N-Tron® Series

700/7000 Managed Industrial Ethernet Switch

Software Manual Firmware Version 3.9.1

Software Manual | January 2019

LP0985-A

COPYRIGHT

©2019 Red Lion Controls, Inc. All rights reserved. Red Lion, the Red Lion logo and N-Tron are registered trademarks of Red Lion Controls, Inc. All other company and product names are trademarks of their respective owners.

Red Lion Controls, Inc.

20 Willow Springs Circle

York, PA 17406

CONTACT INFORMATION

Inside US: +1 (877) 432-9908
Outside US: +1 (717) 767-6511

Website: www.redlion.net

Email: support@redlion.net

TABLE OF CONTENTS

PREFACE vii
Purpose vii
Audience vii
Trademark Acknowledgments vii
Conventions vii
FCC Statement vii
Industry Canada viii
Related Publications and Document Updates viii
Revision History ix
Disclaimer ix
1 INTRODUCTION & OVERVIEW 1-3
Mode of Operation Overview 1-3
Half Duplex 1-3
Full Duplex 1-3
Auto Negotiation 1-3
Advanced Features Overview 1-4
Port Mirroring 1-4
Port Trunking 1-4
Quality of Service 1-4
DHCP 1-4
DHCP Client 1-4
DHCP Relay Agent 1-5
DHCP Server 1-5
Virtual LAN 1-5
Rapid Spanning Tree Protocol 1-6
SNMP Traps 1-6
IGMP Snooping 1-7
N-Ring 1-7
N-Link 1-7
CIP 1-8
LLDP 1-8
Port Security - MAC Address Based 1-8
System Defaults 1-9
2 WEB SOFTWARE CONFIGURATION 2-15

Accessing the Web Software Interface 2-15
web management interface Home 2-16
web management interface Menu Structure 2-16
Administration 2-18
Administration > System 2-18
Administration > SNMP 2-21
Administration > Fault 2-23
Help > Administration 2-25
DHCP 2-26
DHCP > Server > Setup Profiles 2-26
DHCP > Server > Setup IP Maps 2-27
DHCP > Server > View Bindings 2-31
DHCP > Relay & Local > Setup 2-32
Help > DHCP 2-34
LLDP 2-35
LLDP > Configuration 2-35
LLDP > Ports 2-36
LLDP > Status 2-36
LLDP > Statistics 2-38
Help > LLDP 2-39
Ports 2-40
Ports > Configuration 2-40
Ports > MAC Security > Learning 2-42
Ports > MAC Security > Authorization List 2-43
Ports > MAC Security > Intruder Log 2-43
Ports > Mirroring 2-44
Ports > Trunking 2-45
Ports > QOS 2-46
Help > Ports 2-48
Statistics 2-49
Statistics > Ports > Statistics 2-49
Statistics > Ports > Utilization 2-50
Help > Statistics 2-51
VLAN 2-52
VLAN > Configuration 2-52
VLAN > Group Configuration 2-53

Help > VLAN 2-55
Bridging 2-56
Bridging > Aging Time 2-56
Bridging > Unicast Addresses 2-56
Bridging > Multicast Addresses 2-57
Bridging > Show MAC By Port 2-59
Help > Bridging 2-61
RSTP 2-62
RSTP > Configuration 2-62
Help > RSTP 2-64
IGMP 2-65
IGMP > Configuration 2-65
IGMP > Show Groups 2-67
IGMP > Show Routers 2-68
IGMP > RFilter Ports 2-68
Help > IGMP 2-70
N-View™ 2-71
N-View > Configuration 2-71
N-View > Ports 2-71
Help > N-View 2-72
N-Ring™ 2-73
N-Ring > Configuration 2-73
N-Ring > Advanced Configuration 2-75
N-Ring > Status 2-78
Help > N-Ring 2-81
N-Link™ 2-82
N-Link > Configuration 2-82
N-Link > Status 2-85
Help > N-Link 2-90
CIP™ 2-91
CIP > Configuration 2-91
CIP > Status 2-91
Help > CIP 2-93
Firmware/Config 2-94
Firmware/Config > TFTP 2-94
Help > Firmware/Config 2-95

Rate Limiting 2-96
Rate Limiting > Broadcast 2-96
Rate Limiting > Multicast 2-97
Help > Rate Limiting 2-98
User Management 2-99
User Management > Authorized Users 2-99
User Management > Add User 2-99
User Management > Remove User 2-100
Help > User Management 2-101
Logical View 2-102
700 Model 2-102
7018 Model 2-102
Configuration 2-103
Configuration > Save 2-103
Configuration > Reset 2-103
Configuration > Factory 2-103
Help 2-104
Help > Overview 2-104
Help > Other 2-105
Service and Support 2-106
Service > Information 2-106
Product > Support 2-106
3 USING THE COMMAND LINE INTERFACE 3-109
Console Connection 3-109
Telnet Connection 3-109
Entering Commands 3-110
Keywords and Arguments 3-110
Minimum Abbreviation 3-110
Getting Help on Commands 3-110
Showing Commands 3-110
Partial Keyword Lookup 3-110
Negating the Effect of Commands 3-111
Using Command History 3-111
Configuration Commands 3-111
Command Line Processing 3-111
CLI Command Groups 3-112

4 CLI GENERAL COMMANDS 4-113
? (Help) 4-113
Logout 4-114
Ping 4-114
Reset 4-115
Show System Information 4-116
5 CLI SYSTEM MANAGEMENT COMMANDS 5-117
Network System Error 5-117
sysip 5-118
system 5-119
6 CLI CONFIGURATION COMMANDS 6-121
Configuration Device Operations 6-121
Save or Reset Configuration Settings 6-122
Show, Add or Delete ARL Entires 6-123
Show or Set CIP™ Configuration 6-124
Show or Set IGMP Configuration 6-125
Show or Set Mirror Configuration 6-126
Show or Set N-Ring™ Configuration 6-127
Show or Set N-View™ Configuration 6-128
Show or Set Port Configuration 6-129
Show or Set SNMP Configuration 6-130
7 VLAN CONFIGURATION 7-131
Add/Delete VLANs 7-131
Add a VLAN 7-131
Delete a VLAN 7-135
VLAN Configuration Examples 7-137
Port - Based VLAN 7-137
Tagged VLAN (Tagged Only) 7-138
Tagged VLAN (All) 7-139
Hybrid VLAN 7-140
Overlapping VLAN 7-141
VLAN with Multicast Filtering 7-142

PREFACE

Purpose

This manual gives specific information on how to operate and use the management functions of the 700/7000 Managed Industrial Ethernet Switch.

Audience

The manual is intended for use by network users who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Trademark Acknowledgments

Red Lion Controls acknowledges and recognizes ownership of the following trademarked terms used in this document.

- Ethernet™ is a registered trademark of Xerox Corporation
- EtherNet/IP™and CIP™ are registered trademarks of ODVA

All other company and product names are trademarks of their respective owners.

Conventions

The following conventions are used throughout this manual to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

FCC Statement

This product complies with Part 15 of the FCC-A Rules.Operation is subject to the following conditions:

- This device may not cause harmful Interference
- 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 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

Related Publications and Document Updates

The publication details the features of the 700/7000 Managed Industrial Ethernet Switch, including the performance-related characteristics, and how to operate the switch.

This document is revised only at major releases and therefore, may not always contain the latest product information. As needed, Tech Notes and or other product documentation can be provided between major releases to describe any new information or document changes.

Also, as part of the 700/7000 Managed Industrial Ethernet Switch software, there is an online web-based help that describes all management related features.

The latest online version of this document and all product updates can be accessed at the Red Lion's N-Tron Series Support Knowledge Base page on the Red Lion web site at: www.redlion.net.

Red Lion appreciates all comments that will help us to improve our documentation quality. The user can submit comments through the Red Lion Customer Service. Simply email us at support@redlion.net.

Revision History

The following information lists the release history of this document.

Issue / Revision Date	Content Description
January 2019	This manual is valid for software release v3.9.1. First document release with software content integrated from 700 Models Managed Industrial Ethernet Switch User Manuals & Installation Guides and 7000 Models Managed Industrial Ethernet Switch User Manuals & Installation Guides.

Disclaimer

Portions of this document are intended solely as an outline of methodologies to be followed during the maintenance and operation of N-Tron® Series 700/7000 Managed Industrial Ethernet Switch equipment. It is not intended as a step-by-step guide or a complete set of all procedures necessary and sufficient to complete all operations.

While every effort has been made to ensure that this document is complete and accurate at the time of release, the information that it contains is subject to change. Red Lion is not responsible for any additions to or alterations of the original document. Industrial networks vary widely in their configurations, topologies, and traffic conditions. This document is intended as a general guide only. It has not been tested for all possible applications, and it may not be complete or accurate for some situations.

GETTING STARTED

This section provides an overview of the N-Tron® Series 700/7000 Managed Industrial Ethernet Switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the web management interface.

This section includes these chapters:

"Introduction & Overview" on page 3

"Web Software Configuration" on page 15

CHAPTER 1 INTRODUCTION & OVERVIEW

This chapter provides an overview of features for the switch. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this 700/7000 managed industrial Ethernet switch. However, there are many options that you should configure to maximize the 700/7000 managed industrial Ethernet switch performance for your particular network environment.

MODE OF OPERATION OVERVIEW

Each port on the switch can be configured into different modes of operation as shown in Table 1.

Table 1: Port Operating Modes

Copper Ports	100Base Fiber Ports	1000Base Copper/Fiber Ports
700/7000 Models		7000 Models
Half Duplex	Full Duplex	Full Duplex
Full Duplex		
Auto Negotiation		

HALF DUPLEX

In half duplex mode, the CSMA/CD media access method is the means by which two or more devices 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 devices 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.

Advanced Features Overview

The switch provides a wide range of advanced performance enhancing features. Some of the management features are briefly described in the following paragraphs.

Port Mirroring

The switch can unobtrusively mirror traffic from any port to a dedicated destination port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking

Ports can be combined into an aggregate connection called a trunk which acts as a single link between two switches. The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail.

Quality of Service

Quality of service (QoS) refers to resource reservation control mechanisms. Quality of service provides the ability to assign different priorities 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 rates 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. In the presence of heavy network traffic, low priority frames may be discarded as they pass through a congested switch.

These QOS methods may be available depending on the switch model:

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

To assign a high priority to all frames received on a port, enable Force High Priority and set the port's default Port Priority to 7.

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's allocate network addresses and deliver configuration parameters to dynamically configured hosts. DHCP is specified by RFC 2131. The switch can be configured to be a DHCP client. 700/700 switches can be configured to be a DHCP server, a DHCP relay agent, or both. Refer to DHCP on page 26 in Chapter 2 for configuration information.

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

A DHCP Relay Agent (Option 82) enables communication between DHCP clients and servers 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

The DHCP Server allows DHCP clients to automatically obtain an IP assignment from the server. 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).

Virtual LAN

The switch supports Virtual Local Area Networks (VLAN). By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to physically change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

The switch provides support for setting up tagged VLANs. A port may belong to any number of VLANs. The VLAN membership of a device connected to a port 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 to be in overlapping VLANs**. Switches forward unicast, multicast, and broadcast traffic only on LAN segments that service 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. By default, all ports belong to only the default VLAN. This allows the switch to operate as a ‘normal’ switch when added into a network of other switches that are also using default VLAN settings.

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 user to set up the switch to support devices on the network that do not support VLAN Tagged packets. The user 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 700 models of the switch also have 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 websites' technical documents.

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.

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.

RSTP dynamically reconfigures bridge (switch) ports in a network of arbitrarily connected bridges. This network may include redundant connections. Some ports are reconfigured to forward traffic and others to block traffic. RSTP builds a loop-free network (a spanning tree) from the forwarding ports thus preventing network storms. RSTP also provides redundancy by dynamically reconfigures ports as connections or bridges fail or are added to the network.

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 inter-operates 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 switch supports up to 5 SNMP Trap devices to which SNMP Traps will be sent. The switch supports five standard traps; Link Up, Authentication Error, Link Down, Cold Start and Warm Start. SNMP Traps will be sent to all the devices configured on the switch (when the corresponding trap is enabled) if an authentication error occurs, a port Link goes up or down, when the switch first powers up and when the switch is reset.

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: "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 700 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 700 Series supports v1 and v2.

N-Ring

Red Lion's proprietary N-Ring technology offers expanded ring topology size, detailed fault diagnostics, and a standard healing time of 30ms.

N-Ring™ is enabled by default, and the switch is *Plug and Play* for N-Ring except that initially a switch must be configured as the N-Ring Manager for a given N-Ring. Subsequently, N-Ring operates dynamically upon each power up. 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

Red Lion's proprietary N-Link technology provides redundant coupling of an N-Ring topology to one or more other topologies, usually other N-Rings.

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 between topologies 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 between topologies. 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.

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 a network by only permitting traffic from devices with authorized MAC addresses. Authorized MAC addresses can be dynamically learned or manually entered.

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. Traffic from a non-authorized MAC address will be discarded and the MAC address will be shown on the intruder log.

System Defaults

The switch's basic system defaults are provided in the table below To reset the switch to the default settings, refer to the section on Configuration on page 103.

Function	Parameter		Default
Console Port Connection	Baud Rate		115200 bps (not configurable)
	Data bits		8 (not configurable)
	Stop bits		1 (not configurable)
	Parity		none (not configurable)
System Configuration	IP Configuration		Static
	IP Address		192.168.1.201
	Subnet Mask		255.255.255.0
	Gateway		192.168.1.1
	Name		N-TRON Switch *xx:xx:xx* (where *xx:xx:xx* is the last three octets of the MAC Address)
	Contact		N-TRON Admin
	Location		Mobile, AL
SNMP Configuration	Status		Enabled
	Read-Only Community Name		"public"
	Read-Write Community Name		"private"
	Trap Community Name		"public"
	V3 Username		"initial"
	V3 Privacy Password		"privpass"
	V3 Authentication Password		"authpass"
	V3 Authentication Protocol		MD5
	Trap Version		1
	IP Address - Trap Stations 1-5		<not configured>
	Send Trap Notification	Power Supply	No
		Cold Start	Yes
		Authentication	Yes
		Warm Start	Yes
		Link Status	Yes

Function	Parameter		Default
Fault Configuration	Contact Operation (Meaning)		Close on Fault
	Signal	Power V_1	Disabled
		Power V_2	Disabled
		N-Link Fault	Enabled
		Port Usage Fault	Enabled
		N-Ring Broken	Enabled
		N-Ring Partial Break (Low)	Enabled
		N-Ring Partial Break (High)	Enabled
		N-Ring Multiple Managers	Enabled
Slots Configuration	N-Tron 7900 Only	Slot A	9006TX
		Slot B	9006TX
		Slot C	9006TX
		Slot D	9006TX
DHCP Configuration	Server	Status	Disabled
		Allow Broadcast	Enabled
		Delay Broadcast	500 (milliseconds)
		ID	<Defaults to the switch name>
		Network Profile Domain Name	localdomain.com
		Network Profile Lease Time	28 Days
	Relay Agent & Local IP	Relay Status	Disabled
		Remote ID Type	IP Address
		Server 1-4 IP	None
		Port Relay Status	Disabled <All ports>
LLDP Configuration	Mode		Disabled
	Transmit Interval		30 (seconds)
	Transmit Hold Multiplier		4
	Re-Initialization Delay		2 (seconds)
	Notification Interval		5 (seconds)
	Port	Transmit	Yes <All ports>
		Receive	Yes <All ports>
		Allow Management Data	Yes <All ports>
		Allow Notification	No <All ports>

Function	Parameter		Default
Ports Configuration	Admin Status		Enabled
	Speed and Duplex	10/100Mb Copper Ports	Auto-Negotiate
		100Mb Fiber Ports	100/Full
		GigaBit (Copper or Fiber) Ports*	1000/Full
			Auto for 7506GX2 Port GB2
	Cross Over	10/100Mb Copper Ports	Auto
		100Mb Fiber Ports	No (not configurable)
		GigaBit (Copper or Fiber) Ports	Auto
	Flow Control		Disabled
	PVID		1
	Usage Alarm Low		0 (%)
	Usage Alarm High		100 (%)
MAC Learning Configuration	Current Mode		Learning
	Port Secured		No <All ports>
Port Mirroring Configuration	Mirror Status		Disabled
	Destination Port		<First port>
	Mirrored Data Only		Disabled
	Source Ports - Tx		None
	Source Ports - Rx		None
Port Trunking	Trunk Status		Disabled
	Trunk Ports	FX1-FX2	If present
		T3-T4	N-Tron 7506GX2
		A3-A4	N-Tron 7900
		<Last two copper ports>	All other models
QOS Configuration	Include DSCP		Enabled <All ports>
	Include 802.1p		Enabled <All ports>
	Force High Priority		Disabled <All ports>
	Port Priority		1 <All ports>

Function	Parameter		Default
VLAN Configuration	Replace VID Tag with Default Port VID		No
	Perform Ingress Filtering		No
	Discard Non-Tagged for Ports		None
	Remove Ports from Default VLAN When Added to Other VLANS		Yes
	VLAN Groups	VLAN ID	1
		VLAN Name	Default VLAN
		Group Members	<All ports>
		Untag on Egress	<All ports>
		Allow Mgmt	Yes
Bridging Configuration	Aging Time		20 (seconds)
	Active IP Probe Status		Disabled
RSTP Bridge Configuration	Status		Fast (RSTP enabled)
	Hello Time		1 (second)
	Forward Delay		13 (seconds)
	Max Age		16 (seconds)
	Priority		32768
	VLAN		1
IGMP Configuration	IGMP Status		Enabled
	Query Mode		Auto
	Router Mode		Auto
	Remove Unused Groups		Enabled
	Manual Router Ports		None <No ports selected>
	RFilter		Enabled <All ports>
N-View Configuration	N-View Status		Enabled
	N-View Internal		5 (seconds)
	Ports	Multicast On Port?	Yes <All ports>
		Send MIB Stats?	Yes <All ports>

Function	Parameter			Default
N-Ring Configuration	N-Ring Mode			Auto Member
	Aging Time			20 (seconds)
	N-Ring Port Pairs	Fixed Port Models		
			Port Pair 1	First two ports
			Port Pair 2	If they exist, first two fiber ports
				If no fiber ports exist, then in order of precedence: 1. Last two 10/100/1000 Mb copper ports. if they exist or 2. Last two 10/100 Mb copper ports
			Port Pair 3	If they exist, first two SFP Gigabit ports
		Modular Models		
			Port Pair per Module	First two ports on each model
	Auto Member Mode	N-Ring Ports		Auto detect N-Ring ports based on port pairs
		VLAND ID		Auto detect
		Tagging		Auto detect
		Advanced	Keep-Alive Timeout	31 (seconds)
	Manager Mode	N-Ring Ports		<First available port pair per model by priority: Priority 1: Gigabit, Priority 2: Fiber, Priority 3: Copper
		VLAN ID		3333
		Tagging		Tagged
		Advanced	Self Health Packet Interval	10 (milliseconds)
			Maximum Missed Packets	2
			Sign-On Delay	1000 (milliseconds)
			Sign-On Match Packets	3
			Sign-On Interval	3000 (milliseconds)
			Sign-On Info Spacing Multiplier	5 (milliseconds)

Function	Parameter		Default	
			Sign-On Info Retry Timeout	1500 (milliseconds
			Delay Before Re-entering Broken State	3000 (milliseconds)
N-Link Configuration	N-Link Mode		Auto Configure	
	Auto Configure Mode	Default Coupler Port	<Fourth port>	E.g., TX4/P4
	Master Mode	Control Port	<Third port>	E.g., TX3/P3
		Primary Coupler Port	<Fourth port>	E.g., TX4/P4
		Partner Port	Auto detect	
	Slave Mode	Control Port	Auto detect	
		Primary Coupler Port	<Fourth port>	E.g., TX4/P4
		Partner Port	Auto detect	
CIP Configuration	CIP Status			Enabled
	Minimum Multicast RPI (RpiClass1)			300 (milliseconds)
	Minimum Unicast RPI (RpiClass3)			300 (milliseconds)
Rate Limiting Configuration	Broadcast	Pass Rate	3%	100 Mb ports
			1%	1000 Mb (1 GB) ports
	Multicast	Pass Rate	100%	<All ports>
User Configuration	Administrator	User Name		admin
		Password		admin
		Access Level		Admin

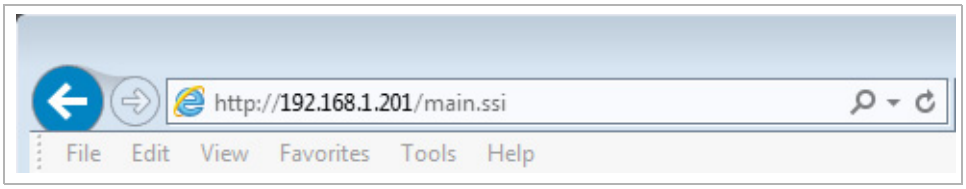
* Gigabit SFPs support 1000 Mb speed only. Copper SFPs will auto-negotiate per the IEEE specification but they will only advertise 1000 Mb with full duplex.

CHAPTER 2 WEB SOFTWARE CONFIGURATION

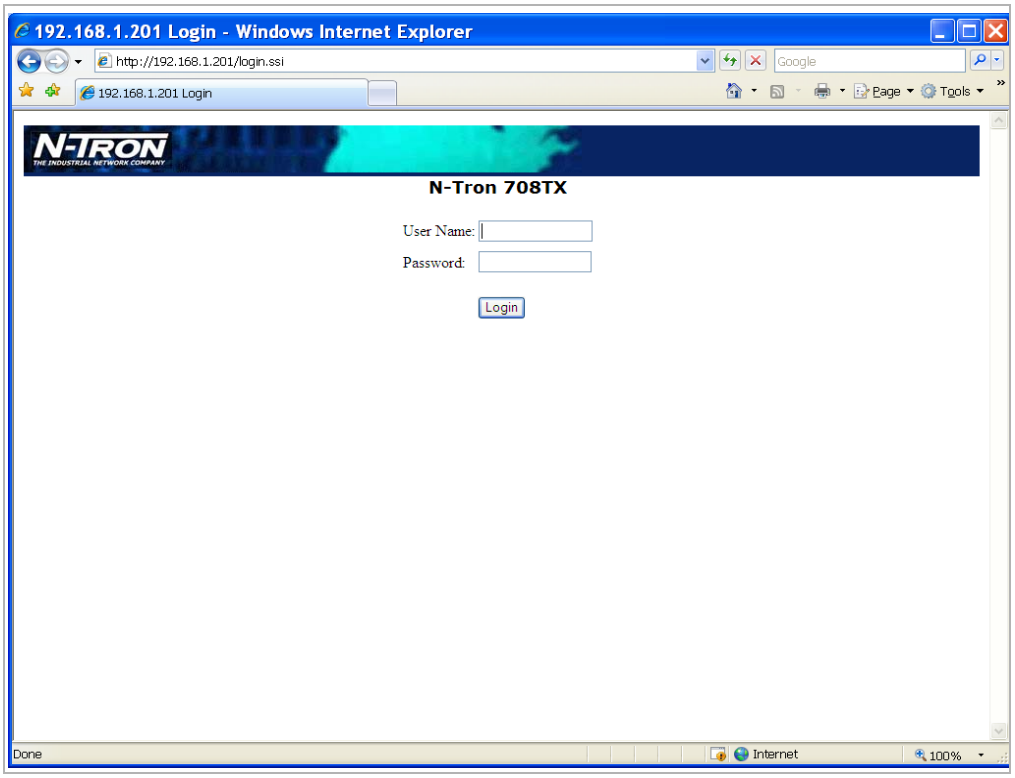
This chapter includes information on connecting to the switch and basic configuration procedures.

ACCESSING THE WEB SOFTWARE INTERFACE

Launch a web browser and enter the IP address of the switch into the address bar.



The following login screen will appear:

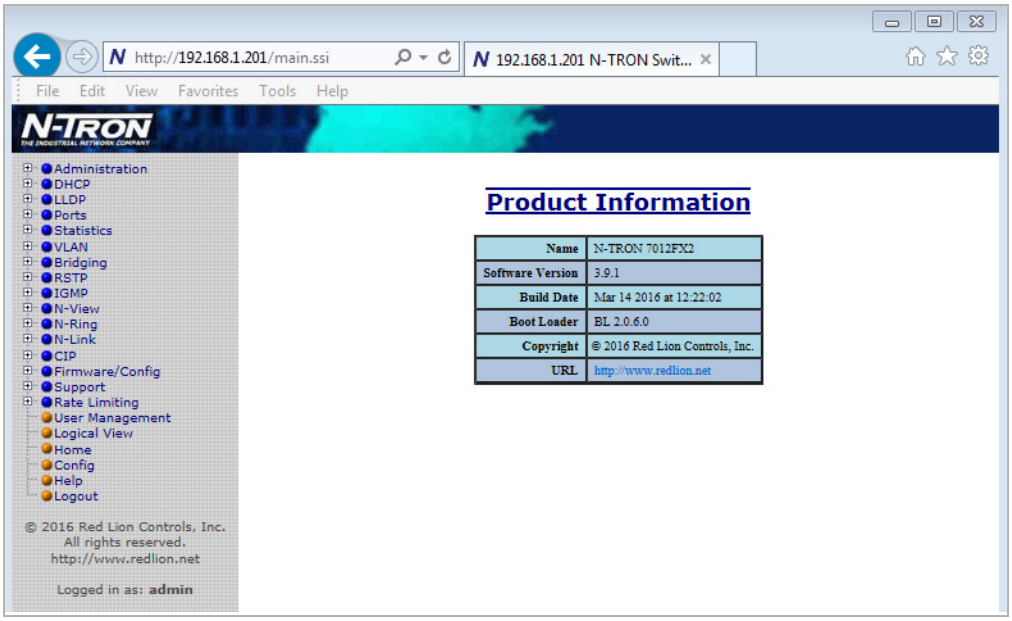


For the User Name, enter: **admin** (all lowercase).

For the password, enter: **admin** (all lowercase).

Note: For security purposes, it is recommended that the default password be changed according to your internal policies. Login credentials can be changed on the User Management page.

Upon successfully logging in, depending on the switch model used, a screen similar to the one below will appear:

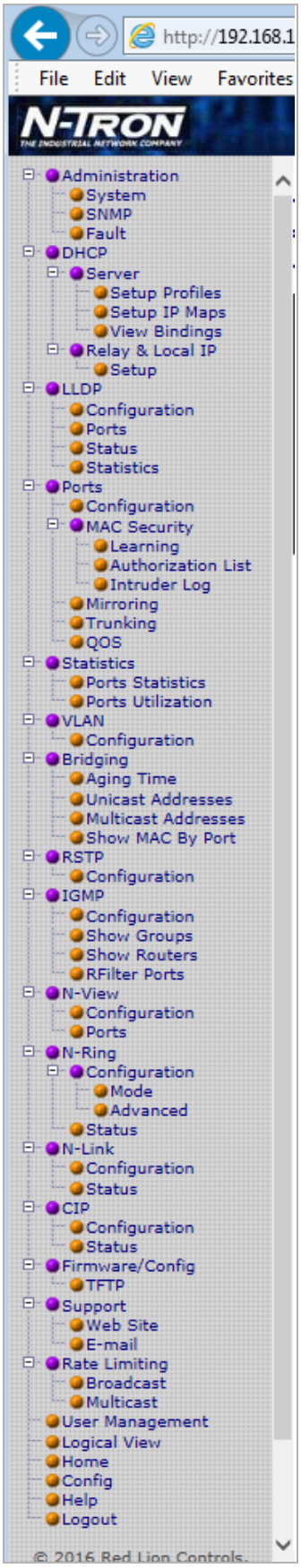


WEB MANAGEMENT INTERFACE HOME

When the user first logs onto a 700/7000 model switch the default home page is displayed. On the left hand side of the screen there is a list of configurable settings. In the center of the main home page the user can see some basic information like what firmware revision the switch is running. The firmware can be upgraded using TFTP.

WEB MANAGEMENT INTERFACE MENU STRUCTURE

The web management interface structure (shown on the web management interface home page left side) in its fully expanded view of the configurable features is shown below. The pages opened by each individual selection are described in the rest of this section. In most of the descriptions, only the selected configurable feature is shown.


http://192.168.1
File Edit View Favorites
N-TRON
Administration
System
SNMP
Fault
DHCP
Server
Setup Profiles
Setup IP Maps
View Bindings
Relay & Local IP
Setup
LLDP
Configuration
Ports
Status
Statistics
Ports
Configuration
MAC Security
Learning
Authorization List
Intruder Log
Mirroring
Trunking
QOS
Statistics
Ports Statistics
Ports Utilization
VLAN
Configuration
Bridging
Aging Time
Unicast Addresses
Multicast Addresses
Show MAC By Port
RSTP
Configuration
IGMP
Configuration
Show Groups
Show Routers
RFilter Ports
N-View
Configuration
Ports
N-Ring
Configuration
Mode
Advanced
Status
N-Link
Configuration
Status
CIP
Configuration
Status
Firmware/Config
TFTP
Support
Web Site
E-mail
Rate Limiting
Broadcast
Multicast
User Management
Logical View
Home
Config
Help
Logout
© 2016 Red Lion Controls

ADMINISTRATION

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 switch.

Subnet Mask

Contains the current Subnet Mask of the switch.

Gateway

Contains the current Gateway of the switch.

MAC Address

MAC Address of the switch.

System Up Time

This parameter represents the total time that has elapsed since the switch was turned ON or RESET.

Name

The name assigned to the switch, which can have alphanumeric and special characters '#', '_', '-', and ':'. This name may be used as the DHCP client ID.

Contact

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

Location

The physical location of the switch.

Temperature*

The temperature measured by the on board temperature sensor of the switch.

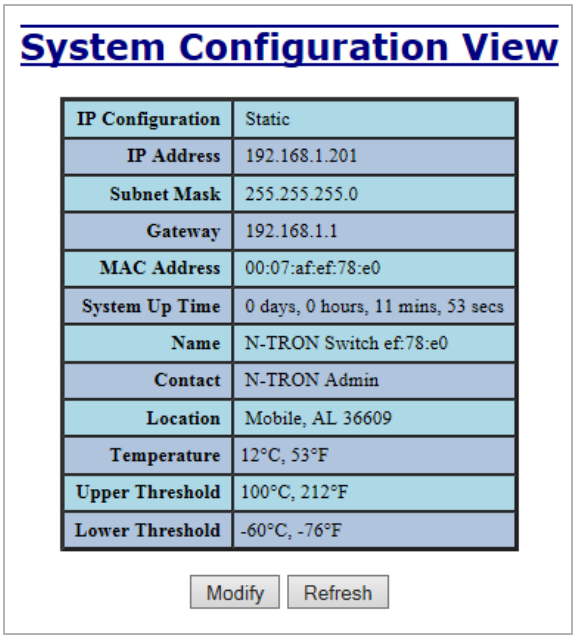
Upper Threshold*

The upper temperature threshold setting of the switch. A temperature measured above this value will cause a fault.

Lower Threshold*

The lower temperature threshold setting of the switch. A temperature measured below this value will cause a fault.

* The following models have an on board temperature sensor and display values on the System Configuration View screen: 7010TX, 7012FX2, 7026TX, 709FX, 710FX2, 711FX3, 712FX4, 714FX6, 7506GX2, and 7900CPU.



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

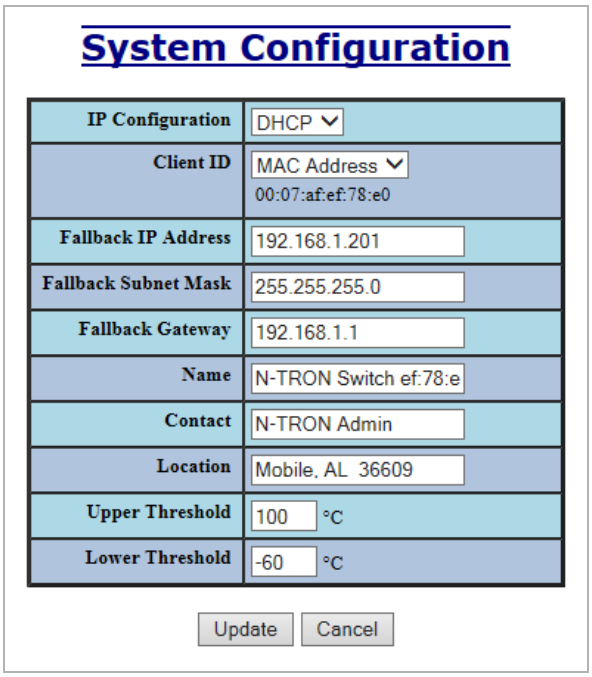
Contains the configured Fallback IP Address of the switch.

Fallback Subnet Mask

Contains the configured Fallback Subnet Mask of the switch.

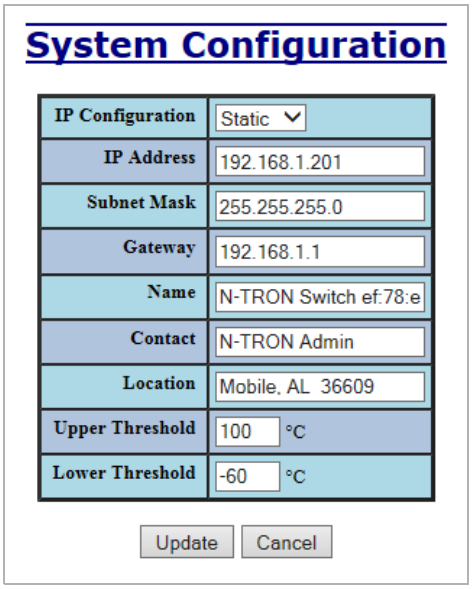
Fallback Gateway

Contains the configured Fallback Gateway of the switch.

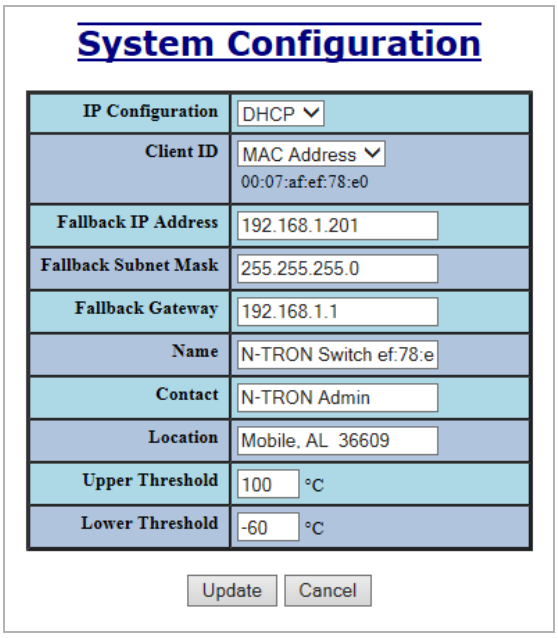


By selecting Modify, you will be able to change the switch's IP Configuration, Client ID, IP Address, Subnet Mask, Gateway, Name, Contact information, and the Location of the switch through the web management interface features, depending on the IP Configuration. It is recommended to change the TCP/IP 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

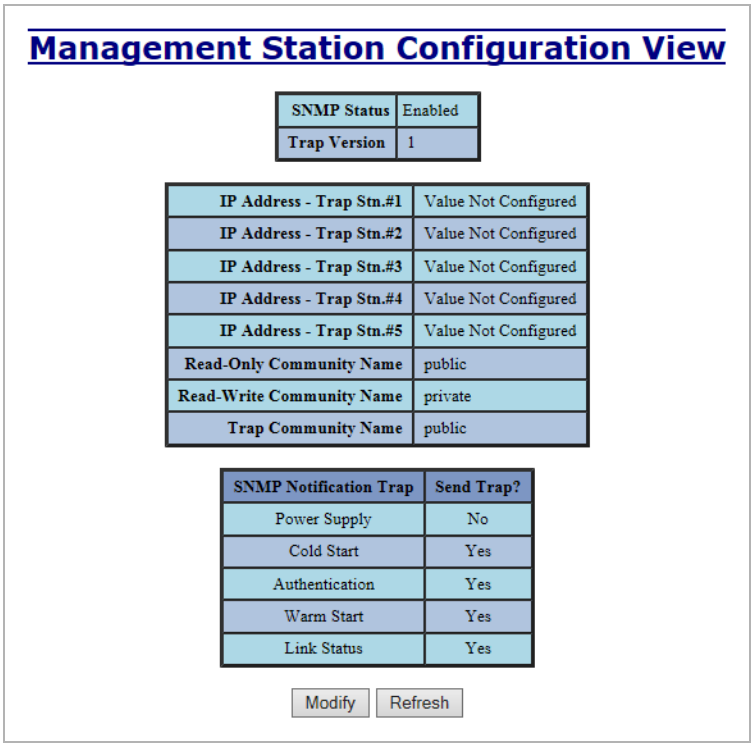


If the IP Configuration mode is set to DHCP and the Fallback IP address is changed from the default IP address, then the switch will use the Fallback addresses if the IP configuration isn't received from a DHCP server in 2 minutes after initial boot. If Fallback address is used, DHCP client will stop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



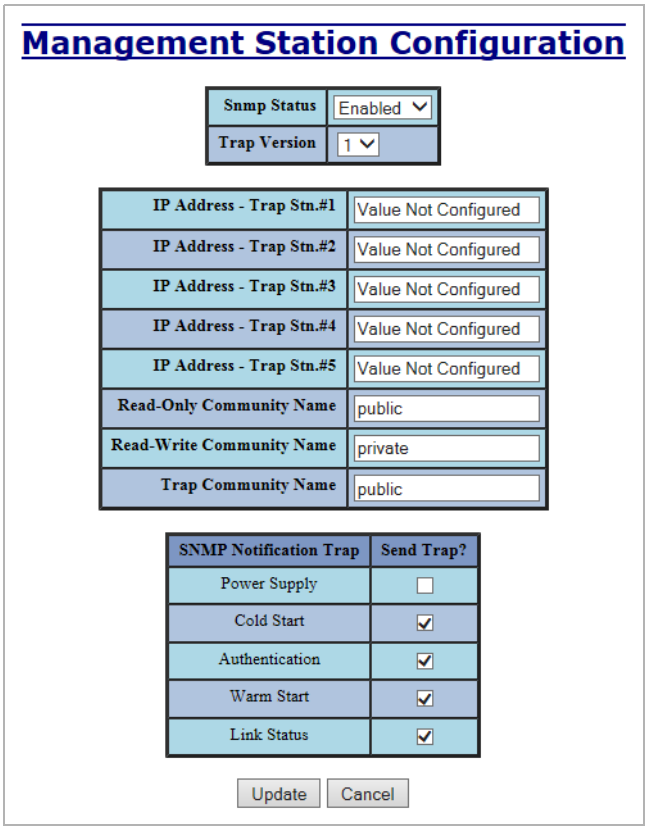
ADMINISTRATION > SNMP

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



By selecting Modify, 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

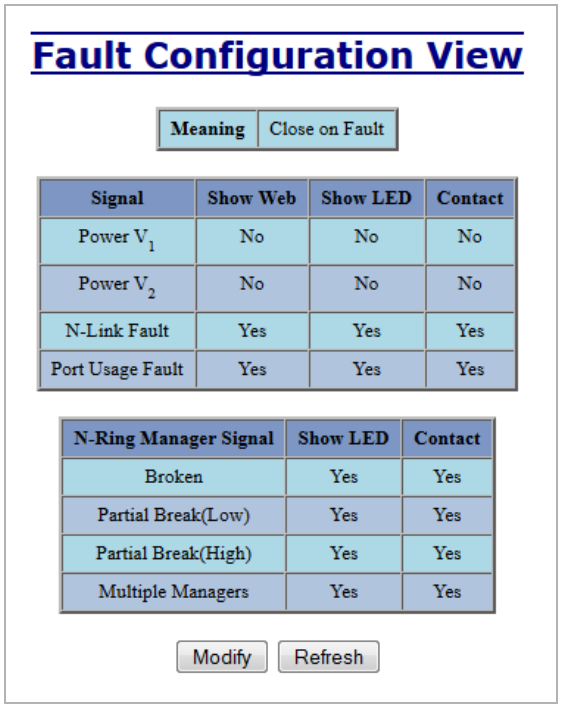
sent the corresponding notification trap. To restore a Trap to “Value Not Configured”, enter ‘0.0.0.0’



ADMINISTRATION > FAULT

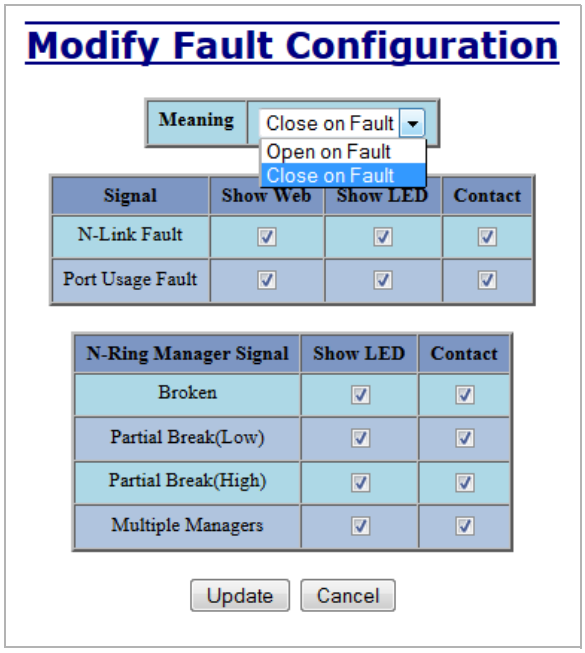
The Fault tab under the Administration category provides configurable selections indicating the way to notify when a Power, N-Ring™ Manager, N-Link fault, or Port Usage Fault occurs. The notification may consist of any combination of the options: Show Web, Show LED, and Contact. Power signal faults consist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

Note: Some switch models do not have a fault contact.

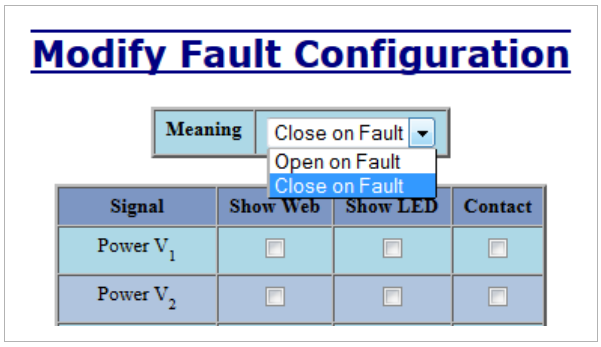


Note: V_1 and V_2 Power Faults are disabled in factory defaults.

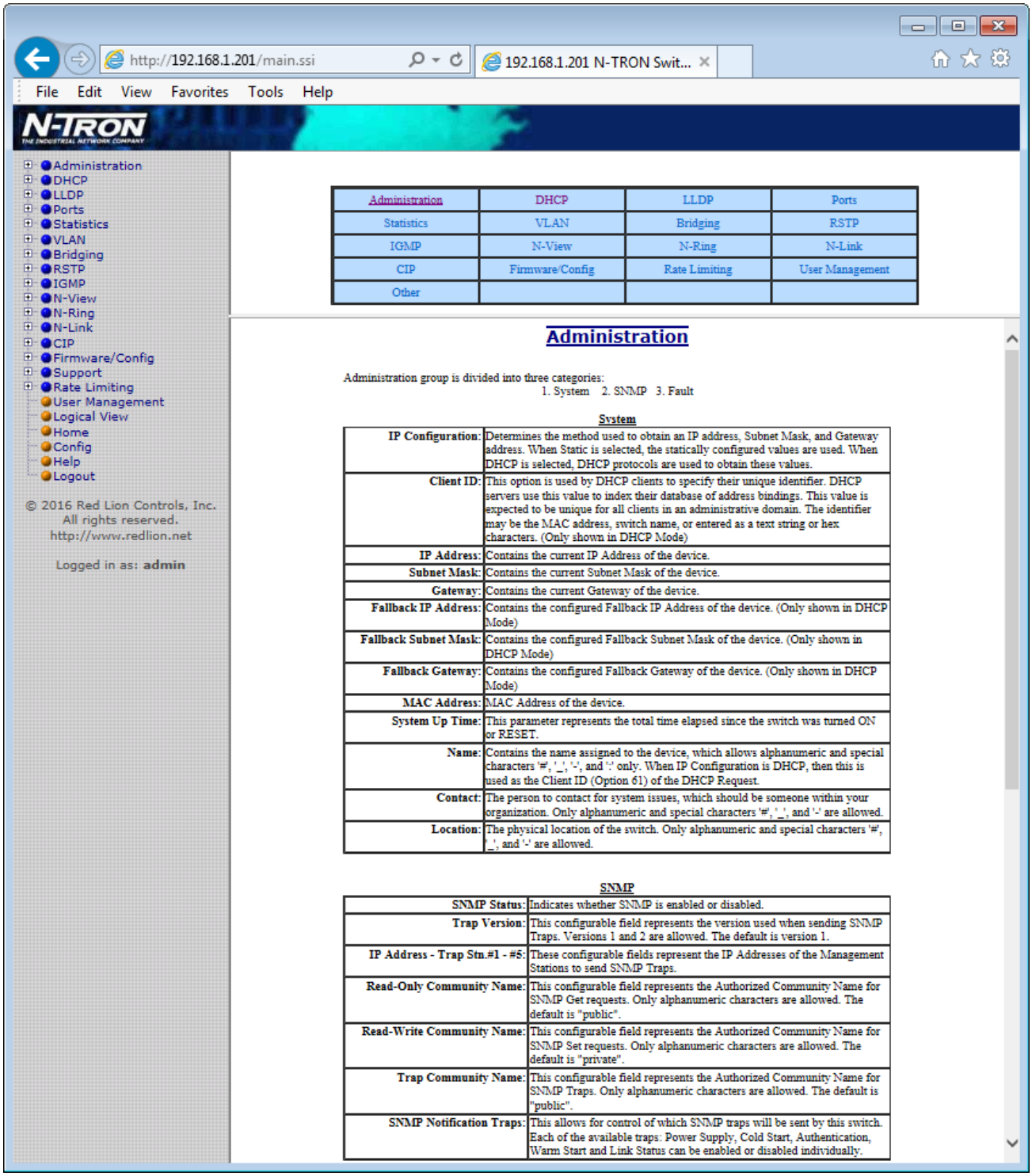
By selecting Modify, the user will see a list of configurable fields for the Fault configuration. The fault relay contact can be configured to open on fault or to close on fault, with the latter being the default. Once these fields are filled in to meet the needs of the user's network, the changes may be updated by clicking the Update button at the bottom of the page.



If a low voltage DC power supply is installed, these additional choices appear:



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



Administration

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

System

IP Configuration:	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.
Client ID:	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)
IP Address:	Contains the current IP Address of the device.
Subnet Mask:	Contains the current Subnet Mask of the device.
Gateway:	Contains the current Gateway of the device.
Fallback IP Address:	Contains the configured Fallback IP Address of the device. (Only shown in DHCP Mode)
Fallback Subnet Mask:	Contains the configured Fallback Subnet Mask of the device. (Only shown in DHCP Mode)
Fallback Gateway:	Contains the configured Fallback Gateway of the device. (Only shown in DHCP Mode)
MAC Address:	MAC Address of the device.
System Up Time:	This parameter represents the total time elapsed since the switch was turned ON or RESET.
Name:	Contains the name assigned to the device, which allows alphanumeric and special characters '#', '_', '-', and ':' only. When IP Configuration is DHCP, then this is used as the Client ID (Option 61) of the DHCP Request.
Contact:	The person to contact for system issues, which should be someone within your organization. Only alphanumeric and special characters '#', '_', and '-' are allowed.
Location:	The physical location of the switch. Only alphanumeric and special characters '#', '_', and '-' are allowed.

SNMP

SNMP Status:	Indicates whether SNMP is enabled or disabled.
Trap Version:	This configurable field represents the version used when sending SNMP Traps. Versions 1 and 2 are allowed. The default is version 1.
IP Address - Trap Stn.#1 - #5:	These configurable fields represent the IP Addresses of the Management Stations to send SNMP Traps.
Read-Only Community Name:	This configurable field represents the Authorized Community Name for SNMP Get requests. Only alphanumeric characters are allowed. The default is "public".
Read-Write Community Name:	This configurable field represents the Authorized Community Name for SNMP Set requests. Only alphanumeric characters are allowed. The default is "private".
Trap Community Name:	This configurable field represents the Authorized Community Name for SNMP Traps. Only alphanumeric characters are allowed. The default is "public".
SNMP Notification Traps:	This allows for control of which SNMP traps will be sent by this switch. Each of the available traps: Power Supply, Cold Start, Authentication, Warm Start and Link Status can be enabled or disabled individually.

DHCP

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.

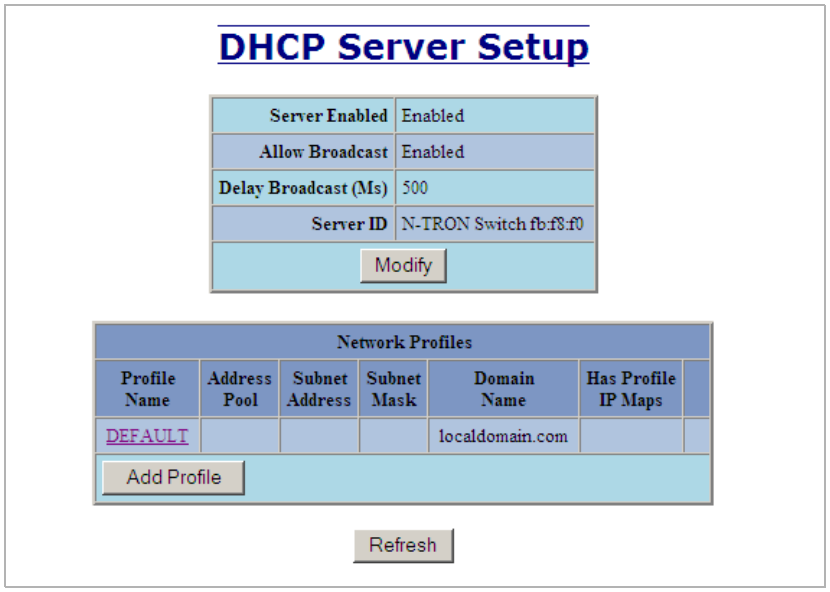
Subnet Address
The most restrictive subnet address calculated from the address pool range.

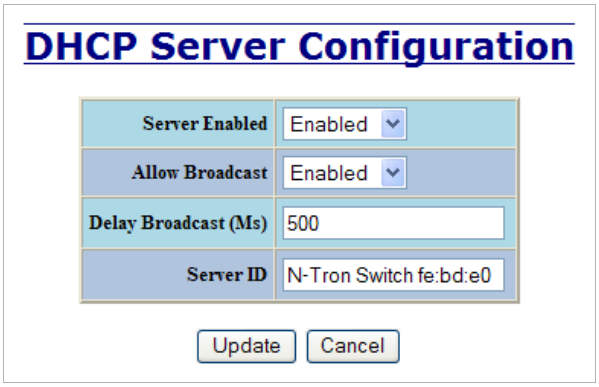
Subnet Mask
The most restrictive subnet mask calculated from the address pool range.

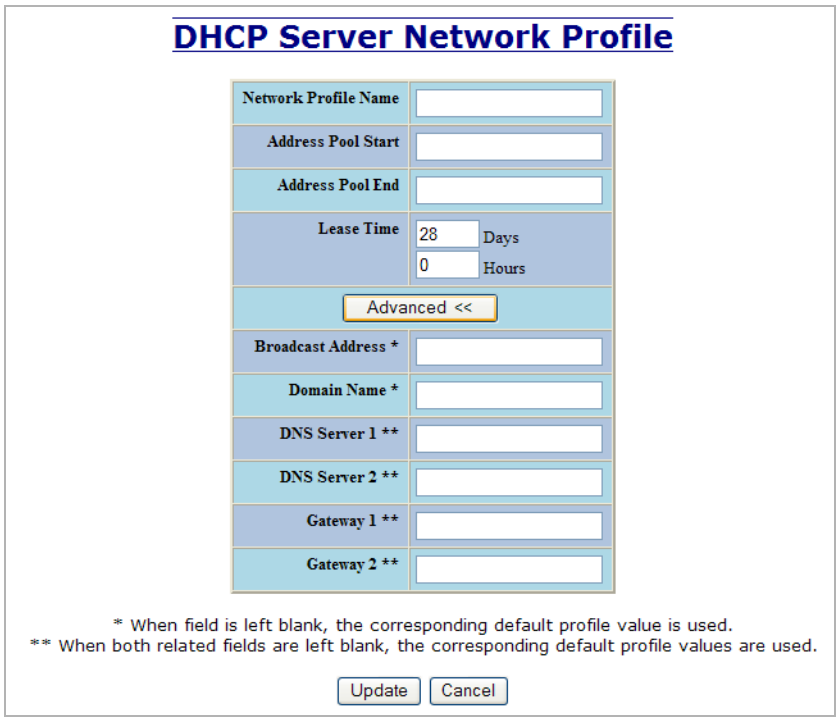
Domain Name
The domain name to be presented to the client.

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.

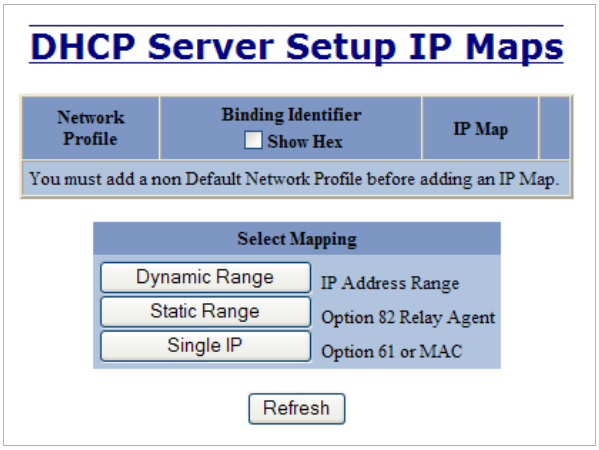






DHCP > Server > Setup IP Maps

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.

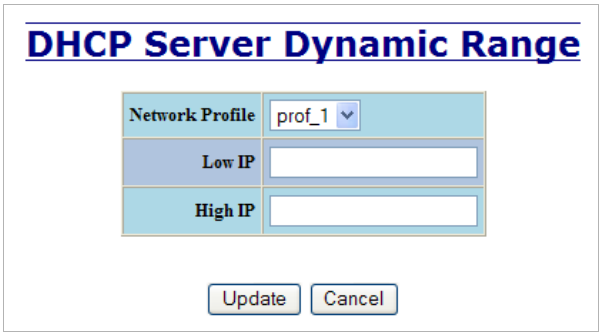


The Dynamic Range type of mapping is used to create a range of dynamic IP addresses for requesting clients. The following information is required:

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

Low IP
The starting IP address of a range.

High IP
The ending IP address of a range.



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

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

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

Relay Agent Type
Should be set to N-Tron.

Switch Model
List of N-Tron models that support this feature.

Remote ID
A unique identifier that designates the N-Tron relay agent switch.

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

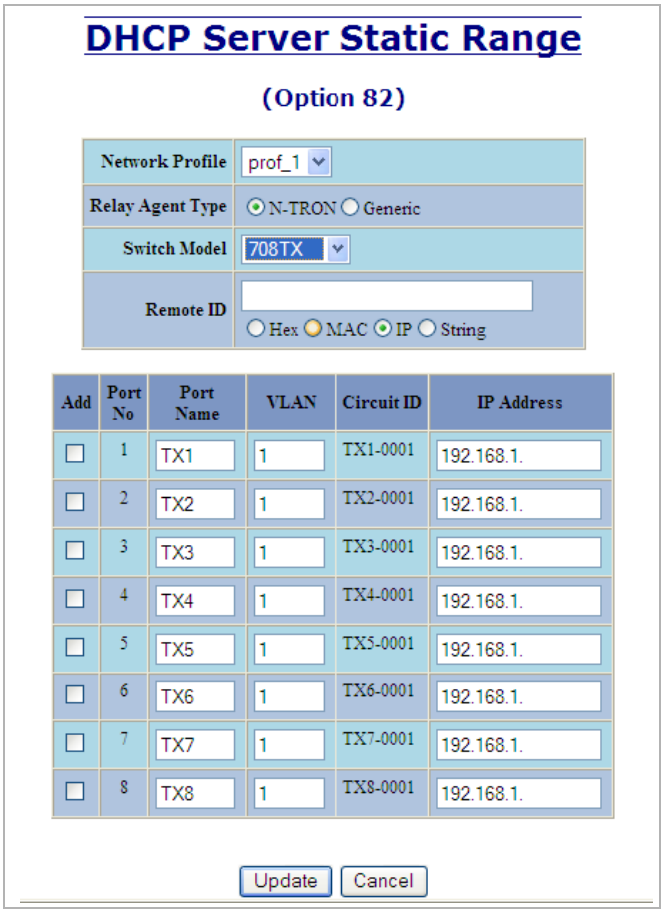
Port No
The actual port number.

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



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.

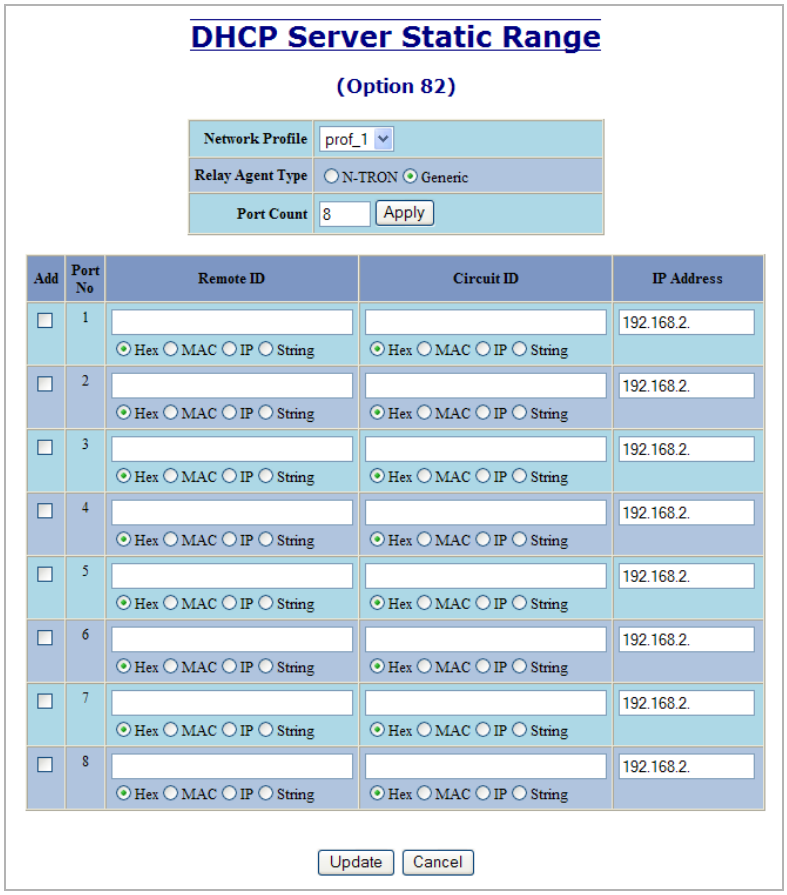
Add
Check box used to add an IP map for the corresponding port.

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.



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

Network Profile

An existing network profile to which the IP map applies.

IP

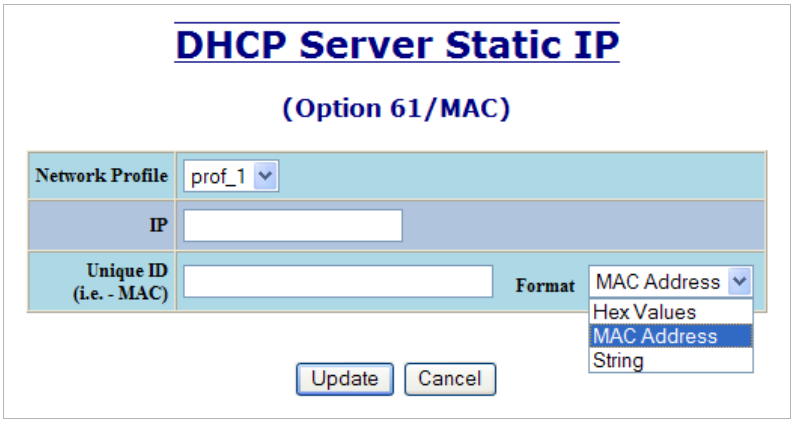
The static IP address to offer to a client.

Unique ID

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

Format

Designates how the Unique ID is interpreted.



DHCP > Server > View Bindings

The View Bindings tab lists the bindings of physical switch's 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.

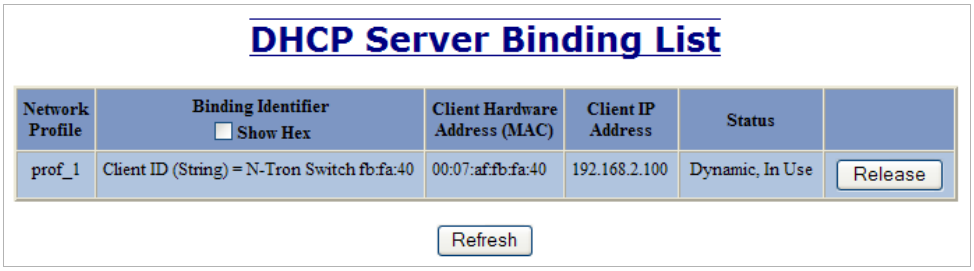
Client Hardware Address (MAC)
The client's MAC address.

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

Status
Indicates the current status of the binding entry.

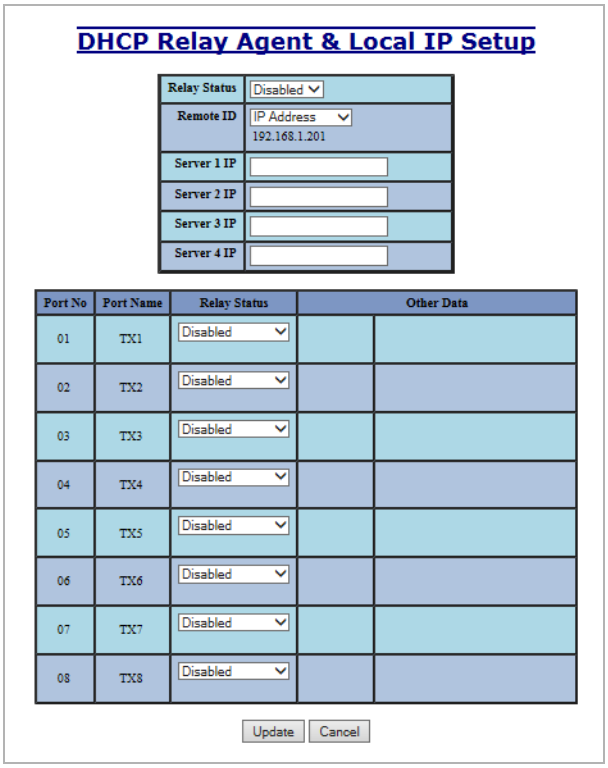
Release
Removes the corresponding binding.

Warning: By releasing an IP address, it is possible to end up with two physical switches with the same IP address which may cause network disruption to that IP address.



DHCP > Relay & Local > Setup

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



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

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.

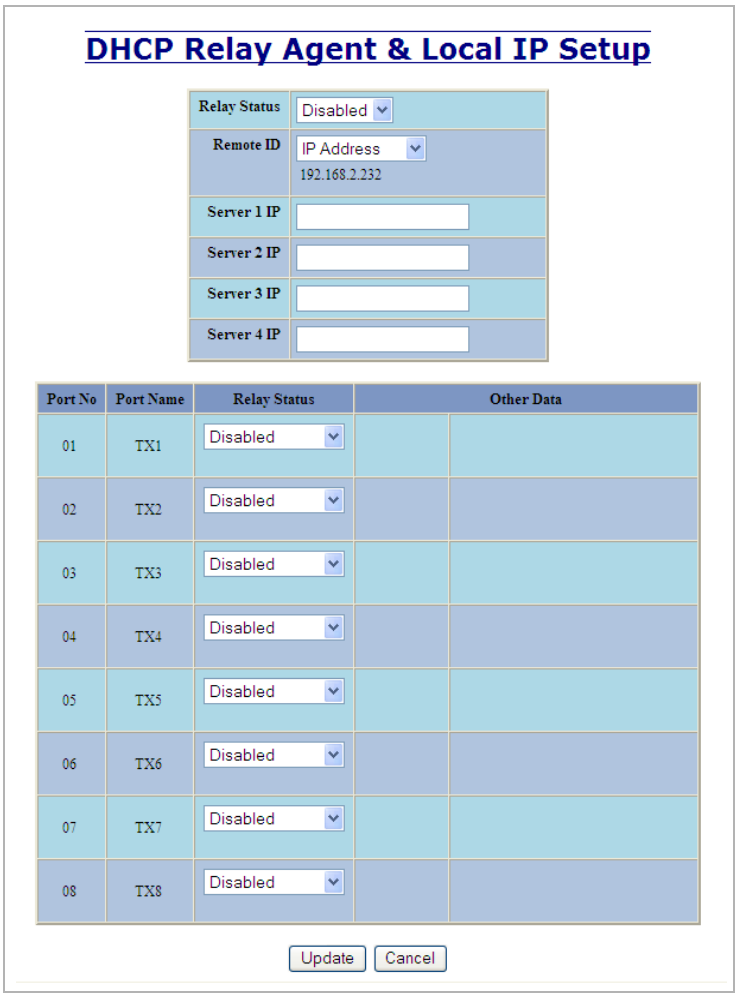
Relay Status

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

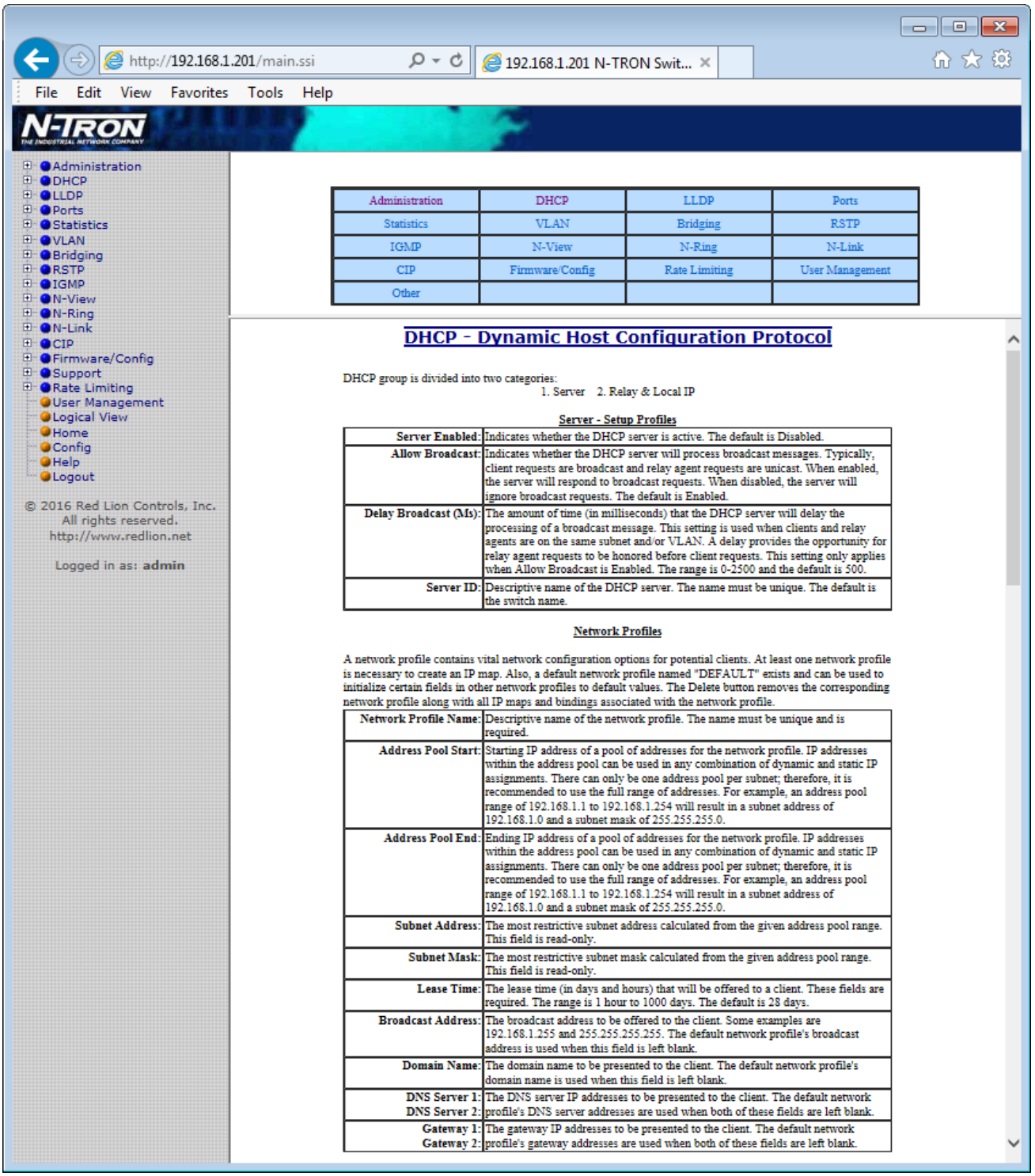
- Disabled - The port will function without relay agent processing.
- Enabled - The port will relay DHCP client-originated broadcast packets to the DHCP servers.
- Assign Local IP - The port will not relay DHCP client-originated broadcast packets. Instead the relay agent will offer the port's locally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



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



LLDP

LLDP > Configuration

Mode:

Enables or Disables LLDP on the Switch.

Default: Disabled

Transmit Interval:

Specifies the interval at which LLDP frames are transmitted.

Default = 30 seconds.

Transmit Hold Multiplier:

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

Default = 4.

Re-Initialization Delay:

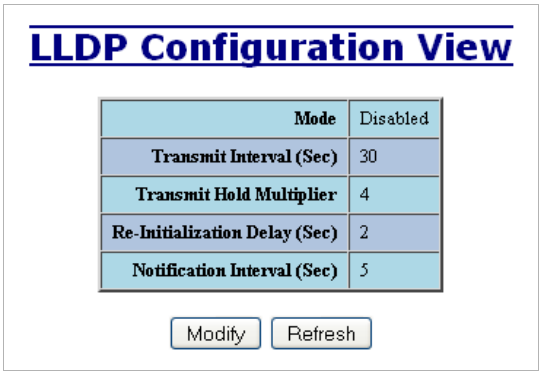
Specifies a minimum time an LLDP port will wait before re-initializing after setting the port to disable followed by setting a port to Tx-Only or Tx/Rx. This prevents excessive Notifications if someone toggles between Disabled and Enabled on LLDP Port settings.

Default = 2 Seconds.

Notification Interval

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

Default = 5 Seconds



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

LLDP > Ports Ports View

Port Name

Descriptive name of the port on the local switch.

Transmit

Enables or Disables LLDP Transmission on the switch.

Receive

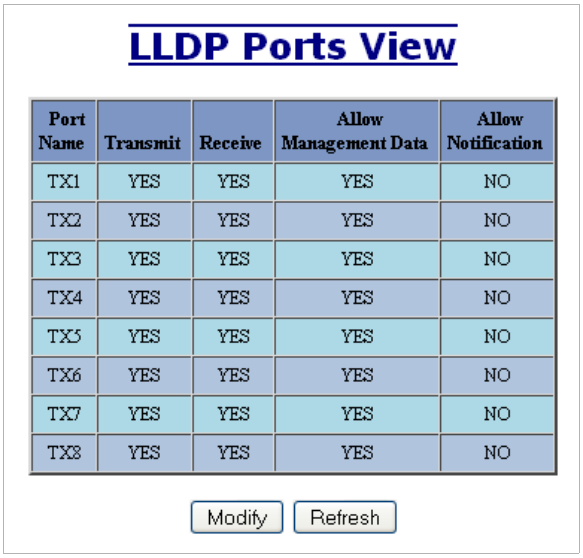
Enables or Disables Receiving of LLDP Frames from neighbor switches.

Allow Management Data

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

Allow Notifications

Notifications are transmitted when local or remote data changes.



LLDP > 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

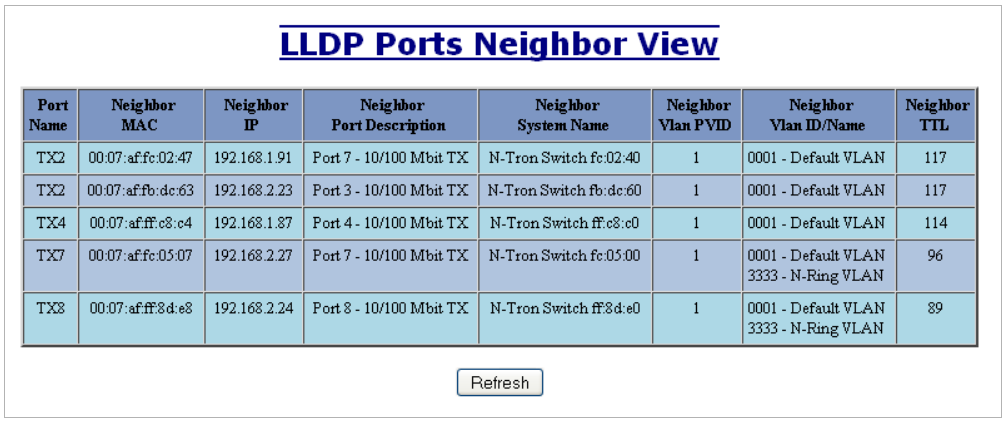
The Port VLAN identifier (PVID) associated with the neighbor port.

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
TX2	00:07:af:fc:02:47	192.168.1.91	Port 7 - 10/100 Mbit TX	N-Tron Switch fc:02:40	1	0001 - Default VLAN	117
TX2	00:07:af:fb:dc:63	192.168.2.23	Port 3 - 10/100 Mbit TX	N-Tron Switch fb:dc:60	1	0001 - Default VLAN	117
TX4	00:07:af:ff:c8:c4	192.168.1.87	Port 4 - 10/100 Mbit TX	N-Tron Switch ff:c8:c0	1	0001 - Default VLAN	114
TX7	00:07:af:fc:05:07	192.168.2.27	Port 7 - 10/100 Mbit TX	N-Tron Switch fc:05:00	1	0001 - Default VLAN 3333 - N-Ring VLAN	96
TX8	00:07:af:ff:8d:e8	192.168.2.24	Port 8 - 10/100 Mbit TX	N-Tron Switch ff:8d:e0	1	0001 - Default VLAN 3333 - N-Ring VLAN	89

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

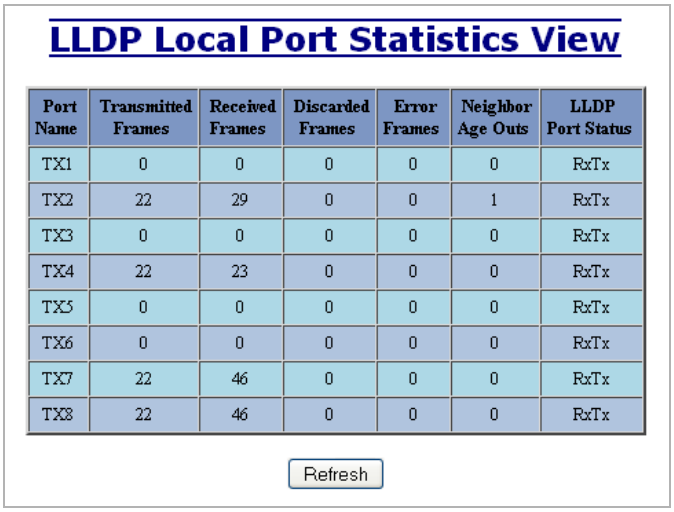
Total count of all LLDP frames received with one or more detectable errors.

Neighbor Age Outs

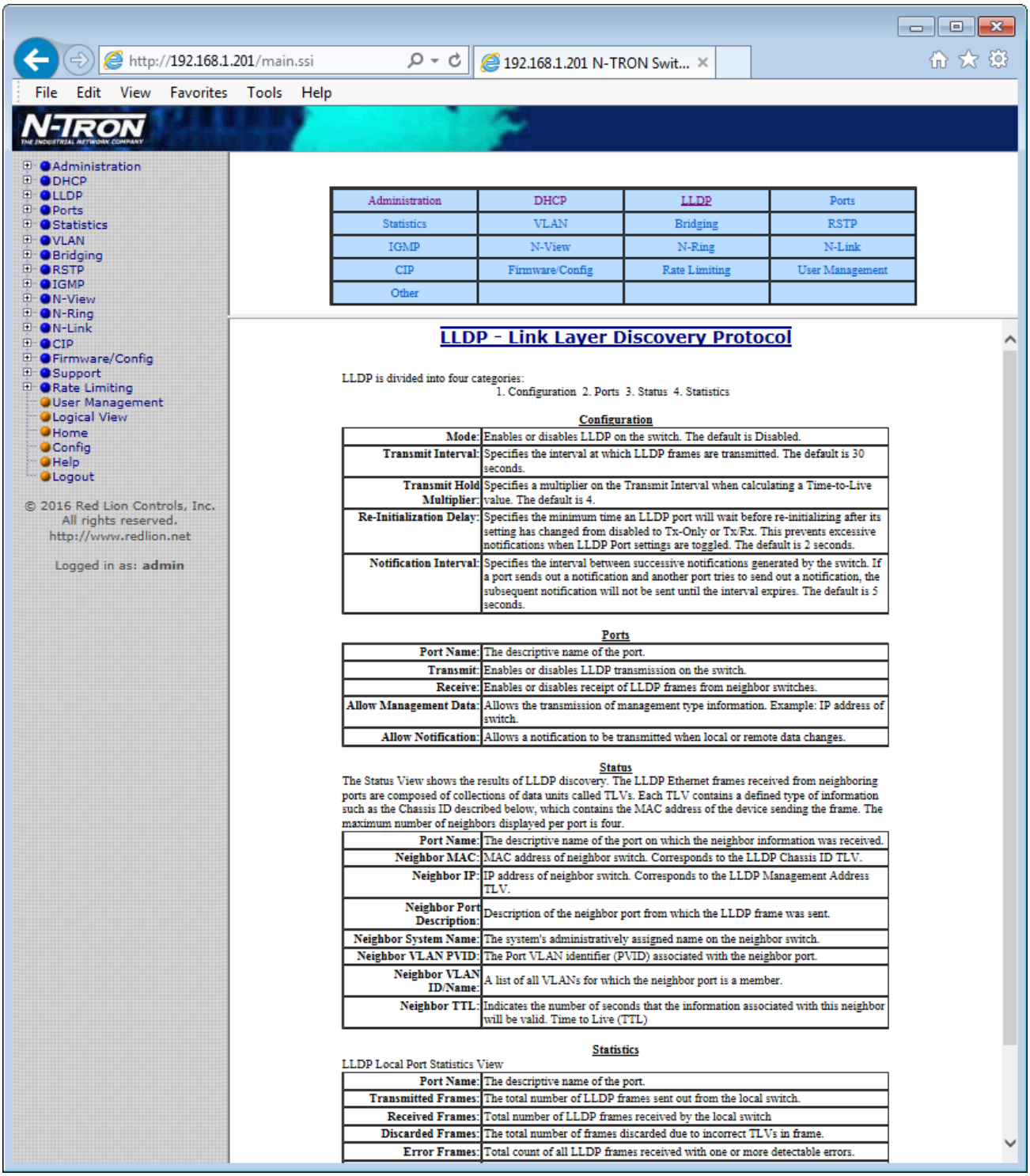
Total count of the times that a neighbor's information has been deleted from the switch because the Time to Live (TTL) has expired.

LLDP Port Status

Local Port setting (Receive-Rx/Transmit-Tx/Disable).



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



PORTS

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 and FX is for fiber optic ports. 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 700 model port **10/100** Mbps and 7000 model port **10/100/1000** Mbps.

Duplex Mode

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

Crossover Mode (7018 models only)

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

Flow Control State

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

Force High Priority State (700 models only)

This configurable field displays the port priority status of each port. When enabled for a port all frames received on that port will be forced to the highest priority queue regardless of 'Default Priority' setting or priority tags within the received frames. The default is **Disabled**. In an untagged N-Ring configuration, the N-Ring ports on the N-Ring Manager and active N-Ring Members will be **Enabled**.

Default Priority (700 models only)

This configurable field displays the default QoS priority for the port when an untagged frame is received. The range is **0-7.**

RSTP State

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

PVID

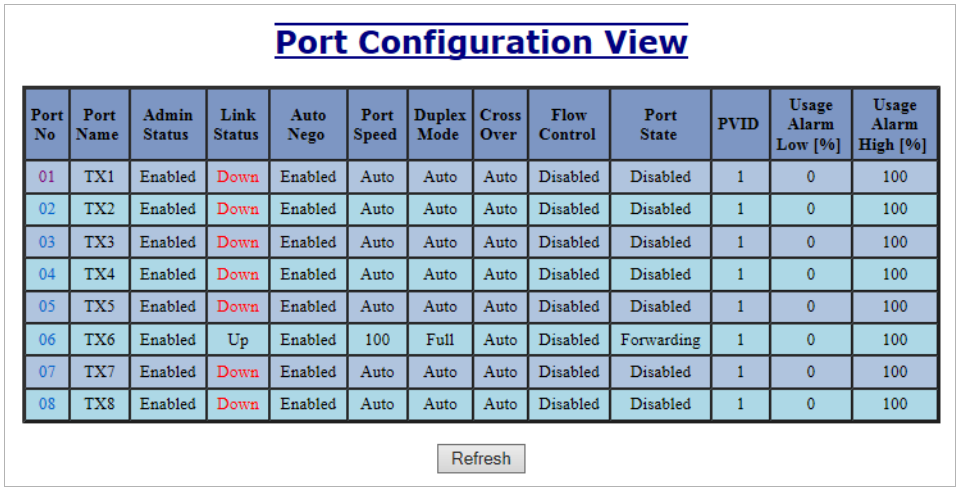
This configurable field displays the existing port VLAN ID setting. The allowable range is **1-4094.**

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.



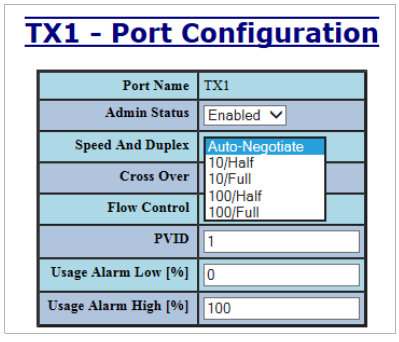
Port Configuration View

Port No	Port Name	Admin Status	Link Status	Auto Nego	Port Speed	Duplex Mode	Cross Over	Flow Control	Port State	PVID	Usage Alarm Low [%]	Usage Alarm High [%]
01	TX1	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100
02	TX2	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100
03	TX3	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100
04	TX4	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100
05	TX5	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100
06	TX6	Enabled	Up	Enabled	100	Full	Auto	Disabled	Forwarding	1	0	100
07	TX7	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100
08	TX8	Enabled	Down	Enabled	Auto	Auto	Auto	Disabled	Disabled	1	0	100

Refresh

The user can click on the Port Number to configure each port individually. This allows 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

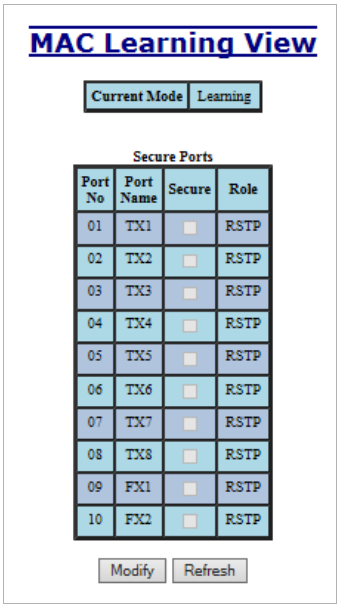


TX1 - Port Configuration

Port Name	TX1
Admin Status	Enabled
Speed And Duplex	Auto-Negotiate / 10/Half / 10/Full / 100/Half / 100/Full
Cross Over	
Flow Control	
PVID	1
Usage Alarm Low [%]	0
Usage Alarm High [%]	100

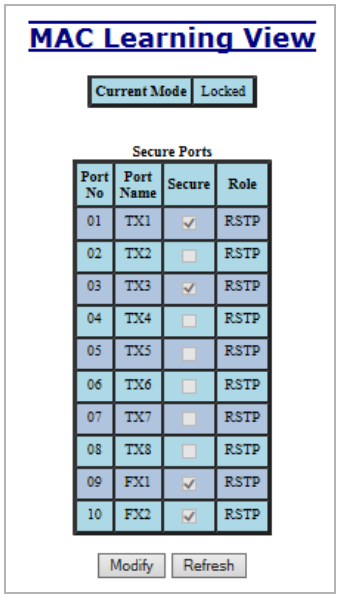
PORTS > MAC SECURITY > LEARNING

The Learning tab allows the user 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.

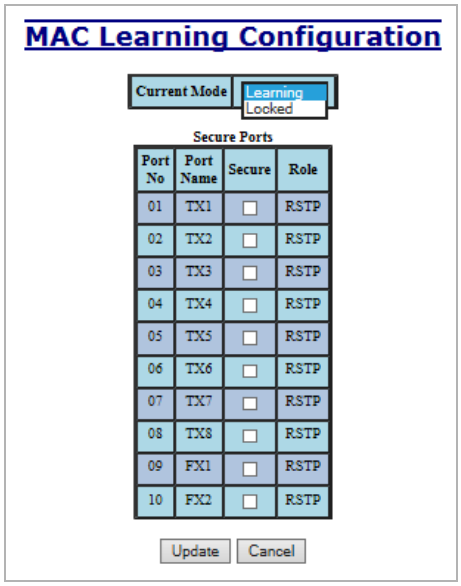


In 'Locked' mode, 'Secured Ports' shows the ports that are presently secured.

Note: When N-Ring and/or N-Link are used, the N-Ring/N-Link ports will not have MAC Security enabled.

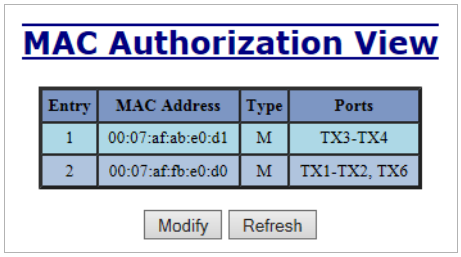


The Modify button allows the user to change the current mode and select the ports to be secured. When transitioning from 'Learning' to 'Locked', the Address Resolution Logic (ARL) table represents the authorized MAC addresses, with the addition of any manually entered addresses (refer to Authorization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

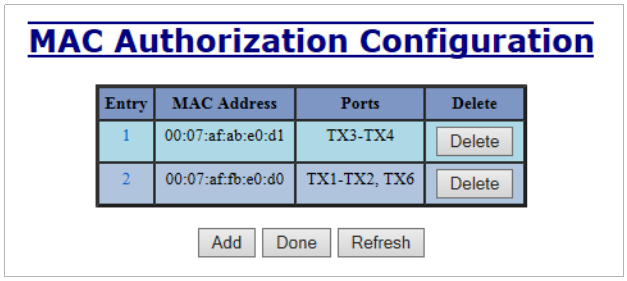


PORTS > MAC SECURITY > AUTHORIZATION LIST

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



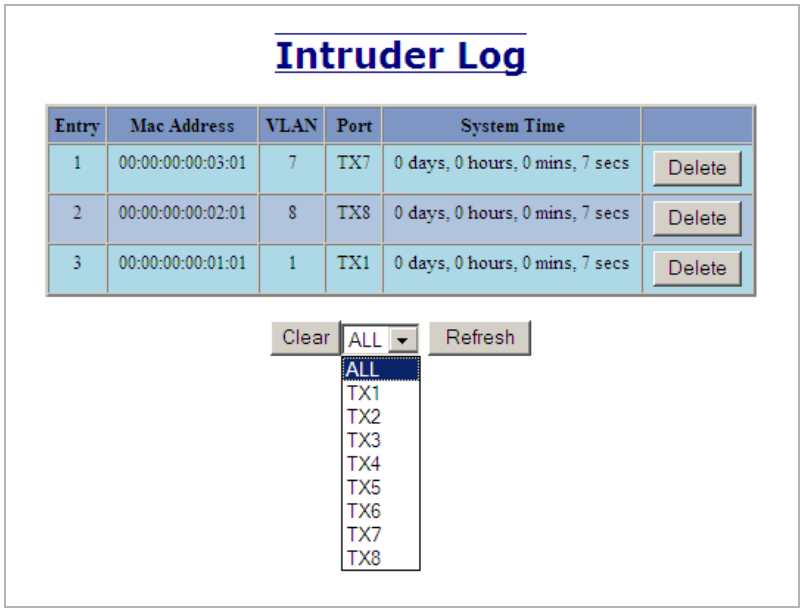
Selecting Modify displays the MAC Authorization Configuration page, which allows the user to add new entries, delete existing entries, or edit authorized ports of existing entries.



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

PORTS > MAC SECURITY > INTRUDER LOG

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

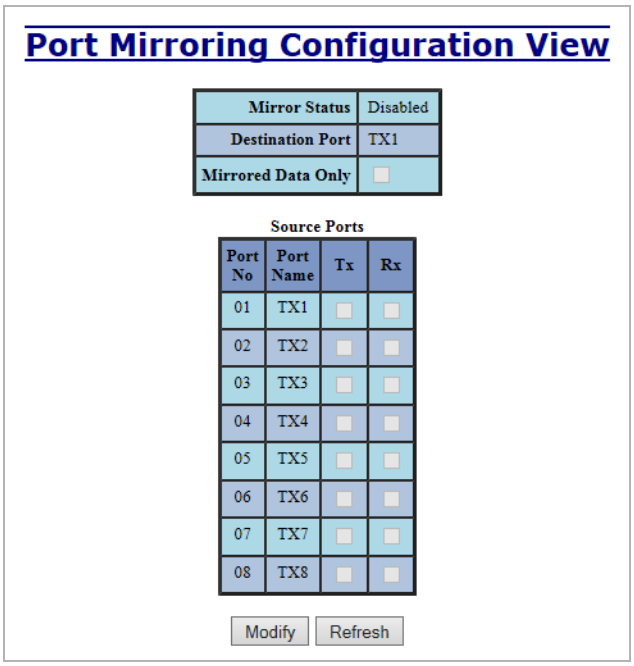


An entry can be individually removed from the log by selecting the associated Delete button. All entries or entries specific to a port can also be removed from the log by choosing the option in the dropdown list and then selecting the Clear button.

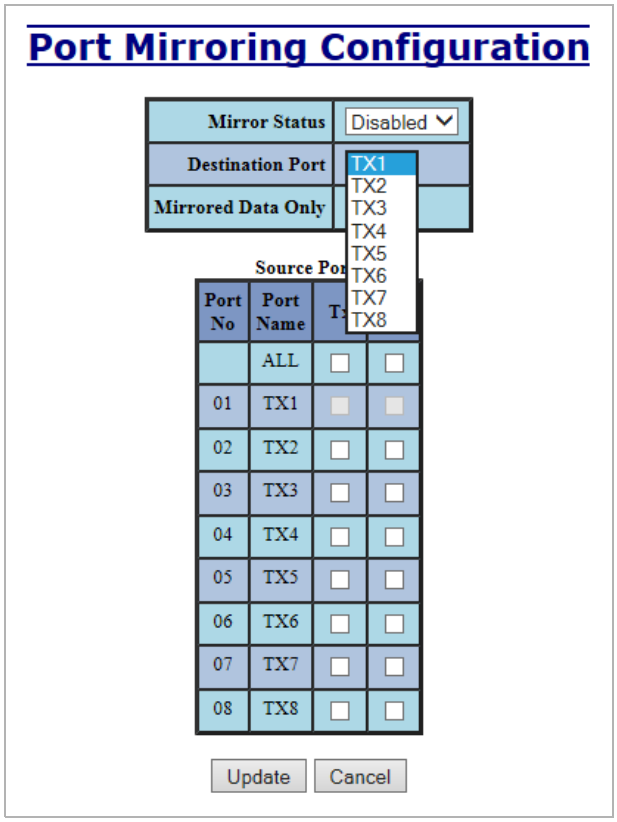
PORTS > MIRRORING

The mirroring destination port retransmits (mirrors) frames transmitted by or received by the configured source ports.

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.



By selecting Modify, you can enable the status of port mirroring and select source ports and the destination port that the source ports will be mirrored to. The number and type of destination ports displayed depends on the 700/7000 model in use.



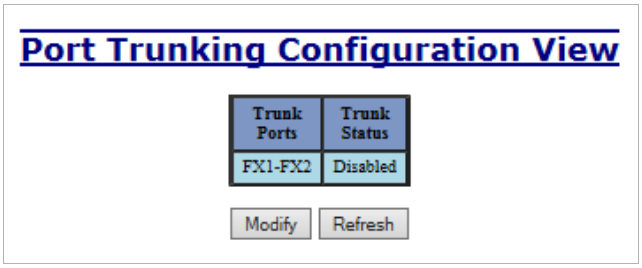
PORTS > TRUNKING The Trunking tab under the Ports category displays the following details:

Trunk Ports

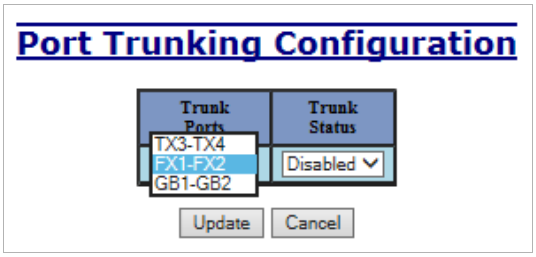
This field displays the ports associated with the trunk.

Trunk Status

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



By selecting Modify, 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 algorithm prioritizes traffic into a Transmit Queue (TA) based on a priority assigned to all frames received on a port or fields found in the frames received by the switch. These mechanisms are:

DSCP (RFC 2472 DSCP TOS)
802.1p (IEEE 802.1p COS)
Port Priority

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

Port No (Number)
This is the port index.

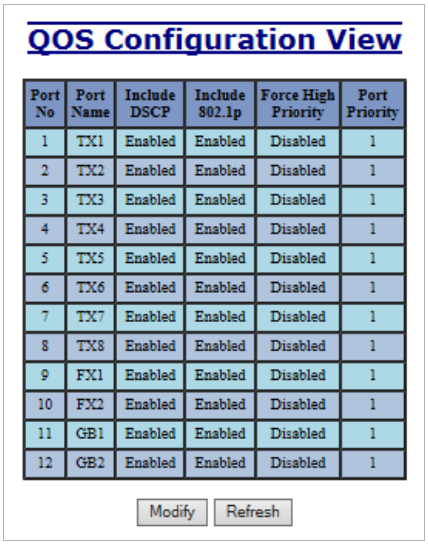
Port Name
This field displays the name of the port.

Include DSCP
This field displays the status of whether or not to include the RFC 2474 DSCP TOS (Type of Service) in the TQ assignment. 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 assignment. 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 assignment for all ports and all frames received on a port will use the default QOS priority for that port in the TQ assignment.

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



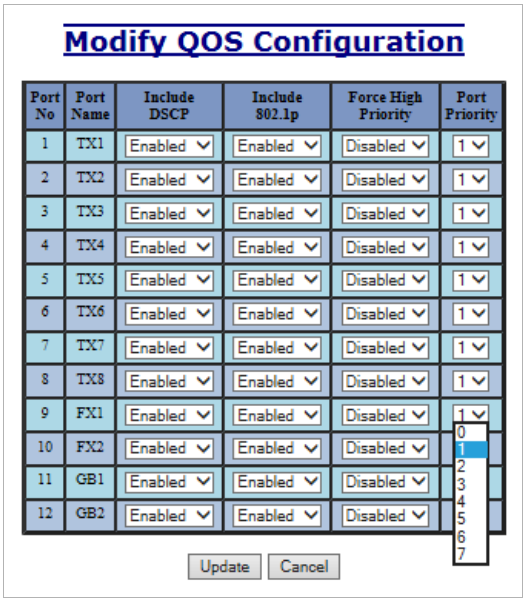
QOS Configuration View

Port No	Port Name	Include DSCP	Include 802.1p	Force High Priority	Port Priority
1	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
10	FX2	Enabled	Enabled	Disabled	1
11	GB1	Enabled	Enabled	Disabled	1
12	GB2	Enabled	Enabled	Disabled	1

Modify Refresh

By selecting Modify, the user can configure the ports for different QOS functionality.

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

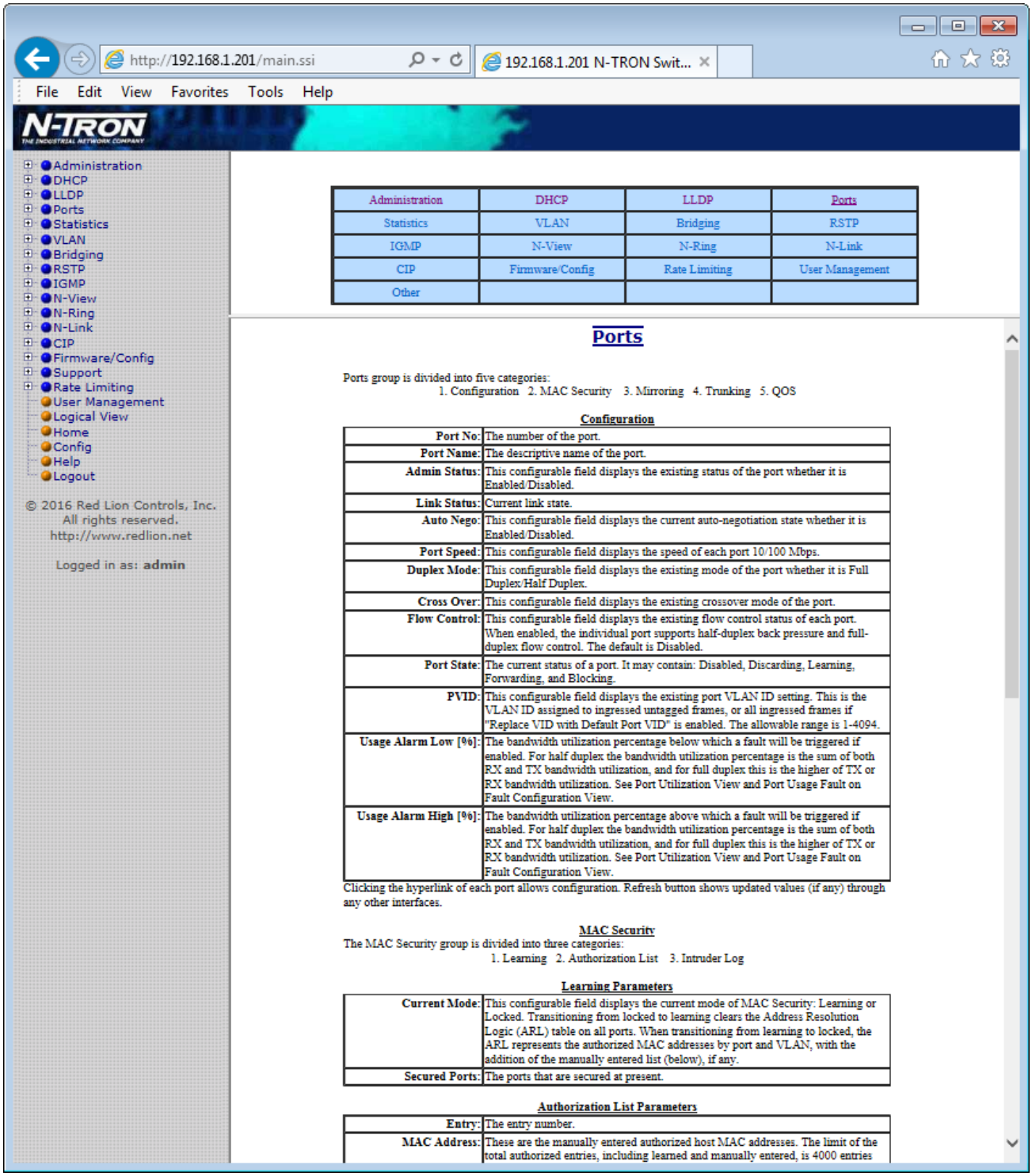


Modify QOS Configuration

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	1
8	TX8	Enabled	Enabled	Disabled	1
9	FX1	Enabled	Enabled	Disabled	1
10	FX2	Enabled	Enabled	Disabled	0 1 2 3 4 5 6 7
11	GB1	Enabled	Enabled	Disabled	
12	GB2	Enabled	Enabled	Disabled	

Update Cancel

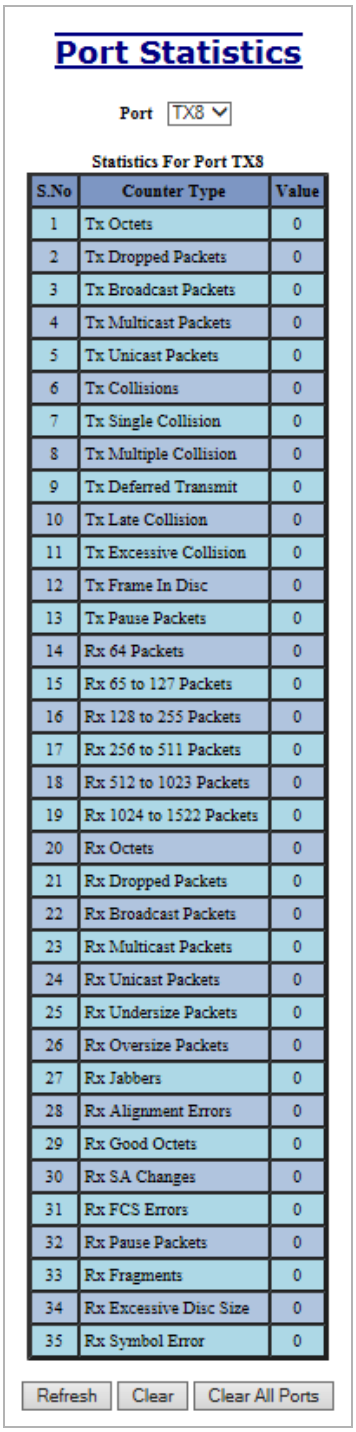
HELP > PORTS Following the Ports link on the help page, the user or user can see some information regarding the configuration options in the Ports category on the left side of the web management interface.



STATISTICS

STATISTICS > PORTS > 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 TX8

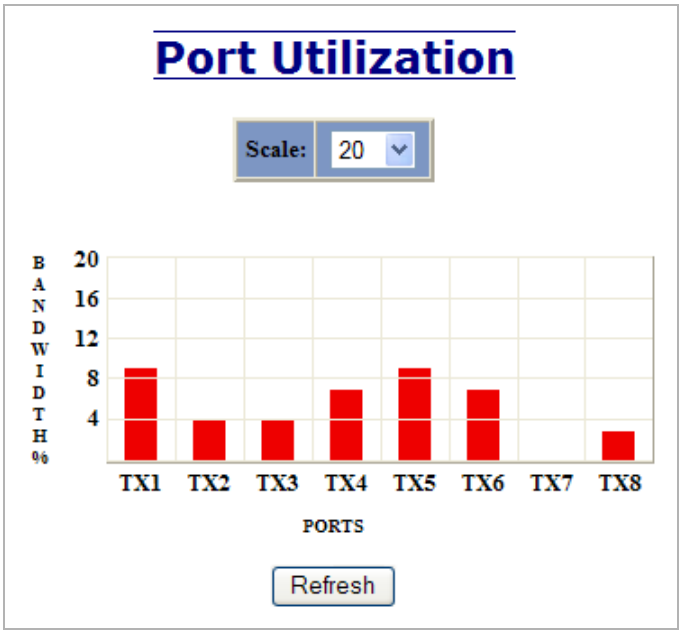
Statistics For Port TX8

S.No	Counter Type	Value
1	Tx Octets	0
2	Tx Dropped Packets	0
3	Tx Broadcast Packets	0
4	Tx Multicast Packets	0
5	Tx Unicast Packets	0
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	0
15	Rx 65 to 127 Packets	0
16	Rx 128 to 255 Packets	0
17	Rx 256 to 511 Packets	0
18	Rx 512 to 1023 Packets	0
19	Rx 1024 to 1522 Packets	0
20	Rx Octets	0
21	Rx Dropped Packets	0
22	Rx Broadcast Packets	0
23	Rx Multicast Packets	0
24	Rx Unicast Packets	0
25	Rx Undersize Packets	0
26	Rx Oversize Packets	0
27	Rx Jabbers	0
28	Rx Alignment Errors	0
29	Rx Good Octets	0
30	Rx SA Changes	0
31	Rx FCS Errors	0
32	Rx Pause Packets	0
33	Rx Fragments	0
34	Rx Excessive Disc Size	0
35	Rx Symbol Error	0

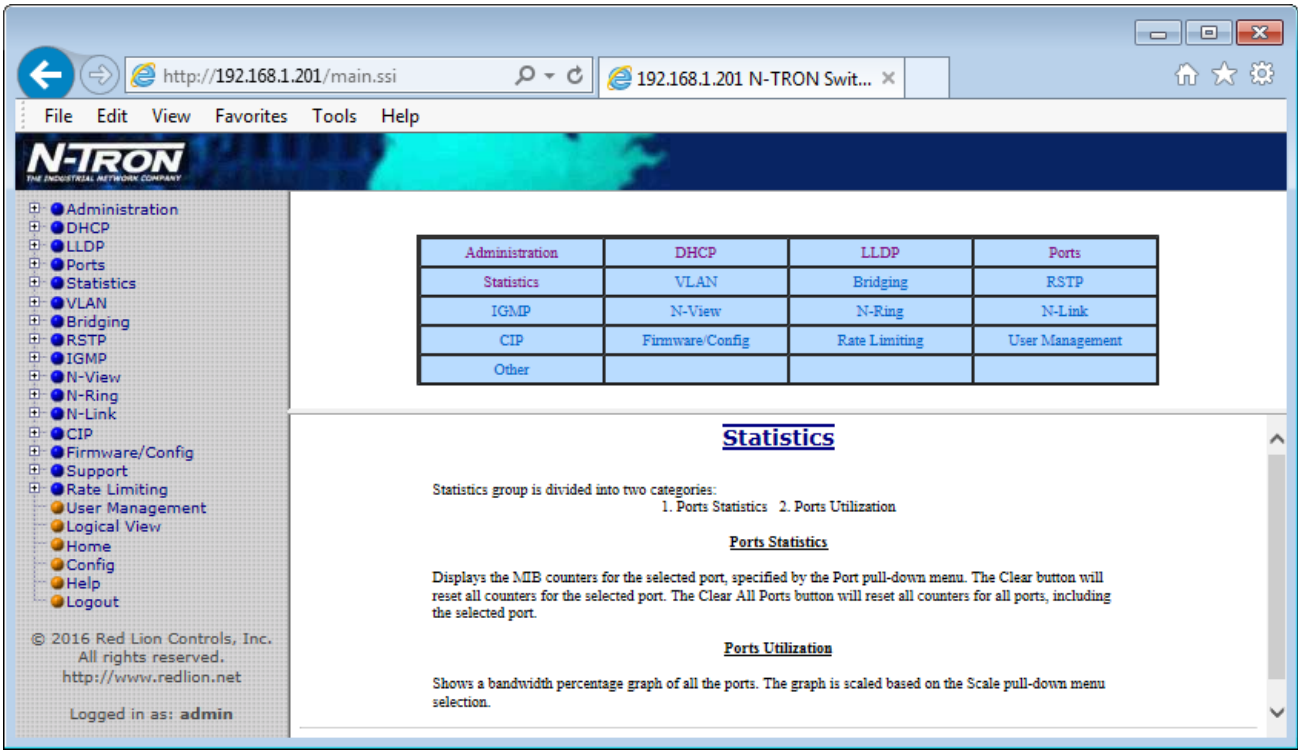
Refresh Clear Clear All Ports

STATISTICS > PORTS > UTILIZATION

Ports Utilization shows all the ports on the switch and will display a bar graph showing the approximate percentage of bandwidth being used. The available Scale options are: 5, 10, 20, 50 or 100. Red Lion recommends the use of N-View in order to get a precise bandwidth usage figure.



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



VLAN

VLAN > CONFIGURATION

Replace VID Tag with Default Port VID

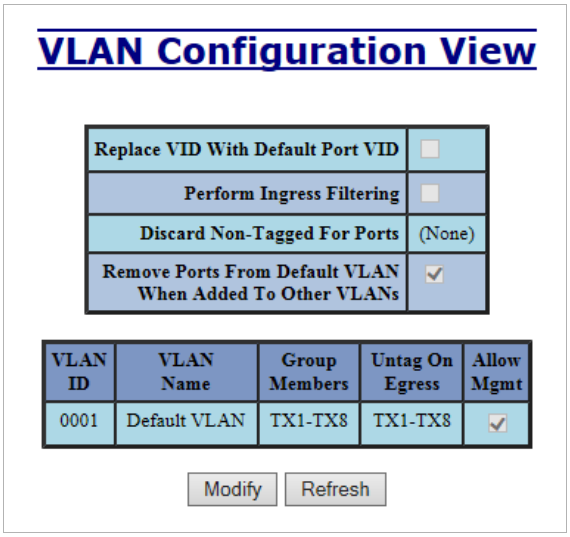
Specifies whether or not to replace the ingress frames' VID tag with the port's designated VID (PVID).

Perform Ingress Filtering

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

Discard Non-Tagged for Ports

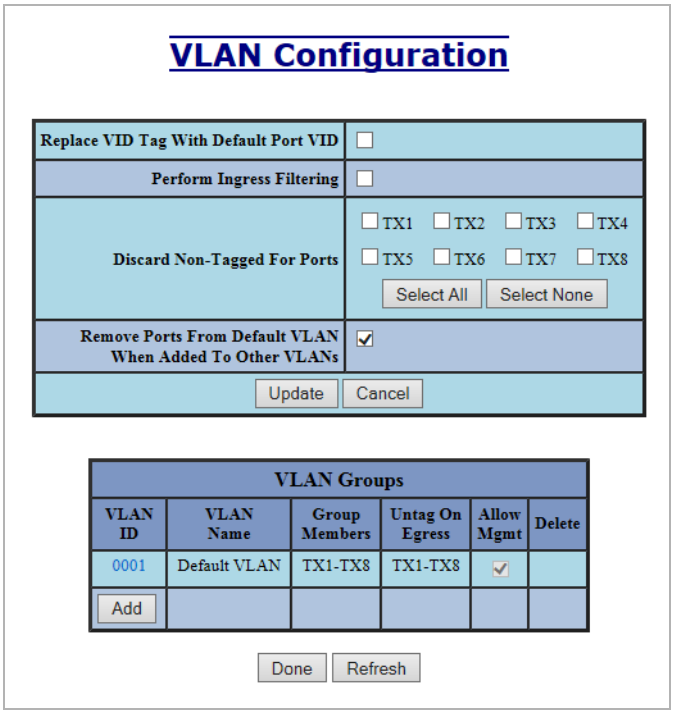
Specifies whether or not non-tagged ingress frames are dropped by the selected ports.



For convenience:

- Ports are deleted from VLAN1 as each port is added to another group.
- Ports are added to VLAN1 if a deletion leaves a port with no group.
- If it is desired to have a port in VLAN1 and also in other VLANs 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

ID

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

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

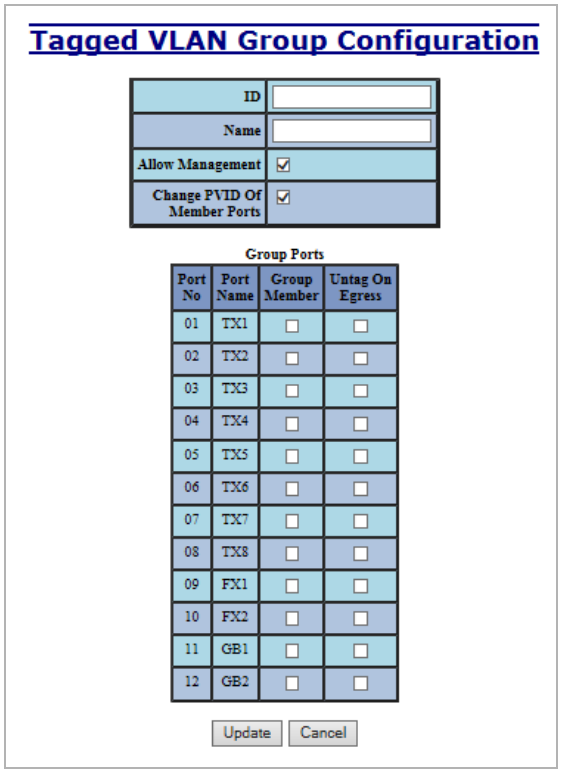
Descriptive name of the port

Group Member

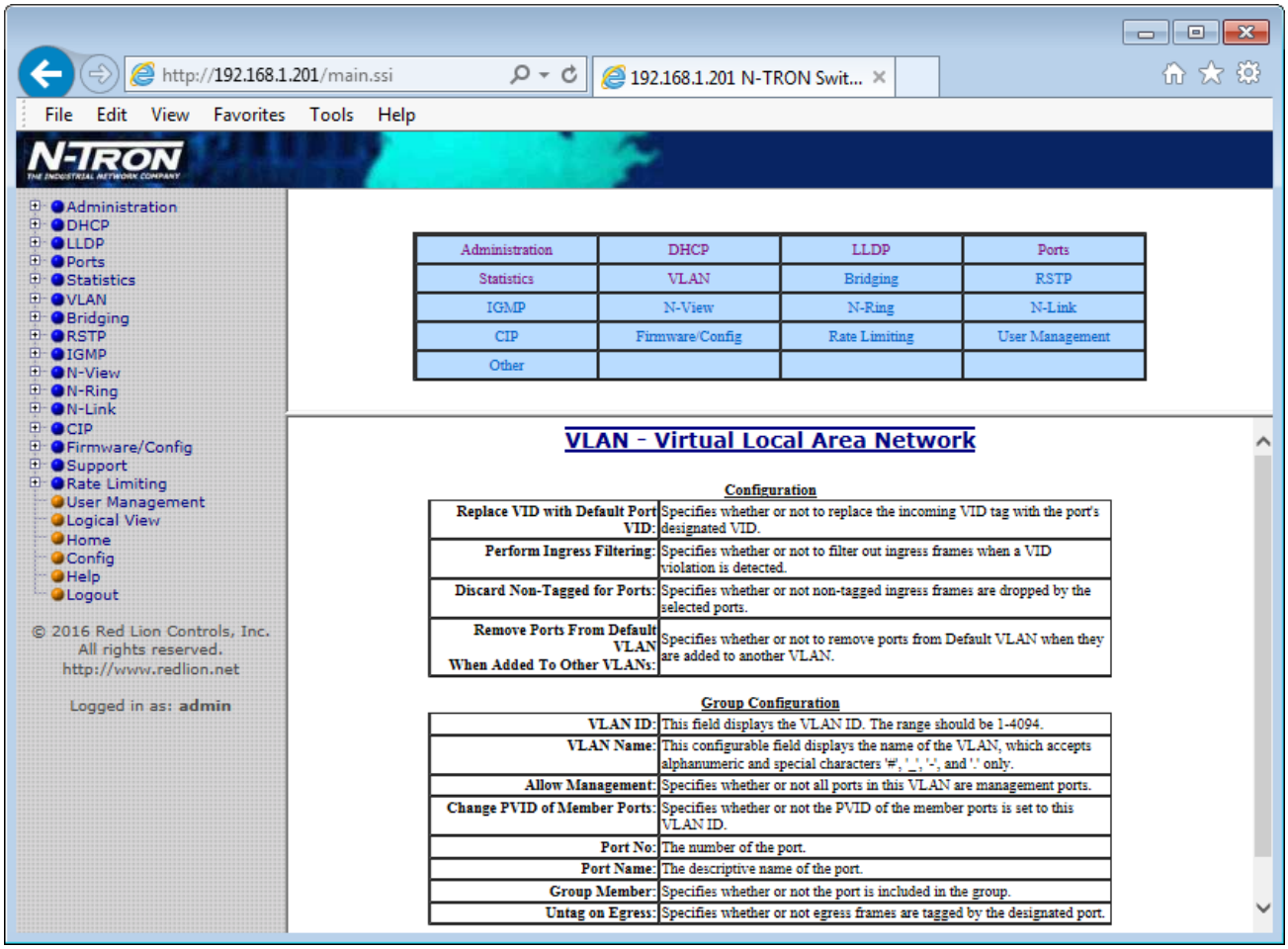
Specifies whether or not the port is included in the group.

Untag on Egress

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


Tagged VLAN Group Configuration
ID
Name
Allow Management
Change PVID Of Member Ports
Group Ports
Port No
Port Name
Group Member
Untag On Egress
01 TX1
02 TX2
03 TX3
04 TX4
05 TX5
06 TX6
07 TX7
08 TX8
09 FX1
10 FX2
11 GB1
12 GB2
Update
Cancel

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



BRIDGING

BRIDGING > AGING TIME

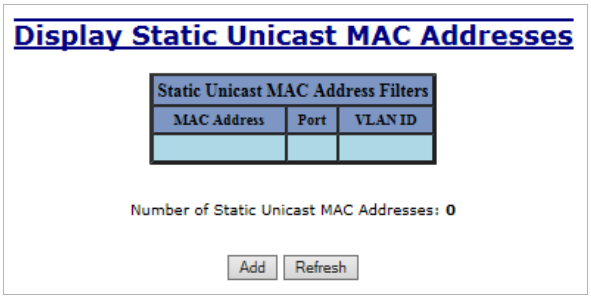
The Aging Time tab under the Bridging category will display the currently configured Aging Time. This page allows users to modify this variable to meet their needs.

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

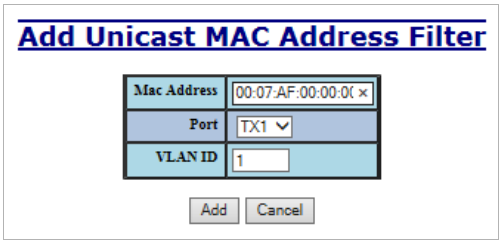
Note: If the switch is an active participant of an N-Ring, then the N-Ring Aging Time will be used instead of the Bridging Aging Time.

BRIDGING > UNICAST ADDRESSES

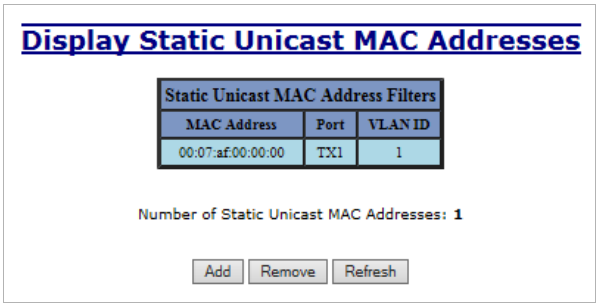
The Unicast Addresses tab under the Bridging category will display a list of MAC addresses that are associated with each respective port number. This can be used to statically assign a MAC address access to a single port on the switch.



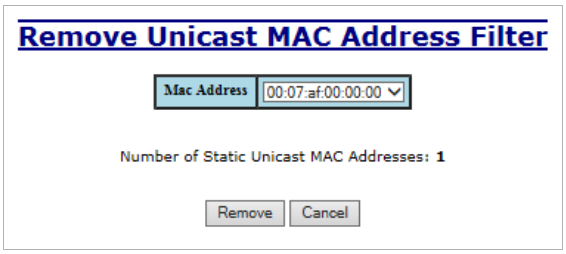
Following the Add button on the page above, the user must enter a valid MAC address and associate it with a port number on the switch. Once the user hits the Add button, the changes will take effect instantly.



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

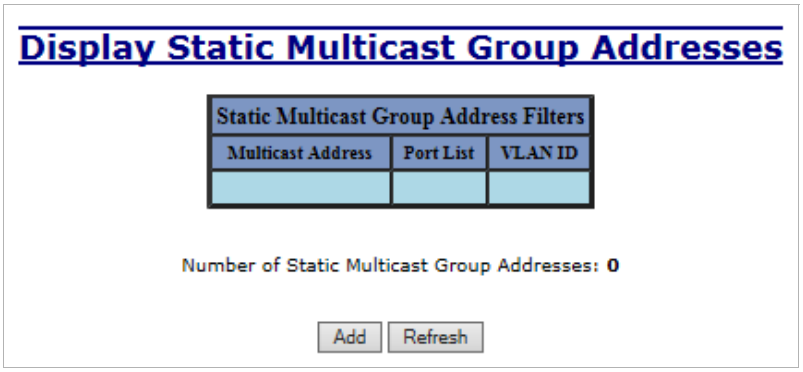


Following the Remove button on the example above, an user can select a static MAC address from the list using a pull-down menu. After selecting the MAC address, the user needs to press the Remove button on the page to remove the entry.

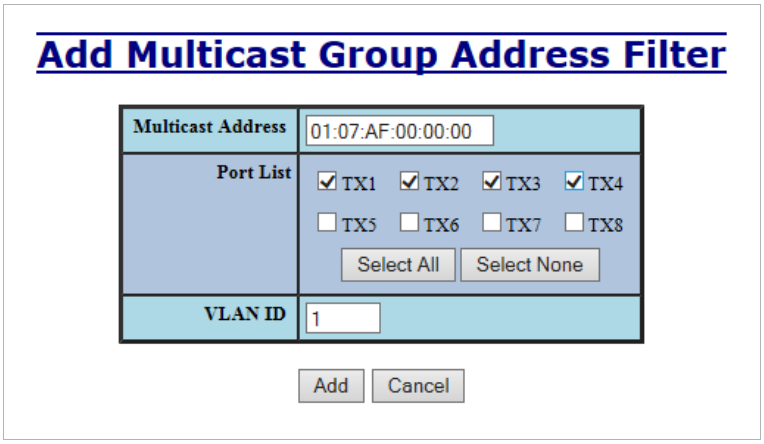


BRIDGING > MULTICAST ADDRESSES

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

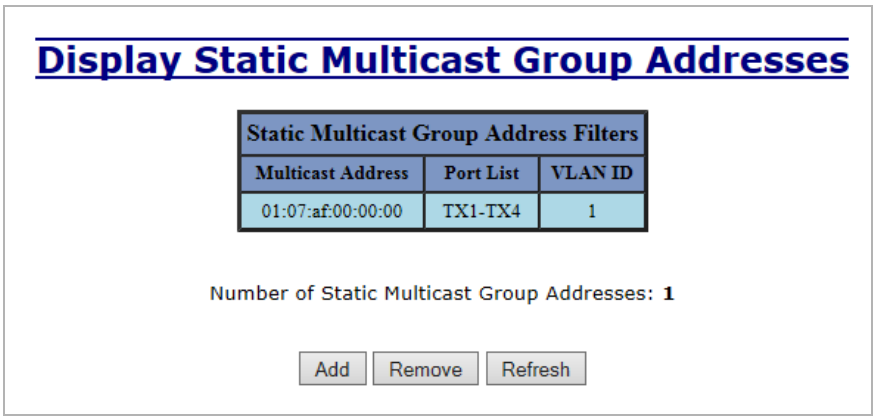


Following the Add button on the page above, the user must enter a valid Multicast Group Address and associate it with a port number or list on the switch. Once the user clicks on the Add button, the changes will take effect instantly.

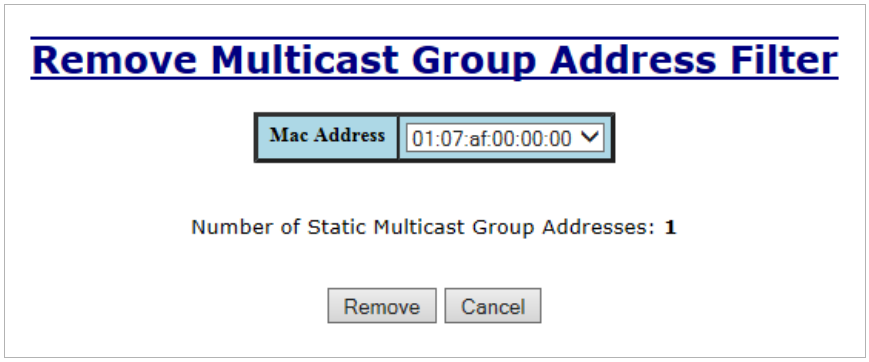


Note: If there are multiple ports on different VLANs, the switch will apply the static multicast address to the lowest VLAN-ID that is associated with one of the ports assigned to the static multicast address. So if the lowest VLAN-ID contains all the ports assigned to the static multicast address (an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

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



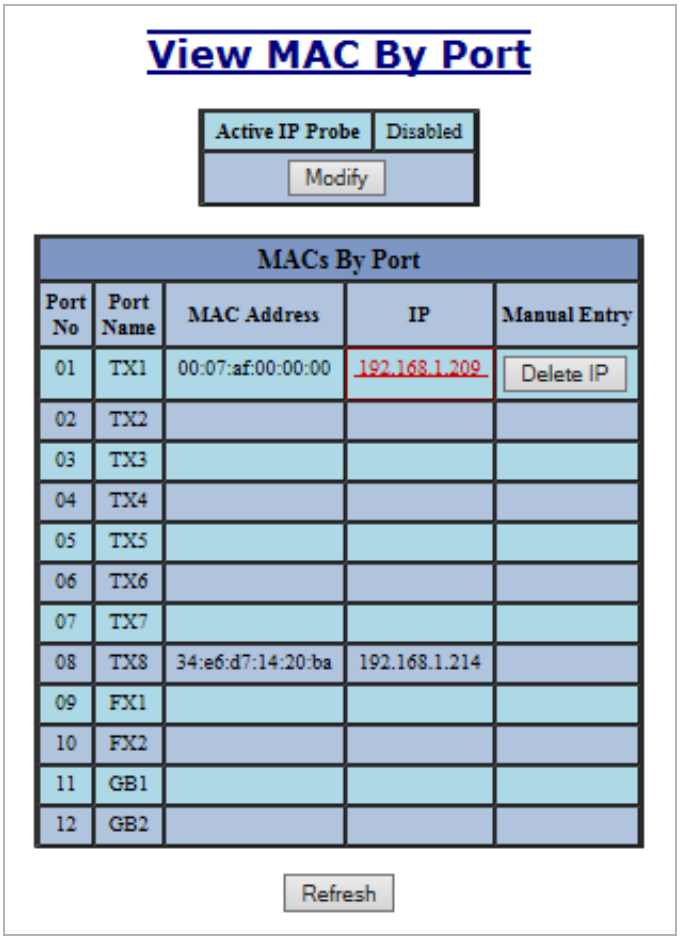
Following the Remove button on the example above, the user will be presented with a list of Multicast Group Addresses that are configured on the switch. Using the pull-down menu, the user should select the desired address to be removed. Then click on the Remove button at the bottom of the page.



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

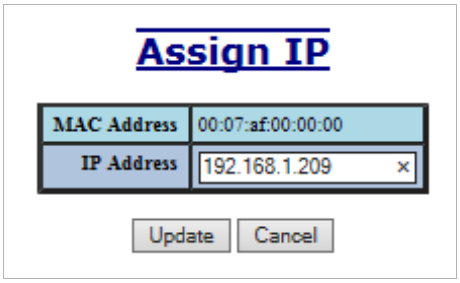


The 'Active IP Probe' field is configurable using the 'Modify' button, and also displays the existing Enabled or Disabled status of this feature. The default is disabled. When disabled the switch generates no Ethernet traffic for this purpose, but can still present some information gathered passively.

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.

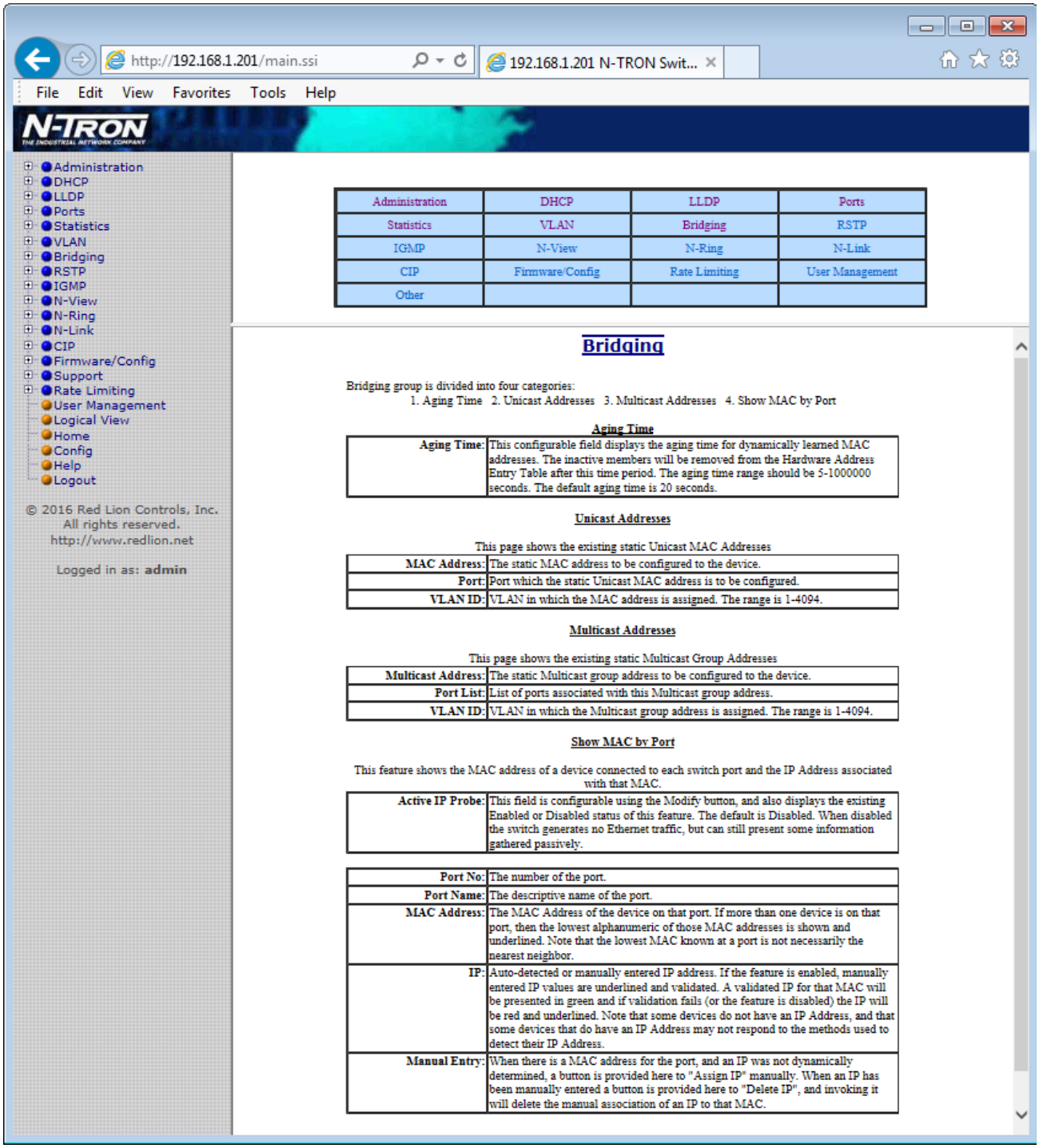
Note: Some devices do not have an IP Address, and that some devices that do have an IP Address may not respond to the methods used to detect their IP Address.

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



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

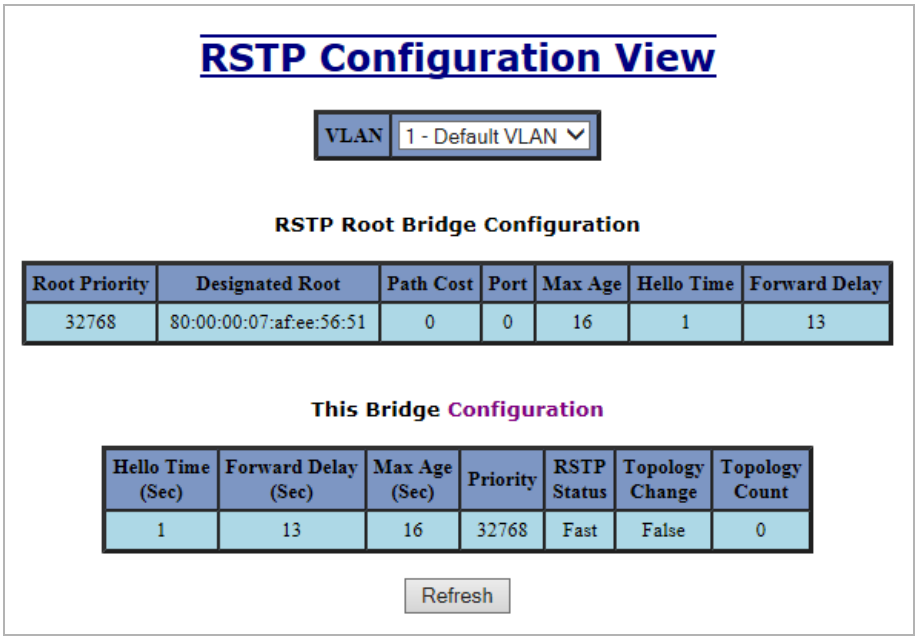
HELP > BRIDGING Following the Bridging link on the help page, the user or user can see some information regarding the configuration options in the Bridging category on the left side of the web management interface.



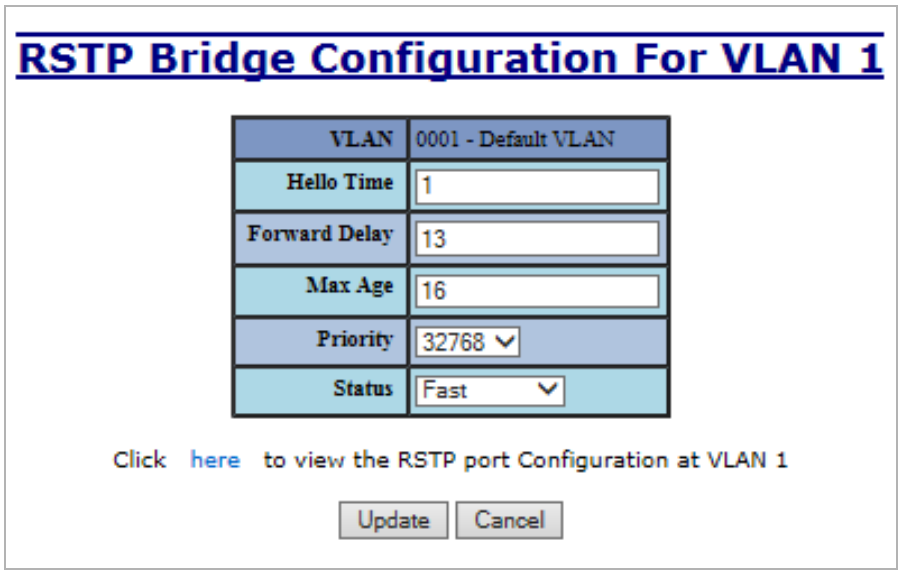
RSTP

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 user can choose which VLAN to configure RSTP on. Once the VLAN is selected, the user may configure the bridge by clicking on the 'This Bridge Configuration' link in the middle of the page.



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



Note: It is recommended that RSTP networks 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.

Following the link for the view RSTP Port Configuration at VLAN#, the user 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, TX3 is a redundant port with port TX2, therefore TX2 is forwarding and TX3 is discarding.

RSTP Configuration View For VLAN 1

Bridge Port Configuration									
Port No	Port Name	Port State	Path Cost	Priority	STP BPDU	Auto Edge	Admin Edge	Designated Bridge	Designated Port
01	TX1	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:01
02	TX2	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:02
03	TX3	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:03
04	TX4	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:04
05	TX5	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:05
06	TX6	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:06
07	TX7	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:07
08	TX8	Forwarding	200000	128	No	Enabled	Disabled	80:00:00:07:af:ef:78:e1	00:08
09	FX1	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:09
10	FX2	Disabled	200000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0a
11	GB1	Disabled	20000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0b
12	GB2	Disabled	20000	128	No	Enabled	Disabled	00:00:00:00:00:00:00:00	00:0c

<< Back | Refresh

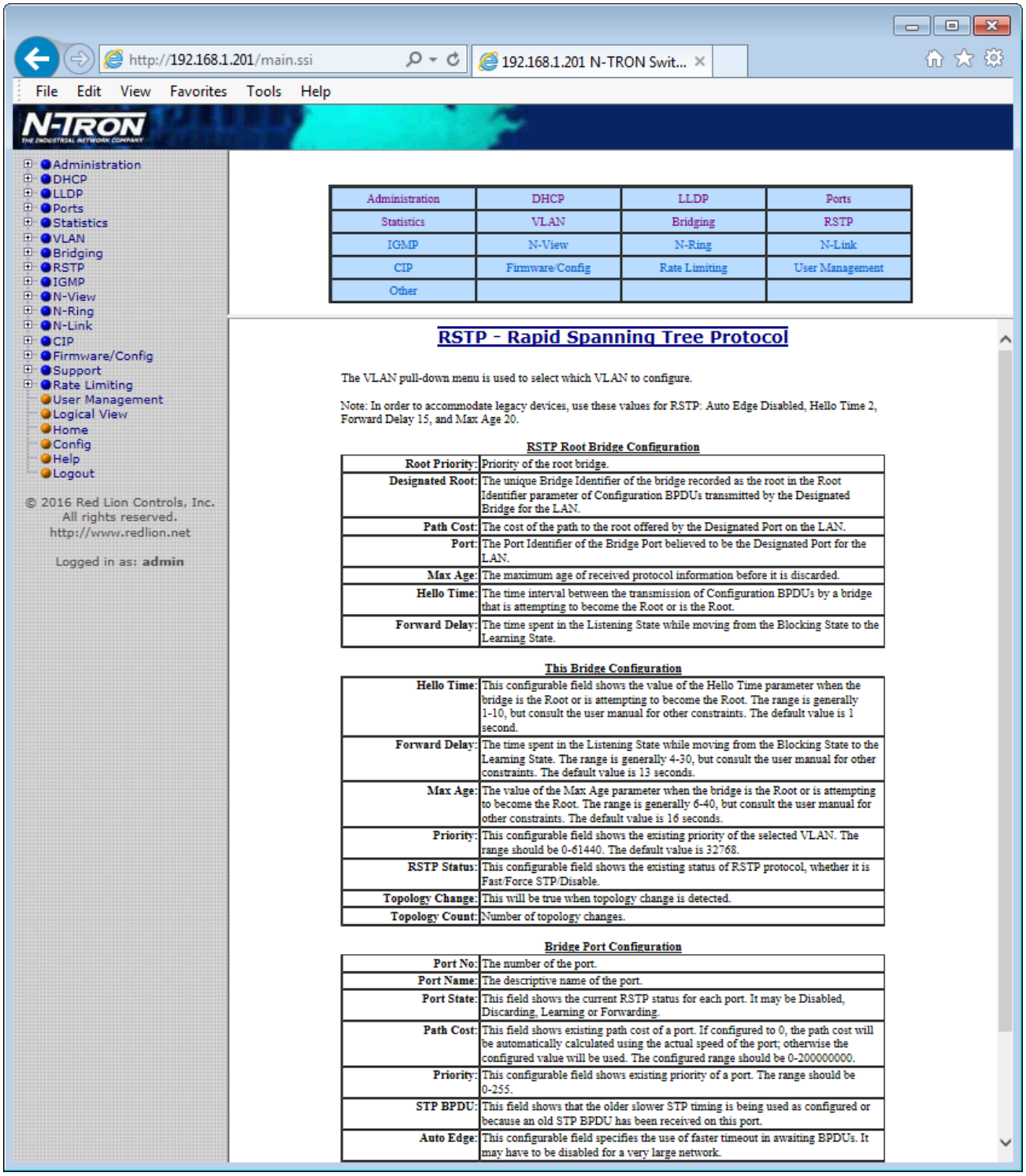
If the user selects one of the ports on the previous screen, he or she can change the Port's Path Cost, Priority, and the status of Admin Edge and Auto Edge.

RSTP Bridge Port Configuration

VLAN	0001 - Default VLAN
Port Name	TX1
Path Cost	0
Priority	128
Admin Edge	Disabled
Auto Edge	Enabled

Update | Cancel

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



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

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

This Bridge Configuration

Hello Time:	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.
Forward Delay:	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.
Max Age:	The value of the Max Age parameter when the bridge is the Root or is attempting to become the Root. The range is generally 6-40, but consult the user manual for other constraints. The default value is 16 seconds.
Priority:	This configurable field shows the existing priority of the selected VLAN. The range should be 0-61440. The default value is 32768.
RSTP Status:	This configurable field shows the existing status of RSTP protocol, whether it is Fast/Force STP/Disable.
Topology Change:	This will be true when topology change is detected.
Topology Count:	Number of topology changes.

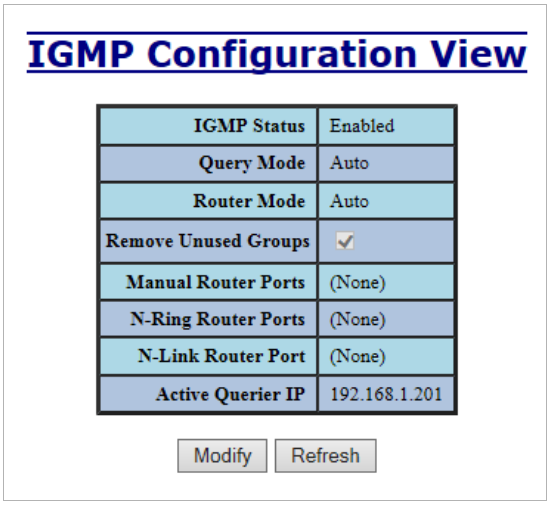
Bridge Port Configuration

Port No:	The number of the port.
Port Name:	The descriptive name of the port.
Port State:	This field shows the current RSTP status for each port. It may be Disabled, Discarding, Learning or Forwarding.
Path Cost:	This field shows existing path cost of a port. If configured to 0, the path cost will be automatically calculated using the actual speed of the port; otherwise the configured value will be used. The configured range should be 0-200000000.
Priority:	This configurable field shows existing priority of a port. The range should be 0-255.
STP BPDU:	This field shows that the older slower STP timing is being used as configured or because an old STP BPDU has been received on this port.
Auto Edge:	This configurable field specifies the use of faster timeout in awaiting BPDUs. It may have to be disabled for a very large network.

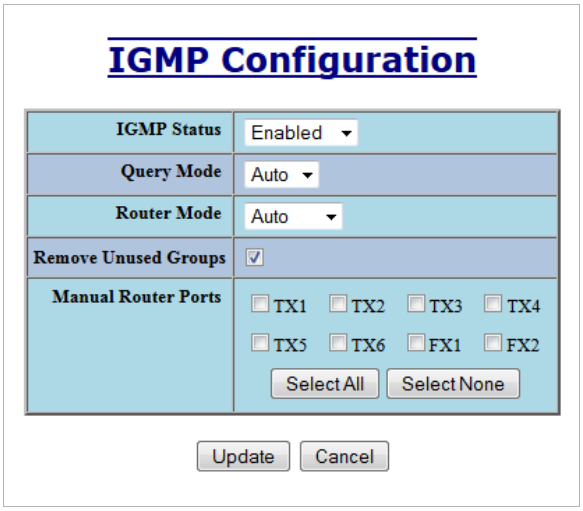
IGMP

IGMP > CONFIGURATION

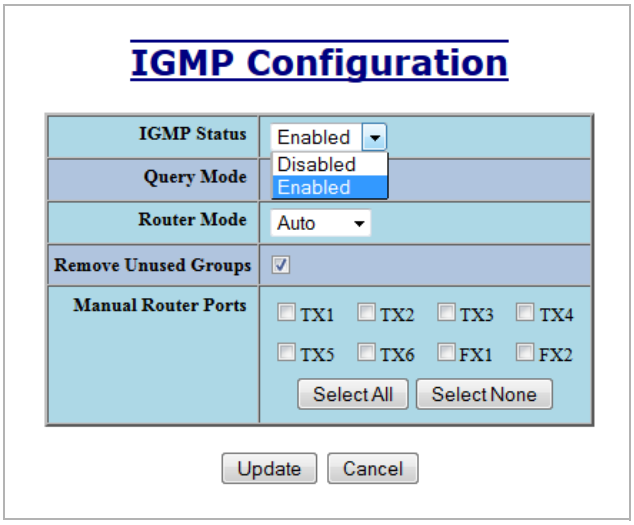
The Configuration tab under the IGMP category will display the IGMP basic configuration settings. By default, IGMP is enabled.



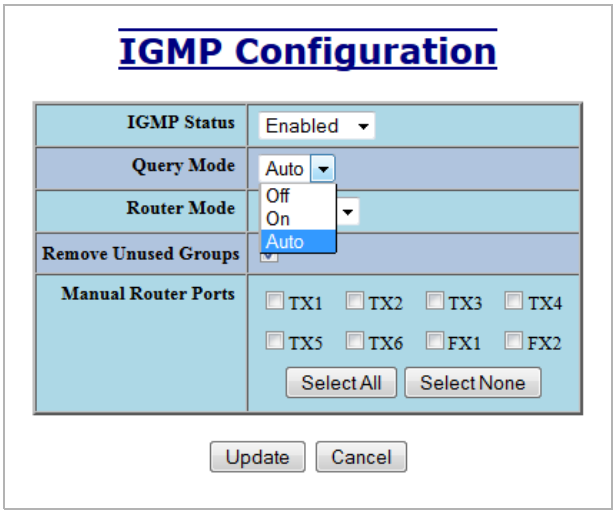
By selecting Modify, the user will see a list of configurable fields for the IGMP configuration. Once these fields are filled in to meet the needs of the user's network, the changes may be updated by clicking the Update button at the bottom of the page.



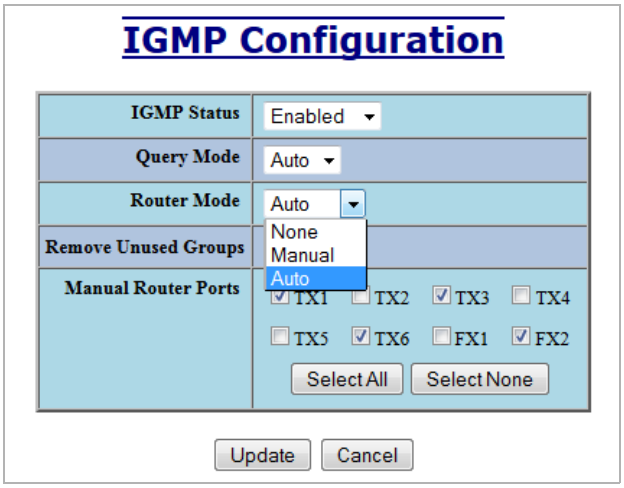
The IGMP Status pull-down allows the user to enable or disable IGMP completely.



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

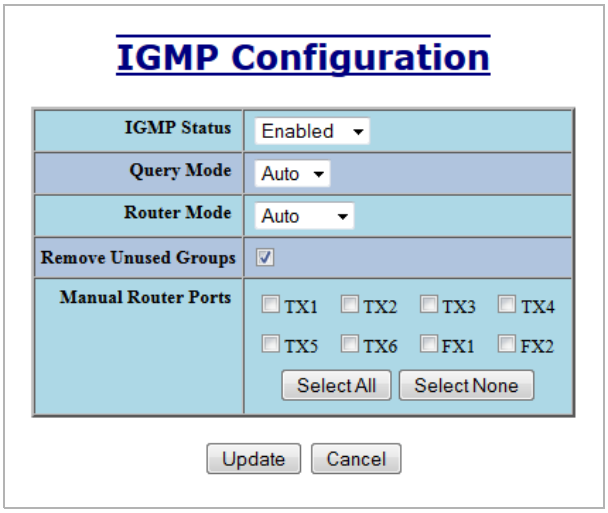


The Router Mode pull-down allows the user to choose router mode. ‘Auto’ allows for dynamically detected and manually set router ports. ‘Manual’ allows only for manually set router ports. ‘None’ allows no router ports.

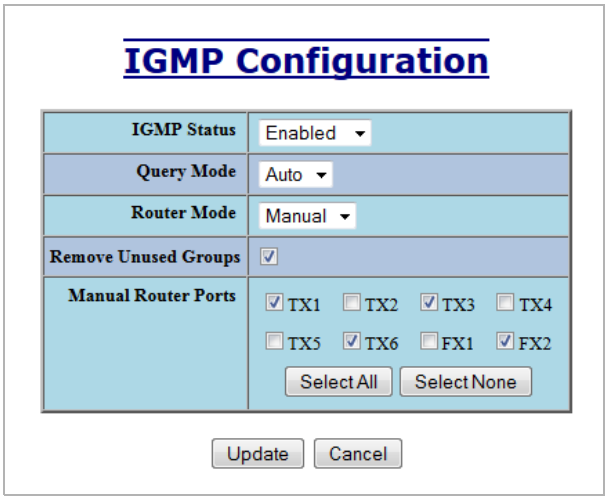


If **Remove Unused Groups** is checked then unused IGMP Groups will be removed and traffic with those multicast addresses will be treated as normal multicast. If unchecked, then unused IGMP Groups are not removed and traffic with those multicast addresses will be limited. The default is checked.

Note: IGMP Groups are not retained through a power cycle.

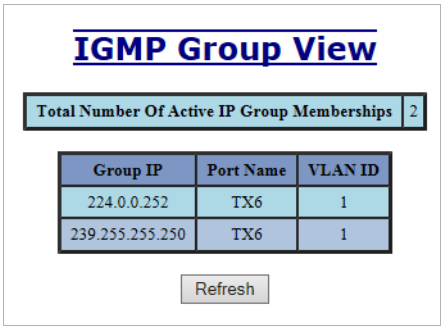


The user can specify the manual router ports:



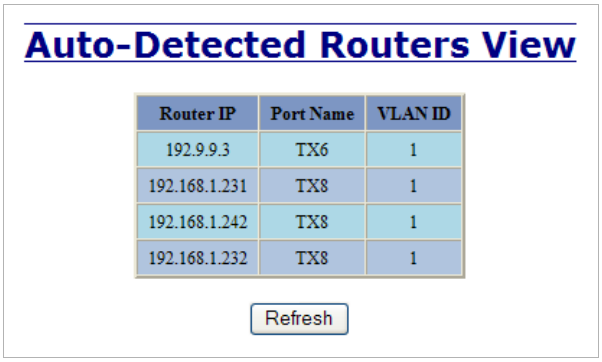
IGMP > Show Groups

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



IGMP > Show Routers

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



IGMP > RFilter Ports

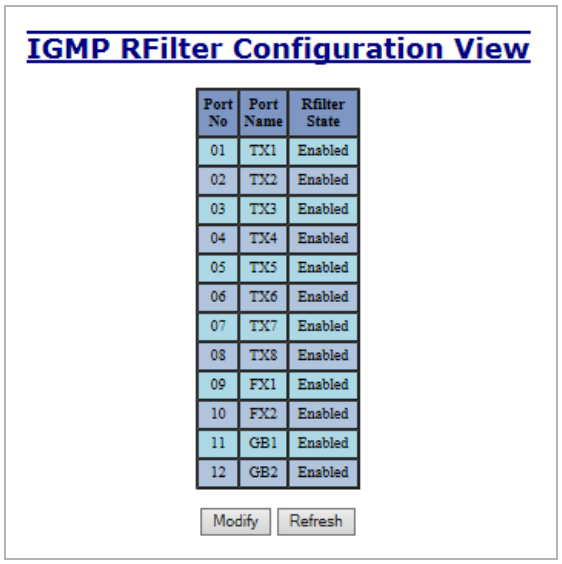
The 'rfilter' (**Router Multicast Data Filter**) function allows you to choose whether or not DATA frames with KNOWN group multicast addresses are sent to the 'router' ports (links to other switches). Control packets (Join, Leave) will be sent to the router(s) regardless of this setting. "KNOWN" is known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

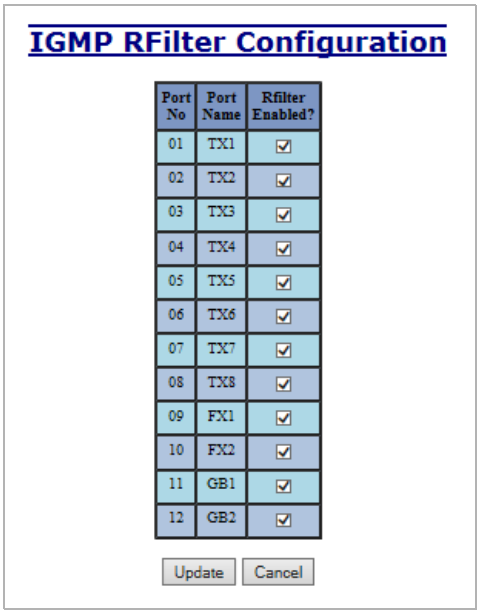
If rfilter is disabled, router ports do get DATA frames with KNOWN multicast destination addresses.

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.

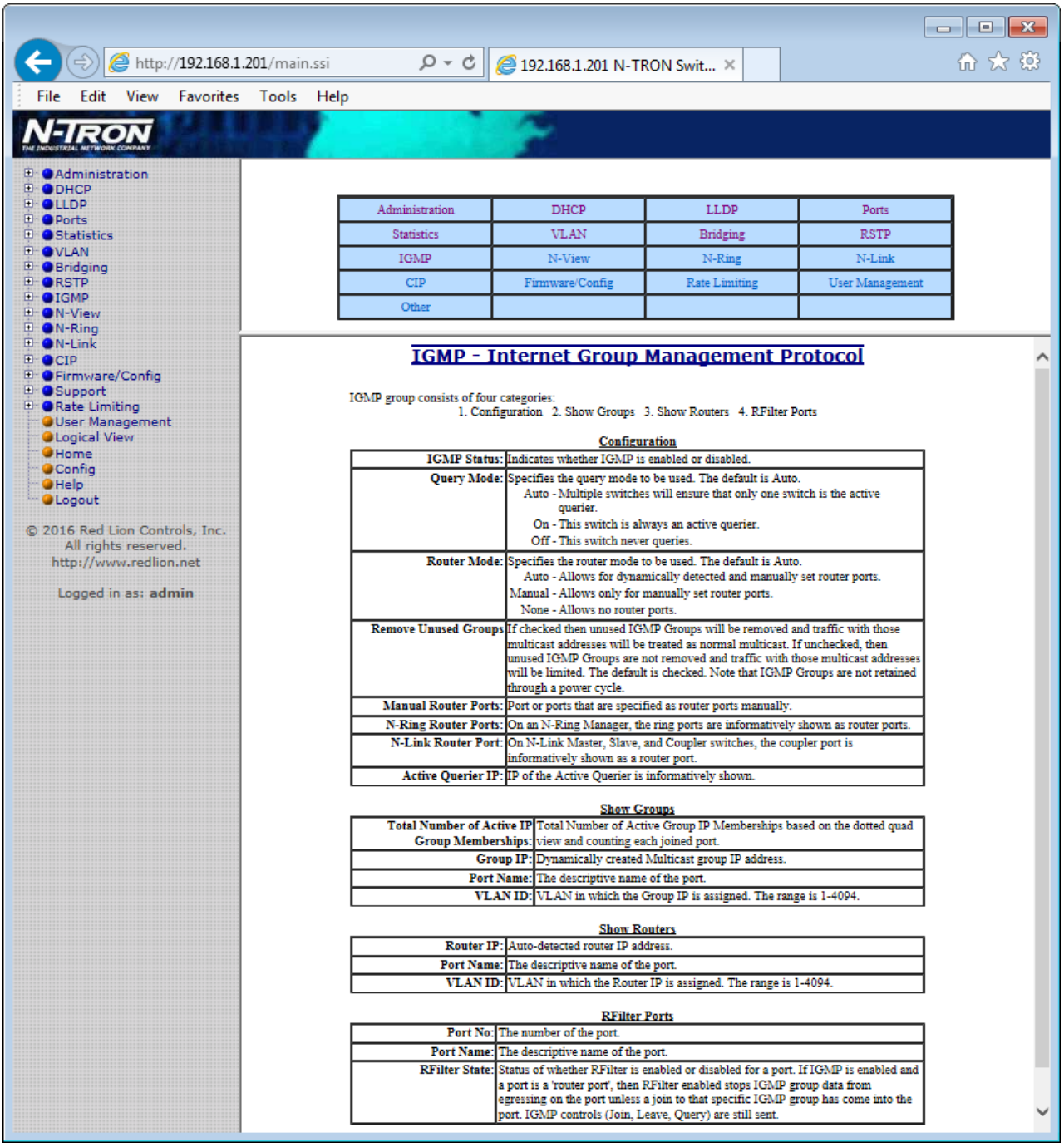
Default Configuration



MODIFYING RFILTER PORT SETTINGS



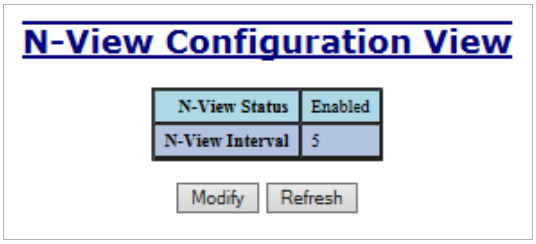
HELP > IGMP Following the IGMP link on the help page, the user or user can see some information regarding the configuration options in the IGMP category on the left side of the web management interface.



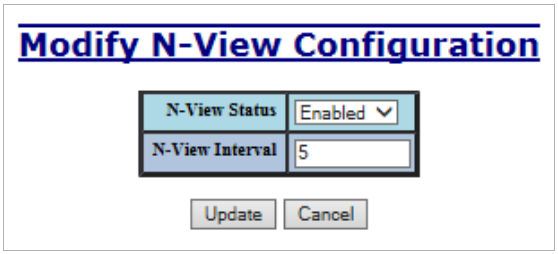
N-VIEW™

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.

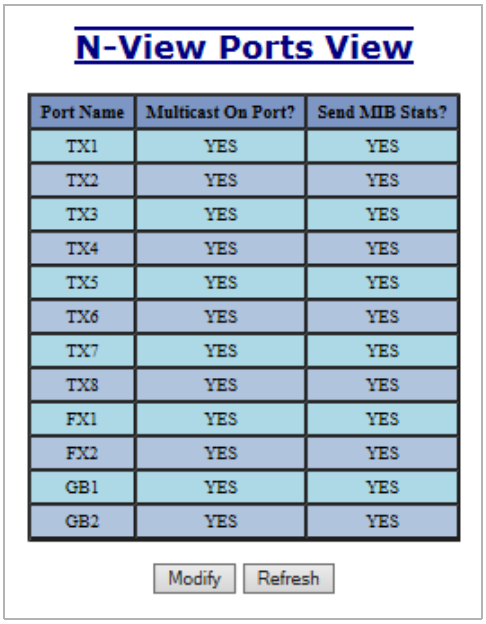


By selecting Modify on the above example, the user can modify the variable to change the frequency with which N-View reports information. Increasing the interval will slow the update rate. Decreasing the interval will allow N-View to report more frequently. Additionally, you may Disable or Enable N-View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

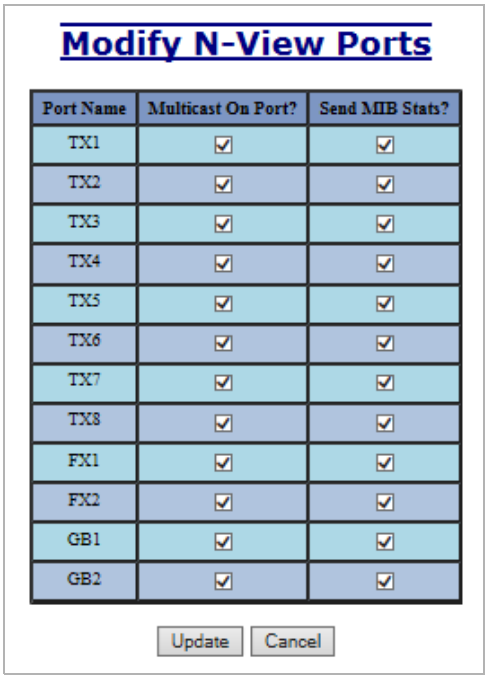


N-VIEW > PORTS

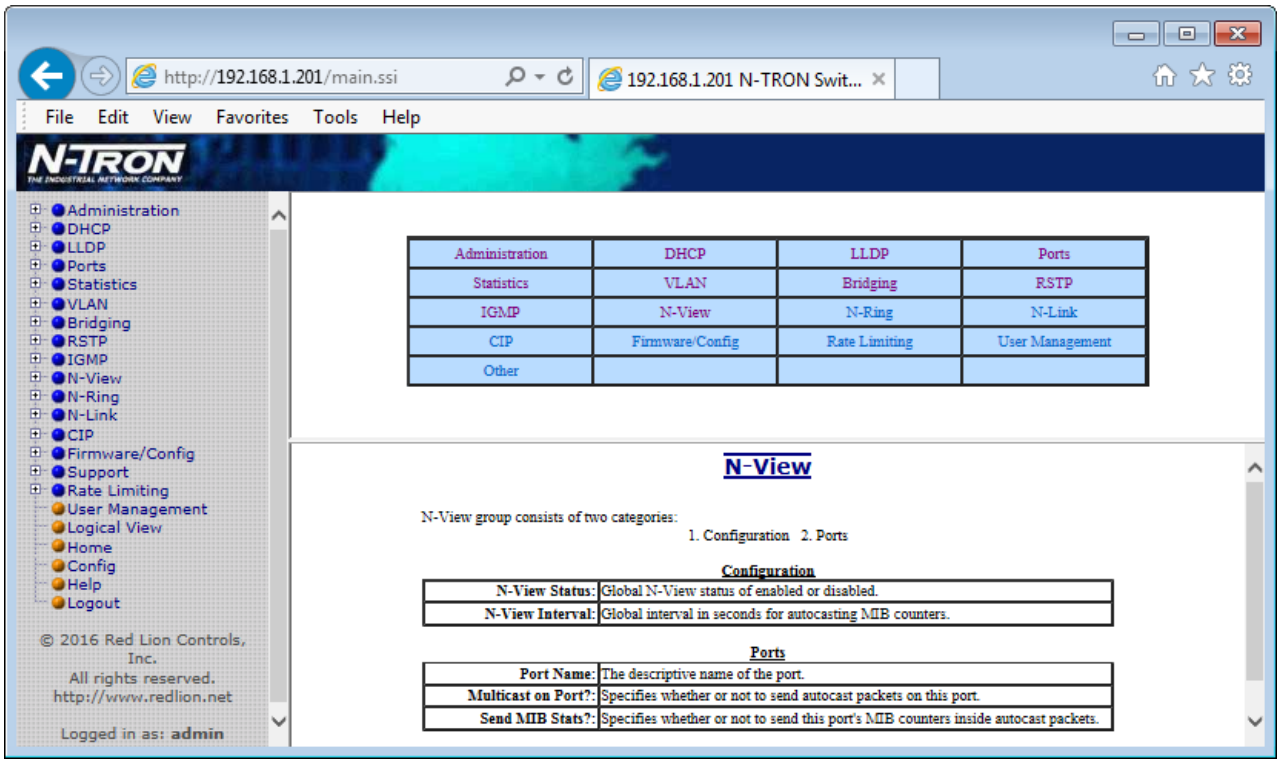
The Ports tab under the N-View category will display a list of all the switch ports along with the ports transmitting multicast packets and MIB stats respectively.



By selecting Modify on the above example, the user can modify these two variables to enable or disable multicast out of a port and if MIB statistics are sent out for those ports.



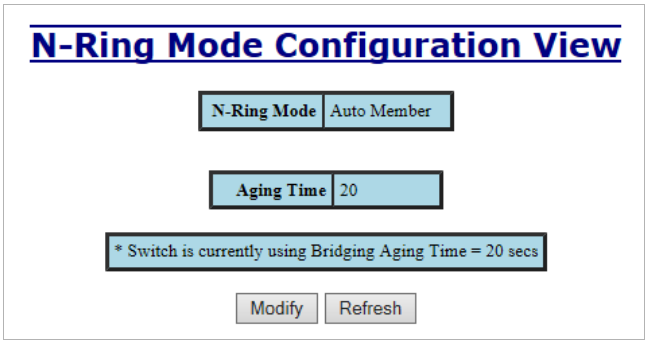
HELP > N-VIEW Following the N-View link on the help page, the user or user can see some information regarding the configuration options in the N-View category on the left side of the web management interface.



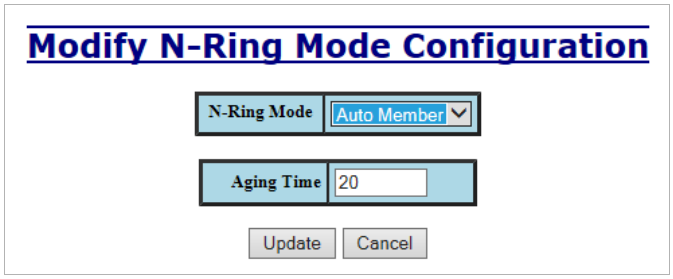
N-Ring™

N-Ring > Configuration

This tab displays the N-Ring basic configuration settings. By default, N-Ring is in Auto Member mode and the N-Ring Aging Time is 20 seconds.



By selecting Modify on the above example, the user will see a list of configurable fields for the N-Ring configuration, as below.



N-Ring Aging Time

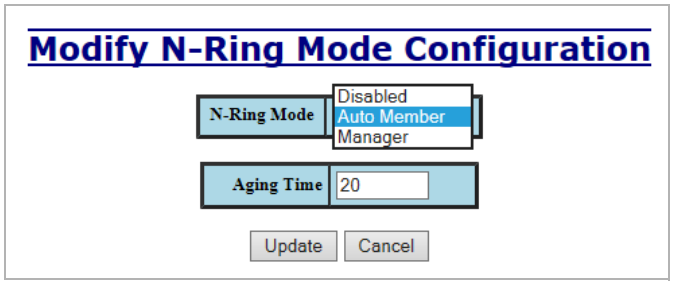
The N-Ring Aging Time has a default of 20 seconds and is separate from the Bridging Aging Time. N-Ring Aging Time overrides the Bridging Aging Time when the switch is an N-Ring Manager or becomes an active N-Ring Member.

Configuration Notes

- N-Ring Manager cannot have RSTP or Trunking enabled.
- RSTP & N-Ring are different modes and cannot share links or segments along those lines.
- See the examples in the RSTP configuration section.
- Do not use Trunking on an N-Ring manager. Do not connect the N-Ring to actively Trunking ports on an Auto Member.
- Do not create redundant links unless either RSTP or N-Ring is enabled.
- Any one 700/7000 can only participate in one N-Ring.
- 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.

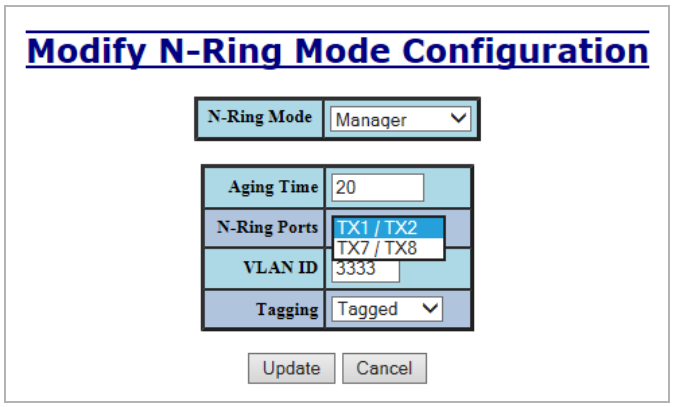
N-Ring Mode

The “N-Ring Mode” is one of three: Auto Member, Manager or Disabled.

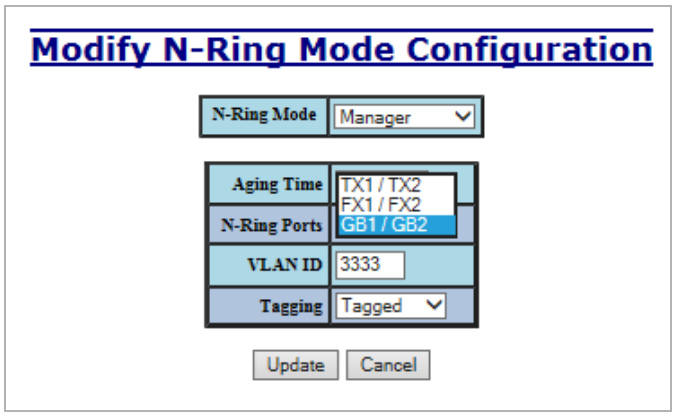


If N-Ring Mode is “Manager”, then a pull-down allows selection of ports available for use as N-Ring ports. The port sets vary depending on the switch model.

(Model 708FX2 shown below)

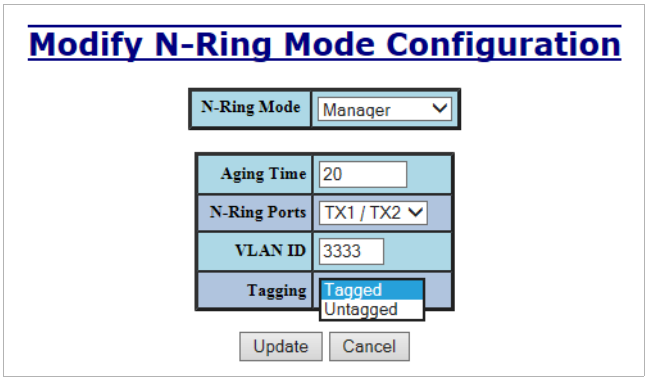


(Model 7012FX2 shown below)



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.



Note: Since VLANs are implemented for security reasons as well as traffic flow, N-Ring only makes minimal changes. It is up to the user to ensure that VLANs are configured correctly on the N-Ring manager and all N-Ring members.

Note: 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.

Note: 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 user 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

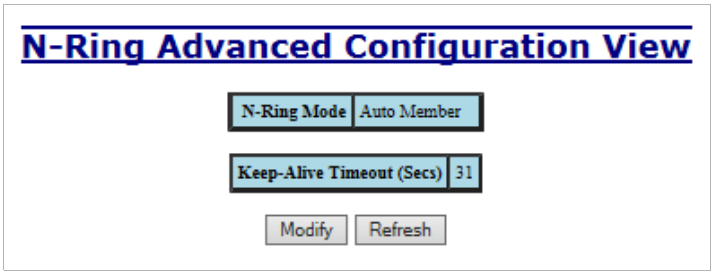
If switch is an N-Ring Member, the following settings will be shown:

N-Ring Mode

Current N-Ring mode of switch.

Keep-Alive Timeout

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



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

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

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

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

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

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

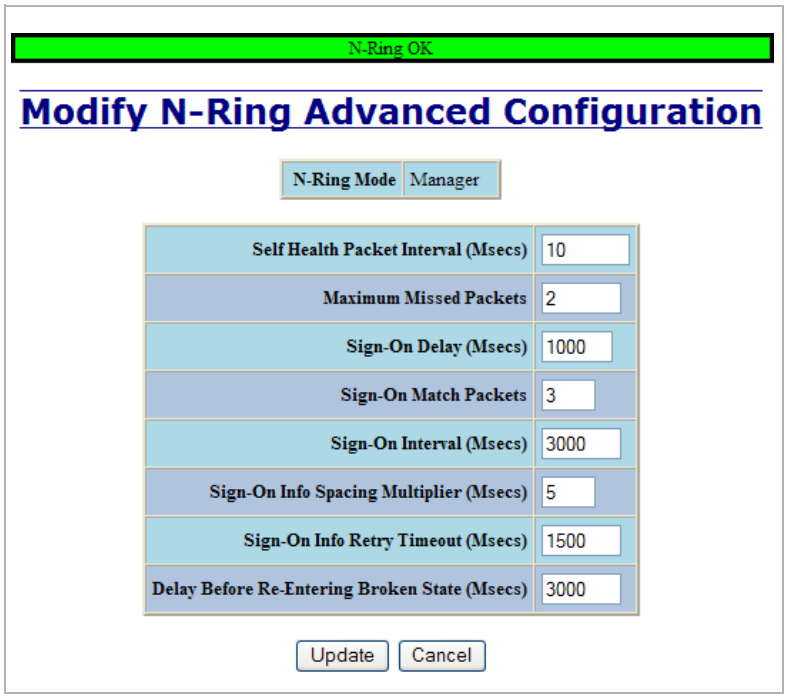
Sign-On Interval
The interval of time to wait in milliseconds before requesting subsequent sign-on information from ring members when the ring is broken. The default is 3000.

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

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

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

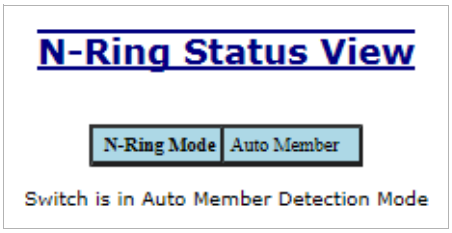
N-Ring OK
N-Ring Advanced Configuration View
N-Ring Mode
Manager
Self Health Packet Interval (Msecs)
10
Maximum Missed Packets
2
Sign-On Delay (Msecs)
1000
Sign-On Match Packets
3
Sign-On Interval (Msecs)
3000
Sign-On Info Spacing Multiplier (Msecs)
5
Sign-On Info Retry Timeout (Msecs)
1500
Delay Before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


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

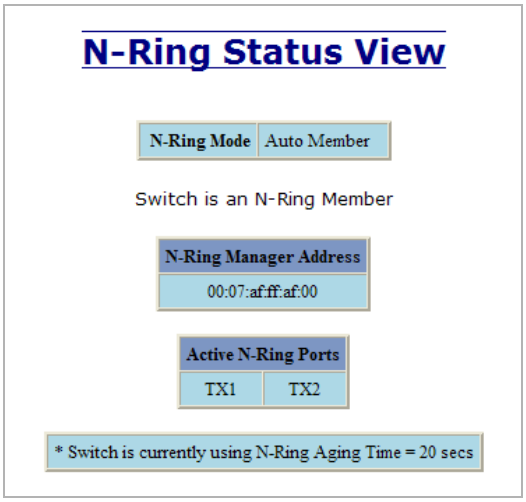
N-Ring > Status

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

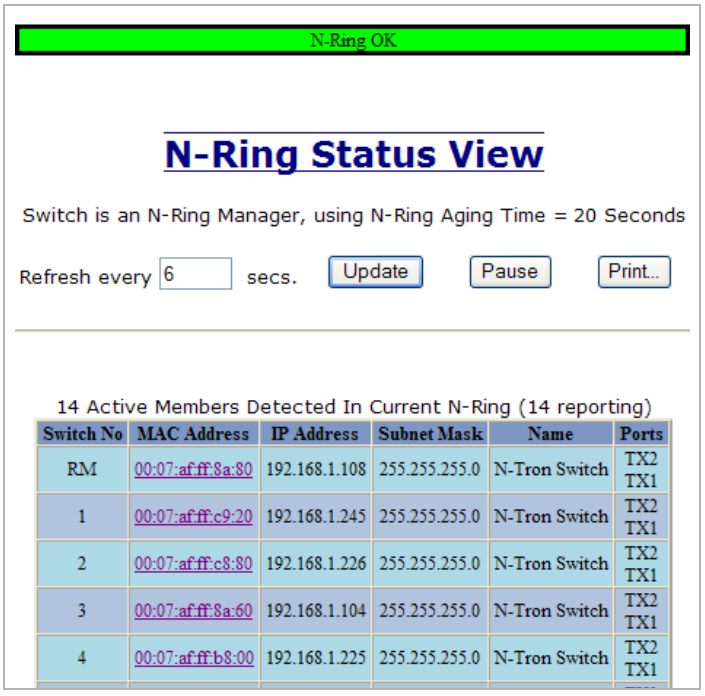
Below is an example of N-Ring Status from a switch in defaults (N-Ring Auto Member) that is not an N-Ring Manager and has not become an “Active” N-Ring Member:



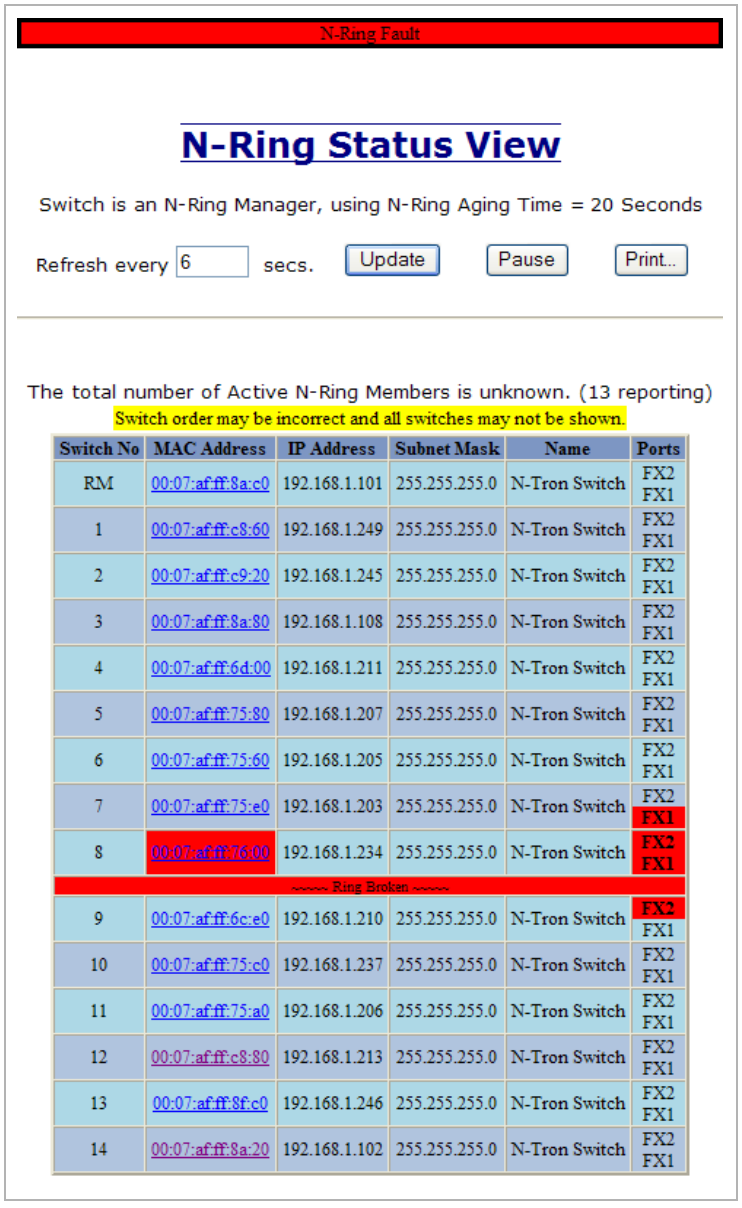
Below is an example of N-Ring Status from an “Active” N-Ring Member:



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

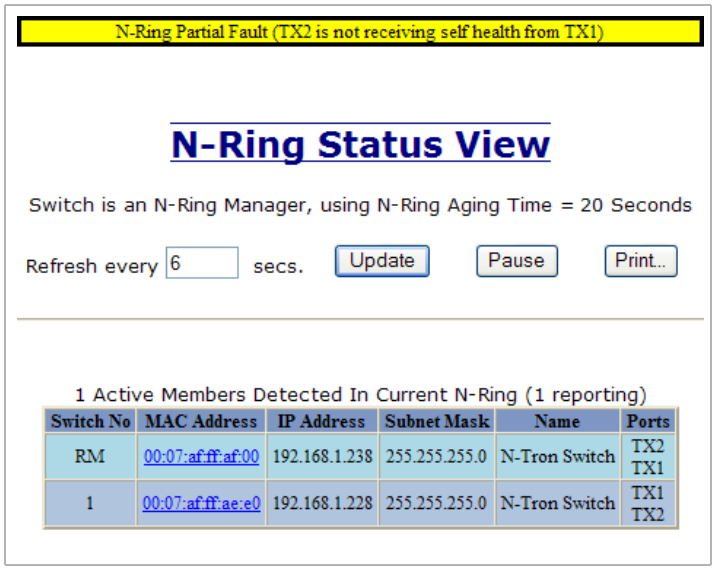


Below is an example of N-Ring Status from an N-Ring Manager with a faulted N-Ring. The red fields on the N-Ring Map show problems. Ports that are red indicate that the port is not linked. MAC addresses that are red indicate that there is no communication to that switch. The red “Ring Broken” line shows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

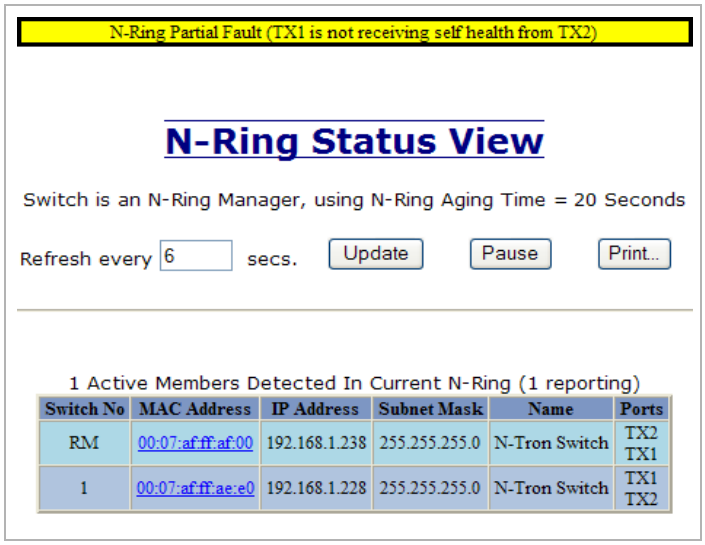


Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	00:07:af:ff:8a:c0	192.168.1.101	255.255.255.0	N-Tron Switch	FX2 FX1
1	00:07:af:ff:c8:60	192.168.1.249	255.255.255.0	N-Tron Switch	FX2 FX1
2	00:07:af:ff:c9:20	192.168.1.245	255.255.255.0	N-Tron Switch	FX2 FX1
3	00:07:af:ff:8a:80	192.168.1.108	255.255.255.0	N-Tron Switch	FX2 FX1
4	00:07:af:ff:6d:00	192.168.1.211	255.255.255.0	N-Tron Switch	FX2 FX1
5	00:07:af:ff:75:80	192.168.1.207	255.255.255.0	N-Tron Switch	FX2 FX1
6	00:07:af:ff:75:60	192.168.1.205	255.255.255.0	N-Tron Switch	FX2 FX1
7	00:07:af:ff:75:e0	192.168.1.203	255.255.255.0	N-Tron Switch	FX2 FX1
8	00:07:af:ff:76:00	192.168.1.234	255.255.255.0	N-Tron Switch	FX2 FX1
~~ Ring Broken ~~~~~					
9	00:07:af:ff:6c:e0	192.168.1.210	255.255.255.0	N-Tron Switch	FX2 FX1
10	00:07:af:ff:75:c0	192.168.1.237	255.255.255.0	N-Tron Switch	FX2 FX1
11	00:07:af:ff:75:a0	192.168.1.206	255.255.255.0	N-Tron Switch	FX2 FX1
12	00:07:af:ff:c8:80	192.168.1.213	255.255.255.0	N-Tron Switch	FX2 FX1
13	00:07:af:ff:8f:c0	192.168.1.246	255.255.255.0	N-Tron Switch	FX2 FX1
14	00:07:af:ff:8a:20	192.168.1.102	255.255.255.0	N-Tron Switch	FX2 FX1

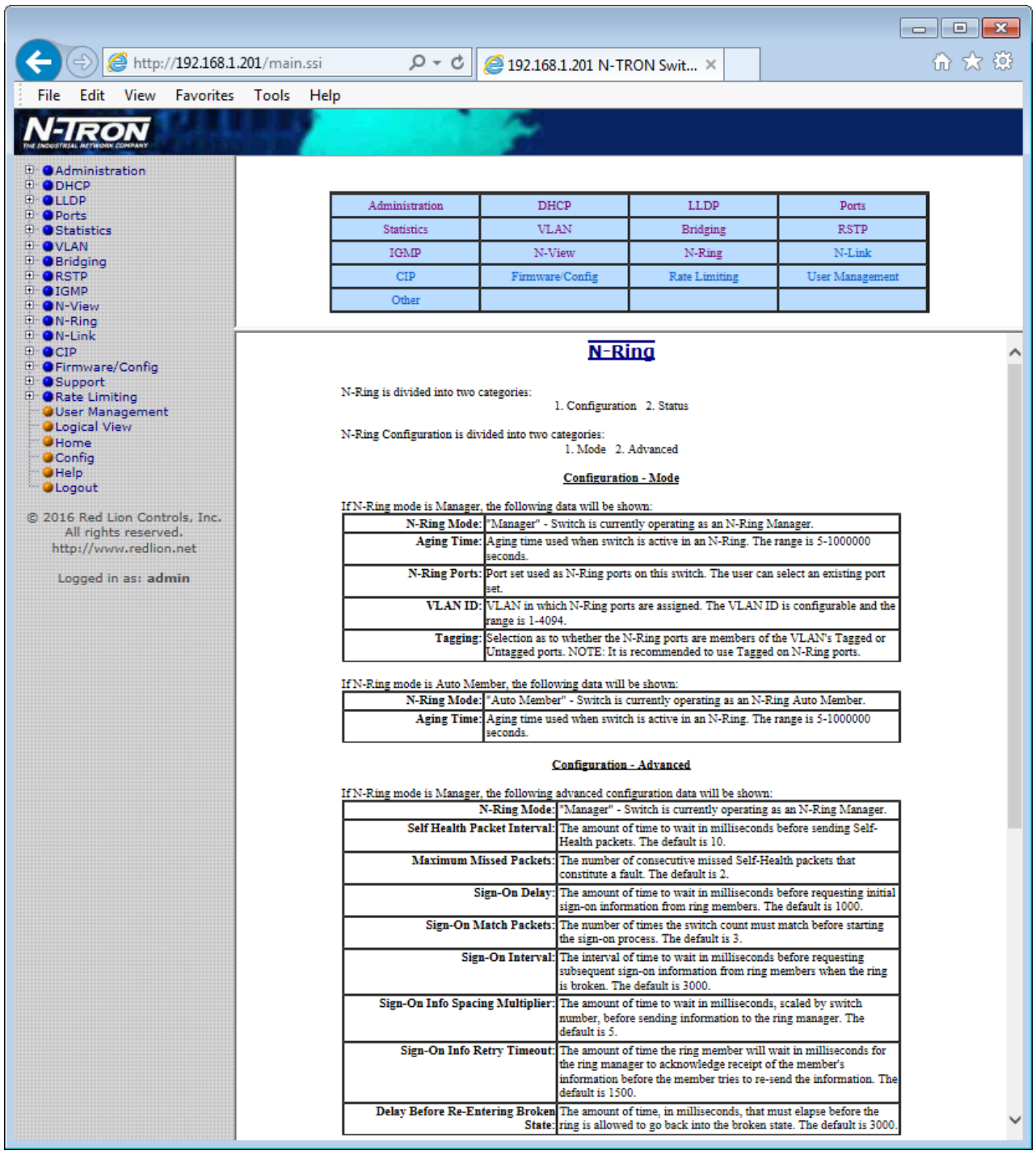
In rare cases an N-Ring can have a “Partial Fault”. An example of this is to have a break in just one fiber in a duplex channel fiber pair. The screenshot below shows N-Ring Manager Status when a ‘Higher’ N-Ring Port (TX2, TX8/FX2) on a 708 model or (TX2, TX8/FX2, or GB2) on a 7018 model is not receiving self health frames all the way around the N-Ring, though the other (low TX1, TX7/FX1) N-Ring port on a 708 model or (low TX1, TX7/FX1, or GB1) on a 7018 model is:



The screenshot below shows N-Ring Manager Status when a 'Lower' N-Ring Port (TX1 or TX7/FX1) on a 708 model or Port (TX1, TX7/FX1, or GB1) on a 7018 model is not receiving self health frames all the way around the N-Ring, though the other (high TX2 of TX8/FX2) on a 708 model or (high TX2, TX8/FX2, or GB2) on a 7018 model N-Ring port is:



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

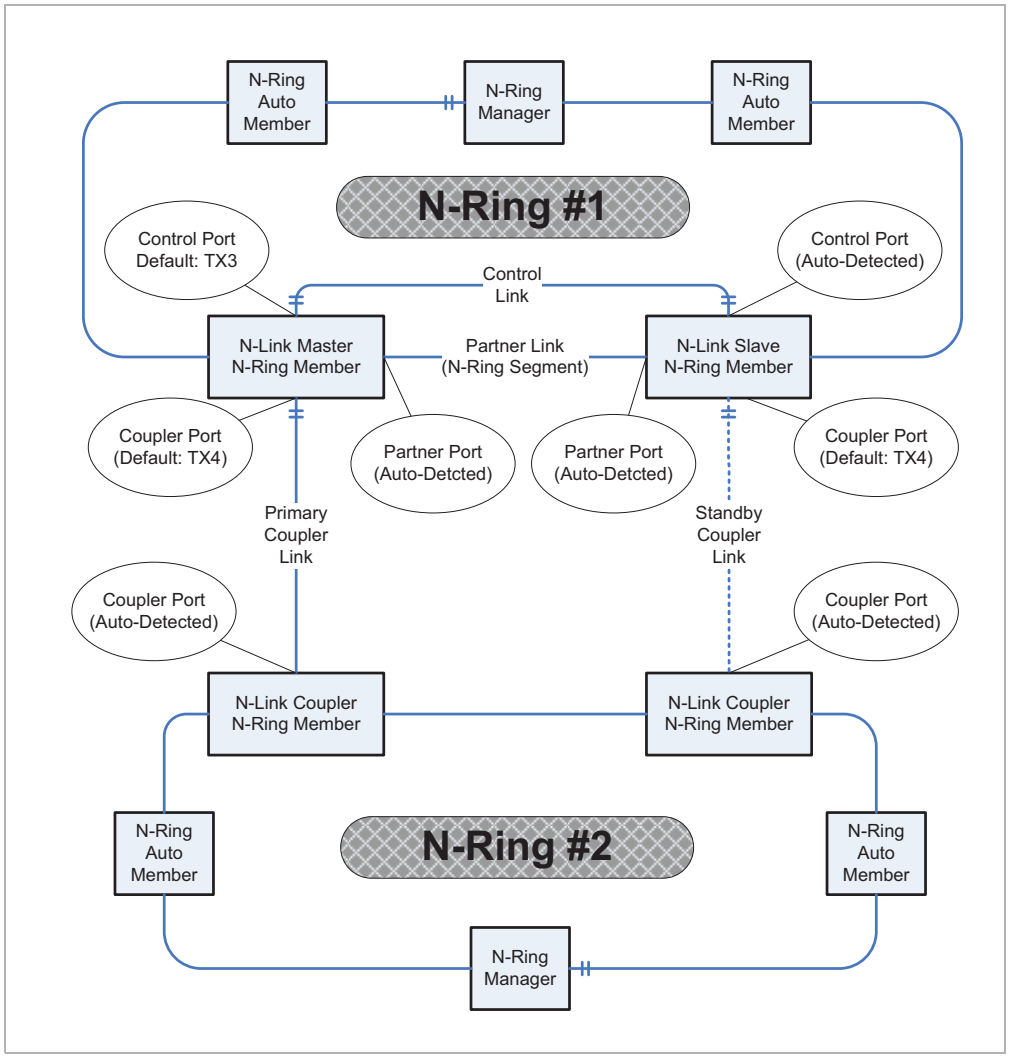


N-LINK™

N-LINK > CONFIGURATION

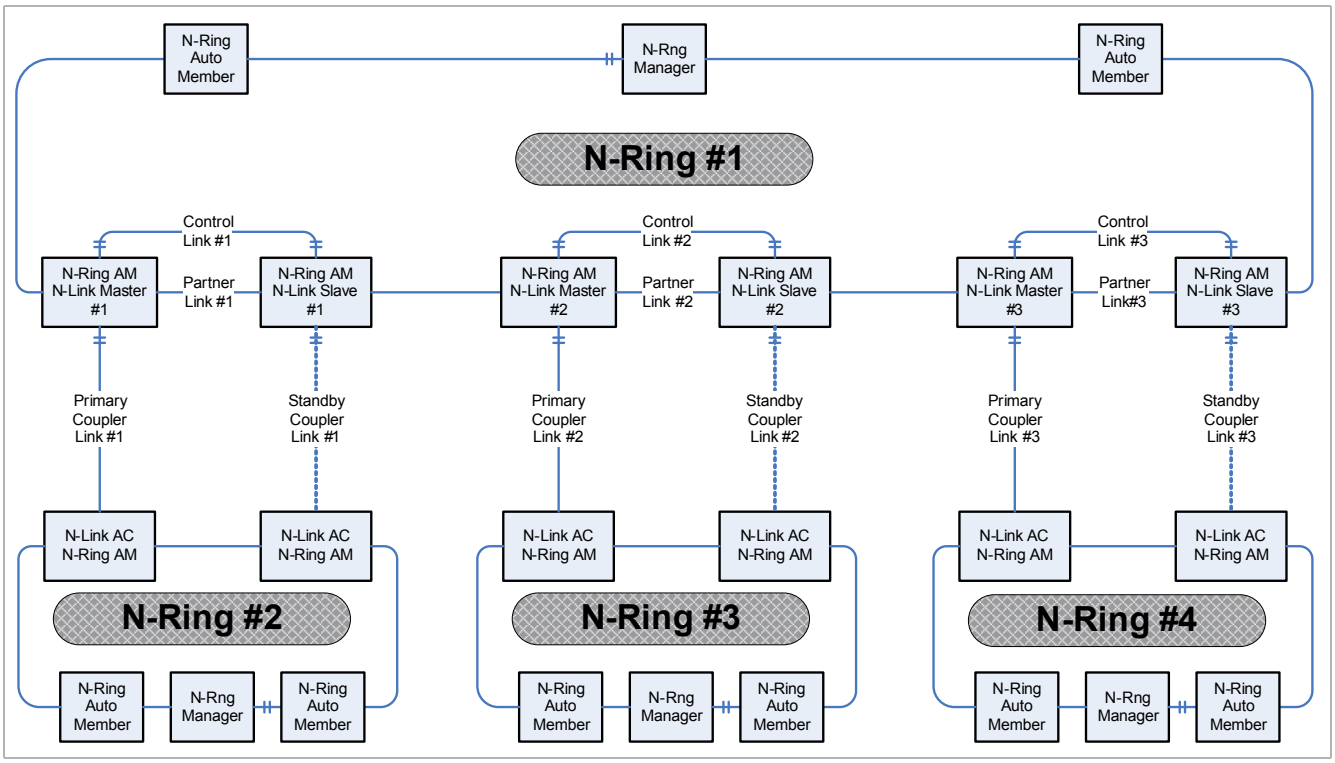
The purpose of N-Link is to provide a way to redundantly couple an N-Ring topology to one or more other topologies, usually other N-Ring topologies. Each N-Link configuration requires 4 switches: N-Link Master, N-Link Slave, N-Link Primary Coupler, and N-Link Standby Coupler.

STANDARD N-LINK CONFIGURATION (EXAMPLE)



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

Complex N-Link Configuration (Example)



Configuration Notes

- The Master and Slave must be part of the N-Ring topology.
- If using default configuration choices, the user 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 user 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.

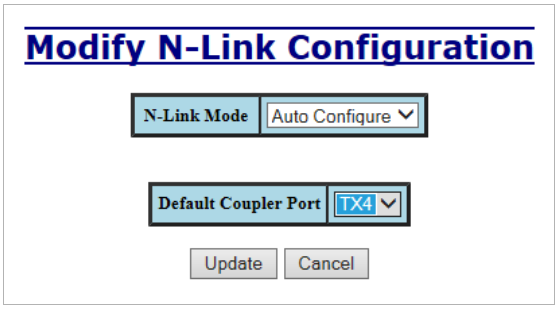
Configuration Steps to Redundantly Couple 2 N-Ring Networks

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.

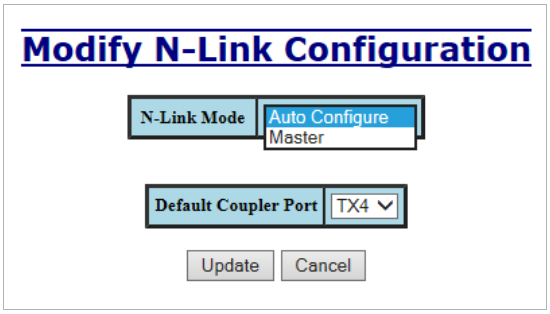
4. Configure N-Link Master: Select the Control and Coupler ports. Save the Configuration.
5. Connect the Control Link cable. Ensure that the Slave switch status now shows a state of “Slave”
6. Connect the Coupler Link cables.
7. Check N-Link status by selecting the N-Link Status View page.

MODIFYING N-LINK CONFIGURATION

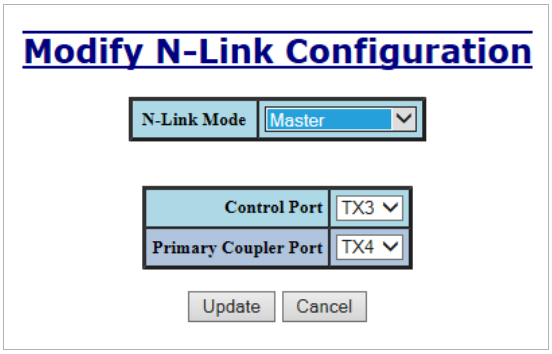
1. The Configuration tab under the N-Link category will display the configuration settings. By default, N-Link is in Auto Configure mode and will use TX4 as the Default Coupler port.
2. By selecting Modify on the above example, the user will see a list of configurable fields for the N-Link configuration, as below.



3. 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.
4. Once these fields are filled in to meet the needs of the user’s network, the changes may be saved by clicking the Update button at the bottom of the page.
5. The “N-Link Mode” is one of two choices, as below:



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



7. Once these fields are filled in to meet the needs of the user'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.

Table 2-1 Switch N-Link Status

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

Table 2-2 Switch N-Link Partner Information

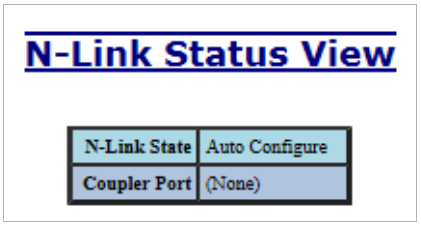
Status Field	Description
State:	Current N-Link mode of switch.
MAC:	The MAC Address of the N-Link Partner switch.
Coupler Port State:	Blocking, Forwarding.
Status:	No errors will show "OK", otherwise a description of the Faults detected.

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

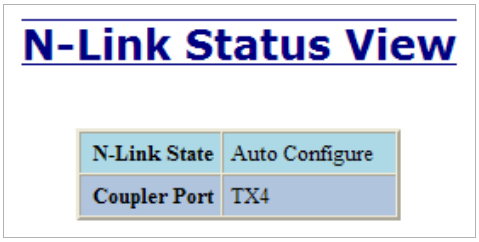
Table 2-3 Switch N-Link Auto Configure Information

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

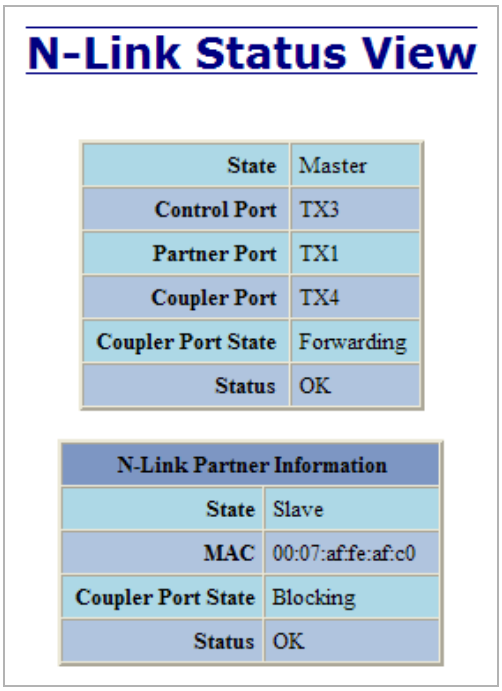
Below is an example of N-Link Status from a switch in defaults (N-Link Auto Configure) that is not an N-Link Master and has not become an N-Link Slave or an N-Link Coupler.



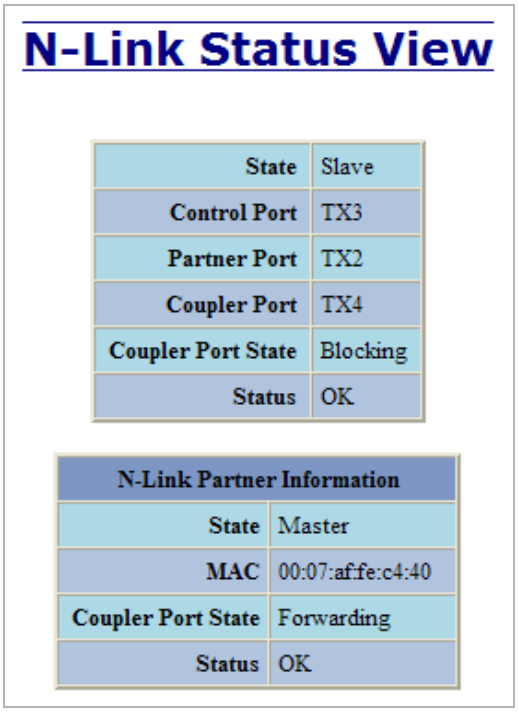
Below is an example of N-Link Status from an N-Link Coupler switch:



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



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

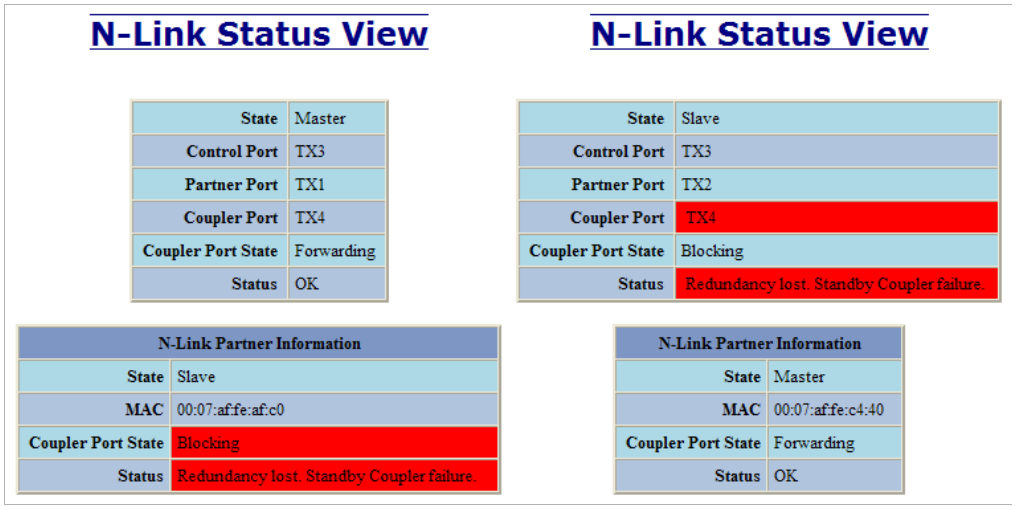


N-Link Status View

State	Slave
Control Port	TX3
Partner Port	TX2
Coupler Port	TX4
Coupler Port State	Blocking
Status	OK

N-Link Partner Information	
State	Master
MAC	00:07:af:fe: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:



N-Link Status View

State	Master
Control Port	TX3
Partner Port	TX1
Coupler Port	TX4
Coupler Port State	Forwarding
Status	OK

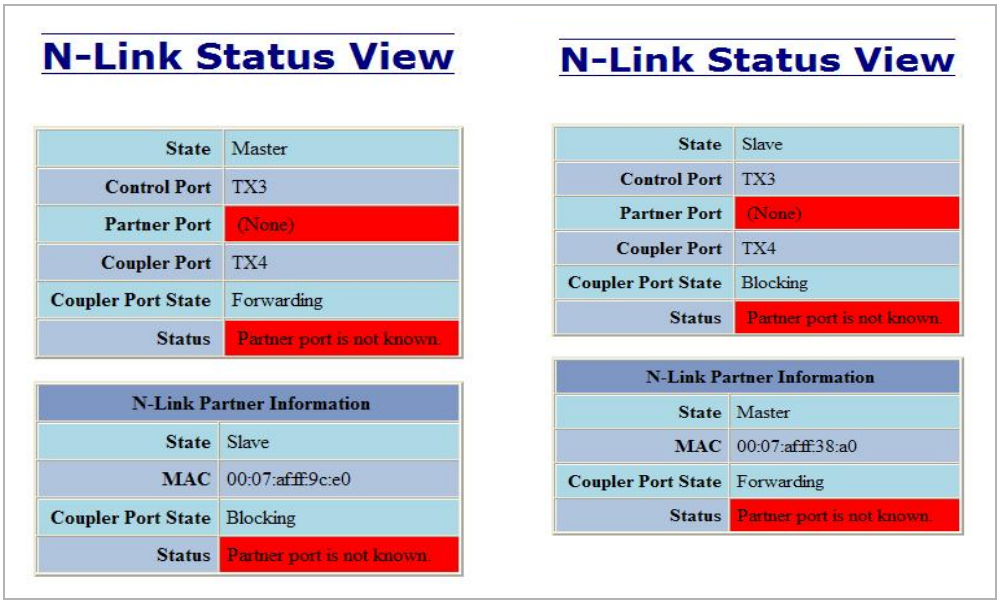
N-Link Partner Information	
State	Slave
MAC	00:07:af:fe:af:c0
Coupler Port State	Blocking
Status	Redundancy lost. Standby Coupler failure.

N-Link Status View

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

N-Link Partner Information	
State	Master
MAC	00:07:af:fe: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 Standby Coupler link is broken:



N-Link Status View

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

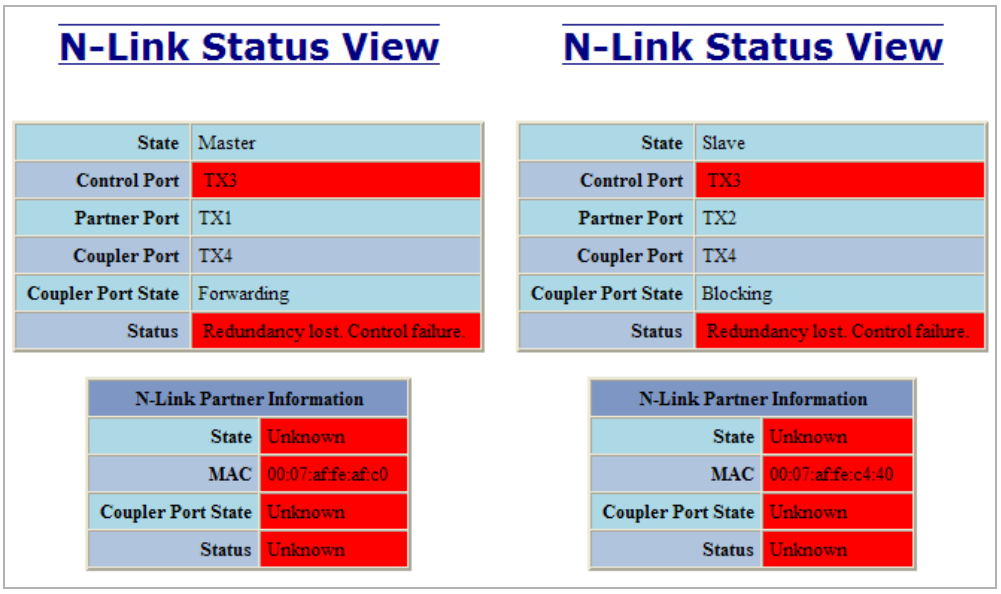
N-Link Partner Information	
State	Slave
MAC	00:07:afff:9c:e0
Coupler Port State	Blocking
Status	Partner port is not known.

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:afff:38:a0
Coupler Port State	Forwarding
Status	Partner port is not known.

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.

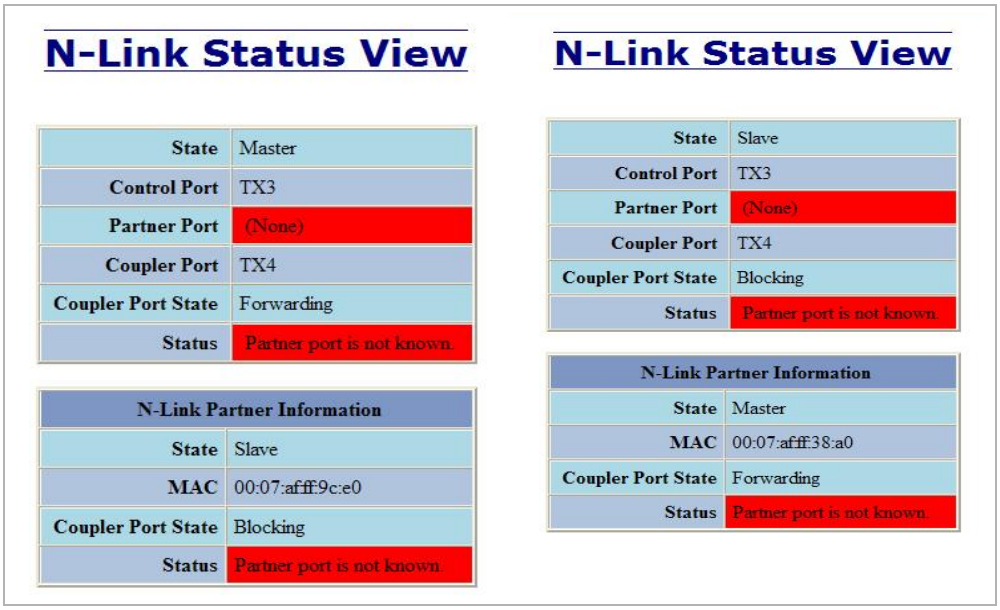
N-Link Partner Information	
State	Unknown
MAC	00:07:af:fe:af:c0
Coupler Port State	Unknown
Status	Unknown

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:af:fe:c4:40
Coupler Port State	Unknown
Status	Unknown

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



N-Link Status View

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

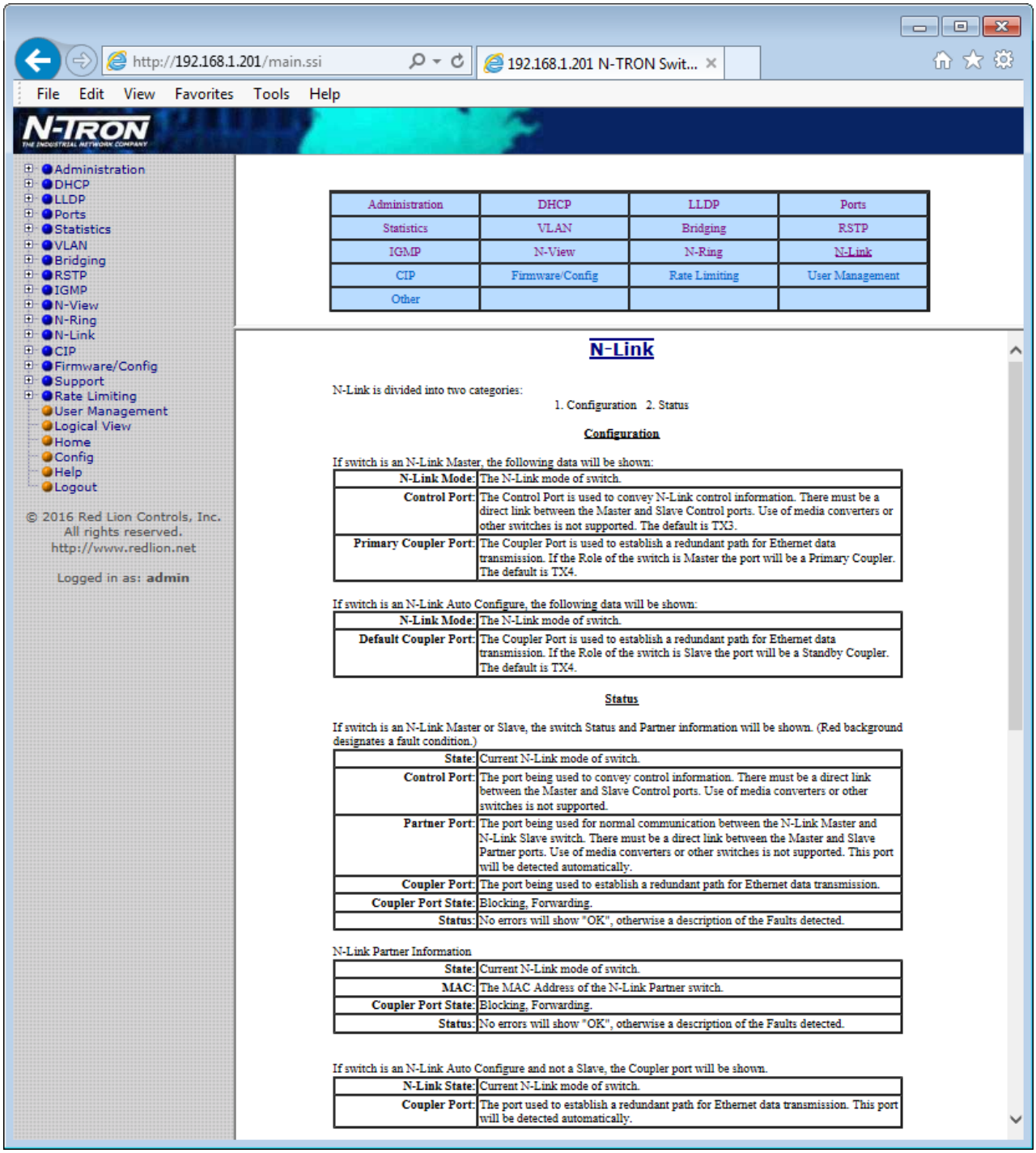
N-Link Partner Information	
State	Slave
MAC	00:07:afff:9c:e0
Coupler Port State	Blocking
Status	Partner port is not known.

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:afff:38:a0
Coupler Port State	Forwarding
Status	Partner port is not known.

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



CIP™

CIP > Configuration

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

CIP Status

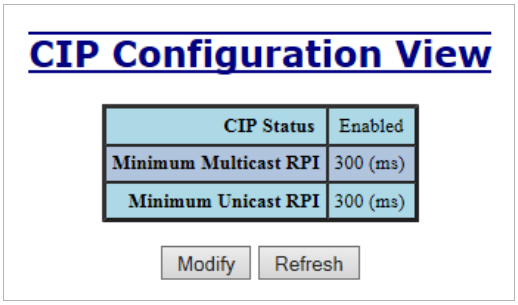
Enables or Disables CIP on the Switch. Default: Enabled.

Minimum Multicast RPI:

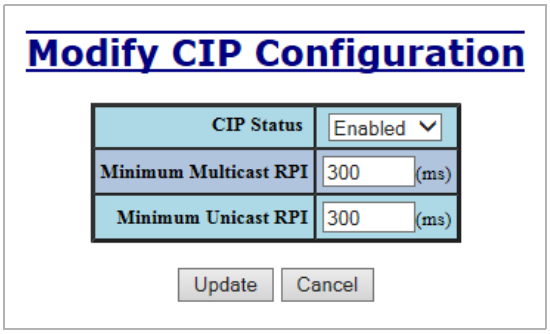
The minimum Requested Packet Interval for Class 1 (multicast) connections, in milliseconds. Requests for less than this value will be rejected. Default = 1 second.

Minimum 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.



By selecting Modify on the above example, the user can modify the variables. Additionally, you may Disable or Enable CIP altogether.



CIP > Status

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

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

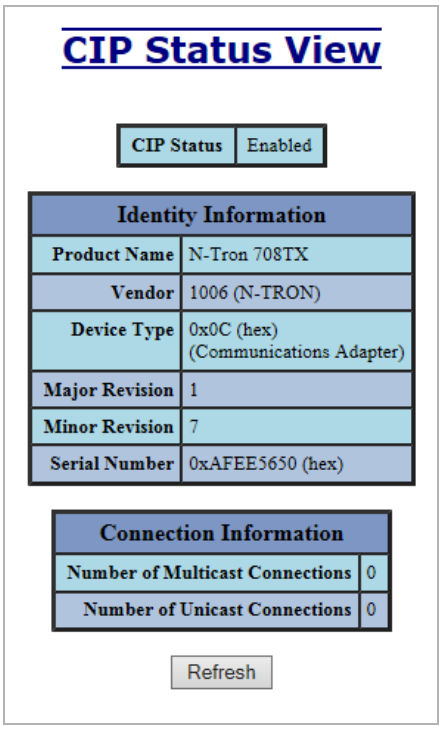
Table 2-4 Switch CIP Identity Information

Status Field	Description
Product Name:	Switch Model Number.
Vendor:	This is N-Tron's ODVA Ethernet/IP Vendor ID (1006).
Device Type:	The ODVA Device Type is Communications Adapter (= 0x0C hex).
Major Revision:	The Major Revision of the CIP implementation.

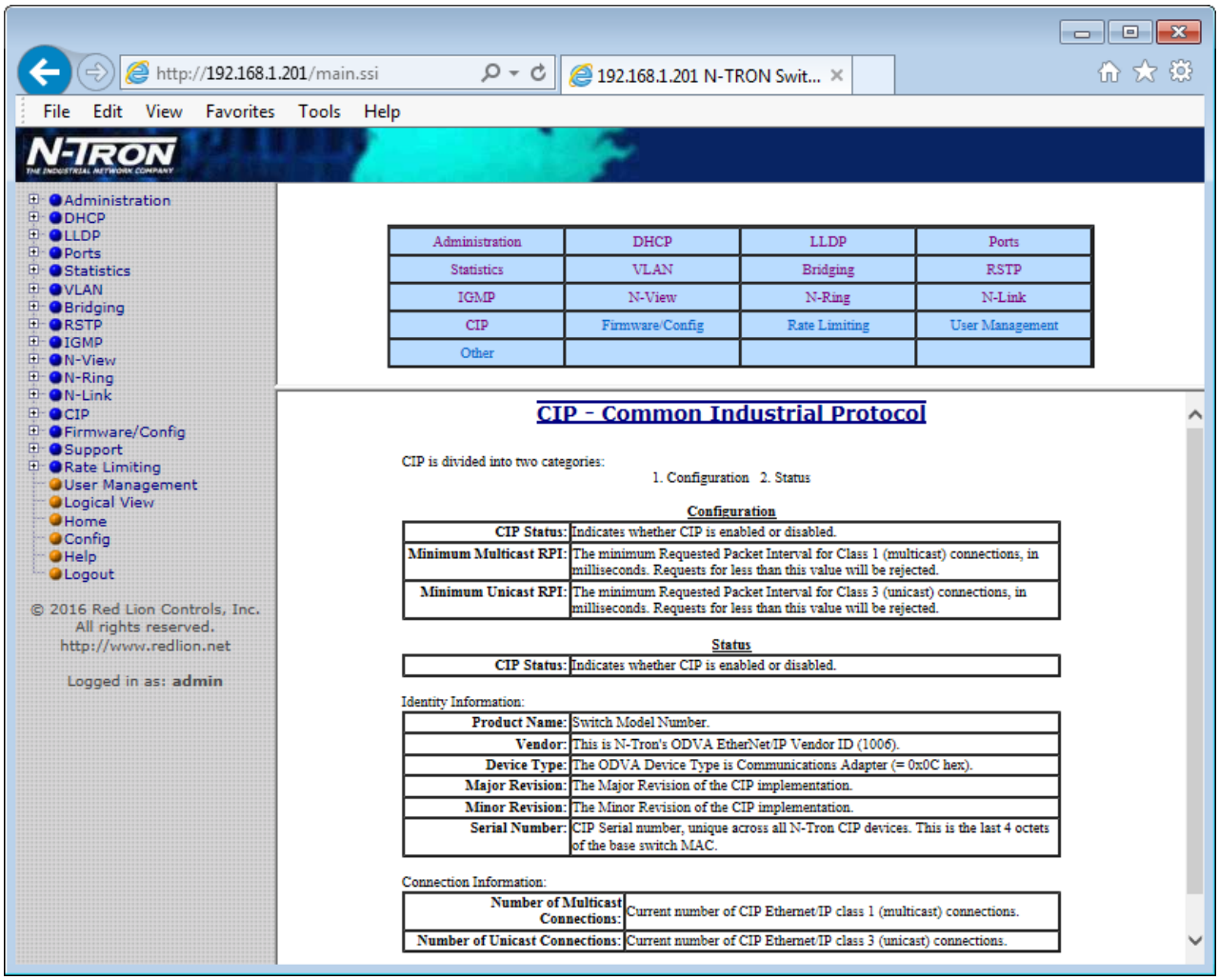
Status Field	Description
Minor Revision:	The Minor Revision of the CIP implementation.
Serial Number (hex):	CIP Serial number, unique across all N-Tron CIP devices. This is the last 4 octets of the base switch MAC.

Table 2-5 Switch CIP Connection Partner Information

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



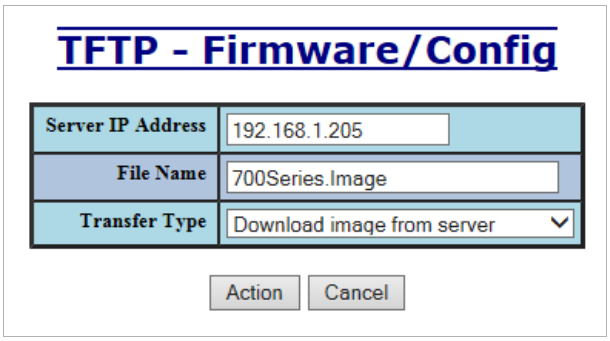
HELP > CIP Following the CIP link on the help page, the user or user can see some information regarding the configuration options in the CIP category on the left side of the web management interface.

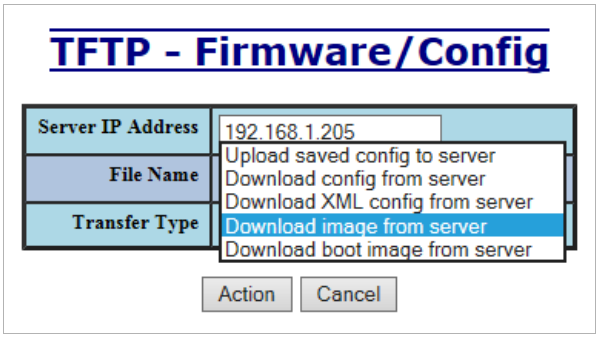


FIRMWARE/CONFIG

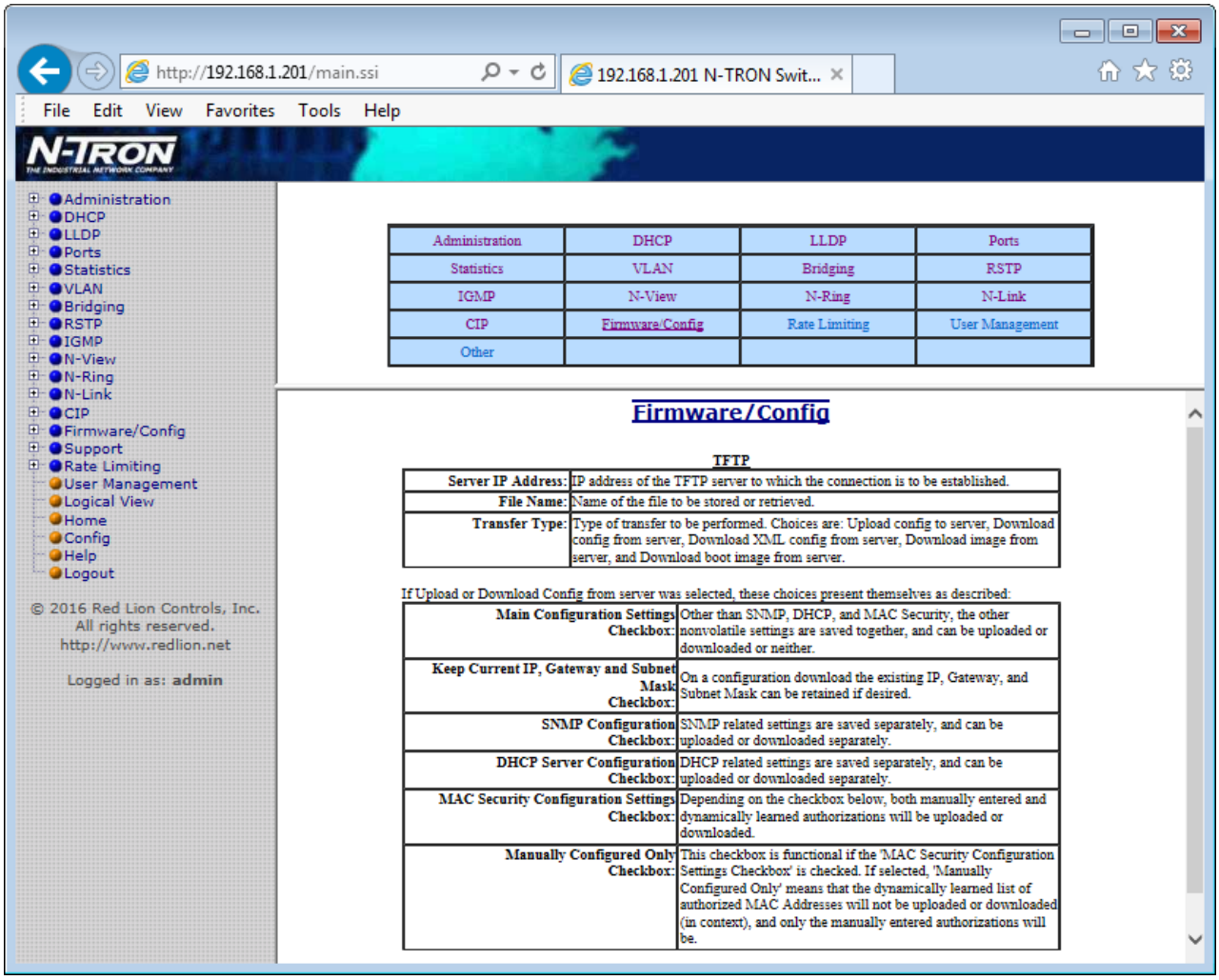
FIRMWARE/CONFIG > TFTP

The TFTP tab under the Firmware/Config category gives an administrator the ability to upload or download a settings configuration file for a 700/7000 model switch. This allows an user to backup their configurations in case they need to reload their custom configurations at a later time. An administrator can also download an Image or Boot Image file to the switch via TFTP, allowing them to update the firmware without losing their current configurations and without having to send the unit back to Red Lion for updates. It is important not to cycle power on the switch or interrupt the data connection between the TFTP server and the switch while downloading or uploading a file. The switch will not stop working if this does occur, but the user will have to re-transfer the file.





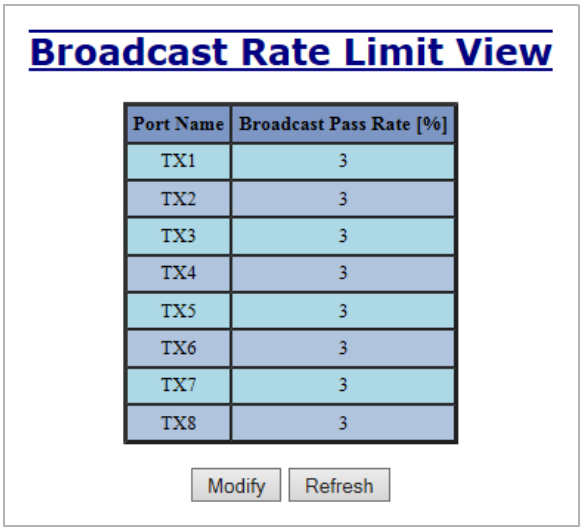
HELP > FIRMWARE/CONFIG Following the Firmware/Config link on the help page, the user or user can see some information regarding the configuration options in the Firmware/Config category on the left side of the web management interface.



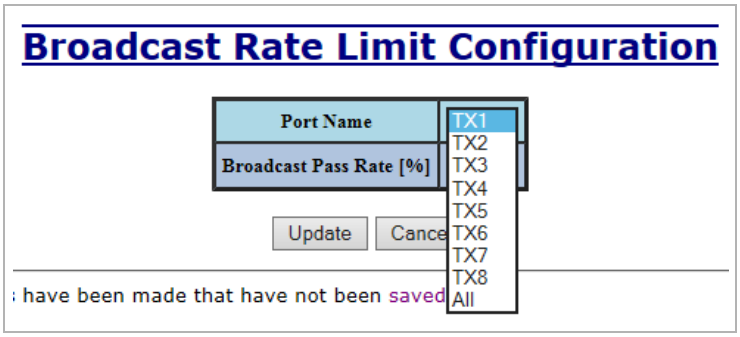
Rate Limiting

Rate Limiting > Broadcast

The Rate Limiting link will display the Broadcast Packet Count Limiting (BPCL) Configuration for all installed ports. Rate Limiting defaults to 3%.

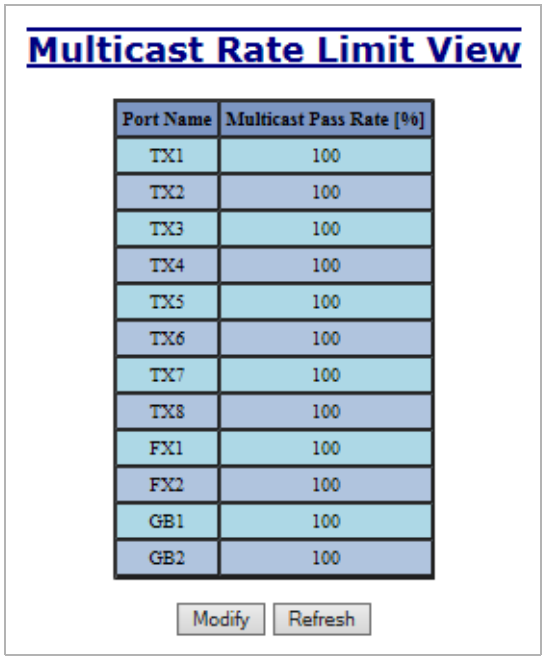


By selecting Modify on the above example, the user can modify the BPCL Percentage for each port.

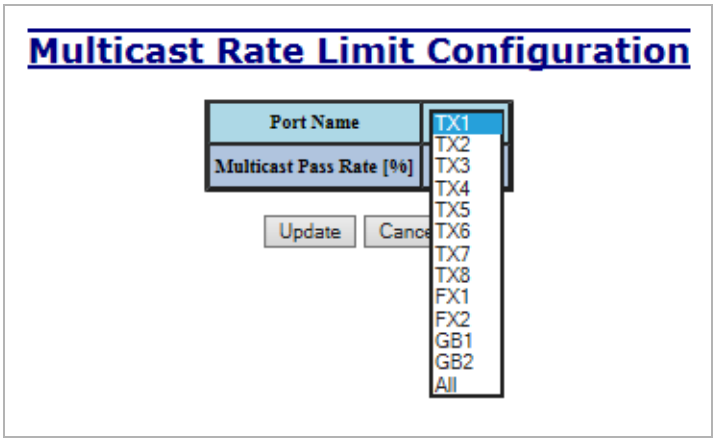


RATE LIMITING > MULTICAST

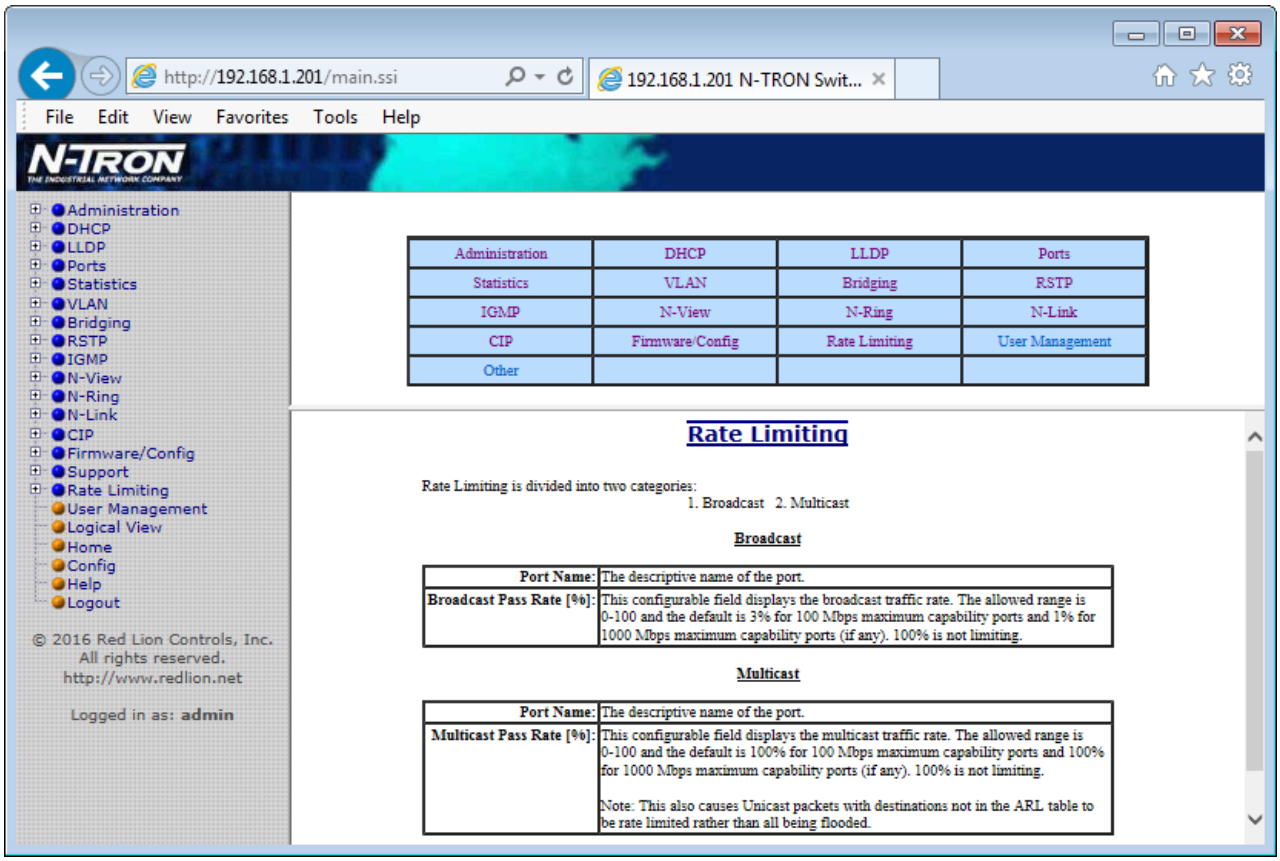
The Rate Limiting link will display the Multicast Packet Count Limiting (MPCL) Configuration for all installed ports. Rate Limiting defaults to 3%.



By selecting Modify on the above example, the user can modify the MPCL Percentage for each port.



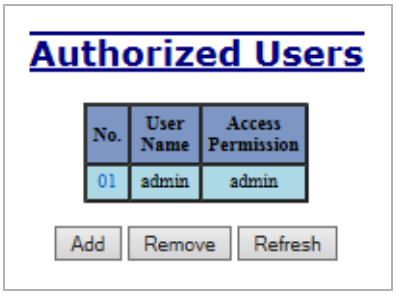
HELP > RATE LIMITING Following the Rate Limiting link on the help page, the user or user can see some information regarding the configuration options in the Broadcast and Multicast rate limiting category on the left side of the web management interface.



User Management

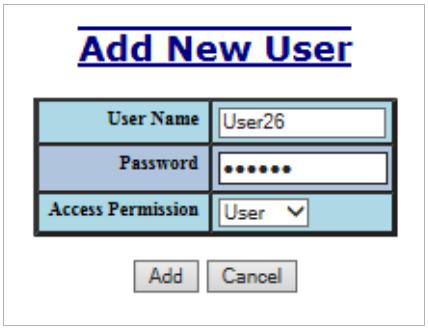
User Management > Authorized Users

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.

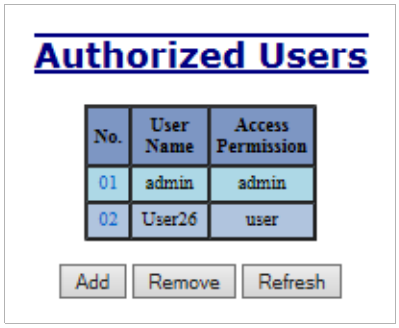


User Management > Add User

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

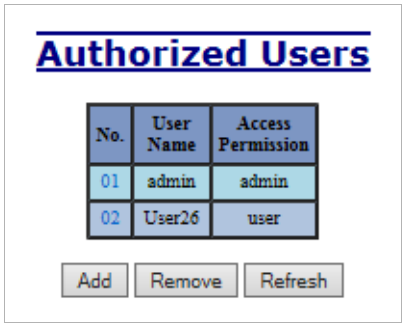


The new user will be added to the table of Authorized Users.



User Management > Remove User

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



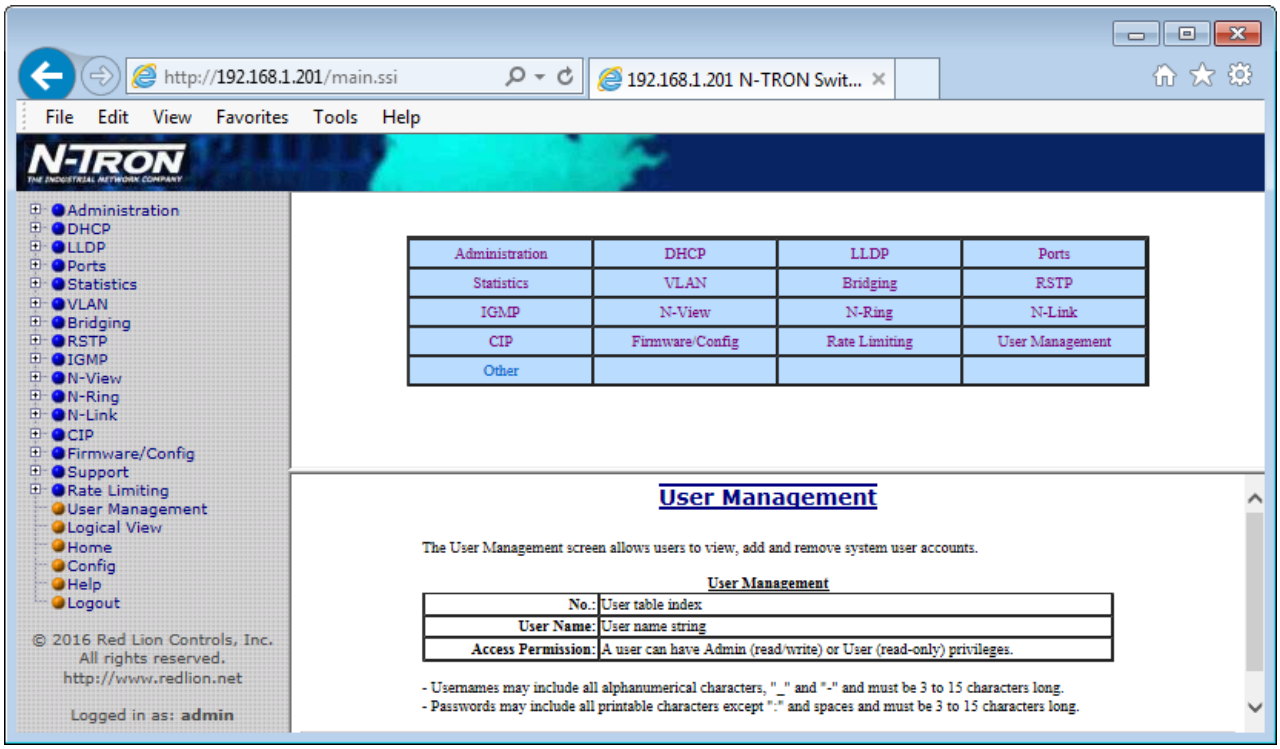
Following the Remove button on the above example, the user can remove a user by entering in the user's name and clicking the Remove button.

The user will be removed from the table of Authorized Users.

Note: There are a maximum number of 5 users per switch. User access permissions grants the right to view switch configurations and to view port settings, but not to make changes to these settings. Admin access permissions grants the right to change and view switch configurations and to change and view port settings.

HELP > USER MANAGEMENT

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

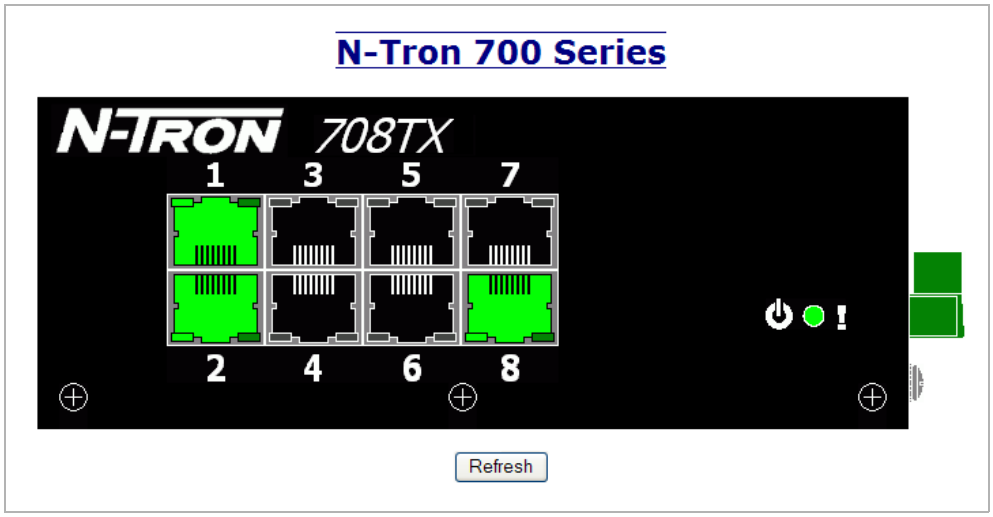


LOGICAL VIEW

The Web Management interface offers a logical view of the switch. Here a user or user can see a graphical depiction of the switch. Ports that are linked will appear in green, while ports that are not linked will appear in black.

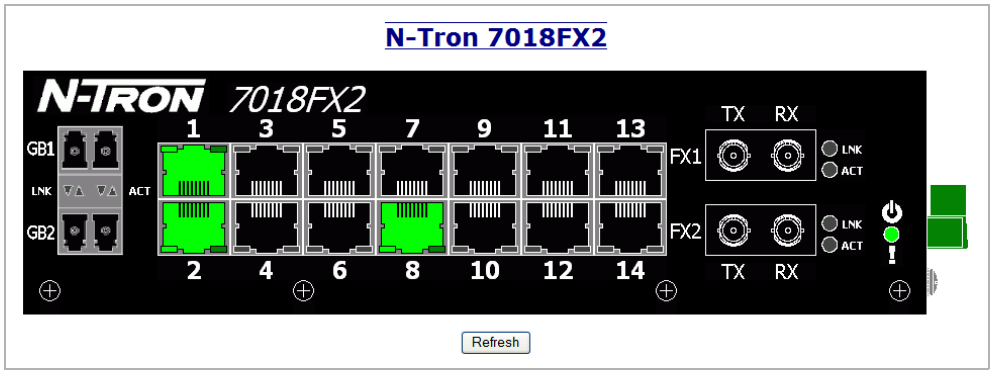
700 MODEL

The example below of an N-Tron Series 708TX model shows ports 1, 2, and 8 linked. The other ports are currently in the down state (not linked).



7018 MODEL

The example below of an N-Tron Series 7018FX2 model shows ports 1, 2, and 8 linked. The other ports are currently in the down state (not linked).



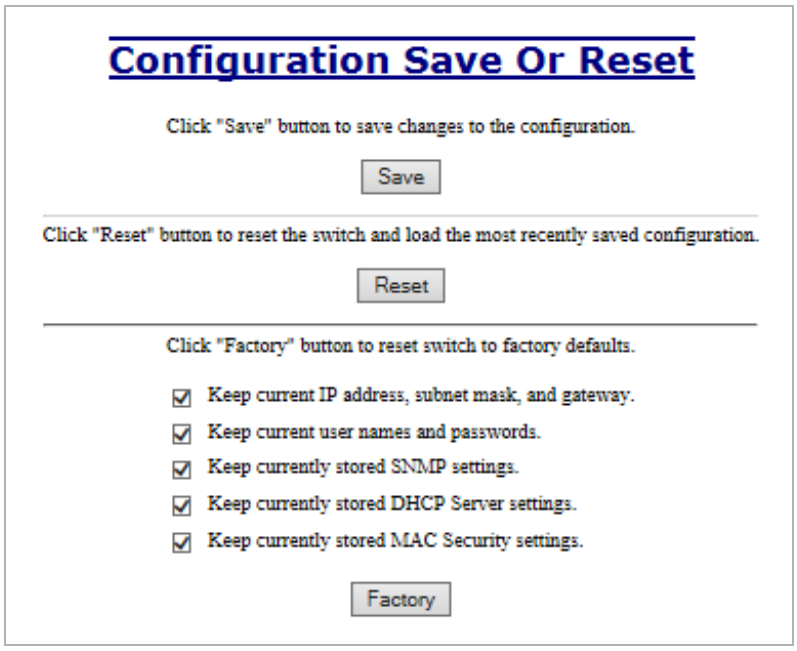
CONFIGURATION

The Configuration section of the web management interface gives an user the ability to save a running configuration into the NVRAM. This allows the switch to remember any changes after a power cycle.

CONFIGURATION > SAVE The “Save” button will save all current changes made to the configuration for use after the next power cycle.

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

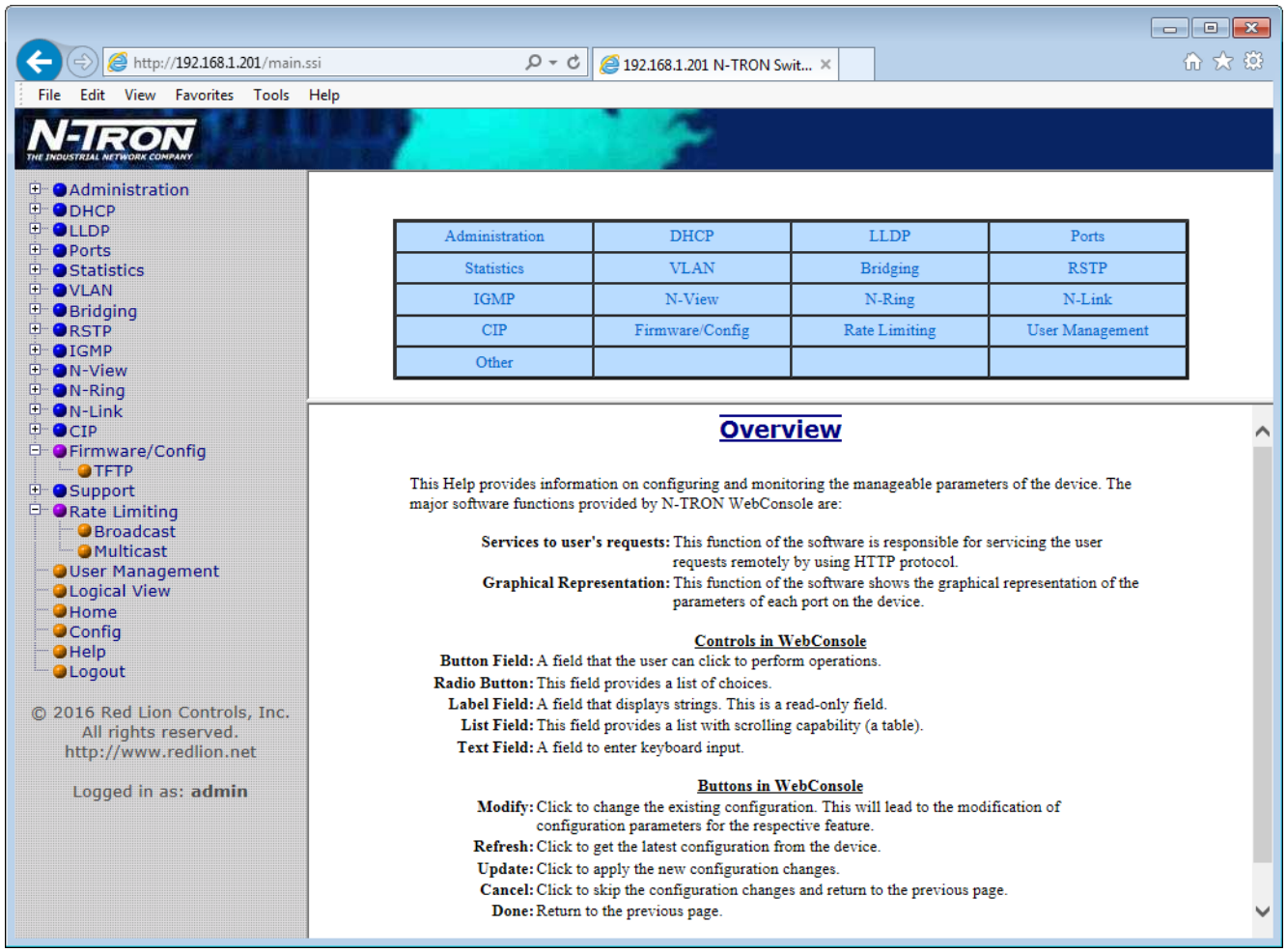
CONFIGURATION > FACTORY The “Factory” button will reload the factory default configuration settings. In many cases it is desirable to restore factory defaults but retain certain settings. Check boxes are provided to select the desired behavior.



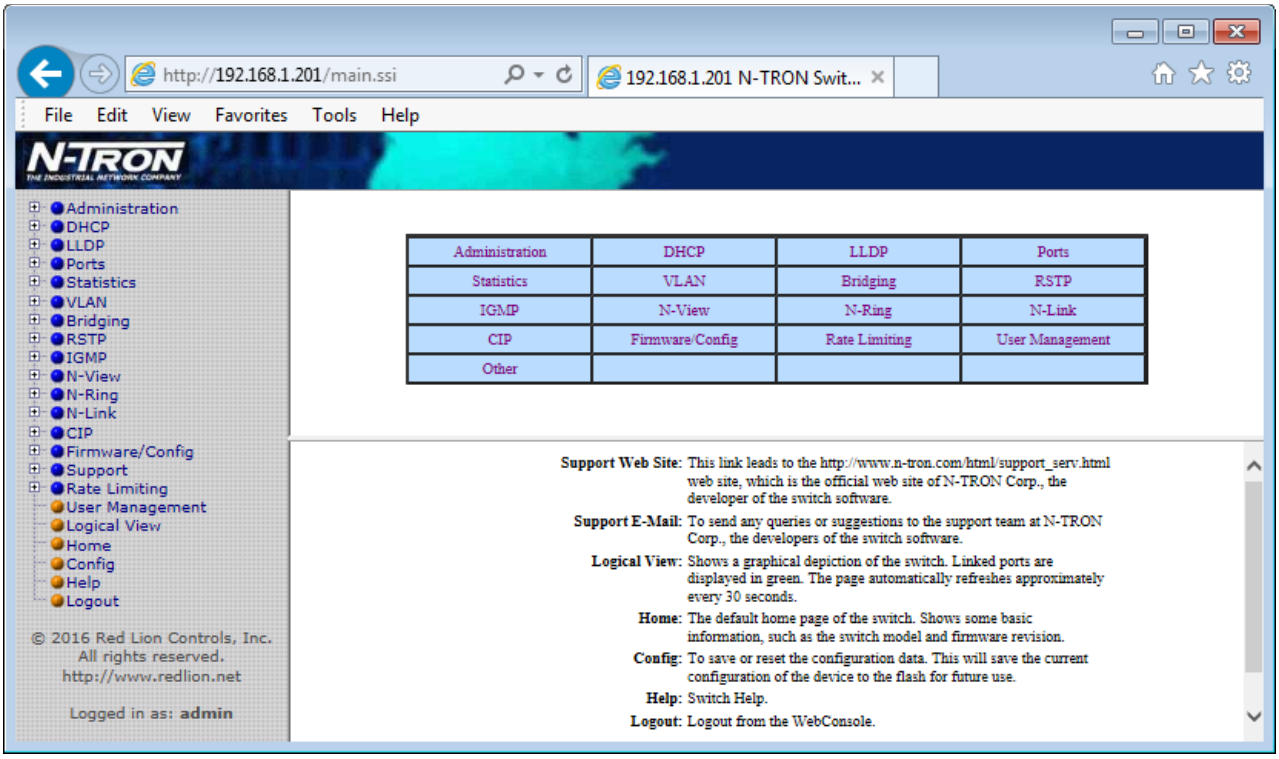
HELP

HELP > OVERVIEW

When the Help link is clicked on, you will see the Overview page containing some basic definitions and more specific choices in the table at the top of the screen. Although this screen page is not as detailed as information contained in the manual, it provides a basic feel for the different switch features. The Help screen displayed with each menu tree item, when selected from the Help Overview page, is provided within the manual pages documenting each menu tree item.



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



Service and Support

Service > Information

We sincerely hope that you never experience a problem with any of our products. If you do need service, call Red Lion at 1-877-432-9908 for Technical Support. A trained specialist will help you determine the source of the problem. Many problems are easily resolved with a single phone call. If it is necessary to return a unit to us, an RMA (Return Materials Authorization) can be obtained on the Red Lion website.

Red Lion tracks the flow of returned material with our RO system to ensure speedy service. You must include this RO number on the outside of the box so that your return can be processed immediately.

Be sure to have your original purchase order number and date purchased available.

We suggest that you give us a repair purchase order number in case the repair is not covered under our warranty. You will not be billed if the repair is covered under warranty.

Please supply us with as many details about the problem as you can. The information you supply will be written on the RO form and supplied to the repair department before your unit arrives. This helps us to provide you with the best service, in the fastest manner. Repairs are completed as soon as possible. If you need a quicker turnaround, ship the unit to us by air freight. We give priority service to equipment that arrives by overnight delivery.

We apologize for any inconvenience that the need for repair may cause you. We hope that our rapid service meets your needs. If you have any suggestions to help us improve our service, please give us a call. We appreciate your ideas and will respond to them.

For Your Convenience:

Please fill in the following and keep this manual with your Red Lion system for future reference:

P.O. #:_____ Date Purchased: _____

Purchased From:_____

Serial Number: _____

Product > Support

Inside US: +1 877 432-9908
Outside US: +1 717 767-6511
Fax: +1 (717) 764-0839
E-mail: support@redlion.net
Hours: 8:00 am to 6:00 pm EST

Red Lion Controls
20 Willow Springs Circle
York, PA 17406
Website: www.redlion.net

COMMAND LINE INTERFACE

This section provides a detailed description of the Command Line Interface, along with examples for the commands.

This section includes these chapters:

"Using the Command Line Interface" on page 109

"CLI General Commands" on page 113

"CLI System Management Commands" on page 117

"CLI Configuration Commands" on page 121

CHAPTER 3 USING THE COMMAND LINE INTERFACE

This chapter describes how to access and use the Command Line Interface (CLI).

The switch can be managed by entering command keywords and parameters at the switch's command-line interface (CLI). The CLI can is accessible over a direct connection to the switch's serial port or over a network connection using Telnet or Secure Shell (SSH).

CONSOLE CONNECTION

To access the switch console through the serial port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user name is "admin" and corresponding passwords of "admin". When the user user name and password is entered, the CLI displays the console prompt N-TRON/ Admin> and enters user access mode.
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "logout" command.

TELNET CONNECTION

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address and gateway of the switch using the SysIP command as described in Chapter 5 CLI System Management Commands.

If your network is connected to another network outside your location or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the user to show that you are using admin access mode where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "logout" command.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “cip -show,” **cip** is a keyword, **-show** is an argument that specifies the desired action to show the CIP™ configuration.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable the CIP configuration, and display the configuration, enter:

N-TRON/Admin> **cip enable**
N-TRON/Admin> **cip -show**

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to change the current static IP configuration, subnet mask, and gateway enter:

N-TRON/Admin> sysip -i 192.168.2.119 -s 255.255.252.0 -g 192.168.1.1

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command “**igmp ?**” displays a list of possible igmp commands:

N-TRON/Admin> **igmp ?**

Configuration Commands

Configuration commands are used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **config save** command.

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

CLI Command Groups

The system CLI commands most frequently used with these switches can be broken down into the functional groups shown below.

Command Group	Description	Page
General	Basic commands for entering access mode using login, restarting the system, or quitting the CLI - logout	page 113
System Management	These commands are used to set the system IP configuration mode, system configuration, and monitor system errors.	page 117
CLI Configuration Commands	Show or set the Mirror, SNMP, IGMP, N-Ring™, N-View™ or CIP Configuration. Show, add or delete ARL entries. Save or reset configuration settings. Show or clear system errors	page 121

CHAPTER 4 CLI GENERAL COMMANDS

These commands are used to control the command access mode, configuration mode, and other basic functions.

Command	Function
? (Help)	Shows a list of all commands or to get help on a specific command.
Logout	Logout of console interface.
Ping	Confirms connectivity with a Host.
Reset	Restarts (reboot) the switch.
Sysinfo	Shows the switch system information.

? (Help)

Show a list of all commands or get help on a specific command.

Without *cmd*, this command will list all the available commands.

If *cmd* is specified and if it matches a specific command, the **usage** of the command will be displayed; otherwise, if *cmd* matches the prefix of a command, the name of the command will be listed.

If **?** is preceded by another **?**, the usage and description of this command will be displayed.

SYNTAX

? [cmd]

PARAMETERS

cmd

The command for which to get help.

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> ?
The above command displays all the available commands.

N-TRON/Admin> abcd ?
Unknown Command: "abcd"

Type "?" for a list of available commands.

N-TRON/Admin> logout ?
Logout
      Log out of console interface.

SYNTAX:
      Logout
```

```
N-TRON/Admin> ? pi

Ping
      Ping a host.
…
N-TRON/Admin> ? ?

?
      Show a list of all commands or get help on a specific command.

SYNTAX:
      ? [cmd]

OPTIONS:
      cmd : The command for which to get help.
```

Logout

Used to log out of the console interface and end a command session.

Syntax

logout

Parameters

None

Default Setting

None

Example

```
N-TRON/Admin> logout
```

Ping

Use to ping a host to confirm connectivity.

Syntax

ping [-t] [-n count] [-w timeout] target_name

Parameters

target name

IP address or host name

-t

Ping the specified host until stopped.

To see statistics and continue - type Space;

To stop - type Control-C.

-n count

Number of echo requests to send.

-w timeout

Timeout in milliseconds to wait for each reply.

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> ping 192.168.1.119
...
N-TRON/Admin> ping –n 6 192.168.1.119
…
N-TRON/Admin> ping –t 192.168.1.119
…
N-TRON/Admin> ping –w 2000 192.168.1.119

Reply from 192.168.1.119: time=970ms
Reply from 192.168.1.119: time<10ms
Reply from 192.168.1.119: time<10ms

Ping statistics for 192.168.1.119:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
Approximate round trip times in milliseconds:
   Minimum = 0ms, Maximum = 970ms, Average = 320ms
```

Reset

Used to reset (reboot) the switch.

SYNTAX

reset

PARAMETERS

None

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> reset

Preparing for reset.
Cleaning up...
   Browser will be redirected to 192.168.1.250.
   Disabling SNMP...
   Disabling DHCP...
   Disabling CIP...
Locking out other processes...
Disable preemption...
Resetting device...
```

Show System Information

Used to display the system information of the switch.

SYNTAX

sysinfo

PARAMETERS

None

DEFAULT SETTING

None

EXAMPLE (708TX MODEL SHOWN)

```
N-TRON/Admin> sysinfo

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+
+ N-Tron 700/7018 Series
+
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+
+ Model:         708TX
+ Boot Loader:  BL 2.0.5.1 (0x02000501)
+ OS Version:   2.0.5
+ Build Date:   Mar 16 2009 at 11:19:27
+ 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, 1432576 Free, 4989952 Used, 0 Bad
+ MAC Address:  00:07:af:fe:af:c0
+ IP Address:   192.168.1.201
+ Subnet Mask:  255.255.255.0
+ Gateway:      192.168.1.1
+
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

CHAPTER 5 CLI SYSTEM MANAGEMENT COMMANDS

These commands are used to set the system IP configuration mode, system configuration, and monitor system errors.

Command	Function
Syserr	Show or clear the last system error.
Sysip	Set or show system IP configuration mode, IP address, subnet mask and gateway of this switch.
System	Show or set System configuration

Network System Error

This command is used to show or clear the last System Error.

If the clear parameter is not specified, this command will display the last system error.

SYNTAX

syserr [clear]

PARAMETERS

Clear

Clear the last system error.

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> syserr
Last System Error: None.

N-TRON/Admin> syserr clear
Last System Error: Cleared.
```

sysip

This command is used to show or set the system IP configuration mode, IP address, subnet mask, and gateway.

If no parameters are specified, this command will show the system IP addresses. A static IP, subnet mask, or gateway can be set while in either DHCP or static configuration mode as they will be used as the IP fallback when in DHCP mode. If the Static IP is set to the default system IP address, IP fallback will not occur. All system addresses must be formatted as: xxx.xxx.xxx.xxx.

SYNTAX

sysip [-c config_mode] [-i static_ip] [-s static_subnet_mask] [-g static_gateway]

PARAMETERS

-c config_mode

s(tatic) or d(hcp).

-i static_ip

Static IP address (for static config mode and IP fallback).

-s static_subnet_mask

Static sub net mask (for static config mode and IP fallback).

-g static_gateway

Static gateway address (for static config mode and IP fallback).

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> sysip

IP Configuration Mode : Static
Static IP Address     : 192.168.1.225
Static subnet Mask    : 255.255.255.0
Static gateway        : 192.168.1.1

N-TRON/Admin> sysip -c dhcp

IP Configuration Mode : DHCP (has been changed)
Fallback IP Address   : 192.168.1.225
Fallback Subnet Mask  : 255.255.255.0
Fallback Gateway      : 192.168.1.1

Press <ENTER> to Save Changes and Restart the System Now
…
N-TRON/Admin> sysip -i 192.168.2.119 -s 255.255.252.0 -g 192.168.1.1

IP Configuration Mode : Static
Static IP Address     : 192.168.2.119 (has been changed)
Static Subnet Mask    : 255.255.252.0 (has been changed)
Static Gateway        : 192.168.1.1 (has been changed)

Press <ENTER> to Save Changes and Restart the System Now
…
```

Note: If the mode is set to DHCP and IP fallback occurs, DHCP requests will stop. If the mode is set to DHCP and the IP Configuration is retrieved from a DHCP server, IP fallback will not occur, even if the lease is lost.

system

This command is used to show or set System configuration.

If no parameters are specified, this command will show the System configuration (same as -show parameter).

SYNTAX

system [-show] [-name label] [-browser state]

PARAMETERS

-show

Show configuration.

-name label

Set the switch name.

-browser state

Set the browser access status to e(nabled) or d(isabled)

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> system –name "Private switch" –browser disabled

IP Configuration : Static
Client ID (hex)    : 0007affbfa40 (7018 models only)
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.
......
```

Note: 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.

CHAPTER 6 CLI CONFIGURATION COMMANDS

This chapter describes the following configuration commands:

- Configuration Device Operations
- Save or Reset Configuration Settings
- Show, Add or Delete ARL Entires
- Show or Set CIP™ Configuration
- Show or Set IGMP Configuration
- Show or Set Mirror Configuration
- Show or Set N-Ring™ Configuration
- Show or Set N-View™ Configuration
- Show or Set Port Configuration
- Show or Set SNMP Configuration

CONFIGURATION DEVICE OPERATIONS

Use the cfgdev command to show, compare or erase information on the configuration device. This command is applicable only to models with configuration device capability: 7010TX, 7012FX2, 7026TX, 709FX, 710FX2, 711FX3, 712FX4, 714FX6, 7506GX2 and 7900CPU.

SYNTAX

CfgDev info | format [-m model] | compare | erase

PARAMETERS

Info

Show information about the configuration device.

Compare

Compare the configuration of the switch to the configuration device.

Erase

Erase the switch configuration the configuration device.

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Factory> cfgdev info

Port A:    0xd080
Board ID:  0x0005 (5)

Configuration device information:
  Name            : SDS128M
```

```
  Model          : 3
  Version        : 1
  Page Size      : 200
  Total Size     : 127008768
  Max Clock (Hz)  : 400000
  Write Cycles (ns): 5000000
  Flags          : 0x00000001

N-TRON/Factory> cfgdev compare

Comparing switch configuration to the configuration device...
The configurations are different.

N-TRON/Factory> cfgdev erase

Erasing configuration device...

Configuration device erase completed.
```

Save or Reset Configuration Settings

Use the config command to save or reset the configuration settings.

Syntax

config -s[ave] | r[eset]

Parameters

-save

Save current running configuration settings.

-reset

Reset configuration settings to factory defaults.

Default Setting

None

Example

```
N-TRON/Admin> config save

Save Settings...

Settings have been saved.

N-TRON/Admin> config reset

Resetting to factory defaults...
Load factory default settings [y/n]?y
Keep IP, subnet mask, and gateway addresses [y/n]?y
Keep current user names and passwords [y/n]?y
...
```

Show, Add or Delete ARL Entires

Use the arl command to show, add or delete ARL entires. If no parameters are specified, this command will show the ARL entries (same as -show parameter).

Syntax

arl -show | showmct | add mac port cpu static vid | del[ete] mac vid

Parameters

-show

Show entire ARL table.

-showmct

Show entire ARL MCT (Multicast Index) table.

-add

Add MAC Address.

-mac

MAC Address.

-port

Port Number.

-cpu

1 = Send to CPU also.

-static

1 = This is a static address; 0 = Non-Static.

-vid

VLAN ID (0-4095).

Default Setting

None

Example

```
N-TRON/Admin> 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> arl showmct

No. Idx Val Port Mask  Port(s)
--- --- --- ----------- ----------
 1   0   1 0x00000000 (None)
 2   1   1 0x00000001 TX1

N-TRON/Admin> arl add 00:19:b9:03:aa:79 3 0 1 1

N-TRON/Admin> arl del 00:19:b9:03:aa:79 1
```

Show or Set CIP™ Configuration

Use the cip command to show or set the CIP configuration. If no parameters are specified, this command will show the CIP configuration (same as -show parameter).

Syntax

cip [-e[nable] [-d[isable] [-show]

Parameters

-cip -show

Show CIP configuration.

-cip [-e[nable] [-d[isable]

Set the CIP status to e(nabled) or d(isabled).

Default Setting

None

Example

```
N-TRON/Admin> cip -show

CIP Configuration:
------------------
Status:              Enabled
EthIp Interval:        10 ms
Cache Interval:        2000 ms

Identity Information:
---------------------
Product Name:          N-TRON 708FX2
Vendor:              1006 (N-TRON)
Device Type:           0x0C (Communications Adapter)
Major Revision:        1
Minor Revision:        1
Serial Number:         0xAFFBF8F0

Connection Information:
-----------------------
Multicast Connections:  0
Unicast Connections:    0

N-TRON/Admin> cip -disable
Changing CIP configuration...

CIP Configuration:
------------------
Status:              Disabled
EthIp Interval:        10 ms
Cache Interval:        2000 ms

Identity Information:
---------------------
Product Name:          N-TRON 708FX2
Vendor:              1006 (N-TRON)
Device Type:           0x0C (Communications Adapter)
Major Revision:        1
Minor Revision:        1
Serial Number:         0xAFFBF8F0

Connection Information:
-----------------------
Multicast Connections:  0
Unicast Connections:    0
N-TRON/Admin>
```

Show or Set IGMP Configuration

Use the IGMP command to show or set IGMP configuration. If no parameters are specified, this command will show the IGMP configuration (same as -show parameter).

Syntax

igmp [-show] [-status state]

Parameters

-show

Show configuration.

-status state

Set the IGMP status to e(nabled) or d(isabled).

Default Setting

None

Example

```
N-TRON/Admin> igmp -show

IGMP Status          : Enabled
IGMP Version         : 2
Query Mode           : Auto
CIP Querier Status   : 2, Active-Auto
Active Querier IP    : 192.168.1.250
Router Mode          : Auto
Manual Router Ports  : (None)
IGMP Number of Groups : 1
IGMP Resource Usage % : 1

N-TRON/Admin> igmp –status disabled

IGMP Status          : Disabled
IGMP Version         : 2
Query Mode           : Auto
CIP Querier Status   : 2, Active-Auto
Active Querier IP    : 192.168.1.250
Router Mode          : Auto
Manual Router Ports  : (None)
IGMP Number of Groups : 1
IGMP Resource Usage % : 1
N-TRON/Admin>
```

Show or Set Mirror Configuration

Use the mirror command to show or set Mirror configuration. If no parameters are specified, this command will show the Mirror configuration (same as -show parameter).

Syntax

mirror [-show] [-status state] [-dp portno] [-tx portlist] [-rx portlist]

Parameters

-show

Show configuration.

-status state

Set the mirror status to e(nabled) or d(isabled).

-dp portno

Set the destination port number for mirrored frames.

-tx portlist

Set the source ports to mirror frames that are transmitted.

-rx portlist

Set the source ports to mirror frames that are received.

Note: The portlist parameter 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.

Default Setting

None

Example

```
N-TRON/Admin> mirror -show

Mirror Status    : Disabled
Destination Port : TX1
Tx Source Ports  : (None)
Rx Source Ports  : (None)

N-TRON/Admin> mirror –status enabled –dp 6 –tx 1,3-5 –rx 1,3,5

Mirror Status    : Enabled
Destination Port : TX6
Tx Source Ports  : TX1, TX3-TX5
Rx Source Ports  : TX1, TX3, TX5

Changes have been made that have not been saved.
. . .
```

Show or Set N-Ring™ Configuration

Use the nring command to show or set N-Ring configuration. If no parameters are specified, this command will show the N-Ring configuration (same as -show parameter).

Syntax

nring [-show] [-mode d | a | m] [-ports set_id]

Parameters

-show

Show configuration.

-mode

Set the N-Ring mode.
d = disabled, a = auto member, m = manager

-**ports** set_id

Set the ring ports for N-Ring manager mode.

Specify port set identifier or use “?” to list available port sets.

Default Setting

None

Example

```
N-TRON/Admin> nring -show

N-Ring Mode  : Auto Member
Aging Time   : 20

N-TRON/Admin> nring –ports ?

ID     Port Set
--     --------
 1     TX1 / TX2
 2     TX7 / TX8

N-TRON/Admin> nring –mode m –ports 2

Do you Want to Save Changes and Restart the System Now [y/n]?
...
```

Show or Set N-View™ Configuration

Use the nview command to show or set N-View configuration. If no parameters are specified, this command will show the N-View configuration (same as -show parameter).

Syntax

nview [-show] [-status state]

Parameters

-show

Show configuration.

-status state

Set the N-View status to e(nabled) or d(isabled).

Default Setting

None

Example

```
N-TRON/Admin> nview -show

N-View Status   : Enabled
N-View Interval : 5

N-TRON/Admin> nview –status disabled

N-View Status   : Disabled
N-View Interval : 5

Changes have been made that have not been saved.
   ...
```

Show or Set Port Configuration

Use the port command to show or set a port configuration.

Syntax

port [-show] [-admin state] [-sd auto | 10h | 10f | 100h | 100f | 1000h | 1000f] [-flow state] [-fhp state] [-dp prio] [-dscp state] [-8021p state] [-pvid vid] [-ual percent] [-uah percent] [-security state] portno

Parameters

portno

Port number to configure or show. Specify “all” to show all ports.

-show

Show configuration.

-admin state

Set the admin status for the port to e(nabled) or d(isabled).

-sd

Set the speed and duplex mode for the port.

auto = enable auto-negotiation

-flow state

Set the flow control for the port to e(nabled) or d(isabled).

-fhp state

Set force high priority for the port to e(nabled) or d(isabled).

-dp

Set the default QOS priority for the port. The range is 0-7.

-dscp state

Set the DSCP Priority for the port to e(nabled) or d(isabled).

-8021p state

Set the 802.1p Priority for the port to e(nabled) or d(isabled).

-pvid

Set the VLAN ID for the port. The range is 1-4094.

-ual percent

Set the usage alarm low percentage. The range is 0-100.

-uah percent

Set the usage alarm high percentage. The range is 0-100.

-security state

Set the security status for all supported ports to e(nabled) or d(isabled).

Default Setting

None

EXAMPLE

```
N-TRON/Admin> port -sd 100f -flow enabled -dp 7 -pvid 2 5

Port  Port  Admin  Link  Auto      Port  Dupl  Flow      Force     Def  Port
 No   Name  Status Stat  Nego      Spd  Mode  Control   High Pri  Pri  State     PVID
----  ---- -------- ----  --------  ----  ----  --------  --------  ---  ----------  ----
  5 T  X5  Enabled Down  Disabled  100   Full  Enabled   Disabled   7   Disabled    2

Changes have been made that have not been saved.
. . .
```

SHOW OR SET SNMP CONFIGURATION

Use the SNMP command to show or set SNMP configuration. If no parameters are specified, this command will show the SNMP configuration (same as -show parameter).

SYNTAX

snmp [-show] [-ro name] [-rw name] [-trap name] [-v number]

PARAMETERS

-show

Show configuration.

-ro name

Set the Authorized Community Name for SNMP Get requests.

-rw name

Set the Authorized Community Name for SNMP Set requests.

-trap name

Set the Authorized Community Name for SNMP Traps.

-v number

Set the Version Number for SNMP Traps to either 1 or 2.

Note: The 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.

DEFAULT SETTING

None

EXAMPLE

```
N-TRON/Admin> snmp -ro users

IP Address - Trap Stn.#1  : Value Not Configured
IP Address - Trap Stn.#2  : Value Not Configured
IP Address - Trap Stn.#3  : Value Not Configured
IP Address - Trap Stn.#4  : Value Not Configured
IP Address - Trap Stn.#5  : Value Not Configured
Read-Only Community Name  : users
Read-Write Community Name : private
Trap Community Name       : public

Changes have been made that have not been saved.
. . .
```

CHAPTER 7 VLAN CONFIGURATION

This chapter includes the following VLAN configuration procedures and examples:

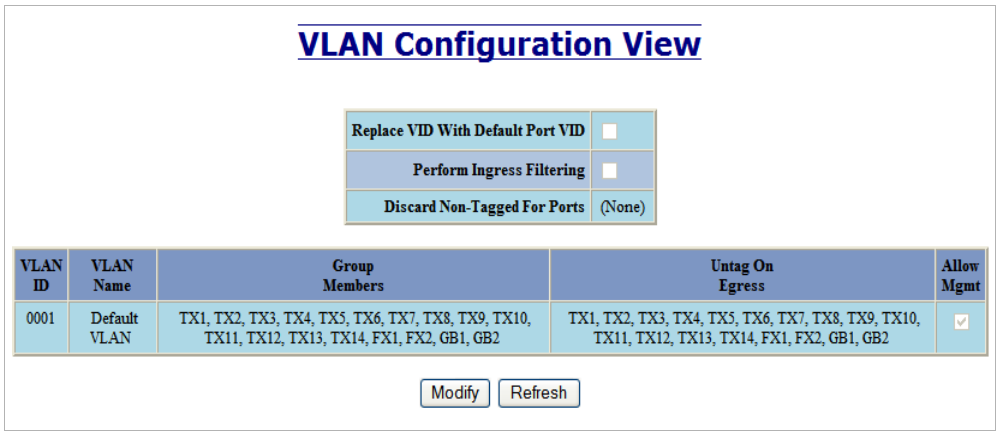
- Add a VLAN
- Delete a VLAN
- VLAN Configuration Examples
- Port - Based VLAN
- Tagged VLAN (Tagged Only)
- Tagged VLAN (All)
- Hybrid VLAN
- Overlapping VLAN
- VLAN with Multicast Filtering

ADD/DELETE VLANS

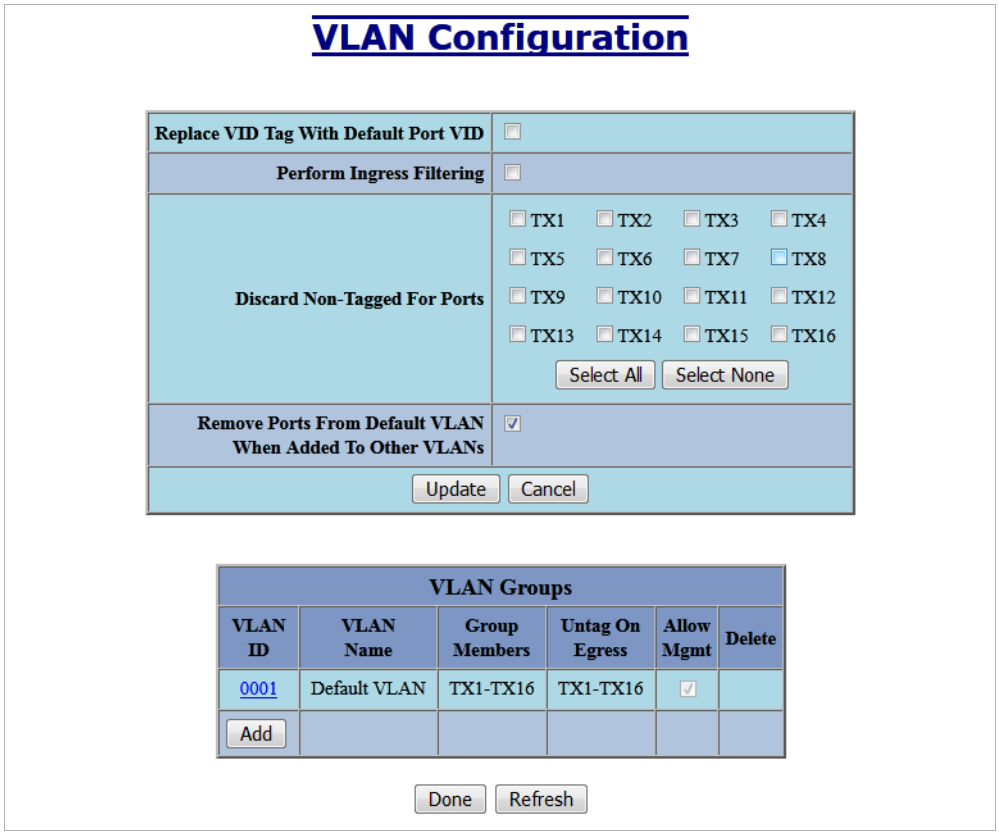
ADD A VLAN

This procedure is provided to guide you in adding a VLAN to your switch.

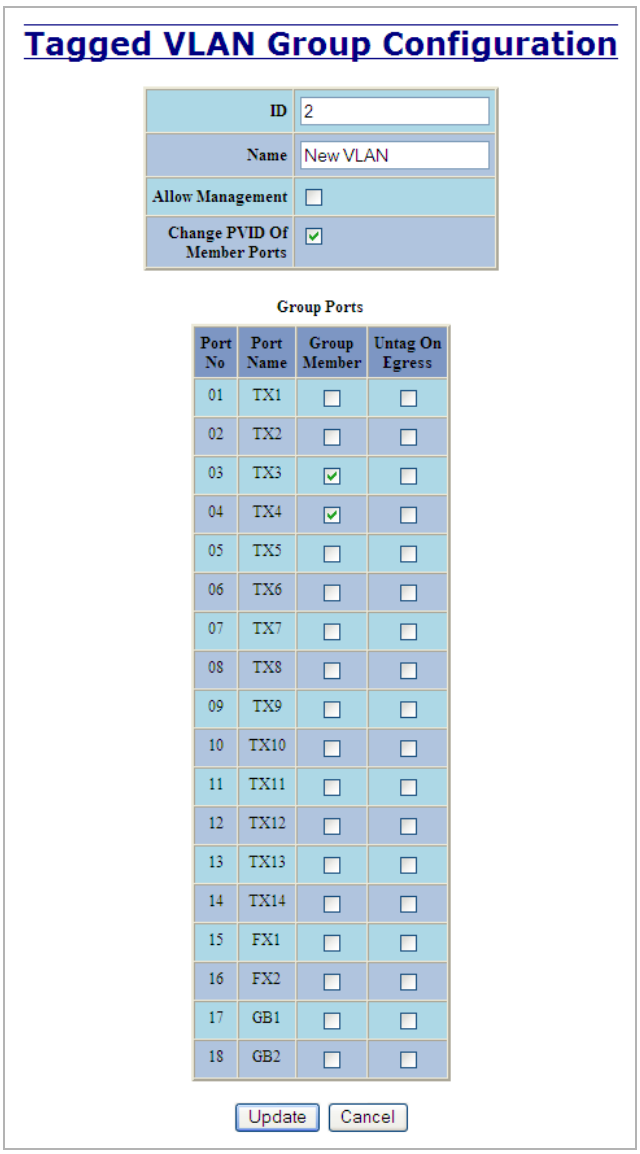
1. Navigate to the VLAN Configuration View screen (the factory default screen is shown for a 7018 model).



2. Click the Modify button to add a new VLAN. The VLAN Configuration screen appears.



3. Click Add in the VLAN Groups area of the VLAN Configuration screen. The Tagged VLAN Group Configuration screen is displayed.

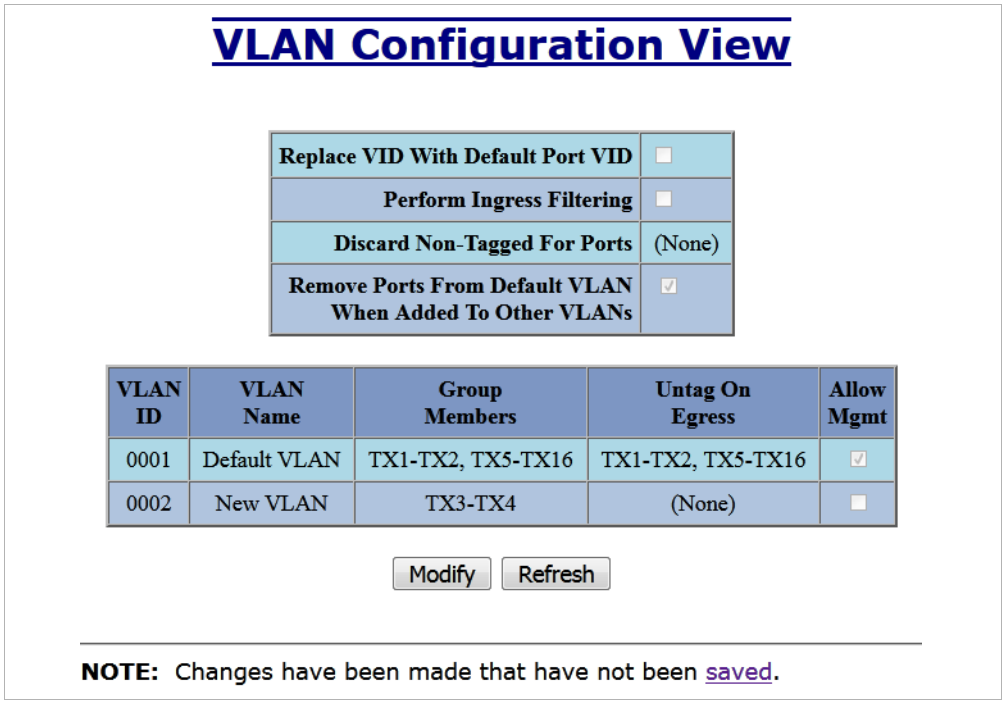


4. Enter a numeric VLAN identifier in the ID field (required).
5. Enter a name for the new VLAN in the Name field.

Note: "N-Ring VLAN" is a reserved name with a special meaning and cannot be used to name a newly added VLAN.

6. Click "Allow Management" box if desired.
7. Click "Change PVID of Member Ports" if desired.
8. Select the port(s) to include in the VLAN by clicking on the corresponding check box in the "Group Member" column.
9. Select the port(s) in the VLAN to untag on egress by clicking on the corresponding check box in the "Untag On Egress" column. Ethernet frames that exit this port will not contain a VLAN field in them.
10. Click the "Update" button to add the VLAN or click the "Cancel" button to exit without completing the VLAN add.

11. The result of adding a VLAN is displayed in the VLAN Configuration View screen. In the example provided, the New VLAN does not overlap the “Default VLAN”.



VLAN Configuration View

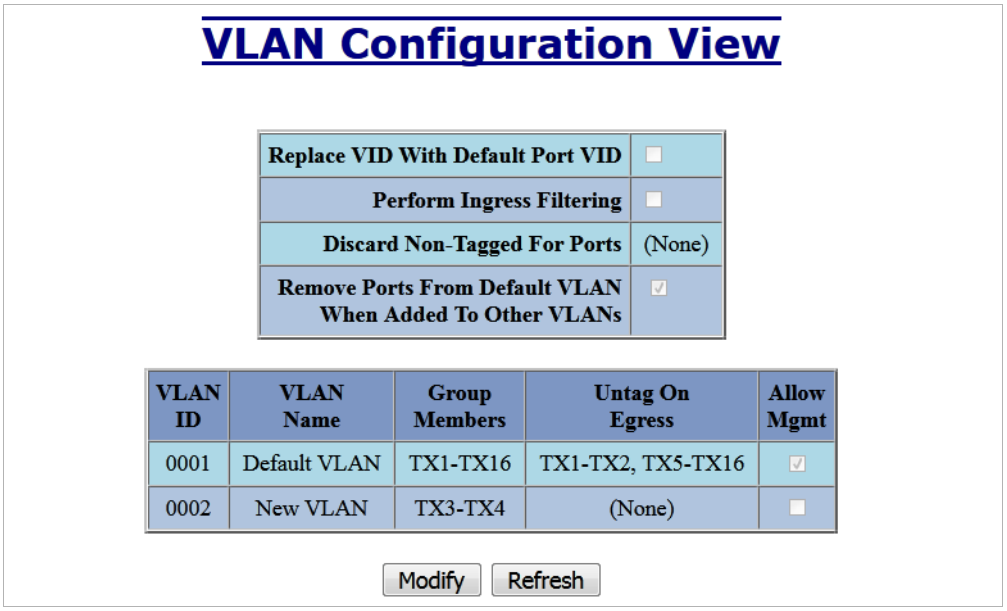
Replace VID With Default Port VID	☐
Perform Ingress Filtering	☐
Discard Non-Tagged For Ports	(None)
Remove Ports From Default VLAN When Added To Other VLANs	☑

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX1-TX2, TX5-TX16	TX1-TX2, TX5-TX16	☑
0002	New VLAN	TX3-TX4	(None)	☐

Modify Refresh

NOTE: Changes have been made that have not been saved.

12. The ports of ”New VLAN” (TX3, TX4 in this example) may be added back to “Default VLAN” to create overlapping VLANs.



VLAN Configuration View

Replace VID With Default Port VID	☐
Perform Ingress Filtering	☐
Discard Non-Tagged For Ports	(None)
Remove Ports From Default VLAN When Added To Other VLANs	☑

VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX1-TX16	TX1-TX2, TX5-TX16	☑
0002	New VLAN	TX3-TX4	(None)	☐

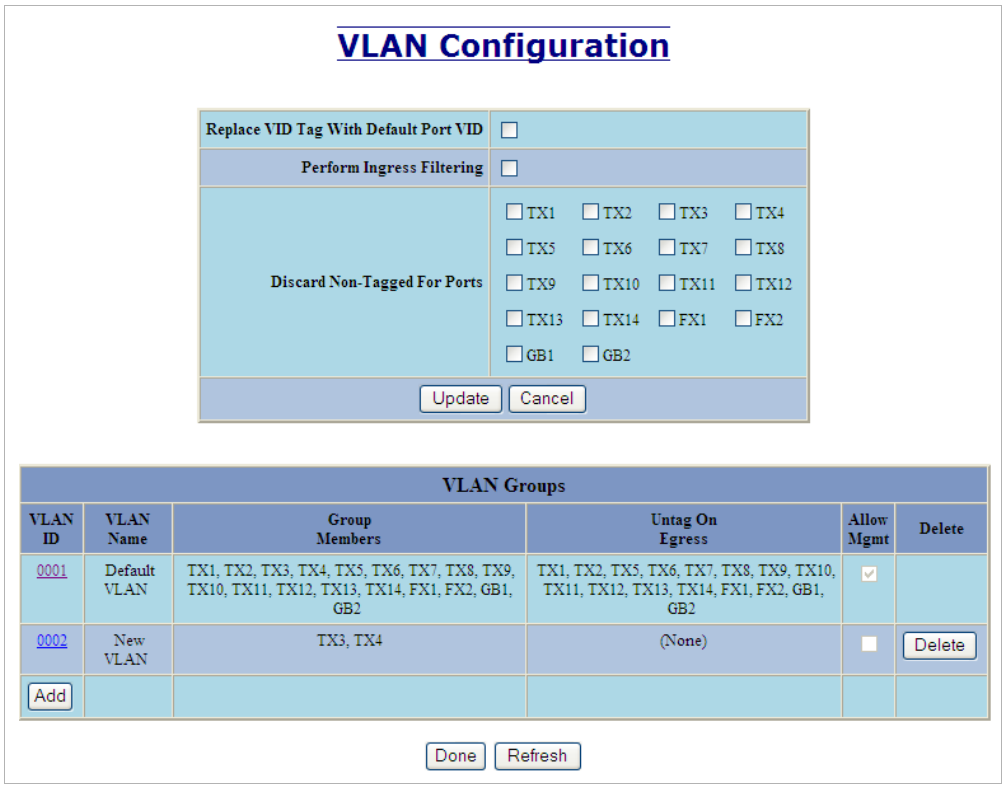
Modify Refresh

Note: Notice the ports in “New VLAN” are not marked as “Untag on Egress” and therefore ensure a VLAN tag is in each egressing Ethernet frame.

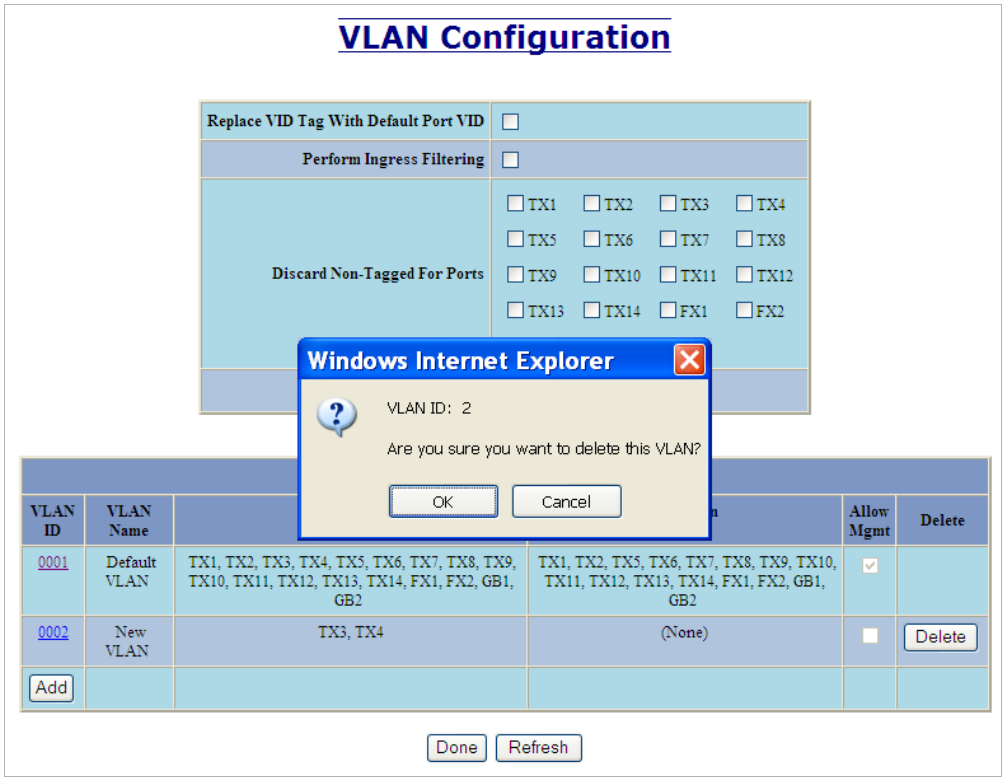
13. Save the new VLAN configuration of the switch by clicking on the saved link and then the **Save** button in order for the new configuration to survive a device power cycle.

DELETE A VLAN

1. Navigate to the VLAN Configuration View screen and the **Modify** button.

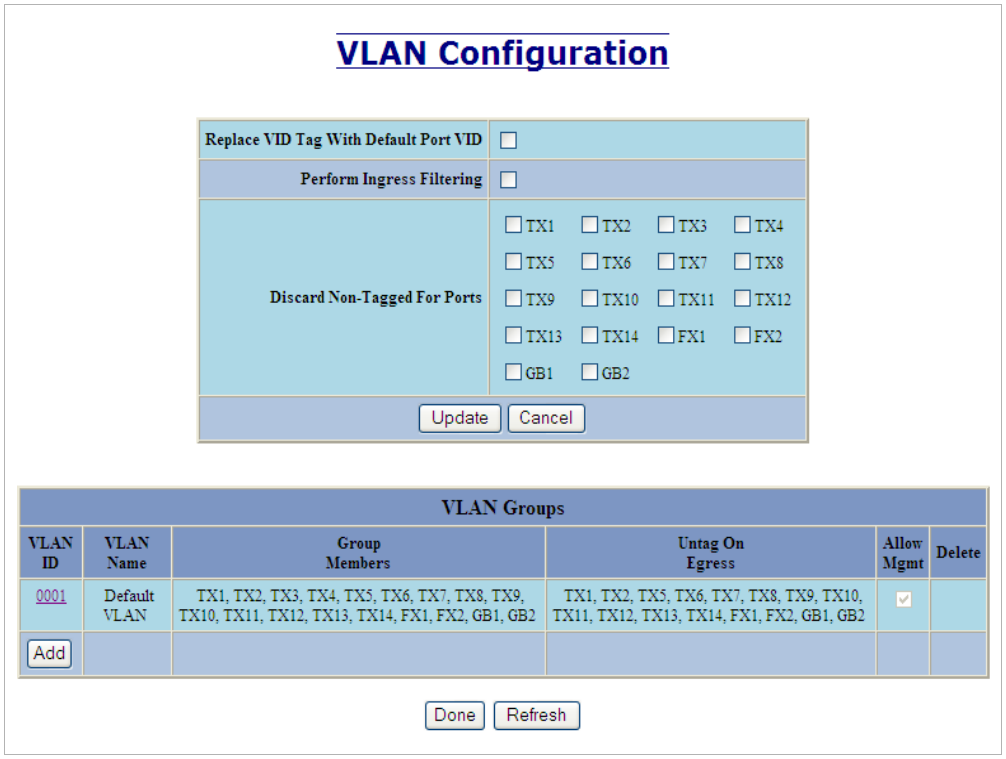


2. Click the **Delete** button corresponding to the VLAN you want to delete.



3. Click OK in the confirmation pop-up screen to remove the selected VLAN or Cancel.

4. Save the new VLAN configuration of the switch by clicking on the saved link and then the Save button for the new configuration to survive a device power cycle.



VLAN Configuration Examples

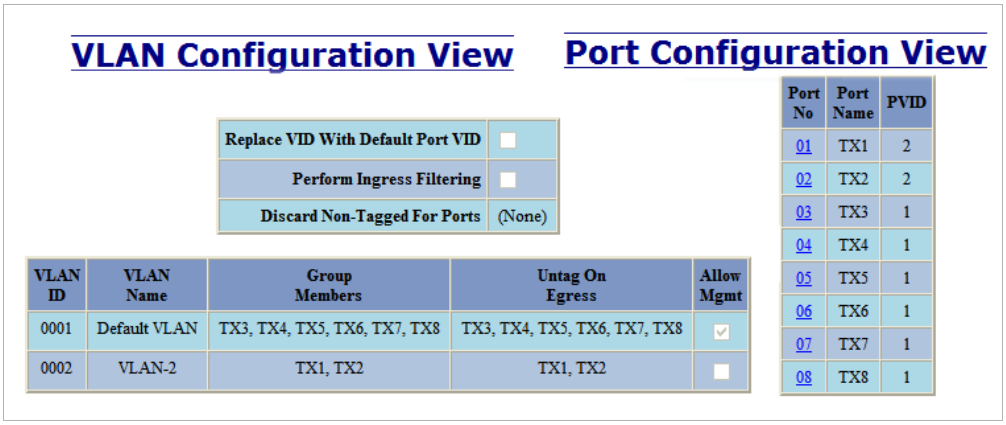
A VLAN is an administratively configured LAN segment that limits the traffic in multiple broadcast domains. Instead of physically reconnecting a device to a different LAN, network users can accomplish this task by configuring a VLAN compliant switch to create logical network segments.

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 other 700 Series and 7000 Series models may be configured similarly.

Port - Based VLAN

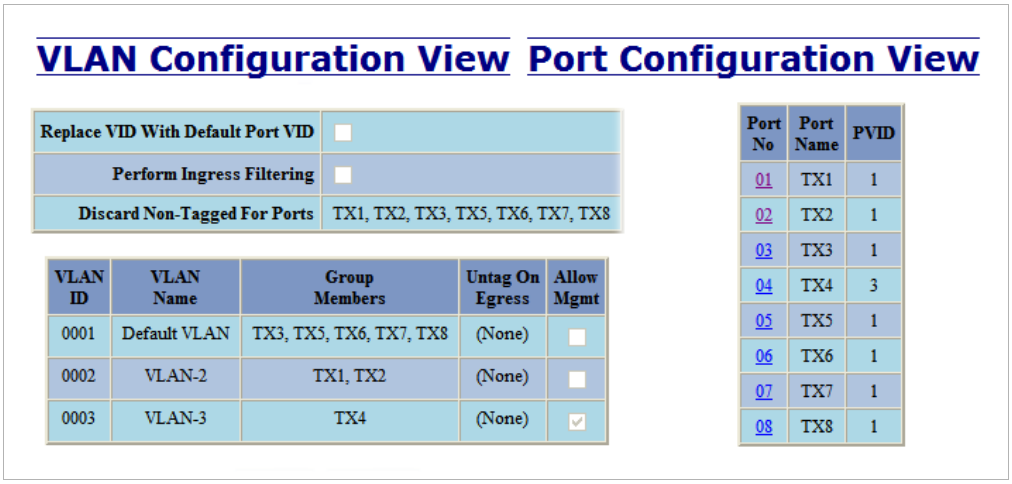
Basic understanding of Port-Based VLANs



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

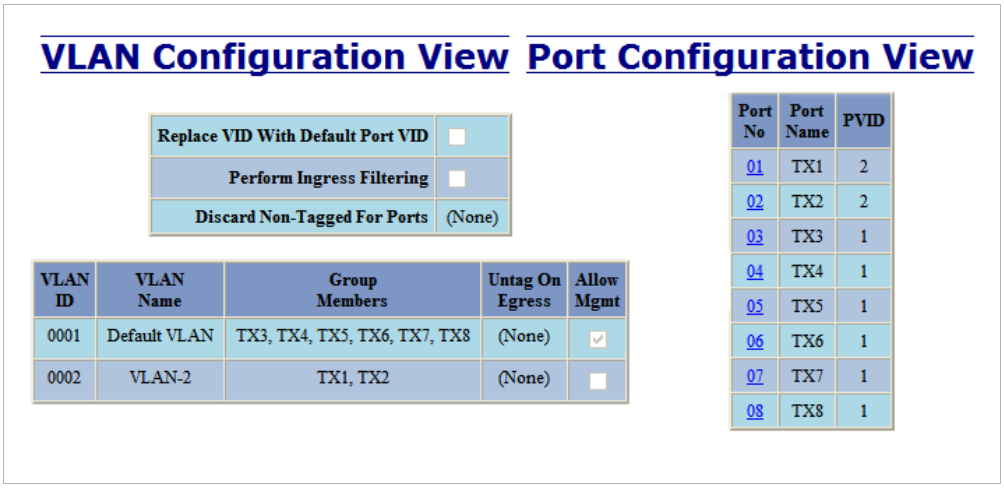
TAGGED VLAN (TAGGED ONLY)

Basic understanding of tagged VLANs (Admit - Tagged Only)



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

TAGGED VLAN (ALL) Basic understanding of tagged VLANs (Admit - All)



VLAN Configuration View

Replace VID With Default Port VID	☐
Perform Ingress Filtering	☐
Discard Non-Tagged For Ports	(None)

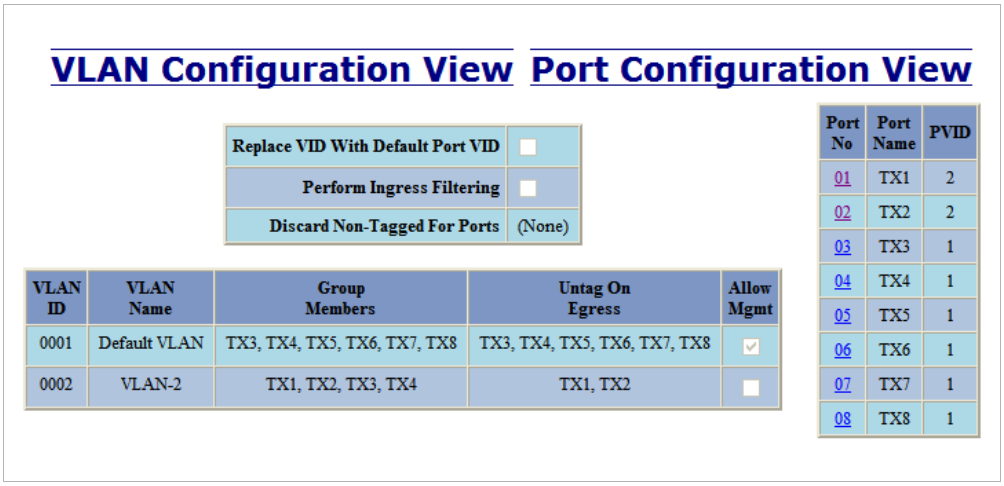
VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt
0001	Default VLAN	TX3, TX4, TX5, TX6, TX7, TX8	(None)	☑
0002	VLAN-2	TX1, TX2	(None)	☐

Port Configuration View

Port No	Port Name	PVID
01	TX1	2
02	TX2	2
03	TX3	1
04	TX4	1
05	TX5	1
06	TX6	1
07	TX7	1
08	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

HYBRID VLAN Basic understanding of Hybrid VLANs



VLAN Configuration View Port Configuration View

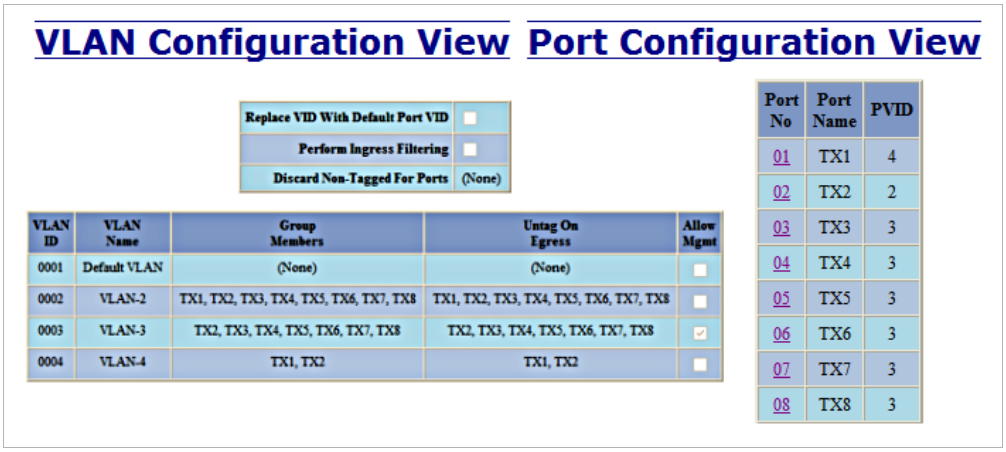
Replace VID With Default Port VID	☐
Perform Ingress Filtering	☐
Discard Non-Tagged For Ports	(None)

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	☑
0002	VLAN-2	TX1, TX2, TX3, TX4	TX1, TX2	☐

Port No	Port Name	PVID
01	TX1	2
02	TX2	2
03	TX3	1
04	TX4	1
05	TX5	1
06	TX6	1
07	TX7	1
08	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	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

OVERLAPPING VLAN Basic understanding of Overlapping VLANs.

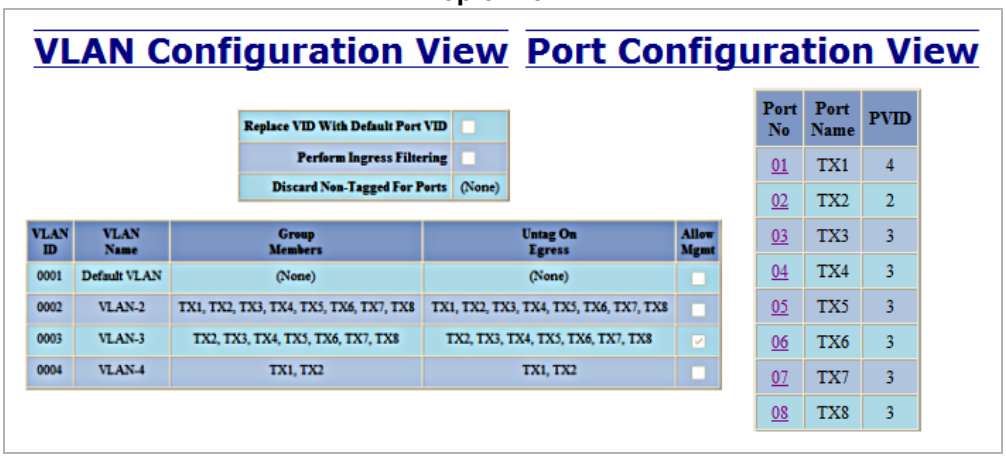


Receiving Port #	Tagged VID in packet	Destination Address	Transmitting Port #s	Notes
TX1	Untagged	MAC on port TX2, VID=4	TX2	Unicast Traffic
TX1	Untagged	MAC on port TX3	TX2	Floods VLAN 4
TX1	VID 4	MAC on port TX2, VID=4	TX2	Strips VID off packet
TX1	VID 4	Unknown MAC	TX2	Strips VID off packet & Floods 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)

VLAN with Multicast Filtering

Basic understanding of VLANs with Multicast Filtering

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 7018 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 is achievable with Overlapping VLANs.

For further information and examples on Overlapping VLANs, see:

http://www.redlion.net/overlappingportvlan.pdf.