latest standard from the TIA for enhanced performance standards for twisted pair cable systems was defined in February 2008 in ANSI/TIA/EIA-568-B.2-10. Category 6a is defined at frequencies up to 500 MHz—twice that of Cat. 6.
Category 6a performs at improved specifications, in particular in the area of alien crosstalk, as compared to Cat 6 UTP (unshielded twisted pair), which exhibited high alien noise in high frequencies.
The global cabling standard ISO/IEC 11801 has been extended by the addition of amendment 2, which defines new specifications for Cat 6A components and Class EA permanent links. These new global Cat 6A/Class EA specifications require a new generation of connecting hardware, which offer superior performance compared to existing products based on the American TIA standard.
Note the performance difference between ISO/IEC and EIA/TIA component specifications for the NEXT transmission parameter. At a frequency of 500 MHz, an ISO/IEC Cat 6A connector performs 3 dB better than a Cat 6A connector that conforms with the EIA/TIA specification. The 3 dB represents a 100% increase of near-end crosstalk noise reduction when measured in absolute magnitudes.
When used for 10GBASE-T, Cat 6 cable's maximum length is 55 meters (180 ft) in a favorable alien crosstalk environment, but only 37 meters (121 ft) in a hostile alien crosstalk environment, such as when many cables are bundled together. However, because the effects of alien crosstalk environments on cables are difficult to determine prior to installation, it is highly recommended that all Cat 6 cables being used for 10GBASE-T are electrically tested once installed. With its improved specifications, Cat6 A does not have this limitation and can run 10GBASE-T at 100 meters (330 ft) without electronic testing.

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.

Center Wavelength

In a laser, the nominal value central operating wavelength. It is the wavelength defined by a peak mode measurement where the effective optical power resides. Center Wavelength (CWL) is the midpoint between the wavelengths where transmittance is 50% of the specified minimum transmission, referred to as the Full Width at Half Maximum (FWHM).

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.

CLI

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

Community

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

CSA

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

CWDM

Prior to the relatively recent ITU standardization of the term, one common meaning for coarse WDM meant two (or possibly more) signals multiplexed onto a single fiber, where one signal was in the 1550 nm band, and the other in the 1310 nm band.
In 2002 the ITU standardized a channel spacing grid for use with CWDM (ITU-T G.694.2), using the wavelengths from 1270 nm through 1610 nm with a channel spacing of 20 nm. (G.694.2 was revised in 2003 to shift the actual channel centers by 1 nm, so that strictly speaking the center wavelengths are 1271 to 1611 nm).
A recent development related to CWDM is the creation of GBIC and small form factor pluggable (SFP) transceivers utilizing standardized CWDM wavelengths. GBIC and SFP optics allow for something very close to a seamless upgrade in legacy systems that support SFP interfaces. See also WDM, DWDM, and Wavelength-Division Multiplexing.

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.

Discovery

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

DMI

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

DMM / DMR

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

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).

DWDM

Dense Wavelength Division Multiplexing (DWDM) refers originally to optical signals multiplexed within the 1550 nm band to leverage the capabilities and cost of erbium doped fiber amplifiers (EDFAs), which are effective for wavelengths between approximately 1525–1565 nm (C band), or 1570–1610 nm (L band). See also WDM, CWDM, and Wavelength-Division Multiplexing. See ftp://ftp.seagate.com/sff/INF-8478.PDF for more information.

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.

ESD

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

Event log

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

FC

Fibre Channel is a high-speed network technology (common rates of 2-, 4-, 8- and 16-Gbps) often used to connect computer data storage. Fibre Channel is standardized in the T11 Technical Committee of INCITS (the International Committee for Information Technology Standards) an ANSI standards committee. **Note**: When FC technology was developed, it supported only optical cabling (fiber). Copper cable support was later added, so the development committee kept the same name but changed to the British spelling 'fibre' for the standard. The American English spelling 'fiber' refers only to optical cabling, so a network using 'fibre' can be implemented either with copper or optical cabling.

The FC protocol has a range of speeds based on a various underlying transport media. Native FC speed variants include:

Media	Line-rate (GBps)	Throughput (full duplex; Mbps)*	Availability
1GFC	1.0625	200	1997
2GFC	2.125	400	2001
4GFC	4.25	800	2004
8GFC	8.5	1,600	2005
10GFC	10.52	2,550	2008

Fibre Channel does not follow OSI Layer modeling, but is similarly split into five layers (FC0 - FC4):
FC4: Protocol-mapping layer, in which application protocols, such as SCSI or IP, are encapsulated into a PDU for delivery to FC2.
FC3: Common services layer, a thin layer that could eventually implement functions like encryption or RAID redundancy algorithms.

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.

FDX

(Full Duplex) Communication in both directions simultaneously.

FEC

Forward Error Correction- a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The central idea is the sender encodes his message in a redundant way by using an error-correcting code (ECC). IETF RFC 5052 describes how to use Forward Error Correction (FEC) codes to efficiently provide and/or augment reliability for bulk data transfer over IP multicast.

Firmware

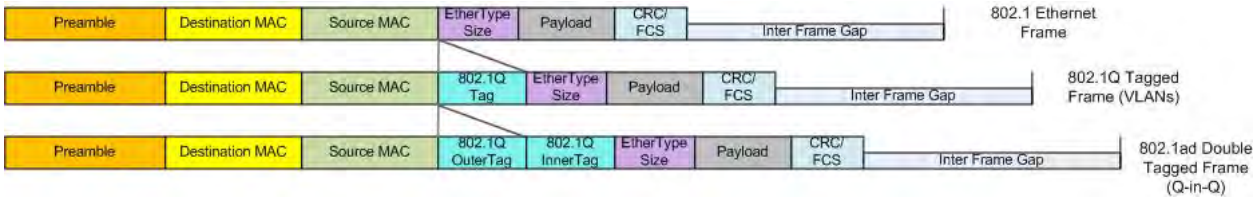
Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Frame

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

Frame Format

In Ethernet, a frame is a way of arranging sections of data for transfer over a computer network. The frame is a key element of an Ethernet system. A typical Ethernet frame is made up of three elements: a pair of addresses, the data itself, and an error checking field.
Frame Formats for 802.1, 802.1Q and 802.1ad are illustrated below.



FTP

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

G.709/Y.1331

ITU-T Recommendation ITU-T G.709/Y.1331 defines the requirements for the optical transport module of order n (OTM-n) signals of the optical transport network, in terms of: the optical transport hierarchy (OTH), the functionality of the overhead in support of multi-wavelength optical networks, frame structures, bit rates, and formats for mapping client signals.
The interfaces defined in this Recommendation can be applied at user-to-network interfaces (UNI) and network node interfaces (NNI) of the optical transport network.
This Recommendation defines “ODUk.ts” as “an increment of bandwidth which when multiplied by a number of tributary slots gives the recommended size of an ODUflex (GFP) optimized to occupy a given number of tributary slots of a higher order OPUk.”
The Optical Transport Hierarchy (OTH) is a new transport technology for the Optical Transport Network (OTN) developed by the ITU. It is based on the network architecture defined in ITU G.872 "Architecture for the OTN". G.872 defines an architecture that is composed of the Optical Channel (OCh), Optical Multiplex Section (OMS) and Optical Transmission Section (OTS). It then describes the functionality needed to make OTN work.
OTN offers these advantages compared to SONET/SDH: stronger Forward Error Correction (FEC), more Levels of Tandem Connection Monitoring (TCM), transparent transport of Client Signals, and switching Scalability.
See http://www.itu.int/rec/T-REC-G.709-201202-I/en for more information on G.709 : Interfaces for the optical transport network.

Gbps

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

GUI

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

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.

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.

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.

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.

Kbps

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

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).

LED

(Light Emitting Diode) An electronic light source.

LRM

Long Reach Multimode. See “10GBASE-LRM”.

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.)

MAU

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

Mbps

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

Media converter

Media converters transparently connect one type of media, or cabling, to another – typically copper to fiber. By bridging the gap between legacy copper infrastructures and fiber growth, media converters provide an economical way to extend the distance of an existing network, extend the life of non-fiber based equipment, or extend the distance between two like devices.
Transition Networks' brand of media converters makes conversion between disparate media types possible; while helping companies leverage their existing network infrastructure. These media conversion technologies are offered across a broad spectrum of networking protocols including Ethernet, Fast Ethernet, Gigabit, T1/E1, DS3, ATM, RS232/485, video, Power-over-Ethernet, and many more.

MSA

(Multi-Source Agreement) Common product specifications for pluggable fiber optic transceivers. Multi-Source Agreements. enhanced Small Form-factor Pluggable transceiver. To support different 10GbE physical layer standards, many interfaces consist of a standard socket into which different PHY modules may be plugged. Physical layer modules are not specified in an official standards body but by multi-source agreements (MSAs) that can be negotiated more quickly. Relevant MSAs for 10GbE include XENPAK (and related X2 and XPAK), XFP and SFP+. When choosing a PHY module, a designer considers cost, reach, media type, power consumption, and size (form factor). A single point-to-point link can have different MSA pluggable formats on either end (e.g. XPAK and SFP+) as long as the 10GbE optical or copper interface (e.g. 10GBASE-SR) inside the pluggable is identical. See also “SFP+”.

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.

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. See also “Media Converter”.

OC

Optical Carrier, used to specify the speed of fiber optic networks conforming to the SONET standard. The speeds for common OC levels include OC-1 = 51.85 Mbps, OC-3 = 155.52 Mbps, OC-12 = 622.08 Mbps, OC-24 = 1.244 Gbps, OC-48 = 2.488 Gbps, OC-192 = 9.952 Gbps, and OC-255 = 13.21 Gbps.

OC-192

(OC-192 / STM-64 / 10G SONET) OC-192 is a network line with transmission speeds of up to 9953.28 Mbit/s (payload = 9510.912 Mbit/s (9.510912 Gbit/s); overhead = 442.368 Mbit/s). A standardized variant of 10 Gigabit Ethernet (10GbE), called WAN PHY, is designed to inter-operate with OC-192 transport equipment while the common version of 10GbE is called LAN PHY (which is not compatible with OC-192 transport equipment in its native form). The naming is a bit misleading since both LAN PHY and WAN PHY can be used on a wide area network.

ODU Bit Rate Tolerance

The ODU bit-rate tolerance is ±20 ppm.

ODU Types and Bit Rates

ODU type	ODU nominal bit rate
ODU0	1 244 160 kbit/s
ODU1	239/238 × 2 488 320 kbit/s
ODU2	239/237 × 9 953 280 kbit/s
ODU3	239/236 × 39 813 120 kbit/s
ODU4	239/227 × 99 532 800 kbit/s

OID

(Object Identifier) Known as a “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.

OTU Bit Rate Tolerance

The OTU bit-rate tolerance is ±20 ppm.

OTU Types and Bit Rates

OTU type	OTU nominal bit rate
OTU1	255/238 × 2 488 320 kbit/s
OTU2	255/237 × 9 953 280 kbit/s
OTU3	255/236 × 39 813 120 kbit/s
OTU4	255/227 × 99 532 800 kbit/s

OTH

(Optical Transport Hierarchy): see “G.709/Y.1331” above.See also “OTN” below.

OTN

(Optical Transport Network): the Optical Transport Hierarchy (OTH) is a new transport technology for the Optical Transport Network (OTN) developed by the ITU. OTH is based on the network architecture defined in ITU G.872 "Architecture for the Optical Transport Network (OTN)".
G.872 defines an architecture that is composed of the Optical Channel (OCh), Optical Multiplex Section (OMS) and Optical Transmission Section (OTS). G.872then describes the functionality that needed to make OTN work. Compared to SONET/SDH, using OTN offers advantages (stronger Forward Error Correction, more levels of TCM, transparent transport of Client signals, switching scalability) and disadvantages (requires new hardware and management system).

OTU Type	OTU Bit Rate (Nominal)
OTU1	255/238 x 2 488 320 kbit/s
OTU2	255/237 x 9 953 280 kbit/s
OTU3	255/236 x 39 813 120 kbit/s

The OTU bit rate tolerance is ±20 ppm for OTU1, OTU2, and OTU3. The nominal OTUk rates are approximately 2 666 057.143 kbit/s (OTU1), 10 709 225.316 kbit/s (OTU2) and 43 018 413.559 kbit/s (OTU3). See http://www.itu.int/rec/T-REC-G.709/ for more information. See also “G.709/Y.1331” above.

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.

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.

PE

(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.

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.

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.

RS-232

(Recommended Standard 232) A standard for serial binary data signals connecting between a DSL (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

SFP

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

SFP+
enhanced Small Form-factor Pluggable transceiver. To support different 10GbE physical layer standards, many interfaces consist of a standard socket into which different PHY modules may be plugged. Physical layer modules are not specified in an official standards body but by multi-source agreements (MSAs) that can be negotiated more quickly. Relevant MSAs for 10GbE include XENPAK (and related X2 and XPAK), XFP and SFP+. When choosing a PHY module, a designer considers cost, reach, media type, power consumption, and size (form factor). A single point-to-point link can have different MSA pluggable formats on either end (e.g. XPAK and SFP+) as long as the 10GbE optical or copper interface (e.g. 10GBASE-SR) inside the pluggable is identical. See also “MSA”.
The newest module standard is the enhanced small form-factor pluggable transceiver, generally called SFP+. Based on the small form-factor pluggable transceiver (SFP) and developed by the ANSI T11 fibre channel group, it is smaller still and lower power than XFP. SFP+ has become the most popular socket on 10GE systems. SFP+ modules do only optical to electrical conversion, no clock and data recovery, putting a higher burden on the host's channel equalization. SFP+ modules share a common physical form factor with legacy SFP modules, allowing higher port density than XFP and the re-use of existing designs for 24 or 48 ports in a 19" rack width blade.
SFP+ modules can further be grouped into two types of host interfaces: linear or limiting. Limiting modules are preferred except when using old fiber infrastructure which requires the use of the linear interface provided by 10GBASE-LRM modules.

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 x4110 has SGMII support for use with 10/100/1000BASE-T copper SFPs. The x4110 uses the **set ether phymode=SGMII** CLI command to select SGMII mode.

SLA

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

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.

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.)

SNMP Version

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

SONET

(Synchronous Optical Networking) SONET and SDH are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber. SONET and SDH, which are essentially the same, were originally designed to transport circuit mode communications (e.g., DS1, DS3) from a variety of sources. Both protocols are widely used today: SONET in the United States and Canada, and SDH in the rest of the world.

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.

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.

Syslog

A service run mostly on Unix and Linux systems (but also available for other OSes) to track events that occur on the system. Analysis can be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

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.

Telnet

A user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. Telnet is a terminal emulation program for TCP/IP networks that runs on your computer and connects your PC to a switch management. (Standard: RFC 854.)

TFTP

(Trivial File Transfer Protocol) A file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). Due to its simple design, TFTP can be implemented using a very small amount of memory. 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 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.

Throughput

The maximum rate at which no frame is dropped. This is typically measured under test conditions.

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.

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.

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).

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).

Wavelength-Division Multiplexing (WDM, DWDM and CWDM)

WDM, DWDM and CWDM are based on the same concept of using multiple wavelengths of light on a single fiber, but differ in the spacing of the wavelengths, number of channels, and the ability to amplify the multiplexed signals in the optical space. See also CWDM, DWDM, and WDM.

WDM

In fiber-optic communications, wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light. This technique enables bidirectional communications over one strand of fiber, as well as multiplication of capacity. WDM systems are divided into different wavelength patterns, coarse (CWDM) and dense (DWDM). See also CWDM, DWDM, and Wavelength-Division Multiplexing.

Index

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322

sales@transition.com | techsupport@transition.com | customerservice@transition.com

ION System x4110 Web User Guide PN 33574 Rev. B