N-TRON
THE INDUSTRIAL NETWORK COMPANY

7900 Series Industrial Gigabit Ethernet Switch

User Manual & Installation Guide

Industrial Gigabit Ethernet Switch Installation Guide

7900 Series

The N-TRON 7900 Series Gigabit Ethernet Capable Industrial Ethernet Switch offers outstanding performance and ease of use. It is ideally suited for connecting Ethernet enabled industrial and or security equipment and is a fully managed switch.

PRODUCT FEATURES

- Full IEEE 802.3 Compliance
- Full IEEE 1613 Compliance (Electric Power Stations)
- NEMA TS1/TS2 Compliance (Traffic Control systems)
- ABS Type Approval (Maritime and Offshore Applications)
- Scalable Switch with 4 I/O Slots
- Up to twenty-four 10/100 Base-TX RJ-45 Ports
- Two Optional Gigabit ports:
    - 1000BaseSX/LX Ports, LC style, and/or
    - 1000BaseT Ports, RJ45 style
- Extended Environmental Specifications
- Autosensing 10/100 Base-TX, Duplex, and MDIX
- Offers Rapid Spanning Tree Protocol
- Trunk with other N-Tron trunking capable switches
- Store & Forward Technology
- Plug and Play IGMP Support
- Rugged Din-Rail Enclosure
- Redundant Power Inputs (10-30 VDC)
- Onboard Temperature Sensor
- Configuration Backup via optional SD Card (NTCD-128)
- Full SNMP
- Web Browser Management with detailed ring map and fault location charting.
- Web Browsing and N-View Switch Monitoring

MODULE / SLOT OPTIONS

- 7900 CPU Module – CPU Module with 2 SFP Gigabit Ports
- 9006 TX – 6 Port 10/100 Base-TX Copper Module
- 9004 FX – 4 Port 100 Base-FX Fiber Module
- 9002 FX – 2 Port 100 Base-FX Fiber Module

MANAGEMENT FEATURES

- IGMP Snooping
- VLAN
- QoS
- Port Trunking
- Port Mirroring
- LLDP
- CIP
- 802.1D-2004 Rapid Spanning Tree
- N-RING™ (N-Tron proprietary Ring Management)
- N-LINK™ (N-Tron proprietary Coupling Management)
- DHCP Server, Option 82 relay
- Port Security—MAC Address Based

7900 Industrial Ethernet Switch Accessories

Do not use, connect, or disconnect the SD Card unless the area is known to be non-hazardous. Connection or disconnection in an explosive atmosphere could result in an explosion.

 **NTCD-128**	Configuration Device Ideal for saving, or restoring switch configuration parameters quickly without the need for a computer or software. One configuration device per switch is recommended.

The configuration device is inserted into the front of the 7900 CPU Module.

Warning

Do not perform any services on the unit unless qualified to do so. Do not substitute unauthorized parts or make unauthorized modifications to the unit.

Do not operate the unit with the top cover removed, as this could create a shock or fire hazard.

Do not block the air vents on the sides or the top of the unit.

Do not operate the equipment in the presence of flammable gasses or fumes. Operating electrical equipment in such an environment constitutes a definite safety hazard.

Do not operate the equipment in a manner not specified by this manual.

Safety Warnings

GENERAL SAFETY

WARNING: If the equipment is used in the manner not specified by N-Tron Corporation, the protection provided by the equipment may be impaired.

LASER SAFETY 7900CPU with these SFPs:

*1000BaseLX (*NTSFP-LX-40):	40 kilometers
*1000BaseLX (*NTSFP-LX-80):	80 kilometers

CAUTION: CLASS 1 LASER PRODUCT. Do not stare into the laser!

SUPPORT:

Contact Information

N-Tron Corporation
3101 International Drive
Building 6
Mobile, AL 36606
TEL: (251) 342-2164
FAX: (251) 342-6353
Website: www.n-tron.com
Email: N-TRON_Support@n-tron.com

ENVIRONMENTAL SAFETY

WARNING: Disconnect the power and allow to cool 5 minutes before touching.

ELECTRICAL SAFETY

WARNING: Disconnect the power cable before removing any modules, or any enclosure panel.

WARNING: Do not operate the unit with the any cover removed.

WARNING: Properly ground the unit before connecting anything else to the unit. Units not properly grounded may result in a safety risk and could be hazardous and may void the warranty. See the grounding technique section of this user manual for proper ways to ground the unit.

WARNING: Do not work on equipment or cables during periods of lightning activity.

WARNING: Do not perform any services on the unit unless qualified to do so.

WARNING: Do not block the air vents.

WARNING: Observe proper DC Voltage polarity when installing power input cables. Reversing voltage polarity can cause permanent damage to the unit and void the warranty.

Installation Requirements

1. **WARNING:** Explosion Hazard - Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

2. **WARNING:** Install only in accordance with Local & National Codes of Authorities having jurisdiction.

3. **WARNING:** This equipment is suitable for use in Class I, Div. 2, Groups A, B, C, D or Non-Hazardous Locations Only.

4. **WARNING:** Explosion Hazard – Substitution of Components May Impair Suitability For Class I, Div. 2.

5. **WARNING:** Explosion Hazard – Do not remove SD Card unless power has been disconnected or the area is known to be free of ignitable concentrations of flammable gases or vapors.

6. **WARNING:** Explosion Hazard – Do not remove Fiber Optic Transceivers unless power has been disconnected or the area is known to be free of ignitable concentrations of flammable gases or vapors.

7. Power must be supplied by an isolating source, and a 3.3 A max rated UL Recognized fuse must be installed immediately before the unit.

8. Class I, Div 2 installations require that all devices connected to this product must be UL listed for the area in which it is installed.

9. Only UL listed wiring with temperature ratings greater than 90°C permitted for Class I, Div 2 installations operating at temperatures up to 70°C ambient.

10. Limited Operating Voltage: 12-30V for Class I, Div 2 installations.

11. Maximum operating voltage of power source shall not exceed 60 VDC including battery charging float voltage.

PACKAGE CONTENTS

Please make sure the 7900 Series Gigabit Ethernet Switch package contains the following items:
1. 7900 Series Gigabit Ethernet Switch and other modules, filler panels, or accessories that may have been ordered.
2. Product CD

Contact your carrier if any items are damaged.

INSTALLATION

Read the following warning before beginning the installation.

WARNING

Never install or work on electrical equipment or cabling during periods of lightning activity. Never connect or disconnect power when hazardous gasses are present.

Disconnect the power cable before removing any enclosure panel.
Do not operate the unit with any covers removed

UNPACKING

Remove all the equipment from the packaging, and store the packaging in a safe place. File any damage claims with the carrier.

CLEANING

Clean only with a damp cloth.

SERVICING

The 7900 Series is a modular based Gigabit Ethernet Switch with up to 4 slots for ports and one slot for the CPU module. Please follow the steps below for adding, removing, or swapping modules in the 7900 series switch. Technicians performing the following steps should wear proper anti-static equipment to protect the circuit boards. **WARNING: The 7900 Series switch is NOT hot swappable. Removing or adding modules while the power is still on can damage the equipment.**

Adding or Replacing a Module:

1. Remove power from the switch.
2. Unscrew the two thumb screws for the filler panel or module that you are replacing.
3. Using both hands pull on both thumb screws to slide the filler panel or module you are replacing.
4. Align the new module such that it slides on the rails and firmly push it into the unit.
5. Screw both thumb screws down till they are finger tight.
6. Reapply the power and configure the slots on the 7900 either through the web management interface or the serial management interface.
7. In order to verify the settings have been configured and saved correctly, you may want to view the Logical View page in the found in the web browser interface. The dynamic illustration displayed on the Logical View page must match the physical switch configuration respectively in order for the switch to function correctly. If not, please repeat the steps listed above.
8. Validation of the configuration and each physical cable segment may be obtained by using
9. N-ViewOPC Server software. The software is freely distributed on the Product CD and our web site (http://www.ntron.com/pdf/setup_nviewopc.zip). Once N-ViewOPC is installed, you should view the Ports Counter page view each connected port. You may find it helpful to copy [Alt]+[PrintScreen] the Port Counter information for each port and paste [Control]+[V] into a Windows document for further review. Please consult your N-View OPC Server manual for additional information.

NOTE: Modules should be installed in slot order (from left to right). So in a 2 slot configuration Slots A and B are populated. Empty slots must be covered with a 9000-FP to meet emission standards.

Replacing a CPU Module:

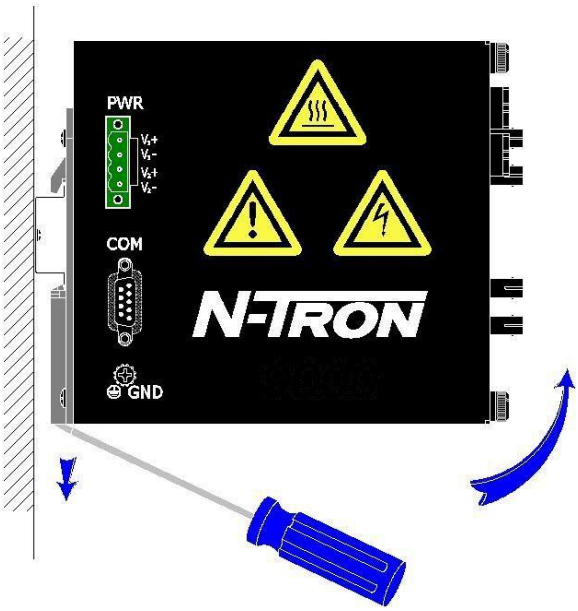
1. Remove power from the switch.
2. Unscrew the two thumb screws for the CPU module that you are replacing.
3. Using both hands pull on both thumb screws to slide the CPU module out of the chassis.
4. Align the new CPU Module such that it slides on the rails and firmly push it into the unit.
5. Screw both thumb screws down till they are finger tight.
6. Reapply the power to the switch.

NOTE: All configuration settings are saved to the NVRAM which is stored locally on the CPU Module. If you replace the CPU Module all settings will move with the CPU Module. You can save and download a custom configuration to a TFTP server. The switch's MAC Address and IP Address will also move with the CPU Module.

DIN-Rail Mounting

Install the unit on a standard 35mm Din-Rail. Recess the unit to allow at least 5” of horizontal clearance for fiber cable bend radius.

To mount the unit to the 35mm din-rail, place top edge of the bracket on the back of the unit against the din-rail at a 45° upward angle. Lower the bottom of the unit until it snaps into place.

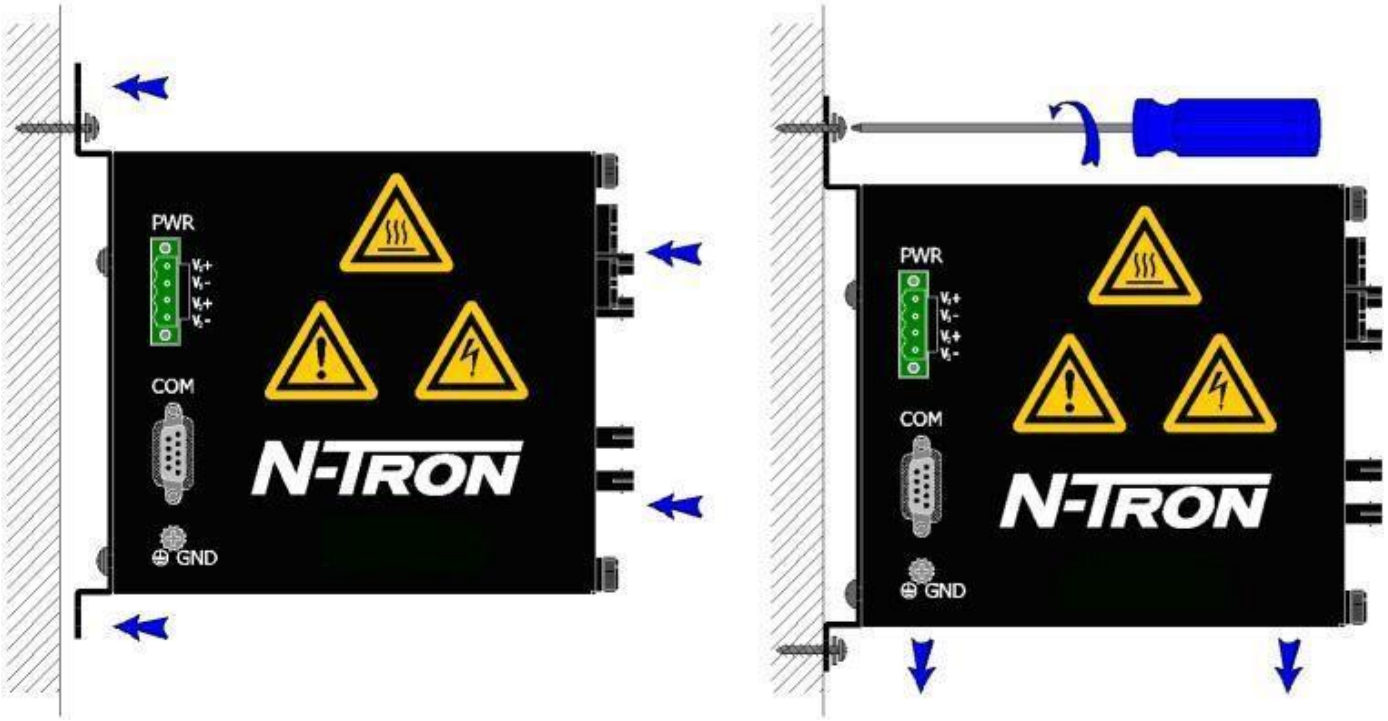


To remove the unit from the 35mm din-rail, place a flat head screwdriver into the release clip at the bottom of the unit, and push down on the clip until it disengages from the bottom of the unit from the din-rail. Lift the bottom of the unit up at an approximate 45° upward angle to completely remove the unit.

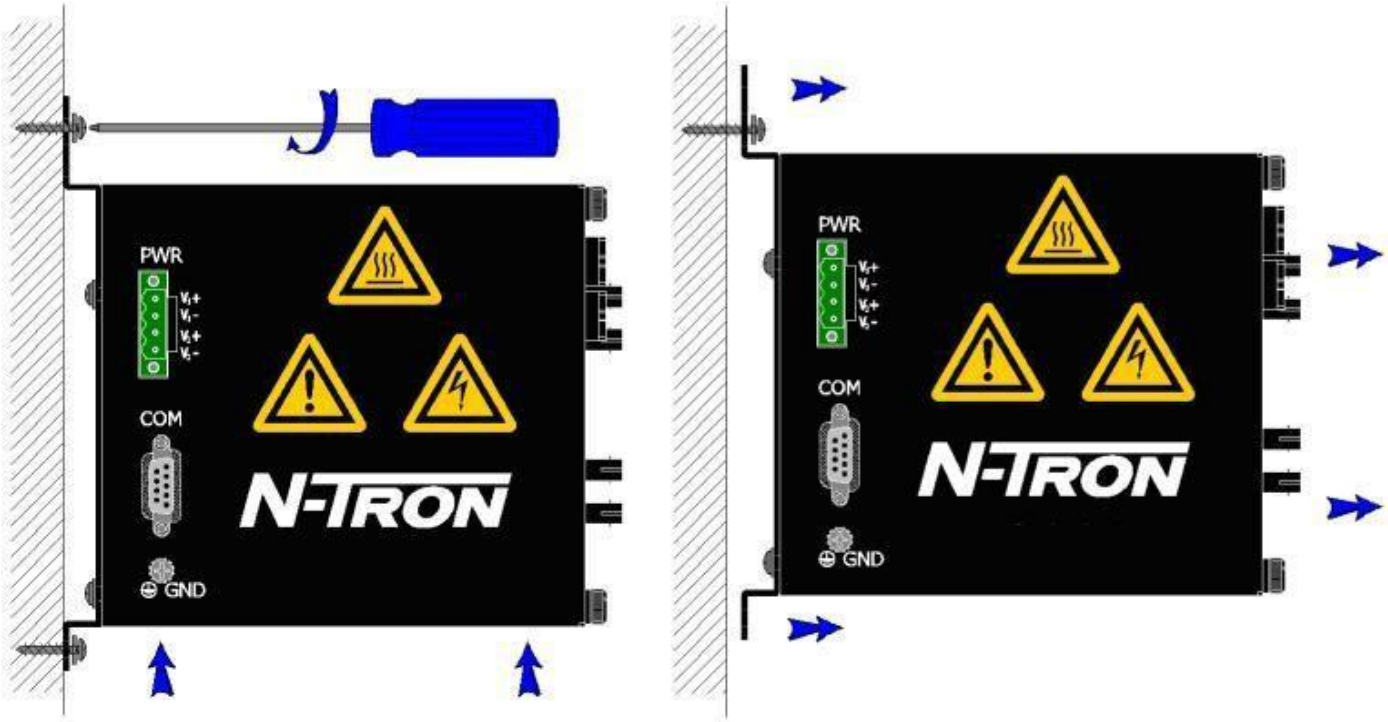
Most N-Tron™ products are designed to be mounted on industry standard 35mm DIN-Rail. However, DIN-Rail mounting may not be suitable for all applications. Our Universal Rack Mount Kit (P/N: URMK) may be used to mount the 7900 Series to standard 19" racks as an option.

Panel Mount Mounting

Install the unit directly on a wall or sturdy panel such as a bulkhead. Recess the unit to allow at least 5” of horizontal clearance for fiber cable bend radius.

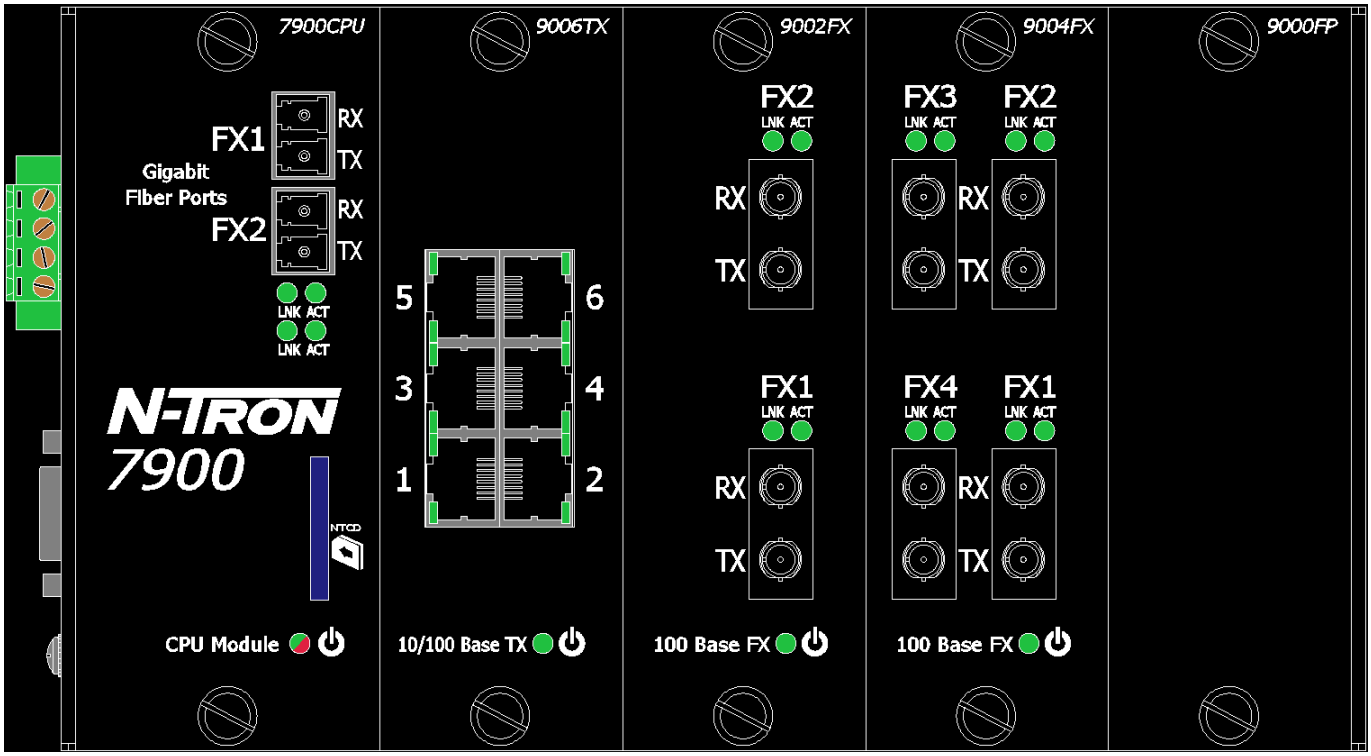


To bulkhead mount the unit, place top edge of the bracket on the back of the unit against two screws at a 45° upward angle. Lower the bottom of the unit until it is flush with the wall, and secure the bottom of the unit with two more screws.



To remove the unit from a wall, remove the bottom two screws that secure it to the wall and slide the unit up until the top two screws will fit through the larger holes on the unit. The switch should then freely come away from the wall.

FRONT PANEL:



From Left to Right:

Gigabit Ports	SFP Connections
RJ45 Ports	Auto sensing 10/100 Base-TX Connections
Fiber Ports	100 Base-FX Connections

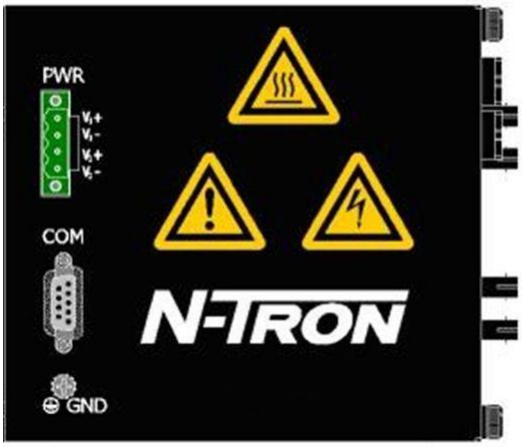
⏻ Green LED lights when Power is supplied to the module and there are no faults. This light is red when there is a fault.

NOTE: The RJ45 data port has two LED's located at the side of the connector. The bottom LED indicates LINK status, and the top LED indicates ACTIVITY.

LED's: The table below describes the operating modes:

LED	Color	Description
⏻	GREEN	Power is Applied and there are no faults.
	RED	Power is Applied and there is a fault.
	OFF	Power is OFF
LNK	GREEN	10/100/1000Mb Link between ports
	OFF	No Link between ports
ACT	GREEN	Data is active between ports
	OFF	Data is inactive between ports

APPLYING POWER (Side View)



- Unscrew & Remove the DC Voltage Input Plug from the Power Input Header
- Install the DC Power Cables into the Plug (observing polarity).
- Plug the Voltage Input Plug back into the Power Input Header.
- Tightening torque for the terminal block power plug is **0.5 Nm/0.368 Pound Foot.**
- Verify the Power LED stays ON (GREEN).

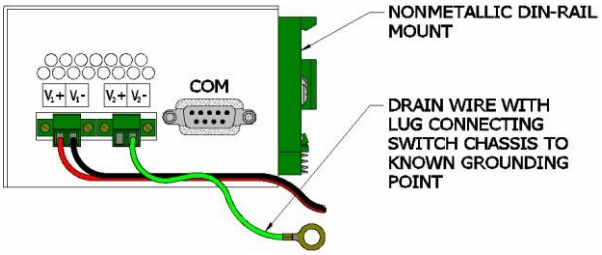
Note: Only 1 power supply must be connected to power for minimal operation. For redundant power operation, V_1 and V_2 inputs must be connected to separate DC Voltage sources. This device will draw current from both sources simultaneously. Use 16-28 gauge wire when connecting to the power supply.

Recommended 24V DC Power Supplies, similar to: N-Tron's P/N **NTPS-24-5**

- Input AC 100V…240V
- Output DC 24V…28V
- Output Current 5A
- Peak Current 7.5A for 4 sec.
- Power 120W
- Peak Power 180W (max 4 sec.)
- 35 mm DIN-Rail Mountable
- Dimensions: 1.57"W x 4.88"H x 4.61"D

N-TRON SWITCH GROUNDING TECHNIQUES

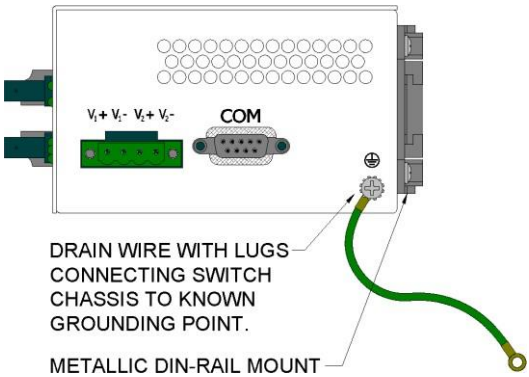
The grounding philosophy of any control system is an integral part of the design. N-Tron switches are designed to be grounded, but the user has been given the flexibility to float the switch when required. The best noise immunity and emissions (i.e. CE) are obtained when the N-Tron switch chassis is connected to earth ground via a drain wire. Some N-Tron switches have metal din-rail brackets that can ground the switch if the din-rail is grounded. In some cases, N-Tron switches with metal brackets can be supplied with optional plastic brackets if isolation is required.



Both V- legs of the power input connector are connected to chassis internally on the PCB. Connecting a drain wire to earth ground from one of the V- terminal plugs as shown here will ground the switch and the chassis. The power leads from the power source should be limited to 3 meters or less in length.

As an alternate, users can run a drain wire & lug from any of the Din- Rail screws or empty PEM nuts on the enclosure. When using an unused PEM nut to connect a ground lug via a machine screw, care should be taken to limit the penetration of the outer skin by less than 1/4 in. Failure to do so may cause irreversible damage to the internal components of the switch.

Note: Before applying power to the grounded switch, you must use a volt meter to verify there is no voltage difference between the power supply's negative output terminal and the switch chassis grounding point.

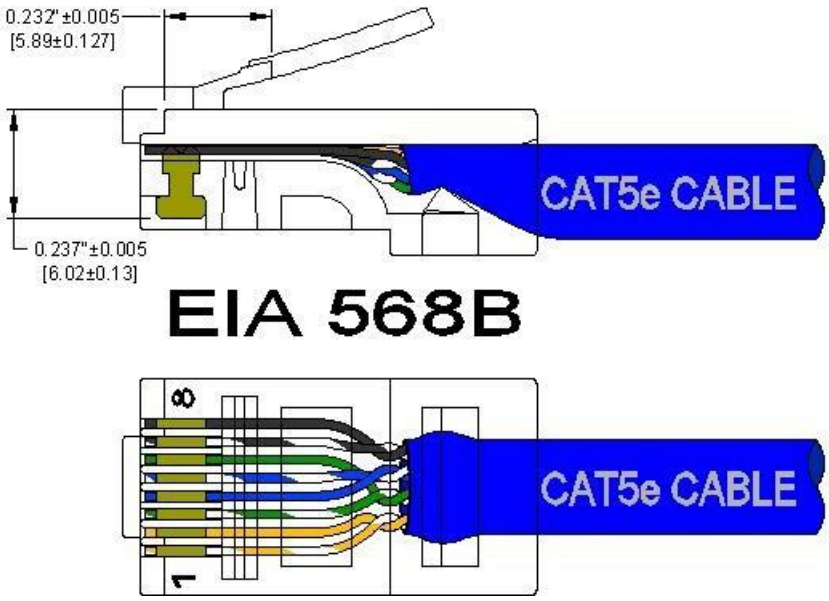


If the use of shielded cables is required, it is generally recommended to only connect the shield at one end to prevent ground loops and interfere with low level signals (i.e. thermocouples, RTD, etc.). Cat5e cables manufactured to EIA-568A or 568B specifications are required for use with N-Tron Switches.

In the event all Cat5e patch cable distances are small (i.e. All Ethernet devices are located the same local cabinet and/or referenced to the same earth ground), it is permissible to use fully shielded cables terminated to chassis ground at both ends in systems void of low level analog signals.

CAT5 CABLE SPECIFICATIONS

Please reference the illustration below for your Cat5 cable specifications:

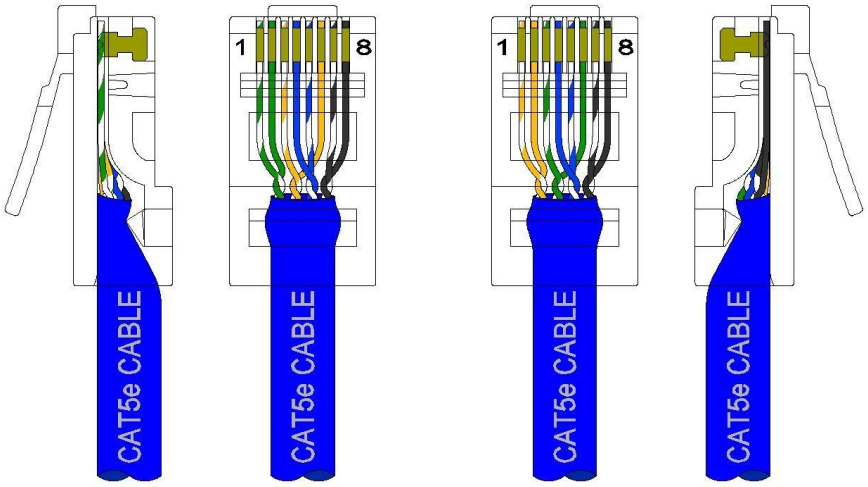


CONNECTING THE UNIT

For FX/FXE units, remove the dust cap from the fiber optic connectors and connect the fiber optic cables. The TX port on the FX/FXE models should be connected to the RX port of the far end station. The RX port on the FX/FXE versions should be connected to the TX port of the far end station.

For 10/100 Base-TX ports, plug a Category 5E twisted pair cable into the RJ45 connector. Connect the other end to the far end station. Verify that the LNK LED's are ON once the connection has been completed. To connect any other port to another Switch or Repeater, use a standard Category 5 straight through or crossover cable.

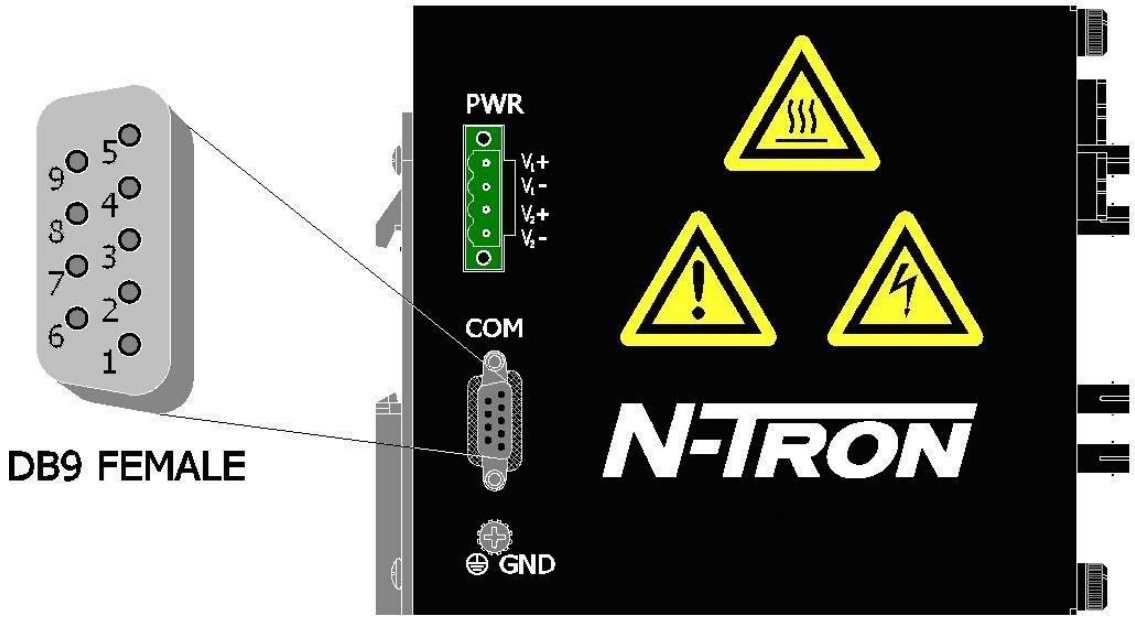
N-Tron recommends the use of pre-manufactured Cat5E cables to ensure the best performance. If this is not an option and users must terminate their own ends on the Cat5E cables; one of the two color coded standards shown to the right should be utilized. If a user does not follow one of these two color code standards then the performance and maximum cable distance will be reduced significantly, and may prevent the switch from establishing a link.



Warning: In absence of RSTP or Proprietary Ring control on the specific ports connected, creating a port to port connection on the same switch (i.e. loop) is an illegal operation and will created a broadcast storm which will crash the network!

SERIAL INTERFACE

The 7900 Series switches provide an EIA-232 interface accessed via a 9 pin female connector (labeled 'COM' on the unit). This is used to access the Command Line Interpreter (CLI). The pin-outs are shown below:



Serial Cable

Connect the serial COM port of your PC and the 7900 Series switch using a standard straight through cable. You will require a cable with a 9-pin or 25-pin sub-D female connector for the PC end, and a 9-pin male sub-D connector for the 7900 Series end.

The following table shows the pin-out and the connections for both types of cable:

PC Port	25-Pin Female	9-Pin Female	7900 series 9-Pin Male	
Signal Name	**Pin #**	**Pin #**	**Pin #**	**Signal Name**
TXD	2	3	3	RXD
RXD	3	2	2	TXD
GND	7	5	5	GND

Shielded cables and null modems are readily available from Radio Shack or a variety of computer stores.

HyperTerminal

The following configuration should be used in HyperTerminal:

Port Settings: 115200
Data Bits: 8
Parity: None
Stop bits: 1
Flow Control: None

Overview of Advanced Features

Mode of Operation

Each port on the switch can be configured into different modes of operation as shown below:

Copper Ports:	100Base Fiber Ports:	1000Base Copper/Fiber Ports:
- Half Duplex	- Full Duplex	- Full Duplex
- Full Duplex		
- Auto Negotiation		

Half Duplex

In half duplex mode, the CSMA/CD media access method is the means by which two or more stations share a common transmission medium. To transmit, a station waits (defers) for a quiet period on the medium (that is, no other station is transmitting) and then sends the intended message in bit-serial form. If, after initiating a transmission, the message collides with that of another station, then each transmitting station intentionally transmits for an additional predefined period to ensure propagation of the collision throughout the system. The station remains silent for a random amount of time (back-off) before attempting to transmit again.

Full Duplex

Full duplex operation allows simultaneous communication between a pair of stations using point-to-point media (dedicated channel). Full duplex operation does not require that transmitters defer, nor do they monitor or react to receive activity, as there is no contention for a shared medium in this mode.

Auto Negotiation

In Auto Negotiation mode, the port / hardware detects the mode of operation of the station that is connected to this port and sets its mode to match the mode of the station.

Port Mirroring

A Mirroring Port is a dedicated port that is configured to receive the copies of Ethernet frames that are being transmitted out and also being received in from any other port that is being monitored. 'Mirrored Data Only' can be selected and this selects for mirrored data only to be transmitted to the destination port, as opposed to mirrored data and whatever other data is otherwise destined for the destination Port.

Port Trunking

Port Trunking is the ability to group two network ports to increase the bandwidth between two machines (switch or any work station). This feature allows grouping of high-speed connectivity and provides redundant connection between switches, so that a trunk can act as a single link between the switches.

Quality of Service (QoS)

Quality of service (QoS) refers to resource reservation control mechanisms. Quality of service is the ability to provide different priority to different applications, users, or data flows. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay

sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.
Each of these three QOS methods below is included or not based on the settings on the relevant browser page:

1) Force High Priority (Port Based),
2) IEEE802.1p (Tagged QOS), or
3) DSCP (differentiated services code points) (RFC 2474).

When Force High Priority is enabled, the port based priority is included in the decision for all ports and all frames received on a port will use the default QOS priority for that port in the decision. For example, if it is desired to have ingress frames on a port egress to the highest priority transmit queue regardless of other factors, then enable Force High Priority and set the port's Default Port Priority to 7.

Virtual LAN

The switch provides support for setting up tagged Virtual LANs (Local Area Networks). A port may belong to any number of Virtual LANs. The VLAN membership of a device is determined by the VLAN(s) that have been defined for the port to which the device is connected. If a device should move from one port to another, it loses its current VLAN membership and inherits that of the new port it is connected to.

VLANs facilitate easy administration of logical groups of devices that can communicate as if they were on the same LAN. **Traffic between VLANs is restricted, unless the ports are explicitly configured as overlapping VLANs**. Switches forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.

A Default Virtual LAN (VID=1) exists to which a port, which is not a member of any other Virtual LAN, will belong. This allows the switch to operate as a ‘normal’ switch when it is used in a network. A port is automatically removed from the Default VLAN when it is reconfigured to belong to another Virtual LAN, because that is the most common operation. But, if desired, the port can be included in VLAN 1 by configuring VLAN 1 last.

If switch ports are configured to transmit and receive untagged frames, end devices are able to communicate throughout the LAN. Using Tagged VLANs, the switch has the ability to take non-tagged packets in some ports, add a VLAN tag to the packet and send it out tagged ports on the switch. The VLANs can also be configured to accept tagged packets in tagged ports, strip the tags off the packets, and send the packets back out other untagged ports. This allows a network administrator to set up the switch to support devices on the network that do not support VLAN Tagged packets. The administrator can also set up the ports to discard any packets that are tagged or to discard any packets that are untagged based on a hybrid VLAN of both tagged and untagged ports, and using the VLAN Ingress Filter on the switch.

For each switch port there is one and only one PVID (port VLAN ID) setting. If an incoming frame is untagged and untagged frames are being accepted, then that frame will inherit the tag of the PVID value for that port. Subsequent switch routing and treatment will be in accordance with that VLAN switch map. By configuring PVIDs properly and configuring for all frames to exit untagged, the switch can achieve a ‘port VLAN’ configuration in which all frames in and out can be untagged, thus not requiring external devices to be VLAN cognizant.

To understand how a VLAN configuration will perform, first look at the port on which the frame enters the switch, then the VLAN ID (if the frame is tagged) or the PVID (if the frame is untagged). The VLAN defined by the VID or PVID defines a VLAN group with a membership of ports. This membership determines whether a port is included or excluded as to frame egress from the switch.

The 7900 Series switch also has the ability to allow overlapping VLANs. Overlapping VLANs give the user the ability to have one or more ports share two or more VLAN groups. For more information and examples on how this could be implemented, please see the 'VLAN Configuration Examples' in this document, and/or our website's technical documents. Note that RSTP on overlapping VLANs is not supported and the system will automatically disable RSTP on all but the lowest VID VLANs that have overlapping ports.

Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol as specified in IEEE 802.1D-2004 is supported. One Spanning Tree per non-overlapping VLAN is supported. The Rapid Spanning Tree Protocol (RSTP) supersedes the Spanning Tree Protocol (STP) which was described in IEEE 802.1D-1998. The RSTP is used to configure a simply connected active network topology from the arbitrarily connected bridges of a bridged network. Bridges effectively connect just the LANs to which their forwarding ports are attached. Ports that are in a blocking state do not forward frames. The bridges in the network exchange sufficient information to automatically derive a spanning tree.

RSTP allows for much quicker learning of network topology changes than the older STP. RSTP supports new and improved features such as rapid transition to forwarding state. RSTP also sends out new BPDUs every hello time instead of just relaying them. RSTP interoperates with older STP switches by falling back to the older STP when the older BPDUs are detected on bridge ports. The user can also manually configure bridge ports to use the older STP when desired.

SNMP Traps

The 7900 Series switch supports up to 5 SNMP Trap Stations to which SNMP Traps will be sent. The switch supports five standard traps; Link Up, Link Down, Cold Start, Warm Start and Authentication Errors. SNMP Traps will be sent to all the trap stations configured on the switch when the corresponding trap is enabled.

IGMP Snooping

IGMP Snooping is enabled by default, and the switch is *Plug and Play* for IGMP. IGMP snooping provides intelligent network support for multicast applications. In particular, unneeded traffic is reduced. IGMP Snooping is configured via the web console and if enabled, operates dynamically upon each power up. Also, there can be manual only or manual and dynamic operation. Note that "static multicast group address" can be used whether IGMP Snooping is enabled or not.

IGMP Snooping will function dynamically without user intervention. If some of the devices in the LAN do not understand IGMP, then manual settings are provided to accommodate them. The Internet Group Management Protocol (IGMP) is a protocol that provides a way for a computer to report its multicast group membership to adjacent 'routers'. In this case N-Tron 7900 series switches provide *router-like functionality*. Multicasting allows one computer to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used to transmit only to an audience that has joined (and not left) a multicast group membership. IGMP version 2 is formally described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2236. IGMP version 1 is formally described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 1112. The 7900 series supports v1 and v2.

N-Ring

N-Ring is enabled by default, and the switch is *Plug and Play* for N-Ring except that initially one must enable an N-Ring enabled device to be the N-Ring Manager for a given N-Ring. Subsequently, N-Ring operates dynamically upon each power up. Using N-Tron's proprietary N-Ring technology offers expanded ring size capacity, detailed fault diagnostics, and a standard healing time of 30ms. The N-Ring Manager periodically checks the health of the N-Ring via health check packets. If the N-Ring Manager stops receiving the health check packets, it times out and converts the N-Ring to a backbone within 30ms. When using all N-Ring enabled switches in the ring, a detailed ring map and fault location chart is also provided on the N-Ring Manager's web browser. N-Ring status is also sent from the N-Ring Manager to the N-View OPC Server to identify the health status of the ring. Up to 250 N-Ring enabled switches can participate in one N-Ring topology. Switches that do not have N-Ring capability may be used in an N-Ring, however the ring map and fault location chart cannot be as detailed at these locations.

N-L ink

The purpose of N-Link is to provide a way to redundantly couple an N-Ring topology to one or more other topologies, usually other N-Ring topologies. Each N-Link configuration requires 4 switches: N-Link Master, N-Link Slave, N-Link Primary Coupler, and N-Link Standby Coupler. N-Link will monitor the link status of the Primary and Standby Coupler links. While the Primary Coupler link is healthy, it will forward network traffic and the Standby Coupler link will block network traffic. When a problem is detected on the Primary Coupler link, the Primary Coupler link will block network traffic and the Standby Coupler link will forward network traffic. While the N-Link Master and Slave are in communication via the Control link, only one Coupler link (Primary or Standby) will forward network traffic while the other Coupler link will block network traffic.

CIP

The CIP (Common Industrial Protocol) feature allows N-Tron switches to directly provide switch information and configuration access to Programmable Logic Controller (PLC) and Human Machine Interface (HMI) applications via a standardized communication protocol. For example, a PLC may be programmed to monitor port links or N-Ring status and cause a status indicator to turn red on an HMI if a port goes link down or if N-Ring has a fault. CIP is formally described in ODVA Publication Number PUB00001 (Volume 1: Common Industrial Protocol (CIP™)), and Publication Number: PUB00002 (Volume 2: EtherNet/IP Adaptation of CIP). N-Tron provides EDS and ICO files. N-TRON_CIP_Tags.pdf is for a particular environment, but reveals the tags available.

DHCP

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. DHCP is controlled by RFC 2131. The N-Tron DHCP Switch can be configured to be a DHCP Client. Alternately the N-Tron DHCP switch can be configured to be a DHCP Server, a DHCP Relay Agent, or both.

For more detailed information on N-Tron DHCP features, reference: http://www.n-tron.com/tech_docs.php. Under 'White papers', see: "Using DHCP to Minimize Equipment Setup Time". Under 'Installation Guides and User Manuals' see "DHCP Technical Instructions for 708 / 716/ 7018 / 7506 Series".

DHCP Client

The switch will automatically obtain an IP assignment from a DHCP Server, or optionally Fallback to a configured IP assignment if unable to get an IP assignment from a DHCP server. Communication between the client and server can optionally go through a DHCP Relay Agent.

DHCP Relay Agent

DHCP Relay Agent (Option 82) allows communication between the client and server to cross subnet and VLAN boundaries. It also allows for a device on a specific port to receive a specific IP address and if the device is replaced, the replacement receives the same IP address as the original device.

DHCP Server

DHCP Server allows DHCP Client devices to automatically obtain an IP assignment. IP assignments can be set up as a dynamic range of IP addresses available to any client device; or specific IP addresses based on the clients MAC address, Client ID (Option 61), or Relay Agent connection (Option 82).

LLDP

Link Layer Discovery Protocol (LLDP) is a Layer 2 discovery protocol allowing devices attached to an IEEE802 LAN to advertise their major capabilities to other devices and to store information they discover in a MIB that can be accessed through SNMP. LLDP is formally described in IEEE Standard - 802.1AB.

Port Security—MAC Address Based

The Port Security feature restricts access to the switch by only accepting dynamically learned MAC addresses and manually entered MAC addresses as authorized. Dynamically learned MAC addresses are those that the switch detects on any port while in ‘Learning’ mode. A manually entered MAC address must designate the ports that the address is authorized on. A non-authorized MAC address will be discarded and will be shown on the intruder log. Locking can be selected or not port by port.

XML Settings Download

XML settings can be downloaded to a switch to achieve some switch configurations. XML settings cover a subset of the settings available through the web browser. Reference *Appendix A. XML Settings File Example* for the complete set of configurations that can be done using XML Settings Download. There are several top level configuration sections and each of these sections is optional. Some sections have a ‘keep or delete’ choice such that one can load only those in the XML file deleting the pre-existing of those particular settings or one can add the settings in the XML file to the already existing settings. The example also shows field character limits, and provides other guidance.

Rate Limiting

Some systems generate a large amount of broadcast or multicast traffic occasionally. When it happens, the entire network may experience failures that persist until there is manual intervention. One way to address this problem is to control the broadcast or multicast traffic to remain below a user configured maximum limit. The most effective limit may be best obtained in test. Thus the user is provided with the capability to ‘tune’ the limit by switch port. These are ingress filters. The percentage values are repeatable to the purpose and rise or fall as compared to each other, but are not meant to be as exact as in a piece of calibrated test equipment.

TROUBLESHOOTING

1. Make sure the ⏻ (Power LED) is ON.
2. Make sure you are supplying sufficient current for the version chosen. Note: The Inrush current will exceed the steady state current by ~ 2X.
3. Verify that Link LED's are ON for connected ports.
4. Verify cabling used between stations.
5. Verify that cabling is Category 5E or greater for 100Mbit Operation.

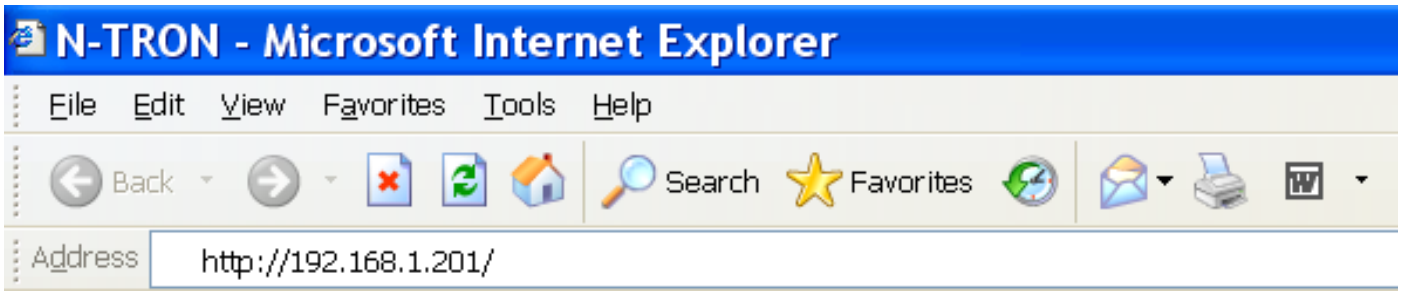
FCC STATEMENT

This product complies with Part 15 of the FCC Rules for a Class A device.
Operation is subject to the following two conditions:
(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Web Software Configuration

Web Management

Enter the switch's IP address in any web browser and login to the web management feature of the 7900 Series.

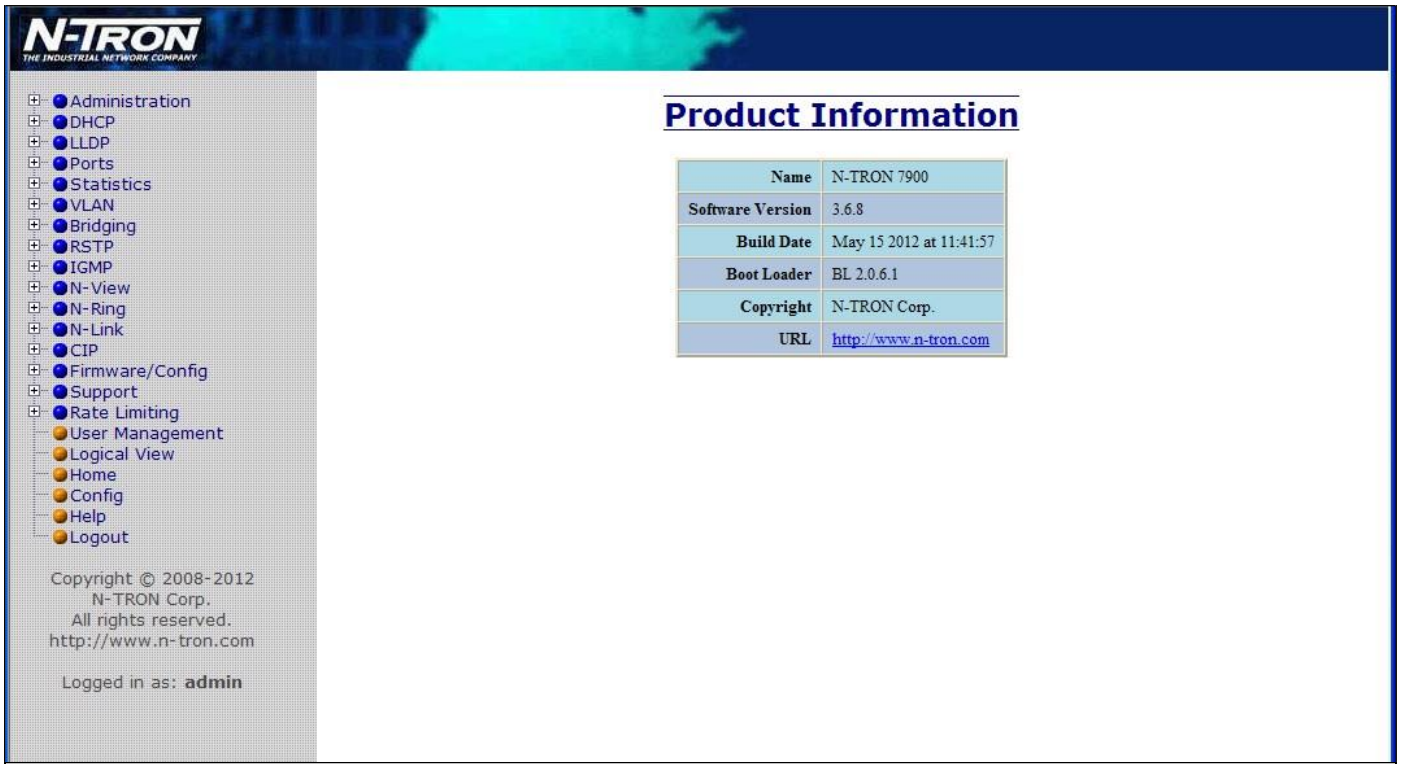


Default:

User Name: ***admin***
Password: ***admin***

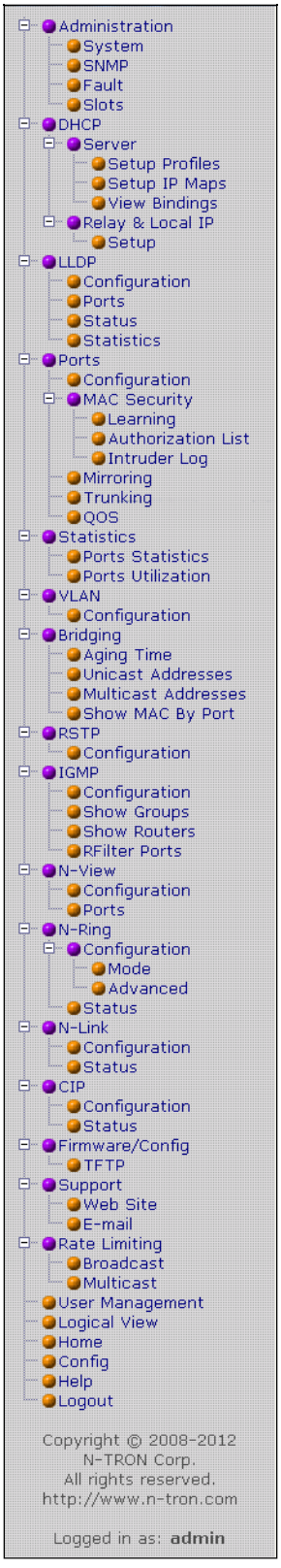
Web Management - Home

When the administrator first logs onto a 7900 Series switch the default home page will be displayed. On the left hand side of the screen there is a list of configurable settings that the 7900 Series switch will support. This section of the manual will go through each and every choice listed on the left hand side of the screen and explain how to configure those settings. In the center of the main home page the administrator can see some basic information like what firmware revision the switch is running. The firmware can be upgraded at a later time in the field using TFTP.



Web Management – Menu Structure

To the left, there is a menu which is shown fully opened below. The pages opened by each of the individual selections are described in the rest of this section. The use of each of these pages is also described in this section. In most of the descriptions, only the right side of the page is shown.



Administration – System

The System tab under the Administration category, lists various information about the switch:

When the IP Configuration is in either DHCP or Static Mode:

IP Configuration
Method used to obtain an IP Address, Subnet Mask and Gateway Address

IP Address
Contains the current IP Address of the device.

Subnet Mask
Contains the current Subnet Mask of the device.

Gateway
Contains the current Default Gateway of the device.

MAC Address
MAC Address of the device.

System Up Time
This parameter represents the total time count. This time has elapsed since the switch was turned ON or RESET.

Name
It shows the name of the product, which allows alphanumeric and special characters (#, _, -) only.

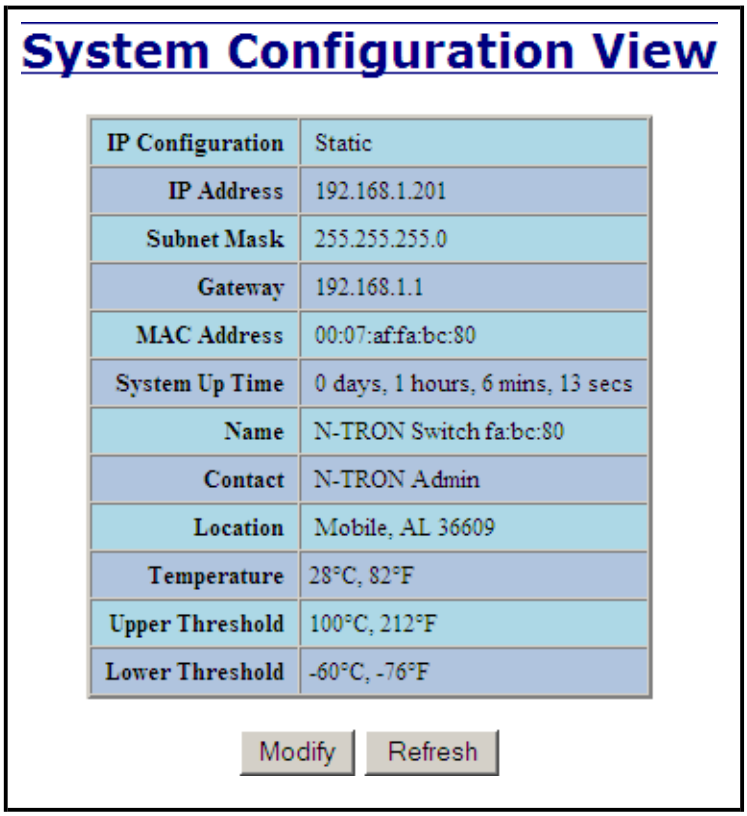
Contact
The person to contact for system issues, which should be someone within your organization.

Location
The physical location of the switch.

Temperature:
The calculated ambient temperature near the switch. This calculation is only valid after a warm-up period. This reading is not meant to be as exact as a calibrated temperature probe, especially if there is moving air around the switch.

Upper Threshold:
The highest temperature for the switch without causing a fault to occur. The threshold is specified as an integer in C degrees. The range is from -60°C to 100°C, and the default is product dependent.

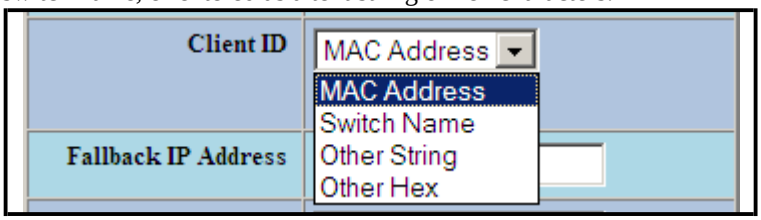
Lower Threshold:
The lowest temperature for the switch without causing a fault to occur. The threshold is specified as an integer in C degrees. The range is from -60°C to 100°C, and the default is product dependent.



When the IP Configuration is in DHCP Mode the following information is added:

Client ID

Option used by DHCP clients to specify their unique identifier. The identifier may be the MAC address, switch name, or entered as a text string or hex characters.



Fallback IP Address

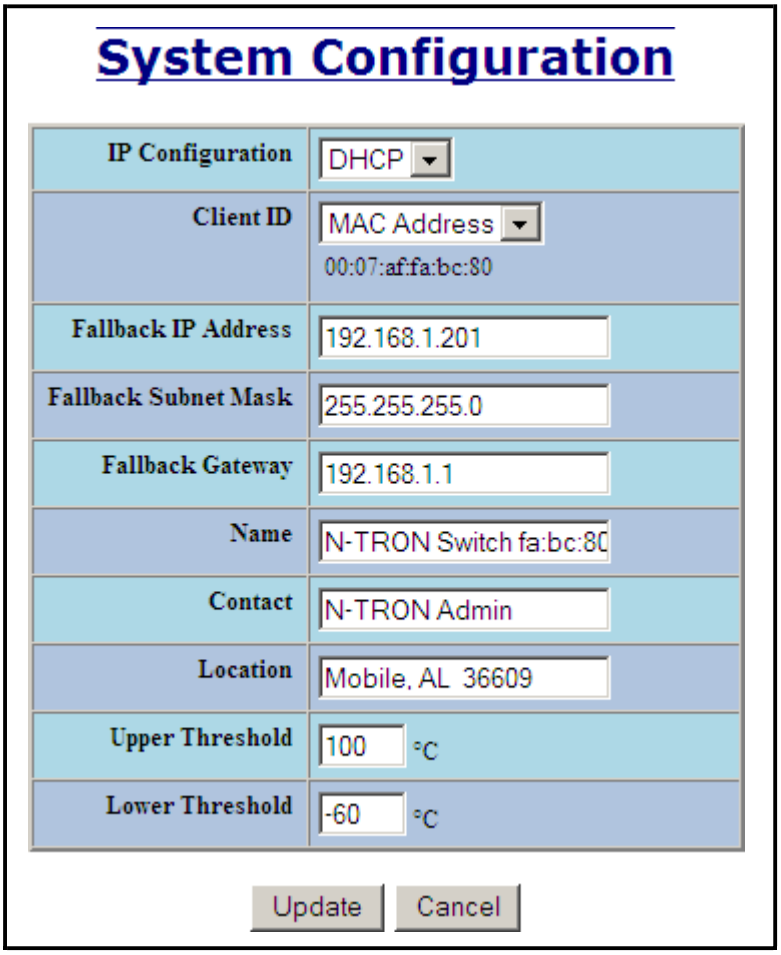
Contains the configured Fallback IP Address of the device.

Fallback Subnet Mask

Contains the configured Fallback Subnet Mask of the device.

Fallback Gateway

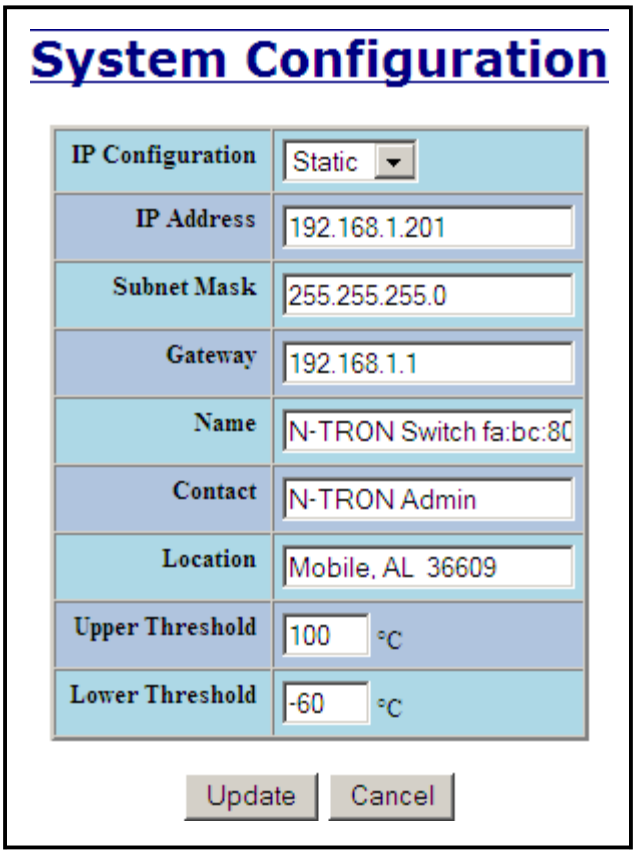
Contains the configured Fallback Gateway of the device.



Administration – System, Continued…

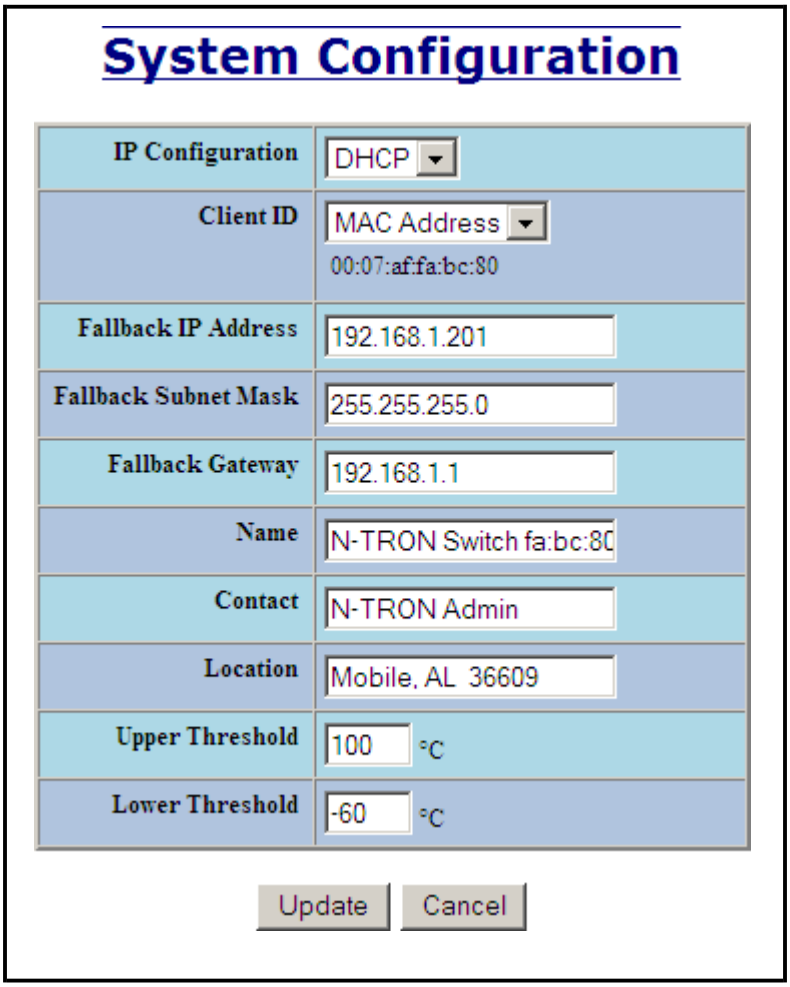
By selecting the Modify button, you will be able to change the switch's IP Configuration, Client ID, IP Address, Subnet Mask, Gateway, Name, Contact information, and the Location of the switch through the web management features, depending on the IP Configuration. It is recommended to change the TCP/IP information through the Command Line Interface (CLI) initially, but it defaults to the following:

IP Configuration – Static
IP Address – 192.168.1.201
Subnet Mask – 255.255.255.0
Gateway – 192.168.1.1



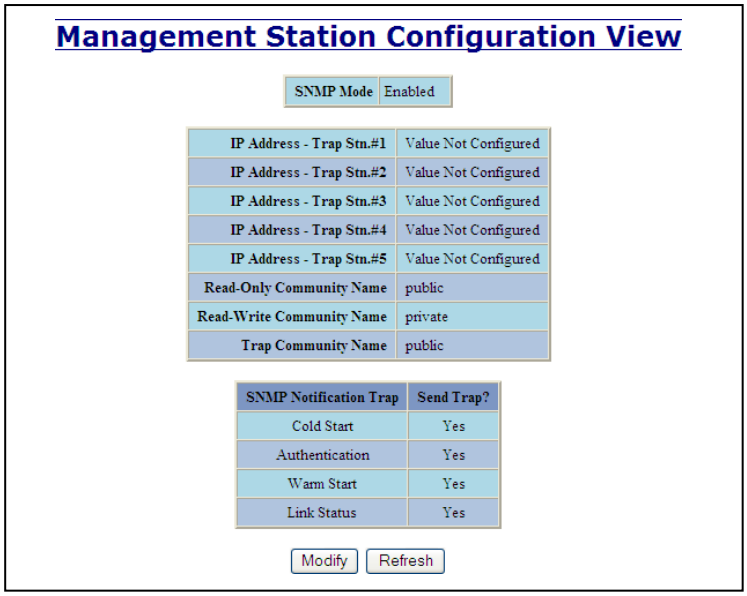
Administration – System, Continued…

If the IP Configuration mode is set to DHCP and the Fallback IP address is changed from the default IP address, then the switch will use the Fallback addresses if the IP configuration isn't received from a DHCP server in 2 minutes after initial boot. If Fallback address is used, DHCP Client will stop sending requests. If the IP Configuration is received from a DHCP server, it will never fallback, even if the lease is lost.

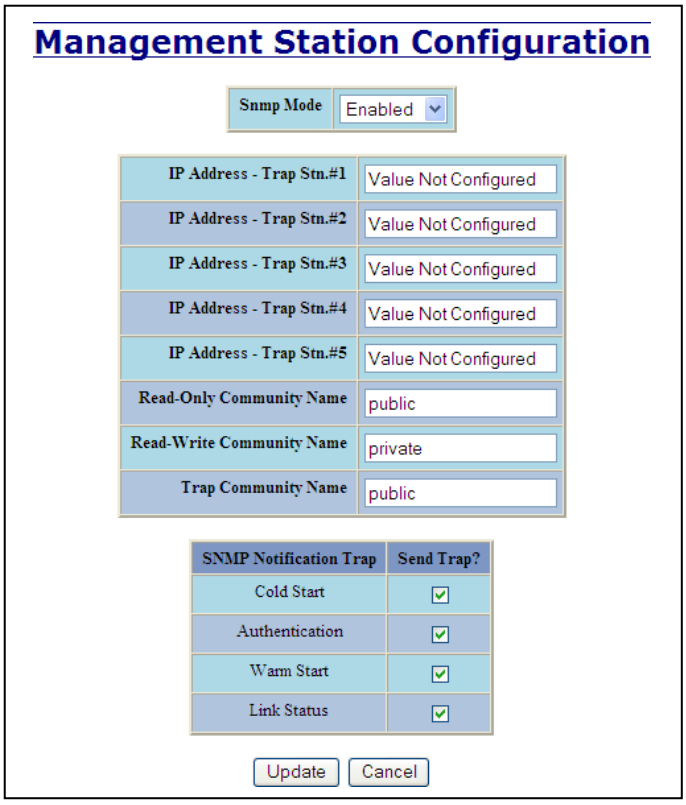


Administration – SNMP

The SNMP tab under the Administration category allows SNMP to be disabled or enabled, and shows a list of IP Addresses that act as SNMP Traps. The Read-Only, Read-Write, and Trap Community Names are also shown here.

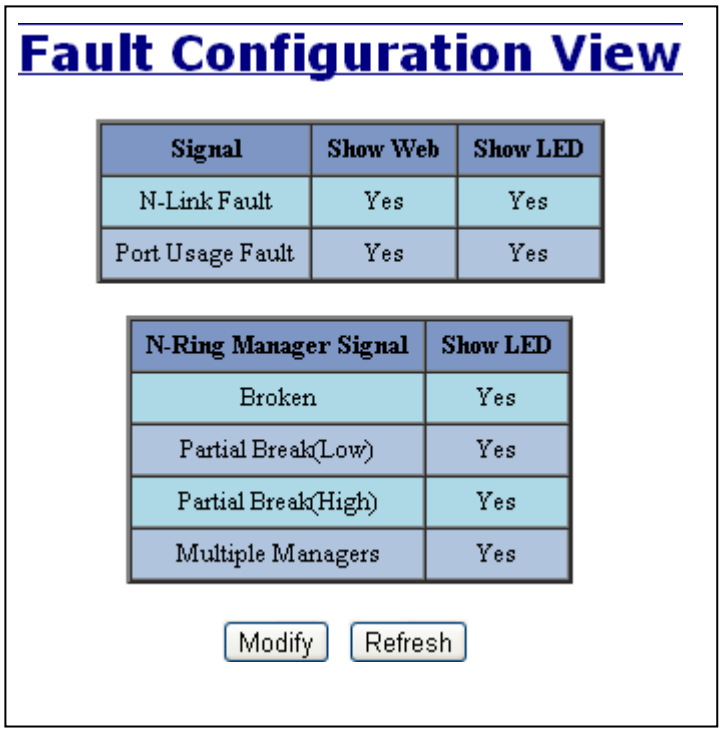


By selecting the modify button you will be able to change any of the fields listed. This allows the user to set an IP address for an SNMP Trap or change the Community Names. Systems that are listed as an SNMP Trap will be sent basic networking changes made to the switch such as ports going down or being linked. To restore a Trap to "Value Not Configured", enter '0.0.0.0'.



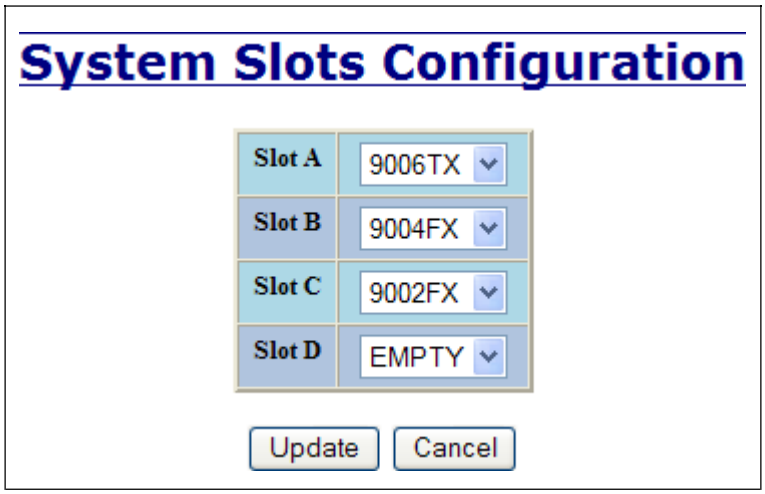
Administration – Fault

The Fault tab under the Administration category provides configurable selections indicating the way to notify when an N-Ring Manager, N-Link fault, or Port Usage Fault occurs. The notification can be indicated by the options: Show Web or Show LED. N-Ring Manager signal faults consist of: Broken, Partial Break (Low), Partial Break (High), and Multiple Managers. N-Link Faults are reported by the N-Link Master and by the N-Link Slave. Port Usage Fault, if enabled, triggers when actual usage is below the Usage Alarm Low setting, or above the Usage Alarm High setting (see Port Configuration View and Port Utilization View).

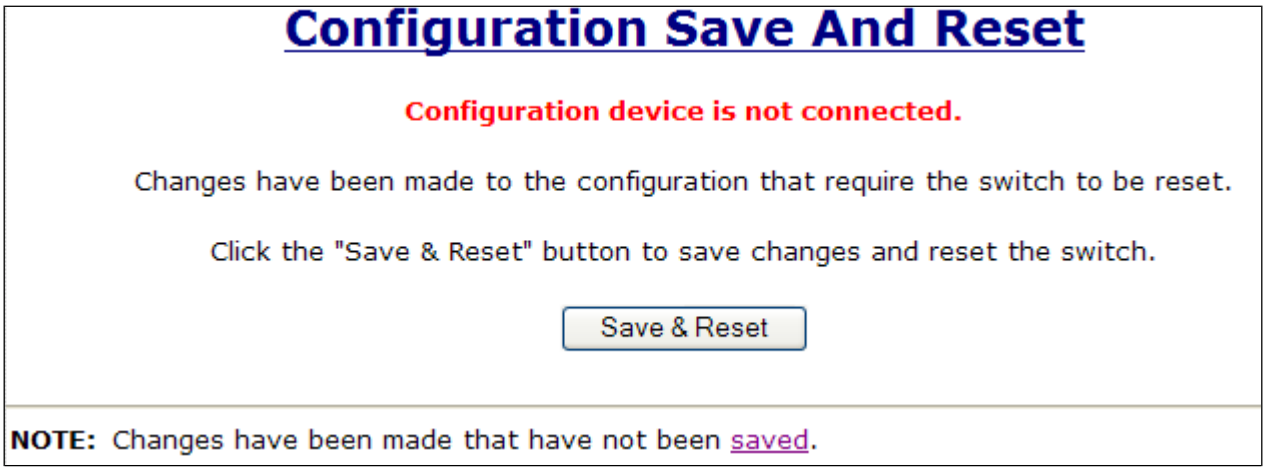


Administration – Slots

The Slots tab under the administration category allows users to change the configuration of the slots that are populated in the 7900 Back Plane. The switch may not operate correctly if the slots are not configured properly. You must click Update if you wish to keep the changes.



Following the Update button, the user may be prompted to Save and Restart the switch in order for changes to take effect. The switch will save the running configuration into the NVRAM and then cycle power automatically. Once the switch comes back online the settings will be updated.



DHCP – Server – Setup Profiles

The Setup Profiles tab under the DHCP/Server category lists the following information about the current state of the server and the existing network profiles:

Server Enabled
Indicates whether the DHCP server is active.

Allow Broadcast
Indicates whether the DHCP server will process broadcast messages.

Delay Broadcast (Ms)
The amount of time the DHCP server will delay processing a broadcast message.

Server ID
Descriptive name of the DHCP server.

Profile Name
Descriptive name of the network profile.

Address Pool
Range of IP addresses which the profile can use.

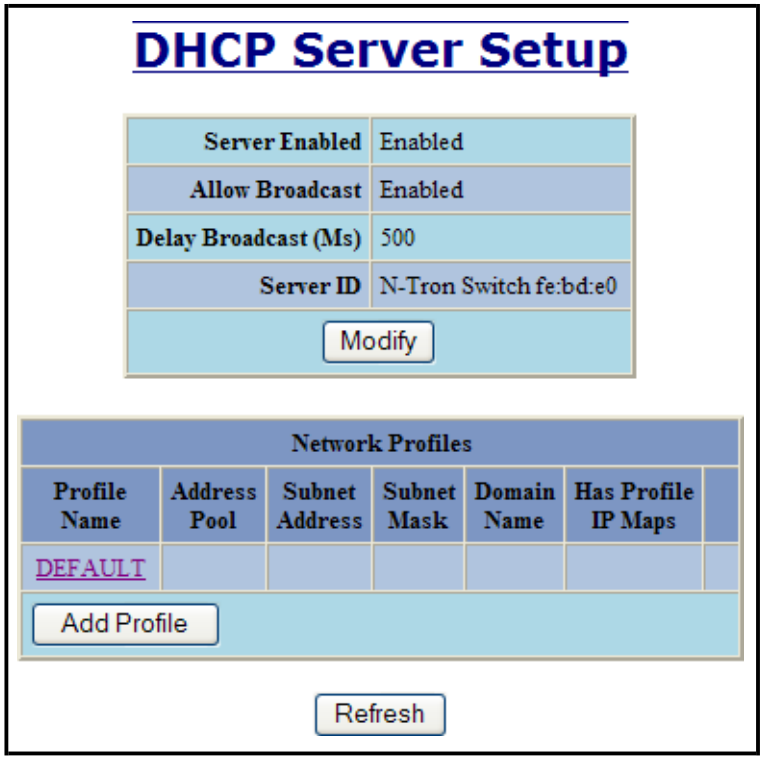
Subnet Address
The most restrictive subnet address calculated from the address pool range.

Subnet Mask
The most restrictive subnet mask calculated from the address pool range.

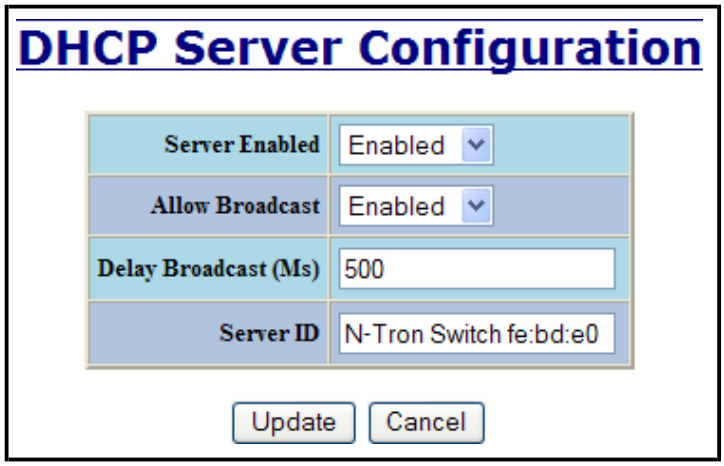
Domain Name
The domain name to be presented to the client.

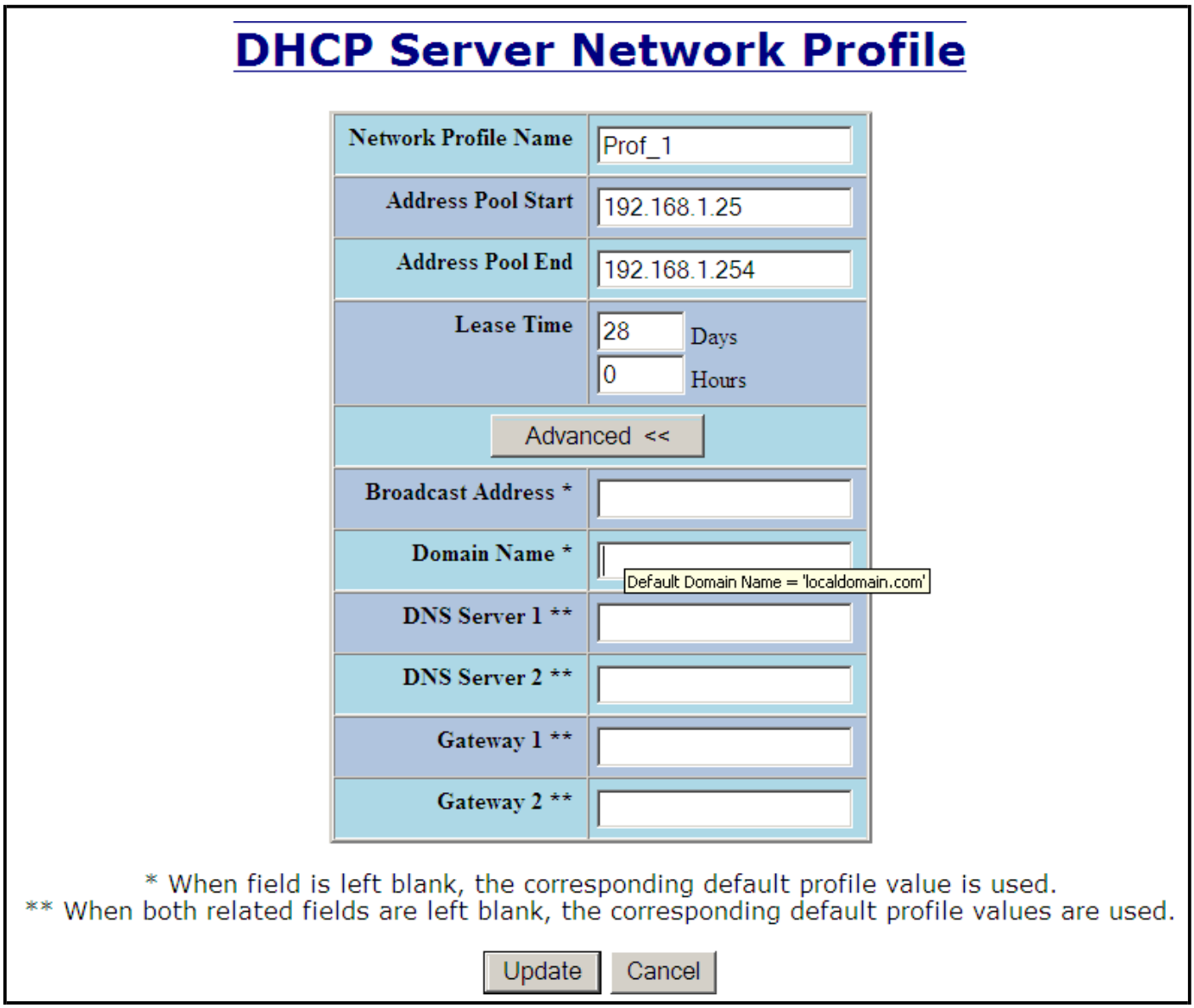
Has Profile IP Maps
Indicates whether the profile has IP maps associated with it.

Delete
Deletes the profile along with all IP maps and bindings associated with it. The Default profile cannot be deleted.



DHCP – Server – Setup Profiles, Continued…

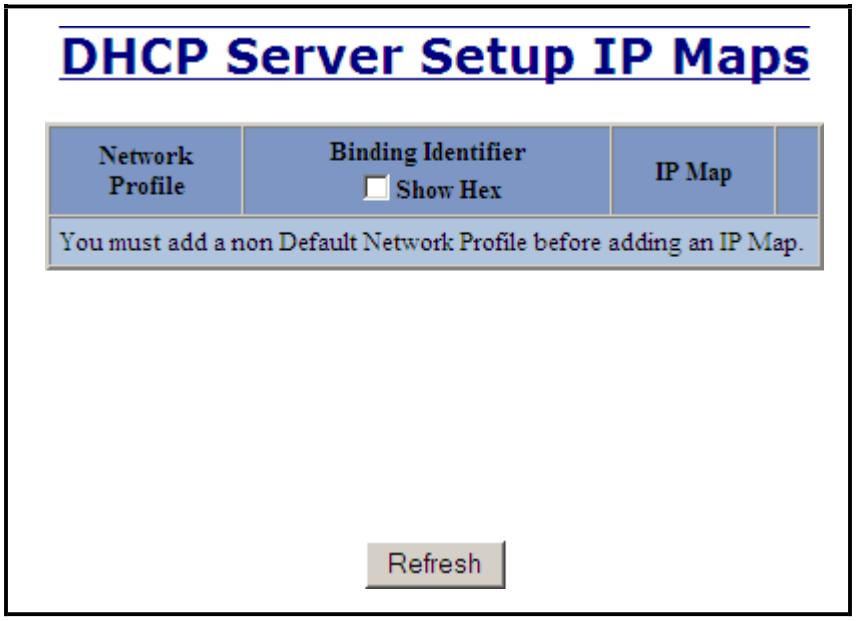




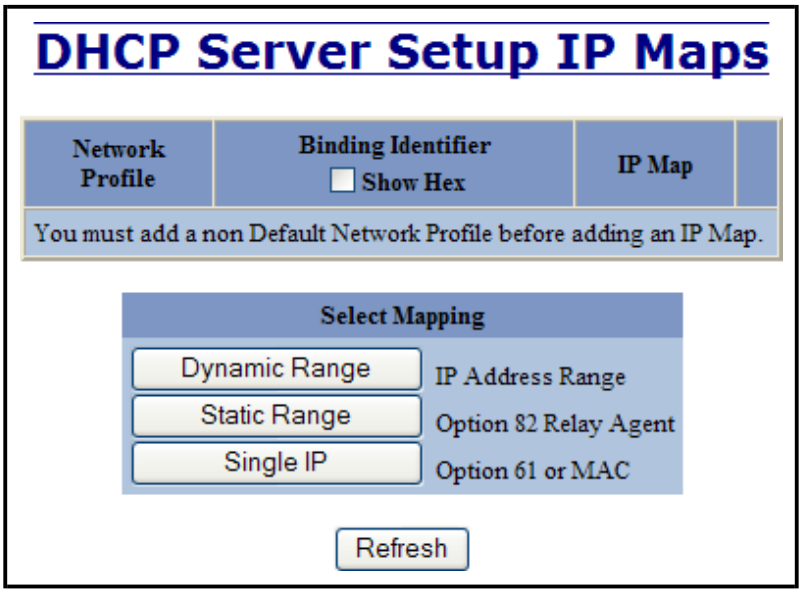
DHCP – Server – Setup IP Maps

The Setup IP Maps tab provides the way to create IP mappings with an existing network profile. There are three types of mappings that can be created: Dynamic Range, Static Range, and Single IP.

Before a non-default Network profile has been configured:



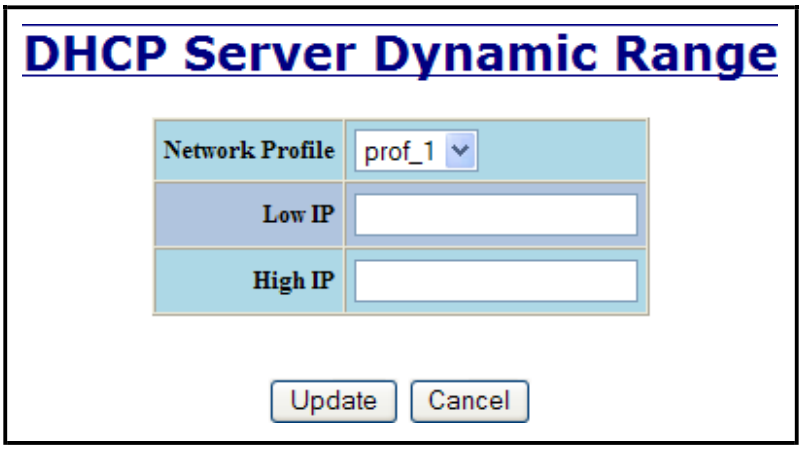
After a non-default Network profile has been configured:



DHCP – Server – Setup IP Maps, Continued…

The Dynamic Range type of mapping is used to create a range of dynamic IP addresses for requesting clients. The following information is required:

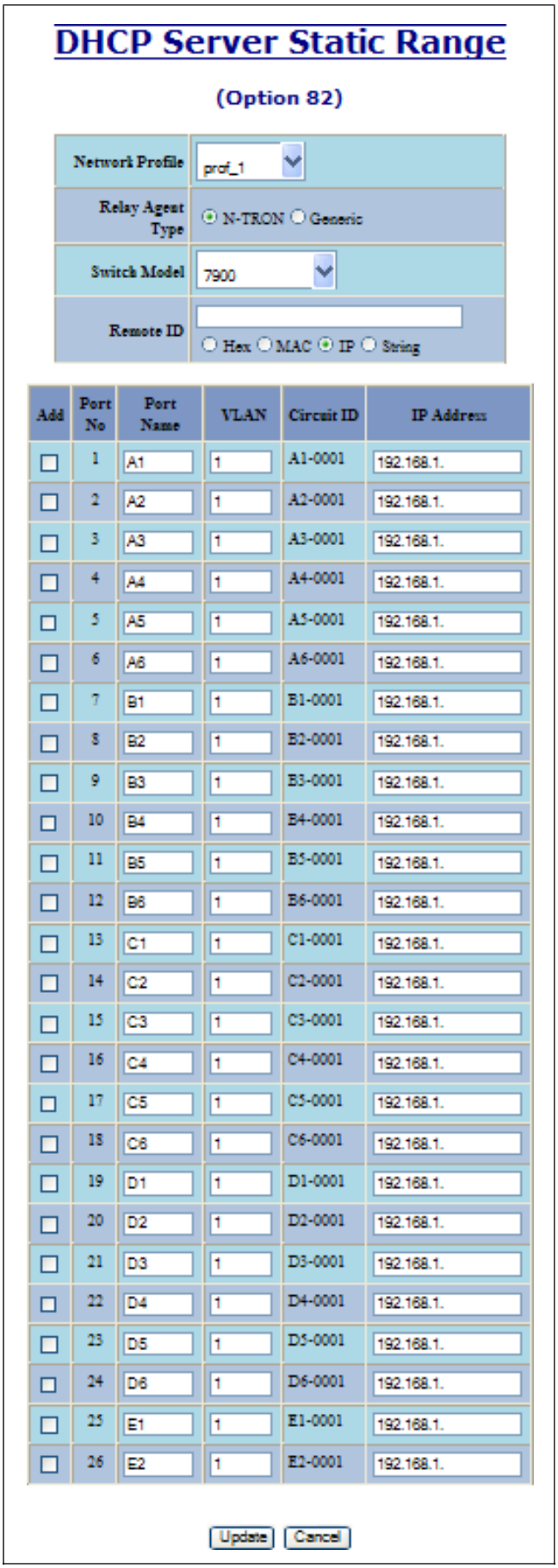
Network Profile
An existing network profile to which the IP map applies.
Low IP
The starting IP address of a range.
High IP
The ending IP address of a range.



The Static Range type of mapping is used to create a range of static IP addresses dedicated to specific ports on a relay agent switch. There are two different data entry formats available according to whether the relay agent type is for an N-TRON or for a generic switch.

To create a range of static IP addresses on an N-Tron relay agent switch:

Network Profile
An existing network profile to which the IP map applies.
Relay Agent Type
Should be set to N-TRON.
Switch Model
List of N-TRON models that support this feature.
Remote ID
A unique identifier that designates the N-TRON relay agent switch.
Add
Checkbox used to add an IP map for the corresponding port.
Port No
The actual port number.
Port Name
Descriptive name of the port.
VLAN
VLAN ID that the port is a member of.
Circuit ID
Auto-generated string based on the port name and VLAN ID.
IP Address
IP address to assign to the IP map.



DHCP Server Static Range

(Option 82)

Network Profile	prof_1
Relay Agent Type	◉ N-TRON ○ Generic
Switch Model	7900
Remote ID	○ Hex ○ MAC ◉ IP ○ String

Add	Port No	Port Name	VLAN	Circuit ID	IP Address
☐	1	A1	1	A1-0001	192.168.1.
☐	2	A2	1	A2-0001	192.168.1.
☐	3	A3	1	A3-0001	192.168.1.
☐	4	A4	1	A4-0001	192.168.1.
☐	5	A5	1	A5-0001	192.168.1.
☐	6	A6	1	A6-0001	192.168.1.
☐	7	B1	1	B1-0001	192.168.1.
☐	8	B2	1	B2-0001	192.168.1.
☐	9	B3	1	B3-0001	192.168.1.
☐	10	B4	1	B4-0001	192.168.1.
☐	11	B5	1	B5-0001	192.168.1.
☐	12	B6	1	B6-0001	192.168.1.
☐	13	C1	1	C1-0001	192.168.1.
☐	14	C2	1	C2-0001	192.168.1.
☐	15	C3	1	C3-0001	192.168.1.
☐	16	C4	1	C4-0001	192.168.1.
☐	17	C5	1	C5-0001	192.168.1.
☐	18	C6	1	C6-0001	192.168.1.
☐	19	D1	1	D1-0001	192.168.1.
☐	20	D2	1	D2-0001	192.168.1.
☐	21	D3	1	D3-0001	192.168.1.
☐	22	D4	1	D4-0001	192.168.1.
☐	23	D5	1	D5-0001	192.168.1.
☐	24	D6	1	D6-0001	192.168.1.
☐	25	E1	1	E1-0001	192.168.1.
☐	26	E2	1	E2-0001	192.168.1.

Update Cancel

DHCP – Server – Setup IP Maps, Continued…

To create a range of static IP addresses on a generic relay agent switch:

Network Profile
An existing network profile to which the IP map applies.

Relay Agent Type
Should be set to Generic.

Port Count
The number of ports on the particular relay agent switch.

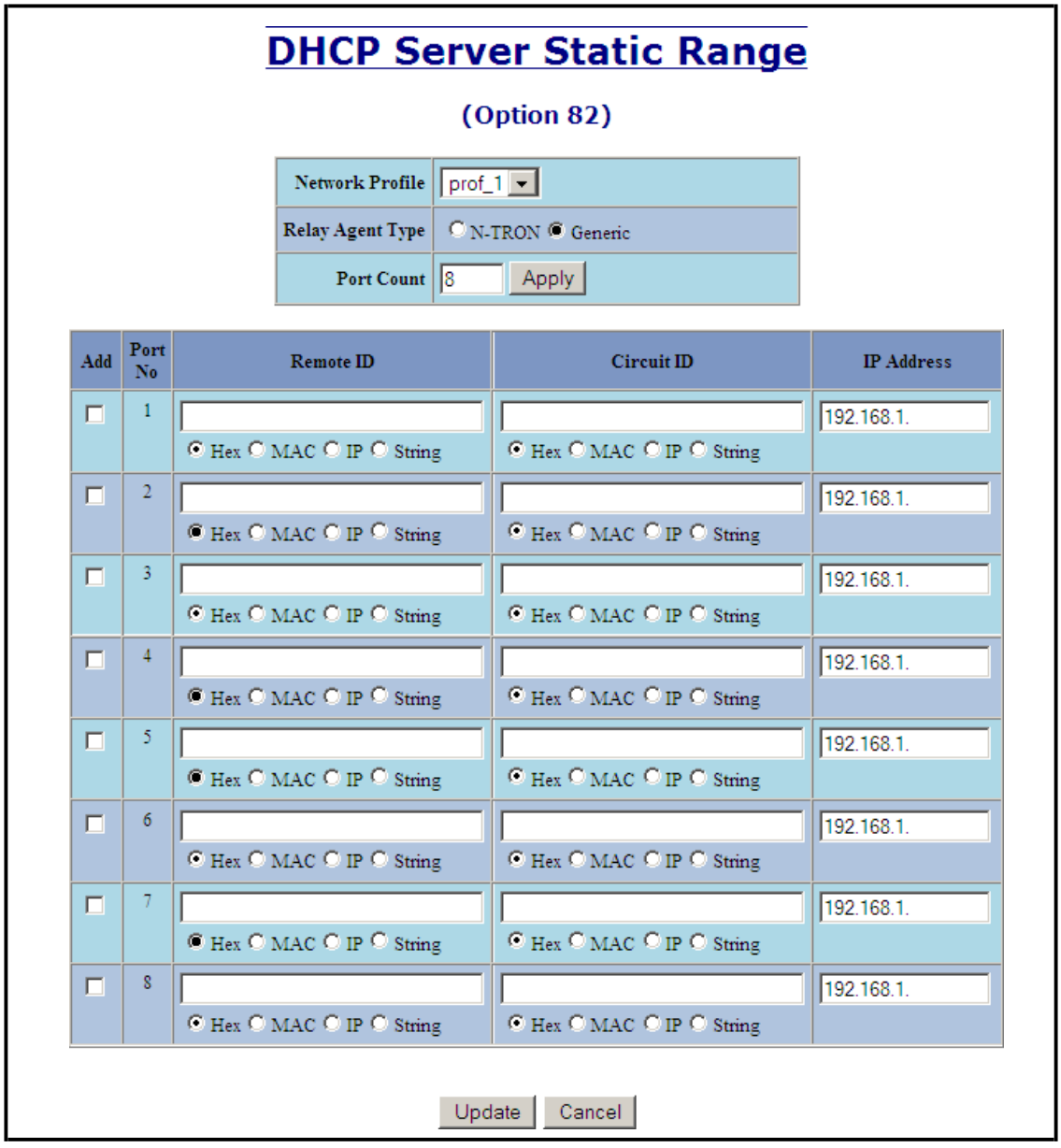
Add
Checkbox used to add an IP map for the corresponding port.

Port No
The actual port number.

Remote ID
The identifier that corresponds to an Option 82 Remote ID sub-option used by the particular relay agent switch.

Circuit ID
The identifier that corresponds to an Option 82 Circuit ID sub-option used by the particular relay agent switch.

IP Address
IP address to assign to the IP map.



DHCP – Server – Setup IP Maps, Continued…

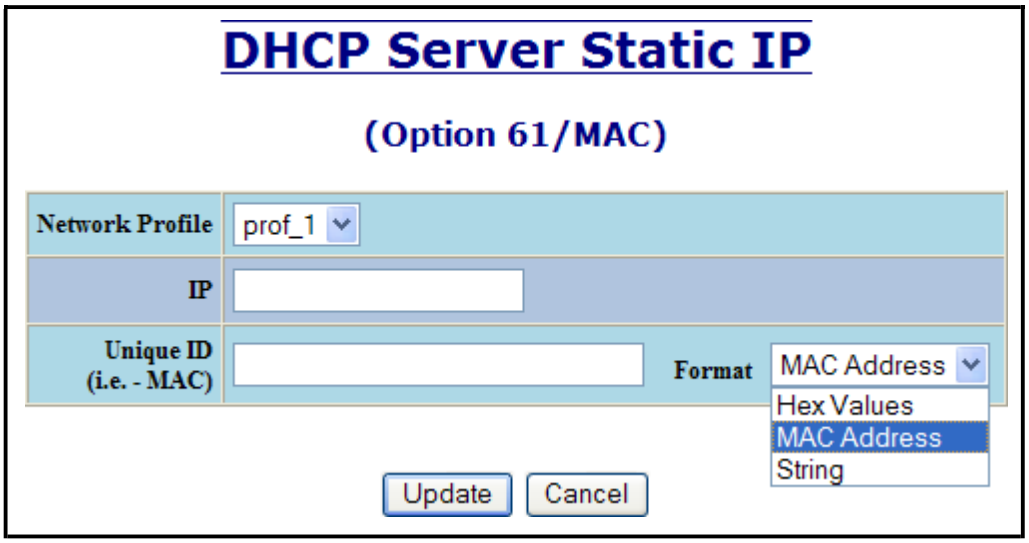
The Single IP type of mapping is used to create a static IP address for an individual client. The following information is required:

Network Profile
An existing network profile to which the IP map applies.

IP
The static IP address to offer to a client.

Unique ID
The unique identifier that must match either the client identifier (Option 61) or the client's hardware address (MAC).

Format
Designates how the Unique ID is interpreted.



DHCP – Server – View Bindings

The View Bindings tab lists the bindings of physical devices to IP addresses that are in use or offered:

Network Profile
The profile applied to the binding entry.

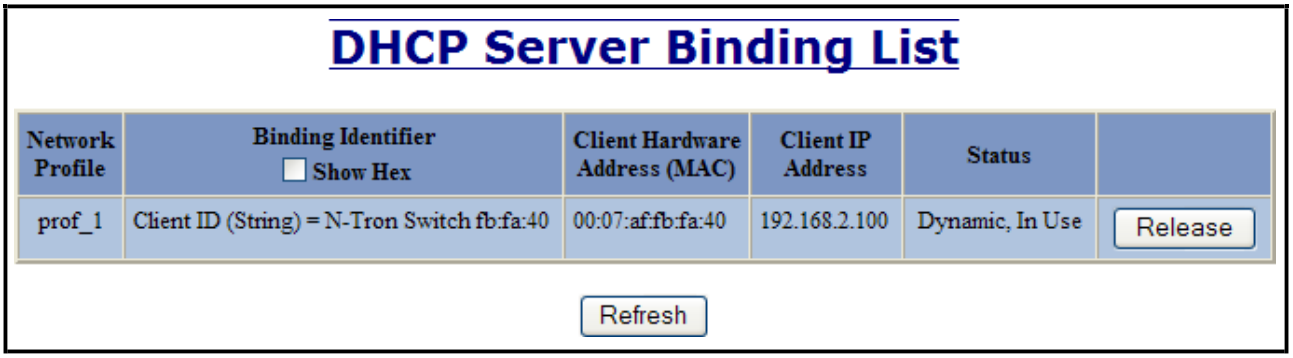
Binding Identifier
The client associated with the binding entry.

Client Hardware Address (MAC)
The client's MAC address.

Client IP Address
The actual IP address assigned to the binding entry.

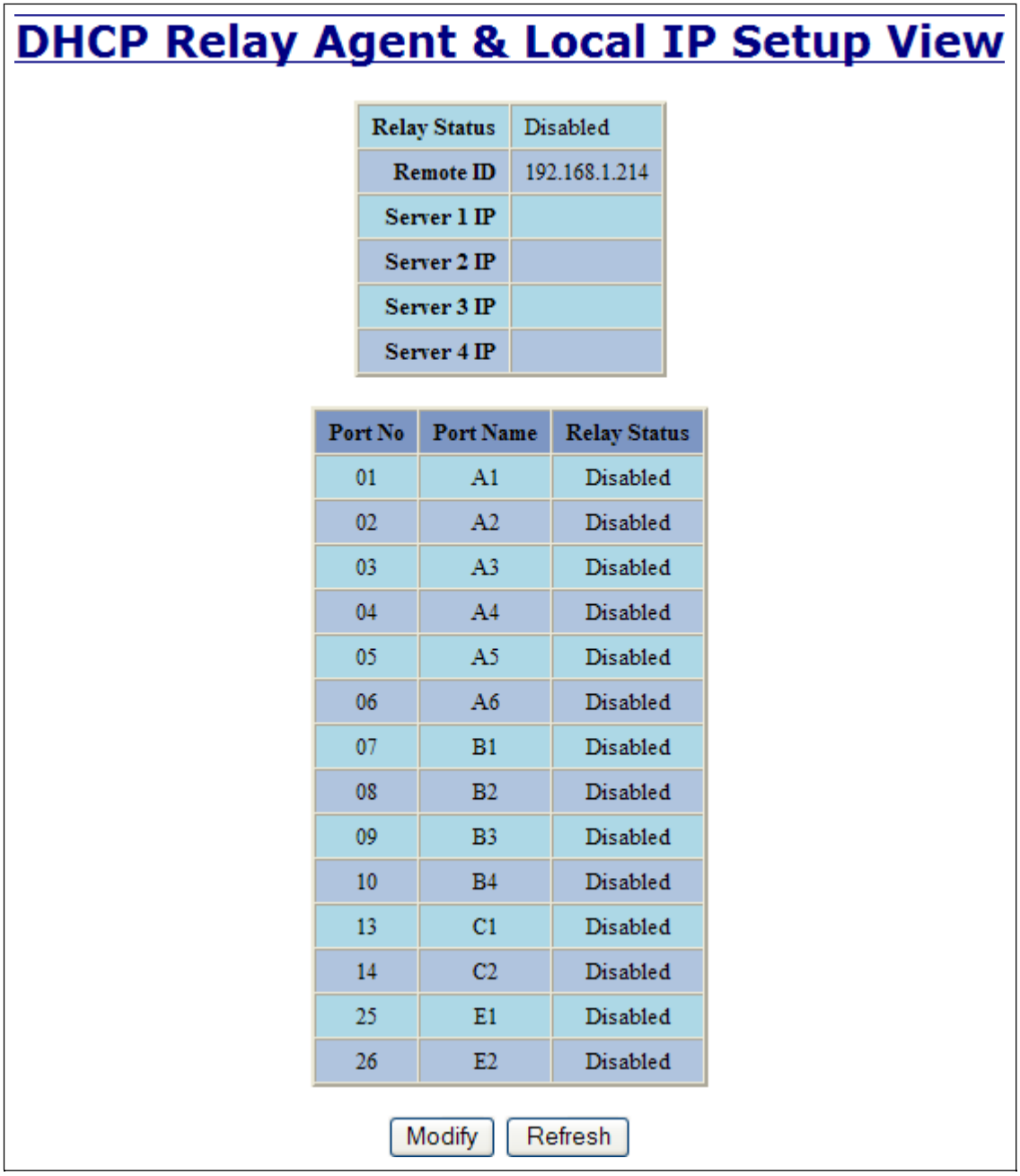
Status
Indicates the current status of the binding entry.

Release
Removes the corresponding binding.
WARNING: By releasing an IP address, it is possible to end up with two physical devices with the same IP address which may cause network disruption to that IP address.



DHCP – Relay & Local IP - Setup

The Setup tab under the DHCP/Relay & Local IP category shows the current state of the relay agent.

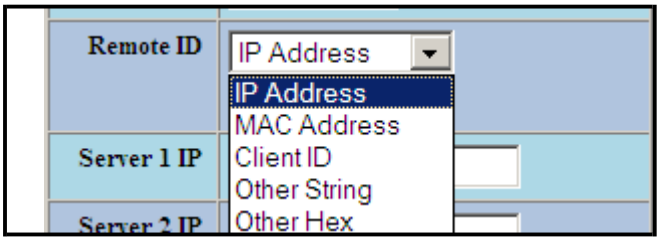


By selecting the Modify button, you can configure general settings of the relay agent, as well as, configure settings on a per port basis. The following describes these settings:

DHCP – Relay & Local IP – Setup, Continued…

Relay Status
Indicates whether the DHCP relay agent is active.

Remote ID
The unique identifier that designates the relay agent switch.



Server # IP
The configured IP address of the DHCP servers.

Port No
The actual port number.

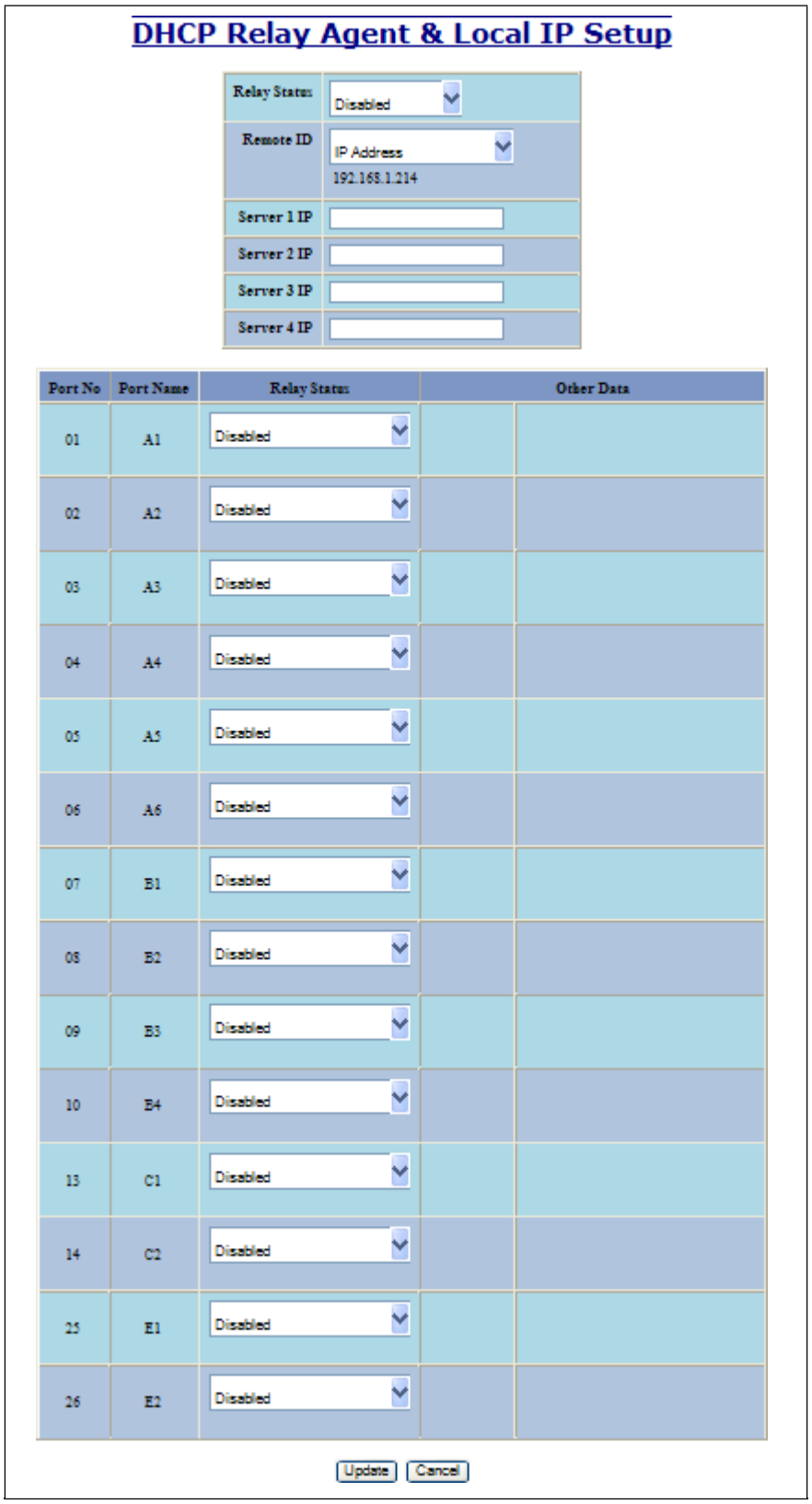
Port Name
The descriptive name of the port.

Relay Status
The selection to designate whether the port will perform relay agent functionality. The choices are:

Disabled	The port will function without relay agent processing.
Enabled	The port will relay DHCP client-originated broadcast packets to the DHCP servers.
Assign Local IP	The port will not relay DHCP client-originated broadcast packets. Instead the relay agent will offer the port's locally assigned IP address to the client.

Other Data
When the Relay Status is set to Enabled, the Circuit ID for the port can be specified. When the Relay Status is set to Assign Local IP, the IP address for the port can be specified.

DHCP – Relay & Local IP – Setup, Continued…



LLDP - Configuration

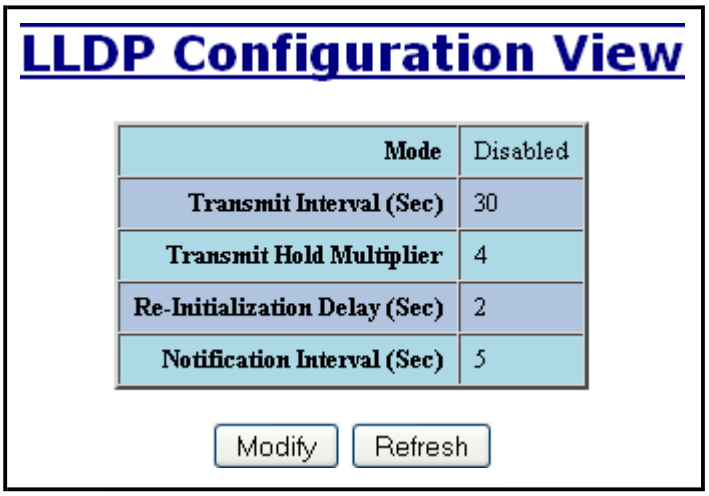
Mode:
Enables or Disables LLDP on the Switch. Default: Disabled

Transmit Interval:
Specifies the interval at which LLDP frames are transmitted. Default = 30 seconds.

Transmit Hold Multiplier:
Specifies a multiplier on the Transmit Interval when calculating a Time-to-Live value. Default = 4.

Re-Initialization Delay:
Specifies a minimum time an LLDP port will wait before re-initializing after setting the port to disable followed by setting a port to Tx-Only or Tx/Rx. This prevents excessive Notifications if someone toggles between Disabled and Enabled on LLDP Port settings. Default = 2 Seconds.

Notification Interval
Specifies the interval between successive Notifications generated by the switch. If a port sends out a notification and another port tries to send out a notification, the notification will not be sent until the interval expires.
Default = 5 Seconds.



Note: *A redundant network topology will have one or more blocking ports to prevent looping and broadcast storms. LLDP will not receive neighbor information into a blocked port, though the LLDP information will be transmitted out of a blocked port. Therefore, the switch that has the blocked port will not know about the neighbor on the other side of the blocked port, but the neighbor will know about the switch that has the blocked port.*

LLDP - Ports

LLDP Ports View

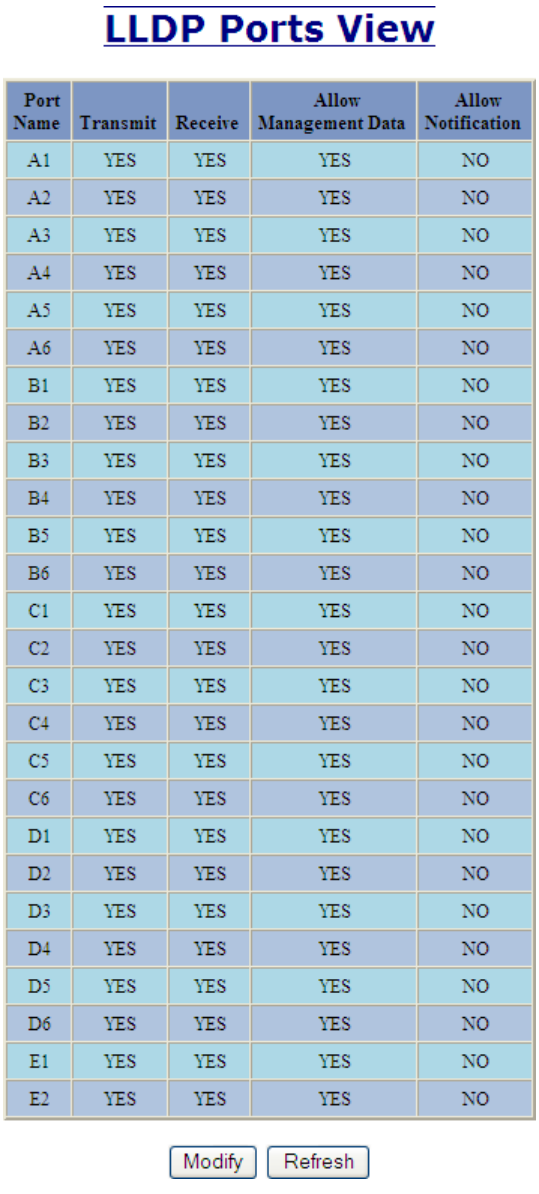
Port Name
Descriptive name of the port on the local switch.

Transmit
Enables or Disables LLDP Transmission on the switch.

Receive
Enables or Disables Receiving of LLDP Frames from neighbor switches.

Allow Management Data
Allow the Transmission of Management type information. For example: IP Address of switch, Port Description, System Name and Vlan information.

Allow Notifications
Notifications are transmitted when local or remote data changes.



LLDP Ports View

Port Name	Transmit	Receive	Allow Management Data	Allow Notification
A1	YES	YES	YES	NO
A2	YES	YES	YES	NO
A3	YES	YES	YES	NO
A4	YES	YES	YES	NO
A5	YES	YES	YES	NO
A6	YES	YES	YES	NO
B1	YES	YES	YES	NO
B2	YES	YES	YES	NO
B3	YES	YES	YES	NO
B4	YES	YES	YES	NO
B5	YES	YES	YES	NO
B6	YES	YES	YES	NO
C1	YES	YES	YES	NO
C2	YES	YES	YES	NO
C3	YES	YES	YES	NO
C4	YES	YES	YES	NO
C5	YES	YES	YES	NO
C6	YES	YES	YES	NO
D1	YES	YES	YES	NO
D2	YES	YES	YES	NO
D3	YES	YES	YES	NO
D4	YES	YES	YES	NO
D5	YES	YES	YES	NO
D6	YES	YES	YES	NO
E1	YES	YES	YES	NO
E2	YES	YES	YES	NO

Modify Refresh

LLDP - Status

LLDP Ports Neighbor View

The Status View shows the results of LLDP discovery. The LLDP Ethernet frames received from neighboring ports are composed of a collection of data units called TLVs. Each TLV contains a defined type of information such as the Chassis ID described below, which contains the MAC address of the device sending the frame. The maximum number of neighbors displayed per port is four.

Port Name
The name of the local port on which the neighbor information was received.

Neighbor MAC
MAC address of neighbor switch. Corresponds to the LLDP Chassis ID TLV.

Neighbor IP
IP address of neighbor switch. Corresponds to the LLDP Management Address TLV.

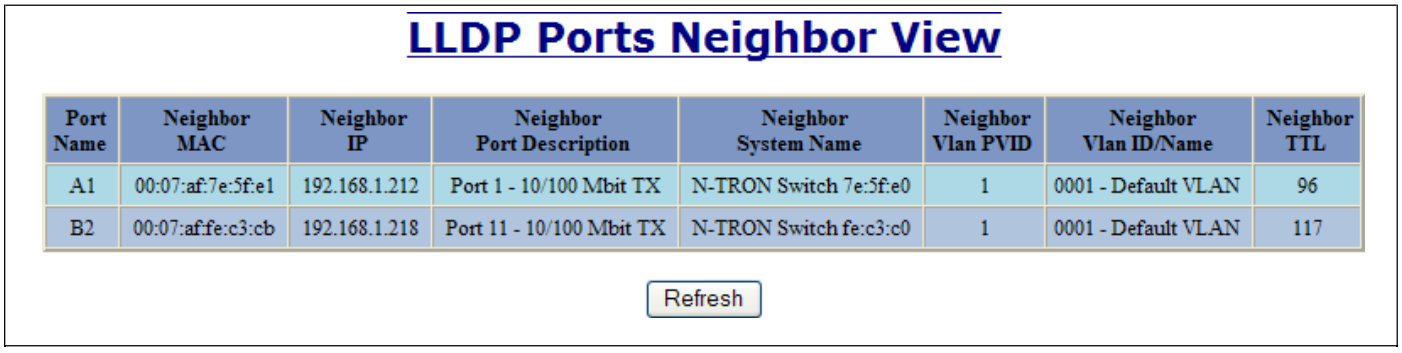
Neighbor Port Description
Description of the neighbor Port from which the LLDP frame was sent.

Neighbor System Name
The system's administratively assigned name on the neighbor switch.

Neighbor VLAN PVID
The Port VLAN identifier (PVID) associated with the neighbor port.

Neighbor VLAN ID/Name
A list of all VLAN's for which the neighbor port is a member.

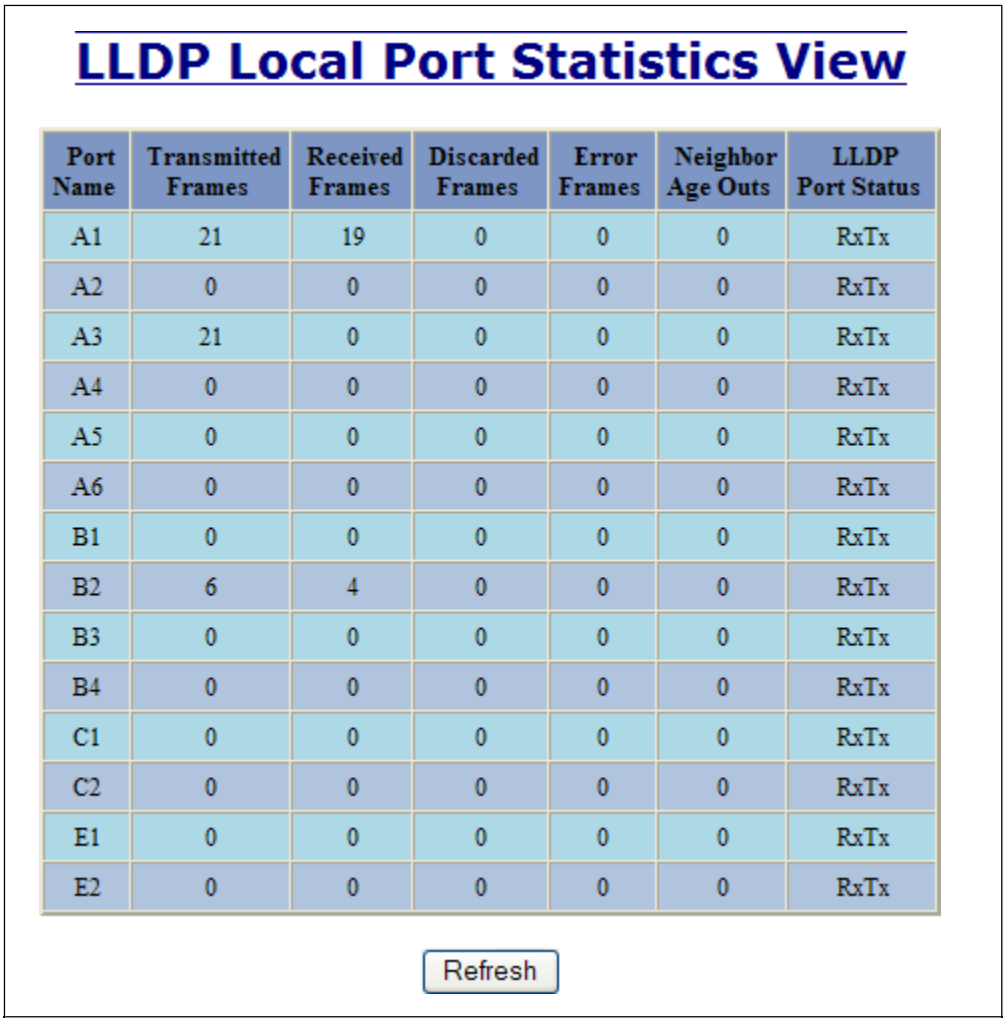
Neighbor TTL
Indicates the number of seconds that the information associated with this neighbor will be valid. Time to Live (TTL)



LLDP - Statistics

LLDP Local Port Statistics View

Port Name
Descriptive name of the port on the local switch.
Transmitted Frames
The total number of LLDP Frames sent out from the local switch.
Received Frames
Total number of LLDP frames received by the local switch.
Discarded Frames
The total number of frames discarded due to incorrect TLV's in frame.
Error Frames
Total count of all LLDP frames received with one or more detectable errors.
Neighbor Age Outs
Total count of the times that a neighbor's information has been deleted from the switch because the Time to Live (TTL) has expired.
LLDP Port Status
Local Port setting (Receive-Rx/Transmit-Tx/Disable).



Ports – Configuration

The Configuration tab under the Ports category will show a detailed overview of all the active ports on the switch. The overview will display the following information:

Port Number
This is the port index.

Port Name
This field displays the name of the port. The designation of TX is for copper ports, FX is for fiber optic ports, and GB is for the Gigabit ports (fiber or copper).

Admin Status
This configurable field displays the existing status of the port whether it is **Enabled/Disabled.**

Link Status
Current Link state of the port.

Auto Negotiation State
This configurable field displays the current auto-negotiation state whether it is **Enabled/Disable.**

Port Speed
This configurable field displays the speed of each port **10/100/1000** Mbps.

Duplex Mode
This configurable field displays the existing mode of the port whether it is **Full Duplex/Half Duplex.**

Crossover Mode
This configurable field displays the existing crossover mode of the port. This can be Yes, No, or Auto. Auto is the default.

Flow Control State
This configurable field displays the existing flow control status of each port. When enabled, the individual port supports half-duplex back pressure and full-duplex flow control. The default is **Disabled.**

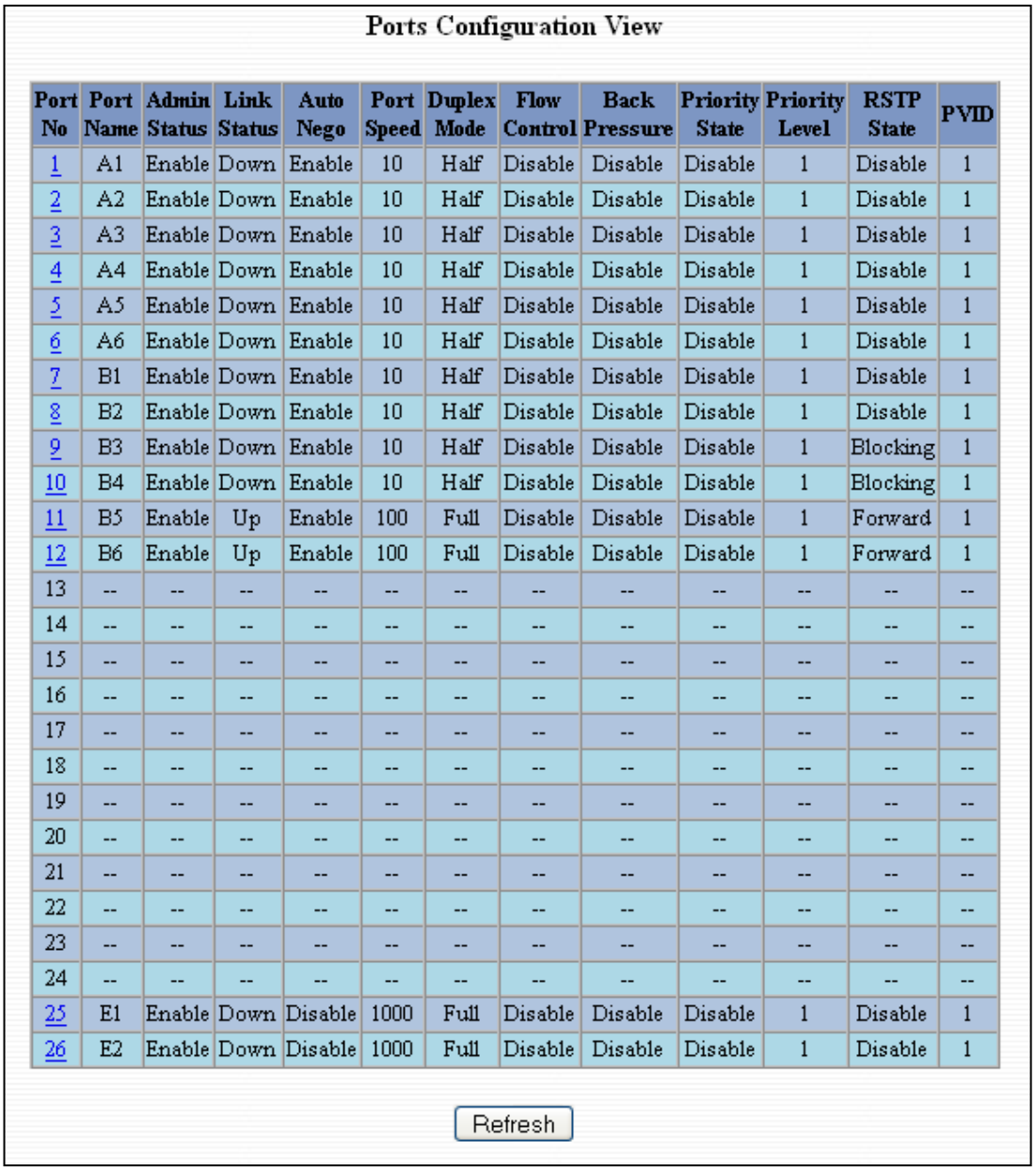
Port State
The current RSTP status of a port. It may contain **Disable/Discarding/Learning/Forwarding.**

PVID
This configurable field displays the existing port VLAN ID setting. The allowable range is **1-4094.**

Usage Alarm Low (%)
The bandwidth utilization percentage below which a fault will be triggered if enabled. For half duplex the bandwidth utilization percentage is the sum of both RX and TX bandwidth utilization, and for full duplex this is the higher of TX or RX bandwidth utilization. See Port Utilization View and Port Usage Fault on Fault Configuration View.

Usage Alarm High (%)
The bandwidth utilization percentage above which a fault will be triggered if enabled. For half duplex the bandwidth utilization percentage is the sum of both RX and TX bandwidth utilization, and for full duplex this is the higher of TX or RX bandwidth utilization. See Port Utilization View and Port Usage Fault on Fault Configuration View.

Ports – Configuration, Continued…



Ports Configuration View

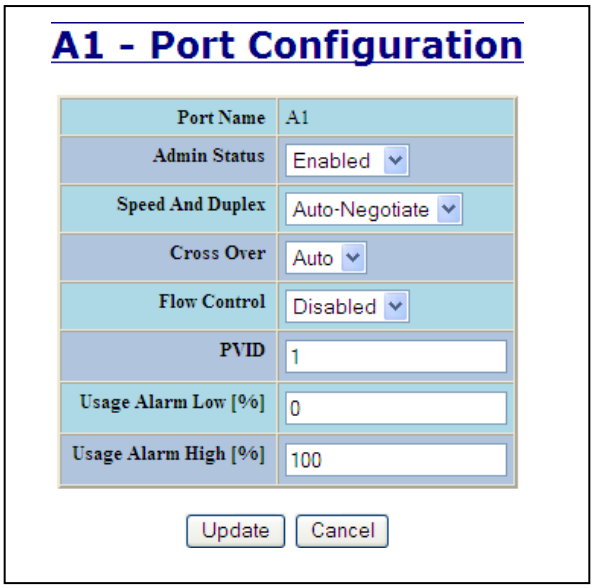
Port No	Port Name	Admin Status	Link Status	Auto Nego	Port Speed	Duplex Mode	Flow Control	Back Pressure	Priority State	Priority Level	RSTP State	PVID
1	A1	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
2	A2	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
3	A3	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
4	A4	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
5	A5	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
6	A6	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
7	B1	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
8	B2	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Disable	1
9	B3	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Blocking	1
10	B4	Enable	Down	Enable	10	Half	Disable	Disable	Disable	1	Blocking	1
11	B5	Enable	Up	Enable	100	Full	Disable	Disable	Disable	1	Forward	1
12	B6	Enable	Up	Enable	100	Full	Disable	Disable	Disable	1	Forward	1
13	--	--	--	--	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--	--	--	--	--
17	--	--	--	--	--	--	--	--	--	--	--	--
18	--	--	--	--	--	--	--	--	--	--	--	--
19	--	--	--	--	--	--	--	--	--	--	--	--
20	--	--	--	--	--	--	--	--	--	--	--	--
21	--	--	--	--	--	--	--	--	--	--	--	--
22	--	--	--	--	--	--	--	--	--	--	--	--
23	--	--	--	--	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--	--	--	--	--
25	E1	Enable	Down	Disable	1000	Full	Disable	Disable	Disable	1	Disable	1
26	E2	Enable	Down	Disable	1000	Full	Disable	Disable	Disable	1	Disable	1

Refresh

Ports – Configuration, Continued…

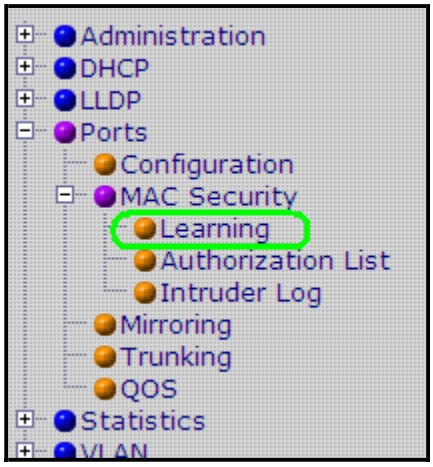
The User can click on the Port Number to configure each port individually. This will allow the user to change the port's settings for the following fields:

Admin Status
Speed and Duplex
Cross Over
Flow Control
PVID
Usage Alarm Low
Usage Alarm High



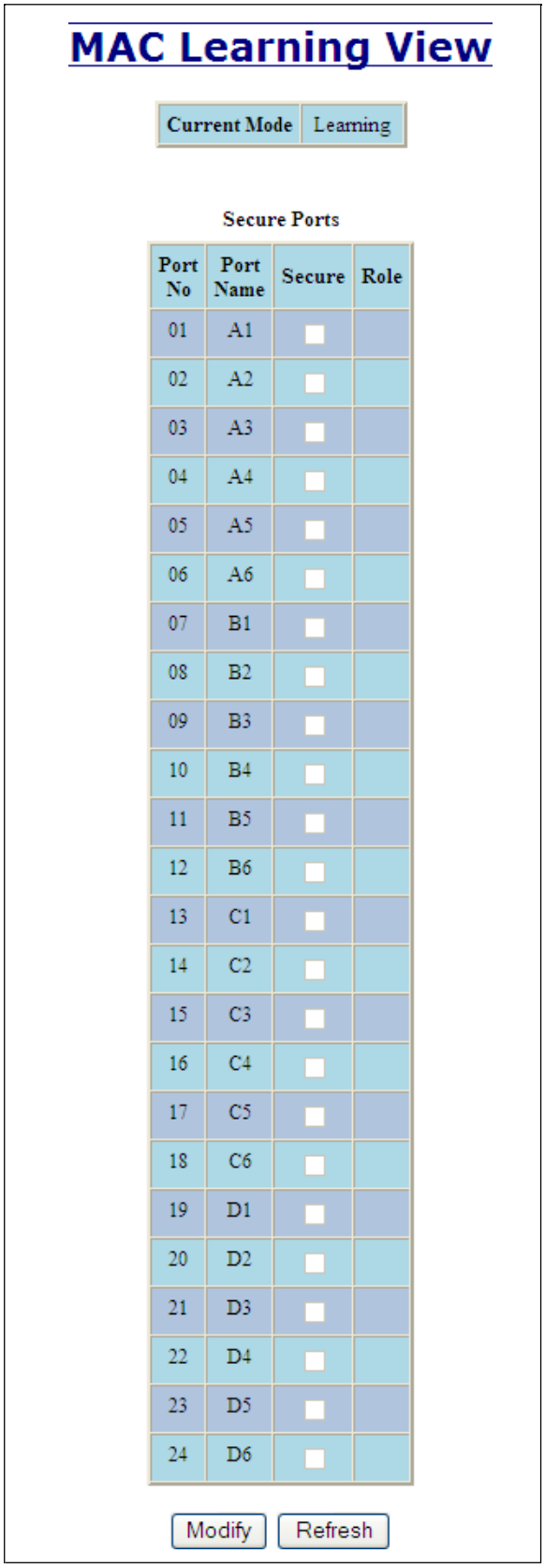
Ports – MAC Security – Learning

MAC Security is reached from the left hand navigation under ‘Ports’:



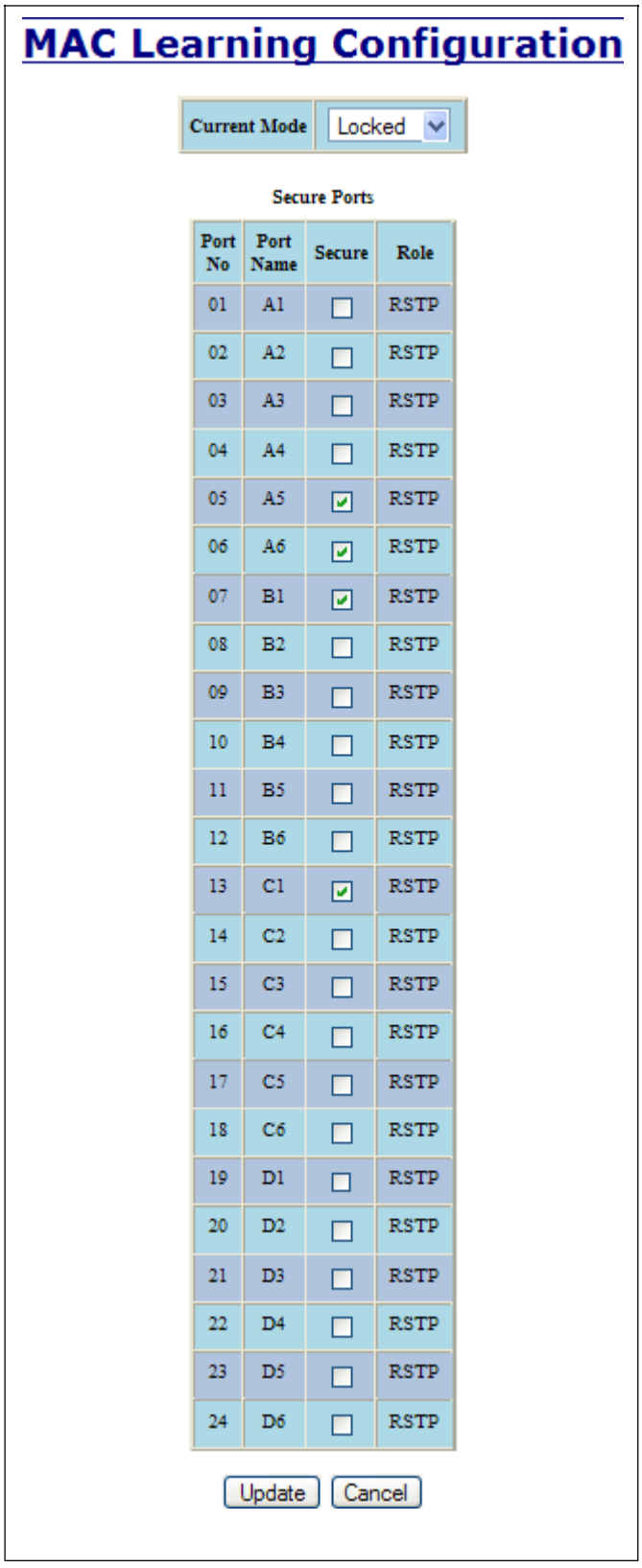
Ports – MAC Security – Learning (continued)

The Learning tab allows the administrator to control the learning or locking modes for the ports. ‘Locked’ is the secure mode. ‘Learning’ builds an internal list of authorized MAC addresses based on an approved LAN. When the current mode is ‘Learning’, no ports are secured.

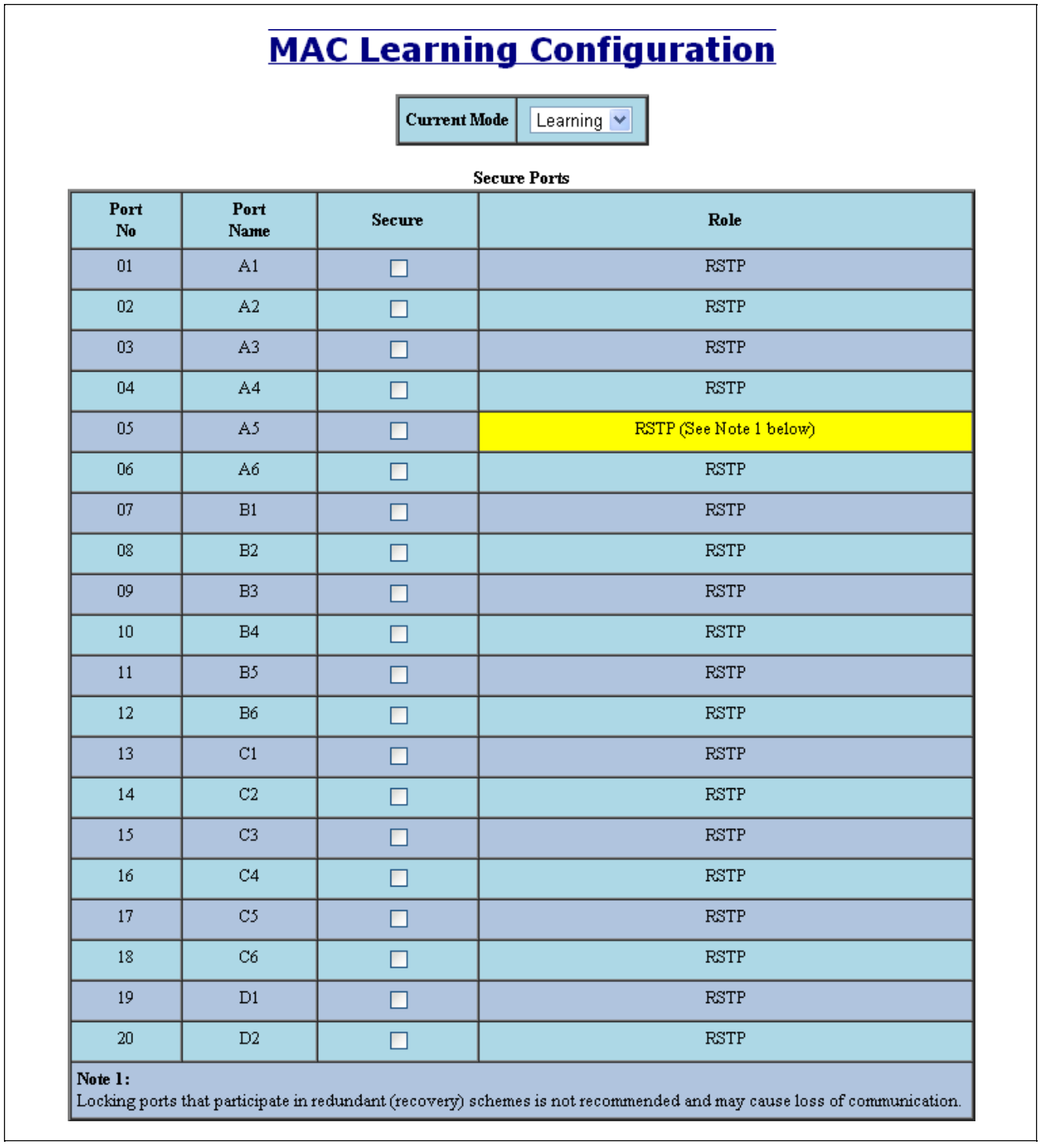


Ports – MAC Security (continued)

In ‘Locked’ mode, ‘Secured Ports’ shows the ports that are presently secured. *Note: when N-Ring and/or N-Link are used, the N-Ring/N-Link ports will not have MAC Security enabled.*



The Modify button allows the administrator to change the current mode. When transitioning from ‘Learning’ to ‘Locked’, the Address Resolution Logic (ARL) table represents the authorized MAC addresses, with the addition of any manually entered addresses (refer to Authorization List section below). Transitioning from ‘Locked’ to ‘Learning’, clears the ARL for all ports.



MAC Learning Configuration

Current Mode	Learning

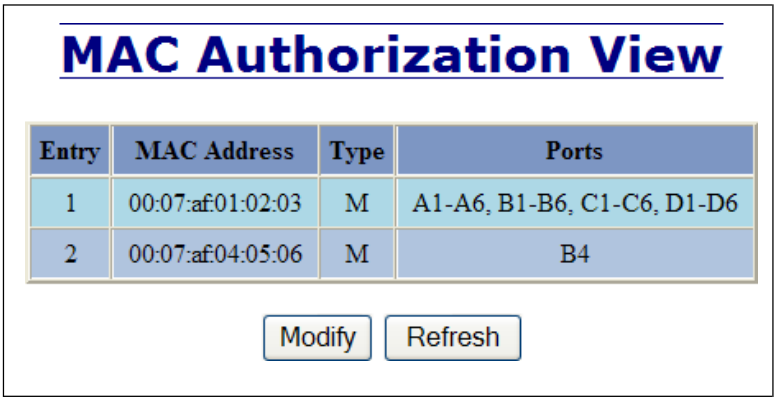
Secure Ports

Port No	Port Name	Secure	Role
01	A1	☐	RSTP
02	A2	☐	RSTP
03	A3	☐	RSTP
04	A4	☐	RSTP
05	A5	☐	RSTP (See Note 1 below)
06	A6	☐	RSTP
07	B1	☐	RSTP
08	B2	☐	RSTP
09	B3	☐	RSTP
10	B4	☐	RSTP
11	B5	☐	RSTP
12	B6	☐	RSTP
13	C1	☐	RSTP
14	C2	☐	RSTP
15	C3	☐	RSTP
16	C4	☐	RSTP
17	C5	☐	RSTP
18	C6	☐	RSTP
19	D1	☐	RSTP
20	D2	☐	RSTP

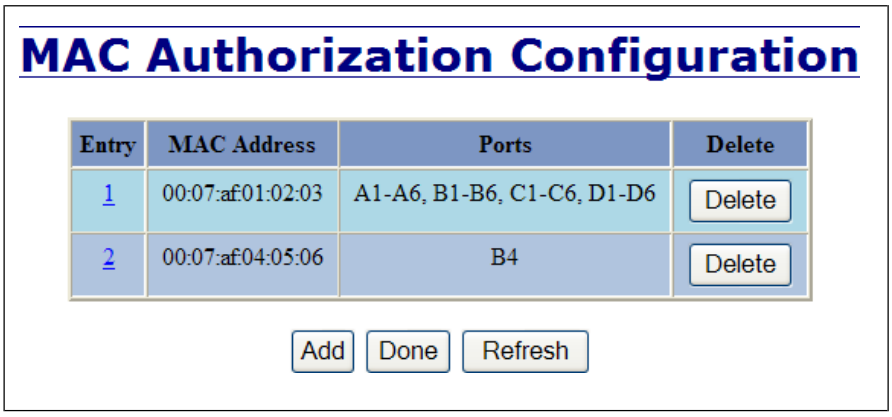
Note 1:
Locking ports that participate in redundant (recovery) schemes is not recommended and may cause loss of communication.

Ports – MAC Security – Authorization List

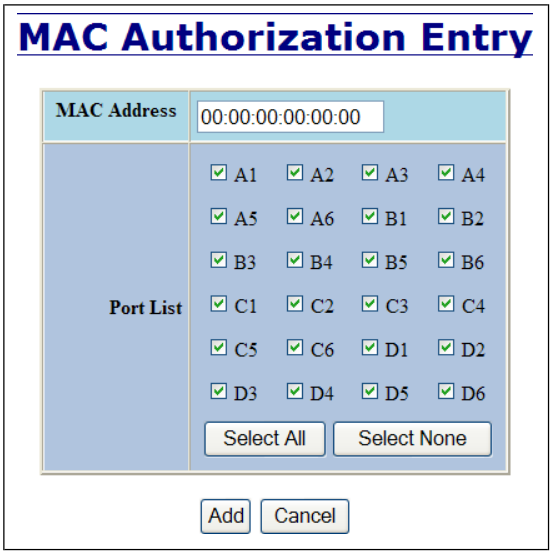
The Authorization List tab allows for manual entry or deletion of authorized MAC source addresses with associated authorized ports.



Selecting Modify displays the MAC Authorization Configuration page, which allows the administrator to add new entries, delete existing entries, or edit authorized ports of existing entries.

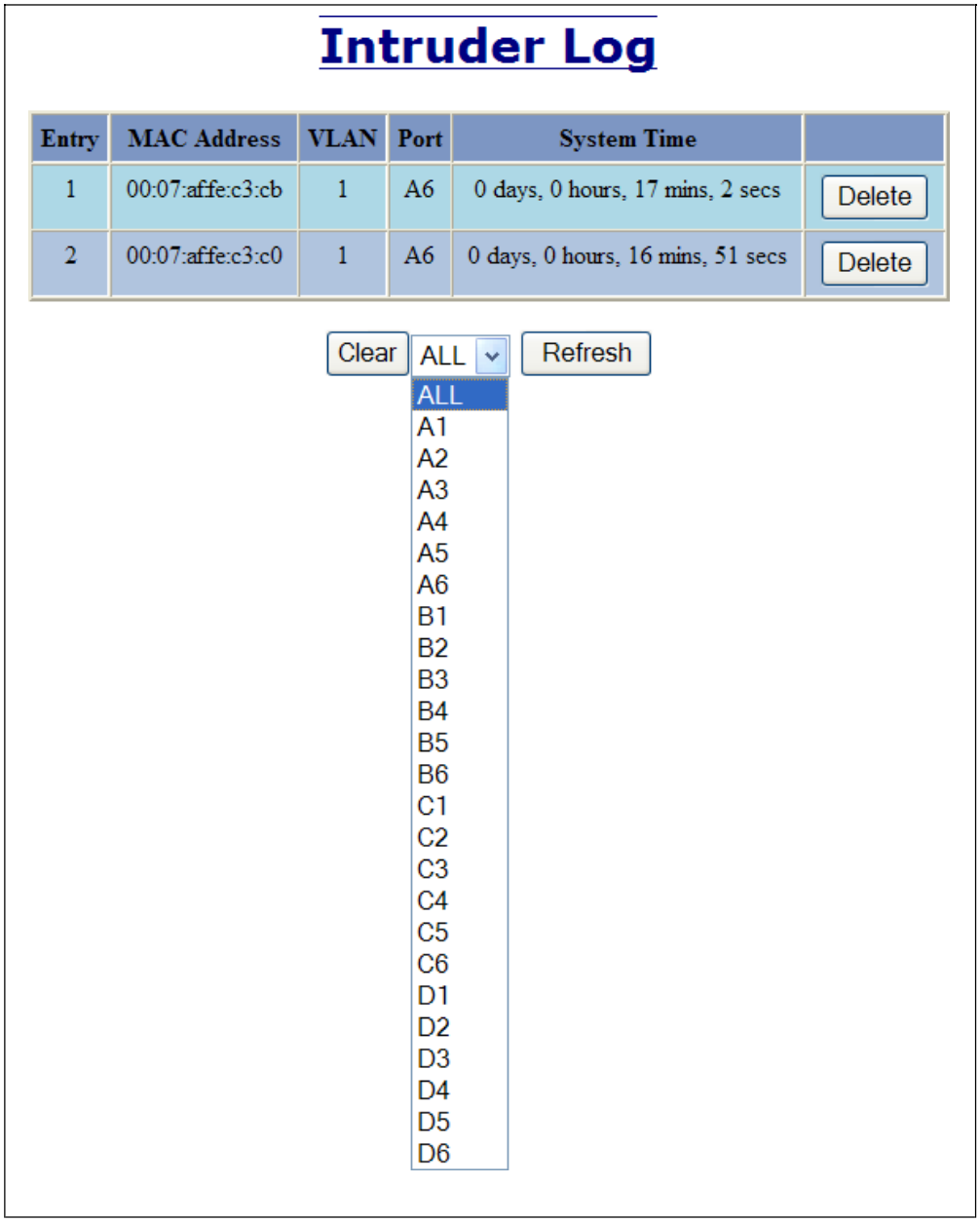


Selecting Delete removes the associated entry. Selecting Add displays the MAC Authorization Entry page, showing default values for the administrator to modify (see below). When an entry number hyperlink is selected, this same page is displayed except it shows the associated MAC address and authorized ports.



Ports – MAC Security – Intruder Log

The Intruder Log tab displays a list of unauthorized MAC addresses that attempted to access the secured device. Each intruder entry in the log is unique, and is based on the combination of MAC address, VLAN, and port. Only the first occurrence of the intruder is listed. The log is ordered by most recent first, based on the system time. The maximum number of entries is 100. If more than 100 intruders are detected, the oldest entries are deleted. The log is not saved through a power cycle.



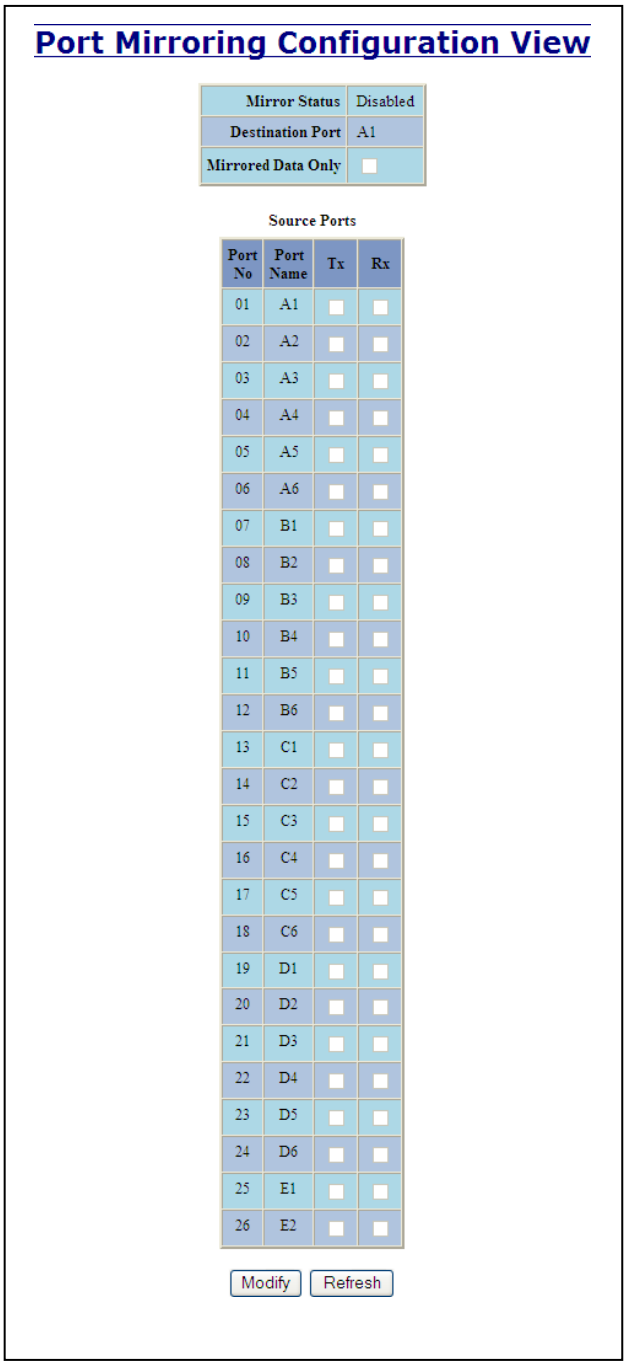
An entry can be individually removed from the log by selecting the associated Delete button. All entries or entries specific to a port can also be removed from the log by choosing the option in the dropdown list and then selecting the Clear button.

Ports – Mirroring

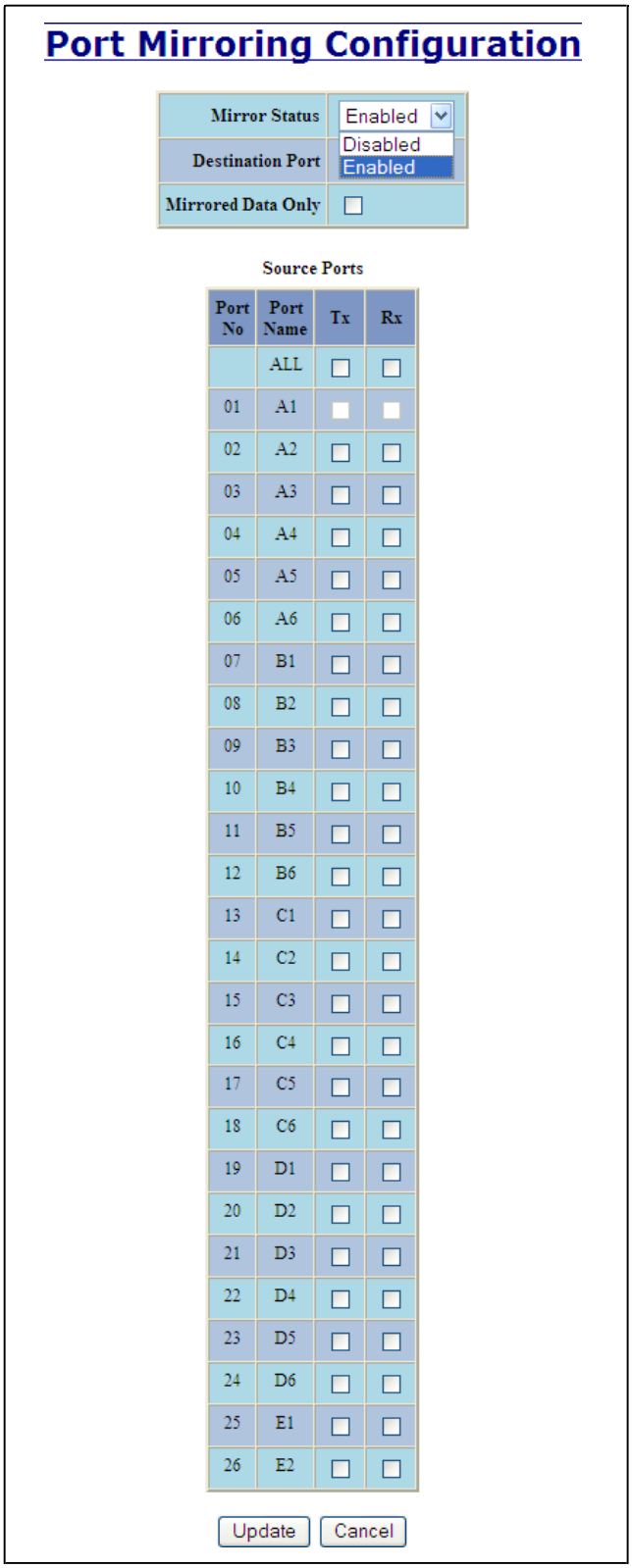
A mirroring port is a dedicated port that is configured to receive the copies of Ethernet frames that are being transmitted out and also being received in from any other port that is being monitored.

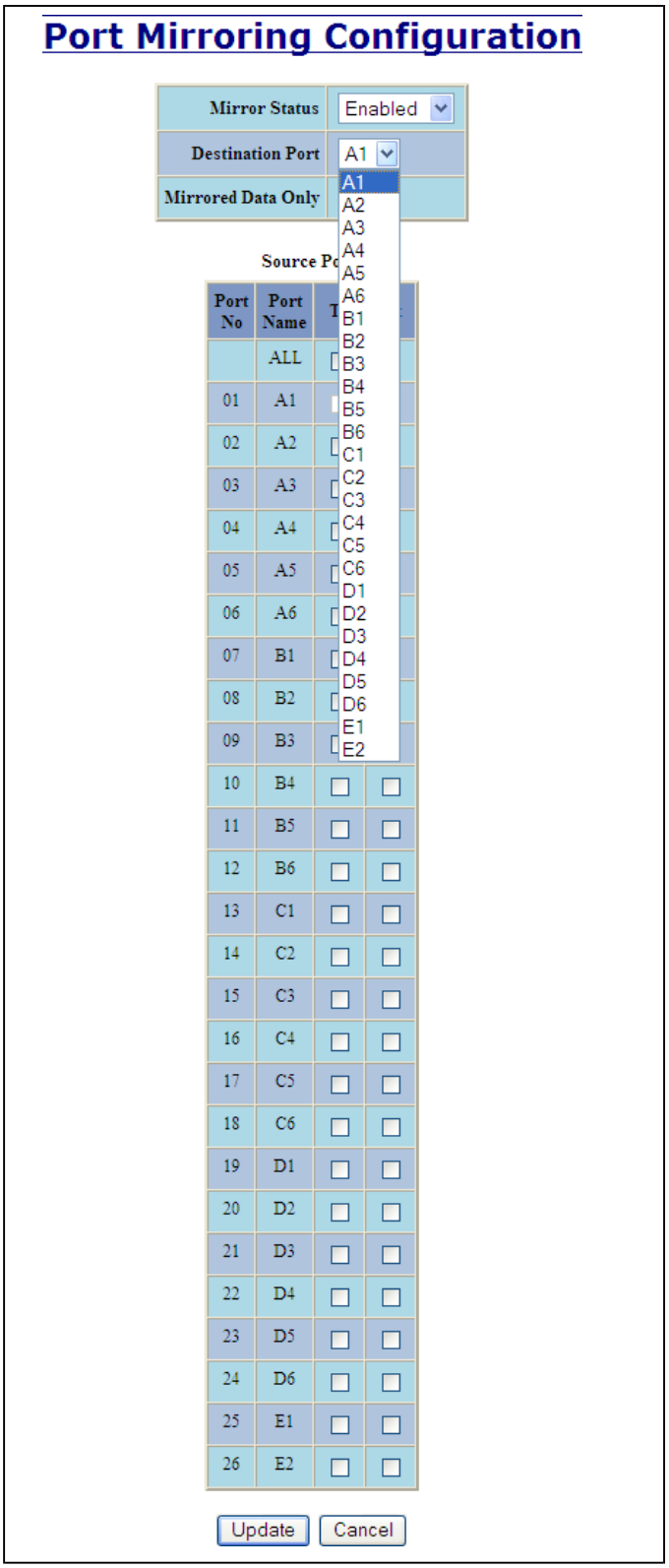
The Mirroring tab under the Ports category displays the status including the list of Source Ports and the Destination Port that the Sources are being mirrored to.

'Mirrored Data Only' can be selected and this selects for mirrored data only to be transmitted to the destination port, as opposed to mirrored data and whatever other data is otherwise destined for the destination Port.



Using the Modify button, you can enable the status of port mirroring(left diagram below) and select source ports and the destination port that the source ports will be mirrored to (right diagram below). The check boxes can be used to select the ports that will be mirrored to the destination port.





NOTE:
Since the gigabit ports cannot be destination ports, they are not available on the pull-down menu.

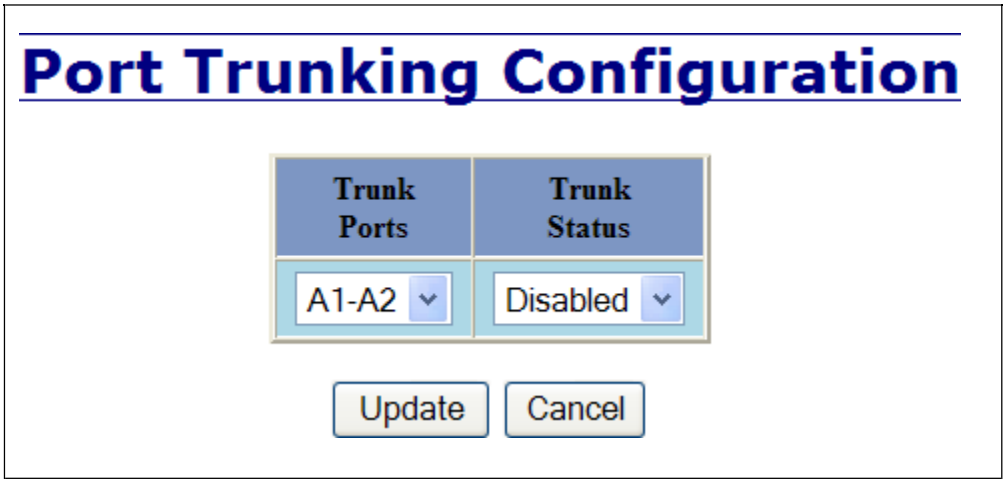
]

Ports – Trunking

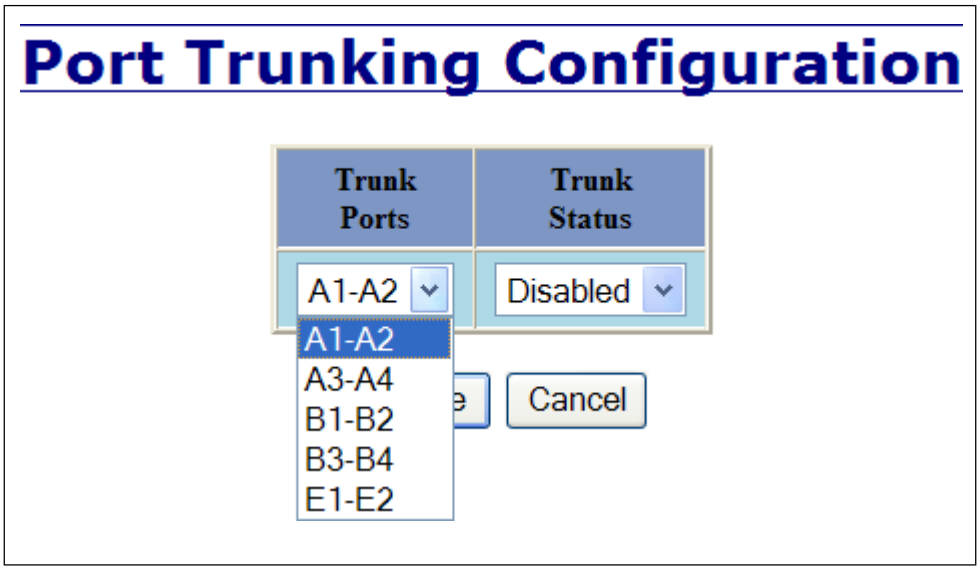
The Trunking tab under the Ports category displays the following details:

Trunk Ports
This field displays the ports associated with the trunk.

Trunk Status
This configurable field displays the existing status of the trunk. It can be either Enabled/Disabled.



By selecting the Modify button, you can select a trunk group.



Note: *RSTP must be disabled in order to use the Trunking feature.*
Two ports of the same speed can constitute a valid trunk.
Only 1 Trunk per switch can be created.

All trunk ports must be at the same speed and duplex mode. If a port is not linked, there could be difficulty as to similar speed and duplex mode. It is best to hard code speed and duplex mode for each trunking link, at both ends.

Do not use Trunking on an N-Ring manager. Do not connect the N-Ring to actively Trunking ports on an Auto Member.

Ports – QOS

The QOS decision tree chooses the highest priority Transmit Queue (TQ) of the following criteria: Force High Priority (Port Based) TQ mapping, IEEE 8021.p TQ mapping, or DSCP TQ mapping.

The QOS tab under the Ports category displays the following details:

Port Number
This is the port index.

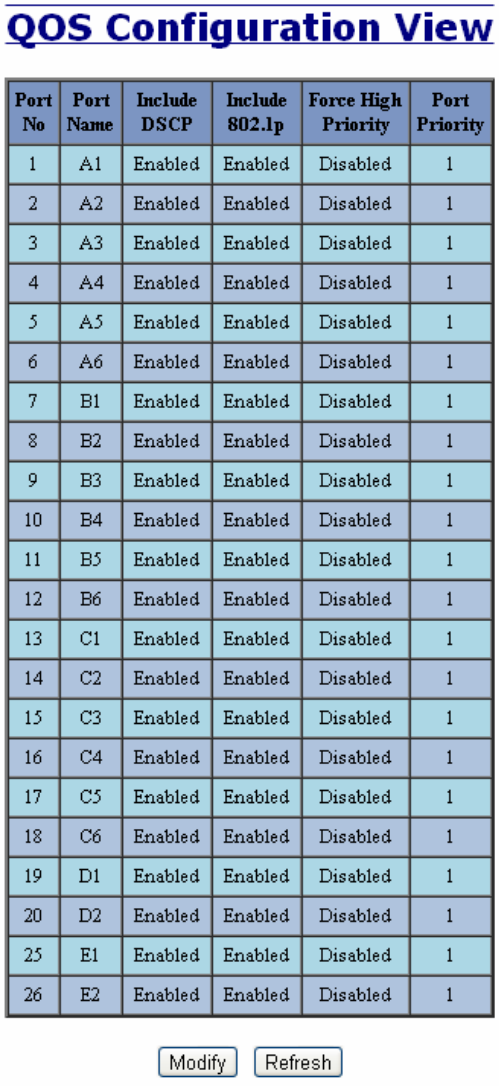
Port Name
This field displays the name of the port.

Include DSCP
This field displays the status of whether or not to include the RFC 2474 DSCP TOS (Type of Service) in the TQ decision. When enabled, the DSCP TOS is included when evaluating traffic priority.

Include 802.1p
This field displays the status of whether or not to include the IEEE 802.1p COS (Class of Service) in the TQ decision. When enabled, the IEEE 802.1p COS is included when evaluating traffic priority.

Force High Priority
This field displays the Force High Priority status. When enabled, the port based priority is included in the TQ decision for all ports and all frames received on a port will use the default QOS priority for that port in the TQ decision.

Port Priority
This field displays the default QOS priority for that port. This is the IEEE 802.1p COS (Class of Service) assigned to all untagged ingress frames, or all ingress frames if Force High Priority is enabled. The range is 0-7.



QOS Configuration View

Port No	Port Name	Include DSCP	Include 802.1p	Force High Priority	Port Priority
1	A1	Enabled	Enabled	Disabled	1
2	A2	Enabled	Enabled	Disabled	1
3	A3	Enabled	Enabled	Disabled	1
4	A4	Enabled	Enabled	Disabled	1
5	A5	Enabled	Enabled	Disabled	1
6	A6	Enabled	Enabled	Disabled	1
7	B1	Enabled	Enabled	Disabled	1
8	B2	Enabled	Enabled	Disabled	1
9	B3	Enabled	Enabled	Disabled	1
10	B4	Enabled	Enabled	Disabled	1
11	B5	Enabled	Enabled	Disabled	1
12	B6	Enabled	Enabled	Disabled	1
13	C1	Enabled	Enabled	Disabled	1
14	C2	Enabled	Enabled	Disabled	1
15	C3	Enabled	Enabled	Disabled	1
16	C4	Enabled	Enabled	Disabled	1
17	C5	Enabled	Enabled	Disabled	1
18	C6	Enabled	Enabled	Disabled	1
19	D1	Enabled	Enabled	Disabled	1
20	D2	Enabled	Enabled	Disabled	1
25	E1	Enabled	Enabled	Disabled	1
26	E2	Enabled	Enabled	Disabled	1

Modify Refresh

Ports – QOS, Continued…

Following the Modify button, the administrator can independently configure the ports for different QOS functionality. Once these fields are filled in to meet the needs of the administrator's network, the changes may be updated by clicking the Update button at the bottom of the page.

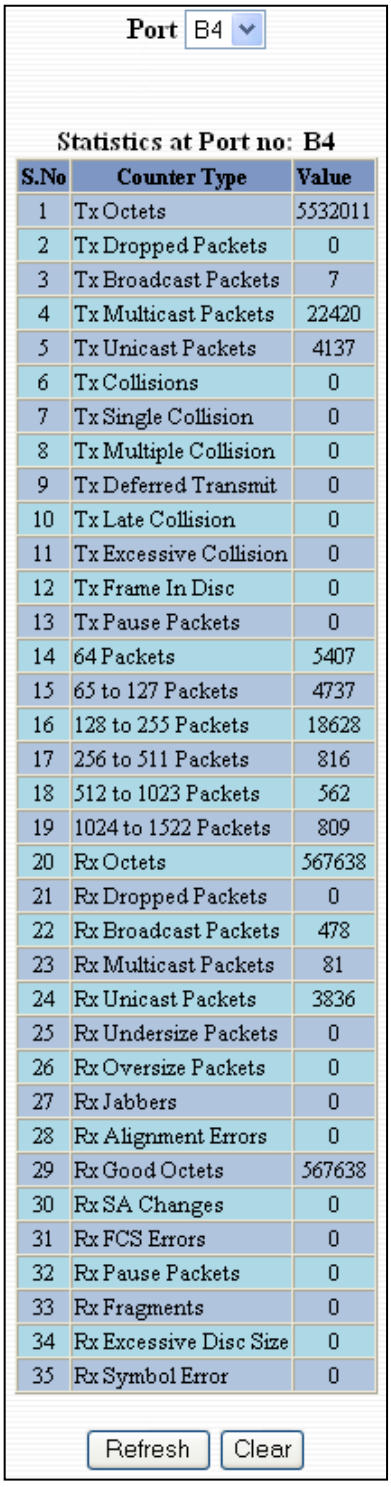
Modify QOS Configuration

Port No	Port Name	Include DSCP	Include 802.1p	Force High Priority	Port Priority
1	A1	Enabled	Enabled	Disabled	1
2	A2	Enabled	Enabled	Disabled	1
3	A3	Enabled	Enabled	Disabled	1
4	A4	Enabled	Enabled	Disabled	1
5	A5	Enabled	Enabled	Disabled	1
6	A6	Enabled	Enabled	Disabled	1
7	B1	Enabled	Enabled	Disabled	1
8	B2	Enabled	Enabled	Disabled	1
9	B3	Enabled	Enabled	Disabled	1
10	B4	Enabled	Enabled	Disabled	1
11	B5	Enabled	Enabled	Disabled	1
12	B6	Enabled	Enabled	Disabled	1
13	C1	Enabled	Enabled	Disabled	1
14	C2	Enabled	Enabled	Disabled	1
15	C3	Enabled	Enabled	Disabled	1
16	C4	Enabled	Enabled	Disabled	1
17	C5	Enabled	Enabled	Disabled	1
18	C6	Enabled	Enabled	Disabled	1
19	D1	Enabled	Enabled	Disabled	1
20	D2	Enabled	Enabled	Disabled	1
25	E1	Enabled	Enabled	Disabled	1
26	E2	Enabled	Enabled	Disabled	1

Update Cancel

Statistics – Port Statistics

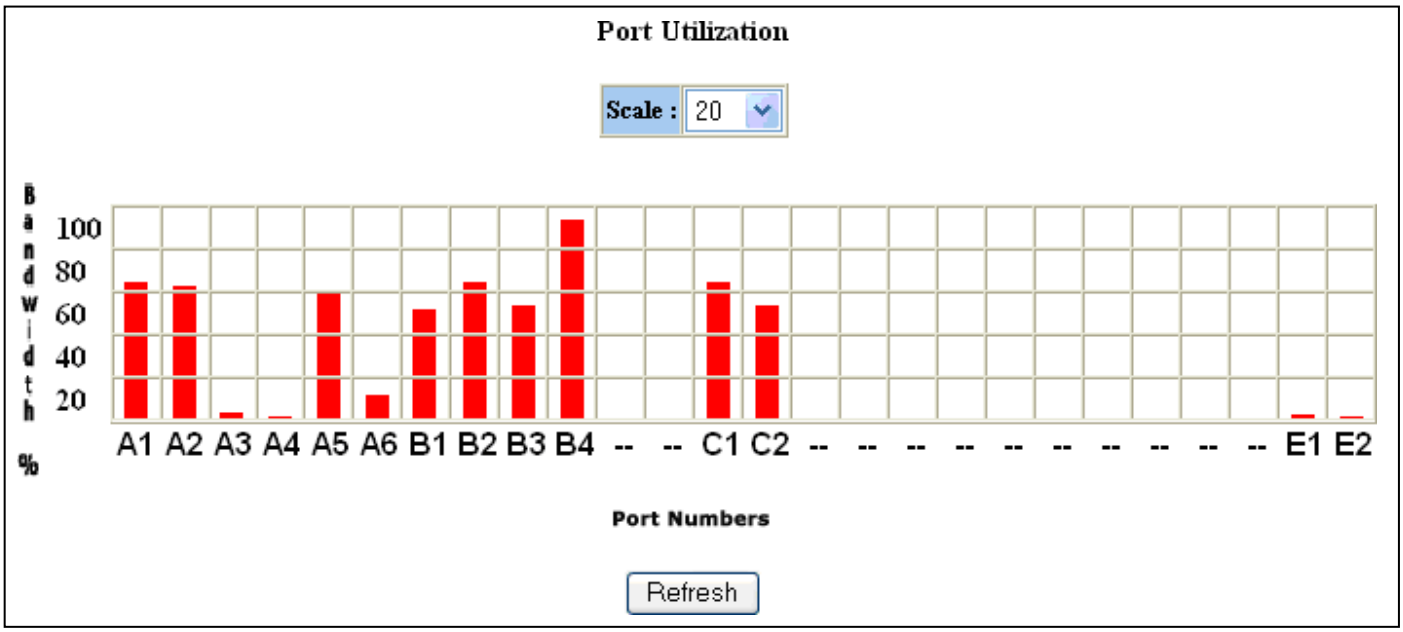
The Ports Statistics tab under the Statistics category displays a list of MIB Parameters. Each port has a separate counter for each parameter. This gives users the ability to see what kind of packets are going over which ports. At the bottom of each page for each port there are two buttons. Refresh will update the statistics for that port number and Clear will reset all the counters for that port number.



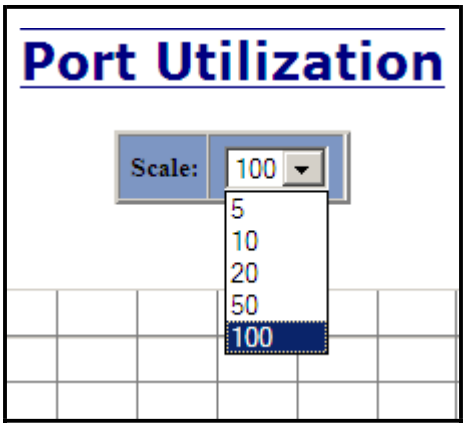
S.No	Counter Type	Value
1	Tx Octets	5532011
2	Tx Dropped Packets	0
3	Tx Broadcast Packets	7
4	Tx Multicast Packets	22420
5	Tx Unicast Packets	4137
6	Tx Collisions	0
7	Tx Single Collision	0
8	Tx Multiple Collision	0
9	Tx Deferred Transmit	0
10	Tx Late Collision	0
11	Tx Excessive Collision	0
12	Tx Frame In Disc	0
13	Tx Pause Packets	0
14	64 Packets	5407
15	65 to 127 Packets	4737
16	128 to 255 Packets	18628
17	256 to 511 Packets	816
18	512 to 1023 Packets	562
19	1024 to 1522 Packets	809
20	Rx Octets	567638
21	Rx Dropped Packets	0
22	Rx Broadcast Packets	478
23	Rx Multicast Packets	81
24	Rx Unicast Packets	3836
25	Rx Undersize Packets	0
26	Rx Oversize Packets	0
27	Rx Jabbers	0
28	Rx Alignment Errors	0
29	Rx Good Octets	567638
30	Rx SA Changes	0
31	Rx FCS Errors	0
32	Rx Pause Packets	0
33	Rx Fragments	0
34	Rx Excessive Disc Size	0
35	Rx Symbol Error	0

Statistics – Ports Utilization

The Ports Utilization tab under the Statistics category shows all the ports on the switch and will display a bar graph showing the percentage of bandwidth being used. These figures and bars are for a general feeling of what the bandwidth usage is. N-Tron recommends the use of N-View in order to get a precise bandwidth usage figure.



The scale can be adjusted for the task at hand:



VLAN – Configuration

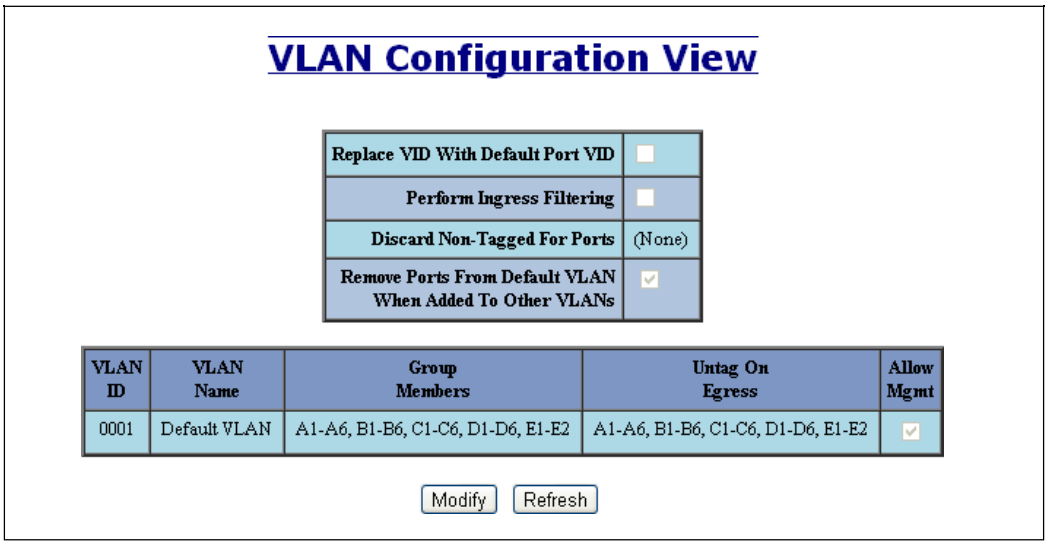
Note: Consult the Table of Contents for ‘VLAN Addition and Deletion Example’, and ‘VLAN Configuration Examples’. These are detailed examples.

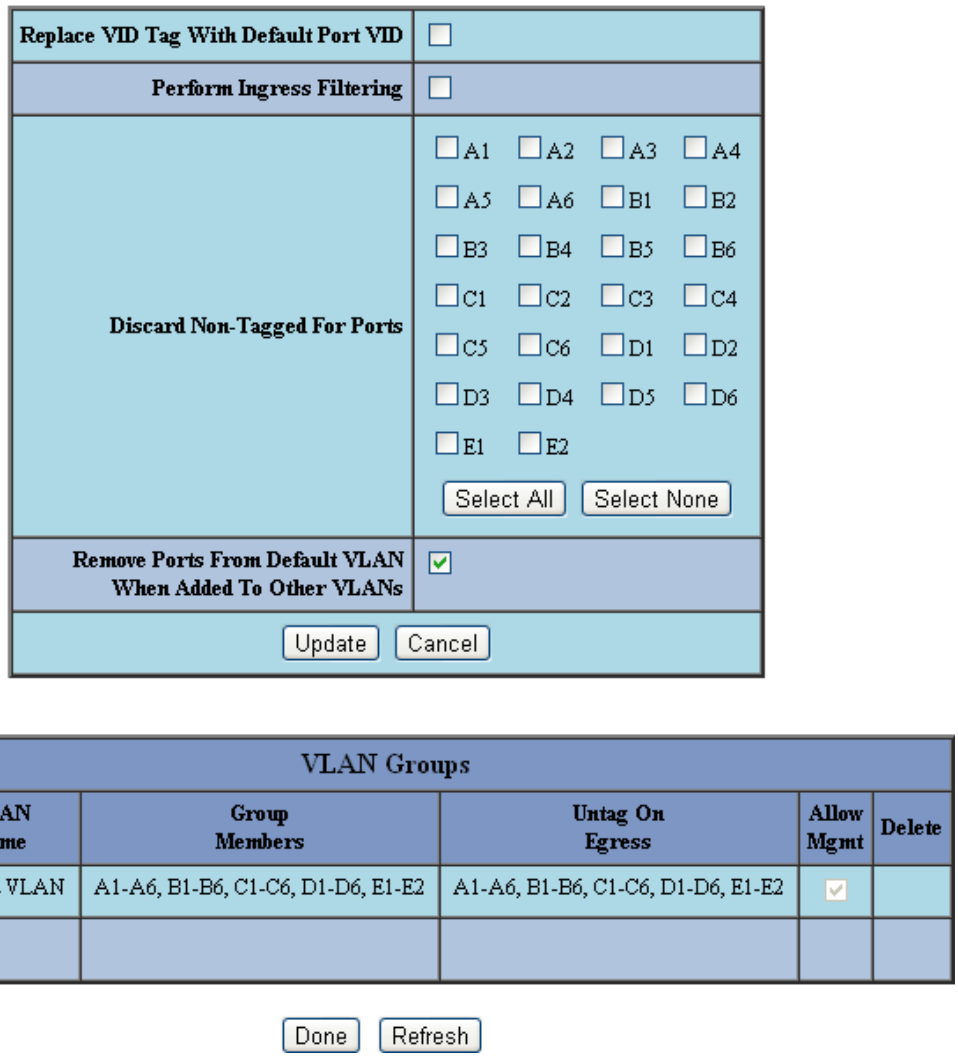
Replace VID Tag with Default Port VID
Specifies whether or not to replace the incoming VID tag with the port's designated VID.

Perform Ingress Filtering
Specifies whether or not to filter out ingress frames when a VID violation is detected.

Discard Non-Tagged for Ports
Specifies whether or not non-tagged ingress frames are dropped by the selected ports.

Remove Ports from Default VLAN when Added to Other VLAN
Specifies whether or not to remove ports from Default VLAN when they are added to another VLAN.





Note that for convenience in most frequent use:

- Ports are deleted from group1 as each port is added to another group, unless selected otherwise.
- Ports are added to group1 if a deletion leaves a port with no group.
- If it is desired to have a port on group1 and also on other group(s) configure group1 last to achieve that, or deselect '**Remove Ports from Default VLAN when Added to Other VLAN'.**

Note: *RSTP on overlapping VLANs is not supported and the system will automatically disable RSTP on all but the lowest VID VLANs that have overlapping ports.*

VLAN – Group Configuration

VLAN ID

This field displays the VLAN ID. The range should be **1-4094.**

VLAN Name

This configurable field displays the name of the VLAN, which accepts alphanumeric and special characters (#, _, -, .) only.

Allow Management

Specifies whether or not all ports in this VLAN are management ports.

Change PVID of Member Ports

Specifies whether or not the PVID of the member ports is set to this VLAN ID.

Port No

This is the port index.

Port Name

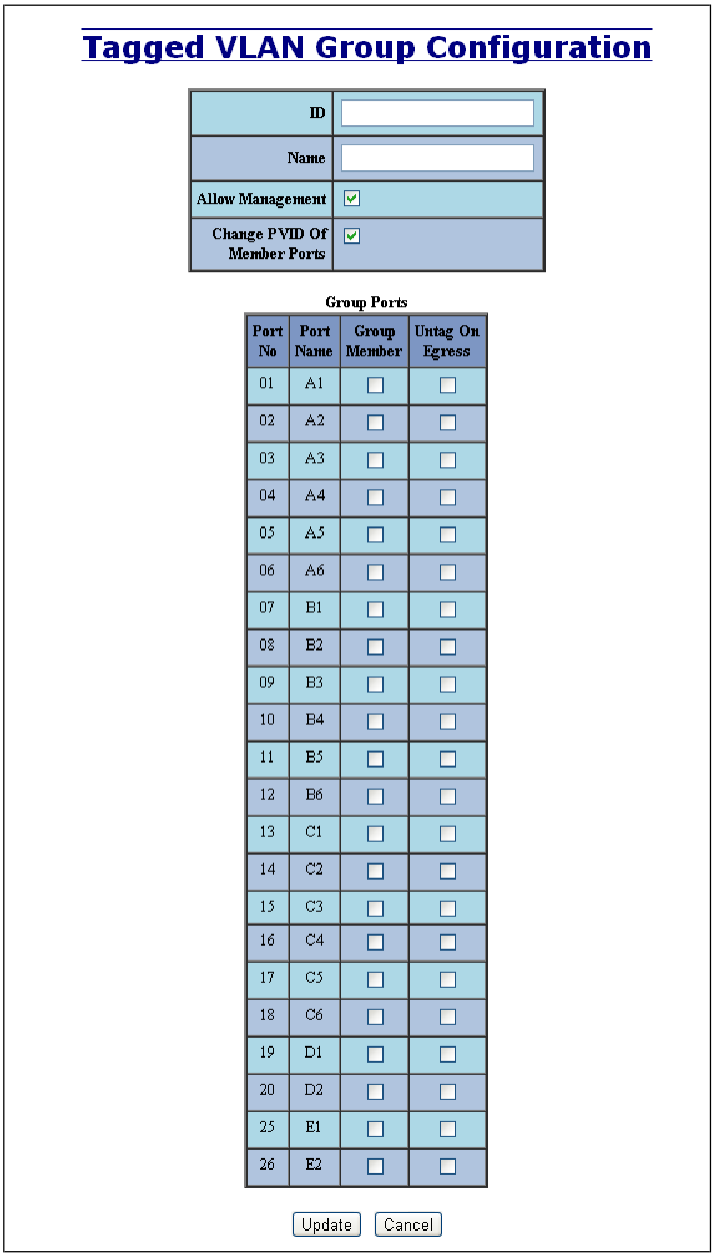
Descriptive name of the port

Group Member

Specifies whether or not the port is included in the group.

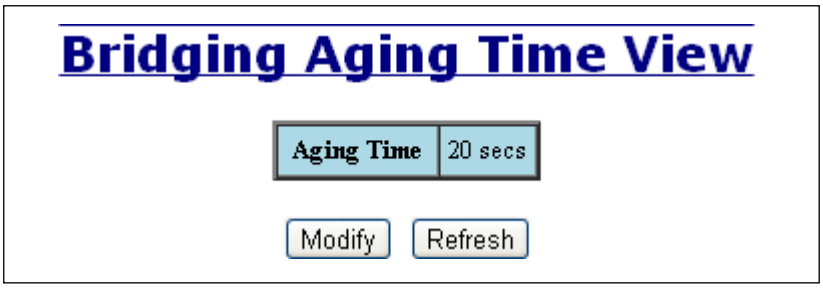
Untag on Egress

Specifies whether or not egress frames are tagged by the designated port.



Bridging – Aging Time

The Aging Time tab under the Bridging category will display the currently configured Aging Time. This page allows users to modify this variable to meet their needs.

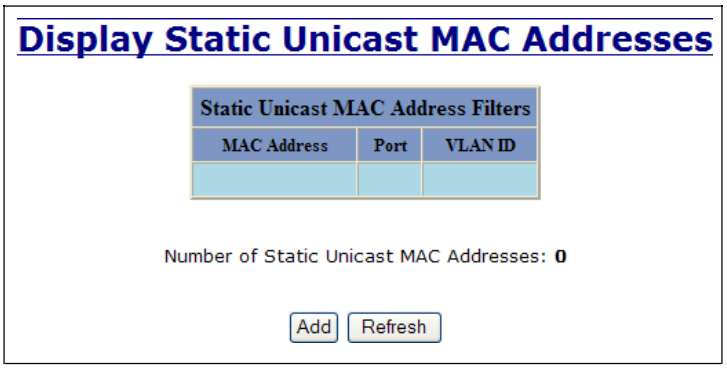


After selecting the Modify button the user will be presented with a page that allows the number to be entered into and updated. The default aging time is 20 seconds.

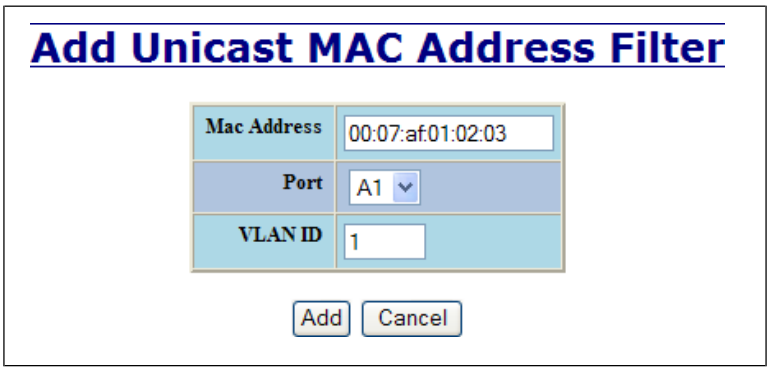
Note: *If the switch is an active participant of an N-Ring, then the N-Ring Aging Time will be used instead of the Bridging Aging Time.*

Bridging – Unicast Addresses

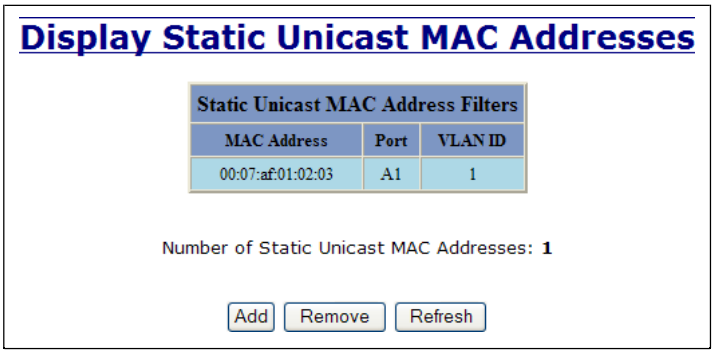
The Unicast Addresses tab under the Bridging category will display a list of MAC addresses that are associated with each respective port number. This can be used to statically assign a MAC address access to a single port on the switch.



Following the Add button on the page above, the administrator must enter a valid MAC address and associate it with a port number on the switch. Once the administrator hits the Update button the changes will take effect instantly.

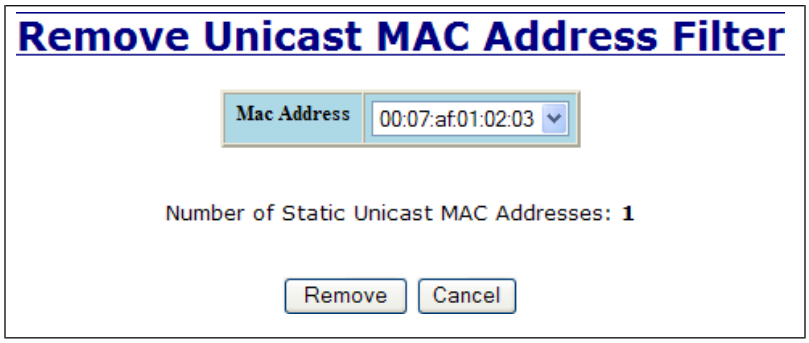


Once a static MAC address has been added, it will be displayed in a list on the main page under Unicast MACs tab.



Bridging – Unicast Addresses, Continued…

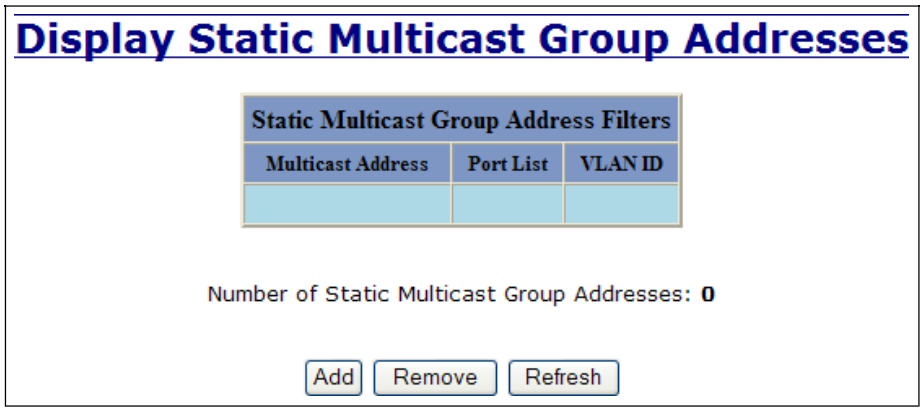
Following the Remove button on the page above, an administrator can select a static MAC address from the list using a pull-down menu. After selecting the MAC address the administrator may press the Remove button on this page to remove the entry



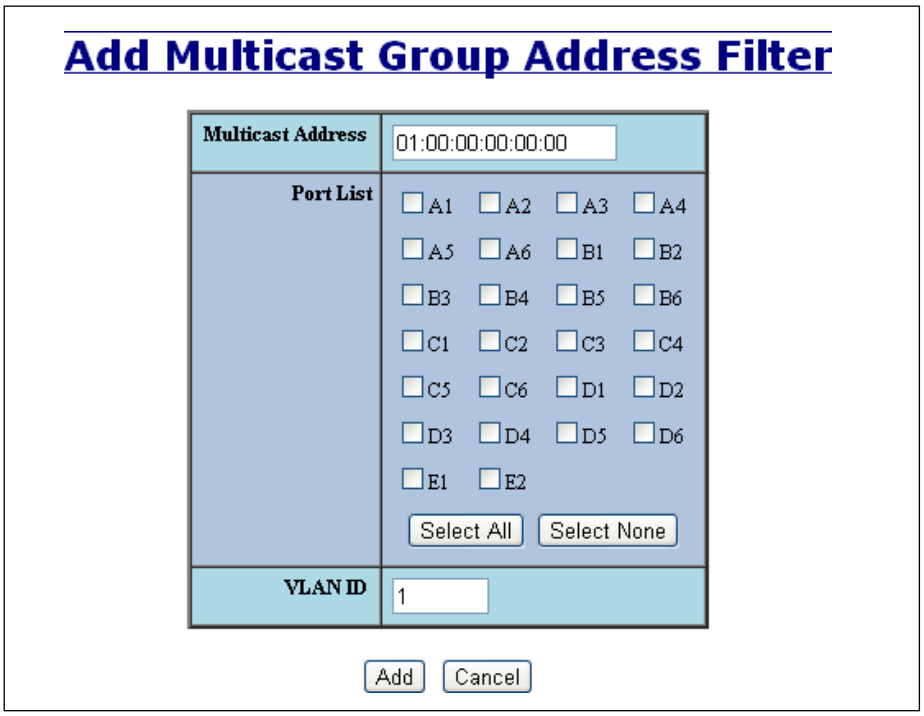
.

Bridging – Multicast Addresses

The Multicast Addresses tab under the Bridging category will display a list of Multicast Group Addresses that are associated with respective port numbers. This may be used to statically assign a Multicast Group Address access to a group of ports on the switch.



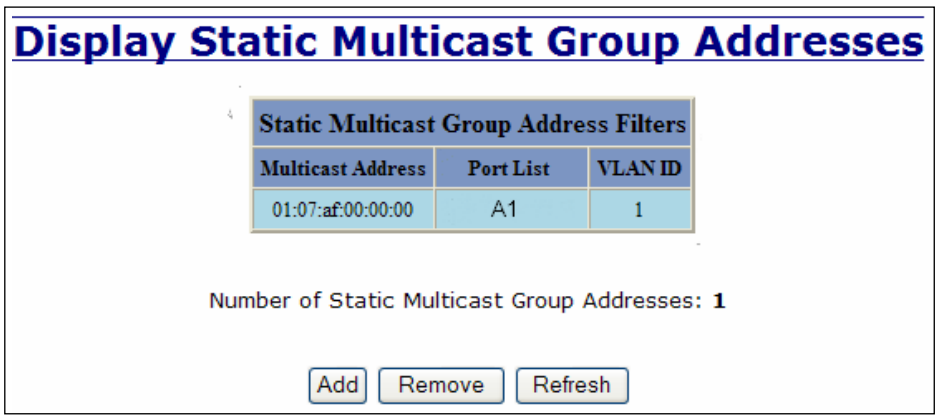
Following the Add button on the page above, the administrator must enter a valid Multicast Group Address and associate it with a port number or list on the switch. Once the administrator clicks on the Add button, the changes will take effect instantly.



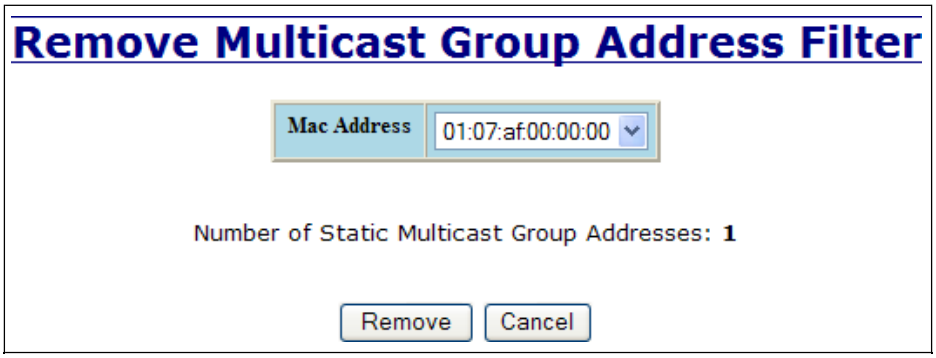
Note: *If there are multiple ports on different VLANs, the 7900 will apply the static multicast address to the lowest VLAN-ID that is associated with one of the ports assigned to the static multicast address. So if the lowest VLAN-ID contains all the ports assigned to the static multicast address (an umbrella VLAN), it will function for all those ports with no problems. This can be achieved with overlapping VLANs.*

Bridging – Multicast Addresses Continued…

After adding a Multicast Group Address, it will appear on the main list and will show the associated ports that go along with that address.



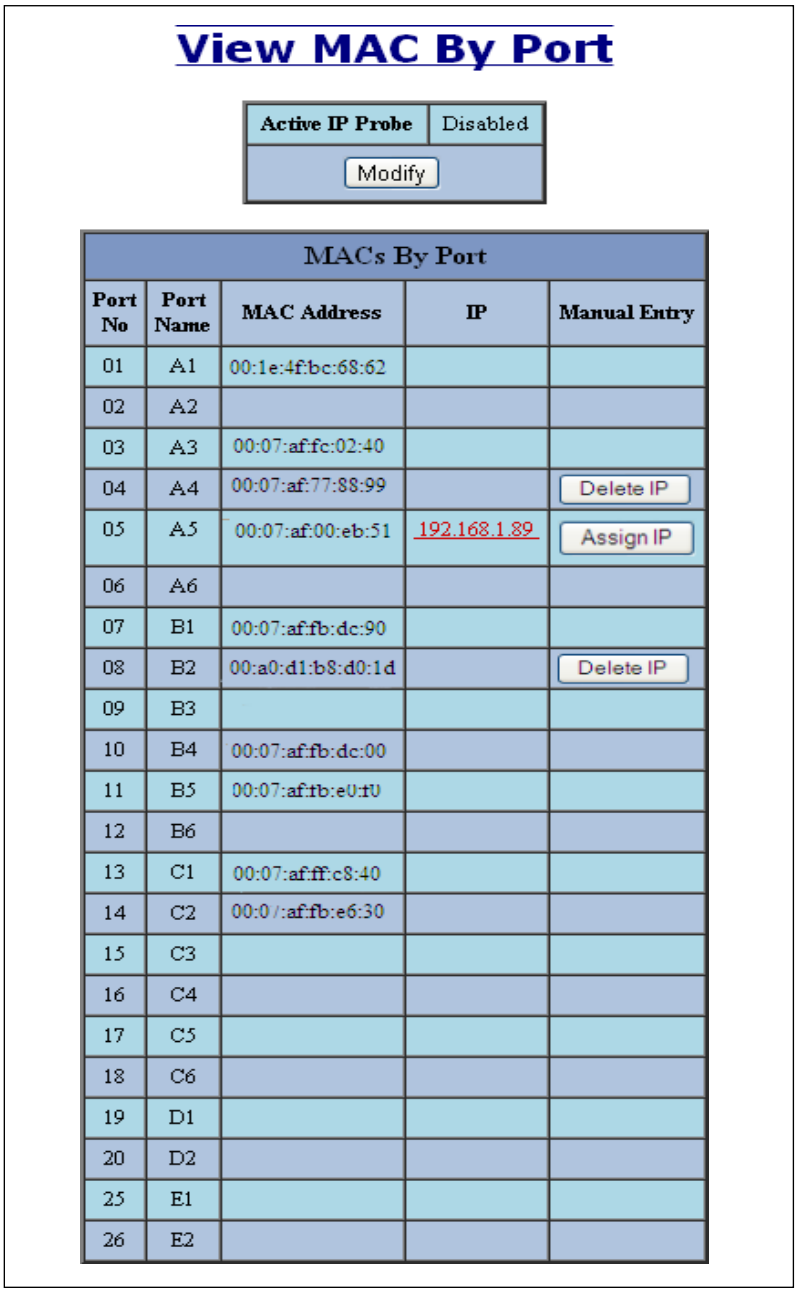
Following the Remove button on the example above, the administrator will be presented with a list of Multicast Group Addresses that are configured on the switch. Using the pull-down menu, the administrator should select the desired address to be removed. Then click on the Remove button at the bottom of the page.



Note: *If there are multiple ports on different VLANs, the 7900 will apply the static multicast address to the lowest VLAN-ID that is associated with one of the ports assigned to the static multicast address. So if the lowest VLAN-ID contains all the ports assigned to the static multicast address (an umbrella VLAN), it will function for all those ports with no problems. This can be achieved with overlapping VLANs.*

Bridging – Show MAC by Port

This feature shows the MAC addresses of devices connected to each switch port and the IP Addresses associated with the MACs. The browser page 'View MAC by Port' shows the MAC for the device found on each port, and the IP for the MAC presented if available. If more than one device is on that port, then the lowest alphanumeric of those MAC addresses is shown and underlined.



View MAC By Port

Active IP Probe	Disabled
Modify	

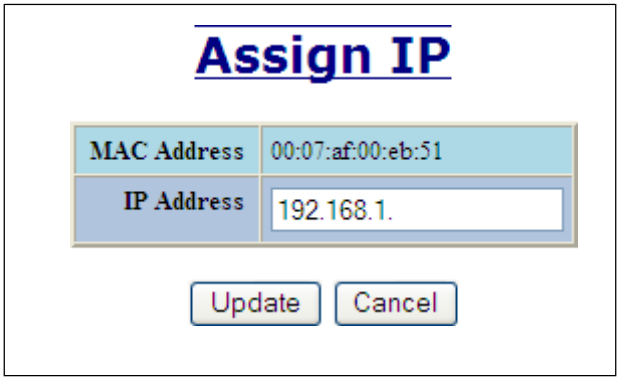
MACs By Port

Port No	Port Name	MAC Address	IP	Manual Entry
01	A1	00:1e:4f:bc:68:62		
02	A2			
03	A3	00:07:af:fc:02:40		
04	A4	00:07:af:77:88:99		Delete IP
05	A5	00:07:af:00:eb:51	192.168.1.89	Assign IP
06	A6			
07	B1	00:07:af:fb:dc:90		
08	B2	00:a0:d1:b8:d0:1d		Delete IP
09	B3			
10	B4	00:07:af:fb:dc:00		
11	B5	00:07:af:fb:e0:f0		
12	B6			
13	C1	00:07:af:ff:c8:40		
14	C2	00:0 /:af:fb:e6:30		
15	C3			
16	C4			
17	C5			
18	C6			
19	D1			
20	D2			
25	E1			
26	E2			

The 'Active IP Probe' field is configurable using the 'Modify' button, and also displays the existing Enabled or Disabled status of this feature. The default is disabled. When disabled the switch generates no Ethernet traffic for this purpose, but can still present some information gathered passively. The 'IP' field shows an Auto-detected or manually entered IP address. If there is a MAC address for the port and an IP address was not discovered there is an 'Assign IP' button to allow the user to enter an IP address.
If 'Active IP Probe' is enabled, manually entered IP values are underlined and validated. A validated IP for that MAC is presented in green and if validation fails the IP will be red and underlined. Note that some

devices do not have an IP Address, and that some devices that do have an IP Address may not respond to the methods used to detect their IP Address.

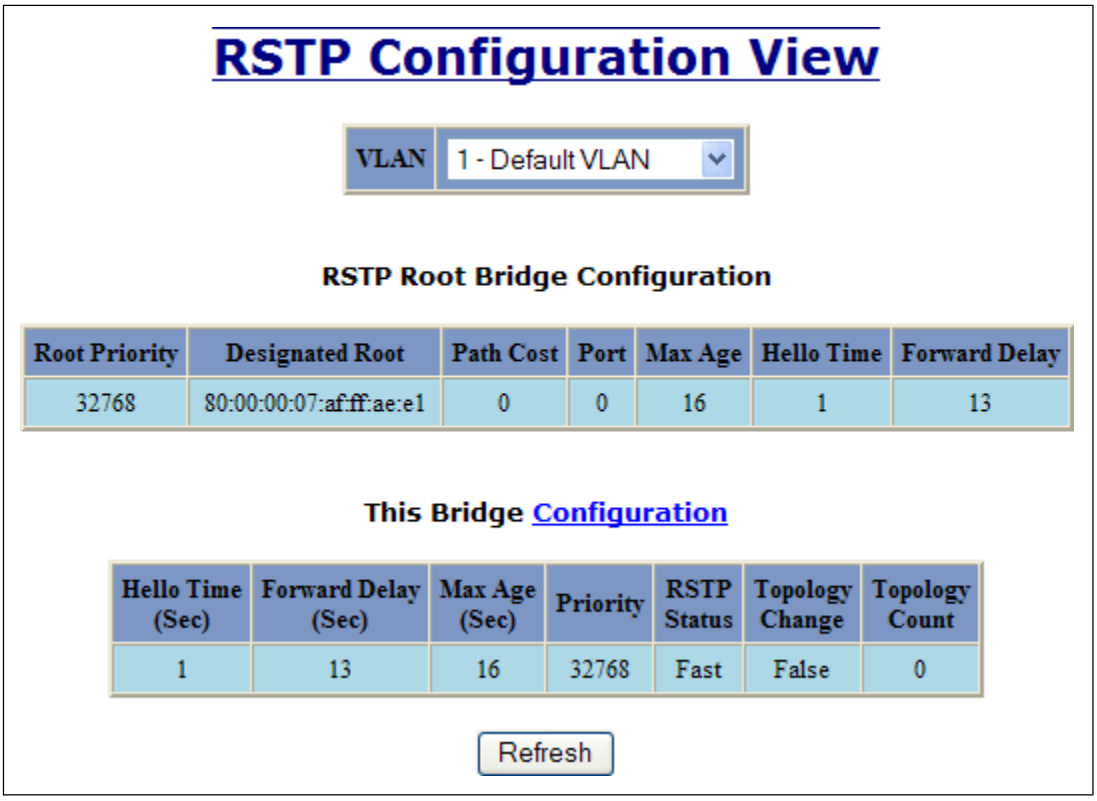
Invoking the ‘Assign IP’ button on the example above, the administrator will be presented with a form in which to enter a manually assigned IP, as below:



When an IP has been manually entered a button is provided to ‘Delete IP’, and invoking it will allow the administrator to delete the manual association of an IP to that MAC.

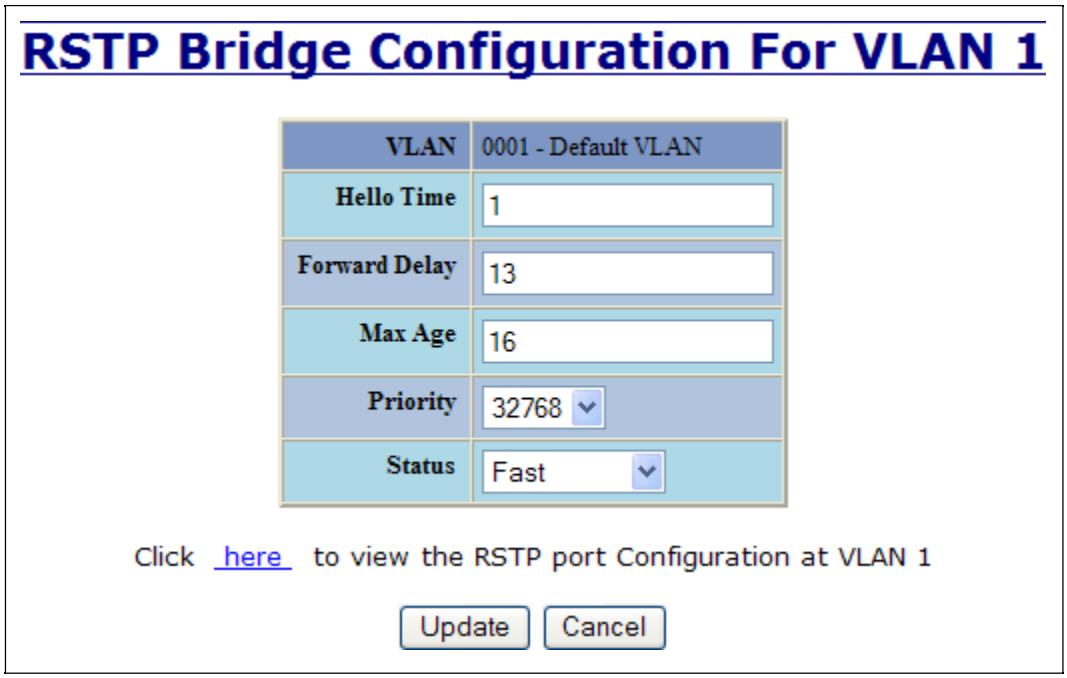
RSTP – Configuration

The Configuration tab under the RSTP category will display the RSTP information for the first VLAN. Using the pull-down menu at the top of the page an administrator can choose which VLAN to configure RSTP on. Once the VLAN is selected, the administrator may configure the bridge by clicking on the 'Configuration' link in the middle of the page.



RSTP – Configuration Continued…

The configuration screen for the VLAN that was previously selected will look like the example below. Here the administrator can make changes such as the Hello Time, Forward Delay, Max Age, Priority, and the Status of RSTP on that VLAN. The administrator or user can see the current RSTP status of the ports on that VLAN by clicking on the 'here' link to view RSTP Port Configuration at VLAN#.



Note: *It is recommended that RSTP rings consist of RSTP capable switches.*
Trunking must be disabled in order to use RSTP.
Do not create redundant links unless either RSTP or N-Ring is enabled.
RSTP on overlapping VLANs is not supported and the system will automatically disable RSTP on all but the lowest VID VLANs that have overlapping ports.

RSTP – Configuration Continued…

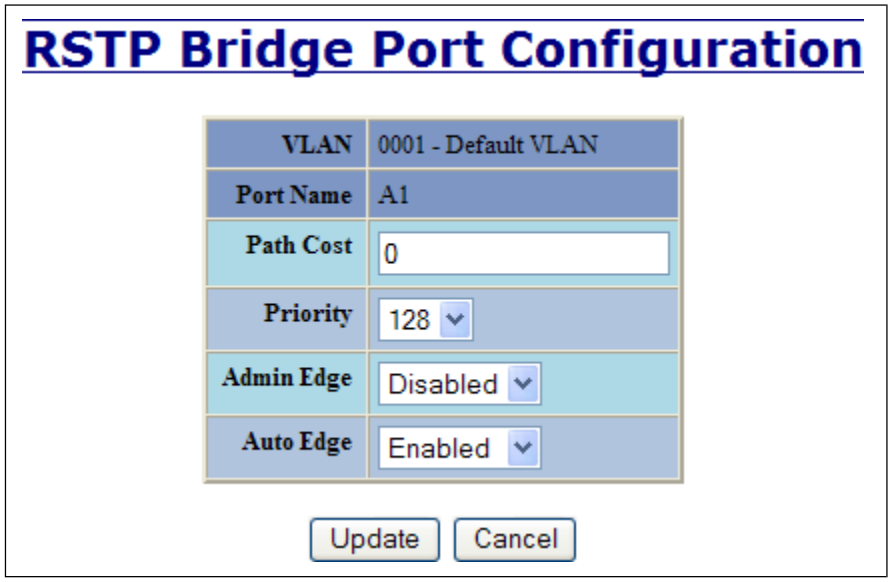
Following the link for the view RSTP Port Configuration at VLAN#, the administrator or user can see the current RSTP status of the ports on that VLAN. This will show information such as the Path Cost and the Port State. If the switch sees a redundant path it will put the port with the highest Path Cost into Blocking mode where it will discard packets coming in on that port. In the example below, A3 is a redundant port with port A2, therefore A2 is forwarding and A3 is discarding.

RSTP Configuration View For VLAN 1

Bridge Port Configuration									
Port No	Port Name	Port State	Path Cost	Priority	STP BPDU	Auto Edge	Admin Edge	Designated Bridge	Designated Port
01	A1	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:01
02	A2	Forwarding	200000	128	No	Enabled	Disabled	80:00:00:07:af:ff:9c:e1	00:02
03	A3	Discarding	200000	128	No	Enabled	Disabled	80:00:00:07:af:ff:9c:e1	00:03
04	A4	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:04
05	A5	Forwarding	200000	128	No	Enabled	Disabled	80:00:00:07:af:7d:ad:01	00:05
06	A6	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:06
07	B1	Forwarding	200000	128	No	Enabled	Disabled	80:00:00:07:af:ff:9c:e1	00:07
08	B2	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:08
09	B3	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:09
10	B4	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0a
11	B5	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0b
12	B6	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0c
13	C1	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0d
14	C2	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0e
15	C3	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0f
16	C4	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:10
17	C5	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:11
18	C6	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:12
19	D1	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:13
20	D2	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:14
25	E1	Disabled	20000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:19
26	E2	Disabled	20000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:1a

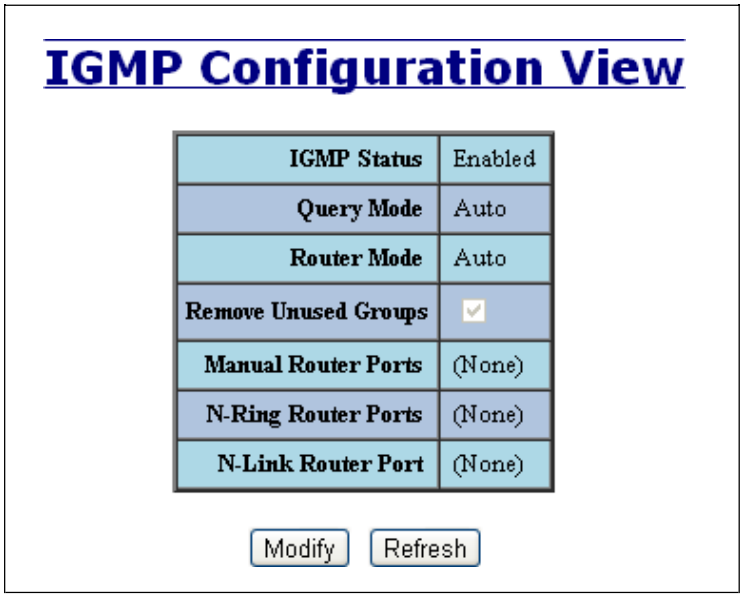
<< Back Refresh

If the administrator selects one of the ports on the previous screen, he or she can change the Port's Path Cost, Priority, and the status of Admin Edge and Auto Edge.

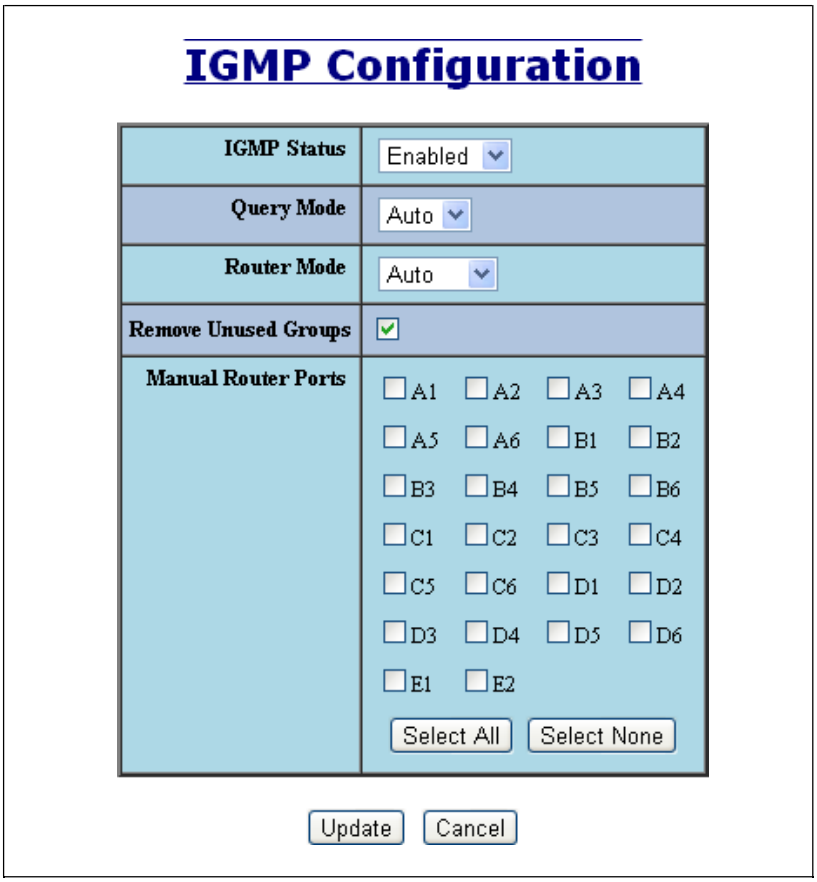


IGMP – Configuration

The Configuration tab under the IGMP category will display the IGMP basic configuration settings. By default, IGMP is enabled.

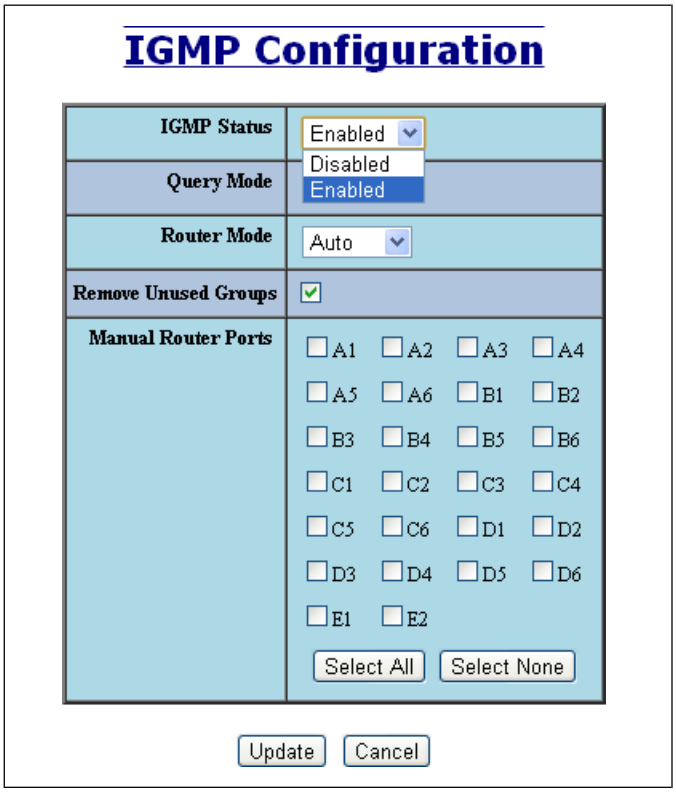


Following the Modify button, the administrator will see a list of configurable fields for the IGMP configuration. Once these fields are filled in to meet the needs of the administrator's network, the changes may be updated by clicking the Update button at the bottom of the page.

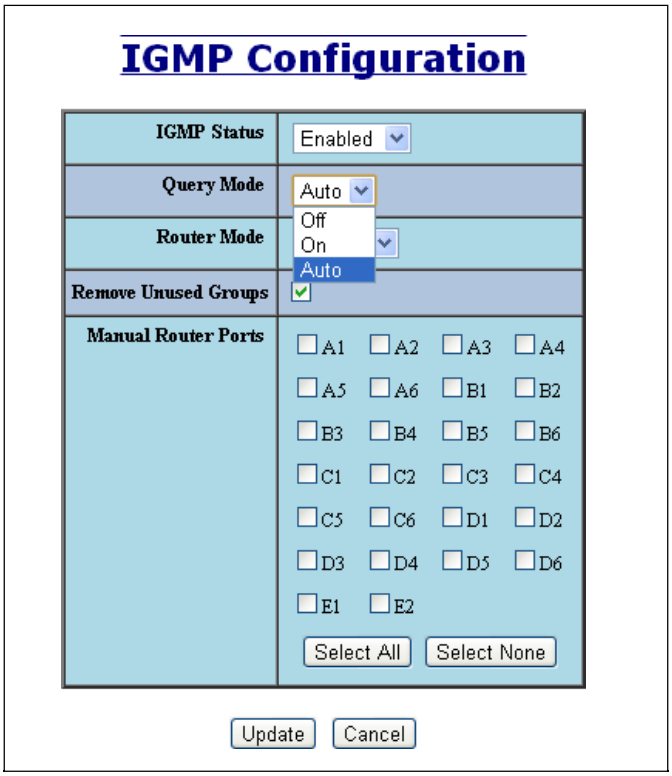


IGMP – Configuration, Continued…

The IGMP Status pull-down allows the user to enable or disable IGMP completely.

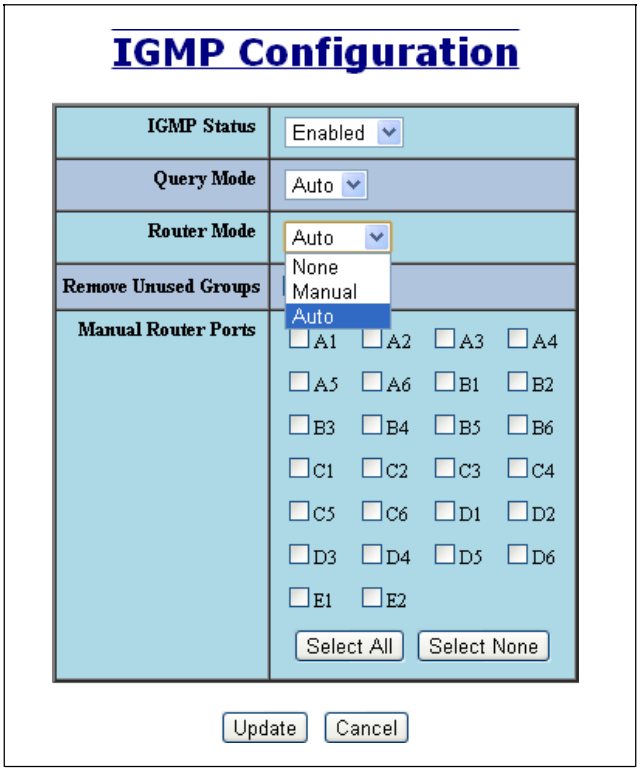


The Query Mode pull-down allows the user to set query mode for Automatic (the default), On (always), or Off (never):

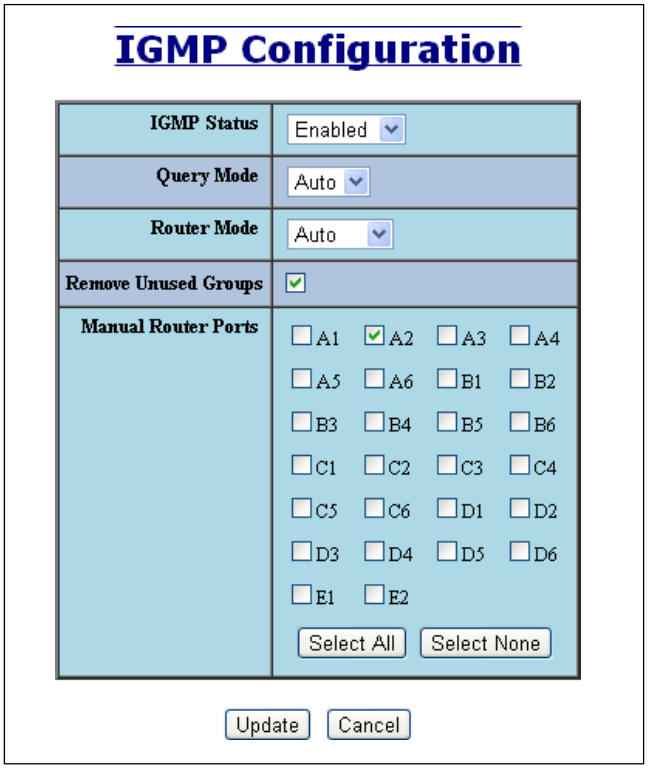


IGMP – Configuration, Continued…

The Router Mode pull-down allows the user to choose router mode. ‘Auto’ allows for dynamically detected and manually set router ports. ‘Manual’ allows only for manually set router ports. ‘None’ allows no router ports.

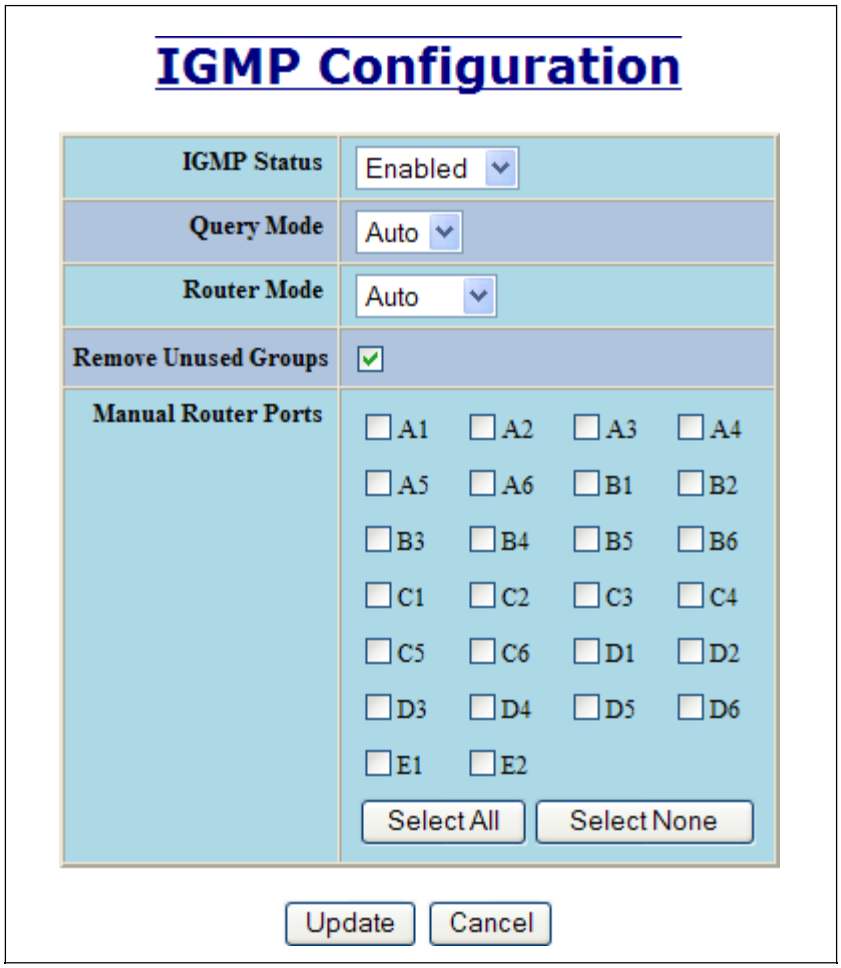


The user can specify the manual router ports:



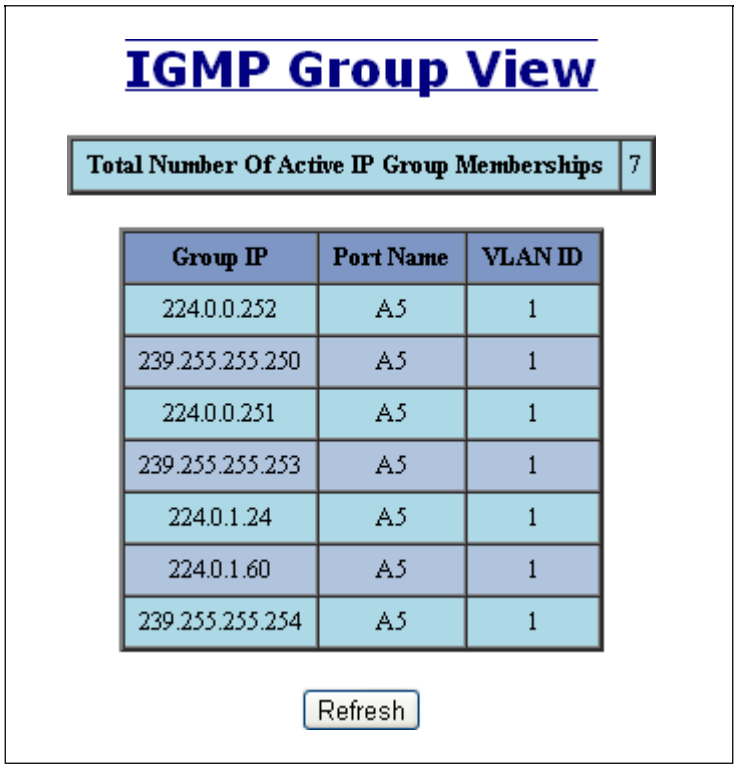
IGMP – Configuration, Continued…

If **Remove Unused Groups** is checked then unused IGMP Groups will be removed and traffic with those multicast addresses will be treated as normal multicast. If unchecked, then unused IGMP Groups are not removed and traffic with those multicast addresses will be limited. The default is checked. Note that IGMP Groups are not retained through a power cycle.

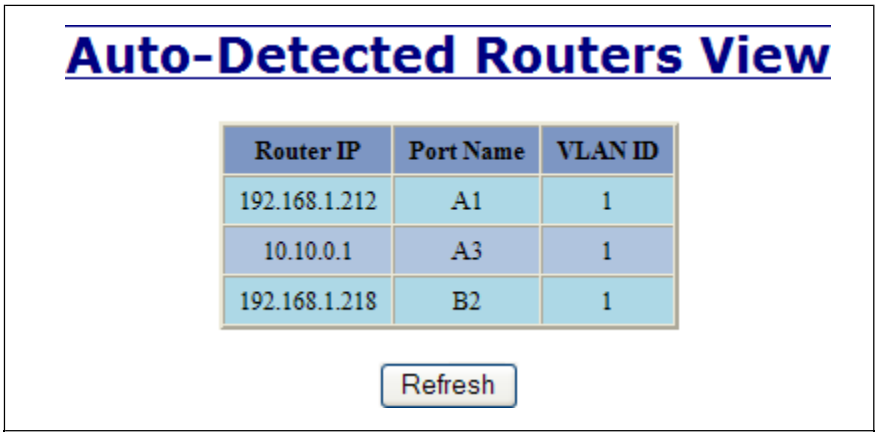


IGMP – Show Group and Show Router

The Show Groups tab under the IGMP category will display a list of IGMP groups based on the Group IP and the port number that it is associated with.



The Show Routers tab under the IGMP category will display a list of Auto-detected Router IPs and the port numbers that they are associated with.



IGMP – RFilter

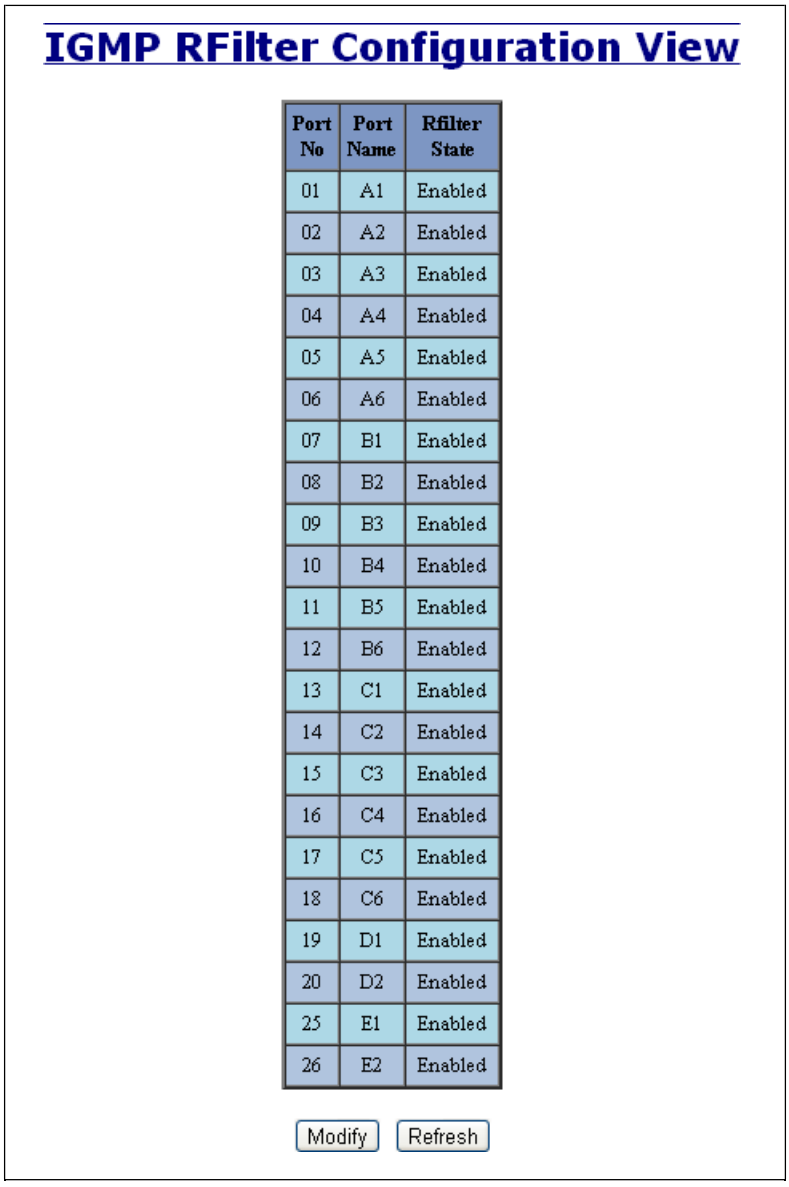
The ‘rfilter’ (**Router Multicast Data Filter**) function allows you to choose whether or not DATA frames with KNOWN group multicast addresses are sent to the ‘router’ ports (links to other switches). Control packets (Join, Leave) will be sent to the router(s) regardless of this setting. “KNOWN” is known from dynamic IGMP Snooping operations.

The factory default is that the Router Multicast Data Filter is enabled for all ports, so any router ports do NOT get DATA frames with KNOWN multicast destination addresses unless a join to a specific multicast address has been received on that port. **Joins override an rfilter.**

If rfilter is disabled, router ports do get DATA frames with KNOWN multicast destination addresses

Rfilter can be set for individual ports: any, all, or none. For each port, rfilter will have an impact only if that port is manually or dynamically chosen as a router port.

Default configuration:



IGMP – RFilter, Continued…

Modifying rfilter port settings:

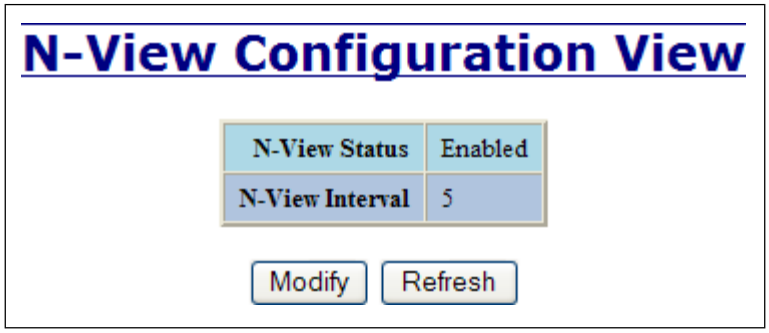
IGMP RFilter Configuration

Port No	Port Name	Rfilter Enabled?
01	A1	☑
02	A2	☑
03	A3	☑
04	A4	☑
05	A5	☑
06	A6	☑
07	B1	☑
08	B2	☑
09	B3	☑
10	B4	☑
11	B5	☑
12	B6	☑
13	C1	☑
14	C2	☑
15	C3	☑
16	C4	☑
17	C5	☑
18	C6	☑
19	D1	☑
20	D2	☑
25	E1	☑
26	E2	☑

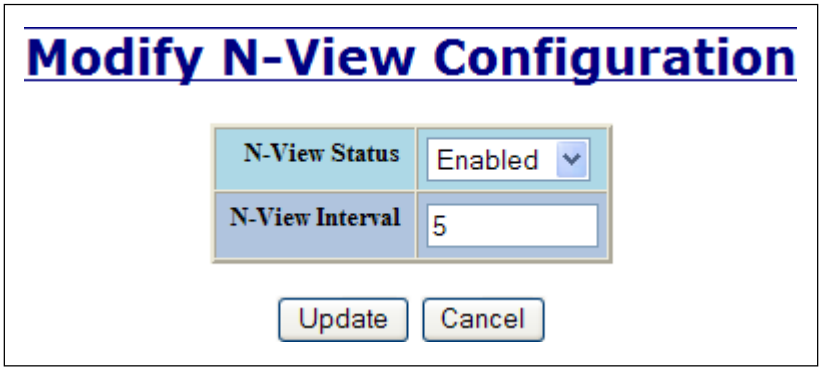
Update Cancel

N-View – Configuration

The Configuration tab under the N-View category will display two basic variables for N-View, the status and the interval between packets.

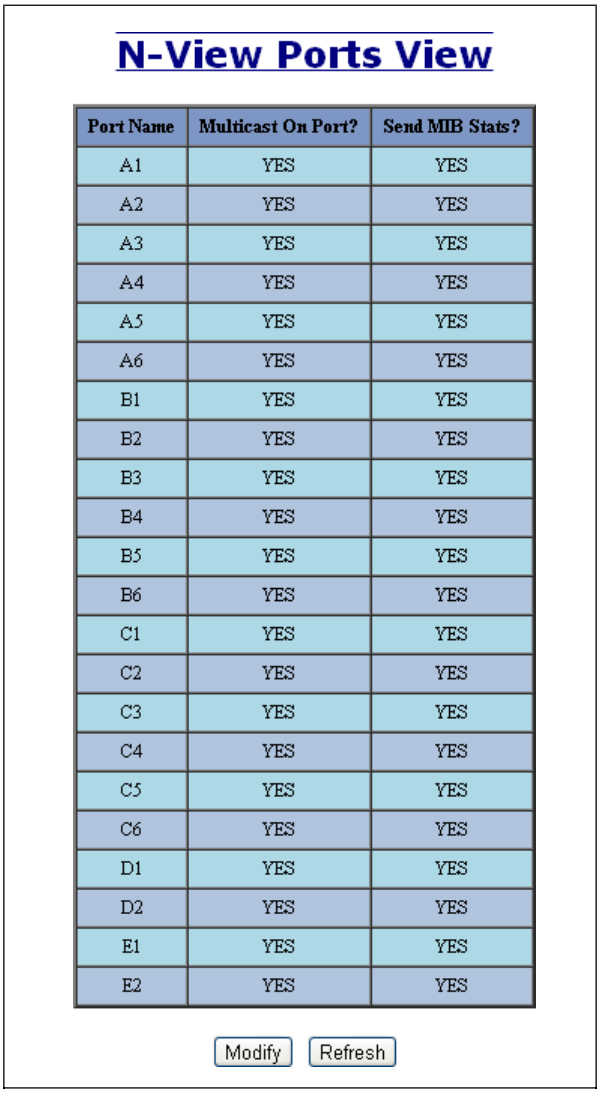


Following the Modify button on the above example, the administrator can modify the variable to change the frequency with which N-View reports information. Increasing the interval will slow the update rate. Decreasing the interval will allow N-View to report more frequently. Additionally, you may Disable or Enable N-View altogether.



N-View – Ports

The Ports tab under the N-View category will display a list of all the configured ports on the 7900 unit along with the ports transmitting multicast packets and MIB stats respectively.



N-View – Ports, Continued…

Following the Modify button on the above example, the administrator can modify these two variables to enable or disable multicast out of the port and if MIB stats are sent out for those ports.

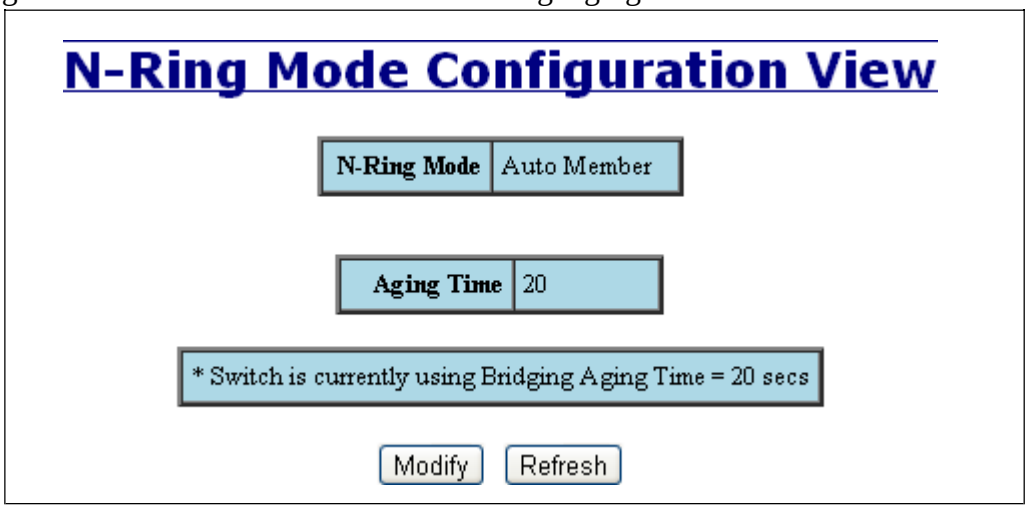
Modify N-View Ports

Port Name	Multicast On Port?	Send MIB Stats?
A1	☑	☑
A2	☑	☑
A3	☑	☑
A4	☑	☑
A5	☑	☑
A6	☑	☑
B1	☑	☑
B2	☑	☑
B3	☑	☑
B4	☑	☑
B5	☑	☑
B6	☑	☑
C1	☑	☑
C2	☑	☑
C3	☑	☑
C4	☑	☑
C5	☑	☑
C6	☑	☑
D1	☑	☑
D2	☑	☑
E1	☑	☑
E2	☑	☑

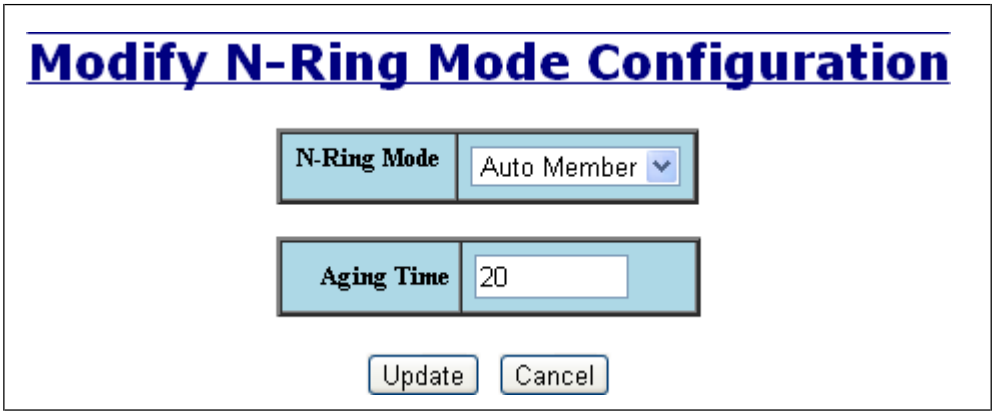
Update Cancel

N-Ring – Configuration

The Configuration tab under the N-Ring category will display the N-Ring basic configuration settings. By default, N-Ring is in Auto Member mode and the N-Ring Aging Time is 20 seconds.



Following the Modify button on the above example, the administrator will see a list of configurable fields for the N-Ring configuration, as below.



The N-Ring Aging Time has a default of 20 seconds and is separate from the Bridging Aging Time. N-Ring Aging Time is used when the switch is an N-Ring Manager or becomes an active N-Ring Member, and in either case N-Ring status includes for example:

"Switch is currently using N-Ring Aging Time = 20 Seconds"

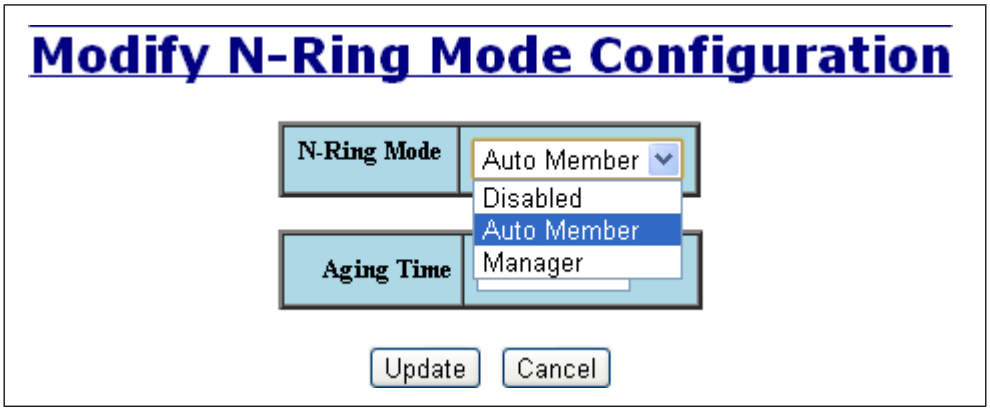
Once these fields are filled in to meet the needs of the administrator's network, the changes may be saved by clicking the Update button at the bottom of the page.

NOTES:

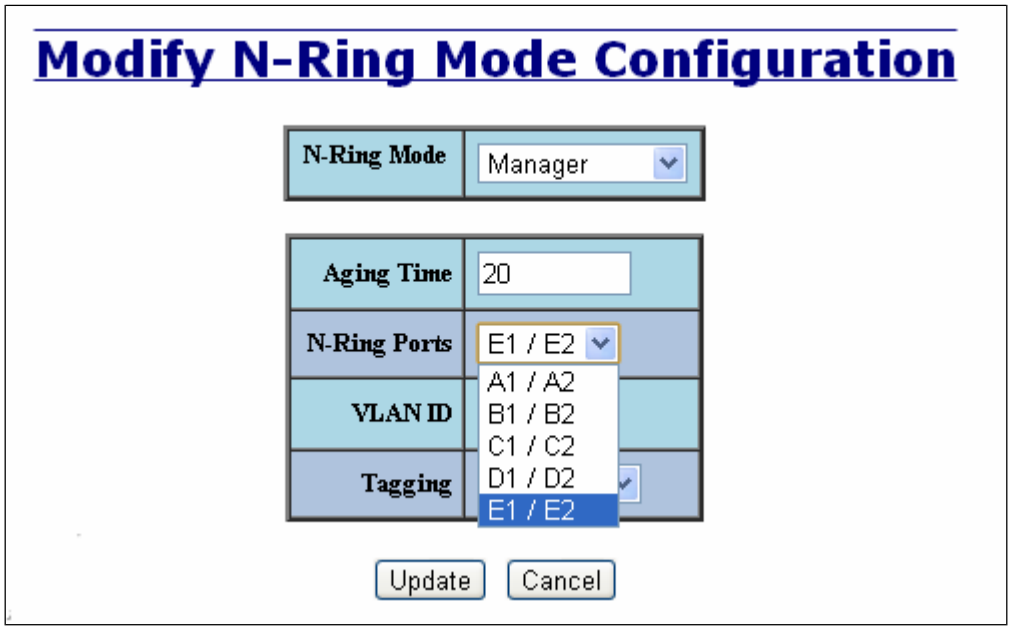
1. ***N-Ring Manager cannot have RSTP or Trunking enabled.***
2. ***RSTP & N-Ring are different modes and cannot share links or segments along those lines. See the examples in the RSTP configuration section.***
3. ***Do not use Trunking on an N-Ring manager. Do not connect the N-Ring to actively Trunking ports on an Auto Member.***
4. ***Do not create redundant links unless either RSTP or N-Ring is enabled.***
5. ***Any one 7900 can only participate in one N-Ring.***
6. ***N-Ring copper ports must be run at 100Mb full duplex, including the default 'autonegotiate' as long as all switches in the ring support 100Mb full duplex.***

N-Ring – Configuration, Continued…

The “N-Ring Mode” is one of three, as below:



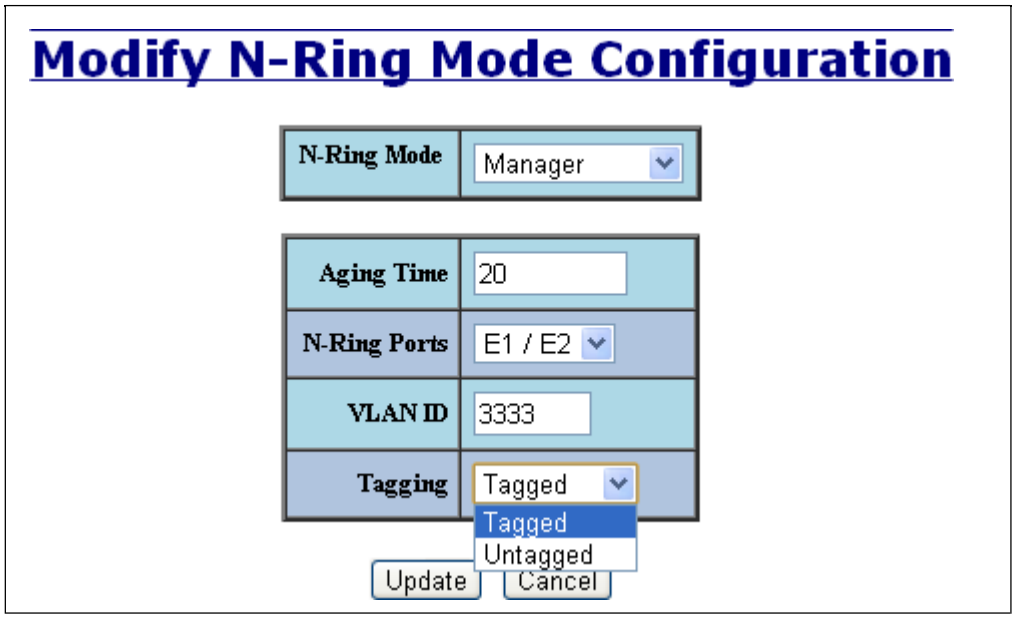
If N-Ring Mode is “Manager”, then a pull-down allows selection as available of ports A1/A2, B1/B2, C1/C2, D1/D2, or E1/E2 as N-Ring ports.



N-Ring – Configuration, Continued…

If N-Ring Mode is "Manager", then VLAN ID can be set to a unique VLAN id (1 ~ 4094). Default is 3333.

If N-Ring Mode is "Manager", then a pull-down allows selection as to whether the N-Ring ports are members of the VLAN's Tagged or Untagged ports. Default is Tagged.



Once these fields are filled in to meet the needs of the administrator's network, the changes may be saved by clicking the Update button at the bottom of the page.

NOTES:

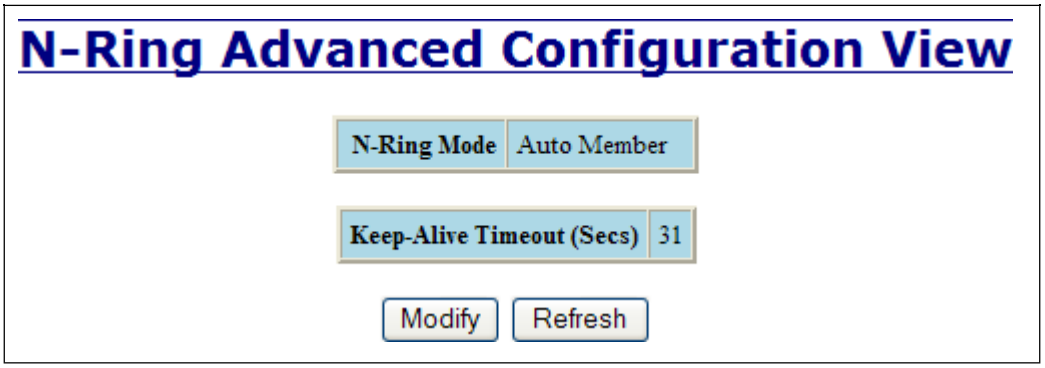
1. ***Since VLANs are implemented for security reasons as well as traffic flow, N-Ring only makes minimal changes. It is up to the administrator to ensure that VLANs are configured correctly on the N-Ring manager and all N-Ring members.***
2. ***When the N-Ring manager and all N-Ring Members are in defaults, changing the N-Ring manager to use a Tagged VLAN requires no user interaction to allow non-ring traffic to pass through the ring. This works because changing to a Tagged VLAN does not remove the ring ports from the default VLAN.***
3. ***When the N-Ring manager and all N-Ring Members are in defaults, changing the N-Ring manager to use an Untagged VLAN other than VID 1, requires the administrator to add non-ring ports to the N-Ring VLAN to allow non-ring traffic to pass through the ring. This occurs because the N-Ring ports must be removed from VID 1 because an untagged port may only be a member of one VLAN.***

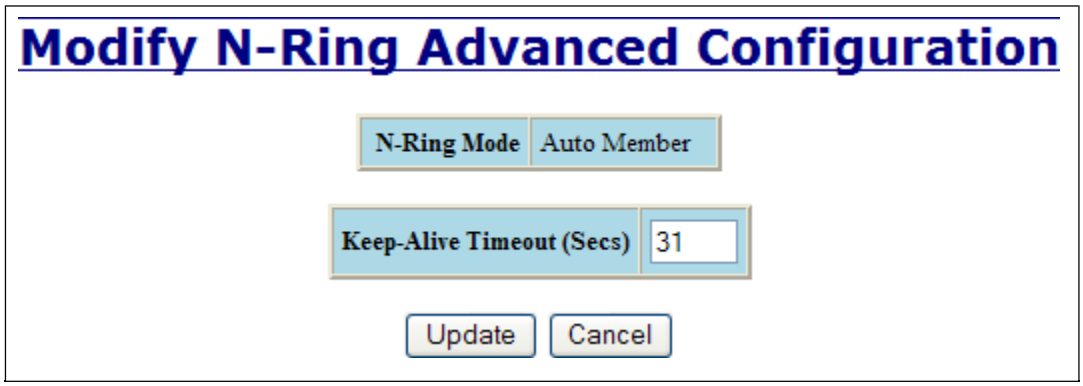
N-Ring – Advanced Configuration

If switch is an N-Ring Member, the following data will be shown:

N-Ring Mode
Current N-Ring mode of switch.

Keep-Alive Timeout:
Keep-Alive timeout is used when switch is active in an N-Ring. The range is **5-1000000** seconds.





If switch is an N-Ring Manager, the following advanced configuration data will be shown:

N-Ring Mode
Current N-Ring mode of switch.

Self Health Packet Interval:
The amount of time to wait in milliseconds before sending Self-Health packets. The default is 10.

Maximum Missed Packets
The number of missed Self-Health packets that constitute a fault. The default is 2.

Sign-On Delay
The amount of time to wait in milliseconds before requesting initial sign-on information from ring members. The default is 1000.

Sign-On Match Packets
The number of times the switch count must match before starting the sign-on process. The default is 3.

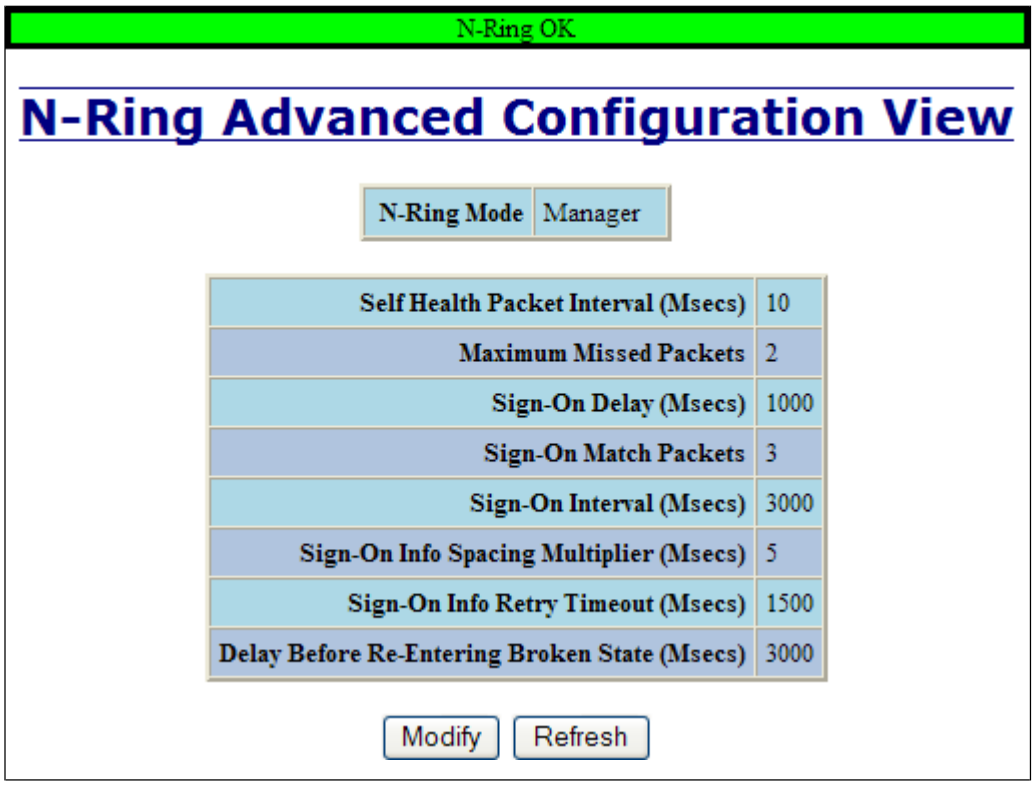
Sign-On Interval
The interval of time to wait in milliseconds before requesting subsequent sign-on information from ring members when the ring is broken. The default is 3000.

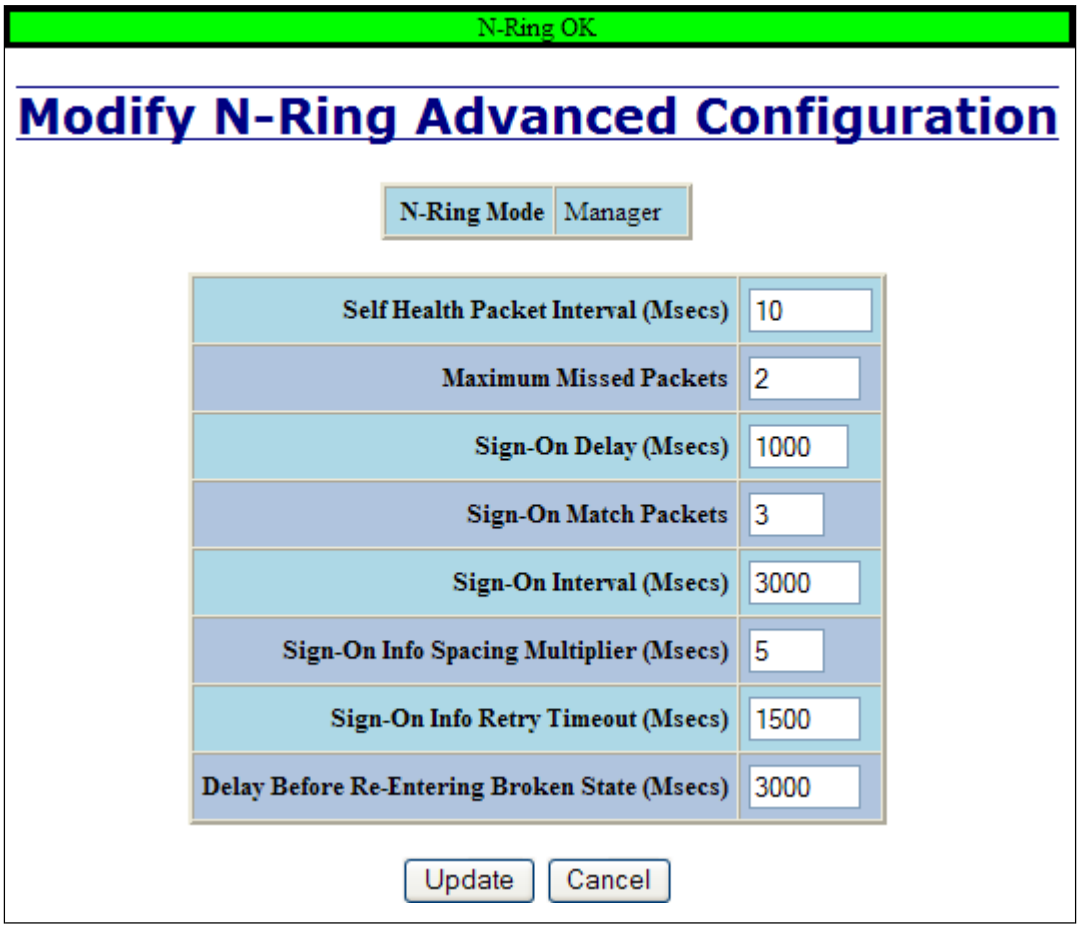
Sign-On Info Spacing Multiplier
The amount of time to wait in milliseconds, scaled by switch number, before sending information to the ring manager. The default is 5.

Sign-On Info Retry Timeout
The amount of time the ring member will wait in milliseconds for the ring manager to acknowledge receipt of the member's information before the member tries to re-send the information. The default is 1500.

Delay Before Re-Entering Broken State
The amount of time, in milliseconds, that must elapse before the ring is allowed to go back into the broken state. The default is 3000.

N-Ring – Advanced Configuration, Continued…

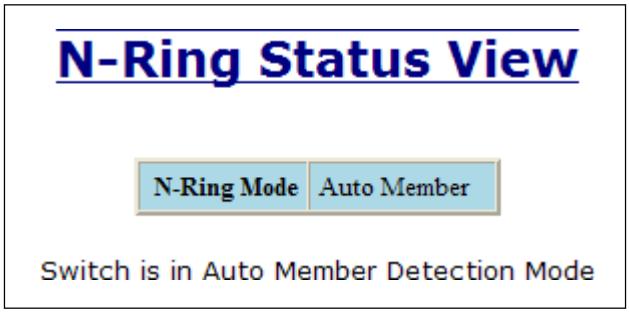

N-Ring OK
N-Ring Advanced Configuration View
N-Ring Mode
Manager
Self Health Packet Interval (Msecs)
10
Maximum Missed Packets
2
Sign-On Delay (Msecs)
1000
Sign-On Match Packets
3
Sign-On Interval (Msecs)
3000
Sign-On Info Spacing Multiplier (Msecs)
5
Sign-On Info Retry Timeout (Msecs)
1500
Delay Before Re-Entering Broken State (Msecs)
3000
Modify
Refresh


N-Ring OK
Modify N-Ring Advanced Configuration
N-Ring Mode
Manager
Self Health Packet Interval (Msecs)
10
Maximum Missed Packets
2
Sign-On Delay (Msecs)
1000
Sign-On Match Packets
3
Sign-On Interval (Msecs)
3000
Sign-On Info Spacing Multiplier (Msecs)
5
Sign-On Info Retry Timeout (Msecs)
1500
Delay Before Re-Entering Broken State (Msecs)
3000
Update
Cancel

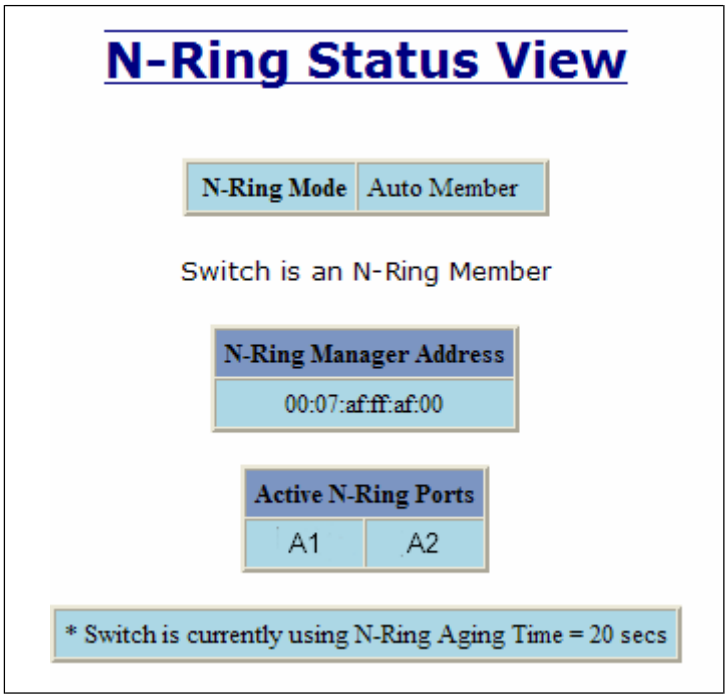
N-Ring – Status

The Status tab under the N-Ring category will display the N-Ring status.

Below is an example of N-Ring Status from a switch in defaults (N-Ring Auto Member) that is not an N-Ring Manager and has not become an “Active” N-Ring Member:



Below is an example of N-Ring Status from an “Active” N-Ring Member:



N-Ring – Status, Continued…

Below is an example of N-Ring Status from an N-Ring Manager with a healthy N-Ring:

N-Ring OK

N-Ring Status View

Switch is an N-Ring Manager, using N-Ring Aging Time = 20 Seconds

Refresh every 6 secs.

12 Active Members Detected In Current N-Ring (12 reporting)

Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	00:07:af:ff:e4:a0	192.168.1.227	255.255.255.0	N-TRON Switch	A2 A1
1	00:07:af:ff:ef:60	192.168.1.224	255.255.255.0	N-TRON Switch	A2 A1
2	00:07:af:ff:e6:a0	192.168.1.217	255.255.255.0	N-TRON Switch	A2 A1
3	00:07:af:ff:ef:80	192.168.1.221	255.255.255.0	N-TRON Switch	A2 A1
4	00:07:af:ff:e4:c0	192.168.1.241	255.255.255.0	N-TRON Switch	A2 A1
5	00:07:af:ff:d5:e0	192.168.1.229	255.255.255.0	N-TRON Switch	A2 A1
6	00:07:af:ff:d7:00	192.168.1.228	255.255.255.0	N-TRON Switch	A2 A1
7	00:07:af:ff:e6:c0	192.168.1.223	255.255.255.0	N-TRON Switch	A2 A1
8	00:07:af:ff:d5:20	192.168.1.231	255.255.255.0	N-TRON Switch	A2 A1
9	00:07:af:ff:e5:e0	192.168.1.238	255.255.255.0	N-TRON Switch	A2 A1
10	00:07:af:ff:e3:c0	192.168.1.239	255.255.255.0	N-TRON Switch	A2 A1
11	00:07:af:ff:d5:40	192.168.1.230	255.255.255.0	N-TRON Switch	A2 A1
12	00:07:af:ff:e3:e0	192.168.1.215	255.255.255.0	N-TRON Switch	A2 A1

N-Ring – Status, Continued…

Below is an example of N-Ring Status from an N-Ring Manager with a faulted N-Ring. The red fields on the N-Ring Map show problems. Ports that are red indicate that the port is not linked. MAC addresses that are red indicate that there is no communication to that switch. The red "Ring Broken" line shows where the N-Ring is broken.

N-Ring OK

N-Ring Status View

Switch is an N-Ring Manager, using N-Ring Aging Time = 20 Seconds

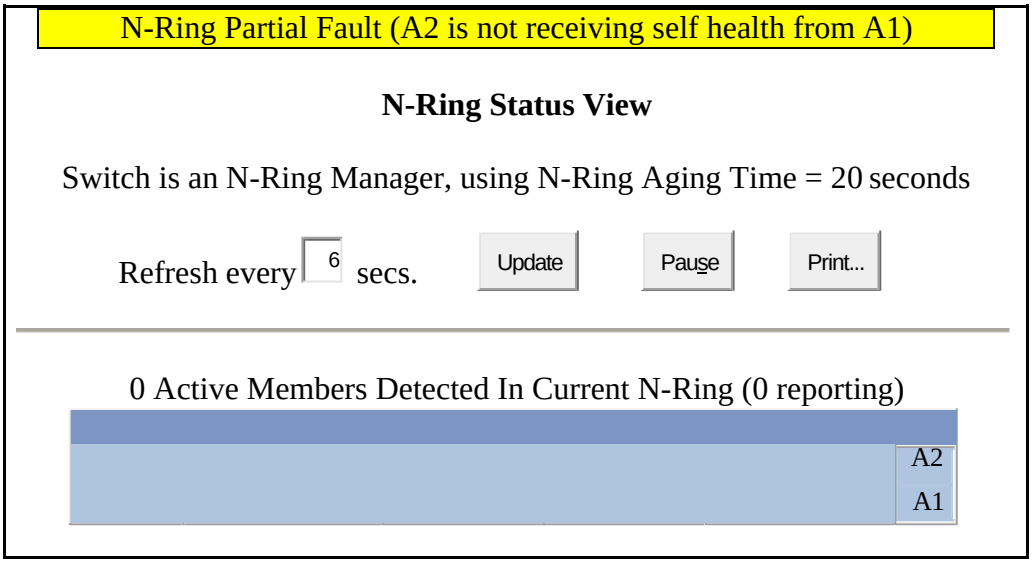
Refresh every 6 secs. Update Pause Print...

12 Active Members Detected In Current N-Ring (12 reporting)

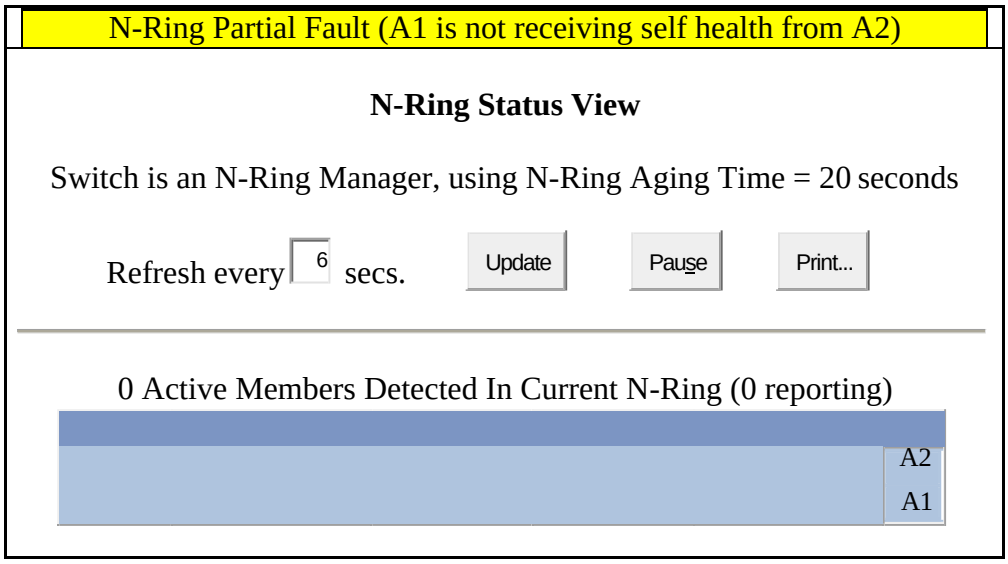
Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	00:07:af:ff:e4:a0	192.168.1.227	255.255.255.0	N-TRON Switch	A2 A1
1	00:07:af:ff:ef:60	192.168.1.224	255.255.255.0	N-TRON Switch	A2 A1
2	00:07:af:ff:e6:a0	192.168.1.217	255.255.255.0	N-TRON Switch	A2 A1
3	00:07:af:ff:ef:80	192.168.1.221	255.255.255.0	N-TRON Switch	A2 A1
4	00:07:af:ff:e4:c0	192.168.1.241	255.255.255.0	N-TRON Switch	A2 A1
5	00:07:af:ff:d5:e0	192.168.1.229	255.255.255.0	N-TRON Switch	A2 A1
6	00:07:af:ff:d7:00	192.168.1.228	255.255.255.0	N-TRON Switch	A2 A1
7	00:07:af:ff:e6:c0	192.168.1.223	255.255.255.0	N-TRON Switch	A2 A1
8	00:07:af:ff:d5:20	192.168.1.231	255.255.255.0	N-TRON Switch	A2 A1
9	00:07:af:ff:e5:e0	192.168.1.238	255.255.255.0	N-TRON Switch	A2 A1
10	00:07:af:ff:e3:c0	192.168.1.239	255.255.255.0	N-TRON Switch	A2 A1
11	00:07:af:ff:d5:40	192.168.1.230	255.255.255.0	N-TRON Switch	A2 A1
12	00:07:af:ff:e3:e0	192.168.1.215	255.255.255.0	N-TRON Switch	A2 A1

N-Ring – Status, Continued…

In rare cases an N-Ring can have a "Partial Fault". An example of this is to have a break in just one fiber in a duplex channel fiber pair. The screenshot below shows N-Ring Manager Status when a 'Higher' N-Ring Port (A2 or E2) is not receiving self health frames all the way around the N-Ring, though the other (low A1/E1) N-Ring port is:



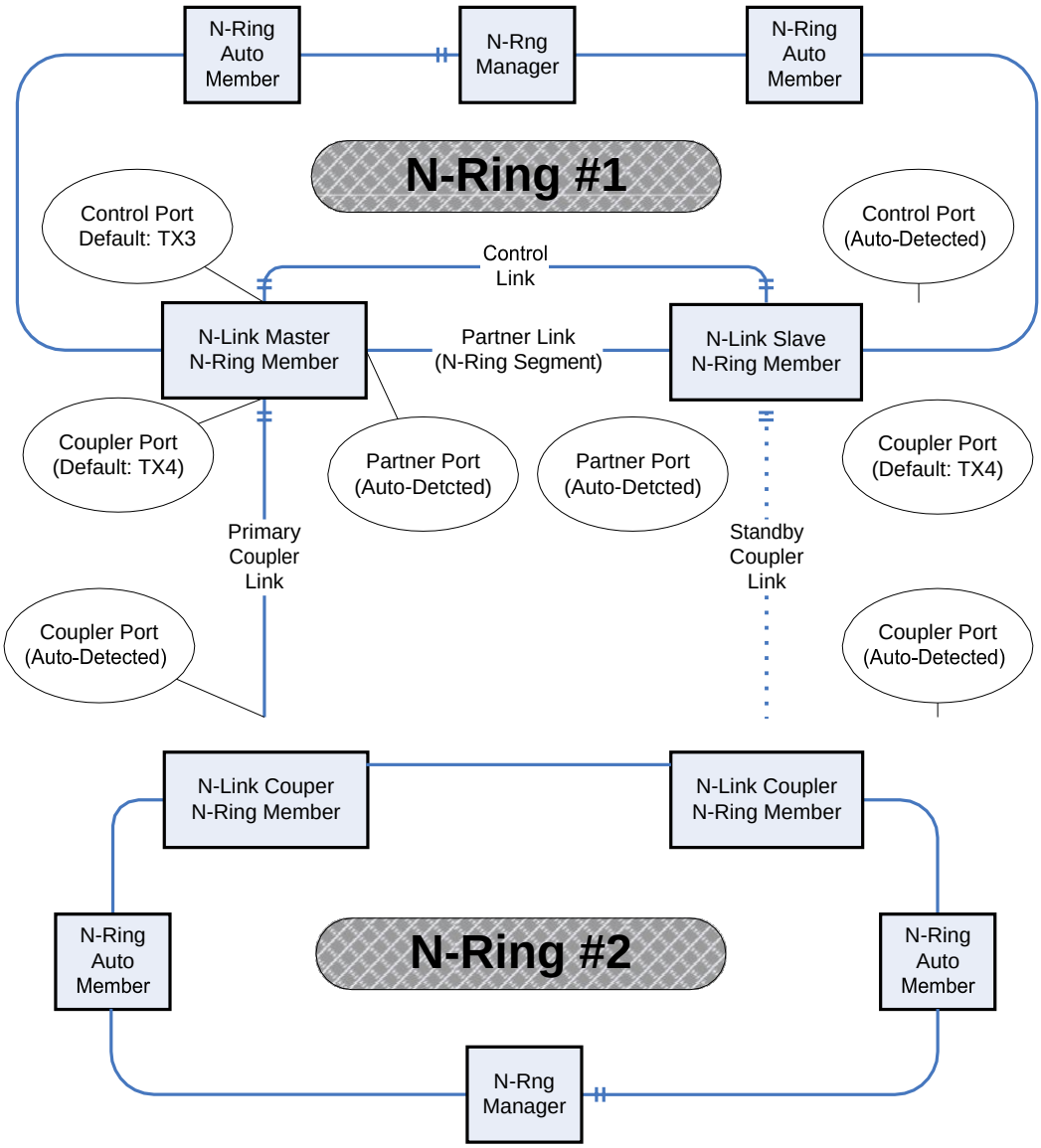
The screenshot below shows N-Ring Manager Status when a 'Lower' N-Ring Port (A1 or E1) is not receiving self health frames all the way around the N-Ring, though the other (high A2/E2) N-Ring port is:



N-Link – Configuration

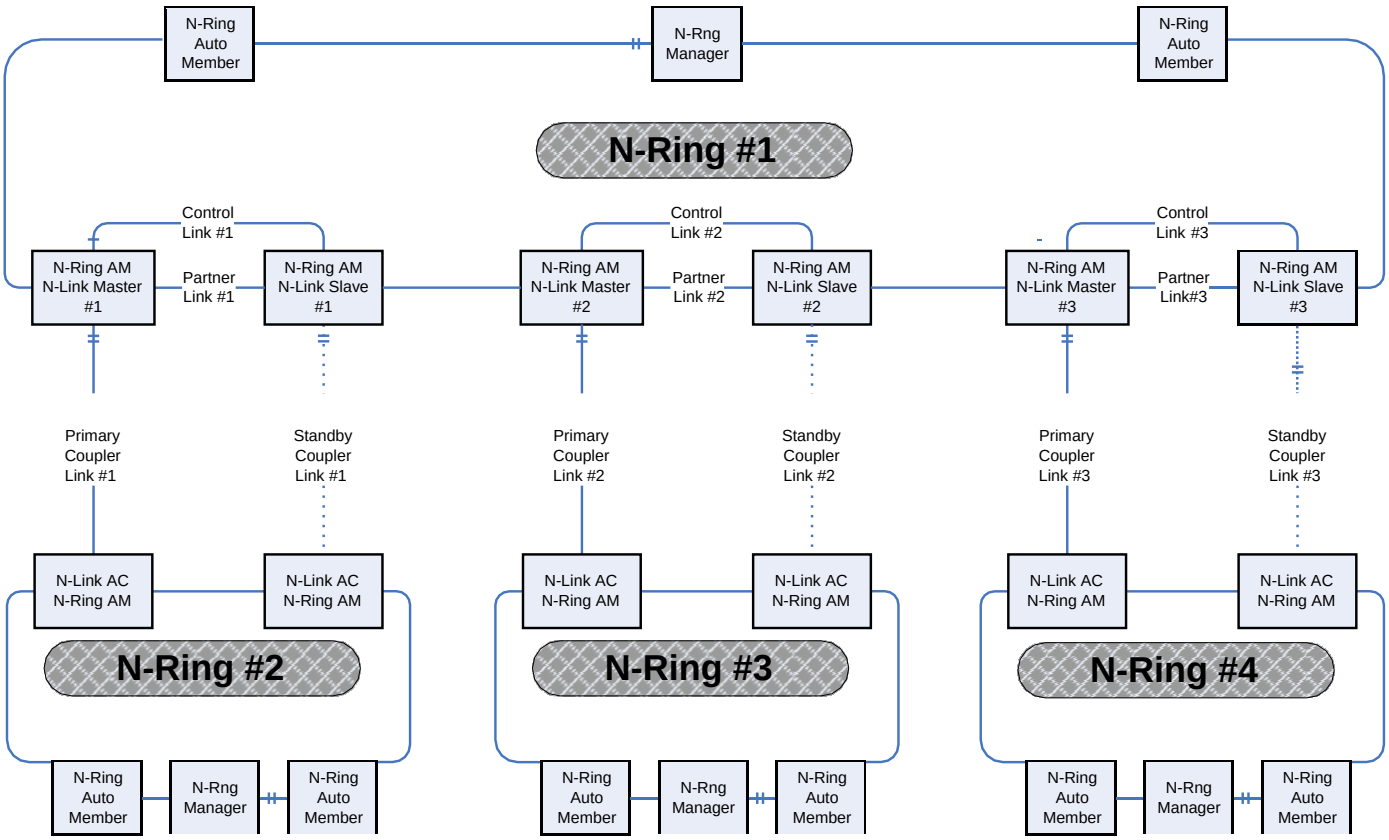
The purpose of N-Link is to provide a way to redundantly couple an N-Ring topology to one or more other topologies, usually other N-Ring topologies. Each N-Link configuration requires 4 switches: N-Link Master, N-Link Slave, N-Link Primary Coupler, and N-Link Standby Coupler.

Standard N-Link Configuration (Example):



For convenience, a diagram similar to the above is provided in the switch's browser help for N-Link.

Complex N-Link Configuration (Example):



Configuration Notes:

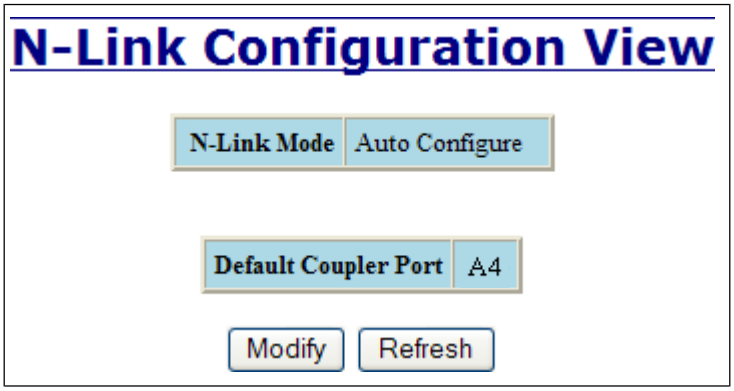
- The Master and Slave must be part of the N-Ring topology.
- If using default configuration choices, the administrator only needs to configure the N-Link Master. The N-Link Slave and both Coupler switches will auto-detect any needed configuration.
- If not using default configuration choices, the administrator may also need to configure the Default Coupler port on the N-Link Slave.
- There must be a direct link between the Master and Slave Control ports. Use of media converters or other switches is not supported.
- There must be a direct link between the Master and Slave Partner ports. Use of media converters or other switches is not supported.
- There must be at least one other switch, besides the Master and Slave, that supports N-Link on the N-Ring.
- N-Link will only support a single point of failure. Multiple points of failure and misconfiguration are not supported and may cause a network storm under some circumstances.

Configuration Steps to redundantly couple 2 N-Ring networks:

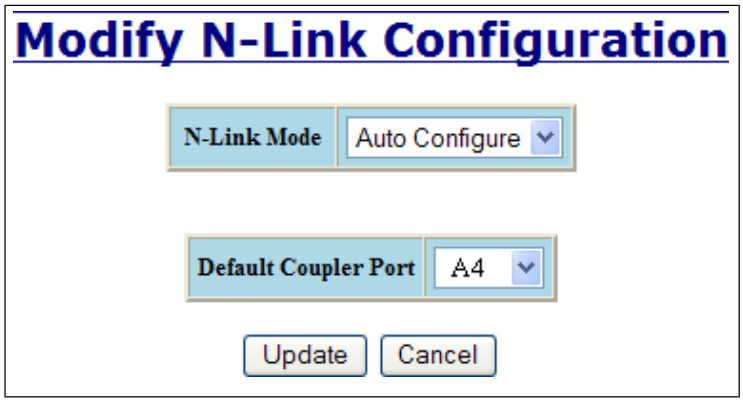
1. Ensure the Coupler and Control cables are disconnected at this point.
2. Get Both N-Rings working with a status of OK.
3. Configure N-Link Slave: Ensure that the N-Link Slave is set to Auto Configure and select a Default Coupler Port. Save Configuration.
4. Configure N-Link Master: Select the Control and Coupler ports. Save the Configuration.
5. Connect the Control Link cable. Ensure that the Slave switch status now shows a state of “Slave”
6. Connect the Coupler Link cables.
7. Check N-Link status by selecting the N-Link Status View page.

N-Link – Configuration, Continued…

The Configuration tab under the N-Link category will display the configuration settings. By default, N-Link is in Auto Configure mode and will use TX4 as the Default Coupler port.



Following the Modify button on the above example, the administrator will see a list of configurable fields for the N-Link configuration, as below.

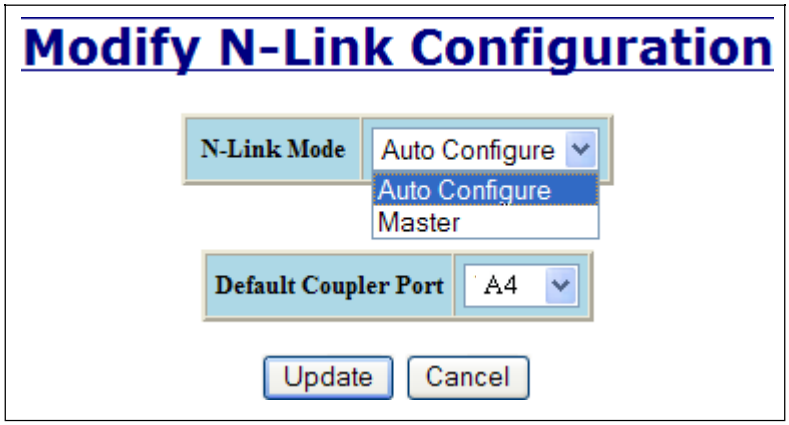


The port configured as the Default Coupler Port will be used as the Standby Coupler port if the switch detects an N-Link Master and becomes an N-Link Slave.

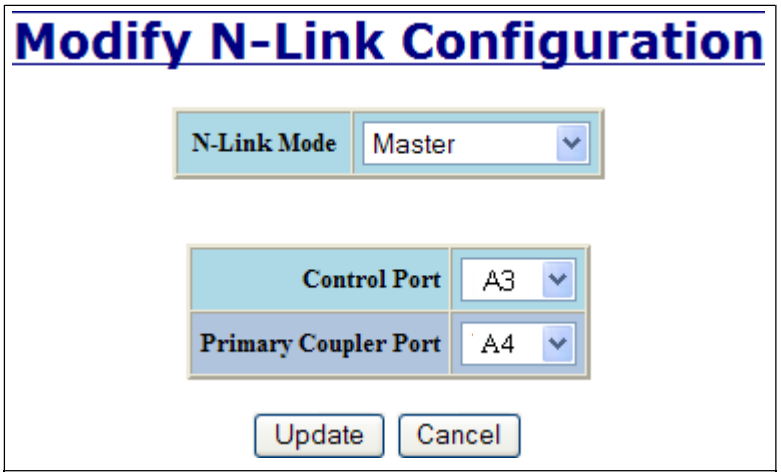
Once these fields are filled in to meet the needs of the administrator's network, the changes may be saved by clicking the Update button at the bottom of the page.

N-Link – Configuration, Continued…

The “N-Link Mode” is one of two choices, as below:



If N-Link mode is “Master”, then the administrator must configure the Control Port (default: TX3) and the Primary Coupler Port (default: TX4).



Once these fields are filled in to meet the needs of the administrator’s network, the changes may be saved by clicking the Update button at the bottom of the page.

N-Link – Status

The Status tab under the N-Link category will display the N-Link status.

If the switch is an N-Link Master or Slave, the following switch status and partner status information will be shown. Fields with a red background designate a fault condition.

State:	Current N-Link mode of switch.
Control Port:	The port being used to convey control information. There must be a direct link between the Master and Slave Control ports. Use of media converters or other switches is not supported.
Partner Port:	The port being used for normal communication between the N-Link Master and N-Link Slave switch. There must be a direct link between the Master and Slave Partner ports. Use of media converters or other switches is not supported. This port will be detected automatically.
Coupler Port:	The port being used to establish a redundant path for Ethernet data transmission.
Coupler Port State:	Blocking, Forwarding.
Status:	No errors will show "OK", otherwise a description of the Faults detected.

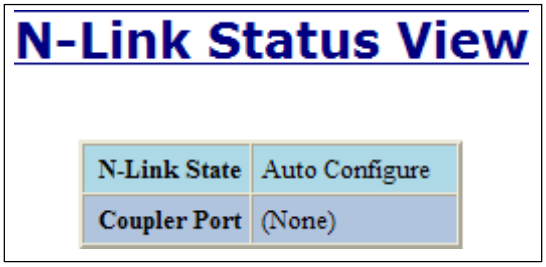
N-Link Partner Information

State:	Current N-Link mode of switch.
MAC:	The MAC Address of the N-Link Partner switch.
Coupler Port State:	Blocking, Forwarding.
Status:	No errors will show "OK", otherwise a description of the Faults detected.

If switch is an N-Link Auto Configure and not a Slave, the Coupler port, if known, will be shown.

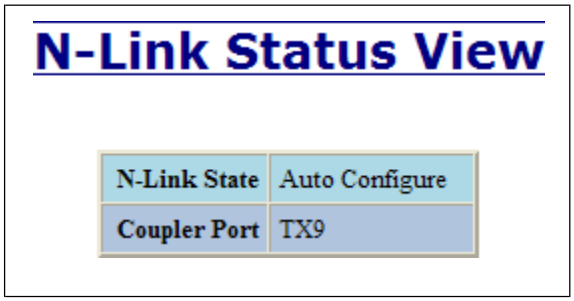
N-Link State:	Current N-Link mode of switch.
Coupler Port:	The port used to establish a redundant path for Ethernet data transmission. This port will be detected automatically.

Below is an example of N-Link Status from a switch in defaults (N-Link Auto Configure) that is not an N-Link Master and has not become an N-Link Slave or an N-Link Coupler:



N-Link – Status, Continued…

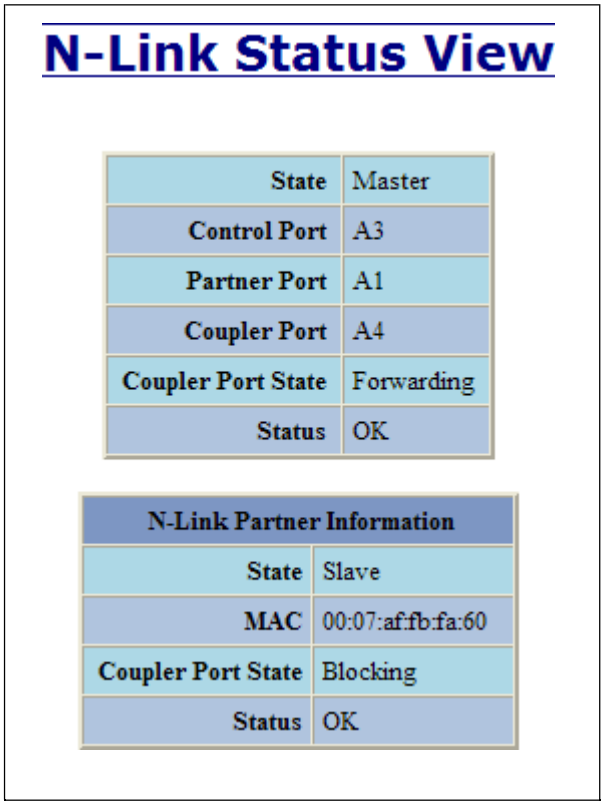
Below is an example of N-Link Status from an N-Link Coupler switch:



N-Link Status View

N-Link State	Auto Configure
Coupler Port	TX9

Below is an example of N-Link Status from an N-Link Master switch:



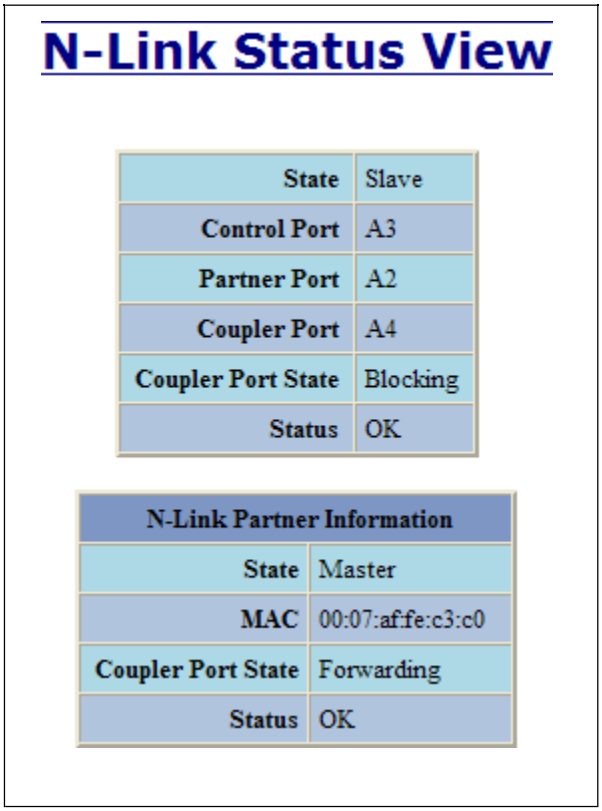
N-Link Status View

State	Master
Control Port	A3
Partner Port	A1
Coupler Port	A4
Coupler Port State	Forwarding
Status	OK

N-Link Partner Information	
State	Slave
MAC	00:07:af:fb:fa:60
Coupler Port State	Blocking
Status	OK

N-Link – Status, Continued…

Below is an example of N-Link Status from an N-Link Slave switch:

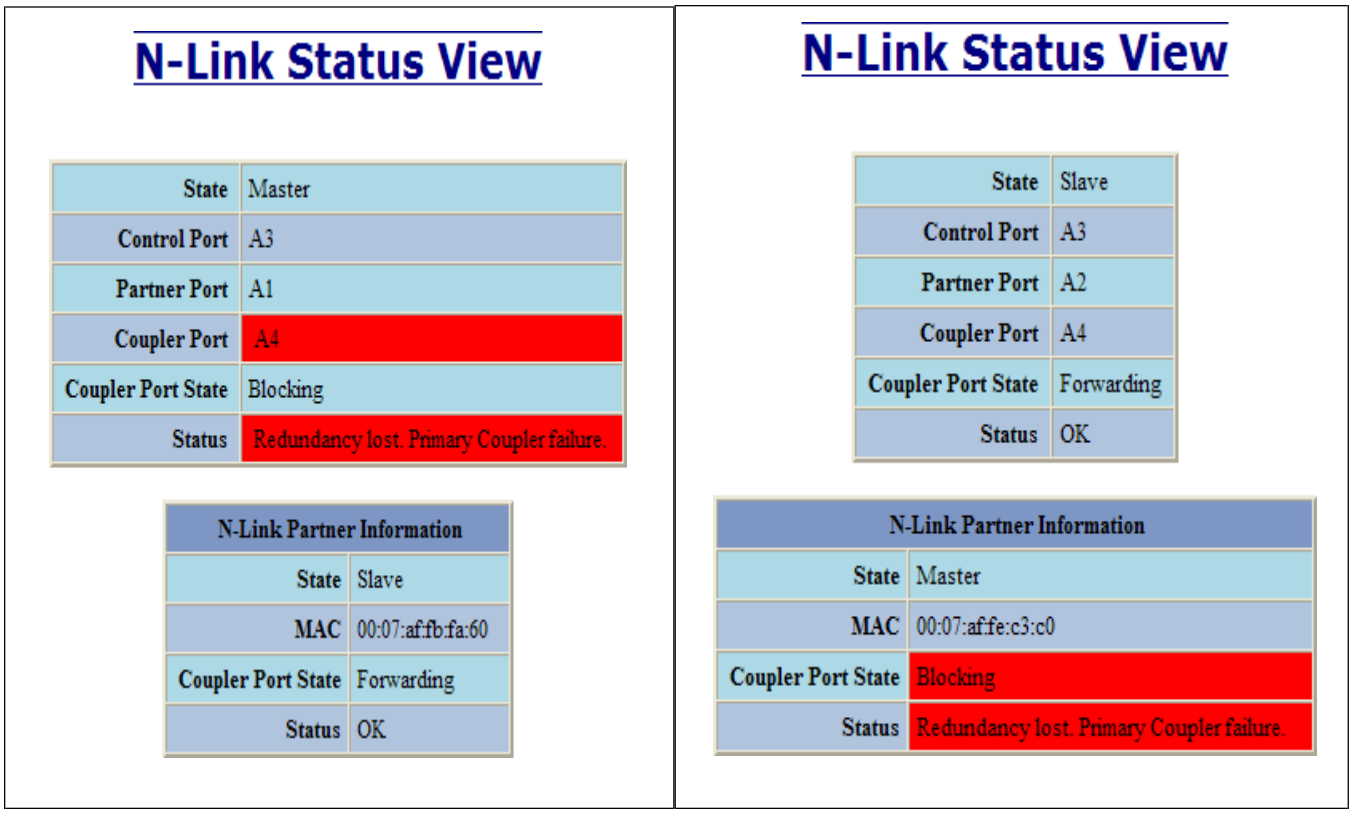


N-Link Status View

State	Slave
Control Port	A3
Partner Port	A2
Coupler Port	A4
Coupler Port State	Blocking
Status	OK

N-Link Partner Information	
State	Master
MAC	00:07:af:fe:c3:c0
Coupler Port State	Forwarding
Status	OK

Below is an example of N-Link Status from an N-Link Master and Slave where the Primary Coupler link is broken:



N-Link Status View

State	Master
Control Port	A3
Partner Port	A1
Coupler Port	A4
Coupler Port State	Blocking
Status	Redundancy lost. Primary Coupler failure.

N-Link Partner Information	
State	Slave
MAC	00:07:af:fb:fa:60
Coupler Port State	Forwarding
Status	OK

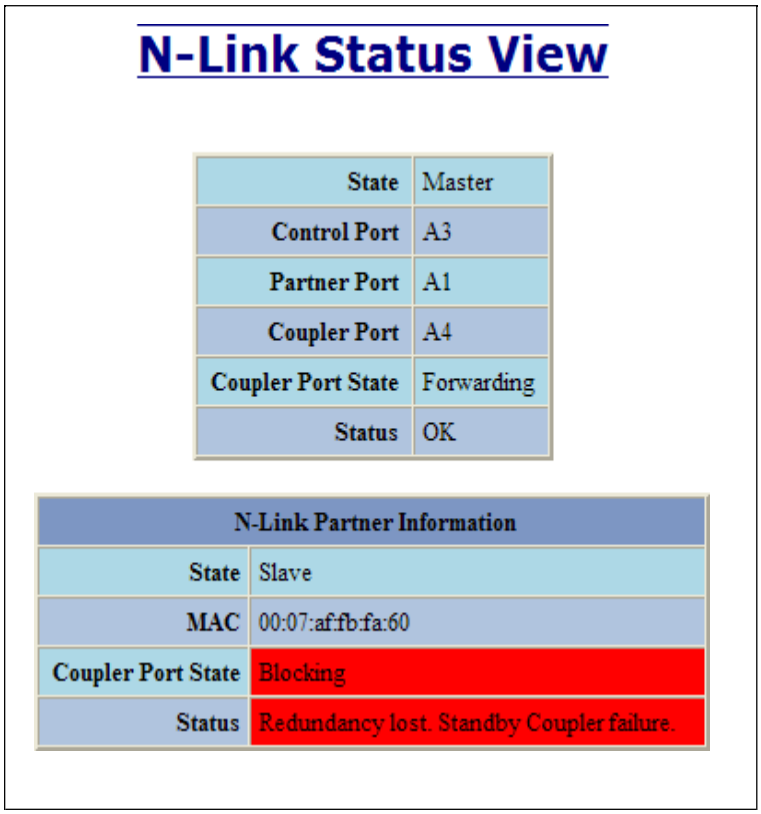
N-Link Status View

State	Slave
Control Port	A3
Partner Port	A2
Coupler Port	A4
Coupler Port State	Forwarding
Status	OK

N-Link Partner Information	
State	Master
MAC	00:07:af:fe:c3:c0
Coupler Port State	Blocking
Status	Redundancy lost. Primary Coupler failure.

N-Link – Status, Continued…

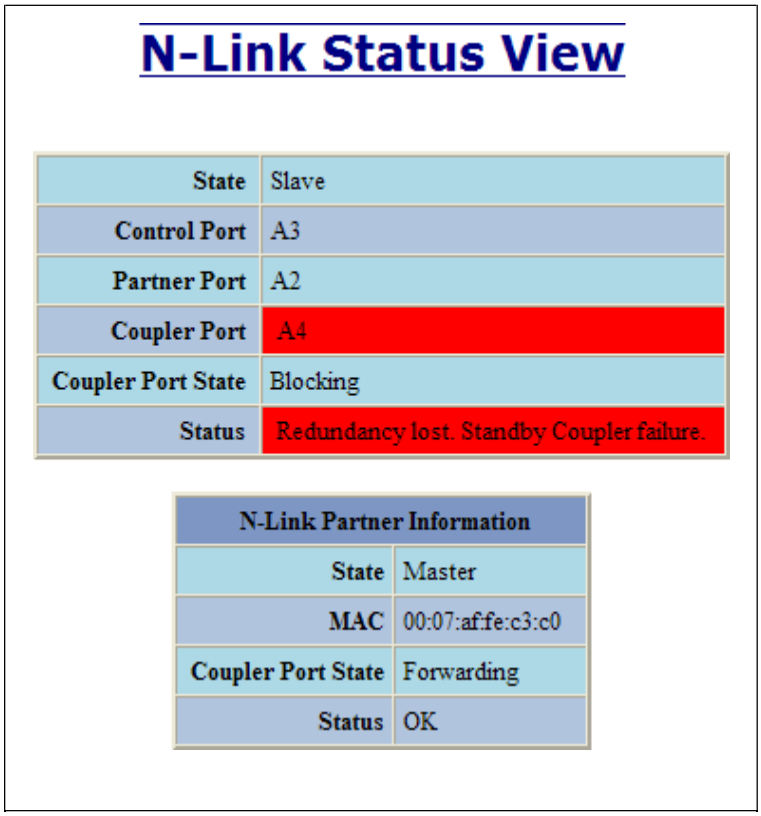
Below is an example of N-Link Status from an N-Link Master and Slave where the Standby Coupler link is broken:



N-Link Status View

State	Master
Control Port	A3
Partner Port	A1
Coupler Port	A4
Coupler Port State	Forwarding
Status	OK

N-Link Partner Information	
State	Slave
MAC	00:07:af:fb:fa:60
Coupler Port State	Blocking
Status	Redundancy lost. Standby Coupler failure.

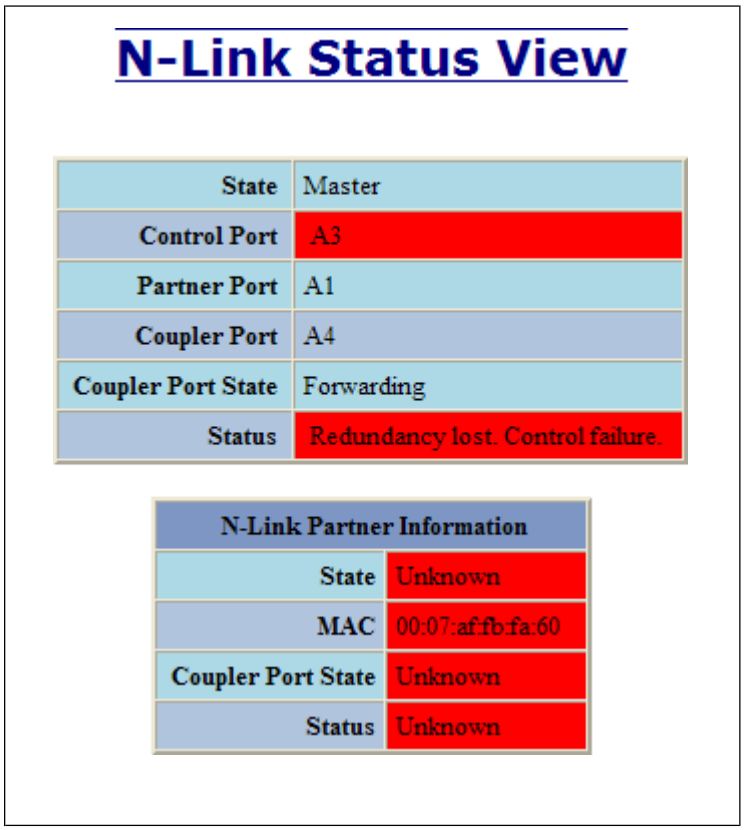


N-Link Status View

State	Slave
Control Port	A3
Partner Port	A2
Coupler Port	A4
Coupler Port State	Blocking
Status	Redundancy lost. Standby Coupler failure.

N-Link Partner Information	
State	Master
MAC	00:07:af:fe:c3:c0
Coupler Port State	Forwarding
Status	OK

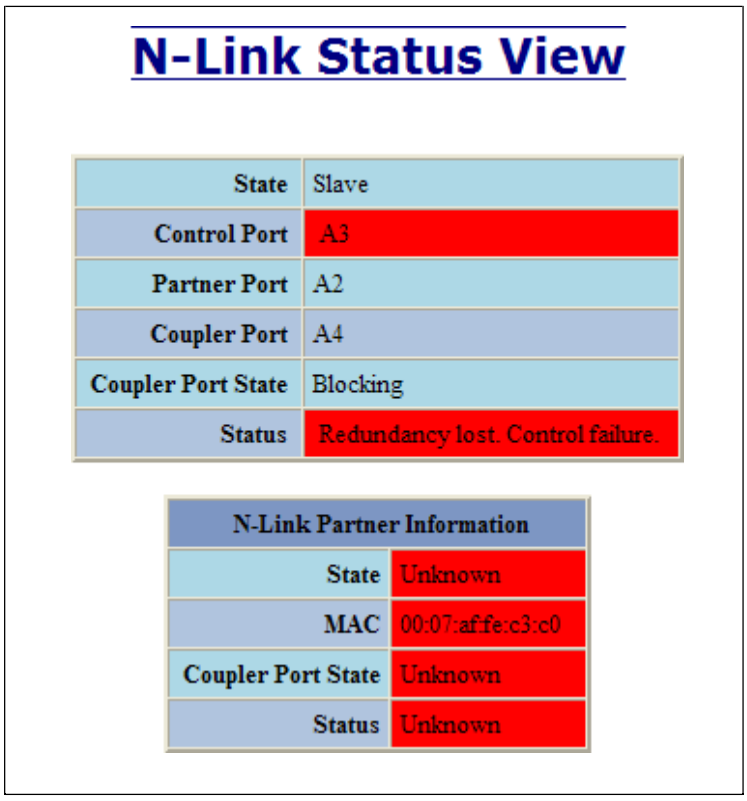
Below is an example of N-Link Status from an N-Link Master and Slave where the Control link is broken:



N-Link Status View

State	Master
Control Port	A3
Partner Port	A1
Coupler Port	A4
Coupler Port State	Forwarding
Status	Redundancy lost. Control failure.

N-Link Partner Information	
State	Unknown
MAC	00:07:af:fb:fa:60
Coupler Port State	Unknown
Status	Unknown



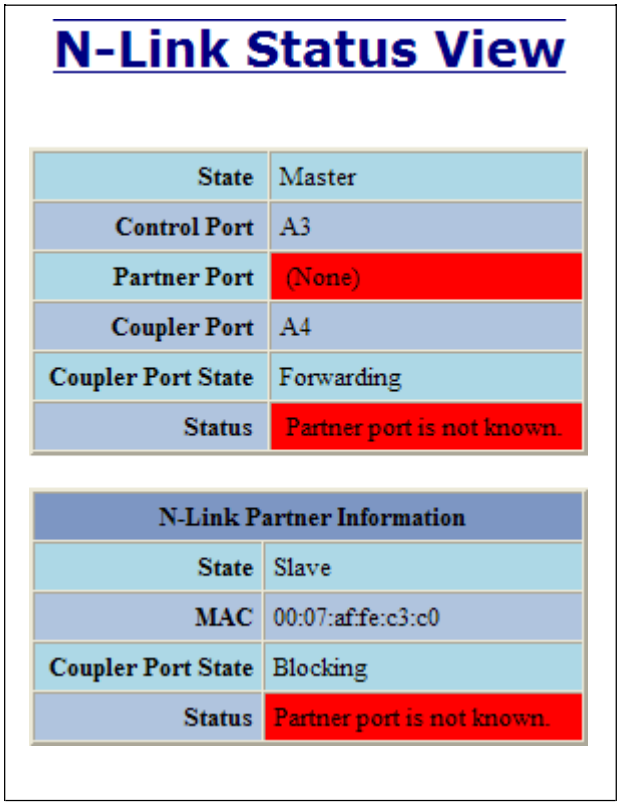
N-Link Status View

State	Slave
Control Port	A3
Partner Port	A2
Coupler Port	A4
Coupler Port State	Blocking
Status	Redundancy lost. Control failure.

N-Link Partner Information	
State	Unknown
MAC	00:07:af:fe:c3:c0
Coupler Port State	Unknown
Status	Unknown

N-Link – Status, Continued…

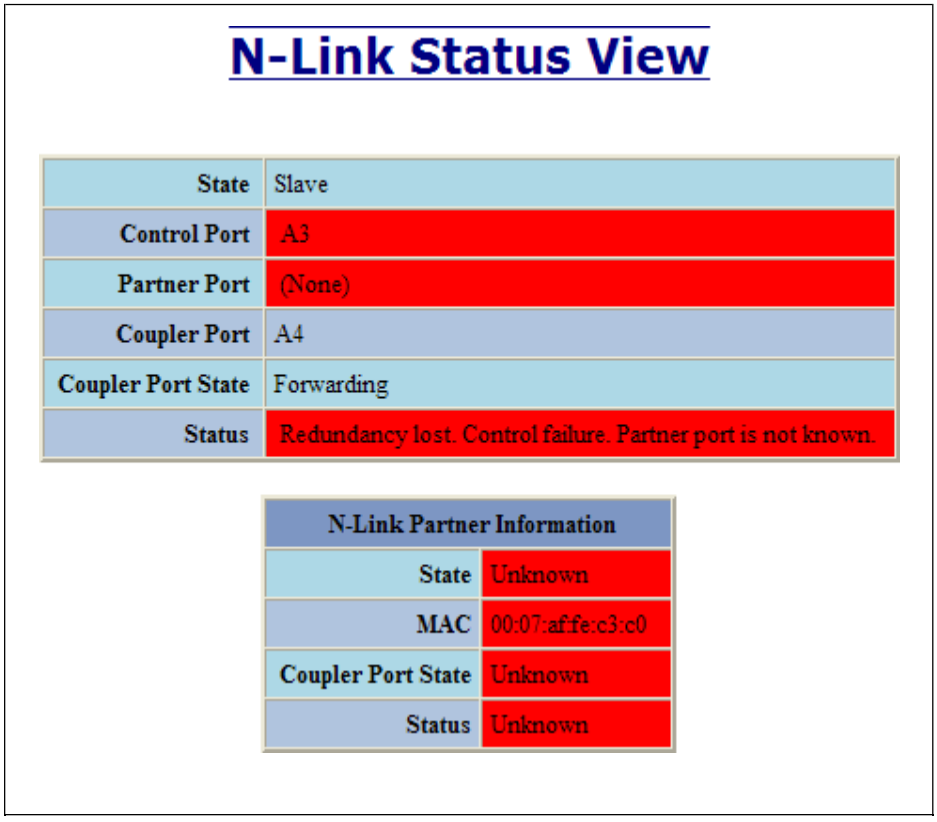
Below is an example of N-Link Status from an N-Link Master and Slave where the Partner link is broken:



N-Link Status View

State	Master
Control Port	A3
Partner Port	(None)
Coupler Port	A4
Coupler Port State	Forwarding
Status	Partner port is not known.

N-Link Partner Information	
State	Slave
MAC	00:07:af:fe:c3:c0
Coupler Port State	Blocking
Status	Partner port is not known.



N-Link Status View

State	Slave
Control Port	A3
Partner Port	(None)
Coupler Port	A4
Coupler Port State	Forwarding
Status	Redundancy lost. Control failure. Partner port is not known.

N-Link Partner Information	
State	Unknown
MAC	00:07:af:fe:c3:c0
Coupler Port State	Unknown
Status	Unknown

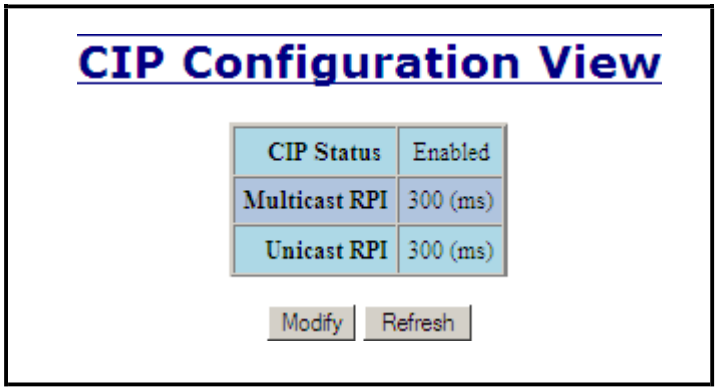
CIP – Configuration

The Configuration tab under the CIP category will display basic variables for CIP, and the status:

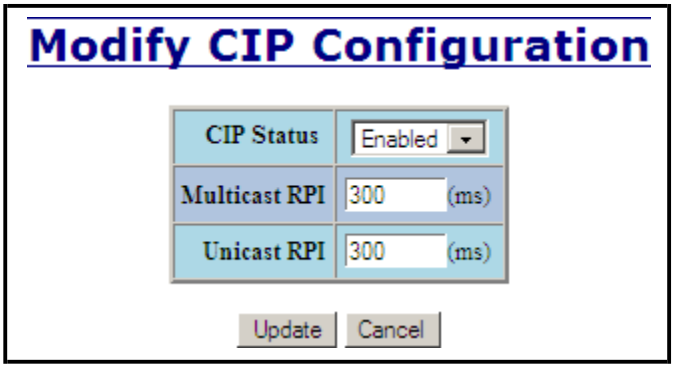
Cip Status:
Enables or Disables CIP on the Switch. Default: Enabled.

Multicast RPI:
The minimum Requested Packet Interval for Class 1 (multicast) connections, in milliseconds. Requests for less than this value will be rejected. Default = 1 second.

Unicast RPI:
The minimum Requested Packet Interval for Class 3 (unicast) connections, in milliseconds. Requests for less than this value will be rejected. Default = 1 second.



Following the Modify button on the above example, the administrator can modify the variables. Additionally, you may Disable or Enable CIP altogether.



CIP – Status

The Status tab under the CIP category will display the CIP status.

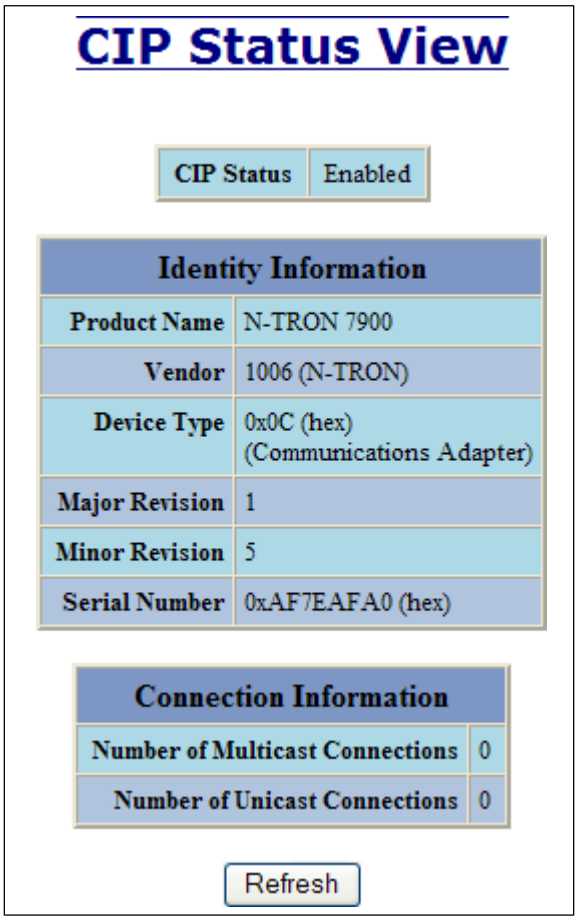
The following switch status and partner status information will be shown:

Identity Information:

Product Name:	Switch Model Number.
Vendor:	This is N-Tron's ODVA EtherNet/IP Vendor ID (1006).
Device Type:	The ODVA Device Type is Communications Adapter (= 0x0C hex).
Major Revision:	The Major Revision of the CIP implementation.
Minor Revision:	The Minor Revision of the CIP implementation.
Serial Number (hex):	CIP Serial number, unique across all N-Tron CIP devices. This is the last 4 octets of the base switch MAC.

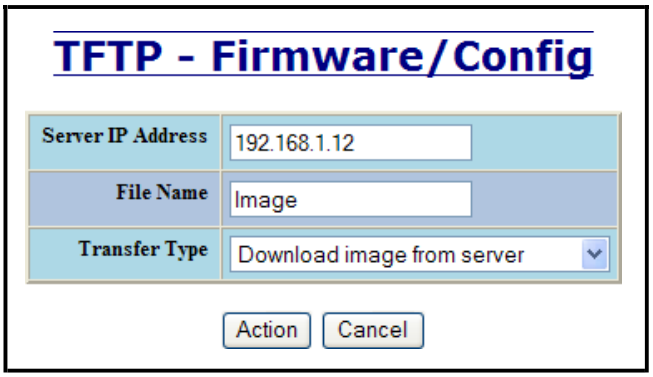
Connection Information:

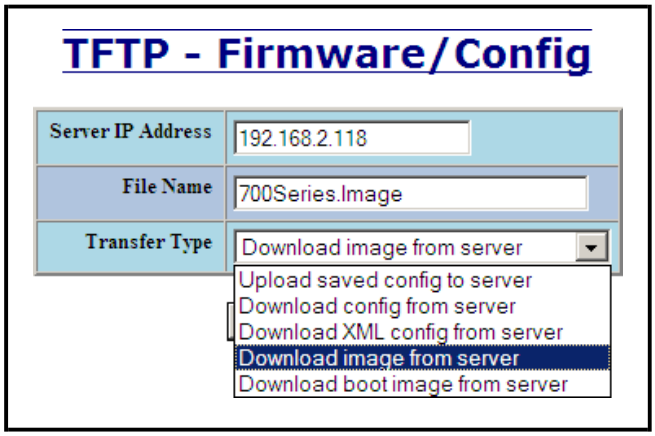
Number of Multicast Connections:	Current number of CIP Ethernet/IP class 1 (multicast) connections.
Number of Unicast Connections:	Current number of CIP Ethernet/IP class 3 (unicast) connections.

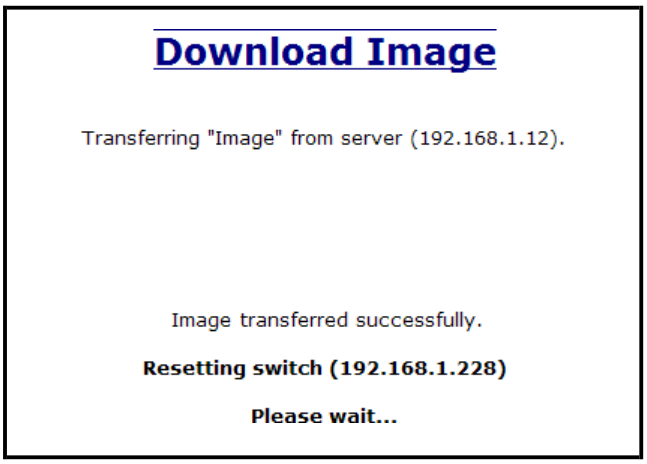


Firmware/Config – TFTP

The TFTP tab under the Firmware/Config category gives the administrator the ability to upload or download a config file for a 7900 switch. This allows administrators to backup their configurations to a server offsite in case they need to reload their custom configurations at a later time. Administrators are also given the ability to flash the switch allowing them to update the firmware in the field without losing their current configurations and without having to send the unit back to N-Tron for updates in the future. It is important not to cycle power on the switch or interrupt the data connection between the TFTP server and the switch while you are flashing or uploading/downloading a config file. The switch will not stop working if this does occur, but the administrator will have to retransfer the file. Also, an XML file can be downloaded to a switch to achieve some switch configurations. XML settings cover a subset of the settings available through the web browser. Reference *Appendix A. XML Settings File Example* for the complete set of configurations that can be done using XML Settings Download.

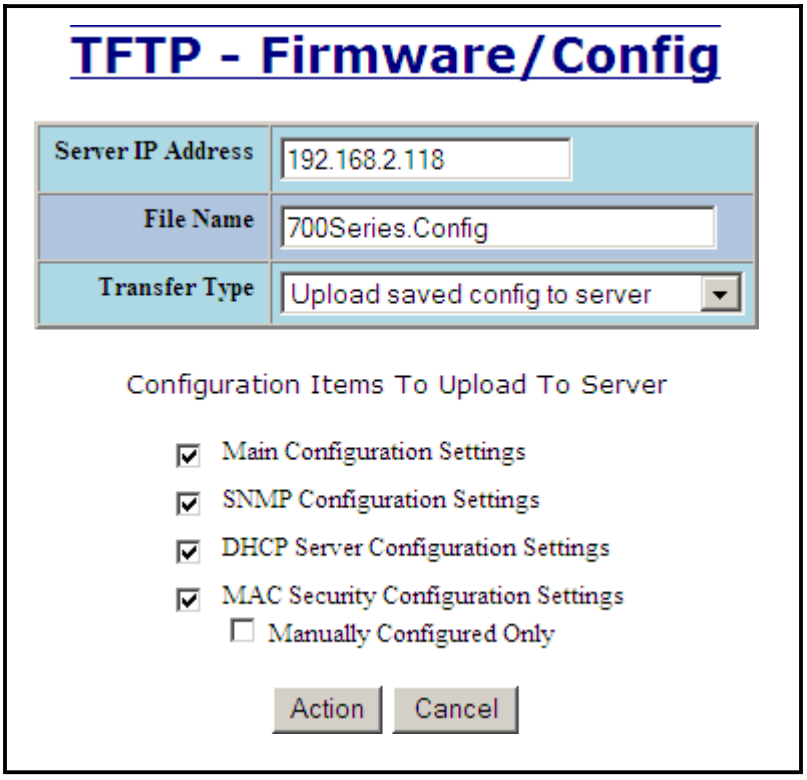


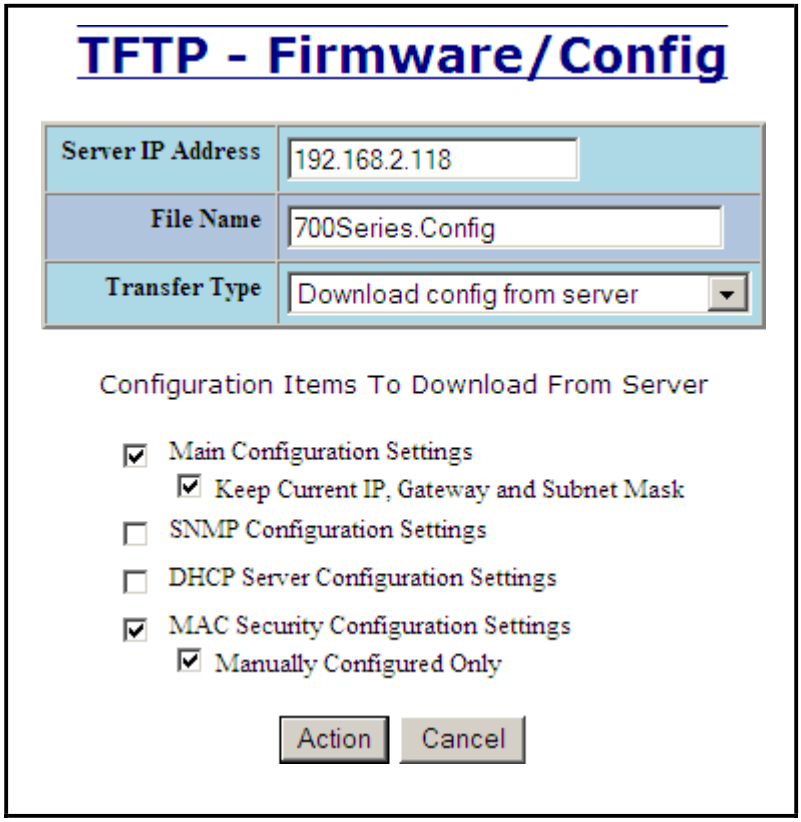




Firmware/Config – TFTP, Continued…

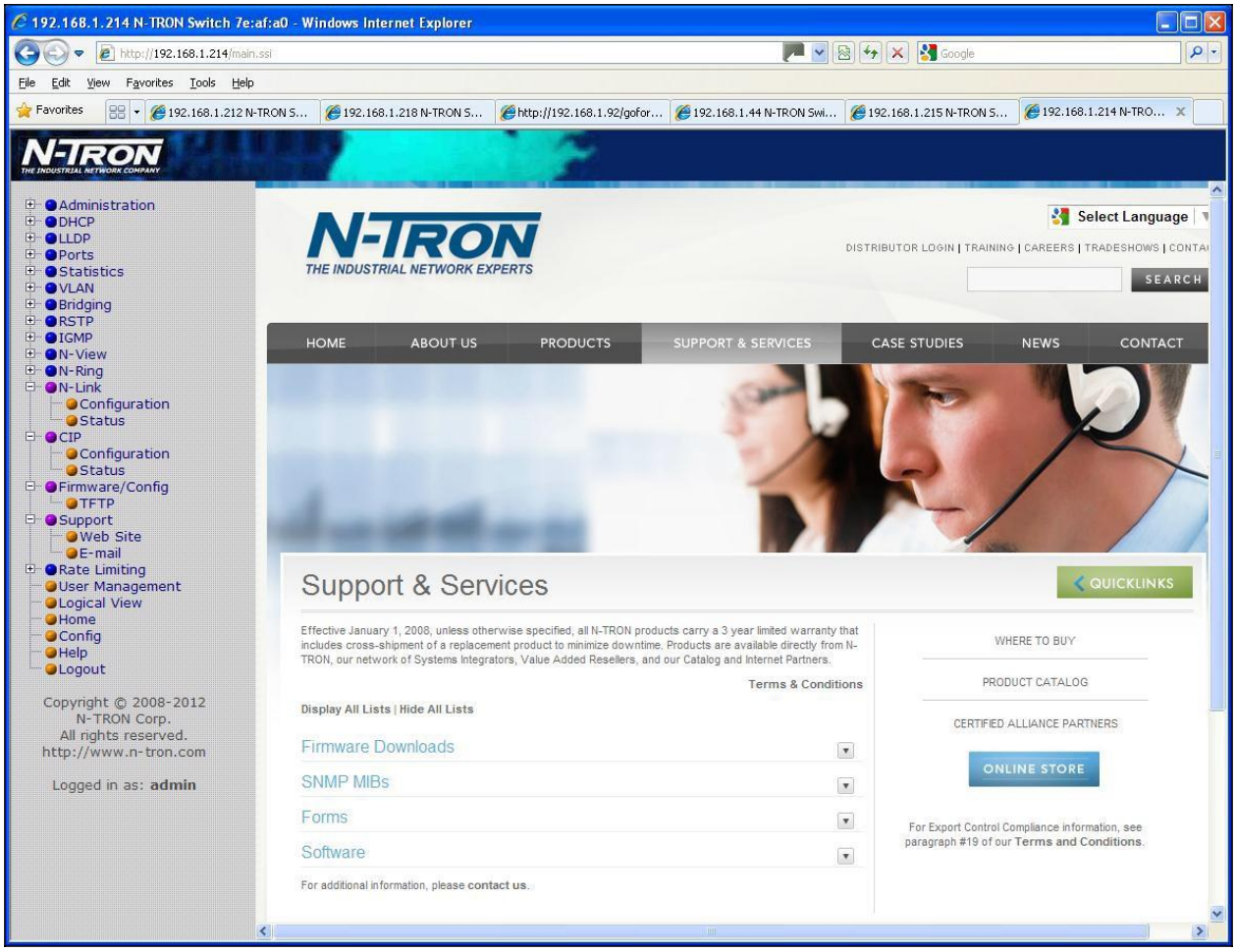
In some cases the administrator may choose to upload or down load only certain configuration settings or to retain his current network settings. These choices are available as below. For more detail on the choices, reference *'Help – Firmware/Config'* in this user manual or from the actual switch.





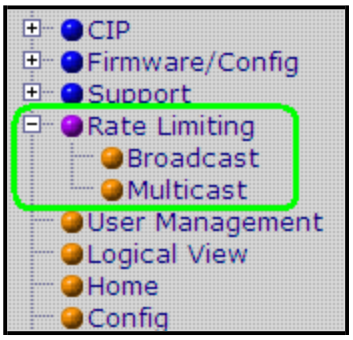
Support – Web Site and E-mail

If at any point in time you get confused or would like additional support directly from N-Tron, you may visit N-Tron's web site, or e-mail N-Tron directory with the links provided for more information.

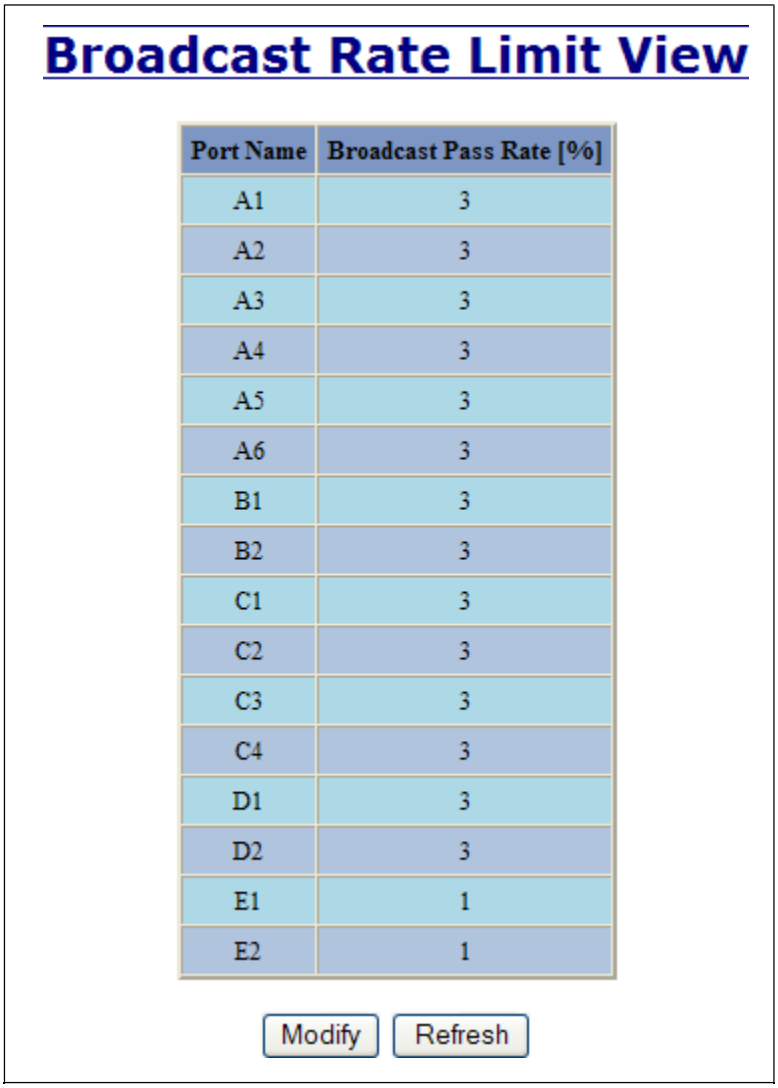


Rate Limiting Configuration

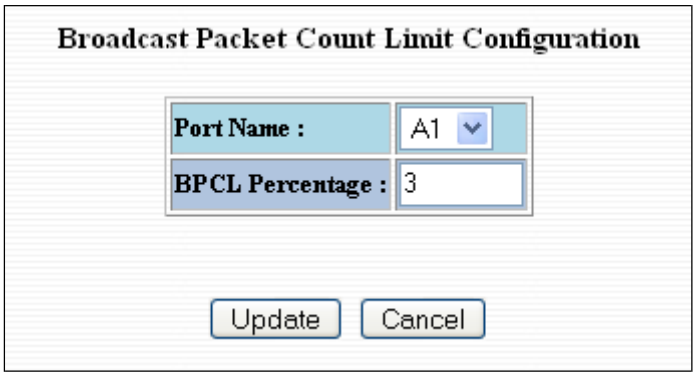
From the left hand navigation, one can choose Broadcast or Multicast Rate Limiting. These are ingress filters.

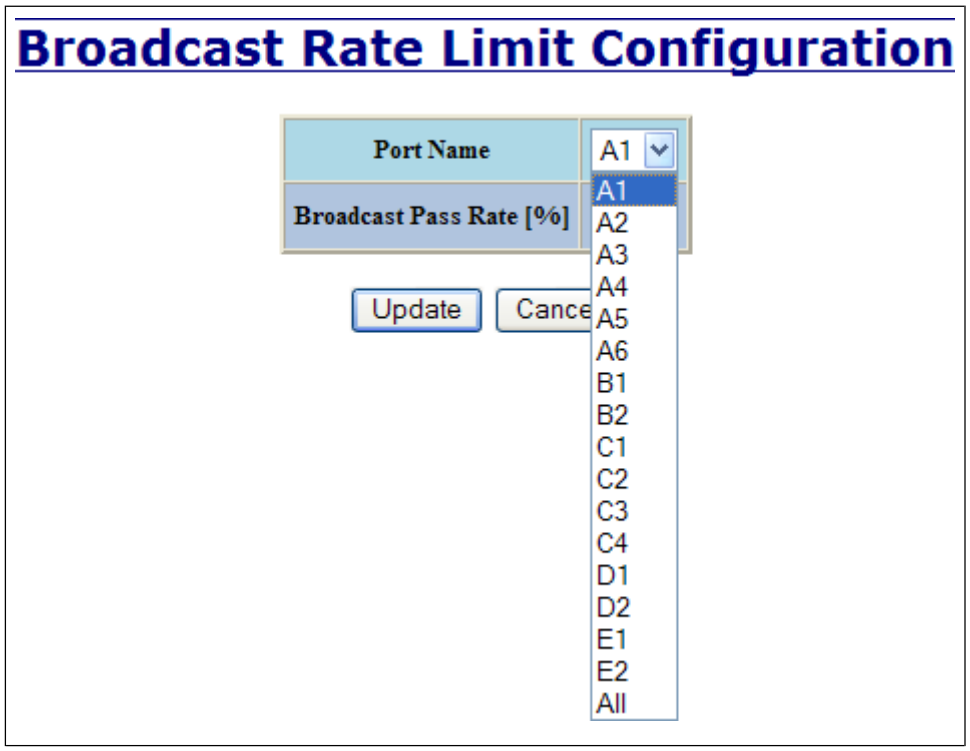


The Broadcast Rate Limit View displays all the ports in the 7900 Series unit and lists the percentage pass rate for each port. The factory defaults for 10/100 ports are 3% and for gigabit ports are 1%. A Modify button is provided to change these fields.

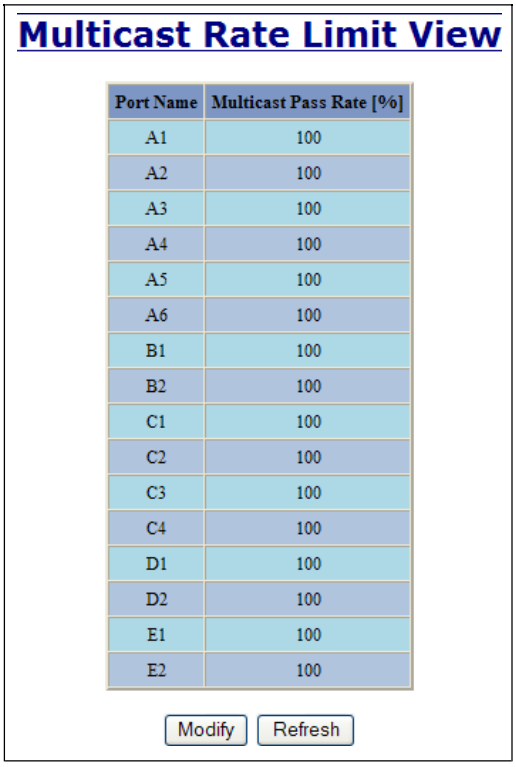


Following the Modify button on the previous example, the administrator can modify the BPCL Percentage for each port. The default BPCL is 3% for all ports.

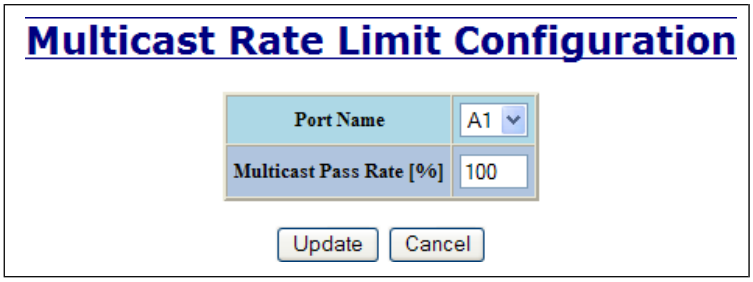


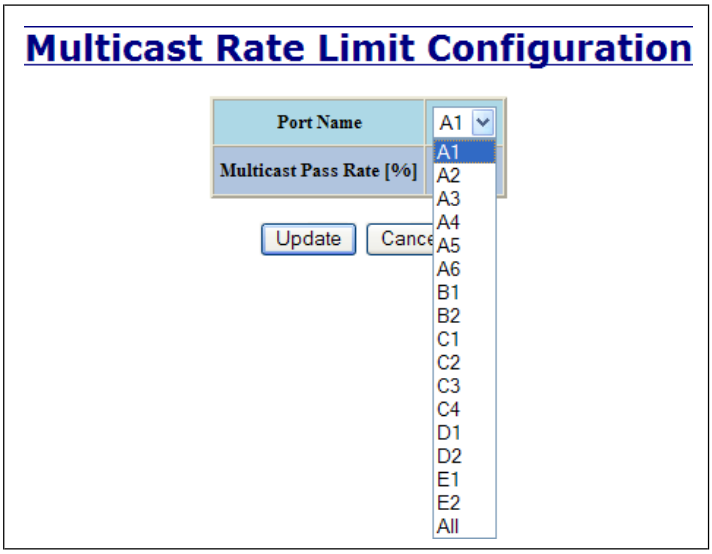


The Multicast Rate Limit View displays all the ports in the 7900 Series unit and lists the percentage pass rate for each port. A Modify button is provided to change these fields. The factory default for multicast rate limiting is 100% pass rate on all ports.



Following the Modify button on the above example, the administrator can modify the percentage for each and every port independently. A selection is provided for all ports to be set at once when that is more convenient.

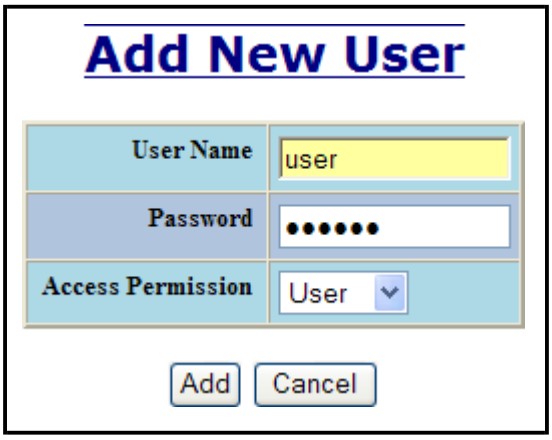




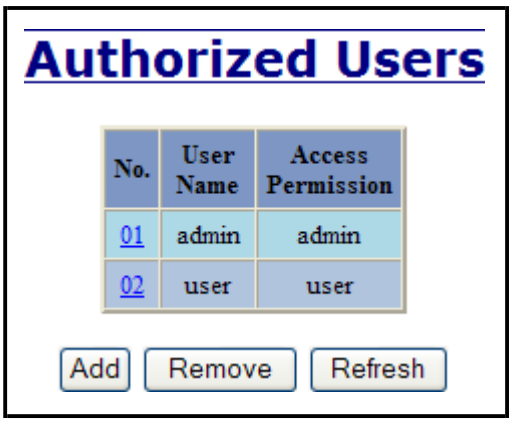
User Management – Adding Users

The User Management link will display a list of all the users who have access to the management features of the switch and their access permissions.

Following the Add button on the above example, the administrator can add another user and assign the user a username, a password, and the user's permissions (user/administrator).



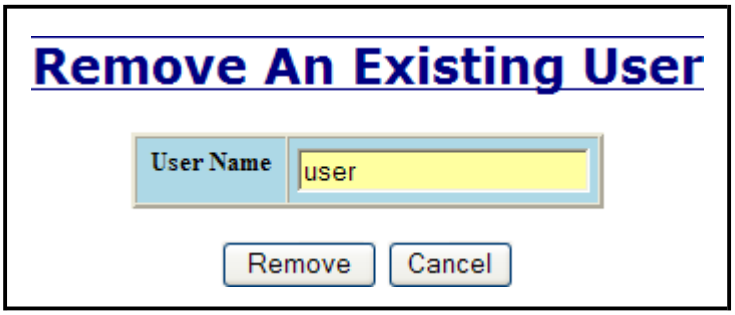
A page should display after the administrator clicks the Add button indicating that the user was successfully added.



User Management – Removing Users

In order to remove a user, simply click on the Remove button at the bottom of the page.

Following the Remove button on the above example, the administrator can remove a user by entering in the user's name and clicking the Remove button.

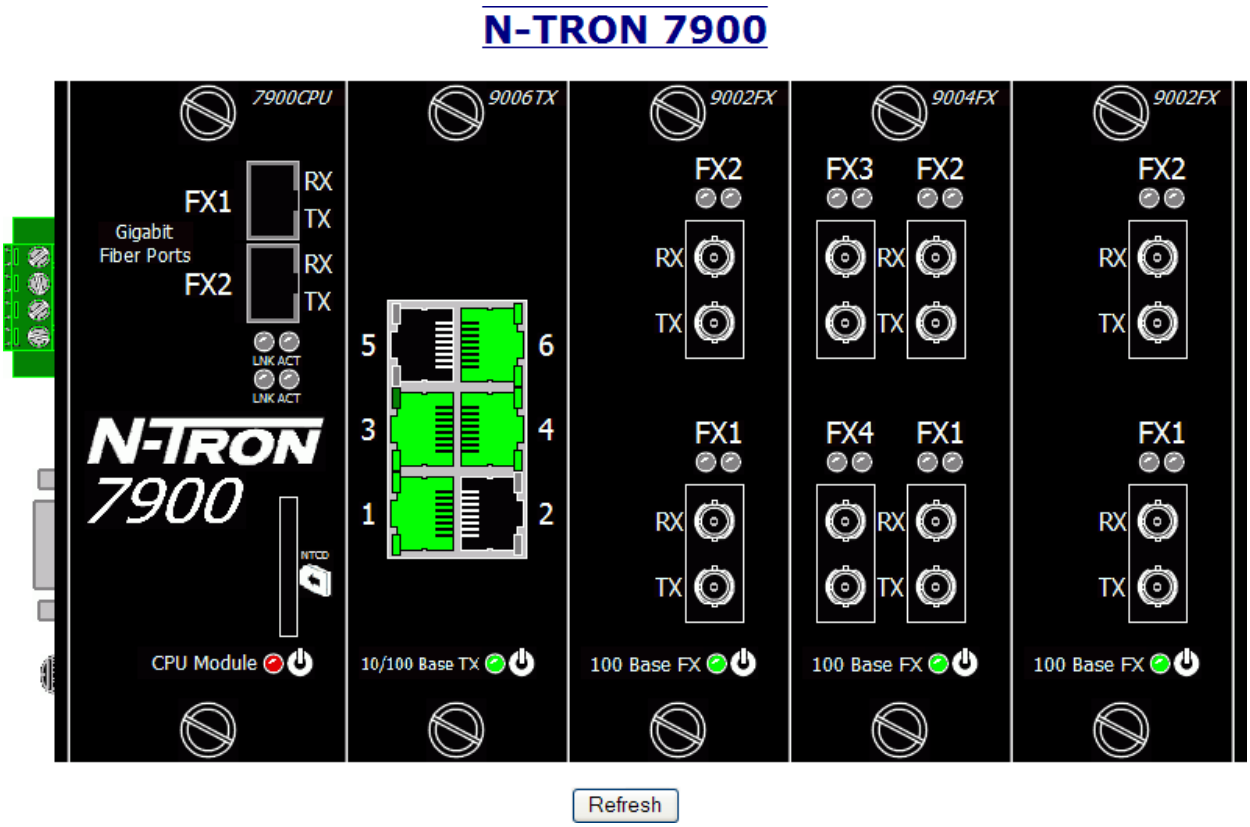


A page should follow indicating that the user was successfully removed from the list.

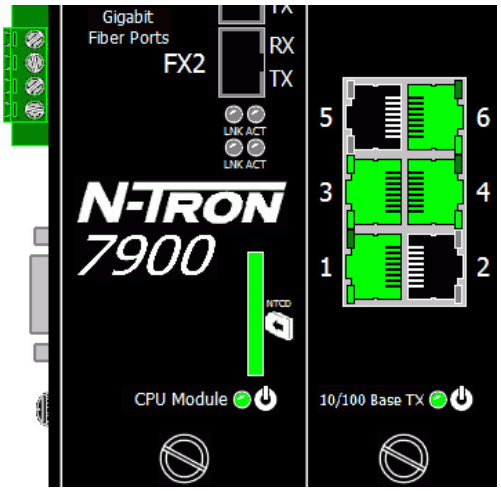
Note: *There are a maximum number of 5 users per switch. User permissions have the right to view switch configurations and to view current port settings, but cannot make any changes to these settings. Admin permissions have the right to change and view any switch configuration and to change and view any current port settings.*

Logical View

The 7900 Web Management offers a logical view of the switch. Here a user or administrator can see a graphical depiction of the 7900 switch with the installed modules that have been configured in it. Ports that are linked will turn green, while ports that are not linked will show up as black. The example below shows only ports 1, 3, 4, and 6 on the 9006TX module linked. The other ports are currently in the down state (not being used).



When the NTCD (N-Tron Configuration Device) is inserted, this is indicated by the slot being green as below:



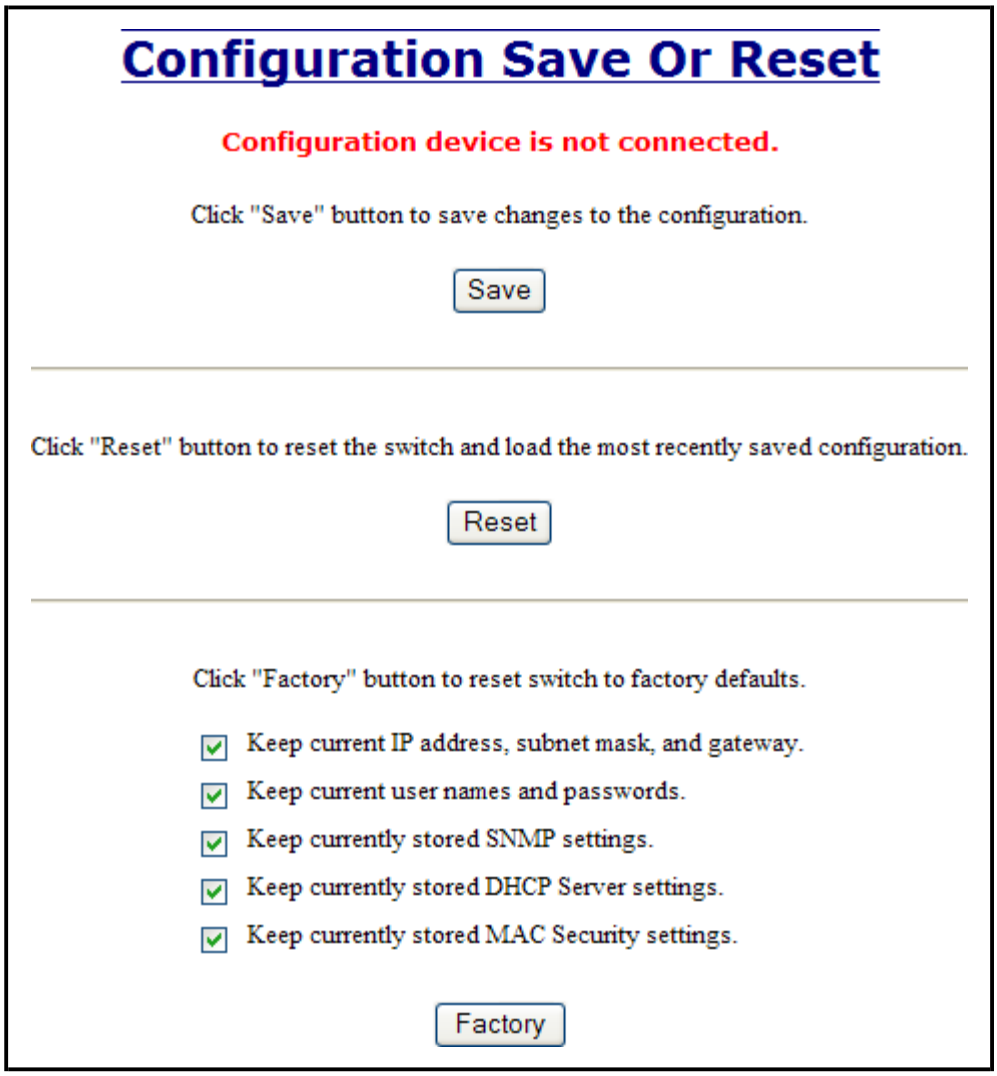
Configuration – Save or Reset

The Configuration section of web management gives an administrator the ability to save a running configuration into the NVRAM. This step is needed in order for the switch to remember any changes after a power cycle.

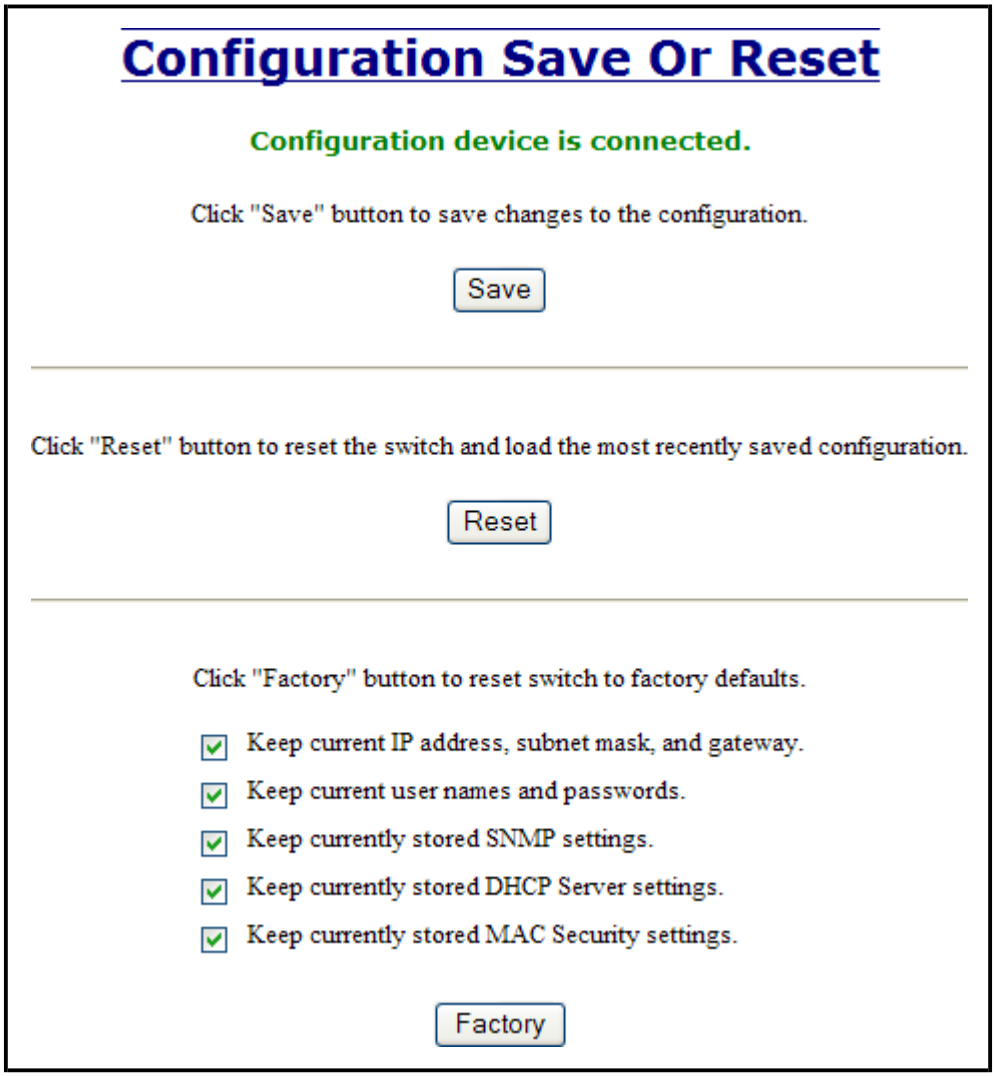
The “Save” button will save all current changes to the configuration for use after the next power cycle. **Note: The current configuration will also be saved to the configuration device when connected.** This page reveals whether the configuration device is installed or not.

The “Reset” button will discard all unsaved changes, reset the switch and load the most recently saved configuration settings. **Note: Upon restart, if a configured configuration device is connected, the switch will load the configured settings from it and save them into NVRAM.**

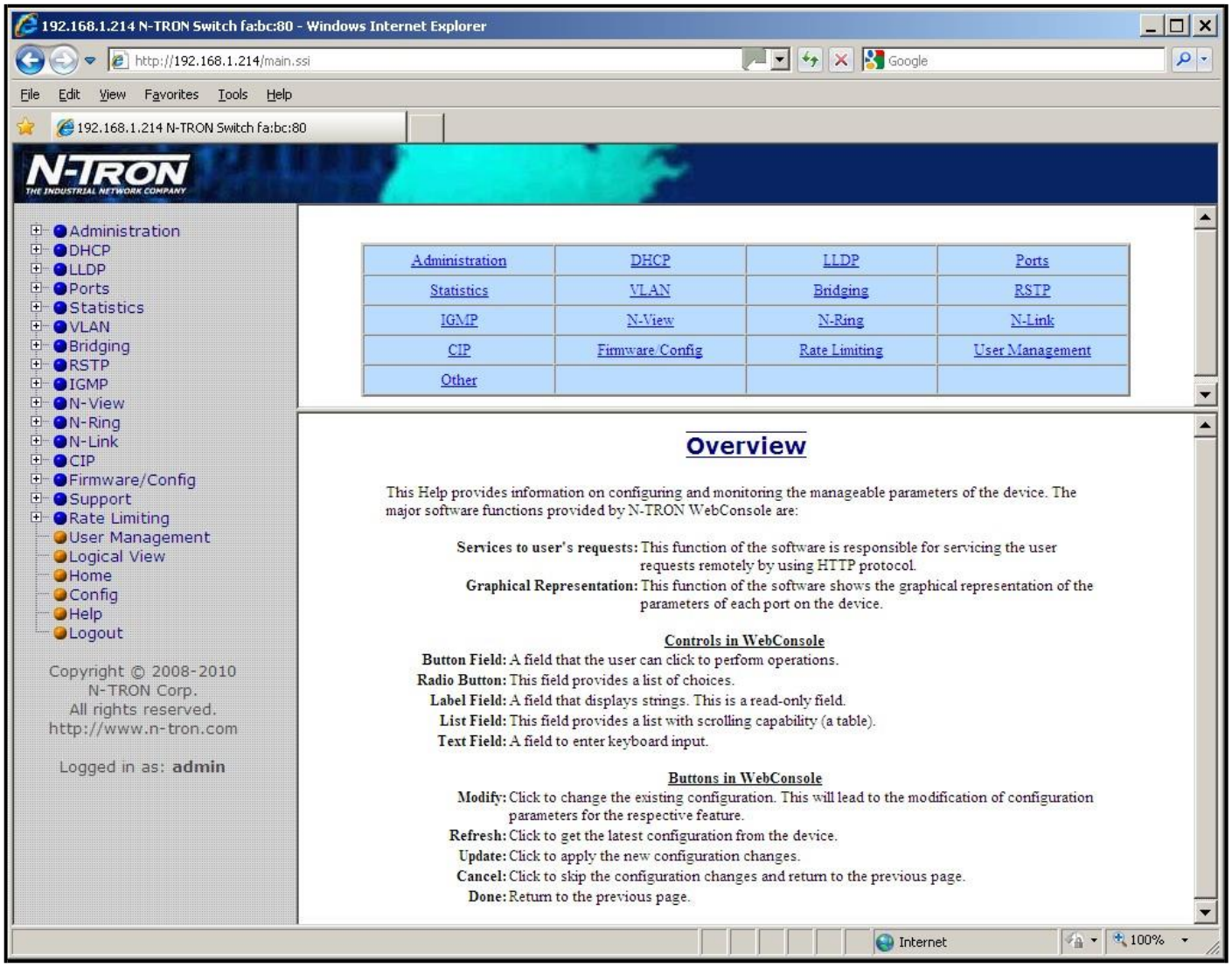
The “Factory” button will reload N-Tron’s factory default configuration settings. Doing so will reconfigure the 7900 switch to factory defaults. In many cases it is desirable to restore factory defaults but retain the IP address, subnet mask, and gateway address settings as well as user names and passwords. Checkboxes are provided to select the desired behavior. **Note: The factory default configuration settings will also be saved to the configuration device when connected.**



If a Configuration Device is present, that is presented:

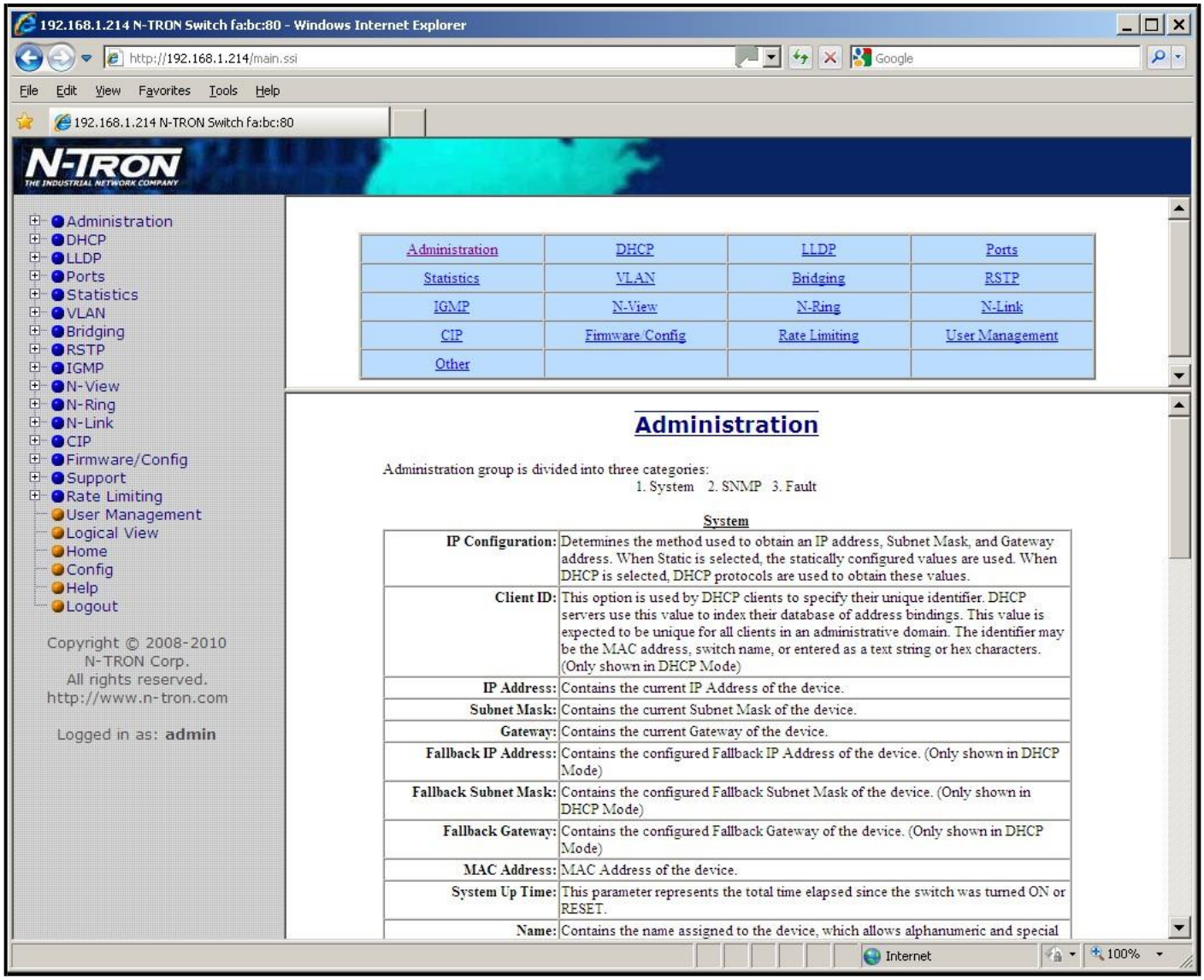


Help – Overview



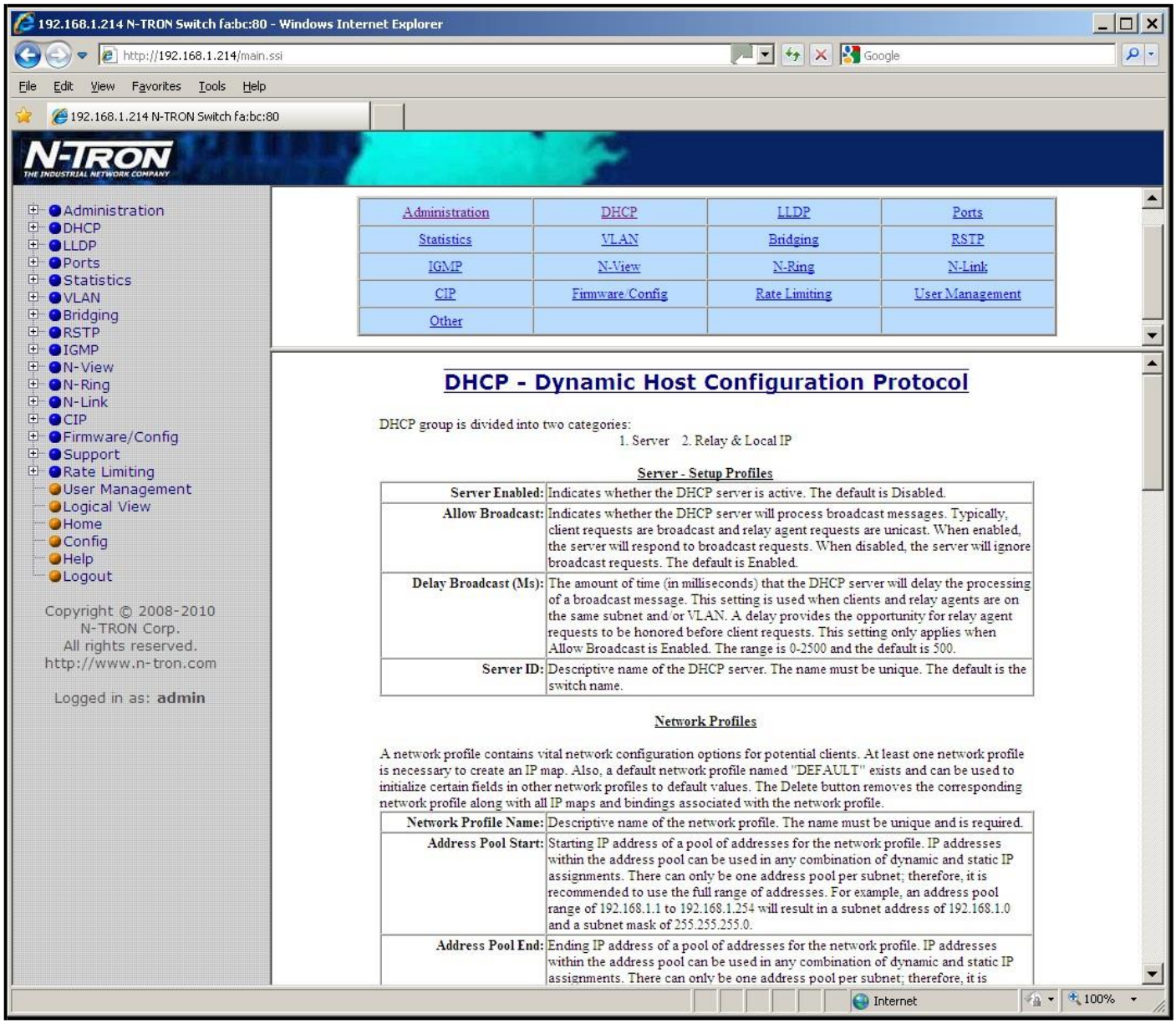
When the Help link is clicked on, you will see the Overview page that will have some basic definitions and more specific choices at the top of the screen. Although this page is not as detailed as the manual, it gives you a basic feel for different features the 7900 offers.

Help – Administration



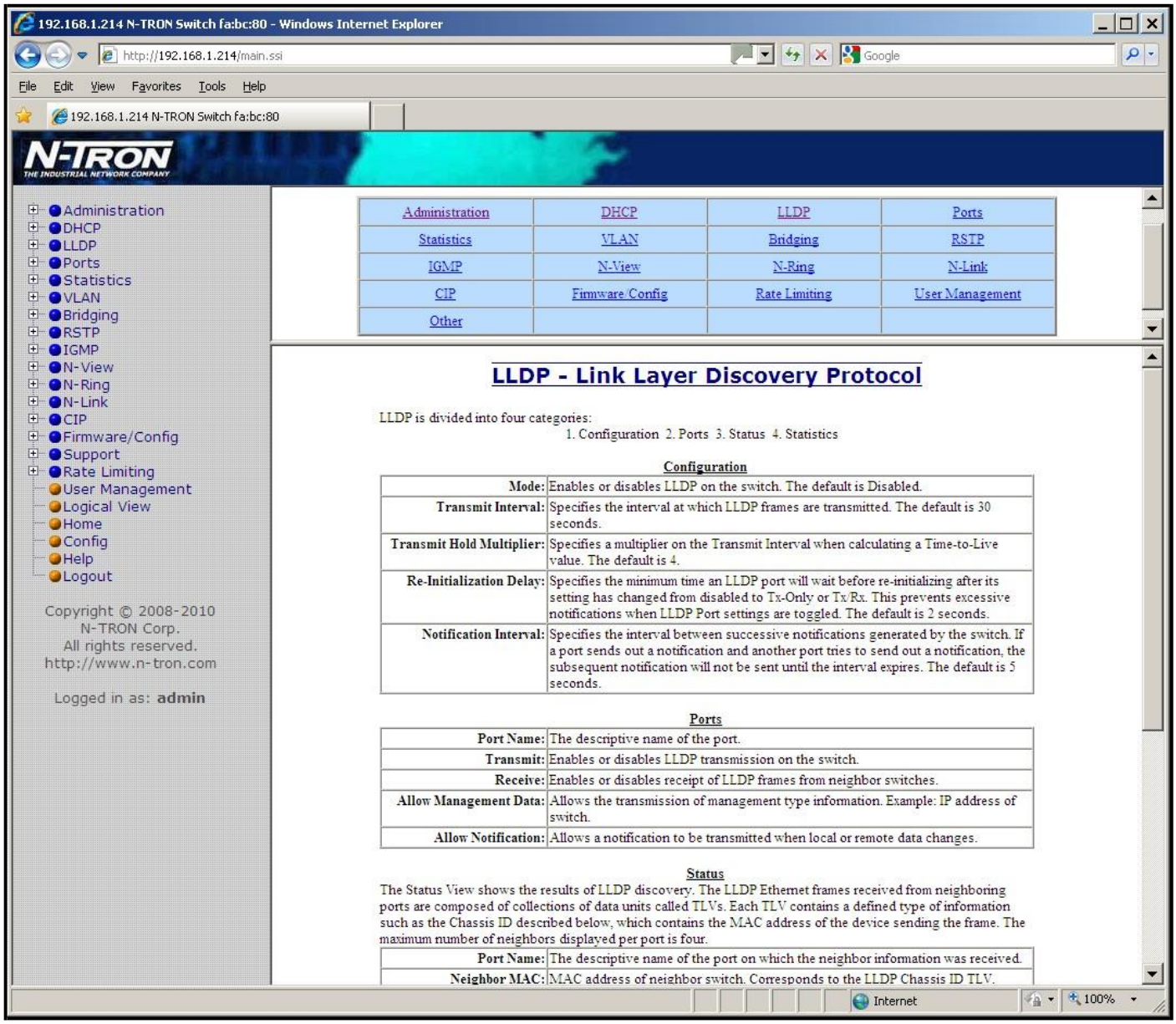
Following the Administration link on the help page, the administrator or user can see some information regarding the configuration options in the Administration category on the left side of the web management.

Help – DHCP



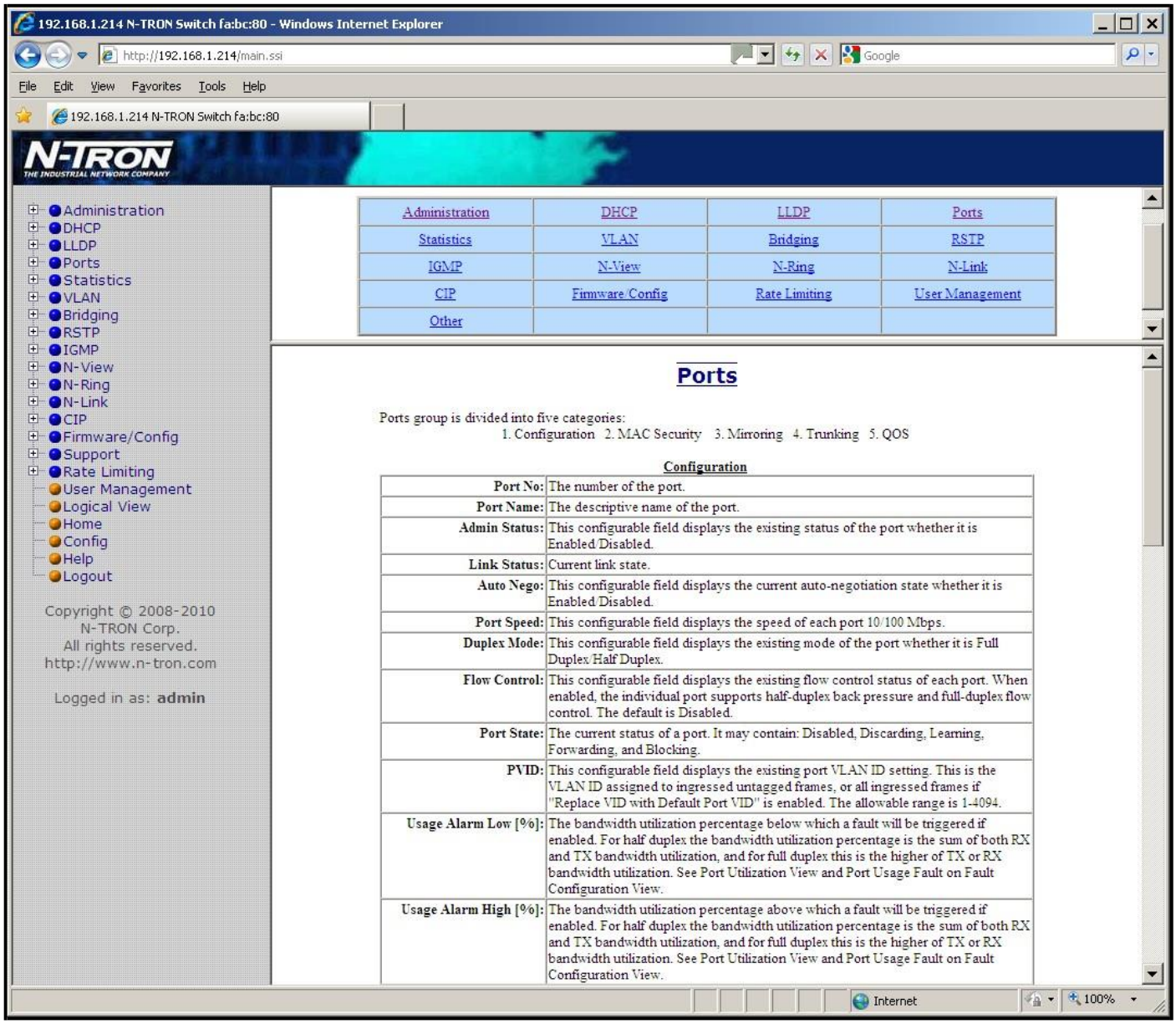
Following the DHCP link on the help page, the administrator or user can see some information regarding the configuration options under the DHCP categories on the left side of the web management.

Help – LLDP



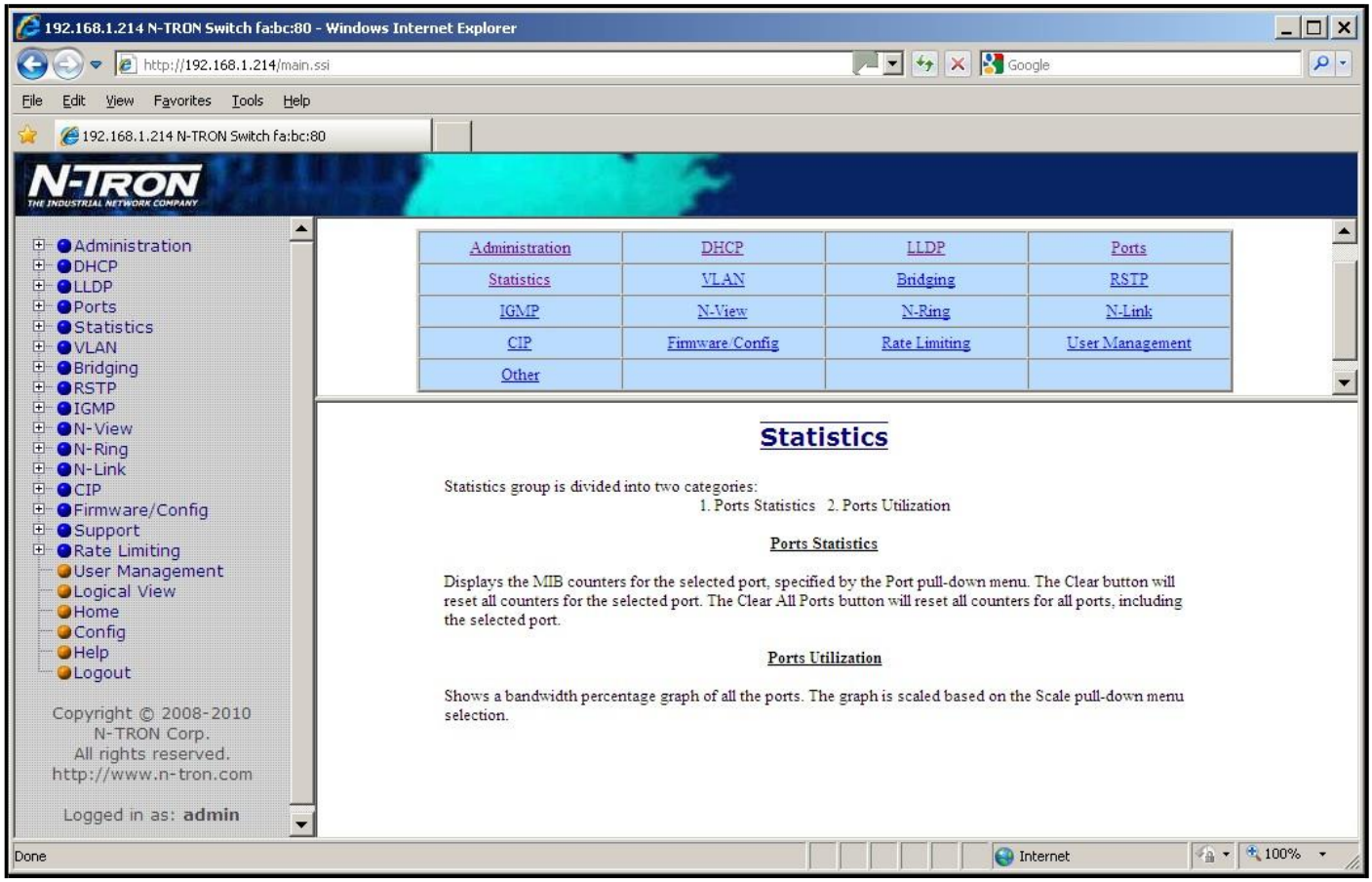
Following the LLDP link on the help page, the administrator or user can see some information regarding the configuration options in the LLDP category on the left side of the web management.

Help – Ports



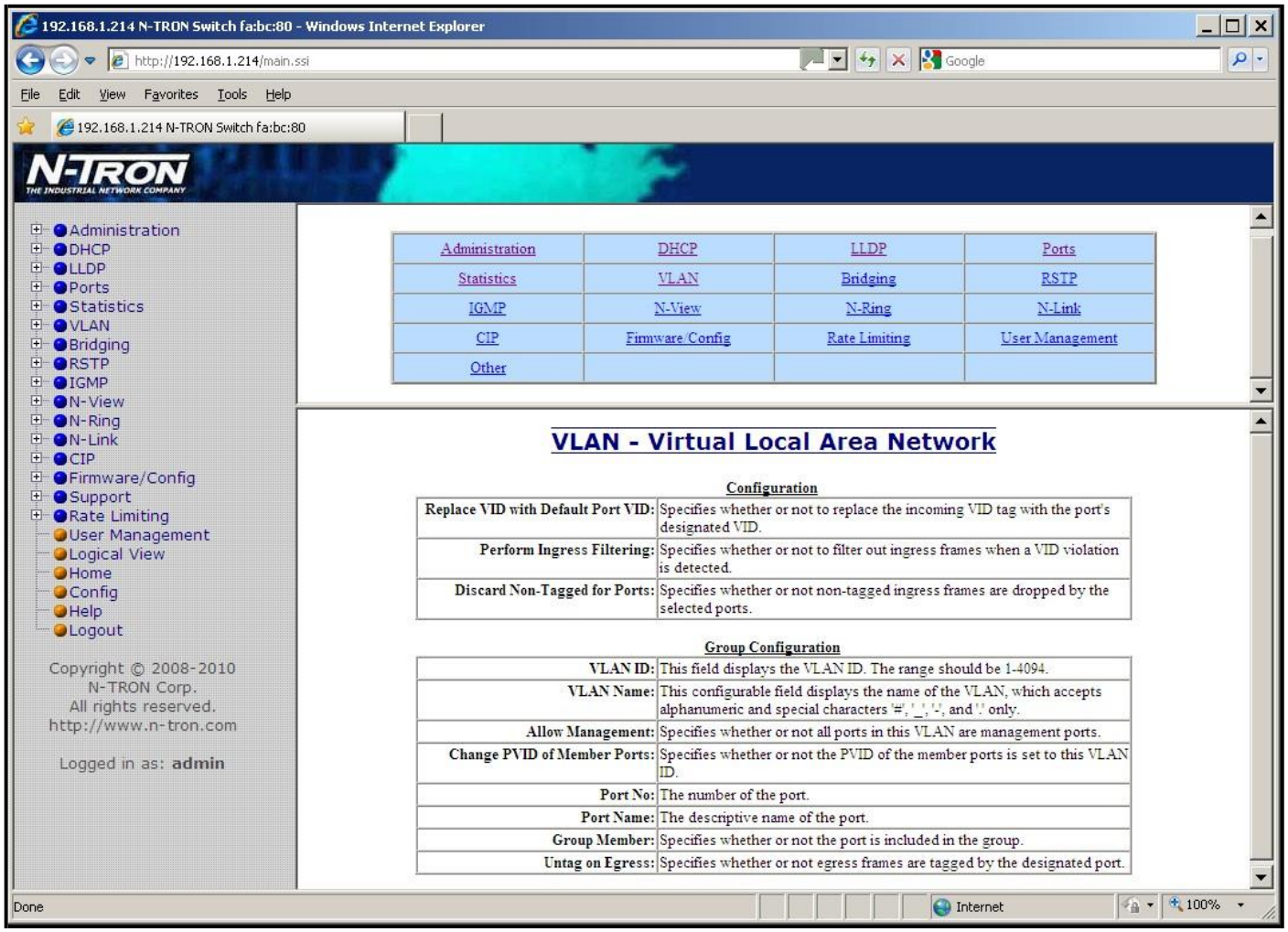
Following the Ports link on the help page, the administrator or user can see some information regarding the configuration options in the Ports category on the left side of the web management.

Help – Statistics



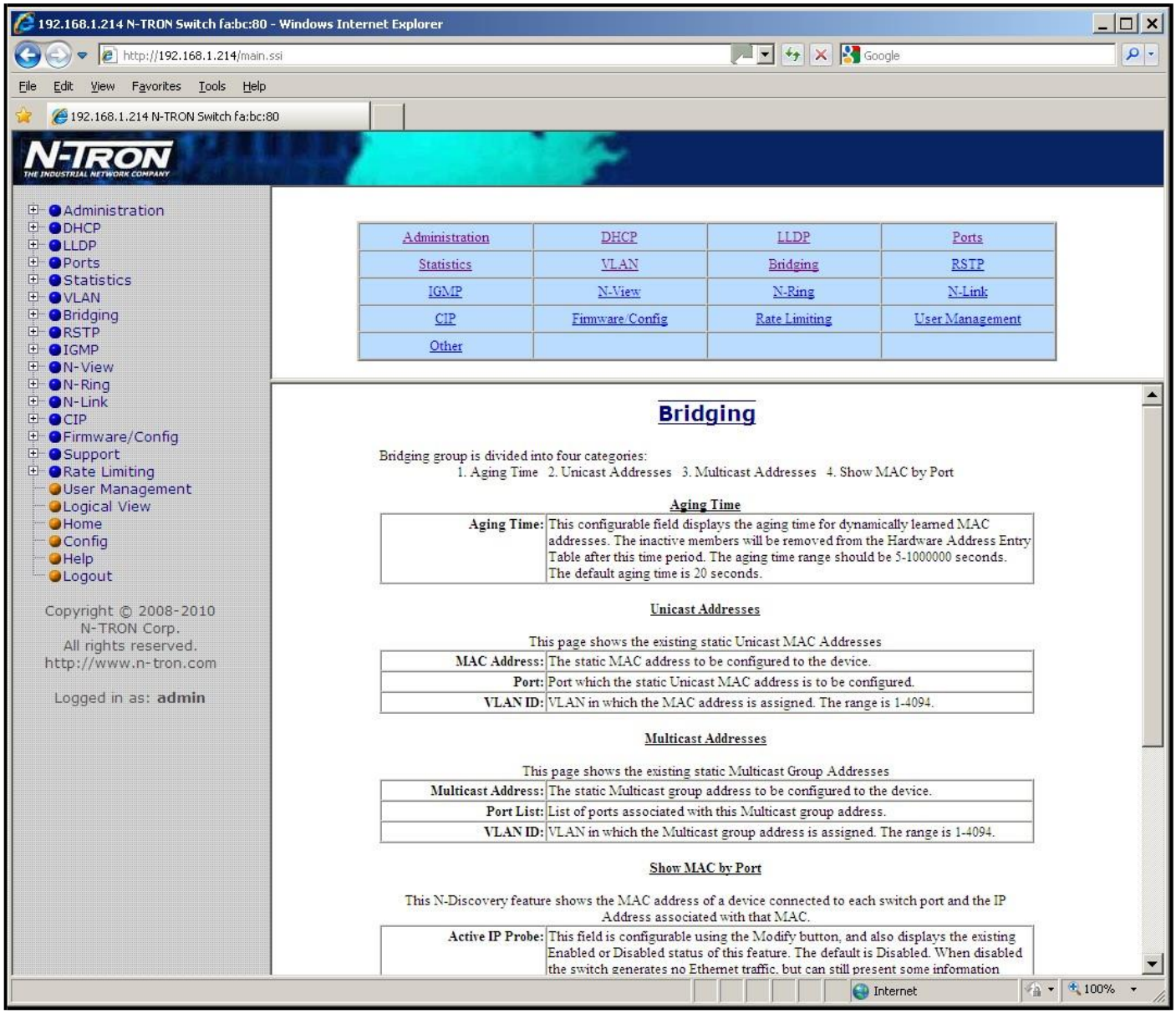
Following the Statistics link on the help page, the administrator or user can see some information regarding the configuration options in the Statistics category on the left side of the web management.

Help – VLAN



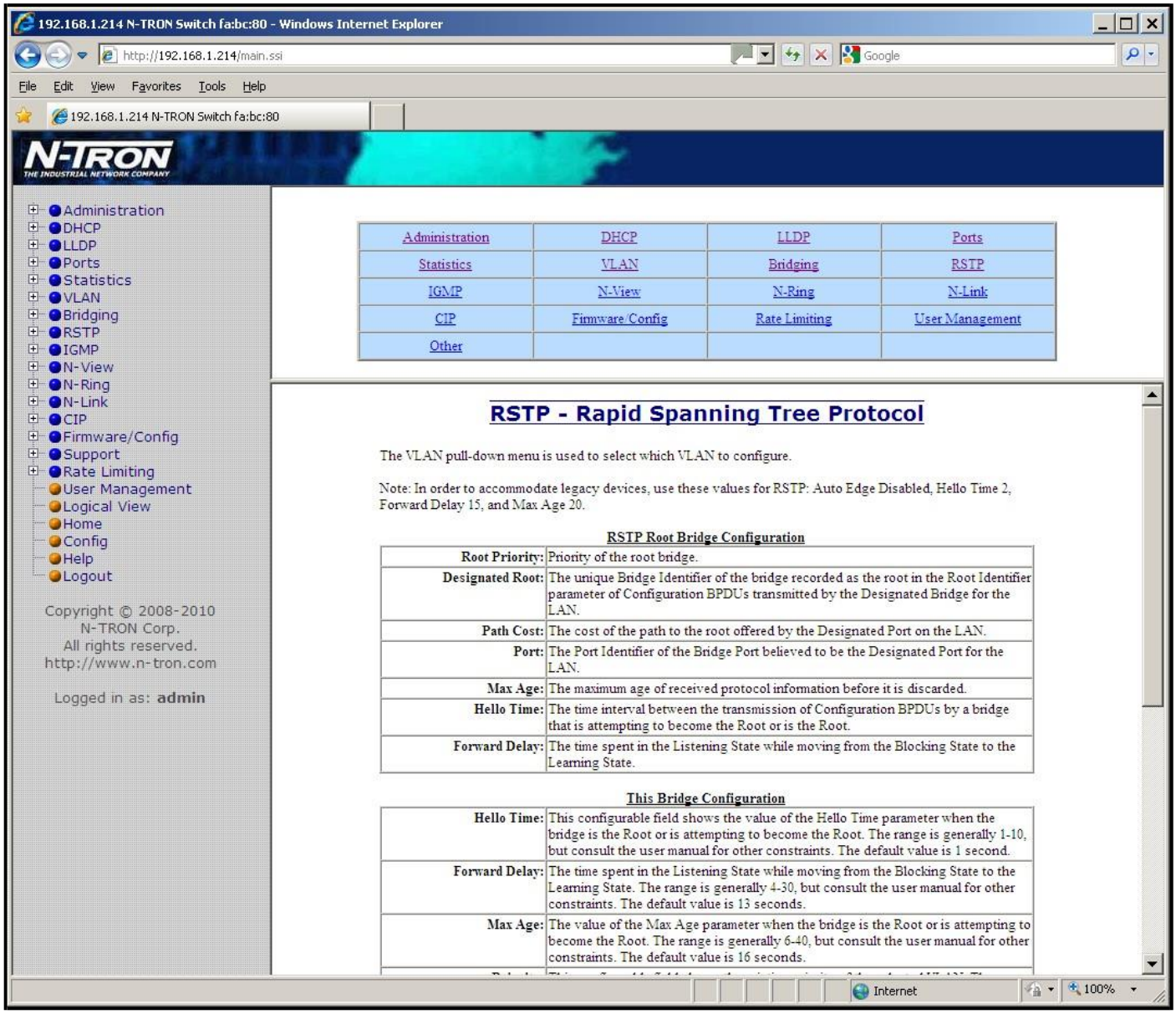
Following the VLAN link on the help page, the administrator or user can see some information regarding the configuration options in the VLAN category on the left side of the web management.

Help – Bridging



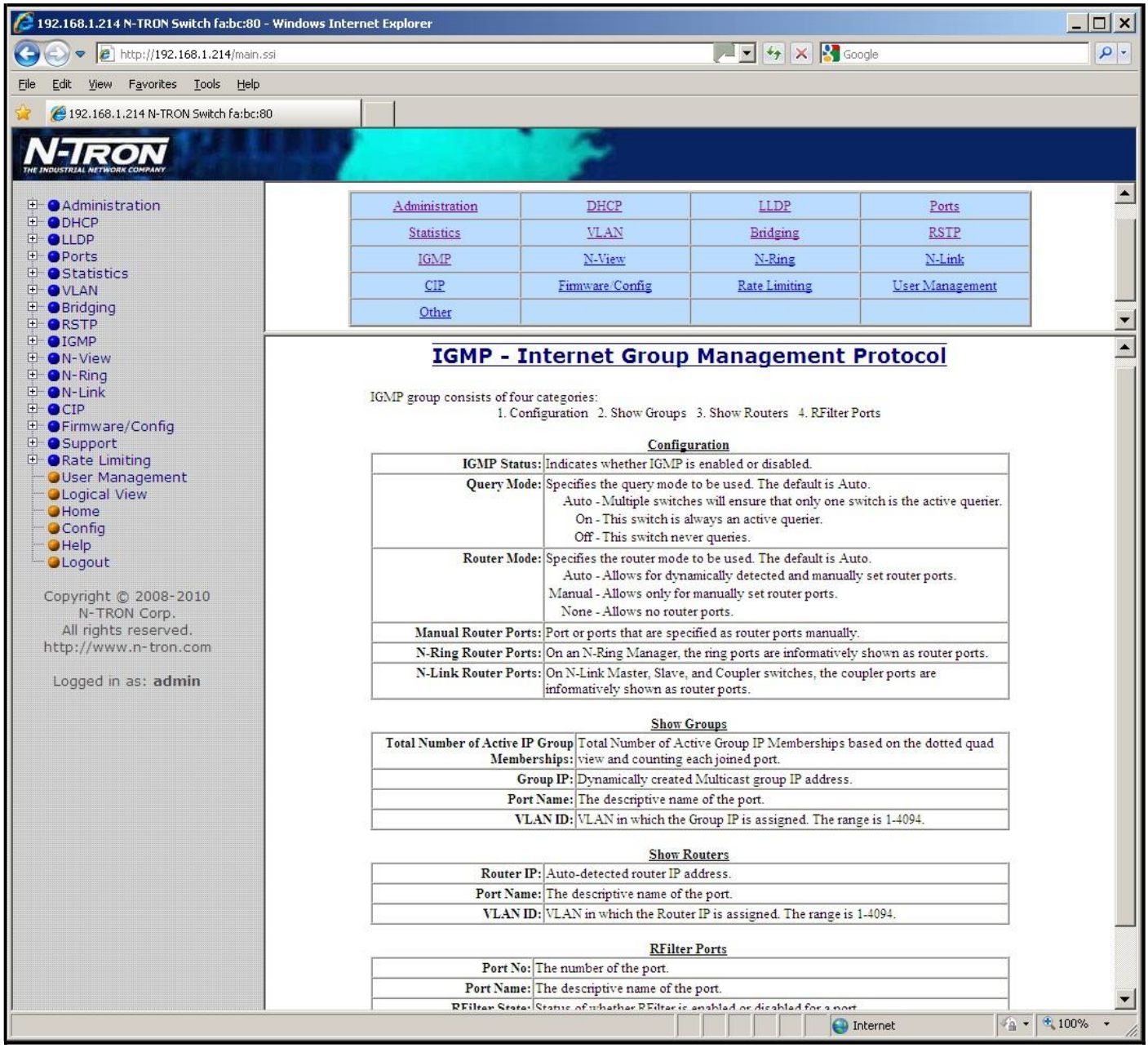
Following the Bridging link on the help page, the administrator or user can see some information regarding the configuration options in the Bridging category on the left side of the web management.

Help – RSTP



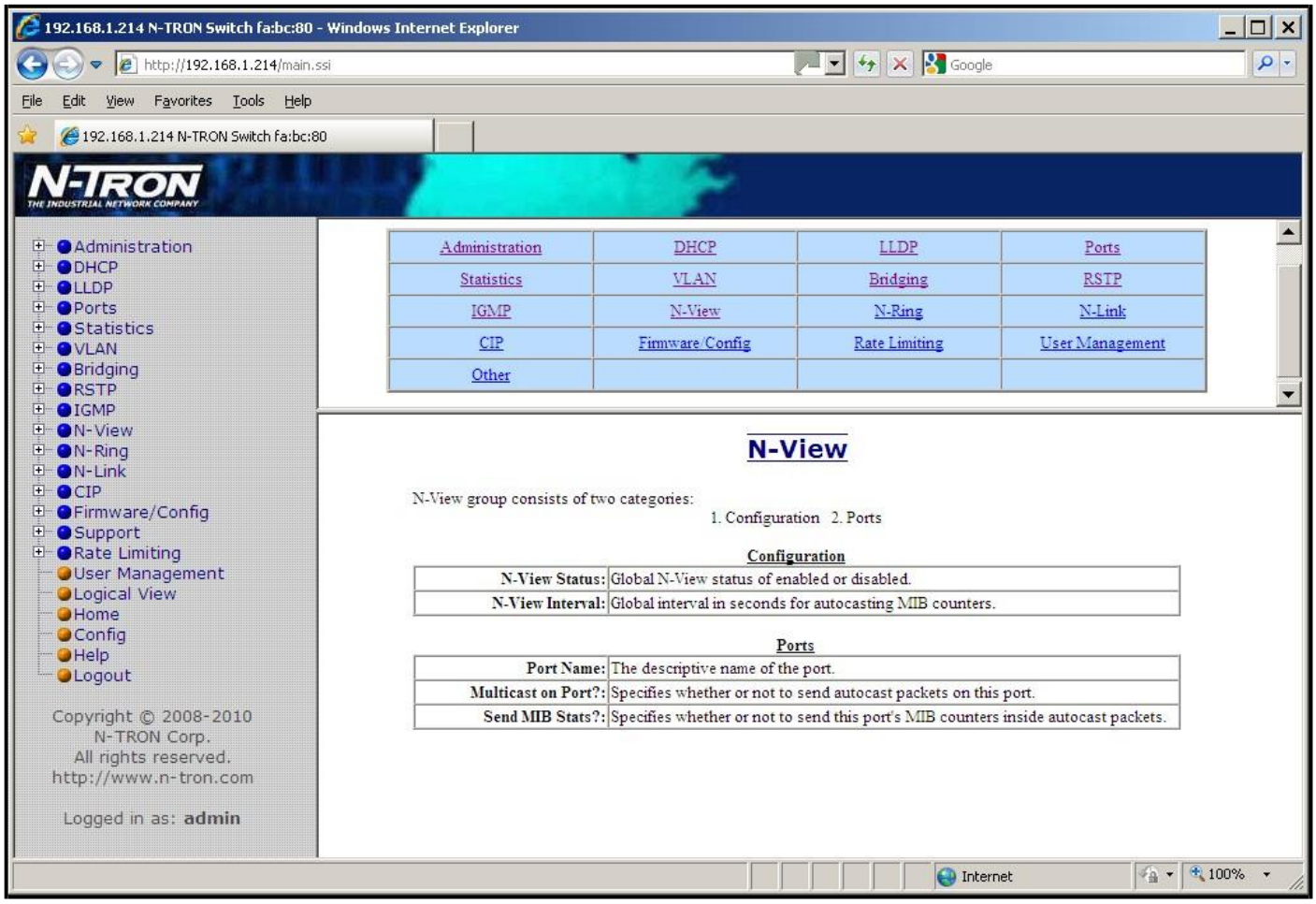
Following the RSTP link on the help page, the administrator or user can see some information regarding the configuration options in the RSTP category on the left side of the web management.

Help – IGMP



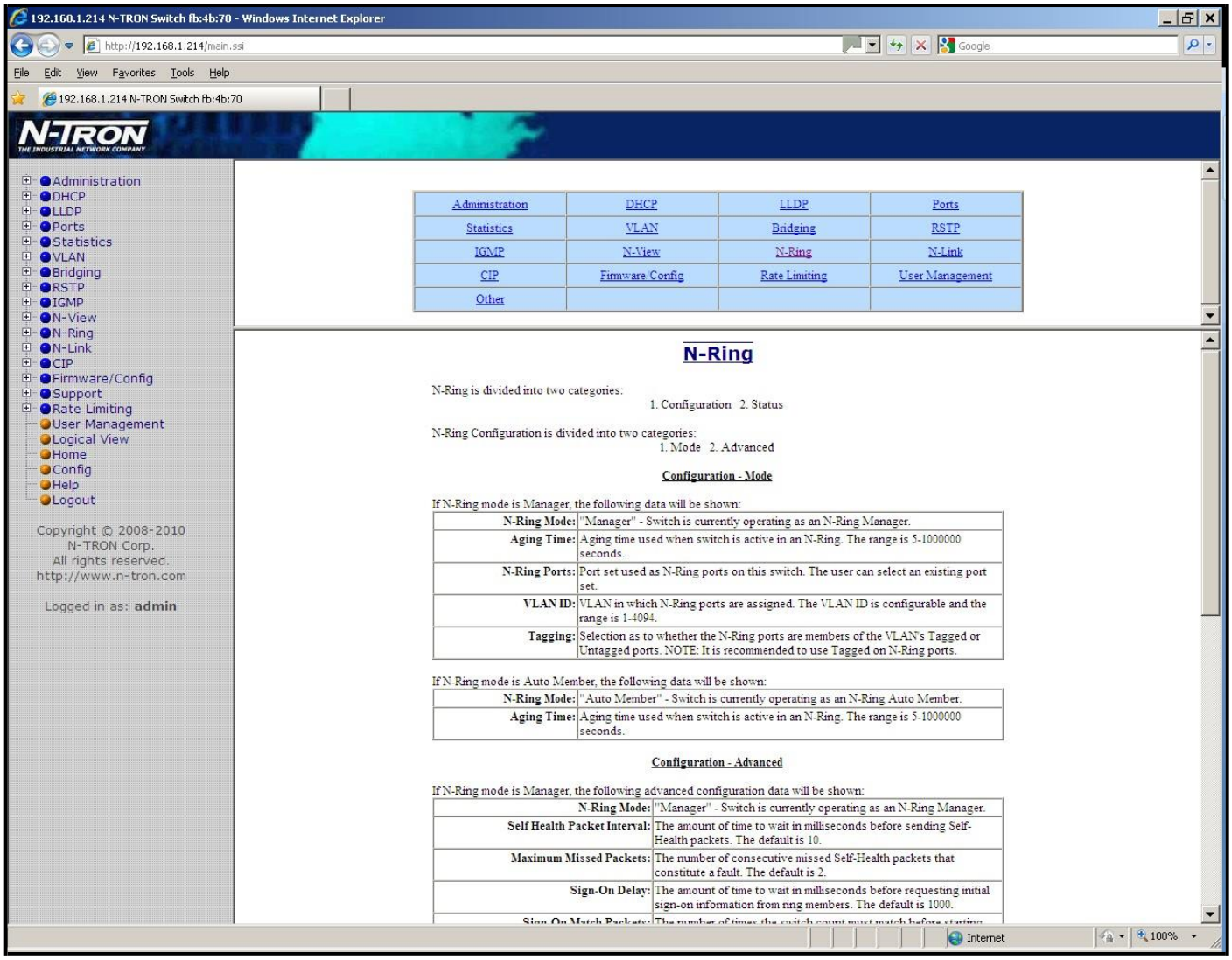
Following the IGMP link on the help page, the administrator or user can see some information regarding the configuration options in the IGMP category on the left side of the web management.

Help – N-View



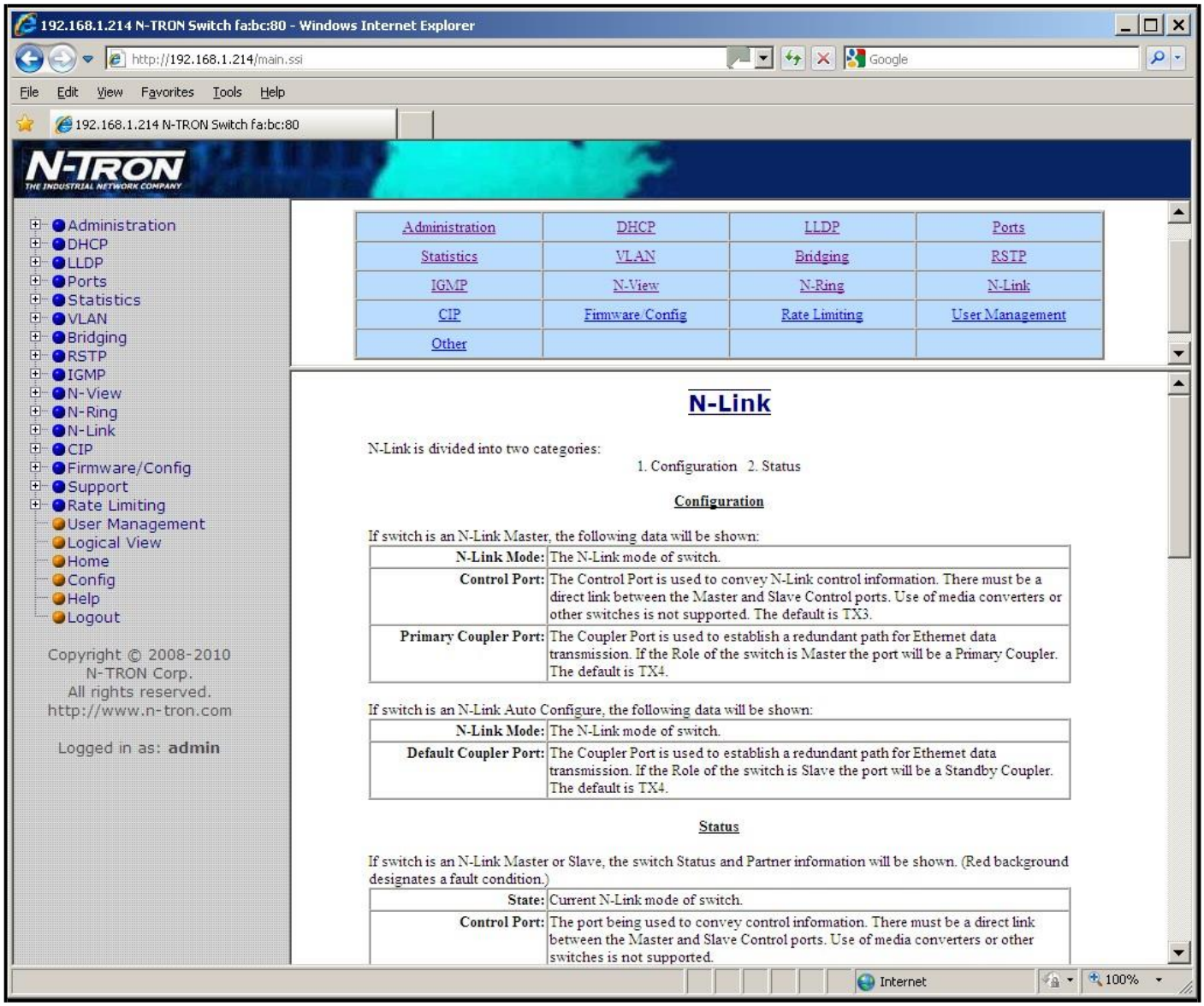
Following the N-View link on the help page, the administrator or user can see some information regarding the configuration options in the N-View category on the left side of the web management.

Help – N-Ring



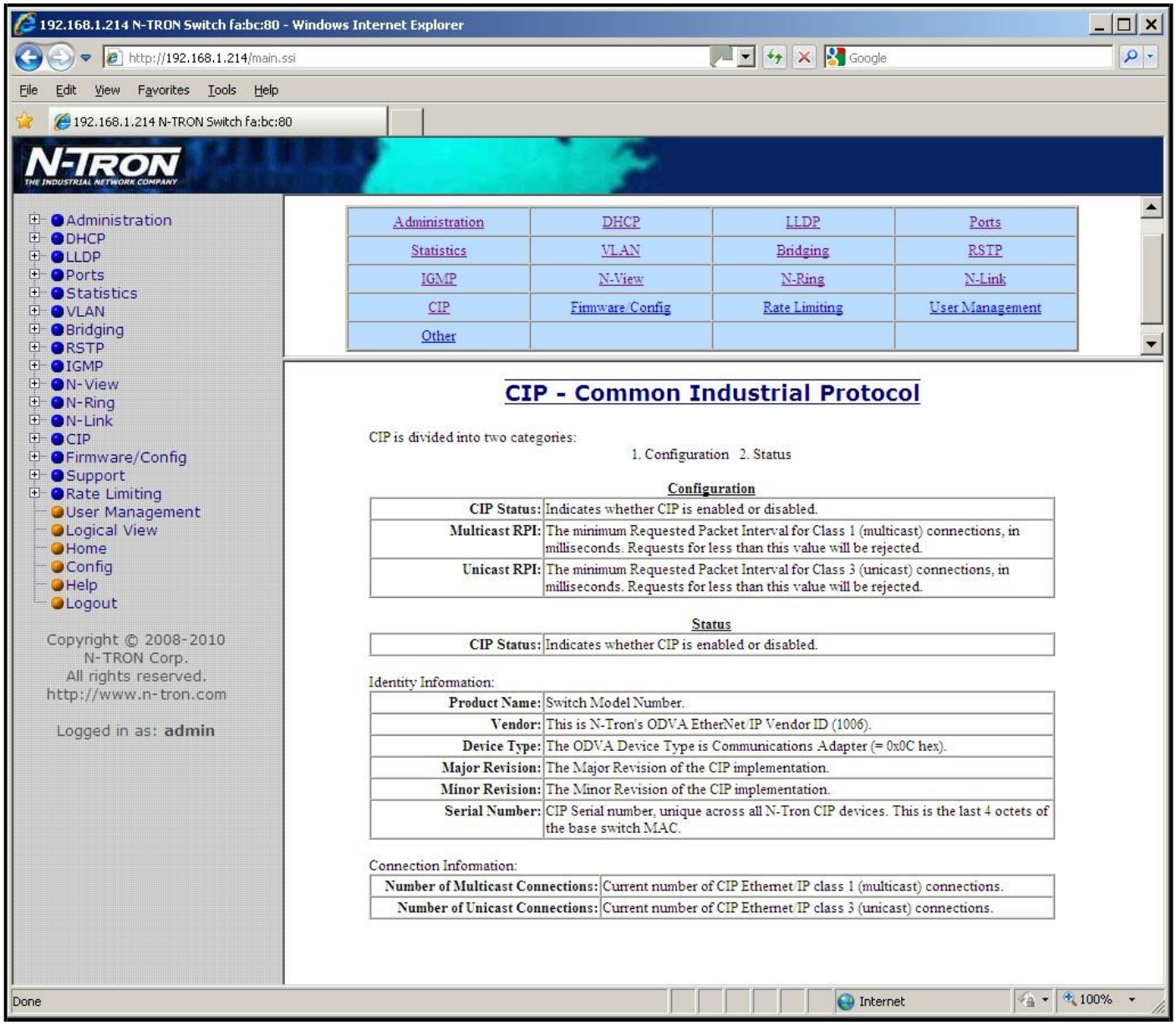
Following the N-Ring link on the help page, the administrator or user can see some information regarding the configuration options in the N-Ring category on the left side of the web management.

Help – N-Link



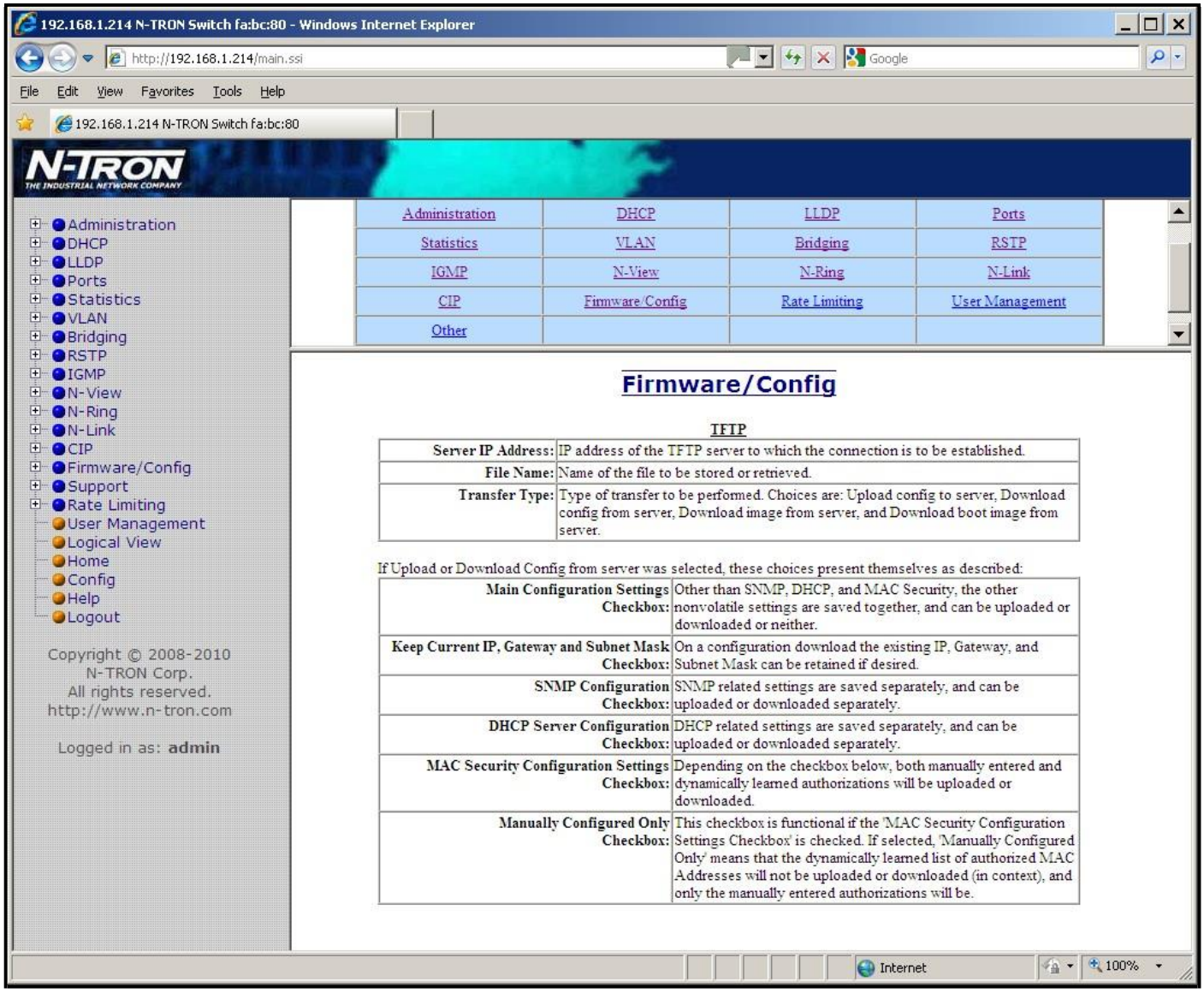
Following the N-Link link on the help page, the administrator or user can see some information regarding the configuration options in the N-Link category on the left side of the web management.

Help – CIP



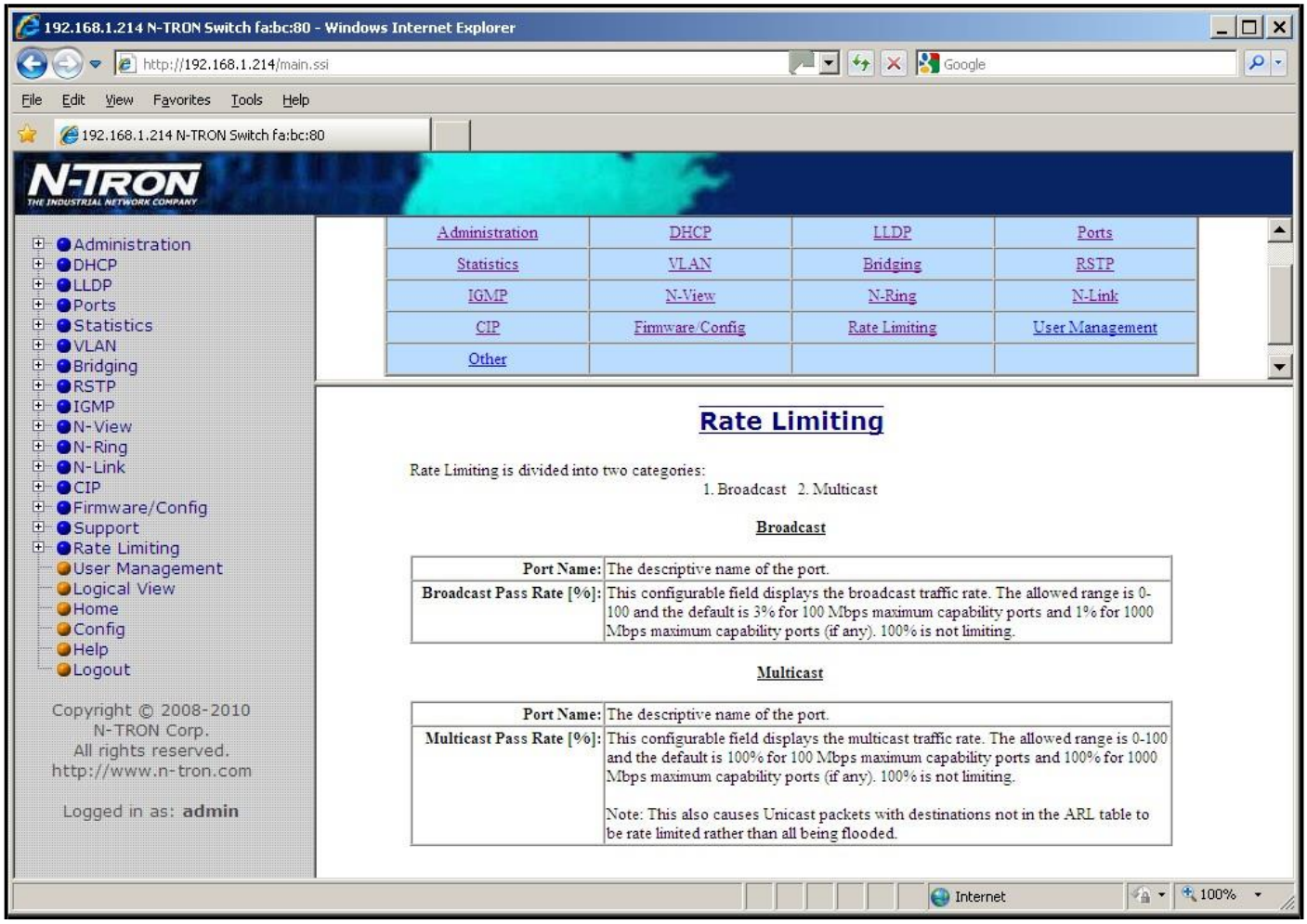
Following the CIP link on the help page, the administrator or user can see some information regarding the configuration options in the CIP category on the left side of the web management.

Help – Firmware/Config



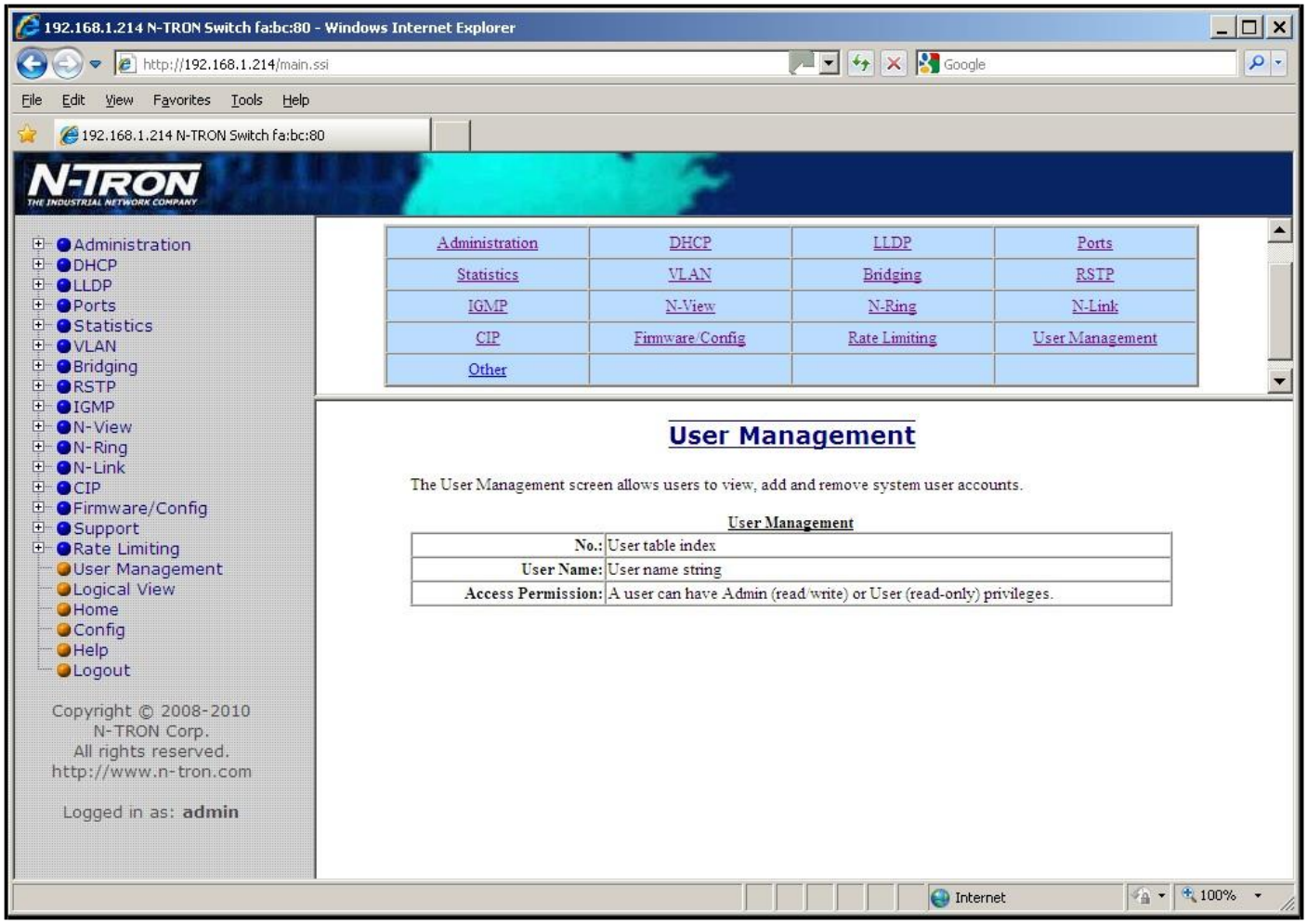
Following the Firmware/Config link on the help page, the administrator or user can see some information regarding the configuration options in the Firmware/Config category on the left side of the web management.

Help – Rate Limiting



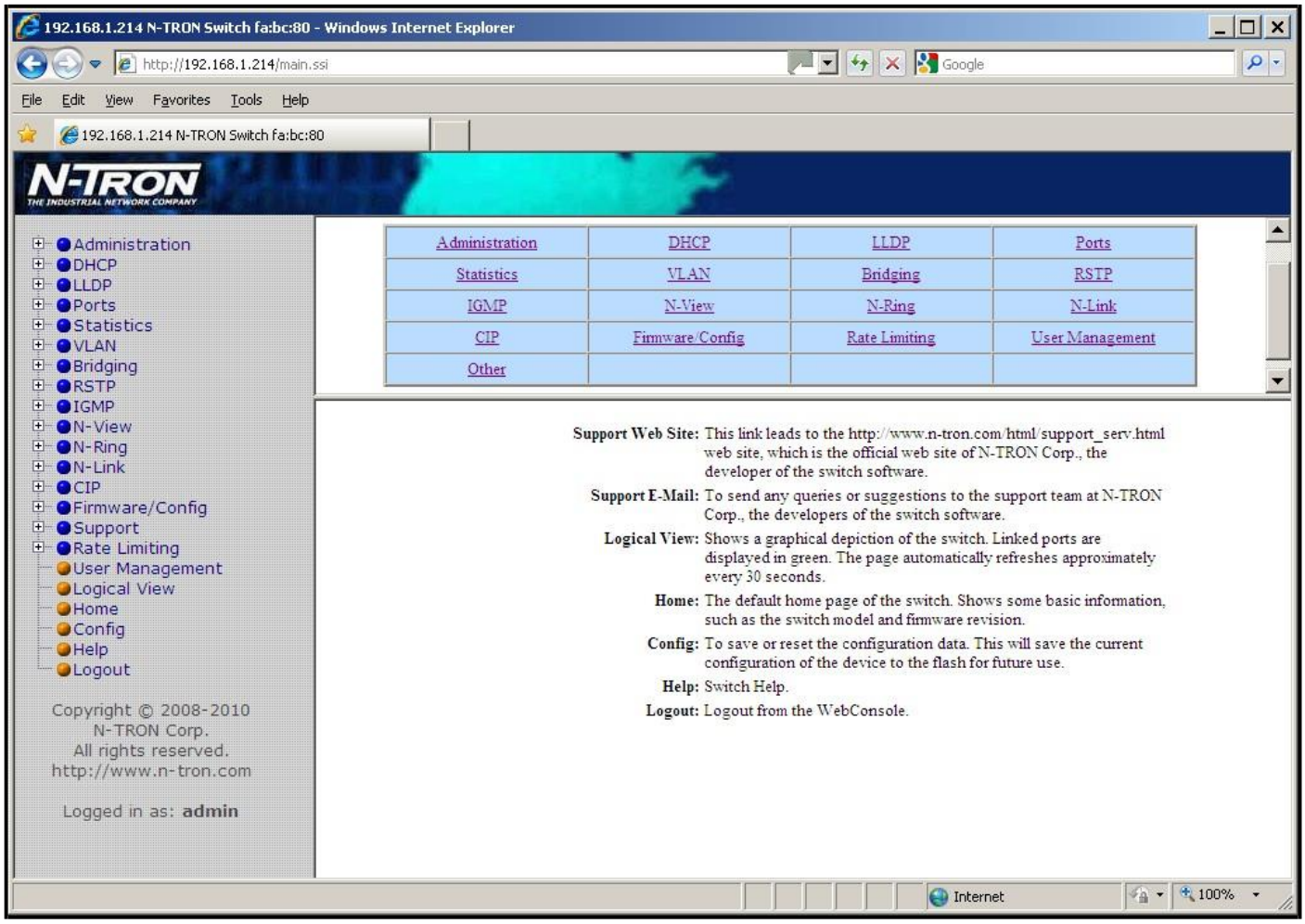
Following the Rate Limiting link on the help page, the administrator or user can see some information regarding the configuration options in the Rate Limiting category on the left side of the web management.

Help – User Management



Following the User Management link on the help page, the administrator or user can see some information regarding the configuration options in the User Management category on the left side of the web management.

Help – Other



Following the Other link on the help page, the administrator or user can see some information regarding other links or categories on the left hand side of the web manager, as above.

CLI Commands

"?" (Help)

Command Name	**"?"**
Description	Show a list of all commands or get help on a specific command. Without *cmd*, this command will list all the available commands. If *cmd* is specified and if it matches a specific command, the **usage** of the command will be displayed; otherwise, if *cmd* matches the prefix of a command, the name of the command will be listed. If **?** is preceded by another **?**, the usage and description of this command will be displayed.
Syntax	**?** [cmd]
Parameters	**cmd** The command for which to get help.
Examples	**N-TRON/Admin> ?** *The above command displays all the available commands.* **N-TRON/Admin> abcd ?** Unknown Command: "abcd" Type "?" for a list of available commands. **N-TRON/Admin> logout ?** Logout Log out of console interface. SYNTAX: Logout **N-TRON/Admin> ? pi** Ping Ping a host. … **N-TRON/Admin> ? ?** ? Show a list of all commands or get help on a specific command. SYNTAX: ? [cmd] OPTIONS: cmd : The command for which to get help.
NOTES	

Logout

Command Name	**logout**
Description	Log out of console interface
Syntax	**logout**
Parameters	**None**
Examples	**N-TRON/Admin> logout**
NOTES	

CLI Commands, Continued…

Show, Add, or Delete ARL Entries

Command Name	**arl**
Description	Show, Add, or Delete Arl Entries.
Syntax	**arl** show | showmct | add mac port cpu static vid | del[ete] mac vid
Parameters	**show** Show entire ARL table. **showmct** Show entire ARL MCT (Multicast Index) table (cache). **showmcthw** Show entire ARL MCT (Multicast Index) table (Hardware). **delete** Delete MAC address. **add** Add MAC address. **mac** MAC Address. **port** Port Number. **cpu** 1 = Send to CPU also. **static** 1 = This is a static address; 0 = Non-Static. **vid** VLAN ID (0-4095)
Example	**N-TRON/Admin> arl show** **No. Val Age Pri Mod Usr Sta VLAN MAC I Port(s)** **---- --- --- --- --- --- --- ---- ----------------- - ----------** **1 1 - - 0 0 1 3333 01:07:af:fa:bc:80 (None)** **2 1 - - 0 0 1 1 01:00:5e:7f:ff:fa TX7** **3 1 - - 0 0 1 3333 01:07:af:00:df:48 (None)** **4 1 - - 0 0 1 3333 01:07:af:00:de:d2 (None)** **5 1 - - 0 0 1 3333 01:07:af:00:de:f0 (None)** **6 1 - - 0 0 1 3333 01:07:af:00:de:f1 (None)** **7 1 - - 0 0 1 3333 01:07:af:00:de:f2 (None)** **8 1 1 0 0 0 1 1 00:07:af:fa:bc:80 CPU** **9 1 - - 0 1 1 0 01:07:af:01:3d:1b CPU** **10 1 - - 0 2 1 0 01:07:af:00:de:d1 CPU** **11 1 - - 0 3 1 0 01:80:c2:00:00:00 CPU** **N-TRON/Admin> arl showmct** **No. Idx Val Port Mask ModTime ms Refs Port(s)** **--- --- --- ---------- ---------- ---- ----------** **1 0 1 0x00000000 1920 6 (None)** **2 1 1 0x00000040 134810 0 TX8** **3 2 1 0x00000080 2160000 1 TX7** **N-TRON/Admin> arl add 00:19:b9:03:aa:79 3 0 1 1** **N-TRON/Admin> arl del 00:19:b9:03:aa:79 1**
Notes	

CLI Commands, Continued…

Configuration Device Operations

Command Name	**cfgdev**
Description	Info, Format, Compare and Erase Configuration Device.
Syntax	**CfgDev** info | format [-m model] | compare | erase
Parameters	**Info** Show information about the configuration device. **Compare** Compare the configuration of the switch to the configuration device. **Erase** Erase the switch configuration on the configuration device.
Example	**N-TRON/Factory> cfgdev info** Port A: 0xd080 Board ID: 0x0005 (5) Configuration device information: Name : SDS128M Model : 3 Version : 1 Page Size : 200 Total Size : 127008768 Max Clock (Hz) : 400000 Write Cycles (ns): 5000000 Flags : 0x00000001 **N-TRON/Factory> cfgdev compare** Comparing switch configuration to the configuration device... The configurations are different. **N-TRON/Factory> cfgdev erase** Erasing configuration device... Configuration device erase completed.
Notes	

CLI Commands, Continued…

Show or Set CIP Configuration

Command Name	**Cip**
Description	Show or set CIP configuration. If no parameters are specified, this command will show the CIP configuration (same as -show parameter).
Syntax	**-Cip [-e[nable] | -d[isable] | -show]**
Parameters	**-Cip -show** Show CIP configuration. **-Cip [-e[nable] | -d[isable]]** Set the CIP status to e(nabled) or d(isabled).
Examples	**N-TRON/Admin> cip –show** CIP Configuration: ------------------ Status: Enabled EthIp Interval: 10 ms Cache Interval: 2000 ms Identity Information: --------------------- Product Name: N-TRON 7900 Vendor: 1006 (N-TRON) Device Type: 0x0C (Communications Adapter) Major Revision: 1 Minor Revision: 5 Serial Number: 0xAF7EAFA0 Connection Information: ----------------------- Multicast Connections: 0 Unicast Connections: 0 N-TRON/Admin> **N-TRON/Admin> cip -disable** Changing CIP configuration... CIP Configuration: ------------------ Status: Disabled EthIp Interval: 10 ms Cache Interval: 2000 ms Identity Information: --------------------- Product Name: N-TRON 7900 Vendor: 1006 (N-TRON) Device Type: 0x0C (Communications Adapter) Major Revision: 1 Minor Revision: 5 Serial Number: 0xAF7EAFA0 Connection Information: ----------------------- Multicast Connections: 0 Unicast Connections: 0 N-TRON/Admin>
NOTES	

CLI Commands, Continued…

Save or Reset the Configuration Settings

Command Name	**config**
Description	Save or reset configuration settings
Syntax	**config** s[ave] | r[eset]
Parameters	**save** save current running configuration settings. **reset** reset configuration settings to factory defaults.
Examples	**N-TRON/Admin> config save** Save Settings... Settings have been saved. **N-TRON/Admin> config reset** Resetting to factory defaults... Load factory default settings [y/n]?y Keep IP, subnet mask, and gateway addresses [y/n]?n Keep current user names and passwords [y/n]?n Keep current SNMP settings [y/n]?n Keep current DHCP Server settings [y/n]?n Keep current MAC Security settings [y/n]?n…
NOTES	

Show or Set IGMP Configuration

Command Name	**igmp**
Description	Show or set IGMP configuration. If no parameters are specified, this command will show the IGMP configuration (same as -show parameter).
Syntax	**igmp** [-show] [-status state]
Parameters	**-show** Show configuration. **-status state** Set the IGMP status to e(nabled) or d(isabled).
Examples	**N-TRON/Admin> igmp -show** **IGMP Status : Enabled** **IGMP Version : 2** **Query Mode : Auto** **CIP Querier Status : 2, Active-Auto** **Active Querier IP : 192.168.1.201** **Router Mode : Auto** **Manual Router Ports : (None)** **IGMP Resource Usage % : 1** **IGMP multicast destination addresses: 1** **IGMP Number Of Active IP Group Memberships: 1** **N-TRON/Admin> igmp -status disabled** **IGMP Status : Disabled** **IGMP Version : 2** **Query Mode : Auto** **CIP Querier Status : 2, Active-Auto** **Active Querier IP : 0.0.0.0** **Router Mode : Auto** **Manual Router Ports : (None)** **IGMP Resource Usage % : 1** **IGMP multicast destination addresses: 0** **IGMP Number Of Active IP Group Memberships: 0** **Changes have been made that have not been saved.**
NOTES	

CLI Commands, Continued…

Show or Set Mirror Configuration

Command Name	**Mirror**
Description	Show or set Mirror configuration. If no parameters are specified, this command will show the Mirror configuration (same as -show parameter).
Syntax	**mirror** [-show] [-status state] [-dp portno] [-tx portlist] [-rx portlist]
Parameters	**-show** Show configuration. **-status state** Set the Mirror status to e(nabled) or d(isabled). **-dp portno** Set the destination port number for mirrored frames. **-tx portlist** Set the source ports to mirror frames that are transmitted. **-rx portlist** Set the source ports to mirror frames that are received.
Examples	**N-TRON/Admin> mirror –show** Mirror Status : Disabled Destination Port : TX1 Tx Source Ports : (None) Rx Source Ports : (None) **N-TRON/Admin> mirror –status enabled –dp 6 –tx 1,3-5 –rx 1,3,5** Mirror Status : Enabled Destination Port : TX6 Tx Source Ports : TX1, TX3-TX5 Rx Source Ports : TX1, TX3, TX5 Changes have been made that have not been saved. …
NOTES	The portlist consists of port numbers and ranges, separated by commas. It may not contain space characters. Use “all” to set all ports as source ports, and use “none” to clear all ports from source ports.

CLI Commands, Continued…

Show or Set N-Ring Configuration

Command Name	**Nring**
Description	Show or set N-Ring configuration. If no parameters are specified, this command will show the N-Ring configuration (same as -show parameter).
Syntax	**nring** [-show] [-mode d | a | m] [-ports set_id]
Parameters	**-show** Show configuration. **-mode** Set the N-Ring mode. d = disabled, a = auto member, m = manager **-ports** set_id Set the ring ports for N-Ring manager mode. Specify port set identifier or use '?' to list available port sets.
Examples	**N-TRON/Admin> nring -show** N-Ring Mode : Auto Member Aging Time : 20 **N-TRON/Admin> nring -ports ?** **ID Port Set** **-- --------** **1 TX1 / TX2** **2 TX7 / TX8** **3 GB1 / GB2** **N-TRON/Admin> nring -mode m -ports 2** Do you Want to Save Changes and Restart the System Now [y/n]? …
NOTES	

Show or Set N-View Configuration

Command Name	**Nview**
Description	Show or set N-View configuration. If no parameters are specified, this command will show the N-View configuration (same as -show parameter).
Syntax	**nview** [-show] [-status state]
Parameters	**-show** Show configuration. **-status state** Set the N-View status to e(nabled) or d(isabled).
Examples	**N-TRON/Admin> nview -show** N-View Status : Enabled N-View Interval : 5 **N-TRON/Admin> nview -status disabled** N-View Status : Disabled N-View Interval : 5 Changes have been made that have not been saved. …
NOTES	

CLI Commands, Continued…

Ping a Host

Command Name	**Ping**
Description	Ping a host
Syntax	**ping** [-t] [-n count] [-w timeout] target_name
Parameters	**target_name** IP Address or host name. **-t** Ping the specified host until stopped. To see statistics and continue - type Space; To stop - type Control-C. **-n count** Number of echo requests to send. **-w timeout** Timeout in milliseconds to wait for each reply.
Example	**N-TRON/Admin> ping 192.168.1.119** … **N-TRON/Admin> ping -n 6 192.168.1.119** … **N-TRON/Admin> ping -t 192.168.1.119** … **N-TRON/Admin> ping -w 2000 192.168.1.119** Reply from 192.168.1.119: time=970ms Reply from 192.168.1.119: time<10ms Reply from 192.168.1.119: time<10ms Ping statistics for 192.168.1.119: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss) Approximate round trip times in milliseconds: Minimum = 0ms, Maximum = 970ms, Average = 320ms
Notes	

CLI Commands, Continued…

Show or Set Port Configuration

Command Name	**Port**
Description	Show or set Port configuration.
Syntax	**port** [-show] [-admin state] [-sd auto | 10h | 10f | 100h | 100f | 1000h | 1000f] [-flow state] [-fhp state] [-dp prio] [-dscp state] [-8021p state] [-pvid vid] [-ual percent] [-uah percent] [-security state] portno
Parameters	**Portno** Port number to configure or show. Specify "all" to show all ports. **-show** Show configuration. **-admin state** Set the admin status for the port to e(nabled) or d(isabled). **-sd** Set the speed and duplex mode for the port. auto = enable auto-negotiation **-flow state** Set the flow control for the port to e(nabled) or d(isabled). **-fhp state** Set force high priority for the port to e(nabled) or d(isabled). **-dp** Set the default QOS priority for the port. The range is 0-7. **-dscp state** Set the DSCP Priority for the port to e(nabled) or d(isabled). **-8021p state** Set the 802.1p Priority for the port to e(nabled) or d(isabled). **-pvid** Set the VLAN ID for the port. The range is 1-4094. **-ual percent** Set the usage alarm low percentage. The range is 0-100. **-uah percent** Set the usage alarm high percentage. The range is 0-100. **-security state** Set the security status for all supported ports to e(nabled) or d(isabled).
Examples	**N-TRON/Admin> port –sd 100f –flow enabled –dp 7 –pvid 2 5** Port Port Admin Link Auto Port Dupl Flow Force Def Port No Name Status Stat Nego Spd Mode Control High Pri Pri State PVID ---- ---- -------- ---- -------- ---- ---- -------- -------- --- ---------- ---- 5 TX5 Enabled Down Disabled 100 Full Enabled Disabled 7 Disabled 2 Changes have been made that have not been saved. N-TRON/Admin> port -sd 100f -flow enabled -dp 7 -pvid 2 5 Usage Usage Security Port Port Admin Link Auto Port Dupl Flow Force Include Include Def Port Alarm Alarm Status= No Name Status Stat Nego Spd Mode Control High Pri DSCP 802.1p Pri State PVID Low % High % Learning ---- ---- -------- ---- -------- ---- ---- -------- -------- -------- -------- --- ---------- ---- ----- ------ -------- 5 TX5 Enabled Down Disabled 100 Full Enabled Disabled Enabled Enabled 7 Disabled 2 0 100 Disabled Changes have been made that have not been saved. N-TRON/Admin>…
NOTES	

CLI Commands, Continued…

Reset the Switch

Command Name	**Reset**
Description	Reset (reboot) the switch
Syntax	**Reset**
Parameters	**None**
Example	**N-TRON/Admin> reset** **Preparing for reset.** **Cleaning up...** **Browser will be redirected to 192.168.1.250.** **Disabling SNMP...** **Disabling DHCP...** **Disabling CIP...** **Locking out other processes...** **Disable preemption...** **Resetting device...** …
Notes	

Show or Set SNMP Configuration

Command Name	**Snmp**
Description	Show or set SNMP configuration. If no parameters are specified, this command will show the SNMP configuration (same as -show parameter).
Syntax	**snmp** [-show] [-ro name] [-rw name] [-trap name]
Parameters	**-show** Show configuration. **-ro name** Set the Authorized Community Name for SNMP Get requests. **-rw name** Set the Authorized Community Name for SNMP Set requests. **-trap name** Set the Authorized Community Name for SNMP Traps.
Examples	**N-TRON/Admin> snmp –ro users** IP Address - Trap Stn.#1 : Value Not Configured IP Address - Trap Stn.#2 : Value Not Configured IP Address - Trap Stn.#3 : Value Not Configured IP Address - Trap Stn.#4 : Value Not Configured IP Address - Trap Stn.#5 : Value Not Configured Read-Only Community Name : users Read-Write Community Name : private Trap Community Name : public Changes have been made that have not been saved. …
NOTES	Community names may only contain alphanumeric, space, ‘-‘, ‘_’, and ‘#’ characters, and may not begin with a number, space, or underscore. A name with embedded space characters must be enclosed in quotes. The maximum length is 15 characters.

CLI Commands, Continued…

Show or Clear the Last System Error

Command Name	**Syserr**
Description	Show or clear the last system error If *clear* is not supplied, then the last system error is displayed.
Syntax	**syserr** [clear]
Parameters	**Clear** Clear the last system error.
Example	**N-TRON/Admin> syserr** Last System Error: None. **N-TRON/Admin> syserr clear** Last System Error: Cleared.
Notes	

Show System Information

Command Name	**Sysinfo**
Description	Show system information
Syntax	**Sysinfo**
Parameters	**None**
Example	**N-TRON/Admin> sysinfo** **++** **+** **+ N-TRON 700/7000 Series** **+** **++** **+** **+ Model: 7900** **+ Boot Loader: BL 2.0.6.1 (0x02000601)** **+ OS Version: 3.6.8** **+ Build Date: May 15 2012 at 11:41:57** **+ Copyright: Copyright (c) 2008-2012 N-TRON Corp. All rights reserved.** **+** **+ Processor: 66 MHz (66000000)** **+ SDRAM Size: 32 MB** **+ Flash Size: 16 MB** **+ File System: 14548992 Bytes, 10613760 Free, 3935232 Used, 0 Bad** **+ MAC Address: 00:07:af:7e:af:a0** **+ IP Address: 192.168.1.214** **+ Subnet Mask: 255.255.255.0** **+ Gateway: 192.168.1.1** **+ Cfg Device: Generic** **+** **++** **N-TRON/Admin>**
Notes	

Set or Show the System Slots Configuration

Command Name	**SysSlots**
Description	Set or Show system slots configuration
Syntax	**SysSlots [-?] [-a Slot_Type] [-b Slot_Type] [-c Slot_Type] [-d Slot_Type]**
Parameters	**Slot_Types:** **9006TX, 9004FX, 9002FX, or EMPTY**
Examples	**Set:** N-TRON/Admin> SysSlots -a 9006TX -b 9004FX -c 9002FX -d EMPTY Slots Configuration Slot A: 9006TX Slot B: 9004FX (has been changed) Slot C: 9002FX (has been changed) Slot D: EMPTY Changes have been made that have not been saved. Press <ENTER> to Save Changes and Restart the System **Show:** N-TRON/Admin> sysslots Slots Configuration Slot A: 9006TX Slot B: 9004FX Slot C: 9002FX Slot D: EMPTY N-TRON/Admin>

CLI Commands, Continued…

Set or Show the System IP Configuration

Command Name	**Sysip**
Description	Set system IP configuration mode, IP address, subnet mask, and gateway If no parameters are specified, this command will show the system IP addresses. Static IP, subnet mask, or gateway can be set while in either DHCP or static configuration mode as they will be used with IP fallback when in DHCP mode. If the Static IP is set to the default system IP address, IP fallback will not occur. All system addresses must be formatted as: xxx.xxx.xxx.xxx.
Syntax	**sysip** [-c config_mode] [-i static_ip] [-s static_subnet_mask] [-g static_gateway]
Parameters	**-c config_mode** s(tatic) or d(hcp). **-i static_ip** Static IP address (for static config mode and IP fallback). **-s static_subnet_mask** Static sub net mask (for static config mode and IP fallback). **-g static_gateway** Static gateway address (for static config mode and IP fallback).
Example	**N-TRON/Admin> sysip** IP Configuration Mode : Static Static IP Address : 192.168.1.225 Static subnet Mask : 255.255.255.0 Static gateway : 192.168.1.1 **N-TRON/Admin> sysip -c dhcp** IP Configuration Mode : DHCP (has been changed) Fallback IP Address : 192.168.1.225 Fallback Subnet Mask : 255.255.255.0 Fallback Gateway : 192.168.1.1 Press <ENTER> to Save Changes and Restart the System Now … **N-TRON/Admin> sysip -i 192.168.2.119 -s 255.255.252.0 -g 192.168.1.1** IP Configuration Mode : Static Static IP Address : 192.168.2.119 (has been changed) Static Subnet Mask : 255.255.252.0 (has been changed) Static Gateway : 192.168.1.1 (has been changed) Press <ENTER> to Save Changes and Restart the System Now …
NOTES	If mode is set to DHCP and IP fallback occurs, DHCP requests will stop. If mode is set to DHCP and IP Configuration is retrieved from a DHCP server, IP fallback will not occur, even if lease is lost.

CLI Commands, Continued…

Show or Set System Configuration

Command Name	**System**
Description	Show or set System configuration. If no parameters are specified, this command will show the System configuration (same as -show parameter).
Syntax	**system** [-show] [-name label] [-browser state]
Parameters	**-show** Show configuration. **-name label** Set the switch name. **-browser state** Set the browser access status to e(nabled) or d(isabled).
Examples	**N-TRON/Admin> system -name "Private Switch" -browser disabled** **IP Configuration : Static** **Client ID (hex) : 0007affabc80** **IP Address : 192.168.1.214** **Subnet Mask : 255.255.255.252** **Gateway : 192.168.1.1** **MAC Address : 00:07:af:fa:bc:80** **System Up Time : 0 days, 0 hours, 1 mins, 3 secs** **Name : Private Switch** **Contact : N-TRON Admin** **Location : Mobile, AL 36609** **Temperature : 28 C, 82 F** **Upper Threshold : 100 C, 212 F** **Lower Threshold : -60 C, -76 F** **Browser Access : Disabled** **Changes have been made that have not been saved.** **N-TRON/Admin>**
NOTES	A switch name may only contain alphanumeric, space, ':', '-', '_', and '#' characters, and may not begin with a number, space, or underscore. A name with embedded space characters must be enclosed in quotes.

VLAN Configuration Examples

Example 1 – Basic understanding of port based VLANs

VLAN Configuration View

VLAN Status : Enable						
VLAN ID	**VLAN Name**	**Untagged Port(s)**	**Tagged Port(s)**	**Mgmt Port**	**Admit**	**Mirror Port**
1	Default VLAN	A3-A6,B1-B6,C1-C6,D1-D6	--	YES	All	0
2	VLAN -2	A1-A2	--	YES	All	0

Ports Configuration View

Port No	Port Name	PVID
1	A1	2
2	A2	2
3	A3	1
...	…	…
23	D5	1
24	D6	1

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
Port A1	Untagged	MAC on port 2	Port A2	Unicast Traffic
Port A1	Untagged	Unknown MAC	Port A2	Floods VLAN 2
Port A1	VID 4	MAC on port 2	Port A2	Strips VID off packet
Port A3	Untagged	MAC on port 5	Port A5	Unicast Traffic
Port A3	Untagged	Unknown MAC	Port A4-D6	Floods VLAN 1
Port A3	VID 4	MAC on port 6	Port A6	Strips VID off packet

Example 2 – Basic understanding of tagged VLANs (Admit – Tagged Only)

VLAN Configuration View

VLAN Status : Enable						
VLAN ID	**VLAN Name**	**Untagged Port(s)**	**Tagged Port(s)**	**Mgmt Port**	**Admit**	**Mirror Port**
1	Default VLAN	--	A3-A6,B1-B6,C1-C6,D1-D6	YES	Tagged Only	0
2	VLAN -2	--	A1-A2	YES	Tagged Only	0

Ports Configuration View

Port No	Port Name	PVID
1	A1	**
2	A2	**
3	A3	**
...	…	…
23	D5	**
24	D6	**

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
Port A1	Untagged	MAC on port A2	--	Packet Discarded
Port A1	VID 2	MAC on port A2	Port A2	Unicast Traffic
Port A1	VID 4	MAC on port A2	--	Packet Discarded
Port A1	VID 2	MAC on port A5	Port A2	Floods VLAN 2
Port A3	Untagged	MAC on port A1	--	Packet Discarded
Port A3	VID 1	MAC on port A6	Port A6	Unicast Traffic
Port A3	VID 1	Unknown MAC	Port A4-D6	Floods VLAN 1
Port A3	VID 4	MAC on port B2	--	Packet Discarded

Example 3 – Basic understanding of tagged VLANs (Admit – All)

VLAN Configuration View

VLAN Status : Enable						
VLAN ID	**VLAN Name**	**Untagged Port(s)**	**Tagged Port(s)**	**Mgmt Port**	**Admit**	**Mirror Port**
1	Default VLAN	--	A3-A6,B1-B6,C1-C6,D1-D6	YES	All	0
2	VLAN -2	--	A1-A2	YES	All	0

Ports Configuration View

Port No	Port Name	PVID
1	A1	**
2	A2	**
3	A3	**
...	…	…
23	D5	**
24	D6	**

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
Port A1	Untagged	MAC on port A2	Port A2	Adds VID 2 to packet
Port A1	VID 2	MAC on port A2	Port A2	Unicast Traffic
Port A1	VID 4	MAC on port A2	--	Packet Discarded
Port A1	VID 2	Unknown MAC	Port A2	Floods VLAN 2
Port A3	Untagged	Unknown MAC	Port A4-D6	Adds VID 1 to packet & Floods VLAN 1
Port A3	VID 1	MAC on port A6	Port A6	Unicast Traffic
Port A3	VID 1	Unknown MAC	Port A4-D6	Floods VLAN 1
Port A3	VID 4	MAC on port B2	--	Packet Discarded

Example 4 – Basic understanding of Hybrid VLANs

VLAN Configuration View

VLAN Status : Enable						
VLAN ID	**VLAN Name**	**Untagged Port(s)**	**Tagged Port(s)**	**Mgmt Port**	**Admit**	**Mirror Port**
1	Default VLAN	A3-A6,B1-B6,C1-C6,D1-D6	--	YES	All	0
2	VLAN -2	A1-A2	A3-A4	YES	All	0

Ports Configuration View

Port No	Port Name	PVID
1	A1	2
2	A2	2
3	A3	1
…	…	…
23	D5	1
24	D6	1

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
Port A1	Untagged	MAC on port A2	Port A2	Unicast Traffic
Port A1	Untagged	MAC on port A3	Port A3	Adds VID 2 in the packet
Port A1	VID 4	MAC on port A2	--	Packet Discarded
Port A1	VID 4	MAC on port A3	--	Packet Discarded
Port A1	VID 2	MAC on port A2	Port A2	Strips VID off packet
Port A3	Untagged	MAC on port A6	Port A6	Unicast Traffic
Port A3	Untagged	Unknown MAC	Port A4-D6	Floods VLAN 1
Port A3	VID 4	MAC on port A5	--	Packet Discarded
Port A3	VID 4	MAC on port A4	--	Packet Discarded
Port A3	VID 2	MAC on port A4	Port A4	Strips VID off packet
Port A3	VID 2	MAC on port A1	Port A1	Strips VID off packet

Example 5 – Basic understanding of Overlapping VLANs

VLAN Configuration View

VLAN Status : Enable						
VLAN ID	**VLAN Name**	**Untagged Port(s)**	**Tagged Port(s)**	**Mgmt Port**	**Admit**	**Mirror Port**
1	Default VLAN	--	--	YES	All	0
2	VLAN -2	A1-A6,B1-B6,C1-C6,D1-D6	--	YES	All	0
3	VLAN -3	A2-A6,B1-B6,C1-C6,D1-D6	--	YES	All	0
4	VLAN -4	A1-A2	--	YES	All	0

Ports Configuration View

Port No	Port Name	PVID
1	A1	4
2	A2	2
3	A3	3
..	…	…
23	D5	3
24	D6	3

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
Port A1	Untagged	MAC on port A2	Port A2	Unicast Traffic
Port A1	Untagged	MAC on port A3	--	Packet Discarded
Port A1	VID 4	MAC on port A2	Port A2	Strips VID off packet
Port A1	VID 4	Unknown MAC	Port A2	Strips VID off packet & Floods VLAN 4
Port A2	Untagged	MAC on port A1	Port A1	Unicast Traffic
Port A2	Untagged	MAC on port A5	Port A5	Unicast Traffic
Port A2	VID 2 or 3	MAC on port A5	Port A5	Strips VID off packet
Port A2	Untagged	Unknown MAC	Port A1, A3-D6	Floods VLAN 2
Port A3	Untagged	MAC on port A1	Port A2-D6	Floods VLAN 3
Port A3	Untagged	MAC on port A2	Port A2	Unicast Traffic
Port A3	Untagged	MAC on port A5	Port A5	Unicast Traffic
Port A3	VID 2 or 3	MAC on port A2	Port A2	Strips VID off packet

Example 6 – Basic understanding of VLANs with Multicast Filtering

VLAN Configuration View

VLAN Status : Enable						
VLAN ID	**VLAN Name**	**Untagged Port(s)**	**Tagged Port(s)**	**Mgmt Port**	**Admit**	**Mirror Port**
1	Default VLAN	--	--	YES	All	0
2	VLAN -2	A1-A6,B1-B6,C1-C6,D1-D6	--	YES	All	0
3	VLAN -3	A2-A6,B1-B6,C1-C6,D1-D6	--	YES	All	0
4	VLAN -4	A1-A2	--	YES	All	0

Ports Configuration View

Port No	Port Name	PVID
1	A1	4
2	A2	2
3	A3	3
..	…	…
23	D5	3
24	D6	3

Display Static Multicast Group Address(es)

Multicast Address	Port List
01:00:00:00:00:01	1-24
01:00:00:00:00:02	1,6,8

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
Port 1	Untagged	01:00:00:00:00:01	Port 2	Goes to Ports 1-24, but port 1 can only send to Port 2 (VLAN 4)
Port 1	Untagged	01:00:00:00:00:02	--	Packet Discarded
Port 2	Untagged	01:00:00:00:00:01	Port 1,3-24	Goes to Ports 1-24, but won't go back out the port it came in on
Port 2	Untagged	01:00:00:00:00:02	Port 1,6,8	Goes to ports 1,6,8
Port 3	Untagged	01:00:00:00:00:01	Port 2,4-24	Goes to Ports 1-24, but can't talk to Port 1 since it is on a different VLAN
Port 3	Untagged	01:00:00:00:00:02	Port 6,8	Goes to Port 1,6,8, but can't talk to Port 1 since it is on a different VLAN

Note: *If there are multiple ports on different VLANs, the 7900 will apply the static multicast address to the lowest VLAN-ID that is associated with one of the ports assigned to the static multicast address. If the lowest VLAN-ID contains all the ports assigned to the static multicast address (an umbrella VLAN), it will function for all those ports with no problems. This can be achieved with overlapping VLANs.*

KEY SPECIFICATIONS

Switch Properties

Number of MAC Addresses:	8,000
Aging Time:	Programmable
Latency Type:	2.6 µs
Backplane Speed:	8.8 Gb/s
Switching Method:	Store & Forward

Physical

Height:	5.2" (13cm)
Width:	9.0" (22.8cm)
Depth:	5.6" (14.2cm)
Weight (max):	5.0 lbs
Din-Rail mount:	35mm

Electrical

Redundant Input Voltage: 10-30 VDC
Input Current (max): 1.53 A@24V (fully populated)
Input Ripple: Less than 100 mV

N-TRON Power Supply: NTPS-24-5 (5 Amp@24VDC*)* (NOTE: Not appropriate for use with M12, POE, and HV models.)

Environmental

Operating Temperature:	-20°C to 70°C
Storage Temperature:	-40°C to 85°C
Operating Humidity: (Non Condensing)	10% to 95%
Operating Altitude:	0 to 10,000 ft.

Shock and Vibration (bulkhead mounting)

Shock:	50g @ 10ms
Vibration/Seismic:	30g, 5-200Hz,Triaxial

Reliability

MTBF: >1Million Hour

Connectors

10/100BaseTX:	Up to Twenty-four (24) RJ-45 Copper Ports
100BaseFX:	Up to Sixteen (16) SC or ST Duplex Ports
1000BaseSX/LX:	Two (2) LC Duplex Ports as an option

Recommended Wiring Clearance:

Front: 4" (10.16 cm)
Side: 1" (2.54 cm)

Network Media

10BaseT:	>Cat3 Cable
100BaseTX:	>Cat5 Cable
*100*BaseFX, 1000BaseSX:	
Multimode:	50-62.5/125µm
*100*BaseFXE, 1000BaseLX:	
Singlemode:	7-10/125µm
1000BaseT (optional)	>Cat5 Cable

SFP Pluggable Modules

*1000BaseT (*NTSFP-TX*)*: >Cat5e Cable
minimum length: 1 meter
maximum length: 100 meter

*1000BaseLX (*NTSFP-LX-10*)*: 10 kilometers
*1000BaseLX (*NTSFP-LX-40*)*: 40 kilometers
*1000BaseLX (*NTSFP-LX-80*)*: 80 kilometers
1000BaseSX (50/125µm): 550 meters
1000BaseSX (62.5/125µm): 275 meters

Gigabit Fiber Transceiver (SFP) Characteristics

Fiber Length	550m* with 50/125 µm 275m @ 62.5/125µm	10km**	40km**	80km**
TX Power Min	-9.5dBm	-9.5dBm	-2dBm	0dBm
RX Sensitivity Max	-17dBm	-20dBm	-22dBm	-24dBm
Wavelength	850nm	1310nm	1310nm	1550nm
Assumed Fiber Loss	3.5 to 3.75 dB/km	0.45 dB/km	0.35 dB/km	0.25 dB/km
Laser Type	VCSEL	FP	DFB	DFB

* Multimode Fiber Optic Cable
** Singlemode Fiber Optic Cable

100 Mb Fiber Transceiver Characteristics

Fiber Length	2km*	15km**	40km**	80km**
TX Power Min	-19dBm	-15dBm	-5dBm	-5dBm
RX Sensitivity Max	-31dBm	-31dBm	-34dBm	-34dBm
Wavelength Min/Max	1310nm	1310nm	1310nm	1550nm

* Multimode Fiber Optic Cable
** Singlemode Fiber Optic Cable

Regulatory Certifications

Product Safety

UL 60950-1; UL 508; ANSI/ISA 12.12.01-2007; CAN/CSA-C22.2 No. 60950;
CAN/CSA-C22.2 No. 142; CAN/CSA-C22.2 No. 213

Emissions

FCC Title 47, Part 15, Radio Frequency Devices, Subpart B; ANSI C63.4-2003;
Industry Canada ICES-003; EN 61000-6-4 (radiated and conducted)

Immunity

EN 61000-6-2; IEC 61000-4-2 (ESD); IEC 61000-4-3 (RFAM);
IEC 61000-4-4 (EFT); IEC 61000-4-5 (SURGE); IEC 61000-4-6 (RFCM);
IEC 61000-4-8 (PFMF); IEC 61000-4-11 (VDI)

Other

EMC Directive 2004/108/EC; ABS (PDA and Type Approval for Shipboard
Applications); GOST-R; RoHS Compliant

Designed to comply with:
IEEE 1613 for Electric Utility Substations

Warranty: Effective January 1, 2008, all N-TRON products carry a 3 year limited warranty from the date of purchase.

Appendix A. XML Settings File Example

```
<!-- Overview of XML settings for N-TRON switches -->

<!-- XML settings can be downloaded to a switch to configure the switch. XML settings cover a
subset of the settings available through a web browser. -->

<!-- There are several top level configuration sections. Each section is optional.

<SystemConfiguration>
     <Switches/>
     <Administration/>
     <IPConfiguration/>
     <Users/>
     <Ports/>
     <DHCPServer/>
     <MACSecurity/>
</SystemConfiguration>
 -->

<SystemConfiguration version="1" minSwVer="3.4.2">
     <!-- The minSwVer attribute is optional. If present, the XML settings are ignored if the
     switch software version does not meet the minimum version requirement -->

<!--_____________________________________________________________________________________-->

     <!-- The Switches block is optional. If present, the model name of the target switch must
     be in the list for the file to be processed. -->
     <Switches>
          <Switch minSwVer="3.4.6">7900</Switch> <!-- If the minSwVer attribute is present, it
                                                      overrides the minSwVer attribute of
                                                      SystemConfiguration. -->
          <Switch>7900</Switch>
     </Switches>


 <!--_____________________________________________________________________________________-->

     <!-- Administration -->
     <Administration>
          <SwitchName>myname</SwitchName>            <!-- optional --><!--255 character limit-->
          <SwitchLocation>mylocation</SwitchLocation><!-- optional --><!--255 character limit-->
          <SwitchContact>mycontact</SwitchContact>   <!-- optional --><!--255 character limit-->
     </Administration>

 <!--_____________________________________________________________________________________-->

     <!-- IP configuration -->
     <IPConfiguration>
          <Mode>static</Mode> <!-- Mode must be static or dhcp -->

          <!-- If dhcp mode, these elements are the "Fallback" Address, Subnet, and Gateway.
          Note: For an IP address of 192.168.1.201, there is no fallback address.   -->

          <!-- All IP addresses have a 15 character limit (xxx.xxx.xxx.xxx) -->
          <Address>192.168.1.222</Address>     <!-- 15 character limit -->
          <Subnet>255.255.255.0</Subnet>       <!-- 15 character limit -->
          <Gateway>192.168.1.1</Gateway>       <!-- 15 character limit -->

          <!-- If dhcp mode, this is the dhcp client id -->
          <ClientID>
               <!-- Use one of the elements (MACAddress, SwitchName, OtherText, OtherHex).
               MACAddress and SwitchName use current switch values. -->
               <MACAddress/>
               <SwitchName/>
               <OtherText>myClientID</OtherText>       <!-- 255 character limit -->
               <OtherHex>0102de03ad00be09ef</OtherHex> <!-- 255*2 character limit -->
          </ClientID>
     </IPConfiguration>
```

```
<!--_____________________________________________________________________________-->

     <!-- User management -->
     <!-- A list of logon accounts (5 maximum) to add to the switch. -->

     <Users mode="keep">     <!-- mode must be "keep" or "delete" -->
          <!-- mode=delete - delete existing accounts before adding accounts (default) -->
          <!-- mode=keep - do not delete existing accounts before adding accounts -->

          <!--  All User elements (name, password, access) are required. -->
          <User>
               <Name>Joe</Name>                <!-- 3-15 character limit -->
               <Password>xxx</Password>        <!-- 3-15 character limit -->
               <Access>admin</Access>           <!-- Access must be admin or user -->
          </User>
     </Users>

 <!--_____________________________________________________________________________-->

     <!-- Port configuration -->
     <!-- You may uses this block to define port VLAN identifiers (PVIDs) -->
     <Ports>
          <ValidatePorts>yes</ValidatePorts>  <!-- optional --> <!-- Must be yes(default)
                                                   or no. If no, invalid ports are ignored. -->

          <!-- Use PortNumber or PortName -->
          <Port>
               <PortNumber>4</PortNumber> <!-- PortNumber ranges from 1 to the maximum port
                                          number for the switch -->
               <PVID>1</PVID>             <!-- PVID ranges from 1 to 4094 -->
          </Port>
          <Port>
               <PortName>TX6</PortName>   <!-- Name of port on switch -->
               <PVID>26</PVID>            <!-- PVID ranges from 1 to 4094 -->
          </Port>
     </Ports>

<!--_____________________________________________________________________________-->

     <!-- DHCP server -->

     <DHCPServer mode="delete">     <!-- mode must be "keep" or "delete" -->
          <!-- mode=delete - delete existing profiles before adding profiles (default) -->
          <!-- mode=keep - do not delete existing profiles before adding profiles -->

          <Enabled>yes</Enabled>     <!-- Enabled must be yes or no -->

          <!-- If the server is enabled (enabled=yes), you can add DHCP server profiles.
          (If not enabled, can not add profiles.) -->
          <Profile>

               <!-- Required: Name, LowIP, HighIP, LeaseDays. LeaseHours is optional, and
               defaults to 0. -->
               <Name>prof1</Name>             <!-- required -->   <!-- 19 character limit -->
               <LowIP>192.168.2.1</LowIP>     <!-- required -->
               <HighIP>192.168.2.254</HighIP> <!-- required -->
               <LeaseDays>28</LeaseDays>      <!-- required -->
               <LeaseHours>0</LeaseHours>     <!-- optional -->

               <!--The Advanced block is optional, and all elements within the block are
               optional.-->
               <Advanced>     <!-- optional -->
                    <!-- All elements below are optional -->
                    <BroadcastAddress>192.168.2.255</BroadcastAddress>
                    <DomainName>N-TRON.com</DomainName>     <!-- 63 character limit -->
                    <DNSServer1>192.168.2.10</DNSServer1>
                    <DNSServer2>192.168.2.11</DNSServer2>
                    <Gateway1>192.168.2.1</Gateway1>
```

```
                    <Gateway2>192.168.2.2</Gateway2>
               </Advanced>

               <IPMaps>
               <!-- The DynamicRange is the only IP Map supported. You may have 0 or more. -->
                    <DynamicRange>
                         <!-- low and high within range of profile -->
                         <LowIP>192.168.2.1</LowIP>       <!-- required -->
                         <HighIP>192.168.2.4</HighIP>     <!-- required -->
                    </DynamicRange>
               </IPMaps>
          </Profile>
     </DHCPServer>

 <!--_____________________________________________________________________________________-->

     <!-- MAC security -->
     <MACSecurity>
          <Mode>learning</Mode>        <!-- Mode must be learning or locked -->

          <!-- Authorized entries -->
          <Authorized mode="keep">     <!-- mode must be "keep" or "delete" -->
                         <!-- mode=delete - delete existing authorized MACs before adding
                         authorized MACs (default) -->
                         <!-- mode=keep - do not delete existing authorized MACs before
                         adding authorized MACs -->

               <ValidatePorts>yes</ValidatePorts>   <!-- optional -->
                                                    <!-- Must be yes(default) or no.
                                                         If no, invalid ports are ignored. -->
               <Entry>
                    <MACAddress>00:07:af:ff:5b:c0</MACAddress>     <!-- 17 character limit -->
                    <!-- MAC is valid on all ports listed in the ports list.
                    If the ports list is missing, then the MAC is valid on all ports. -->
                    <Ports>
                         <Port>
                              <!-- Use PortNumber or PortName -->
                              <PortNumber>4</PortNumber>   <!-- 1 to maximum port for switch -->
                         </Port>
                         <Port>
                              <PortName>TX5</PortName>     <!-- Name of port on switch -->
                         </Port>
                    </Ports>
               </Entry>
               <Entry>
                    <MACAddress>0007af1d6460</MACAddress>  <!-- Example of a MAC with no
                                                           delimiters, valid on all ports. -->
               </Entry>
          </Authorized>
     </MACSecurity>

</SystemConfiguration>
```

N-TRON Limited Warranty

N-TRON, Corp. warrants to the end user that this hardware product will be free from defects in workmanship and materials, under normal use and service, for the applicable warranty period from the date of purchase from N-TRON or its authorized reseller. If a product does not operate as warranted during the applicable warranty period, N-TRON shall, at its option and expense, repair the defective product or part, deliver to customer an equivalent product or part to replace the defective item, or refund to customer the purchase price paid for the defective product. All products that are replaced will become the property of N-TRON. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer. N-TRON shall not be responsible for any custom software or firmware, configuration information, or memory data of customer contained in, stored on, or integrated with any products returned to N-TRON pursuant to any warranty.

OBTAINING WARRANTY SERVICE: Customer must contact N-TRON within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from N-TRON or its authorized reseller may be required. Products returned to N-TRON must be pre-authorized by N-TRON with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment. Responsibility for loss or damage does not transfer to N-TRON until the returned item is received by N-TRON. The repaired or replaced item will be shipped to the customer, at N-TRON's expense, not later than thirty (30) days after N-TRON receives the product. N-TRON shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to N-TRON for repair, whether under warranty or not.

ADVANCE REPLACEMENT OPTION: Upon registration, this product qualifies for advance replacement. A replacement product will be shipped within three (3) days after verification by N-TRON that the product is considered defective. The shipment of advance replacement products is subject to local legal requirements and may not be available in all locations. When an advance replacement is provided and customer fails to return the original product to N-TRON within fifteen (15) days after shipment of the replacement, N-TRON will charge customer for the replacement product, at list price.

WARRANTIES EXCLUSIVE: IF AN N-TRON PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT N-TRON'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. N-TRON NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. N-TRON SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, N-TRON ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF N-TRON OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT N- TRON'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER: Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the State of Delaware, U.S.A.