



N-Tron® Series NT5000 Gigabit Managed Ethernet Switches

Software Guide | January 2023

LP1183 | Revision A

COPYRIGHT

©2023 Red Lion Controls, Inc. All rights reserved. Red Lion, the Red Lion logo, N-Tron, N-View, N-Ring, and NT24k are trademarks of Red Lion Controls, Inc. All other company and product names are trademarks of their respective owners.

SOFTWARE LICENSE

Software supplied with each Red Lion® product remains the exclusive property of Red Lion. Red Lion grants with each unit a perpetual license to use this software with the express limitations that the software may not be copied or used in any other product for any purpose. It may not be reverse engineered or used for any other purpose other than in and with the computer hardware sold by Red Lion. The software supplied may contain open source software. Please see Appendix D for a complete listing of open source components and licenses.

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

Preface	1
Disclaimer.....	1
Trademark Acknowledgments.....	1
Document History and Related Publications.....	1
Additional Product Information.....	1
Chapter 1 Security Best Practices	3
Introduction.....	3
Default Passwords	3
Admin account/User Passwords.....	3
SNMP v1/v2c Community Names.....	3
Legacy Protocols.....	3
Disabling Unused Protocols.....	3
Chapter 2 Introduction	5
Summary of Features	6
Description of Features.....	7
Alarms and Events.....	7
Bridging and Forwarding.....	8
Configuration Management.....	9
DHCP.....	10
IP Multicast Filtering and Routing.....	10
L2 Redundancy Protocols.....	10
Link Aggregation (Port Trunking).....	11
Link Layer Discovery Protocol.....	11
Network Security.....	12
Port Configuration.....	12
Quality of Service and Traffic Management.....	13
Switch Management.....	14
Traffic Monitoring.....	15
Virtual Local Area Networks.....	15
System Defaults.....	16
Chapter 3 Web Interface	19
Web Browser Support	19
Accessing the Web Software Interface.....	19
First Login.....	19
Login.....	20
Navigation.....	20
Using the Online Help.....	21
Ending a Session.....	21
Logical View.....	22

Chapter 4 Dashboard 23

- Dashboard23
- Quick Start.....24
 - Users24
 - IP.....25
 - Ports.....25
 - Import Config.....25

Chapter 5 System..... 27

- IP Interfaces.....27
 - Interfaces.....27
 - Routes28
 - Status.....29
 - Neighbors30
- System Info31
- Product Info.....32
- Time33
 - Config.....33
 - Time Zone.....34
 - Daylight Saving.....35
 - NTP.....36
- Config.....37
 - Save.....37
 - Restart.....37
 - Factory Defaults37
 - Import38
 - Export.....39
 - Manage39
- Firmware.....40
 - Activate.....40
 - Update FW41
- Diagnostics42
 - CPU Load.....42
 - Ping43
 - Traceroute.....44

Chapter 6 Alarms..... 47

- Alarms47
 - Active.....47
 - History.....47
 - Config.....48
 - Port Alarms.....50
- Syslog.....51

Log.....	51
Config.....	52
Chapter 7 Ports and VLANs	53
Ports.....	53
Status/Config.....	53
Advanced.....	55
Mirroring.....	56
Rate Limiting.....	58
Port Diag.....	59
Utilization	59
Basic Stats.....	60
Detailed Stats.....	61
Cable Diag.....	62
VLANs.....	63
Config.....	63
Advanced.....	65
FDB	66
Entries.....	66
Aging.....	67
Port Learning.....	68
VLAN Learning.....	69
Static Entries.....	69
Link Aggr	70
Status	70
Groups Config	71
Hashing.....	72
LACP Status	73
LACP Config.....	74
LACP Int Status.....	75
LACP Neighbors.....	76
LACP Port Stat.....	77
Chapter 8 Redundancy.....	79
Loop Protection	79
Config.....	79
Ports.....	80
N-Ring™	81
Config.....	81
Port Sets.....	82
Status	83
Spanning Tree (STP).....	84
Bridge Config.....	84

Bridges	85
MSTI VLANs.....	87
CIST Ports.....	88
MSTI Ports	89
Port Status.....	90
Port Statistics.....	91
Chapter 9 Security.....	93
Users	93
Config.....	93
Privileges.....	94
Connections.....	95
User Lockout.....	96
RADIUS.....	97
Config.....	97
Servers.....	98
802.1X Ports.....	100
Config.....	100
Ports.....	102
Port Security.....	107
Ports	107
Detailed Status.....	109
Config.....	110
MAC Addresses.....	111
Chapter 10 Remote Management.....	113
Access.....	113
IP Access Stats.....	113
IP Access Config.....	114
HTTPS	115
Telnet/SSH.....	117
LLDP.....	118
Neighbors	118
Statistics.....	119
Ports	120
Config.....	121
N-View™.....	122
Config.....	122
Ports	123
RMON	124
Statistics.....	124
Stats Config.....	125
History.....	126

History Config.....	127
Alarm.....	128
Events.....	130
Events Config.....	131
SNMP.....	132
Config.....	132
Access (v3).....	133
Views (v3).....	134
Groups (v3)	135
Users (v3).....	136
Communities	138
Trap Sources.....	139
Trap Dest	140
Chapter 11 Traffic Management.....	143
IGMP.....	143
Groups.....	143
Snooping.....	144
VLAN Config.....	145
Port Status.....	147
VLAN Status.....	148
Statistics.....	149
QoS.....	150
Statistics.....	150
Classification	151
Port Policing.....	153
Storm Policing	154
Filters.....	155
PTP	155
Appendix A CLI Commands	157
Introduction.....	157
Initialize (Disable) Mode Commands	160
Enable Mode Commands	163
Configure Mode Commands.....	168
Interface Mode Commands for Port Interfaces.....	176
Interface Mode Commands for VLAN Interfaces	181
Interface Mode Commands for Local Link Aggregation Interfaces	183
Line Terminal Configuration Mode Commands.....	184
Spanning Tree Aggregation Mode Commands.....	186
IPMC Profile Configuration Mode Commands	187
Appendix B Add/Remove a Table Row Using SNMP	189
Adding a New Table Row	189

Removing an Existing Table Row 190
Appendix C Glossary.....191
Appendix D License Agreements.....215

Preface

Disclaimer

Portions of this document are intended solely as an outline of methodologies to be followed during the maintenance and operation of the N-Tron® Series NT5000 Gigabit Managed Ethernet Switches equipment. It is not intended as a step-by-step guide or a complete set of all procedures necessary and sufficient to complete all operations.

While every effort has been made to ensure that this document is complete and accurate at the time of release, the information that it contains is subject to change. Red Lion Controls, Inc. 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.

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™ is a registered trademark of Xerox Corporation.

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

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 and all product updates can be accessed through the Red Lion web site at www.redlion.net/support/documentation.

Additional Product Information

Additional product information can be obtained by contacting the 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 Controls strongly recommends 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	
SNMP v1/v2c	read community	public
SNMP v1/v2c	write community	private
SNMP v1/v2c	trap community	public

Default Passwords

Admin account/User Passwords

The NT5000 ships from the factory with a default **admin** user account. Upon first login a new admin account will be prompted to be created.

Passwords may not be blank and may not be admin. Passwords will be case sensitive. It is recommended that users utilize upper and lower case characters, special characters, and numbers.

SNMP v1/v2c Community Names

The NT5000 ships with default Community Names for SNMP v1/v2c operation. SNMP v1/v2c traffic, per the standard, is neither hashed nor encrypted. Therefore, it is Red Lion's recommendation that customers requiring SNMP use SNMP v3, which offers more secure SNMP communication.

If SNMP v1/v2c is required in your application, Red Lion strongly recommends changing the default SNMP credentials before deployment.

See the [Disabling Unused Protocols](#) section if SNMP will not be used.

Legacy Protocols

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

LEGACY PROTOCOL	SECURE PROTOCOL EQUIVALENT
HTTP	HTTPS
Telnet	SSH

Disabling Unused Protocols

Certain network protocols 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 meet these criteria:

- SNMP
- LLDP

Chapter 2 Introduction

The NT5000 Gigabit Industrial Ethernet Managed switches offer compact, hardened solutions for reliable operation in harsh industrial applications.

Designed for quick installation and ease of use, the NT5000 series includes a modern graphical user interface with a quick start wizard to assist administrators through configuration for fast and easy deployment.

Graphical dashboards and a logical view of the switch provide status and diagnostic information in easy to read color-coded gauges, so network engineers can quickly assess conditions that may disrupt network stability.

The NT5000 rugged feature-set includes:

- Wide operating temperature range from -40 °C to 85 °C (model dependent)
- Redundant power inputs (10-49 VDC)
- Shock: IEC 68-2-27: 200 g @ 10 ms Triaxial; non-operational; panel mounted
- Vibration: IEC 68-2-6: 15 g @ 5-200 Hz Triaxial; operational; panel mounted
- Fast boot (traffic passes <20 seconds)
- Configurable alarm contact
- Configurable bi-color fault status LED
- LED port status indicators
- Reverse polarity protection
- ESD and surge protection

The NT5000 is available in 6, 8, 10, 16 and 18 port configurations.

MODEL	10/100/1000BaseT RJ45 PORTS	DUAL MODE (100/1000Base) SFP PORTS	100Base FIBER PORTS	1000Base FIBER PORTS
NT5006	6			
NT5006-DM2	4	2		
NT5008	8			
NT5008-DM2	6	2		
NT5008-FX2	6		2	
NT5008-GX2	6			2
NT5010-DM2	8	2		
NT5010-FX2	8		2	
NT5010-GX2	8			2
NT5016	16			
NT5018-DM2	16	2		
NT5018-FX2	16		2	
NT5018-GX2	16			2

Visit www.redlion.net for detailed model specifications .

Summary of Features

FEATURE	DESCRIPTION
Alarms and Events	Supports Alarms, Alarm Relay Contact, Event Logging, and Syslog
Bridging and Forwarding	IEEE 802.1D/802.1Q transparent bridging Dynamic data switching Store-and-forward wire-speed switching Frame buffering MAC address learning <ul style="list-style-type: none"> • Configurable aging time or aging disable • Per-port learning modes: auto, disabled, secure (static only) • Learning-disabled VLANs MAC address table capacity up to: <ul style="list-style-type: none"> • 4K MAC addresses on 6, 8, and 10-port models, 8K MAC addresses on 16 and 18-port models • 64 static MAC addresses
Configuration Management	<ul style="list-style-type: none"> • Save, restore, activate, and delete configurations • Reset factory defaults • Import and export configurations
DHCP	DHCP IPv4 Client
Diagnostics	Front panel view: browser displays port and LED status Ping and traceroute VeriPHY cable diagnostics
IP Multicast Filtering and Routing	IGMP: IPv4 Internet Group Management Protocol <ul style="list-style-type: none"> • IGMPv1 (IETF RFC 1112) • IGMPv2 (IETF RFC 2236) • IGMPv3 (IETF RFC 3376) Options <ul style="list-style-type: none"> • Snooping, Querier, Proxy, Leave Proxy • Control of unregistered multicast flooding
L2 Redundancy Protocols	Spanning Tree Protocols <ul style="list-style-type: none"> • STP • RSTP • MSTP Ring Protocol <ul style="list-style-type: none"> • N-Ring™ automember Loop Protection
Link Aggregation (Port Trunking)	Supports static or dynamic port groups (LACP). The capacity of Link Aggregation Groups is up to 1/2 the device port count. Configurable destination port selection algorithm
Link Layer Discovery Protocol	LLDP advertises information about a device and neighboring devices.
Maintenance	Restart Reset to factory defaults Firmware upgrade Active and alternative firmware images
Network Security	Port Security <ul style="list-style-type: none"> • Limits the number of MAC addresses using a port
Port Configuration	Configurable <ul style="list-style-type: none"> • Port enable/disable • Speed • Duplex • Flow Control • Priority Flow Control (on 6, 8, and 10-port models) • Maximum Frame Size • Excessive Collision Mode

FEATURE	DESCRIPTION
	<ul style="list-style-type: none"> • Frame Length Check • Port Description
Quality of Service and Traffic Management	CoS (IEEE 802.1Q) and Differentiated Services (DiffServ/DSCP) Ingress Port Frame Classification Ingress Port Policing (rate limiting, flow control) DSCP-Based QoS Storm Policing (control storming of broadcast, multicast, and unknown unicast) Filters PTP
Switch Management and Security	Management Interfaces <ul style="list-style-type: none"> • Console port session with automatic logout after inactivity • IPv4 access • Up to 4 Telnet and SSH sessions with automatic logout after inactivity • Up to 20 HTTP and HTTPS sessions • SNMP v1, v2c, and v3 • Access managed by user's VLAN and IP address Date and Time <ul style="list-style-type: none"> • Manual or NTP (Network Time Protocol) • Time Zone and Daylight Saving Time User Management <ul style="list-style-type: none"> • Up to 20 user accounts • Users are assigned to one of 15 privilege levels • Privilege levels grant access to specific switch features SNMP Security <ul style="list-style-type: none"> • SNMPv2 community strings • SNMPv3 users with MD5 or SHA passwords RMON <ul style="list-style-type: none"> • Statistics, history, alarms, and events System Information Contact, name, and location RADIUS authentication 802.1X port security
Traffic Monitoring	Port Mirroring <ul style="list-style-type: none"> • Mirrors frames from one or more ingress port to an analysis port • Rmirror: Remote mirroring access across switches
Virtual Local Area Networks	IEEE 802.1Q VLAN IDs from 1 to 4094 Management Access VLANs Standard VLAN tagging Learning-disabled VLANs

Description of Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from overwhelming the network. VLANs provide traffic security and efficient use of network bandwidth. CoS priority queuing ensures the minimum delay for moving real-time multimedia data across the network, while IP multicast filtering and routing provides support for real-time network applications.

Some of the key features are briefly described in the following sections.

Alarms and Events

Alarm and Event Logging

The switch logs alarms and important system events as they occur and can be viewed or configured via the switches web page.

Active: Displays active alarms. An alarm is considered active while it remains present. Once an alarm is cleared, then it will no longer be displayed in the active list.

History: Displays the alarms that have occurred during the system uptime. These include active and cleared alarms.

Configuring

Config general alarms: Configure the alarms and relay operation. Allows the user to set the alarm indicators to use if a specific alarm occurs. The relay allows the user to connect an external device to indicate an alarm occurred.

Configure Port Alarms: Each port can be configured with a low and high utilization threshold. An alarm is triggered when the activity is no longer in the specified threshold range.

Alarms and Alarm Relay Contact

Certain system events (such as a port going link down or loss of a power input) can be configured to trigger an alarm. Alarms engage the Alarm Relay Contact on the exterior of the switch and are displayed on the web interface.

Syslog

The Syslog protocol, as specified in RFC-3164 and RFC-5424, allows sending system events to a remote logging device, known as a Syslog Collector or Server.

Log

The log contains a record of events that occur during uptime. The log is RAM based and is therefore empty after a reset.

The log level can be configured to show the specific events of the selected severity, or all of the events.

The messages stored in the log can be cleared manually. Clearing a specific level is accomplished by first setting the level to clear and then performing a clear operation. A message is logged to indicate when and who cleared the events.

Config: Configure to send messages to an external syslog collector.

Bridging and Forwarding

The switch supports IEEE 802.1D/802.1Q transparent bridging.

MAC Address Table

A MAC address table facilitates data switching by learning MAC addresses on specific interfaces (ports and VLANs), and filtering or forwarding traffic based on this information. The address table is commonly called an FDB (forwarding database), an ARL (address resolution logic) table, or a FIB (forwarding information base).

MAC Learning

Normally, a given MAC address is learned on a particular interface (VLAN and port). This happens every time a frame enters the port with the given MAC address set as the **source** address. The MAC/VLAN/Port combination is stored in the MAC address table.

When a frame enters the switch the **destination** MAC address in the frame is checked against the table and the frame is forwarded to the appropriate port. If the destination MAC is not in the table, then the frame is forwarded to all ports in the VLAN.

Aging Time

The configurable Aging Time determines how long that MAC will remain in the table. If the MAC is not seen again on that interface, then after the aging time elapses, the MAC is removed (aged out) from the table. When aging is disabled, a learned MAC is never aged out.

Port MAC Learning Mode

The MAC learning mode of a port can be one of three modes.

- **Auto:** MACs are learned automatically when an unknown source MAC is seen. This is the default mode.
- **Disable:** Learning is disabled for all MACs. No source MAC entering the port is learned and traffic sent to that MAC therefore floods to ports in the VLAN.
- **Secure:** Learning is disabled for all MACs, except for MACs in the Static MAC Address Table. This allows traffic to flow to only authorized MACs on authorized ports.

Learning-disabled VLANs

If learning is disabled on a VLAN, then no source MAC addresses arriving on that VLAN are stored in the MAC address table. As a result, all frames entering a port in the VLAN will forward to every port in that VLAN. The only exception would be any static MAC addresses.

Static MAC Addresses

A static MAC address can be assigned to a specific interface on the switch. A static address will not be learned dynamically on any other interface. As a result, all traffic having that particular MAC destination will forward only to the assigned interface. Static addresses can be used to provide network security by restricting traffic for a known host to a specific interface or to ensure that a MAC destination is always known to the switch even if traffic from the device is rarely seen on that interface.

Store-and-Forward and Buffering

The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been checked for corruption using a cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping egressing frames on congested ports, the switch queues up frame buffers and transmits them when able within the limits of the available frame buffers.

Configuration Management

A switch configuration consists of all the options that can be modified by a user. A user with the appropriate privilege can:

- Modify the configuration and apply changes dynamically to the switch
- Save the current configuration to a persistent file so that this configuration is applied when the switch reboots
- Restore the current configuration to the last saved configuration
- Reset the configuration to factory defaults
- Export the configuration to a computer where it can be edited
- Import a configuration

This switch can manage multiple configurations (maximum of 10). This includes creating, deleting, and activating (applying) configurations.

An imported configuration can be saved as a new configuration or it can replace or be merged into an existing configuration.

The running-config is not persistent. It is the currently active configuration and can be modified and saved as the new startup-config.

This switch begins with two persistent configurations:

- startup-config: this configuration is applied at boot up. It is copied to the running-config.
- default-config: this is the factory default configuration and can never be modified.

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).

This switch can be configured as a:

- DHCP client

DHCP Client

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

DHCP Option 61 allows a client to specify its unique client identifier. A server can assign a unique IP address to the client based on this identifier.

IP Multicast Filtering and Routing

IGMP

IGMP (Internet Group Management Protocol) is a protocol that manages how multicast traffic is routed across a network. Without IGMP, all multicast traffic is forwarded across the entire network. With IGMP, an IGMP-aware client can request specific multicast group data from a data provider. An IGMP-aware router or switch can intelligently route the multicast traffic from the data provider to only the ports where the clients are connected. This reduces unneeded network traffic.

IGMP Snooping

When IGMP Snooping (for IPv4) is enabled on an interface, the switch snoops IGMP protocol traffic to route the multicast traffic. Various options are configurable including:

- IGMP version
- IGMP mode: Snooping, Querier, Proxy, and Leave Proxy
- Allowing or disallowing the flooding of unregistered multicast traffic.

Multicast Static Routing

Multicast traffic may be routed to specific ports via an entry in the Static MAC table. This ensures that a client will receive multicast data, even if it does not support the IGMP protocol.

L2 Redundancy Protocols

This switch can be connected to other devices using a Spanning Tree Protocol or N-Ring™. A Loop Protection protocol can be enabled to detect network loops and shutdown and/or log this event.

Spanning Tree Protocols

STP establishes a simple connected active network topology (a spanning tree) from the arbitrary connections between the bridges (switches) of a bridged network. STP will set some ports to forwarding and others to blocking to prevent network loops. The bridges in the network will exchange sufficient information to automatically derive the spanning tree.

The switch supports these spanning tree protocols:

- **Spanning Tree Protocol (STP, IEEE 802.1D and IEEE 802.1Q-2014):** This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. If the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.
- **Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w and IEEE 802.1Q-2014):** This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but will still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.
- **Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s and IEEE 802.1Q-2005):** This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP). MSTP will interoperate with RSTP and STP devices.

N-Ring™

N-Ring is designed for easy setup. Switches are configured for N-Ring membership, by default. 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. An N-Ring Manager capable switch (700, 7000, NT24k®) must be configured for the protocol to work. 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.

Loop Protection

Loop protection is a protocol that sends frames (PDUs) out selected ports and listens for these PDUs to detect when there is a loop in a connected network. If a loop is found, this event can be logged and the port can be shutdown for a configurable amount of time.

Link Aggregation (Port Trunking)

Multiple ports can be combined (aggregated) into a group that behaves like a single connection. Groups can be manually set up or dynamically configured using the Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by redistributing the load if a port in the group should fail.

Link Layer Discovery Protocol

LLDP is specified by IEEE 802.1AB and IEEE 802.3-2012. LLDP is used by networking devices to advertise their identity, capabilities, and to determine their neighboring devices. It can be used by other applications and protocols to discover a network's topology.

Network Security

Port Security

Port Security limits which devices can communicate through the port by examining the source MAC address on frames.

On this switch, each port can be configured to allow traffic from 0 to 1023 unique source MAC addresses. When this number is exceeded, the violating frame is simply dropped, the port can be shutdown (and re-enabled later), or some additional quota of source MAC addresses can be used for a limited time.

Port Configuration

Each port on the switch can be configured to support different modes of operation. You can configure:

- Administrative Status
- Auto-Negotiation or Speed plus Duplex Mode
- Flow Control
- Priority Flow Control (on 6, 8, and 10-port models)
- Maximum Frame Size
- Excessive Collision Mode
- Frame Length Check
- Port Description
- PVID
- Fastboot

Administrative Status

The Admin Status allows a port to be disabled so that no traffic can enter or leave the port.

Auto-Negotiation

In Auto-Negotiation mode, two connected ports automatically detect and use the best speed and duplex mode that they have in common. Both ports should have auto-negotiation enabled.

Full-Duplex

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

Use full-duplex mode on ports whenever possible to double the throughput of switch connections.

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 (when 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.

Flow Control

Flow control may be enabled to pause network traffic during periods when port buffering thresholds are exceeded. It is intended to prevent loss of packets. Flow control is based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

Flow control is generally left disabled in favor of using modern protocols and traffic management techniques (like QoS and packet resends). However, it may be very helpful when configuring ports that communicate with a single end device that has limited traffic processing capabilities.

Priority Flow Control

PFC (IEEE 802.1Qbb) is supported on 6, 8, and 10-port models and is similar to Flow Control, but it can be enabled per CoS priority in the entering frames. Traffic can be paused for some CoS priorities and not for others.

Maximum Frame Size

This is the maximum frame size allowed for this port, including the FCS field. This is related to the MTU, but not the same value.

Excessive Collision Mode

When sending a frame, if there is a collision on the link, after 16 collisions the frame will be discarded.

Frame Length Check

If the length of the frame does not match the length field in the frame, then the frame is dropped. This can be used to eliminate corrupt or malicious frames.

Port Description

A user friendly description can be assigned to this port.

PVID

VLAN ID associated to a port.

Fastboot

Fastboot allows a port to pass traffic through the switch within a few seconds of boot up, before protocols have been initialized.

Quality of Service and Traffic Management

QoS is a general term referring to various mechanisms that manage the priority and resources available to critical network traffic. It is particularly important for time-critical traffic, especially when a network is congested. The switch supports a rich set of features for managing QoS.

QoS Through Prioritization

QoS can 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 high resolution images and Voice over IP. Since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource. Prioritization helps to ensure that time-sensitive traffic is given preference over less critical traffic when a network is congested. QoS mechanisms are not required in the absence of network congestion.

QoS is typically implemented by categorizing traffic into 8 priority levels and by assigning a drop precedence which indicates whether a frame at a given priority may be dropped when traffic is congested.

The 8 priority levels correspond to 8 priority **queues** in the switch hardware.

QoS Through Rate Limiting

Rate Limiting controls the maximum rate of (non-critical) traffic transmitted or received on an interface. Rate limiting may be configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that exceeds the acceptable rate can be dropped or subjected to further filtering.

Ingress Prioritization

For incoming traffic, the switch prioritizes traffic using CoS values and ToS/DiffServ values.

- **CoS:** The priority of an L2 frame can be specified by the IEEE 802.1p value inside an 802.1Q VLAN tag of an Ethernet frame. This is commonly known as the Class of Service (CoS).
- **ToS/DiffServ:** The priority of an L3 IP packet can be specified by the ToS/DiffServ field in the IP header. This field may have different values known as ToS (Type of Service), IP Precedence, or DSCP (Differentiated Services Codepoint) values.
- **Default Classification:** The priority of all incoming traffic on a port can be set to a default value.
- **Remapped CoS Classification:** The priority of incoming traffic can also be remapped through a table that converts the frame's CoS priority into a different priority.

Policing

A policer manages excessive rates of ingress traffic. It can limit traffic at a port level. It can drop traffic or enable flow control.

Storm Policing

Storm Policing can block or rate limit traffic that is broadcast, unknown unicast, or multicast.

Switch Management

These are the various methods and protocols used to configure and monitor the switch.

Management Interfaces

Secure management interfaces are available and unsecured interfaces are provided for backwards compatibility with less secure clients. Management access can be limited to specific IP addresses.

A command line interface is available through the Console port on the exterior of the switch, and through the Secured Shell (SSH) and unsecured Telnet network protocols.

A graphical interface is available over the Hypertext Transfer Protocol Secure (HTTPS) and the unsecured Hypertext Transfer Protocol (HTTP).

Available management protocols which cooperate with external applications include Simple Network Management Protocol (SNMP), Remote Network Monitoring (RMON), and N-View™.

User Management

User accounts can be created to manage access to the management interfaces and to manage the privileges available to a user. Each user is assigned to a specific privilege level. The privilege level grants the user specific permissions to view and modify the switch configuration and to view and modify status information.

Date and Time

The date and time can be set manually or dynamically by enabling NTP (Network Time Protocol) which takes its time from an NTP server. The time can be further configured to a specific Time Zone and for a specific Daylight Saving Time adjustment.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used to monitor and manage the switch. This switch supports SNMPv1, v2c, and v3. In short, SNMPv2c adds performance and error-handling improvements and SNMPv3 adds authentication and encrypts SNMP network traffic.

The switch supports sending traps (notifications) to SNMP Trap Stations. The SNMP traps are: Cold Start, Warm Start, Link Up, Link Down, Authentication Failure, Entity Configuration Change, New Root, Topology Change, LLDP Remote Tables Change, Rising Alarm, Falling Alarm, Alarm Trap Status, IP Trap Interfaces Link, Port Security Trap Globals Main, Port Security Trap Interface. SNMP Traps are sent to all trap stations when the corresponding trap is enabled.

RMON

RMON (Remote Networking Monitoring) is a protocol that allows the switch to send specific data to an RMON application. The application uses this data to monitor traffic and analyze protocols on the LAN.

The RMON groups supported by the switch are statistics, history, alarm, and event.

N-View™

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

Traffic Monitoring

Port Mirroring

The switch can unobtrusively mirror (copy and transmit) traffic from any port to a designated analysis port. A protocol analyzer or RMON probe can be attached to the latter port to perform traffic analysis, such as verifying connection integrity. This is typically used to troubleshoot and debug a network, and is disabled during normal operations.

This switch supports standard port mirroring where the source port and analysis port are on the same switch. It also supports remote mirroring which directs the mirrored traffic to an analysis port on a different switch. This port is called a reflector port and it is tied to a specific VLAN.

Virtual Local Area Networks

Overview of VLANs

VLANs (Virtual Local Area Networks) facilitate easy administration of logical groups of devices that can communicate as if they were physically on the same LAN. A port can be assigned to one or more specified VLANs. The switch forwards traffic (broadcast, multicast, or unicast) only between ports that belong to the same VLAN.

The switch supports tagged VLANs as specified by IEEE 802.1Q. A frame entering the switch can have a VLAN tag or a default VLAN can be applied to it. Any traffic entering a port can be discarded if it does not have a VLAN tag that matches a port's VLAN membership. Traffic leaving the switch can be configured to have a VLAN tag or be untagged.

By default, all ports belong to VLAN 1 (VID=1) and are set to untag the frame on egress.

By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the physical network wiring.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- Use protocol-based VLANs to assign traffic of a specific protocol to a specific VLAN.

- Use VLAN translation to replace a specific VLAN ID of incoming traffic with a different VLAN ID.
- Use private VLANs (port isolation) to restrict a group of ports to have one common uplink port. These ports cannot send or receive traffic between themselves (they are isolated from each other); they may only exchange traffic with the designated uplink port.

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 port VLAN ID (PVID) setting. If an incoming frame is untagged and untagged frames are being accepted, then that frame may be assigned to the port VLAN ID. Subsequent switch routing and treatment will be in accordance with that VLAN. 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 are untagged, thus not requiring external devices to be VLAN cognizant.

Port VLAN Modes

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 specific ports. This membership determines whether a port is included or excluded regarding frame egress from the switch.

Overlapping VLANs give the user the ability to have one or more ports share two or more VLAN groups. For information and examples on implementation, refer to [VLAN Configuration](#).

System Defaults

The switch's default configuration can be restored using the web interface or CLI. Under the web menu item System → Config → Factory Defaults, enable or disable any of the factory reset options as desired and click the Factory Defaults button to reset the configuration. The CLI command "reload defaults" will do the same.

The following table lists some of the basic system defaults.

FUNCTION	PARAMETER	DEFAULT
Console Port Connection	Baud Rate Data bits Stop bits Parity Flow Control Local Console Timeout	115200 bps 8 1 None None 10 minutes
IP Settings	Management Access VLAN IP Address DHCP	VLAN 1 DHCP Client: Enabled Fallback IP Address: 192.168.1.201 Netmask: 255.255.255.0
Switch Authentication	Default user name Default password	Username "admin" There is no default password Admin account must be changed on first login

FUNCTION	PARAMETER	DEFAULT
Switch Management	SSH Telnet HTTPS HTTP IP Access Management SNMP SNMP Communities SNMP Users SNMP Groups SNMP Views SNMP Access	Enabled Disabled Enabled Disabled Disabled Enabled public, private default_ro_group
Port Configuration	Speed Flow Control Maximum Frame Size Excessive Collision Mode Frame Length Check	Auto Disabled 10240 Discard Disabled
Link Aggregation (Port Trunking)	Static Groups LACP (all ports)	None Disabled
Quality of Service	Storm Policing Port Policing	Disabled Disabled
MAC Address Table	Aging Time	300 seconds
L2 Redundancy Protocols	Spanning Tree N-Ring™ Loop Protection	MSTP Enabled on all ports Enabled Disabled
LLDP	Mode	Enabled
Virtual LANs	Default VLAN PVID Acceptable Frame Type Ingress Filtering	1 1 All Enabled
IP Multicast Filtering and Routing	IGMP Snooping	Enabled
Alarms and Events	Logging Port Link Down Alarms Power Alarm Syslog	Enabled Disabled Disabled Disabled
NTP	Clock Synchronization	Disabled

Chapter 3 Web Interface

This chapter describes using the Red Lion Controls NT5000 switch web interface and presents the menu tree view broken down into major functional groups.

The switches are password protected by a login security system. You can login to the switch with the user name and password provided below.

All of the switches have the same default user name (admin) and there is no default password. You are required to change the admin account and password at the first log in. Additional user accounts can be added and configured to have different privilege levels.

Web Browser Support

IE 7 (or newer version) with the following default settings is recommended:

Language Script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Unicode (UTF-8)
Text size	Medium

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

Google Chrome with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

Accessing the Web Software Interface

Launch a web browser and enter the IP address of the device into the address bar, 192.168.1.201 is the fallback address.

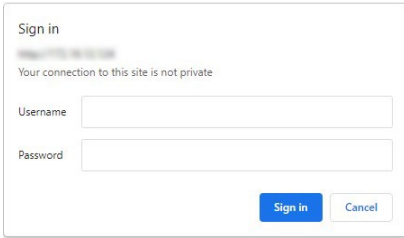
First Login

When logging in for the first time using the default credentials, you will be prompted to change the admin account name and password.

Initial Default Username	admin
Initial Default Password	No password required

Login

The following login screen will appear:



Sign in

Your connection to this site is not private

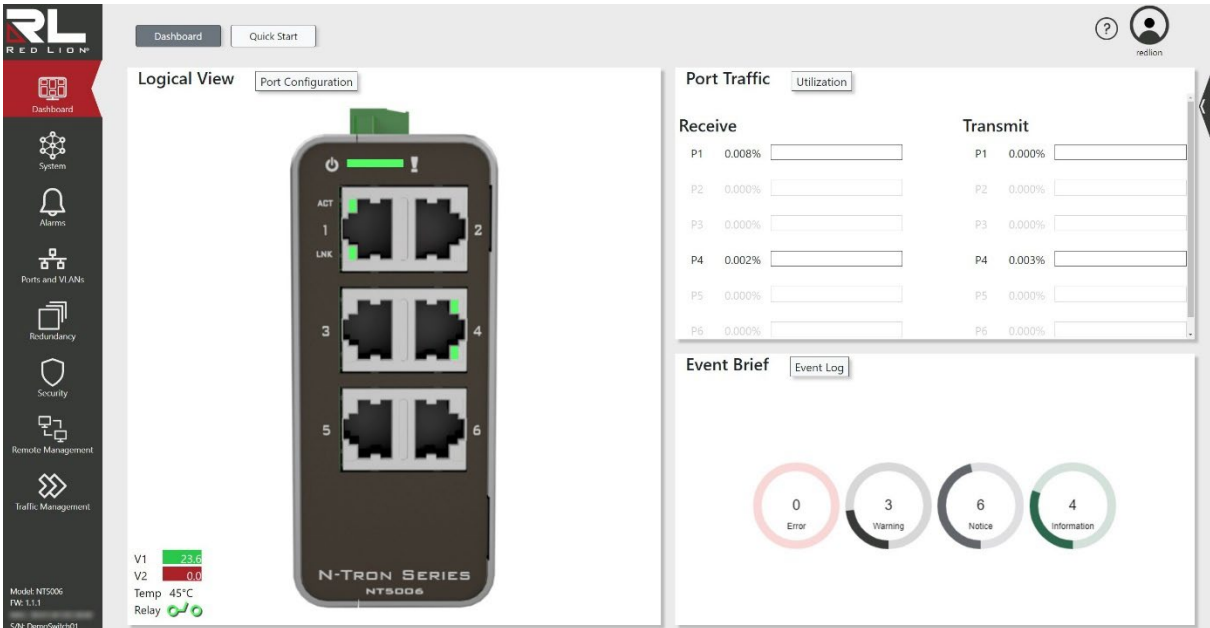
Username

Password

Username: Login user name. The maximum length is 31 characters.

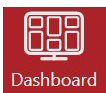
Password: Login password. The default minimum length is 3 characters. The maximum length is 31 characters.

Upon successful login, a screen similar to the one below will appear.



Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the eight main icons in the menu tree on the left side of the system home screen:



Dashboard: Displays the dashboard showing: logical view, traffic usage, alarm and event notifications. Clicking the Quick Start button displays the startup wizard to quickly set the Users, IP, and Ports.



System: Configure the system, restart the system, save, import and export settings, factory reset, firmware upgrade, and image selection.



Alarms: Configure alarms and events, view the log.



Ports and VLANs: Configure ports, VLANs, FDB, and link aggregation.



Redundancy: Configure loop protection, N-Ring™, and STP.



Security: Configure switch users, RADIUS, 802.1X, and port security.



Remote Management: Configure access, LLDP, N-View™, RMON, and SNMP.



Traffic Management: Configure IGMP and QoS.

At the bottom of this list of icons is system information showing the Model, Firmware (FW), MAC Address, and Serial Number (S/N). You can find more detailed information by navigating to the help link “?” located at the top-right of the screen.

Using the Online Help



Each screen has a Help page containing information relevant to the current screen. The help pages are displayed in a modal that can be detached to a separate browser window. Clickable links are also available to open the tech support website and email tech support. To close a help page, simply close the containing window. Each web interface page has a corresponding help page.

Ending a Session

A user must click on “User Name” → Logout and close the web browser to end a session. This prevents unauthorized access to the system with the user’s login name and password.

Logical View

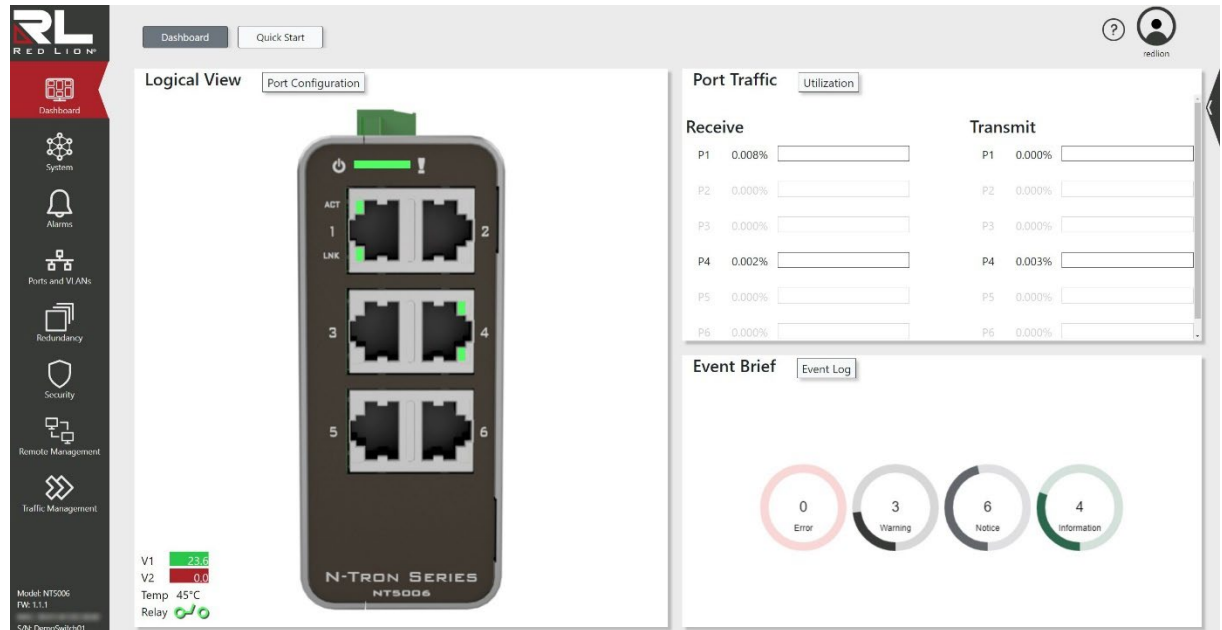


The logical view displays the real status of the system's panel. It can be accessed from the Dashboard and also on any other page by clicking on the left chevron icon at the upper left side of the interface.

Chapter 4 Dashboard

This chapter lists the Dashboard related functions available for Red Lion Controls NT5000 switch models.

Dashboard



This page shows an at-a-glance overview of the switch's port status and traffic, as well as any events that occur.

Logical View

This box shows an image of the switch with lights indicating each individual port's status. The display also gives information about power, temperature, and contact relay.

Clicking on **Port Configuration** takes you to the Ports and VLANs > Ports > Status/Config page.

Port Traffic

This box shows an overview of traffic on each individual port as a percentage of total traffic.

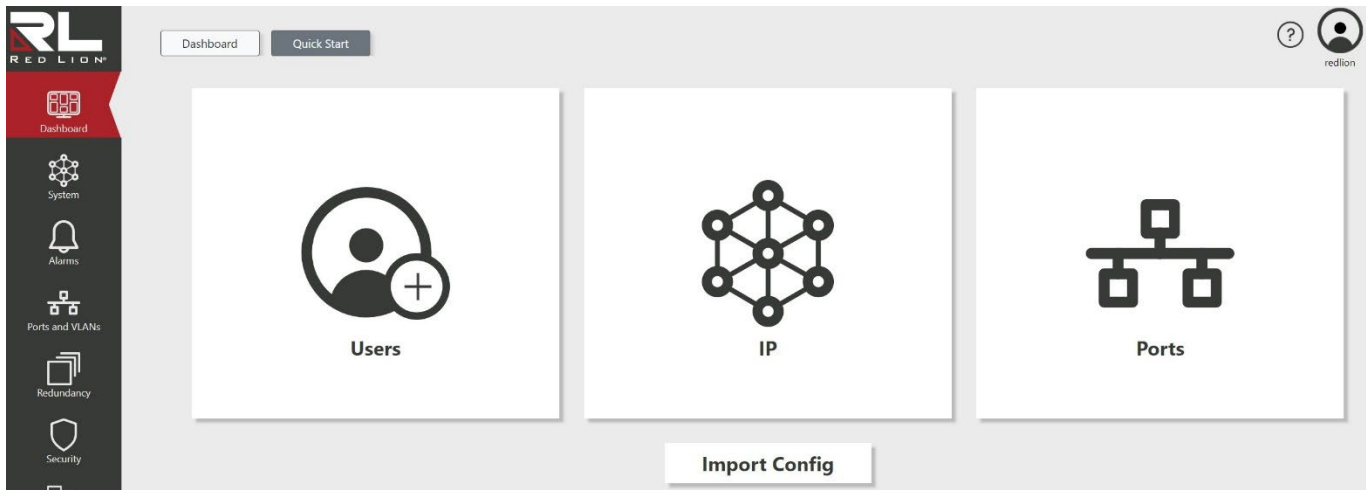
Clicking on **Utilization** takes you to the Ports and VLANs > Port Diag > Utilization page.

Event Brief

This box shows the number of alarm events at four different severity levels: Error, Warning, Notice, and Information. Each has a circle graph representing the ratio of instances of events at that severity level compared to the total number of events.

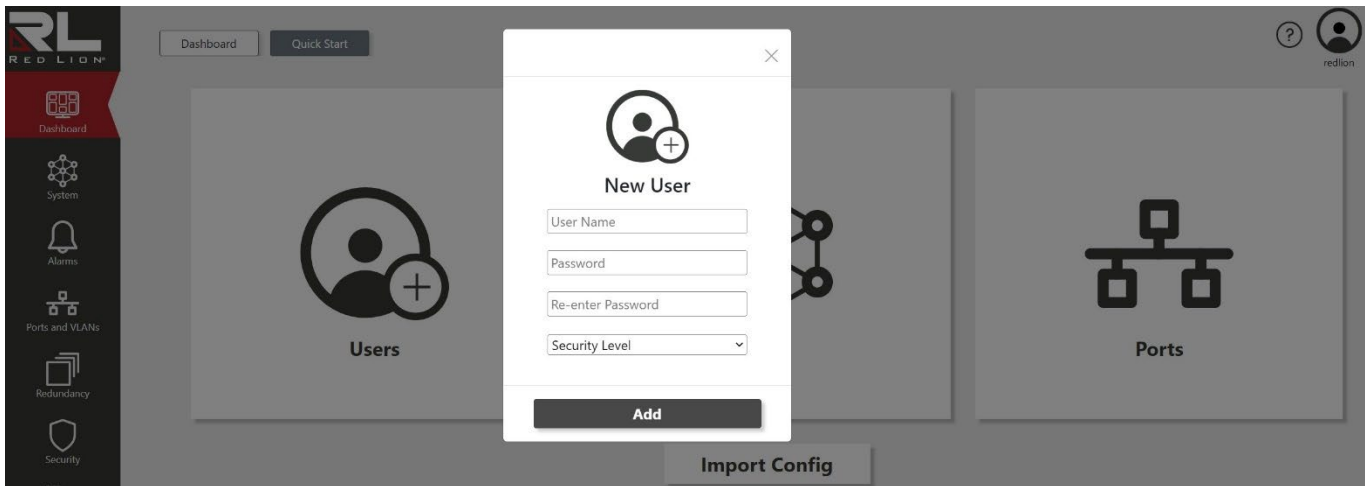
Clicking on **Event Log** takes you to the Alarms > Syslog > Log page.

Quick Start



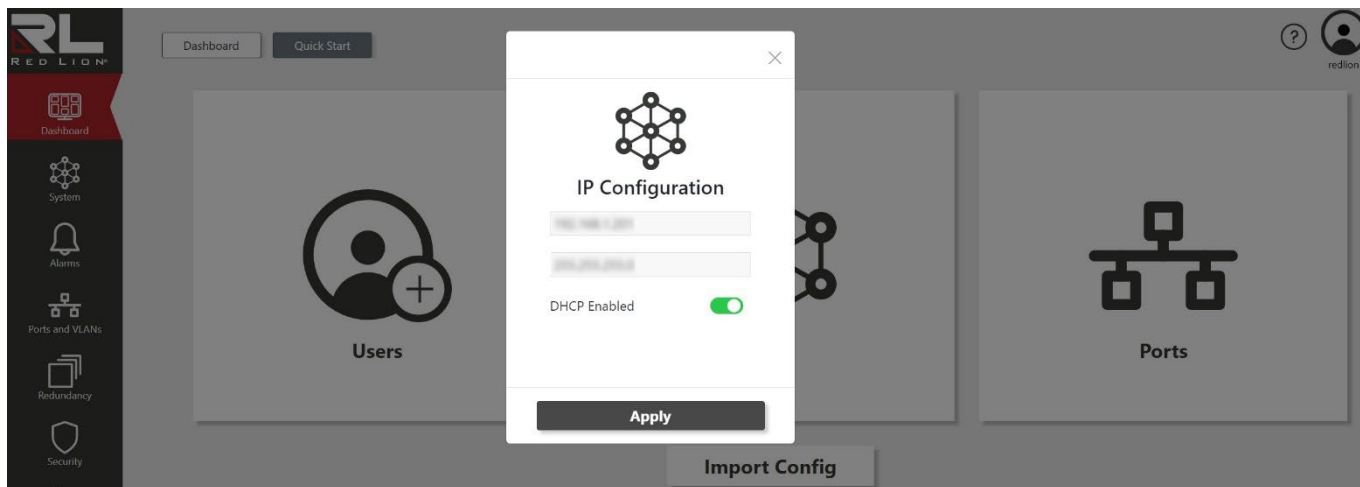
This page contains shortcuts to some first steps in the setup process that will allow you to get up-and-running quickly with the switch.

Users



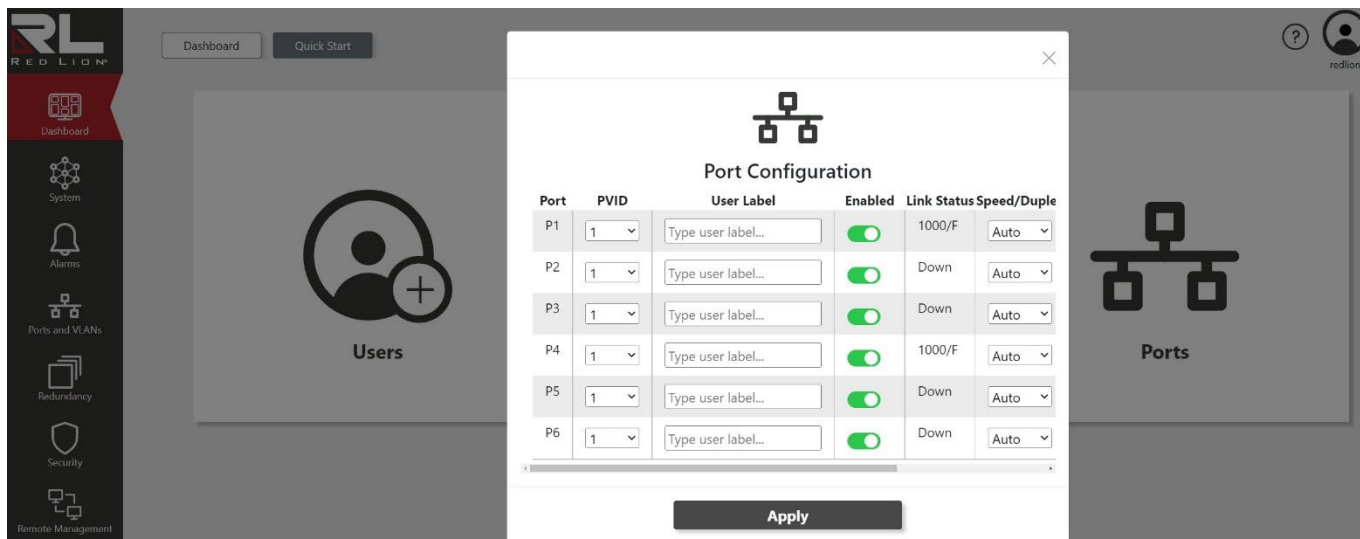
Clicking on this section opens up a pop-up window that allows you to add a new user, entering credentials such as the username, password, re-entering the password, and user security level.

IP



Clicking on this section opens up a pop-up window that allows you to configure the switch's IP address, subnet mask, and whether or not DHCP is enabled.

Ports



Clicking on this section opens up a pop-up window that allows you to configure the switch's ports.

Import Config

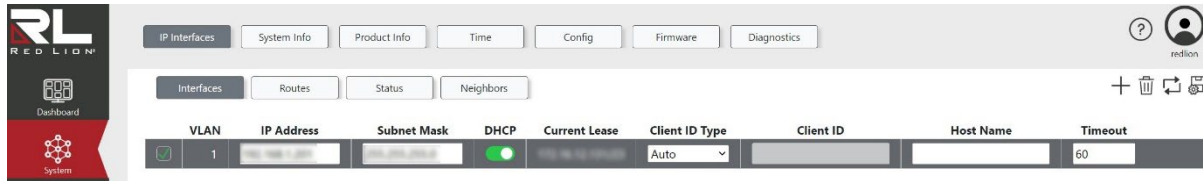
Clicking on this button opens up a file browser window and allows you to quickly import a configuration to the switch.

Chapter 5 System

This chapter contains a listing of all functionality that can be configured for the Red Lion Controls NT5000 switch models.

IP Interfaces

Interfaces



This page displays the IP interfaces.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

VLAN: The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

IP Address: The IPv4 address of the interface in dotted decimal notation ('x.y.z.w'). If DHCP is enabled, this field configures the fallback address. This field may be left blank if no DHCP fallback address is desired. The following restrictions apply:

- 'x.y.z.w' cannot be equal to the network address or the broadcast address for the assigned subnet.
- x must be a decimal number between 1 and 223.
- x must not be 127.
- y, z, and w must be decimal numbers between 0 and 255.

Subnet Mask: The IPv4 network mask in dotted decimal notation ('x.y.z.w') where the binary representation of the mask must be all ones followed by only zeros. For example, 255.255.255.0 or 255.255.255.128. If DHCP is enabled, this field configures the fallback network mask. This field may be left blank if no DHCP fallback address is desired.

DHCP: Enable or disable the DHCPv4 client. When enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol.

Default: Enabled

Current Lease: The current IP address of the interface as assigned by the bound DHCP server or fallback IP setting.

Client ID Type:

This specifies which type shall be used for the Client Identifier. Possible values are:

- Auto
- MAC
- ASCII
- HEX

See RFC-2132 section 9.14.

Default: Auto

Note: When DHCPv4 is enabled and the client identifier type is 'MAC', the interface's hardware MAC address will be used in the DHCP option 61 field, and this field becomes a drop down to select a port MAC address. The default in this case is the MAC address of the first port.


Client ID: The DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'MAC', the interface's hardware MAC address will be used in the DHCP option 61 field.


Host Name: The hostname of the DHCP client. When this value is an empty string, the host name will be the configured system name plus the last three bytes of the system MAC address.


Timeout: The number of seconds to wait for a DHCP lease. After this period expires, the configured IPv4 address will be used as the IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.


Default: 0

Buttons

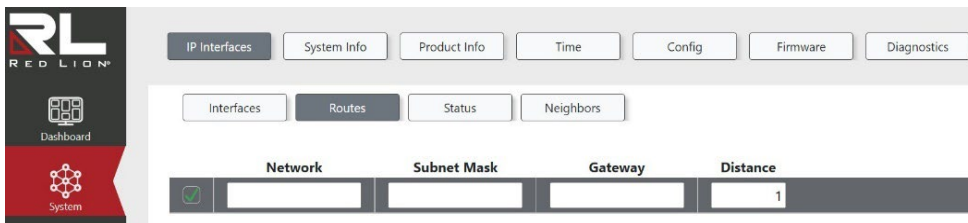
 Click to refresh the values on the page.

 Applies the changes to the device.

 Add a new interface.

 Click to remove the selected interface(s).

Routes



This page allows for the configuration of IP routes. An IP route specifies the destination address and the switch interface through which the switch can reach the destination.

Note: Existing IP routes are not editable but can be over-written. Adding new IP routes with the same network, subnet mask, and gateway as an existing route will replace the existing route. To change an IP route it is recommended to first delete the existing route and then re-create the route with the correct configuration.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Network: Configures the IPv4 destination network or host address for this IP route in dotted decimal notation ('x.y.z.w'). The following restrictions apply:

- x must be a decimal number between 0 and 223.
- x must not be 127.
- If x is 0 then y, z, and w must also be 0.
- y, z, and w must be decimal numbers between 0 and 255.

Note: A default IP route can use the default value '0.0.0.0' as their network address.

Subnet Mask: Configures the IPv4 destination network mask for this IP route. A valid IP route subnet mask contains 4 octets in dotted decimal notation ('x.y.z.w'). The binary representation of the mask must be only ones, or all ones followed by only zeros. For example, 255.255.255.255 has a binary representation of all ones and 255.255.255.0 has a binary representation of all ones followed by all zeros.

Note: Only default IP routes may use the value '0.0.0.0' as their subnet mask.





Gateway: Configures the IPv4 address of the IP gateway for this IP route in dotted decimal notation ('x.y.z.w'). The following restrictions apply:

- x must be a decimal number between 1 and 223.
- x must not be 127.
- y, z, and w must be decimal numbers between 0 and 255.

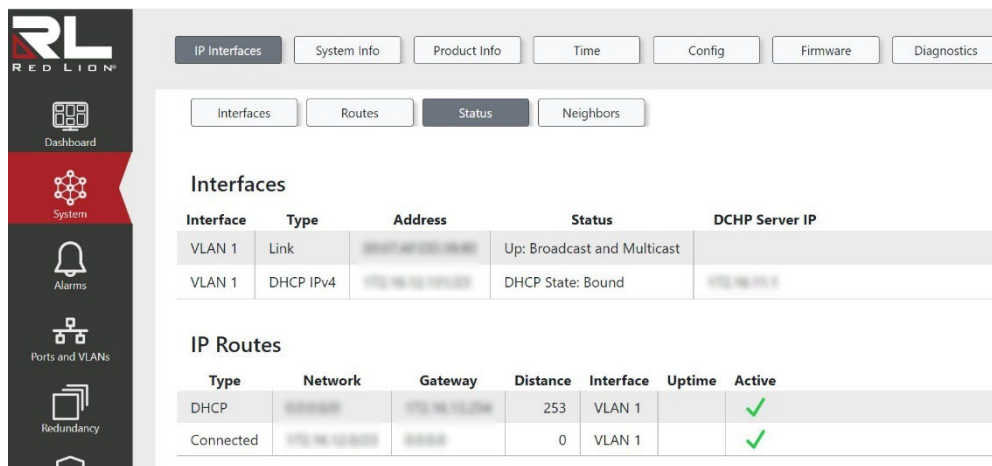
Distance: Configures the distance value of the route entry. This distance is used to set a priority for the route. If two or more routes have the same destination the distance will be used to select the best path. Valid values are between 1 and 255.

Default: 1

Buttons

-  Click to refresh the values on the page.
-  Applies the changes to the device.
-  Click to add new IP route.
-  Click to delete selected IP routes.

Status



The screenshot shows the 'Status' page in the RedLion web interface. It features a sidebar with navigation icons for Dashboard, System, Alarms, Ports and VLANs, and Redundancy. The main content area has a top navigation bar with tabs for IP Interfaces, System Info, Product Info, Time, Config, Firmware, and Diagnostics. Below this, there are sub-tabs for Interfaces, Routes, Status (which is selected), and Neighbors. The Status page displays two tables: 'Interfaces' and 'IP Routes'.

Interface	Type	Address	Status	DHCP Server IP
VLAN 1	Link	192.168.1.1	Up: Broadcast and Multicast	
VLAN 1	DHCP IPv4	192.168.1.1	DHCP State: Bound	192.168.1.1

Type	Network	Gateway	Distance	Interface	Uptime	Active
DHCP	192.168.1.0/24	192.168.1.1	253	VLAN 1		✓
Connected	192.168.1.0/24	192.168.1.1	0	VLAN 1		✓

This page displays the status of the interfaces and IP routes found on the switch.

Interfaces

The Interfaces table contains a row for each interface found on the switch.

IP Routes

The IP Routes table contains a row for each IP route found on the switch.

Interfaces Interface: Displays the name of the interface.

Interfaces Type: Displays the address type of the interface. Possible values are:

Link: Indicates this is a link interface.

IPv4: Indicates that the interface IP is static.

DHCP IPv4: Indicates that the interface IP address is set by DHCP.

Interfaces Address: Displays the current address of the interface entry.

Interfaces Status: Displays the status of the interface (and/or address) entry.

Interfaces DHCP Server IP: Displays the IP address of the DHCP server the interface entry is bound to. This field will be empty if the interface is not of type 'DHCP IPv4'.

IP Routes Type: Displays the type of IP route entry. Possible types are:

DHCP: Indicates this IP route was created by DHCP.

Static: Indicates this IP route was created by an admin user.

Connected: Indicates the destination network is directly connected to the switch.

IP Routes Network: Displays the IPv4 network/prefix of the IP route entry in dotted decimal notation.

IP Routes Gateway: Displays the IPv4 address of the IP route entry's gateway in dotted decimal notation. IP routes that are directly connected will have a gateway of '0.0.0.0.'


IP Routes Distance: Displays the distance value of the route entry. Directly connected IP routes will have a value of '0'.

IP Routes Interface: Displays the VLAN interface that the IP route entry's gateway falls within. If the gateway IP address does not fall within the IP subnet of any existing VLAN interfaces, this field will be empty.

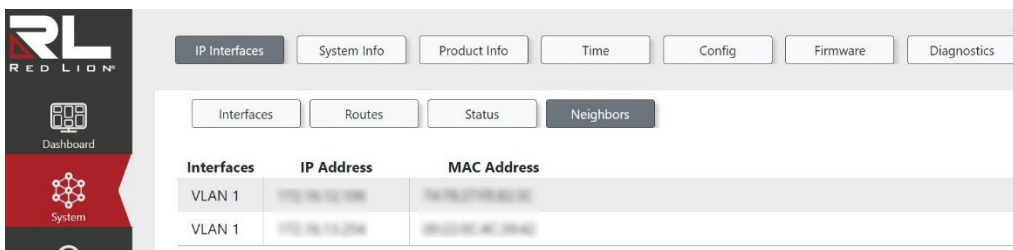
IP Routes Uptime: Displays the time that has elapsed since this IP route was created.

IP Routes Active: Indicates whether or not the IP route destination is active.

Buttons

 Click to refresh the values on the page.

Neighbors




This page displays the neighbors cache (ARP cache).

Interfaces: The name of the interface.

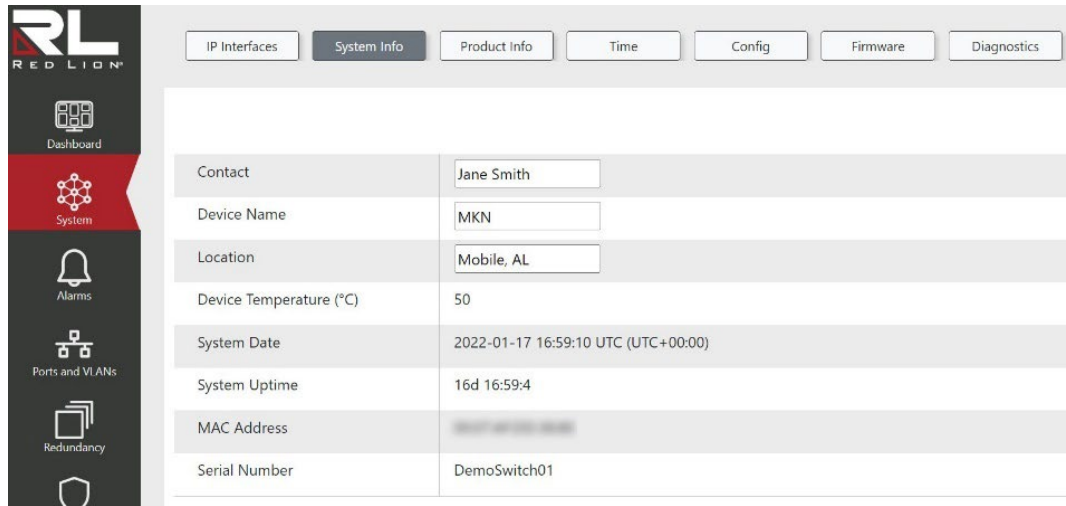
IP Address: The IPv4 address of the neighbor.

MAC Address: The Link (MAC) address of the neighbor.

Buttons

 Click to refresh the values on the page.

System Info



Contact	Jane Smith
Device Name	MKN
Location	Mobile, AL
Device Temperature (°C)	50
System Date	2022-01-17 16:59:10 UTC (UTC+00:00)
System Uptime	16d 16:59:4
MAC Address	XXXXXXXXXX
Serial Number	DemoSwitch01

The switch system information is provided here.

Contact: The system contact is the textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Device Name: The system name is an administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), or minus sign (-). No space characters are permitted as part of the name. The first character must be an alpha character, and the first or last character must not be a minus sign. The allowed string length is 0 to 255.

Location: The system location is the physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Device Temperature (C): The system Temperature is displayed in degrees Celsius.


System Date: The current (GMT) system time and date is obtained through the Timing server running on the switch, if any.


System Uptime: The System Uptime indicates the period of time the device has been operational.

MAC Address: The MAC Address indicates the MAC Address of this switch, which can be found on the lower left of the screen, beneath the firmware version.

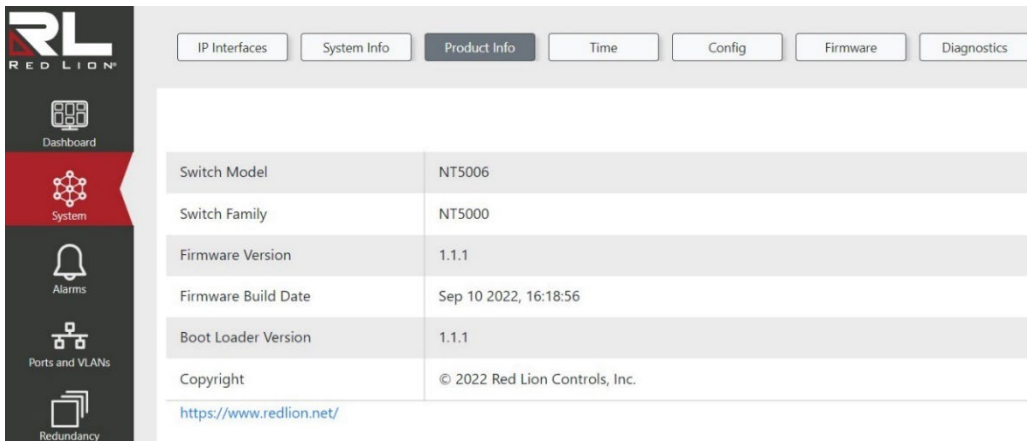
Serial Number: The serial number of this switch. This information can be found on the lower left of the screen, beneath the MAC address.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Product Info



Product Information	Value
Switch Model	NT5006
Switch Family	NT5000
Firmware Version	1.1.1
Firmware Build Date	Sep 10 2022, 16:18:56
Boot Loader Version	1.1.1
Copyright	© 2022 Red Lion Controls, Inc.

<https://www.redlion.net/>

This page displays the Product Information.

Switch Model: The base model of this switch is shown here. This information is also displayed in the lower left of the user interface.

Switch Family: The switch family is the family of switches in which this model, and similar models, belong.

Firmware Version: The firmware version indicates the firmware's version. Firmware is the foundation of the software stack that hardware uses to run operations. A version number is assigned for reference.

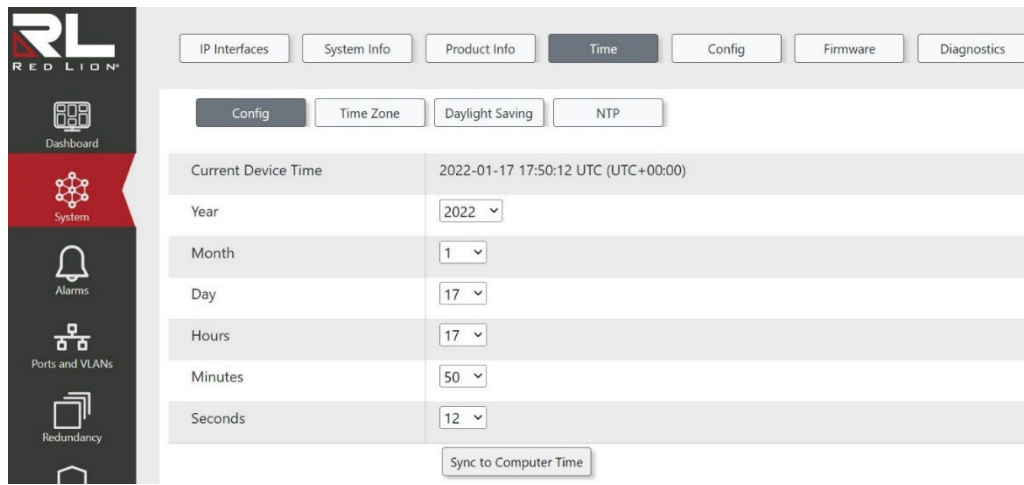
Firmware Build Date: The firmware's build date indicates the date and time the firmware was built, in Month DD YYYY HH:MM:SS formatting. This helps the user discern when the firmware was last revised.

Boot Loader Version: The boot loader version indicates the bootloader's version. When the device powers on, the boot loader is loaded first, and provides an interface through which the firmware is loaded.

Copyright: The copyright is a section that indicates the year of copyright, as well as the corporation that holds the copyright for this system.

Time

Config



This page allows you to configure the system Time. System time can be synced to the computer using the button **Sync to Computer Time**.

Year: This section allows the user to select the year of the device. Menu options are selectable through the current year and extend fifteen years into the future.

Month: This section allows the user to select the month of the device. Menu options are selectable through options January and end in December, and are selectable through menu options 1-12.


Day: This section allows the user to select the day of the device. Menu options are selectable through options 1-31. Attempts to set the day and time to nonexistent dates, like 2022-02-30 or 2022-02-31, will see the day and month corrected by the system upon save.


Hours: This section allows the user to select the hour of the device. Menu options are selectable through options 0-23.

Minutes: This section allows the user to select the minute of the device. Menu options are selectable through options 0-59.

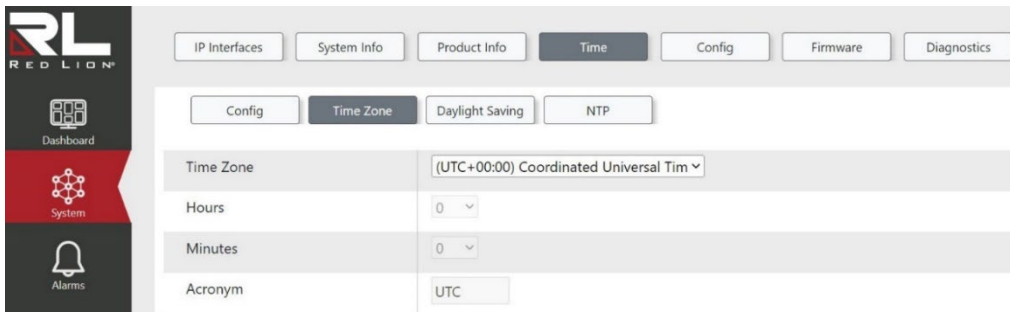
Seconds: This section allows the user to select the second of the device. Menu options are selectable through options 0-59.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Time Zone



The screenshot shows the Red Lion system configuration interface. The top navigation bar includes buttons for IP Interfaces, System Info, Product Info, Time (selected), Config, Firmware, and Diagnostics. Below this, there are sub-navigation buttons for Config, Time Zone (selected), Daylight Saving, and NTP. The main configuration area has four rows: 'Time Zone' with a dropdown menu showing '(UTC+00:00) Coordinated Universal Tim', 'Hours' with a dropdown menu showing '0', 'Minutes' with a dropdown menu showing '0', and 'Acronym' with a text input field containing 'UTC'. On the left side, there is a sidebar with the Red Lion logo and icons for Dashboard, System, and Alarms.

This page allows for the configuration of the system Time Zone


Time Zone: Select appropriate Time Zone from the drop down list of world-wide time zones, and click Save to set it. The 'Manual Setting' is used to specify a custom time zone.


Hours: Hours represents the number of hours offset from UTC. This field is only available within the time zone manual setting.

Minutes: Minutes represents the number of minutes offset from UTC. This field is only available within the time zone manual setting.

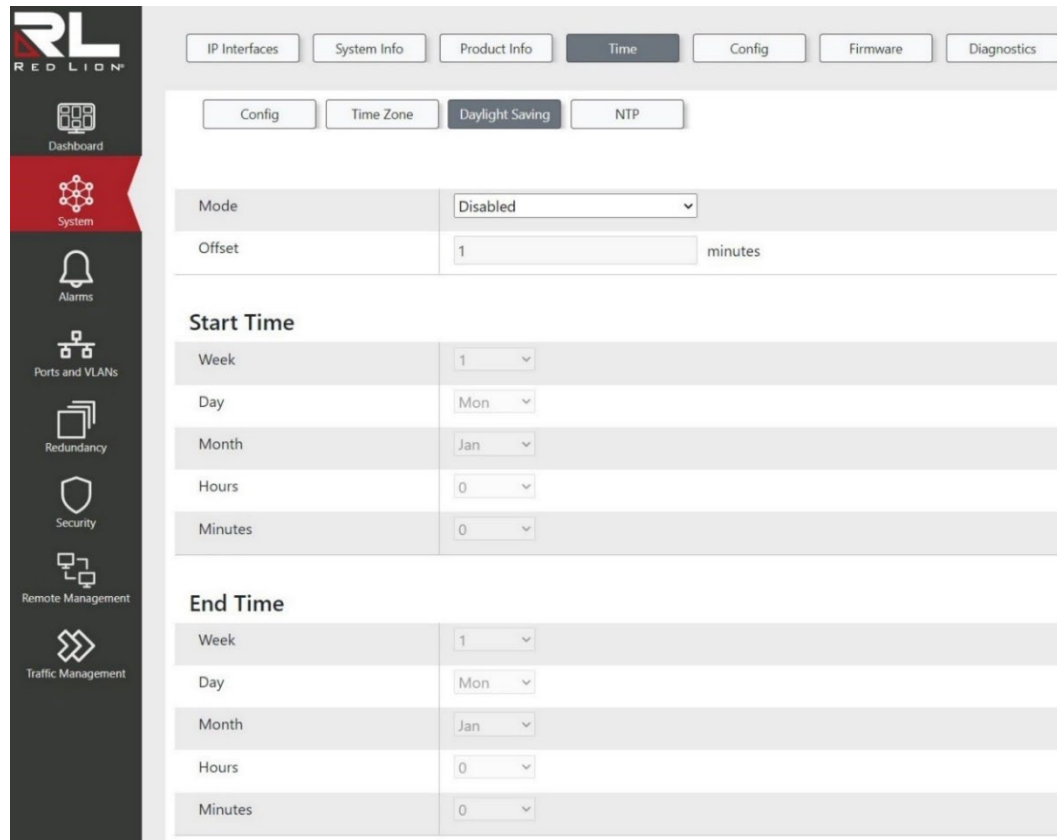
Acronym: Within this field, the user can set the acronym of the time zone. This is a User configurable acronym to identify the time zone, with an allowable range of up to 16 characters. Notice the string " is a special syntax that is reserved for null input.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Daylight Saving



Mode	Disabled
Offset	1 minutes
Start Time	
Week	1
Day	Mon
Month	Jan
Hours	0
Minutes	0
End Time	
Week	1
Day	Mon
Month	Jan
Hours	0
Minutes	0

Daylight Saving Time is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration.

Selecting the Recurring mode configures a start time and end time, of the form '#th Weekday of a Month at a Time'. For example, 'the 3rd Wednesday of January at 21:35'.

Selecting Non-Recurring configures a start time and end time in the form of Month, Date, Year, Hour Minute. For example, February 19, 2037 at 15:35.

Mode:

Selecting Disabled disables Daylight Saving Time.

Selecting Recurring enables the Daylight Saving Time duration to repeat the configuration every year.

Selecting Non-Recurring enables the Daylight Saving Time duration for single time configuration.

Default: Disabled

Offset: Enter the number of minutes to add during Daylight Saving Time, with a range from 1 to 1439.

Default: 1

Week: Select the starting and ending week number, from the dropdown selection of weeks 1-5.

Default: 1

Day: Select the starting and ending day, from the dropdown selection of days Monday-Sunday.

Default: Monday

Month: Select the starting and ending month, from the dropdown selection of January-December.

Default: January

Hours: Select the starting and ending hour, from the dropdown selection of options 0-23.

Default: 0

Minutes: Select the starting and ending minute, from the dropdown selection of options 0-59.

Default: 0


Date: Select the starting and ending date, from the dropdown selection of 1-31.


Default: 1

Year: Select the starting and ending year, from the dropdown selection from 2000 to 2097.

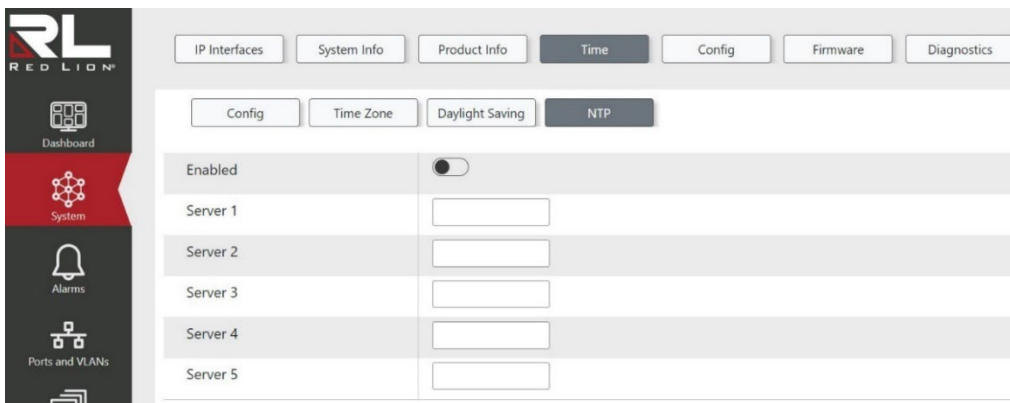
Default: Start: 2014, End: 2097

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

NTP




Configure NTP on this page.


Enabled: Enable or disable NTP mode operation.

Default: Disabled.

Server #: Provide the IPv4 or domain address of an NTP server.

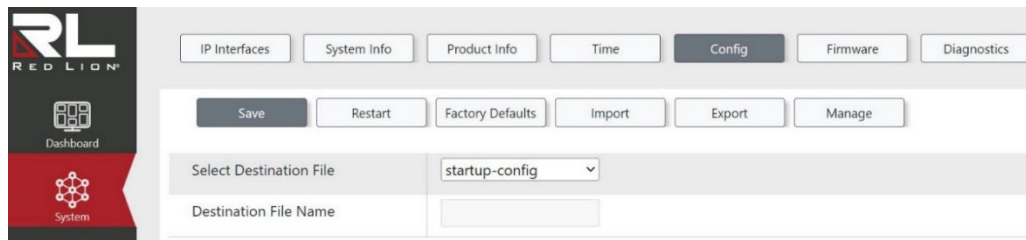
Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Config

Save



This page is used to copy the current running-config to the specified file.

Select Destination File: The file to copy running-config to. Available options are:

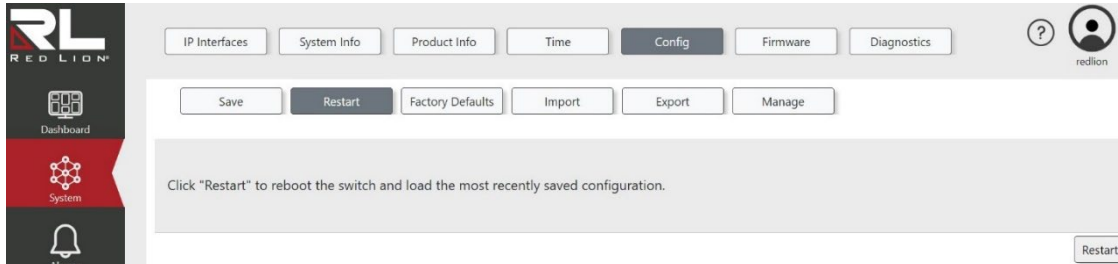
- startup-config: Ensures that the currently active configuration will be used at the next reboot.
- Create New File: Copies the running-config to a brand new file.

Destination File Name: If "Create New File" is selected, enter the name of the new file here.

Buttons

-  Saves the current running configuration to the selected destination.

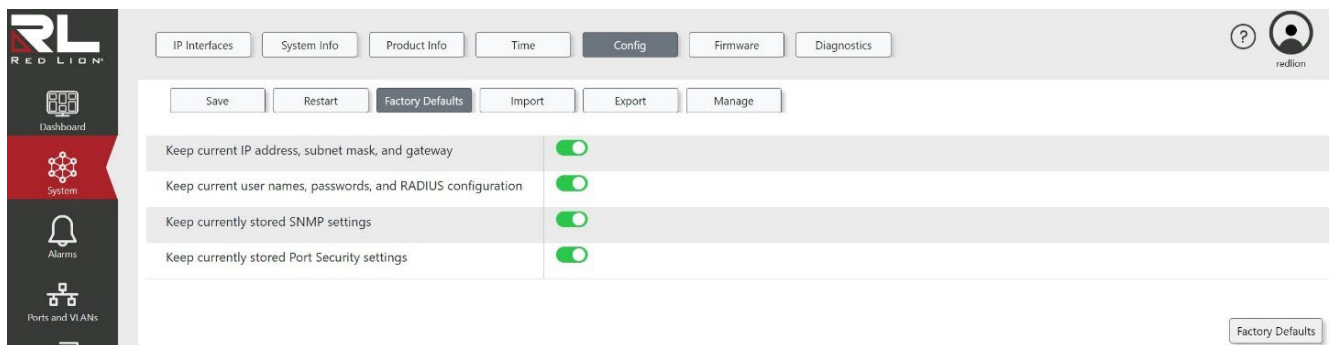
Restart



You can restart the switch on this page.

Restart: Click to restart device.

Factory Defaults



Resets the switch's configuration to factory defaults except for any of the selected items. This only affects the current configuration. A save must be performed to retain these changes after a power cycle or reboot.

The new configuration is available immediately, which means that no restart is necessary.

Keep current IP address and subnet mask for VLAN 1: Enable or disable to retain the existing IP address and subnet mask for VLAN 1.

Default: Enabled

Keep current user names, passwords, and RADIUS configuration: Enable or disable to retain the existing user names, passwords, and RADIUS configuration.

Default: Enabled

Keep currently stored SNMP settings: Enable or disable to retain the existing SNMP settings.

Default: Enabled

Keep currently stored Port Security settings: Enable or disable to retain the existing Port Security settings.

Default: Enabled

Import

The screenshot shows the Red Lion switch configuration web interface. The left sidebar contains navigation icons for Dashboard, System, Alarms, and Ports and VLANs. The main content area has a top navigation bar with tabs for IP Interfaces, System Info, Product Info, Time, Config (selected), Firmware, and Diagnostics. Below this is a secondary bar with buttons for Save, Restart, Factory Defaults, Import (selected), Export, and Manage. The main form area contains the following fields:

Action	Replace
Protocol	HTTPS
Server	
File Name	
Select Destination File	running-config
Destination File Name	

You can use this page to upload a file from the web browser to all the files on the switch, except default-config which is read-only.

Action: The import action to take. Available options are:

Replace: The currently selected configuration is fully replaced with the configuration in the uploaded file.

Merge: The uploaded file is merged into the currently selected configuration.

Create New File: Uploads the file as a new file in the flash file system of the switch. If the flash file system is full, it is not possible to create new files. Instead, an existing file must be overwritten, or another file must be deleted.

Protocol: Select the protocol used to transfer files onto the switch. Available options are:

HTTPS
TFTP


Server: If TFTP is the selected protocol, specify the IP address of the server.

File Name: If TFTP is the selected protocol, specify the exact file name to upload with file type extension. File names are case-sensitive.

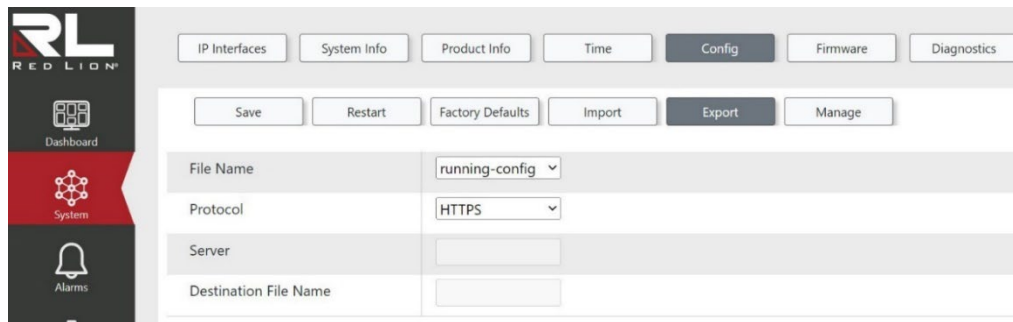
Select Destination File: If the Replace or Merge action is selected, select the name of the configuration file to act upon.

Destination File Name: If the Create New File action is selected, enter the name of the file you wish to create.

Buttons

 Starts the configuration file upload.

Export



You can use this page to export any of the files on the switch through the web browser.

File Name: Select the name of the file on the switch to export.


Protocol: Select the protocol used to export files from the switch. Available options are:

- HTTPS
- TFTP

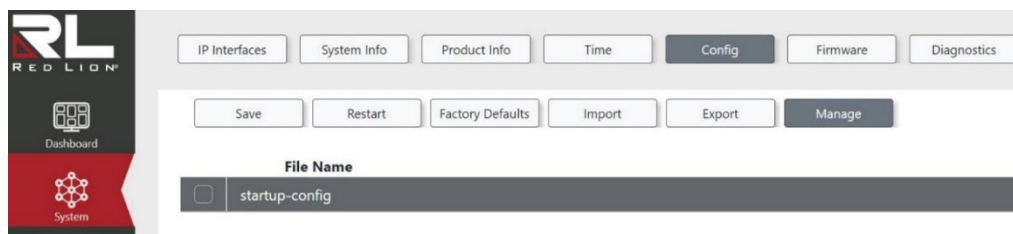
Server: If TFTP is the selected protocol, specify the IP address of the server.

Destination File Name: If TFTP is the selected protocol, specify the file name you wish to export the file as.

Buttons



 Starts the download of the configuration file.

Manage



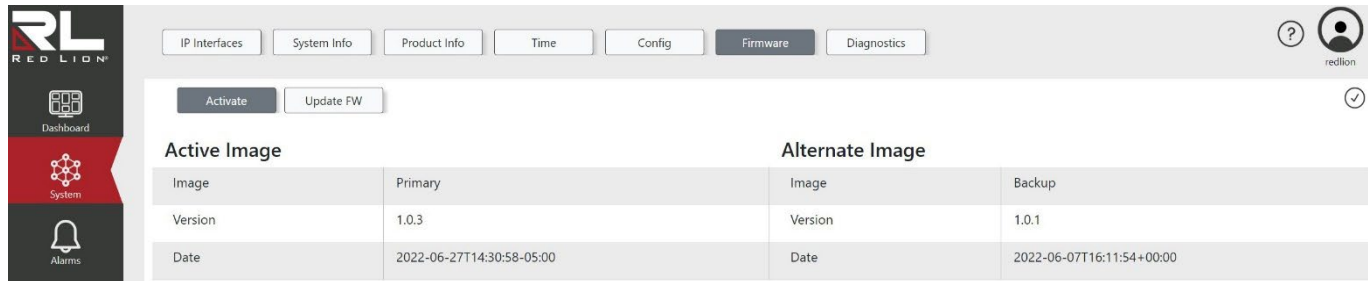
This page allows you to manage all of the files currently on the switch. From here, you can click on the checkbox to the left of the file name to select it and then click on the delete button to remove it from the switch.

Buttons

-  Delete the selected entry.
-  Applies the changes to the device.

Firmware

Activate



Active Image		Alternate Image	
Image	Primary	Image	Backup
Version	1.0.3	Version	1.0.1
Date	2022-06-27T14:30:58-05:00	Date	2022-06-07T16:11:54+00:00

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:

If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the active/primary image slot. The active firmware before the upload will become the new alternate.


The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image: This field displays 'Primary' for the active image, or 'Backup' for the alternate image.

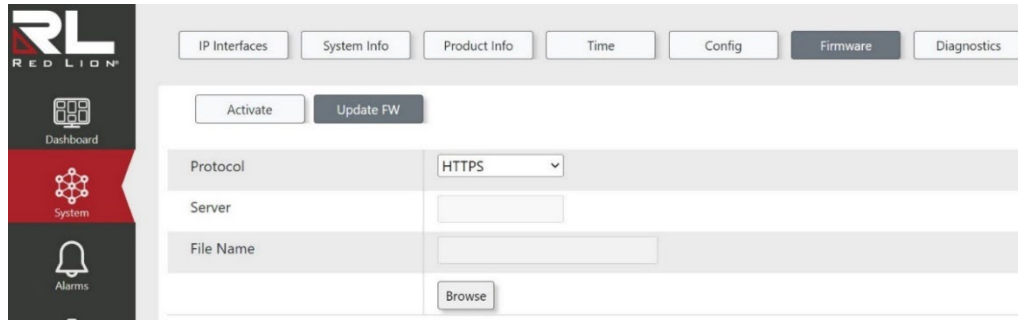
Version: The version of the firmware image.

Date: The date when the firmware was produced.

Buttons

-  This button activates the alternate firmware image, swapping the active/primary and alternate/backup images.

Update FW



This page facilitates an update of the firmware controlling the switch. The status of the firmware update will be displayed once an upload has been initiated. After some time, the firmware update is complete and the switch will restart, and the user will be logged out.

Warning: While the firmware update is in progress, the front LED flashes green. Do not restart or power off the device at this time or the switch may fail to function afterwards.

Protocol:

This field indicates the protocol to be used for transfers. Available options are:

HTTPS: Selecting HTTPS disables the 'Server' and 'File Name' fields, and displays a 'Browse' button to select a file.

TFTP: Selecting TFTP enables the 'Server' and 'File Name' fields, and the 'Browse' button is hidden.

Default: HTTPS

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

File Name: This field is the name of the file to be transported and flashed onto the switch. File names are limited to a maximum length of 63 characters.

Browse: When HTTPS is selected, click this button to browse for the location of the firmware image to upload.

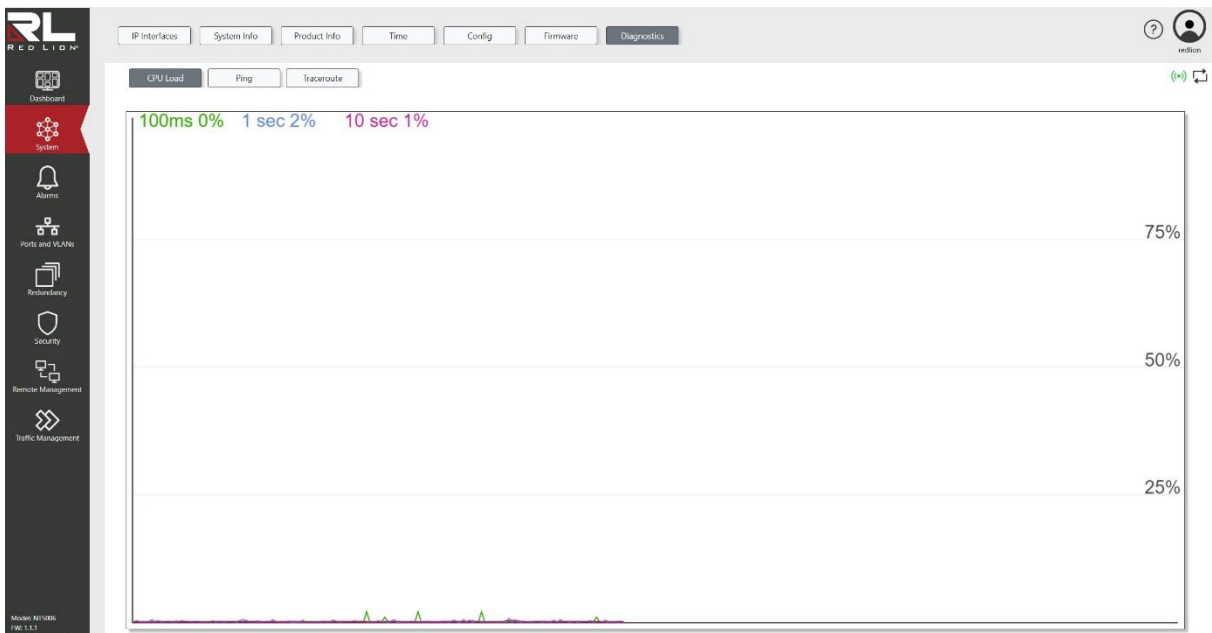
Buttons



This button updates the firmware with the currently selected image.

Diagnostics


CPU Load




This page displays the CPU load.

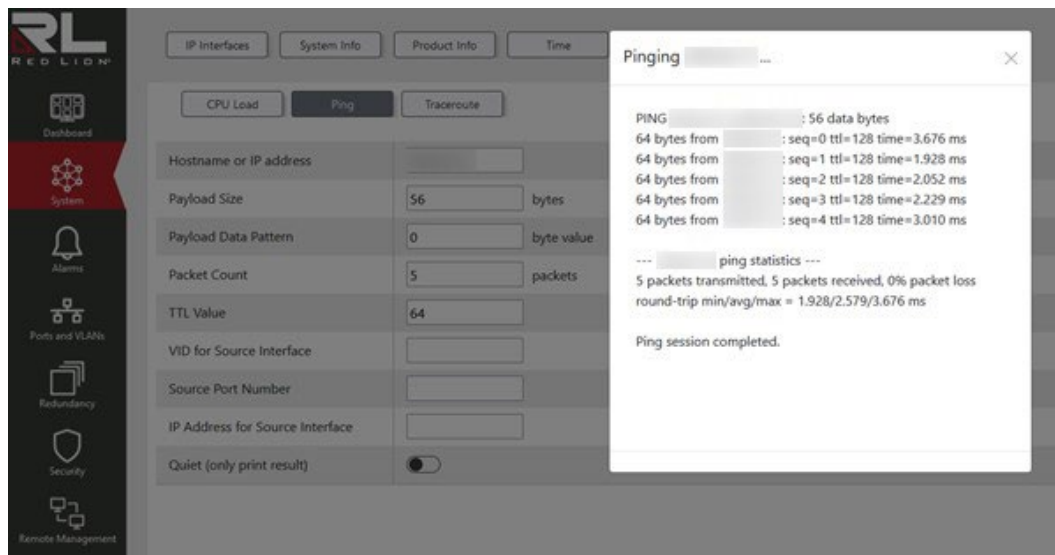
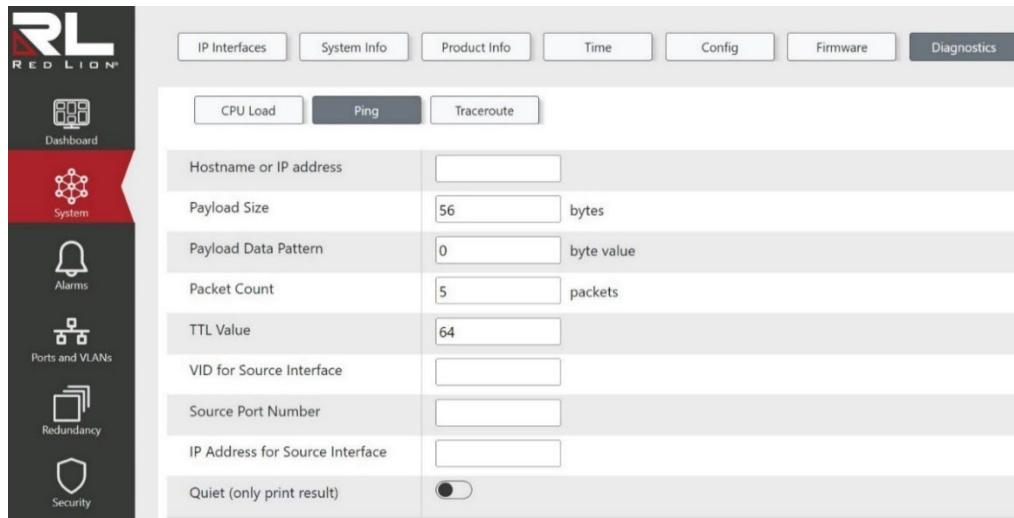
The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

Ping



This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues. You can configure the following parameters for the test:

Hostname or IP address: The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size: Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern: Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count: Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

TTL Value: Determines the Time-To-Live (TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.


Source Port Number: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the Source Port Number or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.


Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result): Checking this option will not print the result of each ping request but will only show the final result.

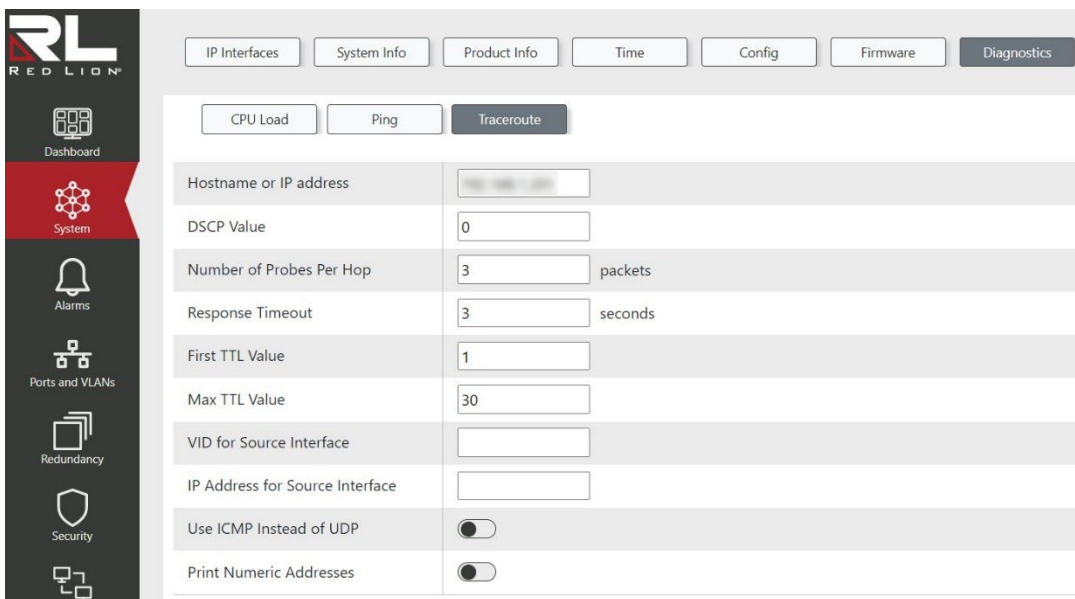
After you press , ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

Buttons

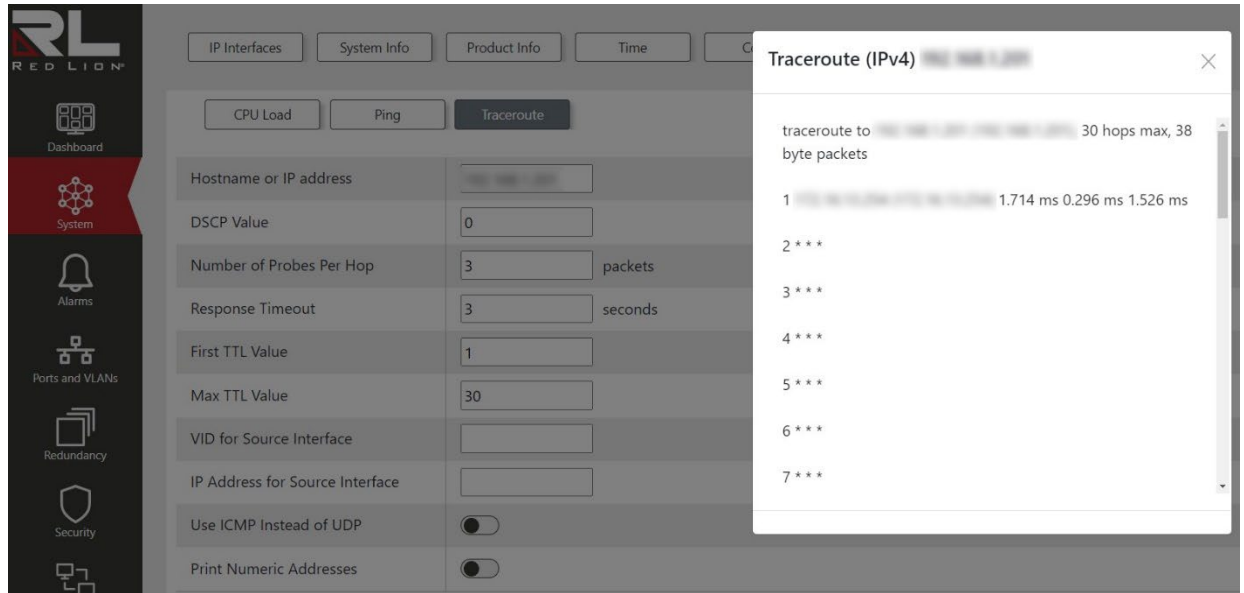
 Click to start transmitting ICMP packets.

Traceroute



The screenshot shows the Red Lion network management interface. The top navigation bar includes tabs for IP Interfaces, System Info, Product Info, Time, Config, Firmware, and Diagnostics. The Diagnostics tab is active, and the Traceroute sub-tab is selected. The configuration form includes the following fields:

Hostname or IP address	<input type="text"/>
DSCP Value	<input type="text" value="0"/>
Number of Probes Per Hop	<input type="text" value="3"/> packets
Response Timeout	<input type="text" value="3"/> seconds
First TTL Value	<input type="text" value="1"/>
Max TTL Value	<input type="text" value="30"/>
VID for Source Interface	<input type="text"/>
IP Address for Source Interface	<input type="text"/>
Use ICMP Instead of UDP	<input checked="" type="checkbox"/>
Print Numeric Addresses	<input checked="" type="checkbox"/>



This page allows you to perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network. You can configure the following parameters for the test:

Hostname or IP address: The destination IP Address.

DSCP Value: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

First TTL Value: Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.


IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Use ICMP Instead of UDP: By default the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

Print Numeric Addresses: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons

 Click to start sending packets.

Chapter 6 Alarms

Alarms

Active



This page displays all currently active, unresolved alarms and provides the following detailed information.

Note: Once an alarm is cleared it is no longer present in the Active table.

ID: The ID number of the alarm. The ID can be used to locate the alarm in History. It also corresponds to the ID used in Syslog if configured to log its severity level.

System Uptime: The length of time from the previous boot of the switch until the alarm was triggered.

Time: The time at which the alarm was triggered.

Component: The component in the system exhibiting the alarm.

LED Activated: Indicates whether or not the alarm set the status LED to an active error condition.

Contact Relay Triggered: Indicates whether or not the alarm triggered the Contact Relay.

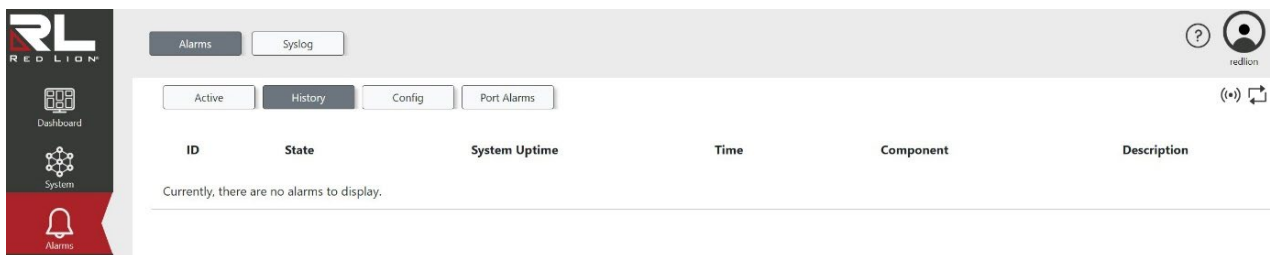
Description: The description of the alarm.

Buttons

Automatic refresh occurs every 3 seconds.

Click to refresh the values on the page.

History



This page displays a log of all alarms and provides the following detailed information.

ID: The ID number of the alarm and corresponds to the ID used in Syslog if configured to log its severity level.

State: The current state of the alarm.

Active - The alarm is currently present.

Clear - The alarm is no longer present.

System Uptime: The length of time from the previous boot of the switch until the alarm was triggered.

Time: The time at which the alarm was triggered.

Component: The component in the system with an alarm.

Description: The description of the alarm.

Buttons

(↻) Automatic refresh occurs every 3 seconds.

↻ Click to refresh the values on the page.

Config

Alarm	Alerts			SysLog	
	Enable	LED	Contact Relay	Event Log	Event Severity
Power DC V1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Warning
Power DC V2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Warning
Port Link Down	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Warning
Port Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Warning
Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Warning

This page allows you to configure which events trigger an alarm and alarm indicators.

Contact Relay Status: The current status of the contact relay. Possible states:

- Open
- Closed

Contact Relay Operation:

Configure the contact relay state.

Close On Alarm

Open On Alarm

Default: Close On Alarm

Alarms: List of configurable alarms.

Power DC V1: Triggered if the primary Voltage drops below 9 volts.

Power DC V2: Triggered if the secondary Voltage drops below 9 volts.

Port Link Down: Triggered when a link on a previously linked port is dropped.

Port Usage: Triggered when port usage is outside of the specified threshold.

Configuration: Triggered if a configuration is found to be invalid or in conflict with another configuration.

Alarm configurations:

The alarm configurations allow the user to determine what indicators to enable when an alarm occurs.

Enable: Enable or disable triggering of the alarm.

Default: Enabled for Port Usage and Configuration otherwise Disabled.

LED: Enable or disable triggering of the Status LED to indicate the presence of an alarm.

Default: Enabled for Port Usage and Configuration otherwise Disabled.

Contact Relay: Enable or disable triggering of the Contact Relay to indicate the presence of an alarm.

Default: Enabled for Port Usage and Configuration otherwise Disabled.

Event Log: Enable or disable logging of events to the Syslog.

Default: Enabled for all Alarms.

Event Severity:

The severity level assigned to the logged event.

Informational: Used to provide general information.


Notice: Used to provide information that may require a response.


Warning: Used to provide information that should be addressed at the earliest convenience.


Error: Used to provide information about an error condition that needs to be addressed immediately.

Default: Warning

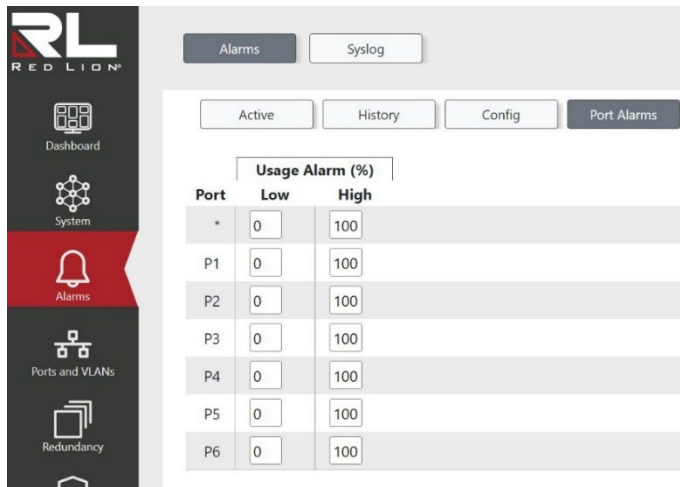
Buttons

 Toggle automatic reloading of the page every 3 seconds. Note: Disable automatic reloading when modifying configurations.

 Click to refresh the values on the page.

 Applies the changes to the device.

Port Alarms



This page allows the user to configure each port with a low and high utilization threshold value in percent. An alarm is triggered when the activity is no longer within the specified threshold range.

Port: The number of the individual port to configure.

Low: Set the minimum allowed port usage before an alarm is raised. Alarm occurs when the usage drops below the set value.

Range: 0 – 100

Default: 0

High: Set the maximum allowed port usage before an alarm is raised. Alarm occurs when the usage rises above the set value.

Range: 0 – 100

Default: 100

Buttons



Applies the changes to the device.



Click to refresh the values on the page.

Syslog

Log

ID	Level	System Uptime	Time	Description
12	Notice	0d 00:03:23	2022-01-01 00:02:53 UTC (UTC+00:00)	USER: Added user='redlion'
11	Notice	0d 00:00:41	2022-01-01 00:00:11 UTC (UTC+00:00)	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
10	Informational	0d 00:00:37	2022-01-01 00:00:07 UTC (UTC+00:00)	N-RING: Active member of N-Ring: Mode=Auto Member, Ports=P1-P2, VID=3333
9	Notice	0d 00:00:36	2022-01-01 00:00:06 UTC (UTC+00:00)	N-RING: Joining N-Ring: Mode=Auto Member, Ports=P1-P2, VID=3333
8	Informational	0d 00:00:36	2022-01-01 00:00:06 UTC (UTC+00:00)	N-RING: Not part of an N-Ring: Mode=Auto Member
7	Warning	0d 00:00:35	2022-01-01 00:00:05 UTC (UTC+00:00)	LINK-UPDOWN: Interface P6, changed state to up.
6	Warning	0d 00:00:34	2022-01-01 00:00:04 UTC (UTC+00:00)	VOLTAGE: Low voltage on power input DC V2
5	Warning	0d 00:00:34	2022-01-01 00:00:04 UTC (UTC+00:00)	LINK-UPDOWN: Interface P1, changed state to up.
4	Notice	0d 00:00:33	2022-01-01 00:00:03 UTC (UTC+00:00)	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
3	Notice	0d 00:00:33	2022-01-01 00:00:03 UTC (UTC+00:00)	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
2	Informational	0d 00:00:32	2022-01-01 00:00:02 UTC (UTC+00:00)	FIRMWARE: User='test'. Restarted after firmware update on 2022-01-04 17:12:09 UTC (UTC+00:00) with file='smb_jubilee-ocelot_pcb120.1.1.5.devkey.mfi'
1	Informational	0d 00:00:32	2022-01-01 00:00:02 UTC (UTC+00:00)	SYS-BOOTING: Switch just made a cool boot.

Displays the most recent events since the latest system startup or since the log was cleared. The event log can contain approximately 100 entries depending on individual message size. If the event log becomes full, new entries will overwrite the oldest entries.

ID: The sequence number indicating the order of the events.

Level:

The severity of events to display from the log.

All: Display all events.

Informational: General informational events.

Notice: Events that are unusual but not error conditions.

Warning: Not an error, but an indication that an error may occur if action is not taken.

Error: Urgent failure in a redundant or non-redundant component, protocol, interface or feature, which should be corrected immediately.

Default: All.


System Uptime: The total time elapsed since the switch was turned on or rebooted when the event was logged.

Time: The date/time when the event was logged.

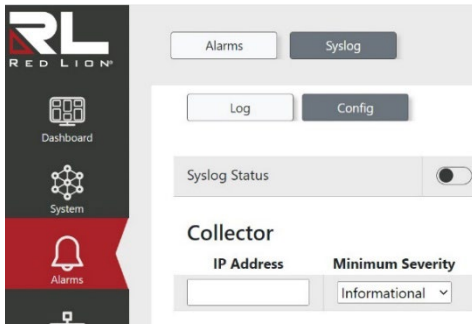
Description: A description of the event or condition logged. When applicable it includes the feature, protocol, interface or system service of the switch that logged the event.

Buttons

 Click to delete the displayed events from the log.

 Click to refresh the values on the page.

Config



This page allows you to configure the sending of events from the event log, in the form of Syslog messages, to a Syslog collector (also known as a Syslog server).

Syslog Status: Enable or disable the sending of Syslog messages.

Default: Disabled

IP Address: Indicates the IPv4 host address of a Syslog collector. If the switch provides a DNS feature, it can also be a domain name.

Minimum Severity:

Indicates the severity of messages that will be sent. Possible values are:

Informational: Send messages with a severity of Informational, Notice, Warning, or Error.


Notice: Send messages with a severity of Notice, Warning, or Error.


Warning: Send messages with a severity of Warning or Error.

Error: Send messages with a severity of Error.

Default: Informational

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Chapter 7 Ports and VLANs

Ports

Status/Config

Port	PVID	User Label	Enabled	Link Status	Speed/Duplex	State
P1	1	Type user label...	<input checked="" type="checkbox"/>	1000/F	Auto	N-Ring Forwarding
P2	1	Type user label...	<input checked="" type="checkbox"/>	1000/F	Auto	N-Ring Forwarding
P3	1	Type user label...	<input checked="" type="checkbox"/>	Down	Auto	N/A
P4	1	Type user label...	<input checked="" type="checkbox"/>	1000/F	Auto	MSTP Forwarding
P5	1	Type user label...	<input checked="" type="checkbox"/>	Down	Auto	N/A
P6	1	Type user label...	<input checked="" type="checkbox"/>	Down	Auto	N/A

This page allows you to inspect the current status of each port and to configure its options.

Port: This is the logical port number for this row.

PVID: This is the PVID for this port.

Default: 1

User Label: This is the user label for this port.

Enabled: Enables or disables the switch port operation.

Default: Enabled

Link Status: Provides the current link speed of the port. Possible values are:

- 1000/F
- 100/F
- 100/H
- 10/F
- 10/H
- Down

Speed/Duplex:

Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:

Auto: Port auto-negotiates speed and duplex with the link partner and selects the highest speed that is compatible with the link partner.

1000/F: Forces the port to 1 Gbps full duplex mode.

100/F: Forces the port to 100 Mbps full duplex mode.

100/H: Forces the port to 100 Mbps half duplex mode.

10/F: Forces the port to 10 Mbps full duplex mode.

10/H: Forces the port to 10 Mbps half duplex mode.

Default: Auto

State: Shows the current port operational state. Possible states are:

Mirror:

Reflector
Destination

N-Ring™:

Forwarding

LLAG#:

Forwarding
Disabled

STP, RSTP, or MSTP:

Disabled
Discarding
Learning
Forwarding

LLAG# + STP, RSTP, or MSTP:

Disabled
Discarding
Learning
Forwarding


802.1x:


Forwarding
Disabled
Authenticated
Unauthenticated
Link Down

Loop Protection:

Shutdown

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Advanced

Port	Adver. Speed			Adver. Duplex		Excessive Collision	Fastboot	Frame		Flow Control	Priority Flow Control	
	10M	100M	1G	Fdx	Hdx			Max Size (MTU)	Length Check		Enabled	Priority
*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7
P1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7
P2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7
P3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7
P4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7
P5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7
P6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Discard ▾	<input checked="" type="checkbox"/>	10240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0-7

This page allows you to inspect the current status of each port and to configure its options.

Port: This is the logical port number for this row.

Adver. Speed: When Speed is not set to Auto, the port will only advertise the specified speeds (10M, 100M, 1G) to the link partner.

Default: The port will advertise all the supported speeds if speed is set as Auto.

Adver. Duplex: When duplex is not set to Auto, the port will only advertise the specified duplex as either full duplex (Fdx) or half duplex (Hdx) to the link partner.

Default: The port will advertise all the supported duplexes if the Duplex is Auto.

Excessive Collision:

Configure port transmit collision behavior. Options are:

Discard: Discard frame after 16 collisions.

Restart: Restart backoff algorithm after 16 collisions.

Default: Discard

Fastboot: Enable or disable Fastboot. Fastboot allows a port to pass traffic through the switch within a few seconds of boot up, before protocols have been initialized. Do not enable Fastboot on ports where loops can be created or security is required at boot up. See the user manual for guidance and cautions.

Default: Disabled

Max Size (MTU): The maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

Default: 10240

Length Check: Enable or disable to configure if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). When enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field does not match the actual payload.

length. When disabled, frames are not dropped due to frame length mismatch.

Default: Disabled

Note: No drop counters count frames dropped due to frame length mismatch.

Flow Control: Enable or disable flow control. When FC (802.3x Flow Control) is enabled on a port, then the port will both generate and send pause frames to its link partner, as well as recognize and respond to pause frames from its link partner in an attempt to prevent packets from being dropped. When enabled, the port generates and sends pause frames to its link partner when the link partner is sending traffic that would otherwise be dropped due to the egress port's capacity being exceeded when forwarding the traffic to its destination. Refer to the IEEE 802.3x standard regarding operation and exceptions.

Flow control and PFC cannot both be enabled on the same port.

Default: Disabled


Priority Flow Control: Enable or disable priority flow control. When PFC (802.1Qbb Priority Flow Control) is enabled on a port, then flow control on a priority level is enabled. Through the Priority field, a range of priorities (one or more) can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation.


PFC and Flow Control cannot both be enabled on the same port.

Default: Disabled

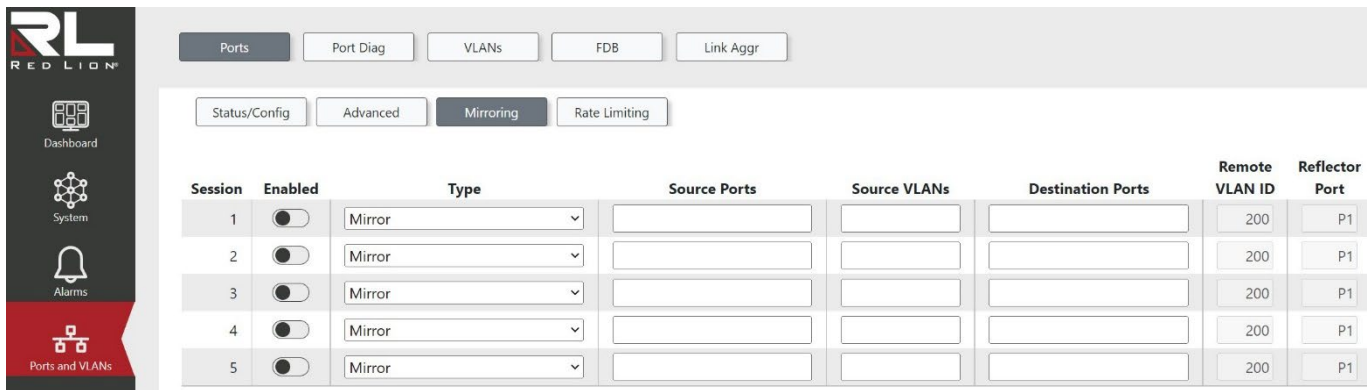
Note: PFC is not available on all switch models.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Mirroring



Session	Enabled	Type	Source Ports	Source VLANs	Destination Ports	Remote VLAN ID	Reflector Port
1	<input type="checkbox"/>	Mirror				200	P1
2	<input type="checkbox"/>	Mirror				200	P1
3	<input type="checkbox"/>	Mirror				200	P1
4	<input type="checkbox"/>	Mirror				200	P1
5	<input type="checkbox"/>	Mirror				200	P1

Mirroring is a feature which sends copies of network frames from one port (Rx, Tx, or both) to another port and is often used by administrators in conjunction with a port analyzer to monitor network traffic and analyze or debug network issues.

Remote Mirroring extends the function of Mirroring in that the network frames can be copied to a port on a separate (Remote) switch in the network, allowing administrators to analyze network traffic on other switches. **Note:** Ports that are used to connect the Remote Mirroring Source and Destination switches are usually referred to as **intermediate ports** and need to be added to the Remote VLAN ID in use (configured to egress tagged) as well as disable MAC Table (FDB) learning to perform Remote Mirroring.

See the user manual for more information on how port mirroring does or does not conflict with other protocols.

Sessions: Session ID to configure.

Enabled: Enable or disable the Mirror or Remote Mirroring session.

Default: Disabled

Type:

Select switch type. The possible Types are:

Mirror: Enables the Source Ports, Source VLANs, and Destination Ports Fields to configure mirroring traffic from one or more source ports or VLANs to a single destination port on the same switch.

Remote Mirroring Source: Enables the Source Ports, Source VLANs, Remote VLAN ID, and Reflector Port fields to configure mirroring traffic from one or more source ports or VLANs to a remote VLAN using the provided reflector port.

Remote Mirroring Destination: Enables the Destination Ports and Remote VLAN ID fields to configure one or more destination ports for remotely mirrored traffic from the specified Remote VLAN ID.

Default: Mirror

Source Ports: Used for Types **Mirror** and **Remote Mirroring Source** to specify the source ports to be mirrored. Each source port can be specified to mirror Rx (only received frames), Tx (only transmitted frames), or Rx/Tx (both received and transmitted frames). Either source ports or source VLANs can be specified, but not both. The exception is that only the CPU port may also be mirrored while mirroring VLANs.

Source VLANs: Used for Types **Mirror** and **Remote Mirroring Source** to specify the source VLANs to be mirrored. VLAN frames ingressing the switch are mirrored. VLAN frames egressing the switch are not mirrored. Either source ports or source VLANs can be specified, but not both. The exception is that only the CPU port may also be mirrored while mirroring VLANs.

Destination Ports: Used for Types **Mirror** and **Remote Mirroring Destination**. When the Type is **Mirror**, one destination port may be specified to receive copied traffic from the same switch. When the Type is **Remote Mirroring Destination**, one or more destination ports may be specified to receive remotely mirrored traffic from another switch.

Note: Each destination port needs to disable MAC Table (FDB) learning.

Remote VLAN ID: Used for Types **Remote Mirroring Source** and **Remote Mirroring Destination** to specify the Remote VLAN ID used for this remote mirroring session.

Default: 200

Reflector Port:

Used for Type **Remote Mirroring Source** to specify the reflector port which redirects the mirrored traffic to a specified Remote VLAN ID which is intended to be received by a separate (Remote) switch on the network (Remote Mirroring Destination).

Note:

The reflector port is only supported on copper ports.

The reflector port needs to disable MAC Table (FDB) learning and the Spanning Tree protocol.


Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.


If a port is shut down, it cannot be a candidate for a reflector port.

If a reflector port is shut down, the remote mirror function cannot work.

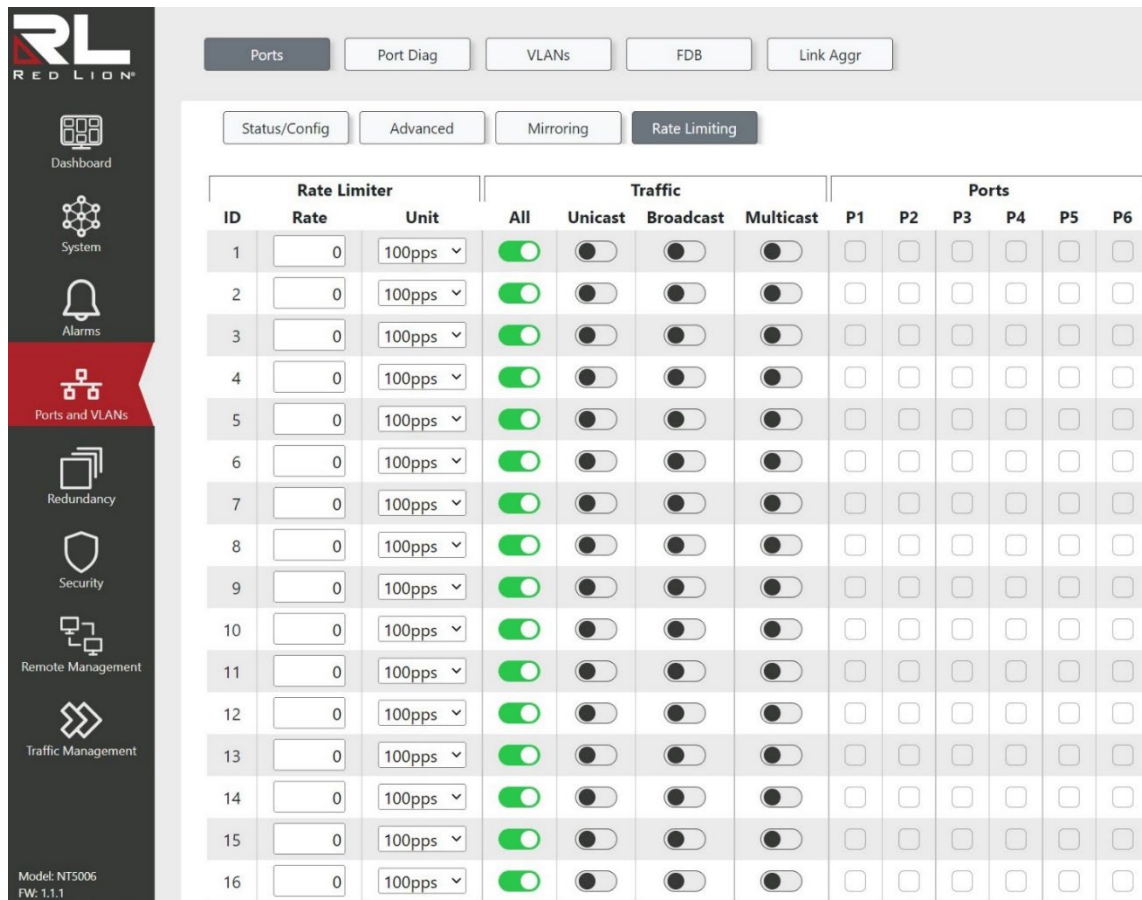
Default: Port 1

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Rate Limiting



ID	Rate Limiter		Traffic				Ports					
	Rate	Unit	All	Unicast	Broadcast	Multicast	P1	P2	P3	P4	P5	P6
1	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	0	100pps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Configure the rate limiter for the ACL of the switch.

ID: The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

Rate: When the selected Unit is 100pps, valid rates are 0-10920.

When the selected Unit is 100kbps, valid rates are 0-10000.

Unit: Specify the rate unit. The allowed values are:

100pps: 100 Packets per second

100kbps: 100 Kilobits per second

All: All frames will be affected by the pass rate when selected.


Unicast: Unicast frames will be affected by the pass rate when selected.


Broadcast: Broadcast frames will be affected by the pass rate when selected.

Multicast: Multicast frames will be affected by the pass rate when selected.

Ports: Use this section to select the ports the rate limit will apply to.

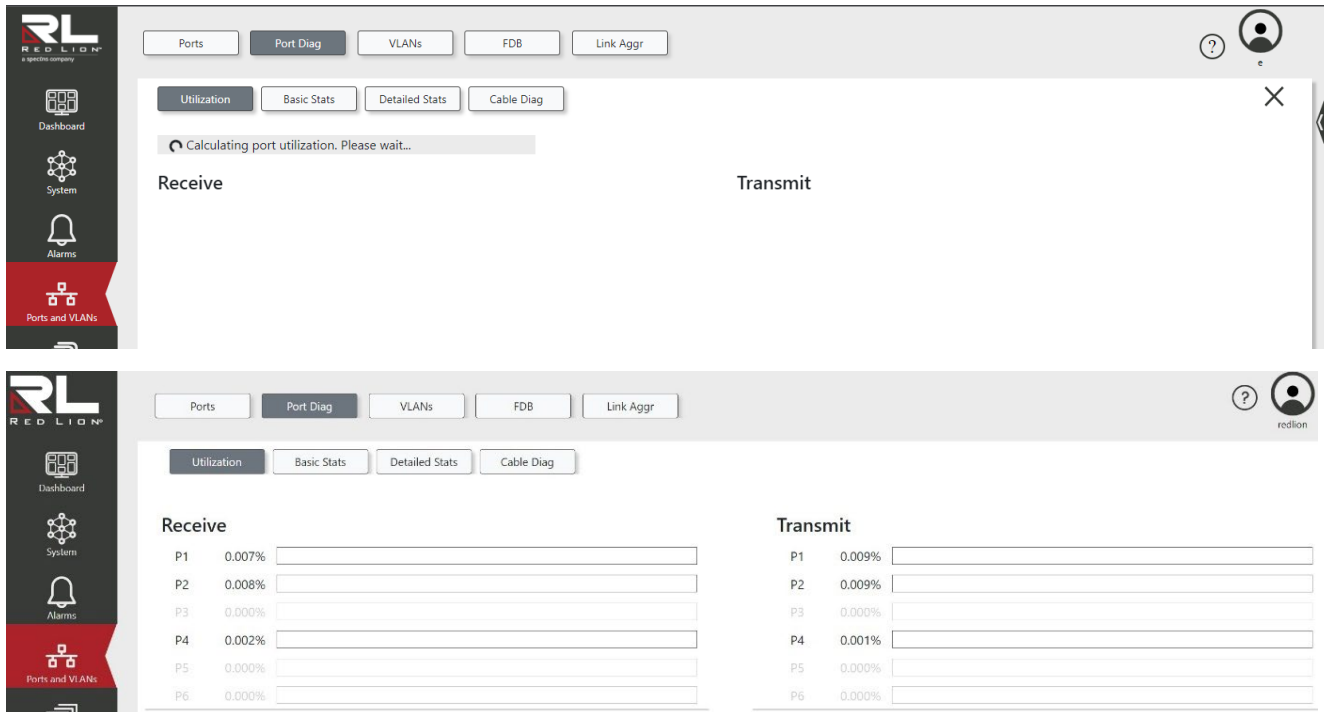
Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Port Diag

Utilization



The screenshot shows the 'Port Diag' section of the web interface. The top navigation bar includes 'Ports', 'Port Diag', 'VLANs', 'FDB', and 'Link Aggr'. The left sidebar has 'Dashboard', 'System', 'Alarms', and 'Ports and VLANs'. The main content area has tabs for 'Utilization', 'Basic Stats', 'Detailed Stats', and 'Cable Diag'. A loading message 'Calculating port utilization. Please wait...' is shown. Below are two columns: 'Receive' and 'Transmit'. The second screenshot shows the data populated in these columns.

Receive		Transmit	
P1	0.007%	P1	0.009%
P2	0.008%	P2	0.009%
P3	0.000%	P3	0.000%
P4	0.002%	P4	0.001%
P5	0.000%	P5	0.000%
P6	0.000%	P6	0.000%

This page displays the bandwidth percentage of all the ports.

Basic Stats

Port	Packets		Bytes		Errors		Drops		Filtered Rx
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	
P1	26938974	3418848	1934172765	293906346	0	0	0	0	23815103
P2	2450509	2565716	176927713	184316618	0	0	0	0	327
P3	0	0	0	0	0	0	0	0	0
P4	1013066	450223	141846966	112032995	0	0	9691	0	150942
P5	0	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	0	0	0	0

This page provides an overview of general traffic statistics for all switch ports. The displayed counters are:

Port: The logical port for the settings contained in the same row.

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.


Drops: The number of frames discarded due to ingress or egress congestion.


Filtered: The number of received frames filtered by the forwarding process.


Rx: The number of received packets/bytes/errors/drops.

Tx: The number of transmitted packets/bytes/errors/drops.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

 Click to clear the basic statistics for each port.

Detailed Stats

The screenshot shows the RedLion N-Tron Series NT5006 switch management interface. The 'Detailed Stats' tab is selected, showing a port status diagram on the left and two data tables on the right. The port status diagram shows six ports (1-6) with 'ACT' and 'LNK' indicators. The 'Received' table shows traffic statistics for port P1, and the 'Transmitted' table shows traffic statistics for the same port. The interface also includes a navigation sidebar with options like Dashboard, System, Alarms, Ports and VLANs, Redundancy, Security, Remote Management, and Traffic Management.

Total	Queue	Bytes	Errors
Packets 53615345	Q0 53609672	64 5893	Drops 0
Octets 3869126389	Q1 0	65-127 52376290	CRC/Alignment 0
Unicast 4968	Q2 0	128-255 1232334	Undersize 0
Multicast 53610334	Q3 0	256-511 620	Oversize 0
Broadcast 43	Q4 0	512-1023 208	Fragments 0
Pause 0	Q5 0	1024-1518 0	Jabber 0
	Q6 0	1519+ 0	Filtered 51967328
	Q7 0		

Total	Queue	Bytes	Errors
Packets 1818332	Q0 1765782	64 537102	Drops 0
Octets 206791696	Q1 0	65-127 649316	Late/Excessive Collisions 0
Unicast 9129	Q2 0	128-255 611906	
Multicast 1178212	Q3 0	256-511 18549	
Broadcast 630991	Q4 0	512-1023 1327	
Pause 0	Q5 0	1024-1518 132	
	Q6 0	1519+ 0	
	Q7 52550		

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Note: "Short" frames are frames that are smaller than 64 bytes, and "long" frames are frames that are longer than the configured maximum frame length for this port.

Packets: The number of received and transmitted (good and bad) packets.

Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Unicast: The number of received and transmitted (good and bad) unicast packets.

Multicast: The number of received and transmitted (good and bad) multicast packets.

Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Queue Counters: The number of received and transmitted packets per input and output queue.

Drops:

Received Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Transmit Drops: The number of frames dropped due to output buffer congestion.

CRC/Alignment: The number of frames received with CRC or alignment errors.

Undersize: The number of short frames received with valid CRC.

Oversize: The number of long frames received with valid CRC.

Fragments: The number of short frames received with invalid CRC.

Jabber: The number of long frames received with invalid CRC.


Filtered: The number of received frames filtered by the forwarding process.

Short frames are frames that are smaller than 64 bytes.

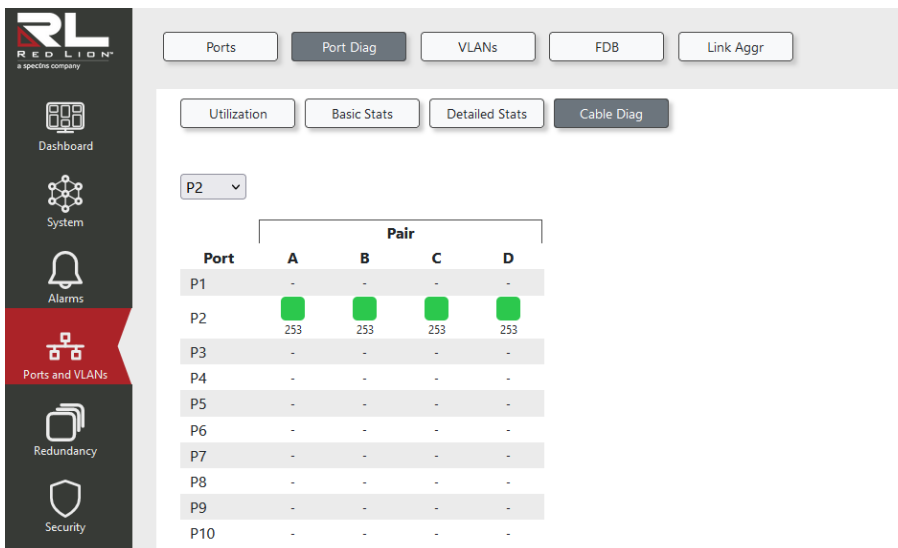
Long frames are frames that are longer than the configured maximum frame length for this port.

Late/Excessive Collisions: The number of frames dropped due to excessive or late collisions.

Buttons

 Click to refresh the values on the page.

Cable Diag



Port	Pair			
	A	B	C	D
P1	-	-	-	-
P2	253	253	253	253
P3	-	-	-	-
P4	-	-	-	-
P5	-	-	-	-
P6	-	-	-	-
P7	-	-	-	-
P8	-	-	-	-
P9	-	-	-	-
P10	-	-	-	-

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Press the "start" button to run the diagnostics. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

Note that VeriPHY is only accurate for cables of length 7-100 meters (25-328 feet).



10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Port Drop Down: Select the port for which you are requesting VeriPHY Cable Diagnostics.

Pair: For each port, 4 cable pair results are returned (A, B, C, and D) indicating each cable pair's status:

- OK** (solid green square): Correctly terminated pair.
- Open** (solid red square): Open pair.
- Short** (red square containing a white lightning icon): Shorted pair.
- Cross** (red square containing a white "X"): Abnormal cross-pair coupling.
- Length**: The length (in meters) of the cable pair appears under each icon. The resolution is 3 meters.

Buttons

-  Click to refresh the values on the page.
-  Begin VeriPHY cable diagnostics for the port(s) selected in the drop down.

VLANs

Config



The screenshot shows the configuration page for VLANs on an N-Tron Series NT5006 switch. The interface includes a navigation sidebar on the left with options like Dashboard, System, Alarms, Ports and VLANs (selected), Redundancy, Security, Remote Management, and Traffic Management. The main area has tabs for Ports, Port Diag, VLANs (selected), FDB, and Link Aggr. Below these are sub-tabs for Config and Advanced. A physical switch diagram shows ports 1-6 with status indicators (ACT, LNK). A table on the right lists VLAN configurations:

VLAN		Ports					
ID	Name	P1	P2	P3	P4	P5	P6
<input checked="" type="checkbox"/>	1 default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3333 N-Ring_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This page allows you to assign ports to VLAN Groups and to configure, for each port/VLAN pair, whether or not frames egressing a port have a VLAN tag.

Note: Protocols such as Port Remote Mirroring, Spanning Tree, and 802.1X Port Security can add to or override these VLAN settings.

Logical View

Select a VLAN Group row to highlight the group's member ports in the logical view.

Add New VLAN

To add a VLAN group, click the "Add" button and enter the VLAN's information.

Add VLANs to a Port and Select Egress Tagging

To modify a port's VLAN membership, click the cell in the table for the corresponding VLAN and port. Clicking multiple times cycles through the options detailed in the "Port Membership Table" section below.

Delete VLAN

To delete a VLAN group, select the VLAN's row and then click the "Delete" button.

Row selection column: Click on the checkbox to select the VLAN group. Click again to de-select.

Default: The first row is selected when a page is loaded.

ID: VLAN identification in the range 1 - 4094.

Name: A user-friendly VLAN name. The name is at most 32 characters long.

Port Membership Table: This table configures the port membership of a VLAN as well as if frames will egress with or without a VLAN tag.

Outlined Cell: The port is a VLAN group member. Frames egress **without** a VLAN tag.

Filled Cell: The port is a VLAN group member. Frames egress **with** a VLAN tag.

Empty Cell: The port is not a VLAN group member.

Buttons



Click to add a new VLAN.



Click to delete the selected VLAN.

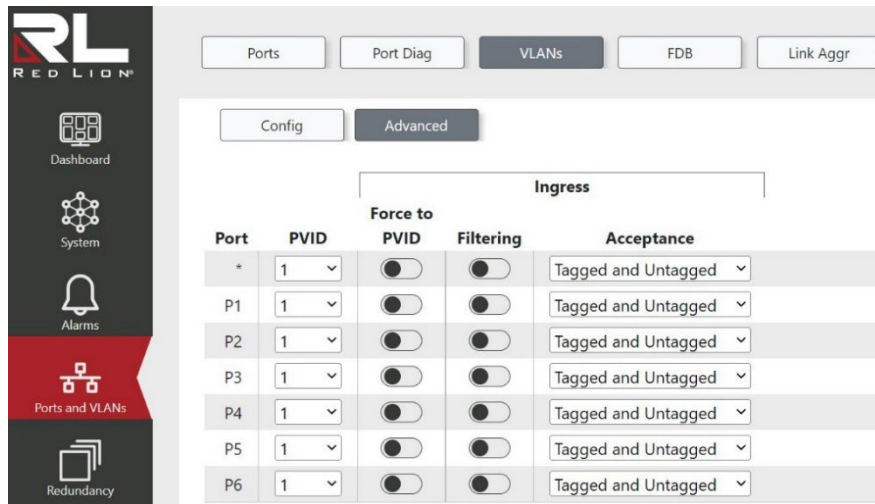


Click to refresh the values on the page.



Applies the changes to the device.

Advanced



This page allows you to configure advanced VLAN settings for ports.

Note: Protocols such as Port Remote Mirroring, Spanning Tree, and 802.1X Port Security can add to or override these VLAN settings.

Port: Port is the name of the port to configure the settings.

PVID: PVID is the Port VLAN ID. Select a VLAN ID from the dropdown menu to set the ports PVID. Only created VLANs will appear in the dropdown.

Force to PVID: Specifies whether or not to replace the VID tag of ingress frames with the PVID.

Filtering: If ingress filtering is enabled, an ingressing frame is discarded if the frame is classified to a VLAN that the ingress port is not a member of. If ingress filtering is disabled, an ingressing frame is accepted and forwarded to the VLAN it is classified to, even if the ingress port is not a member of that VLAN.

Note: A port will never transmit frames classified to a VLAN that the port is not a member of.


Acceptance: Specifies whether or not ingressing frames must be tagged or untagged (or either) to be accepted. Unaccepted frames are discarded.


Tagged and Untagged: Both, tagged and untagged frames are accepted on ingress.

Tagged Only: Only tagged frames are accepted on ingress.

Untagged Only: Only untagged frames are accepted on ingress.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

FDB

Entries

VLAN		MAC Address	Type	Ports						
ID	Name			CPU	P1	P2	P3	P4	P5	P6
1	default		Static	■						
1	default		Dynamic			■				
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Dynamic					■		
1	default		Static	■	■	■	■	■	■	■
3333	N-Ring_VLAN		Dynamic			■				
3333	N-Ring_VLAN		Dynamic		■					
3333	N-Ring_VLAN		Dynamic			■				
3333	N-Ring_VLAN		Static	■						
3333	N-Ring_VLAN		Static		■	■				

The entries in the FDB are shown in this table. They are sorted first by VLAN ID and then by MAC address.

If desired, the entries may be filtered by VLAN with the filter drop down above the entries.

VLAN ID: VLAN ID is the ID of the VLAN where the MAC Address was detected.

VLAN Name: VLAN Name is the name of the VLAN where the MAC Address was detected.




MAC Address: Mac Address indicates the MAC address of the entry.

Type: Type indicates whether the entry is a static or a dynamic entry.

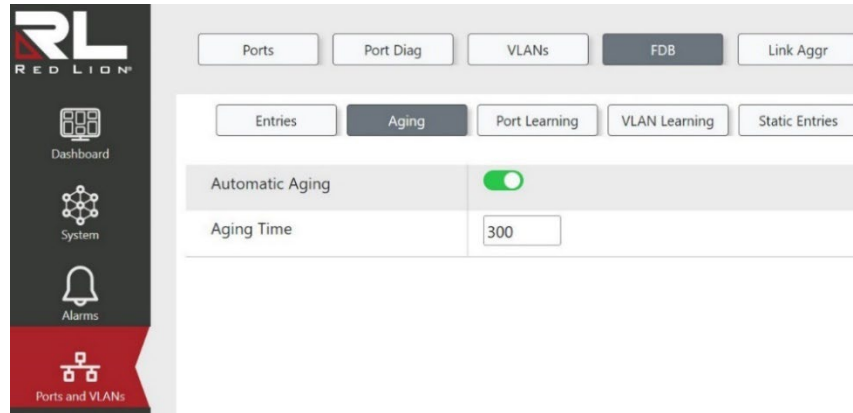
CPU: CPU indicates whether or not the frame is forwarded to the CPU.

Ports: Ports indicate to which ports the traffic for the destination MAC/VLAN will forward.

Buttons

-  Click to erase all dynamic entries.
-  Automatic refresh occurs every 3 seconds.
-  Click to refresh the values on the page.

Aging





By default, dynamic entries are removed from the FDB after 300 seconds. This timed removal is also called aging.

Configure the aging time by setting the following values:

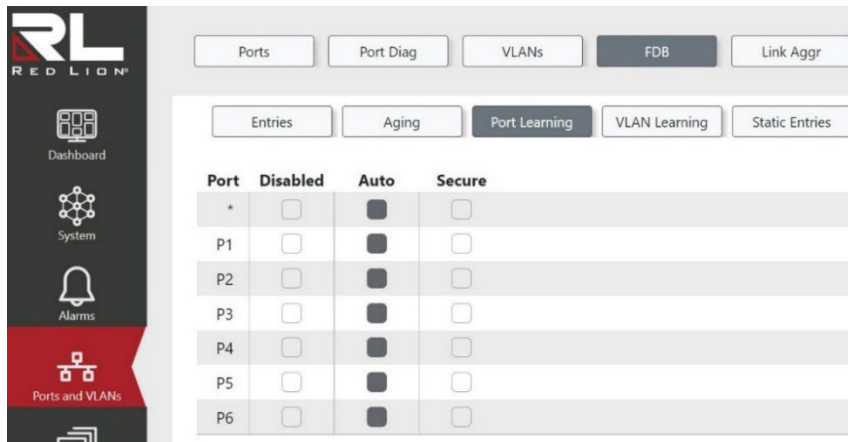
Automatic Aging: Enable or disable the automatic aging of dynamic entries.

Aging Time: Configure the aging time by entering a value here in seconds; for example, 600 seconds. The allowed range is 10 to 1000000 seconds.

Buttons

-  Click to refresh the values on the page.
-  Applies the changes to the device.

Port Learning



Each port learns source MAC addresses based upon the following settings:

Disabled: Learning is disabled.

Auto: Learning is enabled and done automatically as soon as a frame with an unknown Source MAC is received.


Secure:


Learning is disabled for all MACs on this port. All traffic ingressing into a secure port is dropped unless there is a static FDB entry with a matching Source MAC and port.

Note: Make sure that the link used for managing the switch is added to the Static FDB Entries before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial console.

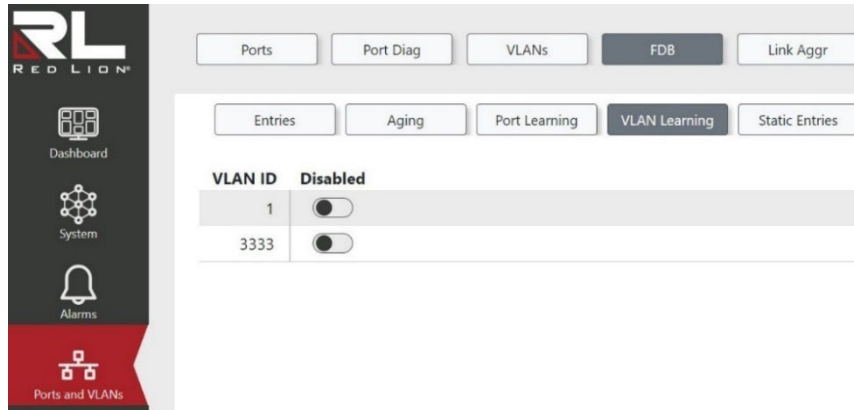
If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.


VLAN Learning




This table allows the configuration of VLANs as learning disabled. When a new MAC arrives into a VLAN where learning has been disabled, the MAC will not be recorded. By default all VLANs are created with learning enabled.

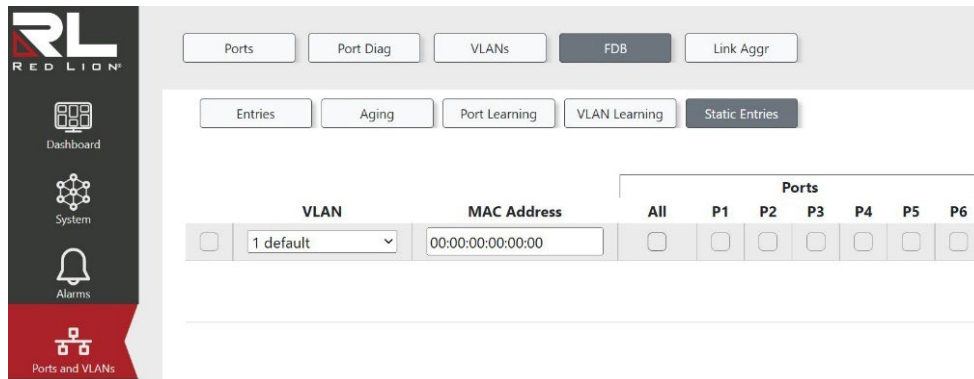
Disabled: If selected learning is disabled on this VLAN.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Static Entries



This page allows for the addition and deletion of static FDB entries.

The entries are sorted first by VLAN ID and then by MAC address.

When adding a static entry, configure it by setting the following values:

Row selection column: Click on the checkbox to select the row. Click again to de-select.





Default: The first row is selected when a page is loaded.

VLAN: The VLAN ID/Name of the entry.

MAC Address: The MAC address of the entry.

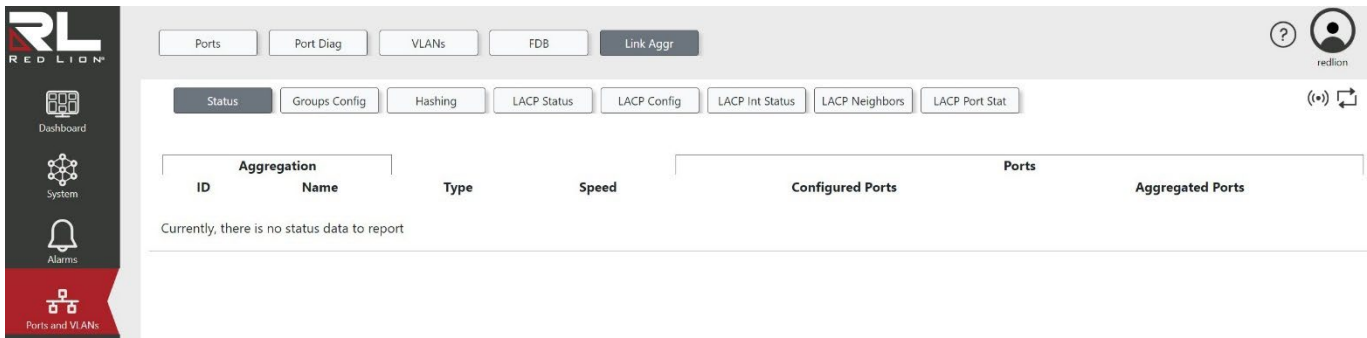
Ports: Traffic for the destination MAC/VLAN will be forwarded to this port.

Buttons

-  Click to add a new static entry to the FDB.
-  Click to delete the selected static entry from the FDB.
-  Click to refresh the values on the page.
-  Applies the changes to the device.

Link Aggr

Status



This page is used to see the status of ports in an aggregation group.

ID: The aggregation ID associated with this aggregation group.

Name: Name of the aggregation group.

Type: Type of the aggregation group. Available types are:

- Static
- LACP (Active)
- LACP (Passive)



Speed: Speed of the aggregation group. Possible speeds are:

- 10M
- 100M
- 1G

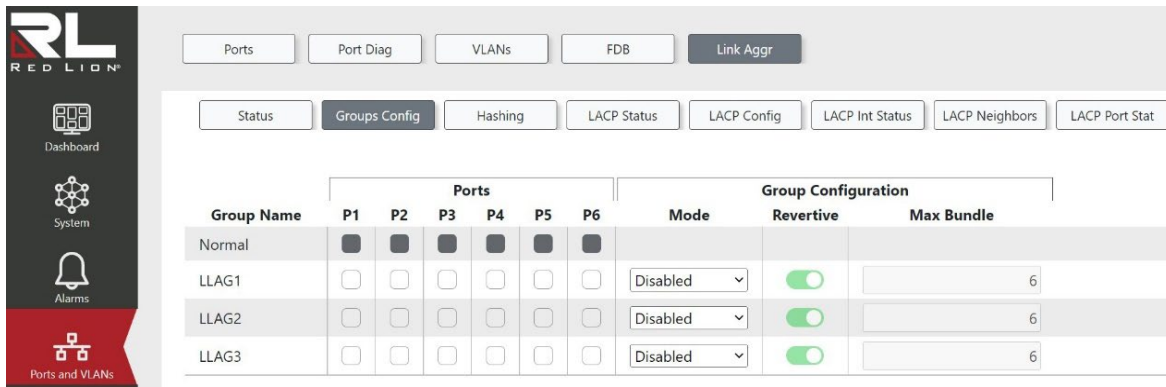
Configured Ports: Configured member ports of the aggregation group.

Aggregated Ports: Aggregated member ports of the aggregation group. These are ports that have negotiated an active aggregation link with another switch or router.

Buttons

-  Click to refresh the values on the page.
-  Automatic refresh occurs every 3 seconds.

Groups Config



This page is used to configure the aggregation groups.

Note: When saving, a group with a mode of Disabled will not save any ports to that group, even if they are checked.

Group Name: Indicates the name of the aggregation group for the settings contained in the same row. Group Name "Normal" indicates there is no aggregation. Only one group name is valid per port.

Ports: Checkboxes indicate to which aggregation group a port is assigned. If a port appears in the "Normal" row, it is not assigned to an aggregation group.

Check a box to include a port in an aggregation group, or uncheck a box to remove the port from the aggregation group. By default, no ports belong to any group.

Only full duplex ports can join an aggregation group and ports must be in the same speed in each group. If in an aggregation group, a port can only exist in one group at a time.

Mode:

This parameter determines the mode for the aggregation group. Available modes are:

Disabled: The group is disabled.

Static: The group operates in static aggregation mode.

LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

LACP (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

Default: Disabled


Revertive: This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority become available.


Default: Enabled

Max Bundle: This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

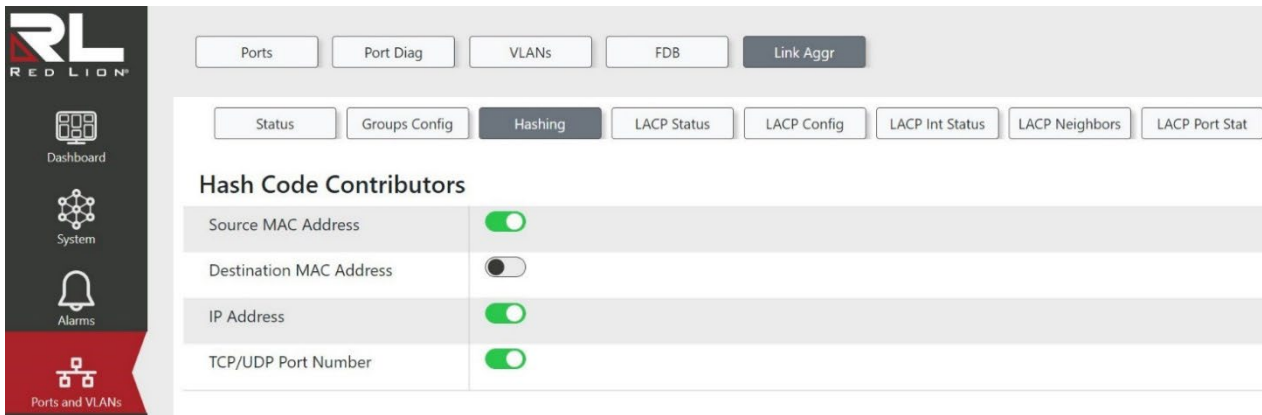
Default: Maximum Number of Ports on Board

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Hashing



This page is used to configure the link aggregation hashing algorithm which determines the destination port of the link aggregation group a frame will be transmitted out of. The value of the contributor comes from the the frame being transmitted.

For best traffic distribution among the LAG member ports, enable all contributions to the aggregation hash.

Source MAC Address: Enable or disable the use of the frame's Source MAC address as a hashing algorithm contributor.

Default: Enabled

Destination MAC Address: Enable or disable the use of the frame's Destination MAC address as a hashing algorithm contributor.

Default: Enabled


IP Address: Enable or disable the use of the frame's IP address as a hashing algorithm contributor.


Default: Enabled

TCP/UDP Port Number: Enable or disable the use of the frame's TCP/UDP Port Number as a hashing algorithm contributor.

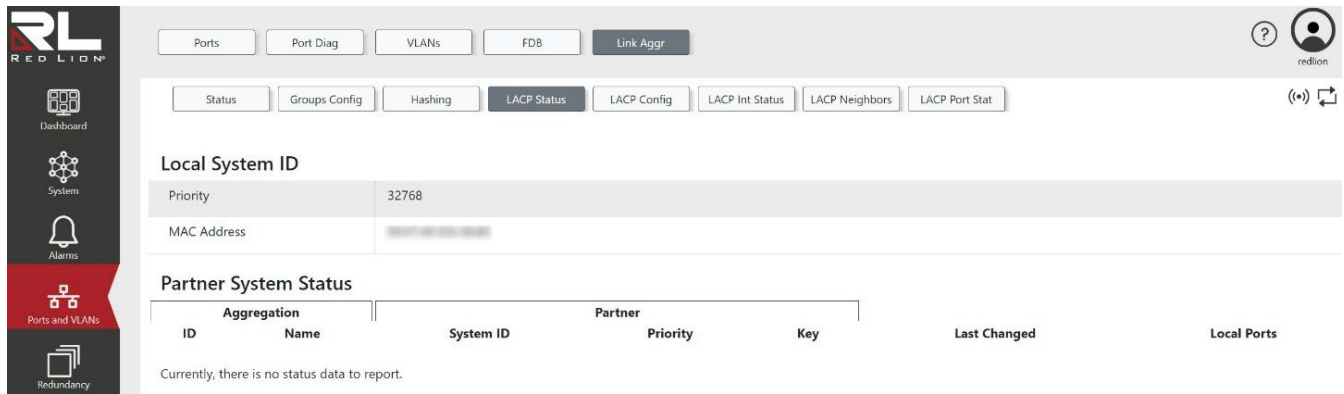
Default: Enabled

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

LACP Status



This page provides a status overview for the system-level LACP information.

Local System ID: This table displays both the local system priority and the local system MAC address which forms the local LACP System ID.

Partner System Status: This table displays the partner system information for each LACP aggregation group. The available information is:

Aggregation ID: The Aggregation ID associated with this aggregation group.

Aggregation Name: The Aggregation Name associated with this aggregation group.

Partner System ID: The System ID (MAC address) of the aggregation partner.


Partner Priority: The priority that the partner has assigned to this aggregation group.


Partner Key: The Key that the partner has assigned to this aggregation group.

Last Changed: The time that has elapsed since a change occurred in this aggregation group.

Local Ports: Shows which ports are a part of this aggregation for this switch.

Buttons

 Click to refresh the values on the page.

 Automatic refresh occurs every 3 seconds.

LACP Config

The screenshot shows the LACP Configuration page in the Red Lion network management interface. The page is divided into two main sections: LACP System Configuration and LACP Port Configuration. The LACP System Configuration section shows a System Priority of 32768. The LACP Port Configuration section shows a table with columns for Port, Enabled, Timeout, and Priority. The table contains six rows, each representing a port configuration.

Port	Enabled	Timeout	Priority
*		Fast	32768
P1		Fast	32768
P2		Fast	32768
P3		Fast	32768
P4		Fast	32768
P5		Fast	32768
P6		Fast	32768

This page allows the user to inspect the current LACP port configurations and possibly change them as well.

System Priority: LACP system priority value between the range of 1-65535.
Default: 32768

Port: The switch port number.

LACP Enabled: Shows whether LACP is currently enabled on this switch port. The LACP Enabled flag is only set when ports are connected to another LACP Active device.

Timeout:

Controls the period between BPDU transmissions. Possible values are:

Fast: Transmits LACP packets each second


Slow: Waits 30 seconds before sending an LACP packet


Default: Fast

Priority: Controls the priority of the port with a value between the range 1-65535. If the LACP partner wants to form a larger group than what is supported by this device, this parameter will control which ports will be active and which ports will be in a backup role. A lower number means greater priority.

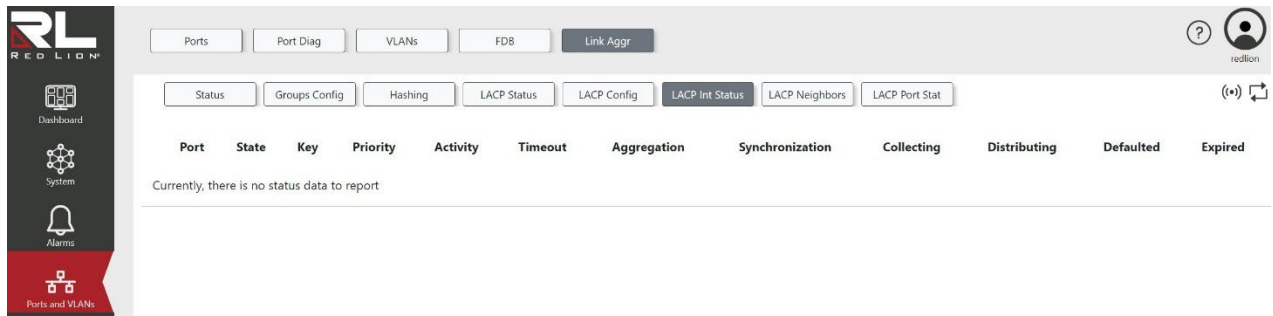
Default: 32768

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

LACP Int Status



This page provides a status overview for the LACP internal (i.e. local system) status for relevant ports. Only ports that are part of an LACP group are shown.

For details on the shown parameters, please refer to IEEE 801.AX-2014.

Port: The switch port number.

State: The current port state. Possible states are:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Priority: The priority assigned to the aggregation group.

Activity: The LACP mode of the group. Possible modes are:

Active

Passive

Timeout: The timeout mode configured for the port. Possible modes are:

Fast

Slow

Aggregation: Indicates whether the system considers this link to be 'aggregateable,' i.e. a potential candidate for aggregation.

Synchronization: Indicates whether the system considers this link to be 'IN_SYNC,' i.e. it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.



Collecting: Indicates if collection of incoming frames on this link is enabled.

Distributing: Indicates if distribution of outgoing frames on this link is enabled.

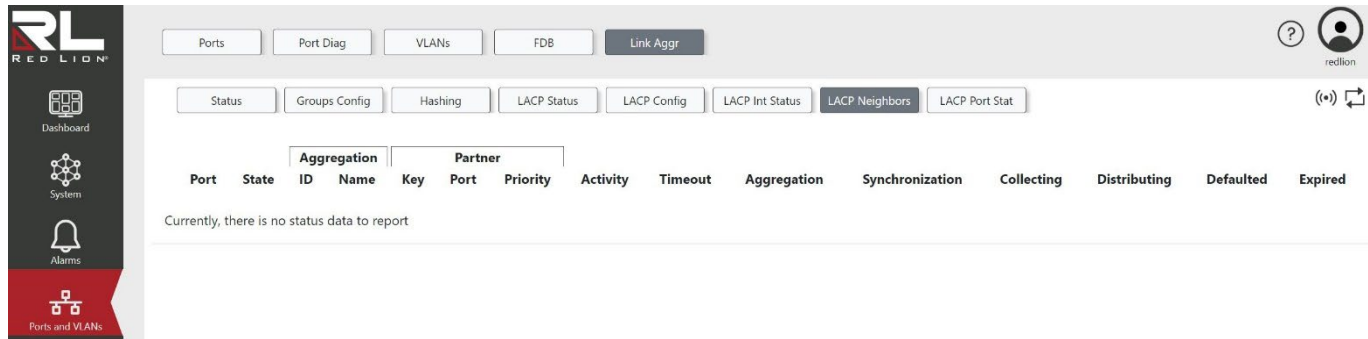
Defaulted: Indicates if the Actor's Receive machine is using Defaulted operational Partner information.

Expired: Indicates if the Actor's Receive machine is in the EXPIRED state.

Buttons

-  Click to refresh the values on the page.
-  Automatic refresh occurs every 3 seconds.

LACP Neighbors



This page provides a status overview for the LACP neighbor status for relevant ports. Only ports that are part of an LACP group are shown.

For details on the shown parameters please refer to IEEE 801.AX-2014.

Port: The switch port number.

State: The current port state.

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Aggregation ID: The aggregation group ID which the port is assigned to.

Aggregation Name: The name of the aggregation group which the port is assigned to.

Partner Key: The key assigned to this port by the partner.

Partner Port: The partner port number associated with this link.

Partner Priority: The priority assigned to this partner port.

Activity: The LACP mode of the group. Possible modes are:

- Active
- Passive

Timeout: The timeout mode configured for the partner port. Possible modes are:

- Fast
- Slow

Aggregation: Indicates whether the partner considers this link to be 'aggregateable,' i.e. a potential candidate for aggregation.

Synchronization: Indicates whether the partner considers this link to be 'IN_SYNC,' i.e. it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.


Collecting: Indicates if collection of incoming frames on this link is enabled.


Distributing: Indicates if distribution of outgoing frames on this link is enabled.

Defaulted: Indicates if the partner's Receive machine is using Defaulted operational Partner information.

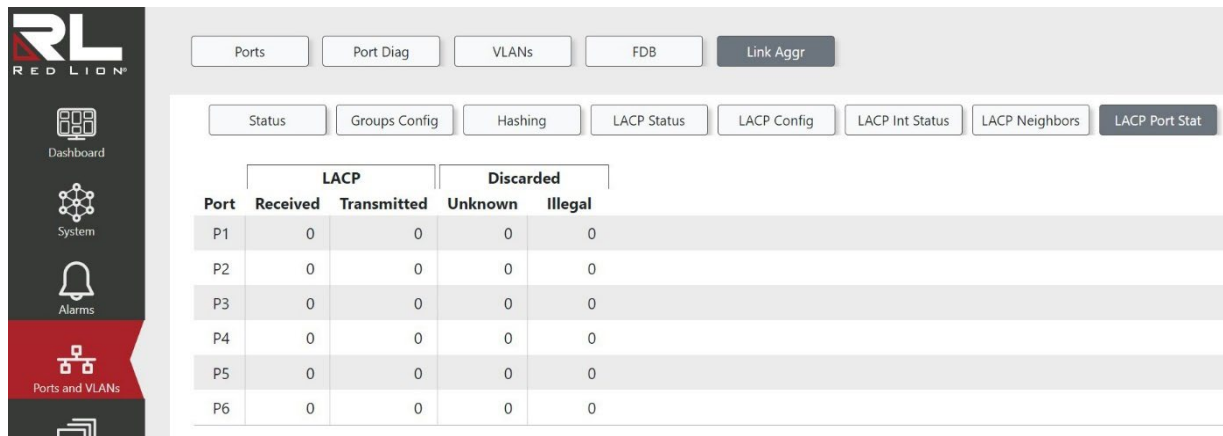
Expired: Indicates if the partner's Receive machine is in the EXPIRED state.

Buttons

 Click to refresh the values on the page.

 Automatic refresh occurs every 3 seconds.

LACP Port Stat



Port	LACP		Discarded	
	Received	Transmitted	Unknown	Illegal
P1	0	0	0	0
P2	0	0	0	0
P3	0	0	0	0
P4	0	0	0	0
P5	0	0	0	0
P6	0	0	0	0

This page provides an overview for LACP statistics for all ports.


Port: The switch port number.


LACP Received: Shows how many LACP frames have been received at each port.

LACP Transmitted: Shows how many LACP frames have been sent from each port.

Discarded: Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

 Click to refresh the values on the page.

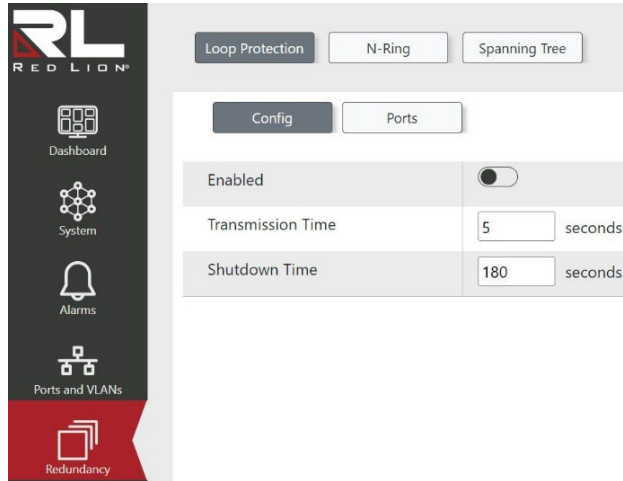
 Automatic refresh occurs every 3 seconds.

 Clears the counters for all ports.

Chapter 8 Redundancy

Loop Protection

Config



Loop protect, when enabled, detects a loop in the network setup by transmitting Protocol Data Units (PDUs) at a configurable time interval. When received and the PDUs have been determined to be self-generated, then the loop condition can be addressed as configured.

Note: If one of the Spanning Tree Protocols (STP, RSTP or MSTP) is enabled, then it shall manage the loop instead of Loop Protect.

Enabled: Enable or disable global loop protections.

Default: Disabled


Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.


Default: 5

Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event a loop is detected and the port action shuts down the port. Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled until next device restart.

Default: 180

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Ports

Port	Enabled	Transmit	Action	Is Looping	Loops	Link Status	Time of Last Loop
*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port				
P1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port		-	Up	-
P2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port		-	Up	-
P3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port		-	Down	-
P4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port		-	Up	-
P5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port		-	Down	-
P6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shutdown Port		-	Down	-

This page allows the user to configure Loop Protection options as well as view current status values for each port.

Port: The port name.

Enabled: Enable or disable loop protection on port.

Default: Enabled

Transmit: Enable or disable transmission of loop protection Protocol Data Units (PDU's).

Default: Enabled

Action:

Configure the action performed when a loop is detected on a port. All messages shall be logged in Syslog.

Shutdown Port

Shutdown Port and Log

Log Only

Default: Shutdown Port

Is Looping: Whether a loop is currently detected on the port.

Loops: The number of loops detected on this port.

Link Status: The current loop protection status of the port link.

Up

Down


Disabled

Time of Last Loop: The time and date of the last detected loop event.

Buttons

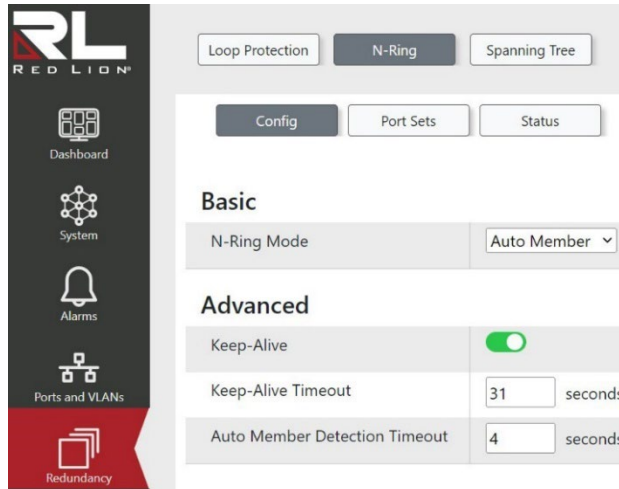
Automatic refresh occurs every 3 seconds.

Click to refresh the values on the page.

 Applies the changes to the device.

N-Ring™

Config



Configure N-Ring basic and advanced settings.

N-Ring Mode:

Indicates the N-Ring mode. Possible modes are:

Auto Member: The switch automatically detects when it is part of an N-Ring for participation in the ring.

Disabled: Prohibits N-Ring capabilities on the switch.

Default: Auto Member

Keep-Alive: Enable or disable the Keep-Alive feature. When enabled, the switch will remain as an active member unless no keep-alive request is received within the keep-alive timeout period.

Default: Enabled


Keep-Alive Timeout: Indicates the amount of time to wait (in seconds) to receive a keep-alive request before switching from active member back to auto member. The available range is 15 to 300 seconds. An entry of 0 will disable the Keep-Alive feature.


Default: 31

Auto Member Detection Timeout: Indicates 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 available range is 2 to 180 seconds.

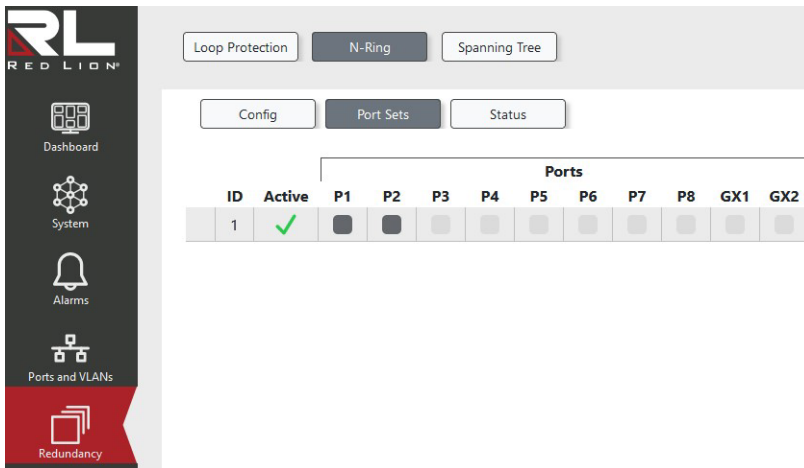
Default: 4

Buttons

 Click to refresh the values on the page.

 This button saves the current settings on the screen to the switch.

Port Sets



A port set is a group of two ports that may be used for an N-Ring™.

Click within the table to assign or unassign a port to a port set. A port set must consist of 2 (and only 2) ports. A port can only belong to one port set.





Row selection column: Click on the checkbox to select the row. Click again to de-select.

ID: Port set ID. An ID cannot be updated after saving, it can only be deleted. Valid values are in the range of 1 to 255.

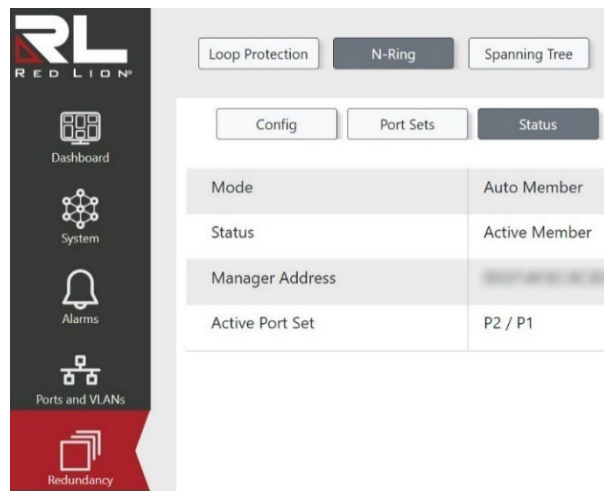
Active: Indicates if a port set is active, i.e. currently connected to an N-Ring.

Ports: Checkboxes indicate which ports belong to a port set.

Buttons

-  Click to add a new port set.
-  Click to delete the selected port sets.
-  Click to refresh the values on the page.
-  This button saves the current settings on the screen to the switch.

Status



View the current N-Ring™ status.

Mode: The current N-Ring mode of this switch. Possible values are:

Auto Member: Denotes the switch is configured to automatically detect when it is part of an N-Ring.

Disabled: Denotes the switch is configured not to participate in an N-Ring.

Status: The current N-Ring status of the switch. Possible values are:

Disabled: Denotes the switch will not participate in an N-Ring.

Detecting: Denotes the switch can participate in an N-Ring but is not actively participating.

Active Member: Denotes the switch is actively participating in an N-Ring.

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

Active Port Set: Shows the ports being used as N-Ring ports on this switch.

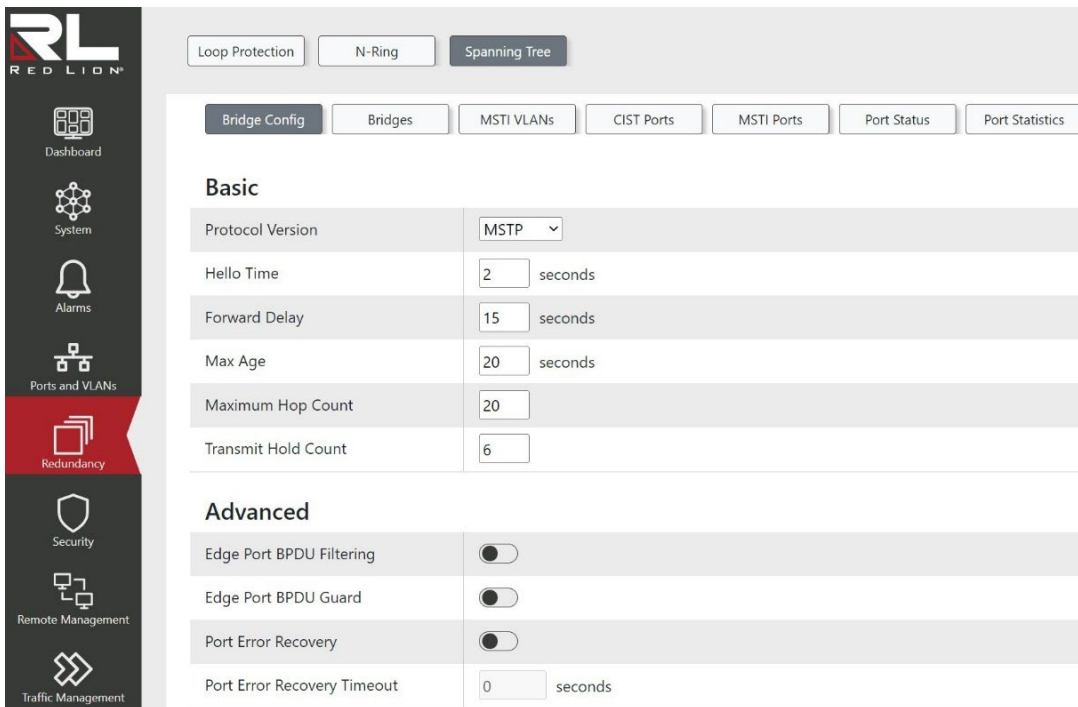
Buttons

(••) Automatic refresh occurs every 3 seconds.

↻ Click to refresh the values on the page.

Spanning Tree (STP)

Bridge Config



This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the switch.

Protocol Version:

Indicates the STP version to be used on all bridges. The options are:

- MSTP
- RSTP
- STP

Default: MSTP

Hello Time:

Indicates the time interval, in seconds, between the transmission of STP BPDU's. Valid values are in the range 1 to 10 seconds.

Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Default: 2 seconds

Forward Delay: Indicates the delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Default: 15 seconds

Max Age: Indicates the maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and Max Age must be less than or equal to $2 \times (\text{Forward Delay} - 1 \text{ second})$.

Default: 20 seconds

Maximum Hop Count: This field defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Default: 20 hops

Transmit Hold Count: Indicates the number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Default: 6 BPDU's per second

Edge Port BPDU Filtering: This field controls whether a port explicitly configured as Edge will transmit and receive BPDUs.

Default: Disabled

Edge Port BPDU Guard: This field controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Default: Disabled


Port Error Recovery: This field controls whether a port in the error-disabled state will automatically be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.


Default: Disabled

Port Error Recovery Timeout: Indicates the time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds.

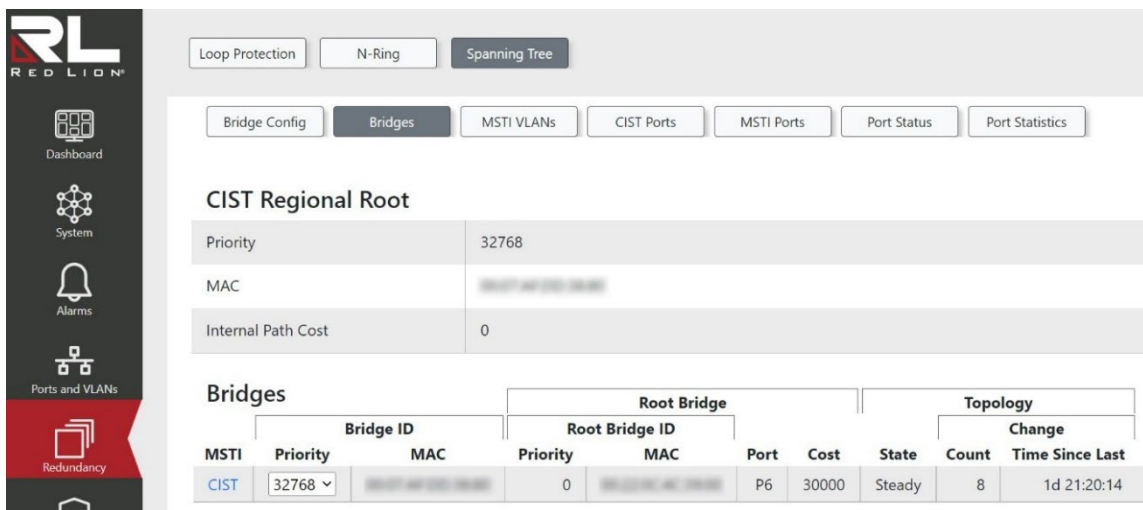
Default: 0 seconds

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Bridges



The screenshot shows the 'Spanning Tree' configuration page in the RedLion interface. At the top, there are tabs for 'Loop Protection', 'N-Ring', and 'Spanning Tree'. Below these are sub-tabs for 'Bridge Config', 'Bridges', 'MSTI VLANs', 'CIST Ports', 'MSTI Ports', 'Port Status', and 'Port Statistics'. The 'CIST Regional Root' section displays the following values:

- Priority: 32768
- MAC: [blurred]
- Internal Path Cost: 0

The 'Bridges' table is as follows:

MSTI	Bridge ID		Root Bridge ID		Port	Cost	State	Topology	
	Priority	MAC	Priority	MAC				Count	Change
CIST	32768	[blurred]	0	[blurred]	P6	30000	Steady	8	1d 21:20:14

This page provides a status overview of all STP bridge instances, as well as the configuration for the Bridge Identifier Priority for each STP bridge instance.

CIST Regional Root

This section displays the priority, MAC address, and the internal path cost of the CIST Regional Root.

Bridges

The displayed table contains a row for each STP bridge instance. Each row displays the Bridge ID, Root Bridge ID, and Topology Change information for the given instance. Bridge priority is also configured from this table.

CIST Regional Root Priority: Displays the priority of the CIST regional root.

CIST Regional Root MAC: Displays the MAC address of the CIST regional root.

CIST Regional Root Internal Path Cost: Displays the internal path cost, which is the cost to the CIST regional root in a region. This cost is only relevant to the IST, instance 0.

MSTI: Displays the Bridge Instance. This is also a link to the STP Port Status page for this bridge instance.

Bridge ID Priority: This field controls and displays the bridge priority for this bridge instance. Lower numeric values have higher priority.

Default: 32768

Bridge ID MAC: Displays the MAC address of this bridge instance.

Root Bridge ID Priority: Displays the priority of the Root Bridge for this bridge instance.

Root Bridge ID MAC: Displays the MAC address of the Root Bridge for this bridge instance.

Root Bridge Port: Displays the switch port currently assigned the root port role for this bridge instance.

Root Bridge Cost: Displays the Root Path Cost for this bridge instance. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least costly path to the Root Bridge.

Topology State: Displays the current topology state of this bridge instance.

Topology Change Count: Displays the number of times a topology change has occurred since the switch has been powered on or rebooted for this bridge instance.

Topology Change Time Since Last: Displays the time that has elapsed since last topology change occurred for this bridge instance.

Buttons

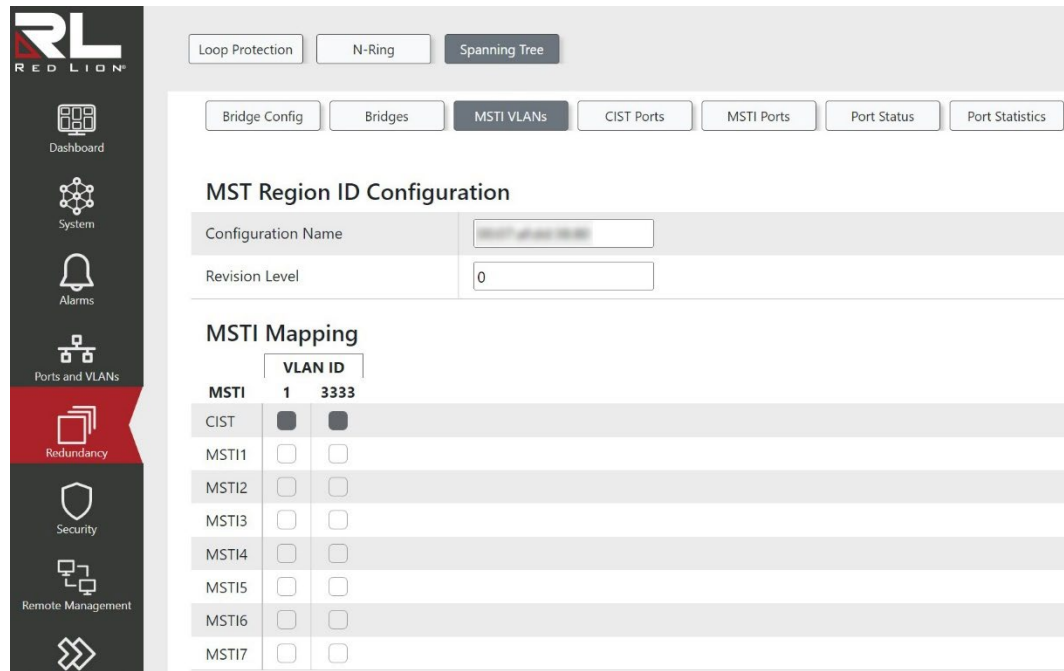


Click to refresh the values on the page.



Applies the changes to the device.

MSTI VLANs



This page allows you to configure the MST Region ID and to map VLANs to bridge instances. These settings apply only to the MSTP protocol.

MST Region ID Configuration

All MSTP capable devices within an MST Region must share the same configuration name and revision, as well as the same VLAN to MSTI mappings in order to create a well-formed Spanning Tree.

MSTI Mapping

Click within the table to assign or unassign a VLAN to an instance. A VLAN can only be mapped to one instance. An instance can have more than one VLAN mapped to it.

The CIST automatically contains every VLAN that is not explicitly mapped to another instance.

Configuration Name: The name identifying this MST configuration. The name is at most 32 characters long.

Default: Switch MAC Address


Revision Level: The revision of this MST configuration. Valid values are in the range of 0 to 65535.


Default: 0

MSTI: The MSTI to map a VLAN to.

VLAN ID: The VLAN ID to map to a MSTI.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

CIST Ports

Port	Enabled	Priority	Path Cost		Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-Point
			Auto	Specific			Role	TCN		
*	<input checked="" type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
LLAGs	<input checked="" type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True
P1	<input type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
P2	<input type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
P3	<input checked="" type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
P4	<input checked="" type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
P5	<input checked="" type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
P6	<input checked="" type="checkbox"/>	128	<input checked="" type="checkbox"/>	0	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

This page allows you to configure the STP port settings for CIST ports.

Port: Displays the switch port number of the logical STP port.

Enabled: This field controls whether the STP is enabled on this switch port.

Default: Enabled

Priority: This field configures the priority of the port or LAG. This can be used to control the relative priority of ports with identical port costs. A lower port priority is better.

Default: 128

Path Cost (Auto or Specific): This field configures the path cost incurred by the port or LAG. The 'Auto' setting sets the path cost as appropriate for the physical link speed, using the IEEE 802.1D recommended values. Otherwise, a user-specific value can be supplied. The path cost is used when establishing the active topology of the network. Ports with a lower path cost are chosen as forwarding ports in favor of those with higher path costs. Valid values are in the range of 1 to 200,000,000.

Default: Auto

Admin Edge: This field configures the port to initialize as an Edge Port.

Default: Non-Edge

Auto Edge: This field controls whether the bridge should enable automatic edge detection on the bridge port. This allows the port to set its Edge Port status by whether BPDU's are received on the port or not.

Default: Enabled

Restricted Role: This field enables or disables the Restricted Role setting. If enabled, this causes the port not to be selected as the root port for the CIST or any MSTI, even if it has the best Spanning Tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the Spanning Tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Default: Disabled

Restricted TCN: This field enables or disables the Restricted TCN setting. If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a Spanning Tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

Default: Disabled

BPDU Guard: This field enables or disables the BDPU Guard setting. If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.


Default: Disabled


Point-to-Point: This field controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for Point-to-Point LANs than for shared media.

Default Port: Auto

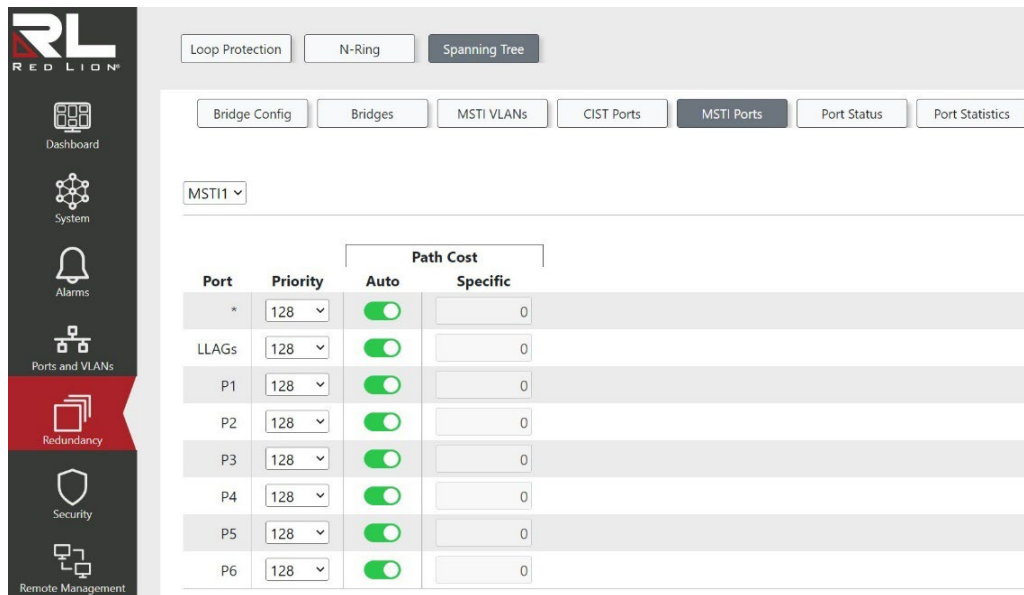
Default LLAGs: Forced True

Buttons

 Click to refresh the values on the page.

 This button saves the current settings on the screen to the switch.

MSTI Ports



Port	Priority	Path Cost	
		Auto	Specific
*	128	<input checked="" type="checkbox"/>	0
LLAGs	128	<input checked="" type="checkbox"/>	0
P1	128	<input checked="" type="checkbox"/>	0
P2	128	<input checked="" type="checkbox"/>	0
P3	128	<input checked="" type="checkbox"/>	0
P4	128	<input checked="" type="checkbox"/>	0
P5	128	<input checked="" type="checkbox"/>	0
P6	128	<input checked="" type="checkbox"/>	0

This page allows you to configure settings for MSTI ports. A port is instantiated separately for each MSTI instance. Use the MSTI dropdown to select the MSTI you wish to configure.

Port: Displays the name of the physical switch port.


Priority: This field configures the priority of the port or LAG. This can be used to control the relative priority of ports with identical port costs. A lower port priority is better.


Default: 128

Path Cost (Auto or Specific): This field configures the path cost incurred by the port or LAG. The 'Auto' setting sets the path cost as appropriate for the physical link speed, using the IEEE 802.1D recommended values. Otherwise, a user-specific value can be supplied. The path cost is used when establishing the active topology of the network. Ports with a lower path cost are chosen as forwarding ports in favor of those with higher path costs. Valid values are in the range of 1 to 200,000,000.

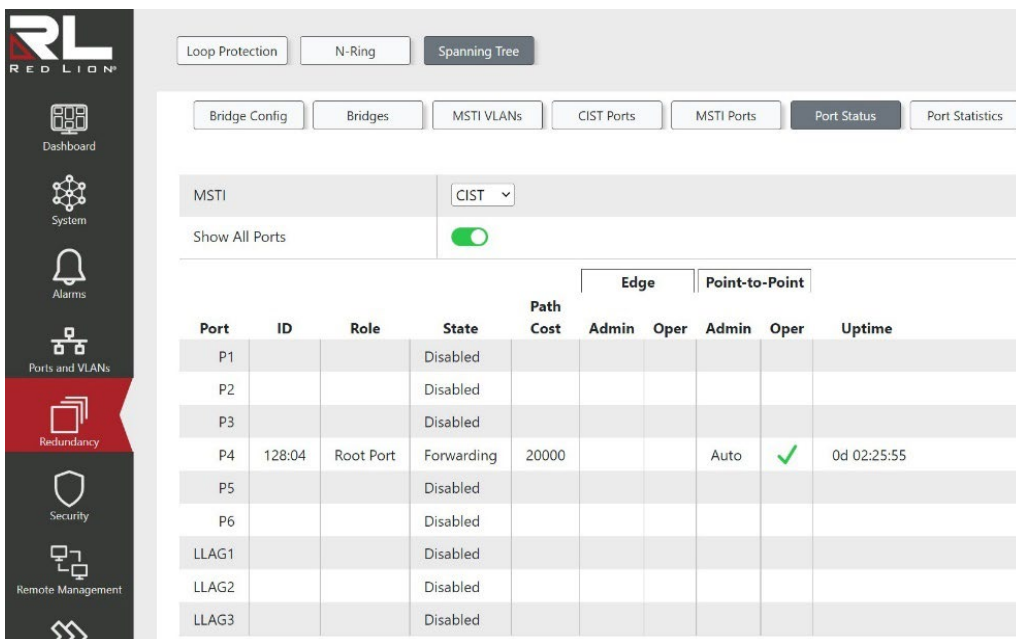
Default: Auto

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Port Status



The screenshot shows the 'Spanning Tree' configuration page in the Red Lion network management interface. The 'Port Status' tab is active, displaying a table of STP port statuses for the CIST instance. The table includes columns for Port, ID, Role, State, Path Cost, Admin, Oper, Uptime, and checkboxes for Edge and Point-to-Point. Port P4 is the Root Port in the Forwarding state with a path cost of 20000 and an uptime of 0d 02:25:55.

Port	ID	Role	State	Path Cost	Edge		Point-to-Point		Uptime
					Admin	Oper	Admin	Oper	
P1			Disabled						
P2			Disabled						
P3			Disabled						
P4	128:04	Root Port	Forwarding	20000			Auto	✓	0d 02:25:55
P5			Disabled						
P6			Disabled						
LLAG1			Disabled						
LLAG2			Disabled						
LLAG3			Disabled						

This page allows you view the current status of STP ports. STP port statuses are separated into instances. Select 'CIST' or one of the MSTIs from the 'MSTI' dropdown menu to view the port statuses for that MSTI. To show/hide non-active STP ports toggle 'Show All Ports.'

Port: Displays the name of the physical switch port.

ID: Displays the port ID as used by STP. ID comprises of port priority and the logical port number of the bridge port. Ports that are members of a LAG will use the ID associated with the LAG they are a member of.

Role: Displays the current STP role of the port or LAG. The role can be one of the following:

- Alternate Port
- Alternate Backup Port
- Backup Port

- Root Port
- Master Port
- Designated Port
- Disabled Port
- Unknown Port
- Member of LLAG

State: Displays the current STP state of the port or LAG. The state can be one of the following:

- Discarding
- Learning
- Forwarding
- Disabled
- Error Disabled

Path Cost: Displays the current STP path cost incurred by the port or LAG. This value will either be computed from the 'Auto' setting, or any explicitly configured value.

Admin Edge: Indicates whether or not the port is configured to be an edge port.


Oper Edge: Indicates whether or not the port is actively an edge port.


Admin Point-to-Point: Indicates whether or not the port the port is configured to be a point-to-point port.

Oper Point-to-Point: Indicates whether or not the port is actively a point-to-point port.

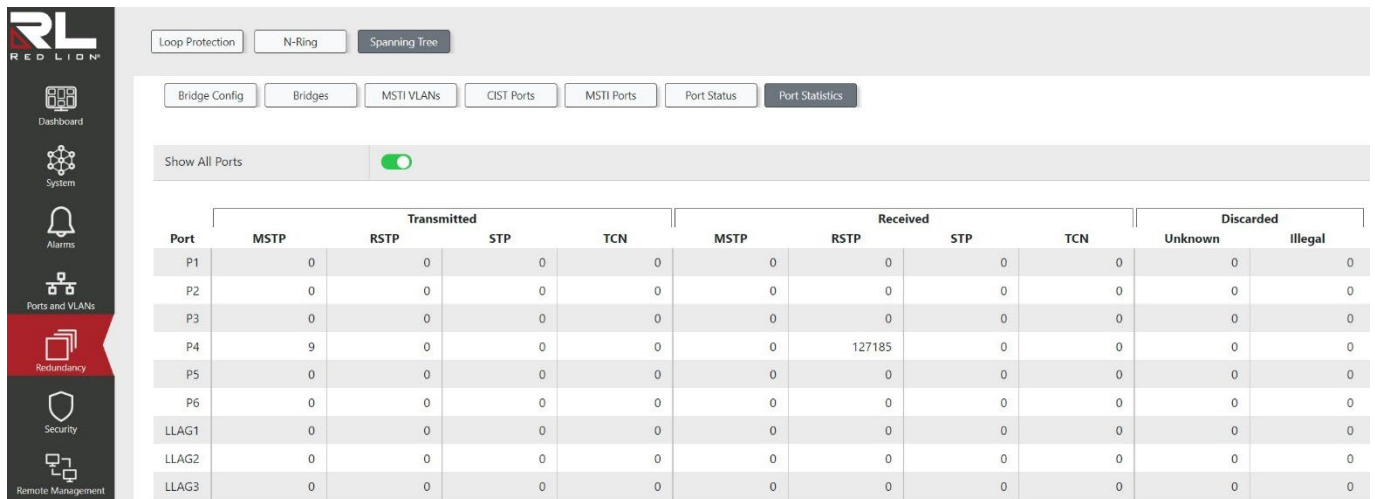
Uptime: Displays the time that has elapsed since the bridge port was last initialized.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

Port Statistics



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
P1	0	0	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0	0	0	0
P4	9	0	0	0	0	127185	0	0	0	0
P5	0	0	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	0	0	0	0	0
LLAG1	0	0	0	0	0	0	0	0	0	0
LLAG2	0	0	0	0	0	0	0	0	0	0
LLAG3	0	0	0	0	0	0	0	0	0	0

This page displays the STP port statistics counters of bridge ports and LAGs in the switch. To show/hide non-active STP ports toggle 'Show All Ports.'

The STP port statistics counters are:

Port: Displays the switch port number of the logical STP port.

MSTP: Displays the number of MSTP BPDU's received/transmitted on the port.

RSTP: Displays the number of RSTP BPDU's received/transmitted on the port.




STP: Displays the number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN: Displays the number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Unknown: Displays the number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Illegal: Displays the number of illegal Spanning Tree BPDU's received (and discarded) on the port.

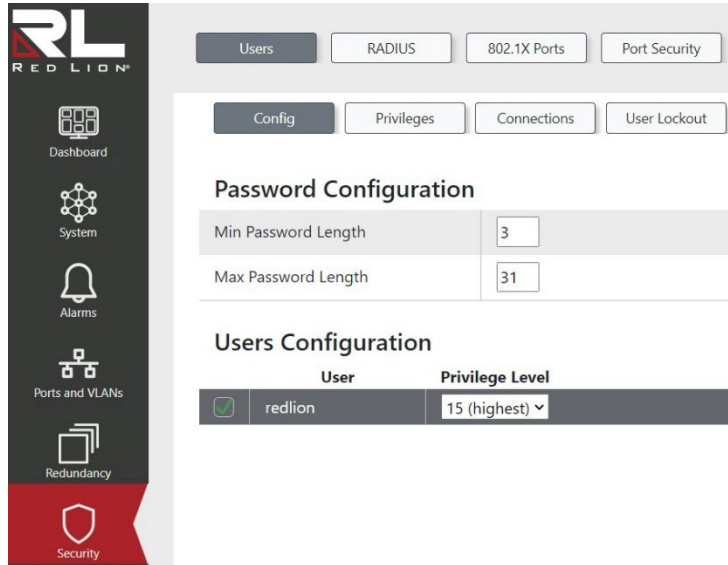
Buttons

-  Click to reset all STP port counters.
-  Automatic refresh occurs every 3 seconds.
-  Click to refresh the values on the page.

Chapter 9 Security

Users

Config



This page provides an overview of the current users and configuration for password length.

Min Password Length: The minimum number of characters allowed in a user password. Valid values are 3-31. The min value must be less than or equal to the max value.

Default: 3

Max Password Length: The maximum number of characters allowed in a user password. Valid values are 3-31. The max value must be greater than or equal to the min value.

Default: 31

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

User: The name identifying the user.

Privilege Level: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, the user has full control of the device, and other level selections depend on the access level of each group. A user's privilege level should meet or exceed the group privilege level to have access to that group.


Default: 0 (lowest)

Buttons

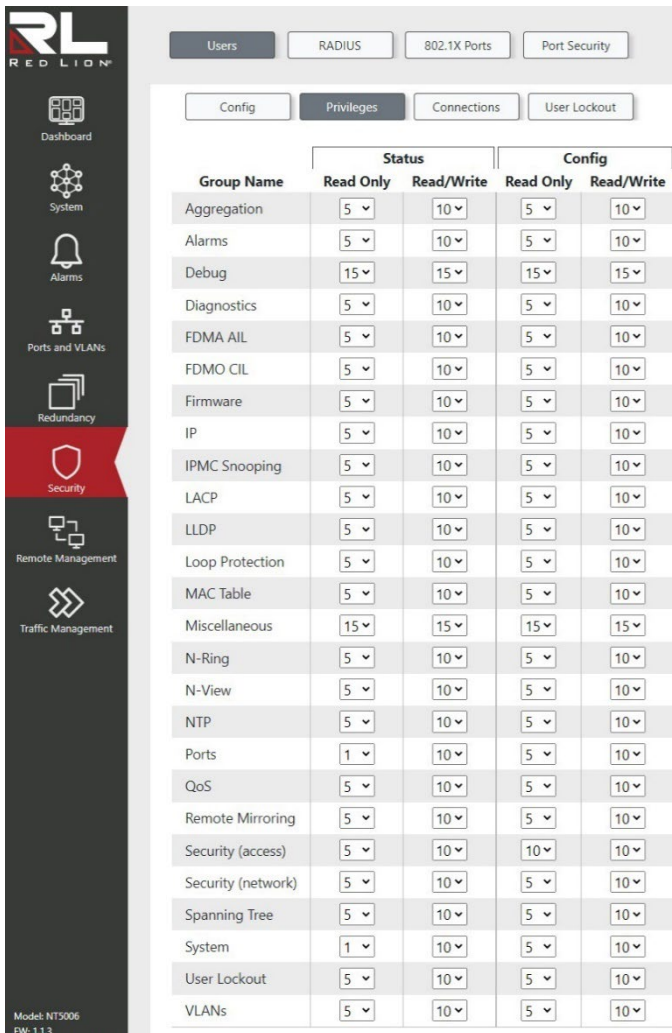
+ Click to add a new user. The maximum numbers of users is 20.

🗑️ This button deletes the currently selected entries from the switch.

↻ Click to refresh the values on the page.

 Applies the changes to the device.

Privileges



Group Name	Status		Config	
	Read Only	Read/Write	Read Only	Read/Write
Aggregation	5	10	5	10
Alarms	5	10	5	10
Debug	15	15	15	15
Diagnostics	5	10	5	10
FDMA AIL	5	10	5	10
FDMO CIL	5	10	5	10
Firmware	5	10	5	10
IP	5	10	5	10
IPMC Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop Protection	5	10	5	10
MAC Table	5	10	5	10
Miscellaneous	15	15	15	15
N-Ring	5	10	5	10
N-View	5	10	5	10
NTP	5	10	5	10
Ports	1	10	5	10
QoS	5	10	5	10
Remote Mirroring	5	10	5	10
Security (access)	5	10	10	10
Security (network)	5	10	5	10
Spanning Tree	5	10	5	10
System	1	10	5	10
User Lockout	5	10	5	10
VLANs	5	10	5	10

This page provides an overview of the privilege levels.

Group Name: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. These privilege level groups in detail are:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH

IP: Everything except 'ping'

Port: Everything except 'VeriPHY'

Diagnostics: 'ping' and 'VeriPHY'

Maintenance:


CLI: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load, and Firmware Load


Web: Users, Privilege Levels and everything in Maintenance

Debug: Only present in CLI

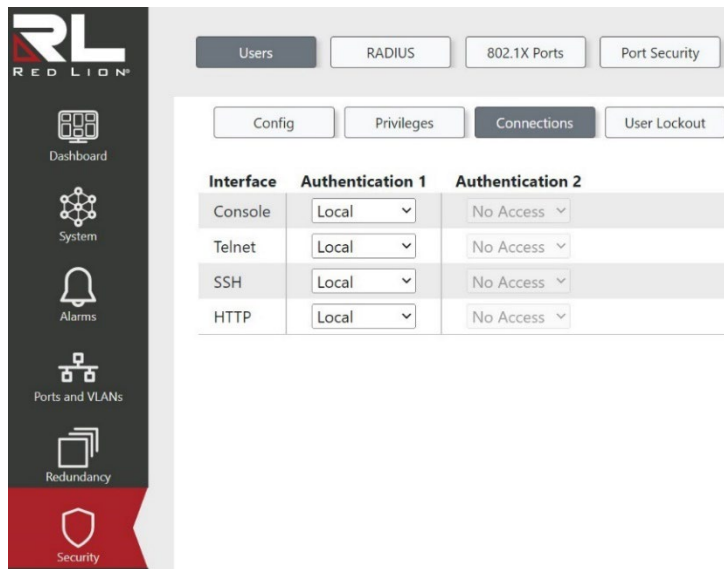
Privilege Levels: The privilege level of the user. The allowed range is 0 to 15. If the value of the privilege level is 15, it has full control of the device, but other values need to refer to each group privilege level. A user's privilege should be same or greater than the group privilege level to access that group. Groups with privilege level 5 have read-only access, and privilege level 10 grants read-write access. System maintenance groups (software upload, factory defaults, etc.) need user privilege level 15. Privilege levels can be assigned for status operations and configuration operations. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Connections



This page allows you to configure how a user is authenticated when they log in to the switch via one of the management client interfaces. The table has one row for each client type.

Interface: The management client for which the configuration below applies.

Authentications:

Select the Authentication Method. Possible values are:


No Access: Authentication is disabled, and login is not possible.


Local: Use the local user database on the switch for authentication.

Radius: Use remote RADIUS server(s) for authentication.

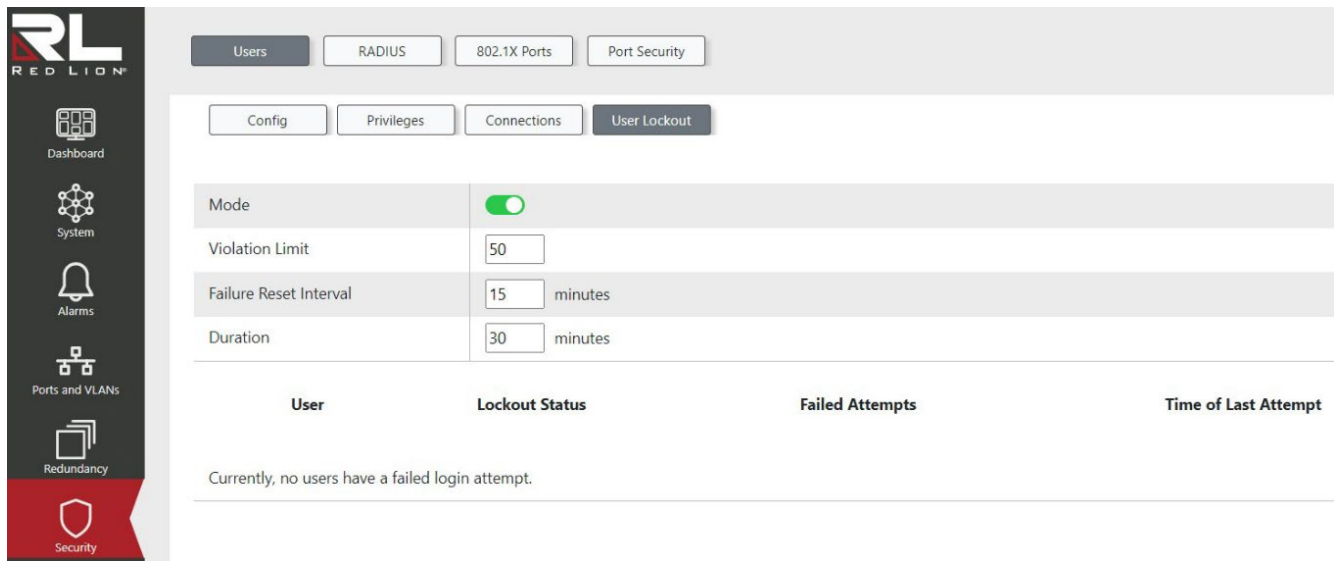
Methods that involve remote servers are timed out if the remote servers are offline. In this case, the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication, it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

User Lockout



Mode	<input checked="" type="checkbox"/>
Violation Limit	<input type="text" value="50"/>
Failure Reset Interval	<input type="text" value="15"/> minutes
Duration	<input type="text" value="30"/> minutes

User	Lockout Status	Failed Attempts	Time of Last Attempt
Currently, no users have a failed login attempt.			

This page allows you to configure settings for user lockout, view the status of all users that have had a failed login attempt or lockout that has not expired, and reset a user's failed attempt count and lockout status. All lockout and unlock events are recorded in the Syslog.

Mode: Enable or disable user lockout.

Default: Enabled

Violation Limit: The number of failed login attempts that can occur before a subsequent failed login attempt will lockout the user. Valid values are 1-999.

Default: 50

Failure Reset Interval: The amount of time, in minutes, that must elapse after a failed login attempt before a user's failed attempts count is reset to 0. Valid values are 1-120 minutes.

Default: 15

Duration: The amount of time that a user will be locked out after the violation limit has been surpassed. Setting a value of 0 will result in locked users remaining locked until an admin unlocks them. Valid values are 0-65535 minutes.

Default: 30




User: The name identifying the user.

Lockout Status: Displays the current lockout status of the user.

Failed Attempts: Displays the number of failed login attempts.

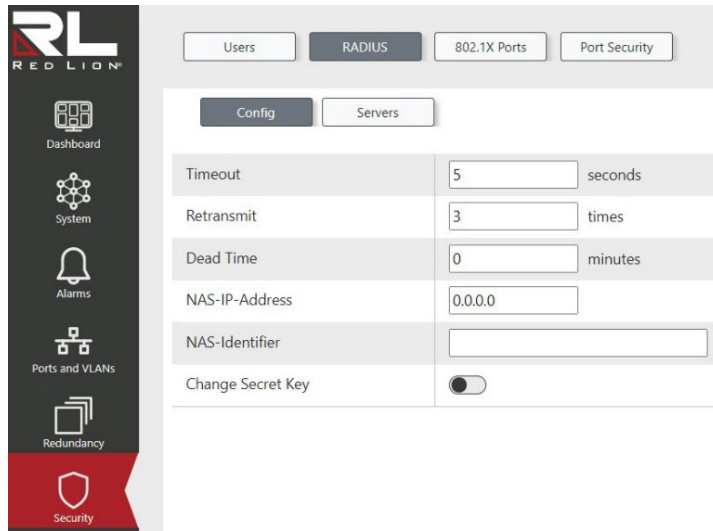
Time of Last Attempt: Displays the time of the last failed login attempt.

Buttons

-  Delete selected users from the lockout table resetting the user's lockout status.
-  Click to refresh the values on the page.
-  This button saves the current settings on the screen to the switch.

RADIUS

Config



RADIUS	
Config	
Timeout	5 seconds
Retransmit	3 times
Dead Time	0 minutes
NAS-IP-Address	0.0.0.0
NAS-Identifier	
Change Secret Key	<input type="checkbox"/>

This page allows you to configure settings that are global to all the RADIUS servers.

Timeout: Configure the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Default: 5

Retransmit: Configure the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Default: 3

Dead Time: Configure the period, in the range of 0 to 1440 minutes, during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Default: 0

NAS-IP-Address: The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. The value must be a valid IPv4 address in dotted decimal notation ('x.y.z.w'). The following restrictions apply:

- x must be a decimal number between 1 and 223.
- x must not be 127.

y, z, and w must be decimal numbers between 0 and 255.

NAS-Identifier: The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.


Change Secret Key: Enable or disable the ability to change the current secret key shared between the RADIUS server and the switch.


Default: Disabled

Secret Key: Enter text to change the secret key - up to 63 characters long - shared between the RADIUS server and the switch.

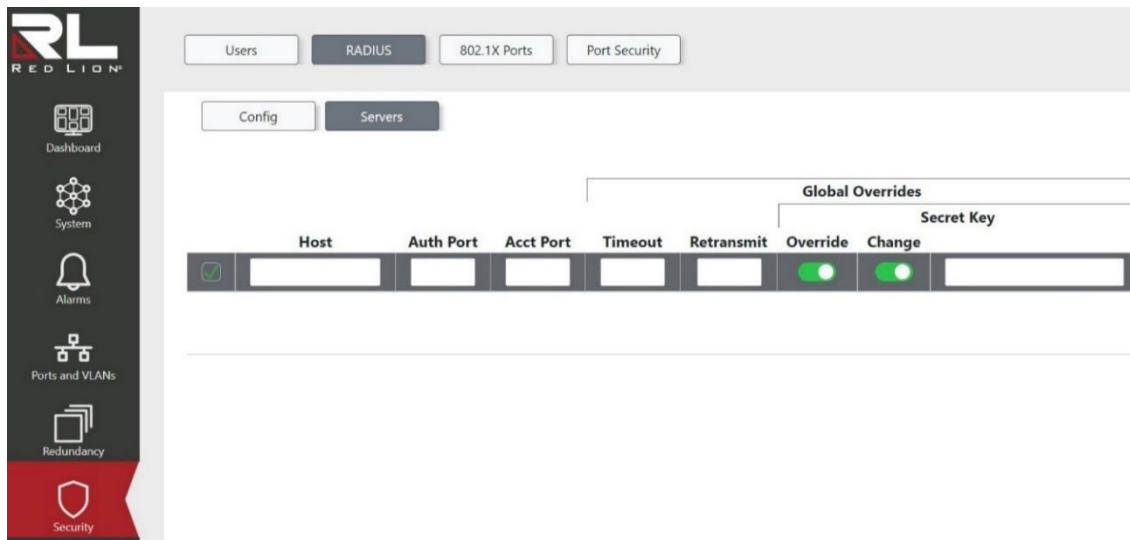
Note: This field is hidden unless **Change Secret Key** is enabled.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Servers



This page allows you to configure up to 5 RADIUS servers.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Host: The IPv4 address of the RADIUS server.

Auth Port: The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Default: 1812

Acct Port: The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

Default: 1813

Timeout: This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. Valid values are from 1 to 1000 seconds.

Retransmit: This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value. Valid values are from 1 to 1000 times.

Override: Enable or disable the server specific secret key that is shared between the RADIUS server and the switch. When enabled, the server specific secret key is used. When disabled, the global secret key is used.

Default: Enabled

Change:

Enable or disable the ability to change the server-specific secret key shared between the RADIUS server and the switch.


Note: This field is hidden unless **Override** is enabled.


Default: Enabled


Secret Key: Enter text to change the server specific secret key. This setting overrides the global key if enabled. Maximum of 63 characters.


Note: This field is not configurable unless **Override** and **Change** are enabled.

Buttons

 Add new RADIUS server. There can be a maximum of 5.

 Delete selected RADIUS server.

 Click to refresh the values on the page.

 Applies the changes to the device.

802.1X Ports

Config

802.1X Ports	
Enabled	<input type="checkbox"/>
Reauthentication	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS	<input type="checkbox"/>
RADIUS-Assigned VLAN	<input type="checkbox"/>
Guest VLAN	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

This page configures the 802.1X ports across the entire system.

Enabled: Enable or disable NAS globally on the switch. If globally disabled, all ports are allowed forwarding of frames.

Default: Disabled

Reauthentication: Enable or disable reauthentication. If enabled, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Default: Disabled

Reauthentication Period: Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if Reauthentication is enabled. Valid values are in the range 1 to 3600 seconds.

Default: 3600

EAPOL Timeout: Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Default: 30

Aging Period:

Determines the aging period. This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

Single 802.1X

Multi 802.1X
MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. If reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Default: 300

Hold Time:

Determines the hold period. This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

Single 802.1X
Multi 802.1X
MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

Default: 10

RADIUS-Assigned QoS: Enable or disable RADIUS-assigned QoS. RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. (See RADIUS-Assigned QoS Enabled below for a detailed description.) The RADIUS-Assigned QoS option provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When enabled, the individual ports' ditto setting determines whether the RADIUS-assigned QoS Class is enabled on that port. When disabled, the RADIUS-server assigned QoS Class is disabled on all ports.

Default: Disabled

RADIUS-Assigned VLAN: Enable or disable RADIUS-assigned VLAN. RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. (See RADIUS-Assigned VLAN Enabled below for a detailed description.) The RADIUS-assigned VLAN option provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When enabled, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When disabled, RADIUS-server assigned VLAN is disabled on all ports.

Default: Disabled

Guest VLAN: A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The Guest VLAN Enabled checkbox provides a quick way to globally enable / disable Guest VLAN

functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Default: Disabled

Guest VLAN ID: This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].

Default: 1


Max. Reauth. Count: The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].


Default: 2

Allow Guest VLAN if EAPOL Seen: Enable or disable whether to allow Guest VLAN if an EAPOL frame has been received. The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled, the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled, the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port. The value can only be changed if the Guest VLAN option is globally enabled.

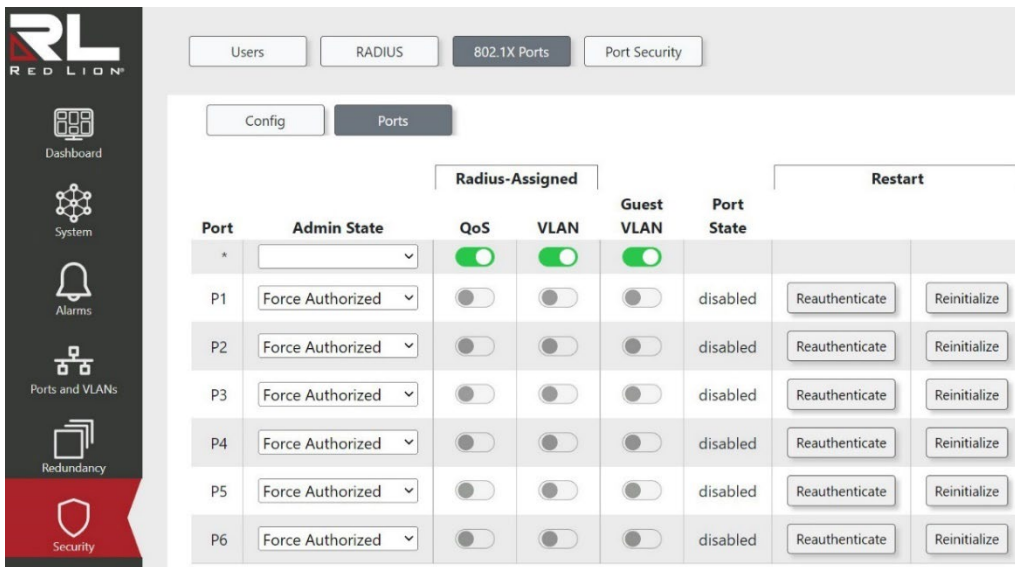
Default: Disabled

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Ports



Port	Admin State	Radius-Assigned			Port State	Restart	
		QoS	VLAN	Guest VLAN		Reauthenticate	Reinitialize
*	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
P1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disabled	Reauthenticate	Reinitialize
P2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disabled	Reauthenticate	Reinitialize
P3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disabled	Reauthenticate	Reinitialize
P4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disabled	Reauthenticate	Reinitialize
P5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disabled	Reauthenticate	Reinitialize
P6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disabled	Reauthenticate	Reinitialize

This page allows you to configure the IEEE 802.1X port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

The port configuration table has one row for each port on the switch and a number of columns, which are:

Port: The port number for which the configuration below applies.

Admin State: If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-Based 802.1X: In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds, and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access, even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard but features many of the same characteristics, as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant

will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X, it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination, to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-Based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string following the form 'xx-xx-xx-xx-xx-xx'. In other words, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users; equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

QoS:

Enable or disable RADIUS-Assigned QoS. When RADIUS-Assigned QoS is both globally enabled and enabled on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.

Port-based 802.1X
Single 802.1X

RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

VLAN:

Enable or disable RADIUS-Assigned VLAN. When RADIUS-Assigned VLAN is both globally enabled and enabled for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.

Port-based 802.1X

Single 802.1X

RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

Value of Tunnel-Medium-Type must be set to 'IEEE-802' (ordinal 6)

Value of Tunnel-Type must be set to 'VLAN' (ordinal 13).

Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN:

Enable or disable Guest VLAN. When Guest VLAN is both globally enabled and enabled for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

Port-based 802.1X

Single 802.1X

Multi 802.1X

Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the 'Allow Guest VLAN if EAPOL Seen' is disabled.

Port State: The current state of the port. It can undertake one of the following values:

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.


X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.


Restart: Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.

Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Port Security

Ports

Port	Mode	Users	Limit	Violation		Sticky	State	MAC Count	
				Mode	Limit			Current	Violating
<input type="checkbox"/>	*	Disabled	4	Protect	4	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	P1	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled	0	0
<input type="checkbox"/>	P2	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled	0	0
<input type="checkbox"/>	P3	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled	0	0
<input type="checkbox"/>	P4	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled	0	0
<input type="checkbox"/>	P5	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled	0	0
<input type="checkbox"/>	P6	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled	0	0

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this limit is exceeded, an action is taken depending on the violation mode, described below.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Port: The port number to which the configuration below applies. This is a clickable link that opens the Detailed Status page for the port.

Mode:

Enable or disable Port Security for the port.

Note: Other pages may still use the underlying Port Security features without enabling Port Security on a given port.

Default: Disabled.

Users: The user field is a combination of whether or not the user is an Admin, as well as whether or not the user has 802.1X enabled. Possible values for this field include:

'- -': Indicates that Port Security has not been admin enabled, and the port is not an 802.1X port.

'Admin, -': Indicates that Port Security has been admin enabled, but that 802.1X is not in use for the port.

'-, 802.1X': Indicates that Port Security has not been admin enabled, and the port uses 802.1X.

'Admin, 802.1X': Indicates that Port Security has been admin enabled, and the port uses 802.1X for the port.

Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. If the limit is exceeded, an action is taken corresponding to the violation mode.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used

all available MAC addresses.

Default: 4

Violation Mode:

This field configures the action to be taken, if the violation limit is exceeded. The available options are:

Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.

Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.

Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned.

Note: If a port has been shut down due to a violation of the MAC address limit, there are three ways to re-enable the port:

In the "Ports Status/Config" page, first disable the port and apply the settings. Then re-enable the port to restore the original configuration and apply the settings.

Make a Port Security configuration change on the disabled port and apply the settings.

Reboot the switch.

Default: Protect

Violation Limit: The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023.

Default: 4.

Sticky: Enable or disable sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky. Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

A port can be Sticky-enabled whether or not Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses managementwise before enabling Port Security. To do that, use the "Port Security MAC Addresses" page.

Default: Disabled

State: Shows the current state of the port. It can take one of these possible values:

Disabled: No users are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user, and is awaiting frames from unknown MAC addresses to arrive. If the limit is reached, the Port Security service is administratively enabled.





Shut Down: The Port Security service is administratively enabled and the port is shut down. No MAC addresses can be learned on the port until it is administratively re-opened by taking the port down and then back up on the "Ports Status/Config" page. Alternatively, the switch may be booted or reconfigured through Port Security.

Limit Reached: The maximum number of MAC Addresses has been learned on this port.

MAC Count Current: Indicates the total count of learned MAC addresses, forwarding as well as blocked, on the port.

MAC Count Violating: Indicates the count of MAC addresses that have exceeded the Violation Limit on the port. This field is only active for ports whose Violation mode is configured as 'Restrict'.

Buttons

-  Click to clear the port data.
-  Click to toggle automatic refresh every 3 seconds.
-  Click to refresh the page. Note that non-committed changes will be lost.
-  Applies the changes to the device.

Detailed Status

This page shows the MAC addresses secured by Port Security. To view only MAC addresses for a specific port, select the port from the dropdown menu above the table.

Note: User-configured Static and Sticky MAC addresses will only be shown on this page for ports that have Port Security enabled.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Port: Indicates the name of the physical switch port to which the MAC address is bound.

VLAN ID: Indicates the VLAN ID with which the ingress frames, associated with the MAC addresses, were tagged.

Mac Address: Indicates the MAC address that is being monitored by Port Security.

Type: Indicates the type of entry. Possible entries are:

Dynamic: The MAC address entry was learned dynamically from ingress frames on a Port Security enabled port that does not have sticky learning enabled.

Static: The MAC address entry was configured and saved by an admin user. Static entries are not subject to aging.

Sticky: The MAC address entry was learned dynamically from ingress frames on a Port Security enabled port that has sticky learning enabled. Sticky MAC address entries will not be lost due to port link changes (in contrast to Dynamic, which will have to be learned again). Sticky MAC address entries are part of the running-config and can therefore be saved to the startup-config, allowing them to survive a reboot of the switch.

State: Indicates the current Port Security state of the MAC address entry. Possible states are:

Forwarding: Frames associated with this MAC address on this port will be forwarded.


Violating: This MAC address was received on a port that has been configured with Violation Mode set to Restricted and this MAC address entry exceeds the Violation Limit. Frames associated with this MAC address on this port will be discarded.


Age/Hold:Indicates the remaining value of the Aging Period or Hold Time for the MAC address entry. Possible configurations based on the state are:


State is Forwarding: This field indicates the remaining time, in seconds, before the MAC Address entry ages out and is removed from the MAC table. A '-' displayed in this field by a forwarding MAC Address entry indicates aging is disabled, or the MAC address has been configured to be held indefinitely.

State is Violating: This field indicates the remaining time, in seconds, that the violating MAC address will be held before being removed from the MAC table.

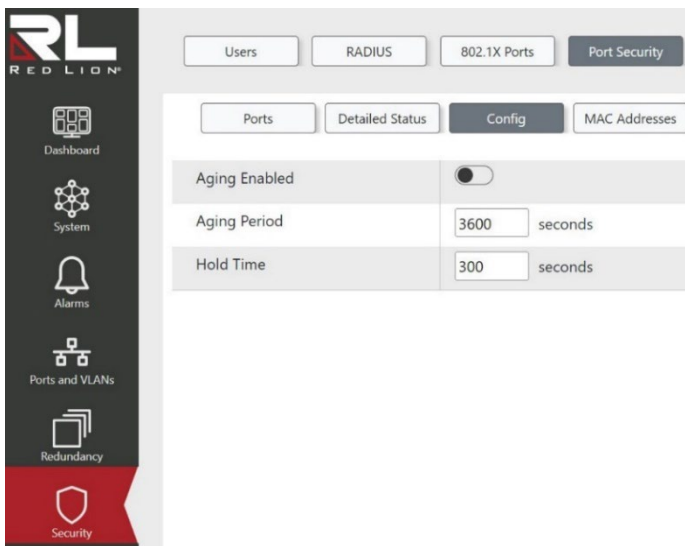
Buttons

 This button deletes the currently selected entries from the switch.

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

Config



This page allows you to configure the global Port Security settings.

Aging Enabled: Enable or disable Aging on the switch.

Default: Disabled


Aging Period: This field configures the time, in seconds, that forwarding MAC addresses will be held in the MAC table before they age out. A MAC address that has aged out will be removed from the MAC table if no frames from the MAC address have been received within the next Aging Period. Valid ranges are between 10 and 100000000 seconds.


Default: 3600

Hold Time: This field configures the time, in seconds, that MAC addresses who are in violation of a ports violation limit will be held before being removed from the MAC table. This is to limit the frequency of Syslog events.

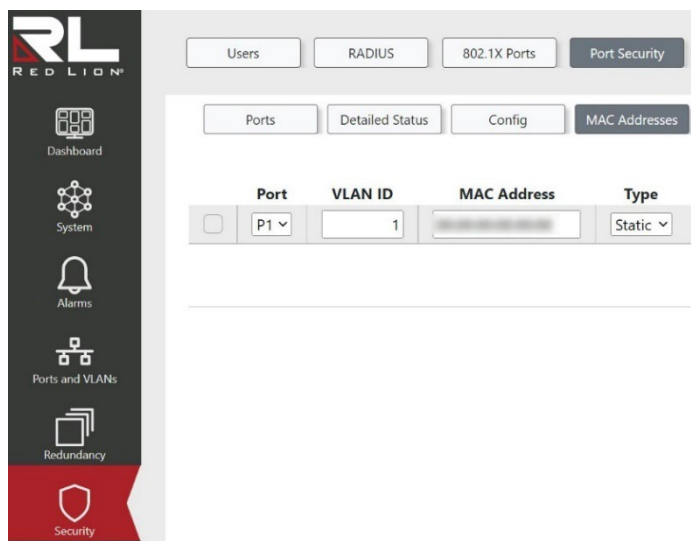
Default: 300

Buttons

 Click to refresh the values on the page.

 This button saves the current settings on the screen to the switch.

MAC Addresses



This page shows the MAC addresses secured by the Port Security module. Port Security may be configured both administratively and indirectly through other software modules - the so-called user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the Port Security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Notice that if you have added static or sticky MAC addresses, they will show up on this page only if Port Security is enabled on the interface to which they pertain.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Port: Select the port ID from the drop down to which the MAC address is bound.

Default: P1

VLAN ID: Enter the VLAN ID that is seen on this port.

Default: 1

MAC Address: Enter the MAC address that is seen on this port.

Default: 00:00:00:00:00:00

Type:

Indicates the type of entry. Possible values are:





Static: The entry is entered by the end-user through management. Entry is not subject to aging.

Sticky: When the port is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config. Though not the intention with Sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

Note: It is not recommended to add Sticky addresses in this way.

Default: Static

Buttons

-  Click to add a new entry.
-  Click to delete the selected MAC Address entry.
-  Click to refresh values on the page.
-  Applies the changes to the device.

Chapter 10 Remote Management

Access

IP Access Stats

Interface	Packets		
	Received	Allowed	Discarded
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

This page provides access statistics for various remote management interfaces. These values are only updated when Access Configuration is enabled via the IP Access Config screen.

Interface: The interface type through which the remote host can access the switch. Possible options are:




- HTTP
- HTTPS
- SNMP
- TELNET
- SSH

Received: Number of received packets from the interface when Access Configuration is enabled.

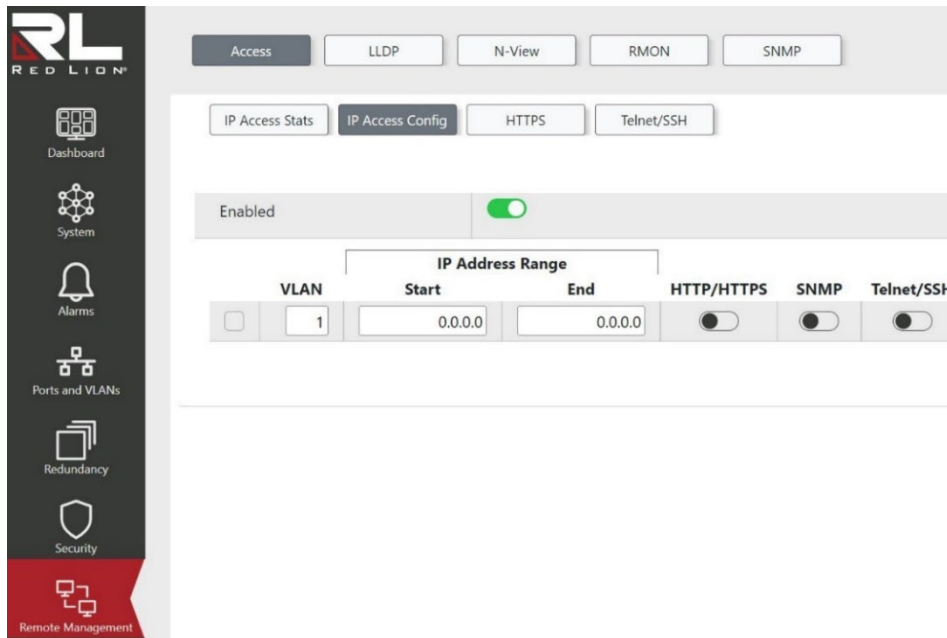
Allowed: Number of allowed packets from the interface when Access Configuration is enabled.

Discarded: Number of discarded packets from the interface when Access Configuration is enabled.

Buttons

-  Click to refresh values on the page.
-  Automatic refresh occurs every 3 seconds.
-  Resets all counters to zero.

IP Access Config



Configure remote management access settings on this page. The maximum number of entries is 16. If enabled, and a remote host uses settings that match an entry on this page (using an IP Address in the specified range), then they will be allowed to access the switch.

When adding a new entry the fields are configurable, but for saved entries the values are read-only. If wanting to change a value for a saved entry, a new entry with the desired settings needs to be added and the undesired entry needs to be deleted.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Enabled: Enable or disable Remote Management Access for this switch.

Default: Disabled

VLAN: The VLAN ID for the entry.

Default: 1

Start: The Start IP Unicast Address for the allowed IP Address Range for the entry. The following restrictions apply:

- 'x.y.z.w' cannot be equal to the network address or the broadcast address for the assigned subnet.
- x must be a decimal number between 1 and 223.
- x must not be 127.
- y, z, and w must be decimal numbers between 0 and 255.

End: The End IP Unicast Address for the allowed IP Address Range for the entry. The following restrictions apply:

- 'x.y.z.w' cannot be equal to the network address or the broadcast address for the assigned subnet.
- x must be a decimal number between 1 and 223.
- x must not be 127.
- y, z, and w must be decimal numbers between 0 and 255.

HTTP/HTTPS: Enable or disable if HTTP/HTTPS can be used as a remote management access method for the entry.

Default: Disabled


SNMP: Enable or disable if SNMP can be used as a remote management access method for the entry.


Default: Disabled


Telnet/SSH: Enable or disable if Telnet/SSH can be used as a remote management access method for the entry.


Default: Disabled

Buttons

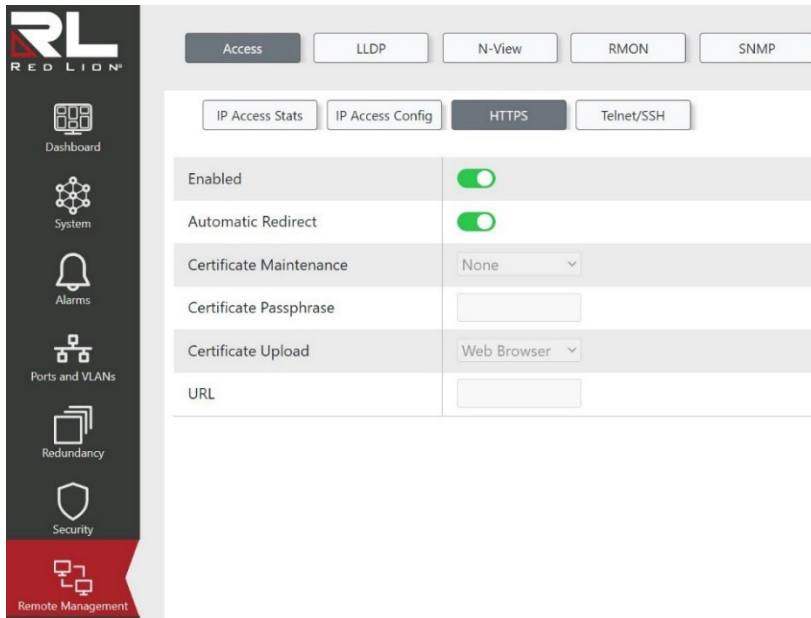
 Click to refresh values on the page.

 Applies the changes to the device.

 Click to add a new access management entry.

 Click to delete the selected entry.

HTTPS



This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.

Enabled: Enable or disable HTTPS mode operation on the switch.

Default: Enabled

Automatic Redirect: Enable or disable HTTPS Automatic Redirect mode operation. This is only significant when HTTPS is enabled via the toggle. When enabled, the HTTP connection will be redirected to an HTTPS connection automatically. Notice that the browser may not allow the redirect operation due to security settings unless the switch certificate is trusted by the browser, which would require the need to manually initialize the HTTPS connection.

Default: Enabled

Certificate Maintenance:

Use the drop down to select an operation to perform relating to the switch HTTPS certificate.

Possible operations are:

None: No operation.

Delete: Delete the current certificate.

Upload: Enables the Certificate Passphrase and Certificate Upload fields to upload a certificate PEM file.

Generate: Generate a new self-signed RSA certificate.

Note: When uploading a certificate PEM file to the switch, the file should contain the certificate and private key together. If you have two separate files for saving the certificate and private key, use the Linux cat command to combine them into a single PEM file. For example: `cat my.cert my.key > my.pem`

Notice that the RSA certificate is recommended since most of the new browser versions have removed support for DSA for certificates.

Default: None

Certificate Passphrase: This field is only enabled when Upload has been selected in the Certificate Maintain drop down field. Enter the required passphrase in this field if the certificate to be uploaded is protected by a specific passphrase.

Certificate Upload:

This field is only enabled when Upload has been selected in the Certificate Maintain drop down field. Select the method for uploading the desired certificate PEM file to the switch. Possible methods are:

Web Browser: Upload a certificate via Web Browser

URL: Upload a certificate via URL. The supported protocols are:

HTTP

HTTPS

TFTP

FTP

Default: Web Browser

URL:

This field is only enabled when Upload has been selected in the Certificate Maintain drop down field and URL has been selected in the Certificate Upload drop down field. Enter the URL for the desired certificate PEM file.

Note: The URL format is `<protocol>://[<username>[:<password>]@<`

`host>[:<port>][/<path>]/<file_name>`. For example,

`tftp://10.10.10.10/new_image_path/new_image.dat,`

`http://username:password@10.10.10.10:80/new_image_path/new_image.dat.`

A valid file name is a text string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), and/or under score (_). The maximum length is 63 and a hyphen must not be the first character. A file name of '.' is not allowed.

Buttons

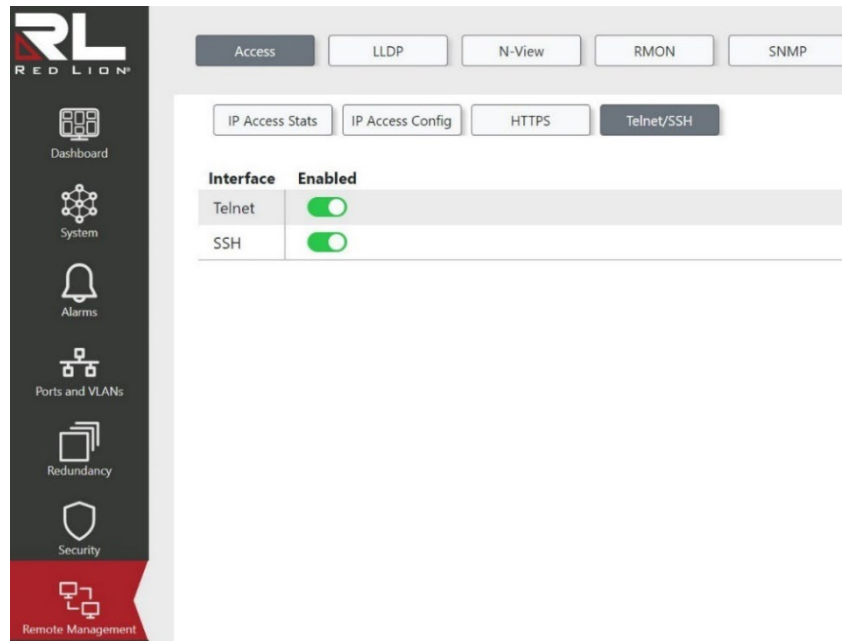


Click to refresh values on the page.



Applies the changes to the device.

Telnet/SSH




This page allows you to Enable/Disable Telnet and SSH on the switch.


Interface: The management interface for which the configuration applies.

Enabled: Enable or disable the management interface for the switch.

Default: Telnet is Disabled. SSH is Enabled

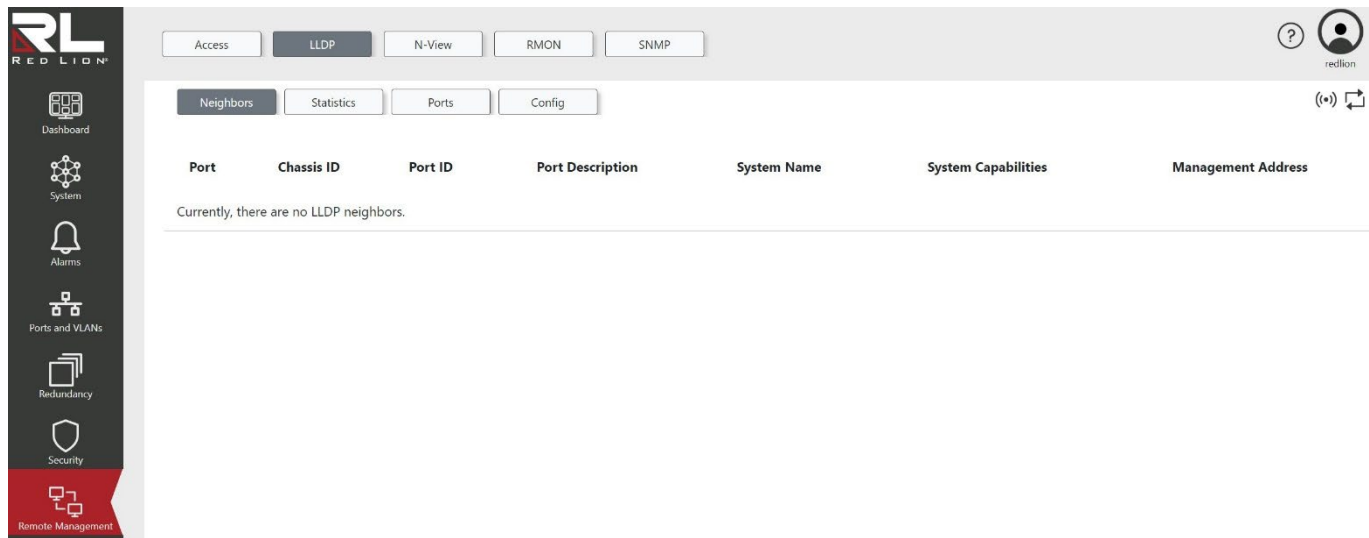
Buttons

 Click to refresh values on the page.

 Applies the changes to the device.

LLDP

Neighbors



This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. The columns hold the following information:

Port: The interface name on which the LLDP frame was received.

Chassis ID: Indicates the identification of the neighbor's LLDP frames.

Port ID: Indicates the identification of the neighbor's port.

Port Description: Indicates the description as advertised by the neighbor.


System Name: Indicates the name advertised by the neighbor.


System Capabilities: Indicates the neighbor's capabilities. The possible entries are:

- Other
- Repeater
- Bridge
- WLAN Access Point
- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

Management Address: Indicates the neighbor's address that is used for higher layer entities to assist discovery by network management. This could for instance hold the neighbor's IP address.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh values on the page.

Statistics

The screenshot displays the LLDP statistics page in the Red Lion network management interface. The page is divided into two main sections: Global Counters and Local Counters.

Global Counters:

Time Since Last Change	5d 00:19:31 (433171) seconds
Neighbors Added	0
Neighbors Deleted	0
Neighbors Dropped	0
Neighbors Aged Out	0

Local Counters:

Port	Tx Frames	Rx					TLV		Aged
		Frames	Errors	Discards	TLV Errors	Unknown	TLV Organiz.		
P1	14437	0	0	0	0	0	0	0	
P2	0	0	0	0	0	0	0	0	
P3	0	0	0	0	0	0	0	0	
P4	14437	0	0	0	0	0	0	0	
P5	0	0	0	0	0	0	0	0	
P6	0	0	0	0	0	0	0	0	

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the switch.

Time Since Last Change: Indicates the elapsed time since the LLDP neighbor table was updated.

Neighbors Added: Indicates the number of new LLDP neighbors added since switch reboot or last clear operation.

Neighbors Deleted: Indicates the number of new LLDP neighbors deleted since switch reboot or last clear operation.

Neighbors Dropped: Indicates the number of LLDP neighbors dropped due to the entry table being full.

Neighbors Aged Out: Indicates the number of LLDP neighbors deleted due to Time-To-Live expiring.

Port: The interface on which LLDP frames are received or transmitted.

Tx Frames: Indicates the number of LLDP frames transmitted on the interface.

Rx Frames: Indicates the number of LLDP frames received on the interface.

Errors: Indicates the number of LLDP frames received containing some form of error.

Discards: Indicates the number of frames discarded on the interface. If an LLDP frame is received on an interface, and the switch's internal table is full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries

are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.




TLV Errors: Indicates the number of malformed TLVs discarded. Each LLDP frame can contain multiple pieces of information, known as TLVs "Type Length Value".

TLV Unknown: Indicates the number of well-formed TLVs, but with an unknown type value.

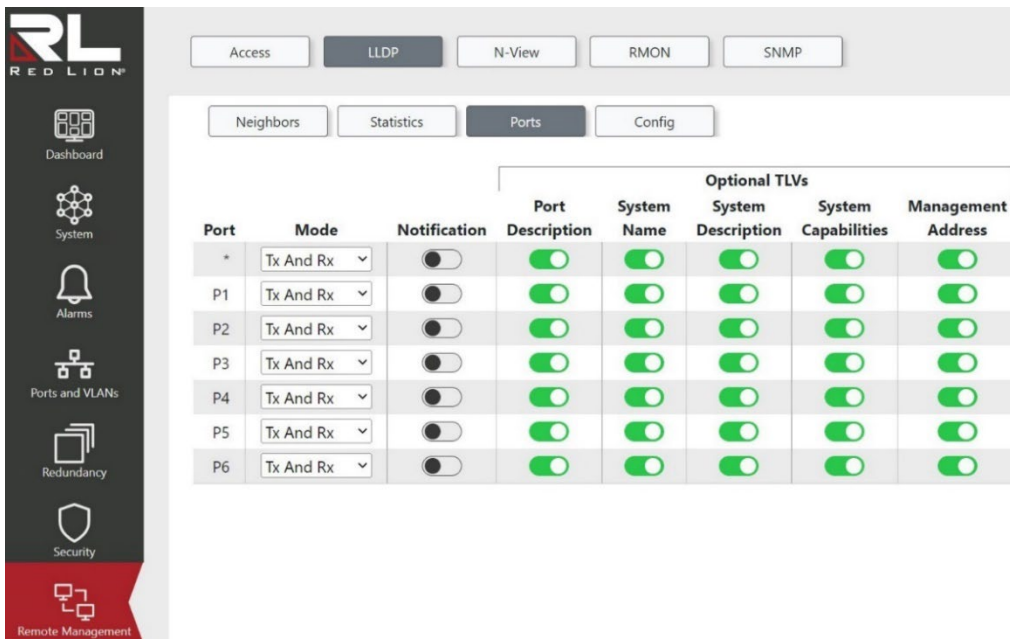
TLV Organiz.: Indicates the number of LLDP frames received with an organizationally specific TLV, but the TLV was not supported and was discarded.

Aged: Indicates the number of Aged out frames. Each LLDP frame contains information about how long the LLDP information is valid. If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

-  Resets all entries.
-  Automatic refresh occurs every 3 seconds.
-  Click to refresh values on the page.

Ports



Port	Mode	Notification	Optional TLVs				
			Port Description	System Name	System Description	System Capabilities	Management Address
*	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P1	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P2	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P3	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P4	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P5	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P6	Tx And Rx	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This page allows the user to inspect and configure the current LLDP interface settings.

Interface: The switch interface name of the logical LLDP interface.

Mode:

Select LLDP mode.

Tx And Rx: The switch will send out LLDP information and will analyze LLDP information received from neighbors.

- Rx Only:** The switch will not send out LLDP information, but LLDP information from neighbors will be analyzed.
- Tx Only:** The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- Disabled:** The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
- Default:** Tx And Rx

Port Description: Enable or disable the port description optional TLV inclusion into the LLDP information transmitted.


System Name: Enable or disable the system name optional TLV inclusion into the LLDP information transmitted.


System Description: Enable or disable the system description optional TLV inclusion into the LLDP information transmitted.

System Capabilities: Enable or disable the system capabilities optional TLV inclusion into the LLDP information transmitted.

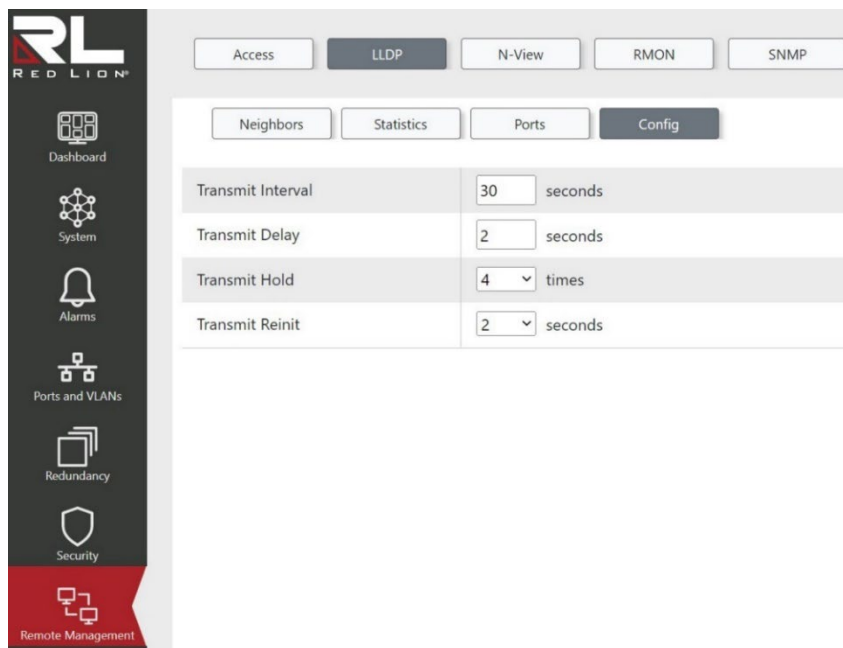
Management Address: Enable or disable the management address optional TLV inclusion into the LLDP information transmitted.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Config



This page allows the user to configure the current LLDP transmit values.

Transmit Interval: The switch periodically transmits LLDP frames to its neighbors to keep the network discovery information up-to-date. The interval between each LLDP frame is determined by the Transmit Interval value. Valid values range from 5 to 32768 seconds.

Default: 30

Transmit Delay: The minimum time allowed between LLDP frame transmission. The time between the LLDP frames will always be at least the value of Transmit Delay. Transmit Delay cannot be larger than 1/4 of the Transmit Interval value. Valid values range from 1 to 8192 seconds.

Default: 2


Transmit Hold: Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Transmit Hold multiplied by Transmit Interval. Valid values range from 2 to 10 times.


Default: 4

Transmit Reinit: The minimum time an LLDP port will wait before re-initializing after its setting has changed from "Disabled" to "Tx Only" or "Tx And Rx". This prevents excessive notifications when LLDP Port settings are changed. Valid values range from 1 to 10 seconds.

Default: 2

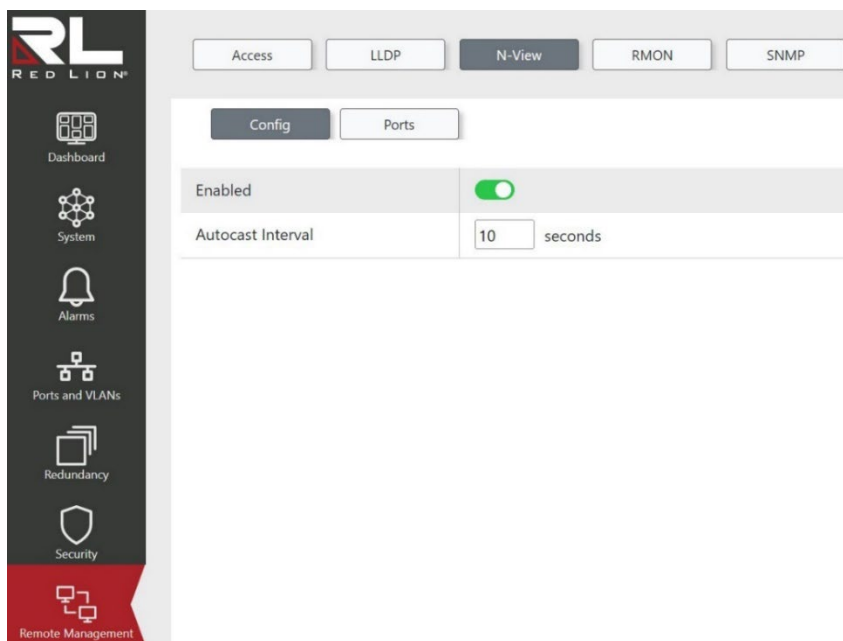
Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

N-View™

Config



Configure N-View settings.


Enabled: Enable or disable the N-View™ feature.


Default: Enabled

Autocast Interval: Indicates the interval in seconds for autocasting MIB counters to the configured Autocast ports. The available range is 5 to 500 seconds. An entry of 0 will disable the N-View feature.

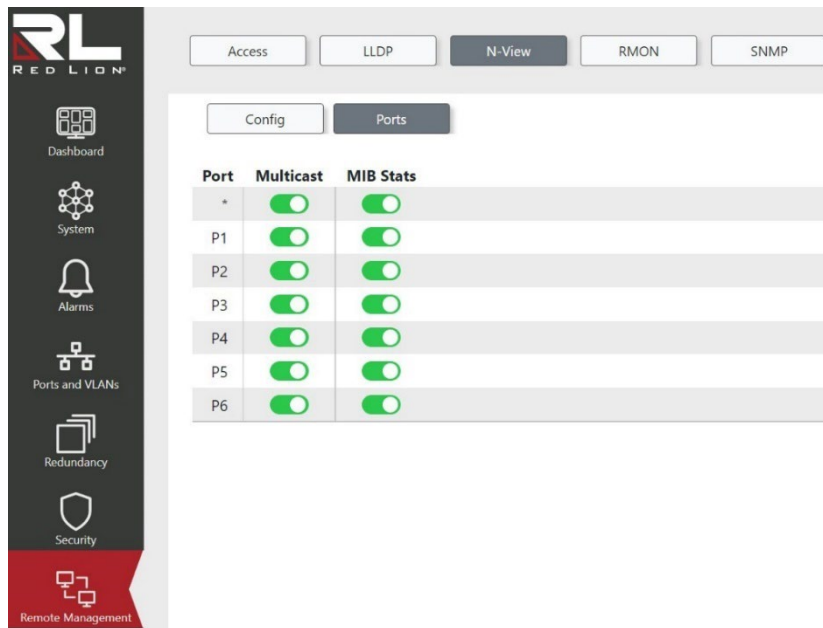
Default: 10

Buttons

 Click to refresh the values on the page.

 This button saves the current settings on the screen to the switch.

Ports



Configure N-View ports

Port: This is the logical port number for this row.


Multicast: Indicates whether or not to send autocast frames on this port.


Default: Enabled

MIB Stats: Indicates whether or not to send this port's MIB counters inside autocast frames.

Default: Enabled

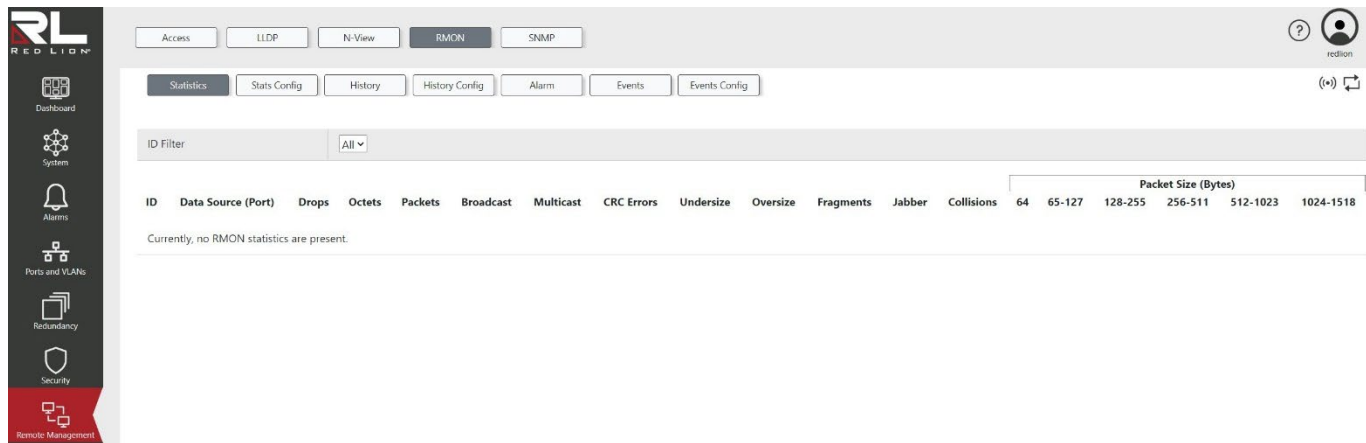
Buttons

 Click to refresh the values on the page.

 This button saves the current settings on the screen to the switch.

RMON

Statistics



This page provides an overview of RMON Statistics entries.

ID Filter: Select the RMON statistic's ID, filtering out all other statistics entries.

Default: All

ID: Indicates the index of the statistics entry.

Data Source (Port): Indicates the ID of the port that the statistics were generated from.

Drops: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received.

Packets: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.

Fragments: The number of frames which size is less than 64 octets received with invalid CRC.

Jabber: The number of frames which size is larger than 64 octets received with invalid CRC.

Collisions: The best estimate of the total number of collisions on this Ethernet segment.

64: The total number of packets (including bad packets) received that were 64 octets in length.

65-127: The total number of packets (including bad packets) received that were between 65 to 127 octets in length.


128-255: The total number of packets (including bad packets) received that were between 128 to 255 octets in length.


256-511: The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512-1023: The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

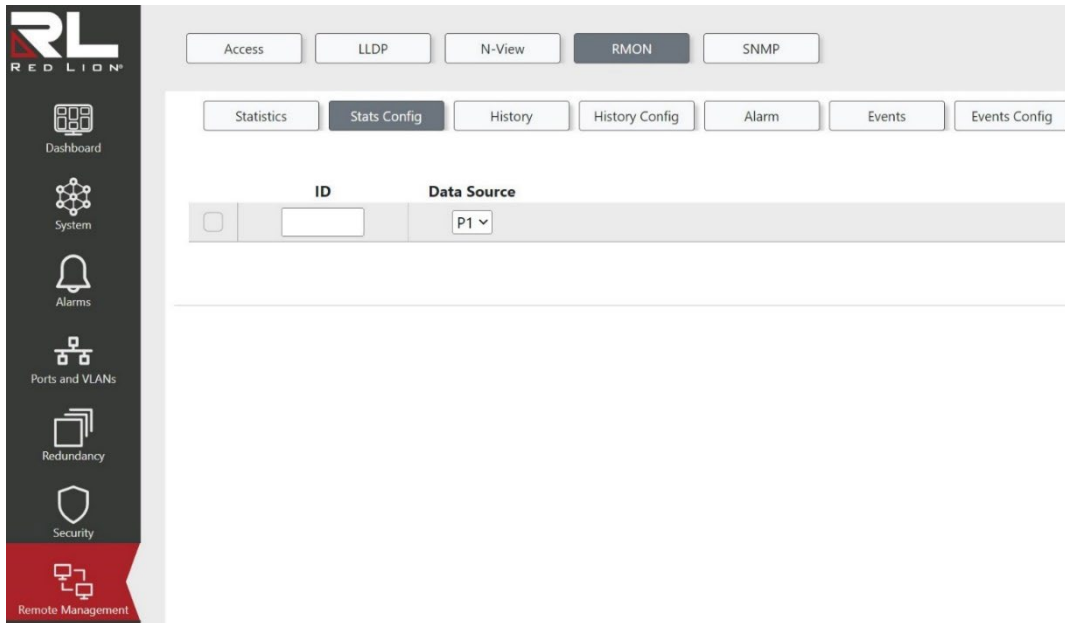
1024-1518: The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons

 Click to refresh the values on the page.

 Automatic refresh occurs every 3 seconds.

Stats Config



Configure the RMON Statistics table on this page. The entry index key is the ID.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

ID: Indicates the index of the entry. The range is from 1 to 65535.

Data Source: Indicates the port ID to be monitored.

Default: P1

Buttons

 Click to add a new RMON statistics entry.



Click to save changes.



Click to undo any changes made locally and revert to previously saved values.



Delete selected RMON statistics entry.

History

This page provides an overview of RMON History control entries.

ID Filter: Select the RMON History control entry's ID, filtering out all other entries.

Default: All.

ID: Indicates the index of History control entry.

Index: Indicates the index of the data entry associated with the control entry.

Start System Uptime: The length of time from the previous boot of the switch until the start of the interval over which this sample was measured.

Drops: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Packets: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.


Fragments: The number of frames which size is less than 64 octets received with invalid CRC.


Jabber: The number of frames which size is larger than 64 octets received with invalid CRC.

Collisions: The best estimate of the total number of collisions on this Ethernet segment.

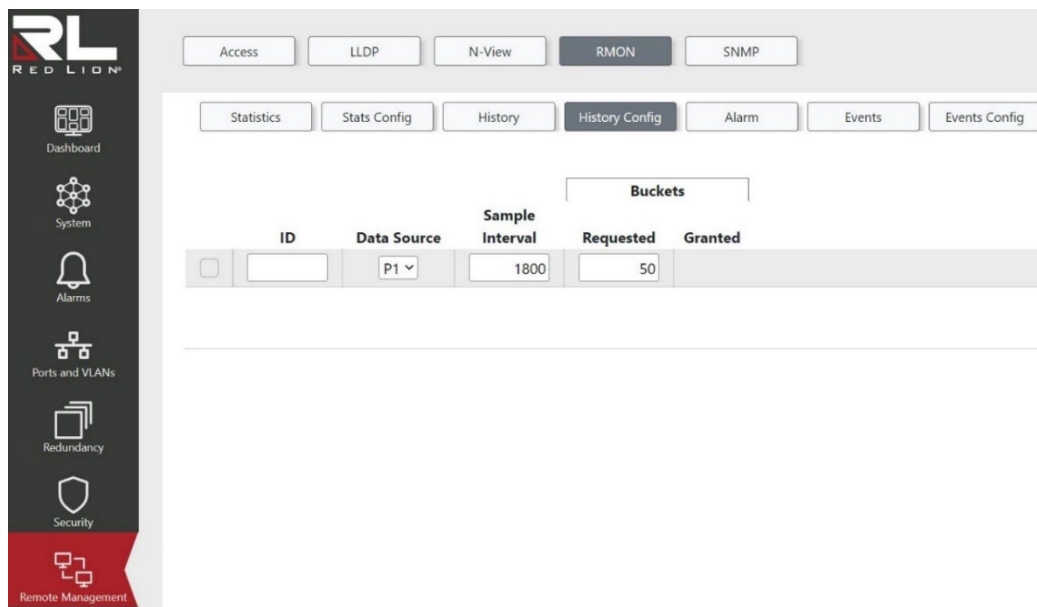
Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

 Click to refresh the values on the page.

 Automatic refresh occurs every 3 seconds.

History Config



Configure the RMON History table on this page. The entry index key is the ID.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

ID: Indicates the index of the entry. The range is from 1 to 65535.

Data Source: Indicates the port ID to be monitored.

Default: P1

Sample Interval: Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600.





Default: 1800

Buckets: Indicates the maximum data entries associated with this History control entry stored in RMON. The range is from 1 to 50.

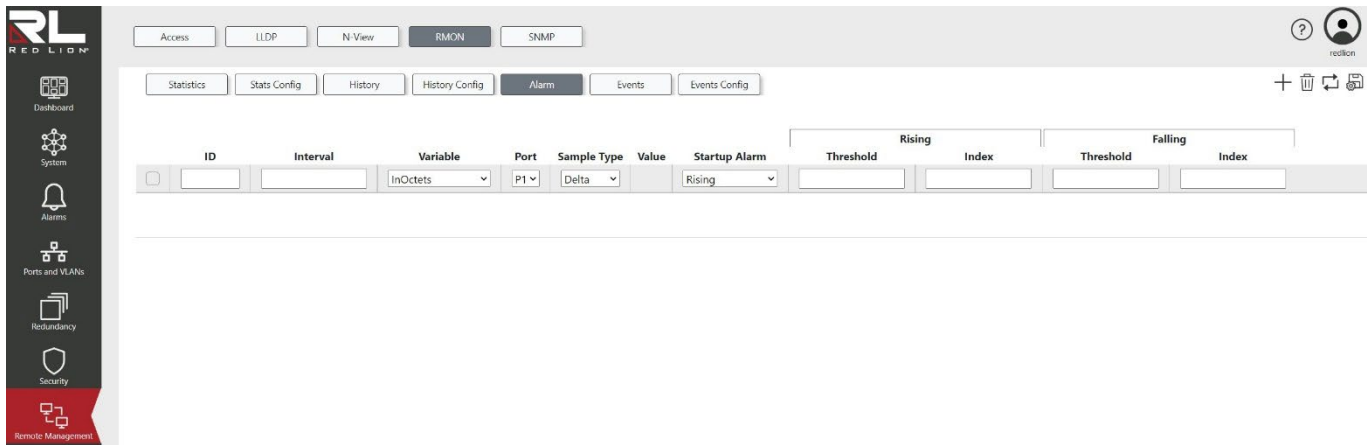
Default: 50

Granted: The amount of data associated with this entry that shall be stored in RMON.

Buttons

-  Click to add a new RMON statistics entry.
-  Click to save changes.
-  Click to undo any changes made locally and revert to previously saved values.
-  Delete.

Alarm



ID	Interval	Variable	Port	Sample Type	Value	Startup Alarm	Threshold	Rising Index	Threshold	Falling Index
<input checked="" type="checkbox"/>		InOctets	P1	Delta		Rising				

Configure the RMON Alarm table on this page. The entry index key is the ID.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

ID: Indicates the index of the entry. The range is from 1 to 65535.

Interval: Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$.

Variable:

Indicates the variable to be sampled. Possible variables are:

InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts: The number of unicast packets delivered to a higher layer protocol.

InNUcastPkts: The number of broadcast and multicast packets delivered to a higher layer protocol.

InDiscards: The number of inbound packets that are discarded, including packets that are normal.

InErrors: The number of inbound packets that contained errors preventing them from being delivered to a higher layer protocol.

InUnknownProtos: The number of the inbound packets that were discarded because of an unknown or unsupported protocol.

OutOctets: The number of octets transmitted out of the interface, including framing characters.

OutUcastPkts: The number of unicast packets that request to transmit.

OutNUcastPkts: The number of broadcast and multicast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded, including packets that are normal.

OutErrors: The number of outbound packets that could not be transmitted because of errors.

OutQLen: The length of the output packet queue (in number of packets).

Default: InOctets

Port: Indicates the port ID to be monitored.

Default: P1

Sample Type:

The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible sample types are:

Absolute: Get the sample directly.

Delta: Calculate the difference between samples.

Default: Delta

Value: The value of the statistic during the last sampling period.

Startup Alarm:

The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible sample types are:

Rising: Trigger alarm when the first value is larger than the rising threshold.

Falling: Trigger alarm when the first value is less than the falling threshold.

Rising Or Falling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

Default: Rising Or Falling


Rising Threshold: Indicates the rising threshold value. The range is from -2147483648 to 2147483647.


Rising Index: Indicates the rising event index with a range from 0 to 65535. If this value is zero, no associated event will be generated, as zero is not a valid event index.


Falling Threshold: Indicates the falling threshold value. The range is from -2147483648 to 2147483647.


Falling Index: Indicates the falling event index with a range from 0 to 65535. If this value is zero, no associated event will be generated, as zero is not a valid event index.

Buttons

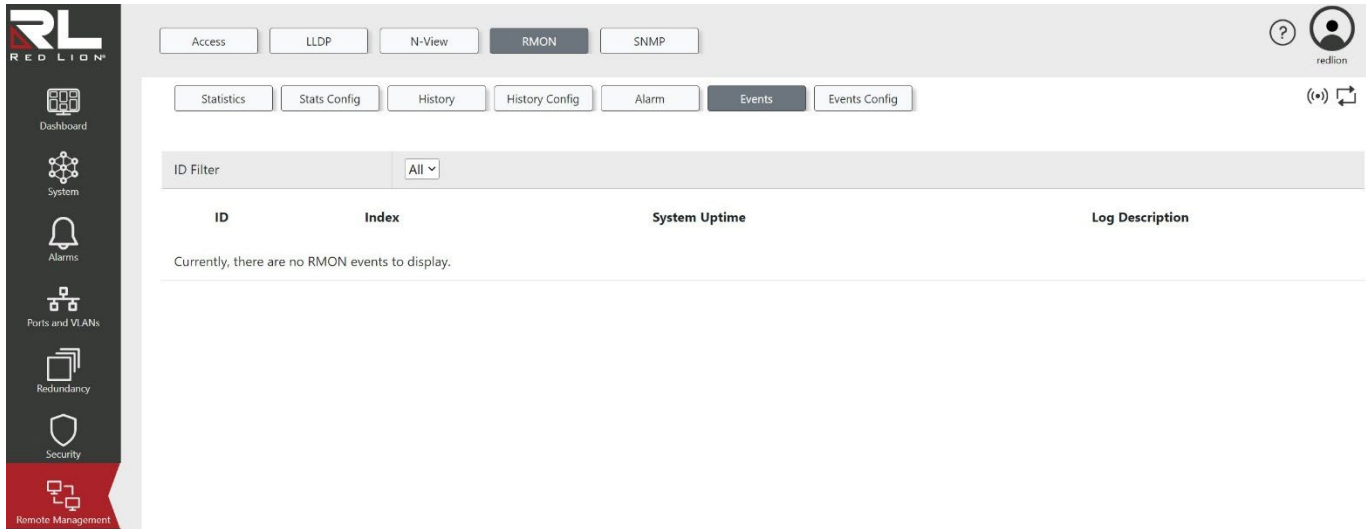
 Add a new event.

 Delete highlighted events.

 Click to refresh the values on the page.

 Applies the changes to the device.

Events



This page provides an overview of RMON Event table entries.

ID Filter: Select the RMON Event entry's ID, filtering out all other entries.

Default: All


Event Index: Indicates the index of the event entry.


Index: Indicates the index of the log entry.

System Uptime: Indicates the length of time from the previous boot of the switch until the event was triggered.

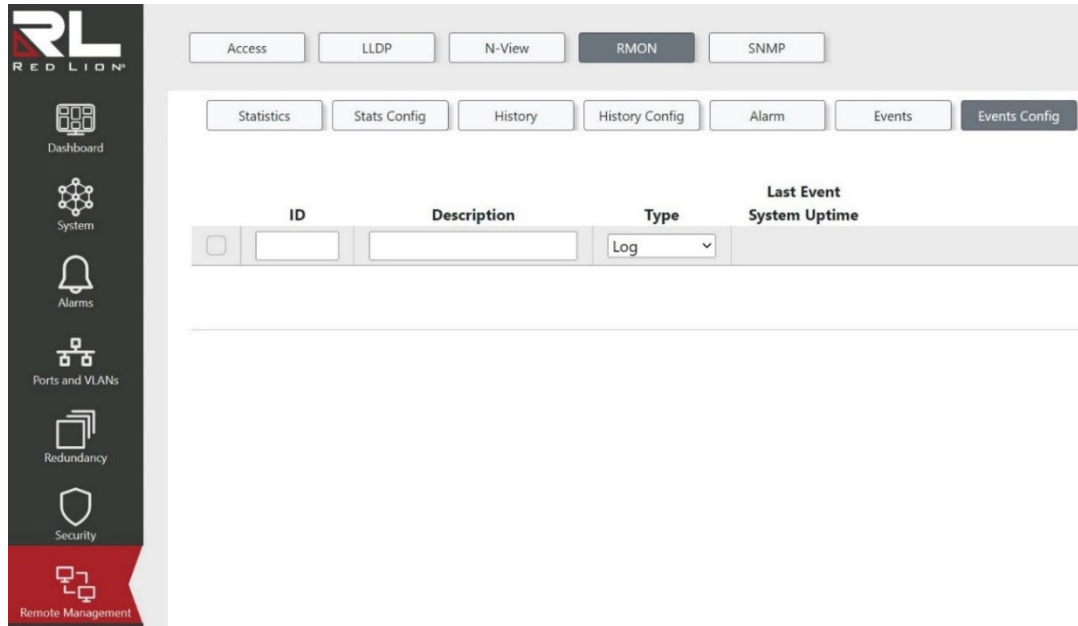
Log Description: Indicates the Event description.

Buttons

 Click to refresh the values on the page.

 Automatic refresh occurs every 3 seconds.

Events Config



Configure the RMON Events table on this page. The entry index key is the ID.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

ID: Indicates the index of the entry. The range is from 1 to 65535.

Description: Describes this event. The allowed string length is from 0 to 127.

Type:

Indicates the type of notification of the event. Possible notification types are:

Log: Create an SNMP log entry when the event is triggered.

SNMP Trap: Send an SNMP trap when the event is triggered.

None: No SNMP log is created, and no SNMP trap is sent.

Log And Trap: Create an SNMP log entry and send an SNMP trap when the event is triggered.

Default: Log

Last Event System Uptime: The length of time from the previous boot of the switch until the last event was triggered.

Buttons

+ Add a new event.

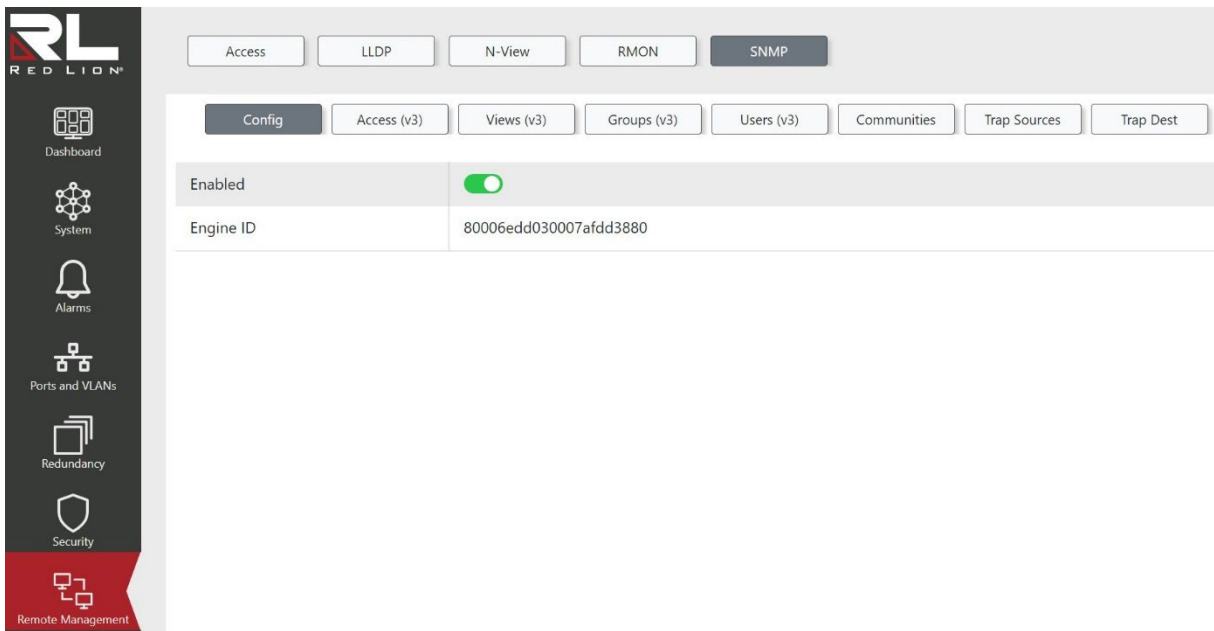
🗑 Delete highlighted events.

↻ Click to refresh the values on the page.

💾 Applies the changes to the device.

SNMP

Config




Configure SNMP on this page.


Enabled: Enable or disable SNMP operation.

Default: Enabled

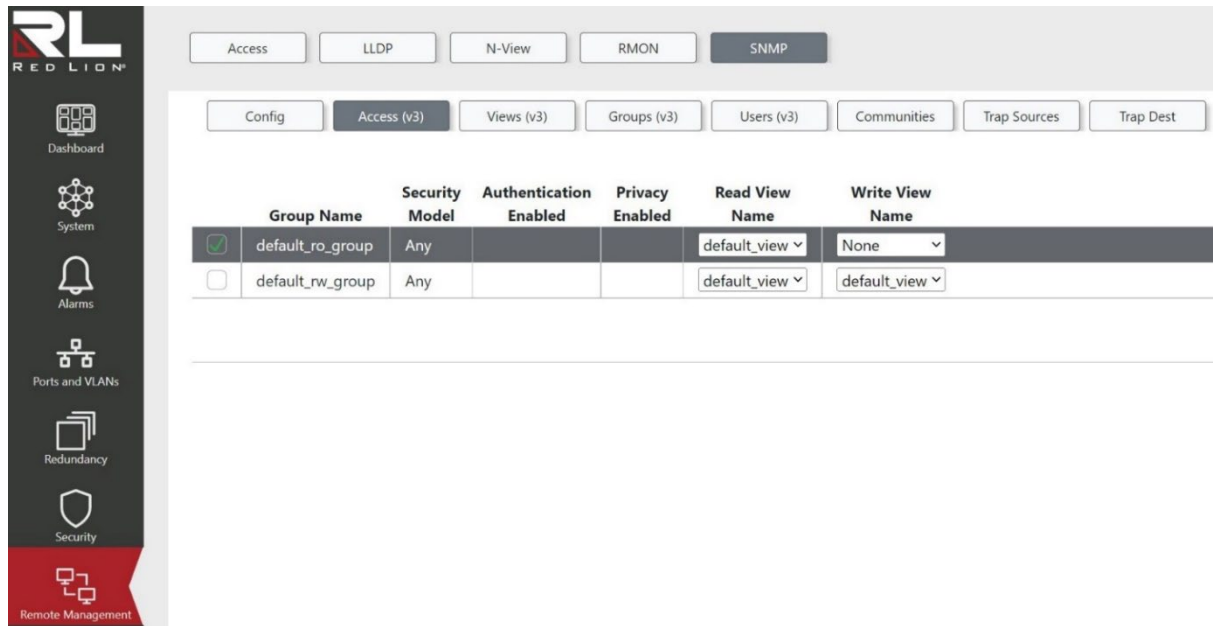
Engine ID: SNMPv3 System Engine ID.

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Access (v3)



Configure access to Read/Write Views of existing SNMPv3 groups with the provided configurations on this page. Users, Groups, and Views may be created via the Users (v3), Groups (v3), and Views (v3) pages, respectively.

Row selection column: Click on the checkbox to select the row. Click again to de-select.
Default: The first row is selected when a page is loaded.

Group Name: Select the existing group name from the drop down provided.

Note: Users may be created via the Users (v3) page, and users can be added to groups via the Groups (v3) page.

Security Model:

Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted (v1|v2c|USM).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

USM: SNMPv3, User-based Security Model (USM).

Default: Any

Authentication Enabled: Enable or disable authentication.

Default: Enabled

Privacy Enabled: Enable or disable privacy/encryption.

Default: Enabled

Read View Name:

Select the existing Read View Name from the drop down provided.

Note: Views may be created via the Views (v3) page.

Default: None


Write View Name:


Select the existing Write View Name from the drop down provided.


Note: Views may be created via the Views (v3) page.


Default: None

Buttons

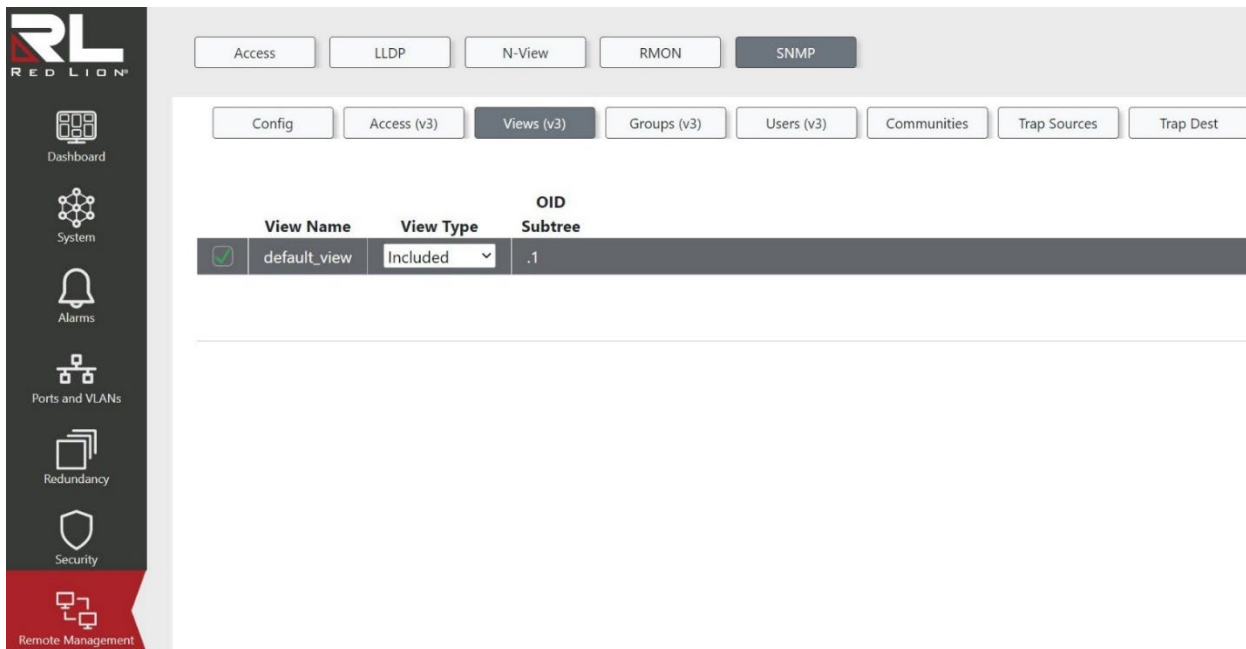
 Click to add a new access entry.

 Click to delete the entry.

 Click to refresh the values on the page.

 Applies the changes to the device.

Views (v3)



View Name	View Type	OID Subtree
<input checked="" type="checkbox"/> default_view	Included	.1

Configure the SNMPv3 views on this page. The entry index keys are the View Name and OID Subtree.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type:

Indicates the view type that this entry should belong to. Possible view types are:





included: A flag to indicate that this view subtree should be included.

excluded: A flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with a view type of 'included', and its OID subtree should overstep the 'excluded' view entry.

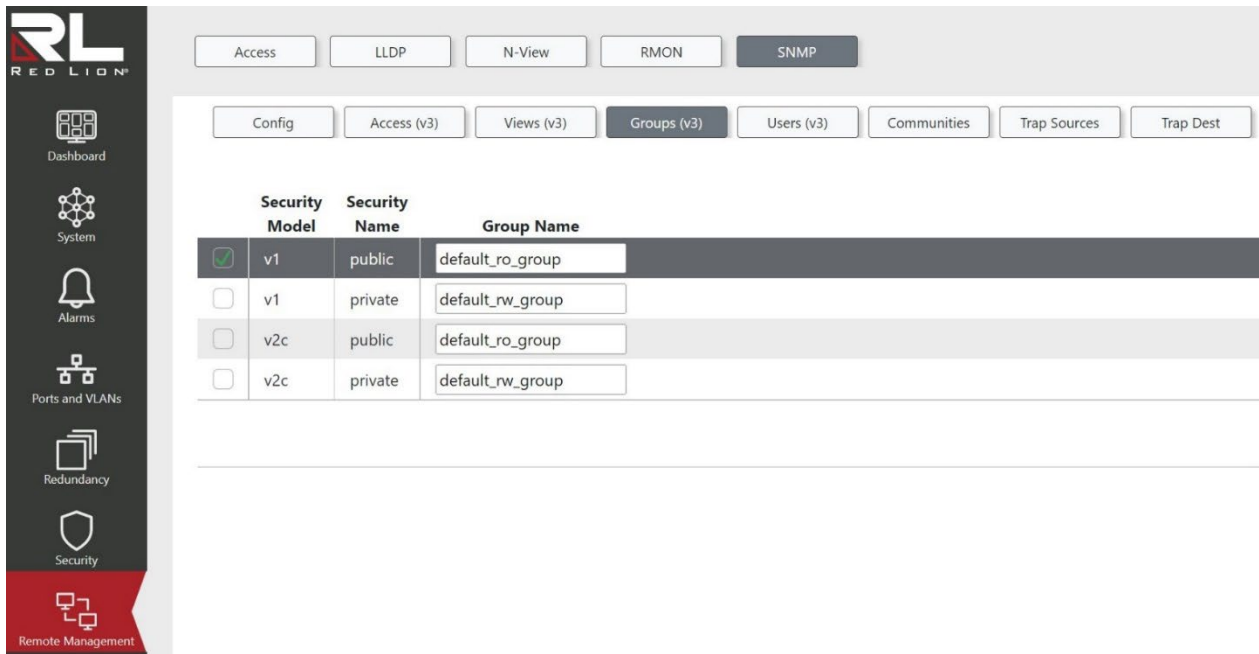
Default: included

OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is a digital number or asterisk (*).

Buttons

-  Click to add a new SNMP view.
-  Click to delete the selected views from the switch.
-  Click to refresh the values on the page.
-  Applies the changes to the device.

Groups (v3)



	Security Model	Security Name	Group Name
<input checked="" type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group

Configure SNMPv3 group table on this page. The entry index keys are **Security Model** and **Security Name**.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.





Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- v1:** Reserved for SNMPv1.
- v2c:** Reserved for SNMPv2c.
- USM:** SNMPv3, User-based Security Model (USM).

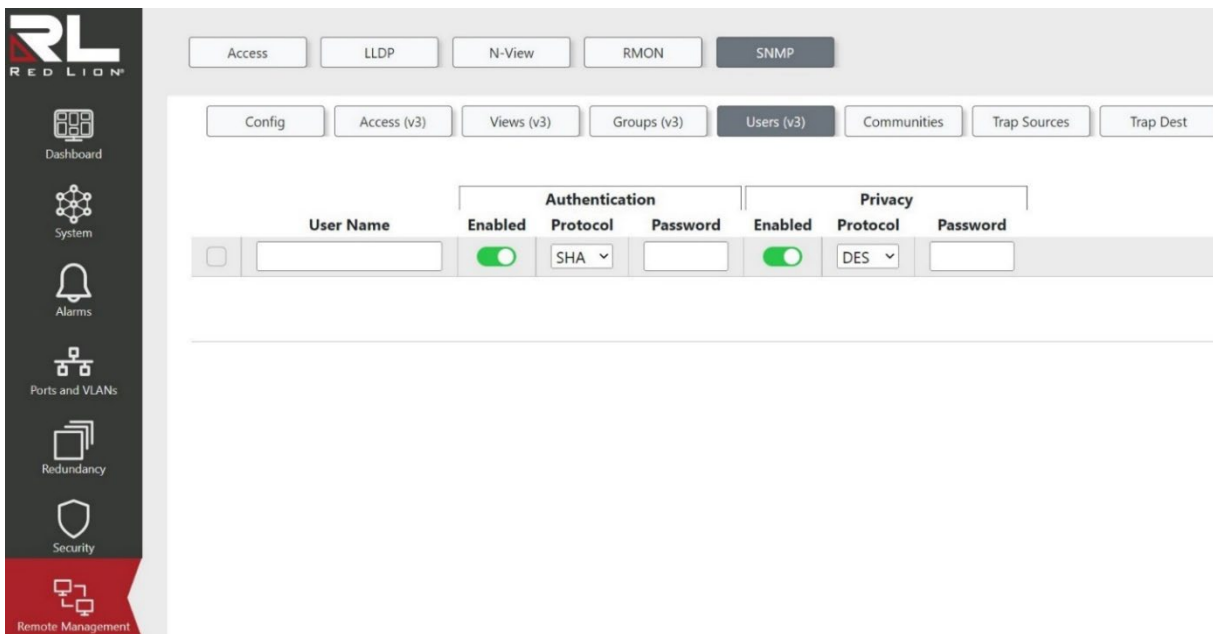
Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

-  Click to add a new group entry.
-  Click to delete the selected group(s).
-  Click to refresh the values on the page.
-  Applies the changes to the device.

Users (v3)



Configure SNMPv3 users on this page. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control.

Once an entry has been saved, only the Authentication Password and Privacy Password can be changed. One must create a new entry to modify all other fields.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Authentication Enabled: Enable or disable authentication for the user.

Default: Enabled

Authentication Protocol:

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

SHA: An optional flag to indicate that this user uses the SHA authentication protocol.

MD5: An optional flag to indicate that this user uses the MD5 authentication protocol.

None: No authentication protocol.

Default: SHA

Authentication Password: A string identifying the authentication password phrase. For the MD5 authentication protocol, the allowed string length is 8 to 32. For the SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Enabled: Enable or disable privacy/encryption for the user.

Default: Enabled

Privacy Protocol:

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

AES: An optional flag to indicate that this user uses the AES authentication protocol.


DES: An optional flag to indicate that this user uses the DES authentication protocol.


None: No privacy protocol.


Default: DES


Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

 Click to add a new user entry.

 Click to delete the selected SNMPv3 users from the switch.

 Click to refresh the values on the page.

 Applies the changes to the device.

Communities

	Community Name	Community Secret	Source IP	Source Prefix
<input checked="" type="checkbox"/>	public	public	0.0.0.0	0
<input type="checkbox"/>	private	private	0.0.0.0	0

Configure SNMPv3 community table on this page. The entry index key is Community.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.





Community Name: Indicates the community name to map onto the security name of the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Community Secret: Indicates the community secret (access string) to permit access to the SNMP agent using SNMPv1 and SNMPv2c. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

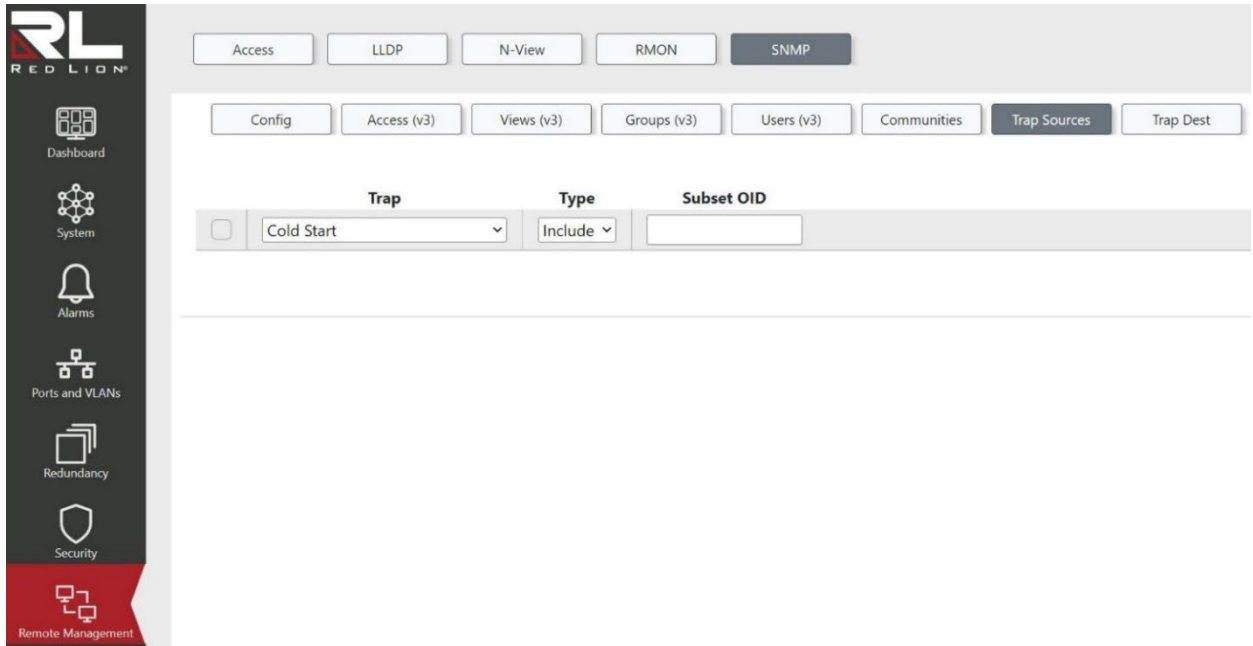
Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict the source subnet when combined with the source IP and prefix.

Source Prefix: Indicates the SNMP access source address prefix.

Buttons

-  Click to add a new community entry.
-  Click to delete the selected entries from the switch.
-  Click to refresh the values on the page.
-  Applies the changes to the device.

Trap Sources



This page provides SNMP trap source configurations. A trap is sent for a given trap source if at least one filter with the included type matches, and no filters with the excluded type matches.

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Trap:

Indicates the name for the entry. Available options are:

- Cold Start
- Warm Start
- Link Up
- Link Down
- Authentication Failure
- Entity Configuration Change
- New Root
- Topology Change
- LLDP Remote Tables Change
- Rising Alarm
- Falling Alarm
- Alarm Trap Status
- IP Trap Interfaces Link
- Port Security Trap Globals Main
- Port Security Trap Interface

Default: Cold Start

Type:

The filter type for the entry. Possible types are:





Include: A flag to indicate a trap is sent for the given trap source if it is matched.

Exclude: A flag to indicate a trap is not sent for the given trap source if it is matched.

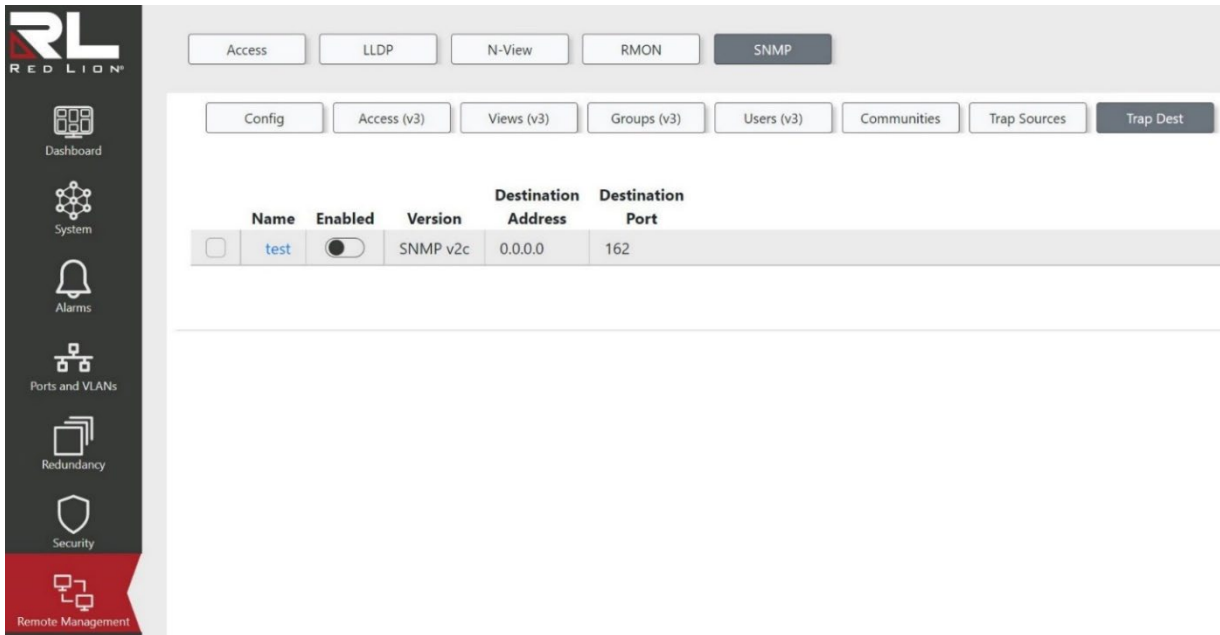
Default: Include

Subset OID: The subset OID for the entry. The value should depend on the trap name. For example, the port index is the subset OID of Link Up and Link Down. A valid subset OID is one or more digital numbers (0-4294967295) or asterisks (*) which are separated by dots (.). The first character must not begin with an asterisk (*), and the maximum OID count must not exceed 128.

Buttons

-  Click to add a new entry. The maximum entry count is 32.
-  This button deletes the currently selected entries from the switch.
-  Click to refresh the values on the page.
-  Applies the changes to the device.

Trap Dest



The screenshot shows the Red Lion web interface. The left sidebar contains navigation icons for Dashboard, System, Alarms, Ports and VLANs, Redundancy, Security, and Remote Management. The main content area has a top navigation bar with tabs for Access, LLDP, N-View, RMON, and SNMP. Below this is a sub-navigation bar with tabs for Config, Access (v3), Views (v3), Groups (v3), Users (v3), Communities, Trap Sources, and Trap Dest. The 'Trap Dest' tab is selected, showing a table with the following data:

	Name	Enabled	Version	Destination Address	Destination Port
<input type="checkbox"/>	test	<input checked="" type="checkbox"/>	SNMP v2c	0.0.0.0	162

Trap Destination Settings	
Configuration Name	test
Mode Enabled	<input type="checkbox"/>
Version	SNMP v2c
Community	public
Destination Address	
Destination Port	162
Inform Mode Enabled	<input type="checkbox"/>
Inform Timeout	3 seconds
Inform Retry Times	5
Security Name	None

Configure SNMP Trap Destinations

Row selection column: Click on the checkbox to select the row. Click again to de-select.

Default: The first row is selected when a page is loaded.

Configuration Name: Indicates the trap destination's name. Click this link to open a modal with the full configuration options for the trap destination.

Mode Enabled: Enable or disable the trap destination mode.

Default: Disabled

Version:

Indicates the SNMP trap supported version. Possible versions are:

- SNMP v1
- SNMP v2c
- SNMP v3

Default: SNMPv2c

Community: Indicates the community address string when sending SNMP trap packets.

Default: public

Destination Address: Indicates the SNMP trap destination address. It allows for a valid IP address in dotted decimal notation.

Destination Port: Indicates the SNMP trap destination port. The SNMP trap agent will send SNMP messages via this port. The port range is 1 to 65535.

Default: 162

Inform Mode Enabled: Enable or disable the SNMP trap inform mode.

Default: Disabled

Inform Timeout: Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Default: 3





Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Default: 5

Security Name: Indicates the SNMP trap security name. SNMP v3 sends traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Default: None

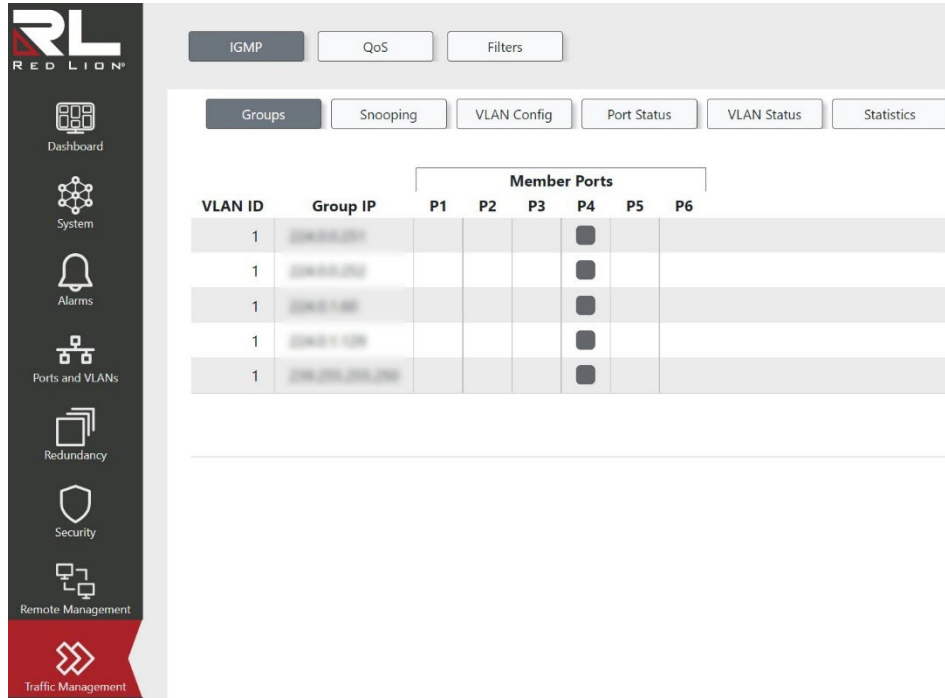
Buttons

-  Click to add a new trap destination entry.
-  Click to delete the selected trap destination(s).
-  Click to refresh the values on the page.
-  This button saves the current settings on the screen to the switch.

Chapter 11 Traffic Management

IGMP

Groups




This page displays all the IGMP group entries, sorted first by VLAN ID and then by group.


VLAN ID: The VLAN ID of the group.

Group IP: The IP address of the group.

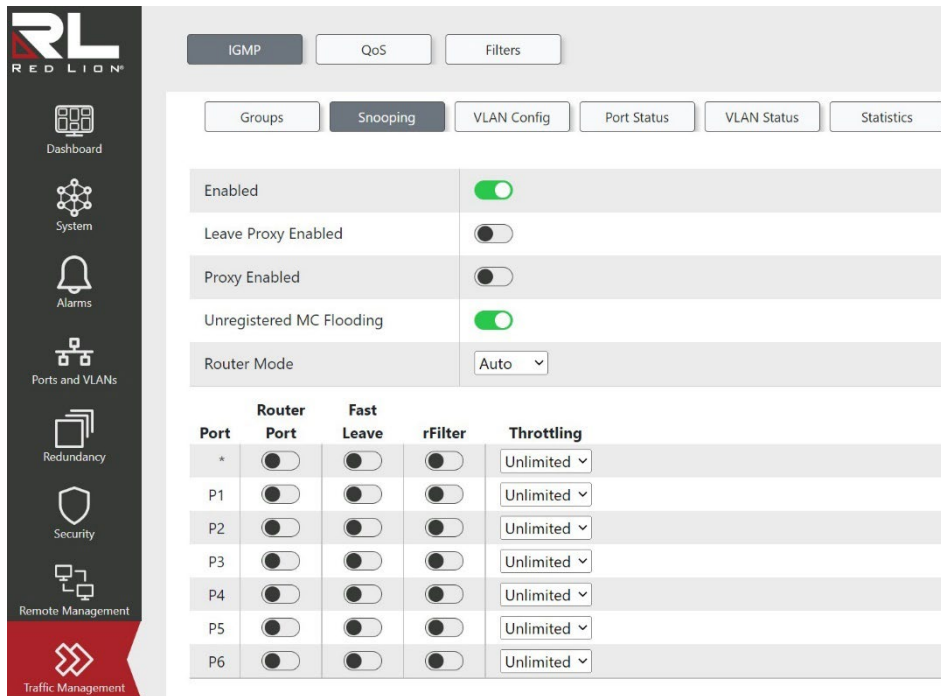
Member Ports: Ports under this group.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

Snooping



This page provides IGMP Snooping related configuration.

Enabled: Enable or disable global IGMP Snooping.

Default: Enabled

Leave Proxy Enabled: Enable or disable feature that, when enabled, avoids forwarding unnecessary leave messages to the router side.

Default: Disabled

Proxy Enabled: Enable or disable feature that, when enabled, avoids forwarding unnecessary join and leave messages to the router side.

Default: Disabled

Unregistered MC Flooding: Enable or disable unregistered MC flooding. When enabled, if IGMP Snooping is enabled then unregistered multicast traffic will flood (egress all ports except the receiving port). When IGMP Snooping is disabled, unregistered multicast traffic flooding is always active and this setting is ignored.

Default: Enabled

Router Mode:

Configure the router mode option.

None: Allows no router ports. Any configured router ports will be ignored.

Manual: Allows one or more ports to be configured as router ports using the Router Mode toggles per port.

Auto: Allows for dynamically detected and manually configured router ports.

Default: Auto

Port: The port name.

Router Port: Enable or disable which ports act as router ports. A router port leads towards the Layer 3 multicast device or IGMP querier. This configuration option is ignored if Router Mode is set to None.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Default: Disabled

Fast Leave: Enable or disable Fast Leave on a port. When enabled, upon receiving an IGMPv2 leave message the group record will be removed and forwarding data will be stopped without sending last member query messages.

It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.

Default: Disabled

rFilter: Enable or disable IGMP group data from egressing on the port unless a join to that specific IGMP group has come into the port and it is configured as a router port. IGMP controls (Join, Leave, Query) are still sent.

Default: Disabled

Throttling:


Set to limit the number of multicast groups to which a switch port can belong.


Unlimited: No limit.

1 - 10

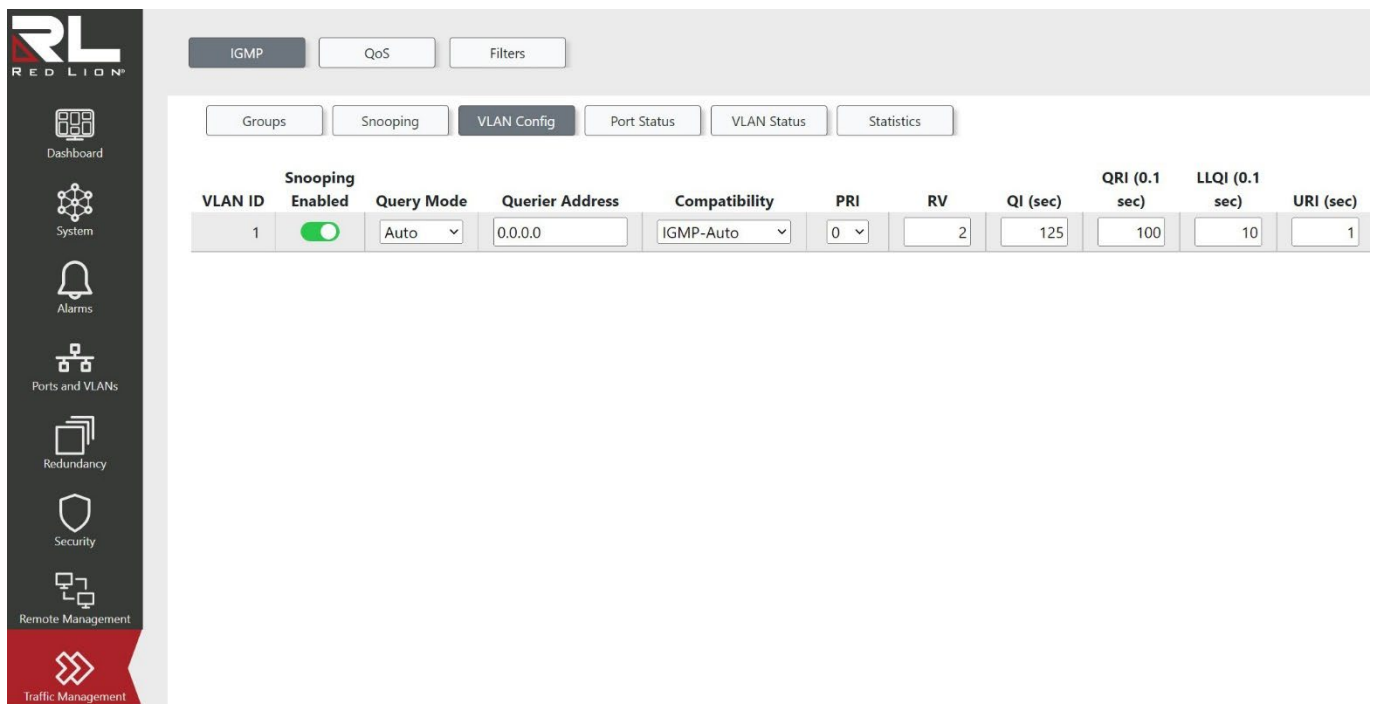
Default: Unlimited

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

VLAN Config



VLAN ID	Snooping Enabled	Query Mode	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input checked="" type="checkbox"/>	Auto	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

This page allows you to configure IGMP Snooping settings for existing IP Interfaces. New interfaces may be added via the System → IP Interfaces → Interfaces screen.

VLAN ID: The VLAN ID of the entry.

Snooping Enabled: Enable or disable per-VLAN IGMP Snooping.

Default: Enabled

Query Mode:

Specifies the query mode to be used in the VLAN.

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.

Default: Auto

Querier Address: Define the IPv4 address to be used as the source address in the IP header for IGMP Query Mode.

When the Querier address is not set, the system uses the IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise the system uses a pre-defined value.

Compatibility:

Compatibility is maintained within a network by hosts and routers taking appropriate actions depending on the versions of IGMP operating on them.

IGMP-Auto: Compatibility mode is selected automatically.

Forced IGMPv1: Compatible with IGMP version 1.

Forced IGMPv2: Compatibility with IGMP version 2.

Forced IGMPv3: Compatible with IGMP version 3.

Default: IGMP-Auto

PRI: Priority of Interface (PRI) indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest).

Default: 0

RV: Robustness Variable (RV) allows tuning for the expected packet loss on a network. The allowed range is **1** to **255**.

Default: 2

QI (sec): Query Interval (QI) is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds.

Default: 125

QRI (0.1 sec): Query Response Interval (QRI) is used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds.

Default: 100 (10 seconds)


LLQI (0.1 sec): LLQI is the Last Member Query Interval (LMQI) for IGMP. It is the time value represented by the Last Member Query Interval multiplied by the Last Member Query Count. The allowed range is **0** to **31744** in tenths of seconds.


Default: 10 (1 second)

URI (sec): Unsolicited Report Interval (URI) is the time between repetitions of a host's initial report of membership in a group. The allowed range is **0** to **31744** seconds.

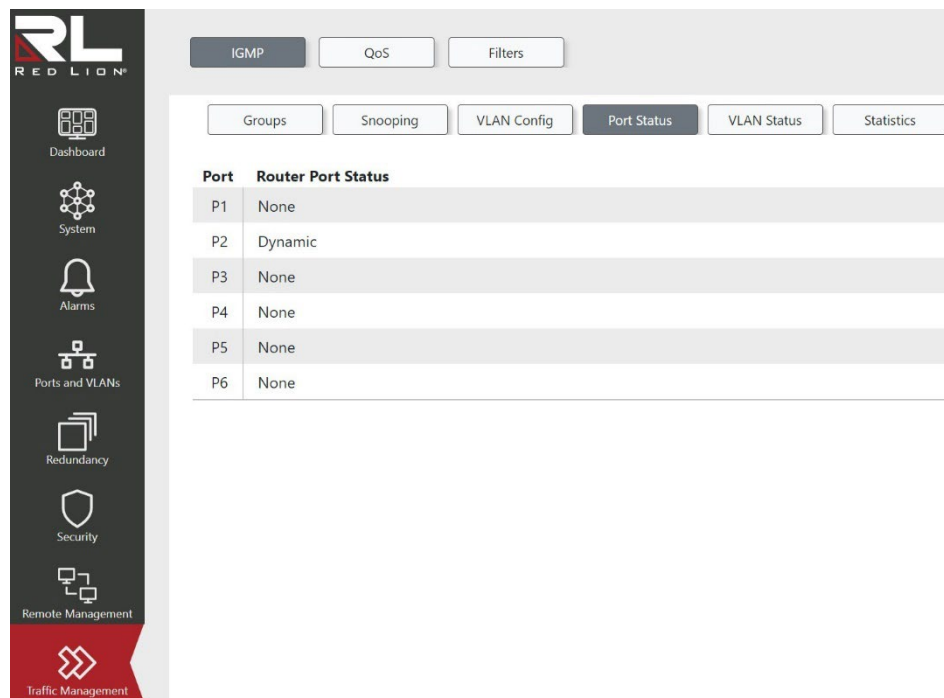
Default: 1

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Port Status



Port	Router Port Status
P1	None
P2	Dynamic
P3	None
P4	None
P5	None
P6	None

This page displays the current Router Port Status for each port.

Port: The port name.

Router Port Status: Indicates the Router Port Status for this port. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Possible values are:


Static: The port has been manually configured to be a router port.


Dynamic: The port has dynamically learned to be a router port.

Both: The port has both been manually configured and has dynamically learned to be a router port.

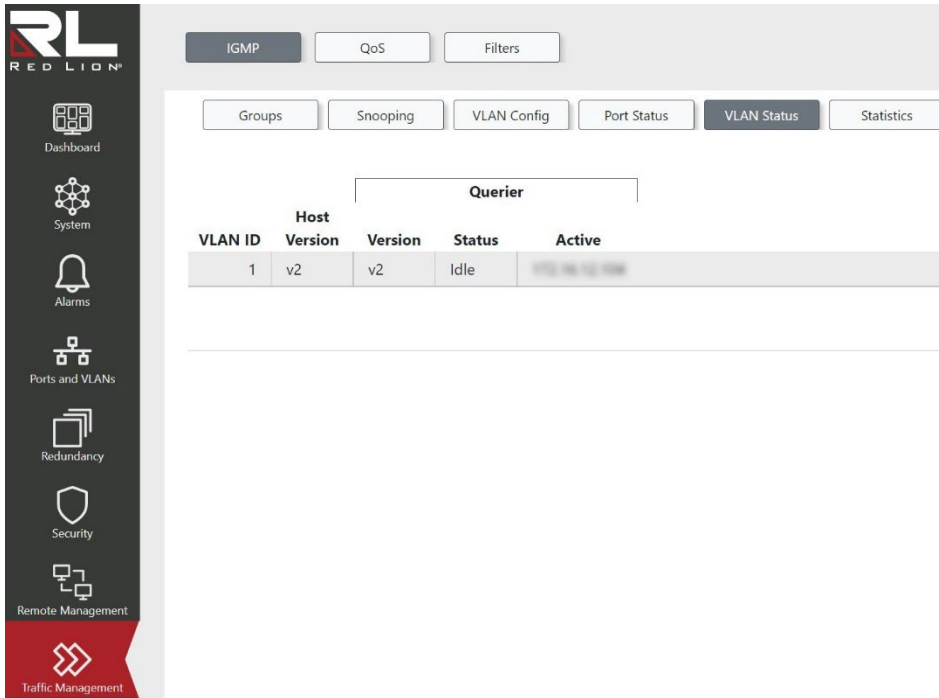
None: The port is not currently a router port. In other words it has not been manually configured nor has it dynamically learned to be a router port.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

VLAN Status



This page displays the current IGMP VLAN status values.

VLAN ID: The VLAN ID of the group.

Host Version: Current host Version.

Querier Version: Current querier Version.

Querier Status: Displays the querier status. Possible values are:

- Init
- Active
- Idle

Disabled: Indicates the specific interface is administratively disabled.

Querier Active: IP Address of the active querier.

Buttons

(↻) Automatic refresh occurs every 3 seconds.

↻ Click to refresh the values on the page.

Statistics

VLAN ID	Queries		Joins			Leaves
	Tx	Rx	V1	V2	V3	
1	1	2808	0	19764	46	92

This page provides IGMP Statistics information.

VLAN ID: The VLAN ID of the entry.

Queries Tx: The number of Transmitted Queries.

Queries Rx: The number of Received Queries.


Joins V1: The number of V1 Joins Received.


Joins V2: The number of V2 Joins Received.

Joins V3: The number of V3 Joins Received.

Leaves: The number of V2 Leaves Received.

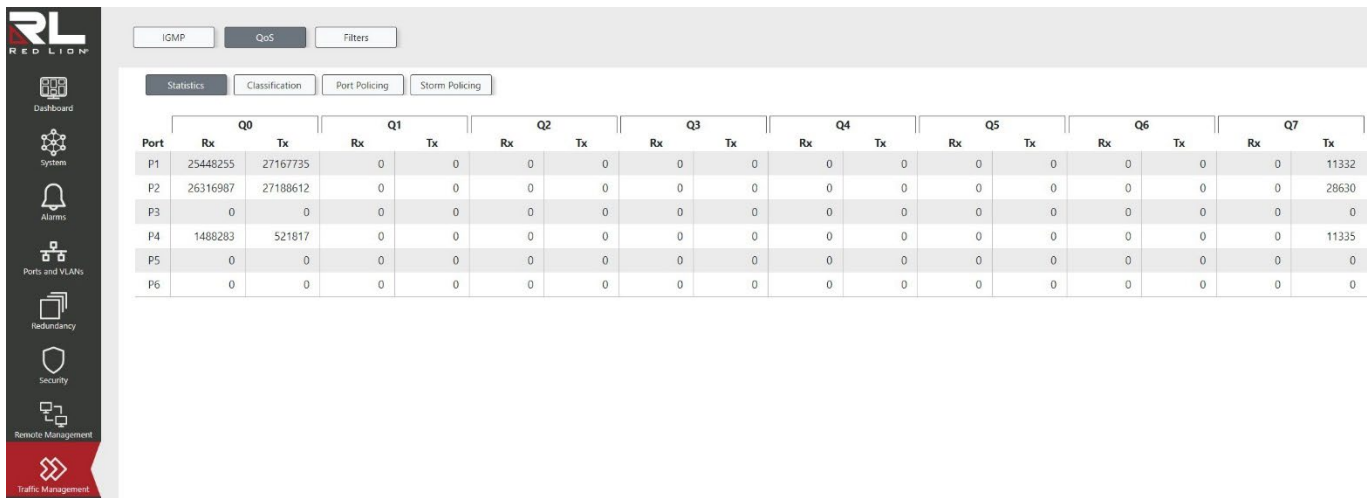
Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

QoS

Statistics



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7		Tx
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	
P1	25448255	27167735	0	0	0	0	0	0	0	0	0	0	0	0	0	0	11332
P2	26316987	27188612	0	0	0	0	0	0	0	0	0	0	0	0	0	0	28630
P3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P4	1488283	521817	0	0	0	0	0	0	0	0	0	0	0	0	0	0	11335
P5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

This page provides statistics for the queues for all switch ports.
The counters are defined as follows:


Port: The logical port for the settings contained in the same row.


Qn: There are 8 QoS queues per port, Q0 - Q7 where Q0 is the lowest priority queue.

Rx: The number of received packets per queue.

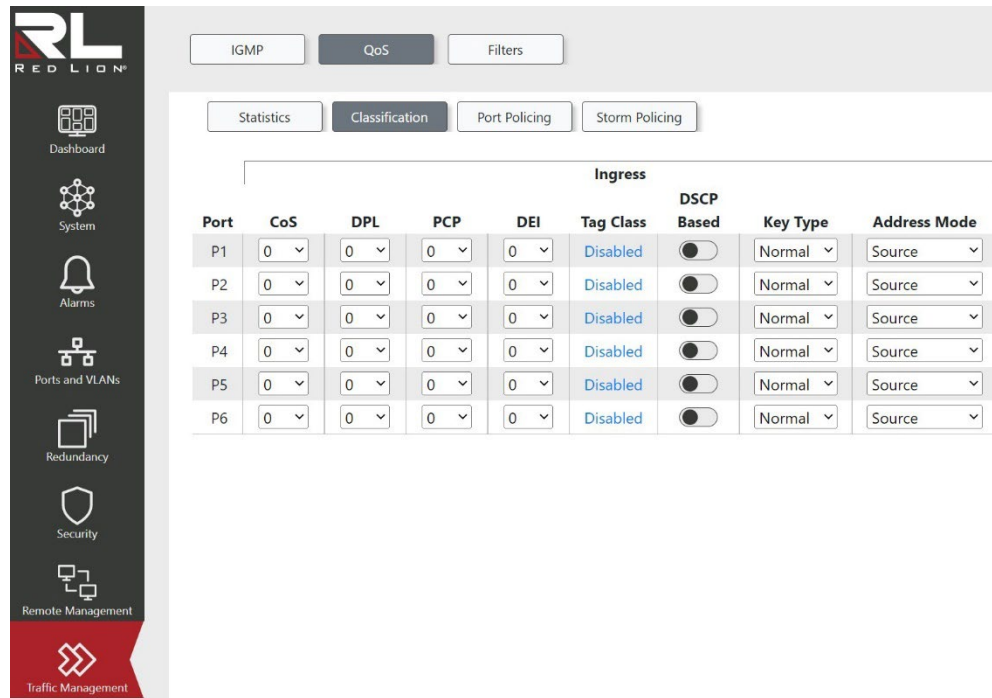
Tx: The number of transmitted packets per queue.

Buttons

 Automatic refresh occurs every 3 seconds.

 Click to refresh the values on the page.

Classification



This page allows you to configure the basic QoS Classification settings for all switch ports. The settings are defined as follows:

Port: The port number for the configuration row.

CoS: Sets the CoS (Class of Service) value. All frames are classified to a CoS. There is a one-to-one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the CoS value set here.

Default: 0

DPL: Sets the DPL (Drop Precedence Level) value. All frames are classified to a DPL value. If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the DPL value set here.

Default: 0

PCP: Sets the PCP (Primary Code Point) value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the PCP value set here.

Default: 0

DEI: Sets the DEI (Drop Eligibility Indicator) value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the DEI value set here.

Default: 0

Tag Class:

Enable or disable the classification mode for tagged frames on this port.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Disabled: Use CoS and DPL values as set on this page for tagged frames.

Clicking on the mode opens a window to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the CoS and DPL values as set on this page.

Default: Disabled

DSCP Based: Enable or disable DSCP Based QoS Ingress Port Classification.

Default: Disabled

Key Type:

Sets the key type specifying the key generated for frames received on the port. The allowed values are:

Normal: Half key, match outer tag, SIP/DIP and SMAC/DMAC.

Double Tag: Quarter key, match inner and outer tag.

IP Address: Half key, match inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only.

MAC and IP Address: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP. Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.

Default: Normal

Address Mode:

Sets the IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. This parameter is only used when the key type is Normal. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

Default: Source

Buttons

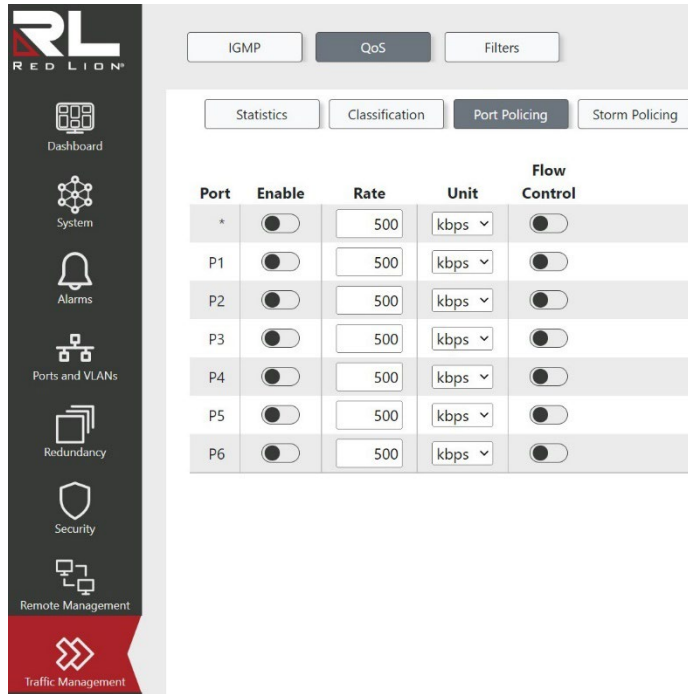


Click to refresh the values on the page.



Applies the changes to the device.

Port Policing



This page allows you to configure the Policing settings for all switch ports. The settings are defined as follows:

Port: The port number for the configuration row.

Enable: Enable or disable the port policing for this switch port.

Default: Disabled

Rate:

Controls the rate for the port policer.

Valid Range is 100-3276700 when Unit is kbps or fps.

Valid Range is 1-3276 when Unit is Mbps or kfps.

The rate is internally rounded up to the nearest value supported by the port policer.

Default: 500

Unit:

Controls the unit of measurement for the port policing rate:

kbps: Kilobits per second

Mbps: Megabits per second

fps: Frames per second


kfps: Kilo frames per second


Default: kbps

Flow Control: Enable or disable, if enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

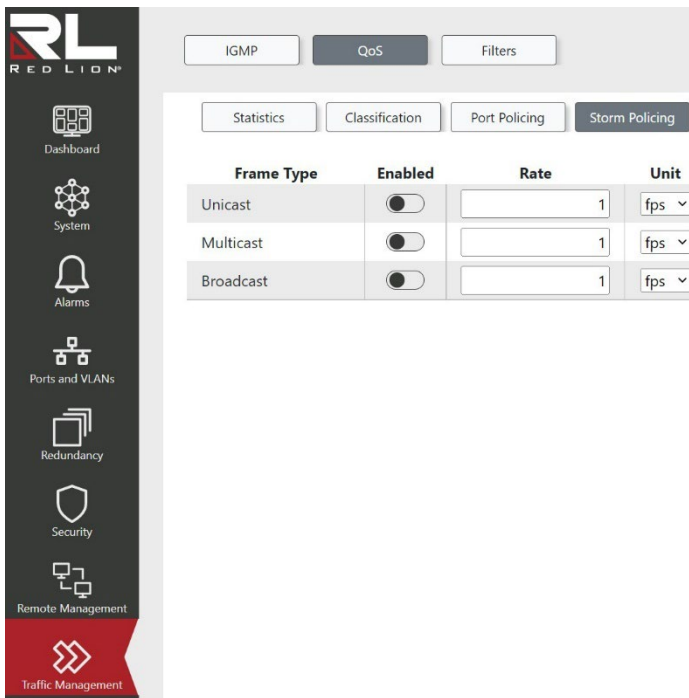
Default: Disabled

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Storm Policing



Frame Type	Enabled	Rate	Unit
Unicast	<input type="checkbox"/>	1	fps
Multicast	<input type="checkbox"/>	1	fps
Broadcast	<input type="checkbox"/>	1	fps

Global storm policing for the switch is configured on this page. There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table. The settings are defined as follows:

Frame Type: The frame type for which the configuration below applies.

Enabled: Enable or disable the global storm policer for the given frame type.

Default: Disabled

Rate: Controls the rate for the global storm policer. This value is restricted to 1-1024000 when Unit is fps, and 1-1024 when Unit is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512 fps for rates <= 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 and 1024 kfps for rates > 512 fps.

Default: 1

Unit:


Controls the unit of measure for the global storm policer rate as fps or kfps.


fps: Frames per second.

kfps: Kilo frames per second.

Default: fps

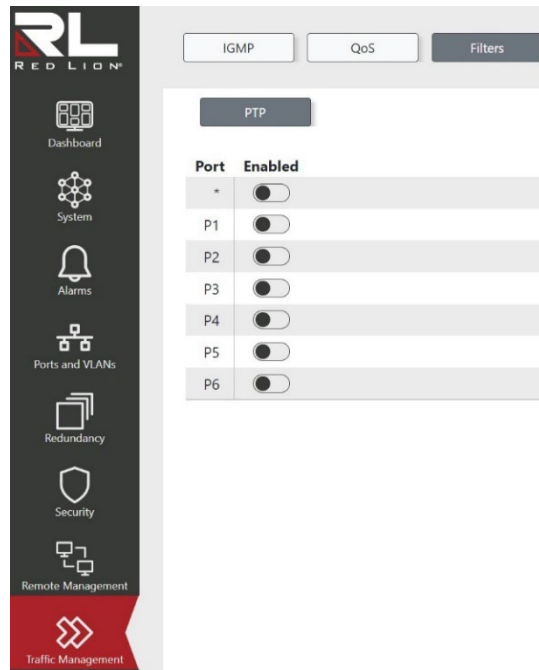
Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Filters

PTP




This page allows for the configuration of the PTP traffic filter on a per port basis. PTP frames received on an enabled port will be discarded.


Port: The name of the port that the filter will apply to.

Enabled: Enable or disable PTP traffic filtering per port.

Default: Disabled

Buttons

 Click to refresh the values on the page.

 Applies the changes to the device.

Appendix A CLI Commands

Introduction

This appendix describes the CLI operator interface provided in the Red Lion Controls NT5000 switch.

The Command Line Interface (CLI) can be accessed by connecting a host device to the console port 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 detailed information, see the “Console Connection” section of the NT5000 Hardware Manual.

There are two additional methods for connecting to the CLI: Telnet and SSH. Using any standard Telnet client, simply 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 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 is 'admin' default password is " (blank). After the first logon in using the default password, the admin user will be prompted to create a new admin user with a new password. 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:

Connection Interface

To connect a host PC to the Console port, an RS232-to-Micro USB or a USB A-to-Micro USB is required. This is supplied with the switch. For details see the Hardware Guide.

INTERFACE	PARAMETER
Console	Baud rate: 115200bps Data bit: 8 Parity: None Stop bit: 1 Flow Control: None
Telnet	Port 23
SSH	Port 22 (In Windows, you can run terminal emulator such as PuTTY)

Login Example

```
Username: test
Password:
#
MAC Address       : 00:07:af:dd:39:50
Serial Number     : J202210271341
Previous Restart  : Cool

System Contact    :
System Name       :
System Location   :
System Time       : 2022-01-01 00:19:52 UTC (UTC+00:00)
System Uptime     : 1D 00:55:35
```

```

Active Image
-----
Image           : Primary
Version        : 1.1.3
Date           : Dec 06 2022, 15:48:41
Upload filename : smb_jubilee-ocelot_pcb120.mfi

Alternate Image
-----
Image           : Backup
Version        : 1.1.3
Date           : Nov 18 2022, 13:36:30
Upload filename : smb_jubilee-ocelot_pcb120.mfi

Boot Loader
-----
Image           : RedBoot
Version        : 1.1.1
Date           : Sep 9 2022, 15:40:46

Product Information
-----
Switch Model    : NT5010-GX2
Switch Family   : NT5000
Port Count     : 10
Firmware Version : 1.1.3
Build Date     : Dec 06 2022, 15:48:41

#
    
```

Execution Modes

The CLI contains several execution modes. Users will see different sets of commands under different execution modes. When users enter an execution mode, the corresponding mode prompt will appear on the screen automatically. Table 1 lists all of the execution modes and mode prompts.

Table 1: List of Execution Modes

MODE	TO ENTER MODE	PROMPT
Initial Mode	login, disable	>
Enable Mode	enable	#
Configure Mode	configure terminal	(config)#
Interface Gigabit Configure Mode	interface P <portNo>	(config-if)#
Interface LLAG Configure Mode	interface llag <number>	(config-llag)#
Interface VLAN Configure Mode	interface vlan <vlanid>	(config-if-vlan)#
Line Terminal Configure Mode.	line <number> line console <number> line vty <number>	(config-line)#
Spanning Tree Aggregation Configure Mode.	spanning-tree aggregation	(config-stp-aggr)#
IC Profile Configure Mode	ipmc profile <word16>	(config-ipmc-profile)#
VLAN Mode	VLAN <vlan_list>	<config-vlan>#

Help

A user can get help by entering a question mark '?' at any position in the command. The displayed result depends on the execution mode and previous input. Entering a question mark again on the same command will display the command syntax.

Terminal Key Function

Following is the list of all the terminal keys and their functions.

Table 2: List of Terminal Keys

KEYS	FUNCTION
ENTER	Run a CLI config script
CTRL-M	
TAB	Tab completion If Tab is pressed after a non-whitespace character, this completes the word before the Tab. If Tab is pressed after a whitespace character, this completes the next word.
CTRL-I	
?	Display available commands If ? is pressed after a non-whitespace character, this shows possible choices for this word. If ? is pressed after a whitespace character, this shows possible choices for the next word.
<Up Arrow>	Up history
CTRL-P	
<Down Arrow>	Down history
CTRL-N	
Home	Move the cursor to the beginning of the input line
CTRL-A	
End	Move the cursor to the end of the input line
CTRL-E	
<Left Arrow>	Move the cursor backward
CTRL-B	
<Right Arrow>	Move the cursor forward
CTRL-F	
BACKSPACE	Erase the character before the cursor
CTRL-H	

Notation Conventions

The notation conventions for the parameter syntax of each CLI command are as follows:

- Parameters enclosed in [] are optional.
- Parameter values are separated by a vertical bar "|" only when one of the specified values can be used.
- Parameter values are enclosed in { } when you must use one of the values specified.

Initialize (Disable) Mode Commands

To enter this mode type “disable” after logging in to the switch. To return to this type end under any other mode and then “disable”.

clear

Description	Clear Address Conflict Detection.
Syntax	<ul style="list-style-type: none">clear ip acd
Example	<ul style="list-style-type: none">clear ip acd

disable

Description	Turn off privileged commands.
Syntax	<ul style="list-style-type: none">disable [<new_priv>]
Examples	<ul style="list-style-type: none">disabledisable 3

do

Description	Run exec commands in the configuration mode.
Syntax	<ul style="list-style-type: none">do <command>
Example	<ul style="list-style-type: none">do show running-config

enable

Description	Turn on privileged commands.
Syntax	<ul style="list-style-type: none">enable [<new_priv>]
Examples	<ul style="list-style-type: none">enableenable 5

exit

Description	Logs out of the switch.
Syntax	<ul style="list-style-type: none">exit
Example	<ul style="list-style-type: none">exit

help

Description	Description of the interactive help system.
Syntax	<ul style="list-style-type: none">help
Example	<ul style="list-style-type: none">help

logout

Description	Exit from EXEC mode.
Syntax	<ul style="list-style-type: none">logout
Example	<ul style="list-style-type: none">logout

ping

Description	Send ICMP echo messages.
Syntax	<ul style="list-style-type: none"> ping ip { <domain_name> <ip_addr> } [ttl <ttl_value>] [repeat <count>] [{ saddr <src_addr> sif { <port_type> <src_if> vlan <vlan_id> } }] [size <size>] [data <data_value>] [{ verbose quiet }]
Example	<ul style="list-style-type: none"> ping ip 192.0.2.11

show

Description	Show various settings.
Syntax	<ul style="list-style-type: none"> show clock show clock detail show dot1x statistics { eapol radius all } [interface (<port_type> [<v_port_type_list>])] show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief] show firmware key show history show interface (<port_type> [<in_port_list>]) switchport show interface (<port_type> [<port_list>]) capabilities show interface (<port_type> [<port_list>]) description show interface (<port_type> [<port_list>]) statistics [{ packets bytes errors discards filtered dot3br { priority [<priority_list>] } }] [{ up down }] show interface (<port_type> [<port_list>]) status [err-disable] [details [clause-73]] show interface (<port_type> [<port_list>]) veriphy show ip acd show ip arp show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail] show ip igmp snooping mrouter [detail] show ip igmp snooping router-mode show ip interface [brief] show ip neighbor show ip route show ip statistics [system] show licenses [details] show line [alive] show lldp med media-vlan-policy [<v_0_to_31>] show lldp med remote-device [interface (<port_type> [<port_list>])] show lldp neighbors [interface (<port_type> [<v_port_type_list>])] show lldp preempt [interface (<port_type> [<v_port_type_list>])] show lldp statistics [interface (<port_type> [<v_port_type_list>])] show mac address-table [conf static aging-time { { learning count } [interface (<port_type> [<v_port_type_list>]) vlan <v_vlan_id_2> }] { address <v_mac_addr> [vlan <v_vlan_id>] } vlan <v_vlan_id_1> interface (<port_type> [<v_port_type_list_1>])] show port-security [interface (<port_type> [<plist>])] show port-security address [interface (<port_type> [<plist>])] show privilege show system cpu status show system identity show system led status [switch <switch_list>] show tech-support show terminal show users [myself] show version [brief] show web privilege group [<group_name>] level
Examples	<ul style="list-style-type: none"> show interface p 1 status show mac address-table

traceroute

Description	Send IP Traceroute messages.
Syntax	<ul style="list-style-type: none">traceroute ip { <domain_name> <ip_addr> } [dscp <dscp>] [timeout <timeout>] [{ saddr <src_addr> sif { <port_type> <src_if> vlan <vlan_id> } }] [probes <probes>] [firstttl <firstttl>] [maxttl <maxttl>] [icmp] [numeric]
Example	<ul style="list-style-type: none">traceroute ip 192.0.2.11 timeout 30 icmp dscp 12

Enable Mode Commands

This is the default mode available after logging in to the CLI.

All commands in this mode can be executed from any other mode using the “do” command.

clear

Description	Clear various settings.
Syntax	<ul style="list-style-type: none"> clear access management statistics clear dot1x statistics [interface (<port_type> [<v_port_type_list>])] clear ip acd clear ip arp clear ip igmp snooping [vlan <v_vlan_list>] statistics clear ip statistics clear known-host-keys clear lacp statistics clear lldp statistics [{ interface (<port_type> [<plist>]) } global] clear logging [informational] [notice] [warning] [error] clear mac address-table clear port-security dynamic [{ address <mac> [vlan <vlan_on_mac>] } { interface (<port_type> [<plist>]) [vlan <vlan_on_interface>] } vlan <vlan>] clear spanning-tree { { statistics [interface (<port_type> [<v_port_type_list>])] } { detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } } clear statistics [interface] (<port_type> [<port_list>]) clear system led status [switch <switch_list>] { fatal software post ztp stack-firmware all }
Examples	<ul style="list-style-type: none"> clear mac address-table

configure

Description	Enter configuration mode.
Syntax	<ul style="list-style-type: none"> configure terminal
Example	<ul style="list-style-type: none"> configure terminal

copy

Description	Copy files.
Syntax	<ul style="list-style-type: none"> copy { startup-config running-config <source_path> } { startup-config running-config <destination_path> } [syntax-check]
Examples	<ul style="list-style-type: none"> copy running-config startup-config syntax-check copy flash:profinet_log.dat tftp://mytftpserver/profinetlog.txt

delete

Description	Deletes a file in the "flash:" file system.
Syntax	<ul style="list-style-type: none"> delete <path>
Example	<ul style="list-style-type: none"> delete flash:profinet_log.dat

dir

Description	List all files in the "flash:" file system.
Syntax	<ul style="list-style-type: none"> dir
Example	<ul style="list-style-type: none"> dir

disable

Description	Turn off privileged commands.
Syntax	<ul style="list-style-type: none"> disable [<new_priv>]

Examples	<ul style="list-style-type: none"> • disable • disable 3
-----------------	--

do

Description	Run exec commands in the configuration mode.
Syntax	<ul style="list-style-type: none"> • do <command>
Example	<ul style="list-style-type: none"> • do show running-config

enable

Description	Turn on privileged commands.
Syntax	<ul style="list-style-type: none"> • enable [<new_priv>]
Examples	<ul style="list-style-type: none"> • enable • enable 5

exit

Description	Exit from EXEC mode.
Syntax	<ul style="list-style-type: none"> • exit
Example	<ul style="list-style-type: none"> • exit

firmware

Description	Firmware upgrade/swap.
Syntax	<ul style="list-style-type: none"> • firmware swap • firmware upgrade <url_file>
Example	<ul style="list-style-type: none"> • firmware swap

help

Description	Description of the interactive help system.
Syntax	<ul style="list-style-type: none"> • help
Example	<ul style="list-style-type: none"> • help

ip

Description	IPv4 commands.
Syntax	<ul style="list-style-type: none"> • ip dhcp retry interface vlan <vlan_id>
Example	<ul style="list-style-type: none"> • ip dhcp retry interface vlan 2

logout

Description	Exit from EXEC mode.
Syntax	<ul style="list-style-type: none"> • logout
Example	<ul style="list-style-type: none"> • logout

more

Description	Display file.
Syntax	<ul style="list-style-type: none"> • more <path>
Examples	<ul style="list-style-type: none"> • more tftp://server/path-and-filename • more flash:path-and-filename

no

Description	Reset settings to defaults.
Syntax	<ul style="list-style-type: none"> no terminal editing no terminal exec-timeout no terminal history size no terminal length no terminal width
Example	<ul style="list-style-type: none"> no terminal history size

ping

Description	Send ICMP echo messages.
Syntax	<ul style="list-style-type: none"> ping ip { <domain_name> <ip_addr> } [ttl <ttl_value>] [repeat <count>] [{ saddr <src_addr> sif { <port_type> <src_if> vlan <vlan_id> } }] [size <size>] [data <data_value>] [{ verbose quiet }]
Example	<ul style="list-style-type: none"> ping ip 192.0.2.11

reload

Description	Reload system and reset configuration to factory defaults.
Syntax	<ul style="list-style-type: none"> reload { cold warm defaults [keep-ip] [keep-users] [keep-snmp] [keep-portsec] [force] }
Examples	<ul style="list-style-type: none"> reload cold reload defaults

send

Description	Send a message to other TTY lines. The command requires a delimiter character. After pressing enter all the text typed before the delimiter character is found will be sent to the specified TTY line.
Syntax	<ul style="list-style-type: none"> send { * <session_list> console 0 vty <vty_list> } <message>
Example	<ul style="list-style-type: none"> send * . hello.

show

Description	Show running system information.
Syntax	<ul style="list-style-type: none"> show aaa show access management [statistics <access_id_list>] show access-list rate-limiter [<rate_limiter_list>] show adc show adcinputs show aggregation [mode] show alarm config show alarm config port-usage (<port_type> [<o_ports_list>]) show alarm logging { active history } show alarm sources [<filter>] show alarm status [<alarm_name>] show clock show clock detail show dot1x statistics { eapol radius all } [interface (<port_type> [<v_port_type_list>])] show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief] show filter ptp show firmware key show history show interface (<port_type> [<in_port_list>]) switchport show interface (<port_type> [<port_list>]) capabilities show interface (<port_type> [<port_list>]) description show interface (<port_type> [<port_list>]) statistics [{ packets bytes errors discards filtered dot3br { priority [<priority_list>] } }] [{ up down }]

- show interface (<port_type> [<port_list>]) status [err-disable] [details [clause-73]]
- show interface (<port_type> [<port_list>]) veriphy
- show interface vlan [<vlist>]
- show ip acd
- show ip arp
- show ip http
- show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
- show ip igmp snooping mrouter [detail]
- show ip igmp snooping router-mode
- show ip interface [brief]
- show ip neighbor
- show ip route
- show ip ssh
- show ip statistics [system]
- show ip telnet
- show ipmc profile [<profile_name>] [detail]
- show ipmc range [<entry_name>]
- show lacp { internal | statistics | system-id | neighbor } [details]
- show licenses [details]
- show line [alive]
- show lldp med media-vlan-policy [<v_0_to_31>]
- show lldp med remote-device [interface (<port_type> [<port_list>])]
- show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
- show lldp preempt [interface (<port_type> [<v_port_type_list>])]
- show lldp statistics [interface (<port_type> [<v_port_type_list>])]
- show logging <log_id>
- show logging [informational] [notice] [warning] [error]
- show loop-protect [interface (<port_type> [<plist>])]
- show mac address-table [conf | static | aging-time [{ { learning | count } } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>]]] [{ address <v_mac_addr> [vlan <v_vlan_id>] }] [vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]]
- show monitor [session { <session_number> | all | remote }]
- show nring
- show ntp status
- show nview
- show platform debug
- show platform phy [interface (<port_type> [<v_port_type_list>])]
- show platform phy id [interface (<port_type> [<v_port_type_list>])]
- show platform phy instance
- show port-security [interface (<port_type> [<plist>])]
- show port-security address [interface (<port_type> [<plist>])]
- show power
- show privilege
- show process list [detail]
- show process load
- show qos [{ interface [(<port_type> [<port>])] }] [storm]
- show radius-server [statistics]
- show rmon alarm [<id_list>]
- show rmon event [<id_list>]
- show rmon history [<id_list>]
- show rmon statistics [<id_list>]
- show running-config [all-defaults]
- show running-config feature <feature_name> [all-defaults]
- show running-config interface (<port_type> [<list>]) [all-defaults]
- show running-config interface vlan <list> [all-defaults]
- show running-config line { console | vty } <list> [all-defaults]
- show running-config vlan [{ <vlan_list> }] [all-defaults]
- show snmp
- show snmp access [<group_name> [{ v1 | v2c | v3 | any }] [{ auth | noauth | priv }]]
- show snmp community [<community>]
- show snmp host [<conf_name>]
- show snmp mib context

	<ul style="list-style-type: none"> • show snmp mib ifmib ifIndex [port] [aggregation] [vlan] • show snmp security-to-group [{ v1 v2c v3 } [<security_name>]] • show snmp trap [<source_name>] • show snmp user [<username>] • show snmp view [<view_name> [<oid_subtree>]] • show spanning-tree [summary active { interface (<port_type> [<v_port_type_list>]) } { detailed [interface (<port_type> [<v_port_type_list_1>])] } { mst [configuration { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }]]]]] • show system cpu status • show system identity • show system led status [switch <switch_list>] • show tech-support • show temperature • show terminal • show user-lockout • show user-lockout username { all <username> } • show user-privilege • show username password length • show users [myself] • show version [brief] • show vlan [id <vlan_list> name <name>] • show vlan status [interface (<port_type> [<plist>])] [admin all combined conflicts mstp nas rmirror] • show web privilege group [<group_name>] level • show webserver
Examples	<ul style="list-style-type: none"> • show running-config • show qos interface P 1 • show interface vlan 1

terminal

Description	Set terminal line parameters.
Syntax	<ul style="list-style-type: none"> • terminal editing • terminal exec-timeout <min> [<sec>] • terminal help • terminal history size <history_size> • terminal length <lines> • terminal width <width>
Examples	<ul style="list-style-type: none"> • terminal exec-timeout 30 50 • terminal length 250

traceroute

Description	Send IP Traceroute messages.
Syntax	<ul style="list-style-type: none"> • traceroute ip { <domain_name> <ip_addr> } [dscp <dscp>] [timeout <timeout>] [{ saddr <src_addr> sif { <port_type> <src_if> vlan <vlan_id> } }] [probes <probes>] [firstttl <firstttl>] [maxttl <maxttl>] [icmp] [numeric]
Example	<ul style="list-style-type: none"> • traceroute ip 192.0.2.11 timeout 30 icmp dscp 12

veriphy

Description	Run veriphy cable diagnostics.
Syntax	<ul style="list-style-type: none"> • veriphy [{ interface (<port_type> [<v_port_type_list>]) }]]
Examples	<ul style="list-style-type: none"> • veriphy interface P 1 • veriphy

Configure Mode Commands

To enter this execution mode type "**configure terminal**" under any execution mode.

access

Description	Access management configuration. It is used to specify access management entries. Up to 16 entries can be added.
Syntax	<ul style="list-style-type: none"> access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] all }
Examples	<ul style="list-style-type: none"> access management 1 1 192.0.0.3 to 192.0.2.5 SNMP access management 1 1 192.0.0.3 all

access-list

Description	Configure access control lists and rate limits. Up to 128 access control entries can be specified. Access control filter policies can be specified by value, bitmask, and frame type. Entries can be port specific or by VLAN. The access control actions can be monitored with mirroring and logging. VLAN filters can also be used. Additionally rate-limiting policies can be implemented. Up to 16 rate-limiting configurations can be specified, using packets per second (pps) or kilobits per second (kbps).
Syntax	<ul style="list-style-type: none"> access-list rate-limiter [<rate_limiter_list>] { [100pps <pps100_rate> 100kbps <kpbs100_rate>] [dmac-type { unicast multicast broadcast any }] [ingress { interface { (<port_type> [<ingress_port_list>) } } any none }] }
Examples	<ul style="list-style-type: none"> access-list rate-limiter 100kbps 200 access-list rate-limiter 2 100pps 33

aggregation

Description	Configure aggregation mode.
Syntax	<ul style="list-style-type: none"> aggregation mode { [smac] [dmac] [ip] [port] } * 1
Example	<ul style="list-style-type: none"> aggregation mode ip

alarm

Description	Configure alarms.
Syntax	<ul style="list-style-type: none"> alarm <alarm_name> <alarm_expression> alarm config contact-relay-operation { close-on-alarm open-on-alarm } alarm config { { [power-dc-v1] [power-dc-v2] [port-link-down] [port-usage] [configuration] all } [enable { yes no }] [led { active ignore }] [contact-relay { trigger ignore }] [event-log { yes no }] [event-severity { error warning notice informational }] }
Example	alarm config power-dc-v2 enable yes led active

banner

Description	Define a banner. Banners can be configured for process execution, login, or a message of the day. Multiple lines can be added by pressing enter before typing the delimiter character.
Syntax	<ul style="list-style-type: none"> banner [motd login exec] <banner>
Examples	<ul style="list-style-type: none"> banner motd ! Today's the day! banner * This banner is delimited by asterisk*

clock

Description	Configure time-of-day clock.
Syntax	<ul style="list-style-type: none"> clock datetime <input_year> <input_month> <input_day> <input_hour> <input_minute> <input_second>

	<ul style="list-style-type: none"> clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]] clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]] clock timezone { preset { <preset_id_var> options } manual <word_var> { <hour_var> } [<minute_var>] }
Examples	<ul style="list-style-type: none"> clock datetime 2020 08 12 15 45 45 clock timezone moria 13 15

default

Description	• Set rate limiters for access control lists to defaults.
Syntax	• default access-list rate-limiter [<rate_limiter_list>]
Example	• default access-list rate-limiter

do

Description	Used to run exec commands in the configuration mode.
Syntax	• do <command>
Example	• do show running-config

enable

Description	Modify enable password parameters.
Syntax	<ul style="list-style-type: none"> enable password [level <priv>] <password> enable secret { 0 5 } [level <priv>] <password>
Examples	<ul style="list-style-type: none"> enable password newpass enable secret 5 encryptedpw

end

Description	Go back to EXEC mode
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

hostname

Description	Set system's network name.
Syntax	• hostname <hostname>
Example	• hostname myswitch

interface

Description	Select an interface to configure. This sets the CLI in interface configuration mode.
Syntax	<ul style="list-style-type: none"> interface (<port_type> [<plist>]) interface llag <llag_id> interface vlan <vlist>
Examples	<ul style="list-style-type: none"> interface vlan 1 interface P 2 P 5 (configure interfaces 2 and 5 together)

ip

Description	Interface Internet Protocol configuration commands.
Syntax	<ul style="list-style-type: none"> ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] delete generate } ip http secure-redirect ip http secure-server ip igmp host-proxy [leave-proxy] ip igmp router-mode { auto manual none } ip igmp snooping ip igmp snooping vlan <v_vlan_list> ip igmp unknown-flooding ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw> [distance <v_distance>] ip route <v_ipv4_subnet> <v_ipv4_gw> [distance <v_distance>] ip ssh ip telnet
Examples	<ul style="list-style-type: none"> ip http secure-server ip igmp snooping

ipmc

Description	IPv4 multicast configuration.
Syntax	<ul style="list-style-type: none"> ipmc profile ipmc profile <profile_name> ipmc range <entry_name> <v_ipv4_mcast> [<v_ipv4_mcast_1>]
Examples	<ul style="list-style-type: none"> ipmc profile testprofile ipmc range testrange 224.0.0.1 224.0.0.4

json

Description	JavaScript Object Notation RPC.
Syntax	<ul style="list-style-type: none"> json notification host <hname> json notification listen <notification> <host>
Examples	<ul style="list-style-type: none"> json notification host jsonhost json notification listen ip.status.interface..update jsondest

lACP

Description	LACP settings.
Syntax	<ul style="list-style-type: none"> lACP system-priority <v_1_to_65535>
Example	<ul style="list-style-type: none"> lACP system-priority 50

line

Description	Configure a terminal line.
Syntax	line { <0~16> console 0 vty <0~15> }
Examples	<ul style="list-style-type: none"> line 0 line console 0 line vty 2

lldp

Description	Link Layer Discover Protocol configuration.
Syntax	<ul style="list-style-type: none"> • lldp holdtime <val> • lldp reinit <val> • lldp timer <val> • lldp transmission-delay <val>
Examples	<ul style="list-style-type: none"> • lldp holdtime 5 • lldp timer 60

logging

Description	System logging configuration.
Syntax	<ul style="list-style-type: none"> • logging host <ipv4_addr> • logging level { informational notice warning error } • logging notification listen <name> level { informational notice warning error } <node> • logging on
Examples	<ul style="list-style-type: none"> • logging host 192.0.3.47 • logging level warning

loop-protect

Description	Loop protection configuration.
Syntax	<ul style="list-style-type: none"> • loop-protect • loop-protect shutdown-time <t> • loop-protect transmit-time <t>
Example	<ul style="list-style-type: none"> • loop-protect shutdown-time 30

mac

Description	MAC table entries/configuration.
Syntax	<ul style="list-style-type: none"> • mac address-table aging-time <v_0_10_to_1000000> • mac address-table learning vlan <vlan_list> • mac address-table static <v_mac_addr> vlan <v_vlan_id> [interface (<port_type> [<v_port_type_list>])]
Examples	<ul style="list-style-type: none"> • mac address-table aging-time 10 • mac address-table static 00:aa:bb:11:33:44 vlan 2

monitor

Description	Configure monitoring (port mirroring)
Syntax	<ul style="list-style-type: none"> • monitor session <session_number> [destination { interface (<port_type> [<di_list>]) remote vlan <drvid> reflector-port <port_type> <rportid> } source { interface (<port_type> [<si_list>]) [both rx tx] remote vlan <srvid> vlan <source_vlan_list> cpu [both rx tx] }]
Examples	<ul style="list-style-type: none"> • monitor session 1 source interface P 1 rx • monitor session 1 destination remote vlan 2 reflector-port P 5

no

Description	Set various settings to the default value.
Syntax	<ul style="list-style-type: none"> • no access management • no access management <access_id_list> • no access-list rate-limiter [<rate_limiter_list>] • no aggregation mode • no alarm [<alarm_name>] • no banner [motd login exec] • no clock summer-time

- no clock timezone
- no enable password [level <priv>]
- no enable secret { [0 | 5] } [level <priv>]
- no hostname
- no interface llag <llag_id>
- no interface vlan <vlist>
- no ip http secure-redirect
- no ip http secure-server
- no ip igmp host-proxy [leave-proxy]
- no ip igmp snooping
- no ip igmp snooping vlan [<v_vlan_list>]
- no ip igmp unknown-flooding
- no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw> [distance <v_distance>]
- no ip route <v_ipv4_subnet> <v_ipv4_gw> [distance <v_distance>]
- no ip ssh
- no ip telnet
- no ipmc profile
- no ipmc profile <profile_name>
- no ipmc range <entry_name>
- no json notification host <name>
- no json notification listen [<notification> [<host>]]
- no lacp system-priority <v_1_to_65535>
- no lldp holdtime
- no lldp reinit
- no lldp timer
- no lldp transmission-delay
- no logging host
- no logging notification listen [<name>]
- no logging on
- no loop-protect
- no loop-protect shutdown-time
- no loop-protect transmit-time
- no mac address-table aging-time
- no mac address-table aging-time <v_0_10_to_1000000>
- no mac address-table learning vlan <vlan_list>
- no mac address-table static <v_mac_addr> vlan <v_vlan_id> [interface (<port_type> [<v_port_type_list>])]
- no monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote | vlan <source_vlan_list> | cpu [both | rx | tx] }]
- no nring { all | automemberdetectiontimeout | keepalivetimeout | mode | portset }
- no ntp
- no ntp server <index_var>
- no nview
- no port-security aging
- no port-security aging time
- no port-security hold time
- no privilege <mode_name> level <0-15> <cmd>
- no prompt
- no qos storm { unicast | multicast | broadcast }
- no rmon alarm <id>
- no rmon event <id>
- no snmp-server
- no snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv }
- no snmp-server community <v3_comm> [ip-range <v_ipv4_addr> <v_ipv4_netmask>]
- no snmp-server contact
- no snmp-server host <conf_name>
- no snmp-server location
- no snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
- no snmp-server trap <source_name> { [id <filter_id>] | [<oid_subtree> { include | exclude }] }
- no snmp-server user <username>
- no snmp-server view <view_name> <oid_subtree>
- no spanning-tree edge bpdu-filter

	<ul style="list-style-type: none"> • no spanning-tree edge bpdu-guard • no spanning-tree mode • no spanning-tree mst <instance> priority • no spanning-tree mst <instance> vlan • no spanning-tree mst forward-time • no spanning-tree mst hello-time • no spanning-tree mst max-age • no spanning-tree mst max-hops • no spanning-tree mst name • no spanning-tree recovery interval • no spanning-tree transmit hold-count • no user-lockout [mode threshold duration failure-reset-interval] • no username <username> • no username password <length> • no vlan protocol { { eth2 { <etype> arp ip ipx at } } { snap { <oui> rfc-1042 snap-8021h } <pid> } { llc <dsap> <ssap> } } [group <word16>] • no vlan <vlan_list> • no web privilege group [<group_name>] level
Examples	<ul style="list-style-type: none"> • no clock timezone • no spanning-tree mst name

nring

Description	Configure N-Ring™ settings.
Syntax	<ul style="list-style-type: none"> • nring automemberdetectiontimeout <v_2_to_180> • nring keepalivetimeout <v_0_15_to_300> • nring mode { automember disable } • nring portset add <v_1_to_255> <ring_port_1> <ring_port_2> • nring portset remove <v_1_to_255> • nring portset set <v_1_to_255> <ring_port_1> <ring_port_2>
Example	<ul style="list-style-type: none"> • nring keepalivetimeout 20 • nring portset add 2 3 4

ntp

Description	Configure NTP.
Syntax	• ntp server <index_var> ip-address { <ipv4_var> <name_var> }
Example	• ntp server 1 ip-address 192.0.2.33

nview

Description	Configure N-View™ settings.
Syntax	<ul style="list-style-type: none"> • nview autocastinterval <v_0_5_to_500> • nview autocastports add { * <port_type> <port_type_list> } • nview autocastports remove { * <port_type> <port_type_list> } • nview mibstatsports add { * <port_type> <port_type_list> } • nview mibstatsports remove { * <port_type> <port_type_list> } • nview mode { disable enable }
Example	<ul style="list-style-type: none"> • nview autocastinterval 5 • nview autocastports remove P 3,5-7

port-security

Description	Configure port security settings.
Syntax	<ul style="list-style-type: none"> • port-security aging • port-security aging time <aging_time> • port-security hold time <hold_time>
Examples	• port-security aging time 20

	<ul style="list-style-type: none"> port-security hold time 30
--	--

privilege

Description	Command privilege parameters.
Syntax	<ul style="list-style-type: none"> privilege <mode_name> level <privilege> <cmd>
Example	<ul style="list-style-type: none"> privilege dhcp-pool level 2 interface

prompt

Description	Set prompt.
Syntax	<ul style="list-style-type: none"> prompt <prompt>
Example	<ul style="list-style-type: none"> prompt testprompt

qos

Description	Quality of Service configuration settings.
Syntax	<ul style="list-style-type: none"> qos storm { unicast multicast broadcast } <rate> [fps kfps kbps mbps]
Examples	<ul style="list-style-type: none"> qos storm broadcast 64 fps

rmon

Description	Remote monitoring configuration.
Syntax	<ul style="list-style-type: none"> rmon alarm <id> { ifInOctets ifInUcastPkts ifInNUcastPkts ifInDiscards ifInErrors ifInUnknownProtos ifOutOctets ifOutUcastPkts ifOutNUcastPkts ifOutDiscards ifOutErrors } <ifIndex> <interval> { absolute delta } rising-threshold <rising_threshold> <rising_event_id> falling-threshold <falling_threshold> <falling_event_id> { [rising falling both] } rmon event <id> [log] [trap [<community>]] { [description <description>] }
Examples	<ul style="list-style-type: none"> rmon alarm 1 ifOutOctets 1 10 absolute rising-threshold 0 3 falling-threshold -12 3 rmon event 1 log

snmp-server

Description	Set SNMP server configuration.
Syntax	<ul style="list-style-type: none"> snmp-server snmp-server access <group_name> model { v1 v2c v3 any } level { auth noauth priv } [read <view_name>] [write <write_name>] snmp-server community <v3_comm> [ip-range <v_ipv4_addr> <v_ipv4_netmask>] { <v3_sec> encrypted <v3_sec_enc> } snmp-server contact <v_line255> snmp-server host <conf_name> snmp-server location <v_line255> snmp-server security-to-group model { v1 v2c v3 } name <security_name> group <group_name> snmp-server trap <source_name> [id <filter_id>] [<oid_subtree> { include exclude }] snmp-server user <username> [{ md5 { <md5_passwd> { encrypted <md5_passwd_encrypt> } } sha { <sha_passwd> { encrypted <sha_passwd_encrypt> } } }] [priv { des aes } { <priv_passwd> { encrypted <priv_passwd_encrypt> } }] snmp-server view <view_name> <oid_subtree> { include exclude }
Examples	<ul style="list-style-type: none"> snmp-server user testusr md5 md5 md5password priv aes privpass snmp-server access testgroup model v3 level noauth

spanning-tree

Description	Spanning Tree protocol.
Syntax	<ul style="list-style-type: none"> spanning-tree aggregation spanning-tree edge bpdu-filter spanning-tree edge bpdu-guard spanning-tree mode { stp rstp mstp } spanning-tree mst <instance> priority <prio> spanning-tree mst <instance> vlan <v_vlan_list> spanning-tree mst forward-time <fwdtime> spanning-tree mst hello-time <hellotime> spanning-tree mst max-age <maxage> [forward-time <fwdtime>] spanning-tree mst max-hops <maxhops> spanning-tree mst name <name> revision <v_0_to_65535> spanning-tree recovery interval <interval> spanning-tree transmit hold-count <holdcount>
Examples	<ul style="list-style-type: none"> spanning-tree mode rstp spanning-tree aggregation

username

Description	Establish User Name Authentication.
Syntax	<ul style="list-style-type: none"> username password length { <n_min> } { <n_max> } username { default-administrator <input_username> } privilege <priv> { password { unencrypted <unency_password> encrypted <encry_password> } }
Example	<ul style="list-style-type: none"> username testuser privilege 3 password unencrypted test

vlan

Description	VLAN commands.
Syntax	<ul style="list-style-type: none"> vlan <vlist>
Examples	<ul style="list-style-type: none"> vlan 1,50

web

Description	Web access settings.
Syntax	<ul style="list-style-type: none"> web privilege group <group_name> level { [configRoPriv <configRoPriv>] [configRwPriv <configRwPriv>] [statusRoPriv <statusRoPriv>] [statusRwPriv <statusRwPriv>] } *1
Example	<ul style="list-style-type: none"> web privilege group iP level configRwPriv 15

Interface Mode Commands for Port Interfaces

aggregation

Description	Create an aggregation.
Syntax	• aggregation group <v_uint> mode { [active on passive] }
Example	• aggregation group 1 mode passive

description

Description	Specify a description of the port.
Syntax	• description <port_desc_str>
Example	• description finance

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

duplex

Description	Configure duplex settings for the current interface.
Syntax	• duplex { half full auto [half full] }
Example	• duplex auto half

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

excessive-restart

Description	Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions).
Syntax	• excessive-restart
Example	• excessive-restart

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

flowcontrol

Description	Configure traffic flow control.
Syntax	• flowcontrol { on off }
Example	• flowcontrol on

frame-length-check

Description	Drop frames with mismatch between EtherType/Length.
--------------------	---

Syntax	<ul style="list-style-type: none"> • frame-length-check
Example	<ul style="list-style-type: none"> • frame-length-check

help

Description	Show a description of the interactive help system.
Syntax	<ul style="list-style-type: none"> • help
Example	<ul style="list-style-type: none"> • help

ip

Description	Interface Internet Protocol configuration commands.
Syntax	<ul style="list-style-type: none"> • ip igmp snooping filter <profile_name> • ip igmp snooping immediate-leave • ip igmp snooping max-groups <throttling> • ip igmp snooping mrouter • ip igmp snooping r-filter
Examples	<ul style="list-style-type: none"> • ip igmp snooping immediate-leave

lACP

Description	Enable and configure LACP on this interface.
Syntax	<ul style="list-style-type: none"> • lacp • lacp port-priority <v_1_to_65535> • lacp timeout { fast slow }
Examples	<ul style="list-style-type: none"> • lacp • lacp port-priority 5

lldp

Description	Link Layer Discover Protocol configuration.
Syntax	<ul style="list-style-type: none"> • lldp receive • lldp tlv-select { management-address port-description system-capabilities system-description system-name } • lldp transmit • lldp trap
Examples	<ul style="list-style-type: none"> • lldp transmit • lldp tlv-select management-address

loop-protect

Description	Loop protection configuration on port.
Syntax	<ul style="list-style-type: none"> • loop-protect • loop-protect action { [shutdown] [log] } *1 • loop-protect tx-mode
Examples	<ul style="list-style-type: none"> • loop-protect • loop-protect action log shutdown

mac

Description	MAC address table learning configuration.
Syntax	<ul style="list-style-type: none"> • mac address-table learning [secure]
Example	<ul style="list-style-type: none"> • mac address-table learning

media-type

Description	Media type configuration for the current interface.
Syntax	<ul style="list-style-type: none"> media-type { rj45 sfp dual }
Example	<ul style="list-style-type: none"> media-type rj45

mtu

Description	Maximum transmission unit. The size should be between 1518 and 10240.
Syntax	<ul style="list-style-type: none"> mtu <max_length>
Example	<ul style="list-style-type: none"> mtu 1518

no

Description	Set various settings to the default value.
Syntax	<ul style="list-style-type: none"> no aggregation group <v_uint> no debug phy loopback [near far connector mac-serdes-input mac-serdes-facility mac-serdes-equipment media-serdes-input media-serdes-facility media-serdes-equipment] no description no duplex no excessive-restart no fastboot no flowcontrol no frame-length-check no ip igmp snooping filter no ip igmp snooping immediate-leave no ip igmp snooping max-groups no ip igmp snooping mrouter no ip igmp snooping r-filter no lacp no lacp port-priority <v_1_to_65535> no lacp timeout { fast slow } no lldp receive no lldp tlv-select { management-address port-description system-capabilities system-description system-name } no lldp transmit no lldp trap no loop-protect no loop-protect action no loop-protect tx-mode no mac address-table learning [secure] no media-type no mtu no port-security no port-security mac-address { [sticky] [<mac> [vlan <vlan_id>]] }*1 no port-security maximum no port-security maximum-violation no port-security violation no priority-flowcontrol prio [<prio>] no qos class no qos cos no qos dei no qos dpl no qos egress-map no qos ingress-map no qos map cos-tag cos <cos> dpl <dpl> no qos map tag-cos pcp <pcp> dei <dei> no qos pcp no qos policer no qos qce { [addr] [key] }*1 no qos storm { unicast broadcast unknown }

	<ul style="list-style-type: none"> • no qos trust dscp • no qos trust tag • no rmon collection history <id> • no rmon collection stats <id> • no shutdown • no spanning-tree • no spanning-tree auto-edge • no spanning-tree bpdu-guard • no spanning-tree edge • no spanning-tree link-type • no spanning-tree mst <instance> cost • no spanning-tree mst <instance> port-priority • no spanning-tree restricted-role • no spanning-tree restricted-tcn • no speed • no switchport acceptable-frame-type • no switchport allowed vlan • no switchport ingress-filtering • no switchport ingress-force-to-pvid • no switchport native vlan
Examples	<ul style="list-style-type: none"> • no duplex • no qos policer • no port-security maximum-violation

port-security

Description	Enable/disable port security per interface.
Syntax	<ul style="list-style-type: none"> • port-security • port-security mac-address { [sticky] [<mac> [vlan <vlan_id>]] }*1 • port-security maximum <limit> • port-security maximum-violation <violate_limit> • port-security violation { protect restrict shutdown }
Example	<ul style="list-style-type: none"> • port-security maximum 10

priority-flowcontrol

Description	Configure Priority Flow Control (802.1Qbb) on this interface. Priority values should be between 0 and 7.
Syntax	<ul style="list-style-type: none"> • priority-flowcontrol prio <prio>
Example	<ul style="list-style-type: none"> • priority-flowcontrol prio 3

qos

Description	Quality of Service configuration.
Syntax	<ul style="list-style-type: none"> • qos cos <cos> • qos dei <dei> • qos dpl <dpl> • qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei> • qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl> • qos pcp <pcp> • qos policer <rate> [kbps mbps fps kfps] [flowcontrol] • qos qce { [addr { source destination }] [key { double-tag normal ip-addr mac-ip-addr }] }*1 • qos trust dscp • qos trust tag
Examples	<ul style="list-style-type: none"> • qos policer 500 fps flowcontrol

rmon

Description	Configure Remote Monitoring on an interface.
Syntax	<ul style="list-style-type: none"> rmon collection history <id> [buckets <buckets>] [interval <interval>] rmon collection stats <id>
Examples	<ul style="list-style-type: none"> rmon collection history 1 rmon collection stats 4

shutdown

Description	Shutdown of the interface.
Syntax	<ul style="list-style-type: none"> shutdown
Example	<ul style="list-style-type: none"> shutdown

spanning-tree

Description	Spanning Tree protocol configuration on an interface.
Syntax	<ul style="list-style-type: none"> spanning-tree spanning-tree auto-edge spanning-tree bpdu-guard spanning-tree edge spanning-tree link-type { point-to-point shared auto } spanning-tree mst <instance> cost { <cost> auto } spanning-tree mst <instance> port-priority <prio> spanning-tree restricted-role spanning-tree restricted-tcn
Examples	<ul style="list-style-type: none"> spanning-tree edge spanning-tree mst 2 cost 1

speed

Description	Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.
Syntax	<ul style="list-style-type: none"> speed { 10 100 1000 auto { [10] [100] [1000] { [no-hdx] [no-fdx] } } }
Example	<ul style="list-style-type: none"> speed 100

switchport

Description	Set VLAN switching mode characteristics on a port.
Syntax	<ul style="list-style-type: none"> switchport acceptable-frame-type { all tagged untagged } switchport allowed vlan none switchport allowed vlan { all [add remove except] <vlan_list> } [egress { untag tag }] switchport ingress-filtering switchport ingress-force-to-pvid switchport native vlan <pvid>

Interface Mode Commands for VLAN Interfaces

do

Description	Run exec commands in the current mode.
Syntax	<ul style="list-style-type: none"> do <command>
Example	<ul style="list-style-type: none"> do reload cold

end

Description	Go back to EXEC mode.
Syntax	<ul style="list-style-type: none"> end
Example	<ul style="list-style-type: none"> end

exit

Description	Exit from current mode.
Syntax	<ul style="list-style-type: none"> exit
Example	<ul style="list-style-type: none"> exit

help

Description	Show a description of the interactive help system.
Syntax	<ul style="list-style-type: none"> help
Example	<ul style="list-style-type: none"> help

ip

Description	Interface Internet Protocol configuration commands.
Syntax	<ul style="list-style-type: none"> ip address <subnet> ip address { { <address> <netmask> } { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] [client-id { <port_type> <client_id_interface> ascii <ascii_str> hex <hex_str> }] [hostname <hostname>] } } ip igmp snooping ip igmp snooping compatibility { auto v1 v2 v3 } ip igmp snooping last-member-query-interval <ipmc_lmqi> ip igmp snooping priority <cos_priority> ip igmp snooping querier { mode { auto on off } address <v_ipv4_ucast> } ip igmp snooping query-interval <ipmc_qi> ip igmp snooping query-max-response-time <ipmc_qri> ip igmp snooping robustness-variable <ipmc_rv> ip igmp snooping unsolicited-report-interval <ipmc_uri>
Examples	<ul style="list-style-type: none"> ip address 192.0.2.1 255.255.255.0 ip igmp snooping

no

Description	Set various settings to the default value.
Syntax	<ul style="list-style-type: none">• no ip address• no ip igmp snooping• no ip igmp snooping compatibility• no ip igmp snooping last-member-query-interval• no ip igmp snooping priority• no ip igmp snooping querier { mode address }• no ip igmp snooping query-interval• no ip igmp snooping query-max-response-time• no ip igmp snooping robustness-variable• no ip igmp snooping unsolicited-report-interval
Examples	<ul style="list-style-type: none">• no ip address• no ip igmp snooping

Interface Mode Commands for Local Link Aggregation Interfaces

do

Description	Run exec commands in the current mode.
Syntax	<ul style="list-style-type: none">do <command>
Example	<ul style="list-style-type: none">do reload cold

end

Description	Go back to EXEC mode.
Syntax	<ul style="list-style-type: none">end
Example	<ul style="list-style-type: none">end

exit

Description	Exit from current mode.
Syntax	<ul style="list-style-type: none">exit
Example	<ul style="list-style-type: none">exit

help

Description	Show a description of the interactive help system.
Syntax	<ul style="list-style-type: none">help
Example	<ul style="list-style-type: none">help

lACP

Description	Configure LACP interface.
Syntax	<ul style="list-style-type: none">lACP failover { revertive non-revertive }lACP max-bundle <v_uint>
Examples	<ul style="list-style-type: none">lACP failover revertivelACP max-bundle 2

no

Description	Set various settings to the default value.
Syntax	<ul style="list-style-type: none">no lACP failover [revertive non-revertive]no lACP max-bundle [<uint>]

Line Terminal Configuration Mode Commands

do

Description	Run exec commands in the current mode.
Syntax	<ul style="list-style-type: none">do <command>
Example	<ul style="list-style-type: none">do reload cold

editing

Description	Enable command line editing.
Syntax	<ul style="list-style-type: none">editing
Example	<ul style="list-style-type: none">editing

end

Description	Go back to EXEC mode.
Syntax	<ul style="list-style-type: none">end
Example	<ul style="list-style-type: none">end

exec-banner

Description	Enable the display of the EXEC banner.
Syntax	<ul style="list-style-type: none">exec-banner
Example	<ul style="list-style-type: none">exec-banner

exec-timeout

Description	Set the EXEC timeout.
Syntax	<ul style="list-style-type: none">exec-timeout <min> [<sec>]
Example	<ul style="list-style-type: none">exec-timeout 10 45

exit

Description	Exit from current mode.
Syntax	<ul style="list-style-type: none">exit
Example	<ul style="list-style-type: none">exit

help

Description	Show a description of the interactive help system.
Syntax	<ul style="list-style-type: none">help
Example	<ul style="list-style-type: none">help

history

Description	Control the command history function.
Syntax	<ul style="list-style-type: none">history size <history_size>
Example	<ul style="list-style-type: none">history size 32

length

Description	Set number of lines on a screen. The number of lines can be zero (for no pausing) or a number between 3 and 512.
Syntax	<ul style="list-style-type: none"> length <length>
Example	<ul style="list-style-type: none"> length 20

location

Description	Enter terminal location description. The location text should not be more than 32 characters.
Syntax	<ul style="list-style-type: none"> location <location>
Example	<ul style="list-style-type: none"> location mycli

motd-banner

Description	Enable the display of the MOTD banner.
Syntax	<ul style="list-style-type: none"> motd-banner
Example	<ul style="list-style-type: none"> motd-banner

no

Description	Set various settings to the default value.
Syntax	<ul style="list-style-type: none"> no editing no exec-banner no exec-timeout no history size no length no location no motd-banner no privilege level no width
Examples	<ul style="list-style-type: none"> no history size 100 no location

privilege

Description	Change privilege level for line. Levels can range from 0 to 15.
Syntax	<ul style="list-style-type: none"> privilege level <privileged_level>
Example	<ul style="list-style-type: none"> privilege level 15.

width

Description	Set width of the display terminal. Width can be zero (unlimited) or a value between 40 and 512.
Syntax	<ul style="list-style-type: none"> width <width>
Example	<ul style="list-style-type: none"> width 50

Spanning Tree Aggregation Mode Commands

do

Description	Run exec commands in the current mode.
Syntax	<ul style="list-style-type: none"> do <command>
Example	<ul style="list-style-type: none"> do reload cold

end

Description	Go back to EXEC mode.
Syntax	<ul style="list-style-type: none"> end
Example	<ul style="list-style-type: none"> end

exit

Description	Exit from current mode.
Syntax	<ul style="list-style-type: none"> exit
Example	<ul style="list-style-type: none"> exit

help

Description	Show a description of the interactive help system.
Syntax	<ul style="list-style-type: none"> help
Example	<ul style="list-style-type: none"> help

no

Description	Set settings to factory defaults.
Syntax	<ul style="list-style-type: none"> no spanning-tree no spanning-tree auto-edge no spanning-tree bpdu-guard no spanning-tree edge no spanning-tree link-type no spanning-tree mst <instance> cost no spanning-tree mst <instance> port-priority no spanning-tree restricted-role no spanning-tree restricted-tcn
Examples	<ul style="list-style-type: none"> no spanning-tree edge no spanning-tree restricted-role

spanning-tree

Description	Spanning Tree protocol settings.
Syntax	<ul style="list-style-type: none"> spanning-tree spanning-tree auto-edge spanning-tree bpdu-guard spanning-tree edge spanning-tree link-type { point-to-point shared auto } spanning-tree mst <instance> cost { <cost> auto } spanning-tree mst <instance> port-priority <prio> spanning-tree restricted-role spanning-tree restricted-tcn
Examples	<ul style="list-style-type: none"> spanning-tree link-type point-to-point spanning-tree restricted-role

IPMC Profile Configuration Mode Commands

default

Description	Set access list rate limiter to defaults.
Syntax	• default range <entry_name>
Example	• default range TestRange

description

Description	Set additional description about the profile in 64 characters.
Syntax	• description <profile_desc>
Example	• description <profile_desc>

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Description of the interactive help system.
Syntax	• help
Example	• help

no

Description	Set settings to defaults.
Syntax	• no description • no range <entry_name>
Example	• no description • no range TestRange

range

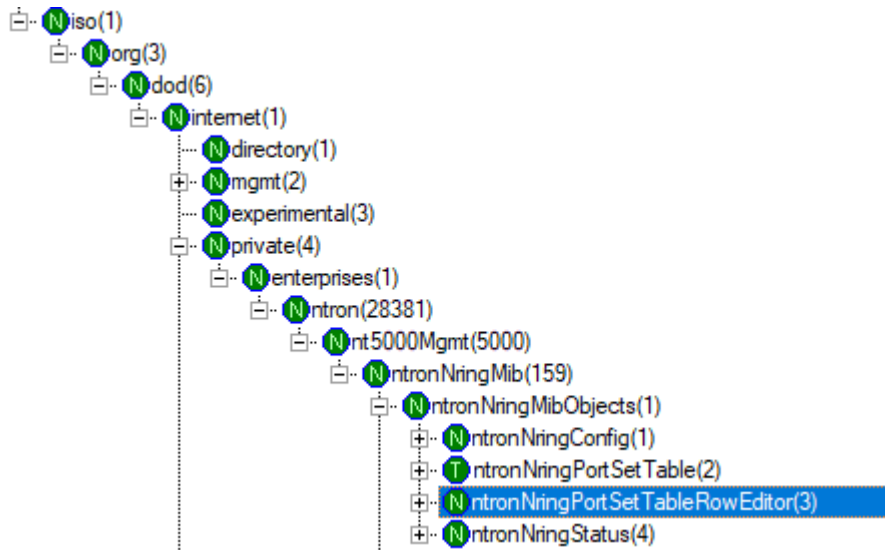
Description	
Syntax	• range <entry_name> { permit deny } [log] [next <next_entry>]
Example	• range TestRange permit log

Appendix B Add/Remove a Table Row Using SNMP

The N-Ring™ Port Set table is used to explain how to add and remove a table row.

Adding a New Table Row

1. Navigate to the entry ntronNringPortSetTableRowEditor and get the subtree.



2. Enter the desired values for the Port Set ID, Ring Port 1, and Ring Port 2 fields. Enter a value greater than 255 for the Action field.

Label	Data Type	Oid	Instance	Value
ntronNringPortSetTableRowEditorPortSetId	Integer	1.3.6.1.4.1.28381.5000.159.1.3.1	0	123
ntronNringPortSetTableRowEditorRingPort1	Gauge	1.3.6.1.4.1.28381.5000.159.1.3.2	0	3
ntronNringPortSetTableRowEditorRingPort2	Gauge	1.3.6.1.4.1.28381.5000.159.1.3.3	0	4
ntronNringPortSetTableRowEditorAction	Gauge	1.3.6.1.4.1.28381.5000.159.1.3.100	0	256

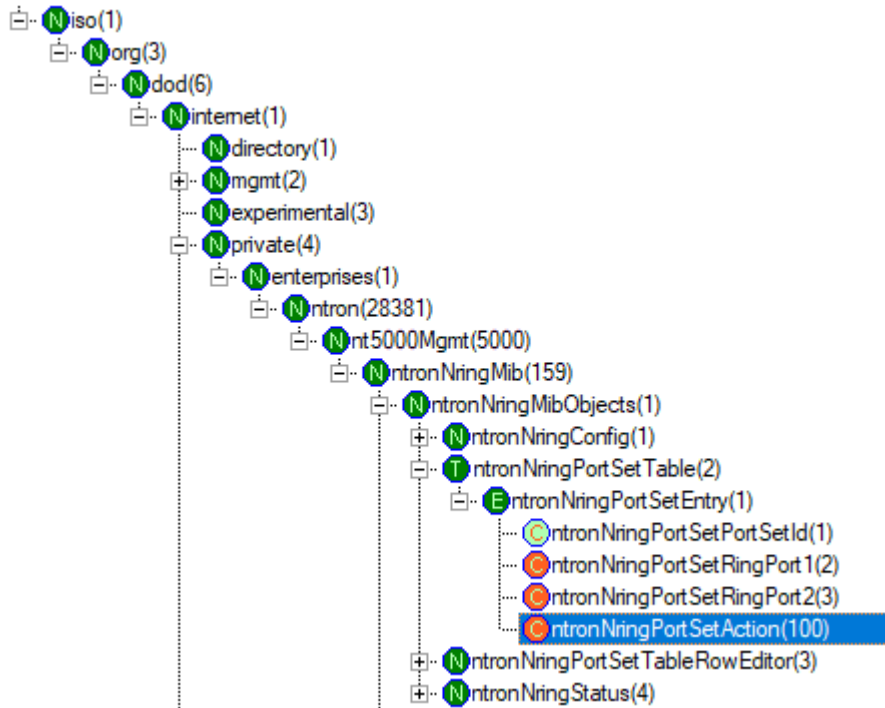
3. Set the values.
4. Enter a value of 2 for the Action field.

Label	Data Type	Oid	Instance	Value
ntronNringPortSetTableRowEditorPortSetId	Integer	1.3.6.1.4.1.28381.5000.159.1.3.1	0	123
ntronNringPortSetTableRowEditorRingPort1	Gauge	1.3.6.1.4.1.28381.5000.159.1.3.2	0	3
ntronNringPortSetTableRowEditorRingPort2	Gauge	1.3.6.1.4.1.28381.5000.159.1.3.3	0	4
ntronNringPortSetTableRowEditorAction	Gauge	1.3.6.1.4.1.28381.5000.159.1.3.100	0	2

5. Set the values.

Removing an Existing Table Row

1. Navigate to the entry ntronNringPortSetAction and get the subtree.



2. Enter/select the desired Instance to remove. Enter a non-zero Value.

Label	Data Type	Oid	Instance	Value
ntronNringPortSetAction	Gauge	1.3.6.1.4.1.28381.5000.159.1.2.1.100	123	1

3. Set the values.

Appendix C Glossary

A

ACE: ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL: ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for different situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACLs can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). By default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" webpage. There are a number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports that obey the same traffic rules. A Traffic Policy is created under the "Access Control List" page. You can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will only apply if the frame gets past the ACE matching without being matched. In that case, a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES: AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS: AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and CU cables are inserted, the port will select the preferred media.

APS: APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation: Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.
(Also Port Aggregation, Link Aggregation).

ARP: ARP is an acronym for Address Resolution Protocol. It is a protocol that is used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet addresses of its neighbors are known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

Auto-Negotiation: Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC: CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM: CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CoS: CoS is an acronym for Class of Service and it is also known as QoS class.

Every incoming frame is classified to a CoS, which is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific CoS.

There is a one to one mapping between CoS, queue and priority.

A CoS of 0 (zero) has the lowest priority.

CoS ID: CoS ID is an acronym for Class of Service ID.

Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame.

D

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES: DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP: DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay: DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client.

The DHCP server can use this information to implement IP address or other assignment policies.

Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option 2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Server: DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

DNS: DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS: DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation: Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DPL: DPL is an acronym for Drop Precedence Level.

Every incoming frame is classified to a DPL, which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DPL. A DPL of 0 (zero) corresponds to 'Committed' (Green) frames and a DPL greater than 0 (zero) corresponds to 'Discard Eligible' (Yellow) frames.

DSCP: DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

ECE: ECE is EVC Control Entry. These rules are ordered in a list to control the preferred classification.

EEE: EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS: EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

ERPS: ERPS is an abbreviation for Ethernet Ring Protection Switching defined in ITU/T G.8032. It provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free.

Ethernet Type: Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

EVC: EVC is an acronym for Ethernet Virtual Connection. MEF standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

F

FTP: FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and allows file writing and reading. It also provides directory service and security features.

Fast Leave: Multicast snooping Fast Leave processing allows the switch to remove the specific member interface, which receives the leave message, from the multicast forwarding-table without sending last member query messages. The specific member interface is also pruned from the multicast tree for the multicast group specified in the original leave message. Fast Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMPv2 and MLDv1, and it is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific interface.

G

GARP: GARP is an acronym for Generic Attribute Registration Protocol. It is a generic protocol for registering attribute with other participants, and it is specified in IEEE 802.1D-2004, clause 12.

GVRP: GVRP is an acronym for GARP VLAN Registration Protocol. It is a protocol for dynamically registering VLANs on ports, and is specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.

H

HQoS: HQoS is an acronym for Hierarchical Quality of Service. It is a method of QoS that can be configured on a service level.

HTTP: HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that is used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS: HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

ICMP: ICMP is an acronym for Internet Control Message Protocol. It is a protocol used for diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X: IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP: IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier: A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IP: IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC: IPMC is an acronym for IP MultiCast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile: IPMC Profile is an acronym for IP MultiCast Profile.

IPMC Profile is used to deploy the access control on IP multicast streams.

IVL: In Independent VLAN Learning, every VLAN uses its own logical source address table as opposed to SVL where two or more VLANs share the same part of the MAC address table.

J

JSON: JSON (JavaScript Object Notation) is a lightweight data-interchange format. As an alternative to XML, it can be used to transmit dynamic data between web server and application. It uses human-readable text and consist with one or more attribute–value pairs.

L

LACP: LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC: The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP: LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station. This includes the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED: LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI: LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC: LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.

M

MAC Table: Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP: MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5: MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm that uses a cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring: For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port (in this context, mirroring a frame is the same as copying the frame).

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MSTP: In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

N

NTP: NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) at the transport layer.

0

OAM: OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionalities like CC and RDI are based on this.

Optional TLVs: A LLDP frame contains multiple TLVs.

Some TLVs are configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.

OUI: OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP: PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PHY: PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING: ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.
ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Policer: A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

PPPoE: PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

POST: POST is an acronym for Post On Self Test.

It is run automatically on various components at power on. The power on self test (POST) is used to test the basic hardware. It includes ready-made tests (e.g. BIST) embedded in hardware or ASICs such as memory tests, server tests, internal loopback test etc.

PSFP: PSFP is an acronym for Per Stream Filtering and Policing.

PSFP functions allow filtering and policing decisions, and subsequent frame queuing decisions on a per-stream basis. PSFP is supported by a table of stream filters that determine the filtering and policing actions that are to be applied to frames received on ingress ports.

PTP: PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE: QCE is an acronym for QoS Control Entry.

A QCE is a combination of keys and actions.

The keys can be configured to match specific parts of a frame and the actions can be configured to override the default classified values of e.g. CoS.

QCL: QCL is an acronym for QoS Control List and is a list of QCEs.

Each and every frame is compared against the QCEs in the list. The comparison starts with the first entry in the list and continues until there is a match between the frame and the key parameters or the end of the list is reached.

If there is a match between the frame and the keys, the frame will be reclassified according to the action parameters.

QL: QL In SyncE - this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS: QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution.

Therefore, QoS is the set of techniques to manage network resources.

QoS Class: See Class of Service (CoS).

Querier Election: Querier election is used to dedicate the Querier, the only router that sends Query messages on a particular link. The Querier election rule defines that the IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

R

RARP: RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS: RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI: RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate a detected defect to the remote peer MEP.

RFC2544: RFC2544 describes a number of tests that may be run to assess the performance characteristics of a network interconnecting devices. In this context, it is specialized towards determining whether a network section conforms to a service level agreement (SLA) and is usually run during service activation.

Router Port: A router port is a port on the Ethernet switch that leads the switch towards the Layer 3 multicast device.

RSA: RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret.

RSTP: In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SHA: SHA is an acronym for Secure Hash Algorithm. It was designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper: A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP: SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP: The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing on networks using IEEE 802.2 LLC for more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values. It also supports vendor-private protocol identifiers.

SNMP: SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP: SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) at the transport layer.

SR: Seamless Redundancy is used to provide the high fault tolerance to link failure with zero failover time. This is done by generating the duplicate streams from the talker (stream source) to listener(s) across statically configured redundant paths, and merging the streams at listener(s).

SSID: Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH: SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM: SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP: Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SVL: Shared VLAN Learning allows for frames initially classified to a particular VLAN (based on Port VLAN ID or VLAN tag information) to be bridged on a shared VLAN. In SVL two or more VLANs are grouped to share common source address information in the MAC table. The common entry in the MAC table is identified by a Filter ID (FID). SVL is useful for configuration of more complex, asymmetrical cross-VLAN traffic patterns, like E-TREE (Rooted-Multipoint) and Multi-netted Server. The alternative VLAN learning mode is IVL. The default VLAN learning mode is IVL and not all switches support SVL.

Switch ID: Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE: SyncE is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACAS+: TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol, which provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

TAS: TAS is an acronym for Time Aware Shaper. 802.1Qbv: This amendment specifies time-aware queue-draining procedures, managed objects and extensions to existing protocols that enable bridges and end stations to schedule the transmission of frames based on timing derived from IEEE Std 802.1AS.

Tag Priority: Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP: TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.
The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET: TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP: TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS: ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0-63).

TLV: TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP: TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

TT-LOOP: TT-LOOP is an acronym for Traffic Test Loop, a firmware module that provides methods to perform tests that are defined in RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) and Y.1564 (remote end).

U

UDLD: UDLD is an acronym for Uni Directional Link Detection. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one-way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

UDP: UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP).

Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP does not provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority: User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN: Virtual LAN. A method to restrict communication between switch ports. At layer 2, the network is partitioned into multiple, distinct, mutually isolated broadcast domains.

VLAN ID: VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

W

WEP: WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi: WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA: WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK: WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

WPA-Radius: WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

WPS: WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED: WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DPL is used as input to WRED. A higher DPL assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR: WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

Appendix D License Agreements

Open Source Software

The Software provided with the NT5000 may contain programming, scripts, tools, modules, libraries, components, or other items that were developed using "open source" code (the "Open Source Software"). Open Source Software is provided to you under one or more open source license agreements that contain important information concerning ownership, terms of use, and rights, and restrictions for the applicable element of the Open Source Software. By obtaining, accessing, downloading and/or using Software or the Open Source Software, you agree that you have read, and understood, and will comply with, the terms and conditions of the applicable Open Source Licenses in addition to all other the terms applicable to Software under this Agreement.

SOFTWARE	VERSION	LICENSE
bind	9.11.19	Mozilla Public License v2.0
busybox	1.31.1	GPL v2
dhcp	4.4.1	Mozilla Public License v2.0
dropbear	2019.78	dropbear
ethtool	5.10	GPL v2
gnupg	1.4.23	GPL v3
hiawatha	10.10	GPL v2
iptables	1.8.3	GPL v2
json-c	0.13.1	json-c
libcurl	7.68.0	libcurl
libevent	2.1.11	libevent
libfcgi	2.4.2	fcgi2
libnet	1.1.6	libnet
libopenssl	1.1.1g	OpenSSL/SSLLeay
libssh2	1.9.0	libssh2
libupnp	1.6.25	pupnp
libzlib	1.2.11	zlib
linux	5.4.45	GPL v2
mbedtls	2.16.6	Apache 2.0
mtd	2.1.4	GPL v2
netsnmp	5.9.3	net-snmp
net-tools	479bb4a7e11a4084e2935c0a576388f92469225b	GPL v2
ntp	4.2.8p14	ntp
pciutils	3.5.5	GPL v2
phytool	2	GPL v2
redboot	mssc-redboot-668849a	GPL v2
strace	5.4	strace
xz-embedded	20130513	xz_embedded

