

ION System

C4221 Remotely Managed
Network Interface Device (NID)

Web User Guide

Part Number 33693
Revision B August 2023

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

All other trademarks and trade names are the property of their respective holders.

Patented: patents.lantronix.com; additional patents pending.

Warranty

For details on the Lantronix warranty policy, go to <http://www.lantronix.com/support/warranty>.

Contacts

Lantronix Corporate Headquarters

48 Discovery, Suite 250

Irvine, CA 92618, USA

Toll Free: 800-526-8766

Phone: 949-453-3990

Fax: 949-453-3995

Technical Support

Online: <https://www.lantronix.com/technical-support/>

Sales Offices

For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev	Description
1/12/18	A	Initial release for C4221 FW v 2.0. The C4221 requires IONMM v1.3.19 or above.
8/29/23	B	FW v 2.0.7: add support for forwarding MACSec and LACP protocols (requires IONMM v1.4.3). IONMM v1.4.4 adds support for older versions of C4221 that didn't have L2CP or STP. (If the version is < v2.0.3 then the Web & CLI turned off L2CP and STP. If the version is = v2.0.3 then the Web & CLI turned off STP. If the version is = 2.0.4 then L2CP & STP are both turned on in the Web & CLI). Add pause frame config options for Gigabit in Auto-Negotiation mode. C4221 no longer participates in STP by default. STP frames can be forwarded through C4221. Reduce extra LLDP frames being sent out ports. LLDP frames are only sent out ports with path back to the IONMM. Disable IPMC snooping by default. IONMM must be upgraded to 1.5.0. Initial Lantronix re-brand. See the Release Notes for important information

Contents

1: Introduction	5
Product Description	5
About This Manual	5
Features	5
Specifications	6
Related Manuals and Online Help	6
Documentation Conventions	7
Cautions and Warnings	7
2: Installation and System Setup	8
3: Management Methods	9
General	9
IONMM Managed NIDs	9
Menu System Descriptions	10
4: Configuration	12
General	12
System Configuration	12
System Configuration	13
Ports Configuration	14
Set Bandwidth Allocation / Rate Limiting	15
Set Bandwidth Allocation / Rate Limiting	15
Configuring Priority Queuing	17
Priority Queuing Config	17
Configuring Security Features	18
Configuring VLANs	18
VLAN Config	19
TNDP (TN Topology Discovery Protocol) Disable/Enable	21
TNDP Config	21
STP Port Admin Status via Web UI	23
DMI (Diagnostic Monitoring Interface)	24
DMI Config	24
5: Operation	28
General	28
Reset to Factory Defaults	28
Resetting Defaults	28
Resetting Uptime	29
Reset System Uptime	29
Resetting Counters	30
Reset Port Counters	30
Port Counter Parameters	31
Reboot and Reset Function Notes	34
Reboot	34
Rebooting	35
6: Troubleshooting	37
General	37
Basic ION System Troubleshooting	37
Error Indications and Recovery Procedures	38
LED Fault and Activity Displays	39
Problem Conditions	40
Web Interface Messages	44
Webpage Messages	52
Recording Model Information and System Information	56

Appendix A: Warranty and Compliance Information 58

List of Tables

Table 1: Documentation Conventions 7
Table 2: System-Level Menu Description 10
Table 3: Port-Level Menu Description 11
Table 4: DMI Parameter Descriptions 25

1: Introduction

Product Description

The ION C4221 Network Interface Device (NID) is a remotely managed product that offers management via the IONMM for the secure delivery of Ethernet services for business and mobile backhaul applications. The C4221 is a 10Gbps product with advanced features like remote management of the local and remote cards, jumbo frames support, and bandwidth allocation of 10G interfaces.

The C4221 offers the additional functionality of a rate converter by also offering a 10/100/1000Base-T RJ-45 port, allowing 10/100/1000 based devices to connect to a 10Gigabit Ethernet fiber backbone.

About This Manual

This manual provides information on the Lantronix C4221 NID Web interface. This manual assumes that the ION C4221 is properly installed and functioning. See the ION C4221 Install Guide for installation and setup topics. This manual documents these models:

Model	Description
C4221-4848	ION Chassis Card, two 10G SFP+ ports, one 10/100/10000 Base-T copper port Remotely-Managed NID

Features

The C4221 NIDs support these features:

- Full non-blocking switching on all interfaces
- Two 10G SFP+ ports supporting 100FX, 1000BaseX, SGMII, and 10G
- Local and remote units can be managed by the ION platform
- Bandwidth Allocation, per port, from 1Gig to 10Gig in 1Gig increments
- Jumbo frames support, up to 10,240 bytes
- 16K maximum MAC Addresses
- 8Mbits shared buffer memory
- Can be used in the ION 19-slot, 6-slot, and 1-slot chassis
- DMI (Diagnostic Monitoring Interface) support
- Management provided via IONMM
 - Telnet
 - Command Line Interface (CLI)
 - Web management

Specifications

See the ION C4221 Install Guide for specifications.

Related Manuals and Online Help

A printed documentation card is shipped with each C4221 NID. Context-sensitive Help screens, as well as cursor-over-help (COH) facilities are built into the Web interface.

For Lantronix Drivers, Firmware, Manuals, Product Notifications, Warranty Policy & Procedures, etc. go to the Lantronix [Technical Resource Center](#).

ION system and related device manuals are listed below.

1. ION C4221 Install Guide, 33692
2. ION C4221 Web User Guide, 33693 (this manual)
3. ION C4221 CLI Reference, 33694
4. ION Management Module (IONMM) User Guide, 33457 and Install Guide, 33420
5. IONMM-232 Install Guide, 33725
6. ION106-x Six Slot Chassis User Guide, 33658
7. IONPS-A-R1 Power Supply User Guide, 33614
8. IONPS-D-R1 DC Power Supply Install Guide, 33707
9. SFP manuals (model specific) (see Lantronix [SFP webpage](#))
10. Release Notes (software version specific)

This manual provides links to third part web sites for which Lantronix is not responsible. Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. Note: Some Documentation may have Transition Networks named or pictured. Transition Networks was acquired by Lantronix in August 2021.

Documentation Conventions

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

Table 1: Documentation Conventions

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

Cautions and Warnings

See the *ION C4221 Install Guide* for important Cautions and Warnings and for Electrical Safety Warnings translated into multiple languages.

2: Installation and System Setup

This manual assumes that the ION C4221 is properly installed and functioning. See the ION C4221 install Guide for topics from unpacking to Web UI login, including:

- Installing the Chassis Model
- Installing SFPs
- Connections and LEDs
- Operating Systems supported
- Installing the USB Driver
- Configuring HyperTerminal
- Starting a USB Session in HyperTerminal
- Terminating a USB Connection from HyperTerminal
- Access via an Ethernet Network
- Accessing the NIDs
- Access via Local Serial Interface (USB)
- Starting the Web Interface
- Sign in to the ION System Web interface
- Terminating the Web Interface (Sign Out)

3: Management Methods

General

The C4221 NIDs are managed through the IONMM. Whether the NID is managed directly or indirectly, management is done using one of these 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).

IONMM Managed NIDs

NIDS that are managed through the IONMM are chassis resident modules. Communications between the IONMM and the NIDs is through the ION Chassis backplane.

Menu System Descriptions

The table below describes the C4221 interface in terms of its system-level pane, dropdowns, tabs and sub-tabs. Note that menus and tabs vary slightly by model.

Table 2: System-Level Menu Description

Dropdown / Tab	Description
ION System pane	<p>ION Stack - consists of one chassis or one standalone. The Stack Members table lists the Stack's chassis member and its type (IONBPC-219) and description.</p> <p>Chassis - the ION System family of products. The Chassis view shows a summary view of one chassis. Model Information includes:</p> <ul style="list-style-type: none"> * Serial Number - The serial number of the chassis itself. Individual NIDs also have their own serial numbers. * Model Name - The exact model name of this device (IONBPC-219). * Software Revision, Hardware Revision, and Bootloader Revision. * Chassis Members table - lists local physical components in slots 1 to 19. <p>Device – provides tabs and sub-tabs for the IONMM and NIDs in the ION system.</p> <p>Port - provides tabs and sub-tabs for a selected NID port.</p>
System dropdown	Sign out.
View dropdown	Refresh.
Help dropdown	Online Help, ION Product Home Page, About ION System Web Interface.
C4221-4848 MAIN tab	Model Information, System Configuration, and Device Description.
C4221-4848 VLAN tab	Add, Edit, or Delete VLANs table data (VLAN ID and Member Tag Port 1, 2, and 3).

* Note that not all tabs are viewable by all user levels.

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

Table 3: Port-Level Menu Description

Tab	Description
MAIN tab	Sections: Circuit ID, Port Configuration, TN Topology Discovery Protocol TX. Buttons: <i>Refresh</i> , <i>Save</i> , and <i>Help</i> .
ADVANCED tab	Sections: Bandwidth Allocation and Egress Queue Mode. Buttons: <i>Refresh</i> , <i>Save</i> , and <i>Help</i> .
COUNTERS tab	Sections: RMON Counters, RX Counter, TX Counter, and MAC Control Frames sections. Buttons: <i>Reset Counters</i> , <i>Refresh</i> , and <i>Help</i> buttons.
DMI tab	Sections: Interface Characteristics, Diagnostic Monitoring, and Supported Media Length (ports 1 and 2 only). Buttons: <i>Refresh</i> , <i>Save</i> , and <i>Help</i> .

4: Configuration

General

After the C4221 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 C4221 device and associated ports. Configuration can be done via the Web interface.

The operating characteristics that can be defined for the NID include Device Description / Circuit ID / System setup, Ethernet Interface (Bandwidth allocation), and VLAN.

Note: Lantronix 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.

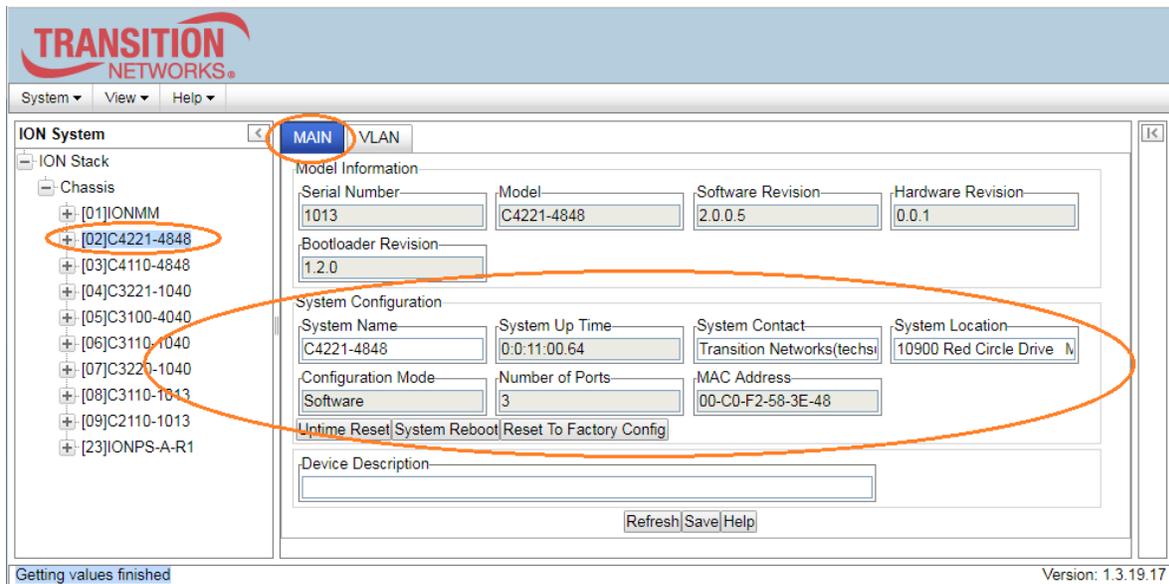
System Configuration

The system configuration defines a name for the NID, contact and location information.

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.

System Configuration

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

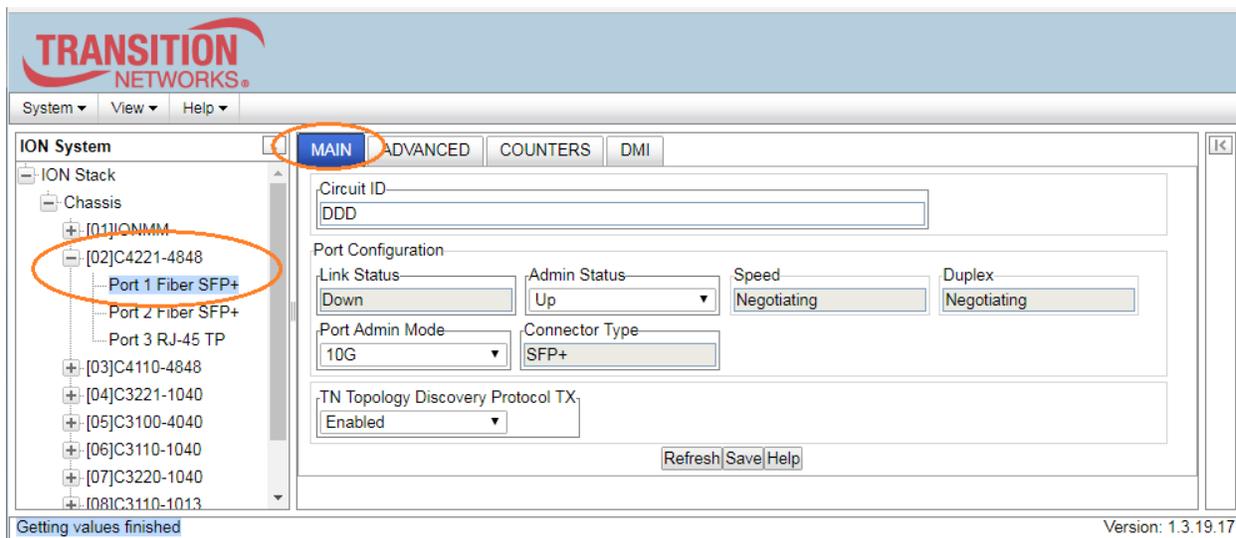


3. In the **System Name** field, enter the name and for the C4221 NID. The name can be alphabetic, numeric, or a combination of up to 32 characters. The default System Name is “C4221-4848”. Do not enter spaces between System Name characters.
4. In the **System Contact** field, enter the name and information of the person to contact if there is a problem with the system. The name and information can be alphabetic, numeric, or a combination.
5. In the **System Location** field, enter the information describing the physical location of where the system is located (e.g., room 110, IT lab, etc.). The information can be alphabetic, numeric, or a combination.
6. Verify the value displayed in the **Configuration Mode** field. The C4221 NID has a jumper that disables software management of the NID.
When the **Configuration Mode** field displays **Hardware**, the C4221 NID takes some of its configuration from a jumper on the NID.
In **Software** mode, all configuration parameters are controlled by management.
Refer to “[Jumper Settings](#)” in the *ION C4221 Install Guide* for details on **Configuration Mode**.
7. When done, scroll to the bottom and click **Save**.

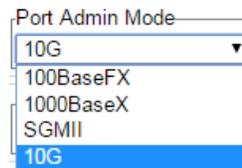
Ports Configuration

The Ethernet ports can be configured for Circuit ID, Admin Status, Port Admin Mode, and TN Topology Discovery Protocol TX. The read-only information displayed at the port-level **MAIN** tab includes Link Status, Speed, Duplex, and Connector Type.

1. Access the C4221 NID via the Web interface (see “Starting the Web Interface”).
2. Select the desired port.



3. At the port MAIN tab, enter a Circuit ID (optional).
4. In the **Port Configuration** section, observe the **Link Status** (Up or Down), **Speed**, and **Duplex**.
5. Set the **Admin Status** to Up or Down (optional).
6. Set **Port Admin Mode** to 100BaseFX, 1000BaseX, SGMII, or 10G.
7. Set the TN Topology Discovery Protocol TX. See the [TN Topology Discovery Protocol TX](#) section.
8. Click the **Refresh** or **Save** button when done.



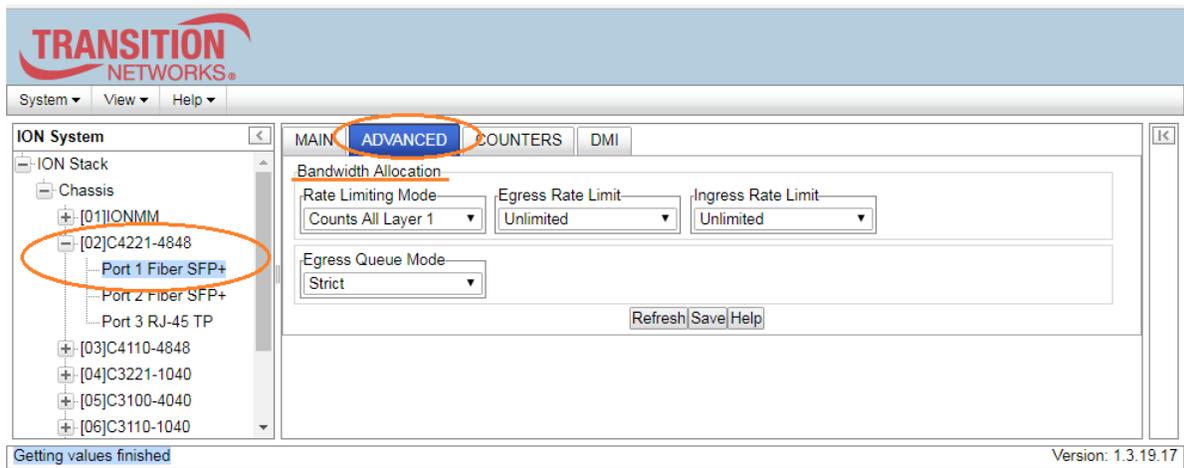
Note that currently, if **Port Admin Mode** is set to SGMII, and connected to an auto-negotiating port, the SGMII setting doesn't stick; it just reverts to 1000BaseX. You must disable the C4221 link partner's fiber auto-negotiation to establish a link with the C4221. The C4221's negotiation is not currently configurable to enable/disable.

Set Bandwidth Allocation / Rate Limiting

The C4221 Bandwidth Allocation (Rate Limiting) can be configured to limit both Ingress bandwidth and Egress bandwidth. If so configured, traffic at rates higher than this CIR (Committed Information Rate) is discarded. Note that these limits cannot be set faster than the port speed.

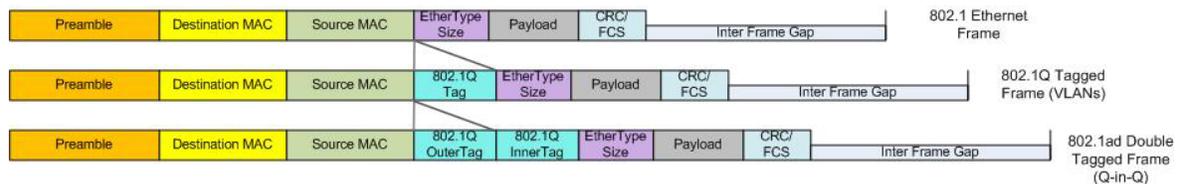
Set Bandwidth Allocation / Rate Limiting

1. Access the C4221 through the Web interface (see “Starting the Web Interface”).
2. Select the appropriate port’s **ADVANCED** tab.
3. Locate the **Bandwidth Allocation** section.

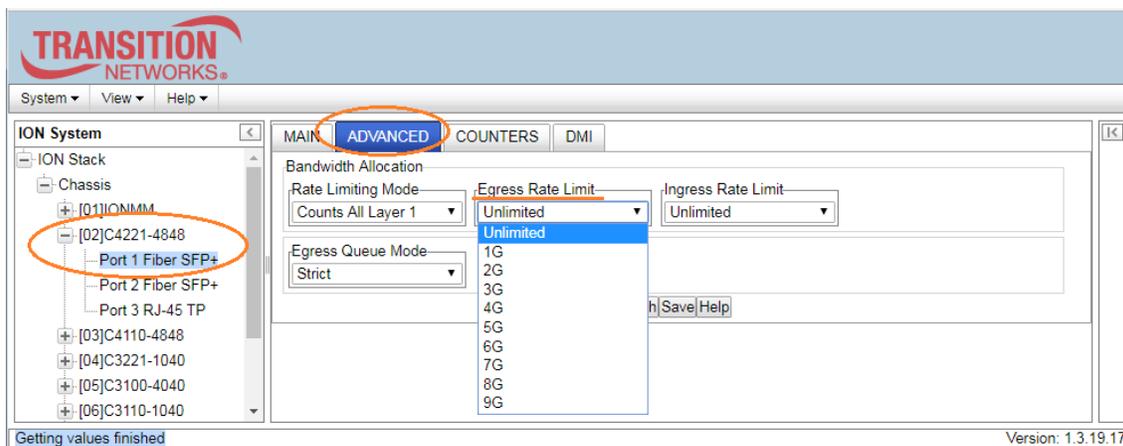


4. In the **Rate Limiting Mode** field, select which bytes in a frame are to be counted in determining the rate limit:
 - **Counts All Layer 1:** (the default): in determining the rate limit, this selection counts the following bytes in a frame: Preamble (8 Bytes) + DA to CRC + Inter Frame Gap (12 bytes).

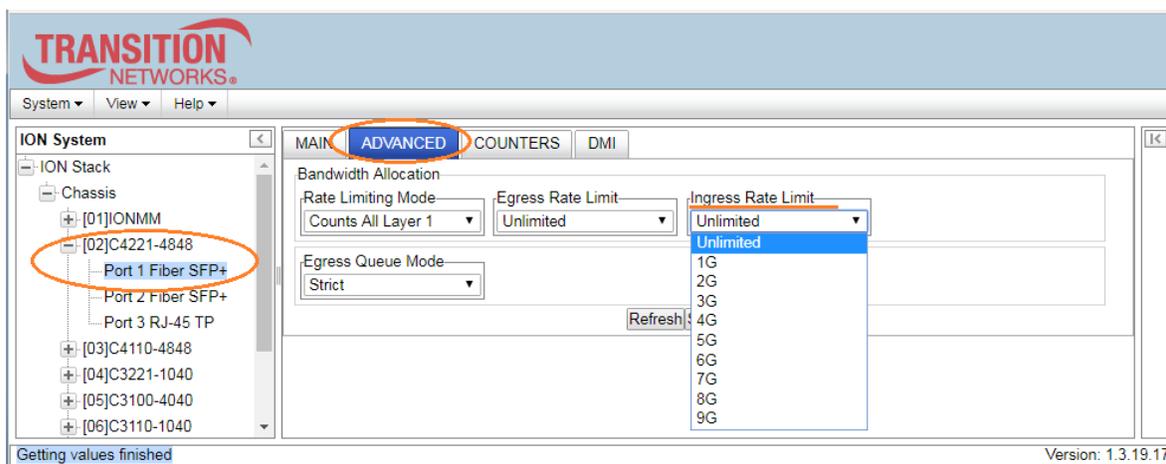
Note: the C4221 only supports "Counts all Layer 1".



- In the **Egress Rate Limit** field, select the Egress bandwidth limit in bits per second. Traffic which goes over this rate is discarded. For all ports, select Unlimited, 1G, 2G, 3G, 4G, 5G, 6G, 7G, 8G, or 9G. The default is **Unlimited** for all ports.



- In the **Ingress Rate Limit** field, select the Ingress bandwidth limit in bits per second. This is the Committed Information rate (CIR) on this interface for Ingress. Traffic which goes over this rate is discarded. For all ports, select Unlimited, 1G, 2G, 3G, 4G, 5G, 6G, 7G, 8G, or 9G. The default is **Unlimited** for all ports.



- At **Egress Queue Mode**, select the Egress Queue mode for a port. The C4221 supports "Strict" Egress Queue modes from the C4221 > Port x > ADVANCED tab > Egress Queue Mode menu path. At the dropdown select "Strict" scheduling. Strict queuing assumes that types of traffic can be differentiated and treated preferentially. Separate FIFO queues are created for each defined priority level and the arriving traffic is sorted into its proper queue as it arrives. So the first task of configuring strict priority queuing is to determine traffic classifications. Usually 2-5 priority levels are defined (e.g., high, medium, normal, low), although more levels can be defined. Having more queues means more complexity in running the algorithm. At the service side of the queue, the processing rule is simple: higher priority FIFO queues always get completely processed before lower priority queues get processed.
- Click the **Save** button when done.
- Repeat steps 3-8 above for other device ports as required.

Configuring Priority Queuing

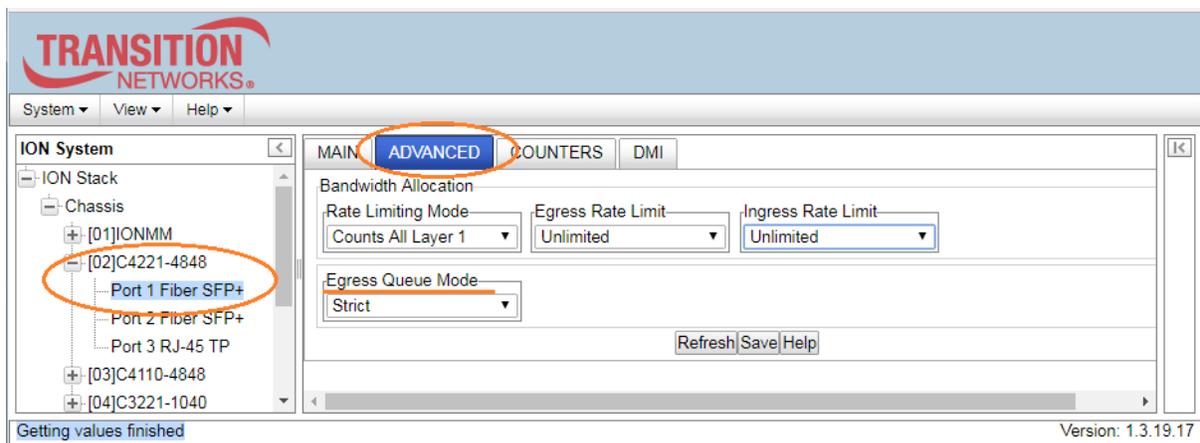
The C4221 has the Egress Queue mode set to “Strict” in the CLI and the Web interface.

SP (Strict priority) queuing is a response to the disadvantages of FIFO in a congested environment. Strict priority queuing assumes that types of traffic can be differentiated and treated preferentially.

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

Priority Queuing Config

1. Access the C4221 through the Web interface (see “Starting the Web Interface”).
2. Select the Port 1 **ADVANCED** tab.
3. Locate the **Egress Queue Mode** field.

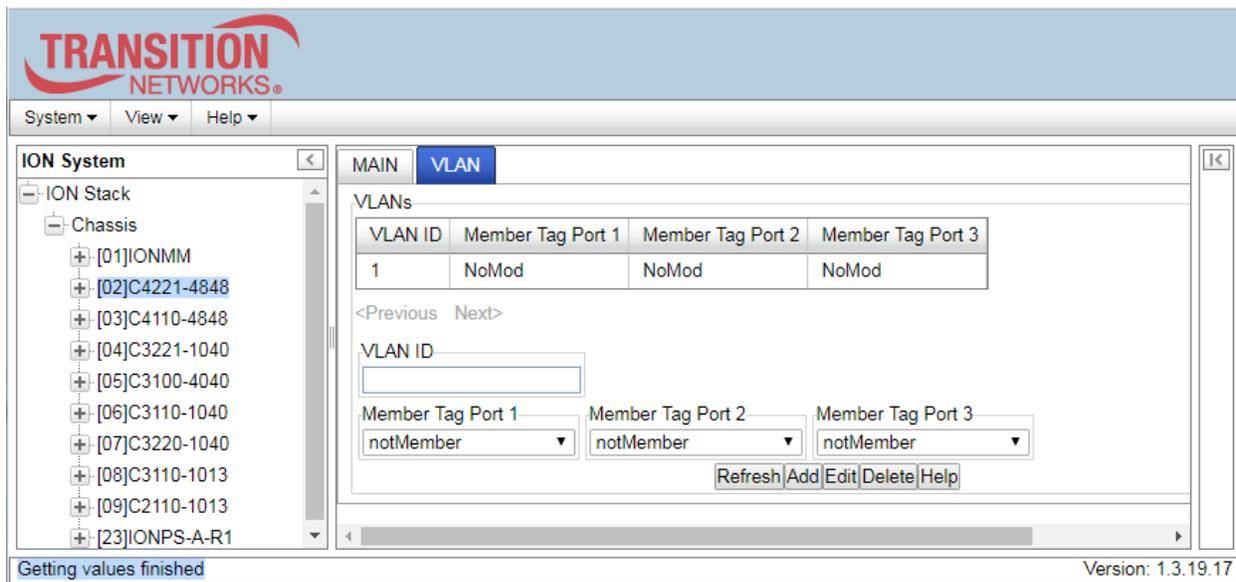


4. At the dropdown you can select only “**Strict**” scheduling.
5. Repeat steps 2-4 above for other device ports as required.

Configuring Security Features

The following can currently be defined for the C4221 NID:

- VLANs from the C4221 **VLAN** tab.



VLAN configuration is discussed in the following sections.

Configuring VLANs

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Ports on a switch can be grouped into VLANs in order to limit traffic flooding since it is limited to ports belonging to that VLAN and its trunk ports. Any switch port can belong to a VLAN. Packets are forwarded and flooded only to stations in the same VLAN. Each VLAN is a logical network, and packets destined for stations that do not belong to the same VLAN must be forwarded through a routing device. Each VLAN can also run a separate instance of the spanning-tree protocol (STP).

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

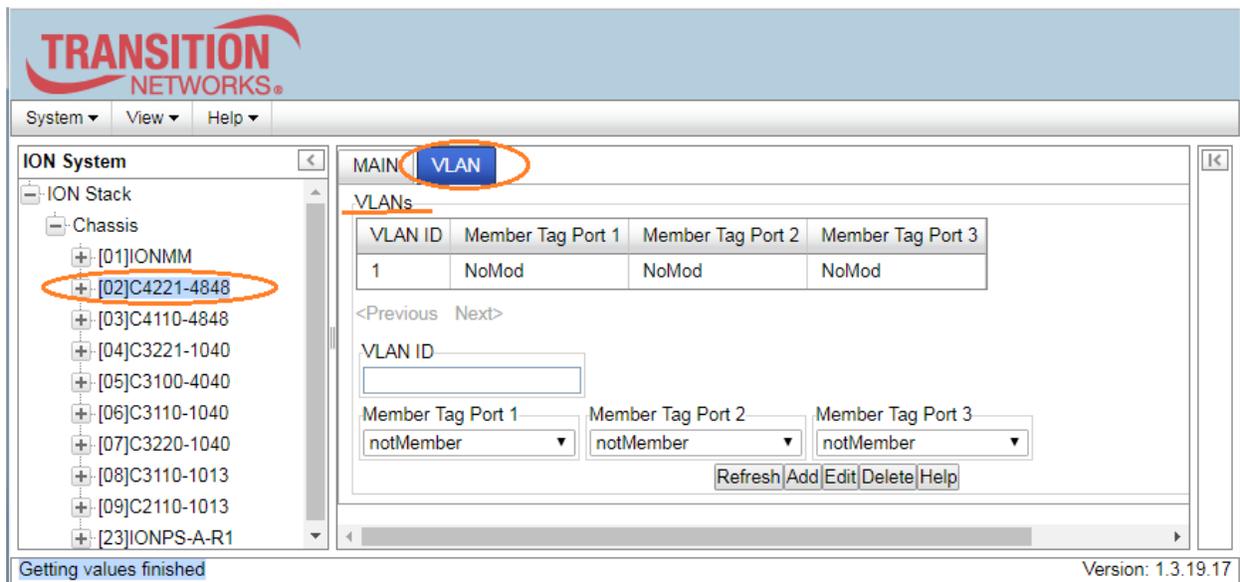
Virtual LANs are essentially Layer 2 constructs, whereas IP subnets are Layer 3 constructs. In a campus LAN employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs.

Virtual LANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to one another and this correspondence is useful during the network design process.

A virtual LAN (VLAN) is a collection of network nodes that share the same broadcast domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers. This allows users to share information and resources as though located on the same LAN. VLANs also allow a single physical LAN to be divided into multiple logical LANs. The default VLAN port type is C-Port. By default, the C4221 passes all tagged and untagged frames.

VLAN Config

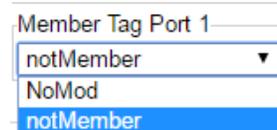
1. Access the C4221 through the Web interface (see “Starting the Web Interface”).
2. Select the **VLAN** tab.



3. Observe VLAN ID 1 in the VLANs table. This is the VLAN ID which is to be used for all management traffic to and from the device. The management station that belongs to this VLAN is the only one able to manage the C4221 NID. By default the VLAN ID is set to 1 (Management VLAN 1 enabled). The default VLAN 1 cannot be modified or removed!
4. In the **VLAN ID** field, enter a VLAN ID. The valid range is from 2–4094.
5. **Member Tag Port 1-3** is used to define which ports are members of the VLAN. The parameters are:
 - NoMod:** Port is a member of this VLAN and frames are to egress unmodified. The frames mapped to this VLAN egress unmodified out on this port (frame maps to a VLAN ID when it ingresses a port, the VLAN ID is mapped based on either the existing VID if it is already tagged or the port default VLAN ID if untagged). Frames are unmodified, they egress the same as they ingress this interface.

notMember: Port is not a member of this VLAN and frames with this VLAN ID will be discarded. Frames mapped to this VLAN will not be forwarded out on this port.

When configuring a VLAN on the C4221 via the IONMM, set the membership of each port to either noMod (traffic with the configured VLAN tag # can ingress and egress that port) or notMember (traffic with the configured VLAN tag will not be allowed to ingress or egress that port).



6. Click the **Add** button to add the new entry to the table.

The screenshot shows the ION C4221 Web User Interface. The 'VLAN' tab is selected. The table below shows the current VLAN configuration:

VLAN ID	Member Tag Port 1	Member Tag Port 2	Member Tag Port 3
1	NoMod	NoMod	NoMod
2	notMember	notMember	notMember
3	NoMod	notMember	notMember
4	NoMod	NoMod	notMember
5	NoMod	NoMod	NoMod
7	notMember	notMember	NoMod
8	NoMod	notMember	NoMod
9	NoMod	notMember	NoMod
10	NoMod	notMember	notMember
11	NoMod	notMember	notMember

Below the table, there are input fields for 'VLAN ID', 'Member Tag Port 1', 'Member Tag Port 2', and 'Member Tag Port 3'. The 'Add' button is highlighted. The left sidebar shows the network tree with '[02]C4221-4848' selected.

7. Repeat steps 4-6 above for other VLANs as required. After the first ten VLAN entries, use the **Next>** button to display the next page of VLANs; use the **<Previous** button to go back a page.

Messages:

A record with the same VLAN ID already exists!

The default VLAN 1 cannot be modified or removed!

VLAN ID is empty or invalid!

Problem: Setting a VLAN for NoMod, NoMod, NoMod causes the config to be reported as NoMod, notMember, NoMod.

Problem: Ports configured as notMember act like they were configured as noMod.

Cause: A VLAN page display issue.

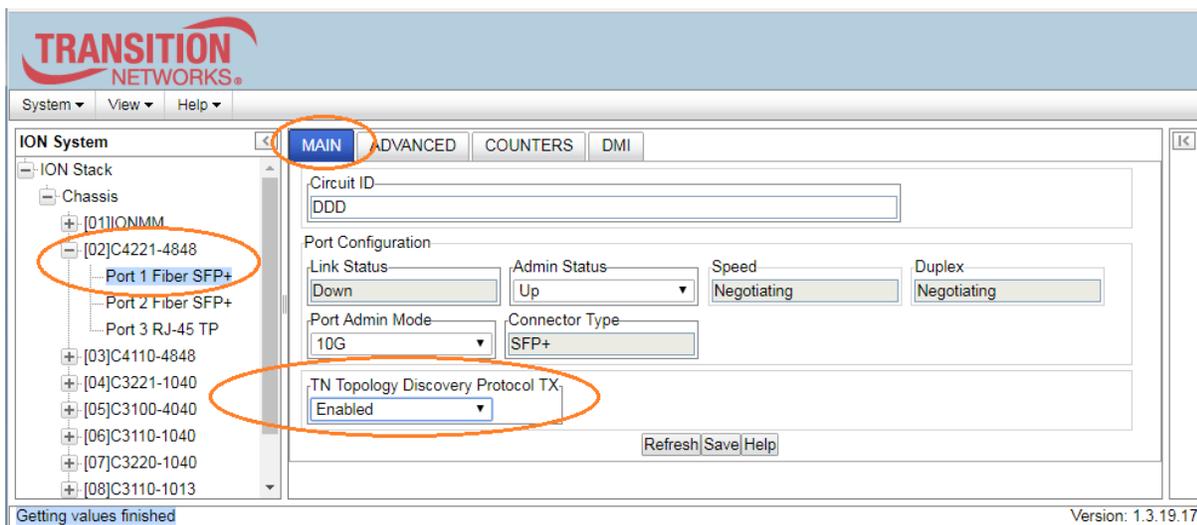
Solution: Navigate away from the VLAN config page, and then back to the VLAN config page.

TNDP (TN Topology Discovery Protocol) Disable/Enable

TNDP (TN Topology Discovery Protocol) is the Lantronix implementation of LLDP. If using the NID with a switch or router, the NID continues to send out LLDP-based information (TN proprietary - sent once every second). While this does not impact the data traffic seen, it drops for unrecognized upper-level protocols in the switch / router. Disabling TNDP can help eliminate invalid errors and make troubleshooting simpler.

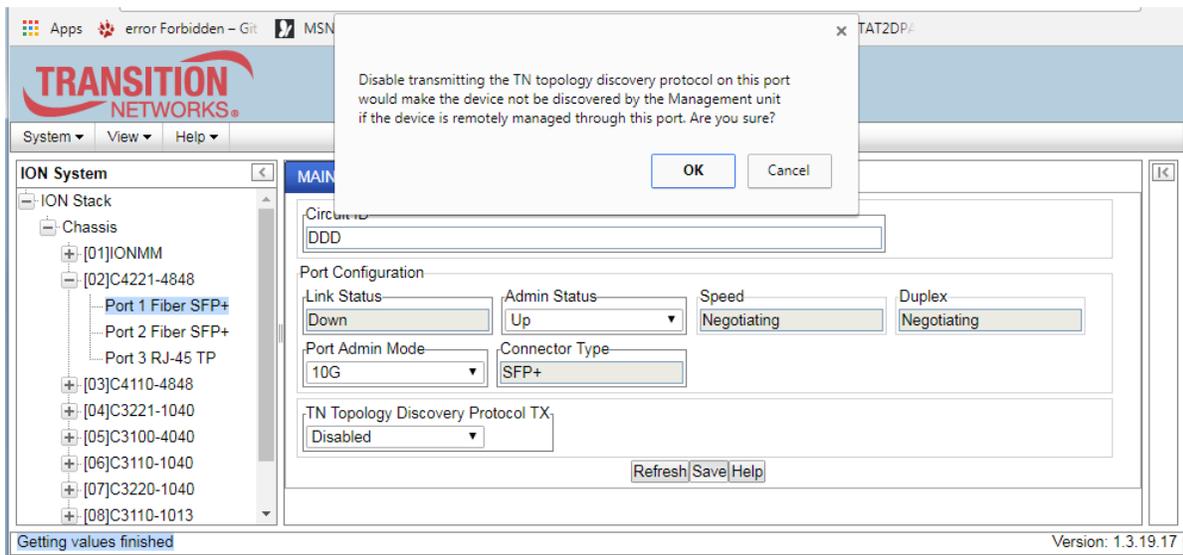
TNDP Config

1. Access the C4221 through the Web interface (see “Starting the Web Interface”).
2. Select the desired port.
3. Locate the **TN Topology Discovery Protocol TX** section.



4. Set TN Topology Discovery Protocol TX to enabled or disabled. The default setting is Enabled. **Enabled**, TN Topology Discovery Data will be sent out from this interface. **Disabled**, TN Topology Discovery Data will not be sent out from this interface. **Note**: when set to **Disabled**, the device entering this command will no longer be discovered by the IONMM if it is remotely managed through this port.
5. Click the **Save** button when done.

Message: Disable transmitting the TN topology discovery protocol on this port would make the device not be discovered by the Management unit if the device is remotely managed through this port. Are you sure?



STP Port Admin Status via Web UI

STP Admin Status commands are added to the CLI and backup/restore at IONMM FW v 1.4.32.

STP (Spanning Tree Protocol) is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the resulting broadcast radiation. Spanning tree also allows a network design to include backup links to provide fault tolerance if an active link fails.

The screenshot shows the ION System web UI configuration page for Fiber Port 1. The left sidebar shows the ION Stack hierarchy: Chassis > [01]C3220-1040 > [09]C4221-4848 > Fiber Port 1. The main configuration area includes tabs for MAIN, ADVANCED, COUNTERS, and DMI. The configuration fields are as follows:

- Circuit ID: [Empty text box]
- Port Configuration:
 - Link Status: Down
 - Admin Status: Up
 - Speed: Negotiating
 - Duplex: Negotiating
 - Port Admin Mode: 10G
 - Connector Type: SFP+
- L2CP Disposition:
 - Spanning Tree Protocols: Pass
 - Slow Protocols: Pass
 - ELMI Protocol: Pass
 - LLDP Protocol: Pass
 - Port Authentication Protocols: Pass
 - GARP/GMRP Block of Protocols: Pass
 - Bridge Block Other Multicast Protocols: Pass
- TN Topology Discovery Protocol TX: Enabled
- Spanning Tree Port Admin Status: Disabled (highlighted with a red box)

Buttons at the bottom: Refresh, Save, Help. A red text label "On all 3 ports" is visible in the bottom left of the configuration area.

Parameter descriptions:

Spanning Tree Port Admin Status: At the dropdown select Enabled or Disabled. The default is Disabled.

DMI (Diagnostic Monitoring Interface)

NID models with Diagnostic Monitoring Interface (DMI) support allow diagnosing problems within the network. The DMI function displays x4221 NID diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. All DMI events will trigger notification. Intrusion detection, based on Rx Power level, can be set to trigger on a drop in the Rx power.

DMI device functions include:

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

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

DMI Config

1. Access the C4221 via the Web interface (see “Starting the Web Interface”).
2. Select the desired device and port.
3. Select the **DMI** tab.

The screenshot displays the web interface for the ION C4221. The left sidebar shows the 'ION System' tree with 'Port 1 Fiber SFP+' selected. The main content area has tabs for 'MAIN', 'ADVANCED', 'COUNTERS', and 'DMI', with 'DMI' being the active tab. The configuration is organized into three sections:

- Interface Characteristics:**
 - DMI ID: SFP/SFP+/SFP28
 - Connector Type: LC
 - Nominal Bit Rate (Mbps): 10300
 - Fiber Interface Wavelength (nm): 110
- Diagnostic Monitoring:**
 - Receive Power (µW): 0
 - Receive Power (dBm): [empty]
 - Receive Power Alarm: Normal
 - Rx Power Intrusion Threshold (µW): 0** (highlighted with a red box)
 - Temperature (°C): 29.4
 - Temperature (°F): 84.9
 - Temperature Alarm: Normal
 - Transmit Bias Current (µA): 81964
 - Transmit Bias Alarm: Normal
 - Transmit Power (µW): 1534
 - Transmit Power (dBm): 1.858
 - Transmit Power Alarm: Normal
- Supported Media Length:**
 - 9/125u Singlemode Fiber (km): 80
 - 9/125u Singlemode Fiber (m): 25500
 - 50/125u Multimode Fiber (m): N/A
 - 62.5/125u Multimode Fiber (m): N/A
 - Copper (m): N/A

At the bottom of the configuration area are 'Refresh', 'Save', and 'Help' buttons. A status bar at the very bottom indicates 'Getting values finished' and 'Version: 1.3.19.17'.

4. Change the “**Rx Power Intrusion Threshold**” setting as desired. The default is 0 uW. The valid range is 0 - 65,535 uW (microwatts).
5. You can click the **Refresh** button to update the information displayed.
6. Click the **Save** button to save the updated information.

The **C4221 > DMI** tab > **Interface Characteristics**, **Diagnostic Monitoring**, and **Supported Media Length** section’s fields are explained below.

Table 4: DMI Parameter Descriptions

Parameter	Description
Interface Characteristics	
DMI ID	Specifies the physical DMI device ID from the standard; for example SFP/SFP+/SFP28, etc.
Connector Type	The external optical or electrical cable connector provided as the interface. For example LC, etc.
Nominal Bit Rate (Mbps)	Bitrate in units of 100Mbps (for example: 10500, or 10.5 Gbps) (measured rate).
Fiber Interface Wavelength (nm)	The Nominal transmitter output wavelength at room temperature (measured wavelength). The unit of measure is nanometers (for example: 1550 nm or 850 nm).
Diagnostic Monitoring	
Receive Power (uW)	Receive power (measured power measurement) on local fiber measured in microwatts (for example: 11 uW).
Receive Power (dBm)	Receive power (measured signal strength) on local fiber measured in dBm (decibels relative to one milliWatts) which defines signal strength. For example: -19.586 dBm.
Receive Power Alarm	Alarm status for receive power on local fiber: Normal -1 Not Supported - 2 Low Warn - 3 High Warn - 4 Low Alarm - 6 High Alarm - 7
Rx Power Intrusion Threshold (uW)	Enter a value of 0-65,535 uW for Rx Power on the Fiber port. The default is 0 uW. If the DMI read value falls below this value, an intrusion is detected, and a trap is generated (0-10). The message displays: <i>ALARM: Receive power is below specified threshold. Fiber trap intrusion may be in progress.</i>
Temperature (°C)	Measured temperature of fiber transceiver in tenths of degrees C (Celsius). For example: 30.1°C.
Temperature (°F)	Measured Temperature of fiber transceiver in tenths of degrees F (Fahrenheit). For example: 86.2 °F.

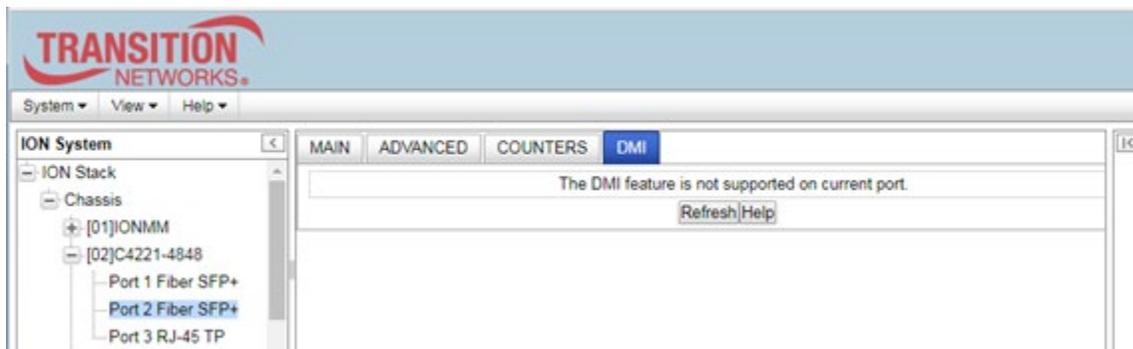
Parameter	Description
Temperature Alarm	Alarm status for temperature of fiber transceiver. An <i>ionDMITemperatureEvt</i> event is sent when there is a warning or alarm on DMI temperature. Normal -1 Not Supported - 2 Low Warn - 3 High Warn - 4, Low Alarm - 6 High Alarm - 7
Transmit Bias Current (uA)	Measured transmit bias current on local fiber interface, in uA (microamperes). For example, 5936 uA (microamps).
Transmit Bias Alarm	Alarm status for transmit bias current on local fiber interface. Normal -1 Not Supported - 2 Low Warn - 3 High Warn - 4 Low Alarm - 6 High Alarm - 7
Transmit Power (uW)	Measured transmit power on local fiber measured in microwatts. For example, 240 uW (microwatts).
Transmit Power (dBm)	Transmit power on local fiber measured in dBm (decibels relative to one milliwatt) which defines signal strength. For example: -2.291 dBm.
Supported Media Length	
Transmit Power Alarm	Alarm status for transmit power on local fiber. Normal -1 Not Supported - 2 Low Warn - 3 High Warn - 4 Low Alarm - 6 High Alarm - 7
9/125u Singlemode Fiber (km)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is kilometers (km). For example, 8Km.
9/125u Singlemode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). For example, 80m.
50/125u Multimode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters.
62.5/125u Multimode Fiber (m)	Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters.
Copper (m)	Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters.

For More Information on topics such as Fiber Optics Power Measurements, Fiber and Cable Loss, OTDRs, Bandwidth, Reflectance/Optical Return Loss, and Fiber Optic Cleaning Procedures see the Fiber

Optic Association - Tech Topic in the FOA Guide to Optics and Premises Cabling on the FOA website at <http://www.thefoa.org/tech/FAQS/FAQ-TEST.HTM#bw>.

DMI Messages

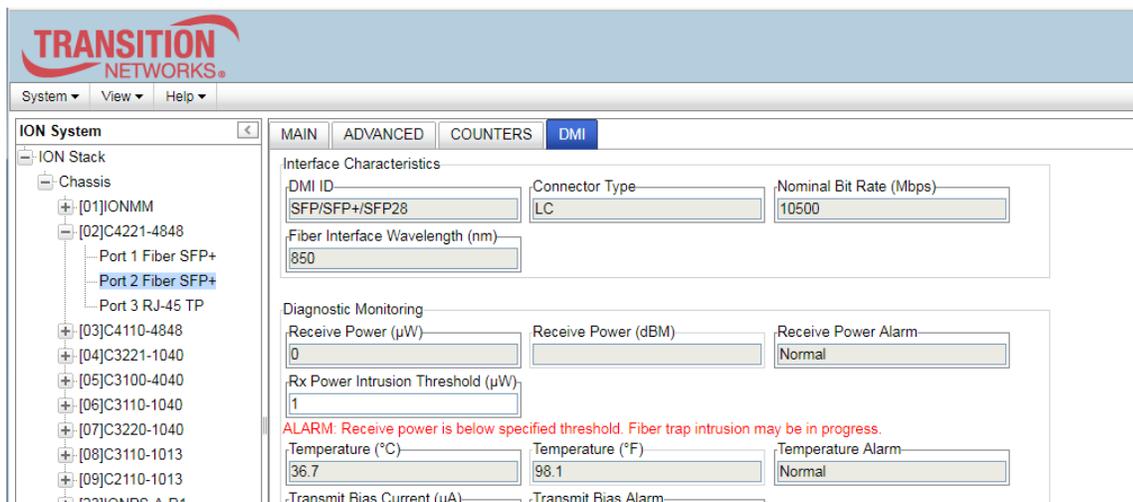
Message: *The DMI feature is not supported on current port.*



Meaning: An SFP supporting DMI is not inserted in this port.

Recovery: Insert an SFP in the port and click the **Refresh** button, or click another port's DMI tab.

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



Meaning: The setting for **Rx Power Intrusion Threshold (µW)** was exceeded. This is a configured level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated.

Recovery: Check for an intrusion or change the Rx Power Intrusion Threshold setting to a different value. Click the **Save** button and click the **Refresh** button.

Message: *Invalid input found!*

Meaning: You entered a parameter value outside of the valid range.

Recovery: Enter a valid parameter, click **Save**, and continue operation.

Message: *No changes to be saved*

Meaning: You clicked the **Save** button without changing any parameter values.

Recovery: Enter a valid parameter, click **Save**, and continue operation.

5: Operation

General

This section describes the non-configuration operations that can be performed for the C4221 NID.

Reset to Factory Defaults

If need be, you can reset all configurations in the SIC back to their original factory defaults.

IMPORTANT

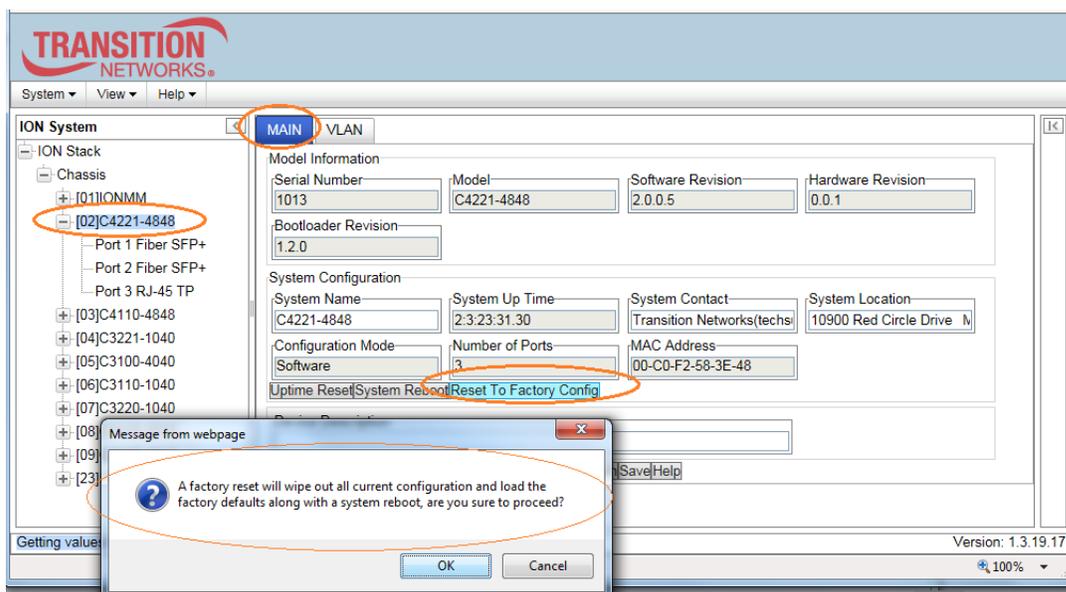


This operation deletes **all** configuration information that was saved in the SIC, including the IP address you assigned to the SIC.

Resetting Defaults

Caution: This operation deletes all configuration information that was saved in the C4221, including the IP address you assigned to the C4221.

1. Select the **MAIN** tab.
2. Locate the **System Configuration** section.



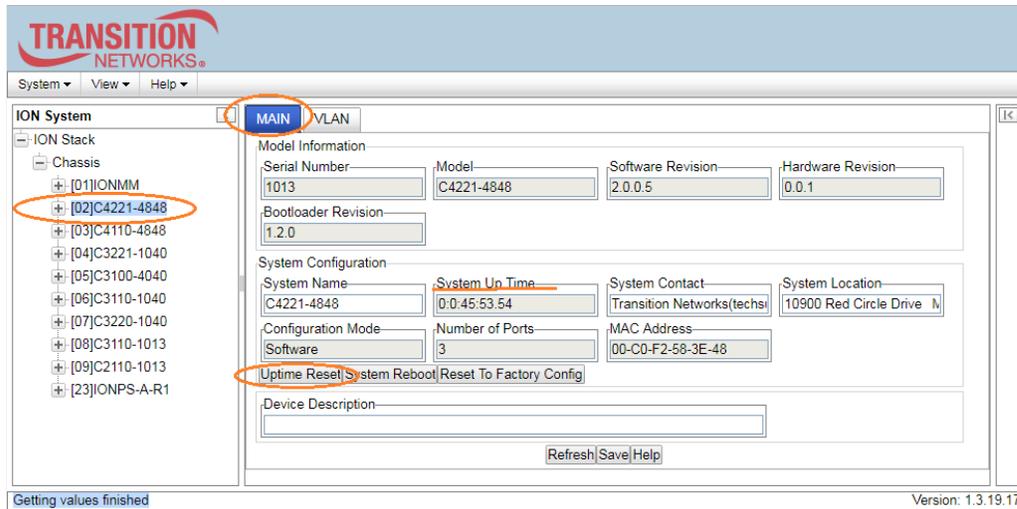
3. Click the **Reset to Factory Config** button. The message “A factory reset will wipe out all current configuration and load the factory defaults along with a system reboot; are you sure to proceed?” displays.
4. Click **Cancel** if you are sure you want to proceed with the Reboot. Click **OK** only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

Resetting Uptime

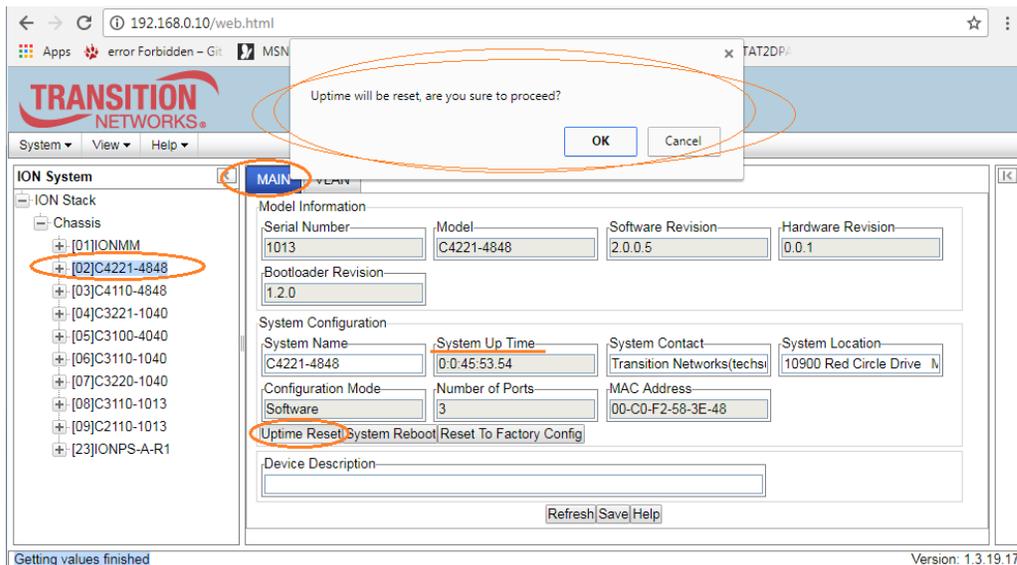
The System Up Time field displays the amount of time that the ION system has been in operation. The uptime is displayed in the format days:hours:minutes:seconds.milliseconds. For example, a **System Up Time** field display of **9:8:15:18.26** indicates the ION system has been running for 9 days, 8 hours, 15 minutes, 18 seconds, and 26 milliseconds.

Reset System Uptime

1. At the device **MAIN** tab, locate the **System Configuration** section.



2. If desired, observe and record the **System Up Time** field count.
3. Click the **Uptime Reset** button. The message *“Uptime reset, are you sure”* window displays.



4. Click **OK** to reset the system up time. The message *“Setting values succeeded”* displays at the bottom left of the screen when the Uptime reset is done.
5. Click the **Refresh** button at the bottom of the screen. The **System Up Time** field resets to zero and immediately begins to increment.

Resetting Counters

Before running certain diagnostics / tests, you may want to reset (zero out) all or some C4221 device and/or port counters.

Reset Port Counters

This is a port-level function used to reset all of a C4221 port's counters.

1. Select the desired C4221 port.
2. Select the **COUNTERS** tab.

The screenshot shows the web interface for the ION C4221 device. The left sidebar shows a tree view of the ION Stack, with the following items highlighted in red circles: [02]C4221-4848, Port 2 Fiber SFP+, and Port 3 RJ-45 1P. The main content area is titled 'COUNTERS' and displays the following data:

RMON Counters			
Total Octets	Packets Received	Broadcast Packets	Multicast Packets
33434	270	0	270
CRC Align Errors	Undersize Packets	Oversize Packets	Fragments
0	0	0	0
Jabbers	Drop Events		
0	270		
64 Octets	65 to 127 Octets	128 to 255 Octets	
0	254	16	
256 to 511 Octets	512 to 1023 Octets	1024 to Max Octets	
0	0	0	
RX Counter			
Total Octets	Unicast Packets	Broadcast Packets	Multicast Packets
33434	0	0	270
Rx Discards	Rx Errors		
270	0		
TX Counter			
Total Octets	Unicast Packets	Broadcast Packets	Multicast Packets
78354	0	0	447
Tx Discards	Tx Errors		
0	0		
MAC Control Frames			
Rx Pause Frames	Tx Pause Frames		
0	0		

At the bottom of the counter section, there are three buttons: 'Reset Counters', 'Refresh', and 'Help'. The 'Reset Counters' button is highlighted with a red circle.

3. If desired, click the **Refresh** button and observe and record the various counter field counts for later comparison.
4. Click the **Reset Counters** button. The C4221 port-level counters are reset to zero and begin incrementing immediately. The counters that are reset include:
 - RMON Counters
 - Rx Counter
 - Tx Counter
 - MAC Control Frames

The Port Counter parameters are described in the following section.

Port Counter Parameters

Ethernet Statistics Counters are available for situations where performance, particularly rate or error counts, is suspect. The **RMON Counters** section is explained below.

Parameter	Description
Total Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets Received	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

128 to 255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to Max Octets	The total number of packets (including bad packets) received that were between 1024 and the set maximum number of octets in length inclusive (excluding framing bits but including FCS octets).

The **RX Counter** and **TX Counter** sections are explained below.

Parameter	Description
Total Octets (Port Counters Received)	The total number of octets received on the interface, including framing characters.
Unicast Packets (Port Counters Received)	The number of packets , delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
Multicast Packets (Port Counters Received)	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses.
Broadcast Packets (Port Counters Received)	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Multicast Packets (Port Counters Sent)	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
Broadcast Packets (Port Counters Sent)	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Rx Discards (Port Counters Received)	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Rx Errors (Port Counters Received)	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

Total Octets (Port Counters Sent)	The total number of octets transmitted out of the interface, including framing characters.
Unicast Packets (Port Counters Sent)	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
Tx Discards (Port Counters Sent)	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Tx Errors (Port Counters Sent)	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

The **MAC Control Frames** counter sections are explained below.

Parameter	Description
Rx Pause Frames	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Tx Pause Frames	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

ION System

ION Stack

- Chassis
 - [01]IONMM
 - [02]C4221-4848
 - Port 1
 - Port 2
 - Port 3
 - [03]C4110-4848
 - [04]C3221-1040
 - [05]C3100-4040
 - [06]C3110-1040
 - [07]C3220-1040
 - [08]C3110-1013
 - [09]C2110-1013
 - [23]IONPS-A-R1

MAIN | ADVANCED | **COUNTERS** | DMI

RMON Counters

Total Octets	Packets Received	Broadcast Packets	Multicast Packets
85028	689	3	686
CRC Align Errors	Undersize Packets	Oversize Packets	Fragments
0	0	0	0
Jabbers	Drop Events		
0	651		
64 Octets	65 to 127 Octets	128 to 255 Octets	
3	641	45	
256 to 511 Octets	512 to 1023 Octets	1024 to Max Octets	
0	0	0	

RX Counter

Total Octets	Unicast Packets	Broadcast Packets	Multicast Packets
85028	0	3	686
Rx Discards	Rx Errors		
651	0		

TX Counter

Total Octets	Unicast Packets	Broadcast Packets	Multicast Packets
194299	0	0	1133
Tx Discards	Tx Errors		
0	0		

MAC Control Frames

Rx Pause Frames	Tx Pause Frames
0	0

Reset Counters Refresh Help

Getting values finished

Version: 1.3.1912

Reboot and Reset 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 of the *ION C4221 Install Guide* for information on how to save the stored files from deletion.

Reboot

At times you may have to reboot (restart) the ION system. This can be done by either the CLI or Web. **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 certain sections. The 'red box' condition occurs while the devices are resetting; this condition can continue several minutes after the reboot. Clicking the **System Reboot** button resets all system states and reinitializes the system; all configuration data is saved during a restart. The message “*Loading, please wait...*” displays.



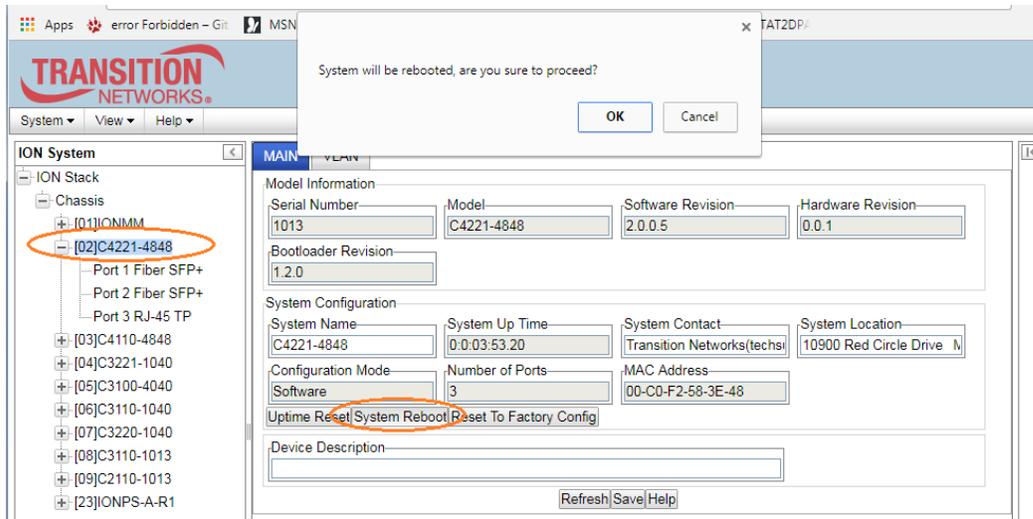
Doing a system reboot, restart, upgrade, or a reset to factory settings may cause some configuration backup files or other files to be deleted.

Rebooting

Caution: Doing a system reboot will cause all configuration backup files to be lost.

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

1. Select the **MAIN** tab.
2. Locate the **System Configuration** section.
3. Click the **System Reboot** button. The confirmation message “*System will be rebooted, are you sure to proceed?*” displays.

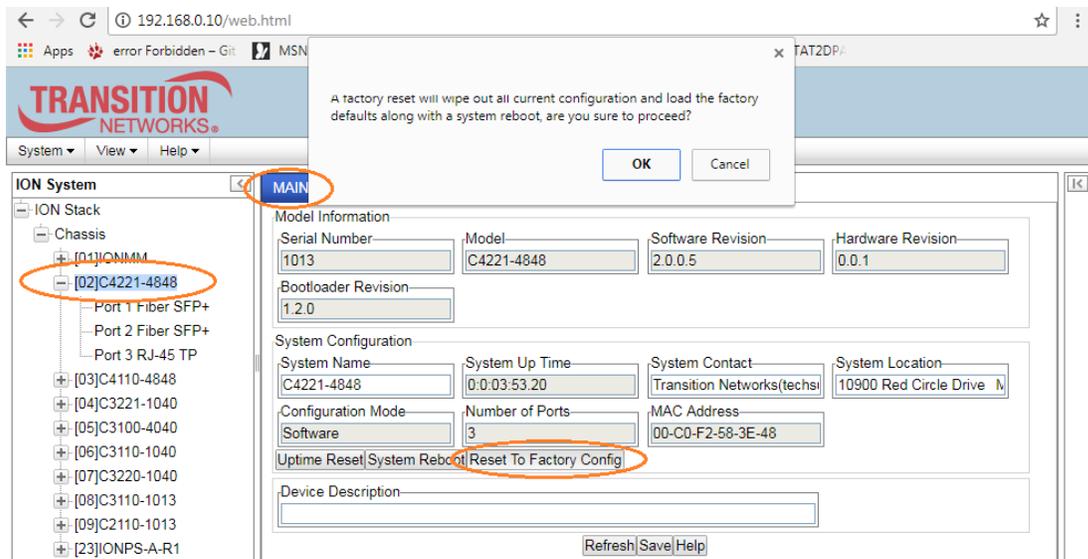


4. At the confirmation window, click the **OK** button to start the reboot, or click **Cancel** to quit the reboot. If you click **OK**, the C4221 will restart and will be available for operation after about **three minutes**.

Reset To Factory Config

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

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



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

Related Functions

Upgrade is only supported on IONMM card. See the *IONMM User Guide* for specific information.

Backup/Restore should be done on the IONMM. Note that when doing a backup with no stack name the CLI prepends the serial number of the chassis to the TARFILE, but the Web UI does not; the Web just prepends an underscore, "_" (_backup.....).

6: Troubleshooting

General

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

IMPORTANT

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

Basic ION System Troubleshooting

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

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

- ION Chassis
- ION NIDs (SICs, or slide-in-cards)
- IONMM
- ION software (ION System Web Interface or ION 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, 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 the Web UI.
5. Start with the most simple and work towards the more complex possible problem causes (e.g., check the network cables and connections, check the device LEDs, verify the NIDs are seated properly, view the CLI **show** command output, check the Syslog file, verify IP addresses and Gateway IP address, check Windows Event Viewer, ping the interface, run the various SOAM tests if functional, etc.).
6. Write down your initial 2-3 guesses as to the cause of the problem.
7. Verify that the product supports the function you are attempting to perform. Your particular 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 the 1-2 most likely main causes of what went wrong, and gain as much information as you can to prove the suspected cause(s).
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 for support.

Error Indications and Recovery Procedures

The types of indications or messages reported include:

- LED fault and activity displays
- Problem Conditions
- Web Interface Messages
- Webpage Messages
- Config Error Log (config.err File) Messages

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

LED Fault and Activity Displays

Refer to this section if the LEDs indicate a problem. For any LED problem indication, review the “[Front Panel Connections and LEDs](#)” section of the ION C4221 Install Guide, and then perform these steps.

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

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 “[Jumper Settings](#)” in the *ION C4221 Install Guide*.

LACT (Link Activity) LED off (not lit):

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

Fault LED is lit:

1. Check for a problem with the IONMM or NID hardware, software, or configuration.
2. Make sure all circuit protection and connection equipment and devices are working.
3. Verify that the ION system power supply is within operating range.
4. Remove the card from the chassis and re-insert it.
5. Make sure the USB cable is properly connected.
6. Reset the IONMM.

TX or RX LED off (not flashing):

1. Check the data cables for obvious problems, incorrect cable type, incorrect wiring, etc.
2. Check if other network devices are working properly.
3. Verify that the ION system devices have the latest firmware versions.
4. Download the latest firmware version and upgrade as necessary.
5. Remove the card from the chassis and re-insert it.

Problem Conditions

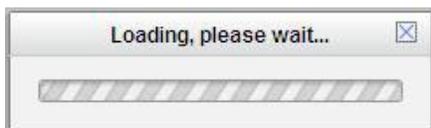
Telnet connection is lost after a CLI command is executed

1. If you can connect to the IONMM through the Web interface (see “Starting the Web Interface”), go to step 3 below. If you cannot connect to the IONMM via the Web UI, continue with step 2 below.
2. Check the following:
 - the IONMM is seated properly in the chassis
 - the IONMM is powered up
 - the network cable is seated
 - the network is operational
3. For all modules (slide-in and remote) check the following:
 - module is properly seated/connected
 - module is powered up
4. Cycle power for the module in question. **Note:** for slide-in cards, pull the module out so it is no longer connected to the backplane, then slide the module back in, ensuring that it is firmly seated.
5. If the problem persists, contact Technical Support.

Ethernet connection works, but at a very low speed

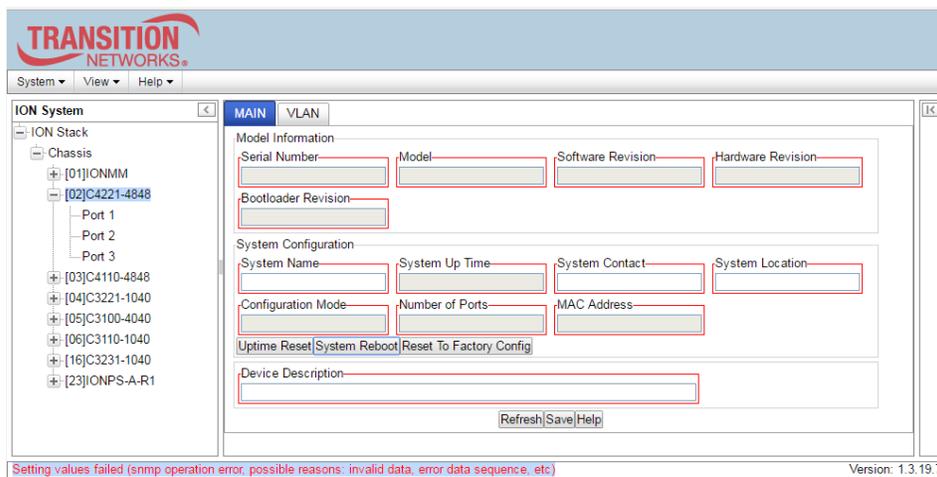
1. Check if the **Auto Negotiate** feature is enabled.
2. If **Auto Negotiate** is enabled, check if one device is using full duplex while the other one is using half-duplex (a duplex mismatch condition). The usual effect of this mismatch is that the connection works but at a very low speed.
3. Change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

loading, please wait ... Displays continuously



1. Wait for one or more minutes for discovery to complete.
2. Click the icon to close the message.
3. Check the parameter entries and retry the operation.
4. Click the **Refresh** button and try the operation again.
5. If the problem persists, contact Technical Support.

Parameter Boxes Outlined in Red / Cannot Enter Parameters



1. Check if the device is physically connected and powered on.
2. If the "Getting values failed" message also displays, refresh the device by clicking the **Refresh** key.
3. Collapse and then expand the ION System tree (i.e., fold and then unfold the "ION Stack" node in the left tree view) to refresh.
4. Cycle power for the device in question.
5. Reboot the device by clicking the **Reboot** key. Check if the parameter boxes are again outlined in black and that you can enter parameters.
6. Upgrade the device(s) to the latest software version.
7. Reboot the ION System using the **System Reboot** button. See the [Reboot](#) section.
8. If the problem persists, contact Technical Support.

Red Box Condition

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

1. Wait a couple of minutes for the current operation to complete, and then continue operation.
2. Check the devices' firmware versions. For example, a C4221 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 C4221 is at an older version and shows the newer functions as 'red boxed'. Since the older version of C4221 does not have knowledge of the new features, it will not respond to the IONMM for the new items, and the IONMM shows those items as 'red boxed'. Upgrade the devices to the latest software version.
3. Reboot the system. See the "[Reboot](#)" section for more information.
4. Contact Lantronix for more information.

Windows XP Cannot Find Drivers For My Device

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

1. Contact Lantronix for more information.

Windows XP Forces a Reboot after Installing a Device

This problem can occur if an application is accessing a file while the New Hardware Wizard is trying to copy it. This usually occurs with the FTD2XX.DLL file.

1. Select not to restart the computer and then unplug and re-plug the device. This may allow the device to function properly without restarting.
2. Restart the computer to allow the device to work correctly.
3. Contact Lantronix for more information.

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 Lantronix for more information.

Windows XP Displays an Error and then Terminates Installation

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



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

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

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

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:

1. Make sure that C4221 ingress rate limiting settings are at or above the advertised speeds.
2. Change the rate, duplex mode, frame size, packet size, or Ingress Rate Limit. See the related section of this manual for details.

Web Interface Messages

IMPORTANT

For each procedure described below, do each step sequentially as indicated. If performing the step fixes the problem, **do not** continue with the other steps in the procedure.

Cannot Ping IONMM Device

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device.
2. After reducing the "Egress Rate Limit" ", 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 reserve some Egress bandwidth for user management traffic. The PC can then ping to the NID again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support.

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.

Invalid password!

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

1. Sign in using the correct password. The default password is **private**.
Note: the password is case sensitive. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.
3. If the problem persists, contact Technical Support.

Admin Status: Down (or Testing)

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

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

1. Verify the initialization process; see "[Section 2: Installation and System Setup](#)".
2. Verify the attempted operation procedure in the related section of this manual.
3. Retry the operation. Wait several minutes for initialization and discovery to take place.
4. If the problem persists, contact Technical Support.

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

This is the current operational state of the interface.

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

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

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

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

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

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

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

1. Review any specific fault and its recommended recovery procedure.
2. Verify the initialization process; see “[Section 2: Installation and System Setup](#)”.
3. Verify the attempted operation procedure in the related section of this manual.
4. Retry the operation. Wait several minutes for initialization and discovery to take place.
5. If the problem persists, contact Technical Support.

Link Status: Dormant: The ION system interface is waiting for external actions (such as a serial line waiting for an incoming connection).

1. Wait several minutes for initialization and discovery to take place, and then retry the operation.
2. If the problem persists, contact Technical Support.

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

1. Verify the ION system installation; see “[Section 2: Installation and System Setup](#)”.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

Link Status: Testing: The ION system interface cannot pass operational packets.

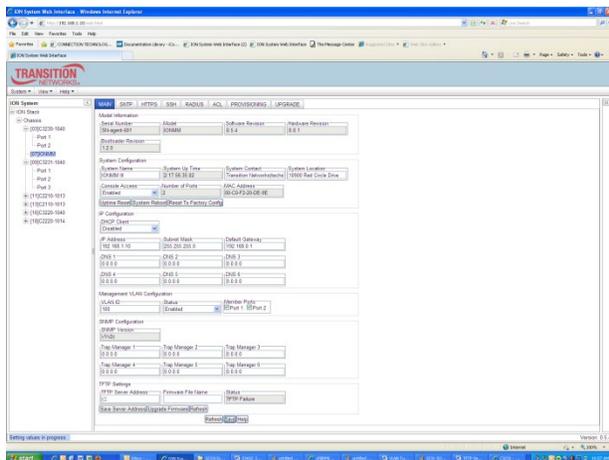
1. Verify that diagnostic tests were run properly and completed successfully.
2. Wait several minutes for initialization and discovery to take place, and then retry the operation.
3. If the problem persists, contact Technical Support.

Message: Web UI Management connection Lost

1. With the "Egress Rate Limit" set to "Unlimited", the PC can ping the device.
2. After reducing the "Egress Rate Limit" 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 reserve some Egress bandwidth for user management traffic.
The PC can ping the C4221 again, and the WEB UI can be managed again.
4. If the problem persists, contact Technical Support.

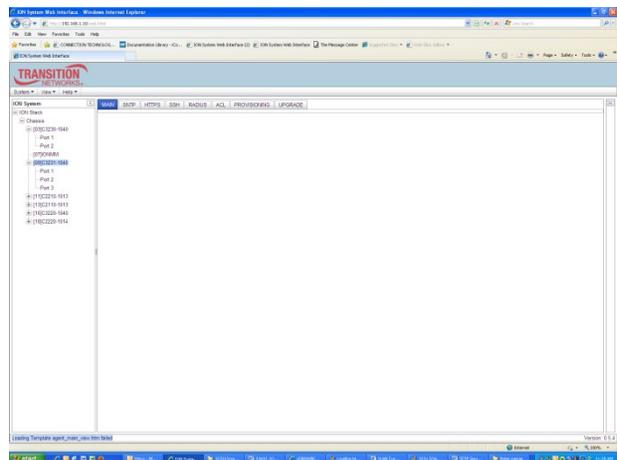
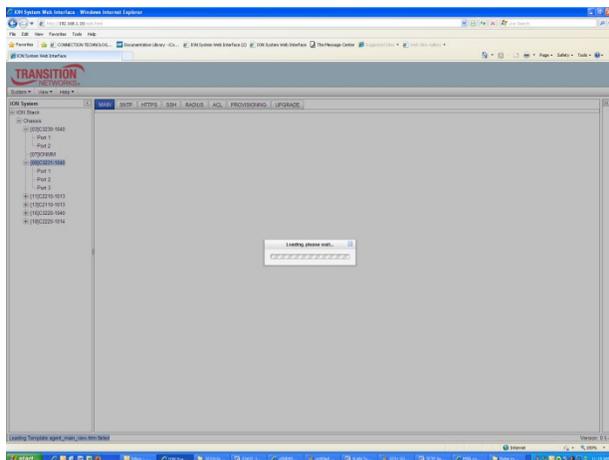
Message: "Setting values in progress ..." displays continuously

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:



Message: *Loading template config file succeeded* displays but the ION Stack node won't expand.

Meaning: Either the loading or the discovery process may be hung up.

Recovery: 1. Click the checkbox to close the "*Loading, please wait ...*" dialog box (if displayed).

2. Contract and expand the ION Stack node again.

3. If the message "*Discovering succeeded*" displays, but the ION Stack node won't expand:

a) Sign out and sign back in to the ION system

b) Cycle power to the ION system.

c) Disconnect and then re-connect the USB cable at the IONMM.

4. If the problem persists, contact Technical Support.

Message: *System initializing or SNMP service busy, please wait...*

Meaning: The system password was accepted, but the system cannot recognize or process it.

Recovery: Sign in using the correct password. The default password is private. Note that the password is case sensitive.

1. Make sure the keyboard's "Caps Lock" is off.

2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the log in to proceed.

3. Verify the SNMP configuration.

4. If the problem persists, contact Technical Support.

Message: *ERROR: Software version of this card (0.7.1) is not supported, please upgrade to the same version as the IONMM*

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

Recovery: 1) Select the IONMM device. 2) Select the UPGRADE tab. 3) Perform a firmware upgrade to this card (and others that may have outdated firmware). See the “Upgrade” section.

2) If a problem persists, contact Technical Support.

Message: *Current power status of this slot is off, please turn it on before you reset it!*

Meaning: The reset function only works when the slot power is in the On position for the unit to re-boot/reset.

Recovery: 1) At **Chassis > MAIN > Chassis Members** click the "On" button in the **Power Status** column of the device before you click the "Reset" button. 2) If a problem persists, contact Technical Support.

Problem: Setting the VLANID failed with an SNMP operation error message:

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

Adding VLAN failed (snmp operation error)

Meaning: You tried to add or edit a VLAN ID but the effort failed.

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

In IE8, at C4221 the ‘Refresh’, ‘Add’, ‘Edit’, ‘Delete’, ‘Help’ buttons do not display.

1. Select **IE8 Tools > Compatibility Mode** to use the IE8 ‘Compatibility View’. The message “**Compatibility View - 192.168.0.10 is now running in Compatibility View.**” displays.



2. Log in to the ION system again.

3. Select the desired tab.

4. Select at least one page item, and then click the web page; the button will display normally.

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

Problem/Message:

Internet Explorer 11 message indicates *“This page can’t be displayed.”*

“Invalid username or password message displays at the ION System Login page in IE 11.

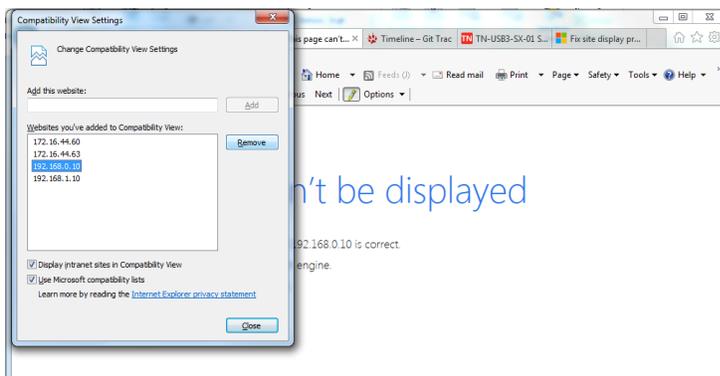
ION System web pages do not display or display incorrectly in Internet Explorer 11.

The ION System message *“loading, please wait ...”* displays continuously and IE11 freezes

Cause: In earlier IE versions, the Compatibility View button would try to fix a broken standards-based website by getting the page to display like it did in Internet Explorer 7. Compatibility issues were largely resolved since IE 7, to the point where the Compatibility View button was removed for IE11.

Recovery: Remove the ION URL from Compatibility View:

1. With ION up, click on the Gear icon at the top right corner of your IE window and choose Compatibility View settings.
2. Select the ION URL in “Websites you’ve added to Compatibility View:” and click the **Remove** button.



3. You also have the option to uncheck (disable) two other features:
 - Display intranet sites in Compatibility View
 - Use Microsoft compatibility lists
4. Click the **Close** button when done and log back in to the ION System.

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>.

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.

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: *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: *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. Click the **Try again** button to retry the operation.
3. If the problem persists, contact Technical Support.

Message: *This Connection is Untrusted*

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

Recovery: 1. Click **Technical Details** for details, or click **I Understand the Risks** to continue operation.

2. If the problem persists, contact Technical Support.

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

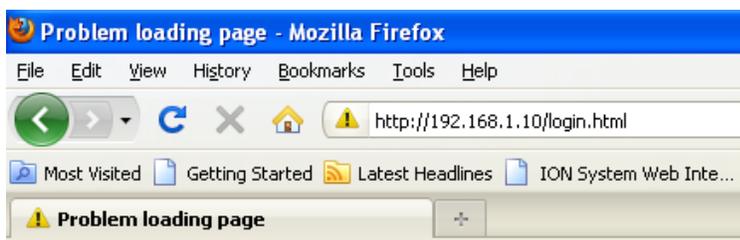


Meaning: You unplugged the USB cable at the NID or IONMM, or the NID or IONMM was unplugged from the ION chassis, or you pressed the **RESET** button on the IONMM.

Recovery:

1. If you pressed the **RESET** button on the IONMM, wait a few moments for the message to clear.
2. Plug the USB cable back into the IONMM's **USB-DEVICE** connector, or plug the USB cable back into the NID's **USB** connector.
3. Try the operation again.
4. If the problem persists, contact Technical Support.

Message: *Problem loading page – Mozilla Firefox*

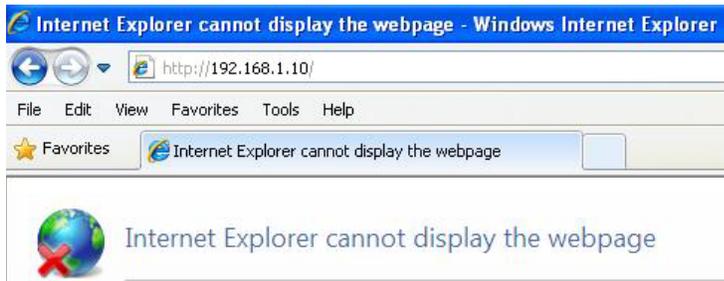


Meaning: You tried to log in to the ION system from the Mozilla Firefox browser, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See "[Web Browsers Supported](#)".
2. Verify the URL entered.
3. Verify NID access. See "[Accessing the NIDs](#)".
4. Verify the IP address setting.
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.

Message: *Internet Explorer cannot display webpage*

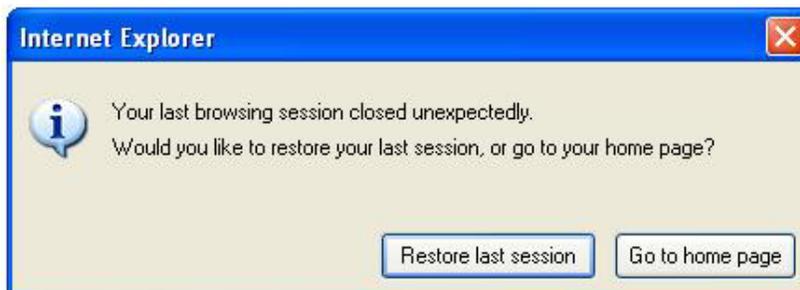


Meaning: You tried to log in to the ION system from IE, but the login failed.

Recovery:

1. Make sure the web browser / version you are using is supported. See "[Web Browsers Supported](#)".
2. Verify the URL entered. See "[Initial Setup with a Static IP Address via the CLI](#)".
3. Verify NID access. See "[Accessing the NIDs](#)".
4. Verify the IP address setting.
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.

Message: *IE - Your last browsing session closed unexpectedly*



Meaning: The IE web browser crashed.

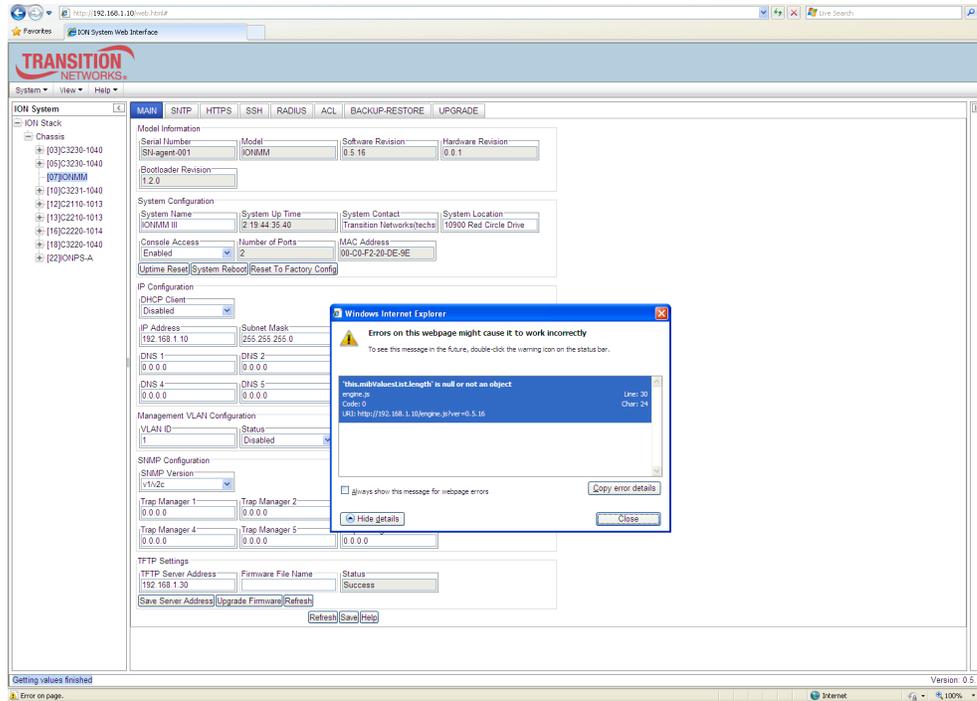
Recovery: Click the **Restore last session** button. The **Sign in to ION System Web Interface** screen displays. Enter your Password and click the **Sign In** button.

Message: *Error on page.*

Message: *Errors on this webpage might cause it to work incorrectly.*

Message: *'this.mibValuesList.length' is null or not an object*

Meaning: In Windows IE, the message displays after some amount of inactivity.



Recovery:

1. On the Windows IE error dialog, click the **“Show details”** button.
2. Click the **“Copy error details”** button.
3. Click the **“Webpage error details”** button. Additional error information is copied (like doing a **Ctrl-C** keyboard command)
4. Paste the error details text (use **Ctrl-V** command) into a text file in Notepad, Wordpad, MS Word, etc., and then save the newly created file. For example:

```
User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
.NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)
```

```
Timestamp: Mon, 6 Dec 2010 14:20:17 UTC
```

```
Message: 'this.mibValuesList.length' is null or not an object
```

```
Line: 30
```

```
Char: 24
```

```
Code: 0
```

```
URI: http://192.168.0.10/engine.js?ver=0.5.16
```

5. Click the **Close** button to close the Windows IE error dialog.
6. Click the ION system **Refresh** button.
7. Retry the operation.
8. If the problem persists, contact Technical Support.

Recording Model Information and System Information

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

1. From the ION system Web interface, select the C4221 device **MAIN** tab. (From the CLI, use the **show** commands to gather the information requested below. This could include commands such as **show card info**, **show slot info**, **show system info**, **show ether config**, **show ip-mgmt config**, **show loam config**, or others as request by the Support Specialist.

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

Serial Number: _____ Model: _____

Software Revision: _____ Hardware Revision: _____

Bootloader Revision: _____

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

System Up Time: _____ Configuration Mode: _____

MAC Address: _____ Number of Ports: _____

4. Provide additional Model and System information to your Technical Support Specialist. See “[Basic ION System Troubleshooting](#)”.

Your Lantronix service contract number: _____

A description of the failure: _____

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

The serial # and revision # of each involved Lantronix product in the network:

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

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

See the *ION C4221 Install Guide* for details on:

- Warranty
- Compliance Information
- Declaration of Conformity
- Electrical Safety Warnings in multiple languages



Lantronix Corporate Headquarters

48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: <https://www.lantronix.com/technical-support/>

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.