NT328G Industrial Ethernet Managed Switch Series

Software Guide | November 2019

LP1105 | Revision B

COPYRIGHT

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.

Red Lion Controls, Inc.
20 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

Disclaimer

Portions of this document are intended solely as an outline of methodologies to be followed during the maintenance and operation of the NT328G Industrial Ethernet Managed Switch. 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.

Purpose

This user manual provides specific information on how to apply and use the functions on NT328G Industrial Ethernet Managed Switch as implemented in the current version of software. These commands are used to set-up and execute applications on the device.

Audience

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

Compliance Statements & User Information

FCC Compliance Statement

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

Operation is subject to the following conditions:

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

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

Déclaration de conformité FCC

Ce produit est conforme à la partie 15 des règles de la FCC –A

Utilisation est soumise aux conditions suivantes:

1. Ce dispositif ne doit pas causer des interférences nuisibles
2. Cet appareil doit accepter toute interférence reçue, y compris les interférences qui peuvent causer un mauvais fonctionnement.

Note: Cet équipement a été testé et jugé conforme aux limites de la classe A des appareils numériques , conformément à la partie 15 des règles de la FCC . Ces limites sont conçues pour fournir

une protection raisonnable contre les interférences nuisibles dans une installation résidentielle . Cet équipement génère, utilise et peut émettre de l'énergie radiofréquence et, si il n'est pas installé et utilize conformément aux instructions, peut causer des interférences nuisibles aux communications radio. L'utilisation de cet appareil dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur sera tenu de corriger les interférences à ses propres frais .

User Compliance Information

If this equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

"How to Identify and Resolve Radio-TV Interference Problems".

This booklet is available from: U.S. Government Printing Office, Washington DC, 20402 Stock No. 004-000- 00345-4

Canadian Compliance Statement

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

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matérial brouilleur du Canada.

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.

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. As needed, Documentation Notes and/or Product Bulletins will be provided 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.

Related Documents

Visit the Technical Resources page on the Red Lion website at the following link to view available documents related to this product 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 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	admin
SNMP v1/v2	read community	public
SNMP v1/v2	write community	private
SNMP v1/v2	trap community	public

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

PROTOCOLS
SNMP
LLDP
DHCP Client
RSTP

Managing Local and Remote Access Using 802.1X

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

Default Passwords

User Passwords

The NT328G ships from the factory with a default ***admin*** user account. Red Lion strongly recommends creating a new user with administrative privileges before the unit is deployed.

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

SNMP v1/v2 Community Names

The NT328G ships with default Community Names for SNMP v1/v2 operation. SNMP v1/v2 traffic per the standard is neither hashed nor encrypted. Therefore, it is Red Lion's recommendation that customers requiring SNMP use SNMP V3, which offers more secure SNMP communication.

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

See the Disabling Unused Protocols 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
- DHCP Client
- RSTP

Chapter 2 Introduction

NT328G Series Key Features

The Red Lion® NT328G, Layer 3 rackmount industrial Ethernet switch, offers 28 high speed ports (24 Gigabit, 4 10 Gigabit) to meet the performance requirements of bandwidth intensive applications. Designed to meet current and future needs with reliable wire-speed switching performance and a flexible mix of copper and fiber ports, the NT328G's robust feature set includes network redundancy, advanced security, policy-based traffic control and easy-to-use configuration and management. Housed in a rugged IP30 metal enclosure, the switch is designed for long-life use in harsh industrial environments, including wide operating temperature conditions and hazardous locations.

Internet Group Management Protocol (IGMP), media/port auto-detection and simple ring configuration makes the NT328G platform one of the industry's easiest managed switches to deploy.

The NT328G switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows for the configuration of the available features. The default configuration can be used for most of the features provided by this switch. However, there are many options that should be configured to maximize the switch's performance for particular network environments.

The NT328G switch delivers high Quality of Service (QoS) and advanced VLAN features. It is ideal for harsh environments and mission critical applications.

FEATURE	DESCRIPTION
Alarms and Events	Supports Alarms and Events, Event Logging, and Syslog
Authentication and General Security	Switch management - console port, Telnet, SSH, HTTP, HTTPS, or SNMP, IPv6 User authentication – IEEE 802.1X RADIUS server, or a local switch database Port Authentication – PAE with IEEE 802.1X RADIUS authentication SNMPv2 – Community strings SNMPv3 – MD5 or SHA passwords DHCP Snooping IP Source Guard Port Isolation (Private VLANs) Capacity up to: • 10 login sessions • 19 VLAN IP interfaces
Access Control Lists	ACL matches: MAC address, IP address, TCP/UDP port, and ToS/DSCP values ACL actions: deny, permit, queue mapping, ToS marking, and mirroring Supports MAC and IP address filtering Capacity up to: • 10 profiles with 16 entries per profile • 96 MAC rules • 96 Ipv6 rules
Bridging and Forwarding	IEEE 802.1D/802.1Q transparent bridging IPv4 and IPv6 Dynamic data switching MAC addresses learning Store-and-forward wire-speed switching while eliminating bad frames Frame buffering. Address table capacity up to: • 16K MAC addresses • 1024 static MAC addresses
Configuration Backup and Restore	Saves the switch configuration to a management station or an FTP/TFTP server

FEATURE	DESCRIPTION
DHCP	DHCP Client with support for Option 61 DHCP Relay Agent with support for Option 82 DHCP Server with support for Option 61 and Option 82 DHCP Snooping. Capacity up to: • 5 DHCP Server IP pools
L2 Redundancy Protocols	Spanning Tree Protocols – STP, RSTP, and MSTP Ring Protocol - Ring and Chain (RingV2) with fast fault recovery
L3 IP Routing and Router Redundancy	Open Shortest Path First (OSPFv2/v3) Routing Information Protocol (RIP) Static routes Virtual Router Redundancy Protocol (VRRP) – for router backup Capacity up to: • 32 static routes • 512 dynamic routes • 8 VRRP groups
Link Aggregation (Port Trunking)	Supports static or dynamic port grouping (LACP). Capacity up to: • 14 LAG groups (effective) • 8 ports per group
Link Layer Discovery Protocol	LLDP is used to discover basic information about a device and neighboring devices
Multicast Filtering and Routing	IGMP - Internet Group Membership Protocol · IGMPv2 (IETF RFC 2236) · IGMPv3 (IETF RFC 3376 and 4604) IGMP snooping, querier, and proxy IGMP MVR - Multicast VLAN Registration Capacity up to: • 64 snooping VLAN interfaces • 512 learned multicast groups • 128 static multicast groups • 15 MVR VLAN profiles • 32 entries per MVR VLAN profile
Port Configuration	Configurable speed, duplex mode, and flow control Can disable ports
Port Mirroring	Can mirror frames from multiple source ports to one analysis port. Can copy frames as an ACL action Capacity up to: • 26 mirror and copy sessions
Quality of Service and Traffic Control	CoS (IEEE 802.1Q) and Differentiated Services (DiffServ/DSCP) Default port priority ACL - queue mapping and CoS marking Policer - CoS, DSCP, coloring, and marking Shaper – rate limiting Storm Control – rate limit for broadcast, unknown unicast, unknown multicast Queue and Scheduler - CoS/Queue Mapping, and per-port queue schedulers
Virtual Local Area Networks (VLANs)	IEEE 802.1Q VLAN IDs from 1 to 4094 Protocol-based VLANs VLAN Translation (VLAN Mapping) VLAN Stacking (QinQ tunneling) Private VLANs (Port Isolation) GARP VLAN Registration Protocol (GVRP) Capacity up to: • 19 VLAN IP interfaces • 2048 static port VLANs • 10 VLAN translation rules • 10 protocol VLAN rules

Description of Software 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. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration, 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 multicast filtering and routing provides support for real-time network applications.

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

Access Control Lists

ACLs provide filtering of L2 frames and L3 packets (based on the MAC address and EtherType, or the IP address and protocol, TCP/UDP port number or ToS/DSCP value). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by preventing access from certain devices or restricting access to specific network resources or protocols.

Alarms and Events

Event Logging

The switch can be configured to log system events as they occur. Event Logging for critical events is enabled by default. Events include:

- System startup and shutdown
- Logins and logouts from the web or console
- Port links going up and down
- System temperature exceeding configurable thresholds

A log of the most recent events is visible via the web interface.

Alarm Profile

The Alarm Profile enables the user to define which systems events will trigger an alarm. Events that are set to “Mask” will not trigger an alarms. Alarms engage the Alarm Relay on the rear of the switch and will display an alert on the web interface.

Syslog

The Syslog protocol, as specified in RFC-3164 and RFC-5424, is supported. Syslog allows sending system events to a remote logging device, known as a Syslog Collector. The Syslog protocol is disabled by default.

Authentication and General Security

There are various mechanisms to authenticate and secure access to the switch or the network. Besides the mechanisms described below, there is also support for SNMP Version 3 and DHCP snooping. Additionally, IP and MAC address filtering and protocol access control can be configured through the Access Control Lists.

IEEE 802.1X Port Access Entity (PAE)

Port-based authentication is supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication (RADIUS) server to verify the client’s right to access the network.

IEEE 802.1X User Authentication

This switch authenticates management access from the console port, Telnet, Secured Shell (SSH), Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS). Authorized user names and passwords can be stored locally (on the switch) or can be verified via a remote authentication (RADIUS) server.

By default, 802.1X User Authentication is not enabled and user credentials are stored on the switch.

IP Source Guard

Access to ports can be controlled using IP Source Guard which restricts traffic sources to specific IP/MAC address pairs that are either stored in the DHCP Snooping table or in an IP Source Guard static table. More complex IP and MAC filtering is available through the Access Control Lists.

Secure Management

The switch supports secure access by Secured Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS), which encrypt their network traffic. The older Telnet Server and Hypertext Transfer Protocol (HTTP) may be enabled to provide backwards compatibility with less secure clients.

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

Bridging and Forwarding

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

Address Table (FDB or ARL)

An 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 forwarding information base.

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 Backup and Restore

You can export the current switch configuration to a file on a management station or send it to an FTP/TFTP server. The file can be imported to the switch at a later time to restore the configuration.

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, with Option 61

- DHCP relay agent, with Option 82
- DHCP server, with Option 61 and Option 82
- And supports DHCP Snooping

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.

DHCP Relay Agent

A DHCP Relay Agent brokers DHCP traffic between a DHCP client and DHCP server.

It is not always practical to have a DHCP server on every subnet of a network. A relay agent enables a client on one network interface or VLAN to communicate with a server on a different interface or VLAN. This enables the use of one centralized DHCP server across multiple networks.

DHCP Option 82 allows a relay agent to have a unique Relay Agent ID and to have unique Relay Agent Circuit IDs for each port of the switch. This information is passed on to the DHCP server when a DHCP client is requesting an IP from the server. A DHCP server can assign a unique IP address based on the identity of the relay agent and the identity of the relay agent port that the client communicates through. As a consequence a device on a specific relay agent port can receive a specific IP address and, if the device is replaced, the replacement receives the same IP address as the original device.

DHCP Server

A DHCP Server allows DHCP Client devices to automatically obtain an IP assignment from the server. IP assignments can be set up as a pool of IP addresses available to any client device; or specific IP addresses based on the clients Client ID (Option 61), or Relay Agent ID and Relay Agent Circuit ID (Option 82).

DHCP Snooping

DHCP snooping is a security enhancement that prevents malicious DHCP attacks. It tracks how trusted DHCP servers assign IP addresses to clients and uses this information to block DHCP traffic from untrusted DHCP servers as well as other malicious DHCP traffic.

L2 Redundancy Protocols

This switch can be connected to other devices using a Spanning Tree Protocol or a Ring & Chain (Ring V2) protocol.

Spanning Tree Protocols

STP establishes a simply 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.

Ring & Chain (RingV2)

Ring & Chain provides for very quick fail-over (in micro-seconds) to a redundant network path when a link in the current network path goes down. The topology of the network must be either a ring or a chain. The setup for Ring & Chain is described in detail in the chapter “Ring Version 2”.

L3 IP Routing

The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch allows the easy linking of network segments or VLANs together while avoiding the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with static routing, Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, and Virtual Router Redundancy Protocol (VRRP).

- **Static Routing** - Traffic is automatically routed between any IP interfaces configured on the NT328G switch. Routing to statically configured hosts or subnet addresses is provided based on next-hop entries specified in the static routing table.
- **RIP** - This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector or hop count, which serves as a rough estimate of transmission cost.
- **OSPF** - This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. OSPFv2 is provided for routing IPv4 traffic, and OSPFv3 for routing IPv6 traffic.
- **VRRP** – VRRP allows multiple routers (typically gateways) to share a virtual network identity. When the master router drops off the network, a backup router will assume the virtual identity and traffic will redirect to the backup router.

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.

LLDP

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

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 Access Control Lists

This switch supports access control lists for IGMP. It can be configured per-port to:

- Permit or deny all multicast traffic
- Permit or deny traffic for specific multicast groups
- Limit the number of multicast groups (channels)

IGMP Snooping

When IGMP Snooping 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, and Proxy

IGMP MVR

Multicast VLAN Registration (MVR) allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN. Meanwhile, the multicast clients can remain in their own standard or private VLAN groups. This helps to isolate the multicast traffic as it transits the network, improving security and making better use of network bandwidth by combining the multicast data traffic from different VLANs into one VLAN stream.

IGMP Static Groups

A static IGMP group is used to route specific multicast traffic to a specific port. One use of this feature is to ensure that a client will receive multicast data, even if it does not support the IGMP protocol.

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

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.

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 later 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.

Quality of Service (QoS) and Traffic Control

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 Voice over IP, high resolution images, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. 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 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 Priority** – The priority of all incoming traffic on a port can be set to a default value.

Access Control Lists

Access Control Lists can search the content of frames and packets and perform particular actions on the matching traffic. These actions including denying, permitting, mapping traffic into a priority queue, applying a CoS marking, or mirroring the traffic.

Policer / Rate Limiting

The Policer can manage excessive rates of ingress traffic. It can drop traffic or prioritize traffic. It supports CoS, DSCP, and three-color marking.

Shaper

The Shaper can control egress traffic rates for a port and egress traffic rates for each priority queue.

Queue and Scheduler

For outgoing traffic, the switch uses eight priority queues that are serviced either by Strict Priority, Weighted Round Robin (WRR), or a combination of strict and weighted queuing. The Queue & Scheduler can also force traffic with particular CoS values to particular priority queues.

Storm Control

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

SNMP

SNMP (Simple Network Management Protocol) is a protocol used to monitor and manage the switch.

SNMP Traps

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

VLANs

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), traffic entering the switch can be untagged, and traffic leaving the switch is untagged. This allows the switch to operate as a 'normal' switch when it is used in a network.

Ports can be assigned to VLANs either manually (using Static VLANs) or dynamically using GVRP (GARP VLAN Registration Protocol).

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 network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.

- Use 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 will inherit the tag of the PVID value for that port. 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.

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 the 'VLAN Configuration Examples' in this document, and/or our website's technical documents.

IEEE 802.1Q Tunneling (QinQ, VLAN Stacking)

This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

System Defaults

The switch's default configuration can be restored using the web interface or CLI. Under the web menu item Configuration Management > Save & Restore, select "Clear active DB including inband" to reset the configuration. The CLI command "runningcfg clear all" 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 Local Console Timeout Flow Control	115200 bps 8 1 None 0 (disabled) None

FUNCTION	PARAMETER	DEFAULT
IP Settings	Management VLAN IP Address DHCPv4	Any VLAN configured with an IP address DHCP assigned Client: Enabled Fallback IP Address: 192.168.1.201 Netmask: 255.255.255.0 Option 61 client ID: MAC Address
Switch Authentication	Default user name Default password	Username “admin” Password “admin”
Security Protocols	802.1X User Authentication 802.1X Port Authentication MAC Authentication HTTPS SSH Port Security IP Filtering DHCP Snooping	Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled
Web Management	HTTP Server HTTP Port Number HTTP Secure Server HTTP Secure Server Port	Disabled 80 Enabled 443
SNMP	SNMP Agent Community Strings SNMPv2 SNMPv3	Enabled “public” (read only); “private” (read/write) Communities: public (get); private (get/set) Users, Groups, Views: none
Port Configuration	Admin Status Auto-Negotation Flow Control	Enabled Enabled Disabled
Link Aggregation (Port Trunking)	Static Trunks LACP (all ports)	None Disabled
Congestion Control	Rate Limiting Storm Control	Disabled Broadcast: Enabled
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status Edge Ports	Enabled, RSTP (Defaults: RSTP standard) Disabled
LLDP	Status	Enabled
Virtual LANs	Default VLAN PVID Acceptable Frame Type Ingress Filtering Switchport Mode GVRP (global) GVRP (port interface) QinQ Tunneling	1 1 All Disabled Hybrid: tagged/untagged frames Disabled Disabled Disabled
Traffic Prioritization	Ingress Port Default Priority Queue Mode Weighted Round Robin	0 WRR Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
Unicast Routing	RIP OSPFv2 OSPFv3	Disabled Disabled Disabled
Router Redundancy	VRRP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2) Multicast VLAN Registration IGMP (Layer 3) IGMP Proxy (Layer 3)	Snooping: Disabled Querier: Disabled Disabled Disabled Disabled

FUNCTION	PARAMETER	DEFAULT
System Log	Status	Disabled
SNTP	Clock Synchronization	Disabled

Chapter 3 Web Software Configuration

This chapter describes using the Red Lion Controls NT328G 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. After three failed login attempts, the switch will lock and refuse further attempts.

After logging in, the system monitors the interface for periods of inactivity. If the interface is inactive for too long, you are automatically logged off.

All of the switches have the same default user name (admin) and password (admin). The password should be changed as soon as possible, as the default password is available to anyone who reads this manual. Best practice is to change the default password immediately after the initial login. The user name can also be changed or additional user names can be added. Use the “account add” command to enter a new user name, password, and/or authorization level. The switch can handle one local login session and at least four remote/OS sessions simultaneously.

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. The DHCP Client is enabled by default with 192.168.1.201 as the fallback address.

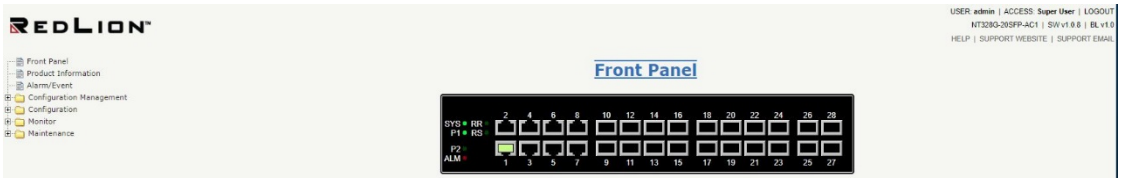
Login

The following login screen will appear:

Operation	Fill in the Username and Password boxes. Click the “Log On” button.
Field	**Description**
User name	Login user name. The maximum length is 32 characters. Default password: admin
Password	Login username. The maximum length is 32 characters. Default password: admin

- For the Username, enter: admin (all lowercase)
- For the Password, enter: admin (all lowercase)

Upon successfully logging in a screen similar to the one below will appear.



For security purposes, it is recommended that the password be changed according to your internal policies. Login credentials can be changed on the **Maintenance/User Administration** page.

Authorization Levels

LEVEL	DESCRIPTION
Superuser	Superusers can access all management features.
Engineer	Engineers can access all management features except user account management.
Guest (default)	Read-only mode (guests can only change their own password).

Navigation

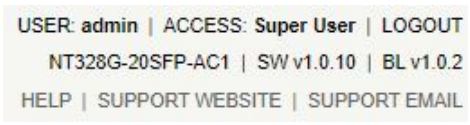
All main screens of the web interface can be reached by clicking on hyperlinks in the four main folders in the menu tree on the left side of the system home screen:

- System Home Screen - View the device Front Panel, Product Information, and Alarms and Events.
- Configuration Management - Restart the system, Save and Restore, and Configure HTTP Import and Export.
- Configuration - Configure the system, interfaces and filters.
- Monitor - Display statistics, status and contents of memory.
- Maintenance - Display system information, download firmware, back up configurations and modify users.

You can find more detailed information in the Navigation drop-down menu.

Home Screen Information and Links

System, user and support information is available in the upper-right corner on the home screen.



USER: displays the current user ID

ACCESS: displays the current user access level

LOGOUT: is an active link to logout function

NT328G-xxx: displays the device name

SW vx.x: displays the active software version

BL vx.x: displays the boot loader version

HELP: is an active link that displays a help page for the screen currently displayed

SUPPORT WEBSITE: is an active link to the Red Lion website NT328G support page(s)

SUPPORT EMAIL: is an active link that opens an email to the Red Lion support organization

Using the Online Help

Each screen has a Help page containing information relevant to the current screen. When the help page is displayed, click on the function in the menu tree to exit a help page.

Each page of Configuration/Status/System functions has a corresponding help page.

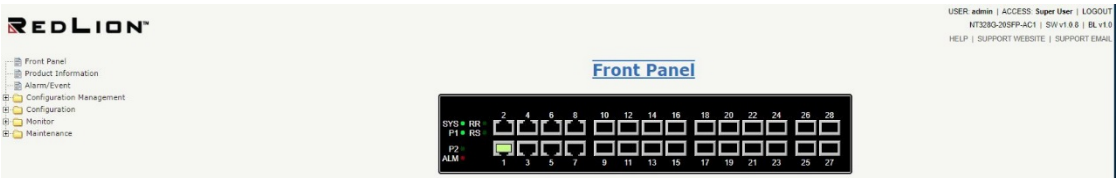
Ending a Session

A user must click on 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.

Organization

The tree view is a menu of the web interface. It offers users quick navigation to the desired page for viewing data or changing configuration parameters.

After logging onto a NT328G switch, the home page with a device Front Panel will be displayed. On the left hand side of the screen is a list of configurable settings supported by the NT328G switch. Below is a list of these settings with a description of their purpose.



Front Panel: Graphic of the switch front panel displaying device and port status information. Port status is displayed when moving the cursor to a port icon

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

Alarm/Event: Alarm/Event Log is used for viewing Current Alarms, Alarm History and the internal event logs.

Configuration Management: Configuration Management is used to Restart the switch, Save and Restore a configuration, and configure HTTP Import/Export.

Configuration: The Configuration page is used to set or change switch configuration parameters.

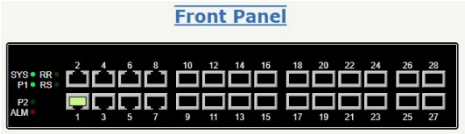
Monitor: Monitor is used to query system data to view and monitor switch operating statistics.

Maintenance: Maintenance is used to upgrade switch operating software, select options, view the syslog and administrate user accounts.

Help: The Help function is used to display information on configuring and monitoring the manageable parameters of the device. Help can be displayed for each software function by selecting a menu tree item and then clicking on "HELP" in the upper right corner of the window.

Front Panel

This page displays the real status of the system's panel.



Product Information

This page shows basic information about the switch and can also be accessed by selecting the ***Product Information*** menu item on the left hand menu.

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

For example, the product name will show NT328G-xxSFP-AC1 if there is one AC power unit in either location and NT328G-xxSFP-AC2 if there are two AC power units.

Switch Model: The base model of the switch.

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

Software Version: The current firmware software version.

Build Date: The build date of the firmware.

Boot Loader: The boot loader version.

Copyright: The software copyright date and owner.

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

Alarm/Event

Use the Alarm/Event function to view and or clear alarms and events from the Alarm table and Events Log.

Alarm Current

Use the Alarm Current tab to refresh the Alarm Current table.

Operation	Refresh: • Click the "Refresh" button to refresh any data.
Field	**Description**
SeqNo	Alarm Sequential Number.
ID	Alarm Type ID.
Description	Alarm Type Description.

Level	LED color is always red for both major and minor alarms.
State	Alarm State. Value is Set/Cleared.
Time	Show the Time when the Alarm occurred.

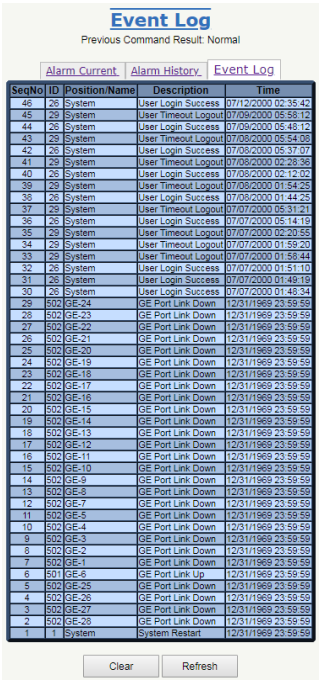
Alarm History

Use the Alarm History tab to clear or refresh the Alarm History table.

Operation	Refresh: • Click the “Refresh” button to refresh any data. Clear: • Click the “Clear” button to clear any data
Field	**Description**
SeqNo	Alarm Sequential Number.
ID	Alarm Type ID.
Description	Alarm Type Description.
Level	LED color is always red for both major and minor alarms.
State	Alarm State. Value is Set/Cleared.
Time	Show the Time when the Alarm occurred.

Event Log

Use the Event Log tab to clear or refresh the Event Log.

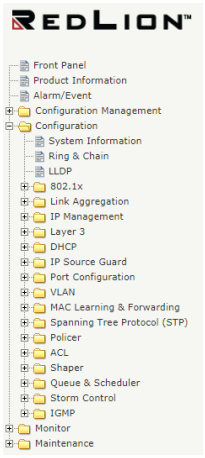


Operation	Refresh: • Click the “Refresh” button to refresh any data. Clear: • Click the “Clear” button to clear any data
Field	**Description**
SeqNo	Alarm Sequential Number.

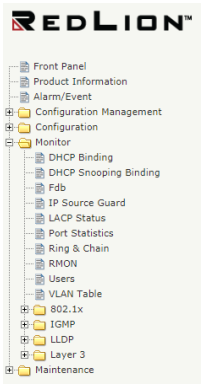
ID	Alarm Type ID.
Description	Alarm Type Description.
Level	LED color is always red for both major and minor alarms.
State	Alarm State. Value is Set/Cleared.
Time	Show the Time when the Alarm occurred.

Configuration Management Menu

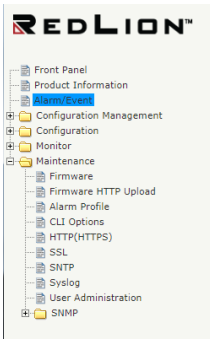
Configuration Menu



Monitor Menu



Maintenance Menu



Chapter 4 Configuration

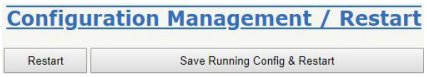
This chapter lists the configuration related functions available for Red Lion Controls NT328G Switch models.

Configuration Management

Note: If you upload a configuration file to the device without IPv4 or IPv6 information on VLAN 1, the device will keep the currently configured IPv4 and IPv6 settings for VLAN 1. This only occurs on VLAN 1 and is a special case so that a user does not lose IP connectivity via the management VLAN.

Restart

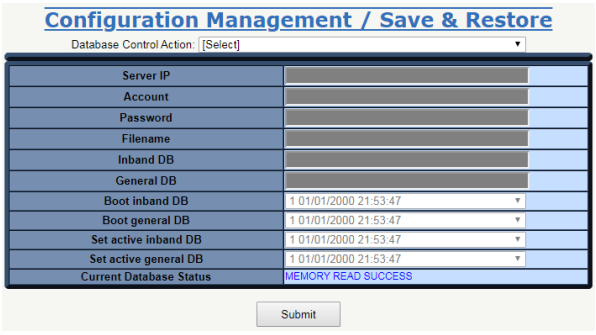
Use this screen to restart the system.
This is a software reset function that does not power down the system.



Operation	Restart: • Click the “Restart” button to restart the system without saving the current running configuration. Save Running Config & Restart: • Click the “Save Running Config & Restart” button to save and restart.

Save & Restore

Save the running configuration and restart the system.

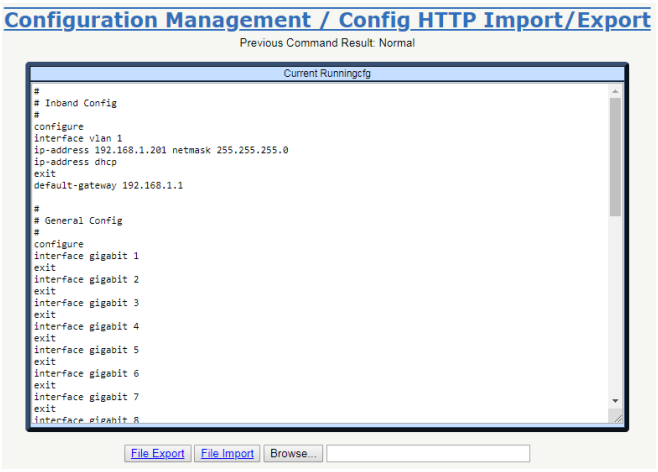


Operation	Save & Restore: • Click the “Database Control Action” drop-down list to select the database (DB) control action to execute when restarting the system. • Enter data into the required fields. Required fields are the fields that are not grayed-out (required fields differ depending on the selected “Database Control Action”). • Click “Submit” to execute the action.
Field/List	**Description**

Fields	Server IP Account Password Filename Inband DB General DB Boot inband DB Boot general DB Set active inband Set active general DB Current Database Status
Database Control Action Drop-down List	The drop-down list contains the following options: • Save inband configuration and runtime configuration as the active restoration database for next power-on restoration. • Restore inband configuration and control plane configuration by setting another restoration database active. • Restore inband configuration and control plane configuration by setting another restoration database active and system restart. • Clear inband configuration and control plane configuration in the active restoration database. • Clear inband configuration and control plane configuration in the active restoration database and system restart. (Warning: runtime config. is also cleared and inband config. is lost)
Database Control Action Drop-down List (Continued)	• Clear control plane configuration in the active restoration database. • Clear control plane configuration in the active restoration database and restore. (Runtime config. is also changed.) • Export runtime configuration in cli command format to FTP server. • Export runtime configuration in binary format to FTP server. • Import database in cli command format from FTP server and set it to the active restoration database. • Import database in cli command format from FTP server and set it to the active restoration database and system restart. • Import database in binary format from FTP server and set it to the active restoration database. • Import database in binary format from FTP server and set it to the active restoration database and system restore. • Save running config to flash replacing the specified backup. • Export runtime configuration in cli command to TFTP server. • Export runtime configuration in binary DB to TFTP server. • Import database in cli command format from TFTP server and set it to the active restoration database. • Import database in cli command format from TFTP server and set it to the active restoration database and system restart. • Import database in binary DB format from TFTP server and set it to the active restoration database. • Import database in binary DB format from TFTP server and set it to the active restoration database and system restart.

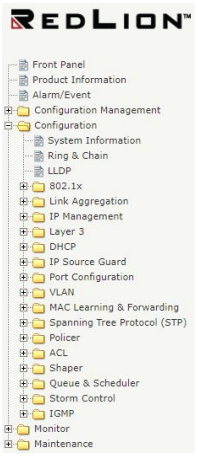
Config HTTP Import/Export

Import or export an HTTP configuration file.

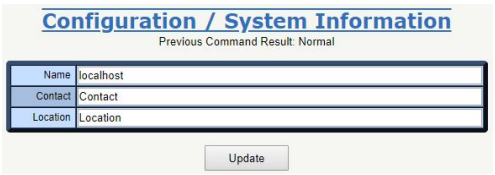


Operation	File Export: • Click the “File Export” button to begin the file export operation. • Click the drop-down list next to “Save” in the pop-up at the bottom of the screen to choose the next action. • Click “Save” to execute the action. File Import: • Click on “Browse” or the empty field to navigate to and select the file to import. • Click the “File Import” button to begin the file import operation.

Configuration

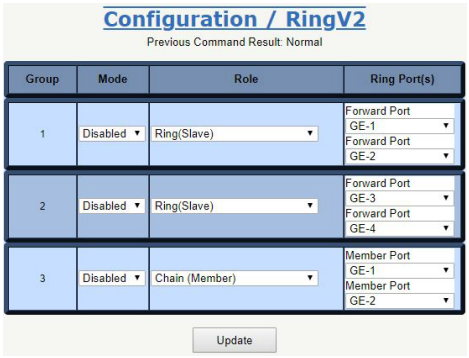


System Information



Ring & Chain

Modify RingV2.

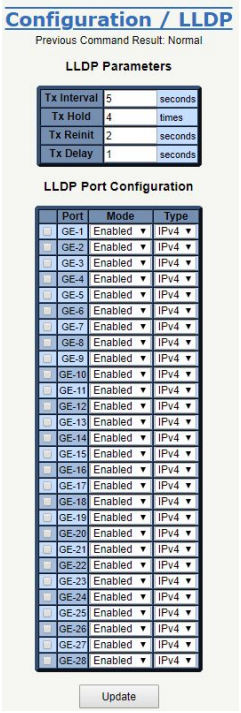


Operation	Modify: • Select from the configuration parameters in the “Mode”, “Role”, and "Ring Port(s)" fields for the “Group”. • Click the "Update" button to apply any changes.
Field	**Description**
Group	The group index; this parameter is used for easy identification of the ring when users configure it. Group 1 - this group supports configuration of the ring. Group 2 - this group supports configuration of the ring, coupling and dual-homing. Group 3 - this group supports configuration of the chain and balancing-chain.
Mode	Enable the Ring in a specific group. When Group 1 or 2 is enabled: • All configurations of Group 3 will be reset to the default settings. • All Group 3 configuration options will be locked. To configure Group 3: • Both Group 1 and Group 2 should be disabled first. • When Group 3 is enabled, all configurations of Group 1 and Group 2 will reset to their default settings. • All Group 1 and Group 2 configuration options will be locked.
Role	Configure the Ring group on this switch to a specific role. Group 1 - supports the options of ring-master and ring-slave. • Ring - can be master or slave. Group 2 - supports configuration of the ring, coupling and dual-homing. • Ring - can be master or slave. • Coupling - can be primary or backup. • Dual-Homing – can be primary or backup. Group 3 - supports the configuration of the chain and balancing-chain. • Chain - can be head, tail or member. • Balancing Chain - can be central-block, terminal-1/2 or member. **Note 1** - Group 1 must be enabled before enabling Group 2 for coupling. **Note 2** - When Group 1 or Group 2 is enabled, configuration for Group 3 will be disabled. **Note 3** - When Group 3 is enabled, configuration for Group 1 and Group 2 will be disabled.

Ring Port(s)	Selecting ring port(s). Each ring port must be unique, i.e. they CANNOT be configured in 2 or more different groups; 2 ring ports between a ring/chain CANNOT be the same. When the port's role is ring-master: ● One ring port is made a forward port and another is made a block port. ● The block port is redundant; it is a blocking port under normal conditions. When the port's role is ring-slave: ● Both ring ports are forward ports. When the switch's role is coupling-primary: ● Only one primary ring port is needed. When the role is coupling-backup: ● Only one backup port is needed. ● This backup port is redundant; it is a blocking port in a normal state. When the role is dual-homing: ● One ring port is the primary port and the other is the backup port. ● This backup port is a redundant port; it is a blocking port in a normal state. When the role is chain-head: ● One ring port is the member port and another is a head port. ● Both ring ports are forwarding ports in a normal state. When role is chain-tail: ● One ring port is the member port and another is a tail port. ● The tail port is a redundant port. It is a blocking port in a normal state. When the role is chain-member: ● Both ring ports are member ports. ● Both ring ports are forwarding ports in a normal state. When the role is balancing-chain/central-block: ● One ring port is the member port and another is a block port. ● The block port is a redundant port. It is a blocking port in a normal state. When the role is balancing-chain/terminal-1/2: ● One ring port is the member port and another is a terminal port. ● Both ring ports are forwarding ports in a normal state. When the role is balancing-chain/member: ● Both ring ports are member ports. ● Both ring ports are forwarding ports in a normal state.

LLDP

Modify LLDP parameters and the LLDP port configuration.



Operation	Modify LLDP Parameters: • Select from the configuration parameters in the LLDP Parameters fields. • Click the "Update" button to apply any changes. Modify LLDP Port Configuration: • Select the port to configure by clicking on the port check box. • Select from the configuration parameters in the LLDP Parameters fields. • Click the "Update" button to apply any changes.
Field	**Description**
Tx Hold	The time-to-live value expressed as a multiple of the TxInterval object. Range: 2–10 times, Default value = 4 times.
Tx Interval	The interval at which LLDP frames are transmitted on behalf of this LLDP agent. Range: 5–32768 seconds, Default value = 5 seconds.
Tx Reinit	Indicates the delay (in units of seconds) from when PortConfigAdminStatus object of a particular port becomes 'disabled' until re-initialization will be attempted. Range: 1–10 seconds, Default value = 2 seconds.
Tx Delay	Indicates the delay (in units of seconds) between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Range: 1–8192 seconds, Default value = 1 second.
Field	**Description**
Port	LLDP Port: Port-1–28.
Mode	Enable/Disable LLDP mode. Default value is Enabled.
Type	LLDP Tx type for management address tlv. Default type is IPv4.

802.1X

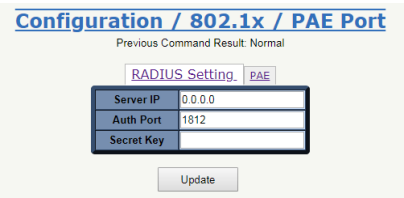
PAE Port

Set System AuthControl and modify PAE Port Authentication.

Operation	Modify System Auth. Control: • Select System Auth. Control. • Click the “Update” button to apply any changes. Modify PAE Port Authentication: • Update fields below. • Check which port(s) are to be changed. • Click the “Update” button to modify PAE Port Authentication options.
Field	**Description**
System AuthControl	Enable/Disable system 802.1X authentication function. Default value: Disabled.
Port	PAE port: 1–28.
Auth Control	The authentication type of PAE port. Allow Force_Unauthorized/Force_Authorized/Auto. Default is Force_Authorized.
ReAuth Enabled	Enable/Disable re-authenticate of PAE port. Default: Disable.
ReAuth Period	The period of authentication of PAE port. Range: 1–3600 seconds. Default: 3600 seconds.
Quiet Period	The quiet period of PAE port. Range: 1–255 seconds. Default: 60 seconds.
Tx Period	The timeout of Authenticator waiting for EAP-Response/ Identity from supplication of PAE port. Range: 1–255 seconds. Default: 30 seconds.
Supp. Timeout	The timeout of Authenticator wait for EAP-Response (exclude EAP-Request/Identify) after sending EAP-Request. Range: 1–255 seconds. Default: 30 seconds.
Server Timeout	The timeout time of Authenticator wait Access-Challenge/ Access-Accept/Access-Reject after sending Access-Request. Range: 1–255 seconds. Default: 30 seconds.
Max Request	The max times of backend Authenticator send EAP-Request to supplicant before restarting the authentication process. Range: 1–10. Default: 2.

RADIUS Setting

Modify the PAE port RADIUS Setting.



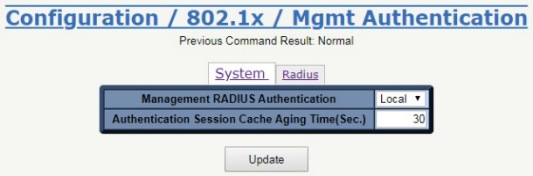
Operation	Modify: • Modify the Server IP, Authentication Port and Secret Key fields. • Click the “Update” button to apply any changes.
Field	**Description**
Server IP	The IP address of the RADIUS server. Allow IPv4 address. 0.0.0.0 indicates that RADIUS is disabled. Default is 0.0.0.0.

Auth Port	The UDP port of the RADIUS server for authentication. Range: 1–65535. Default: 1812
Secret Key	The key is for use between the RADIUS server and Authenticator. Range: 0–16 characters. Default: empty string.

Mgmt Authentication

Update the System setting.

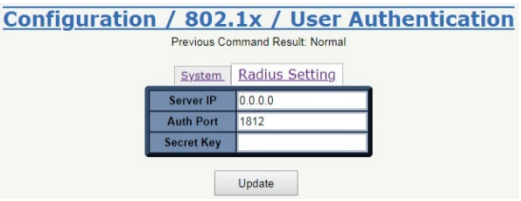
Note: Mgmt Authentication and User Authentication are both located under the "User Authentication" tab in the menu tree.



Operation	Modify: • Modify the Management RADIUS Authentication and Authentication Session Cache Aging Time(Sec.) fields. • Click the "Update" button.
Field	**Description**
Management RADIUS Authentication	The management authentication method used by the device. Values: Local and Both. Default: Local.
Authentication Session Cache Aging Time	Range: 10–600 seconds. Default: 30 seconds.

User Authentication

Modify the User Authentication Radius setting.

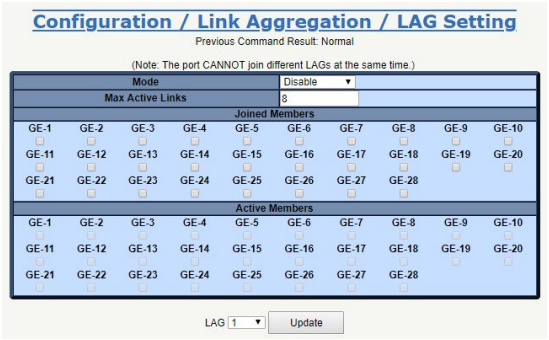


Operation	Modify: • Modify the Server IP, Auth Port, and Secret Key fields. • Click the "Update" button to update User Authentication.
Field	**Description**
Server IP	The IP address of the RADIUS server. Allow IPv4 address. 0.0.0.0 indicates that RADIUS is disabled. Default is 0.0.0.0.
Auth Port	The UDP port of the RADIUS server for authentication. Range: 1–65535. Default: 1812
Secrety Key	The key is for use between the RADIUS server and Authenticator. Range: 0–16 characters. Default: empty string.

Link Aggregation

LAG Setting

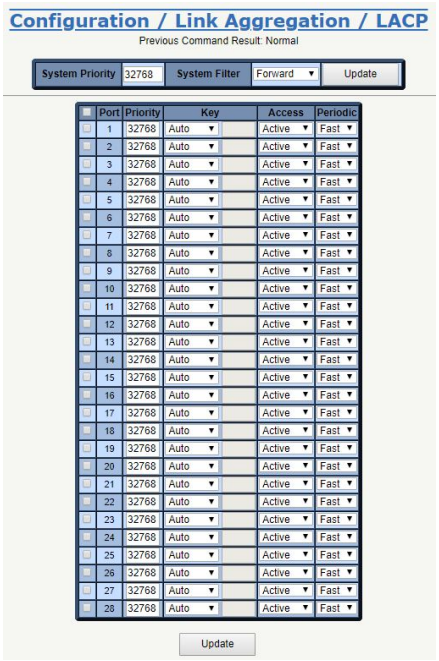
Configure Link Aggregation Groups.



Operation	Modify: • Click the checkbox for the port you wish to update. • Change the Mode, Max Active Links, and LAG. • Click the “Update” button.
Field	**Description**
LAG	There are 28 LAGs in the system. Users can choose the index of LAG to configure it and to get current information from the LAG.
Mode	There are multiple link aggregation modes supported: Disable: No link aggregation process on this LAG. Static: Process static link aggregation on this LAG. LACP: Process LACP for link aggregation on this LAG.
Max Active Links	The maximum links which LAG can bundle at the same time. Range: 1–8. Default: 8.
Joint Members	The ports which join the LAG are configured by the operator. User can select any available port as member of this LAG. When the port is selected for the LAG, it cannot join any other LAG.
Active Members	The ports which are aggregated into the LAG.

LACP

Set the LACP configuration.

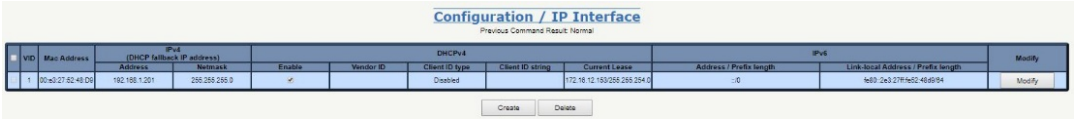


Operation	To modify system LACP configuration: • Modify global configuration. • Click the “Update” button to apply new configuration. To modify LACP port configuration: • Modify the configuration of multi-selected LACP ports. • Click the “Update” button to apply a new configuration.
Field	**Description**
System Priority	LACP system priority. Range: 1–65535. Default: 65535.
System Filter	LACP system filter mode. There are four modes: • Disable: Bypass incoming LACP PDUs. • Forward: Accept LACP PDUs on LACP Port and bypass it on the non-LACP port (default). • Soft-Drop: Accept LACP PDUs on LACP Port and discard it on the non-LACP port. • Hard-Drop: Always drop incoming LACP PDUs.
Port	Interface Port Index.
Priority	The Priority of LACP port. Range: 1–65535. Default: 65535.
Key	The Key of LACP port. It supports "Auto" and "Specific" mode. When "auto" is the mode setting, the key will be auto-generated according to link speed of the physical port. When "specific" is the mode setting, users can configure the key value in the range of 1 to 65535.
Access	Access mode of the LACP port. It supports "Active" and "Passive" mode. When "Active" is the mode setting, this LACP port always generates LACP packet to negotiate with a partner. When "Passive" is the mode setting, this LACP port will do nothing until it receives LACP packet to negotiate with a partner.
Periodic	Periodic mode of the LACP port. It supports "fast" and "slow" mode. When "fast" is the mode setting, the number of seconds between periodic transmissions uses Short Timeouts. When "slow" is the mode setting, the number of seconds between periodic transmissions uses Long Timeouts. These two timeout values are specified in "IEEE-Std 802.1AX™-2008", as follows: • The "Short Timeouts" are 1 second. • The "Long Timeouts" are 30 seconds.

IP Management

IP Interface

Create, modify or delete an IP Interface.

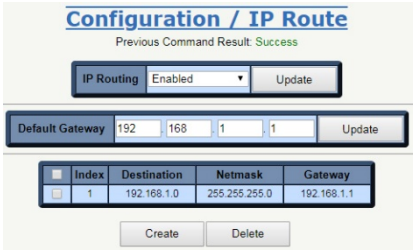


Operation	<u>To Create an IP Interface:</u> • Click the “Create” button. • When the “Configuration / IP Interface – Create” dialog box appears, fill VID and specify the values of the following fields. • Click the “Apply” button to create the new IP Interface. <u>To Modify an IP Interface:</u> • Check the box beside the IP Interface you wish to modify and then click the “Modify” button. • Change the necessary fields. • Click the “Apply” button. <u>To Delete an IP Interface:</u> • Mutli-select IP interfaces for deletion. • Click the “Delete” button to delete the IP interface(s).
Field	**Description**
VID	The identity for an IP Interface. Range: 1–4094. 1st IP interface always exists for VLAN 1 (This is a support setting and cannot be deleted).
IPv4 Address	IP address for the IP interface. Range: 0–255. Default value: 0.0.0.0.
Netmask	Network subnet mask for the IP interface. Range: 0–255. Default value: 0.0.0.0.
IPv6 Address/Prefix Length	IPv6 unicast addresses are aggregatable with prefixes of arbitrary bit-length, similar to IPv4 addresses under Classless Inter-Domain Routing. Here only Global Unicast address is considered and other types of unicast addresses (ex: site-local unicast, Link-Local unicast ...etc) are not. The general format for IPv6 Global Unicast addresses is as follows: | n bits | m bits | 128-n-m bits | +----------+----------+----------+ | global routing prefix | subnet ID | interface ID | +----------+----------+----------+ where the global routing prefix is a (typically hierarchically- structured) value assigned to a site (a cluster of subnets/links), the subnet ID is an identifier of a link within the site, and the interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros, but it can appear only once. It can also represent a valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired. The prefix length is accepted in the range of 1 to 128.

IPv6 Link-Local Address/ Prefix Length	IPv6 Link-Local addresses are for use on a single link. Link-Local addresses have the following format: | 10 | | bits | 54 bits | 64 bits | +--------------+----------------------------------+----------------------------------+ |1111111010| 0 | interface ID | +--------------+----------------------------------+----------------------------------+ Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery or when no routers are present. Automatically generate a link-local address in format of EUI-64 when the address is not specified. The prefix length is accepted in the range of 64 to 128.
MAC Address	MAC address is generated internally while the VLAN interface is created. A user cannot modify the value of this field.

IP Route

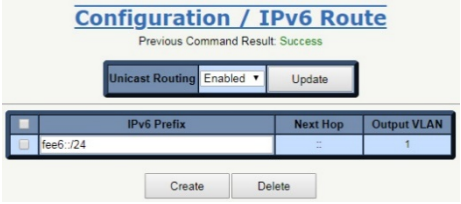
Set IP routing ability and routes.



Operation	<u>To create a new static route:</u> • Click the “Create” button to go to the Configuration / IP Route – Create screen. • Fill in the Destination, Netmask and Gateway. • Click the “Apply” button to create one static route. <u>To set IP routing:</u> • Set IP Routing to “Enabled” or “Disabled”. • Click the “Update” button to enable or disable IP routing on the device. <u>To modify the default gateway:</u> • Click the “Update” button to apply the new gateway. <u>To delete a static route:</u> • Select the static route entry/entries to be deleted. • Click the “Delete” button to delete the entry/entries selected.
Field	**Description**
IP Routing	Layer 3 IP routing/forwarding. Allow Disabled/Enabled. Default value is Disabled.
Default Gateway	Input the default gateway IP address for management and Layer 3 VLAN interface routing.
Destination	Destination network address of the static route.
Netmask	Network subnet mask for the static route.
Gateway	Next hop IP address for the destination network.

IPv6 Route

Configure IPv6 unicast-routing.

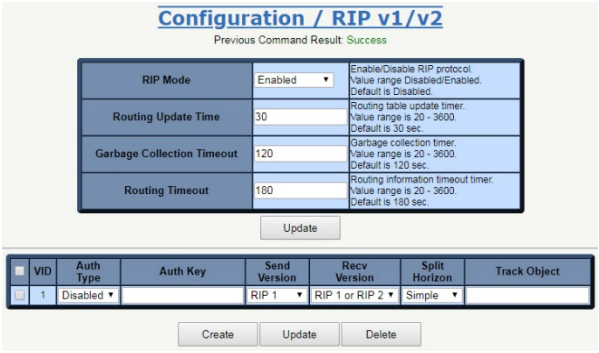


Operation	To create a new static IPv6 route: • Click the "Create" button. • When the "Configuration / IPv6 Route – Create" screen appears, fill in the IPv6 Prefix Address / Length, Next Hop, and Output VLAN fields. • Click the "Apply" button to create an IPv6 route. To modify IPv6 Unicast Routing: • Set Unicast Routing to "Enabled" or "Disabled". • Click the "Update" button to apply a new configuration. To delete the static IPv6 route(s): • Select the route(s) for deleting. • Click the "Delete" button to delete selected route(s).
Field	**Description**
Unicast Routing	Enable/Disable Unicast Routing.
IPv6 Prefix Address/Length	Destination prefix address and length of the route.
Next Hop	Next hop of the route.
Output VLAN	Direct output VLAN of the route on the device.

Layer 3

RIPv1/v2

Modify Layer 3 RIP data.

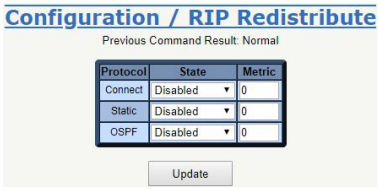


Operation	Create RIP interface VLAN settings: • Click the "Create" button. • When the "Configuration / RIP v1/v2 – Create" screen appears, fill in the fields shown. • Click the "Apply" button to create an RIP interface. Modify RIP settings: • Select RIP Mode, Routing Update Time, Garbage Collection Timeout and Routing Timeout. • Click the "Update" button to apply any changes. Modify RIP interface VLAN settings: • Modify RIP Mode, Auth Type, Auth Key, Send Version, Recv Version and Split Horizon. • Click the "Update" button to apply any changes.

Field	Description
RIP Mode	RIP protocol mode. Allow Disabled/Enabled. Default value: Disabled.
Routing Update Time	Routing table update timer. Range: 20–3600. Default value: 30 seconds.
Garbage Collection Timeout	Garbage collection timer. Range: 20–3600. Default value: 120 seconds.
Routing Timeout	Routing information timeout timer. Range: 20–3600. Default value: 180 seconds.
VID	The identity for the RIP interface VLAN. Range: 1–4094. 1st RIP interface VLAN always exists for VLAN 1. (Can't be deleted)
RIP Mode	RIP Mode is used to enable RIP on an VLAN interface. Range Disabled/Enabled. Default value: Disabled.
Auth Type	Auth Type is the type of Authentication used on this interface. Range Disabled/Enabled. Default value: Disabled.
Auth Key	Authentication Key. The max length is 16 characters. The default value is empty string which is all nulls.
Send Version	Version of RIP packet sent from this interface. Range NoSend/RIP 1/RIP 2/RIP 1 and RIP 2. Default value: RIP 1.
Recv Version	Version of RIP packet which will be received by this interface. Range NoRecv/RIP 1/RIP 2/RIP 1 or RIP 2. Default value: RIP 1 or RIP 2.
Split Horizon	SplitHorizon is used to control split horizon routing update behavior. Range Disabled/Simple/Poison. Default value: Simple.
Track Object	Track Object binding list. RIP can bind a maximum of 64 track objects. Value Range: 1–64. Default value: 0. Before binding the specific track object, the track object must exist. If the track object does not exist, binding is denied. Configuration example: • Add Track Object: 1,2,3. • To remove Track Object 2: change the Track Object 2 to Track Object 1, or Track Object 3. • To remove all Track Objects: clear the Track Object box.

RIP Redistribute

Modify RIP Redistribute data.

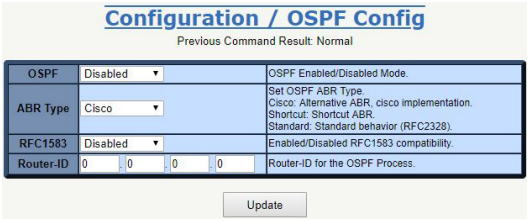


Operation	Modify: • Modify State and Metric. • Click the “Update” button to apply any changes.

Field	Description
Protocol	RIP Redistribute System supports Connect, Static, OSPF Three entry Protocol.
State	Disabled/Enabled Protocol.
Metric	Range: 0–16. Default value: 0.

OSPF Config

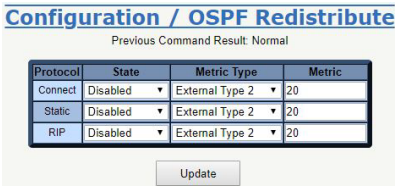
Modify OSPF Config data.



Operation	Modify: • Modify OSPF, ABR Type, RFC 1583 and Router-ID. • Click the “Update” button to apply any changes.
Field	**Description**
OSPF	Value range: Disabled/Enabled. Default: Disabled.
ABR Type	Set OSPF ABR Type. Cisco: Alternative ABR, Cisco implementation. Shortcut: Shortcut ABR. Standard: Standard behavior (RFC2328).
RFC 1583	Enabled/Disabled RFC1583 compatibility. Value range: Disabled/Enabled. Default: Disabled.
Route-ID	Router-ID for the OSPF Process.

OSPF Redistribute

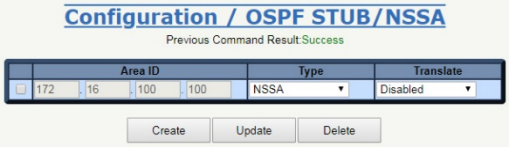
Modify OSPF Redistribute data.



Operation	Modify: • Modify State, Metric Type and Metric. • Click the “Update” button to apply any changes.
Field	**Description**
Protocol	OSPF Redistribute System supports Connect, Static, RIP Three entry Protocols.
State	Disabled / Enabled Protocol.
Metric Type	Select: External Type1 or External Type2. Default: External Type2.
Metric	Range: 1–16777214. Default value: 20.

OSPF STUB/NSSA

Modify OSPF STUB/NSSA data.



Operation	Create: • Click the “Create” button. • When the “Configuration / OSPF STUB/NSSA – Create” screen appears, fill in the Area ID, Type, and Translate fields. • Click the “Apply” button to create a new Area ID. Modify: • Modify Area ID, Type, and Translate. • Click the “Update” button to apply any changes. Delete: • To delete, select the check box of any items to be deleted. • Click the “Delete” button to Delete OSPF STUB/NSSA.
Field	**Description**
Area ID	IP Address Format Range 0.0.0.1–255.255.255.255.
Type	STUB (No support Translate Function) STUB NO SUMMARY (No support Translate Function) NSSA NSSA NO SUMMARY
Translate	Range: Disabled/Enabled. Default: Disabled.

OSPF Virtual-Link

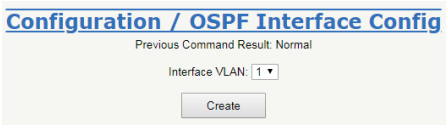
Modify OSPF Virtual-Link data.

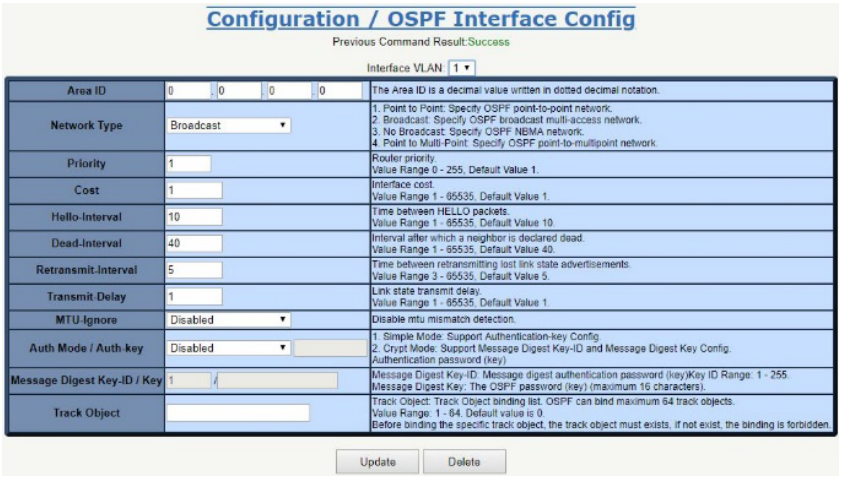
Operation	Create: • Click the “Create” button. • When the “Configuration / OSPF Virtual-Link – Create” screen appears, fill in the Area ID and Neighbor ID fields. • Click the “Apply” button to create OSPF Virtual-Link. Delete: • To delete, select the check box of any items to be deleted. • Click the “Delete” button to delete OSPF Virtual-Link.
Field	**Description**
Area ID	IP Address Format Range 0.0.0.1–255.255.255.255.
Neighbor ID	IP Address Format Range 0.0.0.0–255.255.255.255.

OSPF Interface Config

Modify OSPF Interface Config data.

Create:





Operation	Modify: • To modify settings. • Click the “Update” button to modify OSPF Interface Config data. Delete: • Click the “Delete” button to delete OSPF Interface Config data.
Field	**Description**
Area ID	OSPF Area ID as a Decimal Value.
Network Type	Point to Point: Specify OSPF point-to-point network. Broadcast: Specify OSPF broadcast multi-access network. No Broadcast: Specify OSPF NBMA network. Point to Multi-Point: Specify OSPF point-to-multipoint network.
Priority	Router priority. Value Range: 0–255. Default Value: 1.
Cost	Interface cost. Value Range: 1–65535. Default Value: 10.
Hello-Interval	Time between HELLO packets. Value Range: 1–65535. Default Value: 10.
Dead-Interval	Interval after which a neighbor is declared dead. Value Range: 1–65535. Default Value: 40.
Retransmit-Interval	Time between retransmitting lost link state advertisements. Value Range: 3-65535. Default Value: 5.
Transmit-Delay	Link state transmit delay. Value Range: 1–65535. Default Value: 1.
MTU-Ignore	Disable MTU mismatch detection.
Auth Mode/Auth-key	Simple Mode: Support Authentication-key Config. Crypt Mode: Support Message Digest Key-ID and Message Digest Key Config. Authentication password (key)
Message Digest Key-ID/Key	Message Digest Key-ID: Message digest authentication password (key) Key ID Range: 1–255. Message Digest Key: The OSPF password (key) (maximum 16 characters).

Track Object	Track Object: Track Object binding list. OSPF can bind maximum 64 track objects. Value Range: 1–64. Default value: 1. Before binding the specific object for tracking, the object must exist. If the object does not exist, binding is impossible. Tracking object configuration example: • Adding Tracking Objects: Type “1,2,3” in the Track Object box to add Track Objects 1, 2 and 3. • To remove Track Object 2: change the Track Object box to read “1,3”. • To delete all Track Objects: clear the Track Object box.

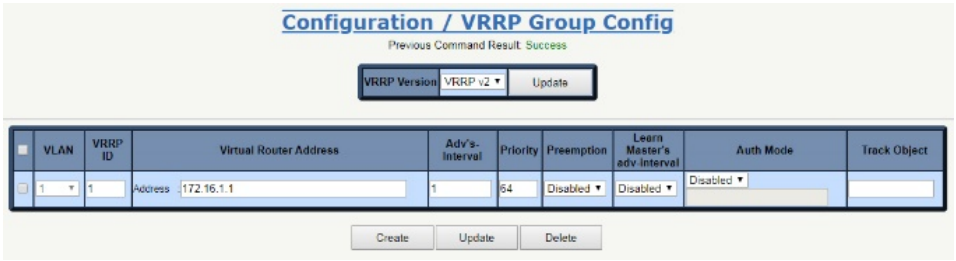
OSPF Neighbor Config

Create, modify or delete OSPF Neighbor Config.

Operation	Create: • Click the “Create” button. • When the “Configuration / OSPF Neighbor Configure – Create” screen appears, fill in the Address, Poll-Interval and Priority. • Click the “Apply” button to create OSPF Neighbor Config. Modify: • To modify the settings, select any check boxes of settings to be modified. • Click the “Update” button to modify OSPF Neighbor Config data. Delete: • Select any check boxes of settings to be deleted. • Click the “Delete” button to delete OSPF Neighbor Config data.
Field	**Description**
Address	IP Address Format Range: 0.0.0.1–255.255.255.255.
Poll-Interval	Value Range: 1–65535 second. Default Value: 60.
Priority	Value Range: 1–255. Default Value: 0.

VRRP Group Config

Configure VRRP.

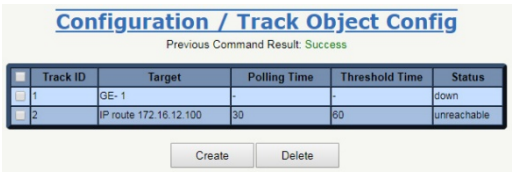


Operation	Create: • Click the “Create” button. • When the “Configuration / VRRP Group Config – Create” screen appears, fill in the fields with relevant data. • Click the “Apply” button to create VRRP Group Config data. Modify: • Update the settings. • Select the row to be modified. • Click the “Update” button to Modify VRRP Group Config data. Delete: • Select the row(s) to be deleted. • Click the “Delete” button to Delete VRRP Group Config data.

Field	Description
VLAN Interface	The identity for the VLAN Interface. Range: 1–4094.
VRRP ID	VRRP group index identity.
Virtual Router Address	Virtual router IP should be in same subnet with VLAN interface. Different VRRP group should not have same virtual router IP.
Advertise-Interval (0.1 sec)	Value Range: 1–2550. Default Value: 10. Value 10 stands for 1 second. (0.1s * 10 = 1s)
Priority	Value Range: 1–254. Default Value: 100.
Preemption	Range: Disabled/Enabled. Default: Enabled.
Learn Master's adv-interval	Range: Disabled/Enabled. Default: Disabled.
Auth Mode	Range: Disabled/Enabled Default: Disabled. Enabled Support VRRP Group Auth Data.
Track Object	Track Object: Track Object binding list. VRRP can bind maximum 64 track objects. Value Range: 1-64. Default value: 1. Before binding the specific object for tracking, the object must have been created. If the object does not exist, binding is impossible. Tracking object configuration example: • Adding Tracking Objects: Type "1,2,3" in the Track Object box to add Track Objects 1, 2 and 3. • To remove Track Object 2: change the Track Object box to read "1,3". • To delete all Track Objects: clear the Track Object box.

Track Object Config

Modify Track Object Config data.



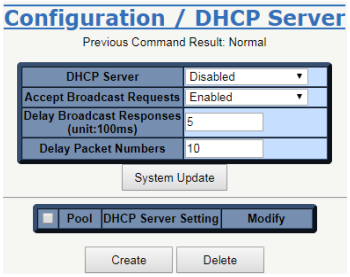
Operation	Create: • Click the "Create" button. • When the "Configuration / Track Object Config – Create" screen appears, fill in the Track ID, Type, Target, Polling Time (sec) and Threshold Time (sec) fields. • Click the "Apply" button to create a Track Object. Delete: • Click the check box to select the Track Object to be deleted. • Click the "Delete" button to delete the selected Track Object. **Note:** When RIP/OSPF/VRRP is binding the track object, the object cannot be deleted.
Field	**Description**
Track ID	Track Object index identity Value Range: 1–64.
Type	Type of Track Object. Currently 3 types are supported. The supported types are VLAN, Port and Route.
Target	When type is VLAN, it indicates "VLAN interface". Value Range: 1–4094 When type is Port, it indicates "Port". Value Range: 1–28 When type is Route, it indicates "IP address". Value Range: 0–255 When type is VRRP, it indicates "---". Value Range: 1–255
Polling Time (sec)	Only available when type is Route. Value Range: 1–600, Unit: second.

Threshold Time (sec)	Only available when type is Route. Value Range: 1–3000. Unit: second.
Status	Show the current status of Track Object.

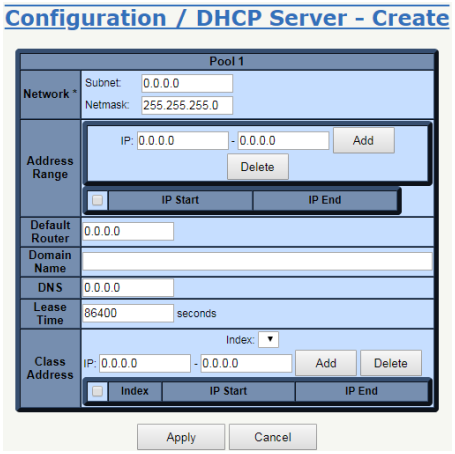
DHCP

DHCP Server

Modify the DHCP server.



Create:



Operation	Create: • Click the “Create” button. • When the “Configuration / DHCP Server – Create” screen appears, fill in the fields shown. • Click the “Apply” button to create a DHCP server. Modify (inside pool 1-19 of DHCP Server) • Click the “Modify” button to enter “DHCP server – Modify” page. • Input the data for the DHCP Server Pool. • Click “Apply” to apply any changes or click “Cancel” to disregard changes and return to the main page of the DHCP server. Delete: • Click the "Delete" button to deleted the selected Pool.
Field	**Description**
Network	Network subnet and netmask. Should match IP address subnet of specific VLAN interface.
Address Range	Indicates the available range of addresses for DHCP client. Both the Start-IP and End-IP must be in the same subnet of the network setting and the Start-IP must be smaller than the End-IP. Max. DHCP Pool size is 1024 per system. This maximum threshold draws from all DHCP pools combined.
Default Router	Default-router in this network.
Domain Name	Domain name of this network. Max. length: 64 characters.

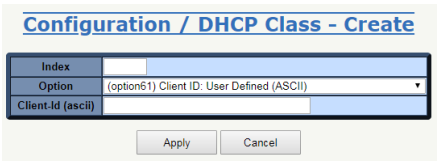
DNS	DNS server of this network.
Lease Time	Define the lease time for IP Address lease. (Range: 1–31536000 seconds, default 86400)

DHCP Class

Modify DHCP Class data.

Note: When configuring the Identifier String to match an NT24K® client ID, if the NT24k's client ID was set using the "Other Hex" format on the NT24K, then on the NT328G you must prefix the Client ID with '00'. For example, if the NT24k's Client ID is set to "fabfab" using the "Other Hex" format, then on the NT328G's DHCP Class page select "(option 61) Client ID: User Defined (Hex)" and enter "00fabfab".

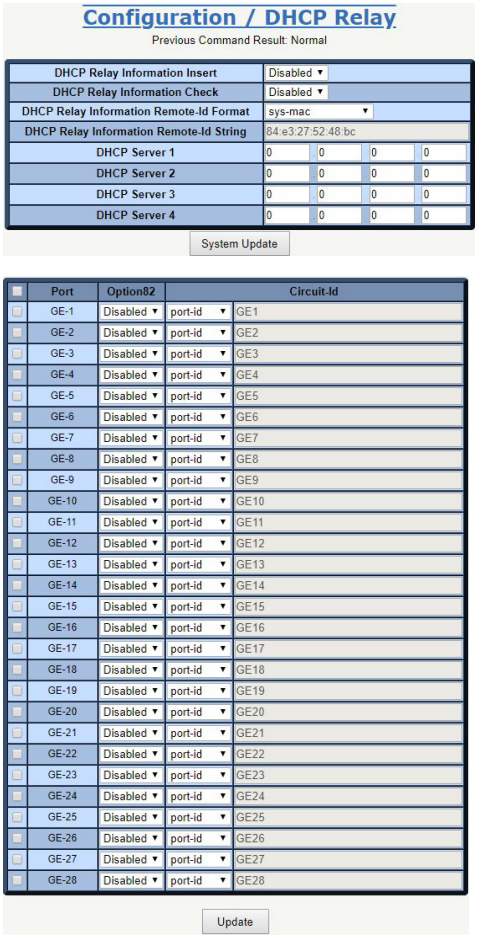
Create:



Operation	Create: • Click the “Create” button. • Enter the Index, Identifier String, and select the Option. • Click “Apply” to apply the parameters and create the class.
Field	**Description**
Index	Unique Index identifier. Max. length 3 characters
Identifier String	Unique Index identifier string. Max. length 32 characters.
Option	Eleven DHCP Class options. • (option61) Client ID: User Defined (ASCII) • (option61) Client ID: User Defined (Hex) • (option61) Client ID: User Defined (MAC) • (option82) Agent Circuit ID (ASCII) • (option82) Agent Circuit ID (Hex) • (option82) Agent Remote ID (ASCII) • (option82) Agent Remote ID (Hex) • (option82) Agent Circuit ID (ASCII) + Agent Remote ID (ASCII) • (option82) Agent Circuit ID (ASCII) + Agent Remote ID (Hex) • (option82) Agent Circuit ID (Hex) + Agent Remote ID (ASCII) • (option82) Agent Circuit ID (Hex) + Agent Remote ID (Hex)

DHCP Relay

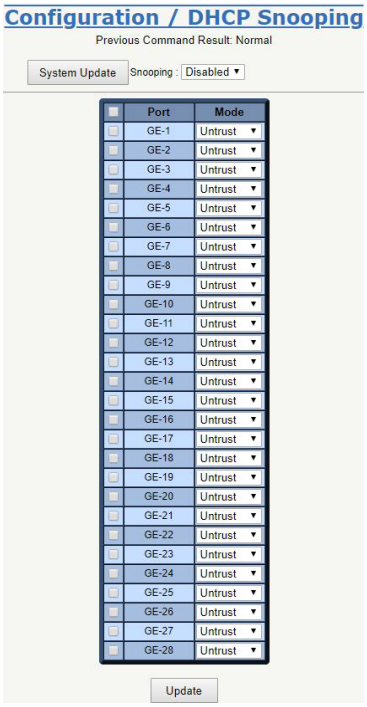
Modify DHCP Relay data.



Operation	• Enter the modified data, select the desired options. • Click “System Update” to apply the changes and modify the Relay. • Select the options for the Circuit-id(s) and click Update.
Field	**Description**
DHCP Relay Information Insert	Select Disabled or Enabled.
DHCP Relay Information Check	Select Disabled or Enabled.
DHCP Relay Information Remote-id Format	Select sys-mac, hostname, or ascii.
DHCP Relay Information Remote-id String	Read only id display
DHCP Relay Server 1-4	Enter the required data. Value Range: 0–255
Port	Port number.
Option82	Select Disabled or Enabled.
Circuit-Id	Select the value to transmit.

DHCP Snooping

Modify DHCP Snooping data

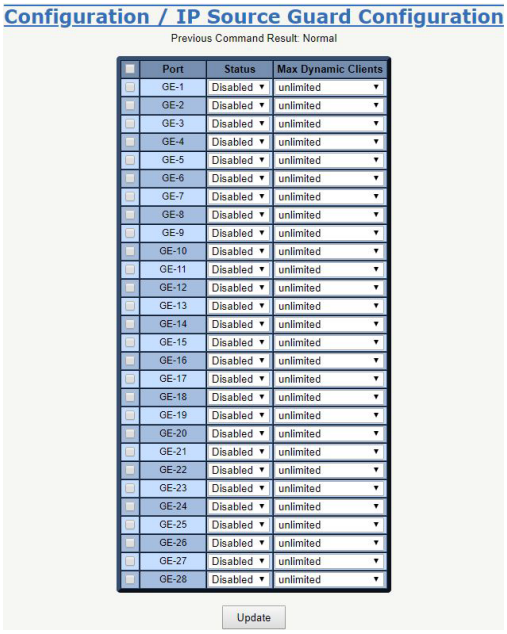


Operation	System Modify: • Click the “System Update” button to modify the DHCP Snooping configuration on the system. Port Modify: • Click the “Update” button to modify the DHCP Snooping configuration on selected ports.
Field	**Description**
Snooping	Control system’s DHCP snooping Enabled or Disabled.
Port	Port Number
Mode	Snooping Mode • Trust: Configures the port as trusted source of the DHCP messages. • Untrust: Configures the port as untrusted source of the DHCP messages.

IP Source Guard

Configuration

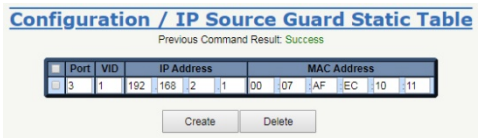
Modify IP Source Guard Port data.



Operation	Modify: • Modify the IP Source Guard port information as desired. • Select the check boxes by any ports to be modified. • Click the “Update” button to apply any changes.
Field	**Description**
Port	Port Number.
Status	Enable/Disable IP Source Guard of port.
Max Dynamic Clients	Maximum dynamic binding source on the port. The value: 0–5 or unlimited. Default value: unlimited.

Static Table

Set, create or delete the IP Source Guard Static Table



Create

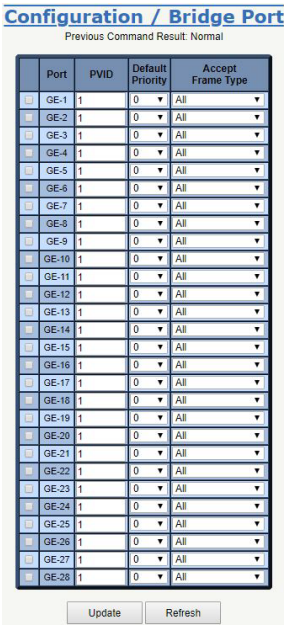
Operation	Create: • Click the “Create” button. • When the “Configuration / IP Source Guard Static Table – Create” screen appears, fill in the Port ID, VID, IP Address and MAC Address fields. • Click the “Apply” button to create new IP Source Guard Static Table data. Delete: • Select the check box by the row to be deleted in the IP Source Guard Static table. • Click the “Delete” button to delete IP Source Guard Static Table data.

Field	Description
Port ID	The identity for the Port. The value range: 1–28.
VID	The identity for the VLAN Interface. The value range: 1–4094.
IP Address	IP address for the VLAN interface. Range: 0–255. Default value: 0.
MAC Address	MAC address for the VLAN interface.

Port Configuration

Bridge Port

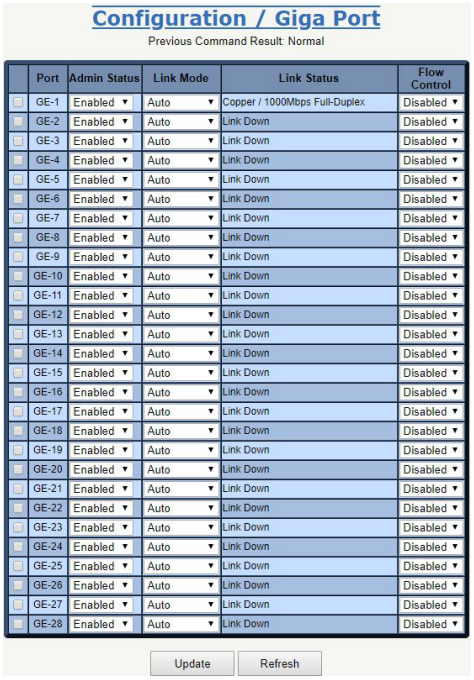
Modify bridge port parameters.



Operation	Modify: • Enter or select row by selecting the corresponding check box. • Modify the configuration as desired. • Press the “Update” button to apply any modifications.
Field	**Description**
Port	Bridge port number
PVID	Value: 1–4094. Default value: 1.
Default Priority	Default Priority value: 0–7. Default: 0.
Accept Frame Type	Type: All/ OnlyVlanTagged/ OnlyUnTagged. Default: All.

Giga Port

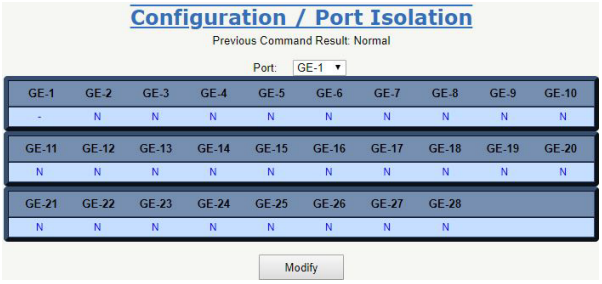
Modify Giga Port parameters.



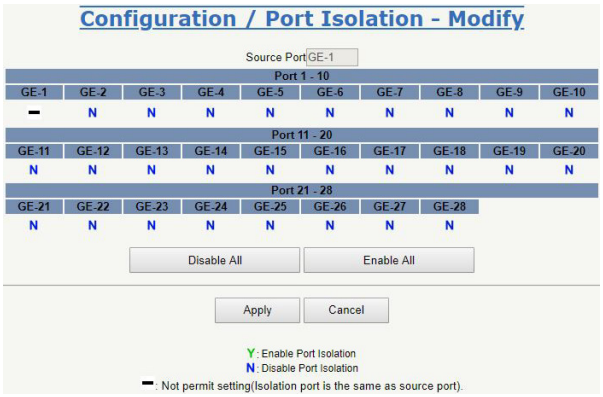
Operation	Modify: • Select the check box by the row(s) to be modified. • Modify the relevant fields. • Click the “Update” button to modify.
Field	**Description**
Port	GE-1–GE-28.
Admin Status	Enabled/Disabled port, default is Enabled.
Link Mode	Configuration for Link Mode: Auto (default is Auto) 10Mbps Half/Full Duplex 100Mbps Half/Full Duplex 1000Mbps Full Duplex 2500Mbps Full Duplex (10 gigabit ports) 10000Mbps Full Duplex (10 gigabit ports) **Note:** 2500Mbps Full Duplex (10 gigabit ports) is reserved for future use.
Link Status	Display Link type and speed Possible Type: Copper/ SFP Possible Status: 10Mbps Half-Duplex or Full-Duplex 100Mbps Half-Duplex or Full-Duplex 1000Mbps Full-Duplex 2500Mbps Full-Duplex (10 gigabit ports) 10000Mbps Full-Duplex (10 gigabit ports)
Copper/SFP Priority	Only some models support Copper/SFP combo port, SFP has first priority by default.
Flow Control	Enabled/Disabled Flow Control. Default: Disabled.

Port Isolation

Modify Port Isolation settings.



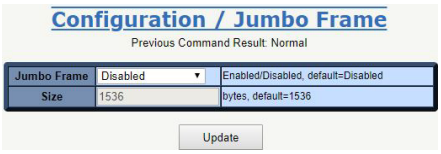
Port Isolation – Modify



Operation	Modify: • Click the “Modify” button to open the modification page. Port Isolation – Modify • Click the “Disable All”, “Enable All” or Y/N/- button to change isolation settings by port. • Click the “Apply” button to apply any changes or press “Cancel” to discard changes and return to the isolation main page.
Field	**Description**
Source Port	GE-1–GE-28
Isolation Port	Range: Y/N. Y: Isolation is true N: Isolation is false -: Not permitted setting (the isolation port is the same as the source port).
Disable All	Disable Isolation to all ports.
Enable All	Enable Isolation to all ports.
Apply	Apply changes to settings.
Cancel	Cancel changes to settings.

Jumbo Frame

Modify the Jumbo Frame.

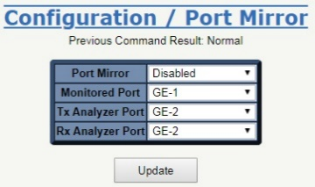


Operation	Modify: • Configure the following fields. • Click the “Update” button to apply any changes.

Field	Description
Jumbo Frame	Option: Enabled / Disabled. Default: Disabled.
Size	Range: 1536–9000 bytes. Default: 1536 bytes.

Port Mirror

Modify Port Mirror parameters.

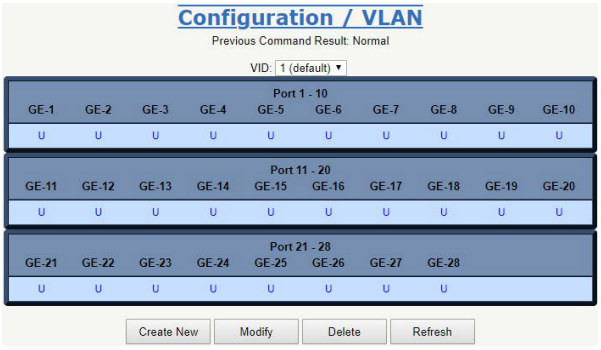


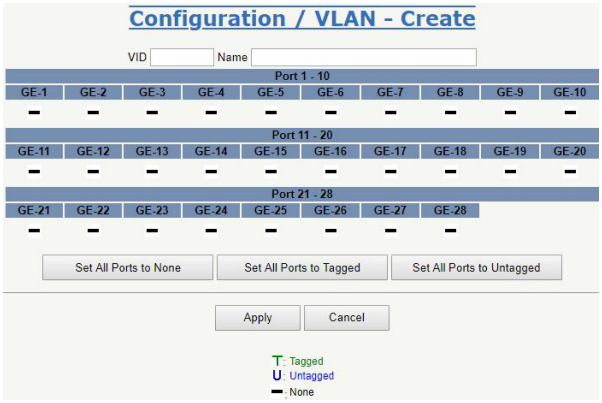
Operation	Modify: • Configure the following fields. • Click the “Update” button to apply any changes.
Field	**Description**
Port Mirror	Enable/Disable Port Mirror function, default is Disabled.
Monitored Port	Value range is GE-1–28, default is GE-1. Port to be monitored.
Tx Analyzer Port	Value range is GE-1–28, default is GE-2. Monitors packets transmitted from the monitored port.
Rx Analyzer Port	Value range is GE-1–28, default is GE-2. Monitors packets received on the monitored port.

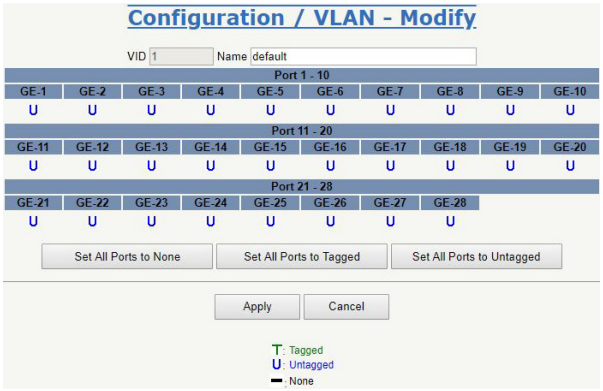
VLAN

Static VLAN

Create, Modify, Refresh, or Delete a VLAN.



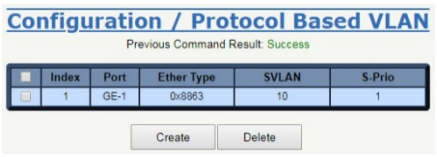




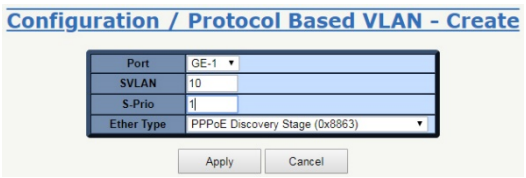
Operation	Create: • Click the “Create New” button to create a new VLAN. • Set VID and Name. • Click the fields to change status. • Click the “Apply” button to create the page. Modify: • Select "VID" to be modified. • Click the “Modify” button to modify the VLAN. • Modify name. • Click the fields to change status. • Click the “Apply” button to update. Refresh: • Click the “Refresh” button to refresh current VLANs. Delete: • Select “VID” to be deleted. • Click the “Delete” button to delete selected VLAN or VID.
Field	**Description**
VID	Value:1–4094. Default value: 1.
Name	Range: 0–32 characters
Tagged	T: Tagged U: Untagged -: None
Set All Ports to None	Set all pors to none (no ports join this VLAN).
Set All Ports to Tagged	Set all ports join the VLAN as Tagged.
Set All Ports to Untagged	Set all ports join the VLAN as Untagged.

Protocol-Based VLAN

Create or Delete a Protocol Based VLAN.



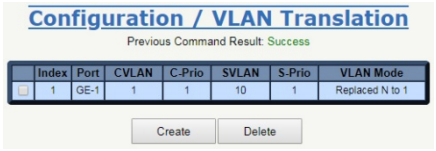
Create



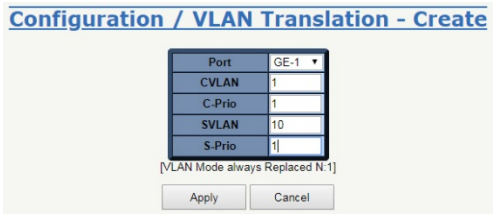
Operation	Create New: • Click the “Create” button to create a new page. • Set Port and Ether Type, input SVLAN and S-Prio. • Click the “Apply” button to create the page. (Max entries: 10.) Delete: • Select the index to be deleted with the adjacent check box. • Click the “Delete” button to delete the selected data.
Field	**Description**
Index	Index: 1–10.
Port	Protocol-base VLAN config port number, Port range: 1–28.
Ether Type	Select Ether Type: PPPoE Discovery Stage (0x8863). PPPoE Session Stage (0x8864). Internet Protocol (0x0800). ARP (0x0806). Others (input ether type), Range 0000–FFFF.
SVLAN	Service VLAN ID, Range: 1–4094
S-Prio	CoS of SVLAN: 0–7 **Note:** When the value is set to 8, the device preserves the priority that the packet entered the switch with.

VLAN Translation

Create or Delete a VLAN Translation.



Create

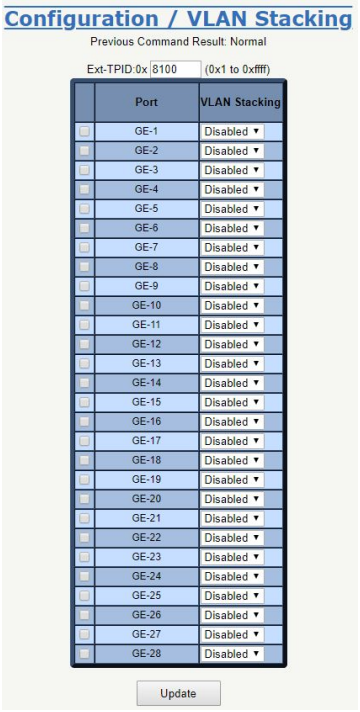


Operation	Create/Delete: • Select Port, fill CVLAN, C-Prio, SVLAN, and S-Prio. • Click the “Create” button to create a new entry. Click the “Delete" button to delete selected
Field	**Description**
Index	Index: 1–10, max entry number: 10.
Port	VLAN translation port number: GE-1–GE-28.
CVLAN	Customer VLAN ID: Range: 1–4094
C-Prio	CoS of CVLAN: Range: 0–7 **Note:** 8 is reserved for future use.
SVLAN	Service VLAN ID: Range: 1–4094
S-Prio	CoS of SVLAN: Range: 0–7 **Note:** 8 is reserved for future use.

VLAN Mode	Currently only supports: Replaced N to 1

VLAN Stacking

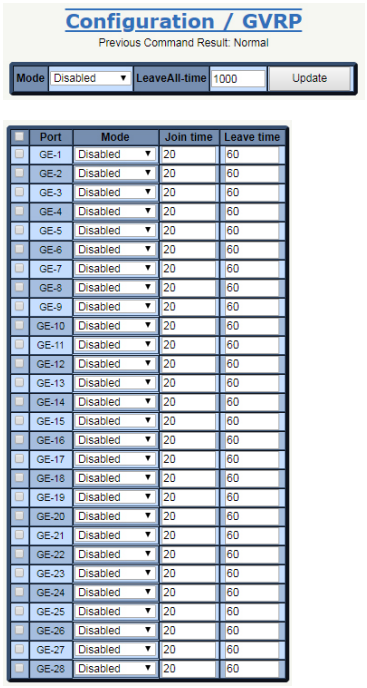
Modify VLAN Stacking.



Operation	Modify: • Select the check box adjacent to the port to be configured. • Select Stacking Disabled/Enabled. • Click the “Update” button to apply any changes.
Field	**Description**
Ext-TPID (Hex)	The range is from 1–FFFF (0x1 to 0xffff) Default: 0x8100
VLAN Stacking Port	Port: GE-1–GE-28
VLAN Stacking	Enable/Disable VLAN Stacking (QinQ) mode. Default value: Disabled.

GVRP

Configure GVRP

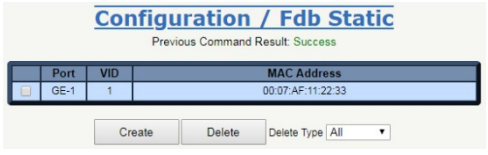


Operation	Configure system GVRP: • Set “Enabled” or “Disabled” system GVRP. • Set GVRP leave-all-time in range of 10 to 10000 (unit: centisecond) • Click "Update" next to Leave All Time to apply the new configuration. Configure port GVRP: • Modify configuration of GVRP port(s). • Click "Update" at the bottom of the page to apply the new configuration.
Field	**Description**
Port	GVRP port id.
Mode	Enable/Disable GVRP on the port.
Join Time	The time which applies to an interface's join timer. Range: 10–10000 (centisecond). Default: 20.
Leave Time	The time which applies to an interface's leave timer. Range: 10–10000 (centisecond). Default: 60.

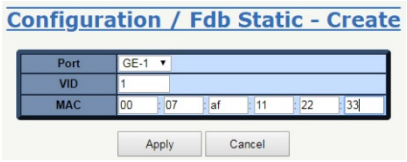
MAC Learning & Forwarding

Fdb Static

Create or Delete a Fdb Static entry.



Create



Operation	Create: • Click the “Create” button. • When the “Configuration / Fdb Static – Create” screen appears, fill in the Port, VID, and MAC fields. • Click the “Apply” button to add the new entry to the table. Delete: • Select Delete Type: "All/ Port/ VID/ Selected" • If Delete Type is "Port", then select a port • If Delete Type is "VID", then fill a VID • If Delete Type is "Selected", then select one row • Click the "Delete" button to delete.
Field	**Description**
Port	Giga Port: GE-1–GE-28
VID	Range: 1–4094. Default value: 1.
MAC Address	Format XX:XX:XX:XX:XX:XX

Aging Time

Modify the Aging Time setting.

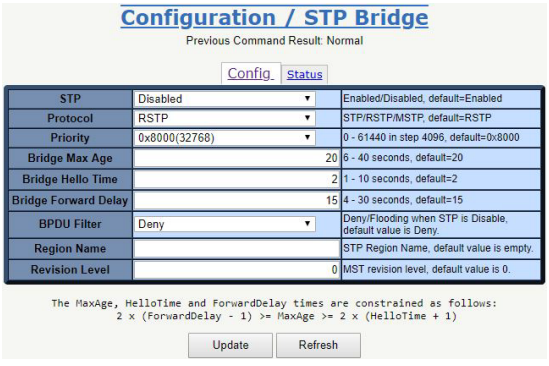
Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply any changes.
Field	**Description**
Aging Time (Sec)	Range: 10–600. Default: 300 seconds.

Spanning Tree Protocol (STP)

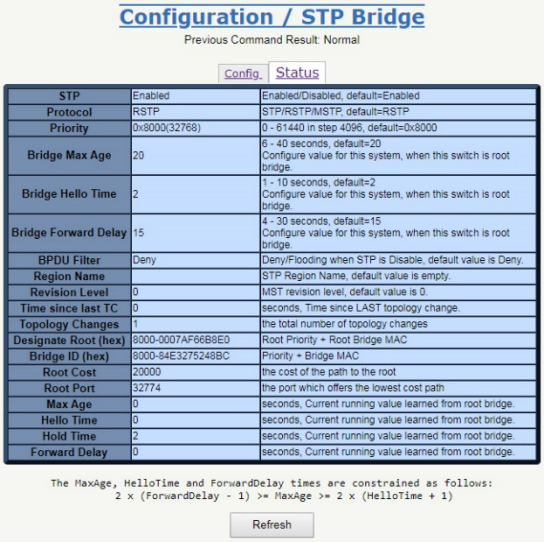
STP Bridge

Modify STP Bridge parameters.

Config



Status

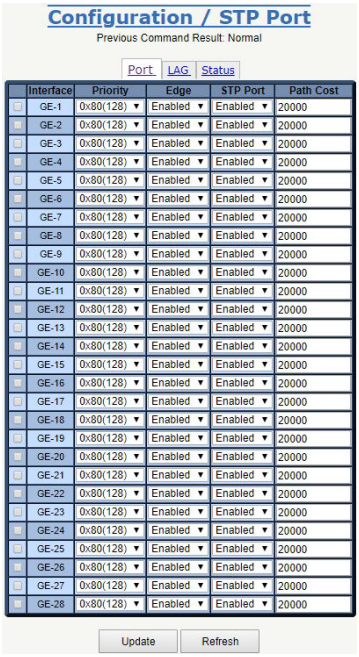


Operation	Modify: • Select the “Config” page. • Modify settings as desired. • Click the “Update” button to apply any changes. Refresh: • Click the “Refresh” button to get current data.
Field	**Description**
STP	Specify whether or not the system implements the spanning tree protocol. Range: Enabled/Disabled. Default: Enabled.
Protocol	RSTP (IEEE 802.1W), STP (IEEE 802.1D) Option: STP/RSTP. Default: RSTP.
Priority	Sets the spanning tree protocol priority. The lower the priority number, the higher priority the bridge. When two bridges have the same priority, their MAC addresses are compared and the smaller MAC address has higher priority. Range: 0–61440 in intervals of 4096. Default: 0x8000(32768).
Bridge Max Age	Sets the maximum age of received spanning tree protocol information before it is discarded. This is used when the bridge either has become or is attempting to become the root bridge. Range: 6–40 seconds. Default: 20 seconds.
Bridge Hello Time	Sets the time after which the spanning tree process sends notification of topology changes to the root bridge. This is used when the bridge either is or is attempting to become the root bridge. Range: 1–10 seconds. Default: 2 seconds.
Bridge Forward Delay	Sets the time that the bridge spends in listening or learning states when the bridge either is or is attempting to become the root bridge. Range: 4–30 seconds. Default: 15 seconds. The maxage, hellotime and forwarddelay times are constrained as follows: 2 x (forwarddelay - 1) ≥ maxage maxage ≥ 2 x (hellotime + 1) For example, the default settings are: 2 x (15 - 1) ≥ 20 20 ≥ 2 x (2 + 1)
BPDU Filter	Deny/Flooding when STP is Disabled.
Region Name	STP Region Name. Maximum Length: 32. Default value: empty.
Revision Level	MST revision level. Range Value: 0–65535. Default value: 0

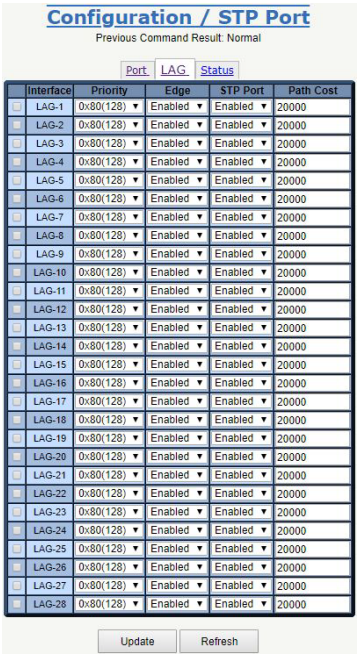
STP Port

Modify STP Port parameters.

Port:



LAG:

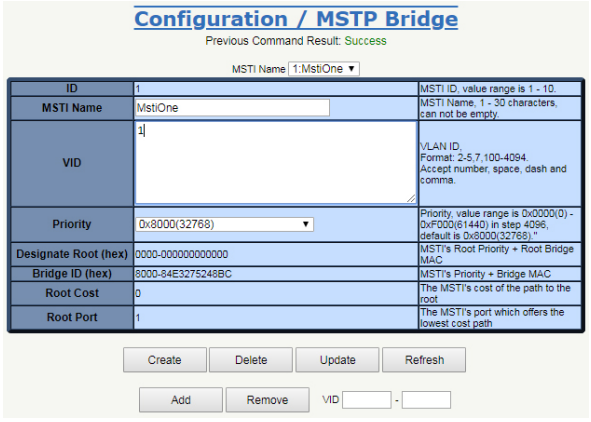


Status:

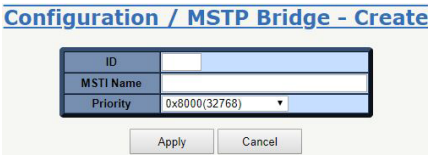
Operation	Modify: • Select the “Port” or “LAG” page. • Select row(s) to be changed by checking the associated check box. • Modify the settings and configuration. • Click the “Update” button to apply any changes. Refresh: • Click the “Refresh” button to get current data.
Field	**Description**
Interface	Identity of port or LAG number.
Priority	Range: 0–240 in Default: 0x80(128).
Edge	Range: Enabled/Disabled. Default: Disabled.
STP Port	Range: Enabled/Disabled. Default: Enabled.
Path Cost	Range: 1–200000000. Default: 20000.
State	*Range*: Disabled/ Blocking/ Listening/ Learning/ Forwarding/ Broken *Disabled*: For ports that are disabled (see dot1dStpPortEnable), this object will have a value of disabled. *Blocking*: The port will go into a blocking state during the selection process if the switch receives a BPDU on a port indicating a better path to the root switch or if the port is not a root port or a designated port. *Listening*: After the blocking state, a root port or a designated port will move to a listening state. All other ports will remain in a blocking state. During the listening state, the port discards frames received from the attached network segment and frames switched from another port for forwarding. In this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After a forward time delay (the default forward delay time is 15 seconds), the switch port moves from the listening state to a learning state. *Learning*: A port changes to a learning state from a listening state. In the learning state, the port is listening for and processing BPDUs. The port processes user frames and updates the MAC address table, though the user frames are not yet forwarded to their destinations. After a forward time delay (the default forward delay time is 15 seconds), the switch port moves from the learning state to a forwarding state. *Forwarding*: A port in a forwarding state forwards frames across the attached network segment. In a forwarding state the port processes BPDUs, updates its MAC Address table with frames that it receives, and forwards user traffic through the port. A forwarding state is the default state. Data and configuration messages are passed through the port when it is in a forwarding state. *Broken*: If a malfunctioning port is detected, the bridge will assign that port to a “broken” state.

MSTP Bridge

Modify a MSTP Instance (MSTI).



Create



Operation	Create: • Click the “Create” button. • When the “Configuration / MSTP Bridge – Create” screen appears, fill in the “ID” and “MSTI Name” fields, then select “Priority” field. (Default MSTI Name will be set when it is not input.) • Click the “Apply” button to create new data. • Max MSTI number: 10. Modify: • Select “MSTI Name” from list. • Modify the configuration of “MSTI Name”, “VID” or “Priority”. • Click the “Update” button to apply any changes. Delete: • Select “MSTI Name”. • Click the “Delete” button to delete the selected name. Add or Remove VID: • Fill in the start VID and the end VID in the two adjacent VID boxes. • Click the “Add” or “Remove” button to edit VID range, or input the VID range with the format in the VID cell.
Field	**Description**
ID	MSTI ID, value range: 1–10.
MSTI Name	MSTI Name, 1–30 characters. Cannot be empty: if empty, system will assign default name.
VID Start	VLAN ID, Range: 1–4094.
VID End	VLAN ID, Range: 1–4094.
VID	VLAN ID, Format: Accepts a single number, dash for ranges and comma for non-contiguous VIDs (ex: 2–5, 7, 100–101). Accept number, space, dash and comma.
Priority	MSTI's priority: The lower the priority number, the higher priority the bridge. Where two bridges have the same priority, their MAC addresses are compared and the smaller MAC address has higher priority. Range: 0–61440 in step 4096. Default: 0x8000(32768).
Designated Root	A unique bridge ID recorded as the “Root” in the configuration of BPDUs transmitted by the designated bridge to the port’s segment. Format: MSTI's Root bridge priority + Root Bridge MAC address
Bridge ID	A bridge ID that denotes the “Designated Bridge” for this port's segment. Format: MSTI's priority + Bridge MAC address. [0x8000-001122334455]
Root Cost	The path cost of the MSTI's Designated Port of the port’s segment. This value is compared to the Root Path Cost field in received BPDUs.
Root Port	The MSTI's port ID Designated Bridge Port for this port’s segment [0x8001].

MSTP Port

Modify the MSTP Port.

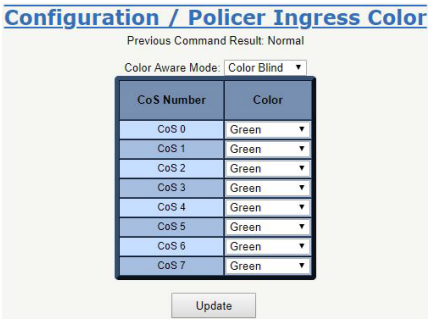
Operation	Modify: • Select a row item to be modified. • Set or configure the relevant fields. • Click the “Update” button to apply any changes.
Field	**Description**
Port	Range: GE-1–GE-28
Priority	Range: 0–240 in intervals of 16. Default: 0x80(128).
Path Cost	Range: 1–200000000. Default: 20000.
Role	Range: Disabled/ Root/ Designated/ Alternate/ Backup/ Master/ Unknown.
State	*Range*: Disabled/ Blocking/ Listening/ Learning/ Forwarding/ Broken. *Disabled*: For ports that are disabled (see dot1dStpPortEnable), this object will have a value of Disabled. *Blocking*: The port will go into a blocking state during the selection process if the switch receives a BPDU on a port that indicates a better path to the root switch, or if the port is not a root port or a designated port. *Listening*: After a blocking state, a root port or a designated port will move to a listening state. All other ports will remain in a blocking state. During the listening state, the port discards frames received from the attached network segment and frames switched from another port for forwarding. In this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After a forward time delay (the default forward delay time is 15 seconds), the switch port moves from the listening state to the learning state. *Learning*: A port changes to a learning state from a listening state. In the learning state, the port is listening for and processing BPDUs. In this state, the port processes user frames and updates the MAC address table, though the user frames are not yet forwarded to their destinations. After a forward time delay (the default forward delay time is 15 seconds), the switch port moves from the learning state to the forwarding state. *Forwarding*: A port in a forwarding state forwards frames across the attached network segment. In a forwarding state, the port processes BPDUs, updates its MAC Address table with frames that it receives, and forwards user traffic through the port. A forwarding state is

	the normal state. Data and configuration messages are passed through the port when it is in a forwarding state. *Broken*: If a malfunctioning port is detected, the bridge will assign that port to a “broken” state.
Designated Root	A unique bridge ID recorded as the Root in the configuration of BPDUs transmitted by the Designated Bridge for the port’s segment. Format: Root Bridge priority + Root Bridge MAC address
Designated Cost	The path cost of the Designated Port of the port’s segment. This value is compared to the Root Path Cost field in received BPDUs.
Designated Bridge	A bridge ID which denotes the “Designated Bridge” for this port's segment. Format: Designated bridge priority + Designated Bridge MAC address. [0x8000-001122334455]
Designated Port	A port ID Designated Bridge Port for this port's segment. (dot1dStpPortDesignatedPort). Format: Designated port priority + Designated Port ID. [0x8001]

Policer

Policer Ingress Color

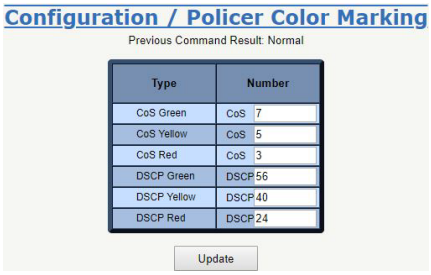
Modify the Policer Ingress Color.



Operation	Modify: • Select “Color Blind” or “Color Aware”. • Modify the configuration of CoS 0–7. • Click the “Update” button to apply any changes.
Field	**Description**
Color Aware Mode	Color Blind/ Color Aware. Default: Color Blind.
CoS 0	Green/Yellow/Red. Default: green
CoS 1	Green/Yellow/Red. Default: green
CoS 2	Green/Yellow/Red. Default: green
CoS 3	Green/Yellow/Red. Default: green
CoS 4	Green/Yellow/Red. Default: green
CoS 5	Green/Yellow/Red. Default: green
CoS 6	Green/Yellow/Red. Default: green
CoS 7	Green/Yellow/Red. Default: green

Policer Color Marking

Modify the Policer Color Marking.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply any changes.
Field	**Description**
CoS Green	Range: 0–7. Default: 7
CoS Yellow	Range: 0–7. Default: 5
CoS Red	Range: 0–7. Default: 3
DSCP Green	Range: 0–63. Default: 56
DSCP Yellow	Range: 0–63. Default: 40
DSCP Red	Range: 0–63. Default: 24

Ingress Policer

Modify Ingress Policer parameters.

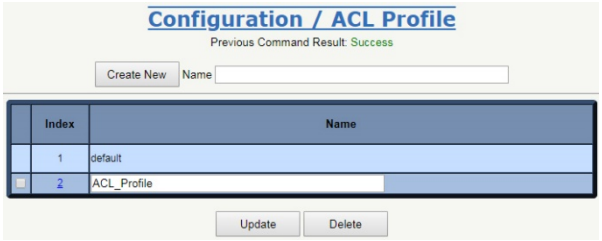
Operation	Modify: • Adjust the configurations as desired. • Click the “Update” button to apply any changes.
Field	**Description**
Port	Bridge port number. GE-1–GE-28.
Mode	Ingress Policer Mode Enabled/Disabled. Default: Disabled.
Exceed Action	Value range is Drop/CoS Mark/DSCP Mark. Default: Drop.
PIR (Kbps)	Value range is 1–1000000 Kbps. Default: 1000000 Kbps.
PBS (Bytes)	Value range is 10240–65535 Bytes. Default: 10240 Bytes.

CIR (Kbps)	Value range is 1–1000000 Kbps. Default: 500000 Kbps.
CBS (Bytes)	Value range is 10240–65535 Kbps. Default: 10240 Kbps.

ACL

Profile

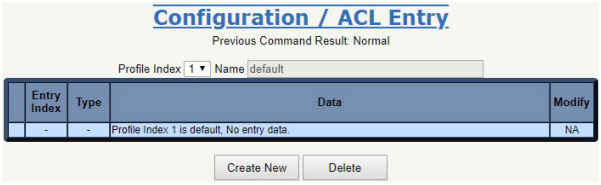
Create, Modify or Delete an ACL Profile.



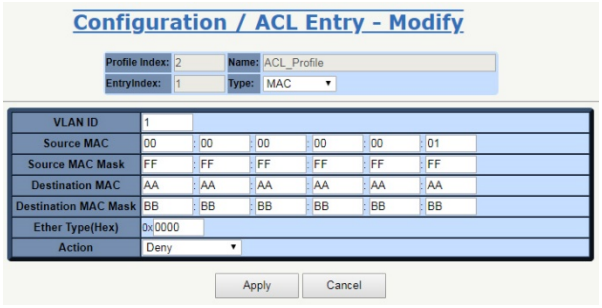
Operation	Create New: • Fill the ACL Profile Name. The max length is 31. • Click the “Create New” button to create a new ACL profile. Modify: • Select the check box of the profile to be changed. • Modify the “Name” of the profile. • Click the “Update” button to apply any changes. Delete: • Select row(s) for deletion. • Click the “Delete” button to delete selected data.
Field	**Description**
Index	ACL Profile Index: index range depends on product type. Profile 1 is the default profile and cannot be modified. Click the Profile Index to modify the ACL Profile Entry.
Name	ACL Profile Name, Max Length: 31 characters.

Entry

Create, modify or delete an ACL Entry.



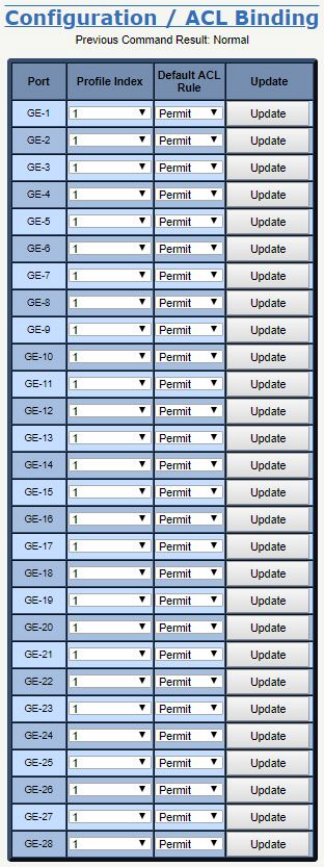
Modify



Operation	Create New: • Click the “Create New” button to open the Create New Entry page. • Fill in the “ACL Entry Index” field and select the “Type”. • Fill fields as desired, then click “Apply” to apply any changes or click the “Cancel” button to cancel any changes Modify: • Modify field data. • Click the “Modify” button to open the modification page. • Select the “Type”. • Fill fields as desired, then click “Apply” to apply any changes or click the “Cancel” button to cancel any changes. Delete: • Select the row to be deleted. • Click the “Delete” button to delete selected data.
Field	**Description**
Profile Index	Range: depends on product type.
Entry Index	Range: 1–16
Type	MAC/IPV4/L4PORT/TOS, Default Value: MAC
Type = MAC	
VLAN ID	ACL Profile VLAN ID, Value Range: 1–4094.
Source MAC	ACL Profile Source MAC format XX:XX:XX:XX:XX:XX, each field value range: 0–FF
Source MAC Mask	ACL Profile Source MAC Mask format XX:XX:XX:XX:XX:XX, each field value range: 0–FF
Destination MAC	ACL Profile Destination MAC format XX:XX:XX:XX:XX:XX, each field value range: 0–FF
Destination MAC Mask	ACL Profile Destination MAC Mask format XX:XX:XX:XX:XX:XX, each field value range: 0–FF
Ether Type (Hex)	Value Range: 0,05DD–FFFF format XXXX. 0 represents any Ether Type.
Action	Value Range: Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
Type = IPv4	
Source IP	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Source IP Mask	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Destination IP	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Destination IP Mask	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Protocol	Value Range: 0–255. 0 represents any protocol.
Action	Value Range: Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
Type = LP4PORT	
Protocol	Option: TCP/UDP.
Source IP	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Source IP Mask	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Port	Source IP Port, value range: 0–65535. 0 means any port.
Destination IP	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Destination IP Mask	Format XXX:XXX:XXX:XXX, each field value range: 0–255.
Port	Destination IP Port, value range: 0–65535. 0 means any port.
Action	Value Range: Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
Type =ToS/DSCP	
Source IP	Format XXX.XXX.XXX.XXX, each field value range: 0–255.
Source IP Mask	Format XXX.XXX.XXX.XXX, each field value range: 0–255.
Destination IP	Format XXX.XXX.XXX.XXX, each field value range: 0–255.
Destination IP Mask	Format XXX.XXX.XXX.XXX, each field value range: 0–255.
ToS/DSCP Type	Value Range: Precedence/ToS/DSCP/Any, 0–7 in Precedence, 0–15 in ToS, 0–63 in DSCP.
Action	Value Range: Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.

Binding

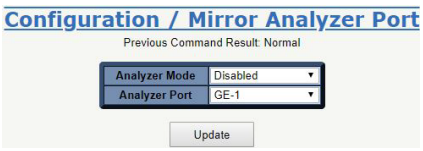
Modify the ACL Binding settings.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected port.
Field	**Description**
Port	Giga Port, GE-1–GE-28.
Profile Index	ACL Profile Index, range is 1–10. Default: 1.
Default ACL Rule	ACL Default Rule, could be Permit/Deny. Default: Permit.

Mirror Analyzer Port

Modify the Mirror Analyzer Port settings.

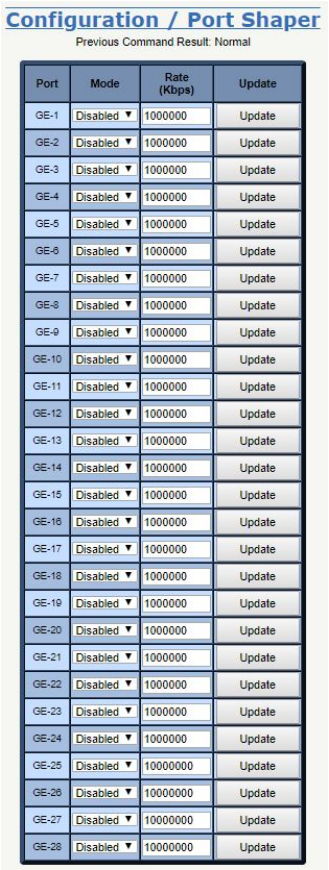


Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply any changes.
Field	**Description**
Analyzer Mode	Enabled/Disabled. Default: Disabled.
Analyzer Port	Giga Port GE-1–GE-28. Default: GE-1.

Shaper

Port

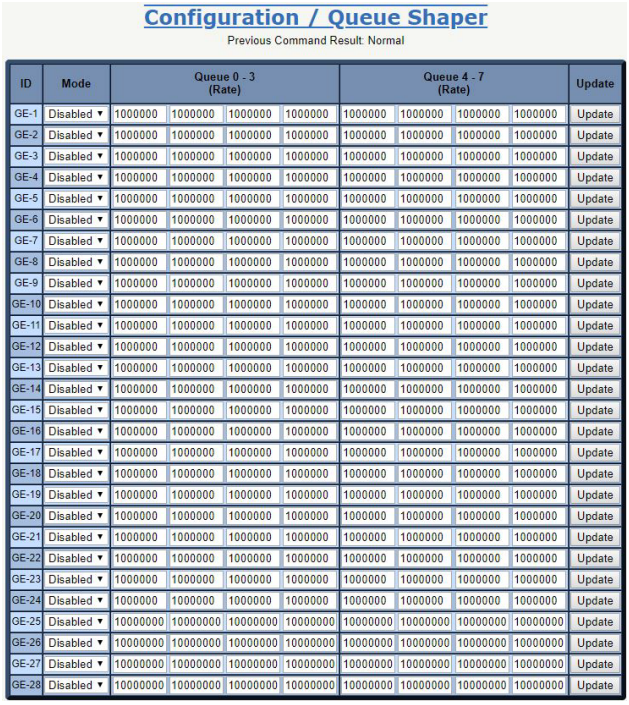
Modify Port Shaper parameters.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected port.
Field	**Description**
Port	Bridge port, range: 1–28.
Mode	Enabled/Disabled. Default: Disabled.
Rate (Kbps)	Rate range: 1–1000000 Kbps. Default: 1000000 Kbps.

Queue

Modify Queue Shaper parameters.

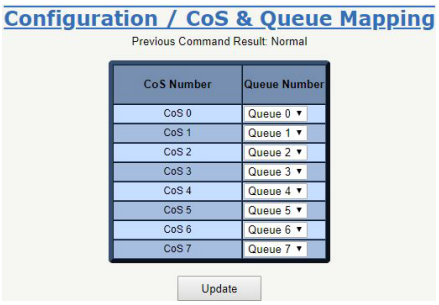


Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected ID.
Field	**Description**
ID	Bridge port, range: 1–28.
Mode	Option: Enabled/Disabled. Default: Disabled.
Queue 0–3 (Rate)	Queue 0–3, rate range: 1–1000000 Kbps. Default: 1000000 Kbps.
Queue 4–7 (Rate)	Queue 4–7, rate range: 1–1000000 Kbps. Default: 1000000 Kbps.

Queue & Scheduler

CoS & Queue Mapping

Modify the CoS & Queue Mapping settings.

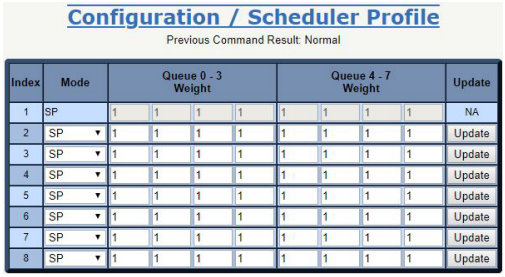


Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply any changes.
Field	**Description**
CoS 0	Queue 0–7, default: Queue 0.
CoS 1	Queue 0–7, default: Queue 1.

CoS 2	Queue 0–7, default: Queue 2.
CoS 3	Queue 0–7, default: Queue 3.
CoS 4	Queue 0–7, default: Queue 4.
CoS 5	Queue 0–7, default: Queue 5.
CoS 6	Queue 0–7, default: Queue 6.
CoS 7	Queue 0–7, default: Queue 7.

Scheduling Profile

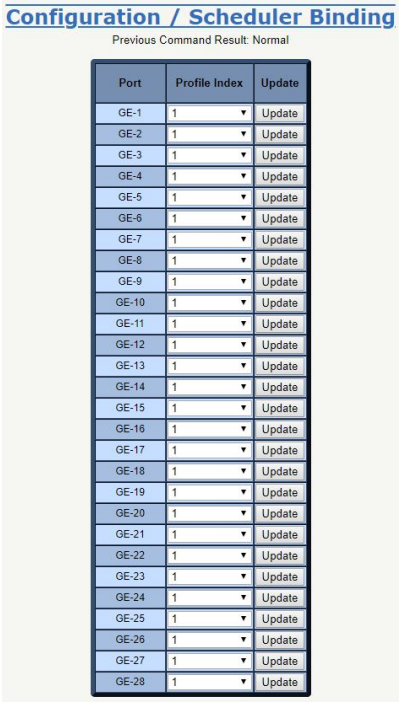
Modify the Scheduler Profile parameters.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected Index.
Field	**Description**
Index	Value range: 1–8.
Mode	Option: SP/SPWRR/WRR. Default: SP.
Queue 0-3 weight	Queue 0–3 Weight: Range 1–255. Default: 1.
Queue 4-7 weight	Queue 4–7 Weight: Range 1–255. Default: 1.

Binding

Modify Scheduler Binding settings.

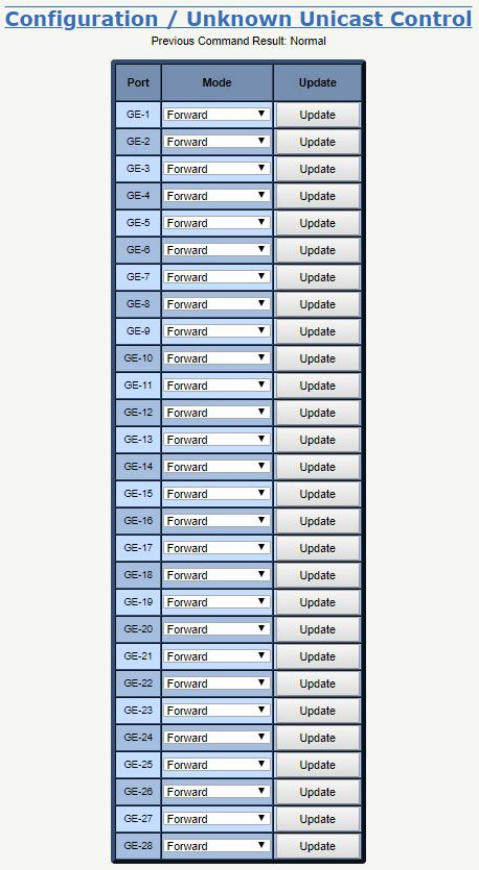


Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected Port.
Field	**Description**
Port	Giga Port GE-1–GE-28.
Profile Index	Range: 1–8. Default: 1.

Storm Control

Unknown Unicast Control

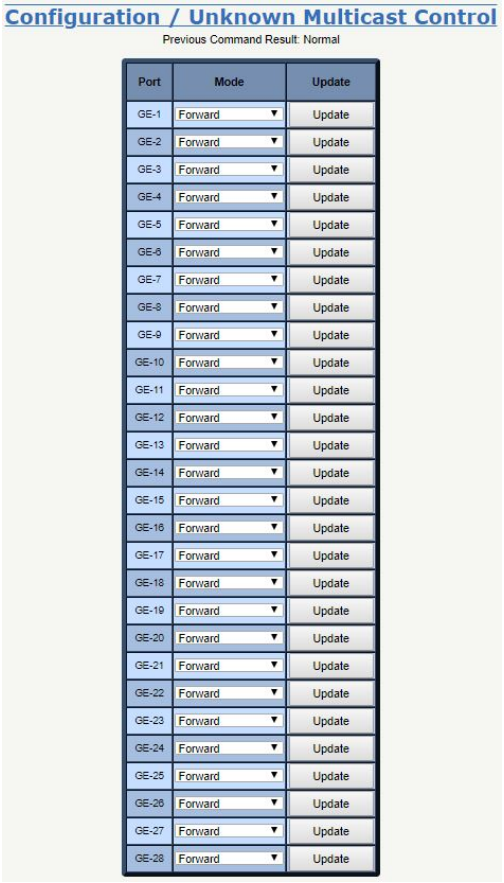
Modify the Unicast Control settings.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected Port.
Field	**Description**
Port	Giga Port GE-1–GE-28.
Mode	Forward: Forward unknown unicast packet (default). Block: Block unknown unicast packet. Rate limit: Control rate. Rate range: 1–1000000 Kbps. Default: 1000000 Kbps.

Unknown Multicast Control

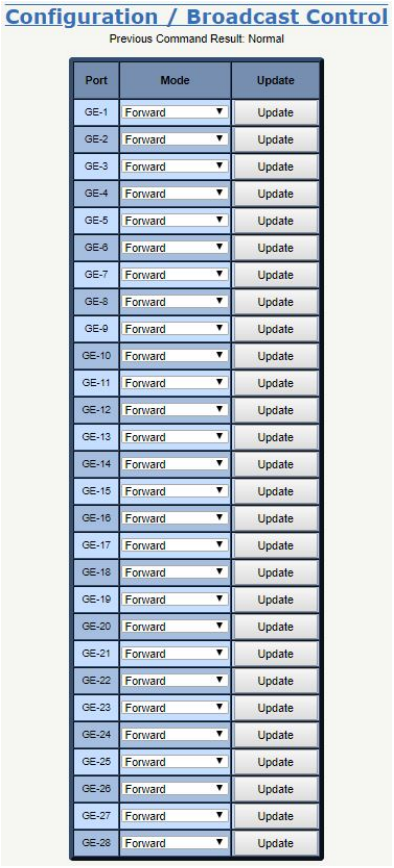
Modify settings.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected Port.
Field	**Description**
Port	Giga Port GE-1–GE-28.
Mode	Forward: Forward unknown multicast packet (default). Block: Block unknown multicast packet. Rate limit: Control rate. Rate range: 1–1000000 Kbps. Default: 1000000 Kbps.

Broadcast Control

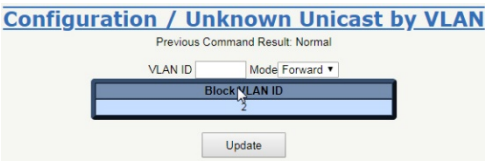
Modify Broadcast Control settings.



Operation	Modify: • Modify the configuration as desired. • Click the “Update” button to apply changes to the selected Port.
Field	**Description**
Port	Giga Port GE-1–GE-28.
Mode	Forward: Forward broadcast packet (default). Block: Block broadcast packet. Rate limit: Control rate. Rate range: 1–1000000 Kbps. Default: 1000000 Kbps.

Unknown Unicast by VLAN

Modify Unknown Unicast for VLAN settings.

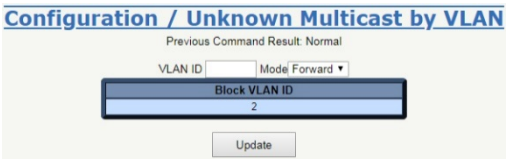


Operation	Modify: • Fill VLAN ID. • Set Mode. • Click the “Update” button to apply any changes.
Field	**Description**
VLAN ID	Value range: 1–4094.

Mode	Forward: Forward unicast packet. Block: Block unicast packet. Default: Forward.
Block VLAN ID	All blocked VLAN ID

Unknown Multicast by VLAN

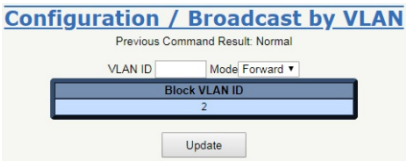
Modify Unknown Multicast for VLAN settings.



Operation	Modify: • Fill VLAN ID. • Set Mode. • Click the “Update” button to apply any changes.
Field	**Description**
VLAN ID	Value range: 1–4094.
Mode	Forward: Forward unknown multicast packet. Block: Block unknown multicast packet. Default: Forward.
Block VLAN ID	All blocked VLAN ID

Broadcast by VLAN

Modify Broadcast for VLAN settings.

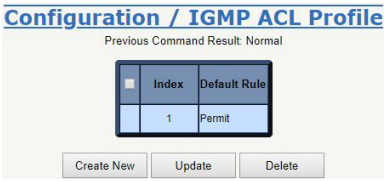


Operation	Modify: • Fill VLAN ID. • Set Mode. • Click the “Update” button to apply any changes.
Field	**Description**
VLAN ID	Value range: 1–4094.
Mode	Forward: Forward broadcast packet. Block: Block broadcast packet. Default: Forward.
Block VLAN ID	All blocked VLAN ID

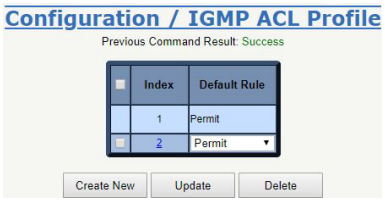
IGMP

ACL Profile

Create, modify and delete a IGMP ACL Profile.



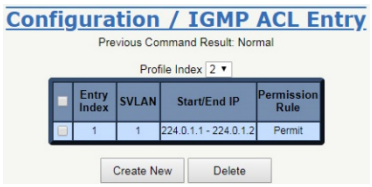
Create



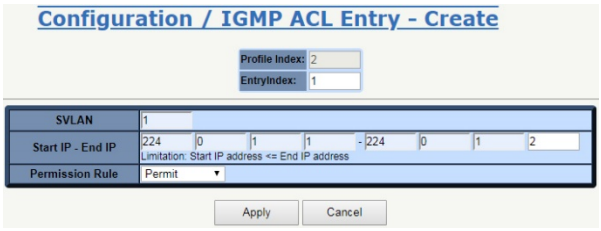
Operation	Modify: • Click the “Create New” button to create a default profile. • Click the “Update” button to modify an existing profile. Modify (allow multiple selection): • Check the associated check box of the relevant Profile Index and select Default Rule for the profile. • Click the “Update” button to modify IGMP ACL Profile. Delete: • Click the “Delete” button to delete the selected profile. Multiple selections can be deleted at once. • If the profile is in use, the delete action will fail.
Field	**Description**
Profile Index	IGMP ACL Profile Index: 1–15, but profile 1 is a default profile and is read-only.
Default Rule	IGMP ACL Default rule: Permit/Deny. Default: Permit.

ACL Entry

Create, delete, and get a IGMP ACL Entry.



Create New

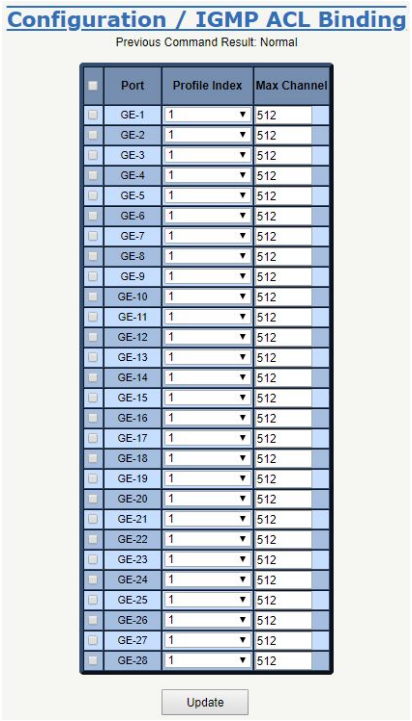


Operation	Create: • Click the “Create new” button to open a new page. • Fill Entry Index, SVLAN, Start IP, End IP, and select the appropriate Permission Rule. • Click the “Apply” button to create IGMP ACL entry or click the “Cancel” button to cancel creation. Delete: • Select the associated check box of the item to be deleted, then click the “Delete” button for deletion. Multiple selections may be deleted at once.
Field	**Description**
Profile Index	IGMP ACL profile index. Range: 2–15.
Entry Index	IGMP ACL entry index. Range: 1–32.
SVLAN	IGMP ACL VLAN: VLAN to be Permitted/Denied, 0 is any VLAN.

Start IP – End IP	IGMP ACL Start IP address. Range: 224.0.1.0–239.255.255.255 Start IP address ≤ End IP address
Permission Rule	IGMP ACL entry parameter. Default: Permit.

ACL Binding

Modify the IGMP ACL Binding.



Operation	Modify: • Check the associated check boxes of the rows to be modified, then select the ACL Profile Index and set the Max Channel. • Click the “Update” button to apply any changes to the IGMP ACL Binding.
Field	**Description**
Port	GE Port: GE 1–28.
Profile Index	IGMP ACL profile index: 1–15. Default: 1.
Max Channel	Port Max channel. Range: 1–512. Default: 512.

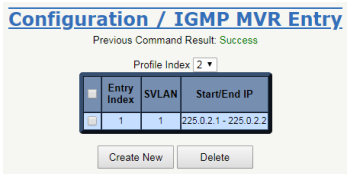
MVR Profile

Create or delete a IGMP MVR Profile.

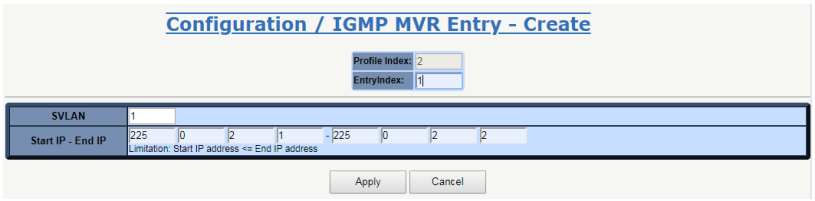
Operation	Create: • Select the “Create New” button to create a new profile. Modify: • Select the Profile Index hyperlink to open the page for profile entry modification. Delete: • Select the associated check box of the profile to be deleted, then click the “Delete” button. Multiple selections may be deleted at once. If the profile is in use, the delete action will fail.
Field	**Description**
Profile Index	Profile 1 is a default profile and is read-only, IGMP MVR Profile 2–15 are creatable and modifiable.

MVR Entry

Create, delete and read the IGMP MVR Entry.



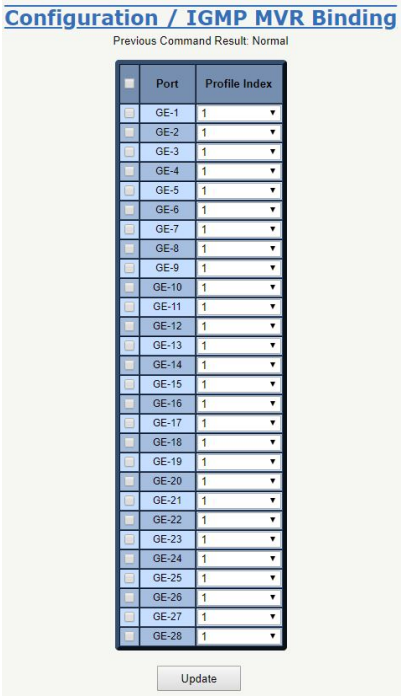
Create



Operation	Create New: • Click the “Create New” button to open a new page for creating an entry. • Fill the Entry Index, SVLAN, Start IP and End IP. • Click the “Apply” button to create an IGMP MVR entry or click the “Cancel” button to discard the entry. Delete: • Check the corresponding check box for the entry to be deleted, then click the “Delete” button to delete. Multiple items may be deleted at one time. Refresh: • Change the Profile Index to refresh the data.
Field	**Description**
Profile Index	IGMP MVR profile index. Index range: 2–15.
Entry Index	IGMP MVR entry index. Range: 1–32.
SVLAN	IGMP MVR VLAN: VLAN to be Permitted/Denied.
Start IP – End IP	IGMP MVR Start IP address. Range: 224.0.1.0–239.255.255.255 Start IP address ≤ End IP address

MVR Binding

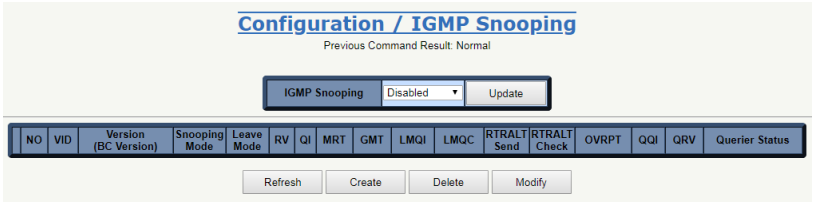
Modify the IGMP MVR Binding.



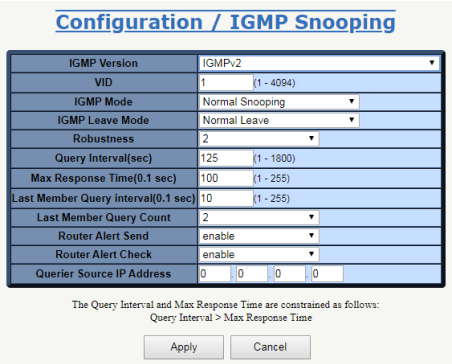
Operation	Modify: • Select the corresponding check box for the rows to be modified and select the MVR Profile Index. • Click the “Update” button to apply any changes to the IGMP MVR Binding.
Field	**Description**
Port	GE Port: GE 1×28
Profile Index	IGMP MVR profile index. Value range: 1–15. Default: 1.

Snooping

Read or configure IGMP Snooping.



Create/Modify



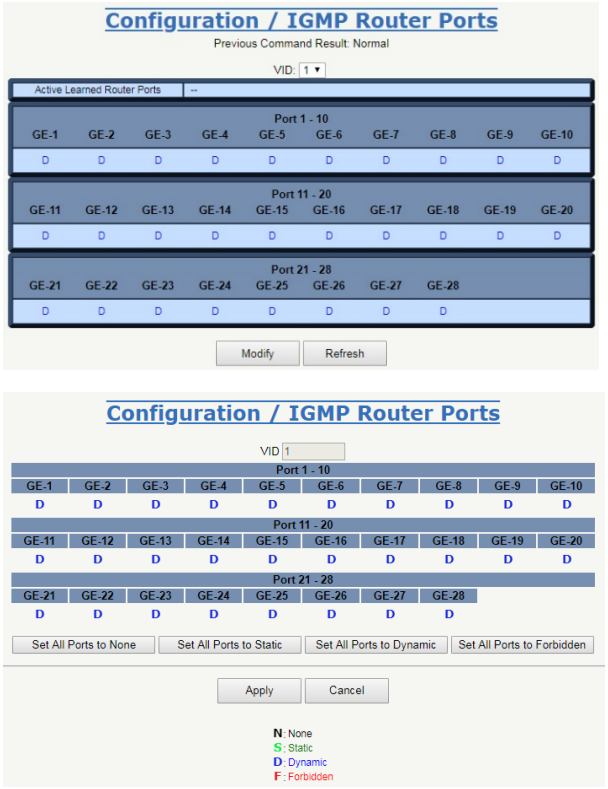
Operation	Create: • Click the “Create” button. • When the “Configuration / IGMP Snooping” screen appears, configure the settings for the interface as desired. • Click “Apply” to create the new interface or click “Cancel” to cancel creation. Modify: • Click the radio box by the interface to be modified. • Click the “Modify” button and change the settings of the interface as desired. • Click the “Apply” button to save any configuration changes or click “Cancel” to cancel changes. Refresh: • Refresh to get current data. Delete: • Delete the selected row.
Field	**Description**
NO	Entry Index: max 64.
VID	VLAN ID: 1–4094
Version	IGMP Version: IGMPv2, IGMPv3 or IGMPv2/v3 Compatible.
Run Version	Current running IGMP version.
Snooping Mode	IGMP Snooping Mode: Normal Snooping (default), Snooping with Querier, or Proxy.
Leave Mode	IGMP Leave Mode: Normal Leave (default) or Fast Leave.
Robustness	IGMP VLAN robustness variable: 1–3
Robustness Run Value	Display QRV value or configured value: To support QRV and QQIC in IGMPv3 mode, the switch supports two parameters to represent the running Robustness Variable and running Query Interval. These parameters are supported for each IGMP VLAN interface. When IGMPv3 is in proxy mode, the parameters will use values from the IGMPv3 Query packet. In other modes, the value used is the configured value.
Query Interval (sec)	IGMP VLAN query interval.(unit: sec) Default: 125 seconds Limitation: Query Interval>Max Response Time
Query Interval Run Value (sec)	Display QQIC value or configured value: To support QRV and QQIC in IGMPv3 mode, the switch supports two parameters to represent the running Robustness Variable and running Query Interval. These parameters are supported for each IGMP VLAN interface. When IGMPv3 is in proxy mode, parameters will use the values from the IGMPv3 Query packet. In other modes, the value used is the configured value.
Max Response Time	IGMP VLAN max response time. Default: 10.0 seconds. (Displays in seconds, configures in 0.1 seconds) The Query Interval and Max Response Time are constrained as follows: Query Interval > Max Response Time
Group Membership Time	IGMP Group Membership Time (Unit: sec), Read-only

Last Member Query Interval	IGMP VLAN last member query interval. (Displays in seconds, configures in 0.1 seconds) Default: 0.1 second
Last Member Query Count	IGMP VLAN last member query count, range 1–3. Default: 2
Router Alert Send	When enabled, the local device generates an IGMP packet that includes a router-alert option. When disabled, the local device generates an IGMP packet without a router-alert option. Default is enabled.
Router Alert Check	When enabled, the local device will always verify the router-alert option of the incoming IGMP packet. If no router-alert option is present in the packet, then the IGMP packet is ignored. When disabled, the local device disregards whether the incoming IGMP packet includes a router-alert option. Default is enabled.
Querier Source IP Address	Querier Source IP Address. Default: 0.0.0.0.

Note: For interoperability with N-Tron series devices with auto IGMP enabled, it is recommended to set the query interval on the NT328G to less than 120 seconds

Router Ports

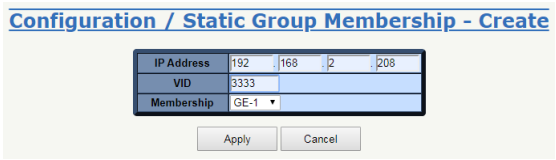
Modify or refresh router ports.



Operation	Modify: • Click the “Modify” button. • When the “Configuration / IGMP Router Ports” screen appears, change the state of the desired port(s). • Click the “Apply” button to apply any changes made.
Field	**Description**
VID	VLAN ID, Range: 1–4094.
Router Port	IGMP VLAN interface: • Bridge port: GE-1–GE-28. Default value: 1 **Note:** Active Router Ports are not bidirectional.

Static Group Membership

Create or Delete a Static Group Membership.



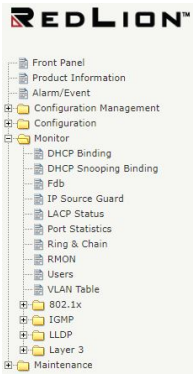
Operation	Create New: • Click the “Create” button. • When the “Configuration / Static Group Membership – Create” dialog box appears, fill in the IP Address, VID and select Membership. • Click the “Apply” button to create a new ID. Delete: • Select Delete Type “All/Membership/VID/Selected” • If delete type is “Membership”, then select a port. • If delete type is “VID”, then fill a VID. • If delete type is “Selected”, then select a row. • Click the “Delete” button to delete the data type.
Field	**Description**
IP Address	Group Membership IP Address, range: 224.0.0.0–239.255.255.255
VID	VLAN ID, Range: 1–4094.
Membership	Giga Port, GE-1–GE-28.

Chapter 5 Monitor

Monitor

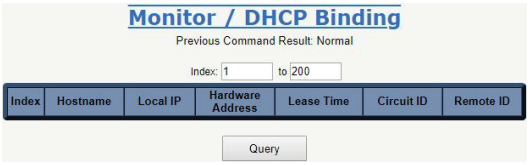
This chapter lists the monitor related functions available for Red Lion Controls NT328G Switch models.

Monitor Menu



DHCP Binding

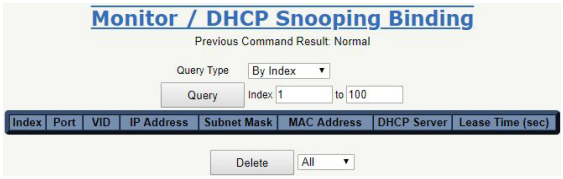
Display the DHCP Binding Table. The DHCP Pool binding table contains the IP address, MAC address, start/end time and VLAN interface of DHCP Server in this switch.



Operation	Query: • Enter the Index range. • Click on Query.
Field	**Description**
Index	The index range for the VLAN Interfaces to query. Default: 1-200 Range: 1-1024
Query	Executes the query for the selected Index range.
Index	Index Number.
Host Name	The Host name.
Local IP Address	IP address of the local device.
Hardware Address	The MAC address where the leased IP address is used.
Lease Time	When the IP address lease started.
Circuit ID	The Client circuit identifier.
Remote ID	The identifier transmitted as the DHCP option 82 Relay Agent Remote ID.

DHCP Snooping Binding

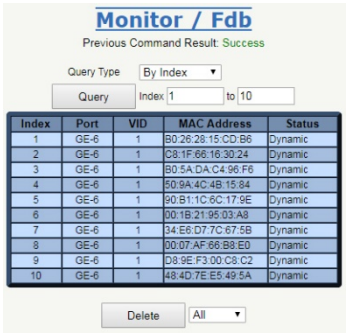
Use this screen to get DHCP Snooping Binding status.



Operation	Query: To Get DHCP Binding Status: • Select a Query Type (by Index, by VID & Index, or by Port & Index). • Fill the query condition. • Modify the query record range (Index Range). • Click the “Query” button to query and get DHCP Snooping Binding Status. Delete: • Select a Delete Type (All, by VID, or by Port). • Fill any delete conditions. • Click the “Delete” button to delete.
Field	**Description**
Index	Default: 1-100 Range: 1-200
Port	GE-1 - Number of Port or Trunk Group.
VID	VLAN ID: 1–4094
IP Address	Format: xxx.xxx.xxx.xxx
Subnet Mask	Format: xxx.xxx.xxx.xxx
MAC Address	Format: XX:XX:XX:XX:XX:XX
DHCP Server	Format: xxx.xxx.xxx.xxx
Lease Time (sec)	Lease time; units in seconds

Fdb

Use this screen to get Fdb status.

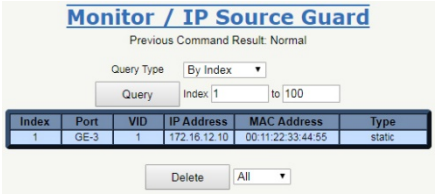


Operation	Query: Select a Query Type (By Index, By VID & Index, or By Port & Index). • Fill the conditions for the query record. • Modify the query record range (Index Range). • Click the “Query” button to query. Delete: • Select a delete type (All, by VID, or by Port). • Fill delete conditions. • Click the “Delete” button to delete.
Field	**Description**
Index	Default: 1-100 Range: 1-8192

Port	GE 1–28.
VID	VLAN ID: 1–4094
MAC Address	Format xx:xx:xx:xx:xx:xx
Status	Data type: Dynamic or Static

IP Source Guard

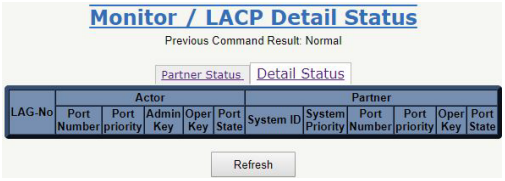
Use this screen to get IP Source Guard Binding status.



Operation	Query: • Select a Query Type (By Index, By VID & Index, or By Port & Index) • Fill the query condition. • Modify the query record range (Index range). • Click the “Query” button to query. Delete: • Select a Delete Type (All, By VID, or By Port). • Fill the delete conditions. • Click the “Delete” button to delete.
Field	**Description**
Index	Default: 1–100 Range: 1–150
Port	GE 1–28.
VID	VLAN ID: 1–4094.
IP Address	Format: xxx.xxx.xxx.xxx
MAC Address	Format: XX:XX:XX:XX:XX:XX
Type	Binding source state: It is static or dhcp-snooping.

LACP Status

Use this screen to display LACP data.



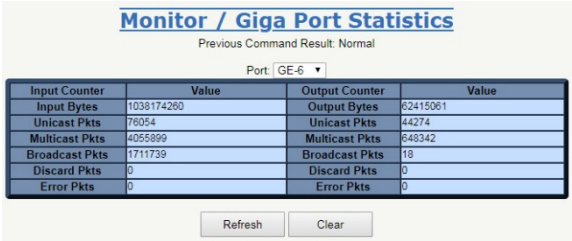
Operation	Refresh: • Click the “Refresh” button to query LACP Status data.
Field	**Description**
LAG-No	The index of the LACP aggregator. This specifies that the LAGs are processed by the LACP.

Actor Port Number	The port number assigned to the port. Assigned by an internal policy.
Actor Port Priority	The priority value assigned to the port, used to converge dynamic key changes.
Actor Admin Key	The administrative key value assigned to this port by an administrator or system policy. When the port is set to "auto", the key will be generated depending on the link speed of the physical port. When the port is set to "specific", a user can configure the key value within a range of 1 to 65535.
Actor Oper Key	The operational key value assigned to this port by the Actor.
Actor Port State	The operational values of the Actor's state parameters. This consists of the following set of variables, encoded as individual bits within a single octet, as follows: • LACP Activity is encoded in bit 0. Active LACP is encoded as a 1. Passive LACP is encoded as a 0. • LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1. Long Timeout is encoded as a 0. • Aggregation is encoded in bit 2. If TRUE (encoded as a 1), this flag indicates that the System considers this link to be Aggregatable. If FALSE (encoded as a 0), the link is considered to be Individual. • Synchronization is encoded in bit 3. If TRUE (encoded as a 1), the System considers this link to be IN_SYNC. If FALSE (encoded as a 0), then this link is currently OUT_OF_SYNC. • Collecting is encoded in bit 4. TRUE (encoded as a 1) means collection of incoming frames on this link is definitely enabled. Its value is otherwise FALSE (encoded as a 0). • Distributing is encoded in bit 5. FALSE (encoded as a 0) means distribution of outgoing frames on this link is definitely disabled. Its value is otherwise TRUE (encoded as a 1). • Defaulted is encoded in bit 6. If TRUE (encoded as a 1), it is using default operational Partner information, administratively configured for the Partner. If FALSE (encoded as a 0), the operational Partner information in use has been received in a LACPDU. • Expired is encoded in bit 7. If TRUE (encoded as a 1), it indicates that the Actor's Receive Machine is in the EXPIRED state. If FALSE (encoded as a 0), it indicates that the Actor's Receive Machine to receive is not in the EXPIRED state.
Partner System ID	The operational value of the MAC address component of the partner's system ID.
Partner System Priority	The operational value of the partner's system Priority of the Partner.
Partner Port Number	The operational value of the port number assigned to this link by the Partner.
Partner Port Priority	The operational value of the priority value assigned to this link by the Partner, used to converge dynamic Key changes.
Partner Oper Key	The operational value of the Key value assigned to this link by the Partner.
Partner Port State	The operational value of the Actor's view of the current values of the Partner's state parameters. The value consists of the following set of variables, as described in "Actor Oper Key".

Actors refer to the transmitting link (i.e. the LACP trunk on the device).
Partner refers to the receiving link (i.e. what is hooked up to the other end).

Port Statistics

Use this screen to display Giga Port Statistics.



Operation	Refresh: • Select the Port to be displayed. • Click the “Refresh” button to refresh the port data. Clear: • Select the port to be cleared. • Click the “Clear” button to clear the port data.
Field	**Description**
Port	Range: GE 1–28.
Input Bytes	The total number of octets received on the interface, including framing characters.
Input Unicast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-) layer, that were not addressed to a multicast or broadcast address at this sub-layer.
Input Multicast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-) layer, that were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses.
Input Broadcast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-) layer, that were addressed to a broadcast address at this sub-layer.
Input Discard Pkts	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Input Error Pkts	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
Output Bytes	The total number of octets transmitted out of the interface, including framing characters.
Output Unicast Pkts	The total number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
Output Multicast Pkts	The total number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
Output Broadcast Pkts	The total number of packets that higher-level protocol requested be transmitted that were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Output Discard Pkts	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Output Error Pkts	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

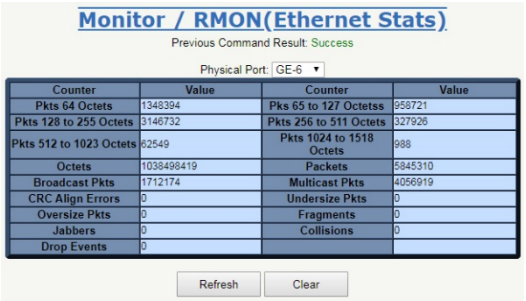
Ring & Chain

Use this screen to view a status overview for all of RingV2 status.

Operation	Refresh: • Click the “Refresh” button to refresh current data.
Group Index	The group number of the ring.
Mode	Indicates whether the group is enabled.
State	When the ring is complete, State will display "Normal”. When the ring is incomplete (at least one link is down), State will display "Fail".
Role	Indicates the role for which the group is configured.
Ring Port(s)	Describes the current status of the ring port(s).

RMON

Use this screen to read or clear Ethernet counters of ports.

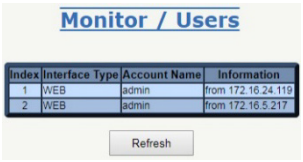


Operation	Refresh: • Select the Physical Port to be refereshed. • Click the “Refresh” button to query and refresh the current counters displayed. Clear: • Select the Physical Port to be cleared. • Click the “Clear” button to clear the port counter data (reset counters to 0).
Field	**Description**
Pkts 64 Octets	Total number of packets (including bad packets) received that were 64 octets in length.
Pkts 65 to 127 Octets	Total number of packets (including bad packets) received that were between 65 and 127 octets in length.
Pkts 128 to 255 Octets	Total number of packets (including bad packets) received that were between 128 and 255 octets in length.
Pkts 256 to 511 Octets	Total number of packets (including bad packets) received that were between 256 and 511 octets in length.
Pkts 512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length.
Pkts 1024 to 1518 Octets	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast Pkts	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Pkts	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, 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 Pkts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Pkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and 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).
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and 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).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is just the number of times that this condition has been detected.

Users

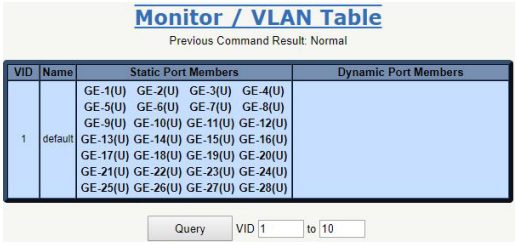
Show users currently logged on the system. The list displayed contains the following information.



Operation	Refresh: • Click the “Refresh” button to refresh current data.
Field	**Description**
Index	Shows the index of login user list.
Interface Type	Shows the mode of access. Possible values: Console, CLI, or Web.
Account Name	Shows the account name of the user.
Information	Shows more information about the user, including the IP address of the management host.

VLAN Table

Display the VLAN learning table.

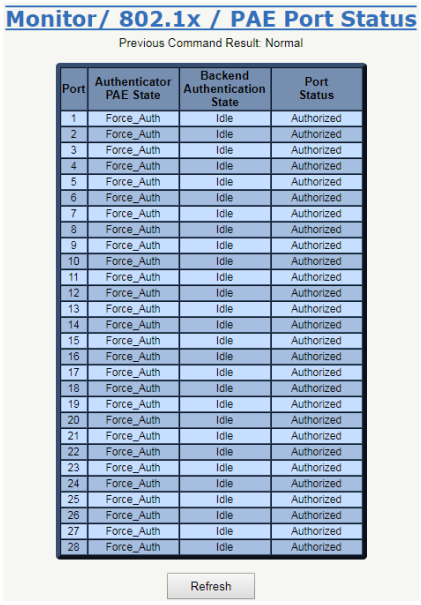


Field	Description
VID	VLAN ID Default: 1-10 Range: 1-4094
Name	Name of the VLAN ID.
Static Port Members	The port members joined on the VLAN through manual settings.
Dynamic Port Members	The port members that the VLAN learns through GVRP.

802.1X

PAE Port Status

Display the status of the Radius client.

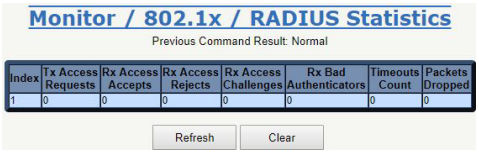


Operation	Refresh: Click the “Refresh” button to refresh current data. **Note:** If System AuthControl is disabled under Configuration→802.1X→PAE Port→PAE, the message “System auth control is disabled” will appear on this screen.
Field	**Description**
Port	The index of PAE Ports: Value Range 1–28.
PAE State	The Authenticator status of the PAE port: Possible state: Initialize Disconnected Authenticating Authenticated Aborting Held Force Auth Force Unauth
Backend State	The backend Authenticator status of PAE port. Possible state: Initialize Idle Request Response Success Fail Timeout Ignore

Port Status	The authentication status of PAE port. Possible state: Authorized/Unauthorized
Re-Authenticate	Set Enable to force PAE port re-authenticate.

RADIUS Statistics

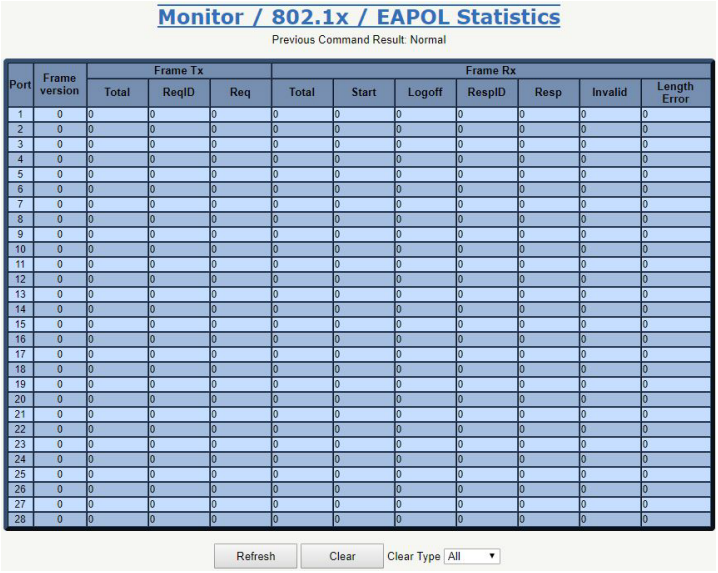
Receive or clear RADIUS statistics.



Operation	Refresh: • Click the “Refresh” button to refresh current data. Clear: • Click the “Clear” button to reset the counters.
Field	**Description**
Index	The index of RADIUS Server: Currently supports only one RADIUS server.
Tx Access Requests	The number of RADIUS Access-Requests sent to RADIUS server: Range: 0–65535.
Rx Access Accepts	The number of RADIUS Access-Accepts received from RADIUS server: Range: 0–65535.
Rx Access Rejects	The number of RADIUS Access-Rejects received from RADIUS server: Range: 0–65535.
Rx Access Challenges	The number of RADIUS Access-Challenges received from RADIUS server: Range: 0–65535.
Rx Bad Authenticators	The number of invalid RADIUS response packets received from RADIUS server: Range: 0–65535.
Timeout Count	The number of server Timeout occurrences on Backend Authentication state machine: Range: 0–65535.
Packets Dropped	The number of packets from RADIUS server that were silently dropped by Authenticator: Range: 0–65535.

EAPOL Statstics

Use the Monitor→802.1X→EAPOL Statistics counters of ports.

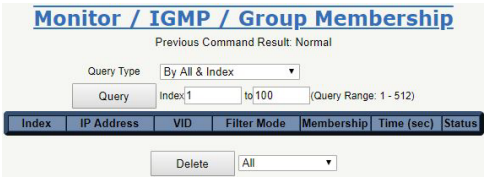


Operation	Clear: • Select “Clear Type”. • If clear type is “Port”, select the port number to be cleared. • Click the “Clear” button.
Field	**Description**
Port	The index of PAE port: Value range: 1–28.
Protocol Version	The protocol version number carried in the most recently received EAPOL frame. Range: 0–65535.
Total Frame Tx	The number of EAPOL frames of any type that have been transmitted. Range: 0–65535.
Req ID Frame Tx	The number of EAP Req/Id frames that have been transmitted. Range: 0–65535.
Req Frame Tx	The number of EAP Request frames (other than Req/Id frames) that have been transmitted. Range: 0–65535.
Total Frame Rx	The number of valid EAPOL frames of any type that have been received. Range: 0–65535.
Start Frame Rx	The number of EAPOL Start frames that have been received. Range: 0–65535.
Logoff Frame Rx	The number of EAPOL Logoff frames that have been received. Range: 0–65535.
Resp Id Frame Rx	The number of EAP Resp/Id frames that have been received. Range: 0–65535.
Resp Frame Rx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received. Range: 0–65535.
Invalid Frame Rx	The number of EAPOL frames that have been received by this Authenticator of which the frame type is not recognized. Range: 0–65535.
Length Error Frame Rx	The number of EAPOL frames that have been received by this Authenticator of which the Packet Body Length field is invalid. Range: 0–65535.

IGMP

Group Membership

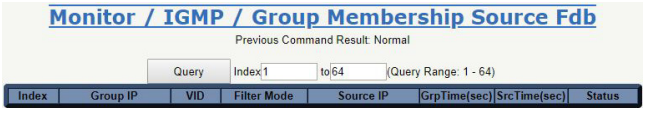
Display Group Membership status.



Operation	Query: • Select the “Query Type”. • Select the query record range (Index Range) • Click the “Query” button to query. Delete: • Select the Delete Type. • Fill VLAN ID when delete type is “By VID”. • Select one membership when delete type is “By Membership”. • Click the “Delete” button to delete selected data.
Field	**Description**
Index	Index Range: 1–512
IP Address	Group IP Address.
VID	VLAN ID Range: 1–4094
Filter Mode	Multicast FDB entry Filter Mode.
Membership	Bridge Port ID Range GE: 1–28.
Time	Remain Time: units in seconds
Status	Group Membership status: Dynamic or Static.

Group Membership Source Fdb

Display Group Membership status.



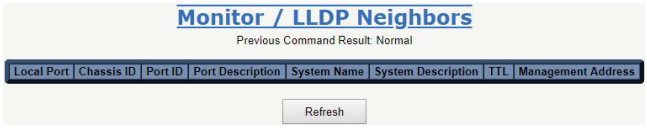
Operation	Query: • Select the query record range (Index Range). • Click the “Query” button to query.
Field	**Description**
Index	Multicast Source Fdb table. Max entry size: 64
Group ID	Multicast Source Fdb group IP address.
VID	Multicast Source Fdb VLAN ID: Range 1–4094
Filter Mode	Multicast Source Fdb Filter Mode: Include/Exclude. In Include mode, the GroupRemainTime has no timeout. In Exclude mode, the block list's source has no timeout.
Source IP	Source IP Address.
GrpTime (sec)	Group Remain Time: if “--“ is displayed, a time of zero is indicated.

SrcTime (sec)	Source Remain Time: if "--" is displayed, a time of zero is indicated.
Status	Multicast Source Fdb entry type: Allow or Block

LLDP

LLDP Neighbors

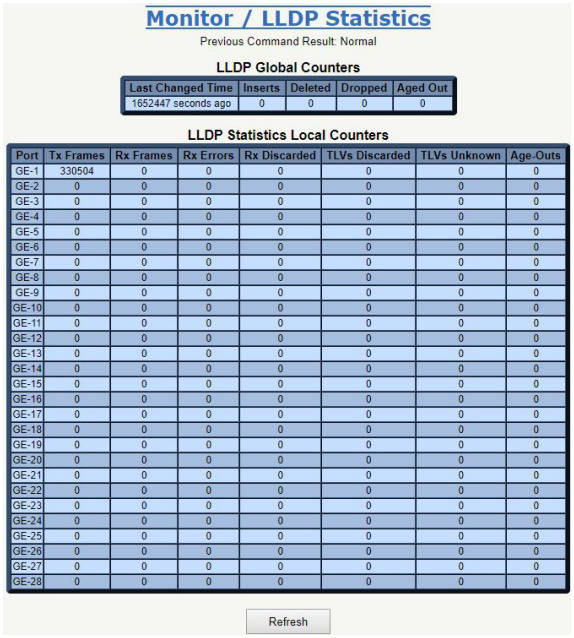
Display LLDP Neighbors information.



Operation	Refresh: • Click the "Refresh" button to refresh
Field	**Description**
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Port ID	The Port ID is the identification of the neighbor port.
Port Description	The port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.
System Description	System Description is the name advertised by the neighbor unit.
TTL	TTL (Time to live) is the remaining time of the remote information. And this valid period is set to TxHold multiplied by TxInterval (seconds).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. For instance, this could hold the neighbor's IP address.

LLDP Statistics

Display LLDP Global Counters, and LLDP Statistics Local Counters.

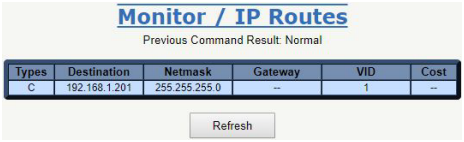


Operation	Refresh: • Click the “Refresh” button to refresh.
Field	**Description**
Last Changed Time	When neighbor entries were last changed.
Inserts	The total number of neighbor’s entry inserts.
Deleted	The total number of neighbor’s entries that were deleted.
Dropped	The total number of neighbor’s entries that were dropped.
Aged Out	The total number of neighbor’s entries that aged out.
Port	The port index.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Rx Discarded	The number of received LLDP frames discarded.
TLVs Discarded	The number of received LLDP TLVs discarded.
TLVs Unknown	The number of received LLDP TLVs unrecognized.
Age-Outs	The number of received LLDP frames Aged Out.

Layer 3

IP Routes

Display IP Route information.



Operation	To refresh the IP Routes Table: • Click the “Refresh” button.
Field	**Description**
Types	C – Connected S – Static R – RIP O – OSPF intra O/IA – OSPF inter O/E1 – OSPF external type 1 O/E2 – OSPF externam type2
Destination	The destination network address for the route.
Netmask	The netmask value for the route.
Gateway	The next hop address of the route.
VID	The VLAN ID where the route is learned on. Range: 1–4094.
Cost	The cost of the route.

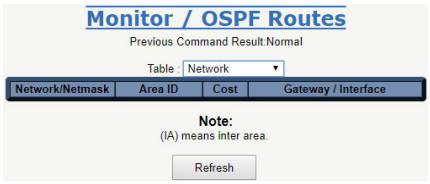
RIP Routes

Query or delete an RIP Route.

Operation	To refresh the RIP Routes Table: • Click the "Refresh" button. To delete RIP Route entry: • Select the RIP route entry(s). • Click the "Delete" button to delete the selected RIP Route entry(s). **Note:** Selection type is reserved for future use.
Field	**Description**
Destination	The destination network address for the RIP route.
Netmask	The network subnet mask for the RIP route.
Gateway	The next hop gateway address of the RIP route.
VID	The VLAN ID that is the Route the RIP packet comes from. Range: 1–4094
Metric	The metric of the route. Range: 1–16
Aging Time	The timeout value of the routing information timeout timer or garbage collection timer. Range: 0–3600 seconds.

OSPF Routes

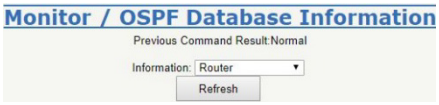
Display OSPF Routes data.



Operation	Refresh: • Select the Table type. • Click the "Refresh" button to get OSPF Routes data.
Field	**Description**
Table: Router	Router Address Area ID Cost Type Gateway/Interface
Table: Network	Network/Netmask Area ID Cost Gateway/Interface
Table: External	Network/Netmask Area ID Cost/Ext Cost Gateway/Interface

OSPF Database Information

Display OSPF Database data.



Operation	To Display OSPF Database Data: • Select the Information type. • Click the “Refresh” button to get OSPF database information data.
Field	**Description**
Information	Router/Network/Summary/ASBR Summary/ External/ NSSA External
Information: Router	Index: max 16 Link Connected Link ID Link Data Number of TOS Metrics TOS 0 Metrics
Information: Network	Network mask Attached Router
Information: Summary	Network mask TOS Metric
Information: ASBR Summary	Network mask TOS Metric
Information: External	Network mask TOS Metric Forward Address External Route Tag
Information: NSSA External	Network mask TOS Metric Forward Address External Route Tag

OSPF Neighbors

Display OSPF Neighbor data.

Operation	To Display OSPF Neighbor Data: • Click the “Refresh” button to display OSPF Neighbor information data.
Field	**Description**
Index	OSPF Neighbor Index.
Neighbor ID	OSPF Neighbor ID.
Priority	OSPF Neighbor Priority.
State	Display format NSM/ISM OSPF Neighbor NSM: DOWN/ Attempt/ Init/ To Way/ Exatart/ Loading/ Full OSPF Neighbor ISM: DOWN/ LoopBack/ Waiting/ Point to Point/ DRother/ Back Up/ DR
Dead Time	OSPF Neighbor Dead Timer.

Address	OSPF Neighbor Source.
Interface	OSPF Neighbor interface VLAN.

VRRP Group State

Display VRRP Group data.

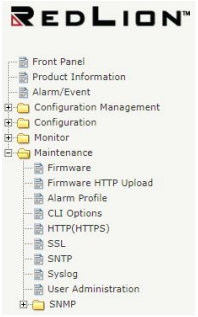
Operation	To Query All: • Select the Query Type “By All”. • Click the “Query” button to query VRRP Group State. To Query By VLAN Interface ID: • Select the Query Type “By VRRP Group ID”. • Select the VRRP Group ID range. • Click the “Query” button to query VRRP Group state data. To Query By VRRP Group ID: • Select the Query Type “By VRRP Group ID”. • Select the VRRP Group ID range. • Click the “Query” button to query VRRP Group state data.
Field	**Description**
Index	The index of VRRP.
Status	Display the VRRP Group number on which the VLAN interface and current VRRP State.
VLAN Interface	The identity for the VLAN Interface. Range: 1–4094.
VRRP ID	The VRRP Group ID.
Family Type	When VRRP is processing on V3, the VRRP group can be set to operate on IPv4 or IPv6. When VRRP is processing on V2, the VRRP group is always operating on IPv4.
Virtual Router Address	When the VRRP group is operating on IPv6, it can have one virtual link-local address and global IPv6 address. When the VRRP group is operating on IPv4, only one virtual IPv4 address is accepted.
Advertise-Interval	When VRRP is processing on V3, it can be setting in the range of 1–4095, unit is 0.01 second. Default value is 100. In other cases, it can be setting in the range of 1–255. Unit is 1 second. Default value is 1.
Priority	Range: 1–254. Default Value: 100.
Preemption	Range: Disabled / Enabled. Default Value: Disabled.
Learn Master’s adv-interval	This parameter is only available when VRRP is processing on V2. Default Value: Disabled.
Auth Mode	This parameter is only available when VRRP is processing on V2. Range: Disabled / Enabled. Default Value: Disabled. The auth key can be set in the range of 1–8 characters.

Track Object	Track Object: Track Object binding list. VRRP can bind a maximum of 64 track objects. Value Range: 1–64. Default value is 0. Before binding the specific track object, the track object must exist; if it does not exist, binding is impossible. Configuration example: ● Add Track Object: 1,2,3. ● To remove Track Object 2: change Track Object as 1,3. ● To remove all Track Objects: clear the Track Object to empty.

Chapter 6 Maintenance

This chapter lists the software menu tree maintenance related functions available for Red Lion® NT328G Switch models.

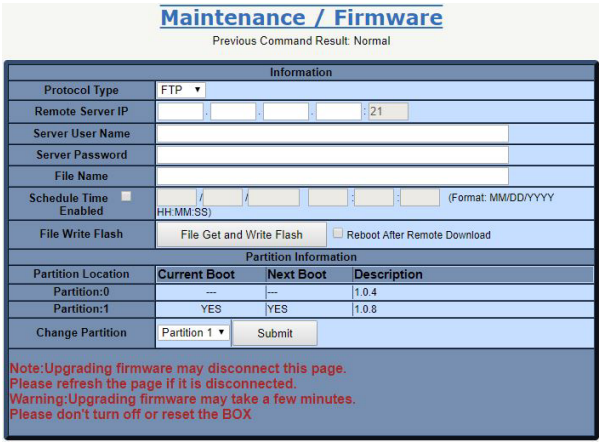
Maintenance Menu



Maintenance

Firmware

Upgrade switch firmware or swap firmware in the system.



Operation	Download New Firmware from a FTP Server: • Enter or select FTP Server IP Address, user name and password for login. • Select “Schedule Time” check box and set schedule (optional) • Click the “File Get and Write Flash” button to load firmware from the remote server IP. **Note:** The following message will be displayed if there are no exceptions or failures. “Remote download starts.....” and “previous command result” will display "Getting firmware image file (in progress)". While getting the firmware file is successful, the system will write the firmware to flash. The “previous command result” will display "Writing firmware image (in progress)". **WARNING:** The firmware upgrade/download (Flash Writing) process may take a few minutes. Do not turn off or reset the system during the process. Once the Flash Write process completes successfully, the system will restart automatically (if you selected the “Reboot After Remote Download” checkbox). Wait for the system to restart, then login to the Web GUI. Go to the System/ Firmware screen and check to see if the firmware update was successful. **Note:** The firmware will be loaded and written to a non-activated partition. If the Current Boot is in Partition 0, then the new firmware will be written in Partition 1.

	If “Reboot After Remote Download” is selected, the system will automatically restart. Swap Firmware Between Currently Running and Alternate Stored Firmware: • Verify that the firmware versions in Partition 0 and Partition 1, displayed in “Partition Information”, are different. • Click on the “Change Partition” drop-down list and select another partition (not Current Boot), then click “Submit” to apply. This action will not automatically restart the system, the system will boot with the selected partition when manually restarted). **WARNING:** System may take a few minutes to finish swapping firmware and reset. Do not reset the system or turn off the power while the system is swapping firmware.
Field	**Description**
Protocol Type	Transfer protocol for FTP or TFTP.
Remote Server IP	Type in the IP address of the FTP or TFTP server where the firmware is stored.
Server User Name	Type in a user name accepted by the FTP server.
Server Password	Type in a password accepted by the FTP server.
File Name	Type in the name of the firmware file (string length 1–64).
Schedule Time	Select Enable check box and type in the scheduled time to update the firmware file. The time format: MM/DD/YYYY HH:MM:SS
File Write Flash	After you have entered the FTP or TFTP server, user name, password and firmware file name, click File Get and Write Flash to start the firmware update process.
Reboot After Remote Download	Select the check box if you want the system to reboot automatically, once the firmware update is finished.

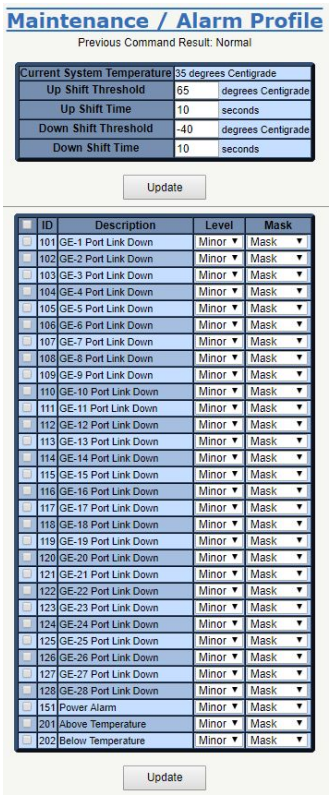
Firmware HTTP Upload

Upload firmware with HTTP.

Operation	To Upload Firmware: • Click the “Browse” button to select “config import file”. • Select the “Reboot after firmware upgraded” check box to reboot the system. • Click the “Upload” button to upload the firmware.

Alarm Profile

Modify the Alarm Profile.

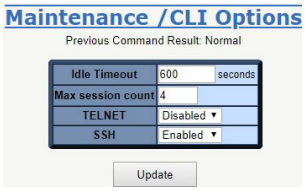


Operation	Modify Temperature Configuration: • Input “Up Shift Threshold”, “Up Shift Time”, “Down Shift Threshold” and “Down Shift Time”. • Click “Update”. Modify Alarm Profile: • Select the alarm entry to be modified with the associated check box. • Modify Level and Mask as required. **Note:** When any alarm exists, the Alarm LED will light and Alarm Output Relay will be enabled. • Click the “Update” button to update data settings.
Field	**Description**
Current System Temperature	Current System Temperature for monitoring purposes only.
Up Shift Threshold	Temperature threshold of the system’s high temperature alarm.
Up Shift Time	This is a time interval threshold used to determine if the alarm is on/set. If the system’s current temperature exceeds the "Up Shift Threshold" and remains so for duration of the "Up Shift Time", the alarm criteria will be met and the system will execute a high temperature alarm.
Down Shift Threshold	Temperature threshold of the system’s low temperature alarm.
Down Shift Time	This is a time interval threshold used to determine if the alarm is off/cleared. If the system’s current temperature is lower than the "Down Shift Threshold" and remains so for the duration of the "Down Shift Time", the alarm criteria will be met and the system will execute a low temperature alarm.
Field	**Description**
ID	Alarm Type ID.
Description	Alarm Type Description.

Level	The Alarm LED color is always red, regardless of whether or not the alarm is major or minor.
Mask	If the alarm is masked, then no alarm items will be captured in alarm history (current) or in an SNMP trap. A masked alarm item will not trigger the Alarm LED either on or off.

CLI Options

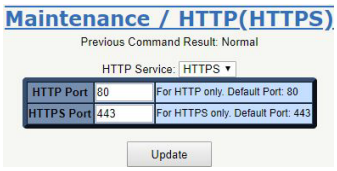
Define characteristics of the operational interface.



Operation	Modify: • Select the appropriate values for parameters • Click the “Update” button to apply any changes.
Field	**Description**
Idle Timeout	Specify the timeout (in seconds) for the operational interface. The session will be closed when the idle time exceeds this timeout value. Value range: 60–65535. A value setting of 0 disables the timeout feature.
Max session count	Specify the maximum allowed sessions for the CLI (command line interface): 1–10.
TELNET	To enable/disable TELNET on the system. Default setting of TELNET is disabled.
SSH	To enable/disable SSH on the system. Default setting of SSH is enabled.

HTTP (HTTPS)

Modify the HTTP(HTTPS) parameters.



Operation	Modify: • Select HTTP or HTTPS. • Change the port number if necessary. • Click the “Update” button to apply any changes. **Note:** The system allows selecting HTTP or HTTPS service. By default, HTTP is enabled, HTTPS is disabled. If HTTPS is selected, then HTTP is disabled.
Field	**Description**
HTTPS Service	HTTPS / HTTP. Default: HTTPS (HTTP disabled).
HTTPS Port	HTTPS service port. Range: 1–65535. Default Port: 443.
HTTP Port	HTTP service port. Range: 1–65535. Default Port: 80.

SSL

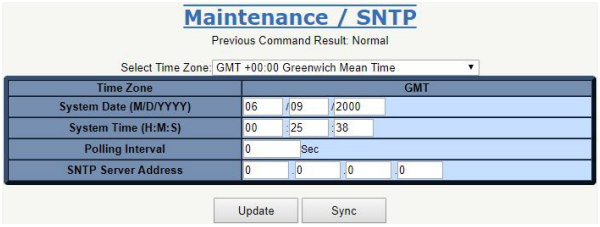
Modify the SSL Certificate setting. The SSL certificate is used to encrypt HTTPS and SSH communications.

This page provides two ways to show the current SSL Certificate - encrypted and decrypted, both of which can be selected by the radio buttons on the page. If any SSL certificate exists, it should be displayed. If no SSL certificate has been uploaded to the system, the screen will display the default certificate.

Operation	Use Default Certificate: • Click the “Use Default Certificate” button. • The system will delete any uploaded certificate, if one has been uploaded. • After deletion, the system will display the default SSL certificate. Upload New: • Click the “Upload New” button. • Copy and paste both Private Key (privatekey) and Self-Signed SSL Certificate (cert) in the input area. • The certificate must be in PEM formatting as follows, otherwise the attempted upload will fail: -----BEGIN RSA PRIVATE KEY----- .... -----END RSA PRIVATE KEY----- -----BEGIN CERTIFICATE----- .... -----END CERTIFICATE----- Regenerate New Certificate: • Click the “Regenerate” button. • The system will regenerate and upload a new certificate. • After successful regeneration, the system will display the new SSL certificate.

SNTP

Establish the address of a Simple Network Time Protocol (SNTP) server. The server is queried to establish the system date and time at startup and to update the SNTP server at specified intervals.



Operation	Modify: • Modify the configuration settings. • Click the “Update” button to modify any changes to the data. Sync: • Click the “Sync” button to manually synchronize the system time from the SNTP server.
Field	**Description**
Select Time zone	Sets the local time zone with Time Zone list. Sixty-six of the world's time zones are available (includes those using standard time and summer/daylight savings time).
System Date	Sets system date (mm/dd/yyyy).
System Time	Sets system time (hh:mm:ss).
Polling Interval	Sets polling interval (seconds) that the SNTP client will sync with the designated SNTP server.
SNTP Server address	Sets SNTP server IP address for your system.

Syslog

Configure the IP address of the syslog server which listens for incoming syslog messages. The system supports UNIX syslog functionality per RFC 3164. The syslog messages are sent via UDP and the source port number is 1027. All events/alarms defined in Appendix Table A-1 and Table B-1 will trigger the system to send syslog messages to the provisioned syslog server. The syslog message is formatted as follows:

For events:

<timestamp> <process name>: Event: <event description>: <position>

Example: Apr 1 08:25:31 oamp: Event: Gigabit Ethernet Loss of Signal: GBE 1

For alarms:

<timestamp> <process name>: Alarm Set: <alarm description>: <position>

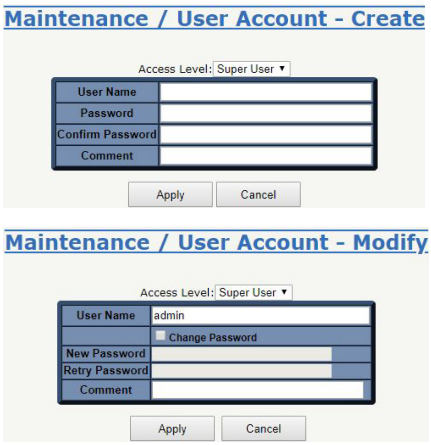
Or

<timestamp> <process name>: Alarm Clear: <alarm description>: <position>

Example: Apr 1 08:24:36 oamp: Alarm Clear: Gigabit Ethernet Loss of Signal: GBE 1

Operation	Modify: • Select Enabled/Disabled option for Syslog function. • Enter the Syslog Server Address. • Click the “Update” button to save changes.
Field	**Description**
Status	Value is Enabled/Disabled. Default: Disabled. Controls the Syslog Server when enabled.
Current Server IP	Current Syslog Server IP address.
Syslog Server Address	New Syslog Server IP address. The server must be a remote host.

User Administration

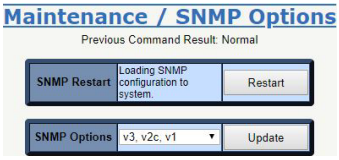


Operation	Create: • Click the “Create” button to create a new user. • Fill in User Name, Access Level, Password, Confirm Password and Comment fields. • Click “Apply” to create the new user account or click the “Cancel” button to cancel creation. Delete: • Select one row of data for deletion. • Click “Delete” to delete the selected data. Modify: • Select one row of data for modification. • Click the “Modify” button to modify the user account. • Select the “Change Password” check box to change the password. • Fill in the User Name, Access Level, New Password, Retry Password and Comment fields.
Field	**Description**
User Name	Shows the user name (up to 32 characters).
Access Level	Shows the access level of the user: Super User - The user can access all functions. Engineer - The user can access all functions except user account management. Guest - The user can access basic display functions.
Password	Enter a login password of 0–31 characters.
Confirm Password	Enter the login password from the previous field again.
Comment	Description of the user account (up to 31 characters).

SNMP

Options

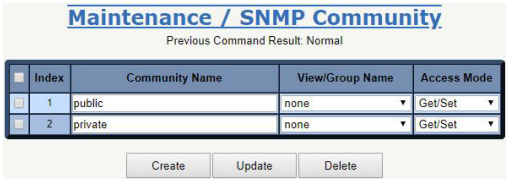
Modify the SNMP Options.



Operation	SNMP Restart: • SNMP changes are not applied to the system until the system is restarted. It may take several seconds to load the SNMP settings after a restart implements any modifications. SNMP Options/Update: • This enables or disables SNMP versions v3, v2c or v1. If SNMP Options is set to “Disable”, the system will use SNMPv2c parameters only. If SNMP v3, v2c, v1 is selected, the system can use versions v3, v2c or v1 parameters. If SNMP v2c, v1 is selected, the system can use SNMP v2c or v1 parameters. Changing this selection restarts SNMP automatically after clicking on Update. SNMPv3 parameters are valid only if SNMP v3, v2c, v1 is selected.

Community

Configure a SNMP Community.
All SNMP configuration changes are applied to the system after SNMP is restarted.

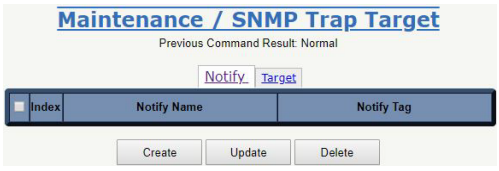


Operation	Create Community: • Click the “Create” button. • When the “Maintenance / SNMP Community – Create” dialog box appears, fill in the Community name and pick the appropriate View/Group Name and Access Mode. • Click the “Apply” button to create the new Community. Update Community Entry: • Select entry to be updated by clicking the associated check box. • Modify the data fields as desired. • Click the "Update” button to apply any changes. Delete Community Entry: • Select the entry for deletion by clicking the associated check box. • Click the “Delete” button. **Note:** This page supports multi-selection, multiple items can be selected for deletion. Users can also choose the select all check box to delete all items.
Field	**Description**
Index	SNMP Community index. The system supports up to 32 Community data records.
Community Name	SNMP Community Name for SNMP v1/v2c. SNMP request is only received if Community Names match. Community Name max length is 31 characters.
View/Group Name	View and Group are used for SNMPv3 only. A community can Bind one of the view or group names. If it does not Bind a view or group name, the community will be treated as a v1/v2c community. If it does Bind a view or a group name, the community will be treated as a v3 community. The v2c and v3 communities can exist in the community table concurrently. "Unknown (name)” will be displayed when view/group name doesn't exist in view/ group table.
Access Mode	Choose the access method. Allow Get operation only, or allow both Get and Set.

Trap Target

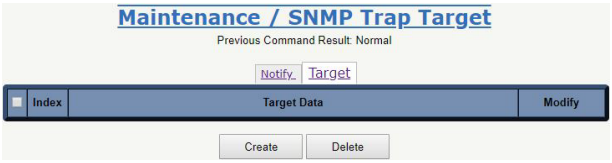
Configure the SNMP notify and target table.
All SNMP configuration changes are applied to the system after SNMP is restarted.

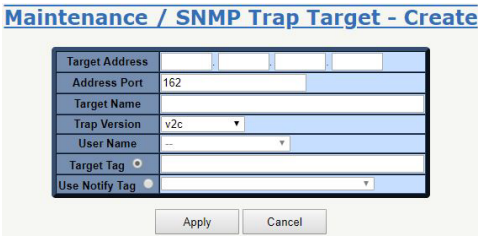
SNMP Notify



Operation	Create SNMP Trap Target Notification: • Click the “Create” button to create a new notify tag. • Fill in notify name and notify tag. • Click “Apply” to create, or “Cancel” to abort. Modify SNMP Trap Target Notification: • Select entry by clicking the associated check box. • Modify any field data as desired. • Click the “Update” button to apply any changes. Delete SNMP Trap Target Notification: • Select entry by clicking the associated check box. • Click the “Delete” button to delete the selected item.
Field	**Description**
Index	SNMP notify tag index. The system supports up to 32 notify tags.
Notify Name	Name of Notify entry. Notify Name max length is 31 characters.
Notify Tag	Notify Tag string. If the tag of the Target entry matches any tags of the Notify Table, then the SNMP trap function will work. Notify Tag max length is 31 characters.

SNMP Target



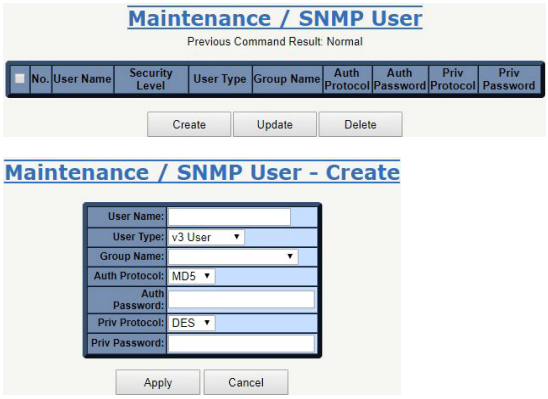


Operation	Create SNMP Trap Target: • Click the “Create” button to create a new SNMP Trap Target. • Fill in Target IP Address, Address Port number, Target Name, and Target Tag. Select the Trap Version and Use Notify Tag. • Click “Apply” to create, or “Cancel” to abort. Modify SNMP Trap Target: • Click the row item “Modify” button to modify target data. Delete SNMP Trap Target: • Select entry by clicking the associated check box, then click “Delete”. **Note:** This page supports multi-selection. Multiple items may be deleted at a time. Users can also click the select all check box to delete all target items.
Field	**Description**
Index	SNMP target index. The system supports up to 32 target entries.
Target Address	Target IP address. The host IP address of trap receiver. Value range 0.0.0.0–255.255.255.255
Address Port	Target Address port number. TCP Port number of trap receiver. Range: 1-65535. Default is 162
Target Name	Name of target. Target Name max length is 31 characters.

Trap Version	Select SNMP trap version. Supports v1/v2c/v3.
Target Tag	Add a target tag or pick up existing notify tag from Notify Table.
Use Notify Tag	Click the ratio button to use the notify tag.

User

Receive/configure a SNMPv3 user account.
All SNMP configuration changes are applied to the system after SNMP is restarted.



Operation	Create New SNMPv3 User: • Click the “Create” button. • When the “Maintenance / SNMP User – Create” dialog box appears, fill in the “User Name” and select “User Type”, “Auth Protocol” and “Priv Protocol”. • Enter the authorization password in the “Auth Password” field. Works only if SNMPv3 is enabled. • Create the user account password in the “Priv Password” field. User Privacy protocol works only if SNMPv3 is enabled. If “Priv Protocol” is not “None”, then “Priv Password” must be input. • Click the “Apply” button to create the new user account. Modify: • Select the user account to be modified in the user account table by clicking the associated check box. • Modify the desired user account field(s). • Click the “Update” button. Delete: • Select data to be deleted in the user account table by clicking the associated check box. Multiple rows of data may be selected and deleted at a time. • Click the “Delete” button to delete the selected user account(s)
Field	**Description**
User Name	User name: length 1–31 characters. Accepts all characters except: spaces, quotation marks, and question marks.
User Type	SNMPv3 user type. Options: • Read Only • Read Write • v3 User If “User Type” is “v3 User”, the “Group Name” should be provided. No matter which User Type is selected, authentication and Privacy options are accessible.
Group Name	Access Group name, length: 1–15 characters. Accepts all characters except: spaces, quotation marks, and question marks. If the user’s type is "Read Only" or "Read Write", then this field is irrelevant.
Auth Protocol	User authentication protocol. Works only if SNMPv3 is enabled. Options: • None • MD5 • SHA

	"Auth Protocol" can be set to something other than “None” and "Priv Protocol” can be set to "None". If "Auth Protocol" is "None", then "Priv Protocol” is "None". If "Auth Protocol" is MD5 or SHA, then "Auth Password" must be input.
Auth Password	Authentication password: length 8–15 characters. Works only if SNMPv3 is enabled. Accepts all characters except: spaces, quotation marks, and question marks. If the Authentication Protocol is "None", then Privacy options are irrelevant.
Priv Protocol	User Privacy protocol: works only if SNMPv3 is enabled. If "Priv Protocol" is not "None", then "Priv Password" must be input. Options: • None • DES • AES
Priv Password	Privacy password: length 8–15 characters. Works only if SNMPv3 is enabled. Accepts all characters except: spaces, quotation marks, and question marks. If "Priv Protocol" is "None", then “Priv Password” is irrelevant.

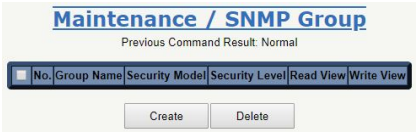
Group

Create/configure an SNMP View-based Access Control Model (VACM) group. All SNMP configuration changes are applied to the system after SNMP is restarted.

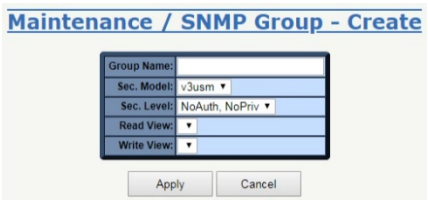
SNMP VACM Group represents the Access Group of SNMPv3 VACM View. This page allows the user to create/ delete a group.

Each group can use the v1/v2c/v3usm model. When using the v3usm model an SNMP Access Group can bind with the Security Level. Read/Write View can be used for access control. If selecting v1/v2c the group is represented as a community-based group. It can be bound in Read/Write View, but without a Security Level.

Note: A community can be bound with a single view or a group (read/write view).



Create



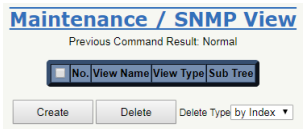
Operation	Create New: • Click the “Create” button to create new SNMP VACM group. • Fill in the “Group Name” field and select “Sec. Model”, "Sec. Level”, “Read View” and “Write View”. • Click the “Apply” button. **Note:** max group entry: 32 Delete: • Select a row in the VACM group table for deletion by clicking the associated check box. Multiple rows may be selected and deleted at a time. • Click the “Delete” button to delete the selected group(s).
Field	**Description**
Group Name	Group name: length 1–15 characters. Accepts characters except: spaces, quotation marks, and question marks.
Security Model	SNMP security model. Options: • v1: Supports Read/Write View. • v2c: Supports Read/Write View. • v2usm: Supports Read/Write View & Security Level.

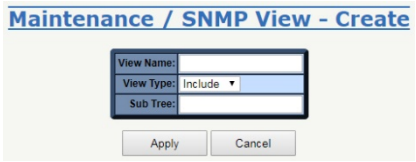
Security Level	User security level. If "Security Model" is "v1" or "v2c", the field is not used and will display as "--". Security level status: • NoAuth, NoPriv (No Authentication and no Privacy) • Auth, NoPriv (Authentication and no Privacy) • Auth, Priv (Authentication and Privacy)
Read View	Access View for Read (snmp-get) Select from the view list. If the list is empty, an access view must be created using page "SNMP View" page first. It will display "Unknown (xxxx)" when the name of xxxx doesn't exist in view name.
Write View	Access View for Write (snmp-set) Select from the view list. If the list is empty, an access view must be created using page "SNMP View" page first. "Unknown(xxxx)" will display when the name of xxxx doesn't exist in the view name.

View

Create/configure SNMP View-based Access Control Model (VACM) View. All SNMP configuration changes are applied to the system after SNMP is restarted.

SNMP View represents the Access View of SNMPv3 VACM View. This page allows a user to have multiple views with the same view name. Usually, these views would have a different view type and subtree.





Operation	• Click the “Create” button to create the new view. • Fill in “View Name” and “Sub Tree” fields, then select the “View Type”. • Click the “Apply” button to create the new view or the “Cancel” button to exit without saving. **Note:** max group entry: 32 Delete: • Select a row in the VACM view table for deletion by clicking the associated check box. Multiple rows may be selected and deleted at a time. • Click the “Delete” button to delete selected user account(s). VACM View can be deleted by Name or by Index. **Note:** If a SNMP View is deleted by name, all entries with the same name will also be deleted.
Field	**Description**
View Name	View name: length 1–15 characters. Accepts all characters except: spaces, quotation marks, and question marks.
View Type	Accessible/Not Accessible of object (SNMP OID). Selection box options: • Include: allows access to the subtree/OID; • Exclude: doesn’t allow access to the subtree/OID. **Note:** the OID is a prefix and there is no need to match it exactly. Example: 1.3.6.1.2.1 (include): means 1.3.6.1.2.1.* are accessible. Example: 1.3.6.1.2.1 (exclude): means 1.3.6.1.2.1.* are NOT accessible. An example of wildcard(*): 1.3.6.1.*.1 (include), means that 1.3.6.1.4.1.* are accessible and 1.3.6.1.2.1.* are accessible.

Sub Tree	SNMP OID or Object Name of MIB Input format is OID, character length 1-31. Accepts MIB object name "iswitch", or wildcard (*). **Note:** iswitch represents 1.3.6.1.4.1.5833.2012 (this is just an example, please refer to the actual OID designed for the product.) Example: 1.3.6.1.2.1 1.3.6.1.4.1.5833.2012 iswitch.1 iswitch.2.6.1.1.*.4 (iswitch.2.6.1.1 is EthernetPort Entry, it means this view includes/excludes the 4th port of the table.)

Chapter 7 Routing Configuration

This chapter provides procedures for configuring Red Lion NT328G Switch models.
The procedures include configuration applications for:

- VLAN
- Ring Version 2
- QoS
- RIP Routing
- OSPF Routing
- VRRP

VLAN Configuration

Introduction

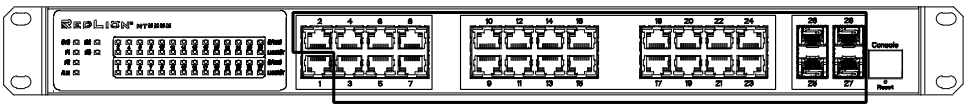
This section provides a guide on how to configure Virtual LANs (VLANs) in the Red Lion NT328G Switch models, including DHCP and Layer 3.

The switch supports up to 60 VLANs. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received on a VLAN can only be forwarded within that VLAN, and multicast and unknown unicast frames are flooded only to ports in the same VLAN.

Example 1: Default VLAN Settings

Each port in the switch has a PVID, which is a configurable default VLAN number. This places all ports on the same VLAN by default, although each PVID is configurable to any VLAN number between 1 and 4094.

The default configuration settings for the switch have all ports set as untagged members of VLAN 1, with all ports configured as PVID=1. In the default configuration example shown below, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID=1).



Port 1
Incoming untagged packets

- DA
- SA
- Data
- CRC

Ports 2-10
Outgoing untagged packet (unchanged)

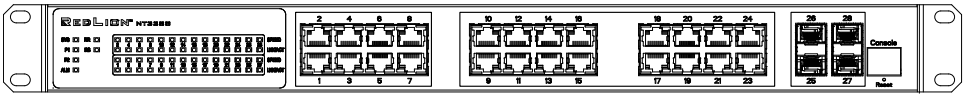
- CRC
- Data
- SA
- DA

Key
By default:

- All ports are assigned PVID=1
- All ports are untagged members of VLAN1

Example 2: Port-based VLANs

When the switch receives an untagged VLAN packet it will add a VLAN tag to the frame according to the PVID setting on the port that received the untagged packet. As shown in the image below, the untagged packet is marked (tagged) as it leaves the switch through Port 2, which is configured as a tagged member of VLAN100. The untagged packet remains unchanged as it leaves the switch through Port 7, which is configured as an untagged member of VLAN100.



Port 1
Incoming untagged packets

- DA
- SA
- Data
- CRC

PVID=1

Port 2
Tagged member of VLAN 100

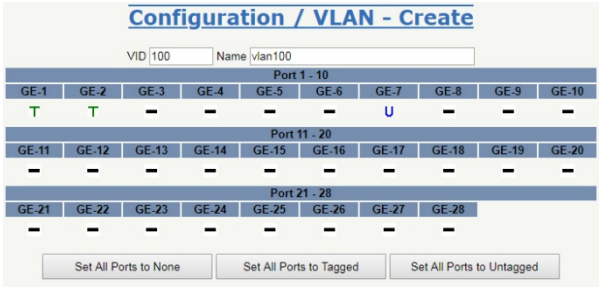
Port 7
Untagged member of VLAN 100

Configuration

1. Go to Configuration→Port Configuration→Bridge Port and configure PVID 100 on Port 1, Port 2, and Port 7.

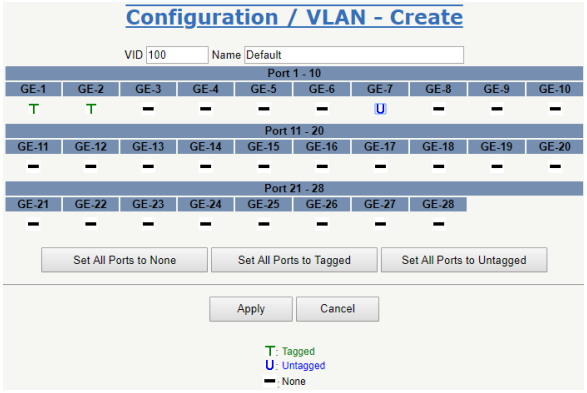
	Port	PVID	Default Priority	Accept Frame Type
☐	GE-1	100	0	All
☐	GE-2	100	0	All
☐	GE-3	1	0	All
☐	GE-4	1	0	All
☐	GE-5	1	0	All
☐	GE-6	1	0	All
☐	GE-7	100	0	All
☐	GE-8	1	0	All
☐	GE-9	1	0	All
☐	GE-10	1	0	All
☐	GE-11	1	0	All
☐	GE-12	1	0	All
☐	GE-13	1	0	All
☐	GE-14	1	0	All
☐	GE-15	1	0	All
☐	GE-16	1	0	All
☐	GE-17	1	0	All
☐	GE-18	1	0	All
☐	GE-19	1	0	All
☐	GE-20	1	0	All
☐	GE-21	1	0	All
☐	GE-22	1	0	All
☐	GE-23	1	0	All
☐	GE-24	1	0	All
☐	GE-25	1	0	All
☐	GE-26	1	0	All
☐	GE-27	1	0	All
☐	GE-28	1	0	All

2. Select Configuration→VLAN→Static VLAN. Create a VLAN with VLAN ID 100. Enter a VLAN name in the Name field.



3. To assign a VLAN tag setting to a port or to remove it from a port, toggle the check box under an individual port number. The tag setting determines whether or not packets are transmitted from the port tagged or untagged with the VLAN ID. The possible tag settings are:
   T Specifies that the egress packet is tagged for the port.
   U Specifies that the egress packet is untagged for the port.
   - Specifies that the port is not part of the VLAN.

Here we set tagged VLAN100 on Port 1 and Port 2 and untagged VLAN100 on Port 7.



4. Transmit untagged unicast packets from Port 1 to Port 2 and Port 7. The switch will tag any egressing packet with VID 100. These packets have access to Port 2 and Port 7. Outgoing packets are stripped of their tags to leave Port 7 as untagged packets. For Port 2, the outgoing packets leave as a tagged packet with VID 100.
5. Transmit untagged unicast packets from Port 2 to Port 1 and Port 7. The switch should tag the packets with VID 100. The packets have access to Port 1 and Port 7. The outgoing packets are stripped of their tags to leave Port 7 as untagged packets. For Port 1, the outgoing packets leave as tagged packets with VID 100.
6. Transmit untagged unicast packets from Port 7 to Port 1 and Port 2. The switch should tag the packets with VID 100. The packets have access to Port 1 and Port 2. For Port 1 and Port 2, the outgoing packets leave as tagged packets with VID 100.
7. Repeat step 4 using broadcast and multicast packets.

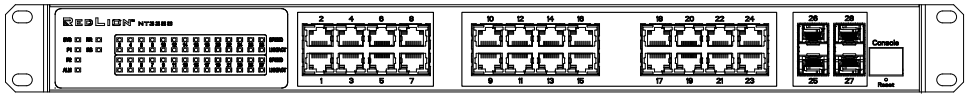
CLI Command

```
enable
configure
interface gigabit 1
default vlan 100
vlan 100 tag
exit
interface gigabit 2
default vlan 100
vlan 100 tag
exit
interface gigabit 7
default vlan 100
vlan 100 untag
exit
exit
exit
```

Example 3: IEEE 802.1Q Tagging

The switch is able to construct Layer 2 broadcast domain by identifying VLAN ID specified by IEEE 802.1Q. It forwards a frame between bridge ports assigned to the same VLAN ID and can set multiple VLANs on each bridge port.

In the following figure, the tagged incoming packets are assigned directly to VLAN 100 and VLAN 200 because of the tag assignment in the packet. Port 2 is configured as a tagged member of VLAN 100 and Port 7 is configured as an untagged member of VLAN 200. Hosts in the same VLAN communicate with each other as if they in a LAN. However, hosts in different VLANs cannot communicate with each other directly.



Port 1 (Group A)
Tagged packet
- VID=100
- VID=200
  - CRC*
  - Data*
  - Tag*
  - SA*
  - DA*

* Before

Port 2
Tagged member of VLAN 100

Port 7 (Group B)
Untagged member of VLAN 200

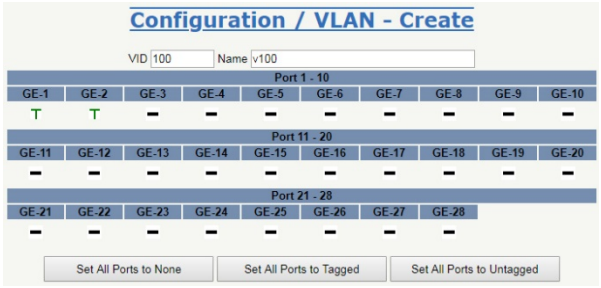
Key
- Group A (VLAN100): Port 1 & Port 2
- Group B (VLAN 200): Port 1 & Port 7

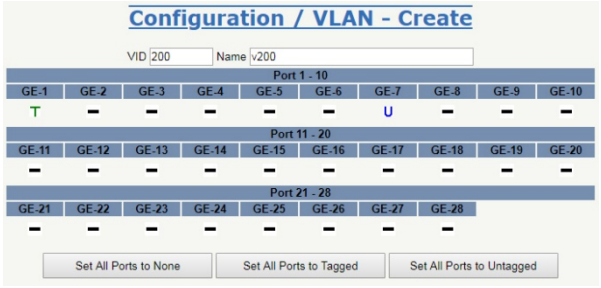
In this case:
1. The hosts from Group A can communicate with each other.
2. The hosts from Group B can communicate with each other.
3. The hosts of Group A and Group B can't communicate with each other.
4. Both Group A and Group B can connect to the Internet through the switch.

Configuration

The Configuration/Static VLAN page specifies the VLAN membership as follows:

1. Transmit unicast packets with VLAN tag 200 from Port 1 to Port 2 and Port 7. The switch should tag the packets with VID 200. The packets only have access to Port 7. The outgoing packets on Port 7 are stripped of their tags as untagged packets.
2. Transmit unicast packets with VLAN tag 100 from Port 2 to Port 1 and Port 7. The switch should tag the packets with VID 100. The packets only have access to Port 1. For Port 1, the outgoing packets leave as tagged packets with VID 100.
3. Transmit unicast packets with VLAN tag 200 from Port 7 to Port 1 and Port 2. The switch should tag the packets with VID 200. The packets only have access to Port 1. The outgoing packets on Port 1 will leave as tagged packets with VID 200.
4. Repeat the steps above using broadcast and multicast packets.





CLI Command

enable
configure

```
vlan 100 v100
vlan 200 v200
interface gigabit 1
vlan 100 tag
vlan 200 tag
exit
interface gigabit 2
vlan 100 tag
exit
interface gigabit 7
vlan 200 untag
exit
exit
exit
```

Security Configuration

Introduction

This section describes the ACL function available for Red Lion NT328G Switch models.

The ACL function supports access control security for MAC address, IP address, Layer 4 Port and Type of Service. Each ACL has five actions: Deny, Permit, Queue Mapping, CoS Marking and Copy Frame. Users can set the default ACL rule to Permit or Deny.

For details regarding ACL function, see following table.

DEFAULT ACL RULE	ACTIONS				
	DENY	PERMIT	QUEUE MAPPING	COS MARKING	COPY FRAME
Permit	(a)	(b)	(c)	(d)	(e)
Deny	(f)	(g)	(h)	(i)	(j)

Table key:

a. Permit all frames, but deny frames set in ACL entry.

b. Permit all frames.

c. Permit all frames and do queue mapping of the transmitted frames.

d. Permit all frames and change CoS value fo the transmitting frames.

e. Permit all frames and copy frame which set in ACL entry to a defined GE port.

f. Deny all frames.

g. Deny all frames, but permit frames set in ACL entry.

h. Deny all frames.

i. Deny all frames.

j. Deny all frames, but copy frames which are set in ACL entry to a defined GE port.

Case 1: ACL for MAC Address

For MAC address ACL, ACL can filter for source MAC address, destination MAC address, or both. When it filters for both source and destination MAC addresses, only packets which meet both criteria will be filtered. In other words, ACL would not filter a packet with only a source or a destination address.

If a user wants to filter a one directional MAC address to only send or receive, the other MAC address should be set to zero. This signifies no preference.

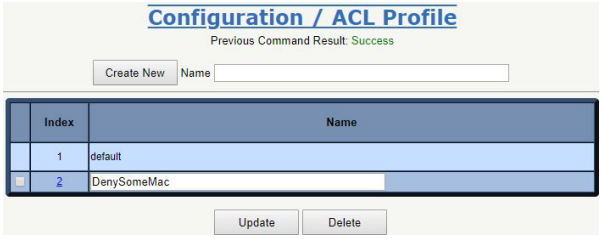
Besides MAC addresses, ACL also supports filtering for VLAN and Ether type. Certain VLANs or Ether types under these MAC addresses will be affected. If VLAN or Ether type filtering is not needed, all values should be set to zero. The following cases are examples regarding the table above.

Case 1(a):

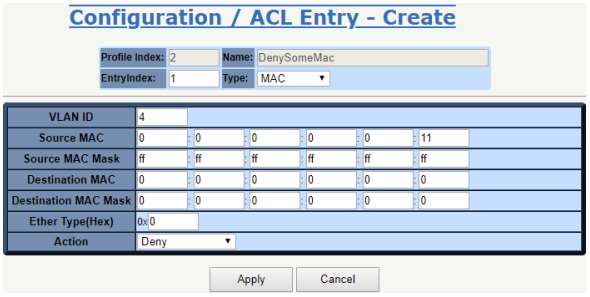
A user can set the default ACL Rule of GE port to “Permit”, then bind the port to a suitable profile with the “deny” action for ACL active. This allows the GE port to pass through all packets but does not allow an ACL entry of the profile binding.

One Directional MAC address with one VLAN deny filtering.

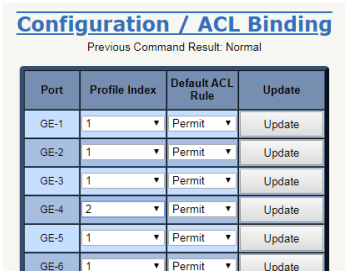
1. Create a new ACL Profile (Profile Name: DenySomeMac)



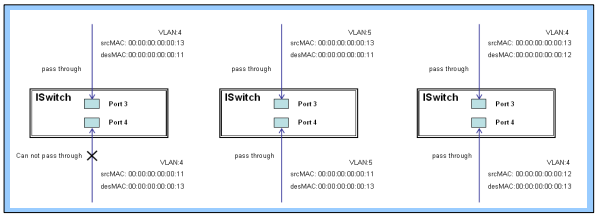
2. Create a new ACL Entry rule under this ACL profile. (Deny MAC: 11 and VLAN: 4)



3. Bind this ACL Profile to a GE port. (GE-4)



4. Send frames between GE-3 and GE-4 and observe the test results.



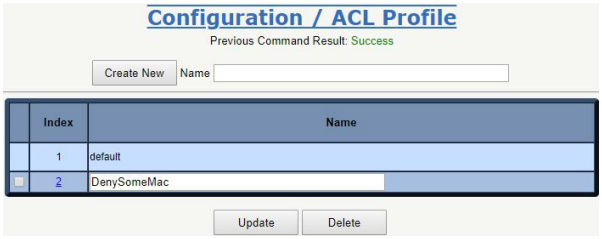
CLI Command

```
enable
configure
profile acl
acl-profile 2 create
acl-profile 2 set name denysomemac
acl-profile 2 create entry 1
acl-profile 2 set entry 1 mac-type set vlan 4
```

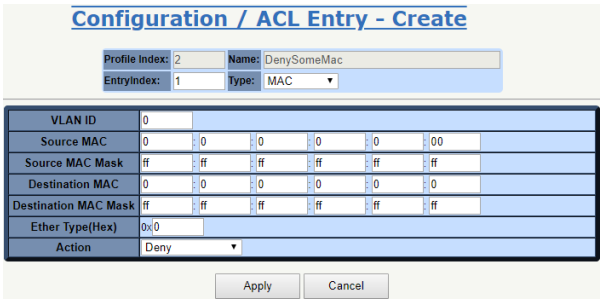
```
acl-profile 2 set entry 1 mac-type set srcmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
exit
vlan 4 v4
vlan 5 v5
interface gigabit 3
vlan 4 tag
vlan 5 tag
exit
interface gigabit 4
vlan 4 tag
vlan 5 tag
acl-profile-bind 2
exit
exit
exit
```

Two Directional MAC address with all VLAN deny filtering.

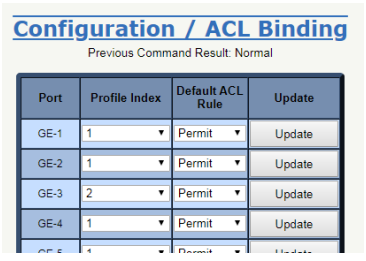
1. Create a new ACL Profile. (Profile Name: DenySomeMac)



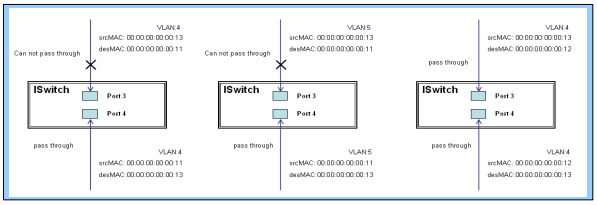
2. Create a new ACL entry rule under this ACL Profile. (Deny SrcMAC: 13 and DesMAC: 11)



3. Bind this ACL Profile to a GE port. (GE-3)



4. Send frames between GE-3 and GE-4 and observe the test results.



CLI Command

```
enable
```

```
configure
profile acl
acl-profile 2 create
acl-profile 2 set name DenySomeMac
acl-profle 2 create entry 1
acl-profile 2 set entry 1 mac-type set src mac 00:00:00:00:00:13 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 mac-type set dstmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
exit
vlan 4 v4
vlan 5 v5
interface gigabit 3
vlan 4 tag
vlan 5 tag
acl-profile-bind 2
exit
interface gigabit 4
vlan 4 tag
vlan 5 tag
exit
exit
exit
```

Case 1(b):

This case does not use an ACL function. All frames will pass through.

Case 1(c):

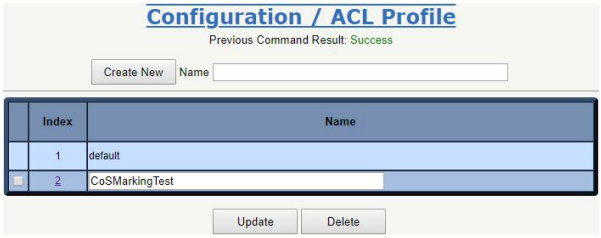
A user can set the default ACL Rule of a GE port to “Permit”, then bind a suitable profile with the “Queue Mapping” action as an ACL function active. This allows the GE port to use queue mapping 0–7 for the frames received from the port.

Case 1(d):

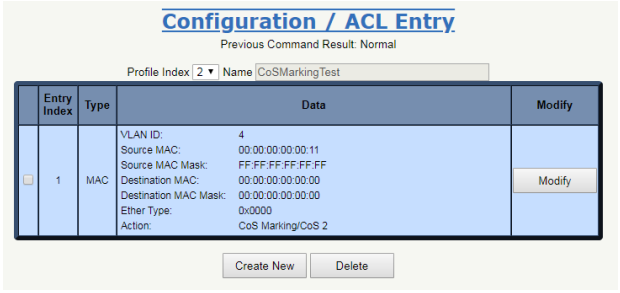
A user can set the default ACL Rule for a GE port to “Permit”, then bind the port to a suitable profile with the “CoS Marking” action as an ACL function active. This allows the GE port to mark the CoS of the VLAN frames received from the port.

One Directional MAC Address with CoS Marking Action. (set to one VLAN with no preference for Ether Type)

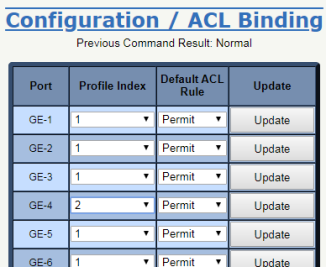
1. Create a new ACL Profile. (Profile Name: CoSMarkingTest)



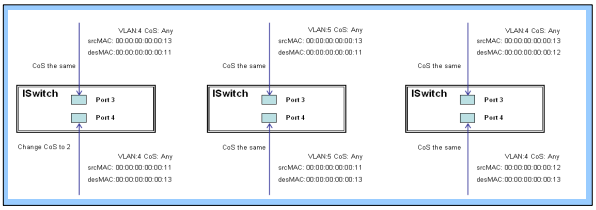
2. Create a new ACL Entry rule under this ACL Profile. (Filter SrcMAC: 11 and VLAN ID: 4 frame to CoS: 2)



3. Bind this ACL Profile to a GE port. (GE-4)



4. Send frames between GE-3 and GE-4 and observe the test results.



CLI Command

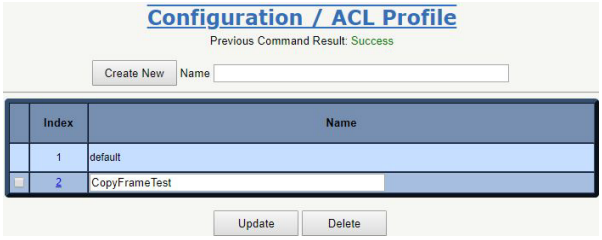
```
enable
configure
profile acl
acl-profile 2 create
acl-profile 2 set name CoSMarkingTest
acl-profile 2 create entry 1
acl-profile 2 set entry 1 mac-type set vlan 4
acl-profile 2 set entry 1 mac-type set srcmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 action cos 2
exit
vlan 4 v4
vlan 5 v5
interface gigabit 3
vlan 4 tag
vlan 5 tag
exit
interface gigabit 4
vlan 4 tag
vlan 5 v5
acl-profile-bind 2
exit
exit
exit
```

Case 1(e):

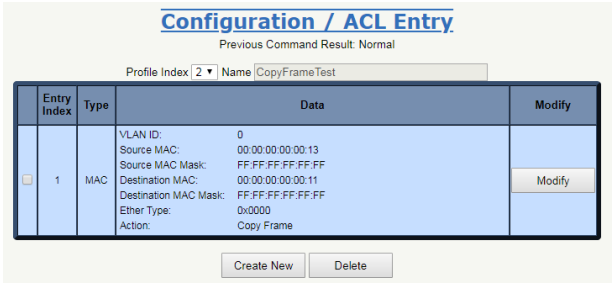
A user can set the default ACL rule for a GE port to “Permit”, then bind the port to a suitable profile with the “Copy Frame” action for active mirror analyzer. This allows the system to copy frames from the binding GE Port to an analyzer port.

Two Directional MAC Address with Copy Frame Action (No Preference for VLAN ID or Ether Type)

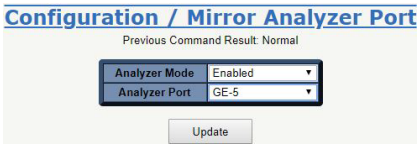
1. Create a new ACL Profile. (Profile Name: CopyFrameTest)



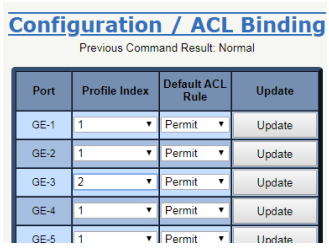
2. Create a new ACL Entry rule under this ACL Profile. (SrcMAC: 13 and DesMAC: 11)



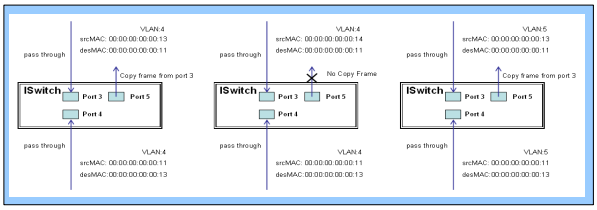
3. Set analyzer port to enable and mirror analyzer port.



4. Bind this ACL Profile to a GE port. (GE-3)



5. Send frames between GE-3 and GE-4 and observe the test results.



CLI Command

```
enable
configure
profile acl
acl-profile 2 create
acl-profile 2 set name CopyFrameTest
acl-profile 2 create entry 1
acl-profile 2 set entry 1 mac-type set srcmac 00:00:00:00:00:13 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 mac-type set dstmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 action copyframe
exit
vlan 4 v4
vlan 5 v5
interface gigabit 3
vlan 4 tag
```

vlan 5 tag
acl-profile-bind 2
exit
interface gigabit 4
vlan 4 tag
vlan 5 tag
exit
mirror analyzer-port enable
mirror analyzer-port 5
exit
exit
exit

Case 1(f):

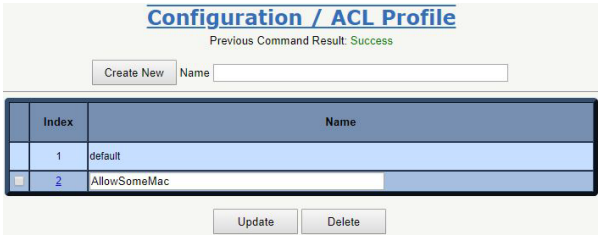
In this case, no frames will pass through.

Case 1(g):

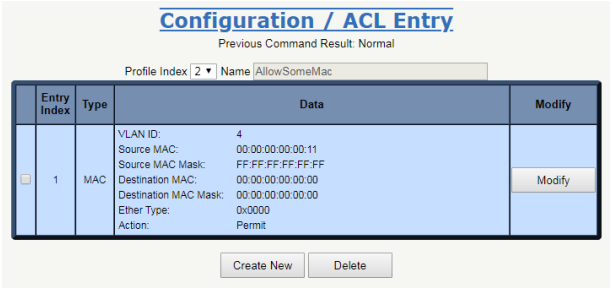
A user can set the default ACL Rule of a GE port to “Deny”, then bind the port to a suitable profile with the ACL “Permit” action set to “Active”. This allows the GE port to deny all packets except the ACL entry of the profile binding.

One Directional MAC Address and One VLAN Permitting Filtering

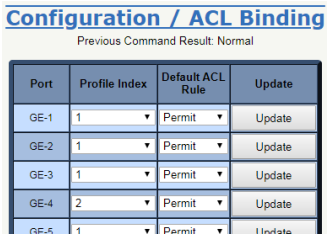
1. Create a new ACL Profile. (Profile Name: AllowSomeMac)



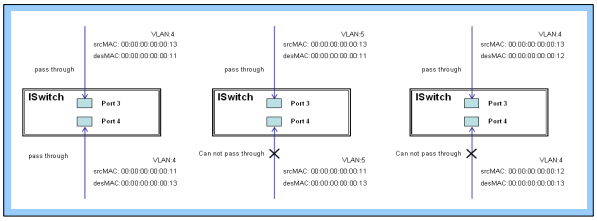
2. Create a new ACL Entry rule under this ACL Profile. (Allow MAC: 11 and VLAN: 4)



3. Bind this ACL Profile to a GE port. (GE-4)



4. Send frames between GE-3 and GE-4 and observe the test results.

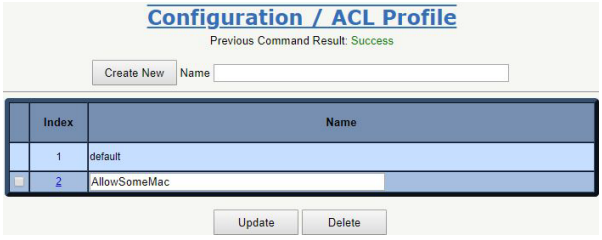


CLI Command

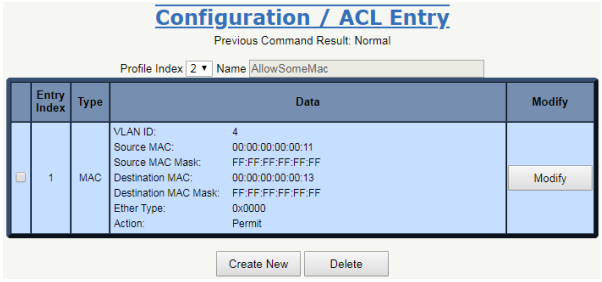
```
enable
configure
profile acl
acl-profile 2 create
acl-profile 2 set name AllowSomeMac
acl-profile 2 create entry 1
acl-profile 2 set entry 1 mac-type set vlan 4
acl-profile 2 set entry 1 mac-type set srcmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 action forwarding permit
exit
vlan 4 v4
vlan 5 v5
interface gigabit 3
vlan 4 tag
vlan 5 tag
exit
interface gigabit 4
vlan 4 tag
vlan 5 tag
def-acl deny
acl-profile-bind 2
exit
exit
exit
```

Two Directional MAC Address with All VLANs Permitting Filtering

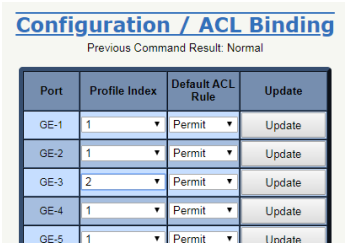
1. Create a new ACL Profile. (Profile Name: AllowSomeMac)



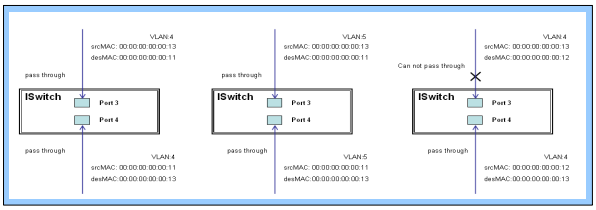
2. Create a new ACL Entry rule under this ACL Profile. (Allow ScrMAC: 13 and DesMAC: 11)



3. Bind this ACL Profile to a GE port. (GE-3)



4. Send frames between GE-3 and GE-4 and observe the results.



CLI Command

```
enable
configure
profile acl
acl-profile 2 create
acl-profile 2 set name AllowSomeMac
acl-profile 2 create entry 1
acl-profile 2 set entry 1 mac-type set srcmac 00:00:00:00:00:13 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 mac-type set dstmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 action forwarding permit
exit
vlan 4 v4
vlan 5 v5
interface gigabit 3
vlan 4 tag
vlan 5 tag
def-acl deny
acl-profile-bind 2
exit
interface gigabit 4
vlan 4 tag
vlan 5 tag
exit
exit
exit
```

Case 1(h):

When the ACL Rule of a GE port is “Deny”, Queue Mapping is not effective. This case is irrelevant.

Case 1(i):

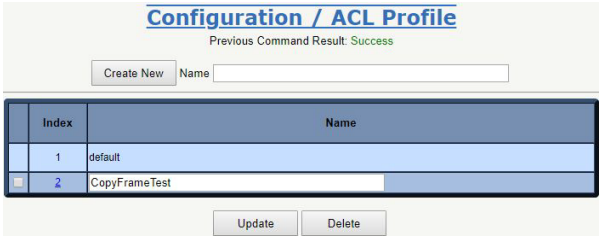
When the ACL Rule of a GE port is “Deny”, CoS Marking is not effective. This case is irrelevant.

Case 1(j):

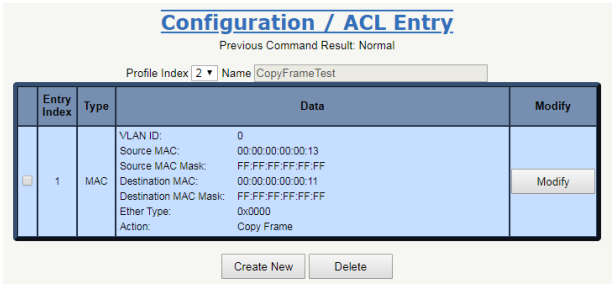
A user can set the default ACL Rule of a GE port to “Deny”, then bind the port to a suitable profile with the “Copy Frame” action for mirror analyzer active. This allows the system to copy frames from the binding GE Port to an analyzer port. No frame is received from the denied GE port except the mirror analyzer port.

One Directional MAC Address with Copy Frame Action. (Don’t Case VLAN, Ether Type)

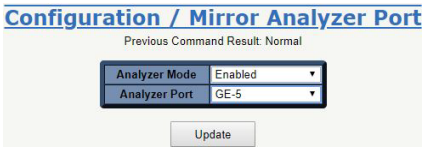
1. Create a new ACL Profile. (Profile Name: CopyFrameTest)



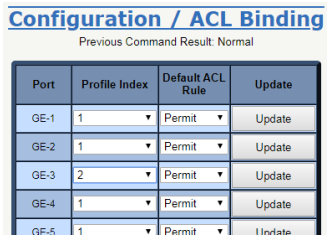
2. Create a new ACL Entry rule under this ACL Profile. (SrcMAC: 13 and DesMAC: 11)



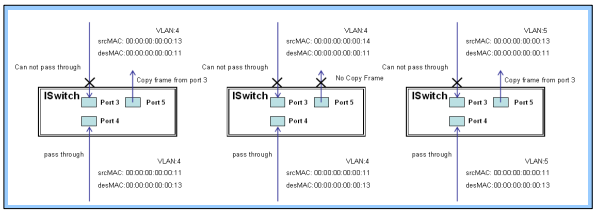
3. Set Analyzer Mode to “Enabled” under “Mirror Analyzer Port”.



4. Bind this ACL profile to a GE port. (GE-3)



5. Send frames between GE-3 and GE-4 and observe the test results.



CLI Command

```
enable
configure
profile acl
acl-profile 2 create
acl-profile 2 set name CopyFrameTest
Acl-profile 2 create entry 1
acl-profile 2 set entry 1 mac-type set srcmac 00:00:00:00:00:13 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 mac-type set dstmac 00:00:00:00:00:11 FF:FF:FF:FF:FF:FF
acl-profile 2 set entry 1 action copyframe
exit
vlan 4 v4
vlan 5 v5
```

```
interface gigabit 3
vlan 4 tag
vlan 5 tag
def-acl deny
acl-profile-bind 2
exit
interface gigabit 4
vlan 4 tag
vlan 5 tag
exit
exit
exit
```

Case 2: ACL for IP Address

For IP addresses, ACL can filter for: the source IP address, destination IP address or both. ACL also supports setting an IP range. When the filter is set for both a source and destination IP address, only packets meeting both criteria will be filtered. Packets which meet only one of these criteria will not be filtered.

If a user wants to filter only the source or only the destination IP address, then set the IP of the source or destination as needed and set the other IP address to 0.0.0.0. Besides IP addresses, ACL also supports protocols for additional filtering. (TCP=6, UDP=17, etc.) If a user wants a filter for a protocol, regardless of the IP address, then they should set both IP addresses to 0.0.0.0. For detailed testing, please refer to the MAC ACL above.

Case 3: ACL for L4 Port

For Layer 4 port ACL, filtering is possible through (1) the source IP address, (2) the source L4 port, (3) the destination IP address, (4) the destination L4 port and (5) the UDP or TCP Protocol. A user can filter through (1)-(4) for some or all values, but should select exactly one protocol from (5), either UDP or TCP.

When ACL filters through both directional IP addresses and through the L4 port, packets which meet all criteria will be filtered. In other words, ACL will not filter if a packet which only meets one requirement (has only a source or has only a destination address).

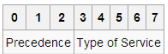
If a user wants to filter only one direction IP addresses or filter only through the L4 port, the other IP address and L4 port should be set to zero. This indicates no preference. For detailed testing, please refer to the MAC ACL above.

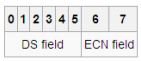
Case 4: ACL for ToS

For Type of Service (ToS), ACL can filter for (1) source IP addresses with ToS type, (2) destination IP addresses with ToS type, (3) both or (4) neither (ToS filtering only). When ACL filters for both IP address sources and destinations, packets must meet both criteria to be filtered. A packet with only a source or destination IP address will not be filtered.

If a user wants to filter only one directional IP addresses, the other IP address should be set to zero. This indicates no preference. For detailed testing, please refer to case 1 MAC ACL above.

Valid Values: Precedence: 0-7, ToS: 0-15, DSCP: 0-63





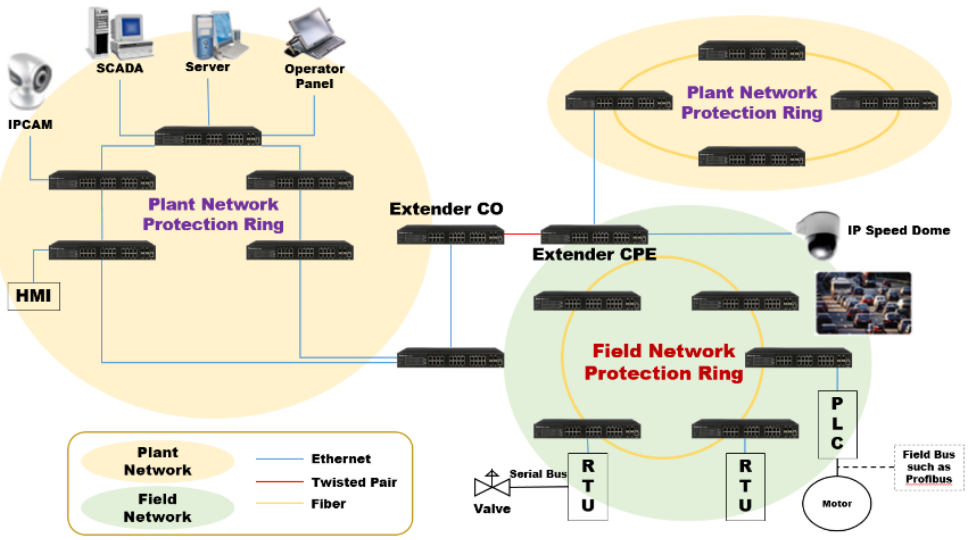
This value (&) is reserved and set to 0.
Ex: Pre (001) means 1
Pre (100) means 4
ToS (00010) means 1
ToS (10000) means 8
DSCP (000001) means 1
DSCP (100000) means 32

Ring Version 2 Configuration

Introduction

This section presents a guide to the Ring Version 2 application available for Red Lion NT328G Switch models.

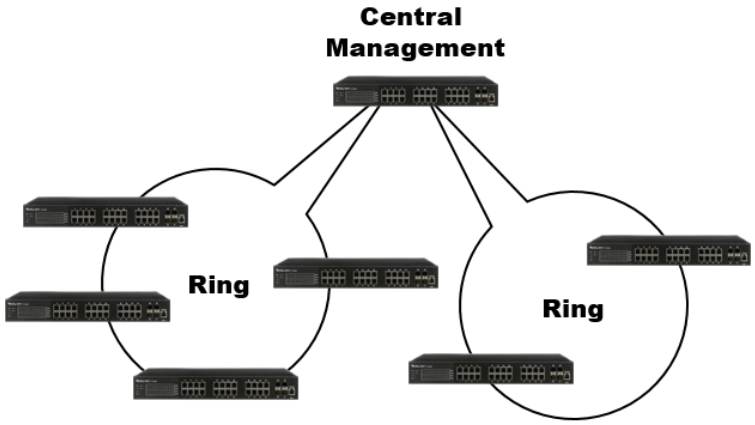
Network reliability is very important for Ethernet applications, especially in the industrial sector. The NT328G provides approximately 20 millisecond failover ring protection and this feature offers seamless network functionality regardless of any connection issues that may arise.



Ring Version 2 Features

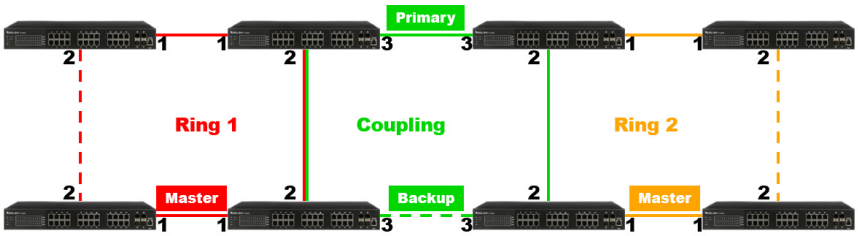
Group 1 – Ring-master and Ring-slave

- Both master and slave roles are supported for the ring.
- When the switch is set to master, one switch port is set as a forward port and another is set as a block port. The block port is not necessary. It is blocked in a normal state.
- When the switch is set to slave, both switch ports are set as forward ports.

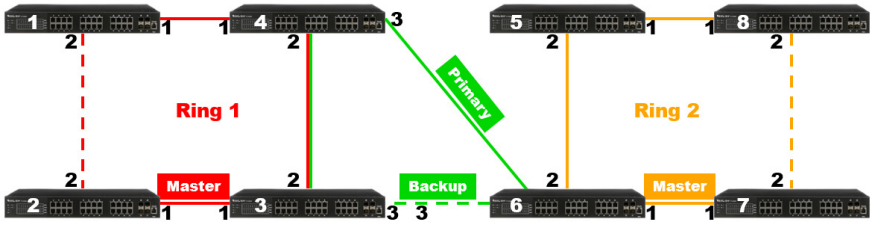


Group 2 – Coupling and Dual-Homing

- Switch – can be master or slave.
- Coupling – can be primary or backup.



- When the switch is set to coupling and/or primary, only one switch port set as the primary port needs to be configured.
- When the switch is set as coupling and/or backup, only one switch port set as the backup port needs to be configured. The backup port is not needed for this setting. The port is blocked in a normal state.
- Dual-Homing

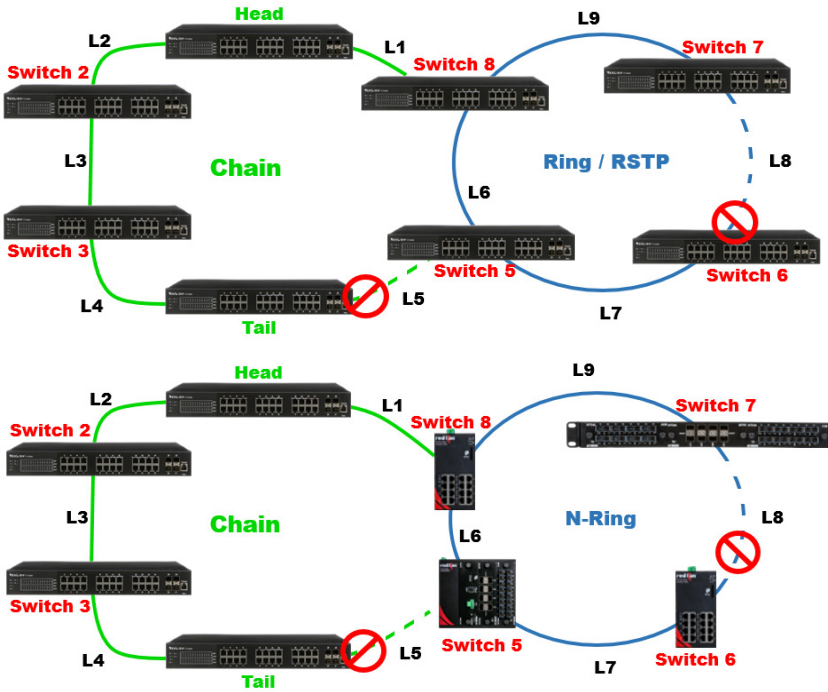


- When the switch is set to dual-homing, one switch port is set as the primary port and another is set as the backup port. This backup port is not needed for this setting. The port is blocked in a normal state.

Note: If your network configuration does not allow primary and backup connections from two different devices, you can use Dual-Homing to connect two rings from a single device.

Group 3 – Chain and Balancing-Chain

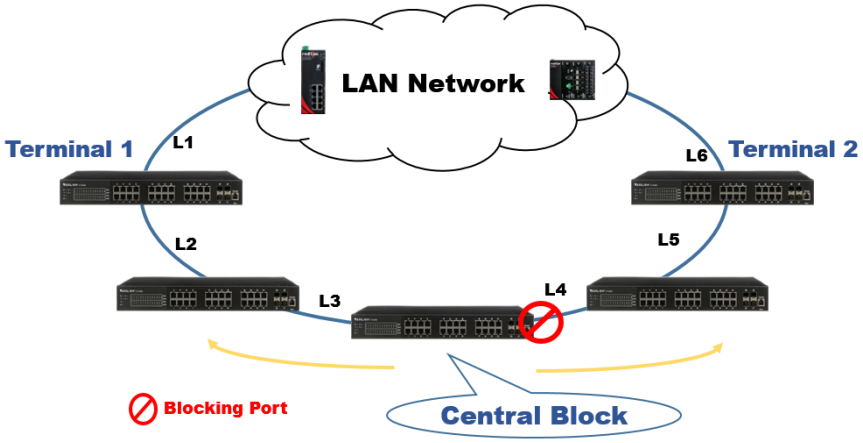
- Chain - Port can be configured as head, tail or member.



- When the switch is set to chain-head, one of the switch ports is set as the head port and another is set as a member port. Both switch ports are forwarded in a normal state.

- When the switch is set to chain-tail, one of the switch ports is set as the tail port and another is set as a member port. The tail port is not necessary. It is blocked in a normal state.
- When the switch is set to chain-member, both switch ports are set as member ports. Both ring ports are forwarded in a normal state.

Group 4 – Balancing Chain



Note: The LAN network can be any type of network.

- When the switch is set to balancing-chain/central-block, one of the ring ports is a member port and another is a block port. The block port is not necessary. It is blocked in a normal state.
- When the switch is set as balancing-chain/terminal-1/2, one ring port is the terminal port and another is a member port. Both ring ports are forwarded in normal state.
- When the switch is set as balancing-chain/member, both ring ports are member ports. Both ring ports are forwarded in a normal state.

Note: Group 1 must be enabled before configuring group 2 as coupling.
Note: When Group 1 or Group 2 is enabled, the configuration of Group 3 is disabled.
Note: When Group 3 is enabled, the configuration of Group 1 and Group 2 is disabled.

How to Configure Ringv2

Console Configuration

To configure the ring protection on the switch:

1. Login to the switch with the “admin” account using the CLI.
2. Go to configure mode through the CLI commands “cli”→“enable”→“configure”.
3. Go to configure ring protection group using CLI commands “ringv2-group 1” or “ringv2-group 2” or “ringv2-group 3”.
4. Set all necessary parameters:
   For Node 1 and Node 1, select the ports that are connected with the other switch.
   For example, selecting PORT-1 and PORT-2 means that PORT-1 is one of the ports connected to the other switch, as is PORT-2.
   Then select one of the ring connection devices to be the “Master,” then accept the “Node 2 port” as the blocking port.
   Node1 1
   Node2 2
   Role ring-master
   When the configuration is finished, enable ring protection by using the command “mode enable”.

Please pay attention to the status “Previous Command Result” after every action.
Configure terminal
Ring protect group 1

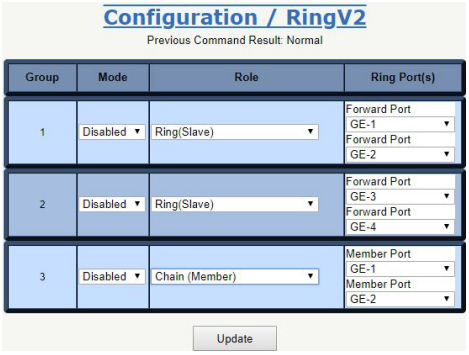
Node1 1
Node2 2
Role ring-master
Mode enable

Exit

Configuration (Web UI)

This document introduces the Industrial Ethernet Switch Software Spec for Ringv2.

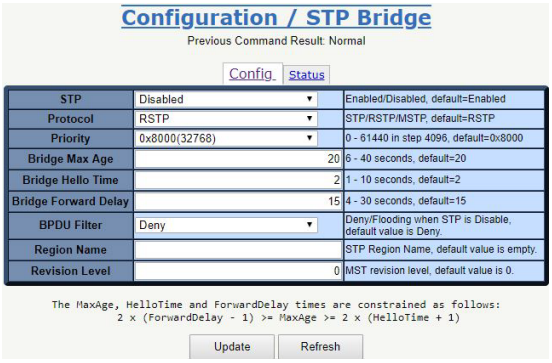
In the current design, one device can support up to 3 ring groups/index, including ring, coupling, dual-homing, chain and balancing-chain.



Note: Group 1 must be enabled before configuring Group 2 coupling role.
Note: If either Group 1 or Group 2 is enabled, the configuration of Group 3 will be limited and not configurable.
Note: If Group 3 is enabled, the configuration of Group 1 and Group 2 will be limited and not configurable.

Disable STP on All Ring Ports

Disable STP mode on a switch that uses Ring and Chain.

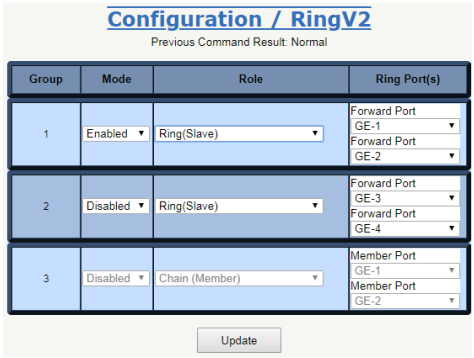


1. Go to “Configuration→Spanning Tree Protocol (STP)→STP Bridge”.
2. Select "STP" and set it to "Disabled".
3. Click the “Update” button.
4. Then navigate to the STP Port page via “Configuration→Spanning Tree Protocol (STP)→STP Port”.
5. Disable Port for ring protection.
6. Click the “Update” button.

Ring Master

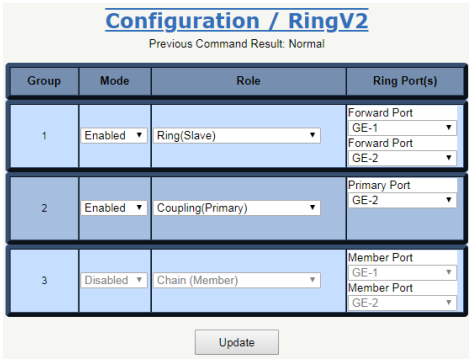
1. Go to “Configuration→Ringv2”.
2. Enable Group 1 and select the role “Ring(Master)”.
3. Select one port linked to neighbor devices to be the “Forward Port” and another to be the “Block Port”.

Ring Slave



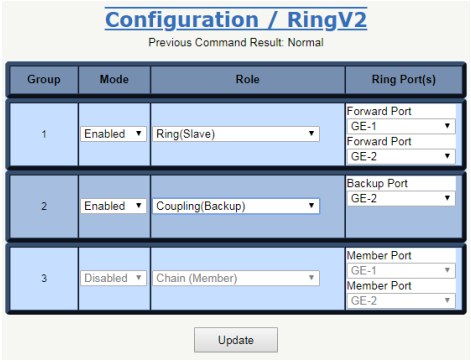
1. Go to “Configuration→Ringv2”.
2. Enable Group 1 and select the role “Ring(Slave)”.
3. Select two ports linked to neighbor devices to both be “Forward Port”.

Coupling Primary



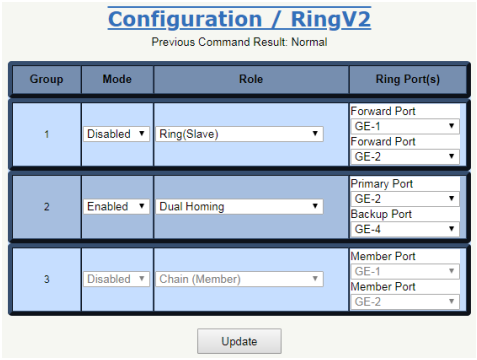
1. Go to “Configuration→Ringv2”.
2. Enable Group 1 and select the role “Ring(Slave)”.
3. Select two ports linked to neighbor devices to both be “Forward Port”.
4. Enable Group 2 and select the role “Coupling(Primary)”.
5. Select one port linked to the above ring to be the “Primary Port”.

Coupling Backup



1. Go to “Configuration→Ringv2”.
2. Enable Group 1 and select the role “Ring(Slave)”.
3. Select two ports linked to neighbor devices to both be “Forward Port”.
4. Enable Group 2 and select the role “Coupling(Backup)”.
5. Select one port linked to the above ring to be the “Backup Port”.

Dual-Homing



1. Go to “Configuration→Ringv2”.
2. Enable Group 2 and select the role “Dual Homing”.
3. Select one port linked to another ring to be the “Backup Port”.

Chain (Member)

1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Chain(Member)”.
3. Select 2 ports that link to the chain member to both be “Member Port”.

Chain (Head)

1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Chain(Head)”.
3. Select one port linked to other rings or networks to be the “Head Port”.
4. Select one port linked to the chain member to be the “Member Port”.

Chain(Tail)

1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Chain(Tail)”.
3. Select one port linked to other rings or networks to be the “Tail Port”.
4. Select one port linked to the chain member to be the “Member Port”.

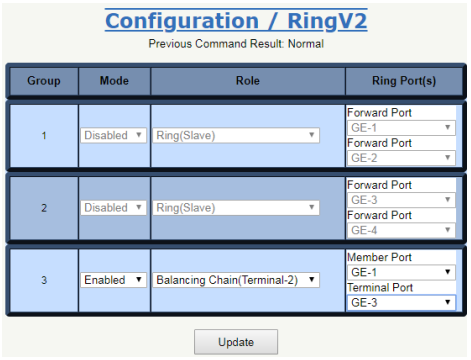
Balance Chain(Central Block)

1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Balance Chain(Central Block)”.
3. Select one port to be the “Block Port” to distribute traffic loading.
4. Select one port that connects to the chain member to be the “Member Port”.

Balance Chain(Terminal-1)

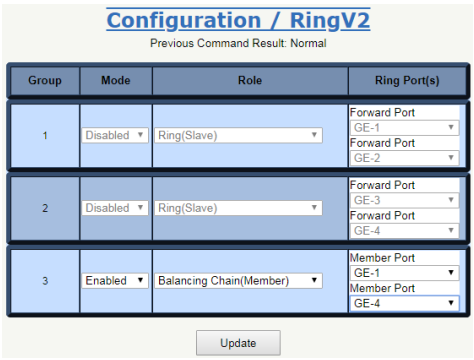
1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Balance Chain(Terminal-1)”.
3. Select one port to be the “Terminal Port” which connects to the other ring group.
4. Select one port that connects to the chain member to be the “Member Port”.

Balance Chain(Terminal-2)



1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Balance Chain(Terminal-2)”.
3. Select one port to be the “Terminal Port” to connect to another ring group.
4. Select one port that connects to the chain member to be the “Member Port”.

Balance Chain(Member)



1. Go to “Configuration→Ringv2”.
2. Enable Group 3 and select the role “Balance Chain(Member)”.
3. Select 2 ports that connect to the chain member to both be the “Member Port”.

QoS Configuration

Introduction

This section guides users through the Quality of Service (QoS) related features available for Red Lion NT328G Switch models.

QoS features allow you to allocate network resources to mission-critical applications at the expense of applications that are less sensitive to factors, such as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that each traffic type is assigned the appropriate QoS level.

SP/SPWRR/WRR

The switch can be configured to have 8 output Class of Service (CoS) queues (Q0-Q7) per port, into which each packet is queued. Q7 is the highest priority queue and Q0 is the lowest. Each packet's 802.1p priority determines its CoS queue. The user can bind a VLAN priority/queue mapping profile to each port and assign a traffic descriptor for every VLAN priority. The traffic descriptor defines the shaping parameter for every VLAN priority for Ethernet interface. Currently the switch supports Strict Priority (SP)/SPWRR (SP+WRR)/WRR (Weighted Round Robin) scheduling methods on each port. Detailed references are available in the user manual.

Default Priority and Queue mapping as below:

Priority0	Priority1	Priority2	Priority3	Priority4	Priority5	Priority6	Priority7
Queue0	Queue1	Queue2	Queue3	Queue4	Queue5	Queue6	Queue7
WRR	WRR	WRR	WRR	SPQ	SPQ	SPQ	SPQ

Several examples have been provided for various QoS combinations. QoS can be configured using the Web-based management system, CLI (Command Line Interface) or SNMP.

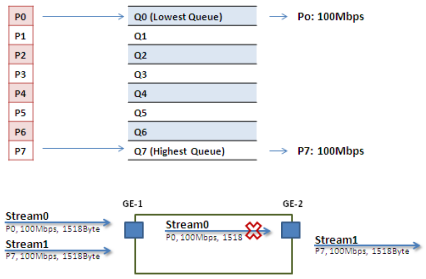
Example 1: SPQ without Shaping (Default Profile)

2 Streams (Stream0, Stream1) were sent GE-1 to GE-2. Both streams transfer at 100Mbps. Stream0 is assigned to VLAN Priority0, Stream1 is assigned to VLAN Priority7. The GE-2 link speed is set to 100Mbps.

Expected Result:

It is expected that GE-2 would only receive 100Mbps of Stream1 and that Stream0 would be discarded. This example shows how SPQ works on the switch.

Gigabit port VLAN Priority & Queue mapping:



Stream0:

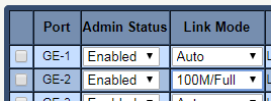
- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1

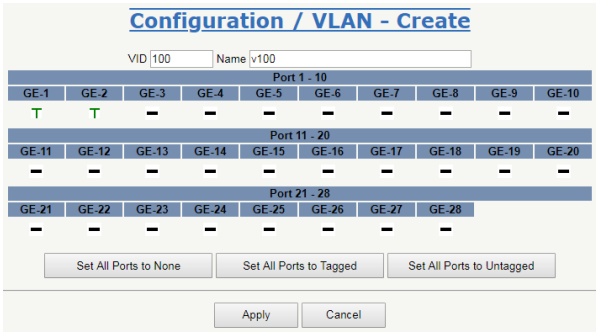
- Dst Mac: 00:00:00:00:20:02
- Src Mac: 00:00:00:00:10:02
- Vlan: 100
- Vlan prio: 7
- Send rate: 100Mbps
- Packet length: 1518bytes

Web Management

1. Go to Configuration→Port Configuration→Giga Port, and set GE-2 link speed to 100Mbps full duplex.



2. Select Configuration→Static VLAN. Create a VLAN with VLAN ID 100. Enter a VLAN name in the Name field. Here we set tagged VLAN100 on GE-1 and GE-2.



CLI Configuration Command

```
enable
configure
interface gigabit 2
speed full-100mbps
exit
vlan 100 v100
interface gigabit 1
vlan 100 tag
exit
interface gigabit 2
vlan 100 tag
exit
exit
exit
```

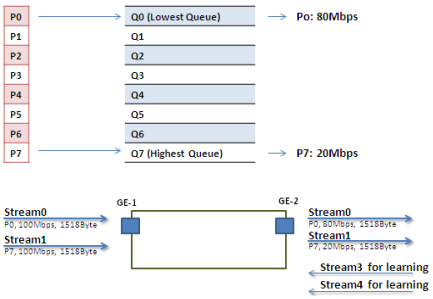
Example 2: SPQ with Shaping

Two Streams (Stream0, Stream1) were sent from GE-1 to GE-2. Both streams transfer at 100Mbps. Stream0 is assigned VLAN Priority0 and Stream1 is assigned VLAN Priority7. Stream3 and Stream4 are only for learning to prevent the traffic from flooding.

Expected Result:

It is expected that GE-2 would only receive 20Mbps of Stream1 and 80Mbps of Stream0. This example shows how SPQ works on the switch.

VDSL port VLAN Priority & Queue mapping:



Stream0:

- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1:

- Dst Mac : 00:00:00:00:20:02
- Src Mac : 00:00:00:00:10:02
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream3: (for Learning)

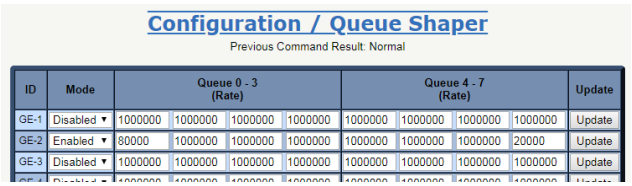
- Dst Mac : 00:00:00:00:10:01
- Src Mac : 00:00:00:00:20:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream4: (for Learning)

- Dst Mac : 00:00:00:00:10:02
- Src Mac : 00:00:00:00:20:02
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Web Management

1. Go to Configuration→Shaper→Queue and set the shaping rate for queue 0 and queue 7 as shown below.



CLI Configuration Command

enable
configure
vlan 100 v100

```
interface gigabit 1
vlan 100 tag
exit
interface gigabit 2
vlan 100 tag
queue-shaper enable
queue-shaper queue 7 20000
queue-shaper queue 0 80000
exit
exit
exit
```

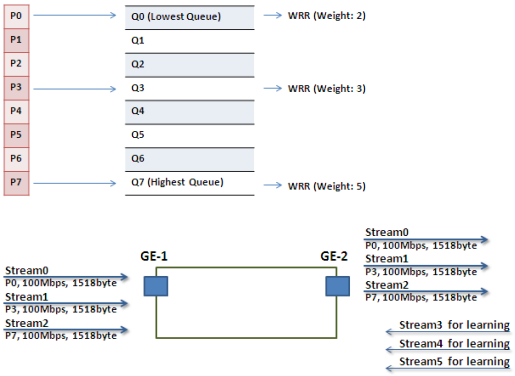
Example 3: WRR

Three Streams (Stream0, Stream1 and Stream2) were sent from GE-1 to GE-2. These Streams transfer at 100Mbps. Stream0 is assigned VLAN Priority0, Stream1 is assigned VLAN Priority3 and Stream2 is assigned VLAN Priority7. Stream3, Stream4 and Stream5 are only for learning to prevent the traffic from flooding. WRR supports weight assignment and the range of weight value is from 1 to 255. The switch applies WRR scheduling and Weight 1 for all Gigabit Ethernet Ports. In the following case, Weight 2 is assigned for Priority0, Weight 3 for Priority3 and Weight 5 for Priority7.

Expected Result:

GE-2 will receive about 20Mbps of Stream0, 30Mbps of Stream1 and 50Mbps of Stream2. This example shows how WRR works on the switch.

Gigabit port VLAN Priority & Queue mapping:



Stream0:

- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1:

- Dst Mac : 00:00:00:00:20:04
- Src Mac : 00:00:00:00:10:04
- Vlan : 100
- Vlan prio : 3
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream2:

- Dst Mac : 00:00:00:00:20:08
- Src Mac : 00:00:00:00:10:08

- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream3: (for Learning)

- Dst Mac : 00:00:00:00:10:01
- Src Mac : 00:00:00:00:20:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream4: (for Learning)

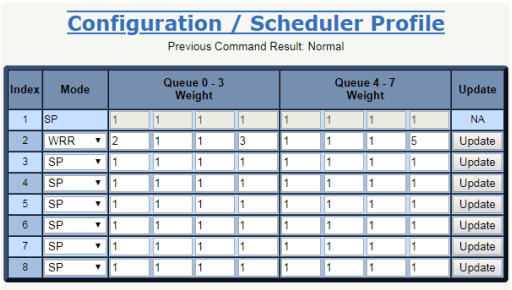
- Dst Mac : 00:00:00:00:10:04
- Src Mac : 00:00:00:00:20:04
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream5: (for Learning)

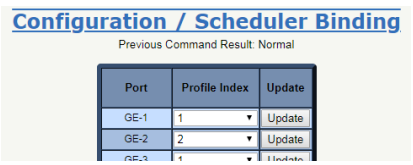
- Dst Mac : 00:00:00:00:10:08
- Src Mac : 00:00:00:00:20:08
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Web Management

1. Go to Configuration→Queue and Scheduler→Scheduling Profile and set the weight value for queue 0, queue 3 and queue 7 as shown below.



2. Go to Configuration→Queue and Scheduler→Binding and bind profile 2 on GE-2.



CLI Configuration Command

```
enable
configure
profile sch
scheduler-profile 2 method wwr
scheduler-profile 2 queue 7 weight 5
scheduler-profile 2 queue 3 weight 3
```

```
scheduler-profile 2 queue 0 weight 2
exit
vlan 100 v100
interface gigabit 1
vlan 100 tag
exit
interface gigabit 2
vlan 100 tag
queue-scheduler bind 2
exit
exit
exit
```

Example 4: SP-WRR

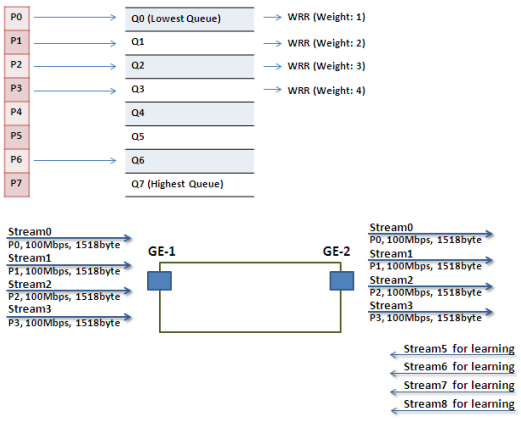
Four Streams (Stream0, Stream1, Stream2 and Stream3) were sent from GE-1 to GE-2. These Streams each transfer at 100Mbps. Stream0 is assigned VLAN Priority0, Stream1 is assigned VLAN Priority1, Stream2 is assigned VLAN Priority2, Stream3 is assigned VLAN Priority3 and Stream4 is assigned VLAN Priority6. Stream5, Stream6, Stream7, Stream8 and Stream9 are only for learning to prevent the traffic from flooding. WRR supports weight assignment and the range of weight value is from 1 to 255. The switch applies WRR scheduling and Weight 1 for all Gigabit Ethernet Ports. In the following case, Weight 1 is assigned for Priority0, Weight 2 for Priority1, Weight 3 for Priority2 and Weight 4 for Priority 3. In SP-WRR mode, queue0 to queue3 belongs to WRR and queue4 to queue6 belongs to SP.

Expected Result:

In Case 1, we expect GE-2 will receive about 10Mbps of Stream0, 20Mbps of Stream1, 30Mbps of Stream2 and 40Mbps of Stream3 if we send Stream0 to Stream3 to GE-1. In Case 2, we expect GE-2 will receive 100Mbps of Stream6 only and Stream0 to Stream3 will be discarded. This example shows how SP-WRR works on the switch.

Case 1:

Gigabit port VLAN Priority and Queue mapping:



Stream0:

- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1:

- Dst Mac : 00:00:00:00:20:02

- Src Mac : 00:00:00:00:10:02
- Vlan : 100
- Vlan prio : 3
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream2:

- Dst Mac : 00:00:00:00:20:03
- Src Mac : 00:00:00:00:10:03
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream3:

- Dst Mac : 00:00:00:00:20:04
- Src Mac : 00:00:00:00:10:04
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream5: (for Learning)

- Dst Mac : 00:00:00:00:10:01
- Src Mac : 00:00:00:00:20:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream6: (for Learning)

- Dst Mac : 00:00:00:00:10:02
- Src Mac : 00:00:00:00:20:02
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream7: (for Learning)

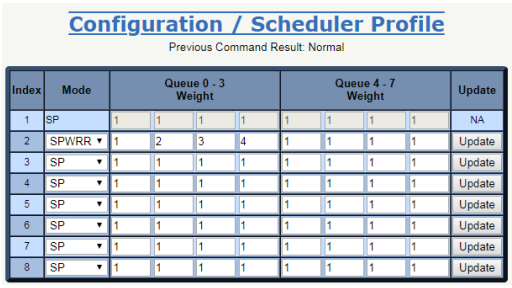
- Dst Mac : 00:00:00:00:10:03
- Src Mac : 00:00:00:00:20:03
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream8: (for Learning)

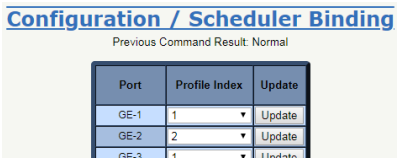
- Dst Mac : 00:00:00:00:10:04
- Src Mac : 00:00:00:00:20:04
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Web Management

1. Go to Configuration→Queue and Scheduler→Scheduling Profile and set the weight value for queue 0 - queue 3 as shown below.



2. Go to Configuration→Queue and Scheduler→Binding and bind profile 2 on GE-2.

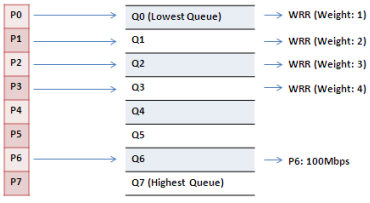


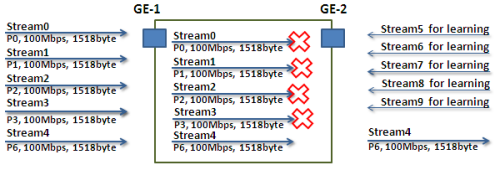
CLI Configuration Command

```
enable
configure
profile sch
scheduler-profile 2 method spq-wrr
scheduler-profile 2 queue 3 weight 4
scheduler-profile 2 queue 2 weight 3
scheduler-profile queue 1 weight 2
exit
vlan 100 v100
interface gigabit 1
vlan 100 tag
exit
interface gigabit 2
vlan 100 tag
queue-scheduler bind 2
exit
exit
exit
```

Case 2:

Gigabit port VLAN Priority and Queue mapping





Stream0:

- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01

- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1:

- Dst Mac : 00:00:00:00:20:02
- Src Mac : 00:00:00:00:10:02
- Vlan : 100
- Vlan prio : 3
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream2:

- Dst Mac : 00:00:00:00:20:03
- Src Mac : 00:00:00:00:10:03
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream3:

- Dst Mac : 00:00:00:00:20:04
- Src Mac : 00:00:00:00:10:04
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream4:

- Dst Mac : 00:00:00:00:20:07
- Src Mac : 00:00:00:00:10:07
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream5: (for Learning)

- Dst Mac : 00:00:00:00:10:01
- Src Mac : 00:00:00:00:20:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream6: (for Learning)

- Dst Mac : 00:00:00:00:10:02
- Src Mac : 00:00:00:00:20:02
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream7: (for Learning)

- Dst Mac : 00:00:00:00:10:03

- Src Mac : 00:00:00:00:20:03
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream8: (for Learning)

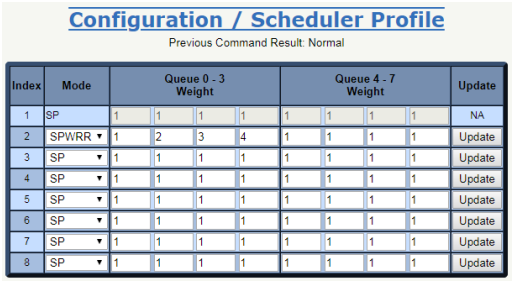
- Dst Mac : 00:00:00:00:10:04
- Src Mac : 00:00:00:00:20:04
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream9: (for Learning)

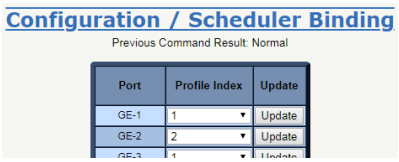
- Dst Mac : 00:00:00:00:10:07
- Src Mac : 00:00:00:00:20:07
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Web Management

1. Go to Configuration→Queue and Scheduler→Scheduling Profile, and set the value for “Queue 0-3 Weight” as shown below.



2. Go to Configuration→Queue and Scheduler→Binding and bind profile 2 on GE-2.



CLI Configuration Command

```
enable
configure
profile sch
scheduler-profile 2 method spq-wrr
scheduler-profile 2 queue 3 weight 4
scheduler-profile 2 queue 2 weight 3
scheduler-profile 2 queue 1 weight 2
exit
vlan 100 v100
interface gigabit 1
vlan 100 tag
exit
interface gigabit 2
vlan 100 tag
```

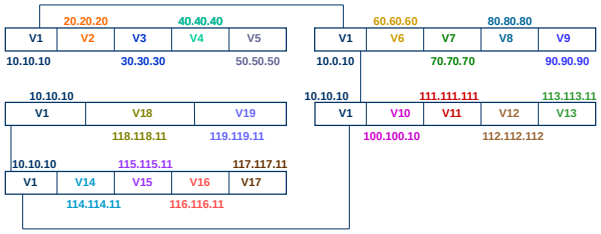
```
queue-scheduler bind 2
exit
exit
exit
```

RIP Routing Configuration

Introduction

This section provides a guide to using the Routing Information Protocol (RIP) function available for Red Lion NT328G Switch models.

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols that employs hop count as a routing metric. RIP prevents routing loops by imposing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed with RIP is 15. This hop limit limits the size of networks that RIP can support. A hop count of 16 registers as an infinite distance and the route is considered unreachable. RIP implements split horizon, route poisoning and holddown mechanisms to prevent inaccurate routing information from propagating.



Creating VLANs

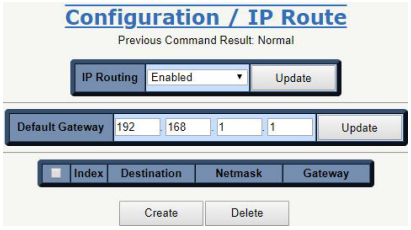
1. On Switch A, select “Configuration→VLAN→Static VLAN”. Create VLANs with VLAN ID 2-5. Configure ports 2-5 to belong to VLAN 2-5 untag port
2. On Switch B, create VLANs with VLAN ID 6-9. Configure ports 2-5 to belong to VLAN 6-9 untag port.
3. On Switch C, create VLANs with VLAN ID 10-13. Configure ports 2-5 to belong to VLAN 10-13 untag port.
4. On Switch D, create VLANs with VLAN ID 14-17. Configure ports 2-5 to belong to VLAN 14-17 untag port.
5. On Switch E, create VLANs with VLAN ID 18-19. Configure ports 2-3 to belong to VLAN 18-19 untag port.

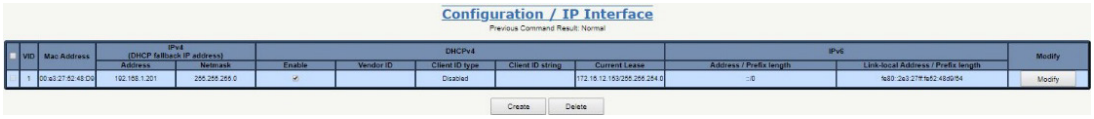
Port Default VLAN

1. On Switch A, go to “Configuration→Port Configuration→Bridge Port”, configure PVID 1-5 on ports 1-5 and click the “Modify” button.
2. On Switch B, configure PVID 6-9 on ports 2-5.
3. On Switch C, configure PVID 10-13 on ports 2-5.
4. On Switch D, configure PVID 14-17 on ports 2-5.
5. On Switch E, configure PVID 18-19 on ports 2-3.

Create Interface

1. On Switch A, go to “Configuration→IP Management→IP Route”, enable “IP Routing” and click the “Modify” button.
2. Then go to “Configuration→IP Management→IP Interface” and create five interfaces as the topology description.





Shown below are all of the interface tables on five layer 3 switches, A-E:

Switch A

VID	IP Address	Netmask
1	10.10.10.1	255.255.255.0
2	20.20.20.1	255.255.255.0
3	30.30.30.1	255.255.255.0
4	40.40.40.1	255.255.255.0
5	50.50.50.1	255.255.255.0

Switch B

VID	IP Address	Netmask
1	10.10.10.1	255.255.255.0
6	60.60.60.1	255.255.255.0
7	70.70.70.1	255.255.255.0
8	80.80.80.1	255.255.255.0
9	90.90.90.1	255.255.255.0

Switch C

VID	IP Address	Netmask
1	10.10.10.1	255.255.255.0
10	100.100.100.1	255.255.255.0
11	111.111.111.1	255.255.255.0
12	112.112.112.1	255.255.255.0
13	113.113.113.1	255.255.255.0

Switch D

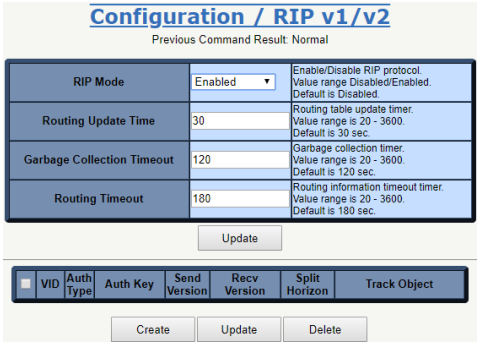
VID	IP Address	Netmask
1	10.10.10.1	255.255.255.0
14	114.114.114.1	255.255.255.0
15	115.115.115.1	255.255.255.0
16	116.116.116.1	255.255.255.0
17	117.117.117.1	255.255.255.0

Switch E

VID	IP Address	Netmask
1	10.10.10.1	255.255.255.0
18	118.118.118.1	255.255.255.0
19	119.119.119.1	255.255.255.0

Enable RIP

1. On all switches, go to “Configuration→Layer 3→RIP v1/v2”, enable “RIP mode” and click the “Modify” button.
2. Create an RIP rule on all VLAN interfaces.
3. Select “Send Version” as ”Both”, “Receive Version” as “RIP 1 or RIP 2” and “Split Horizon” as “Simple”.

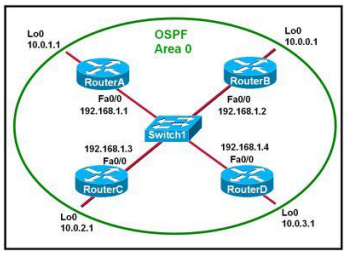


OSPF Routing Configuration

This section presents a guide to the Open Shortest Path First (OSPF) routing function available for Red Lion NT328G Switch models.

OSPF is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system

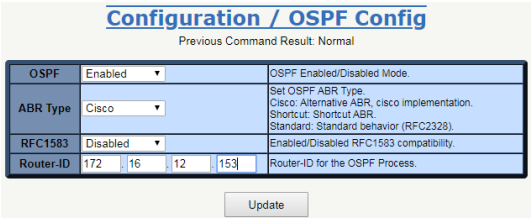
(AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).



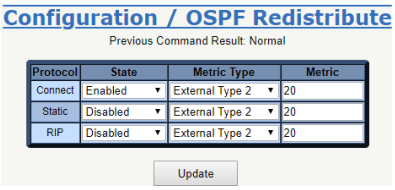
To configure the OSPF in the switch to support the scenario above, WebUI configuration procedures are shown below:

Modify Setting Data

1. Enable OSPF on all devices using the Configuration/OSPF Config screen to Modify OSPF Config data

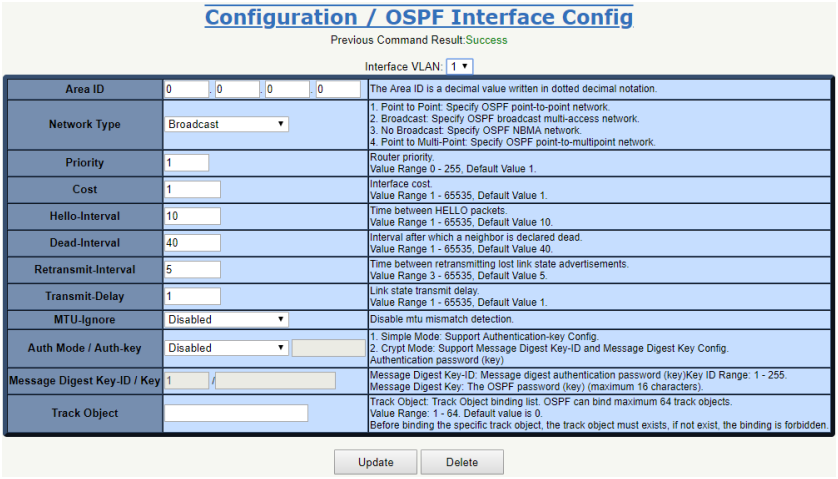


2. Set the Router-ID as device IP
3. Click the "Modify" button to Modify OSPF Config.
4. Use the Configuration / OSPF Redistribute screen to modify OSPF and redistribute data on all devices.



Modify OSPF Redistribute (Enable the Connect Protocol)

1. Click the "Modify" button to modify OSPF Redistribute.
2. Enable OSPF in all interfaces of all devices.
3. Use the Configuration/Interface Config screen to modify Interface Config data.



Modify Setting Data

1. Modify the setting data.
2. Click the "Modify" button to apply the changes to the OSPF Interface Config data.
3. Use the Configuration/Interface Config screen to Modify Interface Config data.

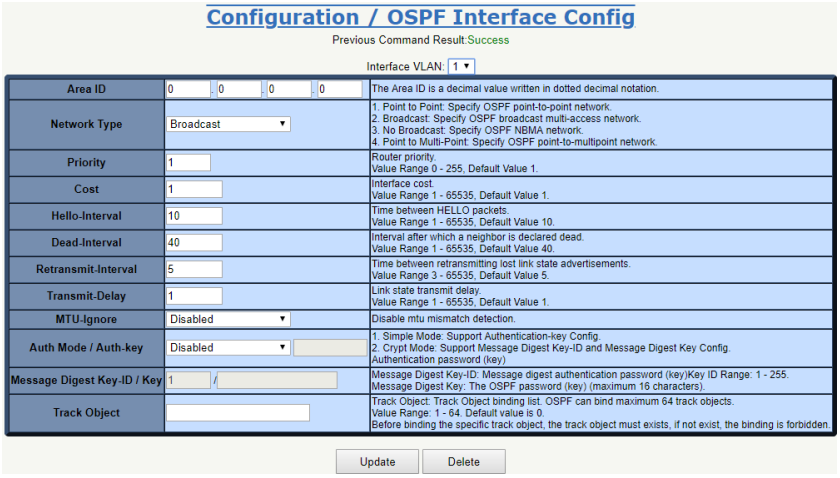
In the central switch, there is an interface that, to be connected with other devices via 192.168.1.0/24 networks, the “Area ID” must be “0.0.0.0”.

In other devices, all interfaces belong to 192.168.1.0/24 networks, and the “Area ID” must be “0.0.0.0”.

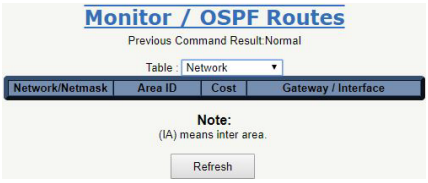
When changing NT328G OSPF interface speeds, the cost of the OSPF interface must be set manually. As a best practice, all ports on an OSPF interface should be set to the same bandwidth, and costs should be lower as bandwidth increases. See the following chart for recommended cost settings based on interface bandwidth.

INTERFACE BANDWIDTH	OSPF COST
1000Mbps	1
100Mbps	1
10Mbps	10

Note: STP/RSTP/MSTP must be disabled on any port belonging to an OSPF interface. The protocols can interfere with one another, causing unexpected results.



4. Repeat for all devices.
5. Check OSPF negotiation status:
6. Use the Monitor / Layer 3 / OSPF Routes screen to display OSPF Routes data.



7. Select Query Type.
8. Fill VID when query type is “by VID”.
9. Click the “Query” button to get OSPF Routes data.

VRRP Configuration

Introduction

This section presents a guide to the Virtual Router Redundancy Protocol (VRRP) function available for Red Lion NT328G Switch models.

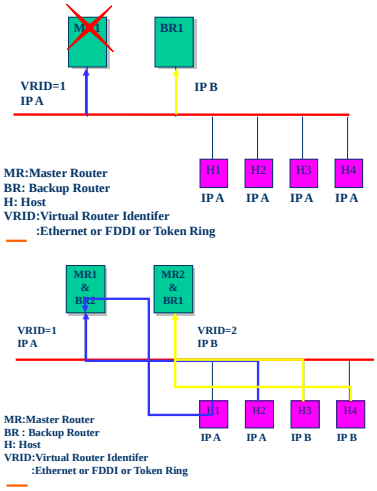
VRRP is a computer networking protocol that provides the automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

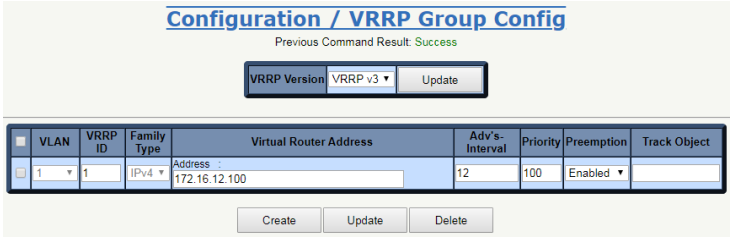
The protocol achieves this through the creation of virtual routers. Virtual routers are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router automatically replaces it. The physical router that is forwarding packets at any given time is called the master router.

Problems with statically configured default route:

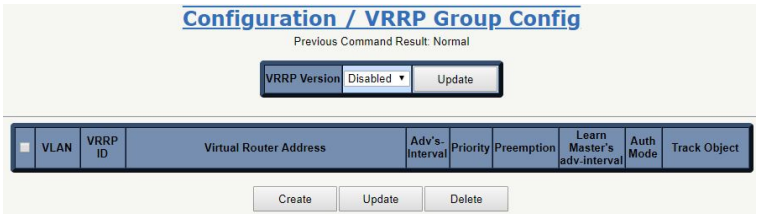
- Single point of failure.
- Inability to find alternate path.

Solution – Redundancy Using VRRP





Enable VRRP In All Interfaces of All Devices



Use the Configuration→Layer 3→VRRP Configuration screen to Modify VRRP Group data.

1. Select VRRP Version and click the "Modify" button.
2. Select a VLAN interface for running VRRP.
3. Set the “Virtual Router Address” the same as the master device IP address.

Appendix A CLI Commands

Introduction

This appendix describes the CLI operator interface provided in the Red Lion Controls NT328G 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 NT328G 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. Both the default username and default password are 'admin'. Once logged in, a listing of available commands can be obtained through the help interface. This is accessible by typing either “?” or “help?”. The following commands are available:

Connection Interface

To connect a host PC to the Console port, an RJ45 (male) connector-to-RS232 DB9 (female) connector cable 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) Level

Authorization Levels

LEVEL	DESCRIPTION
Superuser	Superuser can access all management features.
Engineer	Engineer can access all management features except user account management.
Guest (default)	Read-only mode (guest can only change his own password). Users of this level can query pages like PM and FM.

Login Example

```
localhost login: admin
Password: *****

NT328G-20SFP-AC1 | SW v1.0.10 (08/18/2017 16:26:41)

localhost:>enable
localhost:%show version

NT328G-20SFP-AC1 | SW v1.0.10 (08/18/2017 16:26:41)
```

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, their access levels, and mode prompts.

Table 1: List of Execution Modes

MODE	ACCESS LEVEL	TO ENTER MODE	PROMPT
Initial Mode	Guest	login, disable	>
Enable Mode	Guest	enable	%
Configure Mode	Guest	configure	(conf)#
Interface Gigabit Configure Mode	Engineer	interface gigabit <portNo>	(gigabit-intf-conf)#
Interface LAG Configure Mode	Engineer	interface lag <number>	(lag-conf)#
Interface VLAN Configure Mode	Engineer	interface vlan <vlanid>	(vlan-intf-conf)#
IP DHCP Pool Configure Mode	Engineer	ip dhcp pool <number>	(dhcp-conf)#
Profile ACL Configure Mode	Engineer	profile acl	(acl-profile-conf)#
Profile Alarm Configure Mode	Engineer	profile alarm	(alarm-profile-conf)#
Profile IGMP ACL Configure Mode	Engineer	profile igmp-acl	(igmp-acl-profile-conf)#
Profile IGMP MVR Configure Mode	Engineer	profile igmp-mvr	(igmp-mvr-profile-conf)#
Profile Scheduler Configure Mode	Engineer	profile sch	(sch-profile-conf)#
RingV2 Group Configure Mode	Engineer	ringv2-group <number>	(ringv2-group-conf)#
Router OSPF Configure Mode	Engineer	router ospf	(router-ospf-conf)#
Router RIP Configure Mode	Engineer	router rip	(router-rip-conf)#

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.

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	

KEYS	FUNCTION
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 Mode Commands

This is the default mode after logging in to the switch. To return to this mode type disable under any other execution mode.

All commands in this execution mode (except the “enable” command) are global and can be executed under all execution modes.

bye

Description	Quit CLI.
Syntax	bye
Parameter	None

!

Description	Execute the specific command number in history.	
Syntax	!<number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–32 **Type:** Mandatory

exit

Description	Exit current mode.
Syntax	exit
Parameter	None

configure

Description	Enter configuration mode.
Syntax	configure
Parameter	None

list alarm table

Description	List valid alarm ID.
Syntax	list alarm table
Parameter	None

list alarm table detail

Description	List detail information for all alarms.
Syntax	list alarm table detail
Parameter	None

list command-tree

Description	List tree of all available CLI commands.
Syntax	list command-tree
Parameter	None

list event table

Description	List valid event ID.
Syntax	list event table
Parameter	None

list execution-modes

Description	List all available command execution modes.
Syntax	list execution-modes
Parameter	None

list timezone

Description	List time zones.
Syntax	list timezone
Parameter	None

show env

Description	Show CLI environment variables.
Syntax	show env
Parameter	None

show history

Description	Show command history (Note: commands issued in an execution mode only appear in the history of that execution mode).
Syntax	show history
Parameter	None

show time

Description	Show current time
Syntax	show time
Parameter	None

show uptime

Description	Show uptime.
Syntax	show uptime
Parameter	None

sleep

Description	Sleep for the specified number of milliseconds.	
Syntax	sleep <time>	
Parameter		
	Name	**Description**
	<time>	**Valid values:** 1–0xFFFFFFFF ms **Type:** Mandatory

enable

Description	Enter enable mode.
Syntax	enable
Parameter	None

Enable Mode Commands

To enter this execution mode type **enable** under the Initial Mode.

All commands in this mode are global and can be executed under all execution modes, except under the Initial Mode which has fewer commands.

All of the “show ...” commands in this mode are global and can be executed under all execution modes, except Initial Mode which has fewer show commands.

disable

Description	Enter Initial mode.
Syntax	disable
Parameter	None

kick

Description	Kick off a logged in user.	
Syntax	kick <index> {cli|console|web}	
Parameter		
	Name	**Description**
	<index>	**Valid values:** Login user index (1 - 10) **Type:** Mandatory
	{cli|console|web}	The interface you want to kick the logged in user off.

ping

Description	Send ping request to specified ip address.	
Syntax	ping <ip>	
Parameter		
	Name	**Description**
	<ip>	**Valid values:** Any valid IP **Type:** Mandatory

ping6

Description	Send IPv6 ping request to specified ip address.	
Syntax	ping <ipv6_subnet>	
Parameter		
	Name	**Description**
	<ipv6_subnet>	**Valid values:** Any valid IPv6 address **Type:** Mandatory

All of the “show ...” commands in this mode are global and can be executed under all execution modes, except Initial Mode which has fewer show commands.

show account

Description	Show account list.
Syntax	show account
Parameter	None

show aging

Description	Show aging time for MAC learning table (system-wide).
Syntax	show aging
Parameter	None

show alarm current

Description	Show current alarm list.
Syntax	show alarm current
Parameter	None

show alarm history

Description	Show alarm history.
Syntax	show alarm history
Parameter	None

show bootloader

Description	Show boot loader information.
Syntax	show bootloader
Parameter	None

show clisettings

Description	Show CLI settings.
Syntax	show clisettings
Parameter	None

show cos-queue-mapping

Description	Show CoS queue mapping table.
Syntax	show cos-queue-mapping
Parameter	None

show cpu

Description	Show CPU name.
Syntax	show cpu
Parameter	None

show dot1x

Description	Show dot1x information.
Syntax	show dot1x
Parameter	None

show dot1x eapol-stats {<portNo>|all}

Description	Show dot1x EAPOL stats.	
Syntax	show dot1x eapol-stats {<portNo>|all}	
Parameter		
	Name	**Description**
	<portNo>	Gigabit port. **Valid values:** 1–28 **Type:** Mandatory
	<all>	All gigabit ports.

show dot1x pae-info-status {<portNo>|all}

Description	Show dot1x PAE status.	
Syntax	show dot1x pae-info-status {<portNo>|all}	
Parameter		
	Name	**Description**
	<portNo>	Gigabit port **Valid values:** 1–28 **Type:** Mandatory
	<all>	All gigabit ports.

show dot1x radius-stats

Description	Show dot1x radius stats.
Syntax	show dot1x radius-stats
Parameter	None

show env

Description	Show CLI environment variables.
Syntax	show env
Parameter	None

show event

Description	Show event list.
Syntax	show event (Refer to event Table)
Parameter	None

show ext-tpid

Description	Show TPID for the VLAN Tag.
Syntax	show ext-tpid
Parameter	None

show fdb

Description	Show forwarding table.
Syntax	show fdb
Parameter	None

show fdb interface gigabit <portNo>

Description	Show forwarding table per gigabit port.	
Syntax	show fdb interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show fdb interface trunk-group <number>

Description	Show forwarding table per trunk group.	
Syntax	show fdb interface trunk-group <number>	
Parameter		
	Name	**Description**
	<number>	Trunk group **Valid values:** 1–2 **Type:** Mandatory

show fdb vlan <vlanid>

Description	Show forwarding table per VLAN index.	
Syntax	show fdb vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

show fdbstatic

Description	Show static MAC forwarding table.
Syntax	show fdbstatic
Parameter	None

show fdbstatic interface gigabit <portNo>

Description	Show static MAC forwarding table per gigabit port.	
Syntax	show fdbstatic interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show fdbstatic vlan <vlanid>

Description	Show static MAC forwarding table per VLAN index.	
Syntax	show fdbstatic vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

show firmware partition

Description	Show firmware partition information.
Syntax	show firmware partition
Parameter	None

show firmware status

Description	Show firmware update status.
Syntax	show firmware status
Parameter	None

show gvrp

Description	Show GVRP information.
Syntax	show gvrp
Parameter	None

show history

Description	Show command history.
Syntax	show history
Parameter	None

show http

Description	Show HTTP and HTTPS information.
Syntax	show http
Parameter	None

show igmp snooping

Description	Show IGMP snooping information.
Syntax	show igmp snooping
Parameter	None

show igmp snooping router-ports

Description	Show IGMP router ports information.
Syntax	show igmp snooping router-ports
Parameter	None

show igmp snooping vlan <vlanid>

Description	Show IGMP VLAN number.	
Syntax	show igmp snooping vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

show igmp-acl-profile {<number>|all}

Description	Show IGMP ACL profile.	
Syntax	show igmp-acl-profile {<number>|all}	
Parameter		
	Name	**Description**
	<number>	IGMP ACL profile number **Valid values:** 1–15 **Type:** Mandatory
	<all>	All profile numbers. **Type:** Mandatory

show igmp-mvr-profile {<number>|all}

Description	Show IGMP MVR profile.	
Syntax	show igmp-mvr-profile {<number>|all}	
Parameter		
	Name	**Description**
	<number>	IGMP MVR profile number **Valid values:** 1–15 **Type:** Mandatory
	<all>	All profile numbers. **Type:** Mandatory

show interface gigabit <portNo>

Description	Show interface information per gigabit port.	
Syntax	show interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory
	<all>	All port numbers. **Type:** Mandatory

show interface gigabit <portNo> acl

Description	Show ACL profile per gigabit port.	
Syntax	show interface gigabit <portNo> acl	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> counter

Description	Show Ethernet statistics per gigabit port.	
Syntax	show interface gigabit <portNo> counter	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> igmp

Description	Show IGMP information per gigabit port.	
Syntax	show interface gigabit <portNo> igmp	
Parameter		
	Name	**Description**
	<portNo>	Gigabit port **Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> msti

Description	Show MSTI information per gigabit port.	
Syntax	show interface gigabit <portNo> msti	
Parameter		
	Name	**Description**
	<portNo>	Gigabit port **Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> port-isolation

Description	Show isolation information per gigabit port.	
Syntax	show interface gigabit <portNo> port-isolation	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> qos

Description	Show QoS per gigabit port.	
Syntax	show interface gigabit <portNo> qos	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> rmon-counter

Description	Show RMON (Ethernet counter) per gigabit port.	
Syntax	show interface gigabit <portNo> rmon-counter	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> storm-control

Description	Show storm control information per gigabit port.	
Syntax	show interface gigabit <portNo> storm-control	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> stp

Description	Show STP information per gigabit port.	
Syntax	show interface gigabit <portNo> stp	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface gigabit <portNo> vlan

Description	Show VLAN information per gigabit port.	
Syntax	show interface gigabit <portNo> vlan	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

show interface lag

Description	Show information of the Link Aggregation Group.
Syntax	show interface lag
Parameter	None

show interface vlan

Description	Show VLAN interface information of all VLANs.
Syntax	show interface vlan
Parameter	None

show interface vlan <vlanid>

Description	Show VLAN interface information of specific VLAN.	
Syntax	show interface vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Optional

show interface vlan ospf

Description	Show OSPF configuration of all VLANs.
Syntax	show interface vlan ospf
Parameter	None

show interface vlan rip

Description	Show RIP configuration of all VLANs.
Syntax	show interface vlan rip
Parameter	None

show ip dhcp binding

Description	Show status of DHCP client bindings of DHCP Server.
Syntax	show ip dhcp binding
Parameter	None

show ip dhcp binding detail

Description	Show status of detail information of the DHCP clients binding.
Syntax	show ip dhcp binding detail
Parameter	None

show ip dhcp class

Description	Show DHCP Class configuration.
Syntax	show ip dhcp class
Parameter	None

show ip dhcp pool

Description	Show DHCP pool configuration for all pools or specific pools.	
Syntax	show ip dhcp pool show ip dhcp pool <pool-id>	
Parameter		
	Name	**Description**
	<pool-id>	DHCP pool index **Valid values:** 1–20 **Type:** Optional

show ip dhcp relay

Description	Show DHCP relay configuration.
Syntax	show ip dhcp relay
Parameter	None

show ip dhcp snooping

Description	Show DHCP snooping configuration.
Syntax	show ip dhcp snooping
Parameter	None

show ip dhcp snooping binding

Description	Show DHCP snooping binding database.	
Syntax	show ip dhcp snooping binding interface gigabit <portNo> show ip dhcp snooping binding vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	Port interface **Valid values:** 1–28 **Type:** Mandatory
	<vlan-id>	Interface VLAN **Valid values:** 1–4094 **Type:** Mandatory

show ip dhcp snooping binding detail

Description	Show DHCP snooping binding database in detail	
Syntax	show ip dhcp snooping binding detail interface gigabit <portNo> show ip dhcp snooping binding detail vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	Port interface **Valid values:** 1–28 **Type:** Mandatory
	<vlan-id>	Interface VLAN **Valid values:** 1–4094 **Type:** Mandatory

show ip neighbors

Description	Show IPv4 neighbors.
Syntax	show ip neighbors
Parameter	None

show ip route

Description	Show routing table. (include RIP, OSPF, static).
Syntax	show ip route
Parameter	None

show ip route dhcp

Description	Show DHCP IPv4 routes.
Syntax	show ip route dhcp
Parameter	None

show ip route ospf

Description	Show OSPF learned IPv4 routes.
Syntax	show ip route ospf
Parameter	None

show ip route rip

Description	Show RIP learned IPv4 routes.
Syntax	show ip route rip
Parameter	None

show ip route static

Description	Show static IPv4 routes.
Syntax	show ip route static
Parameter	None

show ip route wire

Description	Show IPv4 routes which are running at wire-speed.
Syntax	show ip route wire
Parameter	None

show ip source binding

Description	Show IP source binding.
Syntax	show ip source binding
Parameter	None

show ip source binding dhcp-snooping

Description	Show the status of IP source binding learned by DHCP-Snooping including interfaces, static entries, and VLAN.	
Syntax	show ip source binding dhcp-snooping show ip source binding dhcp-snooping interface gigabit <portNo> show ip source binding dhcp-snooping static vlan <vlanid> show ip source binding dhcp-snooping vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	Port Number **Valid values:** 1–28 **Type:** Mandatory
	<vlanid>	VLAN Number **Valid values:** 1–4094 **Type:** Mandatory

show ip source binding interface gigabit <portNo>

Description	Show the status of dynamic IP source binding from interfaces per gigabit port.	
Syntax	show ip source binding interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	Port Number **Valid values:** 1–28 **Type:** Mandatory

show ip source binding static

Description	Show the status of static IP source binding including interfaces.	
Syntax	show ip source binding static show ip source binding static interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	Port Number **Valid values:** 1–28 **Type:** Mandatory

show ip source binding vlan <vlanid>

Description	Show the status of dynamic IP source binding per VLAN ID.	
Syntax	show ip source binding vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	VLAN Number **Valid values:** 1–4094 **Type:** Mandatory

show ip verify source

Description	Show IP verify source information.
Syntax	show ip verify source
Parameter	None

show ipv6 route static

Description	Show IPv6 static routes.
Syntax	show ipv6 route static
Parameter	None

show jumboframe

Description	Show jumbo frame settings.
Syntax	show jumboframe
Parameter	None

show lacp config

Description	Show LACP local configuration.
Syntax	show lacp config
Parameter	None

show lacp status

Description	Show information of either all or specific LACP groups.	
Syntax	show lacp status show lacp status <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Optional

show lacp status detail

Description	Show detail information of all LACP groups.
Syntax	show lacp status detail
Parameter	None

show lldp

Description	Show LLDP information.
Syntax	show lldp
Parameter	None

show lldp config

Description	Show LLDP configuration.
Syntax	show lldp config
Parameter	None

show lldp neighbors

Description	Show LLDP neighbors information.
Syntax	show lldp neighbors
Parameter	None

show lldp statistics

Description	Show LLDP statistics information.
Syntax	show lldp statistics
Parameter	None

show login-users

Description	Show logged-in users.
Syntax	show login-users
Parameter	None

show mgmt-radius-srv

Description	Show management authentication configuration.
Syntax	show mgmt-radius-srv
Parameter	None

show msti

Description	Show MSTI setting/status by instance or all.	
Syntax	show msti <index> show msti all	
Parameter		
	Name	**Description**
	<index>	**Valid values:** 1–10 **Type:** Optional

show multicast-fdb

Description	Show IGMP multicast forwarding table including by interface and VLAN.	
Syntax	show multicast-fdb show multicast-fdb interface gigabit <portNo> show multicast-fdb vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Optional
	<vlanid>	**Valid values:** 1–4094 **Type:** Optional

show multicast-fdb srclist

Description	Show IGMP multicast source list table.
Syntax	show multicast-fdb srclist
Parameter	None

show multicast-fdb static

Description	Show IGMP static multicast forwarding table including by interface and VLAN.	
Syntax	show multicast-fdb static show multicast-fdb static interface gigabit <portNo> show multicast-fdb static vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Optional
	<vlanid>	**Valid values:** 1–4094 **Type:** Optional

show ospf

Description	Show OSPF configure parameters.
Syntax	show ospf
Parameter	None

show ospf database

Description	Show OSPF database information.
Syntax	show ospf database
Parameter	None

show ospf database asbr-summary

Description	Show OSPF database information detail for ASBR summary link states.
Syntax	show ospf database asbr-summary
Parameter	None

show ospf database external

Description	Show OSPF database information detail for external link states.
Syntax	show ospf database external
Parameter	None

show ospf database network

Description	Show OSPF database information detail for network link states.
Syntax	show ospf database network
Parameter	None

show ospf database nssa-external

Description	Show OSPF database information detail for NSSA external link state.
Syntax	show ospf database nssa-external
Parameter	None

show ospf database router

Description	Show OSPF database information detail for NSSA router link states.
Syntax	show ospf database router
Parameter	None

show ospf database summary

Description	Show OSPF database information detail for network summary link states.
Syntax	show ospf database summary
Parameter	None

show ospf neighbor

Description	Show OSPF neighbor.
Syntax	show ospf neighbor
Parameter	None

show policer

Description	Show Ingress Policer table.
Syntax	show policer
Parameter	None

show port-isolation

Description	Show isolation information for all ports.
Syntax	show port-isolation
Parameter	None

show port-mirror

Description	Show port mirror information.
Syntax	show port-mirror
Parameter	None

show port-shaper

Description	Show port shaper information.
Syntax	show port-shaper
Parameter	None

show profile acl {<number>|all}

Description	Show ACL profile detail information.	
Syntax	show profile acl {<number>|all}	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–10 **Type:** Mandatory
	all	Show all ACL profile.

show profile alarm

Description	Show alarm profile list.
Syntax	show profile alarm
Parameter	None

show protocol-vlan

Description	Show protocol based VLAN information for all entries.
Syntax	show protocol-vlan
Parameter	None

show queue-scheduler profile

Description	Show Scheduler Profile table.
Syntax	show queue-scheduler profile
Parameter	None

show queue-shaper

Description	Show Queue Shaper information.
Syntax	show queue-shaper
Parameter	None

show ringv2

Description	Show ringv2 information.
Syntax	show ringv2
Parameter	None

show rip

Description	Show RIP information.
Syntax	show rip
Parameter	None

show runningcfg

Description	Show running configuration.
Syntax	show runningcfg
Parameter	None

show runningcfg backup

Description	Show running configuration backup.
Syntax	show runningcfg backup
Parameter	None

show runningcfg default

Description	Show default running configuration.
Syntax	show runningcfg default
Parameter	None

show snmp

Description	Show SNMP v2c, v3 information.
Syntax	show snmp
Parameter	None

show snmp group

Description	Show SNMP v3 group.
Syntax	show snmp group
Parameter	None

show snmp notify

Description	Show SNMP notify.
Syntax	show snmp notify
Parameter	None

show snmp target

Description	Show SNMP target.
Syntax	show snmp target
Parameter	None

show snmp user

Description	Show SNMP v3 user.
Syntax	show snmp user
Parameter	None

show snmp view

Description	Show SNMP v3 view.
Syntax	show snmp view
Parameter	None

show sntp

Description	Show SNTP information.
Syntax	show sntp
Parameter	None

show ssh

Description	Show SSH service.
Syntax	show ssh
Parameter	None

show ssl decrypted

Description	Show SSL certificate with decrypted format.
Syntax	show ssl decrypted
Parameter	None

show ssl encrypted

Description	Show SSL certificate with encrypted format.
Syntax	show ssl encrypted
Parameter	None

show stp

Description	System Wide Spanning Tree Setting/Status.
Syntax	show stp
Parameter	None

show syslog

Description	Show syslog configuration.
Syntax	show syslog
Parameter	None

show system information

Description	Show system information.
Syntax	show system information
Parameter	None

show system inventory

Description	Show system inventory.
Syntax	show system inventory
Parameter	None

show system layer3

Description	Show system layer3.
Syntax	show system layer3
Parameter	None

show telnetd

Description	Show telnet service.
Syntax	show telnetd
Parameter	None

show temperature

Description	Show temperature information.
Syntax	show temperature
Parameter	None

show time

Description	Show current time.
Syntax	show time
Parameter	None

show track

Description	Show Track object information.	
Syntax	show track show track <number>	
Parameter		
	Name	**Description**
	<number>	**Valid Values:** 1-64. **Type:** Optional

show uptime

Description	Show uptime.
Syntax	show uptime
Parameter	None

show version

Description	Show version information.
Syntax	show version
Parameter	None

show version detail

Description	Show detail version information.
Syntax	show version detail
Parameter	None

show vlan

Description	Show the port membership of all VLANs.
Syntax	show vlan
Parameter	None

show vlan <vlanid>

Description	Show the port membership of one VLAN.	
Syntax	show vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

show vlan { broadcast | unknown-mc | unknown-uc }

Description	Show storm control information by VLAN.	
Syntax	show vlan broadcast show vlan unknown-mc show vlan unknown-uc	
Parameter		
	Name	**Description**
	broadcast	Show broadcast storm control information by VLAN. **Type:** Mandatory
	unknown-mc	Show unknown multicast storm control information by VLAN. **Type:** Mandatory
	unknown-uc	Show unknown unicast storm control information by VLAN. **Type:** Mandatory

show vlan-trans

Description	Show VLAN translation table.
Syntax	show vlan-trans
Parameter	None

show vrrp

Description	Show VRRP information.
Syntax	show vrrp
Parameter	None

system restart

Description	Restart the system.
Syntax	system restart
Parameter	None

system restart <time>

Description	Schedule a system restart for the specified time.	
Syntax	system restart <time>	
Parameter		
	Name	**Description**
	<time>	**Valid values:** (“MM/DD/YYYY HH:MM:SS”) **Type:** Mandatory

system restart cancel

Description	Cancel a previously scheduled system restart.
Syntax	system restart cancel
Parameter	None

system stop ftp

Description	Stop a running FTP transfer.
Syntax	system stop ftp
Parameter	None

telnet <ip>

Description	Telnet to remote host at the specified ip address.	
Syntax	telnet <ip>	
Parameter		
	Name	**Description**
	<ip>	**Valid values:** Any valid IP **Type:** Mandatory

traceroute <ip>

Description	Print the route packets take to the specified IP address.	
Syntax	traceroute <ip>	
Parameter		
	Name	**Description**
	<ip>	**Valid values:** Any valid IP **Type:** Mandatory

Configure Mode Commands

To enter this execution mode type **configure** under any execution mode.

interface gigabit <portNo>

Description	Enter Interface Gigabit Mode.	
Syntax	interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

interface lag <number>

Description	Enter Interface LAG Mode.	
Syntax	interface lag <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–28 **Type:** Mandatory

profile acl

Description	Enter Profile ACL Mode.
Syntax	profile acl
Parameter	None

profile alarm

Description	Enter Profile Alarm Mode.
Syntax	profile alarm
Parameter	None

profile igmp-acl

Description	Enter Profile IGMP ACL Mode.
Syntax	profile igmp-acl
Parameter	None

profile igmp-mvr

Description	Enter Profile IGMP MVR Mode.
Syntax	profile igmp-mvr
Parameter	None

profile sch

Description	Enter ProfileScheduler Mode.
Syntax	profile sch
Parameter	None

interface vlan <vlanid>

Description	Enter Interface VLAN Mode.	
Syntax	interface vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

account add <username>

Description	Add an account.	
Syntax	account add <username> account add <username> password <password> account add <username> password <password> comment <comment> account add <username> password <password> level <account_level> account add <username> password <password> level <account_level> comment <comment>	
Parameter		
	Name	**Description**
	<username>	**Valid values:** 1–31 characters **Type:** Mandatory
	<password>	**Valid values:** 0–31 characters **Type:** Mandatory
	<account_level>	**Valid values:** superuser, engineer, and guest
	<comment>	**Valid values:** 0–31 characters **Type:** Mandatory

account delete <username>

Description	Delete an account	
Syntax	account delete <username>	
Parameter		
	Name	**Description**
	<username>	**Valid values:** 1–31 characters **Type:** Mandatory

account modify <username>

Description	Modify an account.	
Syntax	account modify <username> account modify <username> comment <comment> account modify <username> level <account_level> account modify <username> level <account_level> comment <comment> account modify <username> password <password> account modify <username> password <password> comment <comment> account modify <username> password <password> level <account_level> account modify <username> password <password> level <account_level> comment <comment>	
Parameter		
	Name	**Description**
	<username>	**Valid values:** 1–31 characters **Type:** Mandatory
	<password>	**Valid values:** 0–31 characters **Type:** Mandatory
	<account_level>	**Valid values:** superuser engineer guest **Type:** Mandatory
	<comment>	**Valid values:** 0–31 characters **Type:** Mandatory

aging <time>

Description	Configure aging time for a bridge port.	
Syntax	aging <time>	
Parameter		
	Name	**Description**
	<time>	**Valid values:** 10–600 (seconds) **Type:** Mandatory

alarm history clear

Description	Clear alarm history.
Syntax	alarm history clear
Parameter	None

clisettings <timeout>

Description	Configure CLI settings.	
Syntax	clisettings <timeout> clisettings <timeout> <flag> clisettings <timeout> <flag> <maxSessions>	
Parameter		
	Name	**Description**
	<timeout>	**Valid values:** 60–65535 seconds, 0: no timeout **Type:** Mandatory
	<flag>	**Valid values:** bitmap showAlarm(0) showEvent(1) showReadWriteStatus(2) **Type:** Optional
	<maxSessions>	**Valid values:** 1–10 sessions **Type:** Optional

cos-queue-mapping cos <priority> queue <number>

Description	Set CoS and queue mapping.	
Syntax	cos-queue-mapping cos <priority> queue <number>	
Parameter		
	Name	**Description**
	<priority>	**Valid values:** 0–7 **Type:** Mandatory
	<number>	**Valid values:** 0–7 **Type:** Mandatory

counter interface-counter clear <portNo>

Description	Clear interface counter per gigabit port.	
Syntax	counter interface-counter clear <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

counter rmon-counter clear <portNo>

Description	Clear Ethernet counter per gigabit port.	
Syntax	counter rmon-counter clear <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

default all

Description	Set all configurations to default.	
Syntax	default all default all except account	
Parameter		
	Name	**Description**
	except account	Set all configurations to default except user account. **Type:** Mandatory

default-gateway <default_gateway>

Description	Configure default gateway IP address.	
Syntax	default-gateway <default_gateway>	
Parameter		
	Name	**Description**
	<default_gateway>	**Type:** Mandatory

dot1x clear dot1x-radius-stats

Description	Clear dot1x radius-stats.
Syntax	dot1x clear dot1x-radius-stats
Parameter	None

dot1x clear eapol-stats {<portNo>|all}

Description	Clear dot1x EAPOL stats.	
Syntax	dot1x clear eapol-stats {<portNo>|all}	
Parameter		
	Name	**Description**
	<portNo>	Gigabit port. **Valid values:** 1–28 **Type:** Mandatory

dot1x radius set <ip> <auth_port> <secret>

Description	Set dot1x parameters.	
Syntax	dot1x radius set <ip> <auth_port> <secret>	
Parameter		
	Name	**Description**
	<ip>	IP address. **Format**: 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<auth_port>	Authentication port. **Valid values:** 1–65535 **Default values:** 1812 **Type:** Mandatory
	<secret>	Authentication key. **Length:** 0–16 **Type:** Mandatory

dot1x system-auth-control {enable|disable}

Description	Set system-auth-control.
Syntax	dot1x system-auth-control {enable|disable}
Parameter	None

event clear

Description	Clear event.
Syntax	event clear
Parameter	None

ext-tpid <number>

Description	Set tpid.	
Syntax	ext-tpid <number>	
Parameter		
	Name	**Description**
	<number>	tpid **Valid values:** 0x0001–0xffff **Type:** Mandatory

fdb-delete interface gigabit <portNo>

Description	Delete forwarding table entries per gigabit port.	
Syntax	fdb-delete interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

fdb-delete all

Description	Delete all dynamic entries from forwarding table.	
Syntax	fdb-delete all	
Parameter		
	Name	**Description**
	all	Delete all dynamic FDB entries. **Type:** Mandatory

fdb-delete interface lag <number>

Description	Delete forwarding table per trunk group.	
Syntax	fdb-delete interface lag <number>	
Parameter		
	Name	**Description**
	<number>	Trunk group index. **Valid values:** 1–28 **Type:** Mandatory

fdb-delete vlan <vlanid>

Description	Delete Forwarding table entries per VLAN index.	
Syntax	fdb-delete vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

fdbstatic <number> interface gigabit <portno> <vlanid> <mac>

Description	Create static MAC forwarding table entry.	
Syntax	fdb <number> interface gigabit <portNo> <vlanid> <mac>	
Parameter		
	Name	**Description**
	<number>	Entry position. **Valid values:** 1–512 **Type:** Mandatory
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory
	<mac>	**Valid values:** xx:xx:xx:xx:xx:xx **Type:** Mandatory

fdb-delete all

Description	Delete all entries of static MAC forwarding table.
Syntax	fdb-delete all
Parameter	None

fdbstatic delete interface gigabit <portNo>

Description	Delete static MAC forwarding table entry per gigabit port.	
Syntax	fdbstatic delete interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

fdb-delete vlan <vlanid>

Description	Delete static MAC forwarding table entry per VLAN index.	
Syntax	fdb-delete vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

firmware partition <partition>

Description	Set boot partition.	
Syntax	firmware partition <partition>	
Parameter		
	Name	**Description**
	<partition>	**Valid values:** 0–1 **Type:** Mandatory

firmware write <ip>

Description	Perform Remote Download. Schedule a remote download (scheduled upgrade).	
Syntax	firmware write <ip> <username> <password> <string> {bootloader| image} firmware write <ip> <username> <password> <string> {bootloader| image} {noreboot|<time>} firmware write <ip> <username> <password> <string> {bootloader| image} noreboot <time>	
Parameter		
	Name	**Description**
	<ip>	**Type:** Mandatory
	<username>	**Valid values:** 1–32 characters **Type:** Mandatory
	<password>	**Valid values:** 0–32 characters **Type:** Mandatory
	<string>	Image path and filename. **Valid values:** 1–64 characters. **Type:** Mandatory
	image	Perform remote download for the software image. **Type:** Mandatory
	bootloader	Perform remote download for the boot loader **Type:** Mandatory
	noreboot	Perform remote download without reboot. Must reboot system manually for the change to take effect! **Type:** Optional
	<time>	Time for scheduled upgrade. (MM/DD/YYYY HH:MM:SS) **Type:** Optional

firmware write cancel

Description	Cancel scheduled firmware upgrade.
Syntax	firmware write cancel
Parameter	None

firmware write tftp <ip>

Description	Perform Remote Download with TFTP server. Schedule a remote download (scheduled upgrade).	
Syntax	firmware write tftp <ip> <string> image firmware write tftp <ip> <string> image {noreboot|<time>} firmware write tftp <ip> <string> image noreboot <time>	
Parameter		
	Name	**Description**
	<ip>	**Type:** Mandatory
	<string>	Image path and filename. **Valid values:** 1–64 characters. **Type:** Mandatory
	image	Perform remote download for the software image. **Type:** Mandatory
	noreboot	Perform remote download without reboot. Must reboot system manually for the change to take effect! **Type:** Optional
	<time>	Time for scheduled upgrade. (MM/DD/YYYY HH:MM:SS) **Type:** Optional

gvrp {enable|disable}

Description	Enable or disable GVRP function.
Syntax	gvrp enable gvrp disable
Parameter	None

gvrp leave-all-time

Description	Configure GVRP leave-all-time.	
Syntax	gvrp leave-all-time <value>	
Parameter		
	Name	**Description**
	<value>	**Range:** 10–10000 in centiseconds.

http port {<portNo>|default}

Description	Set HTTP server port.	
Syntax	http port <portNo> http port default	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–65535 **Type:** Mandatory
	default	Set http server port to default (80) **Type:** Mandatory

https {enable|disable}

Description	Enable/Disable https.
Syntax	https {enable|disable}
Parameter	None

https port {<portNo>|default}

Description	Set https port by specific port or default port.	
Syntax	https port {<portNo>|default}	
Parameter		
	Name	**Description**
	<portNo>	https port number. **Valid values:** 1–65535 **Type:** Mandatory
	default	https default port number is 433. **Type:** Mandatory

igmp snooping {disable}

Description	Enable/Disable system IGMP snooping.
Syntax	igmp snooping igmp snooping disable
Parameter	None

ip dhcp class <index> disable

Description	Enable/Disable the specified DHCP class.	
Syntax	ip dhcp class <index> ip dhcp class <index> disable	
Parameter		
	Name	**Description**
	<index>	DHCP class identifier. **Value:** 1-128 **Type:** Mandatory

ip dhcp class <index> option {agent-circuit-id|agent-remote-id|client-id} {user-ascii|user-hex|hw-addr} <string>

Description	Configure the DHCP class option for the specified class.	
Syntax	ip dhcp class <index> option agent-circuit-id {user-ascii|user-hex} ip dhcp class <index> option agent-remote-id {user-ascii|user-hex} ip dhcp class <index> option client-id {hw-addr|user-ascii|user-hex}	
Parameter		
	Name	**Description**
	<index>	DHCP class identifier. **Value:** 1-128 **Type:** Mandatory
	agent-circuit-id	Configure option82 agent circuit identifier. **Type:** Mandatory (select either agent-circuit-id, agent-remote-id, or client-id)
	agent-remote-id	Configure option82 agent remote identifier. **Type:** Mandatory (select either agent-circuit-id, agent-remote-id, or client-id)
	client-id	Configure option61 client identifier. **Type:** Mandatory (select either agent-circuit-id, agent-remote-id, or client-id)
	user-ascii <string>	User defined identifier for the selected option. **Value:** ASCII string (length 1-32) **Type:** Mandatory (select either user-ascii or user-hex for option 82, either user-ascii, user-hex or hw-addr for option 61)
	user-hex <string>	User defined identifier for the selected option. **Value:** hex string (length 1-32) **Type:** Mandatory (select either user-ascii or user-hex for option 82, either user-ascii, user-hex or hw-addr for option 61)
	hw-addr <string>	Use a MAC address as the identifier for client-id. **Value:** MAC address (xx:xx:xx:xx:xx:xx) **Type:** Mandatory (select either user-ascii, user-hex or hw-addr for option 61)

ip dhcp pool <pool-id> disable

Description	Enter IP DHCP Pool Mode or disable a DHCP pool.	
Syntax	ip dhcp pool <pool-id> ip dhcp pool <pool-id> disable	
Parameter		
	Name	**Description**
	<pool-id>	DHCP Pool index **Valid values:** 1–20 **Type:** Mandatory

ip dhcp relay information check

Description	Check the relay information present in BOOTREPLY.
Syntax	ip dhcp relay information check
Parameter	None

ip dhcp relay information insert {disable}

Description	Enable/Disable the insertion of relay information in DHCP packets.
Syntax	ip dhcp relay information insert ip dhcp relay information insert disable
Parameter	None

ip dhcp relay information remote-id ascii <string>

Description	Configure an ASCII string as the value for remote-id.	
Syntax	ip dhcp relay information remote-id ascii <string>	
Parameter		
	Name	**Description**
	<string>	User defined value for remote-id. **Valid values:** ASCII string **Type:** Mandatory

ip dhcp relay information remote-id {hostname|sys-mac}

Description	Configure the system hostname or MAC address as the value for remote-id.	
Syntax	ip dhcp relay information remote-id {hostname|sys-mac}	
Parameter		
	Name	**Description**
	hostname	Use system hostname as remote-id value. **Type:** Mandatory (choose either hostname or sys-mac)
	sys-mac	Use system MAC address as remote-id value. **Type:** Mandatory (choose either hostname or sys-mac)

ip dhcp relay server <index> {<ip>|disable}

Description	Enable/Disable DHCP relay server. Set IP while enabling	
Syntax	ip dhcp relay server <index> {<ip>|disable}	
Parameter		
	Name	**Description**
	<index>	Specify index of the DHCP server to configure. **Type:** Mandatory
	<ip>	IP address in dotted notation (x.x.x.x) **Type:** Mandatory (choose between <ip> or disable)
	disable	Disable the specified server. **Type:** Mandatory (choose between <ip> or disable)

ip dhcp server accept-broadcast {disable}

Description	Enable/Disable the acceptance of dhcp broadcast request messages.
Syntax	ip dhcp server accept-broadcast ip dhcp server accept-broadcast disable
Parameter	None

ip dhcp server delay-packet

Description	Set the max delayed packet number.	
Syntax	ip dhcp server delay-packet <number>	
Parameter		
	Name	**Description**
	<number>	Destination network address. **Value:** 1-20 **Type:** Mandatory

ip dhcp server delay-response

Description	Set the delay response for DHCP broadcast messages.	
Syntax	ip dhcp server delay-response <time>	
Parameter		
	Name	**Description**
	<time>	Delay response time. Multiply <time> by 100ms for actual value. **Value:** 1-25 **Type:** Mandatory

ip dhcp server {restart|start|stop}

Description	Restart/start/stop DHCP server.
Syntax	ip dhcp server restart ip dhcp server start ip dhcp server stop
Parameter	None

ip dhcp snooping binding delete all

Description	Delete all binding entries.
Syntax	ip dhcp snooping binding delete all
Parameter	None

ip dhcp snooping binding delete interface gigabit <portNo>

Description	Delete specific port binding entry.	
Syntax	ip dhcp snooping binding delete interface gigabit <portNo>	
Parameter		
	Name	**Description**
	<portNo>	Port Number **Valid values:** 1–28

ip dhcp snooping binding delete vlan <vlanid>

Description	Delete specific VLAN binding entry.	
Syntax	ip dhcp snooping binding delete vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	VLAN Number **Valid values:** 1–4094

ip dhcp snooping disable

Description	Disable system DHCP snooping.
Syntax	ip dhcp snooping disable
Parameter	None

ip route add <network> netmask <netmask> gateway <gateway>

Description	Add a route.	
Syntax	ip route add <network> netmask <netmask> gateway <gateway>	
Parameter		
	Name	**Description**
	<network>	Destination network address. **Type:** Mandatory
	<netmask>	**Type:** Mandatory
	<gateway>	**Type:** Mandatory

ip route delete <network> netmask <netmask>

Description	Delete a route.	
Syntax	ip route delete <network> netmask <netmask>	
Parameter		
	Name	**Description**
	<network>	Destination network address. **Type:** Mandatory
	<netmask>	**Type:** Mandatory

ip route rip delete all

Description	Delete all RIP routes.
Syntax	ip route rip delete all
Parameter	None

ip routing {enable|disable}

Description	Enable/Disable IP routing.
Syntax	ip routing {enable|disable}
Parameter	None

ip source binding add interface gigabit <portNo> <vlan> <ip> <hwaddr>

Description	Add IP source binding to an interface.	
Syntax	ip source binding add interface gigabit <portNo> <vlan> <ip> <hwaddr>	
Parameter		
	Name	**Description**
	<portNo>	Port Number **Valid values:** 1–28
	<vlan>	VLAN ID **Valid values:** 1–4094
	<ip>	IP address number
	<hwaddr>	Hardware address

ip source binding delete

Description	Delete all dynamic IP source binding or delete them from interfaces, static entries, or VLAN.	
Syntax	ip source binding delete all ip source binding delete interface gigabit <portNo> ip source binding delete vlan <vlanid> ip source binding delete static all ip source binding delete static interface gigabit <portNo> ip source binding delete static vlan <vlanid> ip source binding delete static interface gigabit <portNo> <vlanid> <ip> <hwaddr>	
Parameter		
	Name	**Description**
	<portNo>	Port Number **Valid values:** 1–28
	<vlanid>	VLAN Number **Valid values:** 1–4094
	<ip>	IP address number
	<hwaddr>	Hardware address

ipv6 route add <x:x:x:x::/1-128> nexthop <x:x:x:x::x> vlan <vlanid>

Description	Add a static route in IPv6 format.	
Syntax	ipv6 route add <x:x:x:x::/1-128> nexthop <x:x:x:x::x> vlan <vlanid> ipv6 route add <x:x:x:x::/1-128> nexthop <x:x:x:x::x> ipv6 route add <x:x:x:x::/1-128> vlan <vlanid>	
Parameter		
	Name	**Description**
	<x:x:x:x::/1- 128>	IPv6 prefix network and length.
	<x:x:x:x::x>	IPv6 address of next-hop.
	<vlanid>	VLAN ID **Valid values:** 1-4094

ipv6 route delete <x:x:x:x::/1-128>

Description	Delete a static route in IPv6 format.	
Syntax	ipv6 route delete <x:x:x:x::/1-128>	
Parameter		
	Name	**Description**
	<x:x:x:x::/1- 128>	IPv6 prefix network and length.

ipv6 unicast-routing

Description	Enable IPv6 unicast routing.
Syntax	ipv6 unicast-routing
Parameter	None

ipv6 unicast-routing disable

Description	Disable IPv6 unicast routing.
Syntax	ipv6 unicast-routing disable
Parameter	None

jumboframe {enable | disable}

Description	Set jumbo frame settings.	
Syntax	jumboframe {enable | disable}	
Parameter		
	Name	**Description**
	enable	Enable jumbo frame.
	disable	Disable jumbo frame.

jumboframe mtu <value>

Description	MTU size.	
Syntax	jumboframe mtu <value>	
Parameter		
	Name	**Description**
	<value>	Range. **Valid values:** 1536–9000 (bytes) **Type:** Mandatory

lacp filter disable

Description	Always bypass incoming LACP PDUs.	
Syntax	lacp filter disable	
Parameter		
	Name	**Description**
	disable	Disable LACP filter.

lacp filter forward

Description	Accept LACP PDUs received on the LACP port and bypass it on the non-LACP port.	
Syntax	lacp filter forward	
Parameter		
	Name	**Description**
	forward	Receive on the LACP port and bypass on the non-LACP port.

lacp filter hard-drop

Description	Always drop incoming LACP PDUs.	
Syntax	lacp filter hard-drop	
Parameter		
	Name	**Description**
	hard-drop	Drop incoming LACP PDUs.

lacp filter soft-drop

Description	Accept LACP PDUs received on the LACP port and drop it on the non-LACP port.	
Syntax	lacp filter soft-drop	
Parameter		
	Name	**Description**
	soft-drop	Receive on the LACP port and drop on the non-LACP port.

lacp priority <value>

Description	Configure LACP system priority.	
Syntax	lacp priority <value>	
Parameter		
	Name	**Description**
	<value>	Range. **Valid values:** 1–65535

lldp delay <TxDelay>

Description	Set LLDP Tx delay (seconds).	
Syntax	lldp delay <TxDelay>	
Parameter		
	Name	**Description**
	<TxDelay>	Range. **Valid values:** 1-8192

lldp holdtime <TxHold>

Description	Set LLDP Tx hold time (times).	
Syntax	lldp holdtime <TxHold>	
Parameter		
	Name	**Description**
	<TxHold>	Range. **Valid values:** 2–10

lldp interval <TxInterval>

Description	Set LLDP Tx interval (seconds).	
Syntax	lldp interval <TxInterval>	
Parameter		
	Name	**Description**
	<TxInterval>	Range. **Valid values:** 5–32768

lldp reinit <TxReinit>

Description	Set LLDP Tx reinitialization delay (seconds).	
Syntax	lldp reinit <TxReinit>	
Parameter		
	Name	**Description**
	<TxReinit>	Range. **Valid values:** 1–10

mgmt-auth mode {both | local}

Description	Configure authentication method for management login.	
Syntax	mgmt-auth mode {both | local}	
Parameter		
	Name	**Description**
	both	Set management authentication method to both (Radius first).
	local	Set management authentication method to local.

mgmt-auth session cache <time>

Description	Configure authentication session cache aging time.	
Syntax	mgmt-auth session cache <time>	
Parameter		
	Name	**Description**
	<time>	Session cache aging time (seconds). **Valid values:** 10-600. Default value is 30.

mgmt-radius-srv set <ipv4>

Description	Set radius server for radius authentication.	
Syntax	mgmt-radius-srv set <ipv4>	
Parameter		
	Name	**Description**
	<ipv4>	Radius server IP Address. **Valid values:** 0.0.0.0-255.255.255.255

mirror analyzer-port {enable | disable}

Description	Enable/Disable mirror analyzer and set port.	
Syntax	mirror analyzer-port {enable | disable}	
Parameter		
	Name	**Description**
	enable	Enable port mirror.
	disable	Disable port mirror.

mirror analyzer-port <portNo>

Description	Set analyzer port.	
Syntax	mirror analyzer-port <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

multicast-fdb delete

Description	Delete dynamic multicast fdb table entries.	
Syntax	multicast-fdb delete all multicast-fdb delete interface gigabit <portNo> multicast-fdb delete vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

multicast-fdb static delete

Description	Delete static multicast fdb table entry or entries.	
Syntax	multicast-fdb static delete <number> multicast-fdb static delete all multicast-fdb static delete interface gigabit <portNo> multicast-fdb static delete vlan <vlanid>	
Parameter		
	Name	**Description**
	<number>	Static multicast forwarding table entry index. **Valid values:** 1–128 **Type:** Mandatory
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

multicast-fdb static <number> interface gigabit <portNo> <vlan> <ipaddr>

Description	Create one static multicast fdb table entry.	
Syntax	multicast-fdb static <number> interface gigabit <portNo> <vlan> <ipaddr>	
Parameter		
	Name	**Description**
	<number>	Static multicast fdb table entry index. **Valid values:** 1–128 **Type:** Mandatory
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory
	<ipaddr>	Static IP address. **Valid values:** 224.0.0.0–239.255.255.255 **Type:** Mandatory

policer cos-mark green <green-number> yellow <yellow-number> red <red-number>

Description	Set ingress policer CoS remark mapping table.	
Syntax	policer cos-mark green <green-number> yellow <yellow-number> red <red-number>	
Parameter		
	Name	**Description**
	<green-number>	Color green and CoS number mapping. **Valid values:** 0–7 **Type:** Mandatory
	<yellow-number>	Color yellow and CoS number mapping. **Valid values:** 0–7 **Type:** Mandatory
	<red-number>	Color red and CoS number mapping. **Valid values:** 0–7 **Type:** Mandatory

policer dscp-mark green <green-number> yellow <yellow-number> red <red-number>

Description	Set ingress policer DSCP remark mapping table.	
Syntax	policer dscp-mark green <green-number> yellow <yellow-number> red <red-number>	
Parameter		
	Name	**Description**
	<green-number>	Color green and DSCP number mapping. **Valid values:** 0–63 **Type:** Mandatory
	<yellow-number>	Color yellow and DSCP number mapping. **Valid values:** 0–63 **Type:** Mandatory
	<red-number>	Color red and DSCP number mapping. **Valid values:** 0–63 **Type:** Mandatory

policer ingress-color {aware|blind}

Description	Enable/Disable ingress-color function.	
Syntax	policer ingress-color {aware|blind}	
Parameter		
	Name	**Description**
	aware	Enable ingress color function.
	blind	Disable ingress color function.

policer ingress-color cos <number> {green|yellow|red}

Description	Set ingress-color mapping table.	
Syntax	policer ingress-color cos <number> {green|yellow|red}	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 0–7 **Type:** Mandatory
	green|yellow|red	Green or yellow or red. **Type:** Mandatory

port-mirror {enable|disable}

Description	Enable/Disable port mirror.
Syntax	port-mirror enable port-mirror disable
Parameter	None

port-mirror monitor-port <portNo>

Description	Set the gigabit port to be monitored.	
Syntax	port-mirror monitor-port <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

port-mirror {tx-analyzer-port|rx-analyzer-port} <portNo>

Description	Set Tx analyzer port (monitor 'out' packet of monitored port)/Rx analyzer port (monitor 'in' packet of monitored port).	
Syntax	port-mirror tx-analyzer-port <portNo> port-mirror rx-analyzer-port <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

prompt <prompt>

Description	Prompt (1–31 characters)
Syntax	prompt <prompt>
Parameter	None

prompt default

Description	Set prompt to default
Syntax	prompt default
Parameter	None

ringv2-group <number>

Description	Enter RingV2 Group Mode.	
Syntax	ringv2-group <number>	
Parameter		
	Name	**Description**
	<number>	Ring group index **Valid values:** 1–3 **Type:** Mandatory

route ospf

Description	Enter Router OSPF Mode.
Syntax	route ospf
Parameter	None

route rip

Description	Enter Router RIP Mode.
Syntax	route rip
Parameter	None

runningcfg clear

Description	Clear configuration.	
Syntax	runningcfg clear all runningcfg clear all noreboot runningcfg clear general runningcfg clear general noreboot	
Parameter		
	Name	**Description**
	all	Clear all configuration. **Type:** Mandatory
	general	Clear general configuration. **Type:** Mandatory
	noreboot	Clear configuration without Reboot. Must reboot system manually for the changes to take effect! **Type:** Optional

runningcfg get <ip> <username> <password> {binary|cli} <string>

Description	Get exported configuration files from a FTP server.	
Syntax	runningcfg get <ip> <username> <password> binary <string> runningcfg get <ip> <username> <password> cli <string>	
Parameter		
	Name	**Description**
	<ip>	**Type:** Mandatory
	<username>	**Valid values:** 1–32 characters **Type:** Mandatory
	<password>	**Valid values:** 0–32 characters **Type:** Mandatory
	binary	Get two binary images. **Type:** Mandatory
	cli	Get two CLI scripts **Type:** Mandatory
	<string>	Remote filename prefix. **Valid values:** 1–64 characters. **Type:** Mandatory

runningcfg import download

Description	Import configuration from files retrieved via 'runningcfg get'.	
Syntax	runningcfg import download binary runningcfg import download binary noreboot runningcfg import download cli runningcfg import download cli noreboot	
Parameter		
	Name	**Description**
	binary	Import configuration from binary images retrieved via 'runningcfg get'. **Type:** Mandatory
	cli	Import configuration from the CLI scripts retrieved via 'runningcfg get'. **Type:** Mandatory
	Noreboot	Import configuration without Reboot. Must reboot system manually for the changes to take effect! **Type:** Optional

runningcfg put <ip> <username> <password> {binary|cli} <string>

Description	Put exported configuration files to a FTP server.	
Syntax	runningcfg put <ip> <username> <password> binary <string> runningcfg put <ip> <username> <password> cli <string>	
Parameter		
	Name	**Description**
	<ip>	**Type:** Mandatory
	<username>	**Valid values:** 1–32 characters **Type:** Mandatory
	<password>	**Valid values:** 0–32 characters **Type:** Mandatory
	binary	Uploads two binary images to the device. **Type:** Mandatory
	cli	Uploads CLI scripts to the device **Type:** Mandatory
	<string>	Remote filename prefix **Valid values:** 1–64 characters **Type:** Mandatory

runningcfg replace-save <inbandBackupIndex>

Description	Save running config to FLASH replacing existing the specified backup.	
Syntax	runningcfg replace-save <inbandBackupIndex> runningcfg replace-save <inbandBackupIndex> <inbandBackupName> runningcfg replace-save <inbandBackupIndex> <inbandBackupName> <generalBack-upIndex> runningcfg replace-save <inbandBackupIndex> <inbandBackupName> <generalBack-upIndex> <generalBackupName>	
Parameter		
	Name	**Description**
	<inbandBackupIndex>	**Valid values:** 1–16 **Type:** Mandatory
	<inbandBackupName>	**Valid values:** 1–31 characters **Type:** Optional
	<generalBackupIndex>	**Valid values:** 1–16 characters **Type:** Optional
	<generalBackupName>	**Valid values:** 1–31 characters **Type:** Optional

runningcfg restore index <inbandBackupIndex>

Description	Restore configuration	
Syntax	runningcfg restore index <inbandBackupIndex> runningcfg restore index <inbandBackupIndex> <generalBackupIndex> runningcfg restore index <inbandBackupIndex> <generalBackupIndex> noreboot	
Parameter		
	Name	**Description**
	<inbandBackupIndex>	**Valid values:** 1–16 **Type:** Mandatory
	<generalBackupIndex>	**Valid values:** 1–16 characters **Type:** Optional (if omitted, use the same index as <inbandBackupIndex>
	noreboot	Restore database without reboot. Must reboot system manually for the changes to take effect! **Type:** Optional

runningcfg restore name <inbandBackupName>

Description	Restore configuration	
Syntax	runningcfg restore name <inbandBackupName> runningcfg restore name <inbandBackupName> <generalBackupName> runningcfg restore name <inbandBackupName> <generalBackupName> noreboot	
Parameter		
	Name	**Description**
	<inbandBackupIndex>	**Valid values:** 1–31 characters **Type:** Mandatory
	<generalBackupIndex>	**Valid values:** 1–31 characters **Type:** Optional (if omitted, use the same index as <inbandBackupName>)
	noreboot	Restore database without reboot. Must reboot system manually for the changes to take effect! **Type:** Optional

runningcfg save

Description	Save running config to FLASH.	
Syntax	runningcfg save runningcfg save <inbandBackupName> runningcfg save <inbandBackupName> <generalBackupName>	
Parameter		
	Name	**Description**
	<inbandBackupIndex>	**Valid values:** 1–31 characters **Type:** Optional
	<generalBackupIndex>	**Valid values:** 1–31 characters **Type:** Optional (if omitted, use the same index as <inbandBackupName>)

setenv pagefilter <enabled>

Description	Configure Page Filter.	
Syntax	sentev pagefilter	
Parameter		
	Name	**Description**
	<enabled>	Enable Page Filter **Valid values:** (0: disable, 1: enable) **Type:** Mandatory

setenv script-delay <delay>

Description	Configure script delay.	
Syntax	setenv script-delay <delay>	
Parameter		
	Name	**Description**
	<delay>	Script Delay **Valid values:** 1–0xFFFFFFFF ms **Type:** Mandatory

setenv show-date-time-in-prompt <enabled>

Description	Show Date/Time in Prompt (0: disable, 1: enable)	
Syntax	setenv show-date-time-in-prompt <enabled>	
Parameter		
	Name	**Description**
	<enabled>	enabled **Valid values:** (0:disable, 1:enable) **Type:** Mandatory

snmp { disable | enable }

Description	Enable or disable the snmp service.	
Syntax	snmp { disable | enable }	
Parameter		
	Name	**Description**
	disable	Disable snmp **Type:** Mandatory
	enable	Enable snmp **Type:** Mandatory

snmp <index> notify <name> <tag>

Description	Configure snmp notify.	
Syntax	snmp <index> notify <name> <tag>	
Parameter		
	Name	**Description**
	<index>	Index. **Valid values:** 1–32 **Type:** Mandatory
	notify	Configure snmp notify **Type:** Mandatory
	<name>	Notify name **Valid values:** 1–31 characters **Type:** Mandatory
	<tag>	Notify tag **Valid values:** 1–31 characters **Type:** Mandatory

snmp <index> notify delete

Description	Configure snmp notify.	
Syntax	snmp <index> notify delete	
Parameter		
	Name	**Description**
	<index>	Index. **Valid values:** 1–32 **Type:** Mandatory
	notify	Configure snmp notify **Type:** Mandatory
	delete	Delete a snmp target. **Type:** Mandatory

snmp <index> target <ip> <port> <name> <tag> { v1 | v2c | v3 }

Description	Configure snmp target.	
Syntax	snmp <index> target <ip> <port> <name> <tag> { v1 | v2c | v3 }	
Parameter		
	Name	**Description**
	<index>	Scheduler profile index. **Valid values:** 1–32 **Type:** Mandatory
	target	Configure snmp target. **Type:** Mandatory
	ip	Target IP address. **Type:** Mandatory
	port	Target port. **Valid values:** 1–65535 **Type:** Mandatory
	name	Target name. **Valid values:** 1–31 **Type:** Mandatory
	tag	Target tag list. **Type:** Mandatory
	v1	Send version 1 trap
	v2c	Send version 2c trap
	v3	Send version 3 trap

snmp <index> target delete

Description	Delete a snmp target.	
Syntax	snmp <index> target delete	
Parameter		
	Name	**Description**
	<index>	Scheduler profile index. **Valid values:** 1–32 **Type:** Mandatory
	target	Configure snmp target. **Type:** Mandatory
	delete	Delete a snmp target. **Type:** Mandatory

snmp community <name> group <name>

Description	Configure snmp community.	
Syntax	snmp community <name> group <name>	
Parameter		
	Name	**Description**
	<name>	Community name. **Valid values:** 1–31 characters **Type:** Mandatory
	group	Configure a community to bind with a group **Type:** Mandatory
	<name>	Group name. **Valid values:** (1–15 characters) (input ‘none’ to unbind) **Type:** Mandatory

snmp community <name> ro

Description	Configure snmp community.	
Syntax	snmp community <name> ro	
Parameter		
	Name	**Description**
	<name>	Community name. **Valid values:** 1–31 characters **Type:** Mandatory
	ro	Configure a community access right as read-only. **Type:** Mandatory

snmp community <name> rw

Description	Config snmp community.	
Syntax	snmp community <name> rw	
Parameter		
	Name	**Description**
	<name>	Community name. **Valid values:** 1–31 characters **Type:** Mandatory
	rw	Configure a community access right as read-write. **Type:** Mandatory

snmp community <name> view <name>

Description	Config snmp community.	
Syntax	snmp community <name> view <name>	
Parameter		
	Name	**Description**
	<name>	Community name. **Valid values:** 1–31 characters **Type:** Mandatory
	view	Config a community to bind with a group. **Type:** Mandatory
	<name>	Group name. **Valid values:** (1–15 characters) (input ‘none’ to unbind) **Type:** Mandatory

snmp create-community { ro | rw } <name> { view | group } <name>

Description	Config snmp community.	
Syntax	snmp create-community { ro | rw } <name> { view | group } <name>	
Parameter		
	Name	**Description**
	ro	Create a snmp community (read only). **Type:** Mandatory
	rw	Create a snmp community (read, write). **Type:** Mandatory
	<name>	Community name. **Valid values:** 1–31 characters **Type:** Mandatory
	view	Create a snmp community (read only) and bind it with a view. **Type:** Mandatory
	group	Create a snmp community (read only) and bind it with a group. **Type:** Mandatory
	<name>	Group or view name. **Valid values:** 1–15 characters **Type:** Mandatory

snmp create-group <name> model { v1 | v2 | v3sum } level { auth | noauth | priv } read <name> write <name>

Description	Create snmp v3 access group.	
Syntax	snmp create-group <name> model { v1 | v2 | v3sum } level { auth | noauth | priv } read <name> write <name>	
Parameter		
	Name	**Description**
	<name>	Group name **Valid values:** 1–15 characters **Type:** Mandatory
	model	Security model of the group (v1/v2c/v3sum) **Type:** Mandatory
	v1	SNMP v1 security model.
	v2c	SNMP v2c security model.
	v3usm	SNMP v3 security model.
	level	Security level of the group (noauth/auth/priv) **Type:** Mandatory
	auth	Authentication, no privacy.
	noauth	No authentication, no privacy.
	priv	Both authentication and privacy.
	read	Specify a read view to this group.
	<name>	View name. **Valid values:** 1–15 characters **Type:** Mandatory
	write	Specify a write view to this group.
	<name>	View name. **Valid values:** 1–15 characters **Type:** Mandatory

snmp create-user { access | group} {ro | rw } {md5 | sha } <passPhrase> des <passPhrase

Description	Create snmp v3 user.	
Syntax	snmp create-user { access | group } { ro | rw } { md5 | sha } <passPhrase> des <passPhrase>	
Parameter		
	Name	**Description**
	<name>	User name **Valid values:** 1–31 characters **Type:** Mandatory
	access	Access right of user (ro/rw) **Type:** Mandatory
	group	Bind user to a group. **Type:** Mandatory
	ro	Read-only user
	rw	Read-write user
	md5	User MD5 as authentication protocol.
	sha	Use SHA as authentication protocol.
	<passPhrase>	Authentication pass phrase. **Valid values:** 8–15 characters **Type:** Mandatory
	des	Use DES as encryption protocol.
	<passPhrase>	Encryption pass phrase. **Valid values:** 8–15 characters **Type:** Mandatory

snmp create-view <name> type { exclude | include } subtree <subtree>

Description	Create snmp v3 view.	
Syntax	snmp create-view <name> type { exclude | include} subtree <subtree>	
Parameter		
	Name	**Description**
	<name>	View name **Valid values:** 1–15 characters **Type:** Mandatory
	type	View type of the subtree **Type:** Mandatory
	exclude	Exclude the subtree.
	include	Include the subtree.
	subtree	Set subtree (oid or name) of a view. **Type:** Mandatory
	<subtree>	Subtree, oid or name. **Valid values:** 1–31 characters **Type:** Mandatory

snmp delete-community name <name>

Description	Delete snmp community.	
Syntax	snmp delete-community name <name>	
Parameter		
	Name	**Description**
	name	Delete SNMP community. **Type:** Mandatory
	<name>	Community name **Valid values:** 1–31 characters **Type:** Mandatory

snmp delete-group name <name>

Description	Delete snmp v3 group.	
Syntax	snmp delete-group name <name>	
Parameter		
	Name	**Description**
	name	Delete snmp v3 group. **Type:** Mandatory
	<name>	Group name **Valid values:** 1–15 characters **Type:** Mandatory

snmp delete-user name <name>

Description	Delete snmp v3 user.	
Syntax	snmp delete-user name <name>	
Parameter		
	Name	**Description**
	name	Delete snmp v3 user. **Type:** Mandatory
	<name>	User name **Valid values:** 1–31 characters **Type:** Mandatory

snmp delete-view { index | name } { <index> | <name> }

Description	Delete snmp v3 access view.	
Syntax	snmp delete-view { index | name } { <index> | <name> }	
Parameter		
	Name	**Description**
	index	Delete snmp v3 view. **Type:** Mandatory
	name	Delete snmp v3 view. **Type:** Mandatory
	<index>	View index **Valid values:** 1–32 **Type:** Mandatory
	<name>	View name **Valid values:** 1–15 characters **Type:** Mandatory

snmp user <name> access { ro | rw }

Description	Config snmp v3 user access.	
Syntax	snmp user <name> access { ro | rw }	
Parameter		
	Name	**Description**
	<name>	User name **Valid values:** 1–31 characters **Type:** Mandatory
	access	Access right of user **Type:** Mandatory
	ro	Read-only user **Type:** Mandatory
	rw	Read-write user **Type:** Mandatory

snmp user <name> { aes | des } <passPhrase>

Description	Config user PRIV encryption	
Syntax	snmp user <name> { aes | des } <passPhrase>	
Parameter		
	Name	**Description**
	<name>	User name **Valid values:** 1–31 characters **Type:** Mandatory
	aes	Config user PRIV to AES encryption **Type:** Mandatory
	des	Config user PRIV to DES encryption **Type:** Mandatory
	<passPhrase>	PRIV pass phrase **Valid values:** 1–31 characters **Type:** Mandatory

snmp user <name> group <name>

Description	Bind user to a group	
Syntax	snmp user <name> group <name>	
Parameter		
	Name	**Description**
	<name>	User name **Valid values:** 1–31 characters **Type:** Mandatory
	group	Bind user to a group **Type:** Mandatory
	<name>	Group name **Valid values:** 1–15 characters **Type:** Mandatory

snmp version { v2c | v3 }

Description	Config snmp version (v2c/v3).	
Syntax	snmp version { v2c | v3 }	
Parameter		
	Name	**Description**
	v2c	Set snmp version to v2c
	v3	Set snmp version to v3

sntp polling-interval <interval>

Description	Set SNTP Polling interval	
Syntax	sntp polling-interval <interval>	
Parameter		
	Name	**Description**
	<interval>	**Valid values:** 60–65535 seconds, 0: disable polling **Type:** Mandatory

sntp server address <ip>

Description	Set SNTP server address.	
Syntax	sntp server address <ip>	
Parameter		
	Name	**Description**
	<ip>	**Type:** Mandatory

sntp sync

Description	Manual SNTP synchronization
Syntax	sntp sync
Parameter	None

ssh { disable | enable }

Description	Configure SSH service	
Syntax	ssh { disable | enable }	
Parameter		
	Name	**Description**
	disable	Disable ssh service **Type:** Mandatory
	enable	Enable ssh service **Type:** Mandatory

ssl default-certificate

Description	Use system default SSL certificate.
Syntax	ssl default-certificate
Parameter	None

ssl regenerate

Description	Regenerate SSL certificate
Syntax	ssl regenerate
Parameter	None

ssl upload

Description	Upload new SSL certificate.
Syntax	ssl upload
Parameter	None

stp {disable|enable}

Description	Configure spanning tree protocol settings.	
Syntax	stp {disable|enable}	
Parameter		
	Name	**Description**
	disable	Disable STP.
	enable	Enable STP.

stp bpdu {deny|flooding}

Description	Set BPDU packet filter (deny/flooding).	
Syntax	stp bpdu {deny|flooding}	
Parameter		
	Name	**Description**
	deny	Deny BPDU packet.
	flooding	Flood BPDU packet.

stp forward-delay <number>

Description	Set STP forward delay time.	
Syntax	stp forward-delay <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 4–30 (seconds) **Type:** Mandatory

stp hello-time <number>

Description	Set STP hello time.	
Syntax	stp hello-time <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–10 (seconds) **Type:** Mandatory

stp max-age <number>

Description	Set STP max age value.	
Syntax	stp max-age <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 6–40 (seconds) **Type:** Mandatory

stp msti <index> { add | delete } { <vlan> | range }

Description	Set MSTP instance.	
Syntax	stp msti <index> { add | delete} { <vlan> | range }	
Parameter		
	Name	**Description**
	<index>	MSTP instance. **Valid values:** 1–10 **Type:** Mandatory
	add	Add VLAN ID to MSTP instance.
	delete	Delete MSTP instance.
	<vlan>	VLAN ID **Valid values:** 1–4094
	range	Add multiple VLAN ID to MSTP instance.

stp msti <index> create <name>

Description	Create MSTP instance.	
Syntax	stp msti <index> create <name>	
Parameter		
	Name	**Description**
	<index>	MSTP instance. **Valid values:** 1–10 **Type:** Mandatory
	<name>	MSTP instance name. Valid values: String (length 1-30)

stp msti <index> set <name>

Description	Set the name for an MSTP instance.	
Syntax	stp msti <index> set <name>	
Parameter		
	Name	**Description**
	<index>	MSTP instance. **Valid values:** 1–10 **Type:** Mandatory
	<name>	MSTP instance name. **Valid values**: String (length 1-30) **Type:** Mandatory

stp msti <index> set <priority>

Description	Set the priority for an MSTP instance.	
Syntax	stp msti <index> set <priority>	
Parameter		
	Name	**Description**
	<index>	MSTP instance. **Valid values:** 1–10 **Type:** Mandatory
	<priority>	MSTP instance name. **Valid values**: (0-61440, step 4096) **Type**: Mandatory

stp priority <number>

Description	Set STP priority.	
Syntax	stp priority <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 0–61440 step 4096 **Type:** Mandatory

stp region-name <name>

Description	Set STP Region Name.	
Syntax	stp region-name <name>	
Parameter		
	Name	**Description**
	<name>	Region Name **Valid values:** Length 0–32 **Type:** Mandatory

stp revision <value>

Description	Set STP Revision Level.	
Syntax	stp revision <value>	
Parameter		
	Name	**Description**
	<value>	Revision Level value. **Valid values:** 0–65535 **Type:** Mandatory

stp version {stp|rstp|mstp}

Description	Set STP version.	
Syntax	stp version {stp|rstp|mstp}	
Parameter		
	Name	**Description**
	stp	Spanning tree protocol.
	rstp	Rapid spanning tree protocol
	mstp	Multiple spanning tree protocol

syslog {enable|disable}

Description	Disable or enable syslog service.
Syntax	syslog enable syslog disable
Parameter	None

syslog server <ip>

Description	Configure syslog server IP address.	
Syntax	syslog server <ip>	
Parameter		
	Name	**Description**
	<ip>	Syslog server IP address **Type:** Mandatory

system-info contact <string>

Description	Modify system contact.	
Syntax	system-info contact <string>	
Parameter		
	Name	**Description**
	<string>	**Valid values:** 0–255 characters (ASCII code: 0x20–0x7E) **Type:** Mandatory

system-info location <string>

Description	Modify system location.	
Syntax	system-info location <string>	
Parameter		
	Name	**Description**
	<string>	**Valid values:** 0–255 characters (ASCII code: 0x20–0x7E) **Type:** Mandatory

system-info name <string>

Description	Modify system name.	
Syntax	system-info name <string>	
Parameter		
	Name	**Description**
	<string>	**Valid values:** 0–255 characters (ASCII code: 0x21–0x7E) **Type:** Mandatory

telnetd {enable|disable}

Description	Disable or enable telnetd service.
Syntax	telnetd enable telnetd disable
Parameter	None

temperature shift down <time>

Description	Set downshift time.	
Syntax	temperature shift down <time>	
Parameter		
	Name	**Description**
	<time>	**Valid values:** 1–255 seconds **Type:** Mandatory

temperature shift up <time>

Description	Set upshift time.	
Syntax	temperature shift up <time>	
Parameter		
	Name	**Description**
	<time>	**Valid values:** 1–255 seconds **Type:** Mandatory

temperature threshold down <threshold>

Description	Set downshift temperature threshold.	
Syntax	temperature threshold down <threshold>	
Parameter		
	Name	**Description**
	<threshold>	**Valid values:** -55 to 85° C **Type:** Mandatory

temperature threshold up <threshold>

Description	Set upshift temperature threshold.	
Syntax	temperature threshold up <threshold>	
Parameter		
	Name	**Description**
	<threshold>	**Valid values:** -55 to 85° C **Type:** Mandatory

time set {date|time}

Description	Set date/time.	
Syntax	time set date <month> <day> <year> time set time <hour> <minute> time set time <hour> <minute> <second>	
Parameter		
	Name	**Description**
	<month>	**Valid values:** 1–12 **Type:** Mandatory
	<day>	**Valid values:** 1–31 **Type:** Mandatory
	<year>	**Valid values:** 0–36 (meaning 2000 – 2036) **Type:** Mandatory
	<hour>	**Valid values:** 0–23 **Type:** Mandatory
	<minute>	**Valid values:** 0–59 **Type:** Mandatory
	<second>	**Valid values:** 0–59 **Type:** Optional

time set timezone

Description	Set timezone.	
Syntax	time set timezone <timezone> time set timezone default	
Parameter		
	Name	**Description**
	<timezone>	**Valid values:** please see 'list timezone' **Type:** Mandatory

track <number> disable

Description	Delete track object.
Syntax	track <number> disable
Parameter	None

track <number> interface

Description	Configure track to interface.	
Syntax	track <number> interface gigabit <portNo> track <number> interface vlan <vlanid>	
Parameter		
	Name	**Description**
	<portNo>	**Range:** 1–28
	<vlanid>	**Range:** 1–4094

track <number> route

Description	Configure track to route.	
Syntax	track <number> route <ip> polling <time> threshold <time> track <number> route <ip> threshold <time>	
Parameter		
	Name	**Description**
	<number>	Track ID. **Range:** 1–64
	<ip>	IP address
	Polling <time>	**Range:** 1–600 in second.
	Threshold <time>	**Range:** 1–3000 in second.

track <number> vrrp <groupid>

Description	Configure track to vrrp group.	
Syntax	track <number> vrrp <groupid>	
Parameter		
	Name	**Description**
	<number>	Track ID **Range:** 1–64
	<groupId>	**Range:** 1–255

vlan <vlanid>

Description	Configure VLAN.	
Syntax	vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	Create an empty VLAN index. **Valid values:** 1–4094 **Type:** Mandatory

vlan <vlanid> {<name> | broadcast | disable | unknown-mc | unknown-uc} {block | forward}

Description	Configure VLAN's name.	
Syntax	vlan <vlanid> {<name> | broadcast | disable | unknown-mc | unknown-uc} { block | forward}	
Parameter		
	Name	**Description**
	<vlanid>	Create an empty VLAN index. **Valid values:** 1–4094 **Type:** Mandatory
	<name>	VLAN Name (0–31) **String Size:** 0–31 **Type:** Mandatory
	broadcast	Set storm control for broadcast packet per VLAN
	disable	Delete VLAN memberset/settting
	unknown-mc	Set storm control for unknown multicast packet per VLAN
	unknown-uc	Set storm control for unknown unicast packet per VLAN
	block	Block broadcast packet
	forward	Forward broadcast packet

vlan <vlanid> disable

Description	Delete VLAN members.	
Syntax	vlan <vlanid> disable	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

vrrp {enable|disable}

Description	Enable or disable VRRP function.	
Syntax	vrrp disable vrrp enable v2 vrrp enable v3	
Parameter		
	Name	**Description**
	disable	Disable VRRP
	v2	Processing VRRPv2
	v3	Processing VRRPv3

Interface Gigabit Mode Commands

To enter this execution mode type **interface gigabit <portNo>** under the Configure Mode.

accfrm

Description	Set acceptable frame type.	
Syntax	accfrm {all|tag|untag}	
Parameter		
	Name	**Description**
	all	Accept all frames.
	tag	Accept tagged frame only.
	untag	Accept un-tagged frame only.

acl-profile-bind <number>

Description	Port ACL profile binding.	
Syntax	acl-profile-bind <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–10 **Type:** Mandatory

broadcast {block|forward}

Description	Block/Forward broadcast packet.
Syntax	broadcast block broadcast forward
Parameter	None

broadcast rate <rate>

Description	Set storm control rate limit for broadcast packet.	
Syntax	broadcast rate <rate>	
Parameter		
	Name	**Description**
	<rate>	**Valid values:** 1–1000000 (Kbps) **Type:** Mandatory

def-acl {permit|deny}

Description	Set port default ACL rule.
Syntax	def-acl permit def-acl deny
Parameter	None

default vlan

Description	Set default VLAN to gigabit port.	
Syntax	default vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

dot1x auth-port-control {auto | force-authorized | force-unauthorized}

Description	Set dot1x authentication type of PAE port.
Syntax	dot1x auth-port-control {auto | force-authorized | force-unauthorized}
Parameter	None

dot1x auth-quiet-period <period>

Description	Set quiet period of PAE port.	
Syntax	dot1x auth-quiet-period <period>	
Parameter		
	Name	**Description**
	<period>	The quiet period of PAE port. **Valid values:** 1–255 seconds **Default values:** 60 seconds **Type:** Mandatory

dot1x auth-server-timeout <timeout>

Description	Set the wait timeout of the Authenticator for Access-Challenge / Access-Accept / Access-Reject after sending Access-Request.	
Syntax	dot1x auth-server-timeout <timeout>	
Parameter		
	Name	**Description**
	<timeout>	Authenticator timeout. **Valid values:** 1–255 seconds **Default values:** 30 seconds **Type:** Mandatory

dot1x auth-supp-timeout <timeout>

Description	Set timeout of Authenticator wait for EAP-Response (exclude EAP-Request / Identify) after sending EAP-Request.	
Syntax	dot1x auth-supp-timeout <timeout>	
Parameter		
	Name	**Description**
	<timeout>	Authenticator timeout. **Valid values:** 1–255 seconds **Default values:** 30 seconds **Type:** Mandatory

dot1x auth-tx-period <period>

Description	Set timeout of Authenticator waiting for EAP-Response / Identity from supplication of PAE port.	
Syntax	dot1x auth-tx-period <period>	
Parameter		
	Name	**Description**
	<period>	The quiet period of PAE port. **Valid values:** 1–255 seconds **Default values:** 30 seconds **Type:** Mandatory

dot1x {force-reinitialize|force-reauthenticate}

Description	Enable for force PAE port re-initialize / re-authenticate.
Syntax	dot1x {force-reinitialize| force-reauthenticate}
Parameter	None

dot1x max-req <number>

Description	Set the max number of times the backend Authenticator can send EAP-Request to supplicant before restarting the authentication process.	
Syntax	dot1x max-req <number>	
Parameter		
	Name	**Description**
	<number>	Max request number **Valid values:** 1–10 **Default values:** 2 **Type:** Mandatory

dot1x reauth {enable|disable}

Description	Enable/Disable re-authentication of PAE port.
Syntax	dot1x reauth {enable|disable}
Parameter	None

dot1x reauth-period <period>

Description	Period of re-authentication of PAE port.	
Syntax	dot1x reauth-period <period>	
Parameter		
	Name	**Description**
	<period>	Period of re-authentication. **Valid values:** 1–3600 seconds **Default values:** 3600 seconds **Type:** Mandatory

flow-control {enable|disable}

Description	Enable/Disable flow-control.	
Syntax	flow-control {enable|disable}	
Parameter		
	Name	**Description**
	enable	Enable flow-control.
	disable	Disable flow-control.

gvrp {enable|disable}

Description	Enable/Disable GVRP on the port.	
Syntax	gvrp {enable|disable}	
Parameter		
	Name	**Description**
	disable	Disable GVRP
	enable	Enable GVRP

gvrp join-time and leave-time

Description	Set GVRP join or leave time.	
Syntax	gvrp join-time <value> gvrp leave-time <value>	
Parameter		
	Name	**Description**
	<value>	**Range:** 10–10000 in centiseconds.

igmp max-channel <number>

Description	Set max channel to specified port.	
Syntax	igmp max-channel <number>	
Parameter		
	Name	**Description**
	<number>	Max channel number. **Valid values:** 1–512 **Type:** Mandatory

igmp profile aclprofile <index>

Description	Binding IGMP ACL profile to specified port.	
Syntax	igmp profile aclprofile <index>	
Parameter		
	Name	**Description**
	<index>	IGMP ACL index. **Valid values:** 1–15 **Type:** Mandatory

igmp profile mvrprofile <index>

Description	Binding IGMP MVR profile to specified port.	
Syntax	igmp profile mvrprofile <index>	
Parameter		
	Name	**Description**
	<index>	IGMP MVR index. **Valid values:** 1–15 **Type:** Mandatory

ip dhcp relay option82 circuit-id ascii <string>

Description	Configure circuit-id for the specified port.	
Syntax	ip dhcp relay option82 circuit-id ascii <string>	
Parameter		
	Name	**Description**
	<string>	Name representing the circuit-id of the port. **Valid values:** ASCII string (max 32 chars) **Type:** Mandatory

ip dhcp relay option82 circuit-id {port-id|port-mac}

Description	Configure circuit-id for the specified port..	
Syntax	ip dhcp relay option82 circuit-id {port-id|port-mac}	
Parameter		
	Name	**Description**
	port-id	Configure the port-id as the circuit-id value.
	port-mac	Configure the port-mac as the circuit-id value.

ip dhcp relay option82 disable

Description	Disable port DHCP relay option 82 information..
Syntax	ip dhcp relay option82 disable
Parameter	None

ip dhcp snooping {trust|untrust}

Description	Configure the interface as either trusted or untrusted.
Syntax	ip dhcp snooping {trust|untrust}
Parameter	None

ip verify source

Description	Validation of source address.	
Syntax	ip verify source ip verify source disable ip verify source limit <number> ip verify source limit disable	
Parameter		
	Name	**Description**
	disable	Disable validation of source address.
	<number>	Number of limitation. **Range:** 0–5
	limit disable	No limitation of source address validation.

lacp access {active|passive}

Description	Configure access mode of LACP port.	
Syntax	lacp access {active|passive}	
Parameter		
	Name	**Description**
	active	Set LACP port as active.
	passive	Set LACP port as passive.

lacp key

Description	Configure key of LACP port.	
Syntax	lacp key <value> lacp key auto	
Parameter		
	Name	**Description**
	<value>	**Range:** 1–65535
	auto	Indicate auto key.

lacp periodic

Description	Configure periodic mode of LACP port.	
Syntax	lacp periodic fast lacp periodic slow	
Parameter		
	Name	**Description**
	fast	Set fast periodic on the port.
	slow	Set slow periodic on the port.

lacp priority

Description	Configure priority of LACP port.	
Syntax	lacp priority <value>	
Parameter		
	Name	**Description**
	<value>	**Range:** 1–65535

lag {<value> | disable}

Description	Join or leave the LAG.	
Syntax	lag <value> lag disable	
Parameter		
	Name	**Description**
	<value>	Join the LAG. **Range:** 1–28
	disable	Leave the LAG.

lldp tlv-set management-address {both|ipv4|ipv6}

Description	Specify the management address TLV messages.	
Syntax	lldp tlv-set management-address {both|ipv4|ipv6}	
Parameter		
	Name	**Description**
	both	Specify both IPv4 and IPv6 management address TLV messages.
	ipv4	Specify IPv4 management address TLV messages.
	ipv6	Specify IPv6 management address TLV messages.

lldp transmit {enable|disable}

Description	Enable/Disable LLDP port transmit.	
Syntax	lldp transmit {enable|disable}	
Parameter		
	Name	**Description**
	enable	Enable LLDP port transmit.
	disable	Disable LLDP port transmit.

policer disable

Description	Disable policer function.
Syntax	policer disable
Parameter	None

policer pir <pir-rate> pbs <pbs-size> cir <cir-rate> cbs <cbs-size> {drop|cos|dscp}

Description	Set ingress policer parameters.	
Syntax	policer pir <pir-rate> pbs <pbs-size> cir <cir-rate> cbs <cbs-size> {cos|drop|dscp}	
Parameter		
	Name	**Description**
	<pir-rate>	Ingress total max rate setting. **Valid values:** 1–1000000 **Type:** Mandatory
	<pbs-size>	Ingress queue size setting. **Valid values:** 1–65535 **Type:** Mandatory
	<cir-rate>	Ingress max rate for first stage setting. **Valid values:** 1–1000000 **Type:** Mandatory
	<cbs-size>	Ingress max rate for second stage setting. **Valid values:** 1–65535 **Type:** Mandatory
	{cos|drop|dscp}	Policer type **Type:** Mandatory **cos**: Mark excessive packets with CoS priority **drop**: Drop excessive packets **dscp**: Mark excessive packets with DSCP priority

port {enable/disable}

Description	Set interface gigabit port enable or disable.	
Syntax	port {enable/disable}	
Parameter		
	Name	**Description**
	disable	Turn off gigabit port.
	enable	Turn off gigabit port.

port-isolation <portNo>

Description	Enable/Disable port-isolation action.	
Syntax	port-isolation <portNo> port-isolation <portNo> disable	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

port-shaper {enable|disable}

Description	Enable/Disable port shaper.
Syntax	port-shaper {enable|disable}
Parameter	None

port-shaper <rate>

Description	Set port shaper rate.	
Syntax	port-shaper <rate>	
Parameter		
	Name	**Description**
	<rate>	**Valid values:** 1–1000000 **Type:** Mandatory

priority <priority>

Description	Set user priority for the gigabit port.	
Syntax	priority <priority>	
Parameter		
	Name	**Description**
	<priority>	**Valid values:** 0–7 **Type:** Mandatory

protocol-vlan <number> create <ether-type> <svlan> <s-prio>

Description	Create protocol VLAN.	
Syntax	protocol-vlan <number> create <ether-type> <svlan> <s-prio>	
Parameter		
	Name	**Description**
	<number>	Protocol VLAN index. **Valid values:** 1–10 **Type:** Mandatory
	<ether-type>	Ether type. **Valid values:** 0–FFFF,(hex) **Type:** Mandatory
	<svlan>	Service VLAN (SVLAN). **Valid values:** 1–4094 **Type:** Mandatory
	<s-prio>	CoS of SVLAN. **Valid values:** 0–8 **Type:** Mandatory

protocol-vlan <number> delete

Description	Delete protocol VLAN.	
Syntax	protocol-vlan <number> delete	
Parameter		
	Name	**Description**
	<number>	Protocol VLAN index. **Valid values:** 1–10 **Type:** Mandatory

queue-scheduler bind <number>

Description	Scheduler profile binding.	
Syntax	queue-scheduler bind <number>	
Parameter		
	Name	**Description**
	<number>	Scheduler profile index. **Valid values:** 1–8 **Type:** Mandatory

queue-shaper {enable|disable}

Description	Enable/Disable queue shaper.
Syntax	queue-shaper {enable|disable}
Parameter	None

queue-shaper queue <number> <rate>

Description	Set queue shaper parameters.	
Syntax	queue-shaper queue <number> <rate>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 0–7 **Type:** Mandatory
	<rate>	**Valid values:** 1–1000000 **Type:** Mandatory

sfp-speed (for copper ports)

Description	Configure copper port Ethernet speed.	
Syntax	sfp-speed {auto|full-l000mbps|full-100mbps|full-10mbps|half-100mbps|half-10mbps}	
Parameter		
	Name	**Description**
	auto	Auto negotiation.
	full-l000mbps	Set 1000Mbps full duplexing.
	full-100mbps	Set 100Mbps full duplexing.
	full-10mbps	Set 10Mbps full duplexing.
	half-100mbps	Set 100Mbps half duplexing.
	half-10mbps	Set 10Mbps half duplexing.

sfp-speed (for 10G SFP ports)

Description	Configure 10G fiber port Ethernet speed.	
Syntax	sfp-speed {auto|full-1000mbps|full-10Gbps}	
Parameter		
	Name	**Description**
	auto	Auto negotiation.
	full-1000mbps	Set 1000Mbps full duplexing.
	full-10Gbps	Set 10Gbps full duplexing.

sfp-speed (for 1G SFP ports)

Description	Configure fiber port Ethernet speed.	
Syntax	sfp-speed {auto|full-1000mbps|full-100mbps	
Parameter		
	Name	**Description**
	auto	Auto negotiation.
	full-1000mbps	Set 1000Mbps full duplexing.
	full-100mbps	Set 100Mbps full duplexing.

stpport {disable|enable}

Description	Configure STP port.	
Syntax	stpport {disable|enable}	
Parameter		
	Name	**Description**
	disable	Disable STP port.
	enable	Enable STP port.

stpport cost <number>

Description	Set STP port path cost.	
Syntax	stpport cost <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–200000000

stpport edge-port {enable|disable}

Description	Set STP port edge-type.	
Syntax	stpport edge-port {enable|disable}	
Parameter		
	Name	**Description**
	enable	Set as edge-type.
	disable	Set as none edge-type.

stpport msti <index> pathcost <number>

Description	Set MSTP port pathcost for MSTP instance.	
Syntax	stpport msti <index> pathcost <number>	
Parameter		
	Name	**Description**
	<index>	MSTI index **Valid values:** 1-10 **Type:** Mandatory
	<number>	**Valid values:** 1 - 200000000 **Type:** Mandatory

stpport msti <index> priority <number>

Description	Set MSTP port priority.	
Syntax	stpport msti <index> priority <number>	
Parameter		
	Name	**Description**
	<index>	MSTI index **Valid values:** 1-10 **Type:** Mandatory
	<number>	**Valid values:** 0-240 step 16 **Type:** Mandatory

stpport priority <number>

Description	Set STP port priority.	
Syntax	stpport priority <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 0–240 step 16 **Type:** Mandatory

unknown-mc rate <rate>

Description	Set storm control rate limit for unknown multicast packet.	
Syntax	unknown-mc rate <rate>	
Parameter		
	Name	**Description**
	<rate>	**Valid values:** 1–1000000 (Kbps) **Type:** Mandatory

unknown-mc {block|forward}

Description	Block/Forward unknown multicast packet.
Syntax	unknown-mc block unknown-mc forward
Parameter	None

unknown-uc rate <rate>

Description	Set storm control rate limit for unknown unicast packet.	
Syntax	unknown-uc rate <rate>	
Parameter		
	Name	**Description**
	<rate>	**Valid values:** 1–1000000 (Kbps) **Type:** Mandatory

unknown-uc {block|forward}

Description	Block/Forward unknown unicast packet.
Syntax	unknown-uc block unknown-uc forward
Parameter	None

vlan <vlanid>

Description	Join VLAN with default setting (tagged).	
Syntax	vlan <vlanid>	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

vlan <vlanid> disable

Description	Leave joined VLAN.	
Syntax	vlan <vlanid> disable	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory
	disable	Leave joined VLAN.

vlan <vlanid> tag

Description	Join tagged VLAN.	
Syntax	vlan <vlanid> tag	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory
	tag	Join Tagged VLAN.

vlan <vlanid> untag

Description	Join untagged VLAN.	
Syntax	vlan <vlanid> untag	
Parameter		
	Name	**Description**
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory
	untag	Join Untagged VLAN.

vlan-stack {enable|disable}

Description	Enable/Disable VLAN stacking.
Syntax	vlan-stack {enable|disable}
Parameter	None

vlan-trans <number> create <cvlan> <c-prio> <svlan> <s-prio> many-to-one-replaced

Description	Create VLAN translation.	
Syntax	vlan-trans <number> create <cvlan> <c-prio> <svlan> <s-prio> many-to-one-replaced	
Parameter		
	Name	**Description**
	<number>	VLAN translation index. **Valid values:** 1–20 **Type:** Mandatory
	<cvlan>	Customer VLAN (CVLAN). **Valid values:** 1–4094 **Type:** Mandatory
	<c-prio>	CoS of VLAN. **Valid values:** 0–8 **Type:** Mandatory
	<svlan>	Service VLAN (SVLAN). **Valid values:** 1–4094 **Type:** Mandatory
	<s-prio>	CoS SVLAN. **Valid values:** 0–8 **Type:** Mandatory

vlan-trans <number> delete

Description	Delete VLAN translation.	
Syntax	vlan-trans <number> delete	
Parameter		
	Name	**Description**
	<number>	VLAN translation index. **Valid values:** 1–20 **Type:** Mandatory

Interface LAG Mode Commands

To enter this execution mode type **interface lag <number>** under the Configure Mode.

max-active-links <number>

Description	Configure maximum active links of the link aggregation group.	
Syntax	max-active-links <number>	
Parameter		
	Name	**Description**
	<number>	Active links. **Valid values:** 1–8

mode {disable | lacp | static}

Description	Configure the mode of the link aggregation group.	
Syntax	mode {disable | lacp | static}	
Parameter		
	Name	**Description**
	disable	Shutdown the link aggregation group.
	lacp	Process LACP on the link aggregation group.
	static	Process static bundling on the link aggregation group.

stpport {disable|enable}

Description	Configure STP port.	
Syntax	stpport {disable|enable}	
Parameter		
	Name	**Description**
	disable	Disable STP port.
	enable	Enable STP port.

stpport cost <number>

Description	Set STP port path cost.	
Syntax	stpport cost <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–200000000

stpport edge-port {enable|disable}

Description	Set STP port edge-type.	
Syntax	stpport edge-port {enable|disable}	
Parameter		
	Name	**Description**
	enable	Set as edge-type.
	disable	Set as none edge-type.

stpport priority <number>

Description	Set STP port priority.	
Syntax	stpport priority <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 0–240 step 16 **Type:** Mandatory

Interface VLAN Mode Commands

To enter this execution mode type **interface vlan <vlanid>** under the Configure Mode.

igmp version {v2 | v3 | v3 compatible}

Description	Set IGMP version.
Syntax	igmp version {v2 | v3 | v3 compatible}
Parameter	None

igmp snooping {disable|normal|proxy|querier}

Description	Create / Delete IGMP VLAN / ipSet snooping mode
Syntax	igmp snooping igmp snooping {disable|normal|proxy|querier}
Parameter	None

igmp router-port <portNo>

Description	Set IGMP VLAN source port.	
Syntax	igmp router-port <portNo>	
Parameter		
	Name	**Description**
	<portNo>	**Valid values:** 1–28 **Type:** Mandatory

igmp leave-mode {normal|fast}

Description	Set IGMP VLAN leave mode.
Syntax	igmp leave-mode {normal|fast}
Parameter	None

igmp version {v2|v3|v3compatible}

Description	Set IGMP VLAN version.
Syntax	igmp version v2 igmp version v3 igmp version v3compatible
Parameter	None

igmp robustness <number>

Description	Set IGMP VLAN robustness.	
Syntax	igmp robustness <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–3 **Type:** Mandatory

igmp query-interval <number>

Description	Set IGMP VLAN query interval.	
Syntax	igmp query-interval <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–1800 (unit: sec) **Type:** Mandatory

igmp max-response-time <number>

Description	Set IGMP VLAN max response time.	
Syntax	igmp max-response-time <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–255 (unit: 100ms) **Type:** Mandatory

igmp last-member-query-count <number>

Description	Set IGMP VLAN last member query count.	
Syntax	igmp last-member-query-count <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–3 **Type:** Mandatory

igmp last-member-query-interval <number>

Description	Set IGMP VLAN last member query interval.	
Syntax	igmp last-member-query-interval <number>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 1–255 (unit: 100ms). **Type:** Mandatory

igmp querier-address <ipaddr>

Description	Set IP address of IGMP VLAN interface.	
Syntax	igmp querier-address <ipaddr>	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 0.0.0.0–223.255.255.255 **Type:** Mandatory

ip ospf authentication {message-digest|null|disable}

Description	Set OSPF authentication mode.	
Syntax	ip ospf authentication {message-digest|null|disable} ip ospf authentication	
Parameter		
	Name	**Description**
	message-digest null disable	Use message-digest authentication Use no authentication Disable authentication **Type:** Optional

ip ospf authentication-key <string>

Description	Set authentication key.	
Syntax	ip ospf authentication-key <string>	
Parameter		
	Name	**Description**
	<string>	Authentication key **Valid length:** 0–8 **Type:** Mandatory

ip ospf cost <number>

Description	Set interface cost	
Syntax	ip ospf cost <number>	
Parameter		
	Name	**Description**
	<number>	Cost **Valid values:** 1–65535 **Type:** Mandatory

ip ospf dead-interval <number>

Description	Set interval after which a neighbor is declared dead.	
Syntax	ip ospf dead-interval <number>	
Parameter		
	Name	**Description**
	<number>	**Interval, unit:** seconds **Valid values:** 1–65535 **Type:** Mandatory

ip ospf hello-interval <number>

Description	Set time between HELLO packets.	
Syntax	ip ospf hello-interval <number>	
Parameter		
	Name	**Description**
	<number>	Interval, unit **Valid values:** 1–65535 **Type:** Mandatory

ip ospf message-digest-key <number> <string>

Description	Set message digest authentication password (key).	
Syntax	ip ospf message-digest-key <number> <string>	
Parameter		
	Name	**Description**
	<number>	Key ID **Valid values:** 1–255 **Type:** Mandatory
	<string>	Key **Valid length:** 0–16 **Type:** Mandatory

ip ospf mtu-ignore disable

Description	Enable/Disable OSPF mtu mismatch detection.	
Syntax	ip ospf mtu-ignore ip ospf mtu-ignore disable	
Parameter		
	Name	**Description**
	<disable>	**Enable** mtu mismatch detection **Type:** Mandatory

ip ospf network {broadcast|non-broadcast|point-to-multipoint|point-to-point}

Description	Set OSPF network type.	
Syntax	ip ospf network {broadcast|non-broadcast) ip ospf network {point-to-multipoint|point-to-point}	
Parameter		
	Name	**Description**
	Broadcast Non-broadcast Point-to-multipoint Point-to-point	Specify OSPF broadcast multi-access network Specify OSPF NBMA network Specify OSPF point-to-multipoint network Specify OSPF point-to-point network **Type:** Mandatory

ip ospf priority <number>

Description	Set router priority.	
Syntax	ip ospf priority <number>	
Parameter		
	Name	**Description**
	<number>	Priority **Valid values:** 0–255 **Type:** Mandatory

ip ospf re-transmit-interval <interval>

Description	Set time between retransmitting lost link state advertisements.	
Syntax	ip ospf retransmit-interval <interval>	
Parameter		
	Name	**Description**
	<interval>	**Interval, unit:** seconds **Valid values:** 3–65535 **Type:** Mandatory

ip ospf transmit-delay <number>

Description	Set link state transmit delay.	
Syntax	ip ospf transmit-delay <number>	
Parameter		
	Name	**Description**
	<number>	**Delay time, unit:** seconds **Valid values:** 1–65535 **Type:** Mandatory

ip ospf enable area {<number>|<ip>}

Description	Configure OSPF area parameters.	
Syntax	ip ospf enable area {<number>|<ip>}	
Parameter		
	Name	**Description**
	<ip> <number>	OSPF area ID in IP address format OSPF area ID as a decimal value **Type:** Mandatory

ip ospf {enable|disable}

Description	Enable/Disable OSPF on the interface.
Syntax	ip ospf {enable|disable}
Parameter	None

ip rip auth {enable|disable}

Description	Enable/Disable RIP for specified VLAN.
Syntax	ip rip auth {enable|disable}
Parameter	None

ip rip auth string <string>

Description	Set RIP Authentication Key.	
Syntax	ip rip auth string <string>	
Parameter		
	Name	**Description**
	<string>	Authentication Key. **Valid values:** 0–16 **Type:** Mandatory

ip rip {send|receive} disable

Description	Disable RIP send/receive function.
Syntax	ip rip {send|receive} disable
Parameter	None

ip rip {send|receive} version {v1|v2|both}

Description	Set RIP version
Syntax	ip rip {send|receive} version {v1|v2|both}
Parameter	None

ip rip split-horizon {simple | poisoned-reverse | disable}

Description	Set RIP split horizon type.
Syntax	ip rip split-horizon {simple | poisoned-reverse | disable}
Parameter	None

ip rip {enable|disable}

Description	Enable/Disable RIP for specified VLAN.
Syntax	ip rip {enable| disable}
Parameter	None

ip-address <ip>

Description	Set layer3 IP address for specified VLAN.	
Syntax	ip-address <ip>	
Parameter		
	Name	**Description**
	<ip>	IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

ip-address <ip> netmask <netmask>

Description	Set layer3 IP address for specified VLAN.	
Syntax	ip-address <ip> netmask <netmask>	
Parameter		
	Name	**Description**
	<ip>	IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<netmask>	IP address. **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

ip-address dhcp {disable}

Description	Enable/Disable DHCP
Syntax	ip-address dhcp ip-address dhcp disable
Parameter	None

ipv6-address disable

Description	Remove IPv6 address on the interface.
Syntax	ipv6-address disable
Parameter	

ipv6-address <ipv6_subnet>

Description	Set IPv6 address on the interface.	
Syntax	ipv6-address <ipv6_subnet>	
Parameter		
	Name	**Description**
	<IPv6_subnet>	IPv6 prefix x:x::y/z

ipv6-link-local-address <ipv6_subnet>

Description	Configure IPv6 link-local address on the interface.	
Syntax	ipv6-link-local-address <ipv6_subnet>	
Parameter		
	Name	**Description**
	<IPv6_subnet>	IPv6 prefix fe80::x/y

ipv6-link-local-address auto

Description	Automatically construct an IPv6 link-local address in the EUI-64 format.
Syntax	ipv6-link-local-address auto
Parameter	None

vrrp <number> address-family (for vrrpv3)

Description	Configure address-family.	
Syntax	vrrp <number> address-family {ipv4|ipv6} vrrp <number> address-family {ipv4|ipv6} disable	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	ipv4	Enable/Disable IPv4 VRRP group.
	ipv6	Enable/Disable IPv6 VRRP group.

vrrp <number> advertise <interval>

Description	Set the advertisement timer.	
Syntax	vrrp <number> advertise <interval>	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	<interval>	Advertisement interval, unit: second for VRRPv2, centisecond for VRRPv3 **Valid values:** 1–255 for VRRPv2, 1–4095 for VRRPv3 **Type:** Mandatory

vrrp <number> authentication disable (for VRRPv2)

Description	Enable/Disable plain-text authentication.	
Syntax	vrrp <number> authentication vrrp <number> authentication disable	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	disable	Disable authentication. **Type:** Optional

vrrp <number> authentication <text> (for VRRPv2)

Description	Set key for plain-text authentication.	
Syntax	vrrp <number> authentication <text>	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	<text>	Key **Valid length:** 1–8 **Type:** Mandatory

vrrp <number> ip-address <x.x.x.x>

Description	Set IP of virtual router redundancy protocol (VRRP).	
Syntax	vrrp <number> ip-address <x.x.x.x>	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	<x.x.x.x>	IP address **Type:** Mandatory

vrrp <number> learn-master-adv-int disable (for VRRPv2)

Description	Enable/Disable advertisement interval from current master.	
Syntax	vrrp <number> learn-master-adv-int vrrp <number> learn-master-adv-int disable	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	disable	Ignore advertisement interval from current master. **Type:** Optional

vrrp <number> preempt disable

Description	Enable/Disable preemption of lower priority Master.	
Syntax	vrrp <number> preempt vrrp <number> preempt disable	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	disable	Disable preemption of lower priority Master. **Type:** Optional

vrrp <number> priority <priority>

Description	Set priority of VRRP group.	
Syntax	vrrp <number> priority <priority>	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory
	<priority>	Priority level **Valid values:** 1–254 **Type:** Mandatory

vrrp <number> disable

Description	Delete VRRP group.	
Syntax	vrrp <number> disable	
Parameter		
	Name	**Description**
	<number>	VRRP group number **Valid values:** 1–255 **Type:** Mandatory

vrrp <number> track <number>

Description	Set VRRP group track object.	
Syntax	vrrp <number> track <number> vrrp <number> track <number> disable	
Parameter		
	Name	**Description**
	vrrp <number>	VRRP group ID **Valid values:** 1–255
	track <number>	Track ID **Valid values:** 1–64
	disable	Disable the track ID.

IP DHCP Pool Mode Commands

To enter this execution mode type **ip dhcp pool <number>** under the Configure Mode.

(conf)# ip dhcp pool <pool-id>

Description	Enter IP DHCP configure mode for a specific pool.	
Syntax	ip dhcp pool <pool-id>	
Parameter		
	Name	**Description**
	<pool-id>	DHCP Pool index **Valid values:** 1–20 **Type:** Mandatory

address-range <start-ip> <end-ip>

Description	Set DHCP pool address range. Start IP must be less than or equal to End IP.	
Syntax	address-range <start-ip> <end-ip>	
Parameter		
	Name	**Description**
	<start-ip>	Start IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<end-ip>	End IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

class <class-id> address-range <start-ip> <end-ip>

Description	Set the address range for the class. Start IP must be less than or equal to End IP.	
Syntax	class <class-id> address-range <start-ip> <end-ip>	
Parameter		
	Name	**Description**
	<class-id>	Class Identifier index **Valid values:** 1-128 **Type:** Mandatory
	<start-ip>	Start IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<end-ip>	End IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

class <class-id> remove

Description	Remove the DHCP class from the DHCP pool.	
Syntax	class <class-id> remove	
Parameter		
	Name	**Description**
	<class-id>	Class Identifier index **Valid values:** 1-128 **Type:** Mandatory

default-router <router-ip>

Description	Set DHCP pool default router.	
Syntax	default-router <router-ip>	
Parameter		
	Name	**Description**
	<router-ip>	Router IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

dns-server <DNS>

Description	Set DHCP pool domain name server address.	
Syntax	dns-server <DNS>	
Parameter		
	Name	**Description**
	<DNS>	DNS IP address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

domain-name <name>

Description	Set DHCP pool domain name.	
Syntax	domain-name <name>	
Parameter		
	Name	**Description**
	<name>	Router IP address **Valid values:** 1–64 characters **Type:** Mandatory

lease <time>

Description	Set DHCP pool lease time.	
Syntax	lease <time>	
Parameter		
	Name	**Description**
	<time>	Lease time **Valid values:** 60–31536000 **Type:** Mandatory

network <subnet> <netmask>

Description	Create/Modify DHCP pool network.	
Syntax	network <subnet> <netmask>	
Parameter		
	Name	**Description**
	<subnet>	Subnet address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<netmask>	Netmask address **Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

Profile ACL Mode Commands

To enter this execution mode type **profile acl** under the Configure Mode.

acl-profile <number> {create|delete}

Description	Create/Delete ACL profile.	
Syntax	acl-profile <number> {create|delete}	
Parameter		
	Name	**Description**
	<number>	**Valid values:** 2–10 **Type:** Mandatory
	create|delete	**Type:** Mandatory

acl-profile <prof-number> {create|delete} entry <entry-number>

Description	Create/Delete ACL profile entry.	
Syntax	acl-profile <prof-number> create entry <entry-number> acl-profile <prof-number> delete entry <entry-number>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set vlan <vlanid>

Description	Set VLAN index for ACL MAC type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> mac-type set vlan <vlanid>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	<vlanid>	**Valid values:** 1–4094 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set vlan any

Description	Set VLAN index for ACL MAC type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> mac-type set vlan any	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set {srcmac|dstmac} <mac> <mask>

Description	Set MAC for ACL MAC type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> mac-type set {srcmac|dstmac} <mac> <mask>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1-16 **Type:** Mandatory
	srcmac|dstmac	source / Destination MAC Address **Type:** Mandatory
	<mac>	**Valid values:** 00:00:00:00:00:00–FF:FF:FF:FF:FF:FF **Type:** Mandatory
	<mask>	**Valid values:** 00:00:00:00:00:00–FF:FF:FF:FF:FF:FF **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set ethertype <ethertype>

Description	Set ether type for ACL MAC type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> mac-type set ethertype <ether-type>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	<ethertype>	**Valid values:** 0x0001–0xFFFF **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set ethertype any

Description	Set ether type for ACL MAC type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> mac-type set ethertype any	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> ipv4-type set {srcip|dstip} <ipaddr> <mask>

Description	Set IP for ACL IPv4 type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> ipv4-type set {srcip|dstip} <ipaddr> <mask>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	srcip|dstip	Source / Destination IP Address **Type:** Mandatory
	<ipaddr>	**Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<mask>	**Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol <protocol-id>

Description	Set protocol for ACL IPv4 type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol <protocol-id>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	<protocol-id>	**Valid values:** 1–255 **Type:** Mandatory

acl-profile <prof-numbers> set entry <entry-number> ipv4-type set ip-protocol any

Description	Set protocol for ACL IPv4 type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol any	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set protocol {tcp|udp}

Description	Set protocol for ACL L4Port type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> l4port-type set protocol {tcp|udp}	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	tcp|udp	TCP or UDP packet. **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcip|dstip} <ipaddr> <mask>

Description	Set IP for ACL L4Port type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> l4port-type set {srcip|dstip} <ipaddr> <mask>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	srcip|dstip	Source / Destination IP Address **Type:** Mandatory
	<ipaddr>	**Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<mask>	**Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} <number>

Description	Set port for ACL L4Port type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} <number>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	srcport|dstport	Source / Destination port **Type:** Mandatory
	<number>	**Valid values:** 1–65535 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} any

Description	Set port for ACL L4Port type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} any	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	srcport|dstport	**Source / Destination port** **Type: Mandatory**

acl-profile <prof-number> set entry <entry-number> tos-type set {srcip|dstip} <ipaddr> <mask>

Description	Set port for ACL L4Port type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> tos-type set {srcip|dstip} <ipaddr> <mask>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	srcip|dstip	Source / Destination IP Address **Type:** Mandatory
	<ipaddr>	Valid values: 0.0.0.0–255.255.255.255 **Type:** Mandatory
	<mask>	**Valid values:** 0.0.0.0–255.255.255.255 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> tos-type set type {precedence|tos|dscp} <number>

Description	Set type for ACL ToS type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> tos-type set type {precedence|tos|dscp} <number>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	precedence|tos|dscp	Precedence or ToS or DSCP Type. **Type:** Mandatory
	<number>	Precedence type. **Valid values:** 0–7 Tos type. **Valid values:** 0–15 DSCP type. **Valid values:** 0–63 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> tos-type set type any

Description	Set type for ACL ToS type entry.	
Syntax	acl-profile <prof-number> set entry <entry-number> tos-type set type any	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> action forwarding {deny|permit}

Description	Set ACL entry action is forwarding.	
Syntax	acl-profile <prof-number> set entry <entry-number> action forwarding {deny|permit}	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	deny|permit	Deny or Permit forwarding **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> action queue <number>

Description	Set ACL entry action to specific queue number.	
Syntax	acl-profile <prof-number> set entry <entry-number> action queue <number>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	<number>	**Valid values:** 0–7 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> action cos <number>

Description	Set ACL entry action is mark CoS number.	
Syntax	acl-profile <prof-number> set entry <entry-number> action cos <number>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory
	<number>	**Valid values:** 0–7 **Type:** Mandatory

acl-profile <prof-number> set entry <entry-number> action copyframe

Description	Set ACL entry action is copy frame.	
Syntax	acl-profile <prof-number> set entry <entry-number> action copyframe	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<entry-number>	**Valid values:** 1–16 **Type:** Mandatory

acl-profile <prof-number> set name <name>

Description	Set ACL profile name.	
Syntax	acl-profile <prof-number> set name <name>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–10 **Type:** Mandatory
	<name>	**Valid length:** 1–31 **Type:** Mandatory

Profile Alarm Mode Commands

To enter this execution mode type **profile alarm** under the Configure Mode.

alarm <alarm-id> {mask | unmask | major | minor}

Description	Configure an alarm profile entry. (default setting for each alarm is mask and minor)	
Syntax	alarm <alarm-id> mask alarm <alarm-id> unmask alarm <alarm-id> major alarm <alarm-id> minor	
Parameter		
	Name	**Description**
	<alarm-id>	Alarm ID **Valid values:** 101–128: Port Link Down for ports GE-1 to GE-28 respectively 151: Power Alarm 201: Above Temperature 202: Below Temperature **Type:** Mandatory
	mask	Clear this alarm **Type:** Mandatory
	unmask	Set this alarm **Type:** Mandatory
	major	Set alarm level to major **Type:** Mandatory
	minor	Set alarm level to minor **Type:** Mandatory

Profile IGMP ACL Mode Commands

To enter this execution mode type **profile igmp-acl** under the Configure Mode.

igmp-acl <number> {create|delete}

Description	Create / Delete IGMP ACL profile.	
Syntax	igmp-acl <number> {create|delete}	
Parameter		
	Name	**Description**
	<number>	IGMP ACL profile index **Valid values:** 2–15 **Type:** Mandatory

igmp-acl <number> {default-deny|default-permit}

Description	Set IGMP ACL default rule.	
Syntax	igmp-acl <number> {default-deny| default-permit}	
Parameter		
	Name	**Description**
	<number>	IGMP ACL profile index **Valid values:** 2–15 **Type:** Mandatory

igmp-acl <p-number> entry <e-number> <startip> <endip> {<vid>|any} {permit|deny}

Description	Create IGMP ACL entry.	
Syntax	igmp-acl <p-number> entry <e-number> <startip> <endip> {<vid>|any} {permit|deny}	
Parameter		
	Name	**Description**
	<p-number>	IGMP ACL profile index **Valid values:** 2–15 **Type:** Mandatory
	<e-number>	IGMP MVR entry index **Valid values:** 1–32 **Type:** Mandatory
	<startIP> <endIP>	IP address **Valid values:** 224.0.1.0–239.255.255.255 **Type:** Mandatory
	<vid>	VLAN ID **Valid values:** 1–4094 **Type:** Mandatory

igmp-acl <p-number> entry <e-number> delete

Description	Delete IGMP ACL entry.	
Syntax	igmp-acl <p-number> entry <e-number> delete	
Parameter		
	Name	**Description**
	<p-number>	IGMP ACL profile index **Valid values:** 2–15 **Type:** Mandatory
	<e-number>	IGMP MVR entry index **Valid values:** 1–32 **Type:** Mandatory

Profile IGMP MVR Mode Commands

To enter this execution mode type **profile igmp-mvr** under the Configure Mode.

igmp-mvr <number, 2-15> {create|delete}

Description	Create / Delete IGMP MVR profile.	
Syntax	igmp-mvr <number,2–15> {create|delete}	
Parameter		
	Name	**Description**
	<number>	IGMP MVR profile index **Valid values:** 2–15 **Type:** Mandatory

igmp-mvr <p-number> entry <e-number> <startip> <endip> <vid>

Description	Create IGMP MVR entry.	
Syntax	igmp-mvr <p-number> entry <e-number> <startip> <endip> <vid>	
Parameter		
	Name	**Description**
	<p-number>	IGMP MVR profile index **Valid values:** 2–15 **Type:** Mandatory
	<e-number>	IGMP MVR entry index **Valid values:** 1–32 **Type:** Mandatory
	<startIP> <endIP>	IP address. **Valid values:** 224.0.1.0–239.255.255.255 **Type:** Mandatory
	<vid>	VLAN ID **Valid values:** 1–4094 **Type:** Mandatory

igmp-mvr <p-number> entry <e-number> delete

Description	Delete IGMP MVR entry.	
Syntax	igmp-mvr <p-number> entry <e-number> delete	
Parameter		
	Name	**Description**
	<p-number>	IGMP MVR profile index **Valid values:** 2–15 **Type:** Mandatory
	<e-number>	IGMP MVR entry index **Valid values:** 1–32 **Type:** Mandatory

Profile Scheduler Mode Commands

To enter this execution mode type **profile sch** under the Configure Mode.

scheduler-profile <number> method {spq|spq-wrr|wrr}

Description	Set scheduler profile method.	
Syntax	scheduler-profile <number> method {spq|spq-wrr|wrr}	
Parameter		
	Name	**Description**
	<number>	Scheduler profile index **Valid values:** 2–8 **Type:** Mandatory
	spq|spq-wrr|wrr	**spq:** strict priority **spq-wrr:** strict priority + weighted round robin **wrr:** weighted round robin **Type:** Mandatory

scheduler-profile <prof-number> queue <queue-number> weight <number>

Description	Set scheduler profile queue weight.	
Syntax	scheduler-profile <prof-number> queue <queue-number> weight <number>	
Parameter		
	Name	**Description**
	<prof-number>	**Valid values:** 2–8 **Type:** Mandatory
	<queue-number>	**Valid values:** 0–7 **Type:** Mandatory
	<number>	**Valid values:** 1–255 **Type:** Mandatory

RingV2 Group Mode Commands

To enter this execution mode type **ringv2-group <number>** under the Configure Mode.

guardtimer <time>

Description	Set guardtimer.	
Syntax	guardtimer <time>	
Parameter		
	Name	**Description**
	<time>	Second. **Range:** Default is 10 seconds **Valid values:** 10–3600 **Type:** Mandatory

mode enable

Description	Enable ring protect on specific ring group.
Syntax	mode enable
Parameter	None

mode disable

Description	Disable ring protect on specific ring group.
Syntax	mode disable
Parameter	None

node1 <portNo>

Description	Ring node1 setting.	
Syntax	node1 <portNo>	
Parameter		
	Name	**Description**
		Port number **Valid values:** 1–28 **Type:** Mandatory

node2 <portNo>

Description	Ring node2 setting.	
Syntax	node2 <portNo>	
Parameter		
	Name	**Description**
		Port number **Valid values:** 1–28 **Type:** Mandatory

role ring-master

Description	Configure the role of the ring group to Ring Master.
Syntax	role ring-master
Parameter	None
Groups	1 and 2

role ring-slave

Description	Configure the role of the ring group to Ring Slave.
Syntax	role ring-slave
Parameter	None
Groups	1 and 2

role coupling-primary

Description	Configure the role of the ring group as Coupling Primary.
Syntax	role coupling-primary
Parameter	None
Group	2

role coupling-backup

Description	Configure the role of the ring group as Coupling Backup.
Syntax	role coupling-backup
Parameter	None
Group	2

role dual-homing

Description	Configure the role of the ring group as Dual Homing.
Syntax	role dual-homing
Parameter	None
Group	2

role chain-head

Description	Configure the role of the ring group as Chain Head.
Syntax	role chain-head
Parameter	None
Group	3

role chain-tail

Description	Configure the role of the ring group as Chain Tail.
Syntax	role chain-tail
Parameter	None
Group	3

role chain-member

Description	Configure the role of the ring group as Chain Member.
Syntax	role chain-member
Parameter	None
Group	3

role balancing-chain-terminal-1

Description	Configure the role of the ring group as Balancing Chain Terminal 1.
Syntax	role balancing-chain-terminal-1
Parameter	None
Group	3

role balancing-chain-terminal-2

Description	Configure the role of the ring group as Balancing Chain Terminal 2.
Syntax	role balancing-chain-terminal-2
Parameter	None
Group	3

role balancing-chain-member

Description	Configure the role of the ring group as Balancing Chain Member.
Syntax	role balancing-chain-member
Parameter	None
Group	3

role balancing-chain-central-block

Description	Configure the role of the ring group as Balancing Chain Central Block.
Syntax	role balancing-chain-central-block
Parameter	None
Group	3

Router OSPF Mode Commands

To enter this execution mode type **router ospf** under the Configure Mode.

abr-type {cisco|shortcut|standard}

Description	Set OSPF ABR type.	
Syntax	abr-type {cisco|shortcut|standard}	
Parameter		
	Name	**Description**
	cisco shortcut standard	Alternative ABR, cisco implementation Shortcut ABR Standard behavior (RFC2328) **Type:** Mandatory

area {<ip>|<number>} {nssa|stub|normal}

Description	Set OSPF area parameters.	
Syntax	area {<ip>|<number>} {nssa|stub|normal}	
Parameter		
	Name	**Description**
	<ip> <number>	IP address, OSPF area ID in IP address format Number, OSPF area ID as a decimal value **Type:** Mandatory
	nssa stub normal	Configure OSPF area as NSSA Configure OSPF area as STUB Configure OSPF area as normal, delete the entry **Type:** Mandatory

area {<ip>|<number>} {nssa|stub} no-summary

Description	Set OSPF area parameters.	
Syntax	area {<ip>|<number>} {nssa|stub} no-summary	
Parameter		
	Name	**Description**
	<ip> <number>	IP address, OSPF area ID in IP address format Number, OSPF area ID as a decimal value **Type:** Mandatory
	nssa stub normal	Configure OSPF area as NSSA Configure OSPF area as STUB Configure OSPF area as normal, delete the entry **Type:** Mandatory

area {<ip>|<number>} nssa translate disable

Description	Configure OSPF NSSA area parameters.	
Syntax	area {<ip>|<number>} nssa area {<ip>|<number>} nssa translate area {<ip>|<number>} nssa translate disable	
Parameter		
	Name	**Description**
	<ip> <number>	IP address, OSPF area ID in IP address format Number, OSPF area ID as a decimal value **Type:** Mandatory
	translate	Configure NSSA-ABR to translate **Type:** Optional
	disable	Never translate NSSA **Type:** Optional

area {<ip>|<number>} virtual-link <virtual-ip> disable

Description	Configure a virtual link.	
Syntax	area {<ip>|<number>} virtual-link <virtual-ip> area {<ip>|<number>} virtual-link <virtual-ip> disable	
Parameter		
	Name	**Description**
	<ip> <number>	IP address, OSPF area ID in IP address format Number, OSPF area ID as a decimal value **Type:** Mandatory
	<virtual-ip>	IP address **Type:** Mandatory
	disable	Delete the virtual link configuration. **Type:** Optional

neighbor <ip> disable

Description	Enable/Disable OSPF neighbor.	
Syntax	neighbor <ip>	
Parameter		
	Name	**Description**
	<ip>	OSPF neighbor address **Type:** Mandatory
	disable	Delete OSPF neighbor **Type:** Optional

neighbor <ip> {poll-interval | priority} {<interval>|<priority>}

Description	Set OSPF neighbor parameters.	
Syntax	neighbor <ip> poll-interval <interval> priority <priority> neighbor <ip> priority <priority> poll-interval <interval>	
Parameter		
	Name	**Description**
	<ip>	OSPF neighbor address **Type:** Mandatory
	<interval>	Polling interval. **Valid values:** 1–65535 **Type:** Mandatory
	<priority>	Priority. **Valid values:** 0–255 **Type:** Mandatory

ospf {enable|disable}

Description	Enable/Disable OSPF.
Syntax	ospf {enable|disable}
Parameter	None

redistribute {connected|static|rip} disable

Description	Redistribute information from another routing protocol.	
Syntax	redistribute {connected|static|rip} redistribute {connected|static|rip} disable	
Parameter		
	Name	**Description**
	connected static rip	Connected routes (directly attached subnet or host) Statically configured routes Routing Information Protocol (RIP) **Type:** Mandatory
	disable	Delete the routing protocol configuration. **Type:** Optional

redistribute {connected|static|rip} metric <number>

Description	Redistribute information from another routing protocol.	
Syntax	redistribute {connected|static|rip} metric <number>	
Parameter		
	Name	**Description**
	connected static rip	Connected routes (directly attached subnet or host) Statically configured routes Routing Information Protocol (RIP) **Type:** Mandatory
	<number>	OSPF default metric **Valid values:** 0–16777214 **Type:** Mandatory

redistribute {connected|static|rip} metric <num> metric-type <num1>

Description	Redistribute information from another routing protocol.	
Syntax	Redistribute {connected|static|rip} metric <num> metric-type <num1>	
Parameter		
	Name	**Description**
	connected static rip	Connected routes (directly attached subnet or host) Statically configured routes Routing Information Protocol (RIP) **Type:** Mandatory
	<num>	OSPF default metric **Valid values:** 0–16777214 **Type:** Mandatory
	<num1>	OSPF exterior metric type for redistributed routes **Valid values:** 1–2 **Type:** Mandatory

redistribute {connected|static|rip} metric-type <1|2>

Description	Redistribute information from another routing protocol.	
Syntax	redistribute {connected|static|rip} metric-type <number>	
Parameter		
	Name	**Description**
	connected static rip	Connected routes (directly attached subnet or host) Statically configured routes Routing Information Protocol (RIP) **Type:** Mandatory
	<number>	OSPF exterior metric type for redistributed routes **Valid values:** 1–2 **Type:** Mandatory

redistribute {connected|static|rip} metric-type <num> metric <num1>

Description	Redistribute information from another routing protocol.	
Syntax	redistribute {connected|static|rip} metric-type <num> metric <num1>	
Parameter		
	Name	**Description**
	connected static rip	Connected routes (directly attached subnet or host) Statically configured routes Routing Information Protocol (RIP) **Type:** Mandatory
	<num>	OSPF exterior metric type for redistributed routes **Valid values:** 1–2 **Type:** Mandatory
	<num1>	OSPF default metric **Valid values:** 0–16777214 **Type:** Mandatory

rfc1583compatibility disable

Description	Enable/Disable for RFC1583 compatibility.	
Syntax	rfc1583compatibility rfc1583compatibility disable	
Parameter		
	Name	**Description**
	disable	Disable RFC1583 compatibility **Type:** Optional

router-id <ip>

Description	Set OSPF router ID in IP address format.	
Syntax	router-id <ip>	
Parameter		
	Name	**Description**
	<ip>	IP address **Type:** Mandatory

Router RIP Mode Commands

To enter this execution mode type **router rip** under the Configure Mode.

gc-timeout <time>

Description	Set RIP garbage collection timeout.	
Syntax	gc-timeout <time>	
Parameter		
	Name	**Description**
	<time>	**Garbage collection timeout, unit:** second **Valid values:** 20–3600 (Default: 120) **Type:** Mandatory

redistribute {connected|ospf|static} disable

Description	Create/Delete another routing protocol configuration.	
Syntax	redistribute {connected|ospf|static} redistribute {connected|ospf|static} disable	
Parameter		
	Name	**Description**
	Connected Ospf static	Connected routes (directly attached subnet or host) Open Shortest Path Protocol (OSPF) Statically configured routes **Type:** Mandatory

redistribute {connected|ospf|static} metric <number>

Description	Redistribute information from another routing protocol with metric.	
Syntax	redistribute {connected|ospf|static} metric <number>	
Parameter		
	Name	**Description**
	<number>	Metric for redistributed routes **Valid values:** 0–16 **Type:** Mandatory

rip {enable|disable}

Mode	
Description	Enable/Disable RIP.
Syntax	rip {enable|disable}
Parameter	None

route-timeout <time>

Description	Set RIP route timeout.	
Syntax	route-timeout <time>	
Parameter		
	Name	**Description**
	<time>	**Update time, unit:** second **Valid values:** 20–3600 (Default: 180) **Type:** Mandatory

update-time <time>

Description	Set RIP update-time.	
Syntax	update-time <time>	
Parameter		
	Name	**Description**
	<time>	**Update time, unit:** second **Valid values:** 20–3600 (Default: 30) **Type:** Mandatory