N-Tron® Series
NT24k® Gigabit Ethernet Switches

Software Guide | February 2024

LP0991 | Revision H

Red Lion Controls, Inc.
35 Willow Springs Circle
York, PA 17406

CONTACT INFORMATION:

AMERICAS
Inside US: +1 (877) 432-9908
Outside US: +1 (717) 767-6511
Hours: 8 am-6 pm Eastern Standard Time
(UTC/GMT -5 hours)

ASIA-PACIFIC
Shanghai, P.R. China: +86 21-6113-3688 x767
Hours: 9 am-6 pm China Standard Time
(UTC/GMT +8 hours)

EUROPE
Netherlands: +31 33-4723-225
France: +33 (0) 1 84 88 75 25
Germany: +49 (0) 1 89 5795-9421
UK: +44 (0) 20 3868 0909
Hours: 9 am-5 pm Central European Time
(UTC/GMT +1 hour)

Website: www.redlion.net
Support: support.redlion.net

Table of Contents

REDLION®

Preface

Disclaimer

This software guide provides guidance on how to use the NT24k®. 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 Controls 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.

This guide is intended to be used by personnel responsible for configuring and commissioning NT24k devices for use in visualization, monitoring, and control applications. Users of this document are urged to heed warnings and cautions used throughout the document.

Trademark Acknowledgments

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

- EtherNet/IP™and CIP™ are trademarks of ODVA.

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

Certifications

Red Lion Controls ensures that this device meets all the ODVA technology and standards guidelines for the Common Industrial Protocol (CIP) for industrial automation.

Document History and Related Publications

The hard copy and electronic media versions of this document are revised only at major releases and therefore, may not always contain the latest product information. Tech Notes and/or product addendums will be provided as needed between major releases to describe any new information or document changes.

The latest online version of this document can be accessed through the Red Lion website at: https://www.redlion.net/support/documentation/user-manuals.

Additional Product Information

Additional product information can be obtained by contacting your local sales representative or Red Lion through the contact numbers and/or support website address listed on the inside of the front cover.

Chapter 1   Security Best Practices

Introduction

It is more important than ever to secure network devices from unauthorized access, both within and outside of your organization. Red Lion strongly recommends installing managed layer-2 switches behind a secure network firewall in access controlled locations, and immediately changing all default user accounts and passwords, as well as disabling protocols that are not needed in your application.

Protocols and user names with their default passwords are listed in the table below.

PROTOCOLS/USERS	DEFAULT NAME	DEFAULT PASSWORD
User Login	admin	Admin
SNMPv3 User Authentication	initial	Authpass
SNMPv3 User Privacy	initial	Privpass
SNMP v1/v2	read community	Public
SNMP v1/v2	write community	Private
SNMP v1/v2	trap community	public

Some protocols and special devices are enabled by default for the best overall out of the box experience. However, if any in this group will not be used or needed in your network, then these should be disabled to prevent unexpected behavior, unauthorized access or usage. These protocols and special devices are listed in the table below:

PROTOCOLS OR SPECIAL DEVICES
CIP™
SNMP
NTCD
DHCP Client
RSTP
LLDP
N-View™

Managing Local and Remote Access Using 802.1X

Red Lion strongly recommends using 802.1X to manage local and remote access as a best practice for larger installations. 802.1X allows for the management of users, devices, profiles, certificates, and so forth from a single location which also provides a high degree of security.

Default Passwords

User Passwords

The NT24k® ships from the factory with a default *admin* user account. Red Lion strongly recommends creating a new user with administrative privileges and then deleting the default *admin* user before the unit is deployed.

At a minimum, the default password for the *admin* user should be changed.

SNMPv3 Users

The NT24k® ships from the factory with SNMP enabled and a default SNMPv3 user. If SNMP will be used, then Red Lion strongly recommends creating a new SNMPv3 user and then deleting the default *initial* SNMPv3 credentials. At a minimum, the default password for the *default* user should be changed.

It is strongly recommended that both authentication and privacy protocols are enabled for all v3 users. Setting the option to *None* for either protocol is discouraged.

See the Disabling Unused Protocols and Special Devices section if SNMP will not be used.

SNMP v1/v2 Community Names

The NT24k ships with default Community Names for SNMP v1/v2 operation. SNMP v1/v2 traffic per the standard is neither hashed nor encrypted. Therefore, it is Red Lion's recommendation that customers requiring SNMP use SNMPv3, which offers more secure SNMP communication.

If SNMP v1/v2 is required in your application, Red Lion strongly recommends changing the default SNMP credentials before deployment.

See the Disabling Unused Protocols and Special Devices section if SNMP will not be used.

Legacy Protocols

When multiple revisions of a protocol are supported, Red Lion enables the most secure version by default and disables legacy (unsecure) versions of the protocol. We strongly recommend leaving the older revisions disabled.

LEGACY PROTOCOL	SECURE PROTOCOL EQUIPMENT
HTTP	HTTPS
Telnet	SSH

Disabling Unused Protocols and Special Devices

Certain network protocols and special devices are enabled by default for the best overall out of the box experience. However, some of these protocols and devices have the capability of configuring and/or reading network settings or causing unexpected network behavior. These protocols and devices should be disabled when they are not being utilized in your network to prevent unexpected behavior, unauthorized access and/or control of your network and individual network devices.

The following protocols or special devices meet these criteria:

- CIP™
- SNMP
- NTCD (Configuration Device)
- DHCP Client
- RSTP
- LLDP
- N-View™

Chapter 2   Features and Specifications

NT24k® Series Common Features

Red Lion's N-Tron® Series NT24k all-Gigabit managed industrial Ethernet switches are available in rack or DIN-rail mountable configurations. The NT24k platform offers a wide array of port configurations, media types and Power over Ethernet Plus (PoE+) models including Fast Ethernet, Gigabit copper and fiber options. All NT24k switches are plug-and-play installable with Internet Group Management Protocol (IGMP) auto-configuration, media/port auto-detection and simple ring configuration, making the NT24k platform one of the easiest to deploy managed switches in the industry. Housed in rugged hardened enclosures, NT24k switches feature extended shock and vibration specifications, wide operating temperature ratings, and best-in-class ring technology.

Connectivity

The modular NT24k switches are available in 2 or 3 slot configurations. Port modules are hot-swappable. Available modules include 10/100/1000Base Copper, 100Base Fiber, 1000Base Fiber, Gigabit Small Form-factor Pluggable (SFP) Ports and Dual Mode (100Base/1000Base) SFP ports. Modules and SFP transceivers are sold separately. Please reference the N-Tron Series "NT24k Modular Series Hardware & Installation Manual" for available configuration options.

The compact series offers a wide variety of copper and fiber configurations, including all Gigabit copper, Gigabit fiber or SFP ports. IEEE 802.3af/at Power over Ethernet (PoE) models are also available. Please reference the N-Tron Series "NT24k Compact Industrial Managed Gigabit Ethernet Switches Hardware Manual" for more information.

Performance

NT24k-managed switches provide uncompromising performance in harsh environments, including network features like N-Ring™, Virtual Local Area Network (VLAN), Quality of Service (QoS), port mirroring, IGMP, Simple Network Time Protocol (SNTP) and Simple Network Management Protocol (SNMP). IEEE 1588v2 (Precision Time Protocol, or simply PTP) models are also available. Additionally, the NT24k offers IEEE 802.1X with RADIUS remote server authentication to ensure port security. These network management features provide best-in-class visibility, security, and uptime performance.

Environmental

The ultra-reliable NT24k switches are available in rackmount or DIN-rail mountable configurations with operating temperatures from -40 to 85°C. With UL Class I, Division 2 listing and CE certifications, these industrial switches are built to last in the most demanding and hazardous environments.

Monitoring

The N-View™ monitoring technology software provides 47 different status points on switch and port conditions and displays that information on any networked computer.

Security

The NT24k series provides a high level of security by utilizing IEEE 802.1X with RADIUS remote server authentication, MAC address based port security, Hyper Text Transfer Protocol Secure (HTTPS), Secure Shell or Secure Socket Shell (SSH), and SNMPv3 communication protocol to ensure the safest networks.

Refer to the NT24k Hardware Manuals for more information on our Modular and Compact Series.

Overview of Advanced Features

Mode of Operation

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

Copper Ports:
- Half-Duplex
- Full-Duplex
- Auto-Negotiation

1000Base Copper or any Fiber Ports:
- Full-Duplex

Half-Duplex

In half-duplex mode, the CSMA/CD media access ports share a common transmission medium. To transmit, a port waits (defers) for a quiet period on the medium (that is, no other port is transmitting) and then sends the intended message in bit-serial form. If, after initiating a transmission, the message collides with that of another port, then each transmitting port intentionally transmits for an additional predefined period to ensure propagation of the collision throughout the system. The port 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 ports 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.

However, a receiving endpoint may request that the transmitting endpoint pause transmission to prevent receive buffer overflow. When the receiving buffer capacity becomes sufficient again, the receiving endpoint will notify the transmitting endpoint that transmission may resume.

Auto-Negotiation

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

Port Mirroring

A Mirroring Port is a dedicated port that is configured to forward copies of Ethernet frames that are being sent or received from a monitored port. This is normally only used during troubleshooting and debug of the network. Under normal operation, Port Mirroring is disabled.

Port Trunking

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

Quality of Service (QoS)

QoS refers to resource reservation control mechanisms. QoS is the ability to provide different priorities to different applications, users, or data flows. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as Voice over IP, high resolution images, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

The QoS of an egressing frame can be set based on the three QoS mechanisms listed below:
1. IEEE 802.1p (Tagged QOS)

2.   DSCP (differentiated services code points) (RFC 2474)
3.   Port (Default Priority)

Virtual Local Area Network (VLAN)

The switch provides support for setting up tagged VLANs. A port may belong to any number of VLANs. The VLAN membership of an end device is determined by the VLAN(s) 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 its new port.

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

A default Virtual LAN (VID=1) exists so if a port is not a member of any other VLAN, it will default back to VLAN 1. This allows the switch to operate as a 'normal' switch when it is used in a network. A port may be automatically removed from the default VLAN when it is reconfigured to belong to another VLAN. By default, the switch will automatically remove a port from the default VLAN when it is reconfigured to another VLAN. See the VLAN configuration section in Chapter 2 for additional information.

If switch ports are configured to transmit and receive untagged frames, then their connected 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 to tagged ports on the switch. VLANs can also be configured to accept tagged packets in tagged ports, strip the tags off the packets, and then send the packets back out to other untagged ports. This allows a network administrator to set up the switch to support devices on the network that do not support VLAN tagged packets. The administrator can also set up the ports to discard any packets that are tagged or to discard any packets that are untagged, based on a hybrid VLAN of both tagged and untagged ports and by 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 (VID) (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 NT24k® switch also has the ability to allow overlapping VLANs. Overlapping VLANs give the user the ability to have one or more ports share two or more VLAN groups. For more information and examples on how this could be implemented, refer to the 'VLAN Configuration Examples' in this document, and/or our website's technical documents.

Note: RSTP is only supported on one VLAN.

Rapid Spanning Tree Protocol (RSTP)

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

REDLION®

RSTP provides quicker learning of network topology changes than the older STP. RSTP supports new and improved features such as the rapid transition of ports to the forwarding state. While STP transmits BPDUs (Bridge Protocol Data Units) from only the root bridge, RSTP transmits BPDUs from every bridge. RSTP inter-operates with older STP switches by falling back to STP when the older BPDUs are detected on bridge ports. The user can also manually configure bridge ports to use STP, if desired.

SNMP Traps

The NT24k® Series switch supports SNMP Trap Stations to which SNMP Traps will be sent. Four standard SNMP traps are supported: Link Status (Link Up / Link Down), Cold Start, Warm Start, and Authentication Errors. SNMP Traps are sent to all trap stations configured on a given switch when the corresponding trap is enabled.

IGMP Snooping

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

The Internet Group Management Protocol (IGMP) is a protocol that provides a way for a device to report its multicast group membership to adjacent 'routers'. In this case NT24k 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 NT24k series supports v1 and v2.

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.

N-Link

The purpose of N-Link is to provide a way to redundantly couple an N-Ring topology to another topology, typically another N-Ring topology. Each N-Link configuration requires 4 switches, two on each network. On the N-Ring network, one switch is the N-Link Master and an adjacent switch is the N-Link Slave. On the connected network, one switch is the N-Link Primary Coupler and another switch is the N-Link Standby Coupler.

N-Link monitors the link status of the Primary and Standby Coupler links. As long as the Primary Coupler link is healthy, N-Link forwards network traffic and the Standby Coupler link blocks network traffic. When a problem is detected on the Primary Coupler link, the Primary Coupler link blocks network traffic and the Standby Coupler forwards network traffic. While the N-Link Master and Slave are in communication via the Control link, only one Coupler link (Primary or Standby) forwards network traffic, while the other Coupler link blocks network traffic.

N-Ring™

N-Ring is designed for easy setup. Switches are configured for N-Ring membership, by default. Setting a switch as the N-Ring Manager is the only required step for enabling the ring as long as preset ports are used to connect ring members. Subsequently, N-Ring operates dynamically upon each power up. N-Ring technology offers expanded ring size capacity, detailed fault diagnostics, and a standard healing time of 30ms. The N-Ring Manager periodically checks the health of the N-Ring via health check packets. If the N-Ring Manager stops receiving the health check packets, it times-out and converts the N-Ring to a

backbone within 30ms. When using all N-Ring enabled switches in the ring, a detailed ring map and fault location chart is also provided on the N-Ring Manager's web browser. N-Ring status is also sent from the N-Ring Manager to the N-View™ OLE for Process Control (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.

Bypass Relay (BR)

BR ports have an internal hardware technology that forces paired BR ports to create a physical connection when the switch powers down. The BR switch is in bypass mode when it is powered down. This feature allows devices connected via these ports to continue communicating despite the BR switch being powered down.

Traffic physically and logically flows through all switches when the BR switch is powered on.

Traffic physically flows through the relay, but from a logical standpoint, bypasses the powered down BR switch.
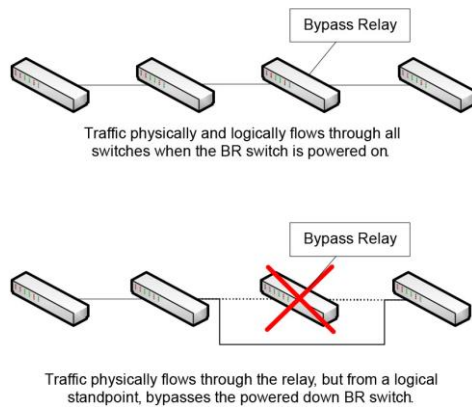
> **Note:** BR ports are only supported on select NT24k® models. BR-capable equipment is denoted by a "-R" in the model name. Likewise, BR capable ports are denoted by a "-R" in the port description.
>
> **Note:** Some port protocols and port properties are not supported or may be affected by BR ports.

Affected Port Protocols

802.1X

802.1X security cannot be enabled on BR ports. Allowing this protocol on BR ports will lead to network security issues when the switch enters bypass mode. Therefore, 802.1X security is not allowed.

N-Link

N-Link Coupler and Control ports cannot be selected on BR ports. If BR ports were utilized for these links, there would be connection issues upon the switch entering bypass mode. It is also a best practice to ensure that neither the Master nor Slave Partner ports are connected to a BR port. Unlike the Coupler and Control ports, these ports are not user configured, but are auto-detected by the N-Link protocol. Use extra care when introducing BR equipment into an N-Link topology and avoid using BR ports for the N-Link connections.

N-Ring™

N-Ring Manager, Auto Member, and Multi Member cannot be enabled on BR port sets. N-Ring port sets exclude BR-capable ports.

RSTP

RSTP is disabled on BR ports to prevent unacceptable performance within an RSTP topology.

IGMP

Caution must be taken when IGMP is enabled. Devices connected to BR ports must be able to accommodate higher traffic rates. Test your network conditions with the BR switch both powered on and off if IGMP is to be enabled on a BR port.

Affected Port Properties

Port Trunking

BR port pairs cannot be members of the same trunk group to prevent a network loop being created in bypass mode.
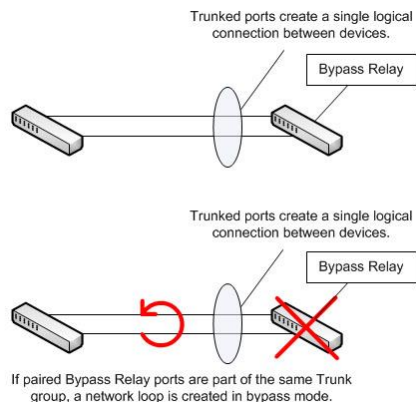
VLAN

VLAN group membership must be identical between BR port pairs to ensure proper flow of traffic when the switch enters bypass mode. Caution must also be taken when modifying VLAN tags or filtering VLAN traffic on BR ports to ensure that all devices connected to BR ports can accommodate VLAN traffic whether the BR switch is powered on or powered off.

> **Note:** The VLAN(s) associated with RSTP may contain BR ports, however RSTP will be disabled on the BR ports.

Port Compatibility

Care should be taken to ensure port characteristics of devices connected via BR ports are compatible, so that there are no interruptions in traffic when a BR switch enters bypass mode.

Ports and/or devices connected to the BR ports must be configured with compatible settings.

The following characteristics should be compatible for devices connected via BR ports:

- Auto-Negotiation
- Port Speed
- Duplex Mode
- Flow Control
- Flow Control
- PVID
- QoS
- Rate Limiting

For example, if switches A and B are connected via a BR switch, the connecting port on switch A should have the same configured port speed as the connecting port on switch B. If these ports have incompatible speeds, they may have issues communicating once the switch enters bypass mode.

The ports connected to the Bypass Relay ports, on each of these devices, must have compatible settings.
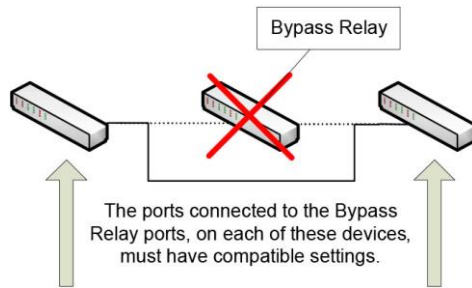
Note: It is still possible to customize port settings in any configuration desired, based on network requirements. Network testing must be performed to ensure correct network operation whether the switch is powered on or powered off.

Segment Length

Based on IEEE specifications, the maximum segment length for 10/100/1000BaseT(X) is 100 meters (328 ft). This requirement applies to combined segment lengths between all devices connected via BR port pairs. Staying within the IEEE specified segment length ensures proper operation.

Maximum cable length of 100 meters in case the relay goes down

Maximum cable length of 100 meters, in case both relays go down
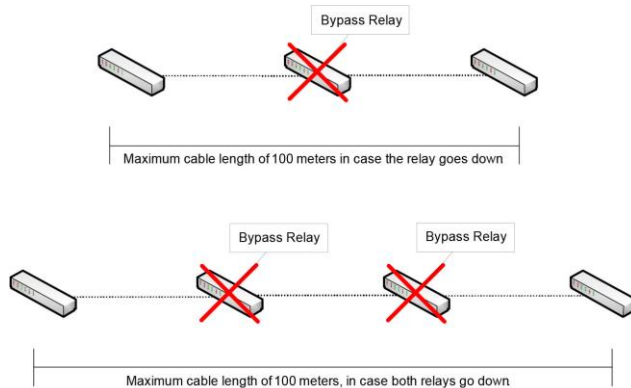
CIP™

The CIP (Common Industrial Protocol) feature allows N-Tron® Series 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 trigger 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). Red Lion created EDS and ICO files are provided with the NT24k® switch series.

Note: Information about using CIP with the NT24k can be found in the CIP User Manual & Installation Guide and the CIP Installation Kit for the NT24k switch family.

PTP

Precision Time Protocol (PTP), IEEE 1588v2, is supported on licensed NT24k models. PTP allows users to configure a network with very accurate, coordinated timing among devices. NT24k models with software implementations of PTP are capable of achieving accuracy in the low microseconds range. PTP is disabled by default and can be enabled as a Boundary or Transparent clock through the Web Browser interface. The switch must have a valid PTP license installed before PTP can be enabled.

RedLion®

Point-to-Point Protocol (PPP)

PPP allows a browser-like interface over the CLI port.

Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) simplifies network configuration by automatically assigning IP addresses from a DHCP server to connected DHCP capable devices (DHCP clients). NT24k® switch configuration options include:

- DHCP Server
- DHCP Relay Agent
- DHCP Client

DHCP Server

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

DHCP Relay Agent (Option 82) allows communication between the client and server to cross subnet and VLAN boundaries.

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 Client is enabled by default, with 192.168.1.201 as the factory fallback address.

Event Logging

The switch can be configured to log certain system events as they occur. Event Logging is enabled by default for critical events. Event log options are easily changed through a Web browser.

Even Logging includes:

- System startup and shutdown
- Logon and logout from the Web or Console
- Ports becoming enabled or disabled
- Port link up or link down changes
- N-Ring™ status changes

The most recent log information is visible via the web interface and the complete log file may be exported for external analysis.

Event Log Filter

The Event Log Filter enables the user to define which events are logged, based on severity level. Events that do not meet the minimum severity level for that component are not logged.

Syslog

The Syslog protocol, as specified in RFC-3164 and RFC-5424, are supported. The Syslog allows users to configure the switch so that certain system events (see Event Logging) are transmitted to a remote

logging device, known as a Syslog Collector. The Syslog is disabled by default but can be enabled/disabled through the Web Browser interface.

Local Security

The switch is configured for secure access by the SSH and HTTPS. The Telnet Server and Hypertext Transfer Protocol (HTTP) may be enabled to provide backwards compatibility with less secure clients.

Secure Shell

SSH, is a secure alternative to Telnet. A maximum of two concurrent SSH / Telnet connections are allowed.

The commands SFTP (SSH File Transfer Protocol or Secure File Transfer Protocol) and SCP (Secure Copy) are not supported.

Port Security

Port Security can be enabled on the MAC address level for additional security. The Port Security feature restricts access to the switch by only accepting dynamically learned MAC addresses and manually entered MAC addresses as authorized. Dynamically learned MAC addresses are those that the switch detects on any port while in 'Learning' mode. A manually entered MAC address must designate the ports that the address is authorized on. A non-authorized MAC address will be discarded and will be listed in the intruder log.

Port security supports RSTP provided the MAC address(es) are manually authorized on the RSTP ports.

LLDP

The Link Layer Discovery Protocol (LLDP), as specified in IEEE 802.1AB and IEEE 802.3-2012, is used by networking devices to advertise there identity and capabilities and to discover their network neighbors. LLDP can be configured in one of three modes: Enabled, Auto and Disabled. The "Auto" mode is an enhancement to the LLDP protocol.

When in Auto mode, LLDP is inactive until a switch sends a wake up packet. At this point, all switches set to Auto mode will become active until the Wake Time interval expires.

Troubleshooting

1. Make sure the Power LED is ON.
2. Make sure sufficient current is supplied to the switch (per model specifications).
        Note: The Inrush current will exceed the steady state current by ~ 2X.
3. Verify that Link LEDs are ON for connected ports.
4. Verify integrity of cabling between stations.
5. Verify that cabling is Category 5E or greater for 100Mbit and Gigabit operation.

Chapter 3   Web Software Configuration

Accessing the Web Software Interface

Launch a web browser and enter the IP address of the device into the address bar. The DHCP Client is enabled by default with 192.168.1.201 as the fallback address.

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 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 unit used, a screen similar to the one below will appear:

Organization

After logging onto a NT24k® switch, the Product Information page will be displayed. On the left-hand side of the screen is a list of configurable settings supported by the NT24k switch. Below is a list of these settings with a description of their purpose.

- **Product Information:** Basic information about the switch is provided in this menu.

- **Configuration:** The Configuration page is used to save or reset a running configuration.

- **Event Log:** The Event Log page is used for modifying and viewing the internal event logs.

- **Fault:** A fault is a notification of a destabilizing event. Which events are watched for and how notifications occur are configured on the Fault page.

- **File Transfer:** The File Transfer page provides the administrator the ability to upgrade the firmware or to import or export a configuration file, and export the Event Log to a file.

- **Network:** The network page is used to setup the device's IP and IP Fallback addresses, as well as Client ID and IP Configuration.

- **System:** The System page provides information pertaining to the whole system.

- **User Management:** The User Management page is used to view, add, modify and remove system user accounts, and set permissions.

- **Advanced:** The Advanced section is used to setup advanced features of the system.

- **Help:** The Help section is used to display information on configuring and monitoring the manageable parameters of the device. Specific help can be found by using the left navigation menu.

Product Information

Once a user logs onto an NT24k® switch, the Product Information page is displayed. This page shows basic information about the switch and can also be accessed by selecting the Product Information menu item on the left-hand menu.

Modular Models

Product Information

Product Name	NT24k-DR24-DC
Switch Model	NT24k-DR24
Switch Family	NT24k
Software Version	1.8.0
Build Date	Mar 04 2015, 16:58:39
Boot Loader	1.8.0
Copyright	Copyright © 2008-2015
URL	http://www.redlion.net/
Switch Modules	Slot A: SFP-DM8 A1: Empty A2: Empty A3: Empty A4: Empty A5: Empty A6: Empty A7: Empty A8: Empty Slot B: TX8 Slot C: FX8

Compact Series

Product Information

Product Name	NT24k-12SFP-DM4
Switch Model	NT24k-12SFP-DM4
Switch Family	NT24k
Software Version	1.8.0
Build Date	Mar 04 2015, 16:58:39
Boot Loader	1.8.0
Copyright	Copyright © 2008-2015
URL	http://www.redlion.net/
SFP Transceivers	DM1: Empty DM2: Empty DM3: Empty DM4: Empty

Product Name: The full name of the switch, including any factory configured options will be displayed in this field.

For example, the product name will show NT24K-AC1 if there is one AC power unit in either location and NT24K-AC2 if there are two AC power units. If the product name ends with DC1 or DC2, this indicates that there is either one or two DC power units.

Switch Model: The base model of the switch.

Switch Family: The switch family this model and similar models belong to.

Software Version: The current firmware software version.

Build Date: The build date of the firmware.

Boot Loader: The boot loader version.

URL: This field links to Red Lion's website.

Switch Modules: The modules currently installed, including installed SFP transceivers. This option may not be present on models where modules or SFPs are not supported.

SFP Transceivers: On models where SFP transceivers are supported, the currently installed SFP transceivers will be shown in this field.

Configuration

The Configuration page allows the Administrator to save a running configuration in the switches non-volatile memory. This step is required if the switch is to remember any configuration changes after a power cycle or reboot. From this page, the Administrator can also restore a previously saved configuration, restore factory defaults or force a system reboot.

Save: Click on the *Save* button to save all current changes to the configuration stored in non-volatile memory for use after the next power cycle or reboot. If a configuration device is installed and enabled, the configuration will also be saved to the device. This option is only available when there is no misconfiguration.

Restore: Click on the *Restore* button to discard all unsaved changes and load the most recently saved configuration. If a configuration device is installed and enabled, the configuration stored on the device will be loaded and used. *See notes below*.

Reboot: Click on the *Reboot* button to reboot the switch and load the most recently saved configuration. If a configuration device is installed and enabled, the configuration stored on the device will be loaded and used. *See notes below*.

Factory: Click on the *Factory* button to reset the switch's configuration to factory defaults except for any of the selected items. Selecting the Factory option will only affect the current configuration. A *Save* must be performed in order to retain these changes after a power cycle or reboot.

- **Keep current IP address, subnet mask, and gateway:** Retains the existing IP address, subnet mask and gateway if desired.
- **Keep current user names, passwords, and RADIUS configuration:** Retain the existing user names, passwords, and RADIUS configuration if desired.

- **Keep currently stored SNMP settings:** Retains the existing SNMP settings if desired.
- **Keep currently stored Port Security settings:** Retain the existing Port Security settings if desired.
- **Keep current PoE Settings:** Retains the existing PoE settings if desired (PoE models only).
  > Note: When the configuration is loaded from the Configuration Device, it must be saved for it to be available if the Configuration Device is removed.
  > Note: When the switch is shipped, it does not have a "configuration file" since the unit is using the factory defaults. Before a configuration can be customized, click on the Save button in order to create the file.

Configuration Fault

When the switch is booted and misconfigured settings are detected, a Configuration Fault will be triggered and the configuration may not be saved. This can occur when updating system firmware where settings permitted in the previous release may no longer be permitted. In this case, the *Save* button will be replaced with a *Show Errors* button (as seen below) and the misconfigured settings must be fixed before the configuration may be saved.

Show Errors: Click on the Show Errors button to view the current configuration and display any detected errors. This button is only visible when there is a settings misconfiguration.

Event Log

The Event Log View page displays the most recent 200 events that have occurred since the latest system startup or since the log was cleared. Event logging is enabled by default for critical events. Only events that occur while the Event Log was enabled will be displayed and saved with the exception of the Clear Log message which will always be displayed. Therefore, previously enabled events are still displayed when Event Logging is disabled albeit they may not be recent events.

If the Event Log was disabled when the latest Startup event occurred, no events will be displayed as shown below.
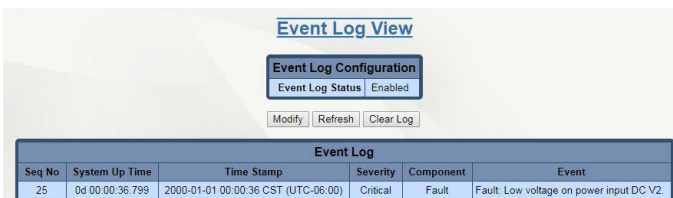
When the Event Log is cleared, an informational event will be displayed.
> Note: All enabled events since the last Clear Log event, including multiple Startup and Shutdown events, are stored on the system and may be exported as a CSV file from the switch for additional analysis.
> Note: The event log can contain 2000 or more entries depending on individual message size. If the event log becomes full, new entries will overwrite the oldest entries.

A normal startup or reboot will show startup, RSTP status, N-Ring™ and logon events. An example reboot is shown below.
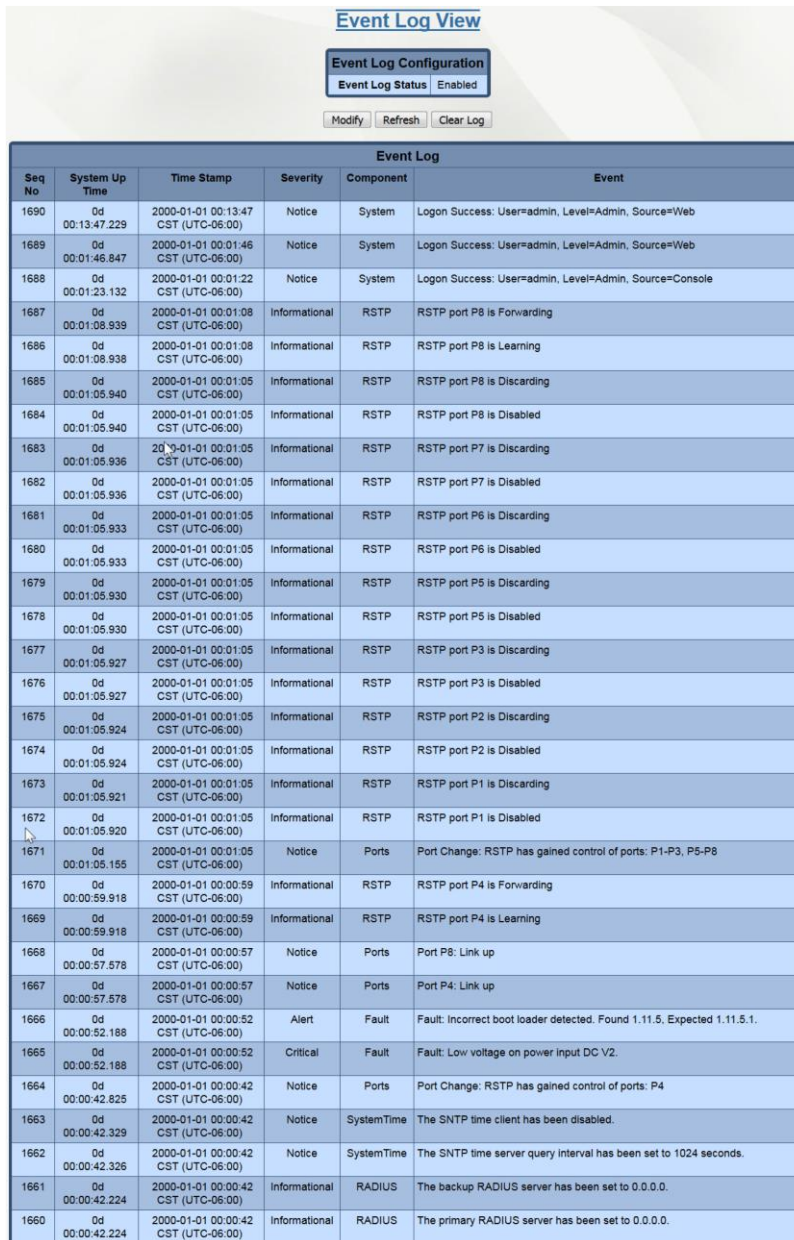
Modify: Display the Modify Event Log Configuration page.

Refresh: Refresh the current Event Log display.

Clear Log: Remove all entries from the event log and then add "The event log has been cleared." message.

The Modify Event Log Configuration page controls whether Event Logging is Enabled or Disabled.
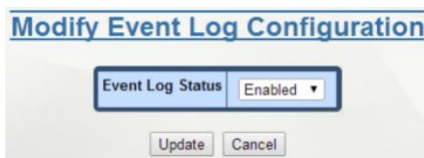
Event Log Status: Select Enabled/Disabled.

Update: Set the new Event Log Status.

Cancel: Return to Event Log View without modifying Event Log Status.

The entire Event Log may be exported to the host PC for further analysis and archiving purposes. It will contain all events that occurred while Event Log was enabled since the last Clear Log event.

On the File Transfer - Firmware/Config page, select Transfer Type: Export Event Log from switch.

Click on Event Log in the Export Event Log from switch panel, and select the storage location for the exported file on the PC.

The default file name is "eventlog.csv", which outputs each line in the Event Log as comma separated fields with the final text field surrounded by quotation marks. This file can be viewed with a spreadsheet application or a simple text file viewer.

The Cancel button selection will return to the Product Information page without executing any transfers.

Example Event Log CSV in Microsoft Excel:

Seq No	Boot Count	System Up Time	Time Stamp	Severity	Component	Event
	Log Ver	File Info				
	1	5423				
2628	3374	0d 15:32:01.753	1/1/2000 15:31	Informational	Event Log	The event log has been cleared.
2629	3374	0d 15:32:34.018	1/1/2000 15:31	Notice	Event Log	The event log has been enabled
2630	3374	0d 15:33:25.933	1/1/2000 15:32	Notice	System	System Shutdown (User initiated)
2631	3375	0d 00:00:35.819	1/1/2000 0:00	Notice	System	System Startup: MAC Address=00:07:af:7d:95:c0 (warm start)
2632	3375	0d 00:00:36.934	1/1/2000 0:00	Informational	N-Ring	Not part of an N-Ring: Mode=Auto Member
2633	3375	0d 00:00:38.872	1/1/2000 0:00	Informational	RSTP	RSTP port A4 is Disabled
2634	3375	0d 00:00:38.873	1/1/2000 0:00	Informational	RSTP	RSTP port A4 is Blocking
2635	3375	0d 00:00:53.568	1/1/2000 0:00	Notice	Ports	Port A7: Link up
2636	3375	0d 00:01:01.874	1/1/2000 0:00	Informational	RSTP	RSTP port A1 is Disabled
2637	3375	0d 00:01:01.874	1/1/2000 0:00	Informational	RSTP	RSTP port A1 is Blocking
2638	3375	0d 00:01:01.878	1/1/2000 0:00	Informational	RSTP	RSTP port A2 is Disabled
2639	3375	0d 00:01:01.878	1/1/2000 0:00	Informational	RSTP	RSTP port A2 is Blocking
2640	3375	0d 00:01:01.881	1/1/2000 0:00	Informational	RSTP	RSTP port A3 is Disabled
2641	3375	0d 00:01:01.881	1/1/2000 0:00	Informational	RSTP	RSTP port A3 is Blocking
2642	3375	0d 00:01:01.884	1/1/2000 0:00	Informational	RSTP	RSTP port A5 is Disabled
2643	3375	0d 00:01:01.885	1/1/2000 0:00	Informational	RSTP	RSTP port A5 is Blocking
2644	3375	0d 00:01:01.888	1/1/2000 0:00	Informational	RSTP	RSTP port A6 is Disabled
2645	3375	0d 00:01:01.888	1/1/2000 0:00	Informational	RSTP	RSTP port A6 is Blocking
2646	3375	0d 00:01:01.891	1/1/2000 0:00	Informational	RSTP	RSTP port A7 is Disabled
2647	3375	0d 00:01:01.892	1/1/2000 0:00	Informational	RSTP	RSTP port A7 is Blocking
2648	3375	0d 00:01:01.895	1/1/2000 0:00	Informational	RSTP	RSTP port A8 is Disabled
2649	3375	0d 00:01:01.895	1/1/2000 0:00	Informational	RSTP	RSTP port A8 is Blocking
2650	3375	0d 00:01:01.898	1/1/2000 0:00	Informational	RSTP	RSTP port B1 is Disabled
2651	3375	0d 00:01:01.899	1/1/2000 0:00	Informational	RSTP	RSTP port B1 is Blocking
2652	3375	0d 00:01:01.902	1/1/2000 0:00	Informational	RSTP	RSTP port B2 is Disabled
2653	3375	0d 00:01:01.902	1/1/2000 0:00	Informational	RSTP	RSTP port B2 is Blocking
2654	3375	0d 00:01:01.905	1/1/2000 0:00	Informational	RSTP	RSTP port B3 is Disabled
2655	3375	0d 00:01:01.905	1/1/2000 0:00	Informational	RSTP	RSTP port B3 is Blocking
2656	3375	0d 00:01:01.909	1/1/2000 0:00	Informational	RSTP	RSTP port B4 is Disabled
2657	3375	0d 00:01:01.909	1/1/2000 0:00	Informational	RSTP	RSTP port B4 is Blocking
2658	3375	0d 00:01:01.912	1/1/2000 0:00	Informational	RSTP	RSTP port B5 is Disabled
2659	3375	0d 00:01:01.912	1/1/2000 0:00	Informational	RSTP	RSTP port B5 is Blocking
2660	3375	0d 00:01:01.915	1/1/2000 0:00	Informational	RSTP	RSTP port B6 is Disabled
2661	3375	0d 00:01:01.916	1/1/2000 0:00	Informational	RSTP	RSTP port B6 is Blocking
2662	3375	0d 00:01:01.919	1/1/2000 0:00	Informational	RSTP	RSTP port B7 is Disabled
2663	3375	0d 00:01:01.919	1/1/2000 0:00	Informational	RSTP	RSTP port B7 is Blocking
2664	3375	0d 00:01:01.922	1/1/2000 0:00	Informational	RSTP	RSTP port B8 is Disabled
2665	3375	0d 00:01:01.923	1/1/2000 0:00	Informational	RSTP	RSTP port B8 is Blocking
2666	3375	0d 00:01:01.926	1/1/2000 0:00	Informational	RSTP	RSTP port C1 is Disabled
2667	3375	0d 00:01:01.926	1/1/2000 0:00	Informational	RSTP	RSTP port C1 is Blocking
2668	3375	0d 00:01:01.929	1/1/2000 0:00	Informational	RSTP	RSTP port C2 is Disabled
2669	3375	0d 00:01:01.930	1/1/2000 0:00	Informational	RSTP	RSTP port C2 is Blocking
2670	3375	0d 00:01:01.933	1/1/2000 0:00	Informational	RSTP	RSTP port C3 is Disabled
2671	3375	0d 00:01:01.933	1/1/2000 0:00	Informational	RSTP	RSTP port C3 is Blocking
2672	3375	0d 00:01:01.936	1/1/2000 0:00	Informational	RSTP	RSTP port C4 is Disabled
2673	3375	0d 00:01:01.936	1/1/2000 0:00	Informational	RSTP	RSTP port C4 is Blocking
2674	3375	0d 00:01:01.940	1/1/2000 0:00	Informational	RSTP	RSTP port C5 is Disabled
2675	3375	0d 00:01:01.940	1/1/2000 0:00	Informational	RSTP	RSTP port C5 is Blocking
2676	3375	0d 00:01:01.943	1/1/2000 0:00	Informational	RSTP	RSTP port C6 is Disabled
2677	3375	0d 00:01:01.943	1/1/2000 0:00	Informational	RSTP	RSTP port C6 is Blocking
2678	3375	0d 00:01:01.946	1/1/2000 0:00	Informational	RSTP	RSTP port C7 is Disabled
2679	3375	0d 00:01:01.947	1/1/2000 0:00	Informational	RSTP	RSTP port C7 is Blocking
2680	3375	0d 00:01:01.950	1/1/2000 0:00	Informational	RSTP	RSTP port C8 is Disabled
2681	3375	0d 00:01:01.950	1/1/2000 0:00	Informational	RSTP	RSTP port C8 is Blocking
2682	3375	0d 00:01:04.848	1/1/2000 0:00	Informational	RSTP	RSTP port A7 is Learning
2683	3375	0d 00:01:04.848	1/1/2000 0:00	Informational	RSTP	RSTP port A7 is Forwarding
2684	3375	0d 00:24:23.223	1/1/2000 0:23	Notice	System	Logon Success: User=admin, Level=Admin, Source=Web
2685	3375	0d 00:24:23.223	1/1/2000 0:23	Informational	Event Log	[End of Events]

Where the fields are:

Sequence Number: Each entry is assigned the next sequence number – these may not always be listed in numerical order due to the priority of the internal tasks which generate the events.

> **Note:** The "[End of Events]" message at the end of the file will contain the next sequence number, but that number will be reused for the next system event on the switch when it occurs.

Boot Count: A count of how many times the switch has been powered up or restarted.

System Up Time: The amount of time since the system was started in days, hours, minutes, seconds, milliseconds.

Time Stamp: Corresponding date, hours, minutes, seconds, based on the initial value of Current System Time as defined in the System Configuration View.

Severity: (most severe to least severe):

Emergency: Major failure, Immediate intervention required

Alert: Failure of a component, Immediate corrective steps should be taken
Critical: Partial failure of a component, Immediate corrective action should be taken
Error: Non-urgent failure
Warning: Not an error, but may lead to an error if action is not taken
Notice: Unusual event, but not an error
Informational: General Information
Debug: Information useful to a support technician for debugging the switch operation.

Component: Internal component that generated the event entry.

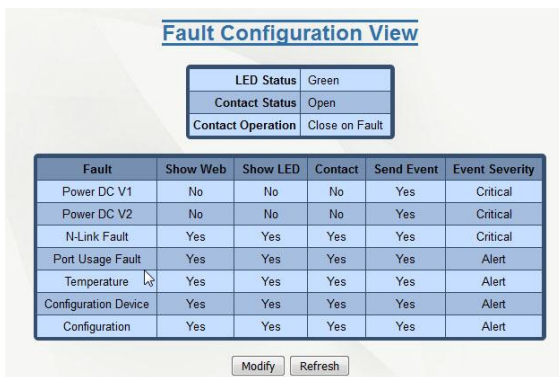**Event Description:** Description of the event entry.

Fault

The Fault page provides configurable selections indicating the different ways to notify an administrator when a fault occurs. In each case, the notification may consist of any combination: Show Web, Show LED and/or Contact. Some fault configurations are only available under specific conditions. For example, Power AC is only available when an AC power supply is installed in the switch. N-Ring™ faults are only available when the switch is set to N-Ring Manager mode. The page below is an example of what may be seen on the Fault dialog window.

Additionally, when a fault is triggered, an event may be generated at the severity selected by the user. The event will be logged unless it is filtered by the Event Log Filter.

The event's severity can be set to any of the following values.

   Note: These are based on the Event Log's Severity:
      Emergency
      Alert
      Critical
      Error
      Warning
      Notice
      Informational
      Debug

Fault Configuration View

LED Status	Green
Contact Status	Open
Contact Operation	Close on Fault

Fault	Show Web	Show LED	Contact	Send Event	Event Severity
Power DC V1	No	No	No	Yes	Critical
Power DC V2	No	No	No	Yes	Critical
N-Link Fault	Yes	Yes	Yes	Yes	Critical
Port Usage Fault	Yes	Yes	Yes	Yes	Alert
Temperature	Yes	Yes	Yes	Yes	Alert
Configuration Device	Yes	Yes	Yes	Yes	Alert
Configuration	Yes	Yes	Yes	Yes	Alert

Modify   Refresh

LED Status: This field shows the current color of the Power/Fault LED. Green indicates there is no fault and Red indicates a fault condition exists.

Contact Status: This field shows the current open/closed status of the fault relay.*

Contact Operation: This field determines if the fault relay is normally open (Close on Fault) or normally closed (Open on Fault).*

Show Web: If the *Show Web* option is enabled, the fault is displayed on the browser pages.

Show LED: If the *Show LED* option is enabled, the fault is indicated on the Power LED as red.

Contact: If *Contact* is enabled, the fault is indicated by opening or closing the contact switch.

Send Event: The fault is sent to the configured log(s). See the Event Log and Syslog configuration.

Event Severity: The fault will generate an event based on the configured severity level.

To make changes to the *Fault Configuration* settings, click on the *Modify* button.
      * **Note:** Fault's contact is only supported on certain NT24k® switches.
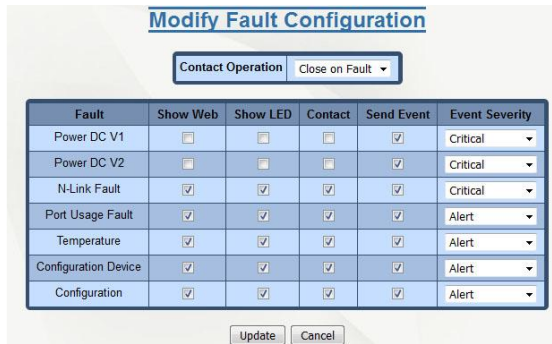
Select the desired notification settings and click on the *Update* button to save any changes. Once the save is complete, the dialog window will change to Fault Configuration.

Power Fault Descriptions

The location of a power input is clearly marked on the device. Depending on the specific device configuration, some of the faults listed below may not be shown.
      Note: Power Fault notifications are disabled in factory defaults on a low voltage power supply.
      Power AC1: Indicates a low voltage on power input AC1.
      Power AC2: Indicates a low voltage on power input AC2.
      Power DC V1: Indicates a low voltage on power input DC V_1.
      Power DC V2: Indicates a low voltage on power input DC V_2.
      Power DC V3: Indicates a low voltage on power input DC V_3.
      Power DC V4: Indicates a low voltage on power input DC V_4.

N-Ring™ Manager Fault Descriptions

The faults listed below appear when the switch is configured as an N-Ring manager.
      N-Ring Broken: Indicates that an N-Ring connection is completely broken.
      N-Ring Partial Break (High): Indicates that an N-Ring connection is only broken in the direction of the higher port.
      N-Ring Partial Break (Low): Indicates than an N-Ring connection is only broken in the direction of the lower port.
      N-Ring Multiple Managers: Indicates that more than one N-Ring Manager exists on an N-Ring.

Miscellaneous Fault Descriptions

      N-Link Fault: Indicates a problem with the N-Link configuration.
      Port Usage Fault: Indicates that the port usage, for one or more ports, is below the Usage Alarm Low setting, or above the Usage Alarm High setting (see Port Configuration View and Port Utilization View).
      Temperature: Indicates that the temperature of the switch is outside of the configured limits.
      Configuration Device: Indicates that the configuration on an installed configuration device is invalid.
      Configuration: Indicates that a setting misconfiguration needs to be resolved.

File Transfer

File Transfer gives the administrator the ability to import files to the switch or export files from the switch.
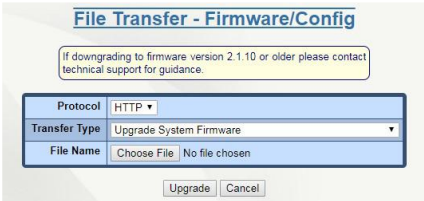
> **Note:** Do not cycle power on the switch or interrupt the data connection between the PC and the switch while a file is being transferred.

Protocol: Select whether HTTP, HTTPS, or TFTP protocol is to be used for transfers.

Transfer Type: The different types of transfer that can be used are listed in the drop-down list. The options are: Upgrade System Firmware, Upgrade BootLoader Firmware, Import Configuration to Switch, Import Port Security Authorization List to Switch, Import License to Switch, Export Saved Configuration from Switch, Export Saved Port Security Authorization List from Switch, and Export Event Log from Switch.
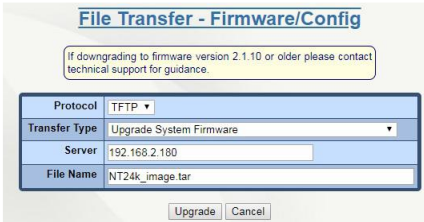
Upgrade System Firmware: Select this option to install the system firmware to the switch.

HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol HTTP ▾ Transfer Type Upgrade System Firmware ▾ File Name Choose File No file chosen Upgrade Cancel	**File Transfer - Firmware/Config** If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol TFTP ▾ Transfer Type Upgrade System Firmware ▾ Server 192.168.2.180 File Name NT24k_image.tar Upgrade Cancel
File Name: Click on the *Browse* button to browse to the desired location and select an image file (typically called NT24k_image.tar). File names are limited to a maximum length of 63 characters.	**Server:** This field displays the IP address of the TFTP server. It is automatically populated with the IP address of the PC which is connected to the switch. **File Name:** This field displays the name of the file to be imported (typically NT24k_image.tar). File names are limited to a maximum length of 63 characters.

Click on the *Upgrade* button to upgrade the system.

> **Note:** After successfully transferring new firmware to the switch, the switch must be rebooted.

> **WARNING:** Due to security enhancements, downgrading the system firmware to 2.1.10 or older will reset all passwords to "password" (users and administrators). The Administrator should immediately change each user's password and notify the user.

Upgrade BootLoader Firmware: Select this option to install the bootloader firmware.

HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: HTTP ▼ Transfer Type: Upgrade BootLoader Firmware ▼ File Name: Choose File No file chosen Upgrade Cancel	**File Transfer - Firmware/Config** If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: TFTP ▼ Transfer Type: Upgrade BootLoader Firmware ▼ Server: 192.168.2.180 File Name: NT24k_bootloader.tar Upgrade Cancel
File Name: Click on the Browse button to browse to the desired location and select an image file (typically NT24k_bootloader.tar). File names are limited to a maximum length of 63 characters.	**Server:** This field displays the IP address of the TFTP server. **File Name:** This field displays the name of the file to be imported (typically NT24k_bootloader.tar). File names are limited to a maximum length of 63 characters.

Click on the *Upgrade* button to upgrade the system.

> **Note:** After successfully transferring new firmware to the switch, the switch must be rebooted.

Import Configuration to Switch: Select this option to change the switch configuration by importing a configuration file.

HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: HTTP ▼ Transfer Type: Import Configuration to switch ▼ File Name: Choose File No file chosen Import Configuration to switch ☐ Keep current IP Address, Gateway and Subnet Mask ☐ Keep current user names, passwords, and RADIUS configuration ☐ Keep current SNMP settings ☐ Keep current Port Security settings Import Cancel	**File Transfer - Firmware/Config** If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: TFTP ▼ Transfer Type: Import Configuration to switch ▼ Server: 192.168.2.180 File Name: NT24k_settings.xml Import Configuration to switch ☐ Keep current IP Address, Gateway and Subnet Mask ☐ Keep current user names, passwords, and RADIUS configuration ☐ Keep current SNMP settings ☐ Keep current Port Security settings Import Cancel
File Name: Click on the Browse button to browse to the desired location and select a configuration file (typically NT24k_settings.xml). File names are limited to a maximum length of 63 characters. **Import Configuration to switch:** Select which configuration settings to keep when the new configuration file is imported by checking on the relevant checkbox.	**Server:** This field displays the IP address of the TFTP server. **File Name:** This field displays the name of the file to be imported (typically NT24k_settings.xml). File names are limited to a maximum length of 63 characters. **Import Configuration to switch:** Select which configuration settings to keep when the new configuration file is imported by checking on the relevant checkbox.

Click on the *Import* button to upgrade the system.

> **Note:** Find out more on working with Configuration Files in **Appendix B Working with Configuration Files.**

Import Port Security Authorization List to Switch: Select this option to change the Port Security Authorization List by importing a configuration file.

HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol [HTTP ▾] Transfer Type [Import Port Security Authorization List to switch ▾] File Name [Choose File] No file chosen [Import] [Cancel]	**File Transfer - Firmware/Config** If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol [TFTP ▾] Transfer Type [Import Port Security Authorization List to switch ▾] Server [192.168.2.180] File Name [NT24k_portsecurity.auth] [Import] [Cancel]
File Name: Click on the Choose File button to browse to the desired location and select a configuration file (typically NT24k_portsecurity.auth). File names are limited to a maximum length of 63 characters. **Import Port Security Authorization List to switch:** Select which configuration settings to keep when the new configuration file is imported by checking on the relevant checkbox.	**Server:** This field displays the IP address of the TFTP server. **File Name:** This field displays the name of the file to be imported (typically NT24k_portsecurity.auth). File names are limited to a maximum length of 63 characters. **Import Port Security Authorization List to switch:** Select which configuration settings to keep when the new configuration file is imported by checking on the relevant checkbox.

Click on the *Import* button to upgrade the system.

> **Note:** Find out more on working with Configuration Files in **Appendix B Working with Configuration Files.**

Import License to Switch: Select this option to install a license to the switch by importing a license file.

HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol [HTTP ▾] Transfer Type [Import License to switch ▾] File Name [Choose File] No file chosen [Import] [Cancel]	**File Transfer - Firmware/Config** If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol [TFTP ▾] Transfer Type [Import License to switch ▾] Server [192.168.2.180] File Name [NT24k_license.lic] [Import] [Cancel]
File Name: Click on the Browse button to browse to the desired location and select a license file (typically NT24k_license.lic). File names are limited to a maximum length of 63 characters.	**Server:** This field displays the IP address of the TFTP server. **File Name:** Click on the Browse button to browse to the desired location and select a license file (typically NT24k_license.lic). File names are limited to a maximum length of 63 characters.

Click on the *Import* button to import the license.
*The same file transfer dialog box is used for both HTTP and HTTPS.

Import Security Certificate to Switch:

HTTP/HTTPS Protocol	TFTP Protocol

File Transfer - Firmware/Config

If downgrading to firmware version 2.1.10 or older please contact technical support for guidance.

Protocol	HTTP ▾
Transfer Type	Import Security Certificate to switch ▾
Certificate File Name	Choose File No file chosen
Key File Name	Choose File No file chosen

Import Cancel

File Transfer - Firmware/Config

If downgrading to firmware version 2.1.10 or older please contact technical support for guidance.

Protocol	TFTP ▾
Transfer Type	Import Security Certificate to switch ▾
Server	192.168.2.180
Certificate File Name	cert.pem
Key File Name	key.pem

Import Cancel

Certificate File Name: Click on the Choose File button to browse to the desired location and select a certificate file (typically cert.pem). File names are limited to a maximum length of 63 characters.

Key File Name: Click on the Choose File button to browse to the desired location and select a key file (typically key.pem). File names are limited to a maximum length of 63 characters.

Server: This field displays the IP address of the TFTP server.

Certificate File Name: This field displays the name of the file to be imported (typically cert.pem). File names are limited to a maximum length of 63 characters.

Key File Name: This field displays the name of the file to be imported (typically key.pem). File names are limited to a maximum length of 63 characters.

Click on the *Import* button to import the Security Certificate.
*The same file transfer dialog box is used for both HTTP and HTTPS.
> **Note:** After successfully transferring a new Security Certificate to the switch, the switch must be rebooted.

Export Saved Configuration from Switch: Select Export Saved Configuration from switch in the Transfer Type field.

HTTP/HTTPS Protocol	TFTP Protocol

File Transfer - Firmware/Config

If downgrading to firmware version 2.1.10 or older please contact technical support for guidance.

| Protocol | HTTP ▾ |
| Transfer Type | Export Saved Configuration from switch ▾ |

Export Saved Configuration from switch

Click Configuration Settings to export the settings to your computer.

Cancel

File Transfer - Firmware/Config

If downgrading to firmware version 2.1.10 or older please contact technical support for guidance.

Protocol	TFTP ▾
Transfer Type	Export Saved Configuration from switch ▾
Server	192.168.2.180
File Name	NT24k_settings.xml

Export Cancel

Click on the *Configuration Settings* link to export the settings to your computer. This option allows administrators to back up their configurations to an offsite server in case a custom configuration must be reloaded at a later time.

A download dialog pop-up will appear, prompting the user to open or save the configuration file. The file is called *NT24k_settings.xml* per default.

Server: This field displays the IP address of the TFTP server.

File Name: This field displays the name of the file to be exported (typically NT24k_settings.xml). File names are limited to 63 characters maximum.

Click on the *Export* button to export the settings to the specified TFTP server.

Export Saved Port Security Authorization List from Switch: Select Export Saved Port Security Authorization List from switch in the Transfer Type field.

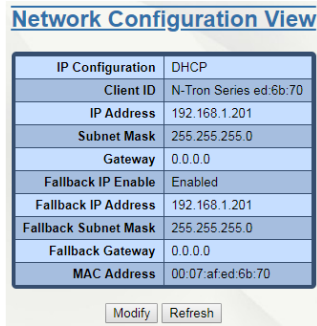| HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: HTTP Transfer Type: Export Saved Port Security Authorization List from switch Export Saved Port Security Authorization List from switch Click Port Security Authorization List to export the Port Security Authorization List to your computer. Cancel	File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: TFTP Transfer Type: Export Saved Port Security Authorization List from switch Server: 192.168.2.180 File Name: NT24k_portsecurity.auth Export Cancel
Click on the *Port Security Authorization List* link to export the authorization list to your computer. This option allows administrators to back up their Port Security Authorization List. A download dialog pop-up will appear, prompting the user to open or save the authorization file. The file is called *NT24k_portsecurity.auth* per default.	**Server:** This field displays the IP address of the TFTP server. **File Name:** This field displays the name of the file to be exported (typically NT24k_portsecurity.auth). File names are limited to 63 characters maximum. Click on the *Export* button to export the configuration file to the specified TFTP server.

Export Event Log from switch: The entire Event Log may be exported to the host PC for further analysis and archiving purposes. The log file lists all events that occurred while event logging was enabled and since the last Clear Log event was performed.

HTTP/HTTPS Protocol	TFTP Protocol
File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: HTTP Transfer Type: Export Event Log from switch Export Event Log from switch Click Event Log to export the Event Log to your computer. Cancel	File Transfer - Firmware/Config If downgrading to firmware version 2.1.10 or older please contact technical support for guidance. Protocol: TFTP Transfer Type: Export Event Log from switch Server: 192.168.2.180 File Name: eventlog.csv Export Cancel
Click on the *Event Log* link to export the log file to your computer. A download dialog pop-up will appear, prompting the user to open or save the configuration file.	**Server:** This field displays the IP address of the TFTP server. **File Name:** This field displays the name of the file to be imported (typically eventlog.csv). File names are limited to a maximum length of 63 characters. Click on the *Export* button to export the log file to the specified TFTP server.

Network

Setting the IP Configuration to DHCP will use the Primary Management VLAN ports to receive an IP address from the DHCP Server. Changes to the Primary Management VLAN are made in the VLAN section. If no changes are made, the default VLAN will be used as the default Primary Management VLAN.

Network Configuration View

IP Configuration	DHCP
Client ID	N-Tron Series ed:6b:70
IP Address	192.168.1.201
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Fallback IP Enable	Enabled
Fallback IP Address	192.168.1.201
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	0.0.0.0
MAC Address	00:07:af:ed:6b:70

Modify   Refresh

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) The DHCP option 61 client identifier will be sent with a preceding type-byte as listed below:

    MAC Address = 0x01
    Switch Name = 0x00 (Default)
    Other String = 0x00
    Other HEX = 0x00

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 Enable: Enables/disables the use of the Fallback IP address.

Fallback IP Address: Contains the configured Fallback IP address of the device. This address will be used if the switch fails to obtain a DHCP address from the DHCP Server. This option is only shown in DHCP Mode and if Fallback IP is enabled.
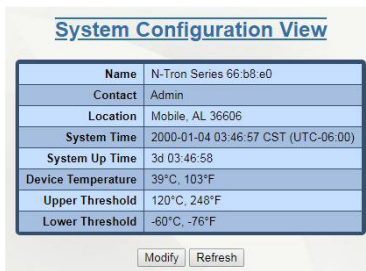
Fallback Subnet Mask: Contains the configured Fallback Subnet Mask of the device. This option is only shown in DHCP Mode and if Fallback IP is enabled.

Fallback Gateway: Contains the configured Fallback Gateway of the device. This option is only shown in DHCP Mode and if Fallback IP is enabled.

MAC Address: MAC Address of the device.

To modify any of the fields, click on Modify. Enter the desired system settings and click on the *Update* button.

REDLION®

System

System Configuration View

Name	N-Tron Series 66:b8:e0
Contact	Admin
Location	Mobile, AL 36606
System Time	2000-01-04 03:46:57 CST (UTC-06:00)
System Up Time	3d 03:46:58
Device Temperature	39°C, 103°F
Upper Threshold	120°C, 248°F
Lower Threshold	-60°C, -76°F

Modify   Refresh

The System page presents the user with current system information.

Name: Contains the name assigned to the device, which allows alphanumeric and special characters (,#_-:) only. When IP Configuration is DHCP, then this may be 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 (,#_-) are allowed.

Location: The physical location of the switch. Only alphanumeric and special characters (,#_-) are allowed.

System Time: Displays the date/time of the system. The system date/time defaults to 2000-01-01 00:00:00 CST (UTC-06:00) at system start.

System Up Time: Parameter represents the total time elapsed since the switch was turned on or rebooted.

Device Temperature: The device temperature reported by the on-board digital temperature sensor. This option is only shown on devices with temperature sensors.

Upper Threshold: The highest temperature for the switch without causing a fault to occur. The threshold is specified as an integer in degrees Celsius. The range is from -60 °C to 120 °C, and the default is product dependent. This option is only shown on devices with temperature sensors.

Lower Threshold: The lowest temperature for the switch without causing a fault to occur. The threshold is specified as an integer in Celsius degrees. The range is from -60 °C to 120 °C, and the default is product dependent. This option is only shown on devices with temperature sensors.

Power DC V1: The voltage measurement on power input DC V1. This option is only shown on devices with a voltage sensor.

Power DC V2: The voltage measurement on power input DC V2. This option is only shown on devices with a voltage sensor.

Total Current: The total input current measurement in Amps. This option is only shown on devices with a current sensor.

Total Power: The calculated power in Watts obtained from voltage and current measurements. This option is only shown on devices with a voltage and current sensor.

To make modifications to the fields above, click on the Modify button. Enter the desired settings and click on the *Update* button.

Bridging

Aging Time

The Aging menu item under the Bridging category displays the currently configured Aging Time. This configurable field shows the desired aging time for dynamically learned MAC addresses. Inactive MAC addresses will be removed from the Hardware Address Entry Table after the aging time period has expired. The internal aging time period will be between 1 and 2 times the selected aging time value.

Bridging Aging Time View

Aging Time   300

Modify   Refresh

To modify the Aging Time field, click on the Modify button. Enter the desired Aging Time (value must be between 10 - 630 seconds) and click on the *Update* button. The default value for this field is 300 seconds. To save the changes made, return to the Configuration menu and click on the *Save* button.

Multicast Addresses

The Multicast Addresses page displays a list of Multicast Group Addresses that are associated with respective port numbers.

Display Static Multicast Group Addresses

Static Multicast Group Address Filters

Multicast Address	Port List	VLAN ID

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

Add   Remove   Refresh

Adding a Multicast Group Address

To add a Multicast Address, click on the Add button and the following dialog window will appear:

Add Multicast Group Address Filter

Show All

Multicast Address 01:00:00:00:00:00

Port List □P1 □P2 □P3 □P4 □P5 □P6 □P7 □P8
□P9 □P10 □P11 □P12 □P13 □P14 □P15 □P16

Select All   Select None

VLAN ID 1

Update   Cancel

Enter a valid Multicast Group Address and VLAN ID, then select the port(s) to which matching packets will be directed.
Click on the *Update* button to return to the Display Static Multicast Group Addresses page.
To save the changes go to the Configuration menu and click on the *Save* button.

Removing a Multicast Group Address

To remove a Multicast Address, click on the *Remove* button. A listing of available Multicast Group Addresses will appear. Click on the *Delete* button to remove an address.

Unicast Addresses

The Unicast Addresses dialog window displays a list of MAC addresses that are associated with each respective port number. This can be used to statically assign a MAC address access to a single port on the switch.

Display Static Unicast MAC Addresses

Static Unicast MAC Address Filters		
MAC Address	Port	VLAN ID

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

Add   Remove   Refresh
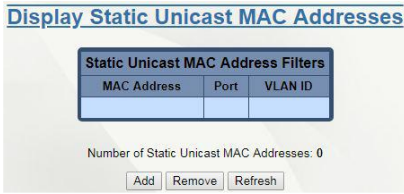
Adding a Unicast Address

To add a Unicast Address, click on the Add button and the following dialog window will appear:
Enter a valid MAC address and VLAN ID, then select the port to which matching packets will be directed.

Add Unicast MAC Address Filter

Show	All
Mac Address	00:00:00:00:00:01
Port	P1
VLAN ID	1

Update   Cancel
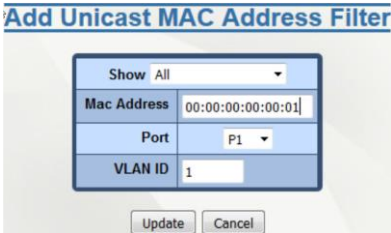
Click on the Update button to add the unicast address and return to the Display Static Unicast MAC Addresses dialog window.
To save the changes go to the Configuration menu and click on the *Save* button.

Removing a Unicast MAC Address

To remove a Unicast Address, click on the *Remove* button and a dialog window with a listing of available Unicast MAC Addresses will appear. Click on the *Delete* button to remove the MAC Address and return to the *Display Static Unicast MAC Addresses* dialog window.

CIP™

EtherNet/IP™, better known as the Common Industrial Protocol (CIP), was designed for use in process control and industrial automation applications. CIP was designed to provide consistent device access to eliminate the need for vendor specific software for configuration and monitoring of their devices.
N-Tron® switches with CIP support can be used to communicate with other industrial devices.
Note: Information about using CIP with the NT24k® can be found in the CIP User Manual & Installation Guide and the CIP Installation Kit for the NT24k switch family. This manual can be found on the Red Lion website.

Configuration

The CIP Configuration View dialog window displays the CIP status as well as the Multicast and Unicast RPIs (Requested Packet Interval).
Click on the *Modify* button to make changes to the CIP Configuration:

CIP Configuration View

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

Modify   Refresh
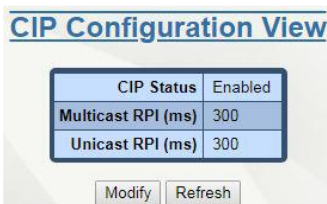
CIP Status: This field determines whether CIP is enabled or disabled on the NT24k switch. The default setting is Enabled.

Multicast RPI: The minimum Requested Packet Interval for Class 1 (multicast) connections in milliseconds is shown in this field. Requests for less than this value will be rejected. The default value for this option is 300 ms. The available range is 300 - 300,000.

Unicast RPI: This field shows the minimum Request Packet Interval for Class 3 (unicast) connections in milliseconds. Requests for less than this value will be rejected. The default value for this field is 300ms. The available range is 300 - 300,000.

Click on the *Update* button once the desired information is entered and to return to the *CIP Configuration View* dialog window. To save the changes made, return to the Configuration menu and click on the *Save* button.

Status

The Status menu item displays the CIP status. The switch status and partner status information will be shown.

Example CIP™ Status View showing a Connection Summary table with one Multicast connection:

Identity Information

Product Name: This field displays the Switch Model Number.

Vendor: This field shows N-Tron®'s ODVA Ethernet/IP™ Vendor ID (1006).

Device Type: This field displays that the ODVA device type is Communications Adapter (0x0C hex).

Major Revision: This field displays the major revision of the CIP implementation.

Minor Revision: This field shows the minor revision of the CIP implementation.

Serial Number (hex): This field shows the CIP serial number, which is unique across all N-Tron CIP devices. The number shown is the last 4 octets of the base switch MAC address.

Connection Information

Number of Multicast Connections: This field shows the current number of CIP Ethernet/IP class 1 (multicast) connections.

Number of Unicast Connections: This field displays the current number of CIP Ethernet/IP class 3 (unicast) connections.

Connection Summary

Transport Class: This field displays the Transport class for the connection, such as class 1 (multicast) or class 3 (unicast).

Connection State: This field indicates the state of the connection (established, timed out, closing or configuring).

RPI: The field displays the Requested Packet Interval in milliseconds.

Config Assembly: This field shows the configuration assembly number.

Output Assembly: This field displays the Output assembly number (the assembly that is sent out from the switch).

Input Assembly: This field displays the input assembly number (the assembly that is received into the switch).

Peer Address: This field shows the peer IP address of the device connected to the switch.

EIP Indicators

The module status indicator shows the current status of the switch. The network status indicator shows the status of the EtherNet/IP™ network interface. These indicators are located on the back of the rack mount version of the switch or on the front of the CPU module on the DIN-Rail versions of the switch.

Module Status

INDICATOR STATE	SUMMARY	DESCRIPTION
Steady Off	No power	The switch is not powered up.
Steady Green	Device operational	The switch is operating normally.
Flashing Green	Standby	The switch has not been configured for CIP™ operations.
Flashing Red	Minor fault	A recoverable minor fault has occurred.
Steady Red	Major fault	A non-recoverable major fault has occurred.

Network Status

INDICATOR STATE	SUMMARY	DESCRIPTION
Steady Off	Not powered, no IP address	The switch is not powered up, or an IP address has not been configured.
Flashing Green	No connections	An IP address is configured, but no connections have been established.
Steady Green	Connected	A connection has been established
Flashing Red	Connection timeout	A connection has timed out.

DHCP Client Configuration

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 Client is enabled by default, with 192.168.1.201 as the factory fallback address.

Refer to [Network](#) for enabling DHCP Client mode.

DHCP Relay Agent Configuration

A relay agent, configured via the Relay Agent Configuration View, provides a way for DHCP client requests to reach DHCP servers, including those that reside on a different subnet and/or VLAN.
Note: DHCP traffic is sent and received only on Management VLANs.

View Page

Click on the *Modify* button to open the DHCP Server Configuration Modification page.

Modify Page

Click on the *Update* button to apply the changes.

Relay Agent Status: Indicates whether the DHCP relay agent is active. The default is Disabled.

Relay Agent ID Format: The format selector with options for IP address, MAC address, Client ID, Other String, or Other Hex characters.

Relay Agent ID: A unique identifier that designates this relay agent switch.

RedLion®

DHCP Server 1-4 IP: The configured IP address of the DHCP servers.

Enable: Indicates whether relay agent functionality is enabled for the port.

Port No: The number of the port. This field is read-only.

Port Name: The descriptive name of the port. This field is read-only.

Circuit ID: When enabled, the Circuit ID for the port can be specified. By default, the Circuit ID is set to the MAC Address of the port. Circuit IDs must be unique for each port.

Circuit ID Format: The format selector with options for MAC, Hex, and String.

DHCP Server Configuration

The DHCP Server provides IP addresses to DHCP clients on the same subnet or VLAN. DHCP traffic is sent and received only on Management LANs.

> **Note:** A DHCP Relay Agent is required, to provide an IP address to clients on a different subnet or VLAN.

The following screen shows the Advanced configuration hidden:
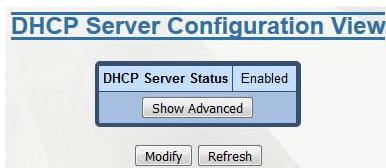
The following screen shows the Advanced configuration unhidden:
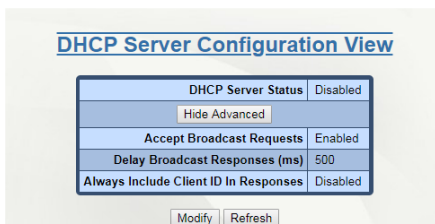
Click on the *Modify* button to open the DHCP Server Configuration Modification page.
Click on the *Update* button to apply the changes.
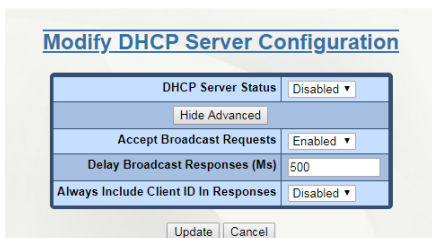
DHCP Server Status: Indicates whether the DHCP server is active. The default is Disabled.

Show/Hide Advanced: Button used to toggle whether or not to show advanced settings.

Accept Broadcast Requests: Indicates whether the DHCP server will process broadcast messages. Typically, client requests are broadcast and relay agent requests are unicast. When enabled, the server will respond to broadcast requests. When disabled, the server will ignore broadcast requests. The default is Enabled.

Delay Broadcast Responses (Ms): The amount of time (in milliseconds) that the DHCP server will delay the processing of a broadcast message. This setting is used when clients and relay agents are on the same subnet and/or VLAN. A delay provides the opportunity for relay agent requests to be honored before client requests. This setting only applies when Allow Broadcast is Enabled. The range is 0-2500 and the default is 500.

Always Include Client ID In Responses: Indicates whether the DHCP Server will always respond to the client with the Client ID in the frame. This should be disabled for a network that is non-compliant to the RFC- 6842(2013). The default is Disabled.

DHCP Server Scope Configuration

Scope Configuration Pools

The DHCP Server Scope Configuration contains vital network configuration options, called scope configuration pools, for potential clients. At least one scope configuration pool is necessary to create static assignments.

View Page

Modify Page

On the Modify page, the last column contains various buttons. The *Remove* button removes the corresponding scope configuration pool along with all static assignment and bindings associated with the pool. The *Add* button is used to add a new scope configuration pool.
Click on the *Add* button to add the new scope.
Click on the *Remove* button to remove an existing or new scope.
Click on the *Update* button to apply the changes.

Enabled: Indicates whether the pool is enabled or disabled.

Pool Name: Descriptive name of the scope configuration pool. This field is required and must be unique.

Pool Range: Starting and ending IP addresses for the pool of addresses.

Subnet Mask: The subnet mask for the IP address pool.

Gateway: The gateway IP address offered to the client. This field is optional.

Domain: The domain name offered to the client. This field is optional.

DNS: The DNS server IP addresses offered to the client. These fields are optional.

Lease Duration: The lease time (in days, hours and minutes) offered to the client. The range is 1 minute to 1000 days. The default is 28 days. If the Forever checkbox is checked, the lease does not expire.

DHCP Server Static Assignments

View Page

Select the Pool Name drop-down list to filter on a specified pool.
Click on the *Modify* button to open the Modify DHCP Server Static Assignments page.

Modify Page

Click on the IP address hyperlink to modify the corresponding static assignment.
Click on the *Add* button to add the new static assignment.
Click on the *Remove* button to remove an existing or new static assignment.
Click on the *Update* button to apply the changes.

Enabled: Indicates whether the pool is enabled or disabled. This field is read-only.

Pool Name: Descriptive name of the scope configuration pool. This field is read-only.

Pool Range: Starting and ending IP addresses of a pool of addresses. This field is read-only.

Subnet Mask: The subnet mask offered to the client. This field is read-only.

Gateway: The gateway IP address offered to the client. This field is read-only.

Domain: The domain name offered to the client. This field is read-only.

DNS: The DNS server IP addresses offered to the client. This field is read-only.

Lease Duration: The lease time (in days, hours and minutes) that will be offered to a client. This field is read-only.

Type: The type of binding identifier for the static assignment. The options are Option 61 and Relay Agent (Option 82).

IP Address: The static IP address offered to the DHCP client.

Binding Identifier: The binding identifier of the static IP address assignment. For Option 61, the binding identifier requires a Client ID, the identifier of the desired client. The identifier formats are MAC, HEX, and String. A type-byte is assumed to precede the identifier and does not have to be entered here. The type-byte value is assumed to be as follows:

> MAC = 0x01
> String = 0x00
> HEX = 0x00

For Option 82, the binding identifier requires a Remote Agent ID and Circuit ID. These identifiers must match the relay agent's Remote ID and Circuit ID. The identifier formats are IP (for a Remote ID), MAC, Hex, and String.

Label: The descriptive name of the static assignment. The field is optional.

DHCP Static Port Assignments

When a static port assignment is enabled on the port, the port will act as a DHCP server and provide a static IP address to the client connected to the port.
> **Note:** Only one DHCP client can be connected per port.

View Page

Select the Show drop-down list to show only enabled ports or all ports. Click on the port number hyperlink to modify the port's static port assignment.

Modify Page

Click on the *Update* button to apply the changes.

Enable: Indicates whether Static Port Assignment is enabled on the port.

Port No: The number of the port.

Port Name: The descriptive name of the port. This field is read-only.

RedLion®

IP Address: The IP address offer to the DHCP client connected to the port.

Subnet Mask: The subnet mask offer to the DHCP client connected to the port.

Gateway: The gateway offer to the DHCP client connected to the port.

Domain Name: The domain name offer to the DHCP client connected to the port. The field is optional.

DNS 1: The primary DNS offer to the DHCP client connected to the port. The field is optional.

DNS 2: The secondary DNS offer to the DHCP client connected to the port. The field is optional.

Label: The descriptive name of the DHCP client connected to the port. The field is optional.

DHCP Server Current Leases

The Current Leases table shows the IP addresses that have been leased, or offered, to devices.

DHCP Server Current Leases View

Pool Name	Binding Identifer ☐ Show Hex	MAC Address	IP Address	Status	Remaining Lease	Label	☐
Office	MAC = a0:36:9f:3b:6a:bf	a0:36:9f:3b:6a:bf	10.0.4.1	Static	2d 02:23	Office Printer	☐
Office	MAC = a0:36:9f:3b:6a:38	a0:36:9f:3b:6a:38	10.0.4.2	Dynamic	20d 04:43	PC	☐
Control1	MAC = a0:36:9f:6b:80:80	a0:36:9f:6b:80:80	10.0.4.90	Static	136d 23:11	Camera 1	☐
Control1	MAC = a0:36:9f:3a:e8:70	a0:36:9f:3a:e8:70	10.0.4.91	Static	6d 05:55	PLC 2	☐
Control2	MAC = a0:36:9f:7c:98:7b	a0:36:9f:7c:98:7b	10.0.4.15	Static	99d 12:02	PLC 3	☐

Refresh | Make Selected Static | Release Selected

Sort By: Sort the current leases by Pool Name, Binding Identifier, MAC Address, IP Address, Status, Remaining Lease, or Label.

Pool Name: The pool from which the lease was obtained.

Binding Identifier: The client associated with the lease entry. If Show Hex checkbox is checked, then detailed hex data about the Binding Identifier is displayed.

MAC Address: Indicates the MAC address of the client associated with the lease.

IP Address: Indicates the IP address assigned to the lease entry.

Status: Indicates the current status of the lease entry.
- Dynamic = Assigned dynamic IP.
- Static = Assigned static IP.

Remaining Lease: The client's remaining lease time.

Label: The descriptive name of the client.

Check Box: Click the individual checkbox to either make the clients static or release its lease.

   Note: Only clients with a dynamic lease can be made static.

Make Selected Static: Make the selected client dynamic IP address static.

Release Selected: Release selected client lease.

Event Notification

Event Notification is a combination of features that deal with filtering and routing system and fault events to different destinations.
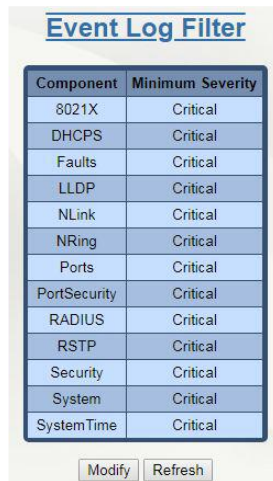
Event Log Filter

The Event Log Filter allows the user to define which events will be logged based on the severity level of the event.

> **Note:** The event log is enabled by default for critical events.

Event Log Filter View

The Event Log Filter page displays the current minimum severity settings for each component. Events below the minimum severity level will not be logged.
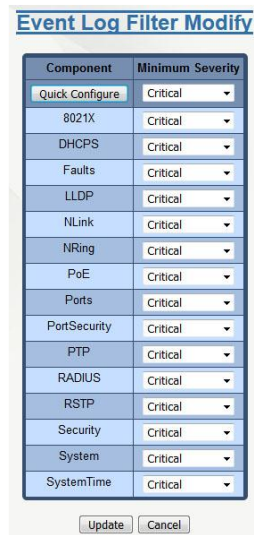
Click on the Modify button to make changes to the Event Log Filter.

Event Log Filter Modify

The Event Log Filter configuration can be changed by clicking on the Modify button.

Quick Configure: Use Quick Configure to change all components to the same severity level.

Component: The feature, protocol, or system service of the switch that generates events. The component list is model dependent.

Minimum Severity: Events below the minimum severity level will not be logged. A severity of None will disable events for that component. For more information, see Severity under the section Event Log.

Syslog

The Syslog feature allows certain system events (see Event Log) to be sent as messages to remote hosts for monitoring and analysis.

The messages can be sent to up to 5 different remote hosts, known as Syslog Collectors. A minimum severity level is associated with each Syslog Collector. Events below the minimum severity level will not be sent out from the switch. Syslog is disabled by default and can be enabled through the Web Browser interface.

Syslog Configuration View

The Syslog Configuration View is accessible under Event Notification within the Advanced section. Below is an example of the current configuration status of Syslog, the configuration of each Syslog Collector, and a list of the Syslog Collectors.

Syslog Configuration View

Syslog Status	Disabled
Facility	(16) - Local Use 0
Originator IP Address	172.16.20.135

Collectors

IP Address	UDP Port Number	Minimum Severity	Send Events
192.168.2.1	514	Debug	Yes

Modify   Refresh

Syslog Configuration Modify

The Syslog configuration may be changed by an admin level user by clicking on the Modify button. In this section the settings of each Syslog Collector can be updated and the Syslog Distributor itself can be disabled or enabled.

Syslog Configuration Modify

Syslog Status	Disabled ▼
Facility	(16) - Local Use 0 ▼

Collectors

IP Address	UDP Port Number	Minimum Severity	Send Events
192.168.2.1	514	Debug ▼	☑
0.0.0.0	514	Debug ▼	☐
0.0.0.0	514	Debug ▼	☐
0.0.0.0	514	Debug ▼	☐
0.0.0.0	514	Debug ▼	☐

Syslog Status: This field indicates whether the Syslog Distributor (client) has been enabled or disabled. To enable Syslog at least one Syslog Collector (server) must be specified.

Facility: This is used to identify which process is logging the message. This is a global setting for the switch and will be used for all messages. Available Facility values as defined per RFC-5424 are 1 (user level) and 16 - 23 (local use).

Originator IP Address: The field displays the configured IP address of the switch.

Collector: The Syslog server to which the messages are sent.

NT24k® Gigabit Ethernet Switches

IP Address: The IP address of the Collector (server) to receive a log message.

UDP Port Number: The UDP port on the Collector (server) to receive the message. The default port number is 514, per RFC-5424, but can be changed to meet installation requirements. Allowed port numbers are 1 - 65535.

Minimum Severity: The minimum Severity level of the messages that will be sent to the specified Collector (server). Values range from Debug (7) to Emergency (0). For example, a Collector configured with a value of Warning (4) will receive all messages from 4 to 0. The importance of a message increases with a lower severity level setting value. These are the same Severity level setting values as the Event Log and Event Log Filter. For more information, see Severity under the section Event Log.

Send Events: This setting can be enabled or disabled, per Collector, to control the distribution of Event Log messages.

IGMP

Configuration

The Configuration dialog window displays the IGMP basic configuration settings. If an active N-Ring™ participant, the ring ports are informatively shown as N-Ring router ports. On an N-Link Master, Slave or Coupler switch, the coupler port is shown as an N-Link router port.

> **Note:** Bypass Relay models affect the implementation of this protocol. For more information, see the section Bypass Relay (BR).

IGMP Configuration View

IGMP	
IGMP Status	Enabled
Query Mode	Auto
Router Mode	Auto
Remove Unused Groups	✓
Manual Router Ports	None
N-Ring Router Ports	None
N-Link Router Port	None
Active Querier IP	172.16.12.160

Modify Refresh

IGMP Configuration

IGMP	
Show	All
IGMP Status	Enabled ▾
Query Mode	Auto ▾
Router Mode	Auto ▾
Remove Unused Groups	✓
Manual Router Ports	☐A1 ☐A2 ☐A3 ☐A4 ☐A5 ☐A6 ☐A7 ☐A8 ☐B1 ☐B2 ☐B3 ☐B4 ☐B5 ☐B6 ☐B7 ☐B8 Select All Select None

Update Cancel

IGMP Status: This field indicates whether the IGMP is enabled or disabled. The default value for this field is *Enabled*.

Query Mode: The default value for this option is Auto. Available options are:

Auto: Multiple switches will ensure that only one switch is the active querier.
On: This switch is always an active querier.
Off: This switch never queries.

RedLion®

Router Mode: The available options for this field are:

Auto: This option allows for dynamically detected and manually set router ports. This is the default value.

None: This option allows for no router ports.

Manual: This option allows for manually set router ports.

Remove Unused Groups: If this option is checked, unused IGMP Groups will be removed and traffic with those multicast addresses will be treated as normal multicast. If this option is unchecked, unused IGMP Groups will remain and traffic with those multicast addresses will be limited. The default value for this field is checked.

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

Manual Router Ports: Manually specify the used ports.

N-Ring™ Router Ports: This field displays the N-Ring ports designated as active IGMP Router ports.

N-Link Router Port: This field indicates the N-Link ports that have been designated as active IGMP Router ports.

Active Querier IP: This field shows the IP address of the Active Querier.

Click on the *Modify* button to make changes to the IGMP Status, Query Mode, Router Mode and Manual Router Ports.

Groups

The Groups dialog window displays a list of IGMP groups based on the Group IP and the port that it is associated with.

Total Number of Active IP Group Memberships: The total number of active group IP memberships based on the dotted quad view (aaa.bbb.ccc.ddd) counting each joined port are displayed here.

Group IP: This field shows the dynamically created multicast group IP address.

Port Name: The descriptive name of the port is shown here.

VLAN ID: This field indicates the VLAN in which the Group IP is assigned. The available range is 1-4094.

RFilter Ports

From the RFilter (Router Multicast Data Filter) option, the user can choose whether or not data frames with known group multicast addresses are sent to the router ports. Control packets will be sent to the router(s) regardless of this setting.
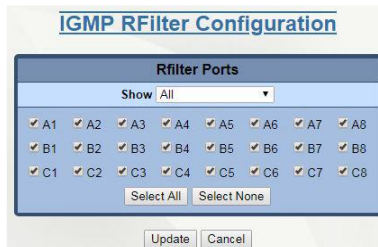
IGMP RFilter Configuration View

Rfilter Ports
All

Modify   Refresh

Known group multicast addresses are learned from dynamic IGMP Snooping operations. If IGMP is enabled and a port is a router port, then having RFilter enabled will stop IGMP group data from egressing on the port unless a join to that specific IGMP group has come into the port. IGMP controls (Join, Leave, Query) are still sent.

The Router Multicast Data Filter is enabled for all ports by default. Router ports do not get data frames with known multicast destination addresses unless a join for that specific multicast address has been received on that port. Join overrides an RFilter.

If RFilter is disabled, the router ports get data frames with known multicast destination addresses.
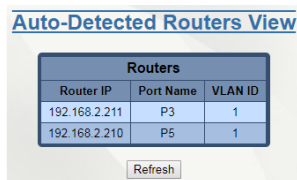
RFilter can be set for individual ports: any, all or none. For each port, RFilter will have an impact only if that port is manually or dynamically chosen as a router port.

Click on the *Modify* button to make changes to the IGMP RFilter Configuration. The following dialog window will appear:

IGMP RFilter Configuration

Rfilter Ports

Show All

✔ A1 ✔ A2 ✔ A3 ✔ A4 ✔ A5 ✔ A6 ✔ A7 ✔ A8
✔ B1 ✔ B2 ✔ B3 ✔ B4 ✔ B5 ✔ B6 ✔ B7 ✔ B8
✔ C1 ✔ C2 ✔ C3 ✔ C4 ✔ C5 ✔ C6 ✔ C7 ✔ C8

Select All   Select None

Update   Cancel

From this dialog window, the administrator selects which ports to identify as RFilter ports and can view all possible ports (Modules), currently installed ports or currently linked up ports. Click on the *Update* button when done with required changes. To save the changes made, return to the Configuration menu and click on the *Save* button.

Routers

Auto-Detected Routers View

Routers		
Router IP	Port Name	VLAN ID
192.168.2.211	P3	1
192.168.2.210	P5	1

Refresh

The Routers dialog window displays a list of the following:

Router IP: Auto-detected router IP address.
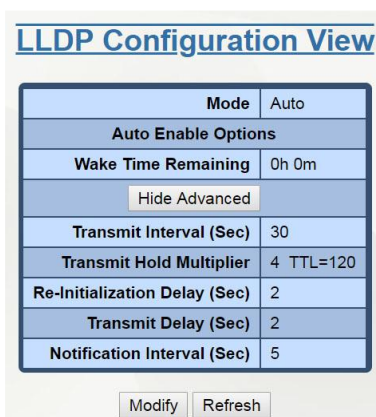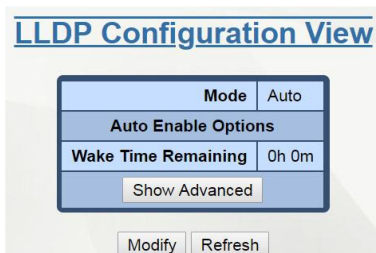
Port Name: The descriptive name of the port.

VLAN ID: VLAN in which the Router IP is assigned. The range is 1 - 4094.

RedLion®

LLDP

LLDP Configuration

The LLDP Configuration Page can be used to view or configure LLDP operation on the switch. The default mode for LLDP is Auto. Other configurable options are revealed by clicking on the "Show Advanced" button.

To enable LLDP on all switches that are in Auto mode, set the mode to Auto, set the Wake Time to a non-zero time, and click the "Send" button.

LLDP Configuration View

Mode	Auto
Auto Enable Options	
Wake Time Remaining	0h 0m
Show Advanced	

Modify   Refresh

LLDP Configuration View

Mode	Auto
Auto Enable Options	
Wake Time Remaining	0h 0m
Hide Advanced	
Transmit Interval (Sec)	30
Transmit Hold Multiplier	4 TTL=120
Re-Initialization Delay (Sec)	2
Transmit Delay (Sec)	2
Notification Interval (Sec)	5

Modify   Refresh

Mode: The LLDP mode can be Enabled, Disabled, or Auto. In Auto mode, LLDP is inactive until a switch sends a wake-up packet. The default is Auto.

Wake Time: The length of time LLDP will be active on switches that are in Auto mode. A value of 0 hours and 0 minutes will deactivate LLDP. Modify this value and click the "Send" button to set the wake time on all switches that are in Auto mode. The default is 0 hours and 0 minutes.

Show/Hide Advanced: Button used to toggle whether or not to show advanced settings.

Transmit Interval (Sec): The interval at which periodic LLDP frames are transmitted. The default is 30 seconds.

Transmit Hold Multiplier: A multiplier on the Transmit Interval when calculating a Time-to-Live value. The default is 4.

Re-Initialization Delay (Sec): The minimum time an LLDP port will wait before re-initializing after its setting has changed from disabled to Tx-Only or Tx/Rx. This prevents excessive notifications when LLDP Port settings are changed. The default is 2 seconds.

Transmit Delay (Sec): When LLDP information is changing on the switch, the time to wait before sending an LLDP frame with the updated information. The default is 2 seconds.

Notification Interval (Sec): The interval between notifications sent by the switch. If a port sends out a notification and another port tries to send out a notification, then the subsequent notification will not be sent until the interval expires. The default is 5 seconds.

LLDP Ports Configuration

The LLDP Ports Configuration Page displays and configures LLDP options for each port.

Show: View the ports that are available to install (Modules) currently installed or currently linked up.

Port No: The number of the port.

Mode: The port mode can be Tx Only, Rx Only, Tx/Rx, or Disabled. This configures whether or not LLDP frames are transmitted or received. The default is Tx/Rx.

Allow Management Data: Allows the transmission of management type information. Example: IP address of the switch. The default is checked.

Allow Notification: Allows an SNMP notification to be transmitted when local or remote data changes. The default is unchecked. Note: SNMP Notification Traps must be enabled under SNMP.

Port Description: Indicates whether or not to send the descriptive name of the port in the transmitted LLDP frame. The default is unchecked.

System Name: Indicates whether or not to send the name assigned to the device on the System page in the transmitted LLDP frame. The default is unchecked.

System Description: Indicates whether or not to send the switch model and current firmware version in the transmitted LLDP frame. The default is unchecked.

System Capabilities: Indicates whether or not to send the primary function(s) of the system in the transmitted LLDP frame. The default is unchecked.

VLAN PVID: Indicates whether or not to send the Port VLAN identifier (PVID) associated with the port in the transmitted LLDP frame. The default is unchecked.

VLAN Name: Indicates whether or not to send the VLAN IDs and Names associated with the port in the trans-mitted LLDP frame. The default is unchecked.

LLDP Ports Neighbors

The LLDP Ports Neighbors shows the results of LLDP discovery. The LLDP Ethernet frames received from neighboring ports are composed of collections of data units called Type Length Value (TLV). 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 six neighbors can be displayed per each port.

LLDP Ports Neighbors View

Port No	Port Name	Neighbor								
		MAC	Port ID	IP	Port Description	System Name	VLAN PVID	VLAN ID	VLAN Name	TTL
03	P3	00:07:af:e5:c1:e0	P1	192.168.2.211	P1	NetSwitch 1	2	2	vlan-2	106
05	P5	00:07:af:73:55:a0	P2	192.168.2.210	P2	NetSwitch 2	2	2	vlan-2	95

Port No: The port the neighbor information was received from.

MAC: MAC address of neighbor device. Corresponds to the LLDP Chassis ID TLV.

Port ID: Identifier of the neighbor port from which the LLDP frame was sent.

IP: IP address of neighbor device. Corresponds to the LLDP Management Address TLV.

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

System Name: The system's administratively assigned name on the neighbor device.

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

VLAN ID: A list of all VLAN IDs associated with the neighbor port.

VLAN Name: A list of all VLAN Names associated with the neighbor port.

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

LLDP Port Statistics

LLDP Port Statistics View

Show Currently Installed ▾

Port No	Port Name	Transmit Frames	Received Frames	Discarded Frames	Error Frames	Discarded TLVs	Unrecognized TLVs	Age Out
1	A1	0	0	0	0	0	0	0
2	A2	6	28	0	0	0	0	0
3	A3	6	0	0	0	0	0	0
4	A4	6	14	0	0	0	0	0
5	A5	6	14	0	0	0	0	0
6	A6	0	0	0	0	0	0	0
7	A7	0	0	0	0	0	0	0
8	A8	0	0	0	0	0	0	0

Refresh   Clear

Port No: The number of the port.

Port Name: The descriptive name of the port.

Transmit Frames: The total number of LLDP frames transmitted by 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 Type Length Values (TLVs) in the frames.

Errors Frames: Total count of all LLDP frames received with one or more errors.

Discarded TLVs: The count of all TLVs discarded for any reason.

Unrecognized TLVs: The count of all TLVs received on the port that are not recognized by LLDP.

Age Out: The count of times that a neighbor's information has been deleted because its Time To Live (TTL) has expired.
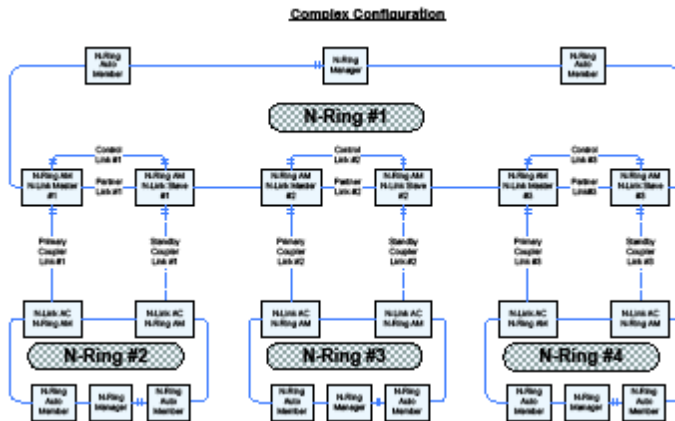
N-Link

   N-Link provides a way to 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.

   Note: Bypass Relay models affect the implementation of this protocol. For more information, see the section Bypass Relay (BR).

Example of a standard N-Link configuration

Example of a complex N-Link configuration

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 on the Master by selecting the N-Link Status View page.

Configuration Requirements:

• The Master and Slave must be part of the N-Ring topology.

- If using default configuration choices, the administrator only needs to configure the N-Link Master. The N-Link Slave and both Coupler switches will auto-detect any needed configuration.

- If not using default configuration choices, the administrator may also need to configure the Default Coupler port on the N-Link Slave.

- There must be a direct link between the Master and Slave Control ports. Use of media converters or other switches is not supported.

- There must be a direct link between the Master and Slave Partner ports. Use of media converters or other switches is not supported.

- There must be an N-Link aware switch on each side of the Master.

- 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.

- Control and Partner connections should be either fiber or 10/100Base-TX copper.

  The use of copper SFP transceivers for N-Link control and partner connections is not recommended due to the variances of link performance between SFP manufacturers.

  Per the IEEE 802.3 standard (Clause 40), a 1000Base-T PHY is required to wait 350-750 milliseconds before reporting a link down condition; and is therefore unsuitable for use as an N-Link control or partner connection.

- For optimal performance:

  The speed of the Partner segment must match the speed of the other N-Ring™ segments. Therefore, the Partner connection must be 1 gigabit fiber when the other N-Ring segments have a 1 gigabit speed.

 When using a 700/7000 Series N-Link Slave, the control port should use a fiber connection.

Configuration/Basic

The Basic tab under the N-Link Configuration category will display the basic configuration settings. By default, N-Link is in Auto-Configuration mode and will use A4 as the Default Coupler port.

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.

N-Link Basic Configuration View

N-Link Mode	Auto Configure
Default Coupler Port	A4

Modify   Refresh

Click on the *Modify* button to make changes. Click on the *Update* button to retain the changes. To save the changes made, return to the Configuration menu and click on the *Save* button.

N-Link Configuration

Show	All ▼
N-Link Mode	Auto Configure ▼
Default Coupler Port	A4 ▼

Update   Cancel
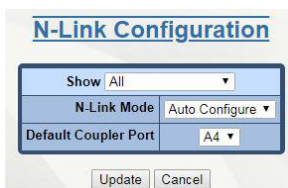
Show: View the ports that are available to install (Modules) currently installed or currently linked up.

N-Link Mode: Select the required N-Link mode from the drop-down list. The available options are:

Disabled: N-Link is disabled and will not operate as an N-Link capable switch.

Auto Configure: In this mode, the switch will automatically detect whether it is a slave or a coupler.

Master: If this option is selected, then the administrator must configure the Control Port (default: A3) and the Primary Coupler Port (default: A4).

Default Coupler Port: The Coupler Port is used to establish a redundant path for Ethernet data. If the role of the switch is Slave the port will be a Standby Coupler. The default is A4.

Click on the *Update* button to retain the changes. To save the changes made, return to the Configuration menu and click on the *Save* button.

Configuration/Advanced

The Advanced dialog window displays the advanced configuration settings. If N-Link is set to *Auto Configure*, the following configuration data will be used. The selected Auto Configure detection timeout value range is 2-180 seconds. The default Auto Configure detection time is 4 seconds.
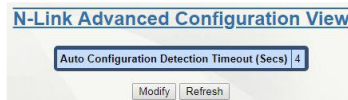
Click on the *Modify* button to change the detection timeout. Click on the *Update* button once the field has been updated with the required information. To save the changes made, return to the *Configuration* menu and click on the *Save* button.

Status

The Status dialog window displays 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.

N-Link Master or Slave

The following switch status and partner status information are shown.

State: This field displays the current N-Link mode of the switch.

Partner Port: This field shows the port being used for normal communication between the N-Link Master and N-Link Slave switches. 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 is displayed in this field.

Coupler Port State: Blocking, Forwarding.

Status: If there are no errors, the status shows OK. Otherwise, a description of the faults detected is shown.

N-Link Partner Information

The following switch statuses are shown.

State: Current N-Link mode of switch.

MAC: The MAC address of the N-Link Partner switch.

Coupler Port State: Blocking or Forwarding.

Status: If there are no errors, the status will show OK. Otherwise, a description of the faults detected will be shown.

N-Link Auto Configure

N-Link State: Current N-Link mode of switch.

Coupler State: The port used to establish a redundant path for Ethernet data transmission. This port will be detected automatically.

Status Examples

N-Link Auto Configure that is not an N-Link Master and has not become an N-Link Slave or an N-Link Coupler:

N-Link Coupler Switch:

N-Link Master Switch:

N-Link Slave Switch:

N-Link Status Master and Slave where the Primary Coupler is broken:

N-Link Master and Slave where the Standby Coupler link is broken:

N-Link Master and Slave where the Control link is broken:

N-Link Master and Slave where the Partner link is broken:

N-Ring™

Configuration/Basic

The Basic dialog window displays the N-Ring basic configuration settings. By default, N-Ring is in Auto Member mode.

> **Note:** Bypass Relay models affect the implementation of this protocol. For more information, see the section Bypass Relay (BR).

Click on the *Modify* button to make changes to the N-Ring Basic Configuration:

Modify N-Ring Mode Configuration

| N-Ring Mode | Auto Member ▼ |

Update Cancel

Disabled: If selected, this option disables the N-Ring capabilities on the switch.

Auto Member: When set to auto member, the switch automatically detects when it is a part of an N-Ring for participation in the ring.

Manager: When in Manager mode, the administrator may select different Port Sets as N-Ring ports. (See the Port Set Configuration section for information on adding and deleting port sets.)

> **N-Ring Ports:** Defines the two ports that are used to connect to the N-Ring.
> **N-Ring™ Number:** The N-Ring number can be selected from a range of 1 - 16 or a custom N-Ring number can also be chosen. The selected N-Ring number determines the VLAN ID. See table below for N-Ring numbers and corresponding VLAN IDs.
> **VLAN ID:** This field is auto-generated based on the selected N-Ring number. See table for N-Ring numbers and corresponding VLAN IDs.
> **Tagging:** The type of VLAN tagging used. Currently, tagged mode is the only supported mode.

Multi-Member: When in Multi-Member mode, a switch can be a member of multiple rings. If selected, then N-Ring Membership Configurations can be added for each N-Ring to which the switch will be connected. The image below shows one configured N-Ring.

Modify N-Ring Mode Configuration

| N-Ring Mode | Multi-Member ▼ |

Update Cancel

N-Ring Membership Configuration
None Configured
Add

Done Refresh
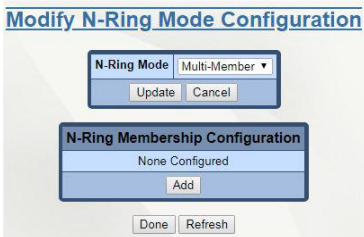
To delete an existing N-Ring Membership, click on the *Delete* button.

To add a new N-Ring Membership, click on the *Add* button. The screen below will appear.

N-Ring Membership Configuration

N-Ring Ports	A1 / A2 ▼
N-Ring Number	1 ▼
VLAN ID	3333
Tagging	Tagged ▼

Update Cancel

Select the N-Ring Ports and N-Ring Number to be used for the N-Ring. The VLAN ID for each N-Ring Membership must match that of the N-Ring Manager on each specific N-Ring to which the N-Ring Multi- Member will be connected.

Click on the *Update* button once the required selection has been made. To save the changes made, return to the *Configuration* menu and click on the *Save* button.

List of available N-Ring Numbers and their corresponding VLAN ID:

N-RING NUMBER	VLAN ID	N-RING NUMER	VLAN ID
1	3333	9	3341
2	3334	10	3342

3	3335	11	3343
4	3336	12	3344
5	3337	13	3345
6	3338	14	3346
7	3339	15	3347
8	3340	16	3348

Configuration Requirements:
1. N-Ring requires tagged frames to optimize frame prioritization.
2. Do not create redundant links unless either RSTP or N-Ring is enabled.
3. The Default VLAN and any active N-Ring VLAN cannot be deleted.
4. RSTP and N-Ring™ are different modes and cannot share links or segments. If a port is both an RSTP port and an active N-Ring port, then RSTP will be disabled for that port. Other ports may have RSTP enabled.
5. Do not connect the N-Ring to actively Trunking ports on an Auto Member or Multi-Member configured switch.
6. An NT24k® switch can only participate in one N-Ring unless in Multi-Member mode.
7. Since VLANs are implemented for security reasons as well as traffic flow, N-Ring only makes minimal VLAN changes. It is up to the administrator to ensure that VLANs are configured correctly on the N-Ring manager and all N-Ring members.
8. For optimal performance, all N-Ring segments must be configured for the same speed.

> **WARNING:** To prevent a network storm, multiple segments between N-Ring members on one or more N-Rings must not occur. N-Ring members should only be connected to each other by the N-Ring ports.

Configuration/Port Sets

A port set is a group of two ports that may be used for an N-Ring. The default N-Ring Port Set is A1/A2. Click on the *Modify* button to make changes to the Port Sets.

Set: This field displays the Port set table index.

Ports: This field indicates the designated pair of N-Ring ports. To reassign different pairs, the Port sets containing those ports, if any, must be deleted before the ports can be reassigned (a port can only belong to one port set).

Delete: To delete a port set, check the box next to the line item to be deleted and click on the *Delete* button.

Click on the *Add* button below the Set column.

N-Ring Ports: A new port set can be added by selecting the N-Ring ports from the N-Ring Ports pull-down lists and clicking on the *Add* button.

Port Sets: Port Sets can be removed by selecting the port set from the Port Sets pull-down and pressing the *Remove* button.

Click on the *Update* button when port set configuration is complete. The N-Ring Port Sets Entry dialog window will appear. Click on the *Done* button. To save the changes made, return to the *Configuration* menu and click on the *Save* button.

Configuration/Advanced

Auto Member Mode

N-Ring Advanced Configuration View

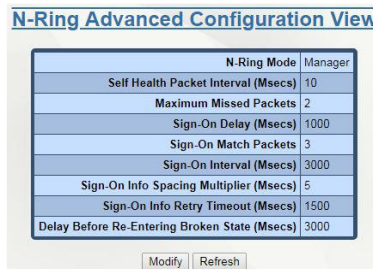|	
N-Ring Mode	Auto Member
Keep-Alive Timeout (Secs)	31
Auto Member Detection Timeout (Secs)	4

Modify   Refresh

N-Ring™ Mode: This field is defined in the N-Ring/Configuration/Basic dialog window.

Keep-Alive Timeout (Sec): This field displays the amount of time to wait (in seconds) to receive a keep-alive request before switching from active member back to auto member. The default value is 31 seconds and the available range is 15 to 300 seconds. A entry of 0 will disable the feature.

Auto Member Detection Timeout (Sec): This field shows the amount of time to wait in seconds to receive N-Ring frames on any auto member port (at boot up) before assuming the switch is not part of an N-Ring. The default value is 4 seconds and the available range is 2 to 180 seconds.

Click on the *Modify* button and enter the required changes. When entries are complete, click on the *Update* button. To save the changes, return to the *Configuration* menu and click on the *Save* button.

Manager Mode

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

When in Manager mode, the following advanced configuration data are displayed in their respective fields:

Self Health Packet Interval (Msecs): The amount of time to wait in milliseconds before sending Self-Health packets. The default value for this field is 10.

Maximum Missed Packets: The number of consecutive missed Self-Health packets that constitute a fault. The default value for this field is 2 packets.

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

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

Sign-On Interval (Msecs): The interval of time to wait in milliseconds before requesting subsequent sign-on information from ring members when the ring is broken. The default value for this field is 3000 Msecs.

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

Sign-On Info Retry Timeout (Msecs): 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 resend the information. The default value for this field is 1500 Msecs.

Delay Before Re-entering Broken State (Msecs): 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 Msecs.

Click on the *Modify* button and make the required changes. Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Multi-Member mode

There are no advanced options when operating in Multi-Member mode.

Configuration Status

When an N-Ring™ Auto Member is not participating in an N-Ring, the following information is shown:

When an N-Ring Auto Member is participating in an N-Ring, the following information is shown:
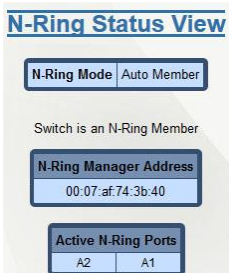
When N-Ring is in Manager Mode, the following data will be as shown below.

If the MAC is selected, more data is retrieved and shown about the N-Ring Member switch.
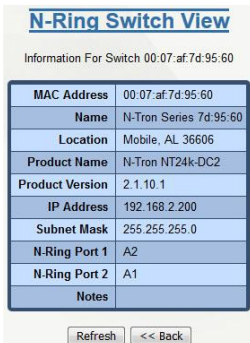
N-Ring™ Manager View for a faulted N-Ring:
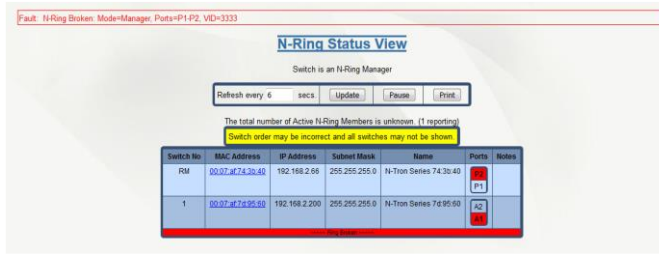
A fault warning *Fault: N-Ring Fault* in red will show at the top of the dialog window.

The break is identified in red. In this case, N-Ring manager A2 to N-Ring active member Switch Number 1 TX2 is broken. A warning *Switch order may be incorrect and all switches may not be shown* is displayed in yellow. This indicates that the Sign On frames cannot get around the N-Ring and the data may not have been updated since the last successful update.

N-Ring Multi-Member Status View

N-Ring Number: N-Ring number to which the N-Ring Membership is associated.

N-Ring Manager Address: Show the MAC address of the switch acting as the N-Ring Manager.

N-Ring Ports: The port set linked to this N-Ring.

VLAN ID: The VLAN ID tag to be used with this N-Ring. The VLAN ID is associated with the N-Ring, and can be changed by switching the N-Ring number.

Status: Current status of the N-Ring Membership. The values are:

Active: The N-Ring Membership is connected and operating normally.
Inactive: The N-Ring Membership is not responding and not functioning correctly.

N-View™

The N-View Configuration dialog window displays the basic configuration for N-View. The status (enabled or disabled) and the interval between packets.
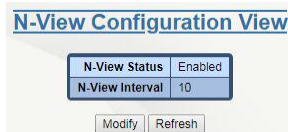
Click on the *Modify* button to make changes to the N-View Configuration.

Red**Lion**®
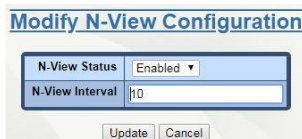
N-View™ Status: This field determines whether the N-Ring™ is enabled or disabled.

N-View Interval: This field determines the frequency in which N-View reports its information. Increasing the interval slows the update rate and decreasing it allows N-View to report more frequently. The available range is 10-500 seconds. Interval values are converted to increments of 10 seconds. The default value is 10 seconds.

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Ports

The Ports dialog window displays a list of the configured ports on the NT24k® unit, along with the ports transmitting N-View related multicast packets and MIB stats respectively.
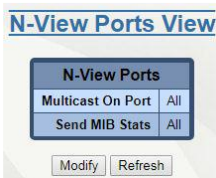
Click on the *Modify* button to make changes to the N-View Ports.
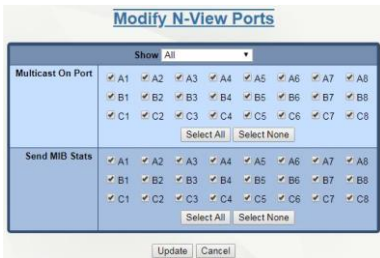
The user can modify these two variables to enable or disable N-View related multicast out of the port and if MIB stats are sent out for those ports. The ports that can be installed (Modules), currently installed or currently linked up can also be viewed.

Click on the *Update* button after required changes have been made. To save the settings, navigate to the *Configuration* menu and click on the *Save* button.

Ports

Configuration

The Ports Configuration dialog window shows a detailed overview of all the ports on the switch. The administrator can view the ports that are available to install (Modules), currently installed or currently linked up.

The information displayed on the page can be changed by changing the *Display Info* from *Basic* to *All*. *Basic* shows the most commonly used information while *All* shows all of the available information.

The screen above represents the Port Configuration View for a PoE model. If not using a PoE model, the page will be similar except the PoE Status column will not be present.

Port No: This field indicates the port number.

Port Name: This field displays the descriptive name of the port.

Port Description: This column provides a brief description of the port. Ports with "-R" in their description are Bypass Relay capable ports. Refer to the section Bypass Relay (BR) for more information on Bypass Relay devices and ports.

User Description: Description of the port set by a user.

Admin Status: This configurable field displays the existing status of the port. The two options are *Enabled* or *Disabled*.

Link Status: Shows the current state of the port. The two options are *Up* or *Down*.

Auto Nego: This configurable field displays the current auto-negotiation state whether it is *Enabled* or *Disabled*. Auto-negotiation cannot be disabled on a port connected to a gigabit device.

Port Speed: This configurable field displays the speed of each port. The available values are 10/100/1000 Mbps.

Duplex Mode: The existing mode of the port, whether it is *Full Duplex* or *Half Duplex*, is shown in this configurable field.

Flow Control: This configurable field displays the existing flow control status of each port.

Cross Over: This configurable field displays the existing crossover mode of the port. This can be indicated with a *Yes*, *No* or *Auto*. The default value for this field is Auto.

Role: A comma separated list of all the active roles for the port, which are based on the switch configuration. The possible roles are RSTP, N-Ring™, N-Link Control, N-Link Partner, and N-Link Coupler. For example, if a port is actively participating in an N-Ring and as an N-Link Partner, the role would be: N-Ring, N-Link Partner.

Port State: This column displays the current RSTP status of a port. It may contain *Disable*, *Discarding*, *Learning* or *Forwarding*.

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

Trunk ID: When the port is an active member of a trunk group, the trunk's ID value is shown. A zero value indicates that the port is not an active trunk member.

Usage Alarm Low [%]: This field indicates the bandwidth utilization percentage below which a fault is triggered if enabled. For the half-duplex option, the bandwidth utilization percentage is the sum of both RX and TX bandwidth utilization. For the full-duplex option, this is the higher of TX or RX bandwidth utilization.

Usage Alarm High [%]: This field displays the bandwidth utilization percentage above which a fault is triggered if enabled. For half duplex the bandwidth utilization percentage is the sum of both RX and TX band-width utilization, and for full duplex this is the lower of TX or RX bandwidth utilization.

PoE Status: The current status of the PoE will be displayed in this column. It may show *Inactive*, *Active*, *Disabled* or *N/A*.

Click on the *Port Number* to configure each port individually. This will allow the user to change the port's settings.

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Mirroring

A Mirroring Port is a dedicated port that is configured to receive copies of Ethernet frames that are sent or received from a monitored port. The Mirroring dialog window displays the status including the list of Source Ports and the Destination Port that the Sources are being mirrored to.

Click on the *Modify* button to make changes to the *Port Mirroring Configuration*.

Mirror Status: Enable or Disable the Mirroring functionality by selecting the option in the drop-down menu.

Drawing No. LP0991   Chapter 3 Web Software Configuration

Revision H   Ports

Destination Port: Select the destination ports that the source ports will be mirrored to.

Mirrored Data Only: Select the mirrored data to be transmitted to the destination port.

Tx Source Ports: Select the transmitting ports to be mirrored by checking on the desired ports or the *Select All* button.

Rx Source Ports: Select the receiving ports to be mirrored by checking on the desired ports or the *Select All* button.

Configuration Notes:
1. Non-mirrored frames take priority over mirrored frames. Mirrored frames may be discarded under rare instances when resource contention occurs.
2. The mirroring destination port is not allowed to overlap with the following features. Care should be taken to avoid configuration conflicts: N-Ring™, N-Link, Trunking.

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

PoE

PoE (Power Over Ethernet) is an internal hardware capability that outputs power and data on Ethernet cabling to Powered Devices (PDs) such as VoIP phones, IP camera, and industrial devices. PoE eliminates the need to run separate data and power cables between the PSE (PoE Source Equipment) and the PoE powered device.

PoE Management on the NT24k® provides the ability to set the PoE power budget, enable/disable PoE on specific ports, and set power limits per port.

    Note: PoE is only supported on certain NT24k switches.

PoE Configuration: Table 1

PoE Status: This configurable field indicates whether the global PoE is enabled or disabled. PoE ports must also be individually enabled on the PoE configuration page. The default value for this field is Enabled.

Safeguard Active PDs: This configurable field indicates whether an active PD is safeguarded from losing power because of a configuration change. If enabled, the Max Power Limit cannot be changed if it can cause a power loss to the active PD. Similarly, Legacy PD Detection cannot be disabled on an active legacy powered device. The default value for this field is Enabled.

Max Power Budget (Watts): The maximum amount of power available for PoE. The value can range from 4 to the max power supply support for the switch.

Quick Configure: The quick configure selection menu updates the PoE port table with the desired settings based on the quick configuration option selected.The following values for 8 PoE Ports are:

- P1-P8 at 30W (Class 4) (default)
- P1-P8 at 15.4W (Class 3/0)
- P1-P8 at 7W (Class 2)
- P1-P8 at 4W (Class 1)
- All ports disabled.

For 16 PoE Ports the values are:

- P1-P8 at 30W (Class 4) (default)
- P9-P16 at 30W (Class 4)
- P1-P16 at 15.4W (Class 3/0)
- P1-P16 at 7W (Class 2)
- P1-P16 at 4W (Class 1)
- All ports disabled.

PoE Configuration: Table 2

PoE Port Status: This configurable field indicates whether PoE is enabled or disabled on the port.The default value is enabled on the first 8 PoE ports.

Max Power Limit: This configurable field indicates the maximum budgeted power for the port. The values are:

- 4W (Class 1)
- 7W (Class 2)
- 15.4W (Class 3/0)
- 30W (Class 4)

Legacy PD Detection: This field indicates whether legacy PD detection is enabled or disabled on the port. If enabled, legacy powered devices will be recognized. The default value is disabled.

> **Note:** The sum of the Port Max Power Limit should not exceed the MaxBudgeted Power.

PoE Status: Table 3

Port Name: This field displays the descriptive name of the port.

PoE Port Status: Current status of the PoE port. The values are:

- Active: PoE power is outputted on the specific port
- Inactive: PoE power is not outputted on the specific port
- Disabled: PoE functionality is disabled on the specific port

Max Power Limit: The maximum budgeted power for the port.

Power Consumption: The actual power consumption of the port.

Detected PD Class: The classification of the connected device, which can range from Class 0-4.

Information: Details about the port's current state. If a Powered Device attempts to negotiate more power than the allocated maximum, PoE will be turned off on the port and a re-negotiation period will start. If re-negotiation is unsuccessful, a Retry button will be displayed below the PD error message. Select the retry button to restart negotiation after the cause of the overload is resolved.

QOS (Quality of Service)

The QOS decision tree chooses a frame's output port priority and the egress frame's IEEE 802.1p User Priority value (if needed) based on the QOS settings and the User Priority value (if any) in the ingress frame. Both the internal port priority setting and the egress frame User Priority value are always assigned the same value. The available values are 0 through 7 where 7 is the highest priority. If the ingress frame is an IP packet, the RFC 2474 DSCP field in the packet will be passed unchanged to the egress frame.

Click on the *Modify* button to make changes to the QOS Configuration.

QOS Configuration View

Port No	Port Name	Include DSCP	Include 802.1p	Default Priority
1	A1	Enabled	Enabled	1
2	A2	Enabled	Enabled	1
3	A3	Enabled	Enabled	1
4	A4	Enabled	Enabled	1
5	A5	Enabled	Enabled	1
6	A6	Enabled	Enabled	1
7	A7	Enabled	Enabled	1
8	A8	Enabled	Enabled	1
9	B1	Enabled	Enabled	1
10	B2	Enabled	Enabled	1
11	B3	Enabled	Enabled	1
12	B4	Enabled	Enabled	1
13	B5	Enabled	Enabled	1
14	B6	Enabled	Enabled	1
15	B7	Enabled	Enabled	1
16	B8	Enabled	Enabled	1
17	C1	Enabled	Enabled	1
18	C2	Enabled	Enabled	1
19	C3	Enabled	Enabled	1
20	C4	Enabled	Enabled	1
21	C5	Enabled	Enabled	1
22	C6	Enabled	Enabled	1
23	C7	Enabled	Enabled	1
24	C8	Enabled	Enabled	1

Modify   Refresh

Include DSCP: This configurable field displays the status of whether or not to include the ingress frame's RFC 2474 DSCP value in determining the transmit priority and egress frame's IEEE 802.1p User Priority value. If the ingress frame type is IP (IPv4 or IPv6) and Include DSCP is enabled, DSCP processing will override all other settings. (see QOS SELECTION CHART below). The default value is enabled.

Include 802.1p: This configurable field displays the status of whether or not to include the ingress frame's IEEE 802.1p User Priority value in determining the transmit priority and egress frame's IEEE 802.1p User Priority value. This setting is used only if the frame type is not IP (IPv4 or IPv6) or the Include DSCP setting is disabled. (see QOS SELECTION CHART below). The default value is enabled.

Default Priority: This configurable field displays the default QOS priority for the transmit priority value and the egress frame's IEEE 802.1p User Priority value if not otherwise assigned by DSCP or IEEE 802.1p processing. The range is 0-7, highest priority=7. The default value is 1.

QOS Selection Chart:

INCLUDE DSCP SETTING	INCLUDE 802.1p SETTING	INGRESS FRAME TYPE	INGRESS FRAME HAS VLAN	OUTPUT PORT PRIORITY AND EGRESS IEEE 802.1p USER PRIORITY
Enabled	N.A.	IP	N.A.	Ingress DSCP Value
N.A.	Enabled	Not IP	Yes	Ingress IEEE 802.1p UP
N.A.	Enabled	Not IP	No	Default Priority Setting
N.A.	Disabled	Not IP	N.A.	Default Priority Setting
Disabled	Enabled	N.A.	Yes	Ingress IEEE 802.1p UP
Disabled	Enabled	N.A.	No	Default Priority Setting
Disabled	Disabled	N.A.	N.A.	Default Priority Setting
Legend				
IP	Ingress packet type is IPv4 or IPv6.			
Ingress DSCP Value	Use the high order three bits of the ingress frame's IP DSCP value.			

INCLUDE DSCP SETTING	INCLUDE 802.1p SETTING	INGRESS FRAME TYPE	INGRESS FRAME HAS VLAN	OUTPUT PORT PRIORITY AND EGRESS IEEE 802.1p USER PRIORITY
Ingress IEEE 802.1p UP	Use the ingress packet's IEEE 802.1p User Priority value.			
N.A.	Not applicable			

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Rate Limiting

The Rate Limiting dialog window shows the NT24k® installed ports and the Pass Rate Percentage per port for each of the following: Broadcast, Multicast, Unknown Unicast and Known Unicast.

A packet type will be affected by the rate limit setting if the check box is selected and it exceeds the total number of packets established by the ingress rate limit within an assigned time period. The time periods are: 1 Gbps = 10 ms, 100 Mbps = 100 ms and 10 Mbps = 1 sec.

Click on the *Modify* button to make changes to the Rate Limiting settings.

Show: View the ports that are available to install (Modules), currently installed or currently linked up.

Pass Rate [%]: Modify the pass rate percentage for each and every port by entering the desired value.

Packet Types: Select what Packet Types are to be passed: Broadcast, Multicast, Unknown Unicast and Known Unicast.

Port Name: Select which ports are affected by the changes made.

Note: Unicast packets with destinations not in the ARL table can be rate limited rather than all being flooded. This is known as "Unknown Unicast".

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Status/Statistics

This dialog window displays the MIB counters for the selected port, specified by the Port pull-down menu.

Port Statistics

Port A1 ▾

Statistics For Port A1

Normal Statistic	Rx Value	Tx Value	Error Statistic	Value
Octets	416298571	190095124	Rx Drop Pkts	0
Broadcast Pkts	770482	6	Rx Undersize Pkts	0
Broadcast Rate Fps	2	0	Rx Oversize Pkts	0
Multicast Pkts	1514171	969481	Rx Jabbers	0
Multicast Rate Fps	5	5	Rx Alignment Errors	0
Unicast Pkts	23121	9233	Rx Bad Octets	0
Unicast Rate Fps	0	0	Rx SA Changes	0
Pause Pkts	0	0	Rx Fcs Errors	0
Good Octets	416298571	N/A	Rx Fragments	0
Pkts 64 Octets	638059		Rx Excessive Discard	0
Pkts 65 to 127 Octets	500980		Rx Symbol Error	0
Pkts 128 to 255 Octets	2035375		Tx Drop Pkts	0
Pkts 256 to 511 Octets	81075		Tx Collisions	0
Pkts 512 to 1023 Octets	26880		Tx Single Collision	0
Pkts 1024 to 10240 Octets	4125		Tx Multiple Collision	0
			Tx Deferred Transmit	0
			Tx Late Collision	0
			Tx Excessive Collision	0
			Tx Frame In Discard	0

Refresh   Clear   Clear All Ports

Pressing the *Clear* button resets all counters for the selected port. The *Clear All Ports* button resets all counters for all ports, including the selected port. The *Refresh* button reloads the dialog window.

Status/Utilization

This dialog window displays the bandwidth percentage graph of all the ports. The graph is scaled based on the "*Scale*" drop-down list.

Port Utilization

Scale 100 ▾
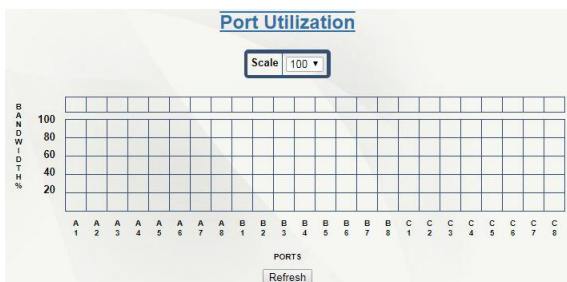
Trunking

The Trunking dialog window displays trunking information.

Note: Bypass Relay models affect this feature. For more information, see the section Bypass Relay (BR).

Port Trunking Configuration View

Trunk ID: This column displays the trunk identifier number. The valid range is 1-127.

Trunk Name: This column shows the descriptive name of the trunk. The name can consist of alphanumeric characters and the following special characters (including the period): **# _ - .**

Trunk Ports: This column displays the ports associated with the trunk.

Trunk Status: The existing status of the trunk is shown in this column. Available trunk status options are *Enabled* or *Disabled*.

Configuration Note:
> **Note:** The trunk ports are not allowed to overlap with the following features. Care should be taken to avoid configuration conflicts: N-Ring™, N-Link, 802.1X, Mirroring.

Click on the *Modify* button to add, modify or delete ports.
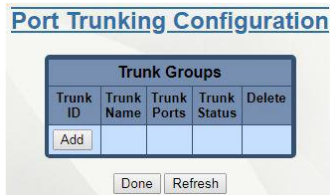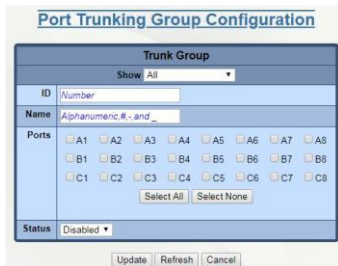
Port Trunking Configuration

Click on the Add button and the following dialog window will appear:

Port Trunking Group Configuration

Show: View the ports that are available to install (Modules) currently installed or currently linked up.

ID: Enter the desired Trunk ID. Valid range is 1- 127. There can be no duplicate Trunk IDs.

Name: Enter the descriptive name of the trunk. The name can consist of alphanumeric characters and the following special characters (including the period): **# _ - .**

Ports: Select the required ports from the Ports list. The list of ports shown will vary depending on the selection in the *Show* field.

Status: Select the status of the port that is being added. Options are *Enabled* or *Disabled*.

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

To modify an existing Trunk Group, click on the *Trunk ID* and make the required changes. To Delete an existing Trunk Group, click on the *Delete* button associated with the Trunk ID to be deleted.

RedL**ion**®

PPP

The console can be either in CLI mode or PPP mode. The PPP mode provides a TCP/IP connection over the serial port. A browser may then be used to view switch information or make configuration changes. PPP mode is entered by using the PPP command on the console. To change from PPP to CLI mode, you must reboot the switch.

PPP Status View

Console Mode	CLI
PPP Link Status	Down
PPP Switch IP Address	172.17.2.1
PPP PC IP Address	172.17.2.2

Refresh
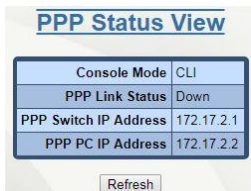
Console Mode: When CLI is shown, the console is in the command mode, which is the default mode. When PPP is shown, the console is in PPP mode.

PPP Link Status: This field indicates the current PPP link state.

PPP Switch IP Address: This field displays the IP address for the switch side of the PPP link.

PPP PC IP Address: This field indicates the IP address for the PC side of the PPP link.

RSTP

Bridge

The Bridge dialog window displays the RSTP information for the RSTP Root Bridge and for the RSTP Bridge on this switch.

> **Note:** Bypass Relay models affect the implementation of this protocol. For more information, see the section Bypass Relay (BR).
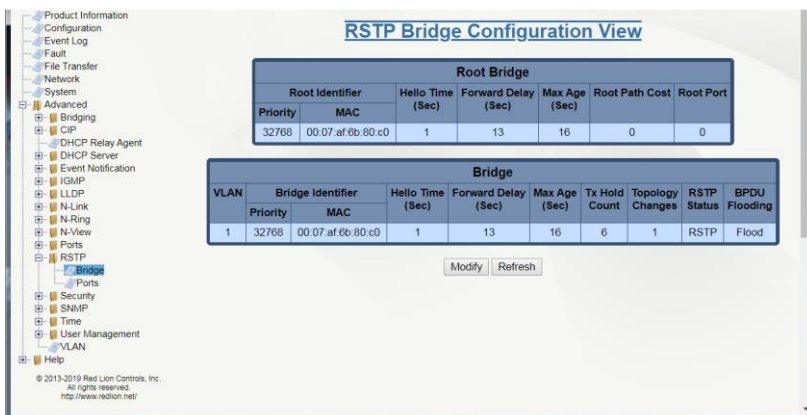
Root Bridge: This is the identity and parameters of the RSTP Root Bridge.

> **Root Identifier - Priority:** This field indicates the priority of the Root Bridge.
> **Root Identifier - MAC:** The unique MAC address of the Root Bridge is shown here.
> **Hello Time (Sec):** This field indicates the time interval, in seconds, between the transmission of configuration BPDUs by designated ports.
> **Forward Delay (Sec):** This field shows the time spent, in seconds, by legacy STP Bridges in transitioning Root and designated ports to forwarding. This delays port transitions until other bridges have received spanning tree information.

Max Age (Sec): For RSTP, this is the maximum time, in seconds, that a bridge will wait for
   configuration BPDUs before deciding it is no longer connected to the root bridge.
Root Path Cost: The cost of the path to the Root Bridge via the Root Port of this bridge.
Root Port: The Root Port of this Bridge. The Root Port provides the lowest cost path from this
   bridge to the Root Bridge.

Bridge: This is the configuration of the RSTP bridge on this switch.

VLAN: RSTP will operate on all ports of this VLAN. BPDUs will be transmitted with or without
   VLAN tags depending on the settings for this VLAN. This should be a valid VLAN ID. The default
   value for this field is VLAN 1.
Bridge Identifier Priority: This field indicates the Bridge priority. The range is 0 - 61440. The
   default value is 32768.
Bridge Identifier MAC: The unique MAC address of the Bridge is displayed in this field. This is
   possibly a different network device.
Hello Time (Sec): This field indicates the Hello time, when this bridge is the Root Bridge or is
   attempting to become the Root Bridge. This is the time interval, in seconds, between the
   transmission of Configuration BPDUs by Designated Ports. The range is 1 - 10. The default
   value is 1.
Forward Delay (Sec): This field displays the Forward Delay, when this bridge is the Root Bridge or
   is attempting to become the Root Bridge. This is the time spent, in seconds, by legacy STP
   Bridges in transitioning Root and Designated Ports to Forwarding. This delays Port transitions
   until other bridges have received spanning tree information. The range is 4 - 30. The default
   value is 13 seconds.
Max Age (Sec): This field displays the Max Age when this bridge is the Root Bridge or is attempting
   to become the Root Bridge. For RSTP, this is the maximum hops allowed for any protocol
   message before it is discarded and no longer retransmitted. For STP, this is the maximum time,
   in seconds, that a bridge will wait for Configuration BPDUs before deciding it is no longer
   connected to the root bridge. The range is 6 - 40. The default value is 16 seconds.
Tx Hold Count: This is the maximum number of configuration BPDUs that can be transmitted in
   one second from a port on this Bridge before transmission is throttled. The range is 1 to 10. The
   default value for this field is 6.
Topology Changes: This is the number of RSTP topology changes since the switch has been
   powered on or rebooted.
RSTP Status: This is the current status of the RSTP protocol on this bridge. The available options
   for this field are RSTP, Force STP or Disabled.
   Note: RSTP & N-Ring™ are different network topology protocols and cannot share links or
      segments. If a port is both an RSTP port and an active N-Ring port, then the port will be
      disabled for RSTP.
   Note: Do not create redundant network paths unless either RSTP or N-Ring is enabled.
   Note: If a port is both an RSTP port and an enabled trunk group member, then the port will be
      disabled for RSTP. The RSTP port status can be seen under advanced RSTP ports.
   Note: It is recommended that an RSTP network consist of RSTP capable switches.
   Note: RSTP is supported on only one VLAN.
   Note: When operating in a VLAN with legacy STP devices, use these values for the Bridge: Hello
      Time (Sec) = 2, Forward Delay (Sec) = 15 and Max Age (Sec) = 20.
BPDU Flooding: This value allows for flooding or blocking of BPDUs to other ports when the
   global spanning tree is disabled or when spanning tree is disabled on a specific port. If Flood is
   selected, BPDUs are flooded to all other ports based on the VLAN assignment. The options are
   Flood or Block. The default is Flood.
Click on the *Modify* button and the following dialog window will appear:
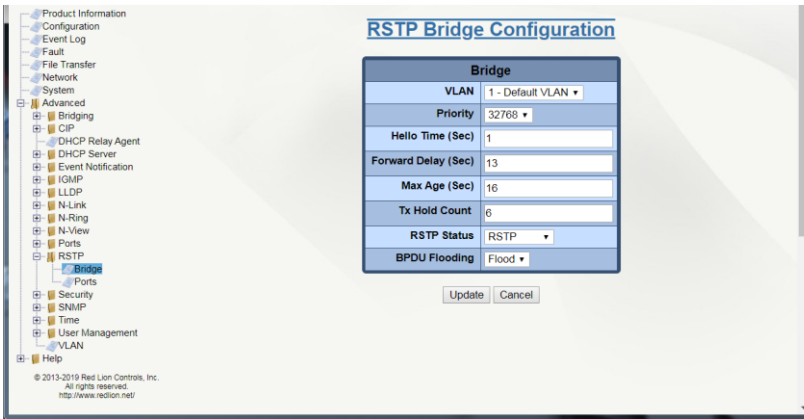
Make the required modifications, and click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

The RSTP Ports dialog window displays information such as the path cost and the port state. If the switch sees a redundant network path, it will put the port with the highest path cost into the Blocking port state where it will discard packets coming in on that port.

In the example shown below, A2 is a redundant port with port A1, therefore A1 is forwarding and A2 is discarding.

Port No	Port Name	Port State	STP BPDU	Path Cost	Priority	Admin Edge	Auto Edge	Point To Point	Designated Bridge Identifier		Designated Port
									Priority	MAC	
01	A1	Forwarding	No	20000	128	Disabled	Enabled	Auto	32768	00:07:af:66:b8:e0	1
02	A2	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
03	A3	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
04	A4	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
05	A5	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
06	A6	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
07	A7	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
08	A8	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
09	B1	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
10	B2	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
11	B3	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
12	B4	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
13	B5	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
14	B6	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
15	B7	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
16	B8	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
17	C1	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
18	C2	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
19	C3	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
20	C4	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
21	C5	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
22	C6	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
23	C7	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0
24	C8	Disabled	No	20000	128	Disabled	Enabled	Auto	0	00:00:00:00:00:00	0

Port No: Indicates the number of the port.

Port Name: Displays the descriptive name of the port.

Port State: The current RSTP state of the port is shown here. This state may be seen as "Forwarding, No STP, Disabled, Listening, Learning, and Discarding.

STP BPDU: Shows whether or not a legacy STP BPDU has been received or not.

Path Cost: Displays the current path cost of the port. The range is 0 - 200,000,000. If configured to 0 or Auto, the path cost will be calculated automatically using the actual speed of the port; otherwise the configured value will be used. The default value for this field is Auto.

Priority: The priority of the port is displayed in this column. The available range is 0 - 255. The default value for this field is 128.

Admin Edge: Indicates whether or not this port is treated as an Edge Port and can immediately enter the forwarding state. If set to Enabled, no BPDUs are expected to be received at the port. Set this option to Enable only when an end device is linked to this port. The default value is Disabled.

Auto Edge: Indicates whether or not to use a short timeout when waiting for BPDUs before determining that this is an Edge Port (if no BPDUs are received). It may have to be disabled for a very large network. The default value is Enabled.

Point to Point: Displays whether at most one other network port is attached to the port's LAN segment. The port may transition to Forwarding very quickly on a point-to-point MAC link. Values may be Auto (full-duplex links are assumed to be point-to-point, half duplex are not), and Force True or Force False (if the automatic determination would be wrong). The default value is Auto.

Designated Bridge Identifier Priority: The priority of the designated bridge associated with the port's LAN segment is shown in this field. The designated bridge provides the lowest cost path from this bridge port's LAN segment, through the designated bridge, to the root bridge.

Designated Bridge Identifier MAC: Indicates the unique MAC of the designated bridge associated with the port's LAN segment.

Designated Port: The designated port of the designated bridge is shown here.

> **Note:** When event logging is enabled, all RSTP controlled ports will log events about their status whether or not the modular based port is currently installed.
> **Note:** When operating in a VLAN with legacy STP devices, set the Auto Edge field to Disabled for Bridge Ports.

To make changes to a Bridge port, click on the *Port No hyperlink* and the following window will appear:

Make the required modifications to the following parameters: Path Cost, Priority, Admin Edge, Auto Edge and Point to Point fields, then click on the *Update* button.

Security

Local Security
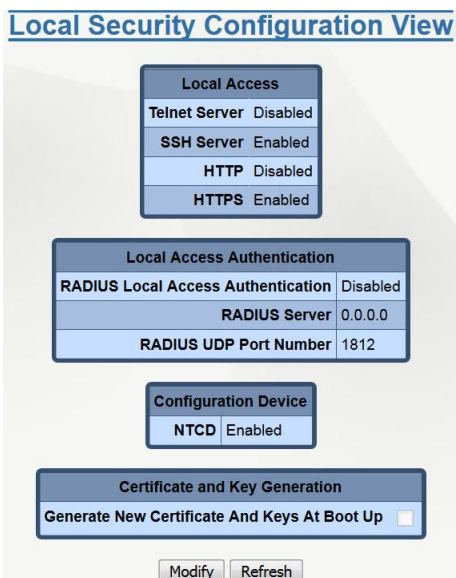
The Local Security feature allows an administrator to control local access (logins) to the switch.

Local Security Configuration View

The Local Security Configuration page displays the status of the Telnet server, SSH Server, HTTP protocol, and HTTPS protocol. The administrator can disable or enable these protocols, as desired. A RADIUS server can be configured to authenticate the user name and password entered for local access.

The N-Tron® Configuration Device (NTCD) SD card slot can be enabled or disabled, allowing an administrator to block and unblock reading and writing settings from the SD card as desired. A new certificate and keys can also be generated at boot up by selecting the *Generate New Certificate and Keys At Boot Up* option.

> **WARNING:** If the NTCD device slot is disabled and the switch password is forgotten, access to the switch can only be recovered by sending it back to the factory to be unlocked.
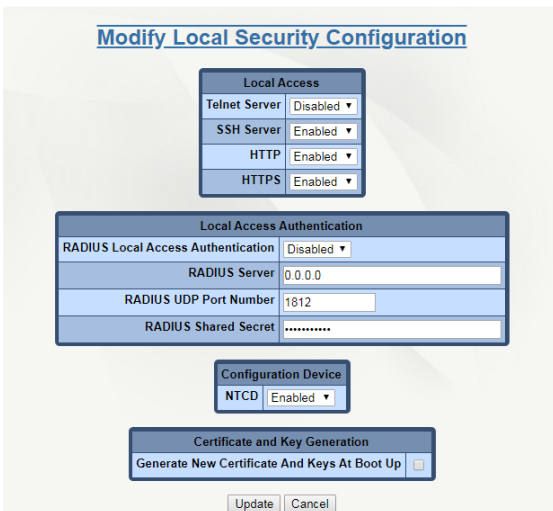
Modify Local Security Configuration

Click on the *Modify* button and the page below will appear. Make the desired changes, and then click on the *Update* button. To save changes, navigate to the Configuration menu and click on the *Save* button.

These settings address local access to the switch. For better security, keep the Telnet Server and HTTP disabled.

Telnet Server: This field indicates whether the Telnet Server is enabled or disabled. Disabling the Telnet Server does not impact SSH. The default is disabled.

SSH Server: This field indicates whether the SSH Server is enabled or disabled. Disabling the SSH Server does not impact Telnet. The default is disabled.

HTTP: This field indicates whether HTTP is enabled or disabled. Disabling HTTP does not affect HTTPS secure connections. The default is disabled. HTTP users are not authenticated by the RADUIS server. If Radius authentication is exclusively required, then HTTP should be disabled.

HTTPS: This field indicates whether HTTPS is enabled or disabled. Disabling HTTPS requires HTTP to be enabled. The default is enabled.

A RADIUS server may be used to manage user accounts that have access to the switches.

RADIUS Local Access Authentication: This field indicates whether RADIUS Local Access Authentication is enabled or disabled. RADIUS authentication is not supported on HTTP connections. The default is disabled.

RADIUS Server: This field is the IP address of the RADIUS server used when RADIUS Local Access Authentication is enabled.

RADIUS UDP Port Number: The UDP port number of the RADIUS Server. The default port number is 1812, per RFC-2865. Allowed port numbers are 1 - 65535.

RADIUS Shared Secret: The shared secret for the local access authentication server. The shared secret authenticates the switch to the RADIUS server and must match the shared secret value on the RADIUS server.

NTCD: This field indicates whether the Configuration Device is enabled or disabled. The default is enabled. Disabling the NTCD SD card slot allows an administrator to block and unblock reading and writing settings to and from the SD card.

Generate New Certificate and Keys at Boot Up: This field indicates whether certificate and keys will be generated when the switch boots up. *A change to this setting requires that settings be saved and that the switch be rebooted before changes take effect*. The value will reset to be unchecked when the switch boots up. The default is no.

Port Security

Port Security can be enabled on the MAC address level for additional security. The Port Security feature restricts access to the switch by only accepting dynamically learned MAC addresses and manually entered MAC addresses as authorized. Dynamically learned MAC addresses are those that the switch detects on any port while in 'Learning' mode. A manually entered MAC address must designate the port(s) that the address is authorized on. A non-authorized MAC address will be discarded and will be shown on the intruder log.

Port security allows secured ports to run with RSTP enabled on the port. Port security also allows the same MAC address to be authorized on multiple ports. When setting up authorization lists for RSTP ports, any MAC address that could migrate to other secured ports should also be placed, by the user, in the authorization list for those ports.

Port Security – Configuration

The Port Security Configuration View displays the status of Port Security and all the ports with their current settings. When Status is 'Locked' it is in secure mode. When Status is 'Learning' it builds an internal list of authorized MAC addresses and no ports are secured during this time.

Port Security Configuration View
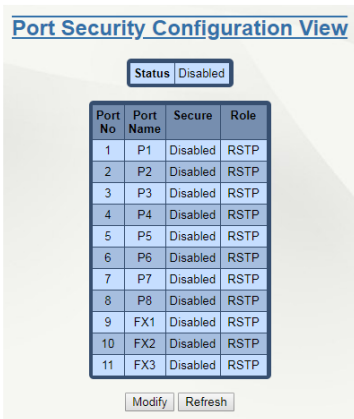
The Modify button allows the administrator to change the Status of Port Security and Secure mode for all ports.

Modify Port Security Configuration
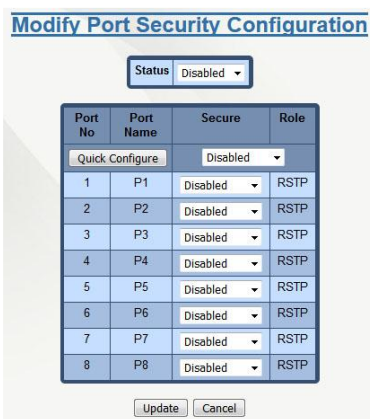
Status: The current status of Port Security. It can be Disabled, Learning, or Locked. Transitioning from Locked to Learning clears the Authorization List table on all ports. Transitioning from Locked to Disabled retains the current Authorization List. When transitioning from Learning to Locked, the Authorization List represents the authorized MAC addresses. The default value is Disabled.

Port No: The number of the port.

Port Name: The descriptive name of the port.

Secure: Displays Secure mode for the associated port. It can be Disabled, Enabled, or Single Mac.

- **Disabled:** Port Security is not active on the port regardless of the current Port Security Status.
- **Enabled:** Port Security is active when the current Port Security Status is Learning or Locked.
- **Single MAC:** Port Security will take the first learned MAC address and lock the port when current Port Security Status is Learning or Locked.

The default value is Disabled.

Role: A comma separated list of all the active roles for the port, which are based on the switch configuration. The possible roles are RSTP, N-Ring™, N-Link Control, N-Link Partner, N-Link Coupler, 802.1X, and Trunk.

Make the required modifications, and click on the Update button. To save the changes made, navigate to the Configuration menu and click on the Save button.

> **Note:** Security is not configurable on N-Ring or N-Link interconnecting ports. These ports must be linked to adjacent switches that have the protocol enabled. This link is considered to be a

closed proprietary connection/segment that is not directly accessible. If both switches are otherwise properly secured then the proprietary connection/segment requires no additional security.

Note: It is recommended that the Bridging Aging Time be 300 seconds (the default) or longer while Port Security is Learning.

Ports Security – Authorization List

The Authorization List View displays a drop-down list of the available ports that is used to filter the authorization list. Below the drop-down list is the table of authorized Static and Learned MAC addresses and ports.

Note: Multicast Source Addresses will not show up in the Authorization List.
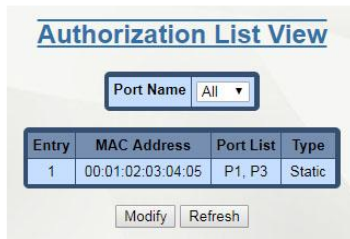
The Modify button allows the administrator to add new MAC addresses, and to modify and remove existing MAC addresses. The last row is used to add new MAC addresses and to change the ports of an existing MAC address.
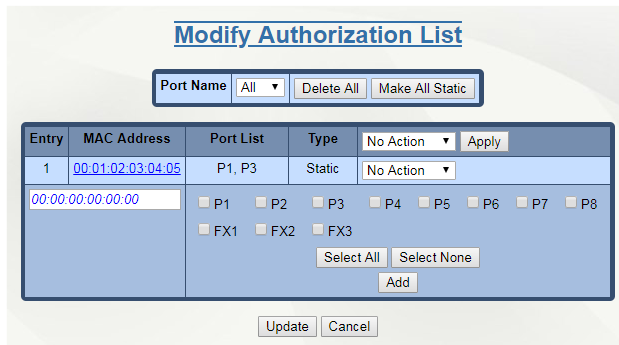
Port Name: The descriptive name of the port.

MAC Address: The authorized host MAC address.

Port List: The port(s) that are authorized for the associated MAC address.

Type: The type of the authorized MAC Address. It can be either Learned, Static, or Single MAC.

Action: Action for the authorized MAC address. It can be No Action, Make Static from Learning mode, or Delete from the Authorization List. The maximum number of actions that may be performed on the Authorization List in a single update is 100.

Make the required modifications, and click on the Update button. To save the changes made, navigate to the Configuration menu and click on the Save button.

Delete All Authorization List

To delete the complete authorization list associated with the selected port(s), click on *Delete All* button. A confirmation dialog pop-up will appear, prompting the user to confirm the action.

Make All Learned Authorization Entries Static

To make all learned authorization entries associated with the selected port(s) as Static, click on *Make All Static* button. A confirmation dialog pop-up will appear, prompting the user to confirm the action.

Note: Ports that are set to Single MAC cannot be included in static entries in the Authorization List.

Ports Security – Intruder Log

The Intruder Log page displays a list of unauthorized MAC addresses that attempted to access the secured device. Each intruder entry in the log is based on MAC address and Port. Multicast source MAC addresses will not be displayed in the Intruder Log table. The log is ordered by most recent first, based on the system up time and time stamp. The maximum number of entries is 100. If more than 100 intruders are detected, the oldest entries are deleted. The log is not saved through a power cycle.

Intruder Log View

System Up Time	Time Stamp	Event
0d 00:49:52.500	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:67.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:4b.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:31.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:30.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8e.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8d.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2e.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8c.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8b.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2c.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8a.
0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2b.
0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:89.
0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2a.
0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:88.
0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:29.

Modify Refresh

To authorize a particular MAC Address from the Intruder Log, click on the Modify button and an "Authorize" field will be added as a checkbox as shown below:

Modify Intruder Log

Authorize	System Up Time	Time Stamp	Event
☐	0d 00:49:52.500	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:67.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:4b.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:31.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:30.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8e.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8d.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2e.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8c.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8b.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2c.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:8a.
☐	0d 00:49:52.499	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2b.
☐	0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:89.
☐	0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:2a.
☐	0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P2 with MAC Address: 00:10:94:00:03:88.
☐	0d 00:49:52.498	2000-01-01 00:49:51 CST (UTC-06:00)	Detected Intruder on Port: P1 with MAC Address: 00:10:94:00:01:29.

Update Cancel

Displays the most recent 100 intruders since the latest system startup. To review a complete list, please see the Event Log page.

FIELD	DESCRIPTION
Authorize	This is the selection to Authorize MAC Address(es) from the Intruder Log.
System Up Time	The elapsed time since the switch was powered on or rebooted.
Time Stamp	The date/time when the event was logged.
Event	The description of the intrusion.

Make the required modifications and click on the Update button. To save the changes made, navigate to the Configuration menu and click on the Save button.

An authorized entry will be displayed as green text color for that particular row in the Intruder Log table. The corresponding checkbox in the Authorize column will be checked and cannot be modified.

Port Security – Single MAC

Single MAC is a port security mode that allows a port to lock on a dynamically learned MAC address. The first MAC address to be learned and processed by the port will be locked in and any further traffic will be blocked as an intruder. The locking of the address is not dependent on switching the port security status to Locked. This feature helps in providing security for ports that may only have a single device plugged into the switch. The Single MAC address is not persistent following a reboot. The Single MAC will remain locked until a reboot upon which time a new MAC address will be learned and assigned as the new Single MAC entry.

Single MAC can be configured per port from the Port Security Configuration page. Manually added MAC addresses are not allowed to be assigned to a port designated as Single MAC. If a port is enabled under port security and then changed to Single MAC all learned addresses will be cleared and the next MAC address that comes in will be the new Single MAC address.

Single MAC addresses reset anytime the port security status is changed to Learning. Single MAC addresses are persistent when port security status is changed from Learning or Locked to Disabled and then back to Locked.

Single MAC limitations include: intruders on the Single MAC port cannot be manually authorized, and new addresses cannot be manually added to a Single MAC port.

Radius Server Configuration Information

The NT24k® takes advantage of Vendor Specific Attributes (VSA) as defined in section 5.26 of RFC 2865 so that multiple user levels can be authenticated using a Radius server. The VSA is defined as follows:

VENDOR ID	28381
Vendor ID	28381
Attribute Number	1
Attribute Format	string
Attribute Value	"AccessLevel:admin" or "AccessLevel:user"

The server and access list will need to be configured accordingly.

802.1X/Configuration

The Configuration dialog window displays the 802.1X status, reauthentication information, and RADIUS server information.

> **Note:** Bypass Relay models affect the implementation of this protocol. For more information, see the section Bypass Relay (BR).

802.1X Configuration View

WARNING: Ports must individually be set to use 802.1X for them to authenticate attached devices. See the 802.1X Ports Page.

802.1X Status	Disabled
Default Reauthentication Status	Enabled
Default Reauthentication Timeout (Sec)	600
Primary RADIUS Server	0.0.0.0
Primary RADIUS UDP Port Number	1812
Backup RADIUS Server	0.0.0.0
Backup RADIUS UDP Port Number	1812

Modify   Refresh

To make changes to the Security settings, click on the *Modify* button and the fields shown below will become editable:

802.1X Configuration

802.1X Status	Disabled ▼
Default Reauthentication Status	Enabled ▼
Default Reauthentication Timeout (Sec)	600
Primary RADIUS Server	0.0.0.0
Primary RADIUS UDP Port Number	1812
Primary Server Shared Secret	··········
Backup RADIUS Server	0.0.0.0
Backup RADIUS UDP Port Number	1812
Backup Server Shared Secret	··········

Update   Cancel

802.1X Status: This field indicates whether the 802.1X feature is enabled or disabled. At least one RADIUS server must be specified for 802.1X to be enabled. Ports must also be individually enabled on the ports configuration page.

Default Reauthentication Status: Select whether the 802.1X Reauthentication option is enabled or disabled. With reauthentication enabled, a device will be required to reauthenticate itself based on the time period specified by the reauthentication timeout field. 802.1X must be disabled to change this value.

Default Reauthentication Timeout (Sec): Enter the time period, in seconds, between 802.1X reauthentication. This value cannot be zero (0). 802.1X must be disabled in order to change this value.

Primary RADIUS Server: This field indicates the IP address of the primary RADIUS server. If contact with this server is lost, then contact with the backup server will be attempted.

Primary RADIUS UDP Port Number: The UDP port number of the Primary RADIUS Server. The default port number is 1812, per RFC-2865. Allowed port numbers are 1 - 65535.

Primary Server Shared Secret: This field displays the shared secret for the primary server. The shared secret authenticates the switch to the RADIUS server and must match the shared secret value on the RADIUS server.

Backup RADIUS Server: This field indicates the IP address of the backup RADIUS server. If contact with the primary server is lost, contact with the backup server will then be attempted.

Backup RADIUS UDP Port Number: The UDP port number of the Backup RADIUS Server. The default port number is 1812, per RFC-2865. Allowed port numbers are 1 - 65535.

Backup Server Shared Secret: This field displays the shared secret for the backup server. The shared secret authenticates the switch to the RADIUS server and must match the shared secret value on the RADIUS server.

Make the required modifications and click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

802.1X/Ports

The 802.1X Port Configuration View dialog window displays all the ports and their current settings. To modify this information, click on the *Modify* button.

Port No: This column shows the number of the port.

Port Name: This column displays the port's descriptive name.

802.1X Status: This column indicates whether the existing 802.1X port is enabled or disabled. Ports only require 802.1X authentication if they are enabled and 802.1X is globally enabled on the configuration page.

802.1X State: This column shows the current state of the port. This option is only valid when the port is enabled and 802.1X is globally enabled.

> **Link Down:** There is no link detected on the port.
> **Initialize:** The port is being setup for 802.1X authentication.
> **Disconnected:** A valid 802.1X client has not been detected.
> **Connecting:** A valid 802.1X client has been detected, but authentication has not begun.
> **Authenticating:** The 802.1X client is being authenticated.
> **Authenticated:** The 802.1X client has been authenticated.

> **Aborting:** The port is no longer authorized and is preparing to move back to the Disconnected state.
>
> **Held:** The 802.1X client failed authentication and the switch is preventing new authentication attempts for a defined period of time. Default: 60 seconds.
>
> **Forced Authorized:** Occurs when a port has had 802.1X disabled. The result is all traffic is allowed to pass through that port.
>
> **Forced Unauthorized:** Occurs when a port is administratively disabled through the port configuration. The result is no traffic is allowed to pass through that port.

Click on the *Modify* button and the page below will appear. Select the required ports, and then click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.
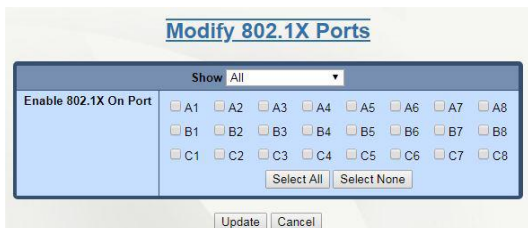
IEEE 802.1X MIB

The IEEE 802.1X MIB, IEEE 8021-PAE-MIB, is supported by the NT24k®. Since the NT24k does not support the supplicant features of 802.1X, the MIB tables pertaining to the supplicant behavior will not be populated and will be blank when queried.

With this release, the IEEE 802.1X MIB support is limited. Ports are only tracked when an 802.1X aware supplicant is attached. This means that not all 802.1X enabled ports will be visible, only those with valid supplicants. The statistics available through the MIB only pertain to the device since it either passed or failed authentication. Once the link goes down on the port, the statistics will be reset. Furthermore, any configuration items accessed through the IEEE 802.1X MIB can be set to modify the behavior of the port, but these changes will not persist across link events or power cycles.

Configuration changes that occur through the NT24k MIB will be persisted across link events and power cycles. Support for persisted statistics and configuration settings in the IEEE 802.1X MIB will be added to the NT24k in a future release.

The IEEE 802.1X MIB allows for the writing to dot1xPaeSystemAuthControl. This is not supported in the current release of the NT24k firmware. dot1xPaeSystemAuthControl is considered a read-only attribute. The functionality for this is located in the NT24k MIB as ntronSecurityDot1xConfigStatus.

The IEEE 802.1X MIB allows for the writing to dot1xAuthAdminControlledDirections. Controlling the direction of the port traffic is not currently supported in the NT24k firmware and writing to dot1xAuthAdminControlledDirections will not have an effect on the system.

SNMP

Configuration

The SNMP Configuration displays the SNMP status and allows the administrator to disable or enable the protocol. The Read-Only, Read-Write and Trap Community Names are also displayed in this dialog window.

Management Station Configuration View

SNMP Status	Enabled

Read-Only Community Name	public
Read-Write Community Name	private
Trap Community Name	public

SNMP Notification Trap	Send Trap?
Cold Start	☐
Authentication	☐
Warm Start	☐
Link Status	☐

Modify | Refresh

SNMP Status: This field indicates whether SNMP is enabled or disabled.

Read-Only Community Name: This configurable field represents the Authorized Community Name for SNMP Get requests. Only alphanumeric characters are allowed. The default value for this field 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 for this field is private. Only administrators can view or modify this field.

Trap Community Name: This configurable field represents the Authorized Community Name for SNMP Traps. Only alphanumeric characters are allowed. The default is for this field is public.

SNMP Notification Traps: This section allows for control of which SNMP traps will be sent by this switch. Each of the four available traps can be enabled or disabled individually. The traps are: Cold Start, Authentication, Warm Start and Link Status.

Click on the *Modify* button to make changes to the SNMP Configuration. This will enable all configurable fields. Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Management Station Configuration

SNMP Status	Enabled ▼

Read-Only Community Name	public
Read-Write Community Name	private
Trap Community Name	public

SNMP Notification Trap	Send Trap?
Cold Start	☐
Authentication	☐
Warm Start	☐
Link Status	☐

Update | Cancel
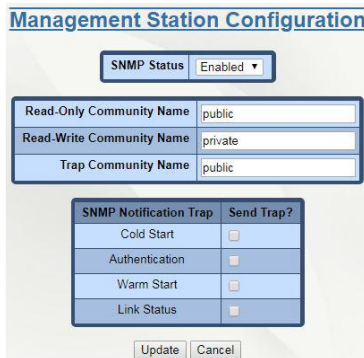
Trap Stations

The Trap Stations dialog window displays the SNMP Trap Stations.

Display Management Trap Stations

IP Address	Parameter

Number of Management Trap Stations: 0

Add   Remove   Refresh

IP Address: This field represents the IP address of the Management Station to be sent SNMP Traps.

Parameter: This field displays the Target Parameters entry (TRAPv1, TRAPv2, etc) to be used for sending traps to the Management Station.

Adding Management Trap Stations

To add trap stations, click on the *Add* button and the following will appear:

Add Management Trap Station

IP Address	0.0.0.0
Parameter	TRAPv2

Update   Cancel

Remove Management Trap Station

IP Address	Parameter	Delete
192.168.2.180	TRAPv2	Delete

Number of Management Trap Stations: 1

Done

Enter the required IP address and select the parameter to be used. Click on the *Update* button and the Display Management Trap Stations screen will appear.

SNMP V3 Default Security Parameters: The SNMP V3 default user parameters are shown here for reference only, as they are necessary for connecting to the switch securely using an SNMP V3 client when in defaults.The default user and other users can be added, deleted or modified by an administrator via either an SNMP V3 client or web browser, and the values below may be invalid if they are changed by an SNMP administrator.

Username: initial
Authentication Password: authpass
Authentication Protocol: MD5
Privacy Password: privpass
Privacy Protocol: DES

To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Groups

The SNMP Groups page allows the customer to configure SNMP group settings for specific SNMP users.

SNMP Groups Configuration View

User Name	Security Model	Group Name
get	V1	mibRead
get	V2c	mibRead
initial	USM	v3AuthPrivGroup
set	V1	mibWrite
set	V2c	mibWrite
trap	V1	mibNotify
trap	V2c	mibNotify

Add   Remove   Refresh

Click on the *Add* button to create a new SNMP group, or click the hyperlink under User Name to modify existing group settings for a user. Click the *Remove* button to display a list of current configured group and user settings, with an option to remove specific ones.

Add SNMP Configuration Groups

User Name	Security Model	Group Name
initial ▼	V1 ▼	

Update   Cancel

Remove SNMP Configuration Groups

User Name	Security Model	Group Name	Remove
get	V1	mibRead	Remove
get	V2c	mibRead	Remove
initial	USM	v3AuthPrivGroup	Remove
set	V1	mibWrite	Remove
set	V2c	mibWrite	Remove
trap	V1	mibNotify	Remove
trap	V2c	mibNotify	Remove

Cancel

User Name: This field represents the SNMP User Name. It is a drop down list with an option for every SNMP user defined on the **Users** page.

Security Model: This field represents the security model the SNMP protocol will use for the defined group. The default is Any, while V1, V2c and USM (User-based Security) are the other available options.

Group Name: This field represents the SNMP Group to which the SNMP user belongs.

Access

The SNMP Access page allows the customer to define various types of MIB access based on the defined view settings for each SNMP group.

SNMP Access Configuration View

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name
mibNotify	Any	None	mibView		mibView
mibRead	Any	None	mibView		
mibWrite	Any	None	mibView	mibView	mibView
v3AuthPrivGroup	USM	Priv	mibView	mibView	mibView

Add   Remove   Refresh

Click on the *Add* button to define new access settings for a group, or click the hyperlink under Group Name to modify existing access for a group. Click the *Remove* button to display a list of current configured group and access settings, with an option to remove specific ones.

Add SNMP Configuration Access

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name
v3AuthPrivGroup ▼	Any ▼	None ▼	▼	▼	▼

Update   Cancel

Remove SNMP Configuration Access

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name	Remove
mibNotify	Any	None	mibView	mibView	mibView	Remove
mibRead	Any	None	mibView			Remove
mibWrite	Any	None	mibView	mibView	mibView	Remove
v3AuthPrivGroup	USM	Priv	mibView	mibView	mibView	Remove

Cancel

Group Name: This field represents the name of the group the user defines access settings for. It is a drop down list with an option for every SNMP group defined on the **Groups** page.

Security Model: This field represents the security model used to validate group access to views. The options are V1, V2c and USM (User-based Security).

Security Level: This field represents the security level of SNMP communications for the defined group. The options are None, Auth, and Priv.

Read View Name: The name of the view that the defined group has read access to. It is a drop down list with an option for every SNMP view defined on the **View** page.

Write View Name: The name of the view that the defined group has write access to. It is a drop down list with an option for every SNMP view defined on the **View** page.

Notify View Name: The name of the view that the defined group has notify access to. It is a drop down list with an option for every SNMP view defined on the **View** page.

Users

The SNMP Users page allows a customer to create custom user names for group access and set the authentication and privacy protocols for that user. It is important to note that authorization and privacy passwords, when created, are hashed internally for security and will not be able to be retrieved.

SNMP Users Configuration View

User Name	Authentication Protocol	Privacy Protocol
initial	MD5	DES

Add   Remove   Refresh

Click on the *Add* button to create a new SNMP user, or click on a hyperlink in the *User Name* column to edit the information for that user. Click the *Remove* button to display a list of current configured users, with an option to remove specific ones.

Add SNMP Configuration Users

User Name	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
	None ▼		None ▼	

Update   Cancel

Remove SNMP Configuration Users

User Name	Authentication Protocol	Privacy Protocol	Remove
initial	MD5	DES	Remove

Cancel

User Name: This field represents the SNMP User Name.

Authentication Protocol: This field represents the authentication protocol utilized by the SNMP user. The options are None, MD5, and SHA1.

Authentication Password: The defined authentication password for the SNMP user. The password can be between 1 and 32 characters in length, but it is recommended that it is at least 8 characters in length. Alphanumeric and special characters are accepted.

Privacy Protocol: This field represents the privacy protocol utilized by the SNMP user. The options are None, DES, and AES-128.

Privacy Password: The defined privacy password for the SNMP user. The password can be between 1 and 32 characters in length, but it is recommended that it is at least 8 characters in length. Alphanumeric and special characters are accepted.

View

The SNMP View page allows a customer to define different view groups, which either include or exclude specific sub trees from the MIB tree based on the configuration.
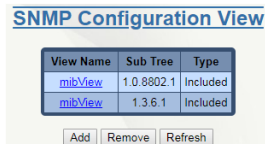
Click on the *Add* button to create a new SNMP view, or click on a hyperlink in the *View Name* column to edit the information for that view. Click the *Remove* button to display a list of current configured views, with an option to remove specific ones.
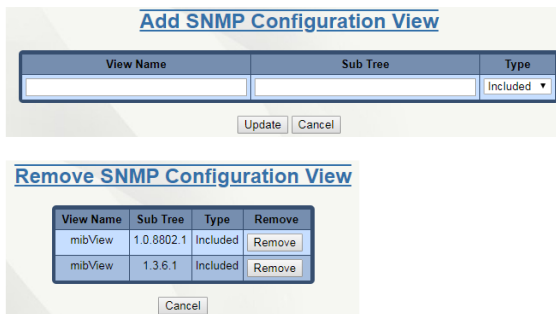
View Name: This field represents the name of the SNMP view.

Sub Tree: This field allows the user to enter an OID string representing the sub tree being included or excluded from the view, based on the **Type** setting.

Type: This field allows the user to configure what the SNMP view does with the sub tree defined in the *Sub Tree* field. The options are Included and Excluded.

Time

Basic

From the Basic Time Configuration View dialog, the administrator can define the system time, time zone, daylight savings time and time source settings for the unit.

Basic Time Configuration View

Click on the *Modify* button to make modifications to the unit's time settings.

Modify Basic Time Configuration

System Time: This field displays the date/time of the system. The system date/time defaults to 2000-01-01 00:00:00 CST (UTC-06:00) at system start. The system date/time can be set manually but in the event of a power cycle or reboot it will revert to the default value.

Time Source: This field controls how the switch will automatically set its clock. The default value of "Set Time Manually" means that the time the switch uses can only be set manually. Setting this field to either "SNTP" or "PTP" causes the protocol to continuously update the system clock. Note that these must be enabled and configured separately from the basic time configuration. PTP is a licensed option and is unavailable otherwise.

Time Zone

Presets: This field provides a list of global time zones and cities within the time zones. Selecting from this list provides easy local time configuration and automatically populates the fields below. Choosing the "Custom..." option allows for editing of the below fields to satisfy specific requirements that are not met by one of the preset time zones.

Description: This field provides a description of the time zone selected. It contains the city and the offset from UTC for the selected location. If a custom preset is selected the description may be edited.

Standard Time Abbreviation: The common abbreviation for the selected time zone during standard daylight time is shown in this field. If a custom preset is selected the abbreviation may be edited.

Daylight Saving Time Abbreviation: This field represents the common abbreviation for the selected time zone during daylight saving time or summertime. If a custom preset is selected the abbreviation may be edited.

UTC Offset (Minutes): This field displays the offset, in minutes, from UTC. This is used to determine the local time. If a custom preset is selected the offset may be edited. Any change to the offset will affect the time calculation.

Daylight Saving Time

Adjust For Daylight Saving Time: This field indicates whether automatic adjustment for daylight saving time is made. The settings for this adjustment are defined below.

Daylight Saving Time Offset (Minutes): This field defines how much, in minutes, to adjust the time when daylight saving time starts and ends.

Daylight Saving Time Start: The week, the day of the week, the month, and the time at which daylight saving time should start.

Daylight Saving Time End: The week, the day of the week, the month, and the time at which daylight saving time should end.

Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

SNTP

From the SNTP Configuration View, the SNTP status can be changed, and the primary and back-up servers can be defined. Click on the *Modify* button to enable or modify the current settings.
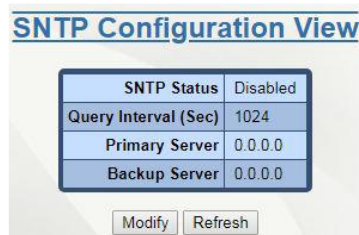
SNTP Status: Indicates whether the SNTP client has been enabled. In order to enable SNTP, at least one SNTP or NTP server must be specified.

Query Interval (Sec): The periodic query interval used to request the time from the server(s). The valid range is between 4 and 129600. The default value is 1024.

Primary Server: The address of the server to query first and most often. If contact with this server is lost, then contact with the backup server will be attempted. Either an SNTP or an NTP server may be specified.

Backup Server: The address of the backup server to query in the event that access is lost to the primary server. Either an SNTP or an NTP server may be specified. Click on the *Update* button. To save the changes made, navigate to the *Configuration* menu and click on the *Save* button.

Precision Time Protocol (PTP)

PTP Basic Configuration

The PTP Basic Configuration View displays the PTP Mode and allows the administrator to disable the protocol, or enable one of two clock modes, Boundary or Transparent.

PTP Basic Configuration View

PTP Mode	Boundary

Modify   Refresh
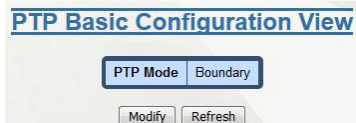
PTP Mode: This field indicates whether PTP is disabled, operating as a Boundary clock, or operating as a Transparent clock. When PTP is disabled, PTP traffic will route through the switch like any other multicast traffic.

Transparent Clock mode generally provides the most accurate time to a PTP client when the network is lightly loaded and there are only a few PTP clients connected to the switch. Boundary Clock mode is a better choice for a congested network. Boundary Clock mode also becomes a better choice as more PTP clients are connected to the switch.

Click on the *Modify* button to change the PTP Mode. When the desired mode has been selected, click *Update*.

Modify PTP Basic Configuration

PTP Mode	Transparent ▾

Update   Cancel

> **Note:** When switching between PTP modes, it will be necessary to save the configuration and reboot the switch for the change to take effect.

PTP Port Configuration

The PTP Port Configuration View displays global and per port settings that relate to PTP.

The settings in the **Boundary Clock** table are applied to every port of a switch in Boundary Clock mode. The **Boundary Clock Ports** or **Transparent Clock Ports** table displays the PTP Port Mode for every port on the switch.

PTP Port Configuration View

Boundary Clock

Announce Interval	2 Seconds (1)
Announce Timeout	3 Announce Intervals
Sync Interval	1/2 Second (-1)
Delay Request Interval	1 Second (0)

Boundary Clock Ports

Show All ▾

Port No	Port Name	PTP Port Mode
1	P1	Enabled
2	P2	Enabled
3	P3	Disabled/Pass-Through
4	P4	Enabled
5	P5	Disabled/Pass-Through
6	P6	Disabled/Pass-Through
7	P7	Disabled/Pass-Through
8	P8	Disabled/Pass-Through

Modify   Refresh

Global Boundary Clock Settings

Announce Interval: This is the log2 value that sets the interval for how often to announce the switch as an eligible PTP Master. The default value of "1" is every 2 seconds. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Announce Timeout: This value determines the number of announce intervals that must elapse without receipt of an announce message before a non-communicating Master is marked as unavailable. The default value is 3 intervals. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Sync Interval: This log2 value determines how often a sync message will be sent. The default value of "- 1" is twice per second. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Delay Request Interval: This log2 value determines how often the switch will request a path delay measurement from its Master. The default value of "0" is once per second. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Boundary Clock Ports or Transparent Clock Ports Settings

Port No: Indicates the number of the port.

Port Name: The descriptive name of the port.

PTP Port Mode: The operation mode of the PTP port. Values are "Enabled", "Disabled/Pass-Through" (default), or "Disabled/Blocked". When Enabled, PTP packets will be processed by the switch PTP software. When Disabled/Blocked, PTP packets will be discarded as they enter the port. When Disabled/Pass- Through, PTP packets will be forwarded to other pass-through ports (within VLAN restrictions) with no PTP processing.

Click the *Modify* button to change any of the global settings or to change the PTP Port Mode of specific ports.

Once modifications to Announce Interval, Announce Timeout, Sync Interval, Delay Request Interval or PTP Port Mode have been made, click on the *Update* button.

> **Note:** The settings on the PTP Port Configuration View page are associated with the mode set on the PTP Basic Configuration View page.

PTP Advanced Configuration

The PTP Advanced Configuration View displays common advanced PTP settings and advanced settings that relate specifically to the Boundary Clock mode of operation. The Common values are read-only and only some values can be modified.
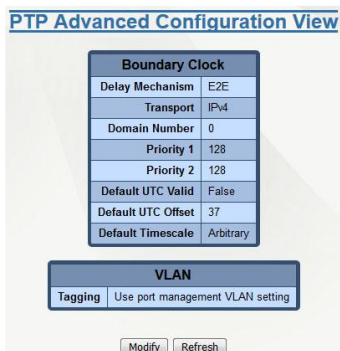
Boundary Clock

Delay Mechanism: The Delay Mechanism specifies the method used by PTP to handle delay correction values. E2E is the only delay mechanism currently supported.

Transport: IPv4/UDP is the only network transport method currently supported.

Domain Number: The Domain Number selects a PTP Domain. Only PTP packets in the same domain will be received and processed, and all sent PTP packets will be tagged with the same Domain Number. The range is 0-127. The default is 0.

Priority1: This value sets the priority of this switch as a Master clock. It is the most important value used by the Best Master Clock (BMC) algorithm of other PTP devices when selecting a Master clock. The range is 0-255, with 0 being most important. The default is 128.

Priority2: This value is used to break ties in the BMC algorithm. The range is 0-255, with 0 being most important. The default is 128.

Default UTC Valid: Current UTC Valid is a field in PTP packets that tells other devices whether the UTC Offset field that is also being sent in the packet should be considered valid. The Current UTC Valid value is set to this default at boot time, until it is updated by making a connection to a PTP Master. The default is "False" because the switch does not boot with a valid calendar time. It can be changed for interoperability reasons.

Default UTC Offset: The Current UTC Offset value is set to this default at boot time. The range is 0-127. The default is 36.

Default Timescale: The Current Timescale value is set to this default at boot time. All times exchanged in the PTP protocol are either "Arbitrary" or "PTP". Times that are "Arbitrary" cannot be converted to calendar time correctly and may have no connection to external accurate time. Times that are "PTP" can be converted to accurate calendar time using the UTC offset. The default is "Arbitrary" because the switch does not boot with a valid calendar time. It can be changed for interoperability reasons.

VLAN Tagging: PTP frames that egress a PTP port may have a VLAN tag or may be untagged. When "Use port Management VLAN setting" is selected, the PTP frame is untagged if the Management VLAN is set to 'Untag on Egress'. Otherwise, the frame is tagged with the Management VLAN ID. This is the default setting. When "Use port PVID setting" is selected, the PTP frame is untagged if the VLAN used as the PVID is set to 'Untag on Egress'. Otherwise, the frame is tagged with the port's PVID.

> **Note:** When PTP Mode is "Transparent Clock", PTP frames will obey VLAN restrictions and will not cross VLAN boundaries.

To make changes, click on the *Modify* button. Once the desired changes have been made, click on the *Update* button to apply changes to settings.

> **Note:** The settings on the PTP Advanced Configuration View page are associated with the mode set on the PTP Basic Configuration View page.
>
> **Note:** The Current UTC Valid, Current UTC Offset and Current Timescale values are not displayed on the View or Modify pages when PTP is currently disabled or in Transparent Clock mode because they do not apply.

Status

The PTP Status and Information page displays read only information about a device's PTP configuration. General and per port information is displayed on this page.

> **Note:** When PTP is disabled, the only information displayed on this page is PTP Mode and Clock ID, because nothing else applies when PTP is disabled.

PTP General Information

PTP Mode: The PTP mode of the switch. Options include "Disabled", "Boundary Clock", and "Transparent Clock". The default is "Disabled". If the PTP protocol is disabled on the switch, all ports behave as Disabled/Pass-Through. Changes to this setting require a reboot of the switch.

Connection Status: This only applies to Boundary Clock mode. This is the current PTP Master clock of the switch. If this switch is the Master clock, then the connection status indicates that PTP is not synchronized with a Grandmaster.

PTP Clock Time: This only applies to Boundary Clock mode. This displays the date/time of the PTP Clock. The PTP Clock defaults to the system clock when not synchronized to a PTP Master clock.

Clock ID: The unique Clock ID of this PTP device. It is constructed automatically based on the switch MAC address.

Current UTC Valid: A field in exchanged PTP packets that says whether the UTC Offset field that is also being sent in the packet should be considered valid. This is a run-time value that is dynamically updated based on the most recently connected PTP Master.

Current UTC Offset: A field in exchanged PTP packets that provides the current offset to UTC. This is a run-time value that is dynamically updated based on the most recently connected PTP Master.

Current Timescale: A field in exchanged PTP packets that provides the most recently received Timescale value from the Master. This is a run-time value that is dynamically updated based on the most recently connected PTP Master. If this value is "PTP", the internal PTP time can be converted to a calendar time using the Current UTC offset.

Current Announce Interval: This only applies to Boundary Clock mode. This is the $\log_2$ value that sets the interval for how often to announce the switch as an eligible PTP Master. The default value of "1" is every 2 seconds. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Current Announce Timeout: This only applies to Boundary Clock mode. This value determines the number of announce intervals that must elapse without receipt of an announce message before a non-communicating Master is marked as unavailable. The default value is 3 intervals. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Current Sync Interval: This only applies to Boundary Clock mode. This $\log_2$ value determines how often a sync message will be sent. The default value of "-1" is twice per second. The current value is dynamically updated by the PTP protocol and may differ from the setting.

Current Delay Request Interval: This only applies to Boundary Clock mode. This $\log_2$ value determines how often the switch will request a path delay measurement from its Master. The default value of "0" is once per second. The current value is dynamically updated by the PTP protocol and may differ from the setting.

PTP Slave Information

Slave Port: This only applies to Boundary Clock mode. This is the port that is connected to and inheriting configuration values from a PTP Master. If no port is acting as a PTP Slave this field will have a value of "N/A".

Slave Announce Interval: This only applies to Boundary Clock mode. This is the $\log_2$ value that sets the interval for how often to announce the switch as an eligible PTP Master. The default value of "1" is every 2 seconds. The slave value is dynamically updated by the PTP protocol and may differ from the setting.

Slave Announce Timeout: This only applies to Boundary Clock mode. This value determines the number of announce intervals that must elapse without receipt of an announce message before a non-communicating Master is marked as unavailable. The default value is 3 intervals. The slave value is dynamically updated by the PTP protocol and may differ from the setting.

Slave Sync Interval: This only applies to Boundary Clock mode. This $\log_2$ value determines how often a sync message will be sent. The default value of "-1" is twice per second. The slave value is dynamically updated by the PTP protocol and may differ from the setting.

Slave Delay Request Interval: This only applies to Boundary Clock mode. This $\log_2$ value determines how often the switch will request a path delay measurement from its Master. The default value of "0" is once per second. The slave value is dynamically updated by the PTP protocol and may differ from the setting.

PTP Port Status

Port No: The number of the port.

Port Name: The descriptive name of the port.

PTP Port Mode: The operation mode of the PTP port. Values are "Enabled", "Disabled/Pass-Through" (default), or "Disabled/Blocked".

PTP Port State: The current PTP state of a port. It should be noted that when PTP is in Transparent Clock mode the port state is not applicable and will not be displayed.

User Management

Authorized Users

The User Management screen allows users to view, add, modify and remove system user accounts. The display includes a list of all the users who have access to the management features of the switch and their access permissions.

Note: Up to 5 web users may be logged into the Web Management tool at once.

Adding Users

The system administrator can add users, change passwords and define access permissions for each user. Click on the *Add* button and the following dialog window will appear:

User Name: User names may include all alphanumerical characters, as well as the following 2 characters: _ - , and must be 3 to 15 characters long.

Password: Passwords can include all printable characters, except for the colon (:) and spaces, and the password length must be in the range specified by the "Password Length Min" and "Password Length

RedLion®

Max" fields. These fields are configurable under the User Management Configuration screen. The background print in the Password entry field will specify the currently configured range.

Access Permission: This field determines whether a user has standard *User* rights or *Admin* access.

- *User* permission gives the right to view switch configurations and to view current port settings.
- *Admin* permission gives the right to change and view any switch configuration and to change and view any current port settings.

Removing Users

Users can be removed by a user with Admin access. Click on the *Remove* button, enter the User Name to be deleted and click on the *Remove* button.

Configuration

The User Management Configuration screen allows for the switch to be configured with a user password length minimum and user password length maximum.

Password Length Min: The minimum number of characters allowed in a user password. The default is 3 characters.

Password Length Max: The maximum number of characters allowed in a user password. The default is 15 characters.

The Configuration screen allows modification of the minimum user password length and the maximum user password length. Both fields, 'Password Length Min' and 'Password Length Max' must be within the overall range of 3 to 15 characters, inclusive.

A configuration change, min or max, will not be allowed if an existing user password will fall out of the desired range (or become non-compliant). Each of the users preventing the change will be listed in the error message. In this case, each of the users that would become non-compliant would need to have their password lengths changed to fall into the new desired range before the configuration change can be applied.

VLAN

The VLAN Configuration View dialog window shows information about the existing VLANs.

> **Note:** Bypass Relay models affect this feature. For more information, see the section Bypass Relay (BR).
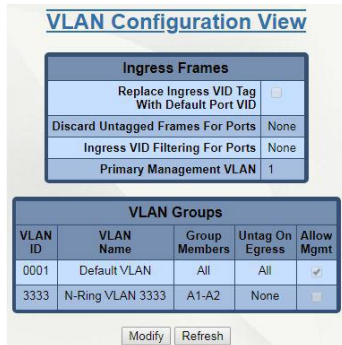
Ingress Frames

Replaces Ingress VID Tag With Default Port VID: Specifies whether or not to replace the VID tag of ingress frames with the port's default VID (PVID).

Discard Untagged Frames For Ports: Specifies whether or not untagged ingress frames are dropped by the selected ports.

Ingress VID Filtering for Ports: Specifies whether or not to filter out ingress frames when a VID violation is detected on the selected ports.

Primary Management VLAN: The default egress VLAN used for communications initiated by the switch i.e. DHCP requests.

VLAN Groups

VLAN ID: Displays the VLAN identification for the group members. The range should be 1 - 4094.

VLAN Name: This field displays the VLAN name, which accepts alphanumeric and only the following special characters (including the period**): # _ - .**

Group Members: This field specifies which ports are members of the VLAN group.

Untag on Egress: Specifies whether or not egress frames are tagged by the port.

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

VLAN Group Members

Port No.: The number of the port.

Port Name: The descriptive name of the port.

Group Member: Specifies whether or not the port is a member of the VLAN group.

Untag on Egress: Specifies whether or not egress frames are tagged by the port.

Click on the *Modify* button and the following VLAN Configuration page will appear:

VLAN Configuration

Ingress Frames								
Show All ▼								
Replace Ingress VID Tag With Default Port VID	☐							
Discard Untagged Frames For Ports	☐A1	☐A2	☐A3	☐A4	☐A5	☐A6	☐A7	☐A8
	☐B1	☐B2	☐B3	☐B4	☐B5	☐B6	☐B7	☐B8
	☐C1	☐C2	☐C3	☐C4	☐C5	☐C6	☐C7	☐C8
	Select All Select None							
Ingress VID Filtering For Ports	☐A1	☐A2	☐A3	☐A4	☐A5	☐A6	☐A7	☐A8
	☐B1	☐B2	☐B3	☐B4	☐B5	☐B6	☐B7	☐B8
	☐C1	☐C2	☐C3	☐C4	☐C5	☐C6	☐C7	☐C8
	Select All Select None							
Primary Management VLAN	1 - Default VLAN ▼							
Update Cancel								

VLAN Groups					
VLAN ID	VLAN Name	Group Members	Untag On Egress	Allow Mgmt	Delete
0001	Default VLAN	All	All	✓	
3333	N-Ring VLAN 3333	A1-A2	None	☐	Delete
Add					

Done Refresh

The top table is used for general VLAN changes. Once the required changes have been made, click on the *Update* button and then go to the Configuration menu and click on the *Save* button to ensure all changes are saved.

The bottom table is where new VLANs are added and existing ones are modified or deleted.Click on the *Add* button in the bottom table and the following dialog window will appear:

VLAN Group Configuration

VLAN Group	
ID	Number
Name	Alphanumeric, #, -, and _
Allow Management	✔
Change PVID Of Member Ports	✔
Remove Ports From Default VLAN When Added To This VLAN	✔

VLAN Group Members			
Show All ▼			
Port No	Port Name	Group Member	Untag On Egress
01	A1	☐	☐
02	A2	☐	☐
03	A3	☐	☐
04	A4	☐	☐
05	A5	☐	☐
06	A6	☐	☐
07	A7	☐	☐
08	A8	☐	☐
09	B1	☐	☐
10	B2	☐	☐
11	B3	☐	☐
12	B4	☐	☐
13	B5	☐	☐
14	B6	☐	☐
15	B7	☐	☐
16	B8	☐	☐
17	C1	☐	☐
18	C2	☐	☐
19	C3	☐	☐
20	C4	☐	☐
21	C5	☐	☐
22	C6	☐	☐
23	C7	☐	☐
24	C8	☐	☐

Update Refresh Cancel
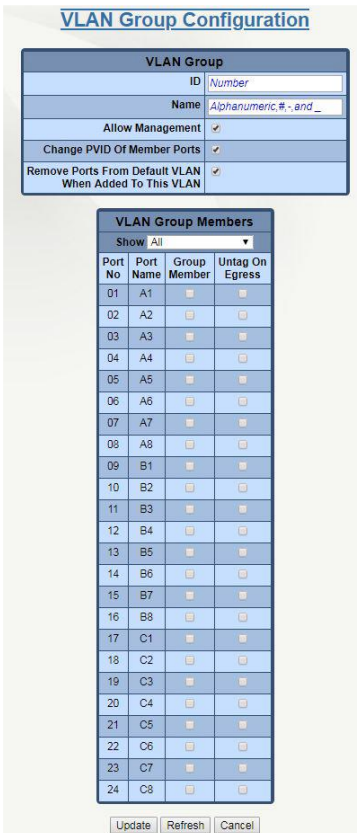
Note: The system is limited to a maximum of 60 configured VLAN groups.
Note: The total number of configured VLAN groups is constrained by system resource usage which varies depending upon network configuration, with VLAN port membership count being the most significant factor.

Note: A port is automatically moved to the Default VLAN if no other VLAN contains that port.
   Once the required changes have been made, click on the *Update* button and then go to the
Configuration menu and click on the *Save* button to ensure all changes are saved.

Help

   The Help menu provides information on monitoring and configuring the manageable parameters of the
device. Specific help can be found by using the left-hand navigation menu or clicking on the Help link in
the top menu.
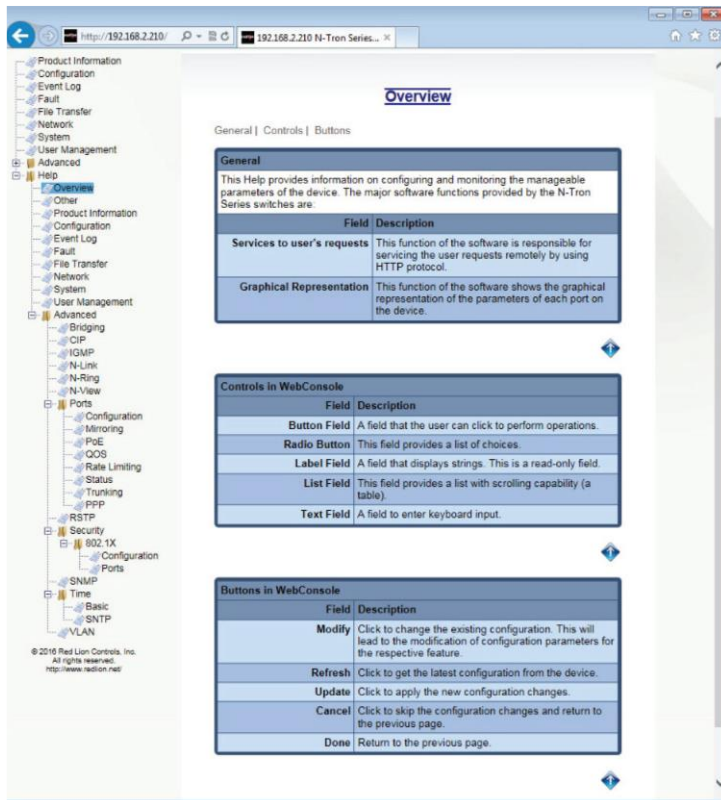
Appendix A

Command Line Interface

The Command Line Interface (CLI) can be accessed by connecting a host device to the USB connector on the switch. Once connected, the switch will appear as a serial connection. A standard terminal application may be used to communicate to the switch through the serial connection. For serial port settings, see the "USB INTERFACE" section of the NT24k® Series Hardware Manual.

There are two additional methods for connecting to the CLI, Telnet and SSH. Using any standard Telnet client, sim-ply enter the IP address of the switch to start a connection to the CLI. SSH, the secure alternative to Telnet, can also be used with any standard SSH client by simply entering the IP address of the switch to start a secure connection to the CLI.

The CLI contains some status and configuration capability. To interact with the CLI, a login is required. The default username and password is 'admin'. Once logged in, a listing of available commands can be obtained through the help interface. This is accessible by typing either "?" or "help?". The following commands are available:

NT24k CLI Commands

COMMAND	ARGUMENTS	DESCRIPTION
?		Show system commands. This command is the same as 'help commands' which is shown below.
admin		Administration settings, including IP settings and DHCP mode.
admin system set		Set general system settings.
admin system set contact	<contactname>	The person to contact for system issues, which should be someone within your organization. Only alphanumeric and special characters '#', '_', and '-' are allowed.
admin system set location	<locationname>	The physical location of the switch. Only alphanumeric and special characters '#', '_', and '-' are allowed.
admin system set name	<switchname>	Contains the name assigned to the device, which allows alphanumeric and special characters '#', '_', '-', and ':' only. When IP Configuration is DHCP, this may be used as the Client ID (Option 61) of the DHCP Request.
admin system set upper Threshold	<upperThreshold> - An integer from -60 to 120.	The highest temperature for the switch without causing a fault to occur. The threshold is specified as an integer in C degrees. The range is from -60 C to 120 C, and the default is product dependent (shown only on switches with temperature sensors).
admin system set lower Threshold	<lowerThreshold> - An integer from -60 to 120.	The lowest temperature for the switch without causing a fault to occur. The threshold is specified as an integer in C degrees. The range is from -60 C to 120 C, and the default is product dependent (shown only on switches with temperature sensors).
admin system show		Show general system information.
admin ip set		Set Internet protocol settings.
admin ip set clientid	<type> - A client ID type: [0-switch name, 1-switch MAC, 2-other text, 3-other hex] <value>	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.

COMMAND	ARGUMENTS	DESCRIPTION
	- A string when the type is 2 or a hex string when the type is 3.	• Usage: admin ip set clientid 0 • Usage: admin ip set clientid 2 "Switch53"
admin ip set dhcp admin ip set no dhcp		Determines the method used to obtain an IP address, Subnet Mask, and Gateway. When DHCP is enabled, DHCP protocols are used to obtain these values. When DHCP is disabled, Static is selected, and the statically configured values are used. • Usage: "admin ip set dhcp" to enable DHCP mode. • Usage: "admin ip set no dhcp" to disable DHCP and return back to Static.
admin ip set ip	[address <ipaddress>] - The IP address of the device. [mask <subnetmask>] - The Subnet mask of the device. [gateway <gateway>] - The Gateway address of the device.	Set the Static IP address, subnet mask, and/or gateway. • Usage: admin ip set ip [address (IP address)] [mask (Subnet mask)] [gateway (Gateway address)] **Example:** CLI> admin ip set ip address 192.168.2.212 mask 255.255.255.0 gateway 192.168.2.1
admin ip show		Show Internet protocol settings. **Example:** CLI> admin ip show
arl		Show ARL Configuration.
arl show		Show ARL Configuration. Example: CLI> arl show Arl Settings Src MAC Address Vlan Sta Drop Blk Loc Destination Ports Applies only to Ports ================ ==== === ==== === === ================ 00:07:af:7d:37:e0 1 Y N N FDB CPU All 01:00:5e:00:00:fb 1 Y N N FDB C7 All 01:00:5e:00:00:fc 1 Y N N FDB C7 All 01:00:5e:7f:ff:fa 1 Y N N FDB C7 All 01:07:af:00:de:d1 ANY Y N N POL CPU A1-A2 01:07:af:00:de:d2 ANY Y N N POL Drop All 01:07:af:00:de:f0 ANY Y N N POL Drop All 01:07:af:00:de:f1 ANY Y N N POL Drop All 01:07:af:00:de:f2 ANY Y N N POL Drop All 01:07:af:00:df:48 ANY Y N N POL Drop All 01:07:af:01:3d:1b ANY Y N N POL CPU All 01:07:af:7d:37:e0 ANY Y N N POL Drop All 01:80:c2:00:00:00 1 Y N Y POL CPU All a0:36:9f:3b:6c:b2 1 N N N FDB C7

COMMAND	ARGUMENTS	DESCRIPTION
		All ff:ff:ff:ff:ff:ff ANY Y N N POL CPU All
arp		Address Resolution display and control.
arp	[<arguments>]	Use arp without arguments to get help. Example: CLI> arp <arp>arguments> - Use arp without arguments to get help. Surround multiple arguments with double quotes. EX: arp "-r 192.168.2.117" CLI> arp NAME arp - address resolution display and control SYNOPSIS arp [-silent] [-V <routetab>] [-i <ifname>] –a arp [-silent] [-V <routetab>] [-i <ifname>] –A arp [-silent] [-V <routetab>] [-i <ifname>] -d <hostaddress> arp [-silent] [-V <routetab>] [-i <ifname>] [-p] [-t] -s <hostaddress> <ether_addr> arp [-silent] [-V <routetab>] [-i <ifname>] -r <hostaddress> DESCRIPTION The arp program displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol. Options: -silent Suppress output. MUST be the first argument. -i <ifname> Specify interface. First one if not specified. -t Temporary ARP entry. -p Public ARP entry (i.e. proxy ARP entry). -r Send an ARP request to the host address. -V <routetab> Specify route table. 0 if not specified. Commands: -a Display the currently existing ARP entries. -A Delete all the ARP entries. -d Delete specified ARP entry. -s Register a ARP entry for a node.
clear		Clear the screen.
config		Save changes to the configuration or reset the configuration to factory defaults.
config reset		Reset configuration settings to factory defaults.
config save		Save current running configuration settings.
dhcpServer		DHCP Server.
dhcpServer status set	<statusValue>	Set DHCP Server status (disabled or enabled).
dhcpServer status show		Show DHCP Server status.
exit		Exit immediate mode. **Example:** CLI> admin ip CLI(admin-ip)> exit CLI>
fileTransfer	tftp server <ip address> transferType	Transfer files to or from the switch.

COMMAND	ARGUMENTS	DESCRIPTION
	\<UpgradeSystem, UpgradeBootLoader, ImportConfig, ExportSavedConfig, ExportEventLog\> [file \<string\>]	
help		Show command help.
help commands		Show system commands. Example: CLI> help commands admin - Administration settings, including IP settings and DHCP mode. arl - Arl Settings arp - Address Resolution Protocol (ARP) clear - Clear the screen config - Save changes to the configuration, or reset switch to factory defaults. dhcpServer - DHCP Server exit - Exit immediate mode fileTransfer - Transfer files help - Show command help history - Show command history lldp - Link Layer Discovery Protocol logout - Log off this system ping - Ping a host. port - Port settings portSecurity - Port Security ppp - Start PPP server (use from serial console only). reboot - Reboot the switch and load the most recently saved configuration. who - Display users currently logged in whoami - Show current user info
help edit		Show editing keys. **Example:** CLI> help edit Available editing keystrokes: Delete current character.......................................Ctrl-d Delete text up to cursor.......................................Ctrl-u Delete from cursor to end of line........................Ctrl-k Move to beginning of line.................................. Ctrl-a Move to end of line...Ctrl-e Get prior command from history........................Ctrl-p Get next command from history........................Ctrl-n Move cursor left... Ctrl-b

COMMAND	ARGUMENTS	DESCRIPTION
		Move cursor right..Ctrl-f Move back one word..Esc-b Move forward one word.....................................Esc-f Convert rest of word to uppercase......................Esc-c Convert rest of word to lowercase......................Esc-l Delete remainder of word..................................Esc-d Delete word up to cursor....................................Ctrl-w Transpose current and previous character.......... Ctrl-t Enter command and return to root prompt......... Ctrl-z Refresh input line.. Ctrl-l
help help		Show command help. **Example:** CLI> help help help - Show command help commands - show system commands edit - Show editing keys
history		Show command history. **Example:** CLI> history 1 admin ip set no dhcp 2 admin ip set ip 192.168.2.212 3 history
history clear		Reset all history.
history enable		Turn history capture on.
history filter		Do not capture repeated input into history.
history info		Information **Example:** CLI> history info 1 admin ip set no dhcp 2 admin ip set ip 192.168.2.212 3 history 3 history info History filter: off History modal : off History ring : on
lldp		Link Layer Discovery Protocol.
lldp mode show		Show LLDP mode.
lldp mode set	disable, enabled, auto	Set LLDP mode.
lldp wakeTime show		Show remaining wake time in auto LLDP mode.
lldp wakeTime send	hours <hours> minutes <minutes>	Send wake time in auto LLDP mode to all switches.
logout		Log off this system.
ping		Ping a host.
ping	[<arguments>]	Use ping without arguments to get help. Surround multiple arguments with double quotes. **Example:** ping "-c 3 192.168.2.121"
port		Port Mirroring configuration display and control.

RED LION®

COMMAND	ARGUMENTS	DESCRIPTION
port config show	<portlist>	Show all port configuration information for the specified ports.
port config show all		Show all port configuration information for all ports on the switch.
port config show basic	[<portlist>]	Show basic port configuration information for the specified ports.
port mirror set		Set Port Mirroring configuration.
port mirror set enable port mirror set no enable		Enable or disable Port Mirroring. Use "no enable" to disable.
port mirror set destination	<port>	Set the destination port for Port Mirroring. For example, "A4".
port mirror set txsource	<portlist>	Set the transmit source ports that are mirrored to the destination port. For example, "A1,A2".
port mirror set rxsource	<portlist>	Set the receive source ports that are mirrored to the destination port. For example, "A1-A3,A6".
port mirror set dataonly port mirror set no dataonly		Set mirrored data only. Use "no dataonly" to disable.
port mirror show		Show Port Mirroring configuration. **Example:** CLI> port mirror show Port Mirroring Settings Mirror Status : Enabled Destination Port : A1 Mirrored Data Only : Enabled Tx Source Ports : None Rx Source Ports : A4
portSecurity		Port Security
portSecurity status set	disabled, learning, locked	Set port security status
portSecurity status show		Show port security status.
portSecurity intruderLog show		Show the contents of the intruder log
portSecurity authList show	[<portlist>]	Show the contents of the authorization list
ppp		Start PPP server (available from the serial console only).
reboot		Reboot the switch and load the most recently saved configuration.
who		Display users currently logged in. **Example:** CLI> who Line User Host(s) Idle Location 00:00:00 admin Console
whoami		Show current user information. **Example:** CLI> whoami

COMMAND	ARGUMENTS	DESCRIPTION
		User name: admin

System Information

Command: admin system show
Description: Show general system information

```
CLI>    admin system show

System Settings

Name                           : NT24k-DR16-DC

Model Name                     : NT24k-DR16

Family Name                    : NT24k

Software Version               : 2.2.3

Build Date                     : Oct 25 2019. 16:36:28

Boot Loader                    : 2.0.7

Copyright                      : Copyright <c> 2013-2019

URL                    : http://www.redlion.net/

Ram Size               : 128 MB

Flash Size             : 64 MB

Internet Protocol (IP) Settings

IP Configuration       : DHCP

DHCP Client ID Type    : Switch Name

DHCP Client ID Data    : N-Tron Series 77:fd:00

Fallback IP Enable     : Enabled

Fallback IP Address    : 192.168.1.201

Fallback IP Subnet     : 255.255.255.0

Fallback IP Gateway    : 0.0.0.0

Current IP Address     : 0.0.0.0

Current Subnet Mask    : 0.0.0.0

Current Gateway Address   : 0.0.0.0

MAC Address            : 00:07:af:77:fd:00

--------

System Up Time         : 0d 04:05:42

System Time            : 2000-01-01 04:05:41 CST (UTC-06:00)

Switch Name            : N-Tron Series 77:fd:00

Switch Contact         : Admin
```

R E D L I O N®

```
Switch Location              : Mobile, AL 36606

--------

Device Temperature           : 50 C, 122 F

Upper Temperature Limit      : 120

Lower Temperature Limit      : -60

CLI>
```

Displaying Port Information

Command: port config show <all|basic> <port-list>
Description: Show general port configuration, similar to what is displayed in the Web Software. The first parameter ("all" or "basic") specifies how much information to show and the port-list parameter can be used to filter the displayed ports. This can be a single port, a range of ports (ex. 1-3) or multiple ranges of ports, separated by a comma. Ports can also be selected by name or by number.

> **Note:** If you want all information for a specific port, or set of ports, simply call **port config show <port-list>**. If you want only basic information, you will need to include "basic" before **<port-list>**.

```
CLI> port config show basic

Port Configuration View

Port Port Port                      Admin    Link    Port  Role Port          PVID
No   Name Description               Status   Status  Speed      State
---- ---- -----------------------  -------  ------  -----  ---- ------------  ----
1    P1   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
2    P2   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
3    P3   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
4    P4   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
5    P5   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
6    P6   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
7    P7   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
8    P8   10/100/1000 Mbps TX Enabled  Up     1000   RSTP Forwarding     1
9    DM1  Not Installed             Enabled  Down   1000   RSTP Not Installed 1
10   DM2  Not Installed             Enabled  Down   1000   RSTP Not Installed 1
11   DM3  Not Installed             Enabled  Down   1000   RSTP Not Installed 1
12   DM4  Not Installed             Enabled  Down   1000   RSTP Not Installed 1

CLI> port config show P1

Port Configuration View

Port Number:           1
Port Name:             P1
Port Description:      10/100/1000 Mbps TX
Admin Status:          Enabled
Link Status:           Down
Auto Nego:             Enabled
Port Speed:            Auto
Duplex Mode:           Auto
Flow Control:          Disabled
Cross Over:            Auto
Role:                  RSTP
Port State:            Discarding
PVID:                  1
Trunk ID:              0
Usage Alarm Low:       0
Usage Alarm High:      100

CLI> port config show basic P1-P2,P5

Port Configuration View

Port Port Port                      Admin    Link    Port  Role Port          PVID
No   Name Description               Status   Status  Speed      State
---- ---- -----------------------  -------  ------  -----  ---- ------------  ----
1    P1   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
2    P2   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1
5    P5   10/100/1000 Mbps TX Enabled  Down   Auto   RSTP Discarding     1

CLI>
```

Setting a Static IP Address

By default, the switch will use the DHCP protocol for IP address assignment. The switch may also be configured to use a static IP address.
Command: admin ip set
Description: Moves the CLI to the IP address settings immediate mode. Typing "?" will provide the command options available here.
Once in the IP immediate mode, it is easy to change the address configuration. Once set, the new configuration must be saved for this change to be retained after a reboot.

```
CLI(admin-ip-set)>> ip address 192.168.2.209 mask 255.255.255.0 gateway 0.0.0.0
CLI(admin-ip-set)>> no dhcp

        +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
        +         Static Settings
        +            IP Address:     192.168.2.209
        +            Subnet Mask:    255.255.255.0
        +            Gateway:        0.0.0.0
        +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
CLI(admin-ip-set)>> exit
CLI> █
```

Performing a File Transfer

File transfers can be initiated through the CLI by using TFTP Protocol.

Command: fileTransfer tftp server <ip address> transferType <UpgradeSystem, UpgradeBootLoader, ImportConfig, ExportSavedConfig, ExportEventLog> [file <string>]

Description: Initiates the file transfer from the CLI.

```
CLI>

CLI> fileTransfer tftp server 192.168.2.1 transferType Upgrade System

CLI> File Transfer: Starting in the background

File Transfer: Please do not turn off power until it's completed

Processing '/ram0/xfr/NT24k_image.tar' will take about 1 minute.

Contents from /ram0/xfr/NT24k_image.tar

file NT24k.image, size 10299280 bytes, 20116 blocks

file NT24k_image.xml, size 1287 bytes, 3 blocks

end of tape encountered, read until eof…

done reading contents


Extracting from /ram0.xfr/NT24k_image.tar

file NT24k.image, size 10299280 bytes, 20116 blocks

extracting file NT24k_image.xml, size 1287 bytes, 3 blocks

end of tape encountered, read until eof…

done extracting tar.

file NT24k_image.xml, size 1287 bytes, 3 blocks

moving file /sffs0/temp/NT24k.image → /sffs0/image/NT24k.image


Stored /sffs0/image/NT24k.image (10299280 bytes) in 1:19.247 (130370
bytes/second)

Done Processing '/ram0/xfr/NT24k_image.tar'. Elapsed time: 1:25.996

File Transfer: Completed

CLI>

CLI> fileTransfer tftp server 192.168.2.1 transferType UpgradeSystem file
NT24k_Image.tar

CLI> File Transfer: Starting in the background

File Transfer: Please do not turn off power until it's completed
```

```
Processing '/ram0/xfr/NT24k_Image.tar' will take about 1 minute.


Contents from /ram0/xfr/NT24k_Image.tar

file NT24k.image, size 10299280 bytes, 20116 blocks

file NT24k_image.xml, size 1287 bytes, 3 blocks

end of tape encountered, read until eof…

done reading contents.


Extracting from/ram0/xfr/NT24k_Image.tar

file NT24k.image, size 10299280 bytes, 20116 blocks

file NT24k_image.xml, size 1287 bytes, 3 blocks

end of tape encountered, read until eof…

done extracting tar.

file NT24k_image.xml, size 1287 bytes, 3 blocks

moving file /sffs0/temp/NT24k.image → /sffs0/image/NT24k.image


Stored /sffs0/image/NT24k.image (10299280 bytes) in 1:19.595 (130370
bytes/second)

Done Processing '/ram0/xfr/NT24k_Image.tar'. Elapsed time: 1:26.333

File Transfer: Completed
```

Saving the Configuration

When configuration changes are made, they are not automatically saved to NVRAM and will be discarded at the next power cycle. Configuration changes must be saved to be retained across power cycles.

Command: config save
Description: Save all current changes to the configuration for use after the next power cycle. If a Configuration Device is installed, the configuration will also be saved to the device.

```
CLI>

CLI> config save

CLI>
```

Appendix B

Working with Configuration Files

Importing a Subset of an XML Configuration File

The XML configuration file may be used to set all of the configurable parameters on a NT24k® switch or to configure a subset of parameters. Setting common parameters across multiple switches can be easily accomplished by creating and importing an abridged configuration file for this purpose.

Appendix C contains an example XML Configuration file. A simple way to start an XML configuration file is to export the existing saved configuration file from the switch and modifying it to meet your new configuration needs.

When creating a configuration file for a subset of available parameters, setting the system configuration mode to *Keep* will maintain the current settings for all parameters other than those explicitly set by the new file being imported. If the system configuration mode is not set to *Keep*, all parameters other than those being set by the configuration file, will be reset to their default setting.

In the example below, the mode is set to Keep so that other switch settings are not reset to defaults. Additional information about the content of the configuration file can be found at the top of any exported configuration file.

```
<SystemConfiguration Mode="Keep"?
  <SystemGroup>
    <SystemConfig>
      <SwitchContact>IT Department Manager</SwitchContact>
      <SwitchLocation>Factory Floor B</SwitchLocation>
    </SystemConfig>
  </SystemGroup>
</SystemConfiguration>
```

Using Port Numbers instead of Port Names

In a configuration file, it is valid to use port numbers instead of names to simplify the sharing of configuration settings. Ports are numbered starting at 1.

Port names may differ between switch models. For example, the NT24k-DR24 uses A1-A8, B1-B8, and C1-C8 and the NT24k-14FX6 uses P1-P8 and FX1-FX6. However the configuration files can reference ports 1-24 for an NT24k and ports 1-14 for an NT24k-14FX6.

In the following example, VLAN 1 is configured for ports 1 through 8 and VLAN 2 is configured for ports 9 through 16. This settings file can be imported into any NT24k switch that supports 16 or more ports. Note that the configuration file must also set the appropriate port PVIDs.

```
<SystemConfiguration Mode="Keep">
  "VlanGroup>
    <IngressDiscardUntagged>None</IngressDisgardUntagged>
    <IngressReplaceVID>Disabled</IngressReplaceVID>
    <IngressVidFilter>None</IngressVidFilter>
    <PrimaryMgmtVlanId>1</PrimaryMgmtVlanId>
    <RemoveportsFromDefaultVlan>Enabled</RemovePortsFromDefaultVlan>
    <TaggedVlans>
      <Vlan>
          <AllowManagement>Enabled</AllowManagement?
          <MemberPorts>1-8</MemberPorts>
          <Name>Default VLAN</Name>
          <UntagEgressPorts>1-8</UntagEgressPorts>
```

REDLION®

```
                <VlanId>1</VlanId>
        </Vlan>
        <Vlan>
                <AllowManagement>Enabled</AllowManagement>
                <MemberPorts>1-8</MemberPorts>
                <Name>Default VLAN</Name>
                <UntagEgressPorts>1-8</UntagEgressPorts>
                <VlanId>1</VlanId>
        </Vlan>
    </TaggedVlans>
    <Type>Tagged</Type>
```

Importing an Incompatible XML Configuration File

Errors related to invalid port names or numbers may occur when importing a configuration file from one model of an NT24k® switch into a different model of an NT24k switch.

Field	Description
Destination	XML line:(216) - Could not set '/SystemConfiguration/MirrorGroup/MirrorConfig/Destination' to value 'P1'
Error Cause	0x80010008 - Invalid Port (ERR_InvalidPort)
ControlPort	XML line:(226) - Could not set '/SystemConfiguration/NLinkGroup/NLinkConfig/ControlPort' to value 'P3'
Error Cause	0x80010008 - Invalid Port (ERR_InvalidPort)
CouplerPort	XML line:(227) - Could not set '/SystemConfiguration/NLinkGroup/NLinkConfig/CouplerPort' to value 'P4'
Error Cause	0x80010008 - Invalid Port (ERR_InvalidPort)
Portx	XML line:(244) - Could not set '/SystemConfiguration/NringGroup/NringConfig/NringPortSets/PortSet/Portx' to value 'P1'
Error Cause	0x80010008 - Invalid Port (ERR_InvalidPort)
Porty	XML line:(245) - Could not set '/SystemConfiguration/NringGroup/NringConfig/NringPortSets/PortSet/Porty' to value 'P2'

Resolving Invalid Port Mappings

If the number of ports in the XML configuration file is greater than on the target model, then the following sections should be removed for each of the extra ports.

- SystemConfiguration/LldpGroup/LldpConfig/LldpPorts/Port
- SystemConfiguration/PoeMgmtGroup/PoeMgmtConfig/PoePorts/Port (PoE models only)
- SystemConfiguration/PortGroup/PortConfig/Ports/Port
- SystemConfiguration/PortSecGroup/PortSecConfig/PortSecList/PortSecEntry
- SystemConfiguration/PtpGroup/PtpConfig/BoundaryClock/PtpPorts/Port (when PTP is licensed)
- SystemConfiguration/PtpGroup/PtpConfig/TransparentClock/PtpPorts/Port (when PTP is licensed)
- SystemConfiguration/RateLimitGroup/RateLimitConfig/RateLimits/Limit
- SystemConfiguration/RstpGroup/RstpConfig/RstpPorts/Port

Notice that if the target switch has additional ports whose settings are not specified in the imported configuration file, then these additional ports will have their settings set to default values if the mode has not been set to "Keep".

Ports on the target switch that do not exist in the configuration file will be added to Default VLAN 1. If the configuration file has extra VLANs with ports that do not exist, an error will be generated for each non-existent port.

Resolving Invalid Port Names

If the port names in the XML configuration file are different than on the target model, then rename the ports for the following sections so that the new names correspond to the intended ports on the target model.

- SystemConfiguration/LldpGroup/LldpConfig/LldpPorts/Port/PortNumber
- SystemConfiguration/MirrorGroup/MirrorConfig/Destination

- SystemConfiguration/NLinkGroup/NLinkConfig/ControlPort

- SystemConfiguration/NLinkGroup/NLinkConfig/CouplerPort

- SystemConfiguration/NringGroup/NringConfig/NringPortSets/Portx

- SystemConfiguration/NringGroup/NringConfig/NringPortSets/Porty

- SystemConfiguration/PoeMgmtGroup/PoeMgmtConfig/PoePorts/PortNumber (PoE models only)

- SystemConfiguration/PortGroup/PortConfig/Ports/Port/PortNumber

- SystemConfiguration/PortSecGroup/PortSecConfig/PortSecList/PortSecEntry/PortNumber

- SystemConfiguration/PtpGroup/PtpConfig/BoundaryClock/PtpPorts/Port/PortNumber (when PTP is licensed)

- SystemConfiguration/PtpGroup/PtpConfig/TransparentClock/PtpPorts/Port/PortNumber (when PTP is licensed)

- SystemConfiguration/RateLimitGroup/RateLimitConfig/RateLimits/Limit/PortNumber

- SystemConfiguration/RstpGroup/RstpConfig/RstpPorts/Port/PortNumber

Depending on the exported values, some of the following sections in the XML configuration file may also need to have their ports renamed.

- SystemConfiguration/BridgingGroup/BridgingConfig/MulticastFilters/PortList

- SystemConfiguration/BridgingGroup/BridgingConfig/UnicastFilters/PortNumber

- SystemConfiguration/IgmpGroup/IgmpConfig/ManualRouterPorts

- SystemConfiguration/IgmpGroup/IgmpConfig/RFilterPorts

- SystemConfiguration/MirrorGroup/MirrorConfig/RxSourcePorts

- SystemConfiguration/MirrorGroup/MirrorConfig/TxSourcePorts

- SystemConfiguration/NViewGroup/NViewConfig/SendAutocastPorts

- SystemConfiguration/NViewGroup/NViewConfig/SendMibStatsPorts

- SystemConfiguration/SecurityDot1xGroup/SecurityDot1xConfig/EnabledPorts

- SystemConfiguration/TrunkGroup/TrunkConfig/Trunks

- SystemConfiguration/VlanGroup/VlanConfig/IngressDiscardUntagged

- SystemConfiguration/VlanGroup/VlanConfig/IngressVidFilterf

- SystemConfiguration/VlanGroup/VlanConfig/TaggedVlans/Vlan/MemberPorts

- SystemConfiguration/VlanGroup/VlanConfig/TaggedVlans/Vlan/UntagEgressPorts

Example Scenarios

MODEL OF EXPORTED CONFIGURATION FILE	TARGET MODEL	EXPECTED RESULTS OF IMPORTING XML CONFIGURATION FILE
NT24k-DR16	NT24k-DR24	Import successful; Last 8 ports on target model will reset to default values if the mode has not been set to "Keep".
NT24k-DR24	NT24k-DR16	Invalid port mappings
NT24k-DR16	NT24k-16TX	Invalid port names
NT24k-DR16	NT24k-8TX	Invalid port mappings and names

REDLION®

Appendix C

XML Configuration File

Factory Defaults

The following is a shortened example of an XML configuration file:

```
<!-- ************************************************************************
    Overview of XML settings for the N-Tron NT24k series switches
    XML settings can be downloaded to a switch to configure the switch.
    There are several top level configuration sections. Each section is optional.
    Common Attributes:
    ******************
    The following attributes are common to all sections. If omitted from a section,
      then the value from the parent section is used. If completely omitted, a
      system default value is used.

    Crc           Optional. This is not used in this release, but may be
                  used in a future release.
    CurSwVer      Optional. String representation of switch version that the
                  settings were exported from.
    Version       Optional. If present, represents the version of the
                  section. If not present, the default value is used instead
                  of being inherited from the parent section.
                  Default = "1".
    MinSwVer      Optional. String representation of switch version. If
                  present, ignore settings for the section if switch
                  software version does not meet minimum requirement.
                  Default = "1.0".
    Mode          Optional. If present, determines the type of action to
                  take on existing data in the section. In the event of a
                  conflict, precedence goes to the deepest level that is
                  explicitly expressed.
                  Possible values:
                  Delete   (Default) Delete all existing data for the
                  section and replace it with the values in this section.
                  Any missing data gets set to factory default values.
                  Keep   Keep existing data, unless new values are specified
                  in this section. A factory default value is used if there
                  is no previously existing data.
    Convert       Optional. If present, determines whether data conversion
                  is performed when necessary.
                  Possible values:
                  Auto   (Default) When a data conversion is determined to
                  be necessary it will be done automatically, without any
                  user intervention.
                  No   Data conversion is not performed, but settings are
                  validated.
    ValidatePorts Optional. If present, determines if port names or numbers,
                  within lists, that are not valid on this device should be
                  ignored or generate an error.
```

RED LION®

```
            Possible values:
            Yes   (Default) Ports are validated.
            No    Invalid ports are ignored.
   Model            Optional. If present, represents the switch model that the
                    settings were exported from.

 Notes:
 ******
 Comments added to this file will not be preserved.
 ********************************************************************** -->
 <!-- **********************************************************************
 SystemConfiguration ***************************************************
********************************************************************** -->
 <SystemConfiguration Model="NT24k-DR16" ValidatePorts="Yes" Convert="Auto"
Mode="Delete" MinSwVer="1.0" Version="2" CurSwVer="1.9.2">
 <BridgingGroup>
     <BridgingConfig>
         <AgingTime>300</AgingTime>
         <EnableIpProbe>Disabled</EnableIpProbe>
         <MulticastFilters></MulticastFilters>
         <UnicastFilters></UnicastFilters>
     </BridgingConfig> </BridgingGroup>
 [ content intentionally omitted ]
 </SystemConfiguration>
```

For a complete example of an XML configuration file, click on the following link:
http://www.redlion.net/resources/software/n-tron-software and refer to section NT24k® Industrial
Ethernet Switches.