ION System x4120 Series

10GBASE-T to 10G Fiber Ethernet Converter Slide-in-Module and NID

User Guide

33551 Rev. B
Trademarks
All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions
Copyright © 2013-2018 Transition Networks. All rights reserved. No part of this work may be reproduced or used in any form or by any means (graphic, electronic or mechanical) without written permission from Transition Networks. Printed in the U.S.A.


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

Revision History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>06/13/13</td>
<td>Initial release for v 1.2.3.</td>
</tr>
<tr>
<td>B</td>
<td>6/8/18</td>
<td>Update for FW v 1.2.6 with support for management and FW upgrade of a C4120 when installed in an unmanaged ION chassis and contact info. Update for FW v 2.0.1 and Bootloader v 0.1.5 with Slot ID and TLPT fixes.</td>
</tr>
</tbody>
</table>
Cautions and Warnings

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

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

Cautions

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

⚠️ **Caution:** When handling chassis cards, observe electrostatic discharge precautions. This requires proper grounding (i.e., wear a wrist strap).

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

⚠️ **Caution:** **Do not** install the x4120 in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor x4120 performance.

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

⚠️ **Caution:** Only trained and qualified personnel should install or perform maintenance on the ION219-A chassis. Failure to observe this caution could result in poor performance or damage to the equipment.

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

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

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

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

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

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

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

See Appendix A on page 144 for Electrical Safety Warnings translated into multiple languages.
# Table of Contents

## Section 1: Introduction

<table>
<thead>
<tr>
<th>Item</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Overview</td>
<td>8</td>
</tr>
<tr>
<td>Document Overview</td>
<td>8</td>
</tr>
<tr>
<td>Documentation Conventions</td>
<td>9</td>
</tr>
<tr>
<td>Related Manuals and Online Helps</td>
<td>10</td>
</tr>
</tbody>
</table>

## Section 2: Management Methods

<table>
<thead>
<tr>
<th>Item</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>11</td>
</tr>
<tr>
<td>IONMM Managed Devices</td>
<td>11</td>
</tr>
<tr>
<td>Managing Slide-In and Remote Modules Using CLI Commands</td>
<td>11</td>
</tr>
<tr>
<td>Managing Slide-In and Remote Modules via the Web Interface</td>
<td>14</td>
</tr>
<tr>
<td>Direct Managed Devices</td>
<td>15</td>
</tr>
<tr>
<td>Managing Standalone Modules Using CLI Commands</td>
<td>15</td>
</tr>
<tr>
<td>Managing Standalone Modules via the IONMM Web Interface</td>
<td>16</td>
</tr>
<tr>
<td>Menu System Descriptions</td>
<td>17</td>
</tr>
<tr>
<td>Reboot, Reset, and Power Off Function Notes</td>
<td>19</td>
</tr>
</tbody>
</table>

## Section 3: Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>22</td>
</tr>
<tr>
<td>System Configuration</td>
<td>23</td>
</tr>
<tr>
<td>System Configuration – CLI Method</td>
<td>23</td>
</tr>
<tr>
<td>System Configuration – Web Method</td>
<td>24</td>
</tr>
<tr>
<td>Device Description Configuration</td>
<td>25</td>
</tr>
<tr>
<td>Device Description– CLI Method</td>
<td>25</td>
</tr>
<tr>
<td>Agent III C1</td>
<td>S17</td>
</tr>
<tr>
<td>Agent III C1</td>
<td>S17</td>
</tr>
<tr>
<td>Device description: thenewone</td>
<td>25</td>
</tr>
<tr>
<td>Agent III C1</td>
<td>S17</td>
</tr>
<tr>
<td>Device Description Config – Web Method</td>
<td>26</td>
</tr>
<tr>
<td>Circuit ID Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Circuit ID Config – CLI Method</td>
<td>27</td>
</tr>
<tr>
<td>Circuit ID Config – Web Method</td>
<td>28</td>
</tr>
<tr>
<td>Transparent Link Pass Through (TLPT) Configuration</td>
<td>29</td>
</tr>
<tr>
<td>Transparent Link Pass Through (LPT) Config – CLI Method</td>
<td>29</td>
</tr>
<tr>
<td>Transparent Link Pass Through (TLPT) Config – Web Method</td>
<td>30</td>
</tr>
<tr>
<td>Displaying AutoCross</td>
<td>31</td>
</tr>
<tr>
<td>AutoCross Config – CLI Method</td>
<td>31</td>
</tr>
<tr>
<td>AutoCross Config – Web Method</td>
<td>32</td>
</tr>
<tr>
<td>Displaying Auto Negotiation</td>
<td>33</td>
</tr>
<tr>
<td>Auto Negotiation – CLI Method</td>
<td>34</td>
</tr>
<tr>
<td>Auto Negotiation – Web Method</td>
<td>35</td>
</tr>
<tr>
<td>Check Ethernet Port Configuration</td>
<td>36</td>
</tr>
<tr>
<td>Check Ethernet Port Config– CLI Method</td>
<td>36</td>
</tr>
<tr>
<td>Check Ethernet Port Config – Web Method</td>
<td>37</td>
</tr>
<tr>
<td>Loopback Management</td>
<td>38</td>
</tr>
<tr>
<td>Loopback Management – CLI Method</td>
<td>38</td>
</tr>
</tbody>
</table>
Section 4: Operation .............................................................................................................. 40
  General ............................................................................................................................ 40
  Backup and Restore Operations (Provisioning) .............................................................. 40
  Displaying Information .................................................................................................. 40
  Reset to Factory Defaults .............................................................................................. 41
     Resetting Defaults – CLI Method .............................................................................. 41
     Resetting Defaults – Web Method ............................................................................ 42
  File Status after Reset to Factory Defaults .................................................................. 43
  Resetting Uptime .......................................................................................................... 44
     Reset System Uptime – CLI Method ........................................................................ 44
     Reset System Uptime – Web Method ........................................................................ 45
  Reboot ............................................................................................................................ 46
     Rebooting – CLI Method ........................................................................................... 46
     Rebooting – Web Method .......................................................................................... 47
     Reboot File Content and Location ......................................................................... 48
  Upgrade the IONMM and/or x4120 Firmware ................................................................ 49
  C4120 Management and FW Upgrade when installed in an Unmanaged ION Chassis . Error! Bookmark not defined.
  Transfer Files via Serial Protocol (X/Y/Zmodem) – CLI Method .................................. 50
  Replacing a Chassis Resident C4120 ............................................................................. 51

Section 5: Troubleshooting ......................................................................................... 52
  General ............................................................................................................................ 52
  Basic ION System Troubleshooting ............................................................................ 52
  Error Indications and Recovery Procedures ................................................................ 53
  LED Fault and Activity Displays ................................................................................ 54
  Problem Conditions ..................................................................................................... 55
  CLI Messages ................................................................................................................ 61
  Web Interface Messages ............................................................................................... 84
     Windows Event Viewer Messages ......................................................................... 97
  The Config Error Log (config.err) File ...................................................................... 98
     config.err Messages ............................................................................................... 99
     config.err Message Responses ............................................................................. 99
  Webpage Messages ...................................................................................................... 102
  DMI (Diagnostic Maintenance Interface) ...................................................................... 111
  Third Party Troubleshooting Tools ............................................................................ 115
  Third Party Tool Messages .......................................................................................... 128
     HyperTerminal Messages ....................................................................................... 128
     Ping Command Messages ....................................................................................... 130
     Telnet Messages ...................................................................................................... 130
     TFTP Server Messages ........................................................................................... 132
     PuTTY Messages ...................................................................................................... 133
  Technical Support .......................................................................................................... 133
  Recording Model Information and System Information ............................................. 134

Appendix A: Warranty and Compliance Information ............................................... 136
  Warranty ....................................................................................................................... 136
Compliance Information.................................................................................................................. 138
Electrical Safety Warnings ........................................................................................................... 139
  Electrical Safety ....................................................................................................................... 139
  Elektrische Sicherheit .............................................................................................................. 139
  Elektrisk sikkerhed .................................................................................................................. 139
  Elektrische veiligheid .............................................................................................................. 139
  Sécurité électrique ............................................................................................................... 139
  Sähköturvallisuus ................................................................................................................. 139
  Sicurezza elettrica ................................................................................................................. 139
  Elektrisk sikkerhet .................................................................................................................. 139
  Segurança elétrica ................................................................................................................. 139
  Seguridad eléctrica ................................................................................................................. 139
  Elsäkerhet .................................................................................................................................. 139

Appendix B: SNMP MIBs and Traps Support .............................................................................. 140
Supported MIBs ........................................................................................................................... 140
  Downloading, Compiling and Integrating MIBs ..................................................................... 142
Trap Service and Functions ........................................................................................................ 143
Trap Server Log .......................................................................................................................... 145
For Additional SNMP MIB Trap Information ............................................................................ 146

Glossary ...................................................................................................................................... 147
  10Gigabit Ethernet Terms .................................................................................................... 178

Index ......................................................................................................................................... 182

List of Figures

Figure 1: CLI Location Hierarchy ............................................................................................. 12
Figure 2: Private MIB Objects .................................................................................................. 141
Figure 3: SNMP Message Sequence ......................................................................................... 143

List of Tables

Table 1: Documentation Conventions ........................................................................................ 9
Table 2: System-Level Menu Description .................................................................................. 17
Table 3: Port-Level Menu Description ...................................................................................... 18
Table 4: File Status after a Reset to Factory Defaults ............................................................... 43
Table 5: File Content and Location after a System Reboot ...................................................... 48
Table 6: DMI Parameters ......................................................................................................... 113
Table 7: Trap Server Log File Description .............................................................................. 146

https://www.transition.com/
Section 1: Introduction

Product Overview

The x4120-1040 is a 10 Gigabit Ethernet copper to fiber media converter. It offers conversion technology by providing one 10GBase-T RJ-45 port and one pluggable 10GBase-X fiber SFP+ port. The open SFP+ port supports a wide variety of Transition Networks 10GE SFP+ fiber modules, as well as third party MSA compatible SFP+ modules.

The x4120 provides several 10G Ethernet enterprise and data center connectivity solutions. Since most 10G Ethernet switches support a combination of copper RJ-45 and open SFP+ ports, the x4120 allows users to convert either of these ports to the media type of their preference to match their network requirements, including direct attached copper SFP+ cables.

The C4120 slide-in-card is a managed device when installed in a managed ION Chassis. The stand-alone S4120 is an unmanaged device, until it is linked to C4120 installed in a managed ION chassis, and then remote in-band management of the S4120 is available.

These devices can be managed via Command Line Interface (CLI), Web interface, or Telnet. Access is through the IONMM (ION Management Module), also installed in the ION chassis. See the related x4120 Installation Guide or locate it on the web at https://www.transition.com/, then click on Products/Product Finder to locate the manual.

Document Overview

The purpose of this manual is to provide the user with an understanding of the Transition Networks x4120 Ethernet media converter. This manual documents the following models:

- **C4120-1040**: 10GBase-T Copper to Fiber Media Converter
- **S4120-1040**: 10GBase-T Copper to Fiber Media Converter
# Documentation Conventions

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

## Table 1: Documentation Conventions

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

A printed Documentation Postcard is shipped with each x4120. 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. C4120 Install Guide, 33549
3. S4120 Install Guide, 33550
4. x4120 User Guide, 33551 (this manual)
5. Local Management of Cards in a Remote Un-managed Chassis
6. x4120 CLI Reference Manual, 33552
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.
Section 2: Management Methods

General

The x4120s are managed either directly or through the IONMM. Whether the x4120s is 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 x4120 can be remotely managed directly (i.e., not through IONMM). This enables administrators to monitor and configure remote stand-alone x4120s 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 (x4120) 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 Using CLI Commands

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

For example:

AgentIII C1|S7|L1D>

or just:

C1|S1|L1D>

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

![Hierarchy Diagram](image)

**Figure 1: CLI Location Hierarchy**

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

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

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

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

- **Attachment port** – These are also ports on a specified device; they are labeled L1AP= and L2AP= and indicate an attachment point for another ION family device that **can** be managed by the IONMM.

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

**Example 1**

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

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

The resulting command line prompt would be:

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

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

**Example 2**

In the CLI location hierarchy, to go to device L2D in the network topology shown in Figure 5, you would enter the following command from the base prompt.

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

The resulting command line prompt would be:

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

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

The following describes the procedure for using CLI commands to manage the x4120s.

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

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

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

3. Configure the x4120 using the appropriate commands. For a complete list of the available commands, see the x4120 CLI Reference Manual.

4. To return the location to the IONMM, type **home** and press Enter.
Managing Slide-In and Remote Modules via the Web Interface

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. Click on the slide-in module or port to be managed.

3. The operations that can be performed depend on the type of slide-in module. Refer to the product documentation for the information. See the “Related Manuals” section on page 38.
Direct Managed 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 Using CLI Commands

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

For example:

```
AgentIII C1|S7|L1D>
```

or just:

```
C1|S7|L1D>
```

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

The `go` command format is:

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

**EXAMPLE**

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

```
C1|S7|L1D> go l1p=1
```

The resulting command line prompt would be:

```
C1|S7|L1P1>
```

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

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

```
C1|S7|L1P1> go l1d
```

The resulting command line prompt would be:

```
C1|S7|L1D>
```
Managing Standalone Modules via the IONMM Web Interface

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Click the plus sign [+ ] next to ION Stack to unfold the "ION Stack" node in the left tree view if not already done.
3. Click the plus sign [+ ] next to Chassis and click the plus sign [+ ] next to a module.

4. Click on the module or port to be managed (e.g., the C4120 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

<table>
<thead>
<tr>
<th>Dropdown / Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ION System pane</strong></td>
<td><strong>ION Stack</strong> - consists of one chassis or one standalone device. The Stack Members table lists the Stack's chassis and its type.</td>
</tr>
<tr>
<td></td>
<td><strong>Chassis</strong> - the ION System family of products; the Chassis View shows a summary view of one such chassis. Model Information includes:</td>
</tr>
<tr>
<td></td>
<td>* Serial Number - The serial number of the chassis itself. Each x4120 also have its own serial number.</td>
</tr>
<tr>
<td></td>
<td>* Model Name - The exact model name of this device (e.g., ION219). When contacting Technical Support, please be sure to give this name</td>
</tr>
<tr>
<td></td>
<td>rather than the less specific Catalog number.</td>
</tr>
<tr>
<td></td>
<td>* Software Revision, Hardware Revision, and Bootloader Revision.</td>
</tr>
<tr>
<td></td>
<td>* Chassis Members table - lists local physical components in slots 1 to 19.</td>
</tr>
<tr>
<td></td>
<td><strong>Device</strong> – provides tabs and sub-tabs for the IONMM and x4120s in the ION system.</td>
</tr>
<tr>
<td></td>
<td><strong>Port</strong> - provides tabs and sub-tabs for a selected x4120 port.</td>
</tr>
<tr>
<td><strong>System Dropdown</strong></td>
<td>Sign out.</td>
</tr>
<tr>
<td><strong>View Dropdown</strong></td>
<td>Refresh.</td>
</tr>
<tr>
<td><strong>Help Dropdown</strong></td>
<td>Online Help, ION Product Home Page, About ION System Web Interface.</td>
</tr>
<tr>
<td><strong>MAIN Tab</strong></td>
<td><strong>Sections</strong>: Model Information, System Configuration, Device Description, and Transparent Link Pass Through (TLPT) sections.</td>
</tr>
<tr>
<td></td>
<td><strong>Buttons</strong>: Uptime Reset, System Reboot, Reset To Factory Config buttons. Refresh, Save, and Help buttons.</td>
</tr>
</tbody>
</table>
The table below describes the ION Web interface in terms of its port-level tabs and sub-tabs.

**Table 3: Port-Level Menu Description**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
</table>
| **MAIN** Tab   | Sections: Circuit ID, Port Configuration, and Loopback Management.  
|                | **Buttons**: Refresh, Save, Start, Stop and Help. |
| **DMI** Tab    | Sections: Interface Characteristics, Diagnostic Monitoring, Supported Media Length.  
| (Port 2 only)  | The DMI (Diagnostic Maintenance Interface) function displays x4120 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths. See “DMI (Diagnostic Maintenance Interface) Parameters” on page 248 for more information.  
|                | **Note**: not all x4120 and 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 x4120 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 starting on page 199 for information on how to save the stored files from deletion.

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

- Table 3: Port-Level Menu Description on page 18
- Table 4: File Status after a Reset to Factory Defaults on page 43
- Table 5: File Content and Location after a System Reboot on page 48

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

### System Reboot

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

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

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

Note that a System Reboot can take several minutes.
**Reset To Factory Config**

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

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

**Reset Power to a Slot**

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

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

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

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

If you are **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 x4120 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 x4120.

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 x4120CLI Reference Manual.

The operating characteristics that can be defined for the x4120 are:

- System setup
- Features
  - Transparent Link pass through (TLPT)
  - Device Description
- Port setup
  - Circuit ID
  - Admin Status
  - Loopback Management

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 C4120
- 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 CLI or the Web interface.

System Configuration – CLI Method

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

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. Type `set system name=NAME`, where NAME is the new system name, and press Enter.

   For example:
   ```
   C1|S5|L1D> set system name=x4120-1013
   ```

3. Verify the new system definition. Type `show card info` and press Enter. For example:

   ```
   Agent III C1|S18|L1D> show card info
   System name: C4120
   Uptime: 00:02:19
   MAC: 00-c0-f2-00-d1-38
   Port number: 2
   Serial number: 789568
   Config mode: software
   Software: 2.0.0
   Bootloader: 0.1.5
   Hardware: 1.0.0
   Agent III C1|S18|L1D>
   ```

   **Note:** the `show card info` command does not work on a Power Supply module.
System Configuration – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

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

3. In the System Name field, enter the name and for the x4120. The name can be alphabetic, numeric or a combination, but cannot contain any spaces between the characters.

4. Scroll to the bottom and click Save.
**Device Description Configuration**

The x4120 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 x4120 using either the CLI or Web method.

**Device Description— CLI Method**

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

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

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

3. Press Enter.

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

   Agent III C1|S17|L1D> set device description thenewone
   Agent III C1|S17|L1D> show dev descr
   Device description: thenewone
   Agent III C1|S17|L1D>
Device Description Config – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. At the x4120 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.
Circuit ID Configuration

The x4120 supports a Device Description at the device level and a Circuit ID at the port level.

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

The Circuit ID can be configured in the x4120 using either the CLI or Web method.

Circuit ID Config – CLI Method

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

2. At the device’s command prompt type: set circuit-ID=<xx> where:
   
   xx = the Circuit ID to be used for this device or port.

3. Press Enter.

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

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

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

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

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

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

1. Access the x4120 via the Web interface (see “Starting the Web Interface” on page 45).

2. Select the appropriate port and locate the **Circuit ID** field.

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

4. Click **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:

   c) Click Refresh, and re-enter a Circuit ID of 64 or fewer characters and click **Save**.

   d) The message “**Setting values succeeded**” displays in the lower left corner of the Web interface.
### Transparent Link Pass Through (TLPT) Configuration

The x4120 supports Transparent Link Pass Through (TLPT) at the device level. The TLPT feature can be configured in the x4120 using either the CLI or Web method.

**Note** that ION x4120 v 2.0.1 corrected issues with TLTP and Slot # ID.

#### Transparent Link Pass Through (LPT) Config – CLI Method

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. At the device’s command prompt type: `set transparent lpt state =xx`, where `xx= <enable or disable>.
3. Press the Enter key.
4. Verify the TLPT setting. Type `show lpt config` and press Enter. For example:

```
Agent III C1|S17|L1D> set transparent lpt state ?
   disable
   enable
Agent III C1|S17|L1D> set transparent lpt state enable
Agent III C1|S17|L1D> set transparent lpt state disable
Agent III C1|S17|L1D> set transparent lpt state enable
Agent III C1|S17|L1D> show lpt config
Link pass through configuration:
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| Link pass through state:     | notSupported |
| Transparent link pass through state: | enable       |
| Selective link pass through state: | notSupported |
| Link pass through monitor port: | 0            |
| Remote fault detect state:    | notSupported |

Agent III C1|S17|L1D>
```

Use the `show lpt config` command to display the current link pass through configuration.
Transparent Link Pass Through (TLPT) Config – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. At the MAIN tab, locate the Transparent Link Pass Through (TLPT) section.

3. Select Enabled or Disabled. The default is Disabled. Click Save when done.
Displaying AutoCross

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

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

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

On x4120 devices the AutoCross feature makes it possible for hardware to automatically correct errors in cable selection, making the distinction between a straight through cable and a crossover cable unimportant.

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

AutoCross Config – CLI Method

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. At the device port’s command line, type show ether autocross=xx where:
   
   xx = cable type. Valid choices are:
   
   - Auto – hardware will automatically correct errors in cable selection.

3. Press Enter.
**AutoCross Config – Web Method**

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. Select the appropriate port’s **MAIN** tab.

3. Locate the **Port Configuration** section.

4. In the **AutoCross Mode** field, select the mode to be used.
   
   - **Auto** – ION System hardware will automatically correct errors in cable selection (default mode - recommended).
Displaying Auto Negotiation

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

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

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

The usual effect of this mismatch is that the connection works but at a very low speed. Disabling the auto negotiate feature allows you to force the connection to the desired speed and duplex mode of operation as long as both devices can support the operation.

**Note:** The auto negotiate feature is always enabled for gigabit devices/ports.
Auto Negotiation – CLI Method

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. Verify the configuration settings Type: `show ether config` and press Enter. The current Ethernet configuration displays. For example:

```plaintext
Agent III C1|S17|L1P1>show ether config
Port-11040
TP port:

<table>
<thead>
<tr>
<th>Link operation status:</th>
<th>down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin status:</td>
<td>up</td>
</tr>
<tr>
<td>Port mode:</td>
<td>RJ-45</td>
</tr>
<tr>
<td>PHY operation mode:</td>
<td>phy10GBaseT</td>
</tr>
<tr>
<td>Speed:</td>
<td>10G</td>
</tr>
<tr>
<td>Duplex:</td>
<td>full</td>
</tr>
<tr>
<td>Autocross:</td>
<td>auto</td>
</tr>
</tbody>
</table>

AutoNeg admin state: enable
Agent III C1|S17|L1P1>
```
Auto Negotiation – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. Select the appropriate port.

3. Locate the Auto Negotiation Settings section on the MAIN tab.

4. In the Auto Negotiation field, observe whether this feature is enabled or disabled.
Check Ethernet Port Configuration

With auto negotiate disabled, the connection is forced to the desired speed and duplex mode of operation as long as both devices can support the operation. **Note:** The Auto Negotiate feature is always enabled for gigabit devices/ports.

A port’s Ethernet port speed and mode can be verified in the x4120 using either the CLI or Web method.

**Check Ethernet Port Config– CLI Method**

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

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

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Check the configuration settings. Type: `show ether config` and press Enter.
   The Ethernet configuration displays. The example below show a TP port, the second example shows a Fiber Port:

   ```
   Agent III C1|S17|L1P1> show ether config
   Port-11040
   TP port:
   -----------------------------------------------------------------------------
   Link operation status: down
   Admin status: up
   Port mode: RJ-45
   PHY operation mode: phy10GBaseT
   Speed: 10G
   Duplex: full
   Autocross: auto
   AutoNeg admin state: enable
   Agent III C1|S17|L1P1>
   ```
Check Ethernet Port Config – Web Method

Use this procedure to define the transmission speed and Duplex mode to be used on the Ethernet port. The defaults are 10 Mbps and Full Duplex. **Note:** This command is only applicable on a copper port.

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. Select the appropriate port.

3. Locate the **Auto Negotiation Settings** section on the port’s **MAIN** tab.
Loopback Management

The x4120 provides a PHY Layer loopback test from the CLI and Web interface.

Loopback Management – CLI Method

Use this procedure to set the type of loopback test and to start and stop the selected loopback test.

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Set the Ethernet Loopback Type. At the command line, type: `set ether loopback type= xx`, where: `xx` = noloopback|phylayer.
3. Start the x4120 PHY Layer loopback test. At the command line, type: `set ether loopback oper=init` and press Enter.
4. Stop the x4120 PHY Layer loopback test. At the command line, type: `set ether loopback oper=stop` and press Enter.
5. For example:

   Agent III C1|S17|L1P1> set ether loop type no
   Agent III C1|S17|L1P1> set ether loop type phy
   Agent III C1|S17|L1P1> set ether loop type remote
   Error: Set Ethernet port loopback type failed.
   Agent III C1|S17|L1P1> set ether loop oper init
   Agent III C1|S17|L1P1> set ether loop oper stop
**Loopback Management – Web Method**

Use this procedure to perform a PHY Layer loopback test from the x4120 Web interface.

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
2. Select the appropriate port.
3. Locate the Loopback Management section on the port’s MAIN tab.
4. At the Loopback type dropdown, select **PHY Layer**.
5. Click the Start button to begin the Loopback test.
6. Click the Stop button to end the Loopback test. The Loopback Status field displays “Local In Loopback” during loopback test operation.
7. Click the Stop button. The loopback test ends, Loopback Status reverts to “No Loopback”, and the Loopback Type field reverts to “No Loopback”.
Section 4: Operation

General
This section describes the non-configuration operations that can be performed for the x4120.

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 x4120s in the ION system.

A Backup is used to get the SIC card running configuration, convert it to CLI commands, and save those CLI commands into the backup file. The backup file is stored in the IONMM.

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

A Restore is used to send the CLI commands in the configuration file to a SIC after removing the current SIC running configuration. If a problem causes the SIC card configuration restoration to stop (e.g., due to a lost network connection between the PC host and Agent card) the SIC card will use the previous configuration to run the traffic. If the IONMM card is downloading the restore configuration data to the SIC card, and the SIC card is physically removed from the chassis, the SIC card will use the factory default configuration setting when it is re-inserted into the chassis.

Transition Networks recommends that you to enter a “show card info” CLI command to view the SIC card’s current configuration before a backup/restore operation to verify the desired configuration settings. There are several CLI show commands that allow you to display (show) information about a SIC card’s configuration. For a complete description of these and other CLI commands see the x4120 CLI Reference Manual, 33497.

Displaying Information
There are several CLI commands that allow you to display (show) information about the x4120 configuration. For a complete description of these and other CLI commands see the x4120 CLI Reference Manual, 33552.
Reset to Factory Defaults

If need be, you can reset all configurations in the IONMM back to their original factory defaults. This operation can be accomplished through either the CLI or Web method.

IMPORTANT

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

Resetting Defaults – CLI Method

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. At the command prompt type: reset factory.

3. Press Enter. The following displays:

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

All configuration parameters will be reset to their factory values. For a list of all factory defaults, see “Appendix B: Factory Defaults” on page 179).

Note: Your USB and/or Telnet session will be disconnected.

4. Set the IP configuration (see “Doing the Initial System Setup” on page 48).
Resetting Defaults – Web Method

**Caution:** This operation deletes all configuration information that was saved in the x4120, including the IP address you assigned to the x4120.

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. Select the **MAIN** tab.

3. Locate the **System Configuration** section.

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

5. Click **Cancel** if you are sure you want to proceed with the Reboot. Click **OK** only if you wish to reboot.

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

   **Note:** Your Web session will be discontinued.

6. Set the IP configuration (see “Doing the Initial System Setup” on page 48).
File Status after Reset to Factory Defaults

The table below shows the status of x4120 files after a system re-boot.

Table 4: File Status after a Reset to Factory Defaults

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

The x4120 system uptime field displays the amount of time that the x4120 has been in operation.

The System Up Time is displayed in the format \textit{days:hours:minutes:seconds.milliseconds}. For example, a \textbf{System Up Time} field display of \textit{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 \textbf{System Up Time} counter can be reset via the CLI method or Web method.

\textbf{Reset System Uptime – CLI Method}

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. At the command prompt type: \texttt{reset uptime} and press Enter. The System Up Time field resets to zero, and immediately begins to increment.

   For example:
   
   \begin{verbatim}
   Agent III C1|S17|L1D>reset uptime
   Agent III C1|S17|L1D>
   \end{verbatim}
Reset System Uptime – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 26).

2. At the MAIN tab, locate the System Configuration section.

3. If desired, observe and record the System Up Time field count.

4. Click the Uptime Reset button.

5. At the “Uptime reset, are you sure” window, click OK to reset the system up time.

   The message “Setting values succeeded” displays at the bottom left of the screen when the up time reset is done.

6. Click the Refresh button at the bottom of the screen. The System Up Time field resets to zero, and immediately begins to increment.
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 – CLI Method
After a x4120 reboot via CLI while connected via USB port, you must disconnect and then reconnect USB cable for the console to become accessible again.

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. At the command prompt type: **reboot** and press **Enter**. A warning displays: *this command will restart system, connection will be lost and please login again!* The ION system reboots the x4120. If this operation is performed on a standalone module, the connection / session is terminated.

3. To reestablish the connection / session, wait about one minute, and then:

   • For a USB connection
     a) Select **Call>Disconnect**.
     b) Select **File>Exit**.
     c) Disconnect then reconnect one end of the USB cable.
     d) Start a USB session (see “Starting a USB Session” on page 41).

   • For a Telnet session
     a) Press **Enter**.
     b) Start a Telnet session (see “Starting a Telnet Session” on page 43).
Rebooting – Web Method

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

**Note:** If you have a USB or Telnet session established, terminate the session before doing the reboot.

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).
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 x4120 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 5: File Content and Location after a System Reboot

<table>
<thead>
<tr>
<th>File Type</th>
<th>Filename</th>
<th>File Description</th>
<th>Stored Directory</th>
<th>Lost after Reboot? (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning backup files</td>
<td>e.g., ‘1-1-IONMM.config’</td>
<td>These files are only used by provisioning Restore</td>
<td>/tftpboot</td>
<td>Yes</td>
</tr>
<tr>
<td>Net-SNMP configuration file</td>
<td>snmpd.conf</td>
<td>This file is a configuration file for Net-SNMP</td>
<td>/agent3/conf/snmp</td>
<td>No</td>
</tr>
<tr>
<td>HTTPS configuration file</td>
<td>lighttpd-ssl.conf</td>
<td>This file is a configuration file for HTTPS</td>
<td>/agent3/conf/lighttpd</td>
<td>No</td>
</tr>
<tr>
<td>HTTPS certificate file</td>
<td>server.pem</td>
<td>HTTPS certificate</td>
<td>/agent3/conf/lighttpd</td>
<td>No</td>
</tr>
<tr>
<td>SSH host key</td>
<td>dropbear_rsa_host_key</td>
<td>SSH host key files</td>
<td>/agent3/conf/lighttpd</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>dropbear_dss_host_key</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH user key file</td>
<td>authorized_keys</td>
<td>Currently we have one ‘root’ user; this file is the user key file for ‘root’</td>
<td>/root/.ssh</td>
<td>No</td>
</tr>
<tr>
<td>Syslog file</td>
<td>sys.log</td>
<td>The syslog file for IONMM</td>
<td>/tftpboot</td>
<td>No</td>
</tr>
<tr>
<td>MIB configuration files</td>
<td>e.g., ‘agent3.conf’</td>
<td>The MIB configuration files for SNMP setting</td>
<td>/agent3/conf</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>‘ifMib.conf’</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Upgrade the IONMM and/or x4120 Firmware

Occasionally changes must be made to the firmware version that is currently stored in IONMM or x4120 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. The latest firmware version is on the C4120 Product Resources page.

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.

**Note:** You cannot upgrade a module with multiple BIN files.

Remote Management in an Unmanaged Chassis

ION x4120 Version 1.2.6 was released August 12, 2016. This release added:

- Support for the management of a C4120 when installed in an unmanaged ION chassis. Management is supported by another C4120 installed in a managed chassis when the two are linked together via a fiber cable. On initial power up, additional time, approximately 1min & 10sec, is now required for the cards to be displayed in the management interface. This time is needed for the cards to determine if they are installed in a managed or an unmanaged chassis.

- Support for remote firmware upgrades of a C4120 in an unmanaged chassis. Remote firmware upgrades in an unmanaged chassis is supported only after a factory bootloader upgrade is performed. Remote firmware upgrades in an unmanaged chassis can take up to 3 minutes to transfer the file, reboot, search for management module, and display card in management interface.

For more information see “Local Management of Cards in a Remote Un-managed Chassis”.
Transfer Files via Serial Protocol (X/Y/Zmodem) – CLI Method

Use the `serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem)` commands to transfer a file over a serial line. These commands can only be entered at the device level (e.g., when the command line prompt is C1|S8|L1P1> or similar). These commands function like the TFTP download function; technical support can download configuration files and firmware files through the x4120 USB port by entering the corresponding CLI commands. If the serial file transfer causes HyperTerminal (HT) to have problems recognizing ION CLI commands, type q and press Enter, and then log back in to HT.

**General Usage:**

- `serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem) file=FILE%$

Perform this procedure to upgrade the x4120 firmware from the CLI.

1. Access the IONMM through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).
2. Sends a request to the server / local file system to download content for a subsequent `put` command. Type `serial get protocol zmodem file=xxxx` and press Enter.
3. Send a request to the server / local file system to upload content. Type `serial put protocol zmodem file=xxxx` and press Enter.
4. Perform a firmware upgrade over the selected serial line. Type `serial upgrade protocol zmodem file=xxxx` and press Enter.

For example:

```
C1|S1|L1D>serial ?
   get
   put
   upgrade
C1|S1|L1D>serial get protocol zmodem file=xxxx
Warning: the input file name will be ignored when using ymodem/zmodem to retrieve file!
now start to transfer the file ...
ŠCCCCCCCCCCCBBBBBBBBBBBBBBBBBBB
file transfer failed!
C1|S1|L1D>serial put protocol zmodem file=xxxx
now start to transfer the file ...
Š1ls: cannot open /tftpboot/xxxx: No such file or directory
      ↑│B'B0↑│B'B0↑│B'B0↑
      ↑│B'B0↑│B'B0↑│B'B0↑
Can't open any requested files.
      ↑│B'B0↑│B'B0↑│B'B0↑│B'B0↑
file transfer failed!
C1|S1|L1D>serial upgrade protocol zmodem file=xxxx
now start to transfer the file ...
**B000000063f694ceive.**B000000063f694
CCCCCCCCCCCCBB0BBB0BBB0BBB0BBB0BBB0BBB0BBB0
file transfer failed!
C1|S1|L1D>
```
Replacing a Chassis Resident C4120

The C4120 is a “hot swappable” device (it can be removed and installed while the chassis is powered on). To replace a chassis resident C4120, do the following.

1. Backup the configuration (see “Backing Up Slide-In and Remote Modules” on page 150).
2. Disconnect any cables attached to the x4120.
3. Loosen the panel fastener by turning it counterclockwise.
4. Pull the x4120 from the ION Chassis.
5. Carefully slide the new x4120 fully into the slot until it seats into the backplane.
6. Push in and rotate the attached panel fastener screw clockwise to secure the x4120 to the ION chassis.
7. Connect the appropriate cables to the x4120.
8. Load the configuration into the new x4120 (see “Restoring Slide-In and Remote Modules”).
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 x4120 and jumpers, and describes where and how to get technical support.

Note: 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 x4120s (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web Interface or ION command line interface - CLI).
- ION power supply
- ION options (ION SFPs, ION LG Kit, etc.)
- Data cables, electrical cables, and electrical outlets
- Third party network equipment (circuit protection equipment, battery backup, 3rd party client or server software – RADIUS or TFTP, etc.)

When troubleshooting an ION system / network problem on site:
1. Document the operation taking place when the failure occurred.
2. Capture as much information as possible surrounding the failure (the date and time, current configuration, the operation in process at the time the problem occurred, the step you were on in the process, etc.).
3. Start a log of your ideas and actions, and record where you were in the overall scheme of the system process (i.e., initial installation, initial configuration, operation, re-configuration, upgrading, enabling or disabling a major feature or function, etc.).
4. Write down the error indication (message, LED indicator, etc.). Take a screen capture if the problem displayed in software.
5. Start with the most simple and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the x4120s 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 before calling Transition Networks for support.

Error Indications and Recovery Procedures
The types of indications or messages reported include:

- LED Fault and Activity Displays (page 54)
- Problem Conditions (page 55)
- CLI Messages (page 57)
- Web Interface Messages (page 62)
- Windows Event Viewer Messages (page 82)
- Config Error Log (config.err) File (page 113)
- Webpage Messages (page 117)
- Third Party Troubleshooting Messages (page 120)

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.

Cannot access the x4120 via the Web Interface

1. Can you access the IONMM?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue with Step 2.</td>
<td>See “Cannot access the IONMM via the Web”.</td>
</tr>
</tbody>
</table>

2. Power cycle the x4120.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

Cannot upgrade modules

See Upgrade fails on page 177.

Cannot upload upgrade files

See Upgrade fails on page 177.
Configuration Mode Mismatch

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

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

1. Refer to the “Jumper Settings” section on page 312 for details on hardware mode configuration.

2. Contact Transition Networks for more information. See Contact Us on page 136.

Ethernet connection works, but at a very low speed

1. Check if the Auto Negotiate feature is enabled.

2. If Auto Negotiate is enabled, check if one device is using full duplex while the other one is using half-duplex (a duplex mismatch condition). The usual effect of this mismatch is that the connection works but at a very low speed.

3. Change Ethernet connection settings; see "Configuring Auto Negotiation" on page 77.

loading, please wait ... Displays continuously

1. Wait for one or more minutes for 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 136.
Parameter Boxes Outlined in Red / Cannot Enter Parameters

1. Check if the device is physically connected and powered on.

2. Verify the x4120 DIP switch settings and HW/SW Jumper setting.

3. Refresh the IONMM or x4120 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 136.
**Red box Condition after Reboot**

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

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

2. Check the devices’ firmware versions. For example, a C2220 has only certain items ‘red boxed’. The IONMM in this case is at latest version and shows certain new functions on the GUI, while the x4120 is at an older version and shows the newer functions as ‘red boxed’. Since the older version of x4120 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as ‘red boxed’. Upgrade the devices to the latest software version.

3. Reboot the system. See the “Reboot” section on page 115 for more information.

4. Contact Transition Networks for more information. See Contact Us on page 136.

**TFTP Server Address is empty or invalid!**

1. On a device MAIN tab, in the TFTP Settings section, you clicked the Save Server Address button with no TFTP Server Address entered, or with an invalid TFTP Server Address entered.

2. Enter a valid TFTP Server Address and click the Save Server Address button.

**Windows XP Cannot Find Drivers For My Device**

This error can occur if the information programmed into the device EEPROM do not match those listed in the INF files for the driver. If they do not match, the driver cannot be installed for that device without either reprogramming the device EEPROM or modifying the INF files.

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.


Driver Installation Fails and Windows XP Gives Error Code 10

Windows error code 10 indicates a hardware error or failed driver installation. This error may appear if a device has insufficient power to operate correctly (e.g. plugged into a bus powered hub with other devices), or may indicate a more serious hardware problem. Also, it may be indicative of USB root hub drivers being incorrectly installed.

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

Windows XP Displays an Error and then Terminates Installation

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

To successfully install the device, you must change the driver signing options to either warn or ignore 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 cannot 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.
CLI Messages

The following are messages that may appear during CLI (Command Line Interface) operations.

Ambiguous command

A. This message indicates either a) the input for one of the parameters is incorrect, or b) a hyphen is missing between two parts of the command.

1. Verify the CLI command syntax.
2. Retry the operation.

B. You typed part of a valid CLI command and pressed Enter before completing the command syntax. For example, if you type

C1|S7|L1D>add v

and then press the Enter key, the message “% Ambiguous command.” displays.

1. Type the part of the command that failed (add v in the example above), type a question mark (?), and the press Enter. The valid commands that start with the part of the command you initially entered are displayed.
2. Verify the CLI command syntax.
3. Retry the operation.

C. The system was unable to resolve the desired command based on the portion of the command entered. For example, you entered the following: C1|S7|L1D>set dot1

1. Verify the command syntax.
2. Retry the CLI command syntax.
3. See the x4120 CLI Reference Manual, 33497.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
**Bad advertisement capability!**

This message indicates that the capabilities specified for the Set Ethernet Port Advertisement Capability command are not valid choices.

1. Verify the command syntax.
2. Retry the operation. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Cannot get link pass through information on this card**

This message indicates that a link pass through (LPT) CLI command was entered for an IONMM. CLI commands for LPT operations are only valid for slide-in modules other than the IONMM. For example:

```
C1|S7|L1D>show lpt config
Cannot get link pass through information on this card!
C1|S7|L1D>
```

1. Use the go command to change from the IONMM to the specific slide-in module. The go command format is:
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
2. Retry the operation. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Cannot get OAM configuration on this port!**

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. The x4120 does not support this function. Use another command or use the go command to switch to a device that supports OAM.
2. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.
**Cannot get port security on this port!**

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the `go` command to change location of where the command operates. The `go` command format is: 
   ```
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
   ```
2. Retry the operation. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Command incomplete**

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

1. Verify the command syntax. Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
2. Retry the operation. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Could not open connection to the host on port 23. Connection failed.**

This message indicates that the Telnet server and client are configured for different ports. For Telnet operations the default port is 23.

1. Ensure that the Telnet port is set to 23 for both the server and the client. This will require someone with administrative rights in order to make a change.
2. Add the port number to the Telnet command. Example:
   ```
   Telnet <ipaddr> <port#>
   ```
3. If the problem persists, contact Technical Support. See Contact Us on page 136.
**Error: this command should be executed on a device**

This message indicates that the CLI command was entered for a port and it is only applicable for a device.

1. Use the `go` command to change location of where the command operates. The `go` command format is:
   ```
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
   ```
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Error: this command should be executed on a port**

This message indicates that the CLI command was entered for a card and it is only applicable for a port.

1. Use the `go` command to change location of where the command operates. The `go` command format is:
   ```
   go [c=CHASSIS] [s=SLOT] [l1ap=PORT] [l2ap=PORT] (l1p=PORT|l2p=PORT|l3p=PORT|l1d|l2d|l3d)
   ```
2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Fail to get MAC address!**

This message indicates that communications to the module cannot be established.

1. Verify that the correct hierarchy has been specified in the command (see “Managing Slide-In and Remote Modules Using CLI Commands” on page 49).
2. For all modules (slide-in and remote) check the following:
   - module is properly seated/connected
   - module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. **Note:** for slide-in modules, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.
6. If the problem persists, contact Technical Support. See Contact Us on page 136.
**Fail to get port type!**

This message indicates that a port level command was entered for the IONMM but the command is only valid for the other types of slide-in modules.

1. Use the `go` command to change location of where the command operates.

2. Retry the operation. For a complete list of the available commands, see the *x4120 CLI Reference Manual, 33497*.

3. If the problem persists, contact Technical Support. See [Contact Us](page 136).

**Failed to set DHCP client state!**

This message indicates a problem in the DHCP setup / configuration.

1. Verify the operation in the “Assigning a Dynamic IP Address” section on page 41.

2. Retry the operation. See the related DHCP command in *the x4120 CLI Reference Manual, 33497*.


**Failed to set current time**

**Failed to set SNTP state!**

**Failed to set SNTP daylight savings time state!**

**Failed to set timezone!**

**Failed to set SNTP server**

**Failed to set SNTP server!**

**Failed to set system contact**

**Failed to set system name**

**Failed to set system location!**

These messages indicate a problem in the SNTP setup / configuration.

1. Make sure this is the command / function you want.

2. See the commands in *the x4120 CLI Reference Manual, 33497*.

3. If the problem persists, contact Technical Support. See [Contact Us](page 136).
Error location parameter number!
Error: parameter out of range, chassis-id range is (0 .. 15)!
Error: parameter out of range, slot-id range is (1 .. 32)
Error: parameter out of range, slot-id range is (0 .. 32)
Incomplete location command!

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

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

1. Verify the command syntax.
2. Re-enter the go command and be sure to include all of the location parameters (chassis / slot / port) in the format:
   go [c=<1-16>] [s=<1-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d) for a slide in card, or
   go [c=<0-16>] [s=<0-32>] [l1ap=<1-15>] [l2ap=<1-15>] (l1p=<1-5>|l2p=<1-15>|l3p=<1-15>|l1d|l2d|l3d) for a standalone card.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

Invalid location parameters, cannot find the physical entity!

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

1. Verify that the correct hierarchy has been specified in the command (see “Managing Slide-In and Remote Modules Using CLI Commands” on page 29).
2. For all modules (slide-in and remote) check the following:
   • module is properly seated/connected
   • module is powered up
3. Wait 60 seconds then retry the operation.
4. Cycle power for the module in question. Note: for slide-in modules pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. Retry the operation.
6. If the problem persists, contact Technical Support. See Contact Us on page 136.
Invalid user!
This message indicates that the specified user is not valid.

1. Verify the user.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

Login incorrect
This message indicates that either the login or password entered while trying to establish a USB or Telnet connection is incorrect.

1. Verify the login/password.
   
   **Note:** the login and password are case sensitive. The default login is ION and the default password is private.
   
   2. Retry the operation.
   
   3. If the problem persists, contact Technical Support. See Contact Us on page 136.

No DMI support on this port!
This message indicates that you entered a DMI command for a port that does not support DMI.

1. Verify that the port supports DMI. For Transition Networks x4120s and SFPs, the model number will have a “D” at the end.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

There is no matched command
This message indicates that there is no such command available on this system.

1. Verify the command syntax.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.
Unable to open xx. Please check your port settings.
This message indicates that HyperTerminal no longer recognizes which COM port to use for its connection.

1. Check that the USB cable is connected to the management station and the IONMM.

2. Check that the COM port is listed for the device manager on the management station.
   a) On the desktop, right-click on My Computer.
   b) Select Manage.
   c) Click Device Manager.
   d) In the right panel, expand the list for COM & LPT.

3. Is the COM port in the list?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restart the management station (PC).</td>
</tr>
</tbody>
</table>

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

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

6. Restart the management station.

7. Reboot the IONMM.

8. If the problem persists, contact Technical Support. See Contact Us on page 136.
Error, you should first give full location parameters

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

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

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

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

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

for a slide in card.

**System is initializing...**

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

1. Wait for a few minutes for the message to clear.
2. Cycle power to the IONMM.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
This command is only available on <x222x / x32xx> card!
1. Verify the command entered is the one you want.
2. Verify that the device for the command entered can support the function of the command.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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

Unknown command!
The command you entered is not supported, or you entered the wrong command format / syntax.
1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

There is no matched command.
The command you entered is not supported, or you entered the wrong command format / syntax.
1. Verify the CLI command syntax.
2. Retry the operation.
3. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
Error location parameter number!
The `go` command you entered had an invalid or missing parameter.

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

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

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

```
C1[S3]L1D>set lpt state=enable
```
and then pressed Enter.

1. Verify the CLI command syntax.
2. Check the `set lpt monitor-port` and `set selective lpt state` command settings.
3. Enter the `show lpt config` command and in the Link Pass Through configuration, check if the Link pass through state is set to **notSupported** or if the Remote fault detect state is set to **notSupported**.

   If either is set to **notSupported**, change the setting to enable (e.g., type `set rfd state enable` and press Enter).

4. Retry the operation.
5. For a complete list of the available commands, see the `x4120 CLI Reference Manual, 33497`.
6. If the problem persists, contact Technical Support. See Contact Us on page 136.

TFTP transfer failed!
1. The attempted firmware upgrade via the `tftp upgrade` command was unsuccessful.
2. Verify the CLI command syntax.
3. Verify the firmware version.
4. Be sure the TFTP server is configured and running.
5. Check that the remote file is in the proper location (e.g., the file `x222x / x32xx.bin.0.5.4` is at `C:\TFTP-Root`).
6. Retry the operation. See the `tftp upgrade` command in the `x4120 CLI Reference Manual, 33497`.
7. If the problem persists, contact Technical Support. See Contact Us on page 136.
Fail to transfer the file!
The file transfer attempt failed. The command you entered to do a tftp file transfer was unsuccessful (e.g., tftp get or tftp put or tftp transfer).

1. Check the command syntax. See “TFTP Commands” page on page 117.
2. Make sure the TFTP server is configured and running.
3. Verify the filename to be transferred and the IP address of the TFTP server.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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

1. Retry the operation using the correct user information. See “Show SSH Public Key of a User” on page 116.
2. If the problem persists, contact Technical Support. See Contact Us on page 136.

Upgrade is only supported on IONMM card!
You entered a firmware upgrade or firmware update command from a device other than the IONMM. For example:

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
</tr>
<tr>
<td>C1</td>
</tr>
<tr>
<td>C1</td>
</tr>
<tr>
<td>C1</td>
</tr>
<tr>
<td>C1</td>
</tr>
</tbody>
</table>

1. Make sure of the command you want to enter. See “Firmware Upgrade Commands” on page 167.
2. Use the home command to go to the IONMM device.
3. Re-enter the firmware upgrade command from the IONMM.

**DMI is only supported on FIBER port!**

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

```
C1|S7|L1Pl>show dmi info
    DMI is only supported on FIBER port!
```

1. Verify if the card supports DMI.
2. Use the `go` command to switch to a different card port supporting Fiber.
3. Verify the command entry. See “DMI Commands” on page 55.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

**System is busy, please retry this command later!**

You entered a `show` or `set` command, but the command was not accepted by the system. For example:

```
C1|S10|L1D>show https config
    System is busy, please retry this command later!
C1|S10|L1D>
```

1. Wait 1-2 minutes and then retry the command.
2. Reboot the system and then retry the command.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Warning: this command will restart system, connection will be lost and please login again!**

Warm start failed.

You entered a `reboot` command, but the reboot was unsuccessful.

1. Wait 1-2 minutes and then retry the command.
2. If the problem persists, contact Technical Support. See Contact Us on page 136.
4 packets transmitted, 0 packets received, 100% packet loss

The attempted ping command failed. For example:

```
PING 192.168.1.10 (192.168.1.10): 56 data bytes
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

1. Verify the IP address.
2. Check the cable connection.
3. Refer to the **Ping** command section.
4. Retry the command.
5. If the problem persists, contact Technical Support. See **Contact Us** on page 136.

**Ping command can only be used on management card!**

The attempted ping command was not accepted by the system. For example:

```
C1|S5|L1D>ping 192.168.1.30
Ping command can only be used on management card!
```

1. Use the **go** command to switch to the IONMM card.
2. Refer to the **Ping** command section.
3. Retry the command.
4. If the problem persists, contact Technical Support. See **Contact Us** on page 136.

**Only 100M fiber port can set far end fault!**

The attempted far end fault command was not accepted by the system. For example:

```
C1|S16|L1P1>set ether fef enable
Only 100M fiber port can set far end fault!
```

1. Use the **go** command to switch to the 100M fiber port.
2. Re-enter the **fef** command.
3. Use an alternate Ethernet test command in place of the **fef** command.
4. If the problem persists, contact Technical Support. See **Contact Us** on page 136.
Please reboot the card for the changes to take effect!

You made a change that requires a system reboot in order for the change to take effect. For example:

```
C1|S5|L1D> set snmp traphost svr 1 type ipv4 addr 192.168.1.30
Please reboot the card for the changes to take effect!
C1|S5|L1D>
```

1. Reboot the card. See the “Reboot” section on page 292.
2. Continue the operation.
3. If a problem persists, contact Technical Support. See Contact Us on page 136.

Long Command Causes Cursor Wrap to Same Line

When the input command reaches the input max length, the cursor does not return to the next line, but back to the beginning of the same line, overwriting the original data.

1. Press the Enter key towards the end of the command string and continue entering command text.
2. Try using HyperTerminal or the Web interface, at least temporarily.
3. Contact Transition Networks for more information. See Contact Us on page 136.
Please change to power supply slot first before showing its configure!

You entered the show power config command from a device other than the power supply. For example:

```
C1|S16|L1D> show power config
Please change to power supply slot first before showing its configure!
C1|S16|L1D>
```

1. Make sure this is the command you want.
2. Verify the command syntax.
3. Use the go command to switch to the slot containing the power supply (typically slot 22 and/or 23).
4. Contact Transition Networks for more information. See Contact Us on page 136.

IP management is not supported on this card!
No tdm loopback supported on this card!
Syslog is not supported on this card!
TAOS status setting is not supported on this card!
TNDP is not supported on this card!

You entered a command for a function that is not supported on the x4120. For example:

```
C1|S15|L1D> set dhcp state disable
IP management is not supported on this card!
C1|S15|L1D>
```

1. Try another command on the x4120.
2. Try the command on another card that supports the attempted function.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

Cannot set if this port can be managed by CPU on this card!
Cannot set USB port state on this card!

tftp get: set address type failed.

You entered a tftp command, but the address entered was not accepted.

```
C1|S15|L1D> tftp get iptype ipv4 ipaddr 192.168.1.30 remotefile
x4120_1.0.4_AP
  tftp get: set address type failed.
C1|S15|L1D>
```

1. Make sure the tftp server address is valid.
2. Verify that the TFTP Server is running and properly configured.
3. Try entering the tftp command again.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
At one time we can only backup at most 10 cards!
At one time we can only restore at most 10 cards!
Backup finished
Error: this command should be executed on a device!
Error: this command should be executed on IONMM or a standalone SIC!
Fail to set card entity index!
Processing...
The MAX provision configure file name is 64!
The specified module does not exist!

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

1. Wait a few moments for the command to complete and the Restore finished or Backup finished message to display.
2. Retry the backup or restore operation with 10 or fewer devices listed.
3. Use the go command to switch to a device that supports this feature (IONMM or a standalone SIC).
4. Enter a config filename with less than 64 characters. See the “Configuring Backup / Restore” section on page 103.
5. If the problem persists, contact Technical Support. See Contact Us on page 136.

Cannot proceed because some other TFTP operation is currently in progress!
Please input config file name!
TFTP file transferring failed! Please make sure the TFTP server is up and the file being transferred does exist.
TFTP Server Address is empty or invalid!
The firmware has been successfully upgraded and the system will be rebooted soon
The specified firmware on the TFTP server will be upgraded to the current module, operation is currently in progress!
The sys.log file will be transferred to the TFTP server, are you sure to proceed?

You tried a TFTP transfer operation, but the operation failed or is still in process.

1. Wait for the "operation is currently in progress!" message to clear.
2. If an entry was requested in the message, enter the required information (e.g., valid TFTP Server address, or config file name).
3. Verify that this is the operation you want (e.g., click OK at the "are you sure to proceed?" message).
4. Verify the related command syntax in the applicable section of this manual (e.g., Syslog, or TFTP Upgrade section).
5. Retry the operation.
6. If the problem persists, contact Technical Support. See Contact Us on page 136..
Can't open any requested files.
cannot open /tftpboot/xxx: No such file or directory
now start to transfer the file ...
file transfer failed!
file transfer succeeded!
now start to upgrade the system ...
/usr/local/bin/flash_firmware /tftpboot/
upgrade failed!
upgrade failed due to wrong file %s!
upgrade succeeded, system will be rebooted ...
Usage: serial (get|put|upgrade) protocol=(xmodem|xmodem-1k|ymodem|zmodem) file=FILE
Warning: the input file name will be ignored when using ymodem/zmodem to retrieve file!
Warning: xmodem/xmodem-1k protocol might append some garbage at the end of the file!
Wrong parameter number!
You entered a Serial File Transfer command, but the operation failed.

1. Verify that this is the operation you want.
2. Retry the operation; be sure to type the parameters as shown in the “Transfer Files via Serial Protocol (X/Y/Zmodem)” section on page 103.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

File Transfer Failed - ZModem Crash Recovery dialog box:

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

1. Either enter the requested information and click **bps**, or click **Skip file**, or click **Cancel**.
2. See the HyperTerminal Helps or the Hilgraeve web site for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “Transfer Files via Serial Protocol (X/Y/Zmodem)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type **q** and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Technical Support. See Contact Us on page 136.
Receiving Files - No response from remote system

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

1. Click the **OK** button to clear the message dialog box.
2. See the HyperTerminal Helps or the [Hilgraeve web site](https://www.hilgraeve.com) for more HT information.
3. Retry the operation; be sure to type the parameters as shown in the “Transfer Files via Serial Protocol (X/Y/Zmodem)” section on page 103.
4. If the serial file transfer causes HT to have problems recognizing ION CLI commands, type *q* and press **Enter**, and then log back in to HT and retry the operation.
5. If the problem persists, contact Technical Support. See [Contact Us](https://www.transition.com) on page 136.

Cannot find software version of this card!

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

1. Check the card’s current firmware version.
2. Upgrade the card firmware. See "Upgrade the IONMM and/or x4120 Firmware” on page 107.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See [Contact Us](https://www.transition.com) on page 136.

Software version of this card is too old, please upgrade it!

The ION card’s firmware version was checked and found to be too old to support this newer CLI command.

1. Upgrade the card firmware. See "Upgrade the IONMM and/or x4120 Firmware” on page 107.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See [Contact Us](https://www.transition.com) on page 136.
This command is only valid on an IONMM!
Cannot show slot info on this card!

You entered a "show slot info" command on an ION card other than an IONMM card.

1. Enter another (supported) show command on this card, or use the "go" command to switch to the IONMM.
2. Retry the operation.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

ERROR Software version of this card ("cardVersion") is not supported, please upgrade to the same version as the IONMM
Getting card version failed
The failure get template config handler was called.

You attempted a function that is not supported by this version of firmware.

1. Enter another (supported) function at this card’s firmware version, or use the "go" command to switch to another card.
2. Upgrade to a newer firmware version. See “TFTP Transfer / Upgrade Commands” on page 204 or “Upgrade / Update Firmware Commands” on page 207.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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

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

1. Click the OK button to close the webpage message.
2. Select an ION device.
3. Click on Help > Online Help again.
ERROR: Software version of this card (0.7.1) is not supported, please upgrade to the same version as the IONMM

You selected a device in the tree, but its firmware version is not compatible with the IONMM.

1. Select the IONMM device.
2. Select the UPGRADE tab.
3. Perform a firmware upgrade to this card (and others that may have outdated firmware). See the Upgrade section on page 347.
4. If a problem persists, contact Technical Support. See Contact Us on page 136.

Failed to retrieve DMI info on current port

You selected C3230 > Port 2 > DMI but the DMI information does not display.

1. Click Refresh.
2. Expand and contract the tree.
3. If a problem persists, contact Technical Support. See Contact Us on page 136.
Current power status of this slot is off, please turn it on before you reset it!
The reset function only works when the slot power is in the On position for the unit to reboot/reset.

1. At Chassis > MAIN > Chassis Members click the "On" button in the Power Status column of the
device before you click the "Reset" button.

2. If a problem persists, contact Technical Support. See Contact Us on page 136.

Setting the VLANID failed with an SNMP operation error message:
Setting values failed (snmp operation error) or
Adding VLAN failed (snmp operation error)
You tried to add or edit a VLAN ID but the effort failed.

1. The card must be in “Network” mode (at Port 1 > Advanced > Frame Tag Mode) to set the VLAN
ID. If it is not set to "Network", an SNMP error will occur. Before adding the ports for Management
VLAN, set the Frame Tag Mode of that port to "Network". When Provider tagging is required for that
port, then set the Frame Tag Mode to "Provider". A port with the Frame Tag Mode set to the default
setting "Customer" cannot be added to Member Ports for Management VLAN.

2. If a problem persists, contact Technical Support. See Contact Us on page 136.

Cannot clear loopback counters on this card!
Cannot set administrate state on this port!
Cannot set advertisement capability on this port!
Cannot set auto cross on this card!
Cannot set auto negotiation state on this port!
Cannot set Ethernet port speed for this card!
Cannot set Ether port duplex mode on this card!
Cannot set far end fault on this card!
Cannot set filter unknown dest multicast frames on this port!
Cannot set filter unknown dest unicast frames on this port!
Cannot set pause on this port!
Cannot set source address lock action on this port!
Cannot get port security configuration on this port!
Fail to get MAC control frames statistics!
Cannot show forwarding port list on this card!
Cannot show slot info on this card!
Cannot show USB port state on this card!
Cannot show USB port configure on this card!
Cannot show TP port cable length on this card!
Cannot set management VLAN on this card!
Cannot set PHY mode on this port!
Cannot clear counters on this port!
Cannot reset all ports' counters on this card!
Cannot set remote fault detect state on this card!

You entered a command for a function not supported on the card.
1. Verify the command entry.
2. Verify if the card supports the desired function.
3. Use the go command to switch to a different card port supporting VLAN.
4. Verify the command entry.
5. If the problem persists, contact Technical Support.
Fail to set aging time!
Get aging time failed!
CLI command remove fwddb all failed
Redundancy is not supported on this card!
Fail to set SSH server state!
Fail to set management VLAN id!
Fail to set management VLAN state!
Cannot show port QoS configuration in this card!
Cannot set tag type for priority in this card!
Cannot set default priority in this card!
Cannot set IEEE tag for priority in this card!
Cannot set VLAN network tagging on this port!
Cannot show system information on this card!
Cannot create VLAN database on this card!
Cannot remove vlan on this card!
Cannot remove forward database rows on this card!
Cannot set bandwidth alloc type on this card!
Cannot set ingress and egress rate on this card!
The specified conn-port does not exist!
The specified monitor-port does not exist!
Cannot show cable length for fiber port!
Get DMI identifier no such object.
Get SNMP version no such object.
Fail to get cable length
Can not set speed on this port!
Fail to set port advertisement capability!
Fail to get system name!
Set system name timeout.
Get HTTPS state no such object.
Get management VLAN state no such object.
IP management state no such object.
L2CP is not supported on this card!
Link OAM is not supported on this card!
No Time-domain reflectometer support on this card!

You entered a command for a function not supported on the card.
6. Verify the command entry.
7. Verify if the card supports the desired function.
8. Use the go command to switch to a different card port supporting VLAN.
9. Verify the command entry.
10. If the problem persists, contact Technical Support. See Contact Us on page 136.
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 136.

Cannot Ping IONMM Device

1. With the "Management VLAN" state set to "enabled", the PC cannot 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 136.

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 136.
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 136.

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 136.

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

1. Verify the parameter value entered; see “Upgrading IONMM Firmware – Web Method” on page 120 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 136.
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 136.

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 136.

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 x4120 supports DMI.
2. See “DMI (Diagnostic Maintenance Interface) Parameters” on page 118 for more information.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

Admin Status: Down (or Testing)

In the device’s port, at the MAIN tab in the Port Configuration section, the Admin Status field displays “Down”. Typically, if 'Admin Status' is Down, then 'Link Status' is also Down.

The status here is the desired state of the interface. The “Testing” status indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with 'Admin Status' in the Down state. As a result of either explicit management action or per configuration information retained by the managed system, 'Admin Status' is then changed to either the Up or Testing states, or remains in the Down state.

1. Verify the initialization process; see “Section 2: Installation and System Setup” on page 40.
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization to take place.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
**Link Status: Down (or Testing or Dormant, or NotPresent)**

This is the current operational state of the interface.

The 'Link Status' Testing state indicates that no operational packets can be passed.

If 'Admin Status' is Down then 'Link Status' likely will be Down.

If 'Admin Status' is changed to Up, then 'Link Status' should change to Up if the interface is ready to transmit and receive network traffic.

'Link Status' should change to Dormant if the interface is waiting for external actions (such as a serial line waiting for an incoming connection);

'Link Status' should remain in the Down state if and only if there is a fault that prevents it from going to the Up state;

'Link Status' should remain in the NotPresent state if the interface has missing (typically, hardware) components.

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

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see “Section 2: Installation and System Setup” on page 40.
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization to take place.
5. If the problem persists, contact Technical Support. See Contact Us on page 136.

**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 136.

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

1. Verify the ION system installation; see “Section 2: Installation and System Setup“ on page 40.
2. Wait several minutes for initialization to take place, and then retry the operation.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**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 136.
**Message: Setting values failed (http server error)**

This message indicates a configuration entry error (e.g., https).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See “Configuring HTTPS” on page 208.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Message: Setting values failed (snmp operation error)**

This message indicates that the SNMP Configuration entered had an invalid SNMP entry (e.g., an unrecognized Trap Manager address entry).

1. Enter a valid value. Refer to the Help screen for more information.
2. Retry the operation. See “Configuring SNMP” on page 226.
3. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Message: TFTP file transferring failed!**

This message indicates that a TFTP operation could not be completed.

**TFTP for Backup download operation:**

1. Verify that:
   a. The correct module(s) has been selected.
   b. The IP address of the TFTP server is correct.
   c. The TFTP server is online and available.
2. Perform a backup of the module(s) for which the download operation was intended. Make sure that the status of the backup operation for each module is “Success”.
3. Retry the operation.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
TFTP for Restore upload operation:

1. Check:
   - The IP address of the TFTP server is correct.
   - The TFTP server is online and available.
   - The file to be uploaded is in the default directory on the server.
   - The correct module(s) has been selected.

2. Retry the operation.

3. If the problem persists, contact Technical Support. See Contact Us on page 136.

Message: TFTP operation failed!

This message indicates that the upload portion of an upgrade operation failed.

1. Check:
   - The IP address of the TFTP server is correct.
   - The TFTP server is online and available.
   - The correct file name (`db.zip` in Windows XP or just “`db`” in Windows 7) is specified.
   - The `db.zip` (or `db`) file is in the default directory on the TFTP server.

2. If the problem persists, contact Technical Support. See Contact Us on page 136.

Message: There is a problem with this website's security certificate.

This message indicates that the security certificate presented by this website was changed.

1. Click the Continue to this website... selection.

2. See the “Configuring HTTPS” section on page 192.
Message: *Web UI Management connection Lost*

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device (e.g., S2220-1013).

2. After reducing the "Egress Rate Limit" to "80m", the ping fails. The return traffic to the PC is non-mgmt packet and is subjected to Egress rate-limiting, hence these packets are getting dropped.

3. Increase the port 1 "Egress Rate Limit" to "900m" or "800m" to reserve some Egress bandwidth for user management traffic. The PC can ping to S2220-1013 again, and the WEB UI can be managed again.

4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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 JavaScript file succeeded
   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 136.

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

**Meaning:** Not all x4120 models support DMI. Transition Networks x4120s that support DMI have a “D” at the end of the model number. If you click the DMI tab on a x4120 model that does not support DMI, the message “The DMI feature is not supported on current port.”

The DMI (Diagnostic Maintenance Interface) function displays x4120 diagnostic and maintenance information such as interface characteristics, diagnostic monitoring parameters, and supported media lengths.
**Recovery:** 1. Verify that the device and port support DMI. See “DMI (Diagnostic Maintenance Interface) Parameters” on page 248 for more information.

**Message:** 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 136.

**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 136.

**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.
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 page 266.
5. Check the Microsoft Support Online website [http://support.microsoft.com/ph/807/en-us/#tab0](http://support.microsoft.com/ph/807/en-us/#tab0) for more information.
   [http://support.microsoft.com/kb/960321](http://support.microsoft.com/kb/960321)
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](http://support.microsoft.com/kb/956197).
Script error message received.

Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues, your computer might become unresponsive. Yes / No

Error: Object doesn't support this property or method.

A Runtime Error has occurred. Do you wish to Debug?

Done, but with errors on page.

1. Click the Yes button to stop the script.
2. Click Show Details to display error details.
3. Disable script debugging.
4. Test a Web page from another user account, another browser, and another computer.
5. Verify that Active Scripting, ActiveX, and Java are not being blocked by Internet Explorer.
6. Remove all the temporary Internet-related files.
7. Install the latest Internet Explorer service pack and software updates.
8. For more advanced troubleshooting, see the Microsoft Support Article ID 308260 at [http://support.microsoft.com/kb/308260](http://support.microsoft.com/kb/308260).
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 7036 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 136.
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.

```
AGENT PK ERROR: CLI command remove vian all failed
AGENT PK ERROR: CLI command set ip-mget state=enable failed
AGENT PK ERROR: CLI command set dhcp state=disable failed
AGENT PK ERROR: CLI command set ip type=ipv4 addr=192.168.0.10 subnet-mask=255.255.255.0 failed
AGENT PK ERROR: CLI command set gateway type=ipv4 addr=192.168.0.1 failed
AGENT PK ERROR: CLI command set dns-srv srv=1 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set dns-srv srv=2 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set dns-srv srv=3 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set dns-srv srv=4 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set dns-srv srv=5 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp transport srv=1 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp transport srv=2 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp transport srv=3 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp transport srv=4 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp transport srv=5 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp state=disable failed
AGENT PK ERROR: CLI command set smtp dst-state=disable failed
AGENT PK ERROR: CLI command set smtp timeout=0 failed
AGENT PK ERROR: CLI command set smtp dst-end="1969 1231 18:00:00" failed
AGENT PK ERROR: CLI command set smtp dst-offset=0 failed
AGENT PK ERROR: CLI command set smtp srv=1 type=dns addr=0.0.0.0 failed
AGENT PK ERROR: CLI command set smtp srv=2 type=dns addr=0.0.0.0 failed
```

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”.

33551 Rev. B  https://www.transition.com/  Page 98 of 183
**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=01:00:00:00:10 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=01:00:00:00:02 conn-port=1 priority=1 type=staticNRL failed
7 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:03 conn-port=1 priority=1 type=staticNRL failed
8 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:04 conn-port=1 priority=1 type=staticNRL failed
9 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:05 conn-port=1 priority=1 type=staticNRL failed
10 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:06 conn-port=1 priority=1 type=staticNRL failed
11 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:07 conn-port=1 priority=1 type=staticNRL failed
12 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:08 conn-port=1 priority=1 type=staticNRL failed
13 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:09 conn-port=1 priority=1 type=staticNRL failed
14 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:10 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=01:00:00:00:02 conn-port=1 priority=1 type=staticNRL failed
18 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:03 conn-port=1 priority=1 type=staticNRL failed
19 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:04 conn-port=1 priority=1 type=staticNRL failed
20 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:05 conn-port=1 priority=1 type=staticNRL failed
21 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:06 conn-port=1 priority=1 type=staticNRL failed
22 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:07 conn-port=1 priority=1 type=staticNRL failed
23 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:08 conn-port=1 priority=1 type=staticNRL failed
24 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:09 conn-port=1 priority=1 type=staticNRL failed
25 AGENT PM ERROR: CLI command add fwddb mac=01:00:00:00:10 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=01:00:00:00:10 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 x4120 CLI Reference Manual, 33497. 4. If the problem persists, contact Technical Support. See Contact Us on page 136.

**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 136.

**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 136.
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 136.

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 x4120 CLI Reference Manual, 33497. 4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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 x4120 CLI Reference Manual, 33497. 4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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 136.

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 136.

Message: set snmp state=disable  failed  
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. 
See Contact Us on page 136.

Message: set snmp 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 136.

Message: set snmp timezone=8  failed  
Response: 1. Check if this command is supported. 2. If the problem persists, contact Technical Support. 
See Contact Us on page 136.

Message: set snmp 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 136.

Message: set snmp 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 136.

Message: set snmp-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 136.

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 136.

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 136.

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 136.

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 136.

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 136.

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 136.

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 136.

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 136.
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” on page 44.

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: The firmware upgrade failed!

The MAIN tab > TFTP Settings section Status area displays “TFTP Failure”.

**Meaning:** While performing a Firmware Upgrade from the MAIN tab > TFTP Settings section, a problem was detected. See the “Upgrade the IONMM and/or x4120 Firmware” section on page 109.

**Recovery:**

1. Click OK to clear the webpage message.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Transition Networks website.
4. Verify the TFTP Server Address entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
5. Verify the Firmware File Name that you entered is the one you intended, and that it is in the proper filename format (e.g., IONMM.bin.0.5.3).
6. Check the log status in the TFTP Server package; when successful, it should show something like “Sent IONMM.bin.0.5.3 to (192.168.1.30), 9876543 bytes”. The TFTP Settings section Status area should display “Success” when done.
7. Make sure that the Management VLAN function is disabled.
8. Reset the IONMM card. The TFTP Settings section Status area should display “Success” when done.
9. If the problem persists, contact Technical Support. See Contact Us on page 136.
Message: Failed to Transfer the Firmware Database File!

Meaning: A problem was detected while performing a Firmware Upgrade from the x4120 MAIN tab > TFTP Settings section or from the IONMM UPGRADE tab. See “Upgrade the IONMM and/or x4120 Firmware” on page 109.

Recovery:
1. Click OK.
2. Make sure you are using a TFTP Server package (not an FTP package). You will not be able to connect to the TFTP Server with an FTP client.
3. Make sure that you downloaded the correct IONMM firmware file from the Transition Networks website.
4. Make sure the TFTP server is running and correctly configured.
5. Verify the TFTP Server Address entry. It should be the IP address of your TFTP Server (e.g., 192.168.1.30).
6. Verify the Firmware File Name that you entered is the one you intended, and that it is in the proper filename format (e.g., IONMM.bin.0.5.3). Include the filename extension if you have not done so.
7. Check the log status in the TFTP Server package; when successful, it should show something like “Sent IONMM.bin.0.5.3 to (192.168.1.30), 9876543 bytes”. The TFTP Settings section Status area should display “Success” when done.
8. Reset the IONMM card. The TFTP Settings section Status area should display “Success” when done.
9. If the problem persists, contact Technical Support. See Contact Us on page 136.
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” on page 44.
6. If the problem persists, contact Technical Support. See Contact Us on page 136.
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” on page 44.

6. If the problem persists, contact Technical Support. See Contact Us on page 136.
Message: *The Connection was Reset*

![The connection was reset]

Meaning: The FireFox web browser connection failed to load the page.

Recovery:
1. Verify the URL (e.g., http:// versus https://).
2. Check if the applicable server is running (TFTP, Syslog, HTTPS server) in the expected location.
3. Click the **Try again** button to retry the operation.

Message: *This Connection is Untrusted*

![This Connection is Untrusted]

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

Recovery: Click **Technical Details** for details, or click **I Understand the Risks** to continue operation.
Message: Static Non Rate Limit entry must have a multiple cast MAC address!

Meaning: When setting up MAC filtering, you entered a unicast MAC address and selected a Static NRL (Non Rate Limit) Entry Type.

Recovery:
1. Click OK to clear the message.
2. Either enter a multicast MAC Address, or select another Entry Type.

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

Meaning: You unplugged the USB cable at the x4120 or IONMM, or the x4120 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 x4120’s USB connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
**Message: Problem loading page – Mozilla Firefox**

Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

Recovery:

1. Make sure the web browser you are using is supported. See “Web Browsers Supported” on page 72.
2. Verify the URL entered. See “Initial Setup with a Static IP Address via the CLI” on page 59.
3. Verify x4120 access. See “Accessing the x4120” on page 60.
4. Verify the IP address setting. See “Setting the IP Addressing” on page 89.
5. Verify the URL (e.g., http:// versus https://).
6. Try to log in to the ION system again.
7. If the problem persists, contact Technical Support. See Contact Us on page 136.

**Message: Internet Explorer cannot display webpage**

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

Recovery:

1. Make sure the web browser you are using is supported. See “Web Browsers Supported” on page 42.
2. Verify the URL entered. See “Initial Setup with a Static IP Address via the CLI” on page 49.
3. Verify NID access. See “Accessing the x4120” on page 50.
4. Verify the IP address setting. See “Setting the IP Addressing” on page 69.
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 136.
**Message:** Upgrade following modules: [15]x4120, are you sure to proceed?

**Meaning:** Verification message that you indeed want to upgrade the x4120 firmware.

**Recovery:**
1. If you are **not** sure you want to upgrade the x4120 firmware, click **Cancel** and continue operation.
2. If you are **sure** you want to upgrade the x4120 firmware, click **OK**. The upgrade process will continue.

See “Upgrade the IONMM and/or x4120 Firmware” in the IONMM User Guide.
DMI (Diagnostic Maintenance Interface)

The DMI (Diagnostic Maintenance Interface) function displays x4120 diagnostic / maintenance information 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. DMI can be configured in the x4120 using either the CLI or Web method.

**DMI Config – CLI Method**

1. Access the x4120 through either a USB connection (see “Starting a USB Session” on page 41) or a Telnet session (see “Starting a Telnet Session” on page 43).

2. Set the Diagnostic Monitoring Interface receive preset power level. Type: `set dmi rx-power-preset-level=xx` where xx is a preset level for Rx Power on the Fiber port, in the range of 1 to 10.

3. Press Enter. For example: `set dmi preset-power-level=10`.

4. Display the DMI information. Type: `show dmi info` and press Enter. For example:

   ```
   Agent III C1|S17|L1P2> set dmi preset-power-level=10
   Agent III C1|S17|L1P2> show dmi info
   Diagnostic monitoring interface information:
   +---------------------------------------------------------------+
   | DMI connector type: LC | DMI identifier: SFP | DMI Nominal bit rate: 10500*Mbps |
   | DMI 9/125u Singlemode Fiber (m): N/A | DMI 50/125u Multimode Fiber (m): 80*m |
   | DMI 62.5/125u Multimode Fiber (m): 3*10m | Copper(m): N/A |
   | DMI fiber interface wavelength: 850*nm | DMI temperature: 42.0*C |
   | DMI temperature: 107.6*F | DMI temperature alarm: normal |
   | DMI transmit bias current: 6240*uA | DMI transmit bais alarm: normal |
   | DMI Transmit power: 589*uW | DMI Transmit power alarm: normal |
   | DMI Receive power: -2.299*dBM | DMI Receive power: -2.418*dBM |
   | DMI Receive power alarm: normal | DMI Receive power intrusion threshold: 0*uW |
   +---------------------------------------------------------------+
   Agent III C1|S17|L1P2>
   ```

The DMI tab parameters are described in the table below.
DMI Config – Web Method

1. Access the x4120 through the Web interface (see “Starting the Web Interface” on page 45).

2. Select the desired device and port.

3. Select the DMI tab.

   ![DMI Configuration Table]

   The Interface Characteristics, Diagnostic Monitoring, and Supported Media Length information fields 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 6: DMI Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Possible Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMI ID</td>
<td>Unknown, GBIC, soldered to motherboard, SFP, Reserved, vendor-specific</td>
<td>Specifies the physical device from SFF-8472 Rev 9.5 Standard: 00h Unknown or unspecified 01h GBIC 02h Module/connector soldered to motherboard 03h SFP 04-7Fh Reserved 80-FFh Vendor specific</td>
</tr>
<tr>
<td>Nominal Bit Rate</td>
<td>(measured rate)</td>
<td>Bitrate in units of 100Mbps (the sample screen above shows 1300, or 1.3 Gbps).</td>
</tr>
<tr>
<td>Fiber Interface Wavelength</td>
<td>(measured wavelength)</td>
<td>The Nominal transmitter output wavelength at room temperature. The unit of measure is nanometers (the sample screen above shows 850 nm).</td>
</tr>
<tr>
<td>Receive Power (uW)</td>
<td>(measured power measurement)</td>
<td>Receive power on local fiber measured in microwatts (the sample screen above shows 11 uW).</td>
</tr>
<tr>
<td>Receive Power (dBm)</td>
<td>(measured signal strength)</td>
<td>Receive power on local fiber measured in dBm (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -19.586 dBm.</td>
</tr>
<tr>
<td>Receive Power Alarm</td>
<td>Normal -1, Not Supported - 2, Low Warn - 3, High Warn - 4, Low Alarm - 6, High Alarm - 7</td>
<td>Alarm status for receive power on local fiber.</td>
</tr>
<tr>
<td>Rx Power Intrusion Threshold (uW)</td>
<td>0-10</td>
<td>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.</td>
</tr>
<tr>
<td>Temperature (°C)</td>
<td>(measured temp.)</td>
<td>Temperature of fiber transceiver in tenths of degrees C (Celsius). The sample screen above shows 40.1°C.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Temperature (°F)</td>
<td>Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). The sample screen above shows 104.2 °F.</td>
<td></td>
</tr>
<tr>
<td>Temperature Alarm</td>
<td>Alarm status for temperature of fiber transceiver. An ionDMI\textit{TemperatureEvt} event is sent when there is a warning or alarm on DMI temperature.</td>
<td></td>
</tr>
<tr>
<td>Transmit Bias Current (uA)</td>
<td>Transmit bias current on local fiber interface, in uA (microamperes). The sample screen above shows 14768 uA (microamps).</td>
<td></td>
</tr>
<tr>
<td>Transmit Bias Alarm</td>
<td>Alarm status for transmit bias current on local fiber interface.</td>
<td></td>
</tr>
<tr>
<td>Transmit Power (uW)</td>
<td>Transmit power on local fiber measured in microwatts. The sample screen above shows 240 uW (microwatts).</td>
<td></td>
</tr>
<tr>
<td>Transmit Power (dBm)</td>
<td>Transmit power on local fiber measured in dB (decibels relative to one milliwatt) which defines signal strength. The sample screen above shows -6.126 dB.</td>
<td></td>
</tr>
<tr>
<td>Transmit Power Alarm</td>
<td>Alarm status for transmit power on local fiber.</td>
<td></td>
</tr>
<tr>
<td>Supported Media Length</td>
<td>Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). The sample screen above shows N/A, indicating the media is not applicable.</td>
<td></td>
</tr>
<tr>
<td>9/125u Singlemode Fiber (m)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50/125u Multimode Fiber (m)</td>
<td>Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 500 meters as the supported media length.</td>
<td></td>
</tr>
<tr>
<td>62.5/125u MM Fiber (m)</td>
<td>Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters. The sample screen above shows 300 meters as the supported media length.</td>
<td></td>
</tr>
<tr>
<td>Copper (m)</td>
<td>Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters. The sample screen above shows N/A, indicating the media is not applicable.</td>
<td></td>
</tr>
</tbody>
</table>
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
           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`.

![Command Prompt](image)

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.

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 Configuration window](image)

PuTTY SSH Options:

![PuTTY Configuration window](image)
**Tracert (Traceroute)**

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

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

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

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

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

Tracert options include:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


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.
**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.
Third Party Tool Messages

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

HyperTerminal Messages

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

Response:

1. Verify your computer’s Ports (COM & LPT) setting. See “Configuring HyperTerminal” on page 53.
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.

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

Response:

1. Verify your computer’s Ports (COM & LPT) setting. See “Configuring HyperTerminal” on page 53.
2. Use the **Computer Management > Device Manager > Troubleshooter** button located on the **General** tab in **Properties**.
3. Unplug and re-plug the USB connector on the IONMM card.
4. If the problem persists, contact Technical Support. See Contact Us on page 136.
**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.*

![Command Prompt]

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.*

![Command Prompt]

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!*

```
   CLI> go c=1 s=7 1iap=3 12ap=3 13d
   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 136.

Message: *Unknown command!*

```
   CLI> go c=1 s=7 1iap=3 12ap=3 13d
   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 *x4120 CLI Reference Manual, 33497.*
TFTP Server Messages

Messages like the ones below may display during TFTP Server operation, depending on the TFTP Server package that you selected.

Message: File does not exist

Meaning: A TFTP Server error - the TFTP Server Address that you specified does not contain the Firmware File Name specified.
Recovery: 1) Verify the TFTP server’s correct file location (e.g., local disk at C:\TFTP-Root). 2) Make sure of the filename / extension. 3) Check the TFTP Server’s online helps for suggestions.

Message: File too large for TFTP Protocol

Meaning: A TFTP Server error - you tried to upload a file e.g., (IONMM.bin.0.5 – 50Mb) but the TFTP server failed. The file you tried to upload via the TFTP server exceeded the file size capability.
Recovery: 1) Check if some extra files ended up in the zip folder – some repeated – 6 FW files total. 2) Remove some of the files from the zip folder and try the upload again. 3) Send the remaining files in a separate file. 4) Check the TFTP Server’s online helps for suggestions.
PuTTY Messages

Messages like the ones below may display during PuTTY (or similar package) operation, depending on the package that you selected.

Message: Server refused key

Meaning: You can connect to a secure telnet session using password authentication, but when you try to connect using public key authentication, you receive a "Server refused our key" message on the client (PuTTY) session. For example, you generated a public/private key (using Puttygen) and saved them, loaded the client public key into the IONMM via TFTP, and enabled SSH. The PuTTY SSH Authentication pointed to the saved private key. You set the auto-log on user name to root as suggested, but when you activated PuTTY, after 20-30 seconds, the refusal message displayed and PuTTY reverted back to password authentication (the default).

Recovery:
1. When generating using puttyGen.exe, select the SSH2 keys - do not select the SSH1 keys.
2. Log in to PuTTY as 'root' with the public key authentication.
3. Use the online helps and documentation to set up Putty as suggested.
4. See the “PuTTY” section notes on page 408.

Technical Support

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
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: ____________________
   - Device Description: ____________________________________________
4. Provide additional Model and System information to your Technical Support Specialist. See “Basic ION System Troubleshooting” on page 151.

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

Warranty
This warranty is your only remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Transition Networks is not liable for any special, indirect, incidental or consequential damages or losses, including loss of data, arising from any cause or theory. Authorized resellers are not authorized to extend any different warranty on transition networks’ behalf.

Limited Lifetime Warranty
To return a defective product for warranty coverage, contact Transition Networks’ technical support department for a return authorization number. Transition Network’s technical support department can be reached 24-hours a day by any of the following means:

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

Warranty
Transition Networks warrants to the original consumer or purchaser that this product and all components thereof, will be free from defects in material and/or workmanship for a period of five years from the original factory shipment date. Any warranty hereunder is extended to the original consumer or purchaser and is not assignable. Transition Networks makes no express or implied warranties including, but not limited to, any implied warranty of merchantability or fitness for a particular purpose, except as expressly set forth in this warranty. In no event shall Transition Networks be liable for incidental or consequential damages, costs, or expenses arising out of or in connection with the performance of the product delivered hereunder. Transition Networks will in no case cover damages arising out of the product being used in a negligent fashion or manner.

This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside of the product’s specified rating, or normal wear and tear of mechanical components.

Transition Networks will, at its option:
• Repair the defective product to functional specification at no charge
• Replace the product with an equivalent functional product
• Refund a portion of purchase price based on a depreciated value

To return a defective product for warranty coverage, contact Transition Networks’ Customer Support for a return authorization number.

Send the defective product postage and insurance prepaid to the following address:
Transition Networks, Inc.
10900 Red Circle Drive
Minnetonka, MN 55343
USA
Attn: RETURNS DEPT: CRA/RMA # ____________

Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number. CRA’s are valid for 60 days from the date of issuance. An invoice will be generated for payment on any unit(s) not returned within 60 days.

Upon completion of a demo/evaluation test period, units must be returned or purchased within 30 days. An invoice will be generated for payment on any unit(s) not returned within 30 days after the demo/evaluation period has expired.

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer’s responsibility).

Before making any non-warranty repair, Transition Networks requires a $200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than $200.00, an estimate is issued to the customer for authorization of repair. If no authorization is obtained, or the product is deemed not repairable, Transition Networks will retain the $200.00 service charge and return the product to the customer not repaired. Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge a $50 fee for all testing and shipping incurred, if after testing, a return is classified as “No Problem Found.”

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. TRANSITION NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY. AUTHORIZED RESELLERS ARE NOT AUTHORIZED TO EXTEND ANY DIFFERENT WARRANTY ON TRANSITION NETWORKS’S BEHALF.
Compliance Information

Standards       CISPR22/EN55022 Class A, CE Mark

FCC Regulations: NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Marking: This is a Class A product. In a domestic environment, this product could cause radio interference; as a result, the customer may be required to take adequate preventative measures.

UL Recognized: Tested and recognized by the Underwriters Laboratories, Inc.

Canadian Regulations: This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Regulations

WARNING:

This is a Class A product. In a domestic environment, this product could cause radio interference in which case the user may be required to take adequate measures.

Achtung!

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fäll ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention!

Ceci est un produit de Classe A. Dans un environment domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les measures spécifiques appropriées.

In accordance with European Union Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, Transition Networks will accept post usage returns of this product for proper disposal. The contact information for this activity can be found in the 'Contact Us' portion of this document.

CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.
Der Anschluss dieses Gerätes an ein öffentliches Telekommunikationsnetz in den EG-Mitgliedstaaten verstoßt gegen die jeweiligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

**Electrical Safety Warnings**

**Electrical Safety**
**IMPORTANT:** This equipment must be installed in accordance with safety precautions.

**Elektrische Sicherheit**
**WICHTIG:** Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

**Elektrisk sikkerhed**
**VIGTIGT:** Dette udstyr skal installeres i overensstemmelse med sikkerhedsadvarslerne.

**Elektrische veiligheid**
**BELANGRIJK:** Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

**Sécurité électrique**
**IMPORTANT:** Cet équipement doit être utilisé conformément aux instructions de sécurité.

**Sähköturvallisuus**
**TÄRKEÄÄ:** Tämä laite on asennettava turvaohjeiden mukaisesti.

**Sicurezza elettrica**
**IMPORTANTE:** questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

**Elektrisk sikkerhet**
**VIKTIG:** Dette utstyret skal installeres i samsvar med sikkerhetsregler.

**Segurança eléctrica**
**IMPORTANTE:** Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

**Seguridad eléctrica**
**IMPORTANTE:** La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

**Elsäkerhet**
**OBS!** Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.
Appendix B: SNMP MIBs and Traps Support

This appendix provides information on SNMP traps supported on the IONMM, including when a trap is generated and what information is in each trap.

All ION system critical events are reported via SNMP Traps. The ION system uses only SNMPv2 traps, with the definition of NOTIFICATION-TYPE in the MIB (Management Information Base).

Traps are generated when a condition has been met on the SNMP agent. These conditions are defined in the Management Information Base (MIB). The administrator then defines thresholds, or limits to the conditions, that are to generate a trap. Conditions range from preset thresholds to a restart.

All of the values that SNMP reports are dynamic. The information needed to get the specified values that SNMP reports is stored in the MIB. This information includes Object IDs (OIDs), Protocol Data Units (PDUs), etc. The MIBs must be located at both the agent and the manager to work effectively.

Supported MIBs

The x4120 implements the following Management Information Bases (MIBs).

- ionDevSysCfgTable
- ifTable
- ifXTable
- ionDMIInfoTable
- ionIfLoopbackTable
- ionEthInterfaceTable
- ionDevSysLPTTable
- ifMauAutoNegTable

The C4120 will expand three options of TNEthPhyMode structure for new PHY mode:

TNEthPhyMode ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "The different Ethernet PHY interfaces supported."
  SYNTAX INTEGER {
    unknown(0)
    phy10-100BaseT(1)
    phy100BaseFX(2)
    phy1000BaseX(3)
    phy10-100-1000BaseT(4)
    phySGMII(5)
    phy10GBase-LRM(6)
    phy10GBase-SR(7)
    phy10GBase-LR(8)
    phy10GBase-ER(9)
    phy10GBase-ZR(10)
    phy10GBase-T(11)
    phy10GBase-auto(12)
  }

The Focal Point SNMP service interface implements the same features as described above.
An example of a private MIB objects tree is shown in the figure below.

Figure 2: Private MIB Objects
Downloading, Compiling and Integrating MIBs

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

To download ION system private MIBs:

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

Set up your ION system SNMP configuration via the command line interface (CLI). Refer to “Configuring SNMP”. For a complete list of the available commands, see the x4120 CLI Reference Manual, 33497.
**Trap Service and Functions**

All ION system SNMP Trap messages conform to SNMPv2 MIB RFC-2573.

See the “Supported MIBs” section on page 32 for information on the x4120s support for public (standard) and private MIBs. For information on “Configuring SNMP” see page 154. See the ION Management Module (IONMM) User Guide manual for SNMP traps supported on the IONMM.

A sample SNMP Message sequence is shown below.

![Sample SNMP Message Sequence](image)

**Figure 3: SNMP Message Sequence**

The ION x4120 supports a Trap function to report the status as follow:

1) Ports link status change:
   - C4120 will send link up trap only once if port link status changes from link down to up;
   - C4120 will send link down trap only once if port link status changes from link up to down.

2) DMI trap:
   - An `ionDMIRxIntrusionEvt` event is sent if the `ionDMIRxPowerLevel` falls below the `ionDMIRxPwrLvlPreset` indicating an intrusion on the fiber
   - `ionDMIRxPowerEvt` event is sent when there is a warning or alarm on Rx Power
   - `ionDMITxPowerEvt` event is sent when there is a warning or alarm on Tx Power
   - `ionDMITxBiasEvt` event is sent when there is a warning or alarm on Tx Bias current
   - `ionDMITemperatureEvt` event is sent when there is a warning or alarm on DMI temperature.
   - C4120 will keep sending DMI traps until it becomes normal. Like the other ION SICS, the C4120 will periodically send out the specific trap every 3 seconds until the trap event condition doesn’t meet.
Only the IONMM SNMP management tool and Focal Point (FP) integrate the trap service function. The Trap Server is not automatically launched in the FP initialization procedure. You can launch the Trap function when needed. Focal Point only shows the traps received; no further action is performed to provide notification about the trap events.

The Trap message includes the following content:

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>SourceIP</th>
<th>Generic Trap</th>
<th>Specific Trap</th>
<th>Enterprise</th>
<th>Variable Bindings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The display format in FP will be as following (example):

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>SourceIP</th>
<th>Generic Trap</th>
<th>Specific Trap</th>
<th>Enterprise</th>
<th>Variable Bindings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Apr 17:43:35 2010</td>
<td>172.16.6.3</td>
<td>Notification</td>
<td>Linkup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri Apr 17:44:45 2010</td>
<td>172.16.6.3</td>
<td>Notification</td>
<td>Linkdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Trap MIBs are listed below:

IF-MIB:
- linkDown
- linkup

TN-ION-MGMT-MIB.smi:
- ionDMIRxIntrusionEvt
- ionDMIRxPowerEvt
- ionDMITxPowerEvt
- ionDMITxBiasEvt
- ionDMITemperatureEvt
Trap Server Log

The Trap Server log file contains information presented to the trap server by ION devices.

A sample part of a trap server log file is shown below.

```
Line
1
2
3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 | iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
12
13 E=
14 Ebig=
15 IP=192.251.144.220
16 com=trap
17 GT=Notification
18 ST=
19 TS=Thu May 13 10:06:42 2010
20 VB-Count=3
21 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266790) 326 days, 15:37:47.90 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 | iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
22
23 E=
24 Ebig=
25 IP=192.251.144.220
26 com=trap
27 GT=Notification
28 ST=
29 TS=Thu May 13 10:10:17 2010
30 VB-Count=3
31 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288348) 326 days, 15:41:23.48 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.2.1.47.2.0.1 | iso.3.6.1.6.3.1.1.4.3.0 = iso.3.6.1.2.1.47.2
32
33 E=
34 Ebig=
35 IP=192.251.144.220
36 com=trap
37 GT=Notification
38 ST=
39 TS=Thu May 13 10:10:18 2010
40 VB-Count=5
41 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822288428) 326 days, 15:41:24.28 | iso.3.6.1.6.3.1.1.4.1.0 = iso.3.6.1.4.1.868.2.5.2.0.1.1.134217728.6 = 6 | iso.3.6.1.4.1.868.2.5.2.1.1.1.134217728.6 = 1
```
The trap server log file lines are described below.

3 E=
4 Ebig=
5 IP=192.251.144.220
6 com=trap
7 GT=Notification
8 ST=
9 TS=Thu May 13 10:06:37 2010
10 VB-Count=3
11 Vars=iso.3.6.1.2.1.1.3.0 = Timeticks: (2822266290) 326 days, 15:37:42.90 | iso.3.6.1.6.3.1.1.4.1.0 =

Table 7: Trap Server Log File Description

<table>
<thead>
<tr>
<th>Category</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>E=</td>
<td></td>
<td>Endian</td>
</tr>
<tr>
<td>Ebig=</td>
<td></td>
<td>bigEndian</td>
</tr>
<tr>
<td>IP=</td>
<td></td>
<td>IP address</td>
</tr>
<tr>
<td>com=</td>
<td></td>
<td>trap</td>
</tr>
<tr>
<td>GT=</td>
<td></td>
<td>Notification</td>
</tr>
<tr>
<td>ST=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TS=</td>
<td>Thu May 13 10:06:37 2010</td>
<td>Timestamp – the log date that the file was recorded</td>
</tr>
<tr>
<td>VB-Count=</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Vars=</td>
<td>iso.3.6.1.2.1.1.3.0 =</td>
<td>Varbinds (Variable bindings) - the variable number of values that are included in an SNMP packet. Each varbind has an OID, type, and value (the value for/from that Object ID).</td>
</tr>
<tr>
<td>Timeticks:</td>
<td>(2822266290) 326 days, 15:37:42.90</td>
<td></td>
</tr>
<tr>
<td>iso.3.6.1.6.3.1.1.4.1.0 =</td>
<td>iso.3.6.1.2.1.47.2.0.1</td>
<td></td>
</tr>
<tr>
<td>iso.3.6.1.6.3.1.1.4.3.0 =</td>
<td>iso.3.6.1.2.1.47.2</td>
<td></td>
</tr>
</tbody>
</table>

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).

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.

ACL

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

ARP

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

Auto-Negotiation

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

Auto MDI / MDIX

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

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

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.

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.

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.

CoS

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

CoS Queues

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

CSA

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

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.

**DHCP**

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

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

**DiffDerv**

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

**Discovery**

Discovery allows a Service OAM-capable device to learn sufficient information (e.g. MAC addresses etc.) regarding other SOAM capable 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).
DNS

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

DoSAP

(Domain Service Access Point) A member of a set of SAPs at which a Maintenance Domain is capable of offering connectivity to systems outside the Maintenance Domain. Each DoSAP provides access to an instance either of the EISS or of the ISS.

Dr. Watson

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

DSCP

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

DSL

(Digital Subscriber Line) A copper loop transmission technology that enables high-speed access to customers in the local loop.

DST

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

DTE

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

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

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

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

EEA

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

Egress Frame

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

Egress rules

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

ESD

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

EtherType

One of two types of protocol identifier parameters that can occur in Ethernet frames after the initial MAC-48 destination and source identifiers. Ethertypes are 16-bit identifiers appearing as the initial two octets after the MAC destination and source (or after a tag).
Implies use of the IEEE Assigned EtherType Field with IEEE Std 802.3, 1998 Edition Local and Metropolitan Area Networks. The EtherType Field provides a context for interpretation of the data field of the frame (protocol identification). Several well-known protocols already have an EtherType Field.

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

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

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

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

**FDX**
(Full Duplex) Communication in both directions simultaneously.

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

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

A Fault Notification Generation (FNG) alarm is generated whenever a CCM (Continuity Check Message) is lost.

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.

Frame Loss Ratio

Frame loss ratio is the number of service frames not delivered divided by the total number of service frames during time interval T, where the number of service frames not delivered is the difference between the number of service frames arriving at the ingress ETH flow point and the number of service frames delivered at the egress ETH flow point in a point-to-point ETH connection.

Frame Delay

Frame delay is the round-trip delay for a frame, defined as the time elapsed from the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the loopbacked frame by the same source node, when the loopback is performed at the frame's destination node.

FTP

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

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

Gbps

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

GUI

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

HSCP

(High-Security Console Password)

HTML

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

HTTPS

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

ICMP

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

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

IEEE

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

IGMP

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

IGMP snooping

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

Ingress

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

Ingress rules

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

IP

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

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

IP Stacking

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

IPToS

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

ITU

ITU is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services. For nearly 145 years, ITU has coordinated the shared global use of the radio spectrum, worked to improve telecommunication infrastructure in the developing world, and established worldwide standards that foster seamless interconnection of a vast range of communications systems. See http://www.itu.int/net/about/itu-t.aspx.

ITU-T OAM Performance Monitoring

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

Jumbo Frame

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

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

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).

L2/L3/L4 Access Control List Port Based ACLs

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

Layer 2 Switch

A network device that functions as multi-port switch.

Layer 3 Switch

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

Layer 4 Switch

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

LBM

(Loopback Message) A unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR.

LBR

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

LED

(Light Emitting Diode) An electronic light source.
LLDP

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

Loopback (LB)

The Loopback feature puts a device in a special mode that enables the device to loop back the signal from the RX port to the TX port on either media for testing and troubleshooting purposes. Test signals can then be inserted into the link and looped back as received by a device to test a particular segment of the link (i.e. copper or fiber). Loopback can be either local or remote depending on the location of the converter in the link.

![Diagram of Loopback](image)

- **1)** Test signal inserted by near end device.
- **2)** Device B set to remote loopback on Fiber.
- **3)** Returned test signal received by near end device.

LPT

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

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.

**MDI**

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

The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX). The x4120 device’s *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection.

**MDIX**

(MDI Crossover) A version of MDI that enables connection between like devices. The standard wiring for end stations is known as Media Dependent Interface (MDI), and the standard wiring for hubs and switches is known as Media Dependent Interface with Crossover (MDIX). The x4120 device’s *AutoCross* feature makes it possible for hardware to automatically correct errors in cable selection. See also “MDI”.
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.

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.

MVRP

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

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

NIC

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

NID

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

NMS

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

NTP

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

OAMPDU

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

(Object Identifier) Known as an “Error! Reference source not found. object identifier” or “MIB variable” in the SNMP network management protocol, an OID is a number assigned to devices in a network for identification purposes. Each branch of the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an Object ID or OID.

In SNMP, an Object Identifier points to a particular parameter in the SNMP agent.

OSI

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

OUI

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

Pause

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

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

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.
PDU

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

PID

(Priority ID) on the x4120, the PID is configured at the ADVANCED tab in the “IEEE Priority Class” section; the selections are Remap 0 to: (PID) 0123.

(Process ID) in Netstat, the -o option displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter is available on Windows XP, 2003 Server (but not on Windows 2000).

Port-Based Rate Limiting

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

Port Labeling

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

Primary VID

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

Priority-tagged frame

A tagged frame whose tag header carries priority information, but carries no VLAN identification information. Note: Priority tagged frames, which, by definition, carry no VLAN identification information, are treated the same as untagged frames for the purposes of VLAN identification. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. These frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).
QoS

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

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

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

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

RADIUS

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

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, Error! Reference source not found., T1, and modern digital telephone systems.

RMON

(Remote Network Monitoring) Software that supports the monitoring and protocol analysis of LAN. A part of SNMP, RMON is a network management protocol that gathers remote network information. (Standard: RFC 1271.)
RS-232

(Recommended Standard 232) A standard for serial binary data signals connecting between a 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).

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 x4120 has SGMII support for use with 10/100/1000BASE-T copper SFPs. The x4120 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 SMI

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

SNMP

(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 Message

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

SNMP Version

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

SNMP Community String

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

SNMP PDU

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

SNTP

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

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

SSL

(Secure Socket Layer) A protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data; a public key known to everyone and a private or secret key known only to the recipient of the message. SSL is used to manage a network device via its web interface. (AKA, HTTPS, Standard: RFC 2818).

Static IP addressing

"Static" comes from the word stationary, meaning not moving. A static IP address means it never changes. A static IP address is an IP address permanently assigned to a workstation. If a network uses static addressing, it means that each network interface has an assigned IP address that it always uses whenever it is online. With static addressing, the computer has a well-defined IP address which it uses always and which no other computer ever uses.

Static MAC Entry

Static MAC entry support means that users can assign MAC addresses to ports manually that never age out.

STID

(Sensor Transaction Identifier) The STID is used for power supply / sensor / IONDCR configuration via the set sensor stid command to define notification, relation, severity, and value parameters. The show power config command displays the power supply sensors information. The STID is shown in the Web interface at the Power Supply tab > Temp, Volt, Power, and Fan sub-tabs.

STP

(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.

TCP/UDP Port Prioritization

The ability to prioritize traffic internally based on a TCP or UDP port number. (AKA, Layer 4 Prioritization.)

TDM

(Time Division Multiplexing) A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing.

Telnet

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

(Trivial File Transfer Protocol) A file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). Due to its simple design, TFTP can be implemented using a very small amount of memory. Because it uses UDP rather than TCP for transport, TFTP is typically used to transfer firmware upgrades to network equipment.

TFTP Download / Upload

The ability to load firmware, configuration files, etc. through a TFTP server. (AKA, TFTP. Standard: RFC 1350.)

TFTP Root Directory

The location on the console device (PC) where files are placed when received, and where files to be transmitted should be placed (e.g., C:\TFTP-Root).

TFTP Server

An application that uses the TFTP file transfer protocol to read and write files from/to a remote server. In TFTP, a transfer begins with a request to read or write a file, which also serves to request a connection. If the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and must be acknowledged by an acknowledgment packet before the next packet can be sent. Examples of available packages include Open TFTP Server, Tftpd32, WinAgents TFTP Server for Windows, SolarWinds free TFTP Server, TFTP Server 1.6 for Linux, and TftpServer 3.3.1, a TFTP server enhancement to the standard Mac OSX distribution.

Throughput

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

TID

Transaction Identifier  The TID is used in the CLI command “show soam mep linktrace mep-id=<1-8191> local-parent-id=<1-4294967295> tid=<0-4294967295>”.

TLS

(Transport Layer Security) A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).
TLV

Type, Length, Value format - LLDP frames are sent by each equipment on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type, length, value (TLV) structures. An LLDP frame should start with mandatory TLVs (e.g., Chassis ID, Port ID, and Time to live). These mandatory TLVs are followed by any number of optional TLVs. The frame should end with a special TLV named end of LLDPDU. The IEEE 802.1ab specification contains a description of all of the TLV types.

TNDP

(TN Topology Discovery Protocol) the Transition Networks implementation of LLDP. When set to Enabled, the device entering this command/setting will no longer be discovered by the IONMM if it is remotely managed through this port. See also “LLDP” and the “set tndp” and “show tndp” CLI commands. See also "Discovery".

TOS

(Type of Service) The ToS byte in the IPv4 header has had several purposes over time, and has been defined in various ways by IETF RFC 791, RFC 1122, RFC 1349, RFC 2474, and RFC 3168. Currently, the ToS byte is a six-bit Differentiated Services Code Point and a two-bit Explicit Congestion Notification field.

The ToS model described in RFC 2474 uses the Differentiated Services Field (DS field) in the IPv4 Header and IPv6 Header. See also CoS and QoS.

TPID

(Tag Protocol Identifier) a field in a VLAN Tag for which EEE802.1Q specifies a value of 0x8100.

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.

**TTL**

(Time to live) an Ethernet counter that records the number of times a transmission is sent/received without errors. TTL specifies how long a datagram is allowed to “live” on the network, in terms of router hops. Each router decrements (reduces by one) the value of the TTL field prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

The default TTL for ION software is 64. This means that a test packet must be successfully sent and received 63 times before a TTL expired message is generated. You can change the TTL value (e.g., a value of 255 is a demanding test because the packet must be sent and received error free 254 times).

**Tunnel**

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one (as in L2TP and VPN).

**Tunneling**

Encapsulating one type of packet inside the data field of another packet. This allows transmitting data that is structured in one protocol within the protocol or format of a different protocol. Tunneling can involve most OSI or TCP/IP protocol layers.

**UAC**

(User Account Control) Technology and security infrastructure of some Microsoft operating systems that improve OS security by limiting application software to standard user privileges until an administrator authorizes an increase.

**UDP**

(User Datagram Protocol) A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.
Unicast

One of the four forms of IP addressing, each with its own unique properties. The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient. See also Multicast.

Untagged frame

A frame that does not contain a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field. An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving Port, or, through proprietary extensions to this standard, based on the data content of the frame (e.g., MAC Address, Layer 3 protocol ID, etc.).

USB

(Universal Serial Bus) A plug-and-play interface between a computer and add-on devices, such as media players, keyboards, telephones, digital cameras, scanners, flash drives, joysticks and printers.

UTC

(Coordinated Universal Time) A time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich.

UTP

(Unshielded Twisted Pair) The most common form of twisted pair wiring, because it is less expensive and easier to work with than Error! Reference source not found. (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.

Varbind

In SNMP, a Sequence of two fields, an Object ID and the value for/from that Object ID. Varbinds is short for Variable bindings. It’s the variable number of values that are included in an SNMP packet. Each varbind is made of an OID, type, and value.

VDC

Volts DC (direct current, as opposed to AC – alternating current).

Web-based Management

Allows users to manage the switch through a web browser. (AKA, Web GUI, Web interface, Web IF.)

Well Known Ethernet Multicast Addresses

Some common Ethernet multicast MAC addresses are shown below with their related Field Type and typical usage.

<table>
<thead>
<tr>
<th>Ethernet Multicast Address</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-00-0C-CC-CC-CC</td>
<td>CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)</td>
</tr>
<tr>
<td>01-00-0C-CC-CC-CD</td>
<td>Cisco Shared Spanning Tree Protocol Address</td>
</tr>
<tr>
<td>01-80-C2-00-00-00</td>
<td>Spanning Tree Protocol (for bridges) (IEEE 802.1D)</td>
</tr>
<tr>
<td>01-80-C2-00-00-01</td>
<td>Ethernet OAM Protocol (IEEE 802.3ah)</td>
</tr>
<tr>
<td>01-80-C2-00-00-02</td>
<td>IEEE Std 802.3 Slow Protocols multicast address</td>
</tr>
<tr>
<td>01-80-C2-00-00-03</td>
<td>IEEE Std 802.1X PAE address</td>
</tr>
<tr>
<td>01-80-C2-00-00-04</td>
<td>IEEE MAC-specific control protocols</td>
</tr>
<tr>
<td>01-80-C2-00-00-08</td>
<td>Spanning Tree Protocol (for provider bridges) (IEEE 802.1AD)</td>
</tr>
<tr>
<td>01-00-5E-xx-xx-xx</td>
<td>IPv4 Multicast (RFC 1112)</td>
</tr>
<tr>
<td>33-33-xx-xx-xx-xx</td>
<td>IPv6 Multicast (RFC 2464)</td>
</tr>
</tbody>
</table>
Well Known Ports

The set of all available port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. The Well Known Ports are those from 0 through 1023. The Registered Ports are those from 1024 through 49151. Registered ports require IANA registration. The Dynamic and/or Private Ports are those from 49152 through 65535.

For example, Port 443 is reserved for the HTTPS, port 179 for the BGP Border Gateway Protocol, and port 161 for SNMP.

To see all the used and listening ports on your computer, use the `netstat` (or similar) command line command. For further port assignment information, see IETF RFC 1700.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>FTP</td>
</tr>
<tr>
<td>22</td>
<td>SSH Remote Login Protocol</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
</tr>
<tr>
<td>25</td>
<td>Simple Mail Transfer Protocol (SMTP)</td>
</tr>
<tr>
<td>53</td>
<td>Domain Name System (DNS)</td>
</tr>
<tr>
<td>69</td>
<td>Trivial File Transfer Protocol (TFTP)</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>143</td>
<td>Interim Mail Access Protocol (IMAP)</td>
</tr>
<tr>
<td>161</td>
<td>SNMP /TCP</td>
</tr>
<tr>
<td>161</td>
<td>SNMP /UDP</td>
</tr>
<tr>
<td>161</td>
<td>SNMPTRAP /TCP</td>
</tr>
<tr>
<td>162</td>
<td>SNMPTRAP /UDP</td>
</tr>
<tr>
<td>179</td>
<td>Border Gateway Protocol (BGP)</td>
</tr>
<tr>
<td>190</td>
<td>Gateway Access Control Protocol (GACP)</td>
</tr>
<tr>
<td>389</td>
<td>Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>514</td>
<td>Syslog UDP</td>
</tr>
<tr>
<td>546</td>
<td>DHCP Client</td>
</tr>
<tr>
<td>547</td>
<td>DHCP Server</td>
</tr>
<tr>
<td>547</td>
<td>DHCP Server</td>
</tr>
</tbody>
</table>

Write View

A view name (up to 64 characters) for each SNMP group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

Xmodem

A simple file transfer protocol developed in 1977 as the MODEM.ASM terminal program. XMODEM, like most file transfer protocols, breaks up the original data into a series of "packets" that are sent to a receiver, along with information that allows the receiver to tell if the packet was correctly received. It provides single file transfer using 128-byte packets with CRC or checksum error detection.
Xmodem-1K

An expanded version of XMODEM. Like other backward-compatible XMODEM extensions, it was intended that a -1K transfer could be started with any implementation of XMODEM on the other end, backing off features as required.

It provides simple serial file transfer between a server and client across a point-to-point link using fixed-length packets. Each server packet contains 1024 bytes of file data and is individually acknowledged by the receiving client. One file can be sent per transmission, and the transmission must be restarted from the beginning if it fails.

Ymodem

A protocol for file transfers between modems. YMODEM was developed as the successor to XMODEM. The original YMODEM was much the same as XMODEM except that it sent the file name, size, and timestamp in a regular XMODEM block before actually transferring the file. It provides multiple file transfer using 1 Kbyte packets, and is similar to Xmodem in other aspects.

Zmodem

A file transfer protocol developed in 1986 to improve file transfer performance on an X.25 network. ZMODEM also offers restartable transfers, auto-start by the sender, an expanded 32-bit CRC, control character quoting, and sliding window support. It provides multiple file transfer, sending packets without waiting for acknowledgement, and permits an interrupted transfer to restart.
10Gigabit Ethernet Terms

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.

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.

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-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 25 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
Over the years 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 Infini-Band 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.

ALR
(Automatic Link Restoration) After a link failure condition has been corrected, the device will automatically re-establish the link in all network conditions using the ALR feature.

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 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.

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

MSA
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+”.

**SFP+**
echoed 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.

**TLPT**
(Transparent Link Pass Through) will notify an end device of a link failure just like Link Pass Through; however, it uses a different method for “passing through” this information. Transparent Link Pass Through sends a link loss signal over the fiber, instructing the remote converter to shut down the copper port thus notifying the end device, while maintaining the fiber link between the two converters. With TLPT, an End device automatically notified of link loss, and the Fiber link remains up as it carries a link loss signal.

**XAUI**
XAUI is a standard for extending the XGMII (10 Gigabit Media Independent Interface) between the MAC and PHY layer of 10 Gigabit Ethernet (10GbE). XAUI is pronounced "zowie", a concatenation of the Roman numeral X, meaning ten, and the initials of "Attachment Unit Interface". The XGMII Extender, which is composed of an XGXS at the MAC end, an XGXS at the PHY end and a XAUI between them, is to extend the operational distance of the XGMII and to reduce the number of interface signals. Applications include extending the physical separation possible between MAC and PHY components in a 10 Gigabit Ethernet system distributed across a circuit board.
Index

Auto negotiate, 33
AutoCross, 31
Circuit ID, 25, 27
CLI error messages, 61
Compliance information, 138
Conventions, documentation, 9
Defaults
   Reset factory settings, 41
Documentation conventions, 9
Error messages
   CLI commands, 61
   Web interface, 84
Firmware
   Upgrading, 49
GUI, 11
MDI, 31
MDIX, 31
Problem conditions, 55
RADIUS
   Configuring, Web method, 112
   Reboot, 46
      Web method, 47
   Reset
      Factory defaults, 41
      Uptime, 44
   Reset to Factory Config, 42
   Resetting Defaults, 42
   Restart
      ION MM, 46
SOAM
   Configuring, CLI method, 111
System Restart, 46
Tech Support, 133
Troubleshooting, 52
Warranty, 136
Web interface
   Error messages, 84