

**709FX**  
**Managed Industrial**  
**Ethernet Switch**

**User Manual &**  
**Installation**  
**Guide**

---

709FX Industrial Ethernet Switch Installation Guide .....	5
709FX Industrial Ethernet Switch Accessories .....	7
SAFETY WARNINGS .....	9
SUPPORT: .....	9
Installation.....	11
DIN RAIL MOUNTING.....	12
FRONT PANEL (709FX).....	14
APPLYING POWER (Top View) .....	16
Connecting the Unit .....	17
Overview of Advanced Features .....	22
Mode of Operation .....	22
Port Mirroring .....	22
Port Trunking .....	22
Quality of Service (QoS).....	22
Virtual LAN .....	23
Rapid Spanning Tree Protocol .....	24
SNMP Traps.....	24
IGMP Snooping .....	24
N-Ring.....	25
N-Link.....	25
CIP .....	25
DHCP .....	25
DHCP Client .....	26
DHCP Relay Agent .....	26
DHCP Server.....	26
LLDP.....	26
Port Security—MAC Address Based .....	26
TROUBLESHOOTING .....	27
Web Software Configuration .....	29
Web Management .....	29
Web Management - Home .....	30
Administration – System.....	33
Administration – SNMP.....	38
Administration – Fault .....	40
DHCP – Server – Setup Profiles .....	42
DHCP – Server – Setup IP Maps .....	46
DHCP – Server – View Bindings.....	52
DHCP – Relay & Local IP - Setup.....	53
LLDP - Configuration .....	56
LLDP - Ports .....	57
LLDP - Status.....	58
LLDP - Statistics .....	59
Ports – MAC Security – Learning .....	64
Ports – MAC Security – Authorization List .....	67
Ports – MAC Security – Intruder Log .....	69
Ports – Mirroring.....	70
Ports – Mirroring, Continued .....	71
Ports – Mirroring, Continued. . . .....	72
Ports – QOS.....	74
Statistics – Port Statistics .....	76
Statistics – Port Utilization.....	78
VLAN – Configuration .....	79
Bridging – Aging Time .....	83
Bridging – Unicast Addresses .....	84
Bridging – Multicast Addresses .....	86

Bridging – Show MAC by Port.....	88
RSTP – Configuration.....	90
IGMP – Configuration .....	94
IGMP – Show Group and Show Router .....	99
IGMP – RFilter .....	101
N-View – Configuration.....	103
N-View – Ports.....	104
N-Ring – Configuration .....	106
N-Ring – Advanced Configuration .....	109
N-Ring – Status .....	112
N-Link – Configuration.....	117
N-Link – Status .....	121
CIP – Configuration .....	129
CIP – Status.....	130
Firmware/Config – TFTP.....	132
Firmware/Config – TFTP, Continued .....	134
Support – Web Site and E-mail.....	135
Rate Limiting – Broadcast Rate Limit Configuration .....	137
Rate Limiting – Multicast Rate Limit Configuration .....	138
User Management – Adding Users .....	140
User Management – Removing Users .....	141
LogicalView .....	143
Configuration – Save or Reset.....	144
Help – Overview .....	146
Help – Administration.....	147
Help – DHCP .....	148
Help – LLDP .....	149
Help – Ports.....	150
Help – Statistics.....	151
Help – VLAN.....	152
Help – Bridging.....	153
Help – RSTP .....	154
Help – IGMP .....	155
Help – N-View .....	156
Help – N-Ring.....	157
Help – N-Link .....	158
Help – CIP.....	159
Help – Firmware/Config .....	160
Help – Rate Limiting.....	161
Help – User Management.....	162
Help – Other .....	163
CLI Commands .....	164
“?” (Help).....	164
Logout .....	164
Show, Add, or Delete ARL Entries .....	165
Configuration Device Operations.....	166
Show or Set CIP Configuration.....	167
Save or Reset the Configuration Settings .....	168
Show or Set IGMP Configuration .....	168
Show or Set Mirror Configuration .....	169
Show or Set N-Ring Configuration .....	170
Show or Set N-View Configuration .....	170
Ping a Host .....	171
Show or Set Port Configuration .....	172
Reset the Switch.....	173
Show or Set SNMP Configuration .....	173
Show or Clear the Last System Error .....	174

Show System Information .....	174
Set or Show the System IP Configuration .....	175
Show or Set System Configuration .....	176
VLAN Addition and Deletion Example.....	177
VLAN Configuration Examples .....	183
Example 1 – Basic understanding of port-based VLANs.....	183
Example 2 – Basic understanding of tagged VLANs (Admit – Tagged Only) .....	184
Example 3 – Basic understanding of tagged VLANs (Admit – All) .....	185
Example 4 – Basic understanding of Hybrid VLANs .....	186
Example 5 – Basic understanding of Overlapping VLANs.....	187
Example 6 – Basic understanding of VLANs with Multicast Filtering.....	188
KEY SPECIFICATIONS (709FX) .....	189
KEY SPECIFICATIONS (709FX-HV) .....	191
Appendix A. XML Settings File Example .....	193
N-TRON Limited Warranty.....	196

**709FX Industrial Ethernet Switch Installation Guide**



The N-TRON 709FX 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
- Eight 10/100 BaseTX RJ-45 Ports
- One 100BaseFX(E) Port
- Extended Environmental Specifications (Surrounding Air): -40 to 70 °C Operating temperature
- ESD and Surge Protection Diodes on all Ports
- Auto Sensing 10/100BaseTX, Duplex, and MDIX
- Offers Rapid Spanning Tree Protocol
- Store & Forward Technology
- Rugged Din-Rail Enclosure
- Onboard Temperature Sensor
- Configuration Backup via optional SD Card (NTCD-128)
- Redundant Power Inputs

## PRODUCT CONFIGURATIONS

- 709FX-XX-VV and 709FXE-XX-YY-VV
    - Eight 10/100 Base-TX RJ45 Copper Ports, one 100BaseFX Port,
- Where: XX = ST or SC  
YY = 10, 40 or 80 for Singlemode, Blank for Multimode  
VV = HV for High voltage, Blank for Standard voltage  
E = Singlemode, Blank Otherwise

## MANAGEMENT FEATURES


- SNMP v1, v2, v3 and Web Browser Management
- SNMP based image or config download and config upload
- Configuration backup via Optional Configuration Device (NTCD)
- EtherNet/IP™ CIP Messaging
- Detailed Ring Map and Fault Location Charting
- N-Ring™ Technology with ~30ms Healing
- Web Browser Management with detailed ring map and fault location charting.
- N-View™ OPC Monitoring
- N-Link™ Redundant N-Ring Coupling
- IGMP Auto Configuration and Plug and Play Support
- 802.1Q tag VLAN and Port VLAN
- 802.1p QoS, Port QoS, and DSCP
- LLDP (Link Layer Discovery Protocol)
- Trunk with other N-Tron trunking capable switches over two ports
- Port Mirroring
- 802.1D RSTP (Rapid Spanning Tree Protocol)
- DHCP Client, Server, Option 82 relay, Option 61
- Local Port IP Addressing
- Port Security—MAC Address Based

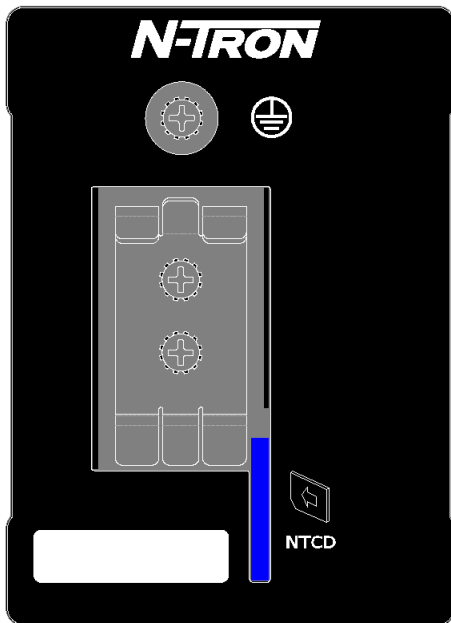
Copyright, © N-Tron Corporation, 2008-2015

## 709FX Industrial Ethernet Switch Accessories

The SD and USB connectors are for temporary connection only. Do not use, connect, or disconnect unless area is known to be non-hazardous. Connection or disconnection in an explosive atmosphere could result in an explosion.

Les SD et USB sont pour la connexion temporaire. Ne pas utiliser, de connecter ou déconnecter sauf si la zone est connue pour être non dangereux. Connexion ou la déconnexion dans une atmosphère explosive pourrait entraîner une explosion.

 A blue SD card with a white label. The label features the N-TRON logo at the top, followed by 'THE INDUSTRIAL NETWORK COMPANY' and 'Industrial' in a stylized font. Below that is a large 'SD' logo with 'TM' to its right. At the bottom of the label, it says 'NTCD-128' and 'SD Card 128MB'. A small 'Lock' indicator is visible on the left side of the card.	<p><u>Configuration Device</u></p> <p>Ideal for saving, or restoring switch configuration parameters quickly without the need for a computer or software. One configuration device per switch is recommended.</p>
<p><b>NTCD-128</b></p>	



The configuration device is inserted in the back of the 709FX.

Copyright, © N-Tron Corporation, 2008-2015  
3101 International Drive, Building 6  
Mobile, AL 36606 USA

All rights reserved. Reproduction, adaptation, or translation without prior written permission from N-Tron Corporation is prohibited, except as allowed under copyright laws.

Ethernet is a registered trademark of Xerox Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks of their respective owners.

The information contained in this document is subject to change without notice. N-Tron Corporation makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. In no event shall N-Tron Corporation be liable for any incidental, special, indirect, or consequential damages whatsoever included but not limited to lost profits arising out of errors or omissions in this manual or the information contained herein.

**WARNING**  
**AVERTISSEMENT**

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.

Ne pas effectuer de services sur l'appareil s'il n'est pas qualifié pour le faire. Ne pas remplacer les pièces non autorisées ou de modifications non autorisées de l'appareil.

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

Ne pas faire fonctionner l'unité avec le couvercle retiré, ce qui pourrait créer une décharge électrique ou un incendie.

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

N'obstruez pas les fentes d'aération sur les côtés ou en haut de l'unité.

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.

Ne pas utiliser le matériel en présence de gaz ou de vapeurs inflammables. L'utilisation de matériel électrique dans un tel environnement constitue un danger certain.

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

Ne pas utiliser le matériel en présence de gaz ou de vapeurs inflammables. L'utilisation de matériel électrique dans un tel environnement constitue un danger certain.



**SAFETY WARNINGS**  
**AVERTISSEMENTS DE SÉCURITÉ**

**GENERAL SAFETY WARNINGS**  
**GÉNÉRAL AVERTISSEMENTS DE SÉCURITÉ**

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

**AVERTISSEMENT:** Si l'équipement est utilisé d'une manière non spécifiée par N-Tron Corporation, la protection fournie par l'équipement peut être compromise.

**LASER SAFETY** (Single Mode Fiber Models -40 and -80)



**CAUTION:** CLASS 1 LASER PRODUCT. Do not stare into the laser!  
**ATTENTION:** PRODUIT LASER CLASSE 1. Ne pas regarder dans le 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.redlion.net](http://www.redlion.net)  
E-MAIL: [customer.service@redlion.net](mailto:customer.service@redlion.net)

**ENVIRONMENTAL SAFETY**



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

**AVERTISSEMENT:** Déconnectez le câble d'alimentation et laissez refroidir 5 minutes avant de la toucher.

**ELECTRICAL SAFETY**



Must be powered by a Class 2 source only.

Doit être alimenté par une source de catégorie 2 seulement.

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

**AVERTISSEMENT:** Ne pas utiliser l'appareil avec n'importe quel couvercle retiré.

**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.

**AVERTISSEMENT:** Correctement à la terre de l'unité avant tout raccordement à l'unité. Unités pas correctement mise à la terre peut entraîner un risque de sécurité et pourraient être dangereux et peut annuler la garantie. Voir la section technique de mise à la terre de ce mode d'emploi des moyens appropriés à la masse de l'appareil.

**WARNING:** Never install or work on electrical equipment or cabling during periods of lightning activity.

**AVERTISSEMENT:** Ne jamais installer ou de travailler sur un équipement électrique ou de câblage pendant les périodes d'activité de la foudre.

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

**AVERTISSEMENT:** Ne pas effectuer de services sur l'appareil s'il n'est pas qualifié pour le faire.

**WARNING:** Do not block the air vents.

**AVERTISSEMENT:** Ne pas obstruer les bouches d'aération.

**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.

**AVERTISSEMENT:** Respecter la polarité correcte de tension DC lors de l'installation des câbles d'alimentation d'entrée. Inversion de polarité de tension peut causer des dommages permanents à l'appareil et annule la garantie.

## **Hazardous Location Installation Requirements**

1. This equipment is suitable for use in Class I, Div. 2, Groups A, B, C, D or non-hazardous locations only.  
Cet équipement est adapté pour une utilisation dans la classe I, Division 2, Groupes A, B, C et D ou non dangereux endroits seulement.
2. **WARNING:** Explosion Hazard – Substitution of components may impair suitability for Class I, Division 2.  
**AVERTISSEMENT:** Risque d'explosion - Remplacement d'un composant peut empêcher la conformité de Classe I, Division 2.
3. **WARNING:** Explosion Hazard - Do not connect or disconnect any connections while circuit is live unless area is known to be non-hazardous.  
**AVERTISSEMENT:** Risque d'explosion - Ne pas brancher ou débrancher les connexions lorsque le circuit est sous tension sauf si la zone est connue pour être non dangereux.
4. **WARNING:** Explosion Hazard – Do not replace the device unless power has been switched off or the area is known to be non-hazardous.  
**AVERTISSEMENT:** Risque d'explosion - Ne pas remplacer le périphérique à moins que l'alimentation a été coupé ou que la zone est connu pour être non dangereux.

5. Use 90°C or higher rated Copper wire, (0.22Nm) 2lb/in Tightening torque for field installed conductors.  
Utilisez 90°C ou plus classé fil de cuivre, (0.22Nm) 2lb/in couple de serrage pour les conducteurs installés sur le terrain.
6. **WARNING:** Exposure to some chemicals may degrade the sealing properties of materials used in the Sealed Relay Device. Relays U13 and U25.  
**AVERTISSEMENT:** L'exposition à certains produits chimiques peut dégrader les propriétés d'étanchéité des matériaux utilisés dans le dispositif de relais scellé. Relais U13 et U25.

Please make sure the 709FX Series Ethernet Switch package contains the following items:

1. 709FX Series Switch
2. Product CD

Contact your carrier if any items are damaged.

## Installation

Read the following warning before beginning the installation:  
Lire l'avertissement suivant avant de commencer l'installation:

### WARNING AVERTISSEMENT



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

Ne jamais installer ou de travailler sur un équipement électrique ou de câblage pendant les périodes d'activité de la foudre. Ne jamais brancher ou débrancher l'alimentation en gaz dangereux sont présents.

Disconnect the power cable before removing any enclosure panel.  
Débrancher le câble d'alimentation avant de retirer le panneau du châssis.

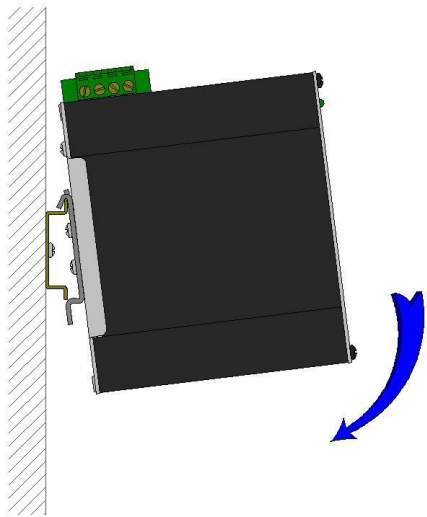
## UNPACKING

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

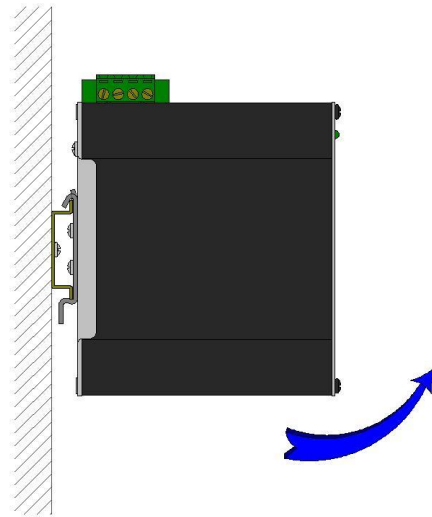
**CLEANING** - Clean only with a damp cloth.

## DIN RAIL MOUNTING

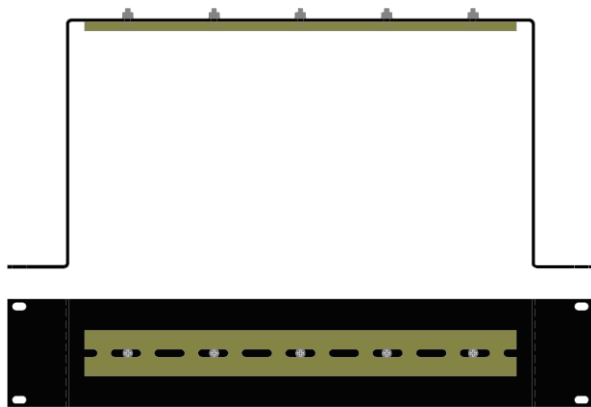
Install the unit on a standard 35mm Din-Rail. Recess the unit to allow at least 3” of horizontal clearance for copper cable bend radius. Recess the unit to allow at least 5” of horizontal clearance for fiber cable bend radius. There should be at least 3” of clearance on both the top and bottom of the unit to allow proper ventilation.



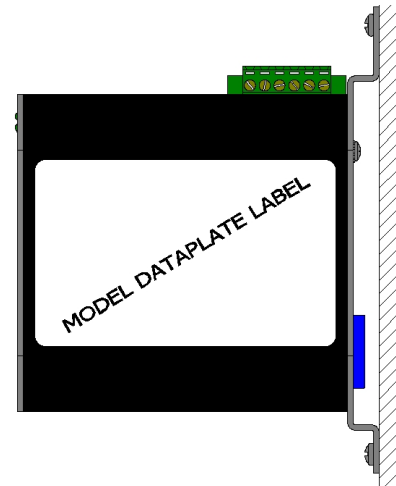
To install the unit to 35mm industrial DIN rail, place the top edge of the included mounting bracket on the back of the unit against the DIN rail at a 15° angle as shown. Rotate the bottom of the unit to the back (away from you) until it snaps into place.



To remove the unit from the 35mm industrial DIN rail, pull forward on the unit until it disengages from the bottom of the DIN rail. Rotate the bottom of the unit towards you and up at an approximate 15° upward angle to completely remove the unit.



**URMK**

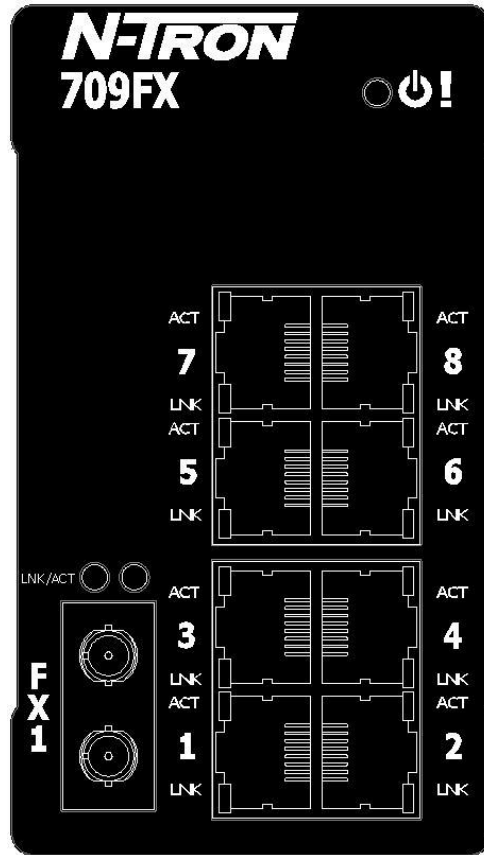


**CPMA**

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 Optional Universal Rack Mount Kit (P/N:

URMK) may be used to mount the enclosure to standard 19" racks, and our Optional Factory Installed Panel Mount Assembly may be used to mount the enclosure to a panel or any other flat surface.

# FRONT PANEL (709FX)



**From Top to Left:**

- RJ45 Ports** Auto Sensing 10/100 Base-TX Connections
- Fiber Port** 100 Base-FX Connection
- ⏻** LED lights when Power is supplied to the unit

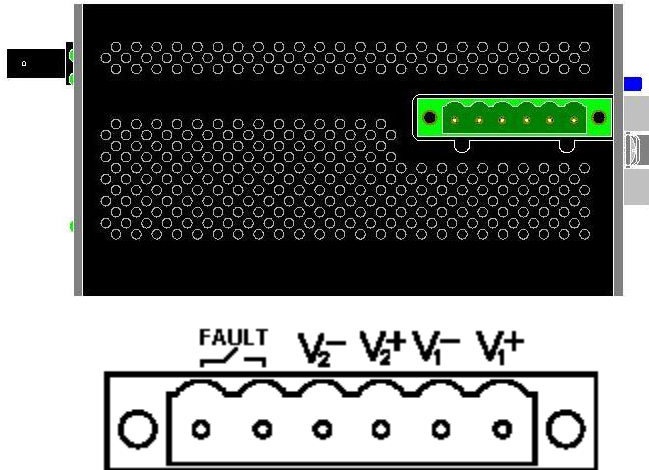
NOTE: The RJ45 data port has two LEDs located on each connector. The left LED indicates LINK status, and the right LED indicates ACTIVITY.

**LEDs:** The table below describes the operating modes:

LED	Color	Description
⏻	GREEN	Power is ON
	RED	Power is ON and a fault condition exists
	OFF	Power is OFF
LNK	GREEN	10/100Mb Link between ports
	OFF	No Link between ports

<b>ACT</b>	GREEN	Data is active between ports
	OFF	Data is inactive between ports

## APPLYING POWER (Top 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).

### Notes:

- Only 1 power supply must be connected to power for minimal operation. For redundant power operation, V<sub>1</sub> and V<sub>2</sub> 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.
- The Fault pins on the power connector can be used for an alarm contact. The current carrying capacity is 1A at 24VDC. It is normally open and the relay closes when a fault condition occurs. These pins can be used to connect an external warning device such as a light in order to provide an external alarm. The conditions for generating a fault condition (closing the relay) can be configured through software.

Recommended 24V DC Power Supplies, similar to: N-Tron's P/N **NTPS-24-1.3** (NOTE: Not appropriate for use with M12, POE, and HV models.):

- Input AC 115/230V
- Output DC 24-28V
- Output Current 1.3A @ 24V  
1.0A @ 28V
- Power 30W
- 35 mm DIN-Rail Mountable
- Dimensions: 45X75X91 mm

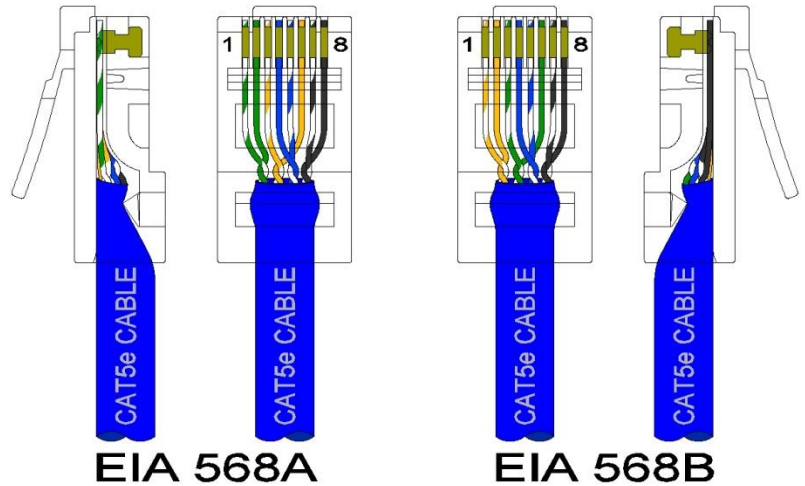


## Connecting the Unit

For FX/FXE units, remove the dust cap from the fiber optic connectors and connect the fiber optic cables. The TX port (located on the bottom connector) on the FX/FXE models should be connected to the RX port of the far end station. The RX port (located on the top connector) 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 LEDs are ON once the connection has been completed. To connect any port to another device (end node, Switch or Repeater), use a standard Category 5E straight through or crossover cable with a minimum length of one meter and a maximum length of 100 meters.

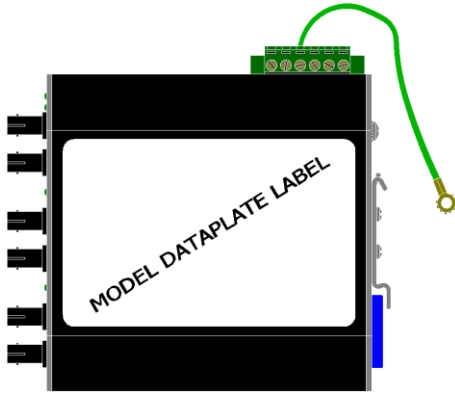
N-Tron recommends the use of pre-manufactured Cat5E cables to ensure the best performance. If this is not an option and users must terminate their own ends on the Cat5E cables; one of the two color coded standards shown to the right should be utilized. If a user does not follow one of these two color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



**Warning:** Creating a port to port connection on the same switch (i.e. loop) is an illegal operation and will create a broadcast storm which will crash the network!

## N-TRON SWITCH GROUNDING TECHNIQUES

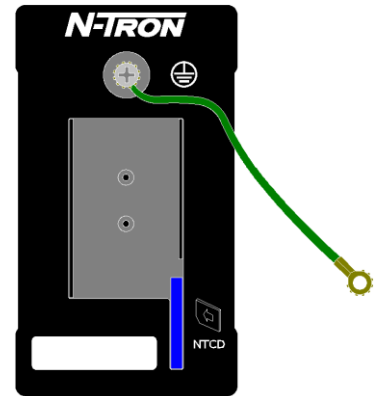
The grounding philosophy of any control system is an integral part of the design. N-Tron switches are designed to be grounded, but the user has been given the flexibility to float the switch when required. The best noise immunity and emissions (i.e. CE) are obtained when the N-Tron switch chassis is 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 (shown in green) 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 (shown in green) & 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.



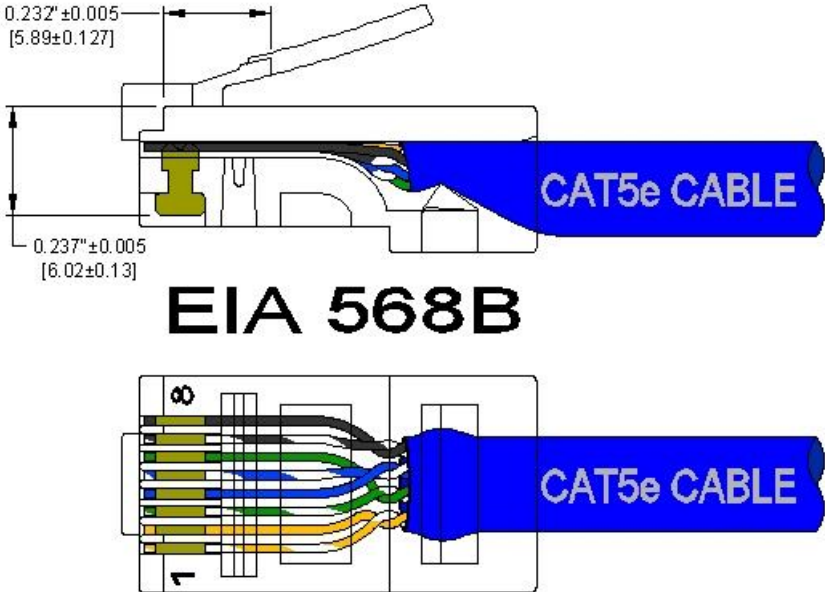
If the use of shielded cables is required, it is generally recommended to only connect the shield at one end to prevent ground loops and interfere with low level signals (i.e. thermocouples, RTD, etc.). Cat5e cables manufactured to EIA-568A or 568B specifications are required for use with N-Tron Switches.



In the event all Cat5e patch cable distances are small (i.e. All Ethernet devices are located in 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.

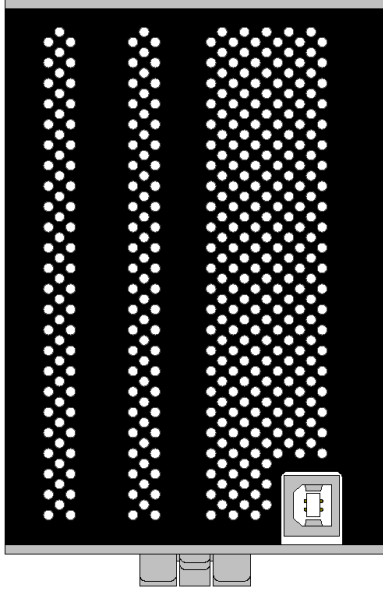
# RJ45 CONNECTOR CRIMP SPECIFICATIONS

Please reference the illustration below for your Cat5 cable specifications:



## USB INTERFACE

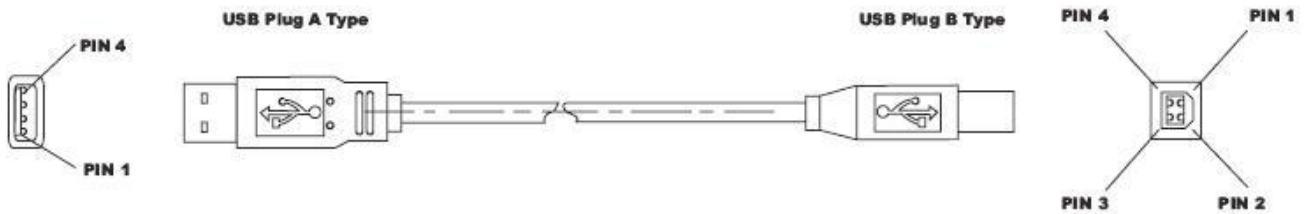
The 709FX Series switches provide a USB interface accessed via the USB connector labeled as “USB” on the unit. This is used to access the Command Line Interpreter (CLI).



The USB connector is at the bottom of the 709FX.

### USB Cable

Connect the USB port of your PC and the Switch using a standard USB cable. You will require a cable with a Type A connector for the PC end, and a Type B connector for the Switch end.



Standard USB cables are readily available from a variety of computer stores.

### HyperTerminal

The following configuration should be used in HyperTerminal:

Port Settings:	<b>115200</b>
Data Bits:	<b>8</b>
Parity:	<b>NONE</b>
Stop bits:	<b>1</b>

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:

- Half Duplex
- Full Duplex
- Auto Negotiation

100Base Fiber Ports:

- Full Duplex

1000Base Copper/Fiber Ports:

- Full Duplex

### 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.

### 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 709FX 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 709FX 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, Authentication Errors, and power supply failure. 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 709FX 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 709FX 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-Link**

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](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 that allows devices attached to an IEEE802 LAN to advertise to other devices the major capabilities they have 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.

## **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 LEDs are ON for connected ports.
4. Verify cabling used between stations.
5. Verify that cabling is Category 5E or greater for 100Mbit operation.

## **SUPPORT**

Contact N-Tron Corporation at:  
TEL: 251-342-2164  
FAX: 251-342-6353  
E-MAIL: [N-TRON\\_Support@n-tron.com](mailto:N-TRON_Support@n-tron.com)  
WEB: [www.n-tron.com](http://www.n-tron.com)

## **FCC STATEMENT**

This product complies with Part 15 of the FCC-A Rules.

Operation is subject to the following conditions:

- (1) This device may not cause harmful Interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

## **INDUSTRY CANADA**

This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. 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.

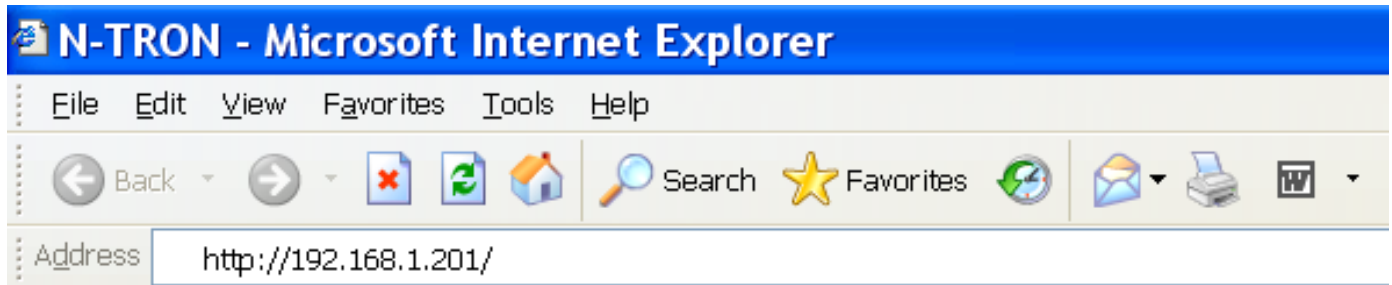
Cet appareillage numérique de la classe A répond à toutes les exigences de l'interférence canadienne causant des règlements d'équipement. L'opération est sujette aux deux conditions suivantes: (1) ce

dispositif peut ne pas causer l'interférence nocive, et (2) ce dispositif doit accepter n'importe quelle interférence reçue, y compris l'interférence qui peut causer l'opération peu désirée.

# Web Software Configuration

## Web Management

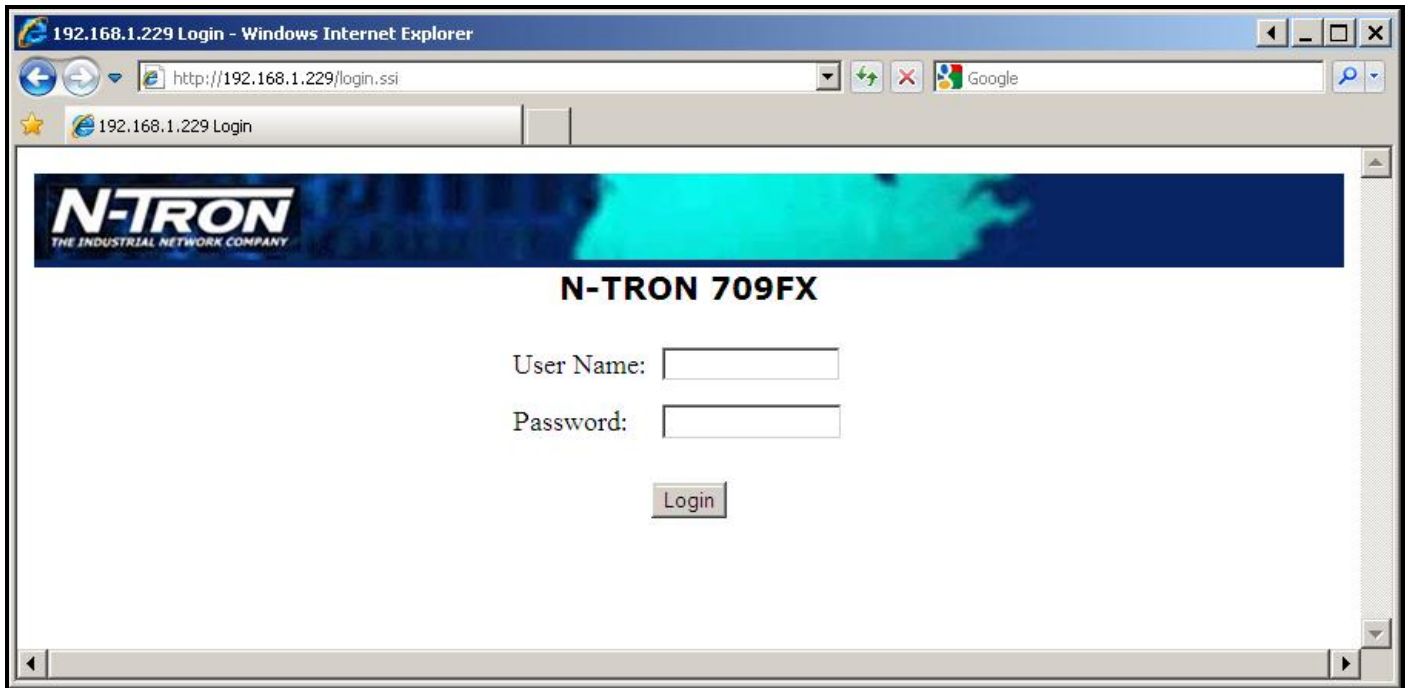
Enter the switch's IP address in any web browser and login to the web management feature of the 709FX Series.



### Default:

User Name: *admin*

Password: *admin*



## Web Management - Home

When the administrator first logs onto a 709FX 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 709FX 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.

**N-TRON**  
THE INDUSTRIAL NETWORK COMPANY

- Administration
- DHCP
- LLDP
- Ports
- Statistics
- VLAN
- Bridging
- RSTP
- IGMP
- N-View
- N-Ring
- N-Link
- CIP
- Firmware/Config
- Support
- Rate Limiting
- User Management
- Logical View
- Home
- Config
- Help
- Logout

Copyright © 2008-2011  
N-TRON Corp.  
All rights reserved.  
<http://www.n-tron.com>

Logged in as: **admin**

### Product Information

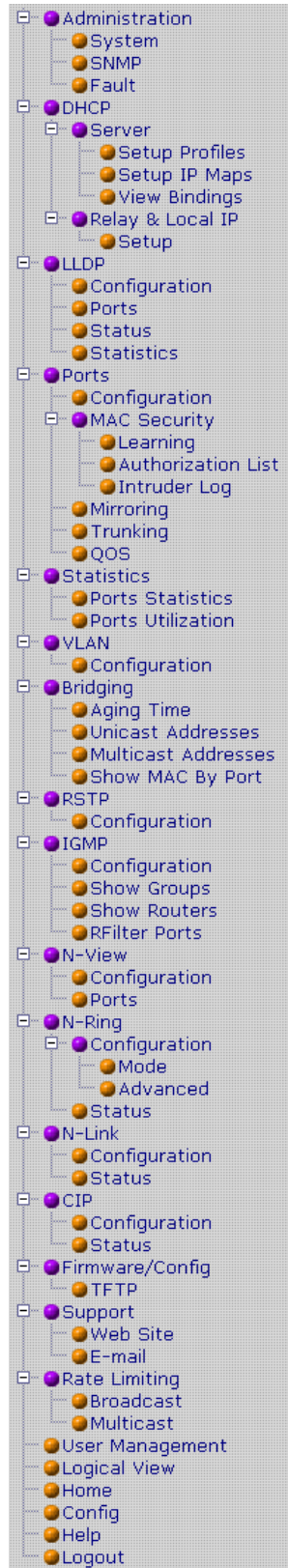
Name	N-TRON 709FX
Software Version	3.5.8
Build Date	Jul 12 2011 at 15:55:13
Boot Loader	BL 2.0.6.0
Copyright	N-TRON Corp.
URL	<a href="http://www.n-tron.com">http://www.n-tron.com</a>

Click to open this folder

Internet 100%

## **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.

**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.

## System Configuration View

<b>IP Configuration</b>	Static
<b>IP Address</b>	192.168.1.201
<b>Subnet Mask</b>	255.255.255.0
<b>Gateway</b>	192.168.1.1
<b>MAC Address</b>	00:07:af:fd:58:c0
<b>System Up Time</b>	0 days, 0 hours, 2 mins, 2 secs
<b>Name</b>	N-TRON Switch fd:58:c0
<b>Contact</b>	N-TRON Admin
<b>Location</b>	Mobile, AL 36609
<b>Temperature</b>	9°C, 48°F
<b>Upper Threshold</b>	80°C, 176°F
<b>Lower Threshold</b>	-40°C, -40°F

Modify

Refresh

## Administration – System, Continued...

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.

<b>System Configuration View</b>	
<b>IP Configuration</b>	DHCP
<b>Client ID</b>	00:07:affd:58:c0 Hex = 0007affd58c0
<b>IP Address</b>	192.168.1.175
<b>Subnet Mask</b>	255.255.255.0
<b>Gateway</b>	192.168.1.1
<b>Fallback IP Address</b>	192.168.1.201
<b>Fallback Subnet Mask</b>	255.255.255.0
<b>Fallback Gateway</b>	192.168.1.1
<b>MAC Address</b>	00:07:affd:58:c0
<b>System Up Time</b>	0 days, 0 hours, 0 mins, 47 secs
<b>Name</b>	N-TRON Switch fd:58:c0
<b>Contact</b>	N-TRON Admin
<b>Location</b>	Mobile, AL 36609
<b>Temperature</b>	9°C, 48°F
<b>Upper Threshold</b>	80°C, 176°F
<b>Lower Threshold</b>	-40°C, -40°F

## 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

<b>System Configuration</b>	
<b>IP Configuration</b>	Static <input type="button" value="v"/>
<b>IP Address</b>	192.168.1.201
<b>Subnet Mask</b>	255.255.255.0
<b>Gateway</b>	192.168.1.1
<b>Name</b>	N-TRON Switch fd:58:c0
<b>Contact</b>	N-TRON Admin
<b>Location</b>	Mobile, AL 36609
<b>Upper Threshold</b>	80 °C
<b>Lower Threshold</b>	-40 °C

## 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.

<b>System Configuration</b>	
<b>IP Configuration</b>	DHCP <input type="button" value="v"/>
<b>Client ID</b>	MAC Address <input type="button" value="v"/> 00:07:af:fd:58:c0
<b>Fallback IP Address</b>	192.168.1.201
<b>Fallback Subnet Mask</b>	255.255.255.0
<b>Fallback Gateway</b>	192.168.1.1
<b>Name</b>	N-TRON Switch fd:58:c0
<b>Contact</b>	N-TRON Admin
<b>Location</b>	Mobile, AL 36609
<b>Upper Threshold</b>	80 °C
<b>Lower Threshold</b>	-40 °C

## 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.

### Management Station Configuration View

<b>SNMP Mode</b>	Enabled
------------------	---------

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	public
Read-Write Community Name	private
Trap Community Name	public

SNMP Notification Trap	Send Trap?
Power Supply	No
Cold Start	Yes
Authentication	Yes
Warm Start	Yes
Link Status	Yes

Modify	Refresh
--------	---------

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 a Trap station or change the Community Names. If the SNMP Notification Trap is enabled, systems that are listed as a Trap station will be sent the corresponding notification trap. To restore a Trap to “Value Not Configured”, enter ‘0.0.0.0’.

## Administration – SNMP, Continued...

### Management Station Configuration

**Snmp Mode** Enabled ▼

<b>IP Address - Trap Stn.#1</b>	<input type="text" value="Value Not Configured"/>
<b>IP Address - Trap Stn.#2</b>	<input type="text" value="Value Not Configured"/>
<b>IP Address - Trap Stn.#3</b>	<input type="text" value="Value Not Configured"/>
<b>IP Address - Trap Stn.#4</b>	<input type="text" value="Value Not Configured"/>
<b>IP Address - Trap Stn.#5</b>	<input type="text" value="Value Not Configured"/>
<b>Read-Only Community Name</b>	<input type="text" value="public"/>
<b>Read-Write Community Name</b>	<input type="text" value="private"/>
<b>Trap Community Name</b>	<input type="text" value="public"/>

SNMP Notification Trap	Send Trap ?
Power Supply	<input type="checkbox"/>
Cold Start	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/>
Warm Start	<input checked="" type="checkbox"/>
Link Status	<input checked="" type="checkbox"/>

UpdateCancel

## Administration – Fault

The Fault tab under the Administration category provides configurable selections indicating the way to notify when a Power, N-Ring Manager, N-Link fault, or Port Usage Fault occurs. The notification may consist of any combination of the options: Show Web, Show LED, and Contact. Power signal faults consist of  $V_1$  and  $V_2$ . 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).

### Fault Configuration View

Meaning Close on Fault

Signal	Show Web	Show LED	Contact
Power $V_1$	No	No	No
Power $V_2$	No	No	No
N-Link Fault	Yes	Yes	Yes
Port Usage Fault	Yes	Yes	Yes

N-Ring Manager Signal	Show LED	Contact
Broken	Yes	Yes
Partial Break(Low)	Yes	Yes
Partial Break(High)	Yes	Yes
Multiple Managers	Yes	Yes

Modify Refresh

Note:  $V_1$  and  $V_2$  Power Faults are disabled in factory defaults.



Following the Modify button, the administrator will see a list of configurable fields for the Fault configuration. The fault relay contacts can be configured to open on fault or to close on fault, with the latter being the default. 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 Fault Configuration

<b>Meaning</b>	Close on Fault <span style="font-size: 0.8em;">▼</span>
	Open on Fault
	Close on Fault

Signal	Show Web	Show LED	Contact
Power V <sub>1</sub>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Power V <sub>2</sub>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
N-Link Fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Port Usage Fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

N-Ring Manager Signal	Show LED	Contact
Broken	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Partial Break(Low)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Partial Break(High)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Multiple Managers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 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

<b>Server Enabled</b>	Enabled
<b>Allow Broadcast</b>	Enabled
<b>Delay Broadcast (Ms)</b>	500
<b>Server ID</b>	N-Tron Switch fe:bd:e0

Network Profiles						
Profile Name	Address Pool	Subnet Address	Subnet Mask	Domain Name	Has Profile IP Maps	
DEFAULT						



## DHCP – Server – Setup Profiles, Continued...

<b>DHCP Server Configuration</b>	
Server Enabled	Enabled <input type="button" value="v"/>
Allow Broadcast	Enabled <input type="button" value="v"/>
Delay Broadcast (Ms)	500
Server ID	N-Tron Switch fe:bd:e0

## DHCP Server Network Profile

Network Profile Name	<input type="text" value="Prof_1"/>
Address Pool Start	<input type="text" value="192.168.1.25"/>
Address Pool End	<input type="text" value="192.168.1.254"/>
Lease Time	<input type="text" value="28"/> Days
	<input type="text" value="0"/> Hours
<input type="button" value="Advanced &lt;&lt;"/>	
Broadcast Address *	<input type="text"/>
Domain Name *	<input type="text" value=""/> <small>Default Domain Name = 'localdomain.com'</small>
DNS Server 1 **	<input type="text"/>
DNS Server 2 **	<input type="text"/>
Gateway 1 **	<input type="text"/>
Gateway 2 **	<input type="text"/>

\* When field is left blank, the corresponding default profile value is used.

\*\* When both related fields are left blank, the corresponding default profile values are used.

## 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.

The screenshot shows a window titled "DHCP Server Setup IP Maps". It features a table with three columns: "Network Profile", "Binding Identifier", and "IP Map". Below the table is a message: "You must add a non Default Network Profile before adding an IP Map." Underneath is a "Select Mapping" section with three buttons: "Dynamic Range" (labeled "IP Address Range"), "Static Range" (labeled "Option 82 Relay Agent"), and "Single IP" (labeled "Option 61 or MAC"). A "Refresh" button is located at the bottom.

**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 screenshot shows a window titled "DHCP Server Dynamic Range". It contains a form with three fields: "Network Profile" (a dropdown menu showing "prof\_1"), "Low IP" (an empty text box), and "High IP" (an empty text box). At the bottom are "Update" and "Cancel" buttons.

**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.

## DHCP – Server – Setup IP Maps, Continued...

### 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 – Setup IP Maps, Continued...

### DHCP Server Static Range

#### (Option 82)

Network Profile	<input type="text" value="prof_1"/>
Relay Agent Type	<input checked="" type="radio"/> N-TRON <input type="radio"/> Generic
Switch Model	<input type="text" value="709FX"/>
Remote ID	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input checked="" type="radio"/> IP <input type="radio"/> String

Add	Port No	Port Name	VLAN	Circuit ID	IP Address
<input type="checkbox"/>	1	<input type="text" value="TX1"/>	<input type="text" value="1"/>	TX1-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	2	<input type="text" value="TX2"/>	<input type="text" value="1"/>	TX2-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	3	<input type="text" value="TX3"/>	<input type="text" value="1"/>	TX3-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	4	<input type="text" value="TX4"/>	<input type="text" value="1"/>	TX4-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	5	<input type="text" value="TX5"/>	<input type="text" value="1"/>	TX5-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	6	<input type="text" value="TX6"/>	<input type="text" value="1"/>	TX6-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	7	<input type="text" value="TX7"/>	<input type="text" value="1"/>	TX7-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	8	<input type="text" value="TX8"/>	<input type="text" value="1"/>	TX8-0001	<input type="text" value="192.168.1."/>
<input type="checkbox"/>	9	<input type="text" value="FX1"/>	<input type="text" value="1"/>	FX1-0001	<input type="text" value="192.168.1."/>



## 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.

192.168.1.214 N-TRON Switch ff:23:80 - Windows Internet Explorer

http://192.168.1.214/main.ssi

File Edit View Favorites Tools Help

192.168.1.214 N-TRON ... 192.168.1.215 N-TRON Swit...

**N-TRON**  
THE INDUSTRIAL NETWORK COMPANY

- Administration
  - System
  - SNMP
  - Fault
- DHCP
  - Server
    - Setup Profiles
    - Setup IP Maps
    - View Bindings
  - Relay & Local IP
- LLDP
- Ports
- Statistics
- VLAN
- Bridging
- RSTP
- IGMP
- N-View
- N-Ring
- N-Link
- CIP
- Firmware/Config
- Support
  - BPCL
  - User Management
  - Logical View
  - Home
  - Config
  - Help
  - Logout

Copyright © 2008-2009  
N-TRON Corp.  
All rights reserved.  
http://www.n-tron.com

Logged in as: **admin**

## DHCP Server Static Range

(Option 82)

Network Profile	prof_1		
Relay Agent Type	<input type="radio"/> N-TRON <input checked="" type="radio"/> Generic		
Port Count	8	Apply	

Add	Port No	Remote ID	Circuit ID	IP Address
<input type="checkbox"/>	1	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	2	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	3	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	4	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	5	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	6	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	7	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.
<input type="checkbox"/>	8	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	<input type="text"/> <input type="radio"/> Hex <input type="radio"/> MAC <input type="radio"/> IP <input type="radio"/> String	192.168.1.

## 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.

The screenshot shows a configuration window titled "DHCP Server Static IP (Option 61/MAC)". The window contains three main input fields: "Network Profile" with a dropdown menu showing "prof\_1", "IP" with an empty text box, and "Unique ID (i.e. - MAC)" with an empty text box. To the right of the Unique ID field is a "Format" dropdown menu with options: "MAC Address" (selected), "Hex Values", "MAC Address", and "String". At the bottom of the window are "Update" and "Cancel" buttons.

Field	Value
Network Profile	prof_1
IP	
Unique ID (i.e. - MAC)	
Format	MAC Address

## 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.

<b>DHCP Server Binding List</b>					
Network Profile	Binding Identifier <input type="checkbox"/> Show Hex	Client Hardware Address (MAC)	Client IP Address	Status	
prof_1	Client ID (String) = N-Tron Switch fb:fa:40	00:07:af:fb:fa:40	192.168.2.100	Dynamic, In Use	<input type="button" value="Release"/>

## DHCP – Relay & Local IP - Setup

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

The screenshot displays the N-TRON web interface for the DHCP Relay Agent & Local IP Setup. The left navigation menu shows the following structure:

- Administration
- DHCP
  - Server
    - Setup Profiles
    - Setup IP Maps
    - View Bindings
  - Relay & Local IP
    - Setup
- LLDP
- Ports
- Statistics
- VLAN
- Bridging
- RSTP
- IGMP
- N-View
- N-Ring
- N-Link
- CIP
- Firmware/Config
- Support
  - BPCL
  - User Management
  - Logical View
  - Home
  - Config
  - Help
  - Logout

The main content area is titled "DHCP Relay Agent & Local IP Setup View" and contains the following information:

Relay Status	Disabled
Remote ID	192.168.1.229
Server 1 IP	
Server 2 IP	
Server 3 IP	
Server 4 IP	

Port No	Port Name	Relay Status
01	TX1	Disabled
02	TX2	Disabled
03	TX3	Disabled
04	TX4	Disabled
05	TX5	Disabled
06	TX6	Disabled
07	TX7	Disabled
08	TX8	Disabled
09	FX1	Disabled

At the bottom of the main content area, there are two buttons: "Modify" and "Refresh".

Copyright © 2008-2009 N-TRON Corp. All rights reserved. <http://www.n-tron.com>

Logged in as: **admin**

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...

### DHCP Relay Agent & Local IP Setup

Relay Status	Disabled ▾
Remote ID	IP Address ▾ 192.168.1.229
Server 1 IP	<input type="text"/>
Server 2 IP	<input type="text"/>
Server 3 IP	<input type="text"/>
Server 4 IP	<input type="text"/>

Port No	Port Name	Relay Status	Other Data	
01	TX1	Disabled ▾		
02	TX2	Disabled ▾		
03	TX3	Disabled ▾		
04	TX4	Disabled ▾		
05	TX5	Disabled ▾		
06	TX6	Disabled ▾		
07	TX7	Disabled ▾		
08	TX8	Disabled ▾		
09	FX1	Disabled ▾		

Update Cancel

## 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:**

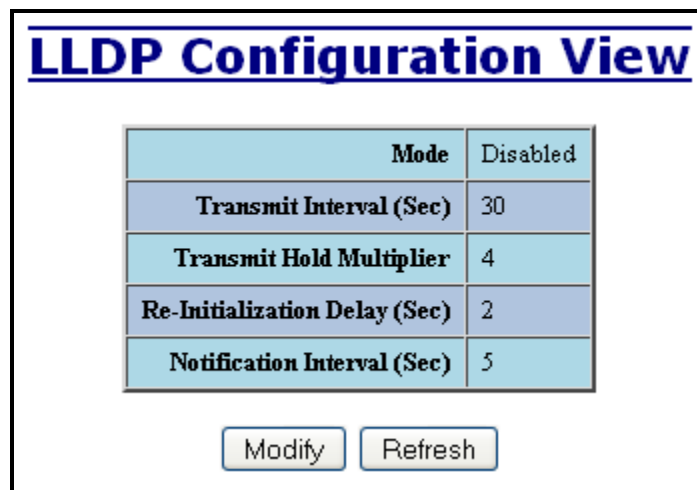
Specifies a multiplier on the Transmit Interval when calculating a Time-to-Live value. Default = 4.

**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.



<b>LLDP Configuration View</b>	
<b>Mode</b>	Disabled
<b>Transmit Interval (Sec)</b>	30
<b>Transmit Hold Multiplier</b>	4
<b>Re-Initialization Delay (Sec)</b>	2
<b>Notification Interval (Sec)</b>	5

Modify Refresh

**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.

Port Name	Transmit	Receive	Allow Management Data	Allow Notification
TX1	NO	YES	YES	NO
TX2	YES	NO	YES	NO
TX3	YES	YES	NO	NO
TX4	YES	YES	YES	YES
TX5	YES	YES	YES	NO
TX6	YES	YES	YES	NO
TX7	YES	YES	YES	NO
TX8	YES	YES	YES	NO
FX1	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 Ports Neighbor View

Port Name	Neighbor MAC	Neighbor IP	Neighbor Port Description	Neighbor System Name	Neighbor Vlan PVID	Neighbor Vlan ID/Name	Neighbor TTL
TX1	00:07:af:fd:58:c1	192.168.1.229	Port 1 - 10/100 Mbit TX	N-TRON Switch fd:58:c0	1	0001 - Default VLAN	118
TX3	00:07:af:fd:57:e3	192.168.1.225	Port 3 - 10/100 Mbit TX	N-TRON Switch fd:57:e0	1	0001 - Default VLAN	95
TX4	00:07:af:fb:e0:b5	192.168.1.247	Port 5 - 10/100 Mbit TX	N-Tron Switch fb:e0:b0	1	0001 - Default VLAN	106
TX8	00:07:af:fd:61:42	192.168.1.228	Port 2 - 10/100 Mbit TX	N-TRON Switch fd:61:40	1	0001 - Default VLAN	94

Refresh

## 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).

<b>LLDP Local Port Statistics View</b>						
Port Name	Transmitted Frames	Received Frames	Discarded Frames	Error Frames	Neighbor Age Outs	LLDP Port Status
TX1	0	14	0	0	0	Rx
TX2	18	0	0	0	0	Tx
TX3	0	0	0	0	0	RxTx
TX4	0	0	0	0	0	RxTx
TX5	18	0	0	0	0	RxTx
TX6	0	0	0	0	0	RxTx
TX7	0	0	0	0	0	RxTx
TX8	18	0	0	0	0	RxTx
FX1	0	0	0	0	0	RxTx

## 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**.

### **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...

### Port Configuration View

Port No	Port Name	Admin Status	Link Status	Auto Nego	Port Speed	Duplex Mode	Flow Control	Port State	PVID	Usage Alarm Low [%]	Usage Alarm High [%]
<a href="#">01</a>	TX1	Disabled	Down	Disabled	10	Half	Disabled	Disabled	1	0	100
<a href="#">02</a>	TX2	Enabled	Up	Enabled	100	Full	Disabled	Forwarding	1	0	100
<a href="#">03</a>	TX3	Enabled	Up	Disabled	100	Half	Disabled	Forwarding	1	0	100
<a href="#">04</a>	TX4	Disabled	Down	Enabled	Auto	Auto	Disabled	Disabled	1	0	100
<a href="#">05</a>	TX5	Enabled	Down	Enabled	Auto	Auto	Disabled	Disabled	99	25	90
<a href="#">06</a>	TX6	Enabled	Down	Enabled	Auto	Auto	Disabled	Disabled	1	0	100
<a href="#">07</a>	TX7	Enabled	Down	Enabled	Auto	Auto	Disabled	Disabled	1	0	100
<a href="#">08</a>	TX8	Enabled	Up	Enabled	100	Full	Disabled	Forwarding	1	0	100
<a href="#">09</a>	FX1	Enabled	Down	Disabled	100	Full	Disabled	Disabled	1	0	100

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 which are explained above:

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

### TX2 - Port Configuration

Port Name	TX2
Admin Status	Enabled <input type="button" value="v"/>
Speed And Duplex	Auto-Negotiate <input type="button" value="v"/>
Cross Over	Auto <input type="button" value="v"/>
Flow Control	Disabled <input type="button" value="v"/>
PVID	<input type="text" value="1"/>
Usage Alarm Low [%]	<input type="text" value="0"/>
Usage Alarm High [%]	<input type="text" value="100"/>

## 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 which are explained above:

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

### TX2 - Port Configuration

Port Name	TX2
Admin Status	Enabled <input type="button" value="v"/>
Speed And Duplex	Auto-Negotiate <input type="button" value="v"/>
Cross Over	Auto <input type="button" value="v"/>
Flow Control	Disabled <input type="button" value="v"/>
PVID	<input type="text" value="1"/>
Usage Alarm Low [%]	<input type="text" value="0"/>
Usage Alarm High [%]	<input type="text" value="100"/>

## Ports – MAC Security – Learning

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.

### MAC Learning View

Current Mode Learning

**Secure Ports**

Port No	Port Name	Secure	Role
01	TX1	<input type="checkbox"/>	RSTP
02	TX2	<input type="checkbox"/>	RSTP
03	TX3	<input type="checkbox"/>	RSTP
04	TX4	<input type="checkbox"/>	RSTP
05	TX5	<input type="checkbox"/>	RSTP
06	TX6	<input type="checkbox"/>	RSTP
07	TX7	<input type="checkbox"/>	RSTP
08	TX8	<input type="checkbox"/>	RSTP
09	FX1	<input type="checkbox"/>	RSTP

Modify Refresh



## Ports – MAC Security – Learning 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.*

### MAC Learning View

Current Mode Locked

**Secure Ports**

Port No	Port Name	Secure	Role
01	TX1	<input checked="" type="checkbox"/>	RSTP
02	TX2	<input checked="" type="checkbox"/>	RSTP
03	TX3	<input checked="" type="checkbox"/>	RSTP
04	TX4	<input checked="" type="checkbox"/>	RSTP
05	TX5	<input checked="" type="checkbox"/>	RSTP
06	TX6	<input checked="" type="checkbox"/>	RSTP
07	TX7	<input checked="" type="checkbox"/>	RSTP
08	TX8	<input type="checkbox"/>	RSTP
09	FX1	<input checked="" type="checkbox"/>	RSTP

Modify Refresh

## Ports – MAC Security – Learning Continued...

The Modify button allows the administrator to change the current mode and select the ports to be secured. 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 Locked ▾  
Learning  
Locked

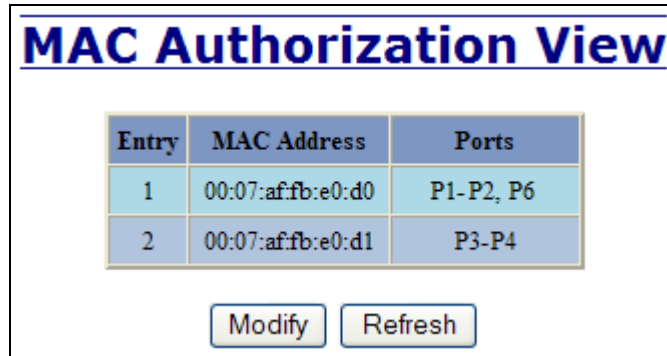
Secure ports

Port No	Port Name	Secure	Role
01	TX1	<input type="checkbox"/>	RSTP
02	TX2	<input type="checkbox"/>	RSTP
03	TX3	<input type="checkbox"/>	RSTP
04	TX4	<input type="checkbox"/>	RSTP
05	TX5	<input type="checkbox"/>	RSTP
06	TX6	<input type="checkbox"/>	RSTP
07	TX7	<input type="checkbox"/>	RSTP
08	TX8	<input type="checkbox"/>	RSTP
09	FX1	<input type="checkbox"/>	RSTP

Update Cancel

## Ports – MAC Security – Authorization List

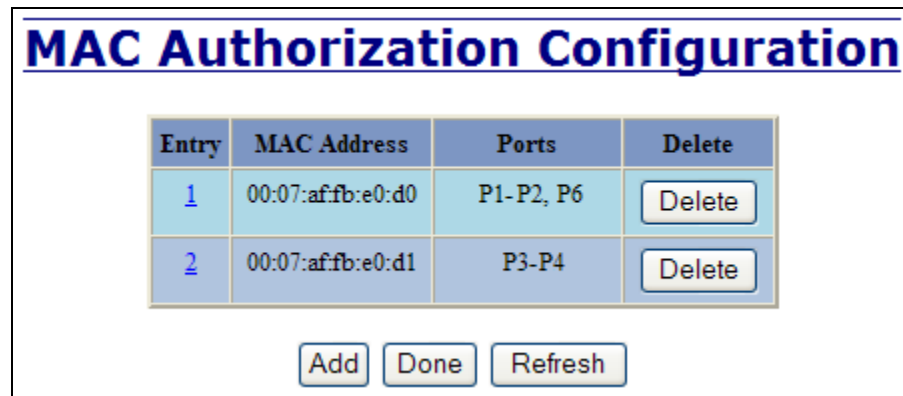
The Authorization List tab allows for manual entry or deletion of authorized MAC source addresses with associated authorized ports.



Entry	MAC Address	Ports
1	00:07:af:fb:e0:d0	P1-P2, P6
2	00:07:af:fb:e0:d1	P3-P4

Modify Refresh

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.



Entry	MAC Address	Ports	Delete
<a href="#">1</a>	00:07:af:fb:e0:d0	P1-P2, P6	Delete
<a href="#">2</a>	00:07:af:fb:e0:d1	P3-P4	Delete

Add Done Refresh

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.

## MAC Authorization Entry

MAC Address	<input type="text" value="00:00:00:00:00:00"/>			
Port List	<input checked="" type="checkbox"/> TX1	<input checked="" type="checkbox"/> TX2	<input checked="" type="checkbox"/> TX3	<input checked="" type="checkbox"/> TX4
	<input checked="" type="checkbox"/> TX5	<input checked="" type="checkbox"/> TX6	<input checked="" type="checkbox"/> TX7	<input checked="" type="checkbox"/> TX8
	<input checked="" type="checkbox"/> FX1			
	<input type="button" value="Select All"/> <input type="button" value="Select None"/>			

## 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.

### Intruder Log

Entry	MAC Address	VLAN	Port	System Time	
1	00:1f:29:2d:2b:f2	1	TX8	0 days, 4 hours, 41 mins, 26 secs	Delete
2	00:19:b9:03:af:51	1	TX8	0 days, 4 hours, 41 mins, 19 secs	Delete
3	00:23:7d:85:8d:c4	1	TX8	0 days, 4 hours, 41 mins, 13 secs	Delete
4	00:19:b9:26:56:6f	1	TX8	0 days, 4 hours, 41 mins, 10 secs	Delete

ALL   

- ALL
- TX1
- TX2
- TX3
- TX4
- TX5
- TX6
- TX7
- TX8
- FX1

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.

### Port Mirroring Configuration View

Mirror Status	Disabled
Destination Port	TX1
Mirrored Data Only	<input type="checkbox"/>

**Source Ports**

Port No	Port Name	Tx	Rx
01	TX1	<input type="checkbox"/>	<input type="checkbox"/>
02	TX2	<input type="checkbox"/>	<input type="checkbox"/>
03	TX3	<input type="checkbox"/>	<input type="checkbox"/>
04	TX4	<input type="checkbox"/>	<input type="checkbox"/>
05	TX5	<input type="checkbox"/>	<input type="checkbox"/>
06	TX6	<input type="checkbox"/>	<input type="checkbox"/>
07	TX7	<input type="checkbox"/>	<input type="checkbox"/>
08	TX8	<input type="checkbox"/>	<input type="checkbox"/>
09	FX1	<input type="checkbox"/>	<input type="checkbox"/>

## Ports – Mirroring, Continued ...

Following the Modify button, you can enable the status of port mirroring and select source ports and the destination port that the source ports will be mirrored to.

### Port Mirroring Configuration

<b>Mirror Status</b>	Disabled ▾
<b>Destination Port</b>	TX1 ▾
<b>Mirrored Data Only</b>	TX1 TX2 TX3 TX4 TX5 TX6 TX7 TX8 FX1

Source Ports			
Port No	Port Name	T	R
	ALL	<input type="checkbox"/>	<input type="checkbox"/>
01	TX1	<input type="checkbox"/>	<input type="checkbox"/>
02	TX2	<input type="checkbox"/>	<input type="checkbox"/>
03	TX3	<input type="checkbox"/>	<input type="checkbox"/>
04	TX4	<input type="checkbox"/>	<input type="checkbox"/>
05	TX5	<input type="checkbox"/>	<input type="checkbox"/>
06	TX6	<input type="checkbox"/>	<input type="checkbox"/>
07	TX7	<input type="checkbox"/>	<input type="checkbox"/>
08	TX8	<input type="checkbox"/>	<input type="checkbox"/>
09	FX1	<input type="checkbox"/>	<input type="checkbox"/>

## Ports – Mirroring, Continued...

**Mirrored Data Only:** If this checkbox is selected, only mirrored data will be transmitted by the destination port. That is, data that was to be transmitted from the Destination Port itself, other than by mirroring, will not be transmitted.

### Port Mirroring Configuration

Mirror Status	Enabled <input type="button" value="v"/>
Destination Port	TX1 <input type="button" value="v"/>
Mirrored Data Only	<input checked="" type="checkbox"/>

**Source Ports**

Port No	Port Name	Tx	Rx
	ALL	<input type="checkbox"/>	<input type="checkbox"/>
01	TX1	<input type="checkbox"/>	<input type="checkbox"/>
02	TX2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
03	TX3	<input type="checkbox"/>	<input type="checkbox"/>
04	TX4	<input type="checkbox"/>	<input type="checkbox"/>
05	TX5	<input type="checkbox"/>	<input type="checkbox"/>
06	TX6	<input type="checkbox"/>	<input type="checkbox"/>
07	TX7	<input type="checkbox"/>	<input type="checkbox"/>
08	TX8	<input type="checkbox"/>	<input type="checkbox"/>
09	FX1	<input type="checkbox"/>	<input type="checkbox"/>



## Ports – Trunking

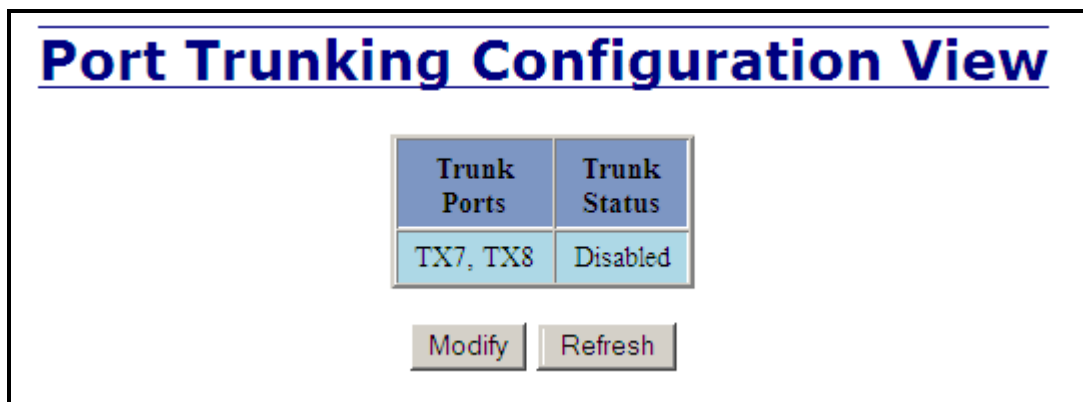
The Trunking tab under the Ports category displays the following details:

**Trunk Ports**

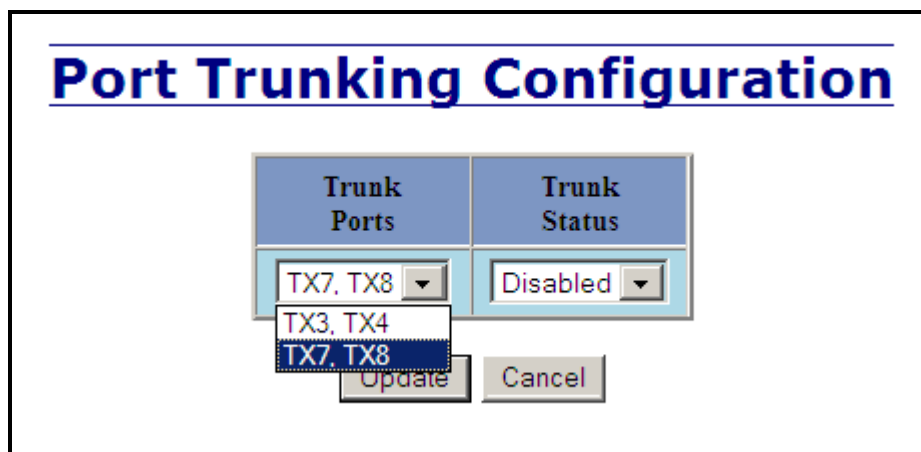
This field displays the ports associated with the trunk.

**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 802.1p 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**

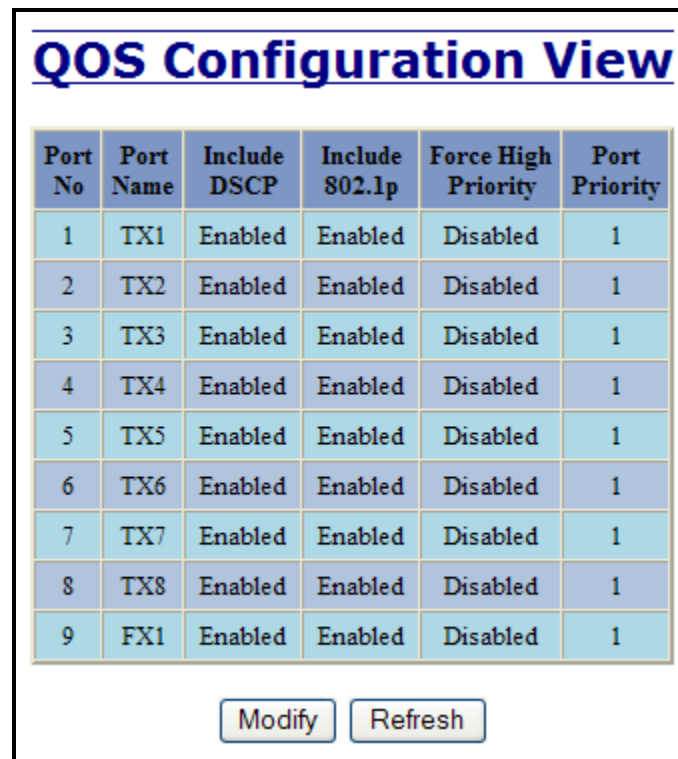
This field displays the status of whether or not to include the IEEE 802.1p COS (Class of Service) in the TQ decision. When enabled, the IEEE 802.1p COS is included when evaluating traffic priority.

**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.



Port No	Port Name	Include DSCP	Include 802.1p	Force High Priority	Port Priority
1	TX1	Enabled	Enabled	Disabled	1
2	TX2	Enabled	Enabled	Disabled	1
3	TX3	Enabled	Enabled	Disabled	1
4	TX4	Enabled	Enabled	Disabled	1
5	TX5	Enabled	Enabled	Disabled	1
6	TX6	Enabled	Enabled	Disabled	1
7	TX7	Enabled	Enabled	Disabled	1
8	TX8	Enabled	Enabled	Disabled	1
9	FX1	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	TX1	Enabled ▾	Enabled ▾	Disabled ▾	1 ▾
2	TX2	Enabled ▾	Enabled ▾	Disabled ▾	1 ▾
3	TX3	Enabled ▾	Enabled ▾	Disabled ▾	1 ▾
4	TX4	Enabled ▾	Enabled ▾	Disabled ▾	1 ▾
5	TX5	Enabled ▾	Enabled ▾	Disabled ▾	1 ▾
6	TX6	Enabled ▾	Enabled ▾	Disabled ▾	1 ▾
7	TX7	Enabled ▾	Enabled ▾	Disabled ▾	0 1 2 3 4 5 6 7
8	TX8	Enabled ▾	Enabled ▾	Disabled ▾	
9	FX1	Enabled ▾	Enabled ▾	Disabled ▾	

## **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 the 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.

## Port Statistics

Port TX2

### Statistics For Port TX2

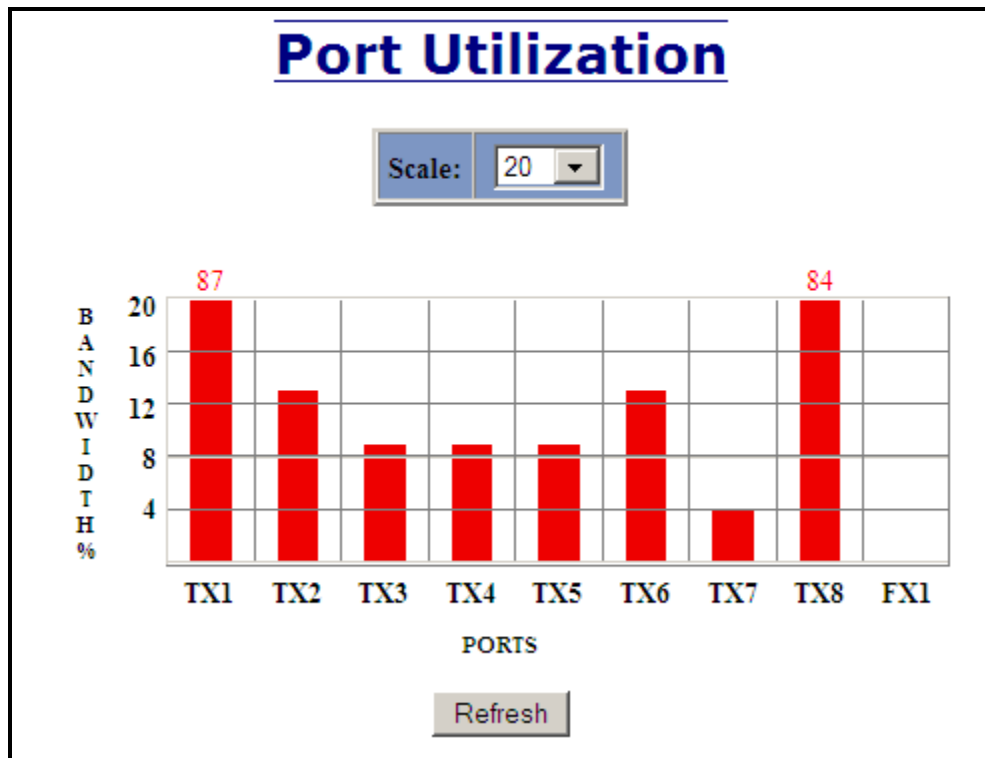
S.No	Counter Type	Value
1	Tx Octets	7293473
2	Tx Dropped Packets	0
3	Tx Broadcast Packets	1
4	Tx Multicast Packets	34320
5	Tx Unicast Packets	618
6	Tx Collisions	0
7	Tx Single Collision	0
8	Tx Multiple Collision	0
9	Tx Deferred Transmit	0
10	Tx Late Collision	0
11	Tx Excessive Collision	0
12	Tx Frame In Disc	0
13	Tx Pause Packets	0
14	Rx 64 Packets	5616
15	Rx 65 to 127 Packets	8858
16	Rx 128 to 255 Packets	13
17	Rx 256 to 511 Packets	4
18	Rx 512 to 1023 Packets	110
19	Rx 1024 to 1522 Packets	0
20	Rx Octets	1081713
21	Rx Dropped Packets	0
22	Rx Broadcast Packets	110
23	Rx Multicast Packets	11806
24	Rx Unicast Packets	2685
25	Rx Undersize Packets	0
26	Rx Oversize Packets	0
27	Rx Jabbers	0
28	Rx Alignment Errors	0
29	Rx Good Octets	1081713
30	Rx SA Changes	6765
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

Refresh

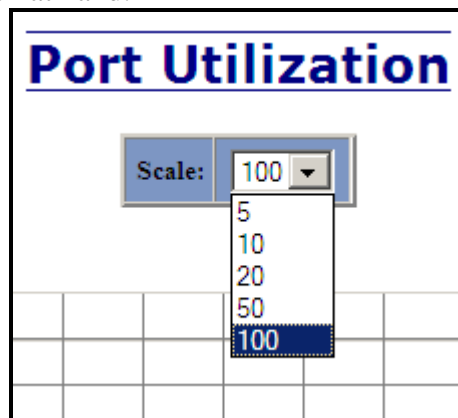
Clear

## Statistics – Port 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 more 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.

### VLAN Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>

### VLAN Configuration

Replace VID Tag With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1

VLAN Groups					
VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
<a href="#">0001</a>	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>	
<input type="button" value="Add"/>					

Note that for convenience in most frequent use:

- Ports are deleted from group1 as each port is added to another group.
- 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.

**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.

## Tagged VLAN Group Configuration

ID	<input type="text" value="2"/>
Name	<input type="text" value="VLAN2"/>
Allow Management	<input checked="" type="checkbox"/>
Change PVID Of Member Ports	<input checked="" type="checkbox"/>

### Group Ports

Port No	Port Name	Group Member	Untag On Egress
01	TX1	<input type="checkbox"/>	<input type="checkbox"/>
02	TX2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
03	TX3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
04	TX4	<input type="checkbox"/>	<input type="checkbox"/>
05	TX5	<input type="checkbox"/>	<input type="checkbox"/>
06	TX6	<input type="checkbox"/>	<input type="checkbox"/>
07	TX7	<input type="checkbox"/>	<input type="checkbox"/>
08	TX8	<input type="checkbox"/>	<input type="checkbox"/>
09	FX1	<input type="checkbox"/>	<input type="checkbox"/>

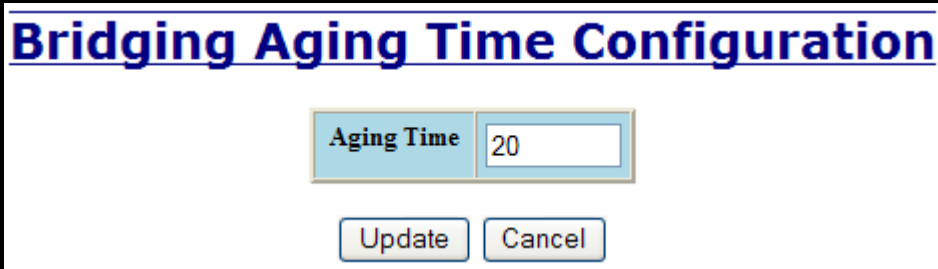
## Bridging – Aging Time

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.



The screenshot shows a web interface titled "Bridging Aging Time View". It features a light blue header bar with the title in bold blue text. Below the header, there is a light blue box containing the text "Aging Time" followed by "20 secs". Below this box, there are two buttons: "Modify" and "Refresh".

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



The screenshot shows a web interface titled "Bridging Aging Time Configuration". It features a light blue header bar with the title in bold blue text. Below the header, there is a light blue box containing the text "Aging Time" followed by a text input field containing the number "20". Below this box, there are two buttons: "Update" and "Cancel".

**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.

### Display Static Unicast MAC Addresses

Static Unicast MAC Address Filters		
MAC Address	Port	VLAN ID

Number of Static Unicast MAC Addresses: **0**

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 Add button, the changes will take effect instantly.

### Add Unicast MAC Address Filter

Mac Address	<input type="text" value="00:07:AF:00:00:00"/>
Port	<input type="text" value="TX1"/>
VLAN ID	<input type="text" value="1"/>

## Bridging – Unicast Addresses, Continued...

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

### Display Static Unicast MAC Addresses

Static Unicast MAC Address Filters		
MAC Address	Port	VLAN ID
00:07:af:00:00:00	TX1	1

Number of Static Unicast MAC Addresses: **1**

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

### Remove Unicast MAC Address Filter

Mac Address

Number of Static Unicast MAC Addresses: **1**

## 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.

### Display Static Multicast Group Addresses

Static Multicast Group Address Filters		
Multicast Address	Port List	VLAN ID

Number of Static Multicast Group Addresses: **0**

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.

### Add Multicast Group Address Filter

<b>Multicast Address</b>	<input type="text" value="01:07:AF0:00:22"/>
<b>Port List</b>	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input checked="" type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1
<b>VLAN ID</b>	<input type="text" value="1"/>

**Note:** *If there are multiple ports on different VLANs, the 709FX 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.

### Display Static Multicast Group Addresses

Static Multicast Group Address Filters		
Multicast Address	Port List	VLAN ID
01:07:af:00:00:00	TX1, TX2, TX3, TX4	1

Number of Static Multicast Group Addresses: **1**

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.

### Remove Multicast Group Address Filter

Mac Address	01:07:af:00:00:00 ▼
-------------	---------------------

Number of Static Multicast Group Addresses: **1**

**Note:** *If there are multiple ports on different VLANs, the 709FX 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	Enabled
<input type="button" value="Modify"/>	

MACs By Port				
Port No	Port Name	MAC Address	IP	Manual Entry
01	TX1			
02	TX2	00:07:af:01:93:de	192.168.1.222	<input type="button" value="Delete IP"/>
03	TX3	00:1e:4f:bc:68:62	192.168.1.118	
04	TX4			
05	TX5			
06	TX6	00:07:af:fd:57:e0	192.168.1.225	
07	TX7	00:07:af:fb:e0:b0	192.168.1.247	
08	TX8	00:07:af:00:e4:0f		<input type="button" value="Assign IP"/>
09	FX1			

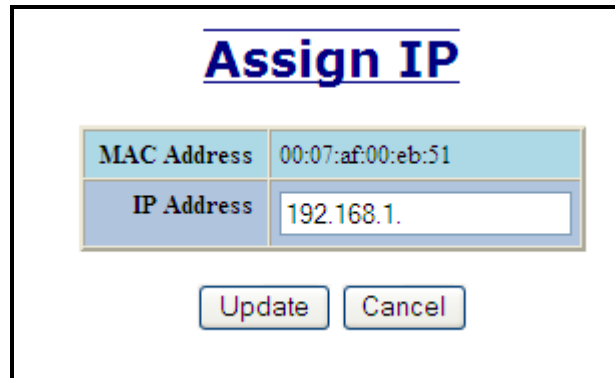
The ‘Active IP Probe’ field is configurable using the ‘Modify’ button, and also displays the existing Enabled or Disabled status of this feature. The default is disabled. When disabled the switch generates no ethernet traffic for this purpose, but can still present some information gathered passively.

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:



The image shows a web form titled "Assign IP" in a blue, underlined font. Below the title is a table with two rows. The first row has "MAC Address" in a light blue box and "00:07:af:00:eb:51" in a white box. The second row has "IP Address" in a light blue box and "192.168.1." in a white box. Below the table are two buttons: "Update" and "Cancel", both in light blue boxes with black text.

<u>Assign IP</u>	
MAC Address	00:07:af:00:eb:51
IP Address	192.168.1.

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 View

VLAN 1 - Default VLAN ▼

**RSTP Root Bridge Configuration**

Root Priority	Designated Root	Path Cost	Port	Max Age	Hello Time	Forward Delay
32768	80:00:00:07:affe:bd:c1	0	0	16	1	13

**This Bridge [Configuration](#)**

Hello Time (Sec)	Forward Delay (Sec)	Max Age (Sec)	Priority	RSTP Status	Topology Change	Topology Count
1	13	16	32768	Fast	False	0

## 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#.

### RSTP Bridge Configuration For VLAN 1

VLAN	0001 - Default VLAN
Hello Time	<input type="text" value="1"/>
Forward Delay	<input type="text" value="13"/>
Max Age	<input type="text" value="16"/>
Priority	<input type="text" value="32768"/> ▼
Status	<input type="text" value="Fast"/> ▼

Click [here](#) to view the RSTP port Configuration at VLAN 1

**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, TX2 is a redundant port with port TX1, therefore TX1 is forwarding and TX2 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
<a href="#">01</a>	TX1	Forwarding	200000	128	No	Enabled	Disabled	00:00:00:07:af:fd:57:e1	00:01
<a href="#">02</a>	TX2	Discarding	200000	128	No	Enabled	Disabled	00:00:00:07:af:fd:57:e1	00:02
<a href="#">03</a>	TX3	Forwarding	567	32	No	Disabled	Enabled	f0:00:00:07:af:fd:61:41	00:03
<a href="#">04</a>	TX4	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:04
<a href="#">05</a>	TX5	Forwarding	200000	128	No	Enabled	Disabled	f0:00:00:07:af:fd:61:41	00:05
<a href="#">06</a>	TX6	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:06
<a href="#">07</a>	TX7	Forwarding	200000	128	No	Enabled	Disabled	f0:00:00:07:af:fd:61:41	00:07
<a href="#">08</a>	TX8	Forwarding	200000	128	No	Enabled	Disabled	f0:00:00:07:af:fd:61:41	00:08
<a href="#">09</a>	FX1	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:09

<< Back

Refresh

## RSTP – Configuration Continued...

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.

### RSTP Bridge Port Configuration

VLAN	0001 - Default VLAN
Port Name	TX2
Path Cost	<input type="text" value="0"/>
Priority	<input type="text" value="128"/> ▼
Admin Edge	<input type="text" value="Disabled"/> ▼
Auto Edge	<input type="text" value="Enabled"/> ▼

## IGMP – Configuration

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

### IGMP Configuration View

IGMP Status	Enabled
Query Mode	Auto
Router Mode	Auto
Remove Unused Groups	<input checked="" type="checkbox"/>
Manual Router Ports	(None)
N-Ring Router Ports	(None)
N-Link Router Port	(None)

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

IGMP Status	Enabled <input type="button" value="v"/>
Query Mode	Auto <input type="button" value="v"/>
Router Mode	Auto <input type="button" value="v"/>
Remove Unused Groups	<input checked="" type="checkbox"/>
Manual Router Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1 <input type="button" value="Select All"/> <input type="button" value="Select None"/>

## IGMP – Configuration, Continued...

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

<b>IGMP Configuration</b>	
IGMP Status	Enabled ▾
Query Mode	Disabled Enabled
Router Mode	Auto ▾
Remove Unused Groups	<input checked="" type="checkbox"/>
Manual Router Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1
	<input type="button" value="Select All"/> <input type="button" value="Select None"/>
	<input type="button" value="Update"/> <input type="button" value="Cancel"/>

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

## IGMP Configuration

IGMP Status	Enabled ▾
Query Mode	Auto ▾
Router Mode	Off On ▾
Remove Unused Groups	Auto <input checked="" type="checkbox"/>
Manual Router Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1 <input type="button" value="Select All"/> <input type="button" value="Select None"/>



## 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.

IGMP Configuration	
IGMP Status	Enabled
Query Mode	Auto
Router Mode	Auto
Remove Unused Groups	None
Manual Router Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1
	Select All Select None
Update Cancel	

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 Configuration

<b>IGMP Status</b>	Enabled ▾
<b>Query Mode</b>	Auto ▾
<b>Router Mode</b>	Auto ▾
<b>Remove Unused Groups</b>	<input checked="" type="checkbox"/>
<b>Manual Router Ports</b>	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1 <input type="button" value="Select All"/> <input type="button" value="Select None"/>

The user can specify the manual router ports:

### IGMP Configuration

<b>IGMP Status</b>	Enabled ▾
<b>Query Mode</b>	Auto ▾
<b>Router Mode</b>	Manual ▾
<b>Remove Unused Groups</b>	<input checked="" type="checkbox"/>
<b>Manual Router Ports</b>	<input checked="" type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input checked="" type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1 <input type="button" value="Select All"/> <input type="button" value="Select None"/>

## 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.

### IGMP Group View

**Total Number Of Active IP Group Memberships** 11

Group IP	Port Name	VLAN ID
239.255.255.253	TX3-TX4	1
224.0.1.60	TX3-TX4	1
239.255.255.254	TX3-TX4	1
224.0.1.24	TX3-TX4	1
239.255.255.250	TX5	1
224.0.0.252	TX5	1
224.1.0.38	TX5	1
239.255.255.254	TX5	1
224.0.1.24	TX5	1
224.0.1.60	TX5	1
224.0.0.251	TX5	1

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.

### Auto-Detected Routers View

Router IP	Port Name	VLAN ID
192.9.9.3	TX6	1
192.168.1.231	TX8	1
192.168.1.242	TX8	1
192.168.1.232	TX8	1



## IGMP – RFilter

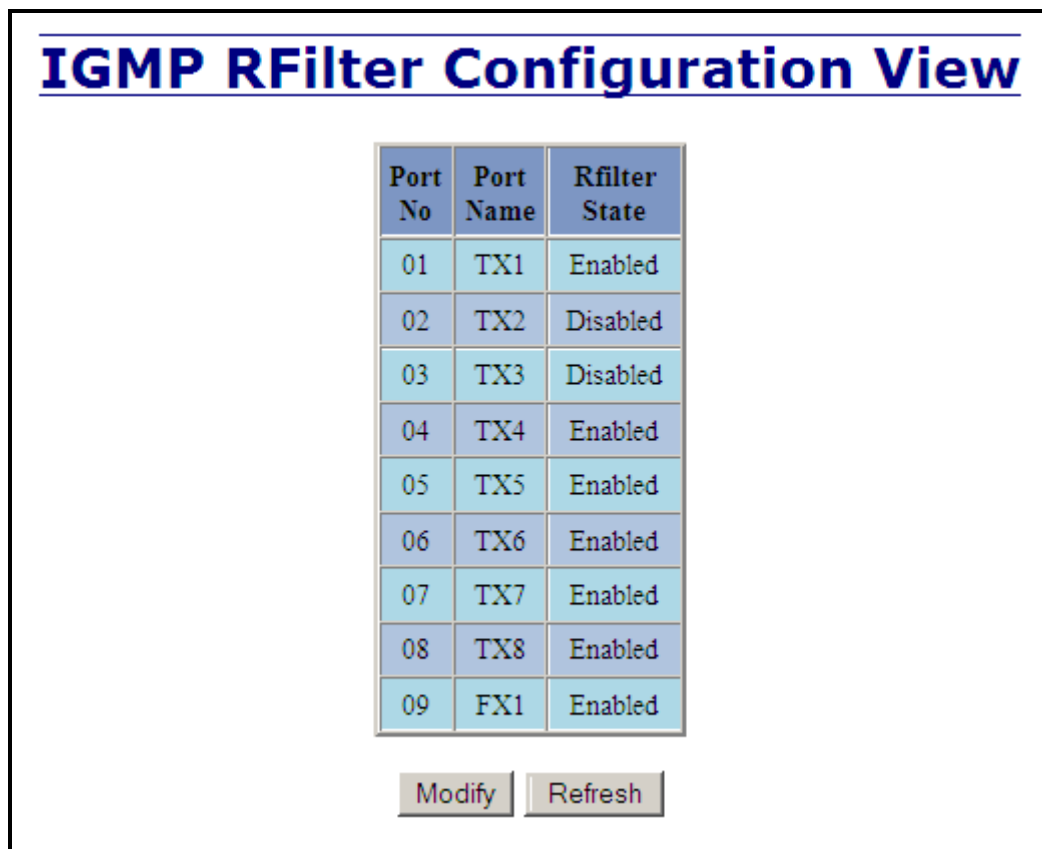
The 'rfilter' (**Router Multicast Data Filter**) function allows you to choose whether or not DATA frames with KNOWN group multicast addresses are sent to the 'router' ports (links to other switches). Control packets (Join, Leave) will be sent to the router(s) regardless of this setting. "KNOWN" is known 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 Configuration View**

Port No	Port Name	Rfilter State
01	TX1	Enabled
02	TX2	Disabled
03	TX3	Disabled
04	TX4	Enabled
05	TX5	Enabled
06	TX6	Enabled
07	TX7	Enabled
08	TX8	Enabled
09	FX1	Enabled

Modify Refresh

## IGMP – RFilter, Continued...

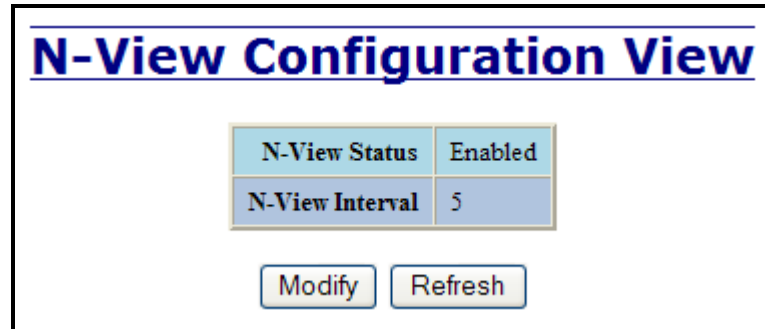
Modifying rfilter port settings:

### IGMP RFilter Configuration

Port No	Port Name	Rfilter Enabled?
01	TX1	<input checked="" type="checkbox"/>
02	TX2	<input type="checkbox"/>
03	TX3	<input type="checkbox"/>
04	TX4	<input checked="" type="checkbox"/>
05	TX5	<input checked="" type="checkbox"/>
06	TX6	<input checked="" type="checkbox"/>
07	TX7	<input checked="" type="checkbox"/>
08	TX8	<input checked="" type="checkbox"/>
09	FX1	<input checked="" type="checkbox"/>

## N-View – Configuration

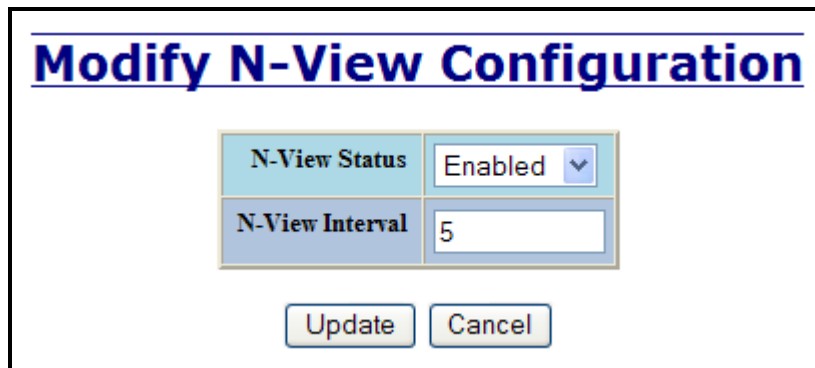
The Configuration tab under the N-View category will display two basic variables for N-View, the status and the interval between packets.



The screenshot shows a web interface titled "N-View Configuration View". It features a table with two rows: "N-View Status" with the value "Enabled" and "N-View Interval" with the value "5". Below the table are two buttons: "Modify" and "Refresh".

N-View Configuration View	
N-View Status	Enabled
N-View Interval	5

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.



The screenshot shows a web interface titled "Modify N-View Configuration". It features a table with two rows: "N-View Status" with a dropdown menu showing "Enabled" and "N-View Interval" with a text input field containing "5". Below the table are two buttons: "Update" and "Cancel".

Modify N-View Configuration	
N-View Status	Enabled ▾
N-View Interval	5

## N-View – Ports

The Ports tab under the N-View category will display a list of all the configured ports on the 709FX unit along with the ports transmitting multicast packets and MIB stats respectively.

<b>N-View Ports View</b>		
Port Name	Multicast On Port?	Send MIB Stats?
TX1	YES	YES
TX2	NO	YES
TX3	YES	NO
TX4	YES	YES
TX5	YES	YES
TX6	YES	YES
TX7	YES	YES
TX8	YES	YES
FX1	YES	YES



## N-View – Ports, Continued...

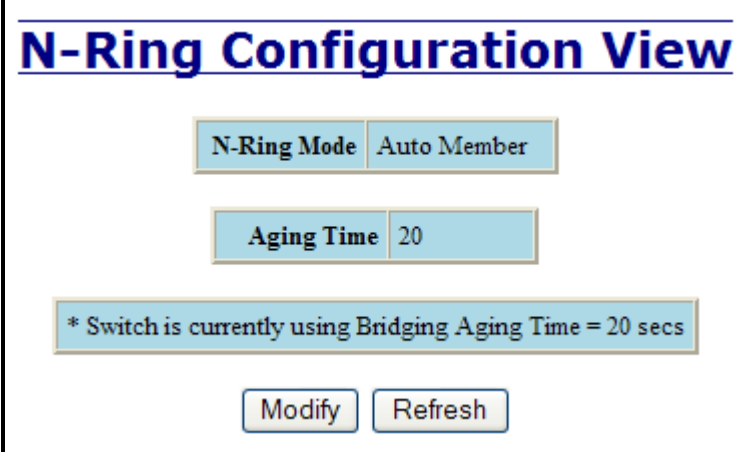
Following the Modify button on the above example, the administrator can modify these two variables to enable or disable multicast out of the port and if MIB stats are sent out for those ports.

### Modify N-View Ports

Port Name	Multicast On Port?	Send MIB Stats?
TX1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TX2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TX3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TX4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TX5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TX6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TX7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TX8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FX1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

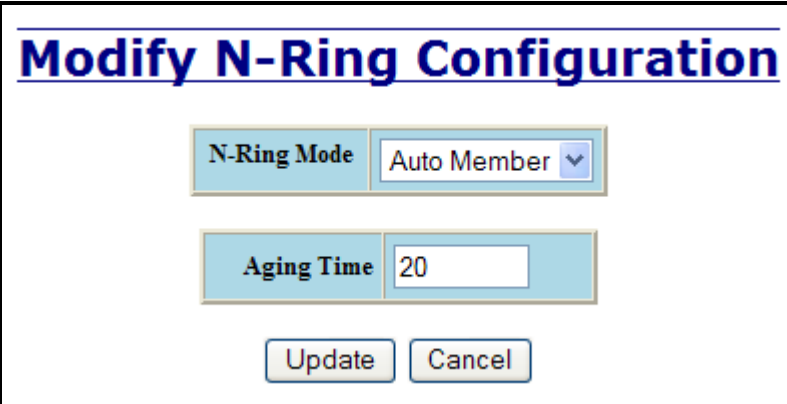
## N-Ring – Configuration

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.



The screenshot shows the 'N-Ring Configuration View' interface. At the top, the title 'N-Ring Configuration View' is displayed in a blue box. Below the title, there are two configuration fields: 'N-Ring Mode' set to 'Auto Member' and 'Aging Time' set to '20'. A status message below these fields reads '\* Switch is currently using Bridging Aging Time = 20 secs'. At the bottom of the interface, there are two buttons: 'Modify' and 'Refresh'.

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 screenshot shows the 'Modify N-Ring Configuration' interface. At the top, the title 'Modify N-Ring Configuration' is displayed in a blue box. Below the title, there are two configuration fields: 'N-Ring Mode' set to 'Auto Member' with a dropdown arrow, and 'Aging Time' set to '20' in a text input field. At the bottom of the interface, there are two buttons: 'Update' and 'Cancel'.

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 709FX 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:

**Modify N-Ring Configuration**

N-Ring Mode	Auto Member ▼
	Disabled
	Auto Member
	Manager
Aging Time	

Update Cancel

If N-Ring Mode is “Manager”, then a pull-down allows selection of available ports TX1/TX2, or TX7/TX8 (on 709FX) as N-Ring ports.

**Modify N-Ring Configuration**

N-Ring Mode	Manager ▼
Aging Time	20
N-Ring Ports	TX1 / TX2 ▼
	TX1 / TX2
	TX7 / TX8
VLAN ID	
Tagging	Tagged ▼

Update Cancel

## 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.

**Modify N-Ring Configuration**

N-Ring Mode	Manager
Aging Time	20
N-Ring Ports	TX1 / TX2
VLAN ID	3333
Tagging	Tagged

Update Cancel

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.

The screenshot shows a web interface titled "N-Ring Advanced Configuration View". It features two data fields: "N-Ring Mode" with a value of "Auto Member" and "Keep-Alive Timeout (Secs)" with a value of "31". Below these fields are two buttons: "Modify" and "Refresh".

The screenshot shows a web interface titled "Modify N-Ring Advanced Configuration". It features two data fields: "N-Ring Mode" with a value of "Auto Member" and "Keep-Alive Timeout (Secs)" with a value of "31" in a text input field. Below these fields are two buttons: "Update" and "Cancel".

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

## 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:

### N-Ring Status View

N-Ring Mode	Auto Member
-------------	-------------

Switch is in Auto Member Detection Mode

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

### N-Ring Status View

N-Ring Mode	Auto Member
-------------	-------------

Switch is an N-Ring Member

N-Ring Manager Address	
00:07:af:ff:af:00	

Active N-Ring Ports	
TX1	TX2

\* Switch is currently using N-Ring Aging Time = 20 secs



## 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  secs.        

---

7 Active Members Detected In Current N-Ring (7 reporting)

Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	<a href="#">00:07:af:fd:61:40</a>	192.168.1.229	255.255.255.0	N-TRON Switch fd:61:40	TX2 TX1
1	<a href="#">00:07:af:fb:9d:d0</a>	192.168.2.220	255.255.252.0	N-TRON Switch fb:9d:d0	T2 T1
2	<a href="#">00:07:af:fb:a3:90</a>	192.168.2.222	255.255.252.0	N-TRON Switch fb:a3:90	T2 T1
3	<a href="#">00:07:af:fb:a2:90</a>	192.168.2.227	255.255.252.0	N-TRON Switch fb:a2:90	T2 T1
4	<a href="#">00:07:af:fb:a2:e0</a>	192.168.2.202	255.255.252.0	N-TRON Switch fb:a2:e0	T2 T1
5	<a href="#">00:07:af:fb:a2:70</a>	192.168.2.203	255.255.252.0	N-TRON Switch fb:a2:70	T2 T1
6	<a href="#">00:07:af:fb:a2:40</a>	192.168.2.229	255.255.252.0	N-TRON Switch fb:a2:40	T2 T1
7	<a href="#">00:07:af:fd:61:60</a>	192.168.1.231	255.255.252.0	N-TRON Switch fd:61:60	TX1 TX2

## 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 Fault**

### N-Ring Status View

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

Refresh every  secs.

---

The total number of Active N-Ring Members is unknown. (7 reporting)

Switch order may be incorrect and all switches may not be shown.

Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	<a href="#">00:07:affd:61:40</a>	192.168.1.229	255.255.255.0	N-TRON Switch fd:61:40	TX2 TX1
1	<a href="#">00:07:affb:9d:d0</a>	192.168.2.220	255.255.252.0	N-TRON Switch fb:9d:d0	T2 T1
2	<a href="#">00:07:affb:a3:90</a>	192.168.2.222	255.255.252.0	N-TRON Switch fb:a3:90	T2 T1
3	<a href="#">00:07:affb:a2:90</a>	192.168.2.227	255.255.252.0	N-TRON Switch fb:a2:90	T2 T1
4	<a href="#">00:07:affb:a2:e0</a>	192.168.2.202	255.255.252.0	N-TRON Switch fb:a2:e0	T2 <b>T1</b>
~~~~~ Ring Broken ~~~~~					
5	<a href="#">00:07:affb:a2:70</a>	192.168.2.203	255.255.252.0	N-TRON Switch fb:a2:70	<b>T2</b> T1
6	<a href="#">00:07:affb:a2:40</a>	192.168.2.229	255.255.252.0	N-TRON Switch fb:a2:40	T2 T1
7	<a href="#">00:07:affd:61:60</a>	192.168.1.231	255.255.252.0	N-TRON Switch fd:61:60	TX1 TX2

## 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 (TX2, TX8) is not receiving self health frames all the way around the N-Ring, though the other (low TX1, TX7) N-Ring port is:

**N-Ring Partial Fault (TX2 is not receiving self health from TX1)**

### N-Ring Status View

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

Refresh every  secs.        

---

1 Active Members Detected In Current N-Ring (1 reporting)

Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	<a href="#">00:07:af:ff:af:00</a>	192.168.1.238	255.255.255.0	N-Tron Switch	TX2 TX1
1	<a href="#">00:07:af:ff:ae:e0</a>	192.168.1.228	255.255.255.0	N-Tron Switch	TX1 TX2

The screenshot below shows N-Ring Manager Status when a ‘Lower’ N-Ring Port (TX1, TX7) is not receiving self health frames all the way around the N-Ring, though the other (high TX2 , TX8) N-Ring port is:

N-Ring Partial Fault (TX1 is not receiving self health from TX2)

## N-Ring Status View

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

Refresh every  secs.

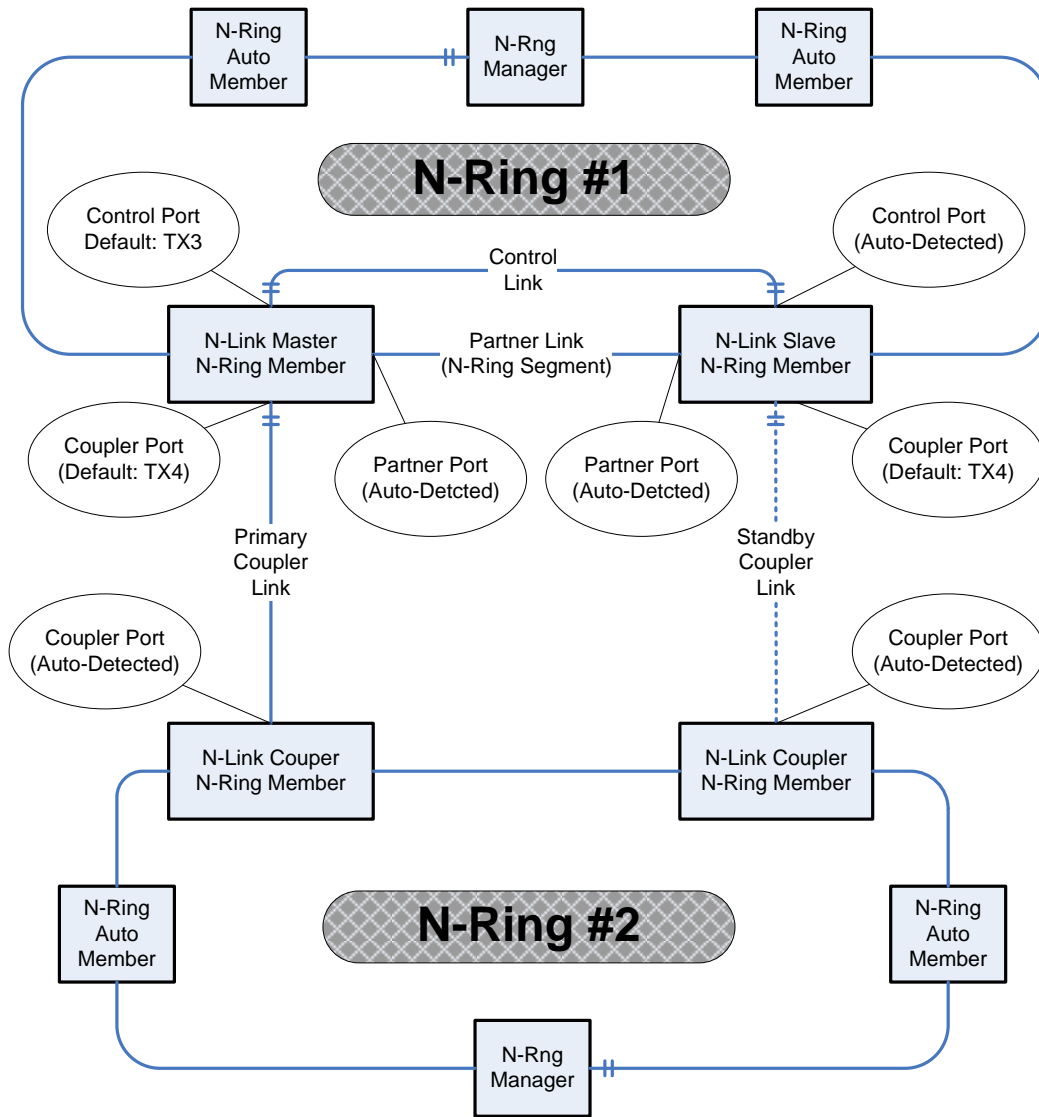
1 Active Members Detected In Current N-Ring (1 reporting)

Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	<a href="#">00:07:aff:af:00</a>	192.168.1.238	255.255.255.0	N-Tron Switch	TX2 TX1
1	<a href="#">00:07:aff:ae:e0</a>	192.168.1.228	255.255.255.0	N-Tron Switch	TX1 TX2

# 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.

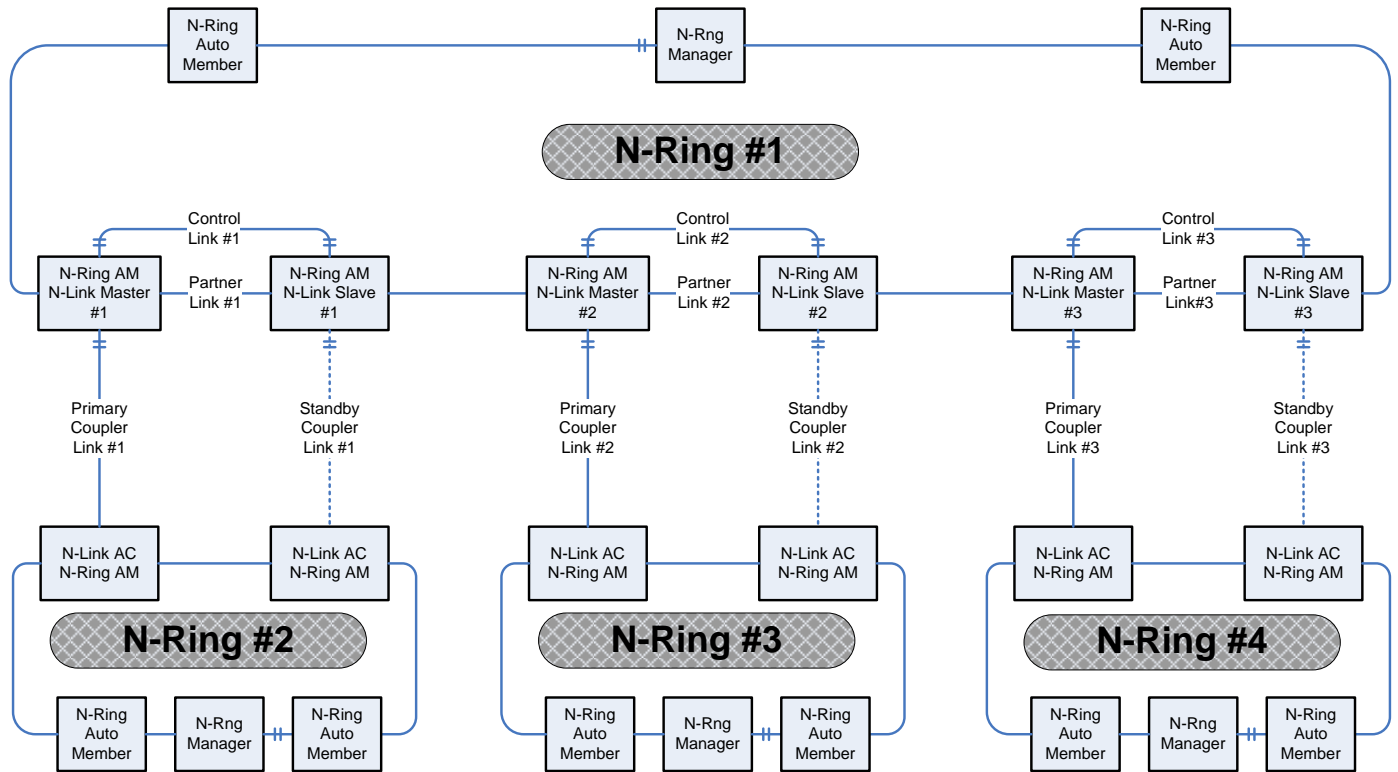
## Standard N-Link Configuration (Example):



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

## N-Link – Configuration, Continued...

### 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.

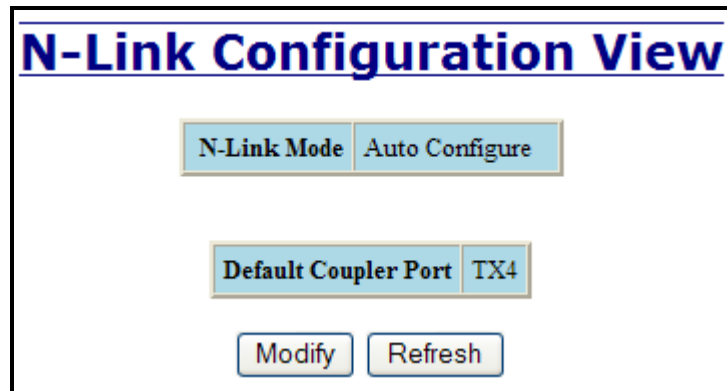
### Configuration Steps to redundantly couple 2 N-Ring networks:

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.

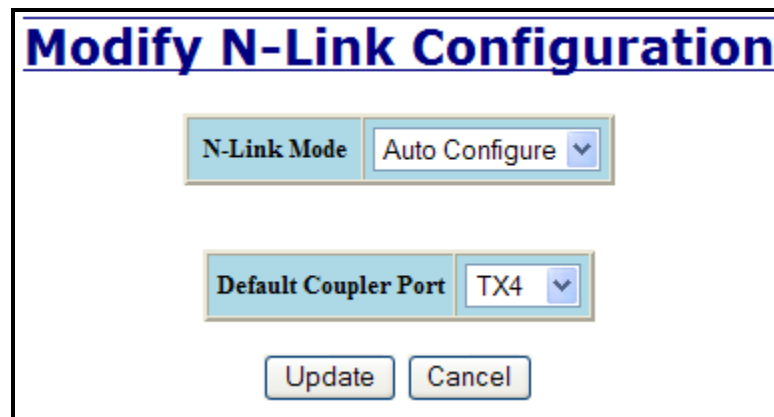
## N-Link – Configuration, Continued...

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.



The screenshot shows the 'N-Link Configuration View' page. It features a title bar with the text 'N-Link Configuration View' in blue. Below the title bar, there are two main configuration sections. The first section is labeled 'N-Link Mode' and has a dropdown menu currently set to 'Auto Configure'. The second section is labeled 'Default Coupler Port' and has a dropdown menu currently set to 'TX4'. At the bottom of the page, there are two buttons: 'Modify' and 'Refresh'.

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



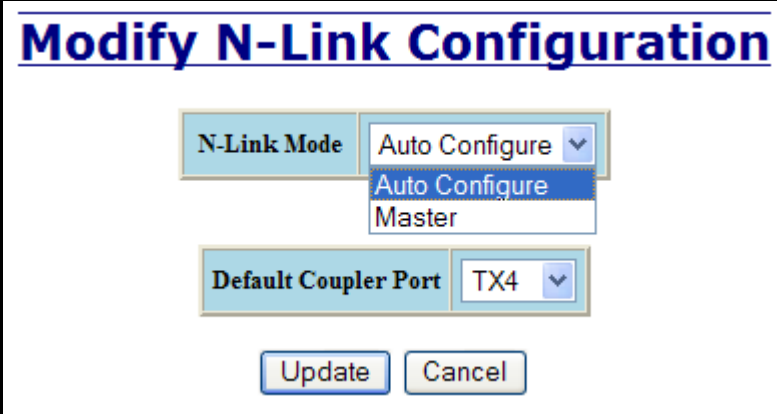
The screenshot shows the 'Modify N-Link Configuration' page. It features a title bar with the text 'Modify N-Link Configuration' in blue. Below the title bar, there are two main configuration sections. The first section is labeled 'N-Link Mode' and has a dropdown menu currently set to 'Auto Configure'. The second section is labeled 'Default Coupler Port' and has a dropdown menu currently set to 'TX4'. At the bottom of the page, there are two buttons: 'Update' and 'Cancel'.

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:



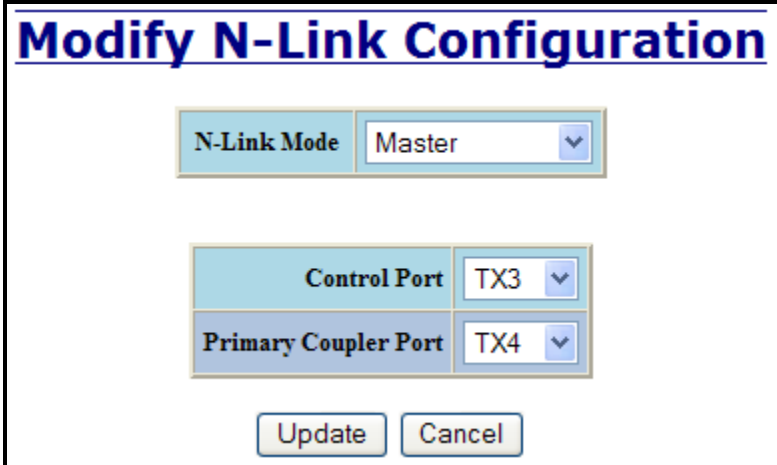
**Modify N-Link Configuration**

N-Link Mode: Auto Configure (dropdown menu open showing Auto Configure and Master)

Default Coupler Port: TX4 (dropdown menu)

Update Cancel

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



**Modify N-Link Configuration**

N-Link Mode: Master (dropdown menu)

Control Port: TX3 (dropdown menu)

Primary Coupler Port: TX4 (dropdown menu)

Update Cancel

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.

<b>State:</b>	Current N-Link mode of switch.
<b>Control Port:</b>	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.
<b>Partner Port:</b>	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.
<b>Coupler Port:</b>	The port being used to establish a redundant path for ethernet data transmission.
<b>Coupler Port State:</b>	Blocking, Forwarding.
<b>Status:</b>	No errors will show "OK", otherwise a description of the Faults detected.

### N-Link Partner Information

<b>State:</b>	Current N-Link mode of switch.
<b>MAC:</b>	The MAC Address of the N-Link Partner switch.
<b>Coupler Port State:</b>	Blocking, Forwarding.
<b>Status:</b>	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.

<b>N-Link State:</b>	Current N-Link mode of switch.
<b>Coupler Port:</b>	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:

<b>N-Link Status View</b>	
<b>N-Link State</b>	Auto Configure
<b>Coupler Port</b>	(None)

## N-Link – Status, Continued...

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

<b>N-Link Status View</b>	
N-Link State	Auto Configure
Coupler Port	TX4

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

<b>N-Link Status View</b>	
State	Master
Control Port	TX3
Partner Port	TX1
Coupler Port	TX4
Coupler Port State	Forwarding
Status	OK

<b>N-Link Partner Information</b>	
State	Slave
MAC	00:07:affe:af:c0
Coupler Port State	Blocking
Status	OK

## N-Link – Status, Continued...

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

<b>N-Link Status View</b>	
State	Slave
Control Port	TX3
Partner Port	TX2
Coupler Port	TX4
Coupler Port State	Blocking
Status	OK

<b>N-Link Partner Information</b>	
State	Master
MAC	00:07:affe:c4:40
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:

<b>N-Link Status View</b>		<b>N-Link Status View</b>	
State	Master	State	Slave
Control Port	TX3	Control Port	TX3
Partner Port	TX1	Partner Port	TX2
Coupler Port	TX4	Coupler Port	TX4
Coupler Port State	Blocking	Coupler Port State	Forwarding
Status	Redundancy lost. Primary Coupler failure.	Status	OK

<b>N-Link Partner Information</b>		<b>N-Link Partner Information</b>	
State	Slave	State	Master
MAC	00:07:affe:af:c0	MAC	00:07:affe:c4:40
Coupler Port State	Forwarding	Coupler Port State	Blocking
Status	OK	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:

<b>N-Link Status View</b>		<b>N-Link Status View</b>	
State	Master	State	Slave
Control Port	TX3	Control Port	TX3
Partner Port	TX1	Partner Port	TX2
Coupler Port	TX4	Coupler Port	TX4
Coupler Port State	Forwarding	Coupler Port State	Blocking
Status	OK	Status	Redundancy lost. Standby Coupler failure.

<b>N-Link Partner Information</b>		<b>N-Link Partner Information</b>	
State	Slave	State	Master
MAC	00:07:affe:afc0	MAC	00:07:affe:c4:40
Coupler Port State	Blocking	Coupler Port State	Forwarding
Status	Redundancy lost. Standby Coupler failure.	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	TX3
Partner Port	TX1
Coupler Port	TX4
Coupler Port State	Forwarding
Status	Redundancy lost. Control failure.

## N-Link Status View

State	Slave
Control Port	TX3
Partner Port	TX2
Coupler Port	TX4
Coupler Port State	Blocking
Status	Redundancy lost. Control failure.

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

N-Link Partner Information	
State	Unknown
MAC	00:07:affe:c4:40
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:

<b>N-Link Status View</b>	
<b>State</b>	Master
<b>Control Port</b>	TX3
<b>Partner Port</b>	(None)
<b>Coupler Port</b>	TX4
<b>Coupler Port State</b>	Forwarding
<b>Status</b>	Partner port is not known.

<b>N-Link Partner Information</b>	
<b>State</b>	Slave
<b>MAC</b>	00:07:aff9c:e0
<b>Coupler Port State</b>	Blocking
<b>Status</b>	Partner port is not known.

## N-Link Status View

State	Slave
Control Port	TX3
Partner Port	(None)
Coupler Port	TX4
Coupler Port State	Blocking
Status	Partner port is not known.

N-Link Partner Information	
State	Master
MAC	00:07:aff:38:a0
Coupler Port State	Forwarding
Status	Partner port is not known.



## CIP – Configuration

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

**Cip Status:**

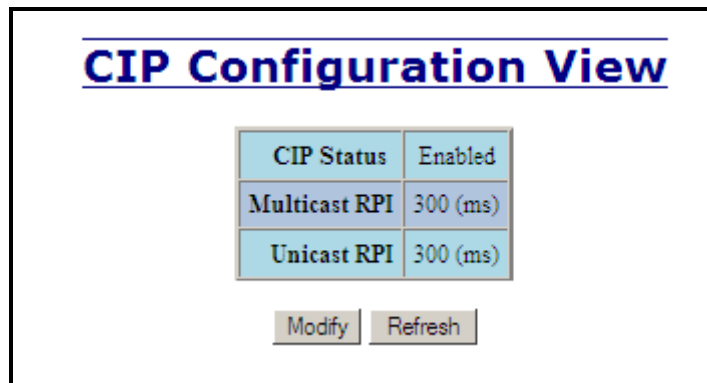
Enables or Disables CIP on the Switch. Default: Enabled.

**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.

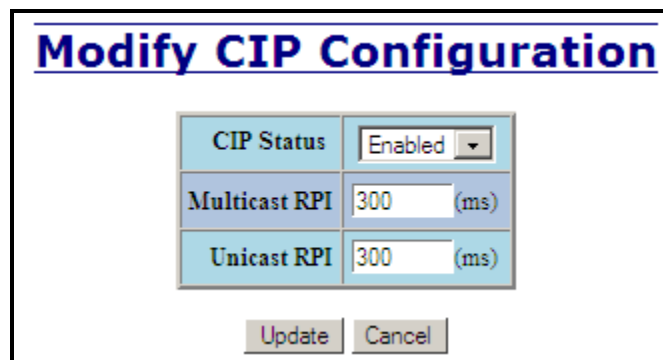


The screenshot shows a window titled "CIP Configuration View". It contains a table with the following data:

CIP Status	Enabled
Multicast RPI	300 (ms)
Unicast RPI	300 (ms)

Below the table are two buttons: "Modify" and "Refresh".

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



The screenshot shows a window titled "Modify CIP Configuration". It contains a form with the following fields:

CIP Status	Enabled
Multicast RPI	300 (ms)
Unicast RPI	300 (ms)

Below the form are two buttons: "Update" and "Cancel".

## 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:

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

### Connection Information:

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

## CIP Status View

CIP Status	Enabled
------------	---------

Identity Information	
Product Name	N-TRON 709FX
Vendor	1006 (N-TRON)
Device Type	0x0C (hex) (Communications Adapter)
Major Revision	1
Minor Revision	3
Serial Number	0xAFF9CA20 (hex)

Connection Information	
Number of Multicast Connections	0
Number of Unicast Connections	0

Refresh

## 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 709FX Series 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 can also download an Image or Boot Image file to the switch via TFTP, 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.

<b>TFTP - Firmware/Config</b>	
Server IP Address	<input type="text" value="192.168.1.12"/>
File Name	<input type="text" value="Image"/>
Transfer Type	<input type="text" value="Download image from server"/>
<input type="button" value="Action"/> <input type="button" value="Cancel"/>	

<b>TFTP - Firmware/Config</b>	
Server IP Address	<input type="text" value="192.168.1.122"/>
File Name	<input type="text" value="700Series.Image"/>
Transfer Type	<input type="text" value="Download image from server"/>
<ul style="list-style-type: none"><li>Upload saved config to server</li><li>Download config from server</li><li>Download XML config from server</li><li><b>Download image from server</b></li><li>Download boot image from server</li></ul>	

## **Download Image**

Transferring "Image" from server (192.168.1.12).

Image transferred successfully.

**Resetting switch (192.168.1.228)**

**Please wait...**

## Firmware/Config – TFTP, Continued

For ‘uploading a saved config to server’ or ‘downloading a config from server’, there are checkbox choices that can be made as below. The most common example is to keep the pre-existing IP, Gateway, and Subnet Mask when otherwisely downloading a config from the server.

### TFTP - Firmware/Config

<b>Server IP Address</b>	<input type="text" value="192.168.2.118"/>
<b>File Name</b>	<input type="text" value="700Series.Config"/>
<b>Transfer Type</b>	<input type="text" value="Upload saved config to server"/> ▼

Configuration Items To Upload To Server

- Main Configuration Settings
- SNMP Configuration Settings
- DHCP Server Configuration Settings
- MAC Security Configuration Settings
- Manually Configured Only

### TFTP - Firmware/Config

<b>Server IP Address</b>	<input type="text" value="192.168.2.118"/>
<b>File Name</b>	<input type="text" value="700Series.Config"/>
<b>Transfer Type</b>	<input type="text" value="Download config from server"/> ▾

Configuration Items To Download From Server

- Main Configuration Settings
  - Keep Current IP, Gateway and Subnet Mask
- SNMP Configuration Settings
- DHCP Server Configuration Settings
- MAC Security Configuration Settings
  - Manually Configured Only

## 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 directly with the links provided for more information.

192.168.1.228 N-TRON Switch fd:61:40 - Windows Internet Explorer

http://192.168.1.228/main.ssi

File Edit View Favorites Tools Help


192.168.1.228 N-TRON Switch fd:61:40



CAREERS | TRADESHOWS | CONTACT

SEARCH

HOME ABOUT US PRODUCTS SUPPORT & SERVICES CASE STUDIES NEWS CONTACT



## Support & Services

QUICKLINKS

Effective January 1, 2008, unless otherwise specified, all N-TRON products carry a 3 year limited warranty that includes cross-shipment of a replacement product to minimize downtime. Products are available directly from N-TRON, our network of Systems Integrators, Value Added Resellers, and our Catalog and Internet Partners.

Display All Lists | Hide All Lists

- Firmware Downloads
- SNMP MIBs
- Forms
- Software

For additional information, please contact us.

WHERE TO BUY

REQUEST A CATALOG

CERTIFIED ALLIANCE PARTNERS

ONLINE STORE

PRESS RELEASES <|> N-TRON Ethernet Switches and Media Converters Receive Globally Recognized D... read

CONTACT | FEEDBACK | SITEMAP | TERMS & CONDITIONS

© 2010 N-TRON and the N-TRON logo are trademarks of N-TRON Corp. Product names mentioned herein are for identification purposes only and may be trademarks and/or registered trademarks of their respective company.

- Administration
- DHCP
- LLDP
- Ports
- Statistics
- VLAN
- Bridging
- RSTP
- IGMP
- N-View
- N-Ring
- N-Link
- CIP
- Firmware/Config
- Support
  - Web Site
  - E-mail
  - BPCL
  - User
- Management
  - Logical View
  - Home
  - Config
  - Help
  - Logout

Copyright © 2008-2010  
N-TRON Corp.  
All rights reserved.  
http://www.n-tron.com

Logged in as: admin



## Rate Limiting – Broadcast Rate Limit Configuration

The Rate Limiting/Broadcast link will display all the ports that are installed in the 709FX Series unit and will list the Broadcast Pass Rate Percentage for each port. Broadcast Pass Rate Percentage defaults to 3% on 10/100Mbs ports. A Modify button is provided to change these fields.

### Broadcast Packet Count Limit Configuration View

Port Name	BPCL [%]
TX1	3
TX2	3
TX3	3
TX4	3
TX5	3
TX6	3
TX7	3
TX8	3
FX1	3

Following the Modify button on the above example, the administrator can modify the Broadcast Pass Rate Percentage for each and every port.

### Broadcast Packet Count Limit Configuration

Port Name	TX1
BPCL Percentage	

- TX1
- TX2
- TX3
- TX4
- TX5
- TX6
- TX7
- TX8
- FX1
- All

## Rate Limiting – Multicast Rate Limit Configuration

The Rate Limiting/Multicast link will display all the ports that are installed in the 709FX Series unit and will list the Multicast Pass Rate Percentage for each port. Multicast Pass Rate Percentage defaults to 100% on all ports. A Modify button is provided to change these fields.

Note: Unicast packets with destinations not in the ARL table will also be rate limited rather than all being Flooded.

<b>Multicast Rate Limit View</b>	
<b>Port Name</b>	<b>Multicast Pass Rate [%]</b>
TX1	100
TX2	100
TX3	100
TX4	100
TX5	100
TX6	100
TX7	100
TX8	100
FX1	100

Following the Modify button on the above example, the administrator can modify the Multicast Pass Rate Percentage for each and every port.

## Multicast Rate Limit Configuration

Port Name	TX1
Multicast Pass Rate [%]	

Update    Cancel

- TX1
- TX2
- TX3
- TX4
- TX5
- TX6
- TX7
- TX8
- FX1
- All

## 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.

**Authorized Users**

No.	User Name	Access Permission
<a href="#">01</a>	admin	admin

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).

**Add New User**

User Name	<input type="text" value="user"/>
Password	<input type="password" value="•••••"/>
Access Permission	<input type="text" value="User"/> ▼

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

**Authorized Users**

No.	User Name	Access Permission
<a href="#">01</a>	admin	admin
<a href="#">02</a>	user	user

## User Management – Removing Users

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

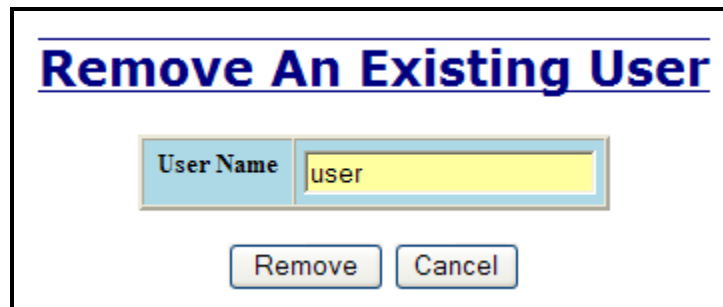


**Authorized Users**

No.	User Name	Access Permission
<a href="#">01</a>	admin	admin
<a href="#">02</a>	user	user

Add Remove Refresh

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.



**Remove An Existing User**

User Name

Remove Cancel

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



**Authorized Users**

No.	User Name	Access Permission
<a href="#">01</a>	admin	admin

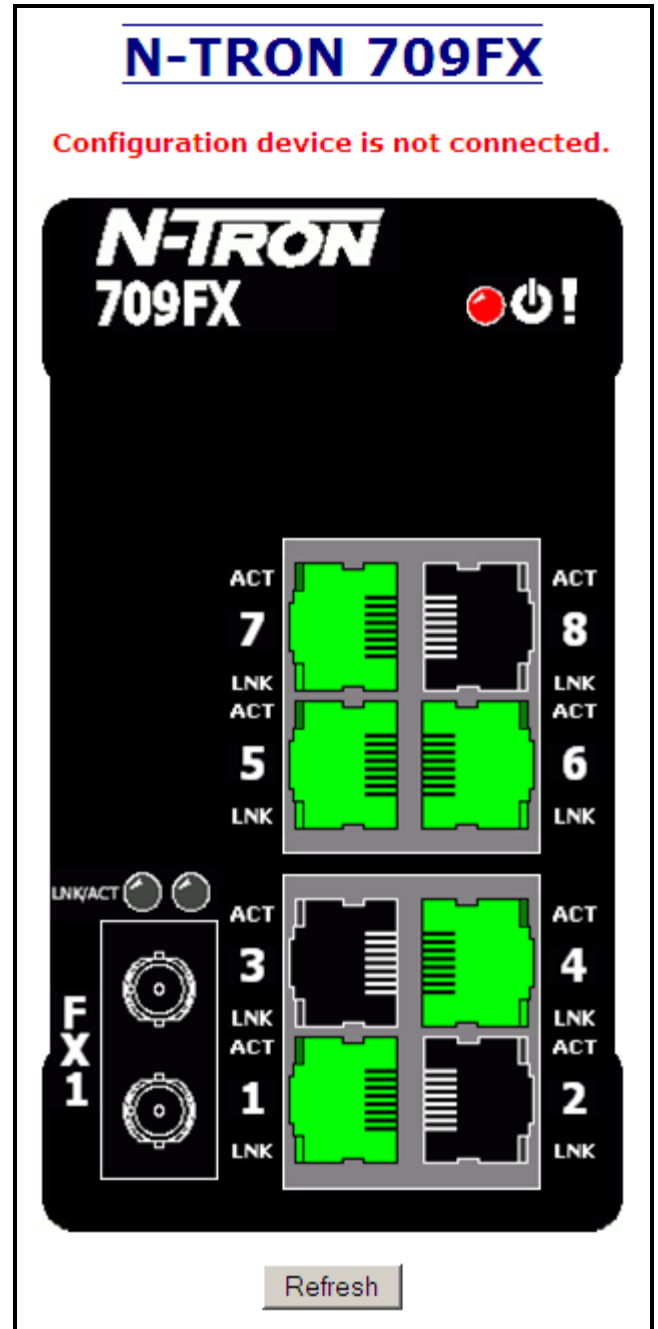
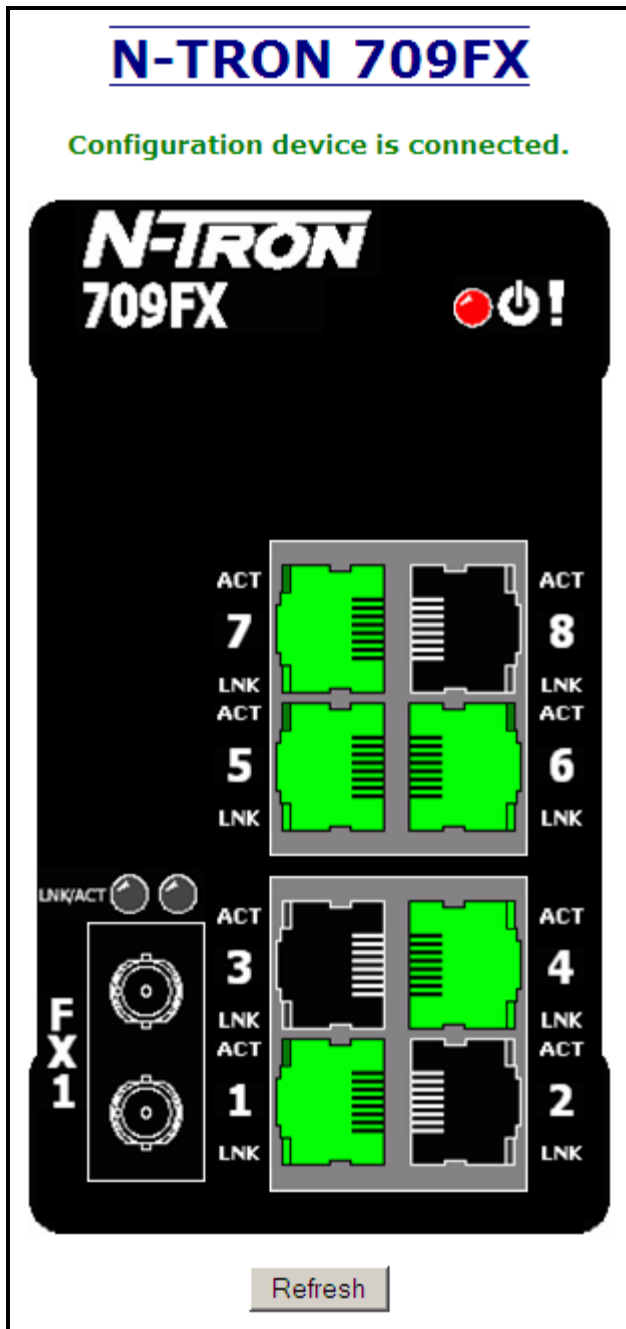
Add Remove Refresh

**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.*



## LogicalView

The 709FX Web Management offers a logical view of the switch. Here a user or administrator can see a graphical depiction of the 709FX series switch. Ports that are linked will appear in green, while ports that are not linked will appear in black. The example below shows a 709FX with ports 1, 4, 5, 6, and 7 linked. The other ports are currently in the down state (not being used). Also, the logical view reveals whether the configuration device (SD card) is installed or not.



## 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.

The “Reset” button will discard all unsaved changes, reset the switch and load the most recently saved configuration settings.

The “Factory” button will reload N-Tron’s factory default configuration settings. Doing so will reconfigure the 709FX Series switch to factory defaults. In many cases it is desirable to restore factory defaults but retain certain settings. Checkboxes are provided to select the desired behavior. Note that if no Configuration Device is present, that is presented.

### Configuration Save Or Reset

**Configuration device is not connected.**

Click "Save" button to save changes to the configuration.

---

Click "Reset" button to reset the switch and load the most recently saved configuration.

---

Click "Factory" button to reset switch to factory defaults.

- Keep current IP address, subnet mask, and gateway.
- Keep current user names and passwords.
- Keep currently stored SNMP settings.
- Keep currently stored DHCP Server settings.
- Keep currently stored MAC Security settings.



If a Configuration Device is present, that is presented:

## Configuration Save Or Reset

**Configuration device is connected.**

Click "Save" button to save changes to the configuration.

---

Click "Reset" button to reset the switch and load the most recently saved configuration.

---

Click "Factory" button to reset switch to factory defaults.

- Keep current IP address, subnet mask, and gateway.
- Keep current user names and passwords.
- Keep currently stored SNMP settings.
- Keep currently stored DHCP Server settings.
- Keep currently stored MAC Security settings.

# Help – Overview

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

## Overview

This Help provides information on configuring and monitoring the manageable parameters of the device. The major software functions provided by N-TRON WebConsole are:

**Services to user's requests:** This function of the software is responsible for servicing the user requests remotely by using HTTP protocol.

**Graphical Representation:** This function of the software shows the graphical representation of the parameters of each port on the device.

### Controls in Web Console

**Button Field:** A field that the user can click to perform operations.

**Radio Button:** This field provides a list of choices.

**Label Field:** A field that displays strings. This is a read-only field.

**List Field:** This field provides a list with scrolling capability (a table).

**Text Field:** A field to enter keyboard input.

### Buttons in Web Console

**Modify:** Click to change the existing configuration. This will lead to the modification of configuration parameters for the respective feature.

**Refresh:** Click to get the latest configuration from the device.

**Update:** Click to apply the new configuration changes.

**Cancel:** Click to skip the configuration changes and return to the previous page.

**Done:** Return to the previous page.

Copyright © 2008-2011  
N-TRON Corp.  
All rights reserved.  
<http://www.n-tron.com>

Logged in as: **admin**

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 709FX offers.

# Help – Administration

The screenshot shows the N-TRON web management interface. On the left is a navigation menu with categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, TFTP, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area is titled 'Administration' and contains a table of links and a detailed configuration table.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

**Administration**

Administration group is divided into three categories:  
1. System 2. SNMP 3. Fault

**System**

<b>IP Configuration:</b>	Determines the method used to obtain an IP address, Subnet Mask, and Gateway address. When Static is selected, the statically configured values are used. When DHCP is selected, DHCP protocols are used to obtain these values.
<b>Client ID:</b>	This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. The identifier may be the MAC address, switch name, or entered as a text string or hex characters. (Only shown in DHCP Mode)
<b>IP Address:</b>	Contains the current IP Address of the device.
<b>Subnet Mask:</b>	Contains the current Subnet Mask of the device.
<b>Gateway:</b>	Contains the current Gateway of the device.
<b>Fallback IP Address:</b>	Contains the configured Fallback IP Address of the device. (Only shown in DHCP Mode)
<b>Fallback Subnet Mask:</b>	Contains the configured Fallback Subnet Mask of the device. (Only shown in DHCP Mode)
<b>Fallback Gateway:</b>	Contains the configured Fallback Gateway of the device. (Only shown in DHCP Mode)
<b>MAC Address:</b>	MAC Address of the device.
<b>System Up Time:</b>	This parameter represents the total time elapsed since the switch was turned ON or RESET.
<b>Name:</b>	Contains the name assigned to the device, which allows alphanumeric and special characters '#' '!' '!' and '\$' only. When IP Configuration is DHCP then this is used

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

The screenshot shows the N-TRON web management interface. On the left is a navigation menu with categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Support, Rate Limiting, User Management, Logical View, Home, Config, Help, and Logout. The main content area is titled "DHCP - Dynamic Host Configuration Protocol". It states that the DHCP group is divided into two categories: 1. Server and 2. Relay & Local IP. Below this is a section for "Server - Setup Profiles" with a table of configuration options:

<b>Server Enabled:</b>	Indicates whether the DHCP server is active. The default is Disabled.
<b>Allow Broadcast:</b>	Indicates whether the DHCP server will process broadcast messages. Typically, client requests are broadcast and relay agent requests are unicast. When enabled, the server will respond to broadcast requests. When disabled, the server will ignore broadcast requests. The default is Enabled.
<b>Delay Broadcast (Ms):</b>	The amount of time (in milliseconds) that the DHCP server will delay the processing of a broadcast message. This setting is used when clients and relay agents are on the same subnet and/or VLAN. A delay provides the opportunity for relay agent requests to be honored before client requests. This setting only applies when Allow Broadcast is Enabled. The range is 0-2500 and the default is 500.
<b>Server ID:</b>	Descriptive name of the DHCP server. The name must be unique. The default is the switch name.

Below this is a section for "Network Profiles" with a paragraph explaining that a network profile contains vital network configuration options for potential clients. It also includes a table of configuration options:

<b>Network Profile Name:</b>	Descriptive name of the network profile. The name must be unique and is required.
<b>Address Pool Start:</b>	Starting IP address of a pool of addresses for the network profile. IP addresses within the address pool can be used in any combination of dynamic and static IP assignments. There can only be one address pool per subnet; therefore, it is recommended to use the full range of addresses. For example, an address pool

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The address bar shows the URL <http://192.168.2.216/main.ssi>. The left sidebar contains a navigation menu with the following items: Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, TFTP, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays the LLDP help page.

**LLDP - Link Layer Discovery Protocol**

LLDP is divided into four categories:  
 1. Configuration 2. Ports 3. Status 4. Statistics

**Configuration**

<b>Mode:</b>	Enables or disables LLDP on the switch. The default is Disabled.
<b>Transmit Interval:</b>	Specifies the interval at which LLDP frames are transmitted. The default is 30 seconds.
<b>Transmit Hold Multiplier:</b>	Specifies a multiplier on the Transmit Interval when calculating a Time-to-Live value. The default is 4.
<b>Re-Initialization Delay:</b>	Specifies the minimum time an LLDP port will wait before re-initializing after its setting has changed from disabled to Tx-Only or Tx/Rx. This prevents excessive notifications when LLDP Port settings are toggled. The default is 2 seconds.
<b>Notification Interval:</b>	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 subsequent notification will not be sent until the interval expires. The default is 5 seconds.

**Ports**

<b>Port Name:</b>	The descriptive name of the port.
<b>Transmit:</b>	Enables or disables LLDP transmission on the switch.
<b>Receive:</b>	Enables or disables receipt of LLDP frames from neighbor switches.
<b>Allow Management Data:</b>	Allows the transmission of management type information. Example: IP address of switch.
<b>Allow Notification:</b>	Allows a notification to be transmitted when local or remote data changes.

**Status**

The Status View shows the results of LLDP discovery. The LLDP Ethernet frames received from neighboring ports are composed of collections of data units called TLVs. Each TLV contains a defined type of information

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser window. The address bar shows the URL <http://192.168.2.216/main.ssi>. The page features a navigation menu on the left with categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Support, Rate Limiting, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays a table of links and a detailed 'Ports' help page.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

## Ports

Ports group is divided into five categories:  
 1. Configuration 2. MAC Security 3. Mirroring 4. Trunking 5. QOS

### Configuration

<b>Port No:</b>	The number of the port.
<b>Port Name:</b>	The descriptive name of the port.
<b>Admin Status:</b>	This configurable field displays the existing status of the port whether it is Enabled/Disabled.
<b>Link Status:</b>	Current link state.
<b>Auto Nego:</b>	This configurable field displays the current auto-negotiation state whether it is Enabled/Disabled.
<b>Port Speed:</b>	This configurable field displays the speed of each port 10/100 Mbps.
<b>Duplex Mode:</b>	This configurable field displays the existing mode of the port whether it is Full Duplex/Half Duplex.
<b>Cross Over:</b>	This configurable field displays the existing crossover mode of the port.
<b>Flow Control:</b>	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.
<b>Port State:</b>	The current status of a port. It may contain: Disabled, Discarding, Learning, Forwarding, and Blocking.
<b>PVID:</b>	This configurable field displays the existing port VLAN ID setting. This is the VLAN ID assigned to ingress untagged frames, or all ingress frames if "Replace VID with Default Port VID" is enabled. The allowable range is 1-4094.
<b>Usage Alarm Low [%]:</b>	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.

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

The screenshot shows a Mozilla Firefox browser window with the URL <http://192.168.2.216/main.ssi>. The page features the N-TRON logo and a navigation menu on the left. The main content area displays a table of links and a help section for the Statistics category.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

### Statistics

Statistics group is divided into two categories:  
1. Ports Statistics 2. Ports Utilization

#### Ports Statistics

Displays the MIB counters for the selected port, specified by the Port pull-down menu. The Clear button will reset all counters for the selected port. The Clear All Ports button will reset all counters for all ports, including the selected port.

#### Ports Utilization

Shows a bandwidth percentage graph of all the ports. The graph is scaled based on the Scale pull-down menu selection.

Copyright © 2008-2011 N-TRON Corp. All rights reserved. <http://www.n-tron.com>

Logged in as: **admin**

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The address bar shows the URL <http://192.168.2.216/main.ssi>. The page features a navigation menu on the left with categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays a table of links and a detailed help page for VLAN.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

## VLAN - Virtual Local Area Network

### Configuration

<b>Replace VID with Default Port VID:</b>	Specifies whether or not to replace the incoming VID tag with the port's designated VID.
<b>Perform Ingress Filtering:</b>	Specifies whether or not to filter out ingress frames when a VID violation is detected.
<b>Discard Non-Tagged for Ports:</b>	Specifies whether or not non-tagged ingress frames are dropped by the selected ports.
<b>Remove Ports From Default VLAN When Added To Other VLANs:</b>	Specifies whether or not to remove ports from Default VLAN when they are added to another VLAN.

### Group Configuration

<b>VLAN ID:</b>	This field displays the VLAN ID. The range should be 1-4094.
<b>VLAN Name:</b>	This configurable field displays the name of the VLAN, which accepts alphanumeric and special characters #, !, ', and ! only.
<b>Allow Management:</b>	Specifies whether or not all ports in this VLAN are management ports.
<b>Change PVID of Member Ports:</b>	Specifies whether or not the PVID of the member ports is set to this VLAN ID.
<b>Port No:</b>	The number of the port.
<b>Port Name:</b>	The descriptive name of the port.
<b>Group Member:</b>	Specifies whether or not the port is included in the group.
<b>Untag on Egress:</b>	Specifies whether or not egress frames are tagged by the designated port.

Copyright © 2008-2011 N-TRON Corp. All rights reserved. <http://www.n-tron.com>  
 Logged in as: admin

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The browser title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox". The address bar shows "http://192.168.2.216/main.ssi". The N-TRON logo is visible at the top left. A navigation menu on the left lists various categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays a table of links at the top, followed by the "Bridging" section. The Bridging section is divided into four categories: 1. Aging Time, 2. Unicast Addresses, 3. Multicast Addresses, and 4. Show MAC by Port. Each category has a corresponding table with detailed information.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

## Bridging

Bridging group is divided into four categories:  
 1. Aging Time 2. Unicast Addresses 3. Multicast Addresses 4. Show MAC by Port

### Aging Time

<b>Aging Time:</b>	This configurable field displays the aging time for dynamically learned MAC addresses. The inactive members will be removed from the Hardware Address Entry Table after this time period. The aging time range should be 5-1000000 seconds. The default aging time is 20 seconds.
--------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Unicast Addresses

This page shows the existing static Unicast MAC Addresses

<b>MAC Address:</b>	The static MAC address to be configured to the device.
<b>Port:</b>	Port which the static Unicast MAC address is to be configured.
<b>VLAN ID:</b>	VLAN in which the MAC address is assigned. The range is 1-4094.

### Multicast Addresses

This page shows the existing static Multicast Group Addresses

<b>Multicast Address:</b>	The static Multicast group address to be configured to the device.
<b>Port List:</b>	List of ports associated with this Multicast group address.
<b>VLAN ID:</b>	VLAN in which the Multicast group address is assigned. The range is 1-4094.

### Show MAC by Port

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The browser title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox". The address bar shows "http://192.168.2.216/main.ssi". The N-TRON logo is visible at the top left. A navigation menu on the left lists various configuration categories, with "RSTP" selected. The main content area displays the "RSTP - Rapid Spanning Tree Protocol" help page. It includes a table of links, a paragraph explaining the VLAN pull-down menu, a note about legacy device values, and two tables: "RSTP Root Bridge Configuration" and "This Bridge Configuration".

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

### RSTP - Rapid Spanning Tree Protocol

The VLAN pull-down menu is used to select which VLAN to configure.

Note: In order to accommodate legacy devices, use these values for RSTP: Auto Edge Disabled, Hello Time 2, Forward Delay 15, and Max Age 20.

#### RSTP Root Bridge Configuration

<b>Root Priority:</b>	Priority of the root bridge.
<b>Designated Root:</b>	The unique Bridge Identifier of the bridge recorded as the root in the Root Identifier parameter of Configuration BPDUs transmitted by the Designated Bridge for the LAN.
<b>Path Cost:</b>	The cost of the path to the root offered by the Designated Port on the LAN.
<b>Port:</b>	The Port Identifier of the Bridge Port believed to be the Designated Port for the LAN.
<b>Max Age:</b>	The maximum age of received protocol information before it is discarded.
<b>Hello Time:</b>	The time interval between the transmission of Configuration BPDUs by a bridge that is attempting to become the Root or is the Root.
<b>Forward Delay:</b>	The time spent in the Listening State while moving from the Blocking State to the Learning State.

#### This Bridge Configuration

<b>Hello Time:</b>	This configurable field shows the value of the Hello Time parameter when the bridge is the Root or is attempting to become the Root. The range is generally 1-10, but consult the user manual for other constraints. The default value is 1 second.
<b>Forward Delay:</b>	The time spent in the Listening State while moving from the Blocking State to the Learning State. The range is generally 4-30, but consult the user manual for other constraints. The default value is 13 seconds.
<b>Max Age:</b>	The value of the Max Age parameter when the bridge is the Root or is attempting

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

The screenshot shows the N-TRON web management interface. The browser title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox". The address bar shows "http://192.168.2.216/main.ssi". The N-TRON logo is visible at the top left. A navigation menu on the left lists various categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays the "IGMP - Internet Group Management Protocol" help page. At the top, there is a table of links: Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Rate Limiting, and User Management. Below this, the text states "IGMP group consists of four categories: 1. Configuration 2. Show Groups 3. Show Routers 4. RFilter Ports". The "Configuration" section includes a table with the following entries:

<b>IGMP Status:</b>	Indicates whether IGMP is enabled or disabled.
<b>Query Mode:</b>	Specifies the query mode to be used. The default is Auto. Auto - Multiple switches will ensure that only one switch is the active querier. On - This switch is always an active querier. Off - This switch never queries.
<b>Router Mode:</b>	Specifies the router mode to be used. The default is Auto. Auto - Allows for dynamically detected and manually set router ports. Manual - Allows only for manually set router ports. None - Allows no router ports.
<b>Remove Unused Groups:</b>	If 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.
<b>Manual Router Ports:</b>	Port or ports that are specified as router ports manually.
<b>N-Ring Router Ports:</b>	On an N-Ring Manager, the ring ports are informatively shown as router ports.
<b>N-Link Router Port:</b>	On N-Link Master, Slave, and Coupler switches, the coupler port is informatively shown as a router port.

The "Show Groups" section includes a table with the following entry:

<b>Total Number of Active IP Group Memberships:</b>	Total Number of Active Group IP Memberships based on the dotted quad view and counting each joined port.
-----------------------------------------------------	----------------------------------------------------------------------------------------------------------

Below this, there is a partially visible entry for "Group IP: Dynamically created Multicast group IP address".

At the bottom left of the page, the copyright information is displayed: "Copyright © 2008-2011 N-TRON Corp. All rights reserved. http://www.n-tron.com". The user is logged in as "admin".

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The browser title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox". The address bar shows "http://192.168.2.216/main.ssi". The N-TRON logo is visible at the top left. A navigation menu on the left lists various categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, TFTP, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays a table of links and the N-View help page.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

### N-View

N-View group consists of two categories: 1. Configuration 2. Ports

<u>Configuration</u>	
<b>N-View Status:</b>	Global N-View status of enabled or disabled.
<b>N-View Interval:</b>	Global interval in seconds for autocasting MIB counters.

<u>Ports</u>	
<b>Port Name:</b>	The descriptive name of the port.
<b>Multicast on Port?:</b>	Specifies whether or not to send autocast packets on this port.
<b>Send MIB Stats?:</b>	Specifies whether or not to send this port's MIB counters inside autocast packets.

Copyright © 2008-2011  
N-TRON Corp.  
All rights reserved.  
<http://www.n-tron.com>

Logged in as: **admin**

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The address bar shows the URL <http://192.168.2.216/main.ssi>. The page title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox".

The left sidebar contains a navigation menu with the following items:

- Administration
- DHCP
- LLDP
- Ports
- Statistics
- VLAN
- Bridging
- RSTP
- IGMP
- N-View
- N-Ring
- N-Link
- CIP
- Firmware/Config
  - TFTP
- Support
- Rate Limiting
  - Broadcast
  - Multicast
- User Management
- Logical View
- Home
- Config
- Help
- Logout

At the bottom of the sidebar, the following information is displayed:

Copyright © 2008-2011  
N-TRON Corp.  
All rights reserved.  
<http://www.n-tron.com>  
Logged in as: admin

The main content area features a table of links at the top:

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

The main content area is titled "N-Ring" and contains the following text:

N-Ring is divided into two categories:  
1. Configuration 2. Status

N-Ring Configuration is divided into two categories:  
1. Mode 2. Advanced

**Configuration - Mode**

If N-Ring mode is Manager, the following data will be shown:

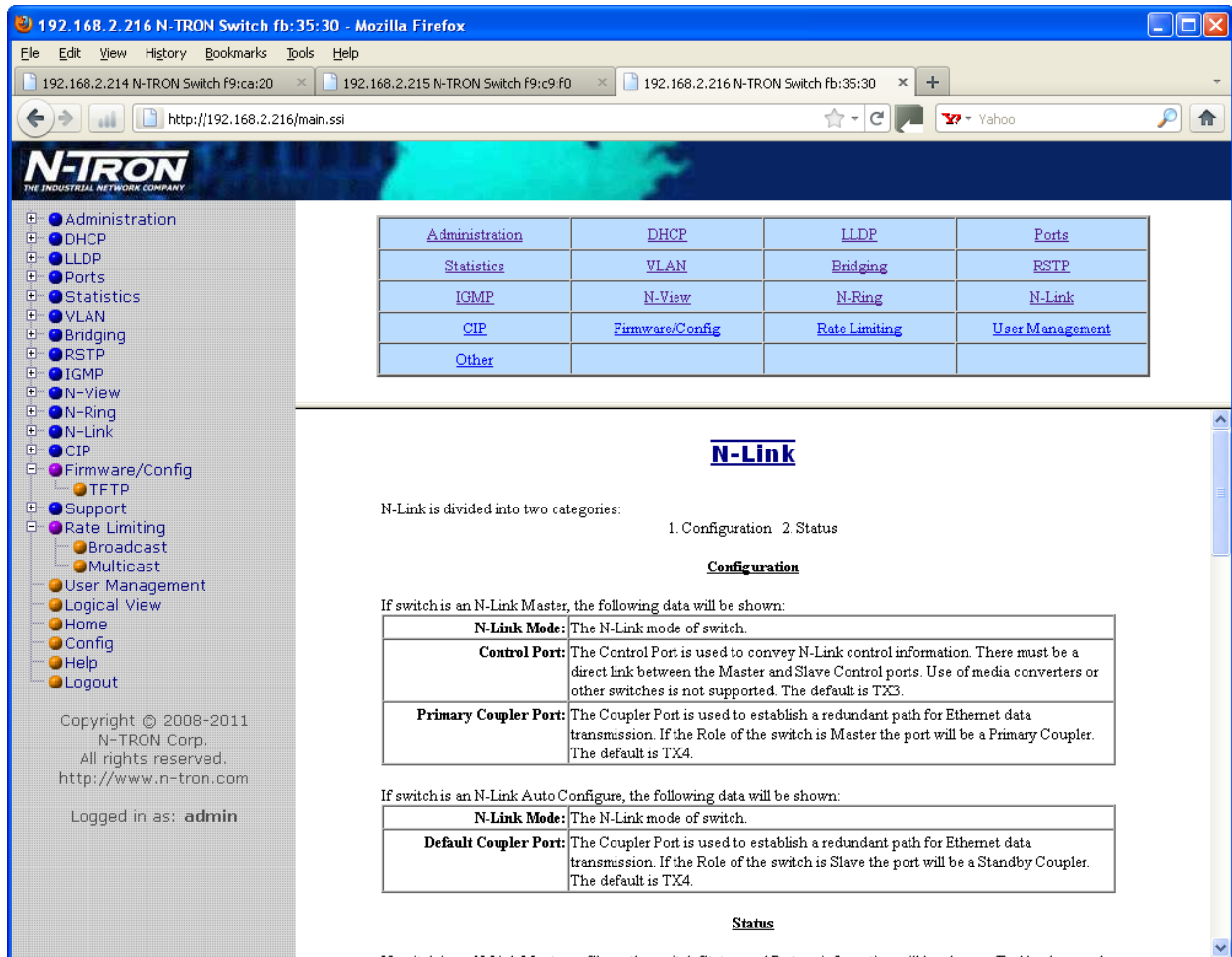
<b>N-Ring Mode:</b>	"Manager" - Switch is currently operating as an N-Ring Manager.
<b>Aging Time:</b>	Aging time used when switch is active in an N-Ring. The range is 5-1000000 seconds.
<b>N-Ring Ports:</b>	Port set used as N-Ring ports on this switch. The user can select an existing port set.
<b>VLAN ID:</b>	VLAN in which N-Ring ports are assigned. The VLAN ID is configurable and the range is 1-4094.
<b>Tagging:</b>	Selection as to whether the N-Ring ports are members of the VLAN's Tagged or Untagged ports. NOTE: It is recommended to use Tagged on N-Ring ports.

If N-Ring mode is Auto Member, the following data will be shown:

<b>N-Ring Mode:</b>	"Auto Member" - Switch is currently operating as an N-Ring Auto Member.
<b>Aging Time:</b>	Aging time used when switch is active in an N-Ring. The range is 5-1000000

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The browser title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox". The address bar shows "http://192.168.2.216/main.ssi". The N-TRON logo is visible at the top left of the page content.

On the left side, there is a navigation menu with the following items: Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, TFTP, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The "CIP" item is highlighted.

At the top right, there is a table of links:

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

The main content area is titled "CIP - Common Industrial Protocol". It states: "CIP is divided into two categories: 1. Configuration 2. Status".

**Configuration**

<b>CIP Status:</b>	Indicates whether CIP is enabled or disabled.
<b>Multicast RPI:</b>	The minimum Requested Packet Interval for Class 1 (multicast) connections, in milliseconds. Requests for less than this value will be rejected.
<b>Unicast RPI:</b>	The minimum Requested Packet Interval for Class 3 (unicast) connections, in milliseconds. Requests for less than this value will be rejected.

**Status**

<b>CIP Status:</b>	Indicates whether CIP is enabled or disabled.
--------------------	-----------------------------------------------

**Identity Information:**

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

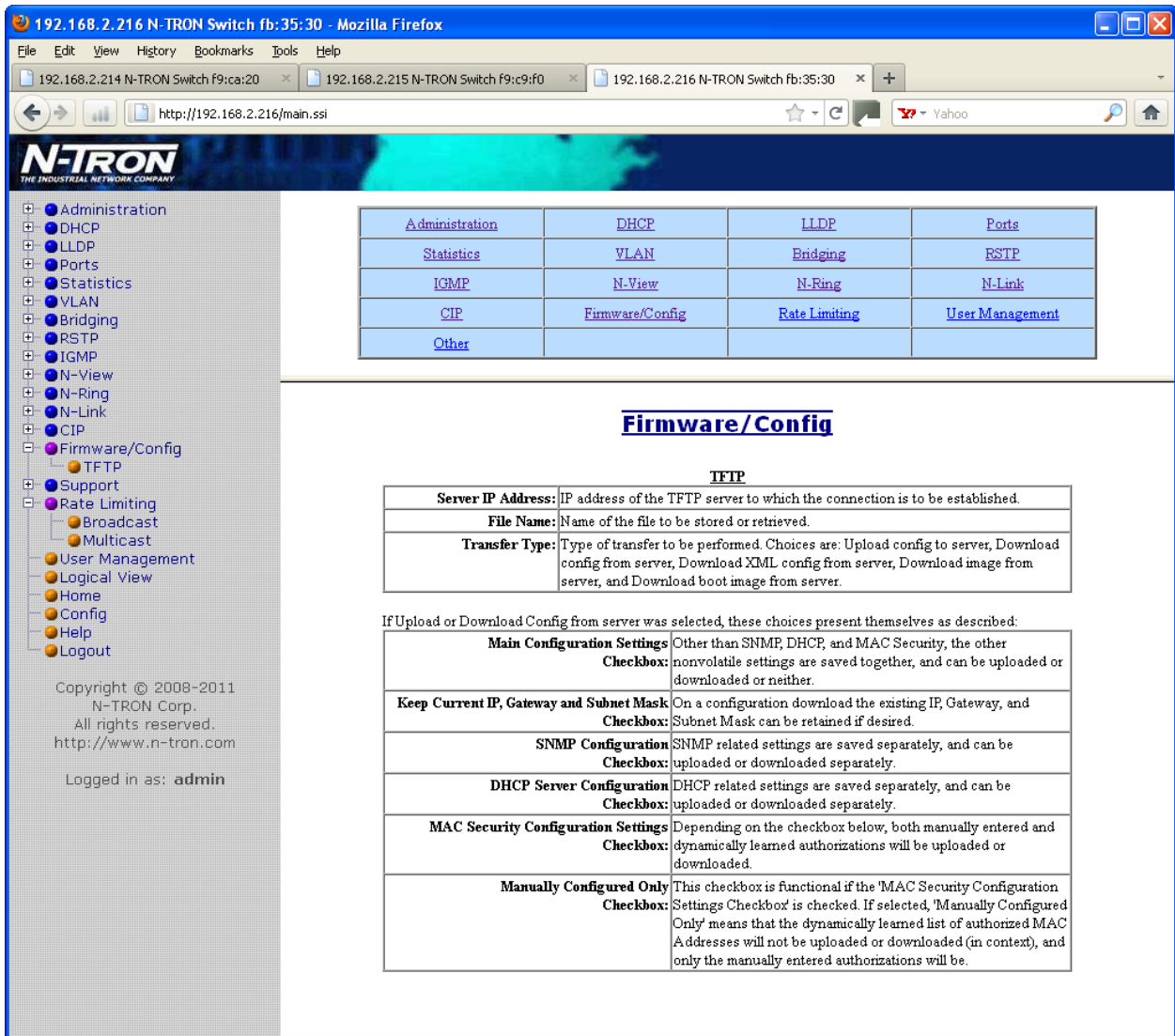
**Connection Information:**

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

At the bottom left of the page, there is copyright information: "Copyright © 2008-2011 N-TRON Corp. All rights reserved. http://www.n-tron.com". It also shows "Logged in as: admin".

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

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The browser title is "192.168.2.216 N-TRON Switch fb:35:30 - Mozilla Firefox". The address bar shows "http://192.168.2.216/main.ssi". The N-TRON logo is visible at the top left of the page content.

On the left side, there is a navigation menu with the following items: Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config (expanded to show TFTP), Support, Rate Limiting (expanded to show Broadcast and Multicast), User Management, Logical View, Home, Config, Help, and Logout. The user is logged in as "admin".

At the top right, there is a table of links:

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

The main content area is titled "Rate Limiting". It states: "Rate Limiting is divided into two categories: 1. Broadcast 2. Multicast".

**Broadcast**

<b>Port Name:</b>	The descriptive name of the port.
<b>Broadcast Pass Rate [%]:</b>	This configurable field displays the broadcast traffic rate. The allowed range is 0-100 and the default is 3% for 100 Mbps maximum capability ports and 1% for 1000 Mbps maximum capability ports (if any). 100% is not limiting.

**Multicast**

<b>Port Name:</b>	The descriptive name of the port.
<b>Multicast Pass Rate [%]:</b>	This configurable field displays the multicast traffic rate. The allowed range is 0-100 and the default is 100% for 100 Mbps maximum capability ports and 100% for 1000 Mbps maximum capability ports (if any). 100% is not limiting.
Note: This also causes Unicast packets with destinations not in the ARL table to be rate limited rather than all being flooded.	

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

# Help – User Management

The screenshot shows the N-TRON web management interface in a Mozilla Firefox browser. The address bar shows the URL `http://192.168.2.216/main.ssi`. The page features a navigation menu on the left with categories like Administration, DHCP, LLDP, Ports, Statistics, VLAN, Bridging, RSTP, IGMP, N-View, N-Ring, N-Link, CIP, Firmware/Config, Support, Rate Limiting, Broadcast, Multicast, User Management, Logical View, Home, Config, Help, and Logout. The main content area displays a table of links and a section titled "User Management" with explanatory text and a table of user management details.

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

### User Management

The User Management screen allows users to view, add and remove system user accounts.

User Management	
<b>No.:</b>	User table index
<b>User Name:</b>	User name string
<b>Access Permission:</b>	A user can have Admin (read/write) or User (read-only) privileges.

- Usenames may include all alphanumerical characters, "-" and "." and must be 3 to 15 characters long.
- Passwords may include all printable characters except "." and spaces and must be 3 to 15 characters long.

Copyright © 2008-2011  
N-TRON Corp.  
All rights reserved.  
<http://www.n-tron.com>

Logged in as: **admin**

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

<a href="#">Administration</a>	<a href="#">DHCP</a>	<a href="#">LLDP</a>	<a href="#">Ports</a>
<a href="#">Statistics</a>	<a href="#">VLAN</a>	<a href="#">Bridging</a>	<a href="#">RSTP</a>
<a href="#">IGMP</a>	<a href="#">N-View</a>	<a href="#">N-Ring</a>	<a href="#">N-Link</a>
<a href="#">CIP</a>	<a href="#">Firmware/Config</a>	<a href="#">Rate Limiting</a>	<a href="#">User Management</a>
<a href="#">Other</a>			

**Support Web Site:** This link leads to the [http://www.n-tron.com/html/support\\_serv.html](http://www.n-tron.com/html/support_serv.html) web site, which is the official web site of N-TRON Corp., the developer of the switch software.

**Support E-Mail:** To send any queries or suggestions to the support team at N-TRON Corp., the developers of the switch software.

**Logical View:** Shows a graphical depiction of the switch. Linked ports are displayed in green. The page automatically refreshes approximately every 30 seconds.

**Home:** The default home page of the switch. Shows some basic information, such as the switch model and firmware revision.

**Config:** To save or reset the configuration data. This will save the current configuration of the device to the flash for future use.

**Help:** Switch Help.

**Logout:** Logout from the WebConsole.

Copyright © 2008-2011  
N-TRON Corp.  
All rights reserved.  
<http://www.n-tron.com>

Logged in as: **admin**

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

## Logout

Command Name	<b>logout</b>
Description	Log out of console interface
Syntax	<b>logout</b>
Parameters	<b>None</b>
Examples	<b>N-TRON/Admin&gt; logout</b>
NOTES	

## CLI Commands, Continued...

### Show, Add, or Delete ARL Entries

Command Name	<b>arl</b>
Description	Show, Add, or Delete Arl Entries.
Syntax	<b>arl</b> show   showmct   add mac port cpu static vid   del[ete] mac vid
Parameters	<p><b>show</b> Show entire ARL table.</p> <p><b>showmct</b> Show entire ARL MCT (Multicast Index) table.</p> <p><b>delete</b> Delete MAC address.</p> <p><b>add</b> Add MAC address.</p> <p><b>mac</b> MAC Address.</p> <p><b>port</b> Port Number.</p> <p><b>cpu</b> 1 = Send to CPU also.</p> <p><b>static</b> 1 = This is a static address; 0 = Non-Static.</p> <p><b>vid</b> VLAN ID (0-4095)</p>
Example	<pre>N-TRON/Admin&gt; arl show  No. Val Age Pri Mod Usr Sta VLAN      MAC              Port(s) -----   1  1  1  0  0  0  1  1  00:07:af:ff:b8:00 CPU   2  1  0  0  0  0  0  1  00:19:b9:03:aa:77 TX3  N-TRON/Admin&gt; arl showmct  No. Idx Val Port Mask  Port(s) -----   1  0  1 0x00000000 (None)   2  1  1 0x00000001 TX1  N-TRON/Admin&gt; arl add 00:19:b9:03:aa:79 3 0 1 1  N-TRON/Admin&gt; arl del 00:19:b9:03:aa:79 1</pre>
Notes	

## CLI Commands, Continued...

### Configuration Device Operations

Command Name	<b>cfgdev</b>
Description	Info, Format, Compare and Erase Configuration Device.
Syntax	<b>CfgDev</b> info   format [-m model]   compare   erase
Parameters	<p><b>Info</b> Show information about the configuration device.</p> <p><b>Format</b> Format the configuration device to factory default.</p> <p><b>-m model</b> Configuration device model number. Valid values are: 1=At32K, 2=At64K, and 3=card.</p> <p><b>Compare</b> Compare the configuration of the switch to the configuration device.</p> <p><b>Erase</b> Erase the switch configuration on the configuration device.</p>
Example	<pre> <b>N-TRON/Factory&gt; cfgdev info</b>  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  <b>N-TRON/Factory&gt; cfgdev compare</b>  Comparing switch configuration to the configuration device... The configurations are different.  <b>N-TRON/Factory&gt; cfgdev erase</b>  Erasing configuration device...  Configuration device erase completed. </pre>
Notes	

## CLI Commands, Continued...

### Show or Set CIP Configuration

Command Name	<b>Cip</b>
Description	Show or set CIP configuration. If no parameters are specified, this command will show the CIP configuration (same as -show parameter).
Syntax	<b>-Cip [-e[nable]   -d[isable]   -show]</b>
Parameters	<p><b>-Cip -show</b> Show CIP configuration.</p> <p><b>-Cip [-e[nable]   -d[isable]]</b> Set the CIP status to e(nabled) or d(isabled).</p>
Examples	<pre> <b>N-TRON/Admin&gt; cip -show</b>  CIP Configuration: ----- Status:                Enabled EthIp Interval:        10 ms Cache Interval:        2000 ms  Identity Information: ----- Product Name:          N-TRON 709FX Vendor:                 1006 (N-TRON) Device Type:            0x0C (Communications Adapter) Major Revision:         1 Minor Revision:         2 Serial Number:          0xAFFBF8F0  Connection Information: ----- Multicast Connections: 0 Unicast Connections:   0  <b>N-TRON/Admin&gt; cip -disable</b> Changing CIP configuration...  CIP Configuration: ----- Status:                Disabled EthIp Interval:        10 ms Cache Interval:        2000 ms  Identity Information: ----- Product Name:          N-TRON 709FX Vendor:                 1006 (N-TRON) Device Type:            0x0C (Communications Adapter) Major Revision:         1 Minor Revision:         2 Serial Number:          0xAFFBF8F0  Connection Information: ----- Multicast Connections: 0 Unicast Connections:   0  <b>N-TRON/Admin&gt;</b> </pre>
NOTES	

## CLI Commands, Continued...

### Save or Reset the Configuration Settings

Command Name	<b>config</b>
Description	Save or reset configuration settings
Syntax	<b>config</b> s[ave]   r[eset]
Parameters	<p><b>save</b> save current running configuration settings.</p> <p><b>reset</b> reset configuration settings to factory defaults.</p>
Examples	<pre> <b>N-TRON/Admin&gt; config save</b>  Save Settings...  Settings have been saved.  <b>N-TRON/Admin&gt; config reset</b>  Resetting to factory defaults... Load factory default settings [y/n]?y Keep IP, subnet mask, and gateway addresses [y/n]?y Keep current user names and passwords [y/n]?y ... </pre>
NOTES	

### Show or Set IGMP Configuration

Command Name	<b>igmp</b>
Description	Show or set IGMP configuration. If no parameters are specified, this command will show the IGMP configuration (same as -show parameter).
Syntax	<b>igmp</b> [-show] [-status state]
Parameters	<p><b>-show</b> Show configuration.</p> <p><b>-status state</b> Set the IGMP status to e(nabled) or d(isabled).</p>
Examples	<pre> <b>N-TRON/Admin&gt; igmp -show</b>  IGMP Status           : Enabled IGMP Version          : 2 Query Mode            : Auto CIP Querier Status    : 2, Active-Auto Active Querier IP     : 192.168.1.250 Router Mode           : Auto Manual Router Ports   : (None) IGMP Number of Groups : 1 IGMP Resource Usage % : 1  <b>N-TRON/Admin&gt; igmp -status disabled</b>  IGMP Status           : Disabled IGMP Version          : 2 Query Mode            : Auto CIP Querier Status    : 2, Active-Auto Active Querier IP     : 192.168.1.250 Router Mode           : Auto Manual Router Ports   : (None) IGMP Number of Groups : 1 IGMP Resource Usage % : 1 N-TRON/Admin&gt;... </pre>
NOTES	



## CLI Commands, Continued...

### Show or Set Mirror Configuration

Command Name	<b>Mirror</b>
Description	Show or set Mirror configuration. If no parameters are specified, this command will show the Mirror configuration (same as -show parameter).
Syntax	<b>mirror</b> [-show] [-status state] [-dp portno] [-tx portlist] [-rx portlist]
Parameters	<p><b>-show</b> Show configuration.</p> <p><b>-status state</b> Set the Mirror status to e(nabled) or d(isabled).</p> <p><b>-dp portno</b> Set the destination port number for mirrored frames.</p> <p><b>-tx portlist</b> Set the source ports to mirror frames that are transmitted.</p> <p><b>-rx portlist</b> Set the source ports to mirror frames that are received.</p>
Examples	<pre> N-TRON/Admin&gt; mirror -show  Mirror Status      : Disabled Destination Port   : TX1 Tx Source Ports    : (None) Rx Source Ports    : (None)  N-TRON/Admin&gt; mirror -show  Mirror Status      : Disabled Destination Port   : TX1 Tx Source Ports    : (None) Rx Source Ports    : (None)  N-TRON/Admin&gt; 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.  N-TRON/Admin&gt;... </pre>
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	<b>Nring</b>
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	<b>nring</b> [-show] [-mode d   a   m] [-ports set_id]
Parameters	<p><b>-show</b> Show configuration.</p> <p><b>-mode</b> Set the N-Ring mode. d = disabled, a = auto member, m = manager</p> <p><b>-ports set_id</b> Set the ring ports for N-Ring manager mode. Specify port set identifier or use '?' to list available port sets.</p>
Examples	<pre> N-TRON/Admin&gt; nring -show  N-Ring Mode   : Auto Member Aging Time    : 20  N-TRON/Admin&gt; nring -ports ?  ID      Port Set --      -   1     TX1 / TX2   2     TX7 / TX8  N-TRON/Admin&gt; nring -mode m -ports 2  Do you Want to Save Changes and Restart the System Now [y/n]? ... </pre>
NOTES	

### Show or Set N-View Configuration

Command Name	<b>Nview</b>
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	<b>nview</b> [-show] [-status state]
Parameters	<p><b>-show</b> Show configuration.</p> <p><b>-status state</b> Set the N-View status to e(nabled) or d(isabled).</p>
Examples	<pre> N-TRON/Admin&gt; nview -show  N-View Status   : Enabled N-View Interval : 5  N-TRON/Admin&gt; nview -status disabled  N-View Status   : Disabled N-View Interval : 5  Changes have been made that have not been saved. ... </pre>
NOTES	

## CLI Commands, Continued...

### Ping a Host

Command Name	<b>Ping</b>
Description	Ping a host
Syntax	<b>ping</b> [-t] [-n count] [-w timeout] target_name
Parameters	<p><b>target_name</b> IP Address or host name.</p> <p><b>-t</b> Ping the specified host until stopped. To see statistics and continue - type Space; To stop - type Control-C.</p> <p><b>-n count</b> Number of echo requests to send.</p> <p><b>-w timeout</b> Timeout in milliseconds to wait for each reply.</p>
Example	<pre>N-TRON/Admin&gt; ping 192.168.1.119 ... N-TRON/Admin&gt; ping -n 6 192.168.1.119 ... N-TRON/Admin&gt; ping -t 192.168.1.119 ... N-TRON/Admin&gt; ping -w 2000 192.168.1.119  Reply from 192.168.1.119: time=970ms Reply from 192.168.1.119: time&lt;10ms Reply from 192.168.1.119: time&lt;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</pre>
Notes	

## CLI Commands, Continued...

### Show or Set Port Configuration

Command Name	<b>Port</b>																																																								
Description	Show or set Port configuration.																																																								
Syntax	<b>port</b> [-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	<p><b>Portno</b> Port number to configure or show. Specify “all” to show all ports.</p> <p><b>-show</b> Show configuration.</p> <p><b>-admin state</b> Set the admin status for the port to e(nabled) or d(isabled).</p> <p><b>-sd</b> Set the speed and duplex mode for the port. auto = enable auto-negotiation</p> <p><b>-flow state</b> Set the flow control for the port to e(nabled) or d(isabled).</p> <p><b>-fhp state</b> Set force high priority for the port to e(nabled) or d(isabled).</p> <p><b>-dp</b> Set the default QOS priority for the port. The range is 0-7.</p> <p><b>-dscp state</b> Set the DSCP Priority for the port to e(nabled) or d(isabled).</p> <p><b>-8021p state</b> Set the 802.1p Priority for the port to e(nabled) or d(isabled).</p> <p><b>-pvid</b> Set the VLAN ID for the port. The range is 1-4094.</p> <p><b>-ual percent</b> Set the usage alarm low percentage. The range is 0-100.</p> <p><b>-uah percent</b> Set the usage alarm high percentage. The range is 0-100.</p> <p><b>-security state</b> Set the security status for all supported ports to e(nabled) or d(isabled).</p>																																																								
Examples	<pre>N-TRON/Admin&gt; port -sd 100f -flow enabled -dp 7 -pvid 2 5</pre> <table border="1"> <thead> <tr> <th>Port No</th> <th>Port Name</th> <th>Admin Status</th> <th>Link Stat</th> <th>Auto Nego</th> <th>Port Spd</th> <th>Dupl Mode</th> <th>Flow Control</th> <th>Force High Pri</th> <th>Def Pri</th> <th>Port State</th> <th>PVID</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>TX2</td> <td>Enabled</td> <td>Down</td> <td>Disabled</td> <td>100</td> <td>Full</td> <td>Enabled</td> <td>Disabled</td> <td>7</td> <td>Disabled</td> <td>2</td> </tr> </tbody> </table> <p>Changes have been made that have not been saved.</p> <pre>N-TRON/Admin&gt; port -dscp e 1</pre> <table border="1"> <thead> <tr> <th>Port No</th> <th>Port Name</th> <th>Admin Status</th> <th>Link Stat</th> <th>Auto Nego</th> <th>Port Spd</th> <th>Dupl Mode</th> <th>Flow Control</th> <th>Force High Pri</th> <th>Include DSCP</th> <th>Include 802.1p</th> <th>Def Pri</th> <th>Port State</th> <th>PVID</th> <th>Usage Alarm Low %</th> <th>Usage Alarm High %</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>TX1</td> <td>Enabled</td> <td>Down</td> <td>Enabled</td> <td>Auto</td> <td>Auto</td> <td>Disabled</td> <td>Disabled</td> <td>Enabled</td> <td>Enabled</td> <td>1</td> <td>Disabled</td> <td>1</td> <td>0</td> <td>100</td> </tr> </tbody> </table> <p>Changes have been made that have not been saved.</p> <pre>N-TRON/Admin&gt;</pre>	Port No	Port Name	Admin Status	Link Stat	Auto Nego	Port Spd	Dupl Mode	Flow Control	Force High Pri	Def Pri	Port State	PVID	5	TX2	Enabled	Down	Disabled	100	Full	Enabled	Disabled	7	Disabled	2	Port No	Port Name	Admin Status	Link Stat	Auto Nego	Port Spd	Dupl Mode	Flow Control	Force High Pri	Include DSCP	Include 802.1p	Def Pri	Port State	PVID	Usage Alarm Low %	Usage Alarm High %	1	TX1	Enabled	Down	Enabled	Auto	Auto	Disabled	Disabled	Enabled	Enabled	1	Disabled	1	0	100
Port No	Port Name	Admin Status	Link Stat	Auto Nego	Port Spd	Dupl Mode	Flow Control	Force High Pri	Def Pri	Port State	PVID																																														
5	TX2	Enabled	Down	Disabled	100	Full	Enabled	Disabled	7	Disabled	2																																														
Port No	Port Name	Admin Status	Link Stat	Auto Nego	Port Spd	Dupl Mode	Flow Control	Force High Pri	Include DSCP	Include 802.1p	Def Pri	Port State	PVID	Usage Alarm Low %	Usage Alarm High %																																										
1	TX1	Enabled	Down	Enabled	Auto	Auto	Disabled	Disabled	Enabled	Enabled	1	Disabled	1	0	100																																										
NOTES																																																									

## CLI Commands, Continued...

### Reset the Switch

Command Name	<b>Reset</b>
Description	Reset (reboot) the switch
Syntax	<b>Reset</b>
Parameters	<b>None</b>
Example	<pre>N-TRON/Admin&gt; 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... ...</pre>
Notes	

### Show or Set SNMP Configuration

Command Name	<b>Snmpp</b>
Description	Show or set SNMP configuration. If no parameters are specified, this command will show the SNMP configuration (same as -show parameter).
Syntax	<b>snmp</b> [-show] [-ro name] [-rw name] [-trap name]
Parameters	<p><b>-show</b> Show configuration.</p> <p><b>-ro name</b> Set the Authorized Community Name for SNMP Get requests.</p> <p><b>-rw name</b> Set the Authorized Community Name for SNMP Set requests.</p> <p><b>-trap name</b> Set the Authorized Community Name for SNMP Traps.</p>
Examples	<pre>N-TRON/Admin&gt; 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. ...</pre>
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	<b>Syserr</b>
Description	Show or clear the last system error  If <i>clear</i> is not supplied, then the last system error is displayed.
Syntax	<b>syserr</b> [clear]
Parameters	<b>Clear</b> Clear the last system error.
Example	<b>N-TRON/Admin&gt; syserr</b> Last System Error: None.  <b>N-TRON/Admin&gt; syserr clear</b> Last System Error: Cleared.
Notes	

### Show System Information

Command Name	<b>Sysinfo</b>
Description	Show system information
Syntax	<b>Sysinfo</b>
Parameters	<b>None</b>
Example	<b>N-TRON/Admin&gt; sysinfo</b>  <pre> +++++ + + N-TRON 700/7000/7500 Series + +++++ + + Model:          709FX + Boot Loader:    BL 2.0.5.1 (0x02000501) + OS Version:     3.2.1 + Build Date:     Dec  8 2009 at 15:10:57 + Copyright:      Copyright (c) 2008-2009 N-TRON Corporation All rights reserved. + + Processor:      66 MHz (66000000) + SDRAM Size:     16 MB + Flash Size:     8 MB + File System:    6422528 Bytes, 2907136 Free, 3515392 Used, 0 Bad + MAC Address:    00:07:af:fd:64:60 + IP Address:     192.168.1.214 + Subnet Mask:    255.255.255.0 + Gateway:        192.168.1.1 + Cfg Device:     Not connected + +++++ </pre> <b>N-TRON/Admin&gt;</b>
Notes	

## CLI Commands, Continued...

### Set or Show the System IP Configuration

Command Name	<b>Sysip</b>
Description	<p>Set system IP configuration mode, IP address, subnet mask, and gateway</p> <p>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.</p>
Syntax	<b>sysip</b> [-c config_mode] [-i static_ip] [-s static_subnet_mask] [-g static_gateway]
Parameters	<p><b>-c config_mode</b> s(tatic) or d(hcp).</p> <p><b>-i static_ip</b> Static IP address (for static config mode and IP fallback ).</p> <p><b>-s static_subnet_mask</b> Static sub net mask (for static config mode and IP fallback ).</p> <p><b>-g static_gateway</b> Static gateway address ( for static config mode and IP fallback ).</p>
Example	<pre> <b>N-TRON/Admin&gt; sysip</b>  IP Configuration Mode : Static Static IP Address      : 192.168.1.225 Static subnet Mask    : 255.255.255.0 Static gateway        : 192.168.1.1  <b>N-TRON/Admin&gt; sysip -c dhcp</b>  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 &lt;ENTER&gt; to Save Changes and Restart the System Now ... <b>N-TRON/Admin&gt; sysip -i 192.168.2.119 -s 255.255.252.0 -g 192.168.1.1</b>  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 &lt;ENTER&gt; to Save Changes and Restart the System Now ... </pre>
NOTES	<p>If mode is set to DHCP and IP fallback occurs, DHCP requests will stop.</p> <p>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.</p>

## CLI Commands, Continued...

### Show or Set System Configuration

Command Name	<b>System</b>
Description	Show or set System configuration. If no parameters are specified, this command will show the System configuration (same as -show parameter).
Syntax	<b>system</b> [-show] [-name label] [-browser state]
Parameters	<p><b>-show</b> Show configuration.</p> <p><b>-name label</b> Set the switch name.</p> <p><b>-browser state</b> Set the browser access status to e(nabled) or d(isabled).</p>
Examples	<pre>N-TRON/Admin&gt; system -name "Private switch" -browser disabled  IP Configuration : Static IP Address       : 192.168.1.201 Subnet Mask      : 255.255.255.0 Gateway          : 192.168.1.1 MAC Address      : 00:07:af:fb:fa:40 System Up Time   : 0 days, 17 hours, 10 mins, 56 secs Name             : Private switch Contact          : N-Tron Admin Location         : Mobile, AL 36609 Browser Access   : Disabled  Changes have been made that have not been saved. ...</pre>
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 Addition and Deletion Example

The screen capture below is the factory default VLAN configuration.

### VLAN Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>

Clicking on the “Modify” button allows one to add a new VLAN:

### VLAN Configuration

Replace VID Tag With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

VLAN Groups					
VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
<a href="#">0001</a>	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>	
<input type="button" value="Add"/>					

When creating a new VLAN, a numeric ID is required, Name is entered. Note that N-Ring VLAN is a reserved name with a special meaning. Choices such as “Allow Management” and “Change PVID of

Member Ports” are made at this time as well as the ports which are going to belong to the new VLAN. Additionally, the ports may be “Untagged on Egress”.

## Tagged VLAN Group Configuration

<b>ID</b>	<input type="text" value="2"/>
<b>Name</b>	<input type="text" value="New VLAN"/>
<b>Allow Management</b>	<input type="checkbox"/>
<b>Change PVID Of Member Ports</b>	<input checked="" type="checkbox"/>

**Group Ports**

Port No	Port Name	Group Member	Untag On Egress
01	TX1	<input type="checkbox"/>	<input type="checkbox"/>
02	TX2	<input type="checkbox"/>	<input type="checkbox"/>
03	TX3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
04	TX4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
05	TX5	<input type="checkbox"/>	<input type="checkbox"/>
06	TX6	<input type="checkbox"/>	<input type="checkbox"/>
07	TX7	<input type="checkbox"/>	<input type="checkbox"/>
08	TX8	<input type="checkbox"/>	<input type="checkbox"/>
09	FX1	<input type="checkbox"/>	<input type="checkbox"/>

The result of add is a “New VLAN”. In this case, it does not overlap the “Default VLAN” ports.

## VLAN Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX1, TX2, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>
0002	New VLAN	TX3, TX4	(None)	<input type="checkbox"/>

Modify

Refresh

The ports of "New VLAN" may be added back to "Default VLAN" to create overlapping VLANs.

Note: If there are multiple ports on different VLANs, the 709FX 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.

## VLAN Configuration

<b>Replace VID Tag With Default Port VID</b>	<input type="checkbox"/>
<b>Perform Ingress Filtering</b>	<input type="checkbox"/>
<b>Discard Non-Tagged For Ports</b>	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4
	<input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8
	<input type="checkbox"/> FX1
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

VLAN Groups					
VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
<a href="#">0001</a>	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>	
<a href="#">0002</a>	New VLAN	TX3, TX4	(None)	<input type="checkbox"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>					
<input type="button" value="Done"/> <input type="button" value="Refresh"/>					

But notice that the ports in “New VLAN” are not marked as “Untag on Egress” and are thus still tagged.

And the “New VLAN” may be deleted when it is no longer required:

## VLAN Configuration

Replace VID Tag With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1 <input type="checkbox"/> FX2 <input type="checkbox"/> FX3
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

### VLAN Groups

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
<a href="#">0001</a>	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1, FX2, FX3	TX1, TX2, TX5, TX6, TX7, TX8, FX1, FX2, FX3	<input checked="" type="checkbox"/>	
<a href="#">0002</a>	New VLAN	TX3, TX4	(None)	<input type="checkbox"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>					

## VLAN Configuration

Replace VID Tag With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4 <input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8 <input type="checkbox"/> FX1
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

**Message from webpage** ✕

VLAN ID: 2  
 Are you sure you want to delete this VLAN?

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
<a href="#">0001</a>	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1	TX1, TX2, TX5, TX6, TX7, TX8, FX1	<input checked="" type="checkbox"/>	
<a href="#">0002</a>	New VLAN	TX3, TX4	(None)	<input type="checkbox"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>					

And the “New VLAN” is removed. Note that the new configuration of the switch must be saved if the configuration must survive a power cycle.

### VLAN Configuration

Replace VID Tag With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	<input type="checkbox"/> TX1 <input type="checkbox"/> TX2 <input type="checkbox"/> TX3 <input type="checkbox"/> TX4
	<input type="checkbox"/> TX5 <input type="checkbox"/> TX6 <input type="checkbox"/> TX7 <input type="checkbox"/> TX8
	<input type="checkbox"/> FX1 <input type="checkbox"/> FX2 <input type="checkbox"/> FX3
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

VLAN Groups					
VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
<a href="#">0001</a>	Default VLAN	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8, FX1, FX2, FX3	TX1, TX2, TX5, TX6, TX7, TX8, FX1, FX2, FX3	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>					

## VLAN Configuration Examples

A VLAN is an administratively configured LAN segment that limits the traffic in multiple broadcast domains. Instead of physically reconnecting a device to a different LAN, network administrators can accomplish this task by configuring a VLAN compliant switch to create logical network segments.

Tagged VLAN allows switch segmentation to span across multiple managed switches. This type of VLAN is ideal for LANs that consist of various types of communication groups such as Office LANs, Controls Systems, and IP Cameras. When used properly, it will effectively isolate two or more groups from each other in a logical manner. This means that Broadcast, Multicast, and Unicast frames in one VLAN will not interfere with another isolated VLAN group.

The examples in this section are shown as configured on a 708TX switch, but the 709FX series may be configured similarly with the additional ports.

### Example 1 – Basic understanding of port-based VLANs

#### VLAN Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX3, TX4, TX5, TX6, TX7, TX8	TX3, TX4, TX5, TX6, TX7, TX8	<input checked="" type="checkbox"/>
0002	VLAN-2	TX1, TX2	TX1, TX2	<input type="checkbox"/>

#### Port Configuration View

Port No	Port Name	PVID
<a href="#">01</a>	TX1	2
<a href="#">02</a>	TX2	2
<a href="#">03</a>	TX3	1
<a href="#">04</a>	TX4	1
<a href="#">05</a>	TX5	1
<a href="#">06</a>	TX6	1
<a href="#">07</a>	TX7	1
<a href="#">08</a>	TX8	1

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	MAC on port TX2	TX2	Unicast Traffic
TX1	Untagged	Unknown MAC	TX2	Floods VLAN 2
TX1	VID 4	MAC on port TX2	--	Packet Discarded
TX3	Untagged	MAC on port TX5	TX5	Unicast Traffic
TX3	Untagged	Unknown MAC	TX4-TX8	Floods VLAN 1
TX3	VID 4	MAC on port TX6	--	Packet Discarded

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

## VLAN Configuration View    Port Configuration View

<b>Replace VID With Default Port VID</b>	<input type="checkbox"/>
<b>Perform Ingress Filtering</b>	<input type="checkbox"/>
<b>Discard Non-Tagged For Ports</b>	TX1, TX2, TX3, TX5, TX6, TX7, TX8

Port No	Port Name	PVID
<a href="#">01</a>	TX1	1
<a href="#">02</a>	TX2	1
<a href="#">03</a>	TX3	1
<a href="#">04</a>	TX4	3
<a href="#">05</a>	TX5	1
<a href="#">06</a>	TX6	1
<a href="#">07</a>	TX7	1
<a href="#">08</a>	TX8	1

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX3, TX5, TX6, TX7, TX8	(None)	<input type="checkbox"/>
0002	VLAN-2	TX1, TX2	(None)	<input type="checkbox"/>
0003	VLAN-3	TX4	(None)	<input checked="" type="checkbox"/>

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	MAC on port TX2	--	Packet Discarded
TX1	VID 2	MAC on port TX2	TX2	Unicast Traffic
TX1	VID 4	MAC on port TX2	--	Packet Discarded
TX1	VID 2	MAC on port TX5	TX2	Floods VLAN 2
TX3	Untagged	MAC on port TX1	--	Packet Discarded
TX3	VID 1	MAC on port TX6	TX6	Unicast Traffic
TX3	VID 1	Unknown MAC	TX5-TX8	Floods VLAN 1
TX3	VID 4	MAC on port TX8	--	Packet Discarded



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

## VLAN Configuration View      Port Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX3, TX4, TX5, TX6, TX7, TX8	(None)	<input checked="" type="checkbox"/>
0002	VLAN-2	TX1, TX2	(None)	<input type="checkbox"/>

Port No	Port Name	PVID
<a href="#">01</a>	TX1	2
<a href="#">02</a>	TX2	2
<a href="#">03</a>	TX3	1
<a href="#">04</a>	TX4	1
<a href="#">05</a>	TX5	1
<a href="#">06</a>	TX6	1
<a href="#">07</a>	TX7	1
<a href="#">08</a>	TX8	1

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	MAC on port TX2	TX2	Adds VID 2 to packet
TX1	VID 2	MAC on port TX2	TX2	Unicast Traffic
TX1	VID 4	MAC on port TX2	--	Packet Discarded
TX1	VID 2	Unknown MAC	TX2	Floods VLAN 2
TX3	Untagged	Unknown MAC	TX4-TX8	Adds VID 1 to packet & Floods VLAN 1
TX3	VID 1	MAC on port TX6	TX6	Unicast Traffic
TX3	VID 1	Unknown MAC	TX4-TX8	Floods VLAN 1
TX3	VID 4	MAC on port TX7	--	Packet Discarded

**Example 4** – Basic understanding of Hybrid VLANs

## VLAN Configuration View      Port Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

Port No	Port Name	PVID
<a href="#">01</a>	TX1	2
<a href="#">02</a>	TX2	2
<a href="#">03</a>	TX3	1
<a href="#">04</a>	TX4	1
<a href="#">05</a>	TX5	1
<a href="#">06</a>	TX6	1
<a href="#">07</a>	TX7	1
<a href="#">08</a>	TX8	1

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX3, TX4, TX5, TX6, TX7, TX8	TX3, TX4, TX5, TX6, TX7, TX8	<input checked="" type="checkbox"/>
0002	VLAN-2	TX1, TX2, TX3, TX4	TX1, TX2	<input type="checkbox"/>

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	MAC on port TX2	TX2	Unicast Traffic
TX1	Untagged	MAC on port TX3	TX3	Adds VID 2 in the packet
TX1	VID 4	MAC on port TX2	--	Packet Discarded
TX1	VID 4	MAC on port TX3	--	Packet Discarded
TX1	VID 2	MAC on port TX2	TX2	Strips VID off packet
TX3	Untagged	MAC on port TX6	TX6	Unicast Traffic
TX3	Untagged	Unknown MAC	TX4-TX8	Floods VLAN 1
TX3	VID 4	MAC on port TX5	--	Packet Discarded
TX3	VID 4	MAC on port TX4	--	Packet Discarded
TX3	VID 2	MAC on port TX4	TX4	Does not strip VID off packet
TX3	VID 2	MAC on port TX1	TX1	Strips VID off packet

**Example 5** – Basic understanding of Overlapping VLANs

## VLAN Configuration View    Port Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

Port No	Port Name	PVID
01	TX1	4
02	TX2	2
03	TX3	3
04	TX4	3
05	TX5	3
06	TX6	3
07	TX7	3
08	TX8	3

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	(None)	(None)	<input type="checkbox"/>
0002	VLAN-2	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8	<input type="checkbox"/>
0003	VLAN-3	TX2, TX3, TX4, TX5, TX6, TX7, TX8	TX2, TX3, TX4, TX5, TX6, TX7, TX8	<input checked="" type="checkbox"/>
0004	VLAN-4	TX1, TX2	TX1, TX2	<input type="checkbox"/>

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	MAC on port TX2, VID=4	TX2	Unicast Traffic
TX1	Untagged	MAC on port TX3	TX2	Floods VLAN 4
TX1	VID 4	MAC on port TX2, VID=4	TX2	Strips VID off packet
TX1	VID 4	Unknown MAC	TX2	Strips VID off packet & Floods VLAN 4
TX2	Untagged	MAC on port TX1, VID=2	TX1	Unicast Traffic
TX2	Untagged	MAC on port TX5, VID=2	TX5	Unicast Traffic
TX2	VID 2 or 3	MAC on port TX5, VID=2 and 3	TX5	Strips VID off packet (or floods if MAC is unknown for VID)
TX2	Untagged	Unknown MAC	TX1, TX3-TX8	Floods VLAN 2
TX3	Untagged	MAC on port TX1, VID=3	TX2, TX4-TX8	Floods VLAN 3
TX3	Untagged	MAC on port TX2, VID=3	TX2	Unicast Traffic
TX3	Untagged	MAC on port TX5, VID=3	TX5	Unicast Traffic
TX3	VID 2 or 3	MAC on port TX2, VID=2 and 3	TX2	Strips VID off packet (or floods if MAC is unknown for VID)

**Example 6 – Basic understanding of VLANs with Multicast Filtering**

## VLAN Configuration View Port Configuration View

Replace VID With Default Port VID	<input type="checkbox"/>
Perform Ingress Filtering	<input type="checkbox"/>
Discard Non-Tagged For Ports	(None)

Port No	Port Name	PVID
<a href="#">01</a>	TX1	4
<a href="#">02</a>	TX2	2
<a href="#">03</a>	TX3	3
<a href="#">04</a>	TX4	3
<a href="#">05</a>	TX5	3
<a href="#">06</a>	TX6	3
<a href="#">07</a>	TX7	3
<a href="#">08</a>	TX8	3

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	(None)	(None)	<input type="checkbox"/>
0002	VLAN-2	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8	<input type="checkbox"/>
0003	VLAN-3	TX2, TX3, TX4, TX5, TX6, TX7, TX8	TX2, TX3, TX4, TX5, TX6, TX7, TX8	<input checked="" type="checkbox"/>
0004	VLAN-4	TX1, TX2	TX1, TX2	<input type="checkbox"/>

Top of Form  
Bottom of Form

Static Multicast Group Address Filters		
Multicast Address	Port List	VLAN ID
01:00:00:00:00:01	TX1, TX2, TX3, TX4, TX5, TX6, TX7, TX8	2
01:00:00:00:00:02	TX1, TX6, TX8	3

Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	01:00:00:00:00:01	TX2	Goes to ports TX1-TX8, but TX1 can only send to TX2 (VLAN 4)
TX3	Untagged	01:00:00:00:00:02	TX6, TX8	Goes to ports TX2, TX6-TX8 (VLAN 3) but filter keeps it on ports TX6 and TX8 only
TX2	Untagged	01:00:00:00:00:01	TX1, TX3-TX8	Goes to ports TX1-TX8, but won't go back out the port it came in on
TX2	Untagged	01:00:00:00:00:02	TX1, TX3-TX8	Goes to ports TX1, TX3-TX8
TX3	Untagged	01:00:00:00:00:01	TX2, TX4-TX8	Goes to ports TX2, TX4-TX8
TX6	Untagged	01:00:00:00:00:02	TX8	Goes to port TX8
TX3	Untagged	01:00:00:00:00:02	TX6, TX8	Goes to ports TX6 and TX8

Note: If there are multiple ports on different VLANs, the 709FX 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.

For further information and examples on overlapping vlans, see:  
<http://www.n-tron.com/pdf/overlappingportvlan.pdf>

# KEY SPECIFICATIONS (709FX)

## Switch Properties

*Number of MAC Addresses:* 8,000  
*Aging Time:* Programmable  
*Latency Type:* 2.6  $\mu$ s  
*Switching Method:* Store & Forward

## Case Dimensions

*Height:* 4.3" / 10.9 cm  
*Width:* 2.4" / 6.1 cm  
*Depth:* 4.6" / 11.7 cm  
*Weight (max):* 1.6 / 0.73 kg  
*Din-Rail mount:* 35mm

## Electrical

*Redundant Input Voltage:* 10-49VDC (Regulated)  
*Input Current (max):* 365mA max. @ 24VDC  
*N-TRON Power Supply:* NTPS-24-1.3 (1.3 Amp@24VDC)

## Environmental

*Operating Temperature:* -40°C to 70°C  
*Storage Temperature:* -40°C to 85°C

*Operating Humidity:* 5% to 95%  
(Non Condensing)

*Operating Altitude:* 0 to 10,000 ft.

## Shock and Vibration

(bulkhead mounting)

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

## Reliability

*MTBF:* >2 Million Hours

## Warranty:

3 years from the date of purchase.



## Connectors

10/100BaseTX: (8) RJ-45 Copper Ports  
100BaseFX: (1) SC or ST Duplex Ports

## Recommended Wiring Clearance:

*Front:* 4" (10.16cm)  
*Top:* 1" (2.54 cm)  
*Bottom:* 1" (2.54 cm)

## Network Media

*10BaseT:* >Cat3 Cable  
*100BaseTX:* >Cat5 Cable

**100 Mb Fiber Transceiver Characteristics**

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

\* Multimode Fiber Optic Cable

\*\* Singlemode Fiber Optic Cable

**Regulatory Approvals:**

**Safety:** Suitable for use in Class I, Division 2, Groups A, B, C and D Hazardous Locations, or Nonhazardous Locations only.

**EMI:** ANSI C63.4  
 FCC 47 CFR Part 15, Subpart B - Class A  
 ICES-003 – Class A

**EMC:** EN 61000-6-2 (Immunity)  
 EN 61000-6-4 (Emissions)  
 IEC 61000-4-2 (ESD)  
 IEC 61000-4-3 (RFI)  
 IEC 61000-4-4 (EFT)  
 IEC 61000-4-5 (Surge)  
 IEC 61000-4-6 (RF)  
 IEC 61000-4-8 (PF)  
 IEC 61000-4-11 (Voltage Dips)



# KEY SPECIFICATIONS (709FX-HV)

## Switch Properties

*Number of MAC Addresses:* 8,000  
*Aging Time:* Programmable  
*Latency Type:* 2.6  $\mu$ s  
*Switching Method:* Store & Forward

## Case Dimensions

*Height:* 4.3" / 10.8 cm  
*Width:* 3.2" / 8.2 cm  
*Depth:* 4.6" / 11.7 cm  
*Weight (max):* 1.6 lbs / 0.73 kg  
*Din-Rail mount:* 35mm

## Electrical

*Redundant Input Voltage:* 43-300VDC (Regulated)  
*Input Current (max):* 80mA max. @ 124VDC  
*Input Ripple:* Less than 100 mV  
*N-TRON Power Supply:* NTPS-48-2 (2 Amp@48VDC)  
*BTU/hr* 34 @ 124VDC



## Environmental

*Operating Temperature:* -40°C to 70°C  
*Storage Temperature:* -40°C to 85°C

*Operating Humidity:* 5% to 95%  
(Non Condensing)

*Operating Altitude* 0 to 10,000 ft.

## Shock and Vibration (bulkhead mounting)

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

## Reliability

*MTBF:* >2 Million Hours

## Warranty

3 years from the date of purchase.

## Connectors

10/100BaseTX: (8) RJ-45 Copper Ports  
100BaseFX: (1) SC or ST Duplex Ports

## Recommended Wiring Clearance:

*Front:* 4" (10.16cm)  
*Top:* 1" (2.54 cm)  
*Bottom:* 1" (2.54 cm)

## Network Media

*10BaseT:* >Cat3 Cable  
*100BaseTX:* >Cat5 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

### EMI, Immunity and Environmental Compliance

IEC 61850-3 Electric Utility Substations

IEEE 1613 Electric Utility Substations

EMC Directive 2004/108/EC

EN 61000-6-2 (Immunity)

NEMA TS 2 Traffic Control Equipment

### Regulatory Certifications

#### Product Safety

TUV/GS EN 60950-1

#### Emissions

FCC Title 47, Part 15, Radio Frequency Devices, Subpart B (Class B)

ANSI C63.4-2003

Industry Canada ICES-003 (Class B)

EN 61000-6-4 (Class B)

#### Immunity

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)

#### Other

GOST-R





## 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="3.2.10">708TX</Switch> <!-- If the minSwVer attribute is present, it
overrides the minSwVer attribute of
SystemConfiguration. -->

    <Switch>7506GX2</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 OR dhcp</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 or delete">      <!-- 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 OR user</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 OR no</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="keep or 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 OR no</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 OR locked</Mode>      <!-- Mode must be learning or locked -->

  <!-- Authorized entries -->
  <Authorized mode="keep or delete">    <!-- 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 OR no</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, Corporation 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, NEGLIGENCE, 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