Beijer
ELECTRONICS

Industrial Managed Ethernet Switches

JetNet Series Switches

Software Manual

DOCUMENT CHANGE SUMMARY				

Copyright, Trademark, and Proprietary Rights Information

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, BEIJER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. BEIJER does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. BEIJER does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to BEIJER that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL BEIJER, BEIJER AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF BEIJER HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

• Trademarks

BEIJER, the BEIJER logo, and JetNet are trademarks of Beijer Electronics and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

I. Important Notes

- Solid state equipment has operational characteristics differing from those of electromechanical equipment.
- Safety Guidelines for the Application, Installation, and Maintenance of Solid-State Controls describe some important differences between solid state equipment and hard-wired electromechanical devices.
- Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.
- In no event will Beijer Electronics be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.
- The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Beijer Electronics cannot assume responsibility or liability for actual use based on the examples and diagrams.

CAUTION

✓ **A Caution symbol indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury and or damage to the device.**
Read the following Instructions:

- Keep vibrations away from it.
- Products should be used in environments with a pollution index of less than 2.
- Ensure that the installation environment does not exceed 85% humidity.

WARNING

✓ **A Warning symbol indicates a hazardous situation which, if not avoided, could result in damage to the device, death or serious injury.**
Read the following Instructions:

- In order to prevent electric arcs, never assemble or wire the products with power applied.

- Otherwise, it may result in unexpected and potentially dangerous actions by field devices. Arching poses an explosion risk in hazardous locations. Before assembling or wiring the modules, ensure that the area is non-hazardous or that the system power has been removed accordingly.
- Check the rated voltage and terminal array before wiring. Avoid environments over 50℃ of temperature. Avoid placing it directly in the sunlight.
- Ensure that inputs and outputs are made according to the module specification. Wire the system using standard cables.
- In order to avoid an electric shock or malfunction, do not touch any terminal blocks or IO modules while the system is running.
- Keep away from the strange metallic materials not related to the unit and wiring works should be controlled by the electric expert engineer. Else it may cause the unit to a fire, electric shock or malfunction.
- Modules should not be placed near inflammable materials. A fire may result if it is not handled properly.

II. Safety Instruction

I.I. Symbols

CAUTION ⚠	A Caution symbol indicates a potentially hazardous situation to you.
WARNING ⚠	A Warning symbol indicates situations that can be potentially lethal or extremely hazardous to you.
ATTENTION	An Attention symbol indicates potential damage to programs, devices, or data.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

I.II. Safety Notes

WARNING ⚠	The modules are equipped with electronic components that may be destroyed by electrostatic discharge. When handling the modules, ensure that the environment (persons, workplace and packing) is well grounded. Avoid touching conductive components, M-bus and Hot swap-bus pin.

I.III. Certification

Note! For specific information relating to certification of this module type, see the separate certification document summary.

The following certification information applies to JetNet 5200G series models:

- CE compliance
- FCC compliance

The following certification information applies to JetNet 5900G series models:

- CE compliance
- FCC compliance
- DNV compliance

The following certification information applies to JetNet 6228G series models:

- CE compliance
- FCC compliance

Chapter 1. Switch Overview

1.1. Introduction

Beijer Electronics offers a diverse range of industrial Gigabit Managed Switches designed to operate reliably in harsh environments. These switches can be applied in various segments, including marine, automation, infrastructure, and more.

Additionally, we provide a wide array of software features that allow users to configure the network switch accordingly. Our software is designed with a concise interface, ensuring user-friendly switch configuration, monitoring, and maintenance.

1.2. Main Features

JetNet industrial Gigabit Managed Switches provide a range of powerful features. These switches support advanced management capabilities like SNMP, RSTP, and VLAN, ensuring efficient network configuration and monitoring. With Gigabit Ethernet connectivity, they enable high-speed data transfer for industrial applications. Designed for rugged environments, these switches offer reliability with wide operating temperature ranges. They also provide enhanced security features such as port security, access control lists, and 802.1X authentication. Please refer to the datasheets for model-specific details.

The following table describes many of the supported features:

Network redundancy	• Multiple Super Ring (MSR) • Rapid Spanning Tree Protocol (RSTP) • Multiple Spanning Tree Protocol (MSTP)
Device management	• SNMP v1/v2c/v3 • Remote Network Monitoring (RMON) • Web Interface (User Interface) • Telnet • Local Console

Layer 2 network performance	• IEEE802.1Q VLAN • Private VLAN (model specific) • Port Configuration • Port Trunk • Packet Filtering • DHCP Server/Client • Traffic Prioritize • Rate Control
Advanced security system	• Port Security • Access IP list • TACACS+
Event notification	• SNMP trap • SysLog
IEEE 802.1AB LLDP software for auto-topology and group management	
Network management	• Cisco-Like CLI • Web • SNMP/RMON
Multiple event relay output for enhanced device alarm control	
Hi-Pot Isolation Protection for ports and power	

1.3. Supported Switch Models

Switch Series	Switch Model
JetNet 5200G Series	JetNet5208G (G-2F)
	JetNet5208GP
	JetNet5210G-2C
	JetNet5210GP-2C
	JetNet5212G-2C2F
	JetNet5212GP-2C2F
	JetNet5216G-4C4F
	JetNet5216GP-4F
JetNet 5900G Series	JetNet 5908G
	JetNet 5908G-2F
	JetNet 5912G-2C2F
	JetNet 5916G-4C4F
JetNet 6228G Series	JetNet 6228G-4F-AC
	JetNet 6228G-4F-2DC
	JetNet 6228G-4F-AC-2DC

Chapter 2. Configuring the JetNet Series Switches

This chapter describes how to log in to a JetNet switch for the first time. The following information demonstrates how to access the switch's configuration settings through the web-based interface. The switch can be configured through a web interface or console management.

2.1. Before You Begin

Using a standard network cable, you can connect the JetNet switch directly to a computer or a network. You will be required to configure your computer's network settings after installing the switch on your intranet. JetNet switches can be accessed with the following default configurations:

PARAMETER	VALUE
USERNAME	admin
PASSWORD	admin
LAN IP	192.168.10.1

2.2. Accessing the Web Interface

The Web Interface is accessible by using Google Chrome, Edge, or Firefox.
To access the Web Interface:

1 - Connect the switch to the management PC or the network and an available network port on the switch.

2 - Connect the switch to power and power it on.

3 - Configure the network settings on your computer within the range of the default static IP address of the switch: 192.168.10.2 to 192.168.10.253.

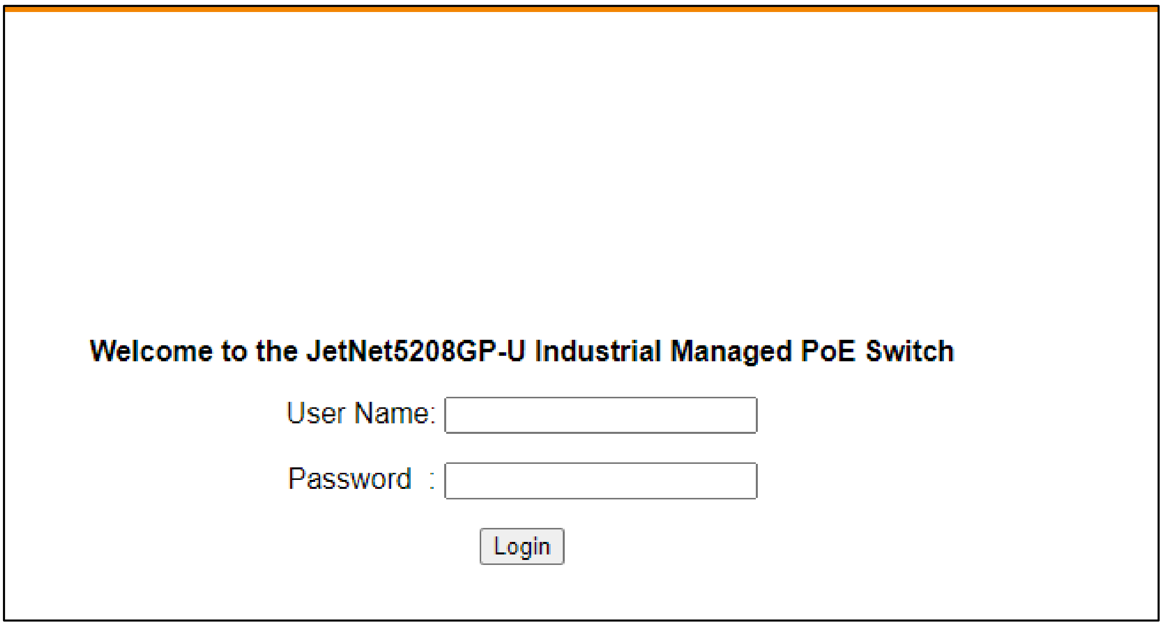
4 - If DHCP is enabled on the DHCP server, ensure it can be reached by the switch and the management computer.

5 - Open a web browser and enter the IP address (default: 192.168.10.1) in the address bar. The interface displays.

6 - In the User Name and Password fields enter the default values:

Default User Name: **admin**

Default Password: **admin**



Welcome to the JetNet5208GP-U Industrial Managed PoE Switch

Figure 1 Login Screen

7 - Click **Login** to enter the user interface. The Overview screen displays.
If this is the first time to log in with the default username and password, it is recommended to change the default settings.

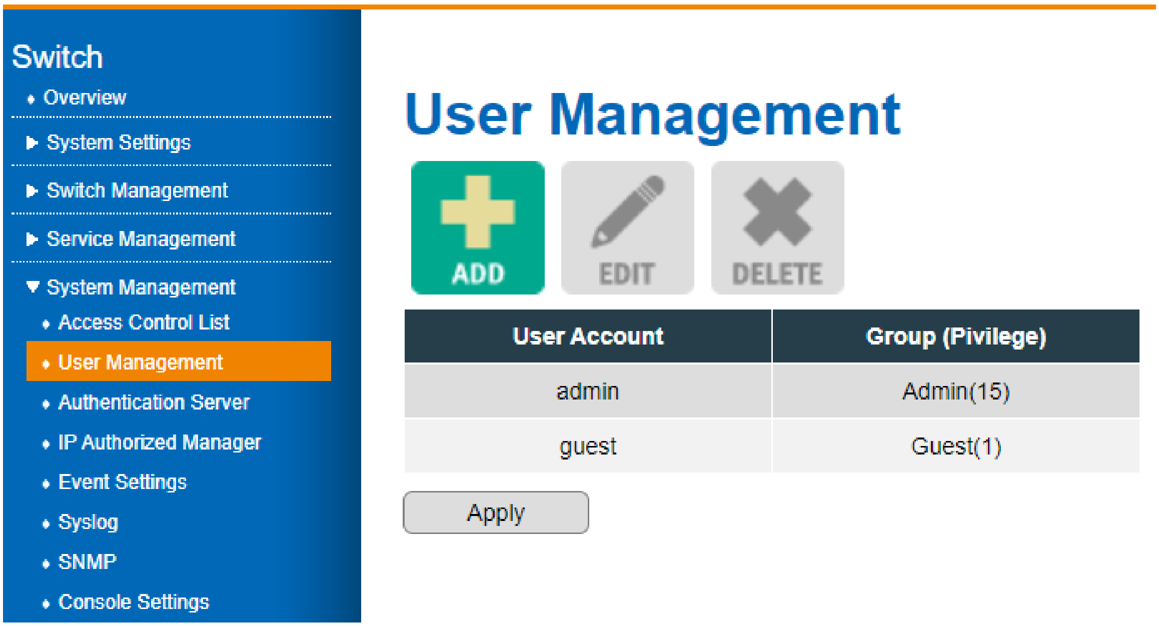
2.3. Changing Passwords

To change the password:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Navigate to **System Management** > **User Management**. The User Management screen displays.

3 - Under User Account, select the admin profile and click **Edit**.

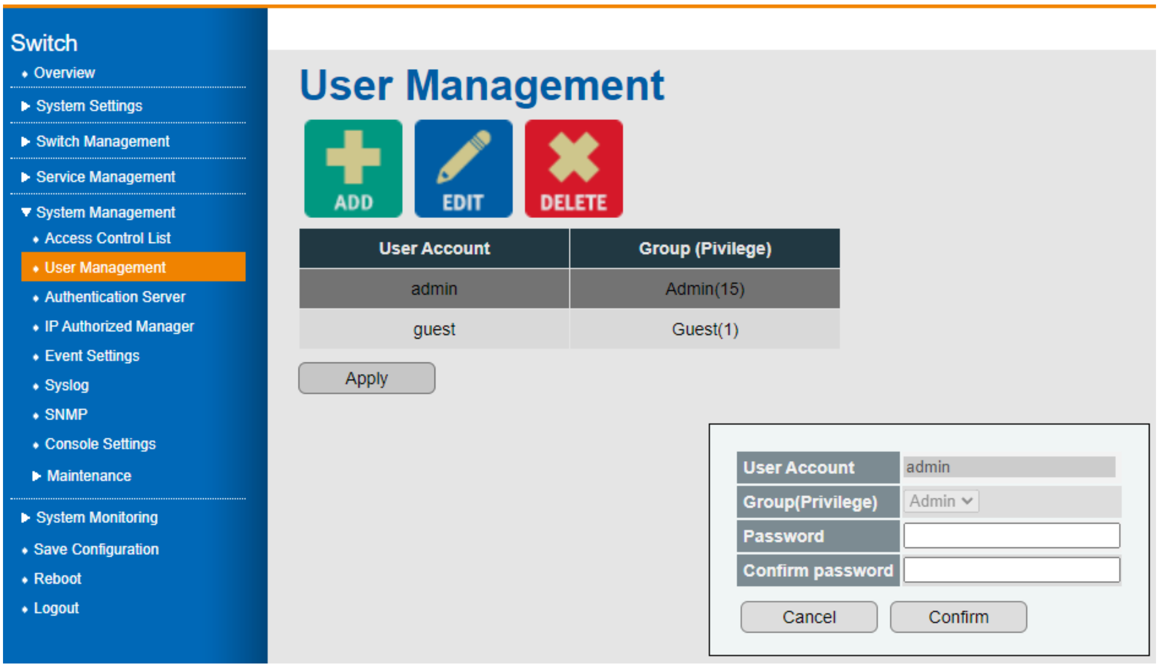


User Account	Group (Pivilege)
admin	Admin(15)
guest	Guest(1)

Figure 2 System Management > User Management

4 - The detailed user profile menu is displayed. In the Password field, enter the new password.

5 - In the Confirm password field, enter the new password to confirm it and click **Confirm**.



User Account	Group (Pivilege)
admin	Admin(15)
guest	Guest(1)

User Account	admin
Group(Privilege)	Admin
Password	
Confirm password	

Figure 3 Confirming a New Password

6 - Under the main menu tree, navigate to Save Configuration. The Save Configuration screen displays.

7 - Click **Apply** to save the new password setting.

Chapter 3. Managing Device Configuration

The following chapter contains the following section, which will guide you on how to install and manage the device.

3.1. Dashboard

You can select a number of functions from the graphical user interface (GUI) to display configuration settings and the available options. From the GUI, you can select the menu and it will load the current settings. The following features are included:

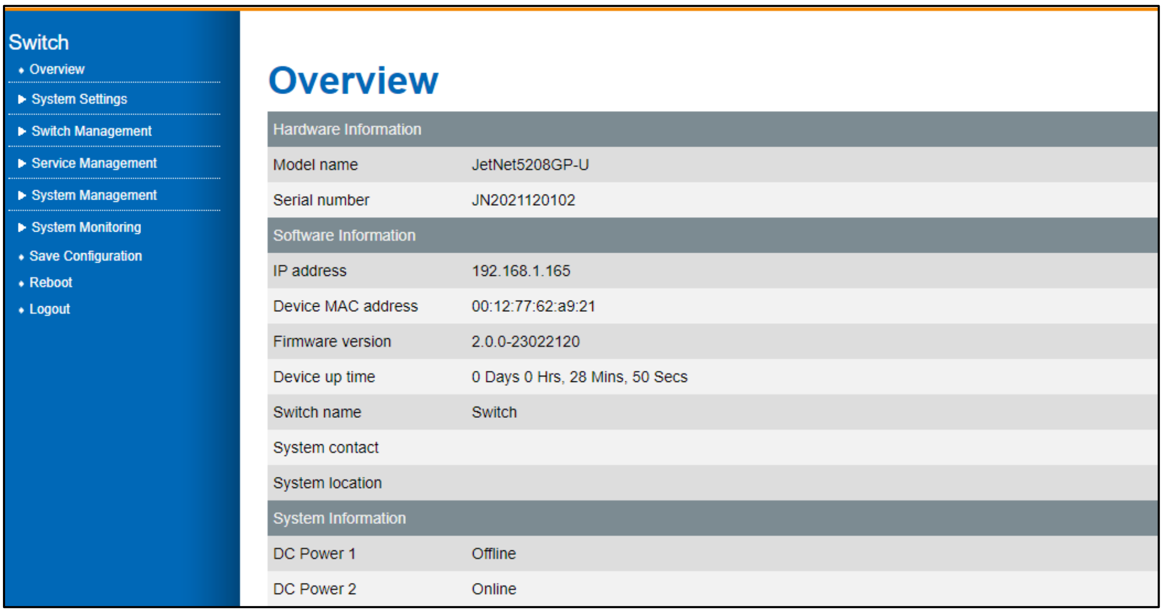
Category	Feature	Submenu
Overview		
System Settings	Device Settings	
	IP Configuration	
	Time Settings	
	Power Over Ethernet	PoE Settings
		PoE Schedule
Switch Management	Port Manager	
	Network Redundancy	Spanning Tree
		Multiple Super Ring
	VLAN	
	802.1X	
	DHCP Snooping	
	Port Mirroring	
	Port Trunking	Port Trunking Basic Settings
		Aggregation Config
	Traffic Prioritization	QoS Settings
		CoS Queue Mapping
		DSCP Priority Mapping
	Multicast	Mode Selection
		GMRP
		IGMP Snooping
		IGMP Query
	Static MAC Address	
	Port Isolation	
Service Management	DHCP	
	RMON	
	LLDP	Global Settings
		Basic Settings
		Interfaces

Category	Feature	Submenu
System Management	Access Control List	MAC ACL
		IP Standard ACL
	User Management	
	Authentication Server	RADIUS
		TACACS+
	IP Authorized Manager	
	Event Settings	
	Syslog	
	SNMP	SNMP Setting
		SNMP Trap
	Console Settings	
	Maintenance	Load Factory Default
		Configuration Export
		Configuration Import
		Firmware Upgrade
		Ping
System Monitoring	System Logs	
	Relay State	
	LLDP Status	
	MAC Address Table	
	DHCP Client List	
	Port Trunking Status	
	Network Redundancy Status	Spanning Tree
		Multiple Super Ring
	Multicast Status	
	VLAN Status	
	RMON	
	PoE Status	
Save Configuration		
Reboot		
Logout		

3.2. Overview

An overview of the system is available. The Overview page enables you to view the current defined settings of the system.

Log in to the interface. The GUI screen displays the Overview menu.



Overview

Hardware Information	
Model name	JetNet5208GP-U
Serial number	JN2021120102
Software Information	
IP address	192.168.1.165
Device MAC address	00:12:77:62:a9:21
Firmware version	2.0.0-23022120
Device up time	0 Days 0 Hrs, 28 Mins, 50 Secs
Switch name	Switch
System contact	
System location	
System Information	
DC Power 1	Offline
DC Power 2	Online

Figure 4 Overview Menu

Item	Description
Hardware Information	
Model name	Specify the device model name.
Serial number	Specify the device serial number.
Software Information	
IP address	Specify the current device IP address.
Device MAC address	Specify the device MAC address.
Firmware version	Specify the current device firmware version.
Device up time	Specify the number of days, hours, minutes, and seconds since the last system restart. The **Device up time** is displayed in the following format: days, hours, minutes, and seconds.
Switch name	Specify the current device name.
System contact	Specify the listed individual to contact relating to device issues.
System location	Specify the current installed location of the device.
System Information	
DC Power 1	Specify the status of the device DC 1 power.
DC Power 2	Specify the status of the device DC 2 power.

3.3. System Settings

3.3.1. Device Settings

The **Device Settings** are configured by running this wizard. The wizard enables you to manage the switch name, system contact, and system location of the system.

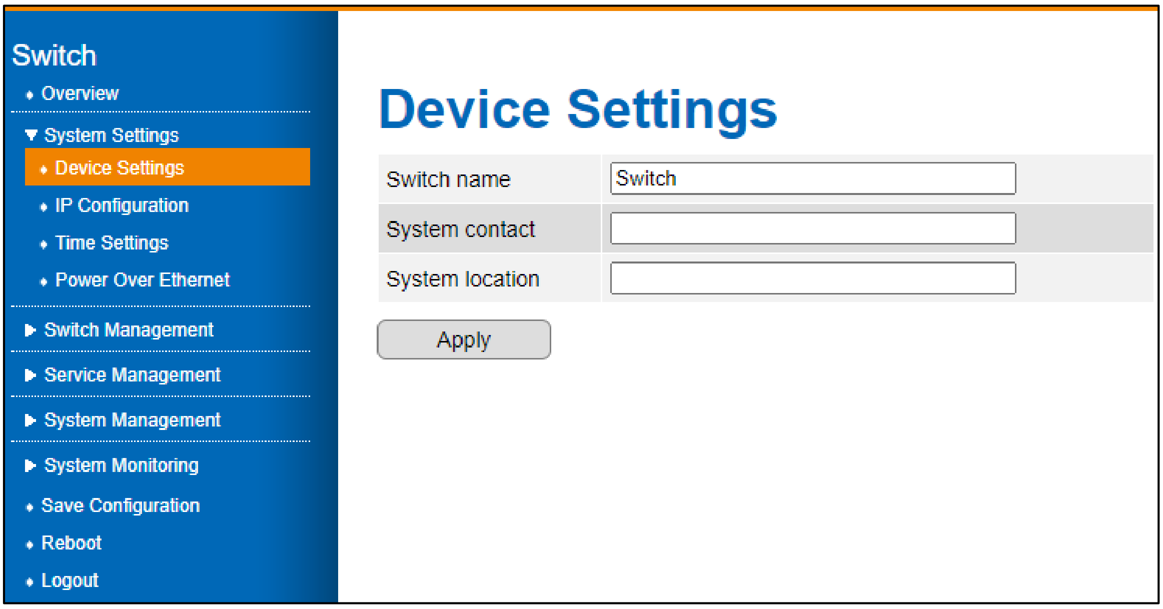
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Settings** > **Device Settings**. The GUI screen displays the Device Settings menu.

3 - Select the fields to be configured to define the device.

4 - Click **Apply**.



Device Settings

Switch name: Switch

System contact:

System location:

Figure 3 Device Settings Menu

Item	Description
Switch name	Specify the name of the device. Enter a value to modify it. By default, the device host name is defined by the word switch.
System contact	Specify the name of a contact person. Enter a value to define it.
System location	Specify the physical location of the device. Enter a value to define it.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.3.2. IP Configuration

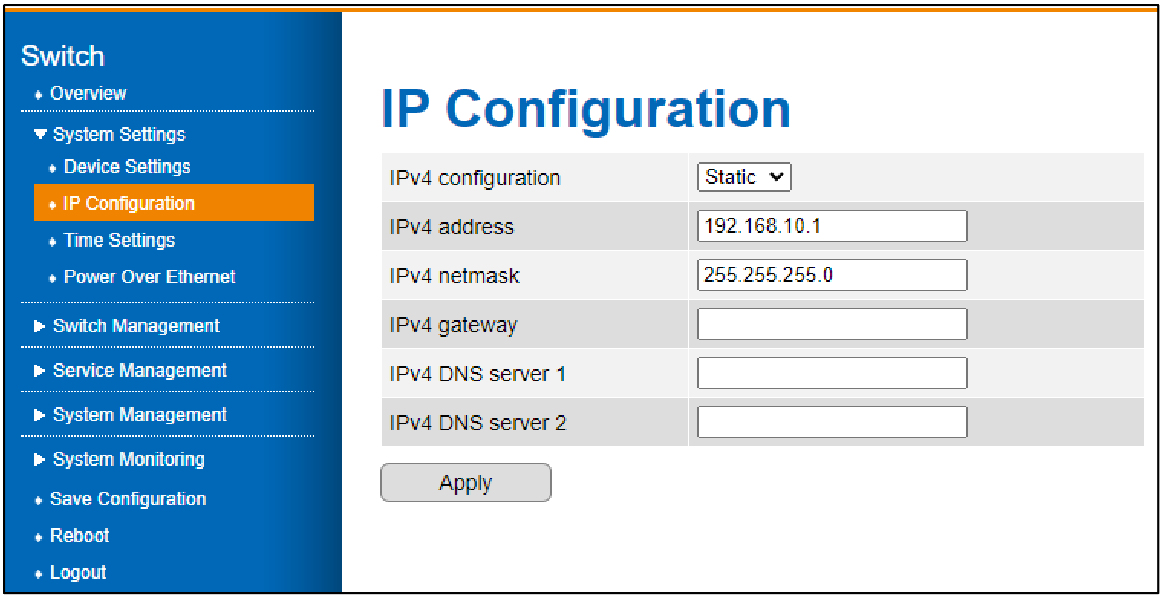
The **IP Configuration** settings are configured by running this wizard. The wizard enables you to manage static (default) or DHCP IP configuration of the system.

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Settings** > **IP Configuration**. The GUI screen displays the IP Configuration menu.

3 - Select the fields to be configured to define the device.

4 - Click **Apply**.



IP Configuration

IPv4 configuration	Static
IPv4 address	192.168.10.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 DNS server 1	
IPv4 DNS server 2	

Figure 3 IP Configuration Menu

Item	Description
IPv4 configuration	Specify the IPv4 interface source: Static (default) or DHCP.
IPv4 address	Specify the IP address of the interface.
IPv4 netmask	Specify the IP mask of the designated IP address.
IPv4 gateway	Specify the IP gateway of the interface.
IPv4 DNS server 1	Specify the IP address of the DNS server 1.
IPv4 DNS server 2	Specify the IP address of the DNS server 2.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.3.3. Time Settings

The **Time Settings** are configured by running this wizard. The wizard enables you to manage the system time configuration of the system. The configuration of the system clock is an essential component of a network. Synchronized system clocks provide a common reference between all network devices. In order to manage, secure, plan, and debug a network, it is imperative that time is synchronized. When tracking network usage or security breaches, it is impossible to correlate log files between devices without synchronized clocks.

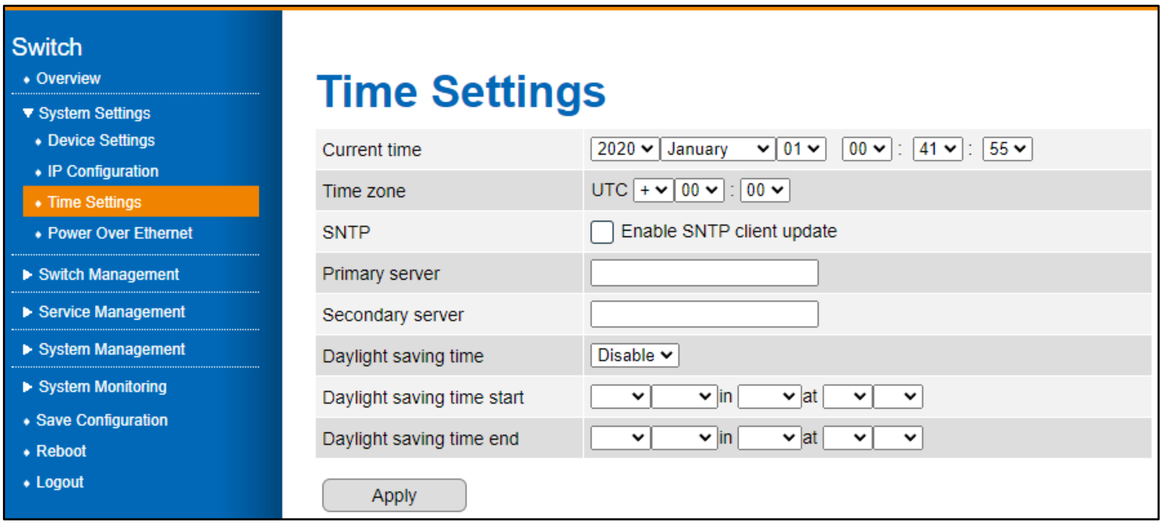
To configure the settings, see the following steps:

1 - Log in to the interface.

2 - Click **System Settings** > **Time Settings**. The GUI screen displays the **Time Settings** menu.

3 - Select the fields to be configured to define the device.

4 - Click **Apply**.



Time Settings

Current time	2020 January 01 00 : 41 : 55
Time zone	UTC + 00 : 00
SNTP	□ Enable SNTP client update
Primary server	
Secondary server	
Daylight saving time	Disable
Daylight saving time start	in at
Daylight saving time end	in at

Apply

Figure 4 Time Settings Menu

Item	Description
Current time	Specify the current system time. The time is displayed in the following format: Year, Month, Day, Hour, Minutes, Seconds.
Time zone	Specify the Time Zone offset. Select the difference in hours between Coordinated Universal Time (UTC) and the local time.
SNTP	Specify a source to set the system clock. Disabled by default.
Primary server	If SNTP is enabled, specify the primary SNTP server to obtain the system time.
Secondary server	If SNTP is enabled, specify the secondary SNTP server to obtain the system time.

Item	Description
Daylight saving time	Specify the daylight savings time (DST) offset. Disabled by default.
Daylight saving time start	If DST is enabled, specify when the function is enabled. The time is displayed in the following format: Order, Day, Month, Hour, Minutes.
Daylight saving time end	If DST is enabled, specify when to disable the function. The time is displayed in the following format: Order, Day, Month, Hour, Minutes.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.3.4. Power Over Ethernet

PoE (Power Over Ethernet) switches* provide power to network devices. Data and power are distributed over the same cabling in PoE models only. This eliminates the need for separate data cables and outlets. In addition, the cost of cabling and installation is significantly reduced since the voltage and power requirements are much lower than those for mains powered devices.
A PoE installation involves two types of equipment:

- Power Sourcing Equipment (PSE), such as an Ethernet LAN switch, supplies power to the cable together with the data.
- Powered Devices (PDs), such as Wireless Access Points or IP Phones, receive power and data over this same cabling.

Whenever there is no power on a circuit, a PoE-capable switch port automatically supplies power to these devices:

- Devices that comply with IEEE 802.3af
- Devices that comply with IEEE 802.3at
- Device that comply with IEEE 802.3bt

When connected to PoE switch ports and AC power sources, powered devices can receive redundant power. When connected only to PoE ports, powered devices do not receive redundant power.

*The Power over Ethernet function is only available on PoE switches.

3.3.4.1.PoE Settings

The **PoE Settings** are configured by running this wizard. The wizard enables you to manage the system’s PoE configuration to deliver power to the powered devices (PD). The PoE function is disabled by default on the JetNet series switches.

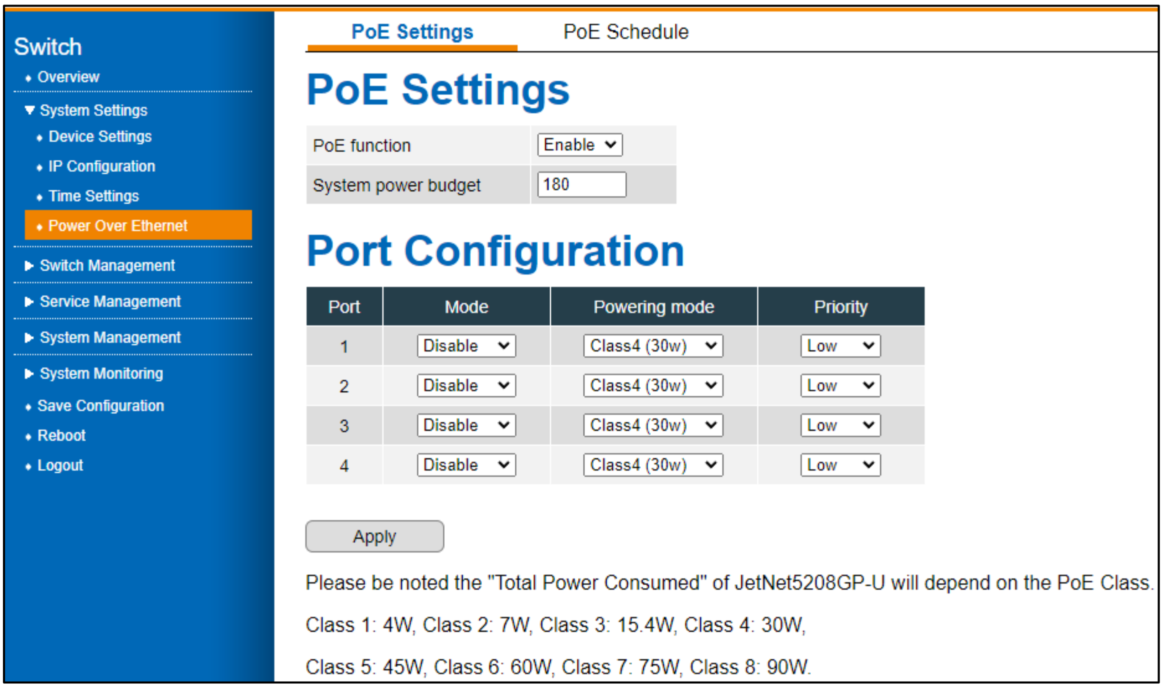
To configure the settings, see the following steps:

1 - Log in to the interface.

2 - Click **System Settings** > **Power Over Ethernet**. The GUI screen displays the PoE Settings menu.

3 - Select the fields to be configured to define the device.

4 - Click **Apply**.



PoE Settings

PoE function	Enable
System power budget	180

Port Configuration

Port	Mode	Powering mode	Priority
1	Disable	Class4 (30w)	Low
2	Disable	Class4 (30w)	Low
3	Disable	Class4 (30w)	Low
4	Disable	Class4 (30w)	Low

Please be noted the "Total Power Consumed" of JetNet5208GP-U will depend on the PoE Class.

Class 1: 4W, Class 2: 7W, Class 3: 15.4W, Class 4: 30W,

Class 5: 45W, Class 6: 60W, Class 7: 75W, Class 8: 90W.

Figure 4 PoE Settings Menu

Item	Description
PoE function	Specify the PoE function state: Disable (default) or enable. By default, the setting is set to default. • Disable – By default PoE is disabled on all respective ports. • Enable – The system sends power to the powered devices.
System power budget	Specify the amount of power (W) budget for all enabled ports. By default, the system power budget is 180W.
Port	Displays the PoE port interface number.

Item	Description
Mode	Specify the PoE function state of the port. By default, the setting is set to default. • Disable – By default PoE is disabled on the respective port. • Enable – The system sends power to the powered devices. • Schedule – The port is enabled only during the scheduled time. See PoE Schedule.
Powering mode	Specify the amount of power allocated to a port by using a class or option: • Class3 (15.4w) • Class4 (30w) • Class6 (60w) • Class8 (90w)
Priority	Specify the priority level for the port, the lowest-numbered port at that level is provisioned first: • Critical: Provides high-priority PoE support for the specified ports. Active PoE ports at this level are provisioned before any others. • High: Specifies the second priority PoE support for port-list>. The active PoE ports at this level are provisioned first. • Low (default): Specifies the third priority PoE support for <port-list>. This level will only provision active PoE ports if there is power available after provisioning all other active PoE ports.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.3.4.2. PoE Schedule

The **PoE Schedule** lets you specify how long power should be delivered to a PoE port. It can be used, for example, as a security feature to prevent wireless access from being available outside of business hours, or to save power when devices are not in use. A PoE schedule can be selected by assigning a specific time and day on the specified port.

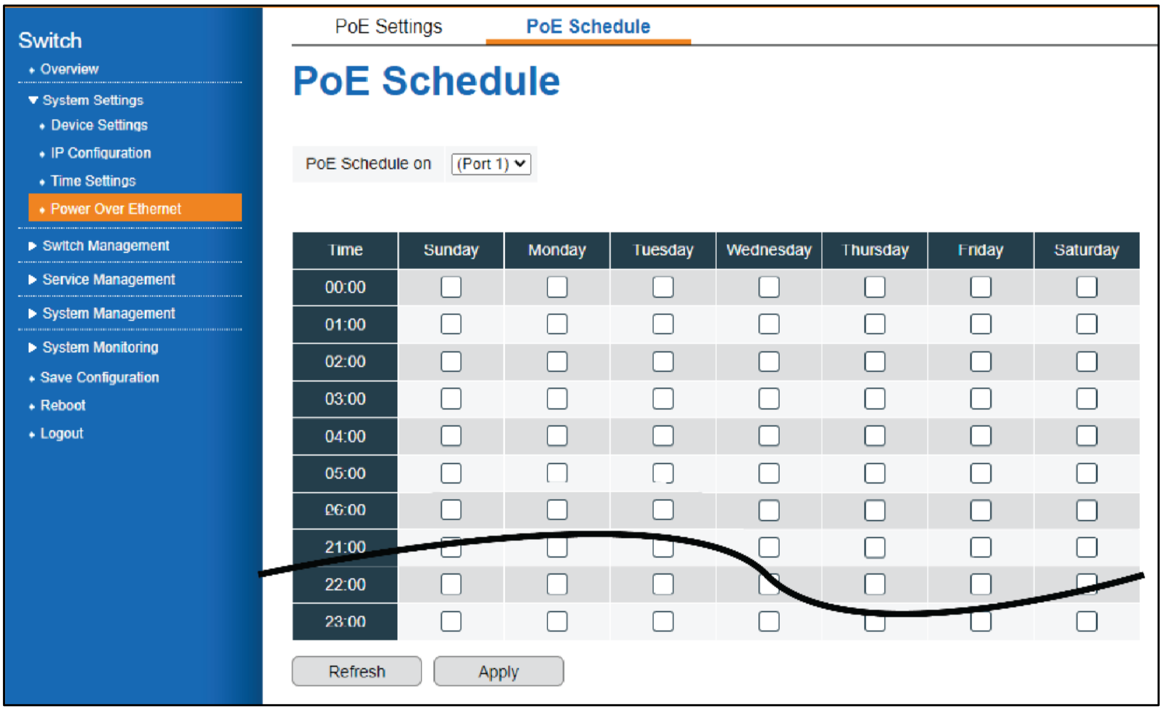
To configure the settings, see the following steps:

1 - Log in to the interface.

2 - Click System **Settings** > **Power Over Ethernet**> **PoE Schedule**. The GUI screen displays the PoE Schedule menu.

3 - Select the fields to be configured to define the device.

4 - Click **Apply**.



PoE Schedule

PoE Schedule on (Port 1)

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	□	□	□	□	□	□	□
01:00	□	□	□	□	□	□	□
02:00	□	□	□	□	□	□	□
03:00	□	□	□	□	□	□	□
04:00	□	□	□	□	□	□	□
05:00	□	□	□	□	□	□	□
06:00	□	□	□	□	□	□	□
21:00	□	□	□	□	□	□	□
22:00	□	□	□	□	□	□	□
23:00	□	□	□	□	□	□	□

Figure 4 PoE Schedule Menu

Item	Description
PoE Schedule on	Specify the PoE port to configure.
Time	Displays the time in hour increments. Specify a specific time to enable the PoE function on the selected port.
Day	Displays the days of the week. Specify a specific day to enable the PoE function on the selected port.
Refresh	Click to refresh the PoE Schedule entry list.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4. Switch Management

3.4.1. Port Manager

The **Port Manager** settings are configured by running this wizard. The wizard enables you to manage the port settings of the system. With the Port Manager page, you can customize the ports on the Switch to find the optimal balance of speed and flow control. When arranging your preferences for the Switch, you will need to consider additional factors when configuring Gigabit ports as opposed to 10/100Mb ports.

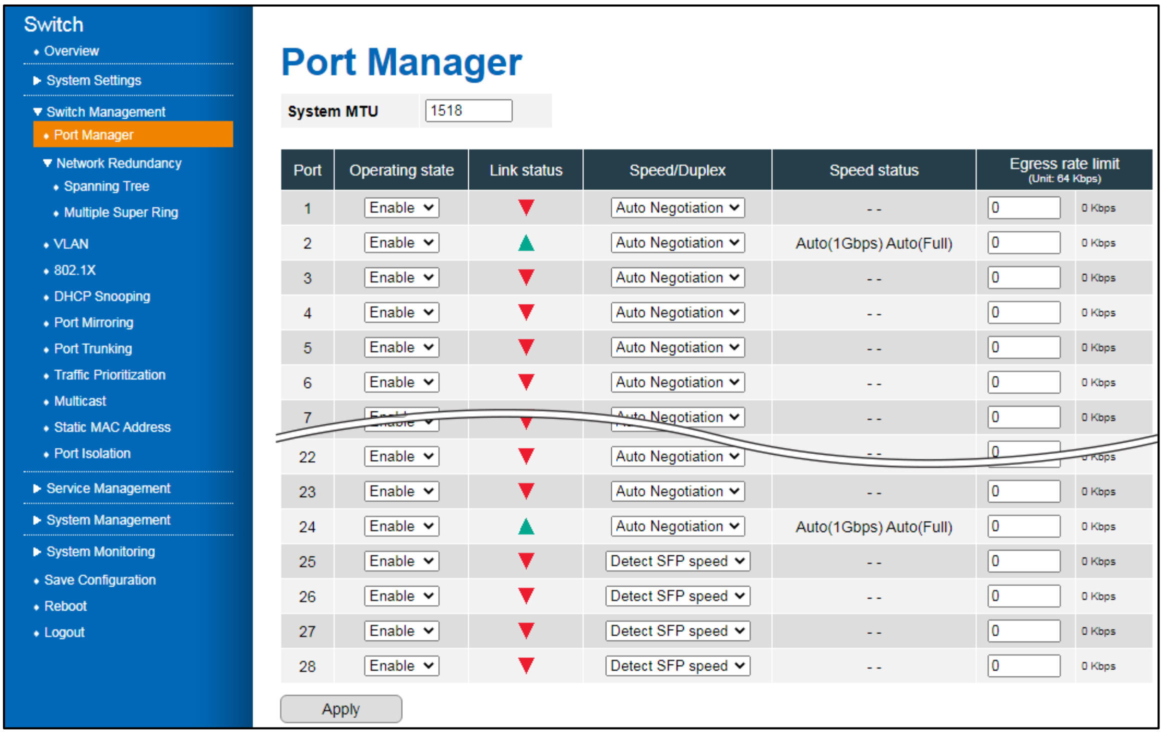
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Port Manager**. The GUI screen displays the **Port Manager** menu.

3 - Select the fields to be configured to define the port.

4 - Click **Apply**.



Port Manager

System MTU 1518

Port	Operating state	Link status	Speed/Duplex	Speed status	Egress rate limit (Unit: 64 Kbps)	
1	Enable	▼	Auto Negotiation	- -	0	0 Kbps
2	Enable	▲	Auto Negotiation	Auto(1Gbps) Auto(Full)	0	0 Kbps
3	Enable	▼	Auto Negotiation	- -	0	0 Kbps
4	Enable	▼	Auto Negotiation	- -	0	0 Kbps
5	Enable	▼	Auto Negotiation	- -	0	0 Kbps
6	Enable	▼	Auto Negotiation	- -	0	0 Kbps
7	Enable	▼	Auto Negotiation	- -	0	0 Kbps
22	Enable	▼	Auto Negotiation	- -	0	0 Kbps
23	Enable	▼	Auto Negotiation	- -	0	0 Kbps
24	Enable	▲	Auto Negotiation	Auto(1Gbps) Auto(Full)	0	0 Kbps
25	Enable	▼	Detect SFP speed	- -	0	0 Kbps
26	Enable	▼	Detect SFP speed	- -	0	0 Kbps
27	Enable	▼	Detect SFP speed	- -	0	0 Kbps
28	Enable	▼	Detect SFP speed	- -	0	0 Kbps

Apply

Figure 5 Port Manager

Item	Description
System MTU	Specify the maximum transmission unit (MTU), packet or frame size, to define the Port list to display. Range includes: 46~9216.
Port	Displays the port interface number.
Operating state	Specify the state of the interface: enabled (default) or disabled.
Link status	Displays the interface link status: up or down.
Speed/Duplex	Specify the port speed and duplex mode of the port. See the following for further information: • JetNet5208G/5210G/5212G/5216G series: A Auto Negotiation (default), 10 Mbps Half (Duplex) mode, 10 Mbps, Full (Duplex) mode, 100 Mbps Half (Duplex) mode, 100 Mbps Full (Duplex) mode, 1Gbps Full (Duplex) mode. • JetNet6228G series: Auto Negotiation (default), 10 Mbps Half (Duplex) mode, 10 Mbps, Full (Duplex) mode, 100 Mbps Half (Duplex) mode, 100 Mbps Full (Duplex) mode, 1Gbps Full (Duplex) mode.
Speed status	Displays the current speed of the interface.
Egress rate limit	Specify the limit rate of the port. 1 unit corresponds to 64 Kbps. Values range: 64 Kbps to 1 Gbps.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.2. Network Redundancy

3.4.2.1.Spanning Tree

Through the Spanning Tree Protocol (STP), a Layer 2 Broadcast domain is protected from Broadcast storms by selectively putting links into standby mode to prevent loops. In standby mode, these links temporarily stop transferring user data. When the topology changes and data transfer resumes, the links are automatically reactivated.

3.4.2.1.1. Mode Selection

The Spanning Tree **Mode Selection** settings are configured by running this wizard. The wizard enables you select a mode and protocol for the spanning tree.
Before configuring a spanning tree:

- Choose between RSTP and MSTP as the spanning tree protocol. When your network has fewer than 100 VLANs, RSTP is the ideal solution. Because of the increased load on switch CPUs, MSTP is recommended when networks have 100 or more VLANs.
- Assign instance priority to the root bridge and leaf node roles.

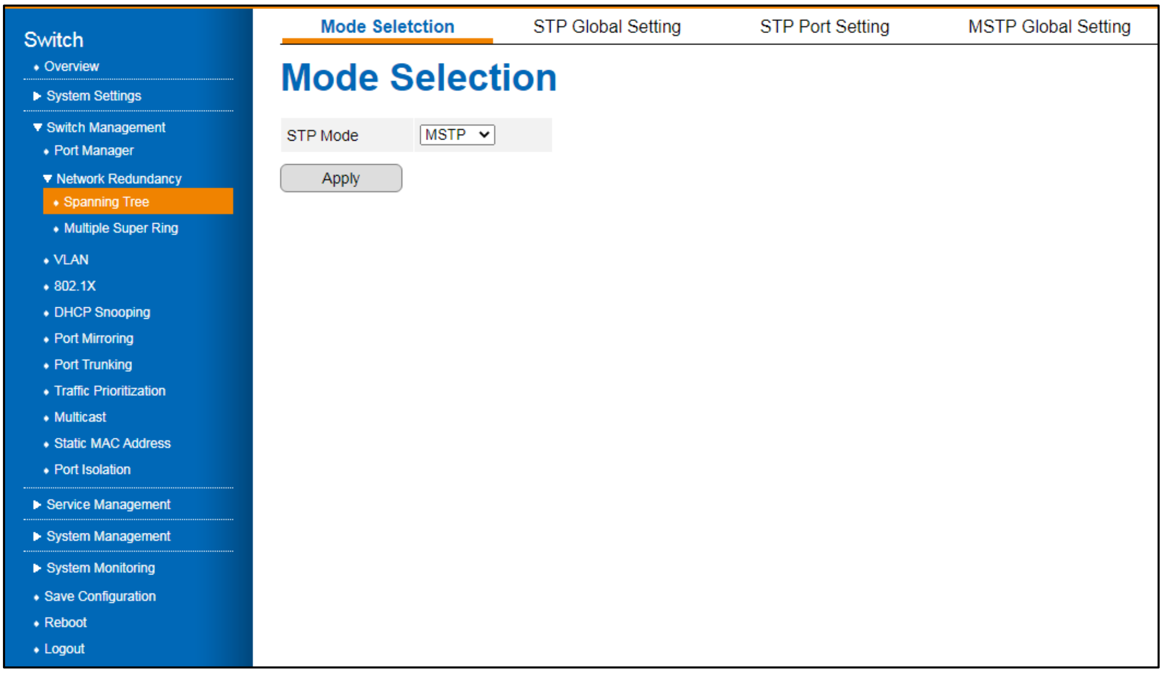
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click Switch Management >Network Redundancy > Spanning Tree. The GUI screen displays the Mode Selection menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



Mode Selection

STP Mode: MSTP

Figure 6 Switch Management >Network Redundancy > Spanning Tree > Mode Selection Menu

Item	Description
STP Mode	Specify the spanning tree protocol (STP), a loop-free active forwarding topology. By default, the setting is set to RSTP. • Disable – By default spanning tree is enabled on all ports. The setting disables the mode. • RSTP – Network loops are prevented by blocking redundant ports. Data is still received on a blocked port, but it will not be sent to other network devices. This ensures that switches receive only one copy of a packet. Any active path that fails will be replaced by one of the blocked ports. Configuration topologies determine the port to be used. • MSTP (default) – This spanning-tree mode is based on the IEEE 802.1s standard. Multiple VLANs can be mapped to a single spanning-tree instance, which reduces the number of instances needed to support a large number of VLANs. As a result of MSTP running on top of IEEE 802.1w, spanning trees can be rapidly converged by eliminating the forward delay and quickly transitioning root ports and designated ports to forwarding.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.2.2.STP Global Setting

The Spanning Tree **STP Global Setting** is configured by running this wizard. The wizard enables you to configure the settings for each mode.

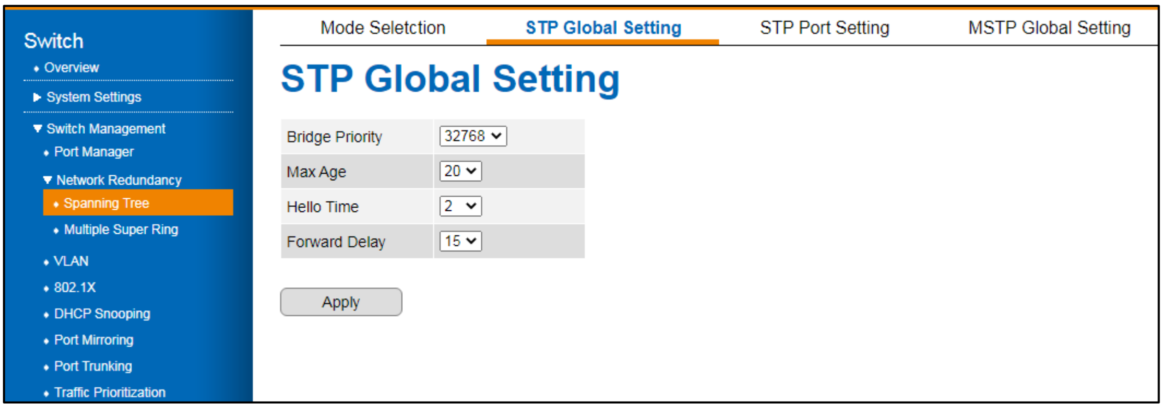
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Network Redundancy** > **Spanning Tree** > **STP Global Setting**. The GUI screen displays the STP Global Setting menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



STP Global Setting

Bridge Priority: 32768
Max Age: 20
Hello Time: 2
Forward Delay: 15

Figure 7 Switch Management > Network Redundancy > Spanning Tree > STP Global Setting Menu

Item	Description
Bridge Priority	Specify the bridge priority. When BPDUs are exchanged, the device with the lowest priority becomes the Root Bridge. When all bridges are using the same priority, then their MAC addresses are used to determine which is the Root Bridge. Each increment of 4096 represents a bridge priority value. A few examples are 4096, 8192, 12288, etc.
Max Age	Specify the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time	Specify the Switch Hello Time. It refers to the time a bridge spends listening before forwarding packets. The default is 15 seconds.
Forward Delay	Specify the Switch Forward Delay Time. This is the amount of time (in seconds) the root switch waits before changing states.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.2.3.STP Port Setting

The Spanning Tree **STP Port Setting** is configured by running this wizard. The wizard enables you to configure the settings for each port.

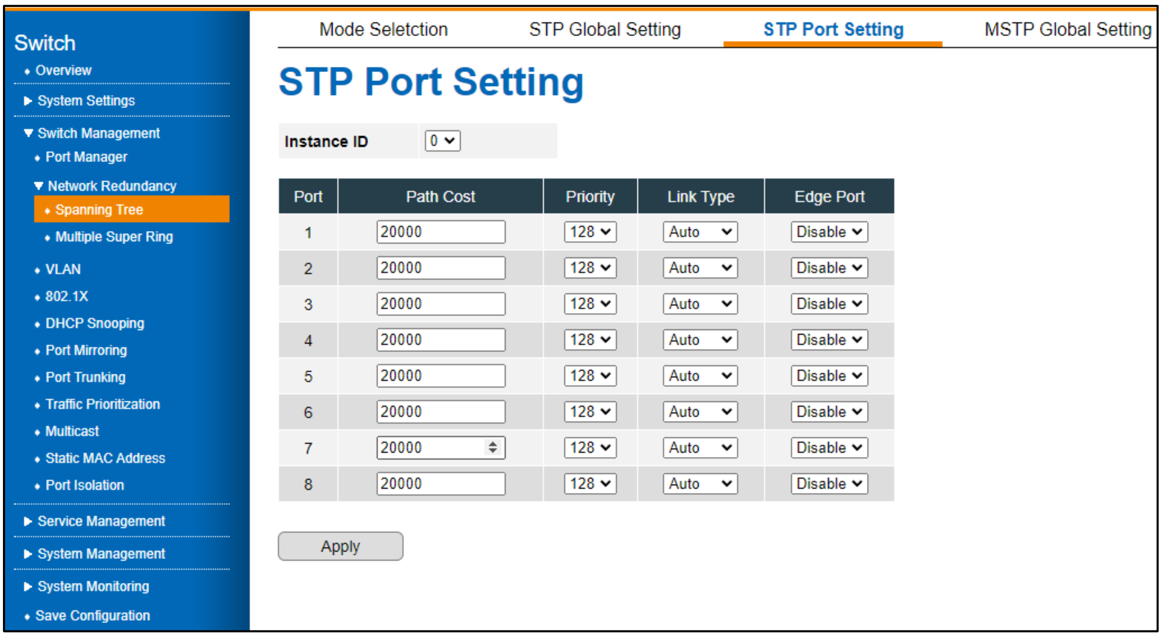
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Network Redundancy** > **Spanning Tree** > **STP Port Setting**. The GUI screen displays the STP Port Setting menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



Instance ID: 0

Port	Path Cost	Priority	Link Type	Edge Port
1	20000	128	Auto	Disable
2	20000	128	Auto	Disable
3	20000	128	Auto	Disable
4	20000	128	Auto	Disable
5	20000	128	Auto	Disable
6	20000	128	Auto	Disable
7	20000	128	Auto	Disable
8	20000	128	Auto	Disable

Figure 8 Switch Management > Network Redundancy > Spanning Tree > STP Port Setting Menu

Item	Description
Instance ID	Specify the created MST group. A maximum of 16 groups can be set for the device. If mode is RSTP, the setting cannot be changed.
Port	Displays the port interface number.
Path Cost	Specify the cost of the path to the other bridge from the transmitting bridge at the specified port. The default is 20000 with a range of 1 to 200,000,000.
Priority	Specify the bridge priority value for the MST. This value determines a port's priority in a LAN. It ranges from 0 to 240 in multiples of 16.

Item	Description
Link Type	Specify the link type of the interface. The values are as follows: • Point-to-Point – Specifies that the port is treated as if it is connected to a point-to-point link. • SharedLan – Specifies that the port is treated as if it is having a shared media connection. In the Port Status Configuration screen, the switch can determine the point-to-point status either directly or as Auto.
Edge Port	Specify the operating edge port state. Range: Disabled (default), Enabled
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.2.4.MSTP Global Setting

The Spanning Tree M**STP Global Setting** is configured by running this wizard. The wizard enables you to configure the settings for each port.

To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Network Redundancy** > **Spanning Tree** > **MSTP Global Setting**. The GUI screen displays the MSTP Global Setting menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.

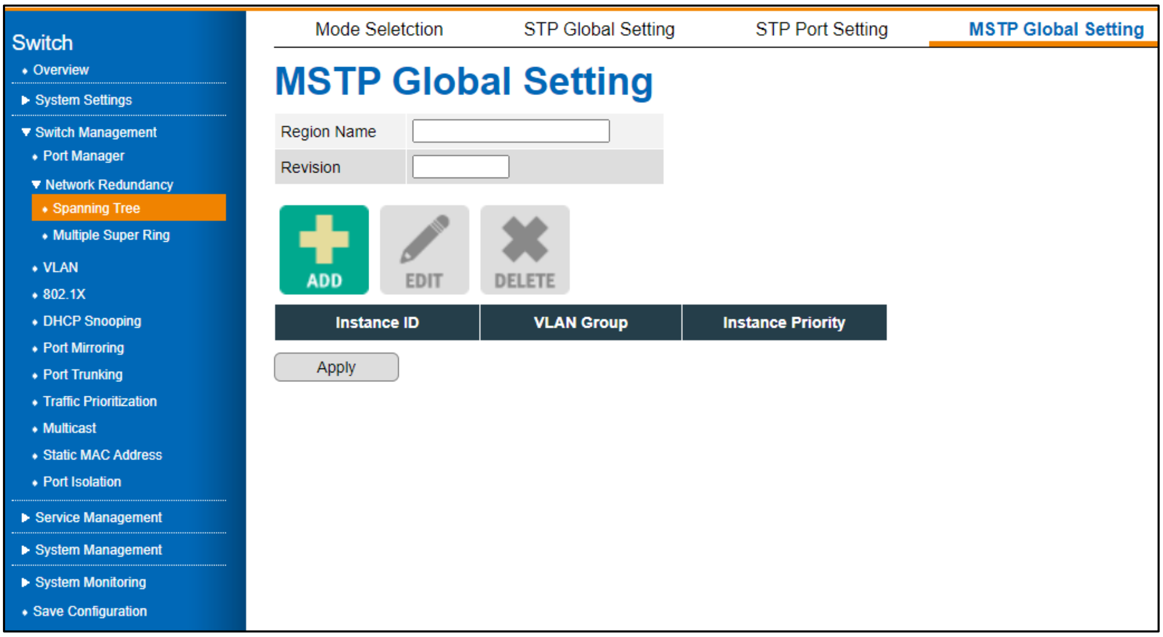


Figure 8 Switch Management > Network Redundancy > Spanning Tree > MSTP Global Setting Menu

Item	Description
Region name	Specify the region name in which the switch resides.
Revision	Specify the revision number designated for the MSTP region. The setting must be the same for all the switches residing in the same region.
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **DELETE** to delete an existing configuration.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.3. Multiple Super Ring

Redundancy in industrial networks is usually achieved by forming a ring or loop. Typically, managed switches are connected in series, with the last switch connected to the first. You can implement Multiple Super Ring technology in such a connection to get the fastest recovery speed.

Multiple Super Ring (MSR) technology is the third generation of Ring redundancy technology. This technology is used throughout the world. For 100Base-TX copper port, MSR ranks as the fastest restore and failover (milliseconds). Other interfaces may take longer due to media characteristics.

Using **Rapid Dual Homing** (RDH) technology, JetNet Managed Switch can also easily and conveniently connect to a core managed switch. RDH technology also allows you to couple multiple Rapid Super Rings or RSTP clouds together, known as Auto Ring Coupling.

The TrunkRing technology integrates MSR with LACP/Port Trunking. LACP/Trunk aggregated ports are virtual interfaces that can function as MSR Ring ports.

Beijer is able to support the **MultiRing technology**. Using different Ring IDs, multiple rings can be aggregated within one switch. The maximum number of rings a switch can support is half of its total port volume. The JetNet5200G, for example, is a 24 Fast Ethernet network Ethernet+ 4 Gigabit port design which can aggregate up to 14 Rings (12 x 100M Rings and 2 Gigabit Rings) into one JetNet228G, which saves time and effort when creating complex networks.

In addition to supporting Legacy Super Ring technology, JetNet Series switches also support Super Ring Client mode. Super Ring ports can pass through control packets extremely well and work with Super Ring.

3.4.3.1.MSR Global Setting

The **Multiple Super Ring** settings are configured by running this wizard. The wizard enables you to configure the redundancy.

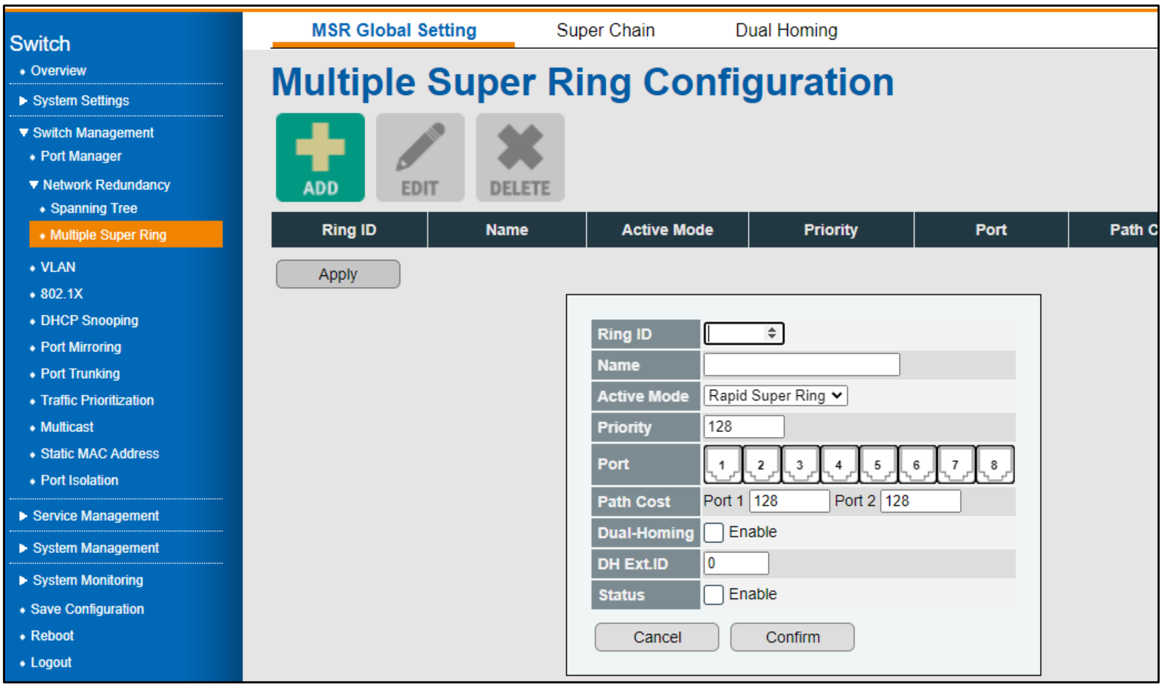
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Network Redundancy** > **Multiple Super Ring** > **STP Port Setting**. The GUI screen displays the STP Port Setting menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



Multiple Super Ring Configuration

Ring ID	Name	Active Mode	Priority	Port	Path C

Ring ID	
Name	
Active Mode	Rapid Super Ring
Priority	128
Port	1 2 3 4 5 6 7 8
Path Cost	Port 1 128 Port 2 128
Dual-Homing	☐ Enable
DH Ext.ID	0
Status	☐ Enable

Figure 9 Switch Management > Network Redundancy > Multiple Super Ring Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **DELETE** to delete an existing configuration.
Ring ID	Specify the ring ID. The range is 0 to 31. If the field is left blank, by default the Name field defines the ring ID. Once the ring is created, the ring ID cannot be changed.
Name	Specify the name of the ring. If the field is left blank, by default the Name field is defined by the RingID variable.
Active Mode	Specify the ring active mode type. The range includes Rapid Super Ring (RSR) (default) and Super Chain. • RSR: Recovery time is reduced from 30ms to a few ms for both copper and fiber rings. When the primary path fails, the second path is recovered within a few milliseconds. The member ring port is the primary path and the border ring port is the block path. In addition, the restoration time is shortened to zero. • Super Chain: Highly flexible, self-healing, and can recover in less than 10 seconds from any failure. A huge network with up to two hundred switches can also be operated efficiently with it. By connecting border switches and member switches, users can create a new independent chain, which can be interoperable with other redundant networks, such as RSTP, MSTP, STP, ERPS, etc.

Item	Description
Priority	Specify the ring priority. A switch with the highest priority (the highest value) will automatically be selected as a Ring Master. When configured, one of its ring ports will become a forwarding port, while another will become a blocking port. If all switches are assigned the same priority, the switch with the highest MAC address will be selected as the Ring Master. The range is: 0 to 255.
Port	Click to select the port to include in the configuration.
Path Cost	Specify the path cost for Port 1 and Port 2. As the Ring Master of a Ring, it determines which port is blocked. In a two-ring port, the port with the higher Path Cost will be the blocking port. If the Path Cost is equal, the port with the larger port number will be the blocking port. The range is: 0 to 255.
Dual-Homing	Click to enable (disabled by default) the Dual-Homing feature. The rapid dual homing feature is one of the key features. In scenarios where you want to connect multiple RSRs or form a redundant topology with other vendors, RDH can support a maximum of seven redundant links.
DH Ext.ID	Specify RDH ID. The range is: 0 to 7, default is 0.
Status	Directly create and enable ring or create only and enable it later. Click to enable (disabled by default) the status of the ring.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.3.2.Super Chain

JetNet series switches can operate quickly and easily in redundant networks of any complexity. Super Chain provides a cost-effective way to link connected chains adding increased scalability and deployment. The Super Chain includes two borders that connect with other rings through an edge port, while member nodes function as reset nodes. As soon as a segment fails, the standby edge port recovers in milliseconds and restores service seamlessly. For increased flexibility and cost savings, users can add a new super ring to an existing super ring.

To configure the settings, see the following steps:

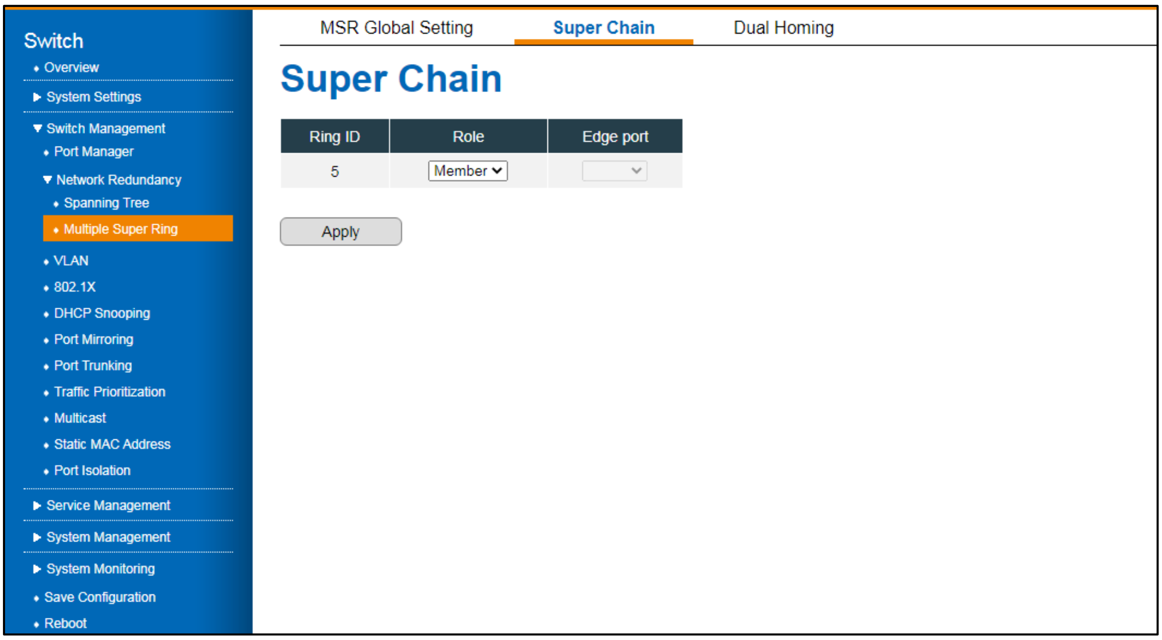
1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Network Redundancy** > **Multiple Super Ring** > **Super Chain**.

The GUI screen displays the Super Chain menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



Super Chain

Ring ID	Role	Edge port
5	Member	

Figure 10 Switch Management > Network Redundancy > Multiple Super Ring > Super Chain Menu

Item	Description
Ring ID	Specify the unique identifier as defined by the MSR configuration.
Role	Specify the priority of the switch: Member or Border.
Edge port	If the interface is assigned the role of Border, specify the edge port from the defined Port listing in the MSR configuration.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.3.3. Dual Homing

JetNet switches support dual homing independent media paths and two upstream switch connections per switch. Traffic is quickly moved to the standby connection when the Link signal is lost on the operating port connected upstream.

To configure the settings, see the following steps:

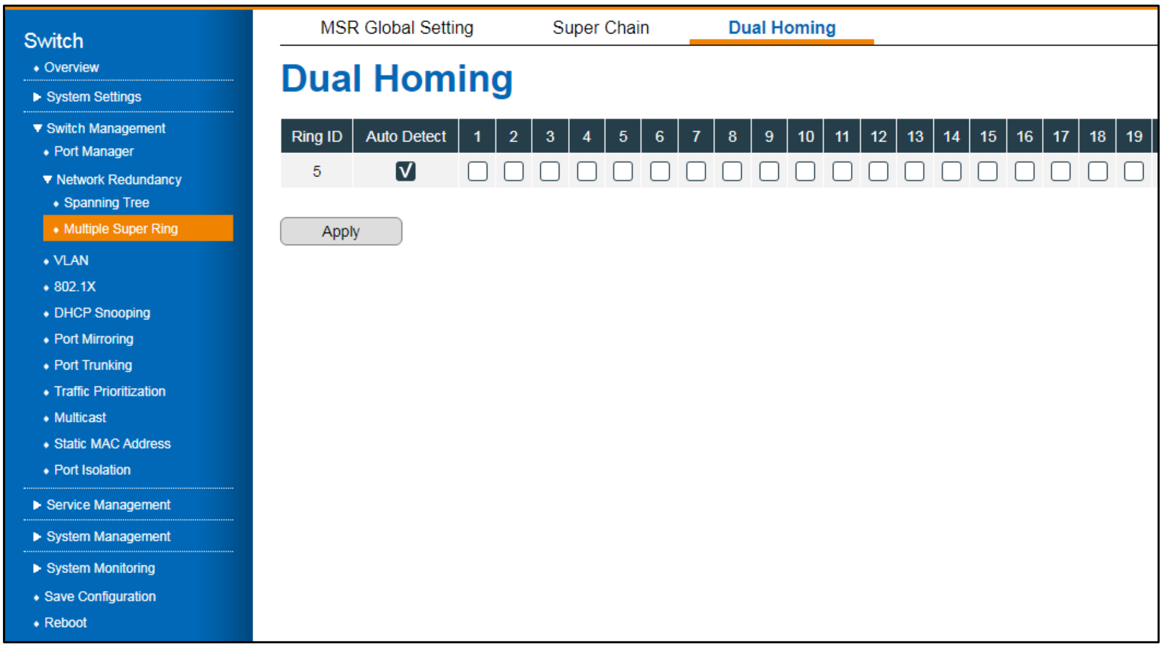
1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Network Redundancy** > **Multiple Super Ring** > **Dual Homing**.

The GUI screen displays the Dual Homing menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



Dual Homing

Ring ID	Auto Detect	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 11 Switch Management > Network Redundancy > Multiple Super Ring > Dual Homing Menu

Item	Description
Ring ID	Specify the ring ID as defined by the MSR configuration. Once the ring is created, the ring ID cannot be changed.
Auto Detect	Specify to enable or disable (default) the function. The system auto detects the connected devices that are running dual homing.
1 - 28	Specify the port to set up dual homing. The function must first be enabled.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.4. VLAN

A Virtual LAN (VLAN) is a logical Ethernet segment on a Layer 2 Switch that provides better administration, security, and management of multicast traffic. VLANs are network topologies configured logically rather than physically. Using a VLAN, you can group users by logical function instead of location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of their physical location. By using VLANs, you can logically segment your network into different broadcast domains so that ports with similar functions can be grouped into logical LAN segments.

3.4.4.1. Basic Settings

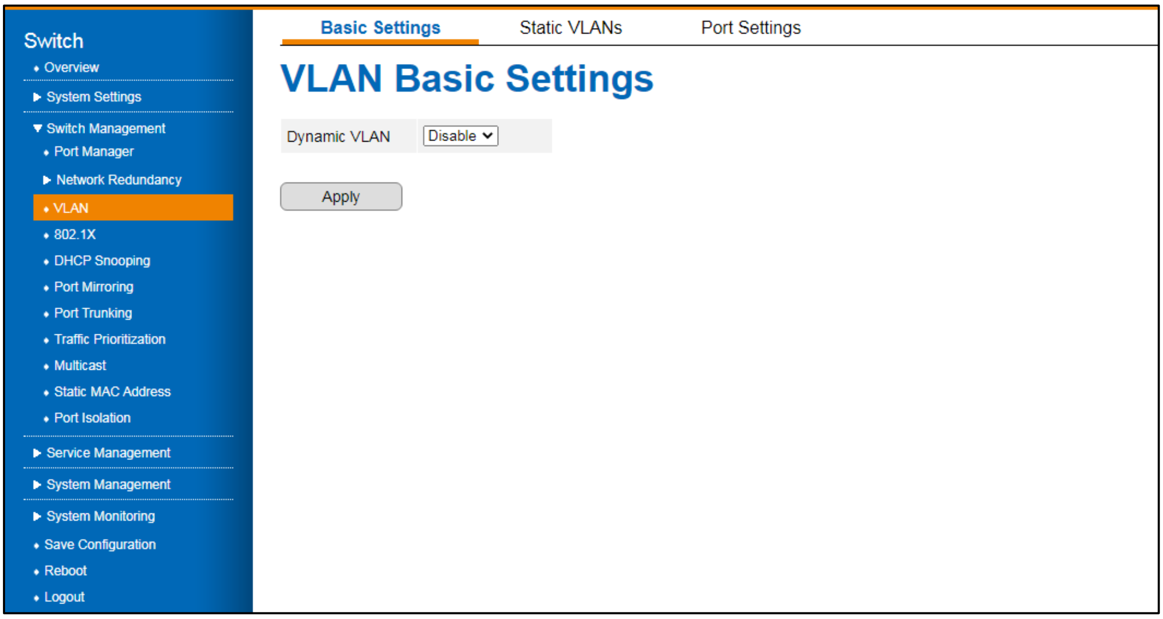
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **VLAN**. The GUI screen displays the **Basic Settings** menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



VLAN Basic Settings

Dynamic VLAN: Disable

Figure 12 Switch Management > VLAN > Basic Settings Menu

Item	Description
Dynamic VLAN	Specify to enable or disable (default) the function.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.4.2.Static VLANs

The function allows for the assignment of a VLAN.

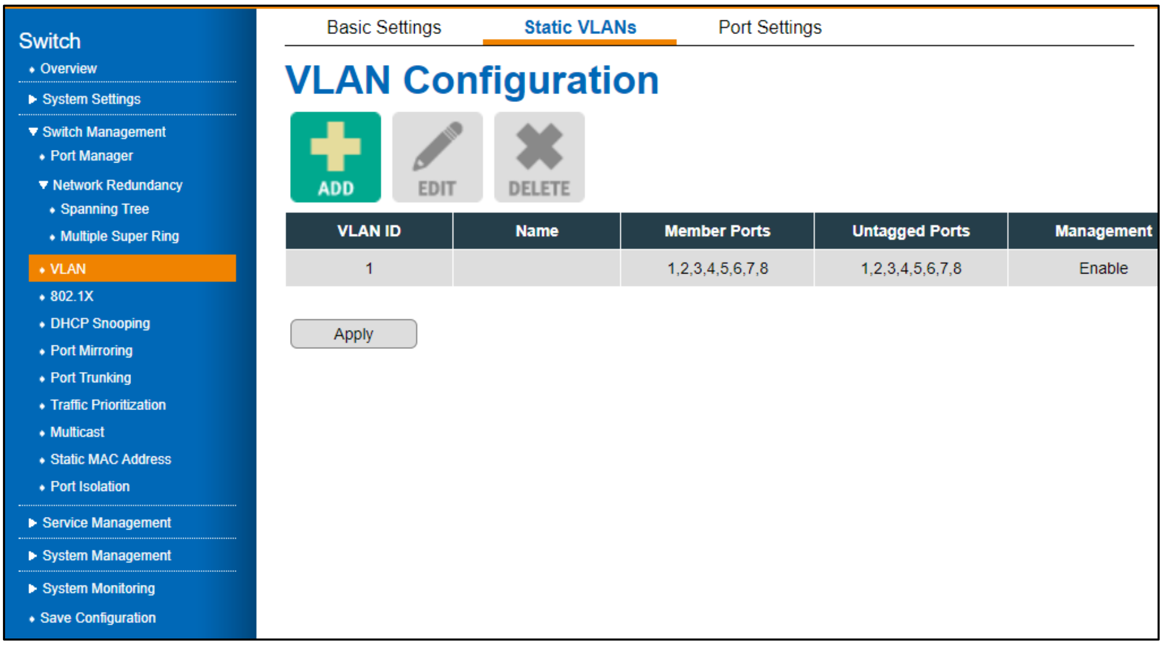
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **VLAN** > **Static VLANs**. The GUI screen displays the VLAN Configuration menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



VLAN Configuration

VLAN ID	Name	Member Ports	Untagged Ports	Management
1		1,2,3,4,5,6,7,8	1,2,3,4,5,6,7,8	Enable

Figure 13 Switch Management > VLAN > Static VLANs Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **DELETE** to delete an existing configuration.
VLAN ID	Specify an identifier for the entry. The range is 1 to 4094. The VLAN default is 1.
Name	Specify a reference name for the entry. The character limit is 12. If a name is not specified, the system automatically assigns a name.
Member Ports	Specify the ports to assign to the VLAN rule.

Item	Description
Untagged Ports	Specify the port to indicate egress/outgoing frames not VLAN tagged or not.
Management	Specify to designate the VLAN ID as supporting management VLAN. Only member ports of the management VLAN are allowed to ping and access the switch.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.4.3. Port Settings

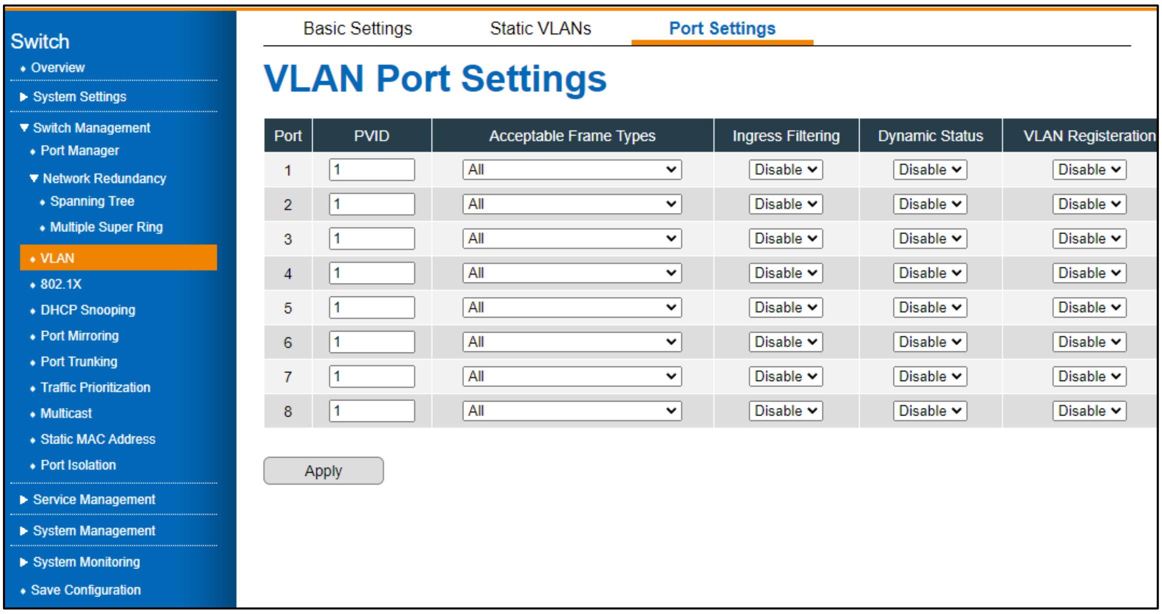
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **VLAN** > **Port Settings**. The GUI screen displays the VLAN Port Settings menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



VLAN Port Settings

Port	PVID	Acceptable Frame Types	Ingress Filtering	Dynamic Status	VLAN Registeration
1	1	All	Disable	Disable	Disable
2	1	All	Disable	Disable	Disable
3	1	All	Disable	Disable	Disable
4	1	All	Disable	Disable	Disable
5	1	All	Disable	Disable	Disable
6	1	All	Disable	Disable	Disable
7	1	All	Disable	Disable	Disable
8	1	All	Disable	Disable	Disable

Figure 14 Switch Management > VLAN > VLAN Port Settings Menu

Item	Description
Port	Displays the port interface number.

Item	Description
PVID	Specify the port VLAN ID. The abbreviation of Port VLAN ID. Switches can identify which ports belong to which VLAN using PVID. It is recommended that PVIDs be the same as VLAN IDs. PVID values range from 2 to 4094.
Acceptable Frame Types	Specify the frame type of the port. Options: All (default), Tagged, UnTagged and Priority Tagged. • All: the interface accepts both tagged and untagged frames. • Tagged: the interface only accepts tagged frames. • UnTagged and Priority Tagged: the interface accepts only untagged and priority frames.
Ingress Filtering	Specify to enable or disable (default) Ingress filtering. The function allows for filtering of undesired traffic on the port. After the function has been enabled, the port checks whether the incoming frames belong to the claimed VLAN.
Dynamic Status	Specify to enable or disable (default) Dynamic Status. If enabled, the function allows the port to receive VLAN information based on the MAC-address that is on the port. A dynamic port can belong to one VLAN only.
VLAN Registration	Specify to enable or disable (default) registration. The function allows for the automatic set up of VLANs rather than manually on every port.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.5. 802.1X

3.4.5.1.802.1X

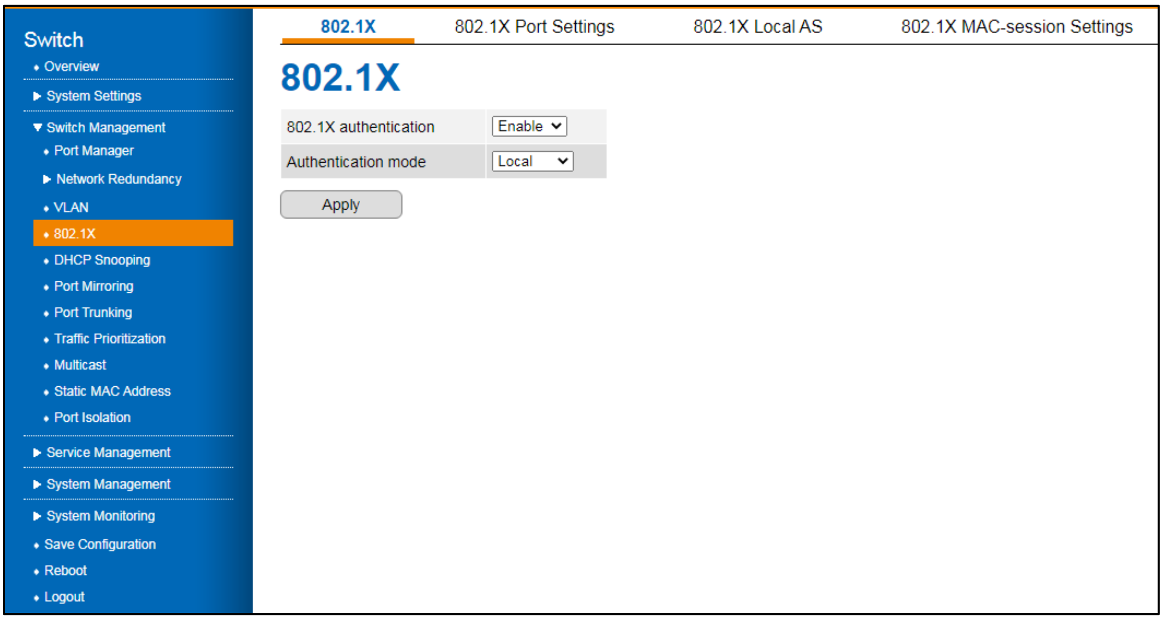
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **802.1X**. The GUI screen displays the 802.1X settings menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



802.1X

802.1X authentication: Enable

Authentication mode: Local

Figure 15 Switch Management > 802.1X > 802.1X Menu

Item	**Description**
802.1X authentication	Specify to enable or disable (default) authentication.
Authentication mode	Specify the method for the authentication function to connect to the switch to the authentication server. Local: In local authentication, a user-created database is used for authentication. RADIUS: This mode connects remotely to an access server for the purpose of authenticating users and authorizing their access.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.5.2. 802.1X Port Settings

IEEE 802.1X port-based authentication prevents unauthorized access to the network.

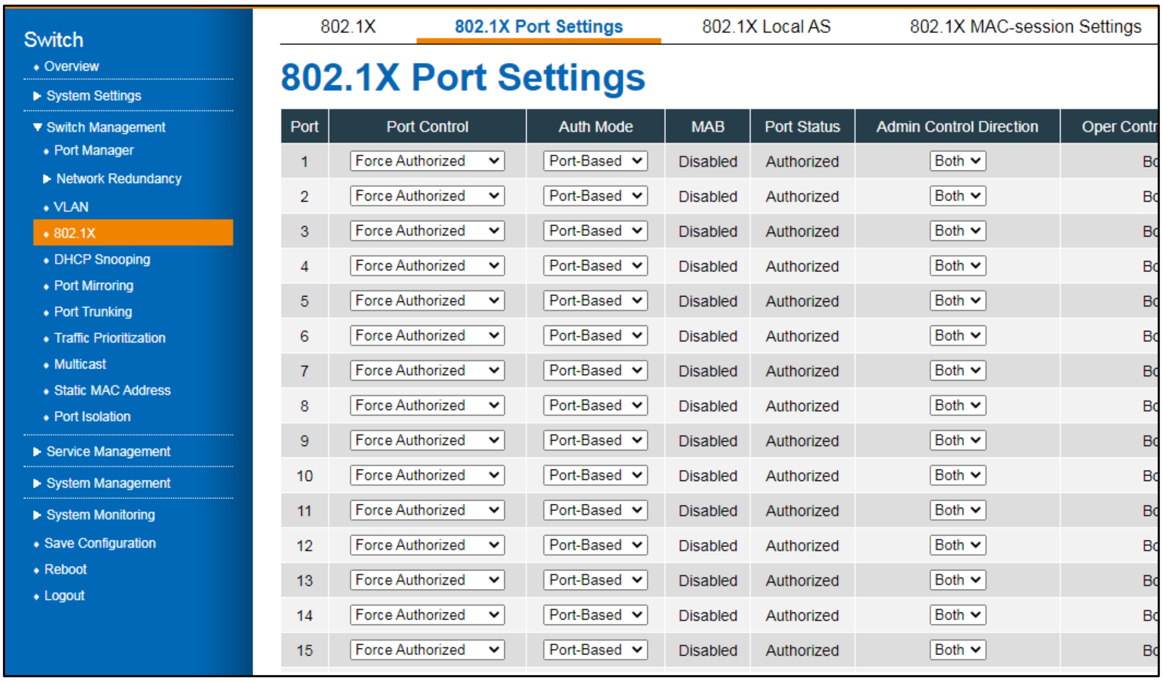
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **802.1X** > **802.1X Settings**. The GUI screen displays the 802.1X Port Settings menu.

3 - Select the fields to be configured to define the setting.

4 - Click **Apply**.



802.1X Port Settings

Port	Port Control	Auth Mode	MAB	Port Status	Admin Control Direction	Oper Contr
1	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
2	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
3	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
4	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
5	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
6	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
7	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
8	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
9	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
10	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
11	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
12	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
13	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
14	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo
15	Force Authorized	Port-Based	Disabled	Authorized	Both	Bo

Figure 16 Switch Management > 802.1X > 802.1X Port Settings Menu

Item	Description
Port	Specify the ID number of the port.
Port control	Specify the authentication behavior. • Force Unauthorized (default): port is blocked and the data is not able to move in/out. • Auto: port control is managed by RADIUS server • Force Authorized: port is authorized and the data is able to move in/out.

Item	Description
Auth mode	Specify the authentication mode. - Port-Based: Authentication based on host port, LAN access is restricted to 802.1X-capable clients who have entered authorized RADIUS user credentials. - MAC-Based: Authentication based on the host's source MAC address, eliminates the need to run an 802.1x user.
MAB	If this field is auto, the functional MAC Address will bypass to Radius Server for authentication.
Port status	Displays if the interface is either authorized or unauthorized.
Admin control direction	Specify the authorization port control direction. - Both: Incoming and outgoing traffic is blocked before authentication occurs. - In: Incoming traffic is blocked before authentication occurs.
Oper control direction	Specify in which flow of incoming and outgoing traffic is blocked. - Both: Incoming and outgoing traffic is blocked before authentication occurs. - In: Incoming traffic is blocked before authentication occurs.

Item	Description
AuthSM state	The state of the Authenticator State Machine for the entry. The options are: • Initialize –This state occurs when the module is disabled and port is down • Disconnected – There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition. • Connecting – This state is the beginning of the PNAC packet exchange • Authenticating – This state occurs whenever authenticator receives response ID from supplicant • Authenticated - This state occurs whenever authenticator SM port transitions to authorized through EAP exchange • Aborting – This state occurs when Authenticator SM receives re-authenticating event or EAP start or supplicant log off • Held - This state occurs when authentication failure occurs due to wrong user name or password • ForceAuth – This state occurs when the port control is changed to force authorized • ForceUnauth - This state occurs when the port control is changed to force unauthorized
Restart authentication	Specify if the port needs to restart authentication function: False, True:
Max request	Specify the number of times that the switch allows client request.
Reauth	Specify to enable or disable (default) the switch to ask clients to re-authenticate. The default time interval is 3600 seconds.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.5.3.802.1X Local AS

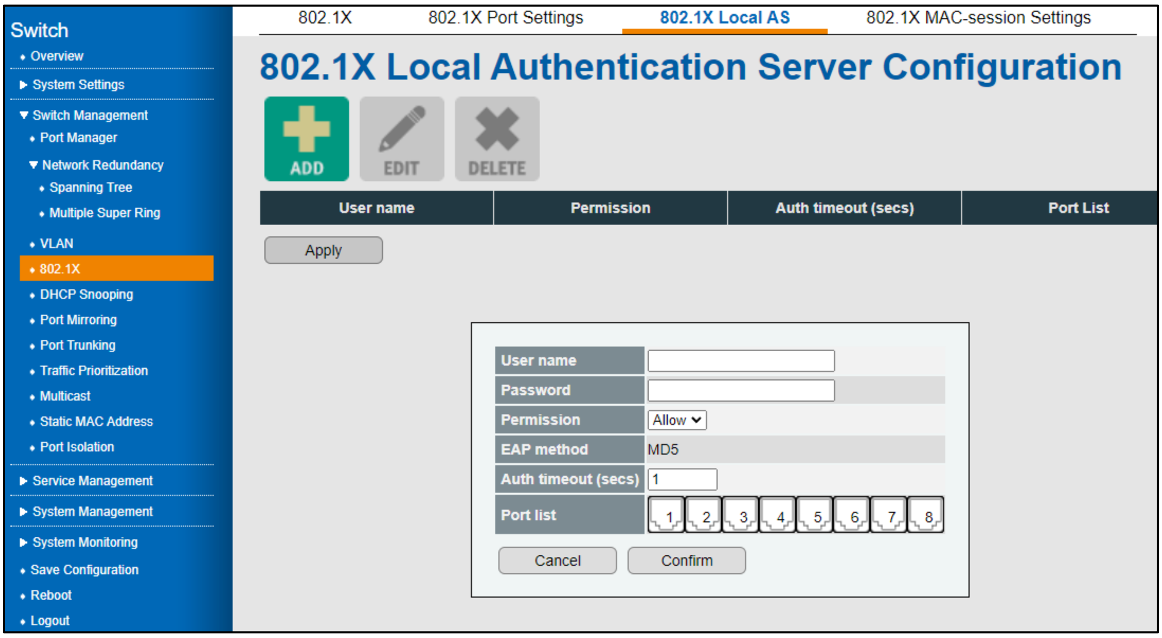
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **802.1X** > **802.1X Local AS**. The GUI screen displays the 802.1X Local AS settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



802.1X Local Authentication Server Configuration

User name	Permission	Auth timeout (secs)	Port List

User name	
Password	
Permission	Allow
EAP method	MD5
Auth timeout (secs)	1
Port list	1 2 3 4 5 6 7 8

Figure 17 Switch Management > 802.1X > 802.1X Local Authentication Server Configuration Menu

Item	Description
ADD	Click **ADD** to create a local authentication database entry.
EDIT	Click **EDIT** to modify a local authentication database entry.
DELETE	Click **EDIT** to delete a local authentication database entry.
User name	Specify the user name of the local server.
Permission	Specify the grant /denial of access for local authentication server: Allow: authentication request is allowed for the selected port(s). Deny: authentication request is denied for the selected port(s).
Auth timeout (secs)	Specify the duration of time for the inactivity timer.
Port List	Specify the port(s) attributed to the configuration.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.5.4.802.1X MAC-session Settings

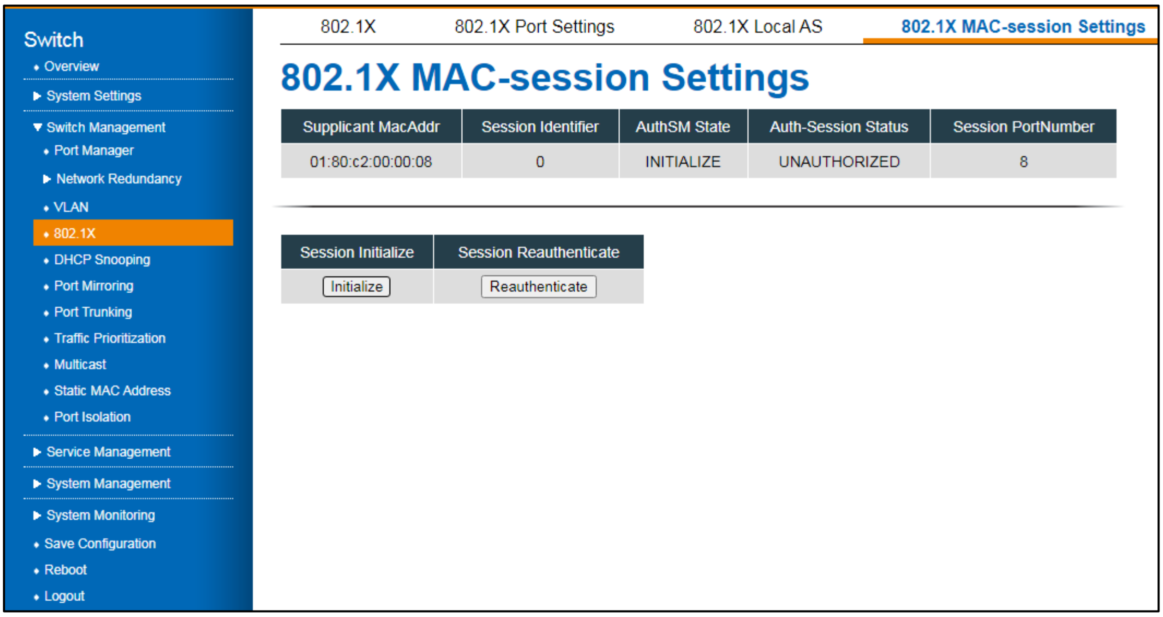
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **802.1X > 802.1X MAC-session Settings**. The GUI screen displays the 802.1X MAC-session Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



802.1X MAC-session Settings

Supplicant MacAddr	Session Identifier	AuthSM State	Auth-Session Status	Session PortNumber
01:80:c2:00:00:08	0	INITIALIZE	UNAUTHORIZED	8

Session Initialize	Session Reauthenticate
Initialize	Reauthenticate

Figure 18 Switch Management > 802.1X > 802.1X MAC-session Settings Menu

Item	Description
Supplicant MacAddr	Displays the supplicant’s MAC Address.
Session identifier	Displays the unique session identifier derived from the supplicant’s MAC address.

Item	Description
AuthSM state	Select the state of the Authenticator State Machine for the entry. The list contains: • Initialize -This state occurs when the module is disabled and down. • Disconnected – There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition. • Connecting – This state is the beginning of the PNAC packet exchange. • Authenticating – This state occurs whenever authenticator receives response ID from supplicant. • Authenticated - This state occurs whenever authenticator SM port transitions to authorized through EAP exchange. • Aborting – This state occurs when Authenticator SM receives re-authenticating event or EAP start or supplicant log off. • Held - This state occurs when authentication failure occurs due to wrong user name or password. • ForceAuth – This state occurs when the port control is changed to force authorized. • ForceUnauth - This state occurs when the port control is changed to force unauthorized.
Auth-session status	Displays the Authentication Session Status. • Authorized to transmit or receive data • Unauthorized to transmit or receive data
Session PortNumber	Displays the port number corresponding to the session of the learned MAC address.
Session initialize	Specify the Session Initialize status for the configured Supplicant MAC Address. The following values apply: • True (default)—the session initialization is set. • False—the session Initialization is reset.
Session reauthenticate	Specify the session reauthentication status for the configured supplicant MAC address. The following values apply: • True (default)—the session re-authentication is initialized. • False—the session re-authentication is reset.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.6. DHCP Snooping

DHCP snooping provides security mechanisms for preventing false DHCP response packets and logging DHCP addresses. Ports on the device are classified as trusted or untrusted, depending on their trustworthiness.

Ports that are trusted can be assigned DHCP addresses by DHCP servers. The switch allows DHCP messages received on trusted ports to pass through.

Untrusted ports are those that cannot assign DHCP addresses. The default setting for all ports is untrusted until they are declared trusted.

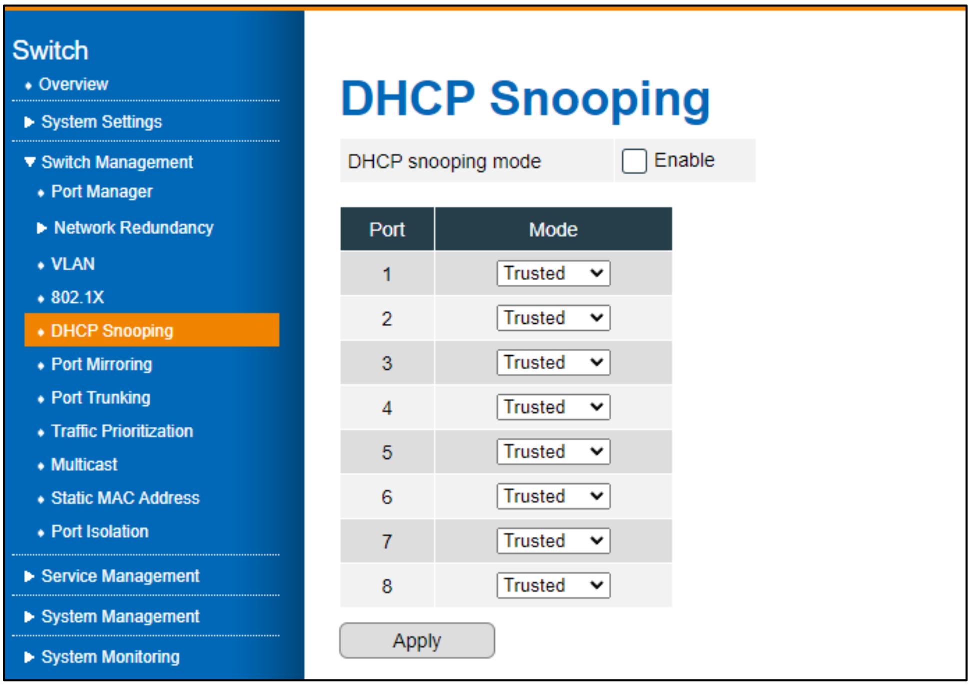
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **DHCP Snooping**. The GUI screen displays the DHCP Snooping settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



DHCP Snooping

DHCP snooping mode ☐ Enable

Port	Mode
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

Figure 19 Switch Management > DHCP Snooping

Item	Description
DHCP snooping mode	Specify to enable or disable (default) the snooping mode.
Port	Displays the port identifier.

Item	Description
Mode	Specify the mode of the interface. Trusted: allow interfaces to forward DHCP offered packets, rogue packets are blocked. Untrusted: block interface to forward DHCP offered packets.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.7. Port Mirroring

A port mirroring tool allows you to mirror traffic between two ports without disrupting traffic flowing between the original ports.

Whenever traffic enters or exits the Source Port(s), it will be duplicated at the Destination Port. A monitoring device or application can then be used to analyze this traffic at the destination port. This tool is typically used by network administrators for diagnostics, debugging, and attack prevention.

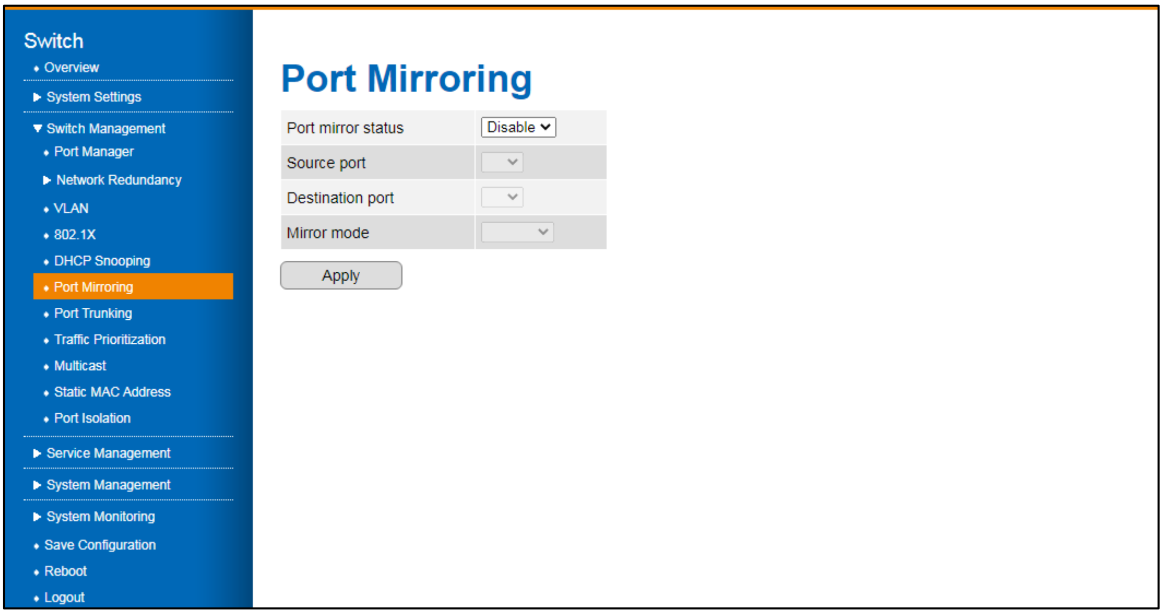
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Port Mirroring**. The GUI screen displays the Port Mirroring settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Port Mirroring

Port mirror status	Disable
Source port	
Destination port	
Mirror mode	

Figure 20 Switch Management > Port Mirroring Menu

Item	Description
Port mirror status	Specify to enable or disable (default) port mirroring.
Source port	Specify the port to monitor. All traffic of the source is copied to destination ports.
Destination port	Specify the analysis port to evaluate the traffic without affecting the traffic flow. Only a single mirror mode of the destination port can be selected.
Mirror mode	Specify the mirror mode: Ingress: Only Rx frames transmitted on this port are mirrored. Egress: Only Tx frames transmitted on this port are mirrored. Both: Ingress and egress frames transmitted on this port are mirrored.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.8. Port Trunking

Using Port Trunking, you can group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as one physical port, increasing bandwidth compared to just one Ethernet port. Member ports of the same trunk group can balance their loading and backup. For backbone networks, port trunking is usually used when higher bandwidth is required. Using this method, you can transfer more data at a lower cost.

Most implementations now conform to IEEE standard 802.3ad, Link Aggregation Group (LAG) or Link Aggregation Control Protocol (LACP).

The aggregated ports can interconnect with other switches that also support Port Trunking. Beijer supports two types of port trunking. Static trunking and 802.3ad trunking. You should assign 802.3ad LACP to the trunk when the other end uses 802.3ad LACP. Static trunking can be used when the other end uses non-802.3ad.

3.4.8.1.Port Trunking Basic Settings

A load balancing mode can be set according to a traffic model. If a field of traffic changes frequently, you can set a load balancing mode based on this field so that the traffic is equally load balanced. If the IP addresses in packets change frequently, use a load balancing mode that takes into account the destination IP address, the source IP address, or both. Use load balancing mode based on the source MAC address, destination MAC address, or both MAC addresses if MAC addresses in packets change frequently.

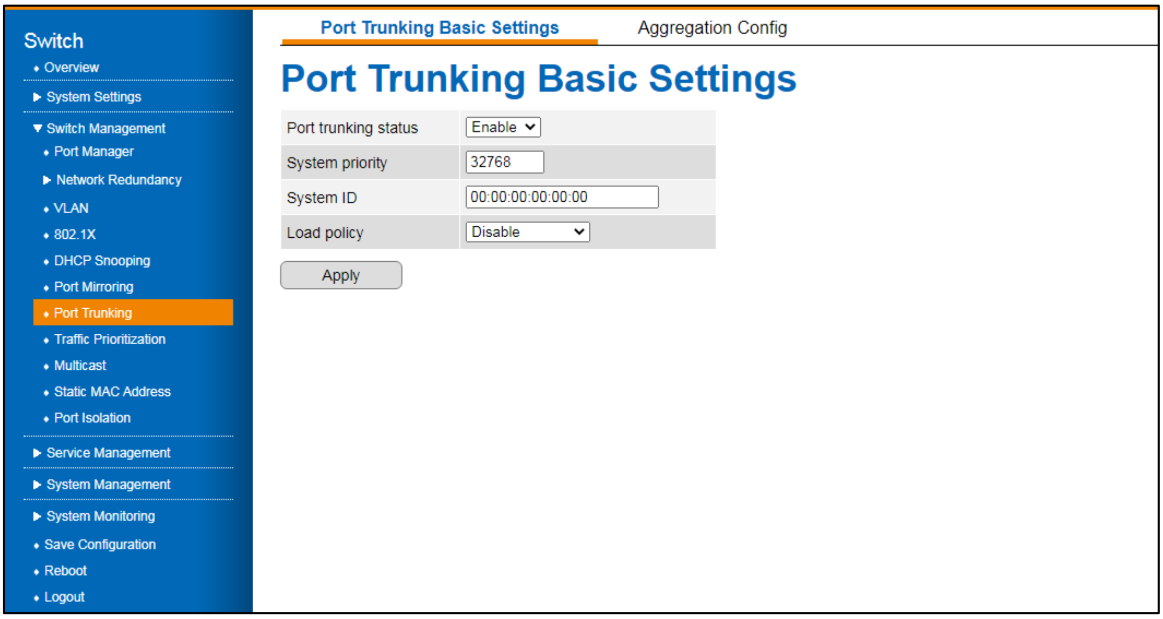
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Port Trunking > Port Trunking Basic Settings**. The GUI screen displays the Port Trunking Basic Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Port Trunking Basic Settings

Port trunking status	Enable
System priority	32768
System ID	00:00:00:00:00:00
Load policy	Disable

Figure 21 Switch Management > Port Trunking > Port Trunking Basic Settings Menu

Item	Description
Port trunking status	Specify to enable or disable (default) port trunking.
System priority	Specify a number between 0 and 32768 that indicates the device's priority. The lower the number, the higher the priority.
System ID	Specify the MAC address of the
Load policy	Specify load balancing for specific network requirements, settings: • Disable (default) • MAC SRC - source MAC address • MAC Dst - destination MAC address • MAC Src & Dst - source and destination MAC addresses • IP Src - source IP address • IP Dst - destination IP address • IP Src & Dst - source and destination IP addresses
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.8.2. Aggregation Config

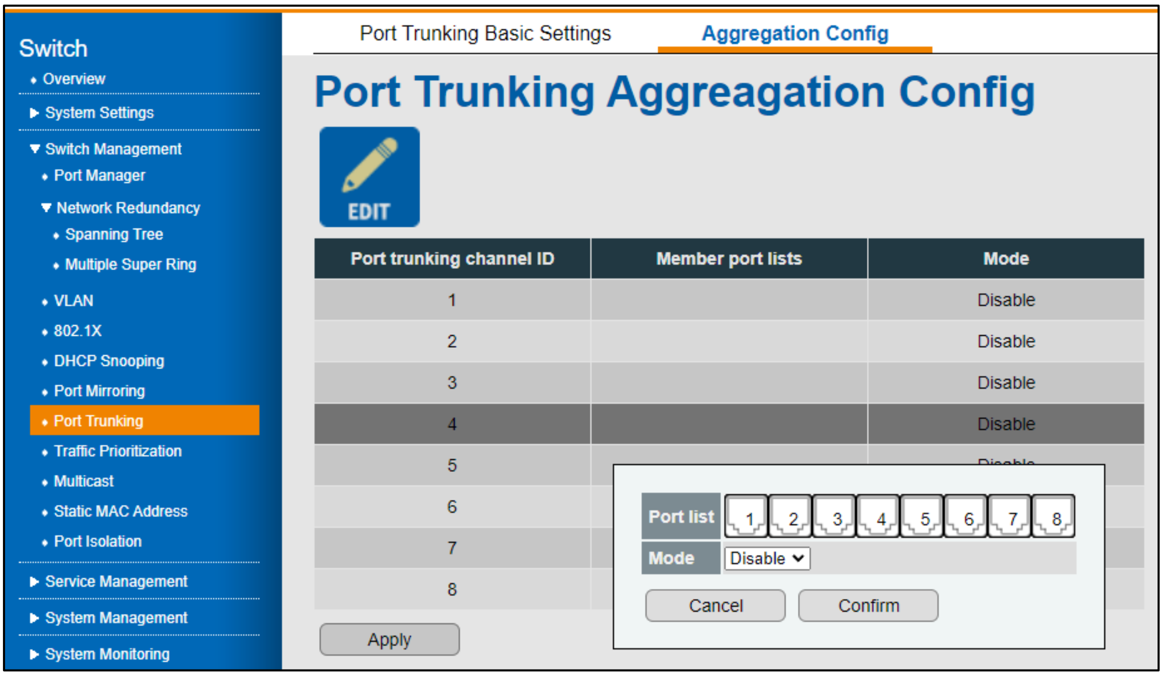
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Port Trunking** > **Aggregation Cofig**. The GUI screen displays the Port Trunking Aggregation Config menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Port Trunking Aggreagation Config

Port trunking channel ID	Member port lists	Mode
1		Disable
2		Disable
3		Disable
4		Disable
5		Disable
6		
7		
8		

Port list: 1 2 3 4 5 6 7 8

Mode: Disable

Figure 22 Switch Management > Port Trunking > Aggregation Config Menu

Item	Description
EDIT	Click **EDIT** to modify an existing configuration. The configuration window displays. • Port list: specify the port(s) to associate to the port trunking configuration. • Mode: Specify the trunk type for the configuration, the following are available: Manual, LACP, or Disable (default).
Port trunking channel ID	Displays the channel ID of the listed entry.
Member port lists	Displays the associated port of the entry.
Mode	Displays the status mode (Disabled/enabled) of the entry.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.9. Traffic Prioritization

By prioritizing traffic, Quality of Service (QoS) allows users to give certain flows better service. Traffic Prioritization can also alleviate congestion problems and make sure that high-priority traffic is delivered first. Each port can be configured differently regarding Traffic Prioritization settings in this section.
With JetNetQOS, 4 physical queues, weighted fair queueing (WRR), and Strict Priority, which follows 802.1p COS and IPv4 TOS/DiffServ information to prioritize your industrial network traffic, are available.

3.4.9.1.QoS Settings

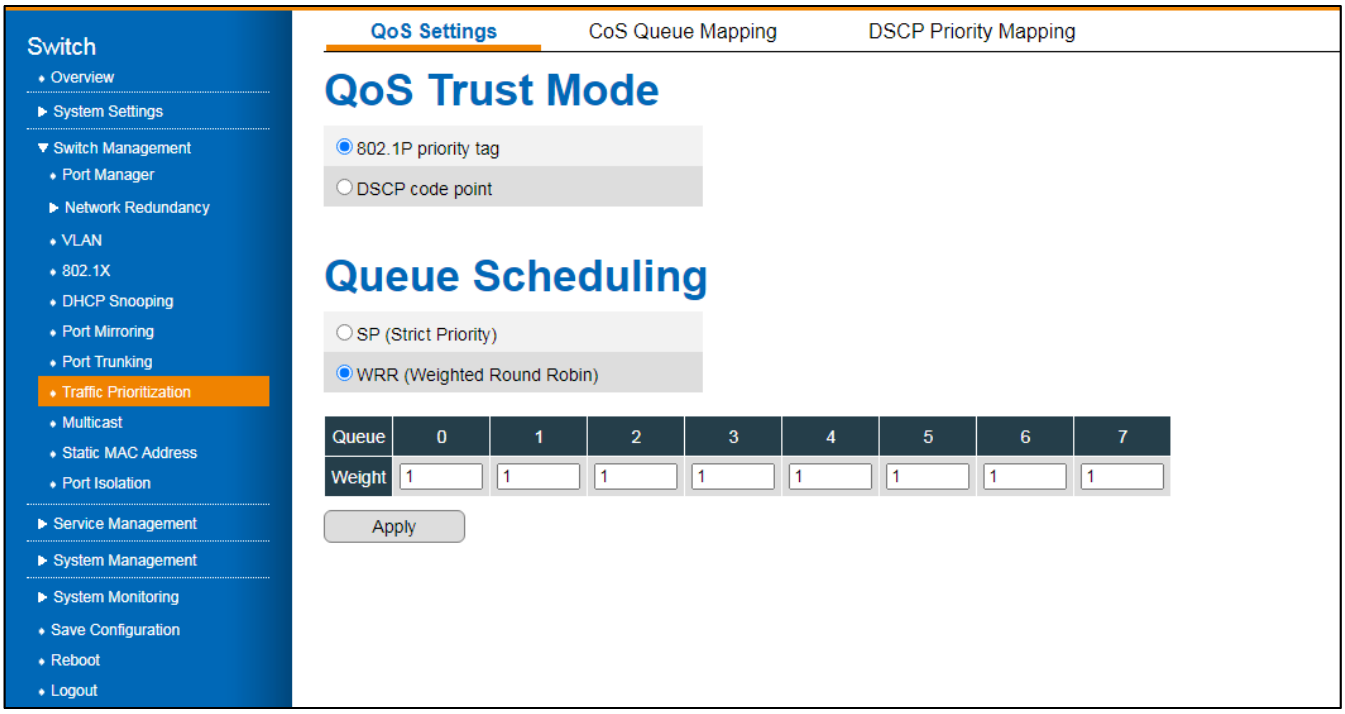
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Traffic Prioritization**. The GUI screen displays the QoS Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



QoS Trust Mode

● 802.1P priority tag
○ DSCP code point

Queue Scheduling

○ SP (Strict Priority)
● WRR (Weighted Round Robin)

Queue	0	1	2	3	4	5	6	7
Weight	1	1	1	1	1	1	1	1

Figure 23 Switch Management > Traffic Prioritization > QoS Settings Menu

Item	Description
QoS Trust Mode	
802.1P priority tag	Specify to use Class of Service (CoS / 802.1p), users can define priority for packets of data when traffic is buffered in a switch due to congestion.
DSCP code point	Specify to use DSCP (IP Differentiated Services Code Point) is a system for detecting packets based on their DSCP values.
Queue scheduling	
SP (Strict Priority)	Specify Queue Scheduling to use SP. The following are available: Packets with higher priority in the queue will always be processed first.
WRR (Weighted Round Robin)	Specify Queue Scheduling to use WRR to allow users to assign new weight ratio for each class. 10 is the highest ratio. The ratio for each class is as follows: Wx / W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7 (Total volume of Queue 0-7)
Queue	Displays the queue identifier.
Weight	Specify the weight ratio of the selection, range: 0 – 10.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.9.2.CoS Queue Mapping

The purpose of this page is to change CoS values in the Physical Queue mapping table. The JetNet switch fabric supports only seven physical queues: lowest, low, middle, and highest. The CoS value should be mapped to the physical queue level by users.

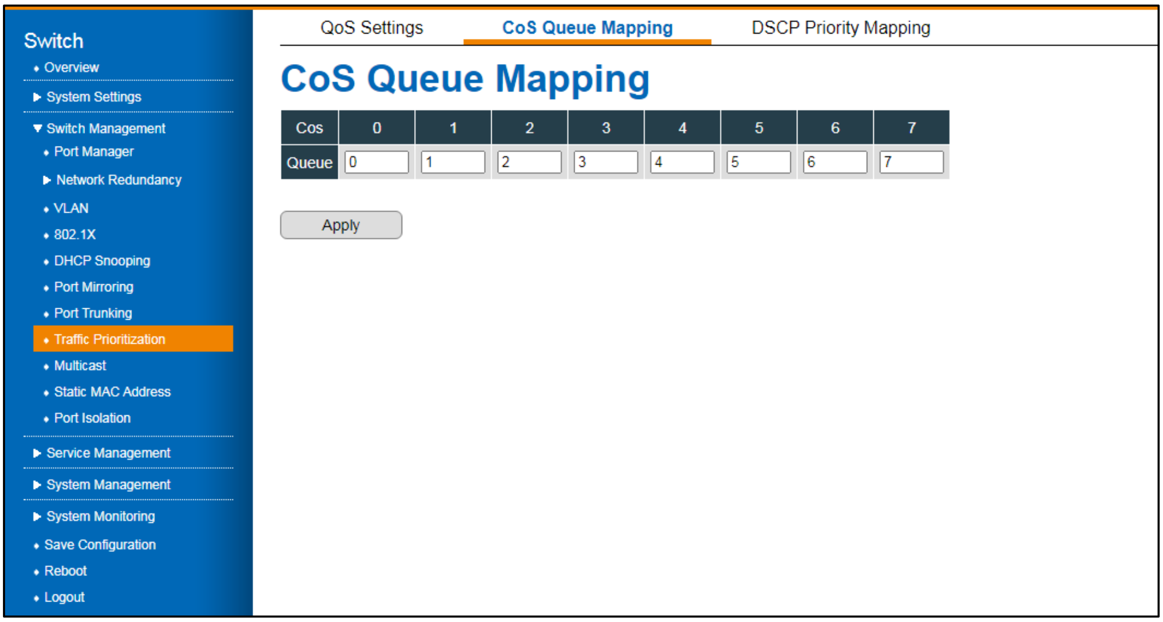
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Traffic Prioritization** > **CoS Queue Mapping**. The GUI screen displays the CoS Queue Mapping menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



CoS Queue Mapping

Cos	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

Figure 24 Switch Management > Traffic Prioritization > CoS Queue Mapping Menu

Item	Description
CoS	Displays the CoS value of the queue listing.
Queue	Displays the queue ranking of the queue listing.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.9.3. DSCP Priority Mapping

The DSC Priority Mapping table is configured through this menu. JetNet only supports 8 physical queues on its switch fabric. As a result, users should determine how to map DSCP values to physical queue levels. JetNet allows users to change the mapping table according to DSCP settings on upper layer 3 switches.

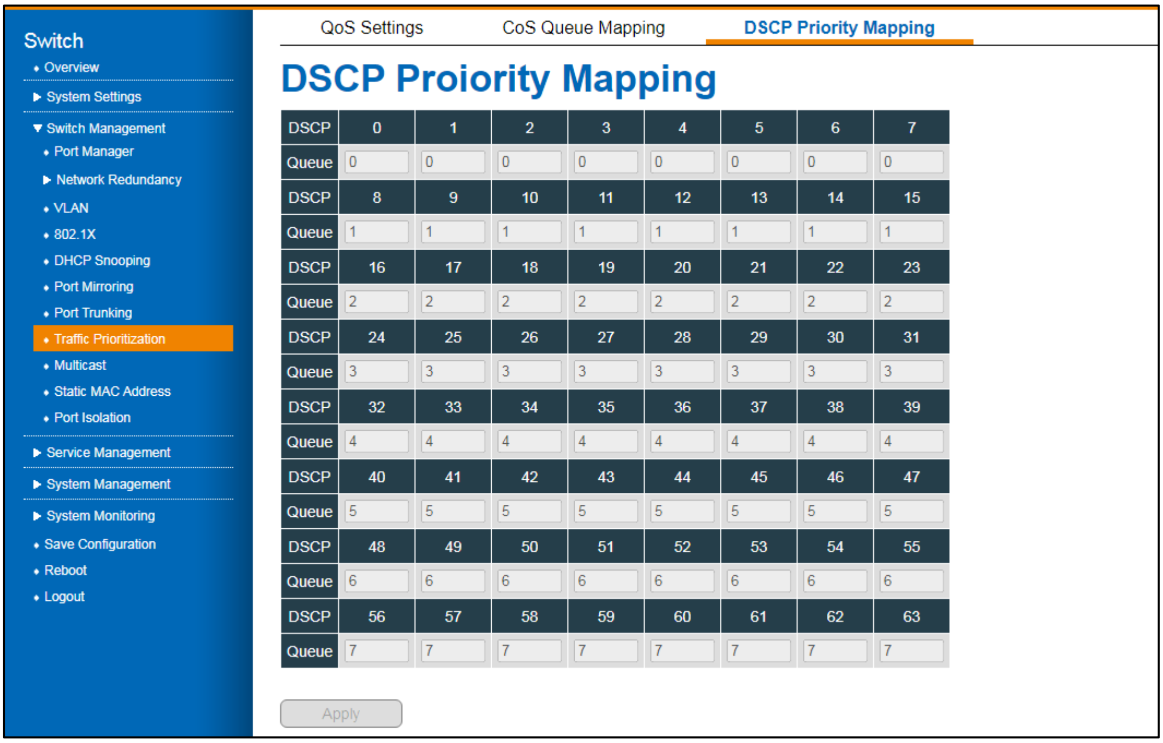
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Traffic Prioritization** > **DSCP Priority Mapping**. The GUI screen displays the DSCP Priority Mapping menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



DSCP Proiority Mapping

DSCP	0	1	2	3	4	5	6	7
Queue	0	0	0	0	0	0	0	0
DSCP	8	9	10	11	12	13	14	15
Queue	1	1	1	1	1	1	1	1
DSCP	16	17	18	19	20	21	22	23
Queue	2	2	2	2	2	2	2	2
DSCP	24	25	26	27	28	29	30	31
Queue	3	3	3	3	3	3	3	3
DSCP	32	33	34	35	36	37	38	39
Queue	4	4	4	4	4	4	4	4
DSCP	40	41	42	43	44	45	46	47
Queue	5	5	5	5	5	5	5	5
DSCP	48	49	50	51	52	53	54	55
Queue	6	6	6	6	6	6	6	6
DSCP	56	57	58	59	60	61	62	63
Queue	7	7	7	7	7	7	7	7

Figure 25 Switch Management > Traffic Prioritization > DSCP Priority Mapping Menu

Item	**Description**
DSCP	Displays the queue value for the listing.
Queue	Specify the DSCP value.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.10. Multicast

JetNet series use IGMP Snooping technology for multicast filtering.
Group Management Protocol is an Internet protocol that allows an Internet device to report its membership in a multicast group to adjacent routers. Through multicasting, data can be sent to users who identify themselves as interested in receiving it.
By setting up multicast group memberships, you can update the address books of mobile computer users in the field. You can also send out newsletters to a distribution list, or broadcast streaming media to viewers who tune into the event.
IGMP Snooping makes use of switches and hosts that support IGMP to manage multicast traffic. IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. As shown below, IGMP has three basic types of messages:

3.4.10.1. Mode Selection

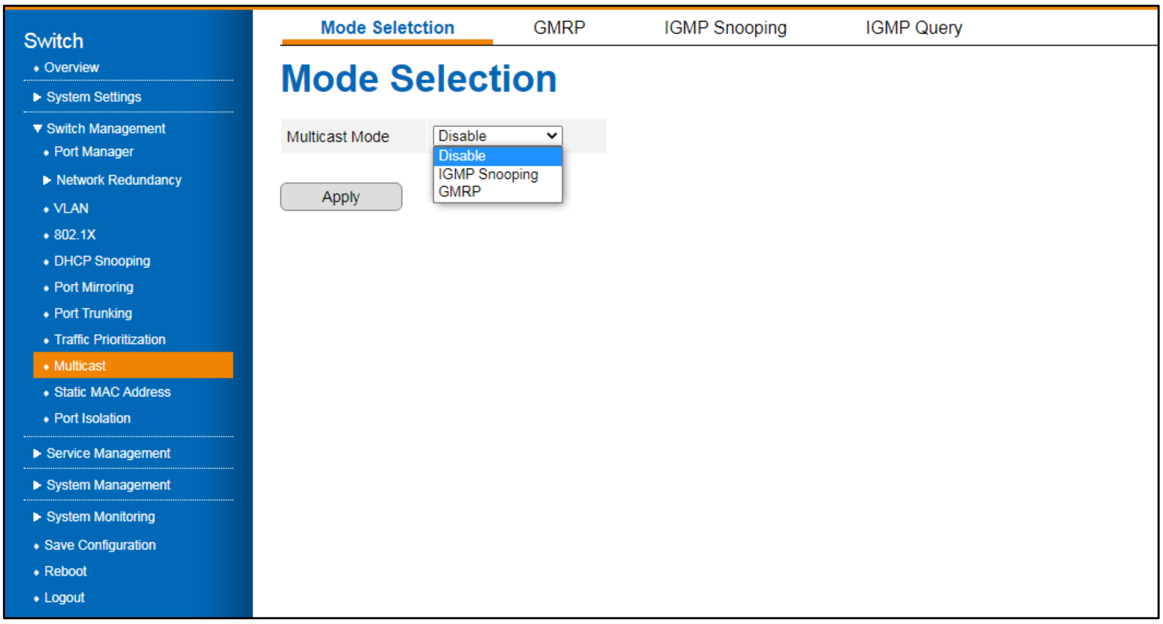
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Multicast**. The GUI screen displays the Mode Selection menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Multicast Mode: Disable

Figure 26 Switch Management > Multicast > Mode Selection Menu

Item	Description
Multicast mode	Specify the multicast selection mode. Settings include: Disable (default): mode is disabled. IGMP Snooping: client reports along with corresponding multicast IDs from the IGMP reports are sent to the infrastructure switch. GMRP: provides a constrained multicast flooding facility.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.10.2. GMRP

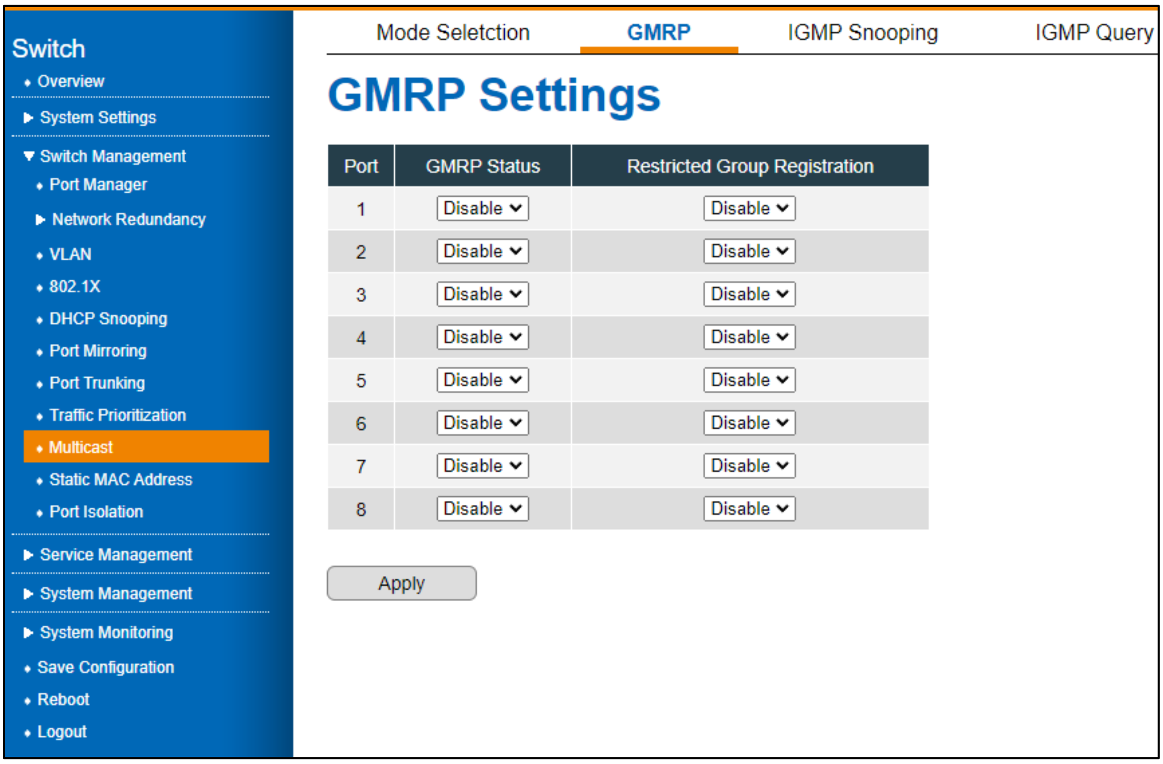
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Multicast** > **GMRP**. The GUI screen displays the GRMRP Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



GMRP Settings

Port	GMRP Status	Restricted Group Registration
1	Disable	Disable
2	Disable	Disable
3	Disable	Disable
4	Disable	Disable
5	Disable	Disable
6	Disable	Disable
7	Disable	Disable
8	Disable	Disable

Figure 27 Switch Management > Multicast > GMRP Menu

Item	Description
Port	Displays the port ID of the interface.
GMRP status	Specify enable or disable (default) the status of the protocol.
Restricted group Registration	Specify enable or disable the restriction of group registration. By default, port-level restricted group registration is disabled. When this feature is enabled, the multicast group attribute is learned dynamically on the port.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.10.3. IGMP Snooping

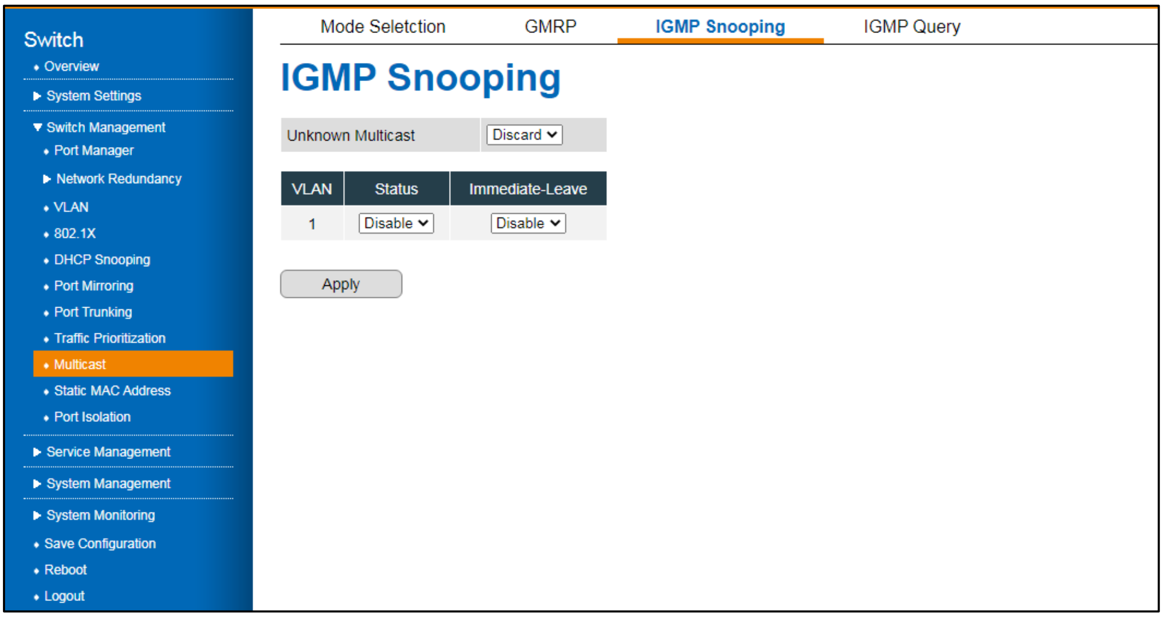
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Multicast** > **IGMP Snooping**. The GUI screen displays the IGMP Snooping menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



IGMP Snooping

Unknown Multicast: Discard

VLAN	Status	Immediate-Leave
1	Disable	Disable

Figure 28 Switch Management > Multicast > IGMP Snooping Menu

Item	Description
Unknown Multicast	Specify enable or disable (default) the forwarding feature of unknown multicast data to the router port. By default the function is disabled and the multicast data is dropped.

Item	Description
VLAN	Displays the current VLAN ID.
Status	Specify the operation status of the function.
Immediate-Leave	Specify enable or disable (default) the immediate leave function. If enabled, the device removes IGMP group-specific queries out of the interface immediately without waiting for a response.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.10.4. IGMP Query

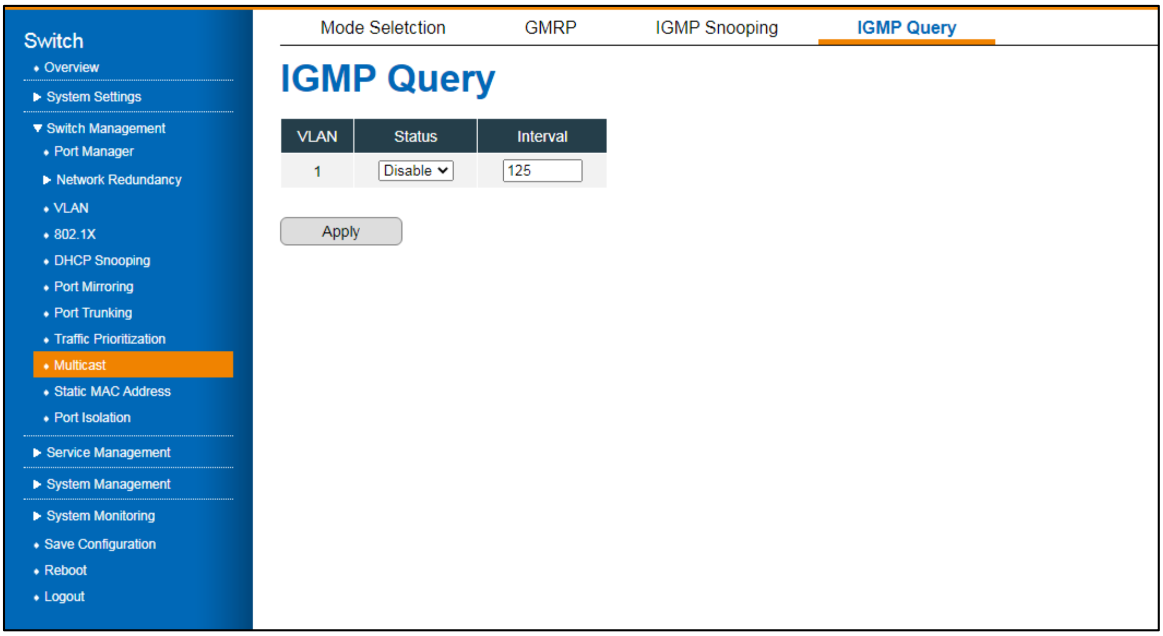
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Multicast** > **IGMP Query**. The GUI screen displays the IGMP Query menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



IGMP Query

VLAN	Status	Interval
1	Disable	125

Figure 29 Switch Management > Multicast > IGMP Query Menu

Item	Description
VLAN	Displays the current VLAN ID.
Status	Specify enable or disable (default) the function. If enabled, the device periodically sends query messages to obtain group membership information.

Item	Description
Interval	Specify the interval time in seconds to calculate the group membership timeout.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.11. Static MAC Address

An address table is maintained by the switch so that frames can be switched efficiently between LAN ports. The switch associates the MAC address of the sending network device with the LAN port on which it received the frame when it obtains it. MAC source addresses of the frames received are used by the switch in dynamically building the address table. A frame received for a MAC destination address not listed in the switch's address table is flooded to all LAN ports except the one that received it. When the destination station replies, the switch adds its relevant MAC source address and port ID to the address table. In subsequent frames, the switch forwards them to a single LAN port without flooding them all.

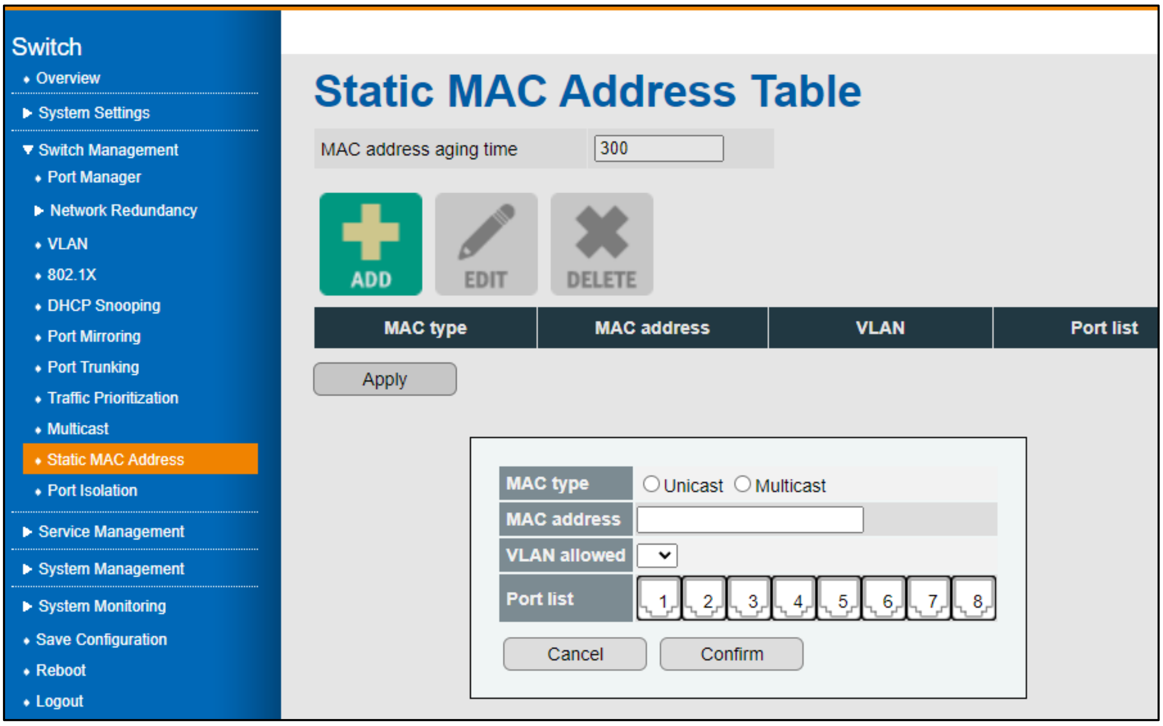
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Static MAC Address**. The GUI screen displays the Static MAC Address Table menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Static MAC Address Table

MAC address aging time: 300

MAC type	MAC address	VLAN	Port list

MAC type: ○ Unicast ○ Multicast

MAC address:

VLAN allowed:

Port list: 1 2 3 4 5 6 7 8

Figure 30 Switch Management > Static MAC Address Menu

Item	Description
MAC address aging time	Specify the timer for unused MAC address entries. Default is 30 seconds.
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **EDIT** to delete an existing configuration.
MAC Type	Specify the packet type, Unicast or Multicast: Unicast: MAC address obtained dynamically by the switch fabric. Multicast: Manual entry, can be deleted through UI.
MAC Address	Specify the interface MAC address
VLAN	Specify the number of allowed VLAN to correspond to the entry.
Port list	Specify the corresponding port.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.4.12. Port Isolation

Switch ports that are members of a protected group can be configured to prevent communication between protected ports within the group. Protected port groups can only be applied if the switch is configured as a standard VLAN switch. A protected port group falls under the Port Isolation category. Isolated (Protected) ports — These ports can only forward traffic to promiscuous ports inside the private VLAN. These ports can receive traffic only from promiscuous ports inside the private VLAN. To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Switch Management** > **Port Isolation**. The GUI screen displays the Port Isolation Setting menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.

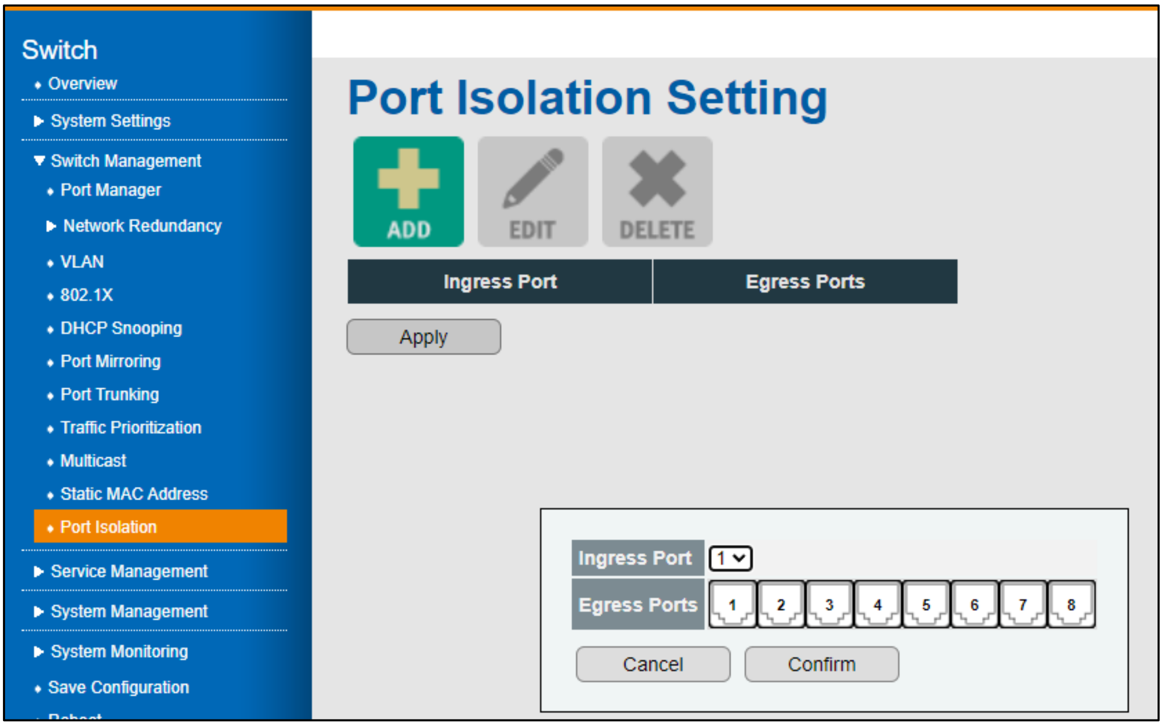


Figure 31 Switch Management > Port Isolation Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **EDIT** to delete an existing configuration.

Item	Description
Ingress port	Specify the port permitted to route ingress traffic.
Egress ports	Specify the port(s) permitted to route egress traffic.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.5. Service Management

3.5.1. DHCP

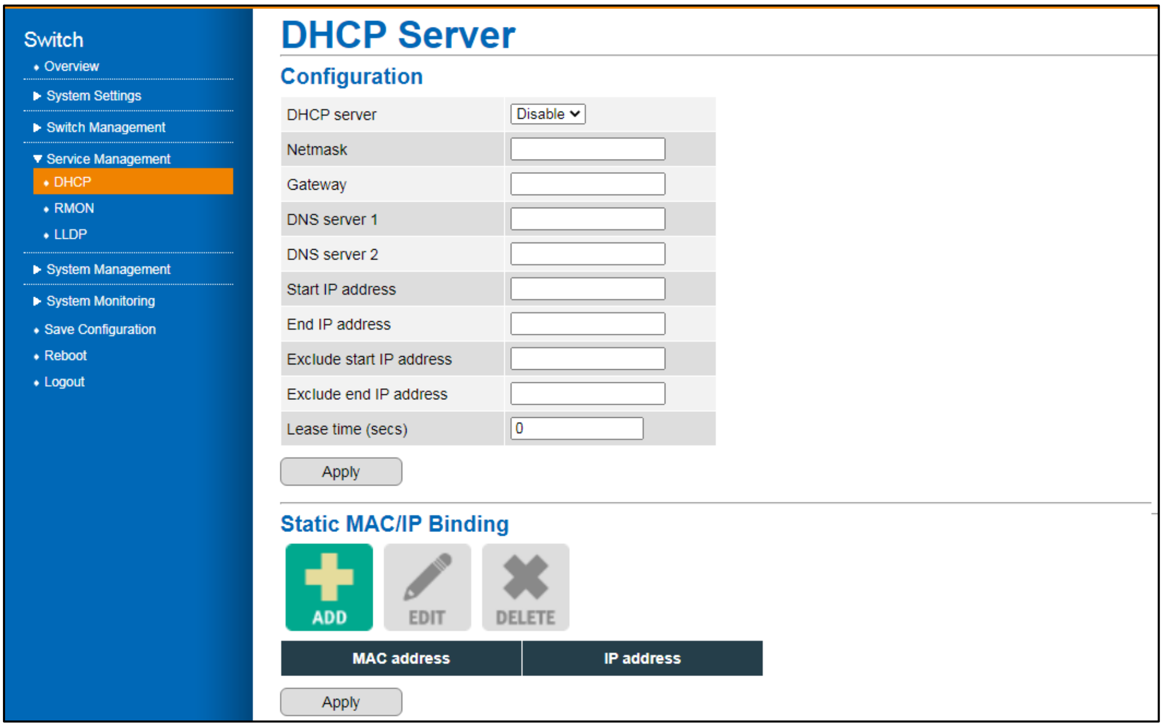
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Service Management** > **DHCP**. The GUI screen displays the DHCP Server menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



DHCP Server

Configuration

DHCP server	Disable
Netmask	
Gateway	
DNS server 1	
DNS server 2	
Start IP address	
End IP address	
Exclude start IP address	
Exclude end IP address	
Lease time (secs)	0

Static MAC/IP Binding

MAC address	IP address

Figure 32 Service Management > DHCP Menu

Item	Description
DHCP server	Specify enable or disable the DHCP client function.

Item	Description
Netmask	Specify the netmask address for the DHCP configuration when the function is enabled. Default is 255.255.255.0.
Gateway	Specify the gateway address for the DHCP configuration when the function is enabled. Default is 192.168.10.254.
DNS server 1	Specify the DNS server 1 address for the DHCP configuration when the function is enabled. Default is 0.0.0.0.
DNS server 2	Specify the DNS server 1 address for the DHCP configuration when the function is enabled. Default is 0.0.0.0.
Start IP address	Specify the starting IP address of the DHCP pool.
End IP address	Specify the ending IP address of the DHCP pool.
Exclude start IP address	Specify the starting IP address of the pool to exclude from being assigned to DHCP clients.
Exclude end IP address	Specify the ending IP address of the pool to exclude from being assigned to DHCP clients.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.
Static MAC/IP Binding	
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **EDIT** to delete an existing configuration.
MAC address	Specify the MAC address to statically bind the following IP address in the DHCP address pool.
IP address	Specify the IP address to statically bind to the define MAC address (previous menu) in the DHCP address pool.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.5.2. RMON

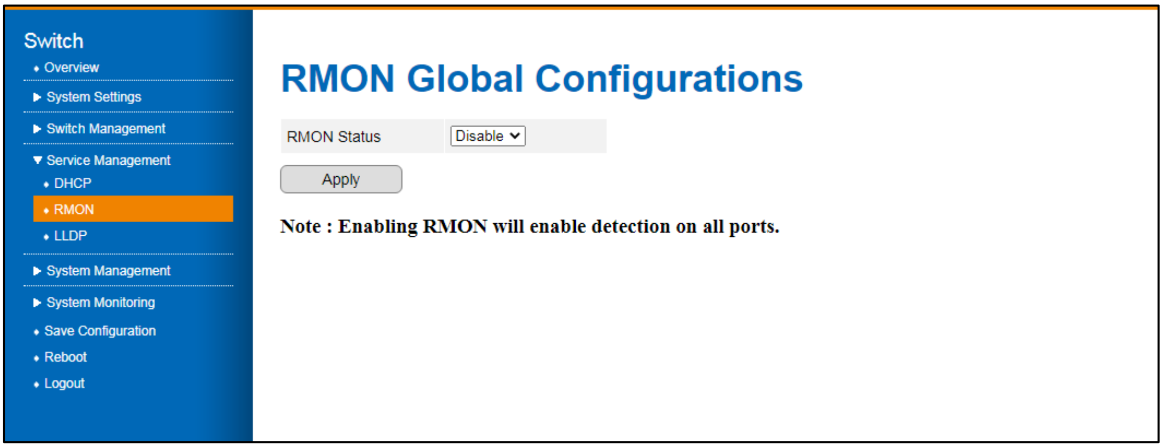
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Service Management** > **RMON**. The GUI screen displays the RMON Global Configurations menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



RMON Global Configurations

RMON Status: Disable

Apply

Note : Enabling RMON will enable detection on all ports.

Figure 33 Service Management > RMON Menu

Item	Description
RMON status	Specify enable or disable (default) for the RMON function. By enabling the function, remote monitoring of network traffic of all ports within the network.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.5.3. LLDP

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) allows network devices to advertise their identity and capabilities on a LAN. The JetNet series support LLDP PDU transmissions that are sent periodically as part of a simple one-way neighbor discovery protocol.

- LLDP frames are constrained to a local link.
- LLDP frames are TLV (Type-Length-Value) form.

3.5.3.1. Global Settings

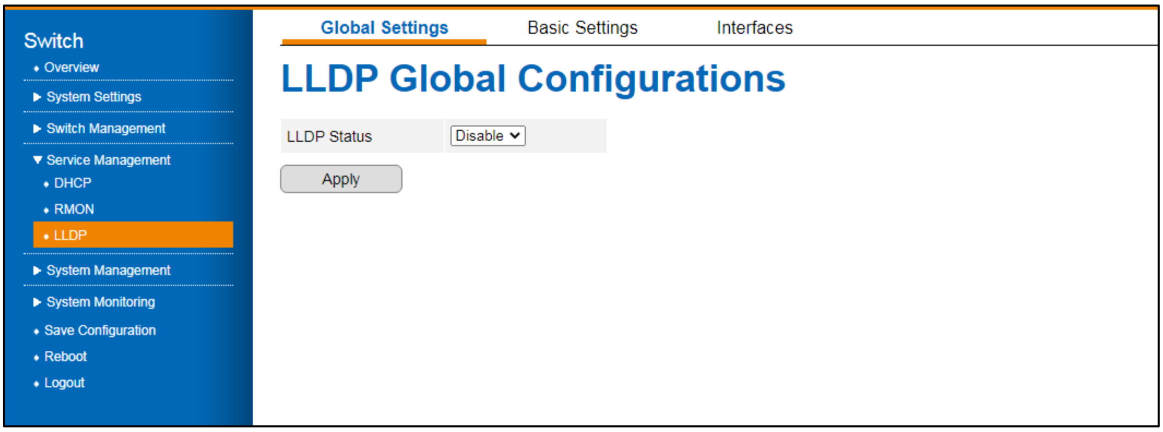
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Service Management** > **LLDP**. The GUI screen displays the LLDP Global Configurations menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



LLDP Global Configurations

LLDP Status: Disable

Figure 34 Service Management > LLDP > Global Settings Menu

Item	Description
LLDP status	Specify enable or disable (default) for the LLDP function.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.5.3.2. Basic Settings

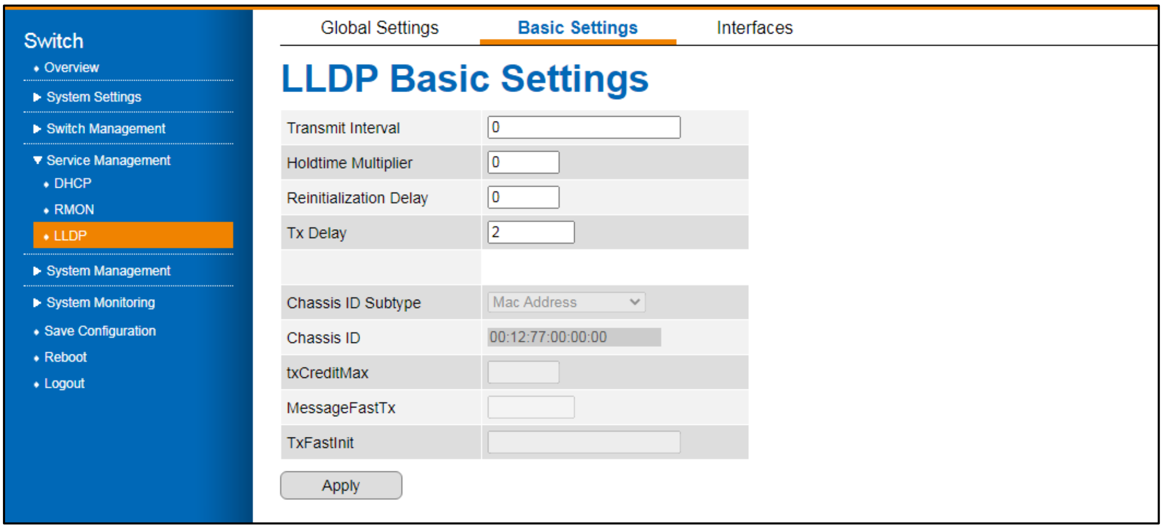
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Service Management** > **LLDP** > **Basic Settings**. The GUI screen displays the LLDP Basic Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



LLDP Basic Settings

Transmit Interval	0
Holdtime Multiplier	0
Reinitialization Delay	0
Tx Delay	2
Chassis ID Subtype	Mac Address
Chassis ID	00:12:77:00:00:00
txCreditMax	
MessageFastTx	
TxFastInit	

Figure 35 Service Management > LLDP > Basic Settings Menu

Item	Description
Transmit interval	Specify the transmit interval, range: 5 to 32768 seconds. Default: 30 seconds. LLDP frames are periodically transmitted by the switch so that the neighbor's network discovery information is current.
Holdtime multiplier	Specify the hold time interval. The interval designates the time in which an LLDP frame is considered valid.
Reinitialization delay	Specify the re-initialization delay interval. When LLDP is disabled, a port is disabled, or a switch is rebooted, a LLDP shutdown frame is transmitted, indicating that the LLDP information is no longer valid. In LLDP, delay defines the interval between a shutdown frame and a new initialization. The range of valid values is 1to 10 seconds.
Tx Delay	Specify the TX delay interval. Any configuration change (for instance, changing the IP address) triggers LLDP frames, but the time between them will always be at least the value of Transmit Delay seconds. The transmit delay cannot exceed 1/4 of the transmission interval. The valid range is 1 to 8192 seconds.
Chassis ID subtype	Displays the current chassis ID subtype.
Chassis ID	Displays the current chassis ID.
txCreditMax	Specify the number of maximum number of consecutive LLDPDUs that can be transmitted at any time. Range: 1 to 10. Default is 5.
MessageFastTx	Specify the interval at which LLDP frames are transmitted on behalf of the LLDP agent during fast transmission periods. Range: 1 to 3600. Default is 1/
TxFastInit	Specify the number of LLDPDUs that can be transmitted during a fast transmission period. Range: 1 to 8. Default is 8.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.5.3.3. Interfaces

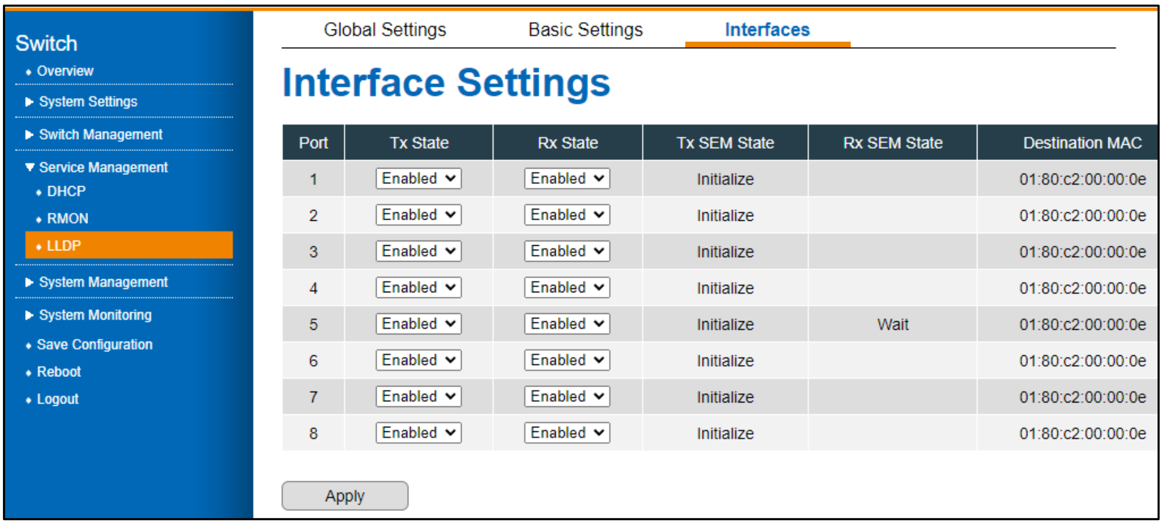
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **Service Management** > **LLDP** > **Interfaces**. The GUI screen displays the Interface Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Interface Settings

Port	Tx State	Rx State	Tx SEM State	Rx SEM State	Destination MAC
1	Enabled	Enabled	Initialize		01:80:c2:00:00:0e
2	Enabled	Enabled	Initialize		01:80:c2:00:00:0e
3	Enabled	Enabled	Initialize		01:80:c2:00:00:0e
4	Enabled	Enabled	Initialize		01:80:c2:00:00:0e
5	Enabled	Enabled	Initialize	Wait	01:80:c2:00:00:0e
6	Enabled	Enabled	Initialize		01:80:c2:00:00:0e
7	Enabled	Enabled	Initialize		01:80:c2:00:00:0e
8	Enabled	Enabled	Initialize		01:80:c2:00:00:0e

Figure 36 Service Management > LLDP > Interfaces Settings Menu

Item	Description
Port	Displays the interface ID.
Tx state	Specify enable (default) or disable the TX state. If enabled, a periodic state machine is driven through the message transmitted via the port.
Rx state	Specify enable (default) or disable the RX state. If enabled, a periodic state machine is driven through the message received via the port.
Tx SEM state	Tx SEM State - Displays current status of the TX state event machine.
Rx SEM state	Rx SEM State - Displays current status of the RX state event machine.
Destination MAC	Specify the destination MAC to receive the configured packets.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6. System Management

3.6.1. Access Control List

Access Control Lists (ACL), otherwise known as Filter Sets, include two major types of filters. One is MAC ACL filter, also known as Port Security. It allows users to define access rules based on MAC address flexibility. One other type is IP Standard ACL.
A list table of access control entries (ACEs) indicates which users or groups are permitted or denied access to a specific traffic object, such as a process or a program, using ACEs. An ACL identifies each accessible traffic object. Access rights to specific traffic objects are determined by privileges.

3.6.1.1.MAC ACL

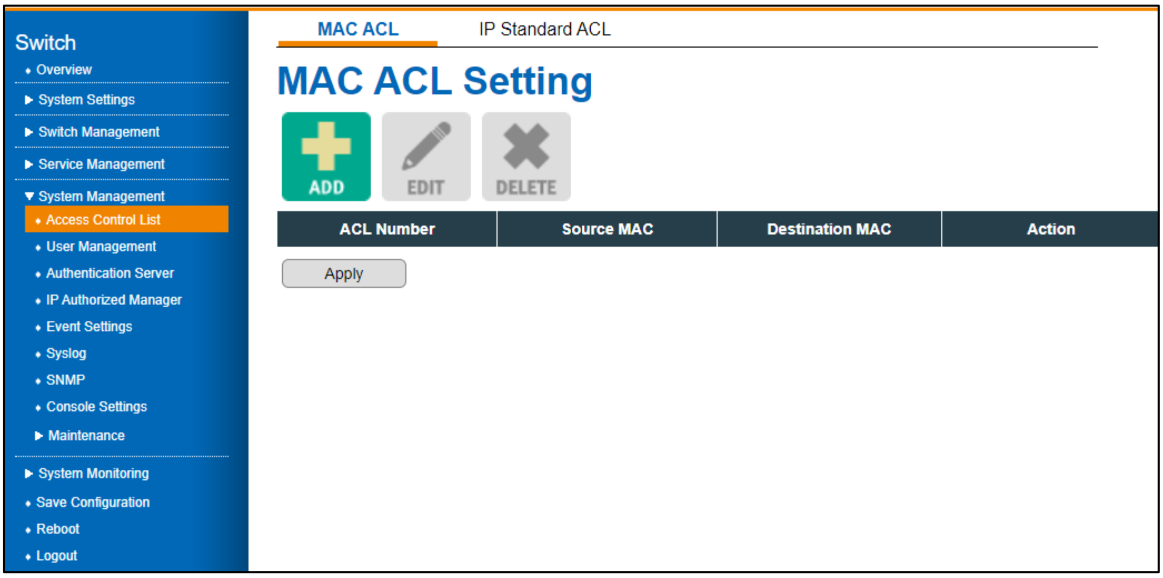
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Access Control List.** The GUI screen displays the MAC ACL Setting menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



ACL Number	Source MAC	Destination MAC	Action

Figure 36 System Management > Access Control List > MAC ACL Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **DELETE** to delete an existing configuration.
ACL Number	Specify the number to identify the entry.
Source MAC	Specify the source MAC filter for the ACE entry.
Destination MAC	Specify the destination MAC filter for the ACE entry.
Action	Specify the forwarding action of the ACE: • Permit (default): Frames matching ACE can be forwarded and learned. • Deny: Frames matching ACE are dropped.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.1.2.IP Standard ACL

In standard ACLs, traffic is controlled by comparing the source address of IP packets against the defined addresses.

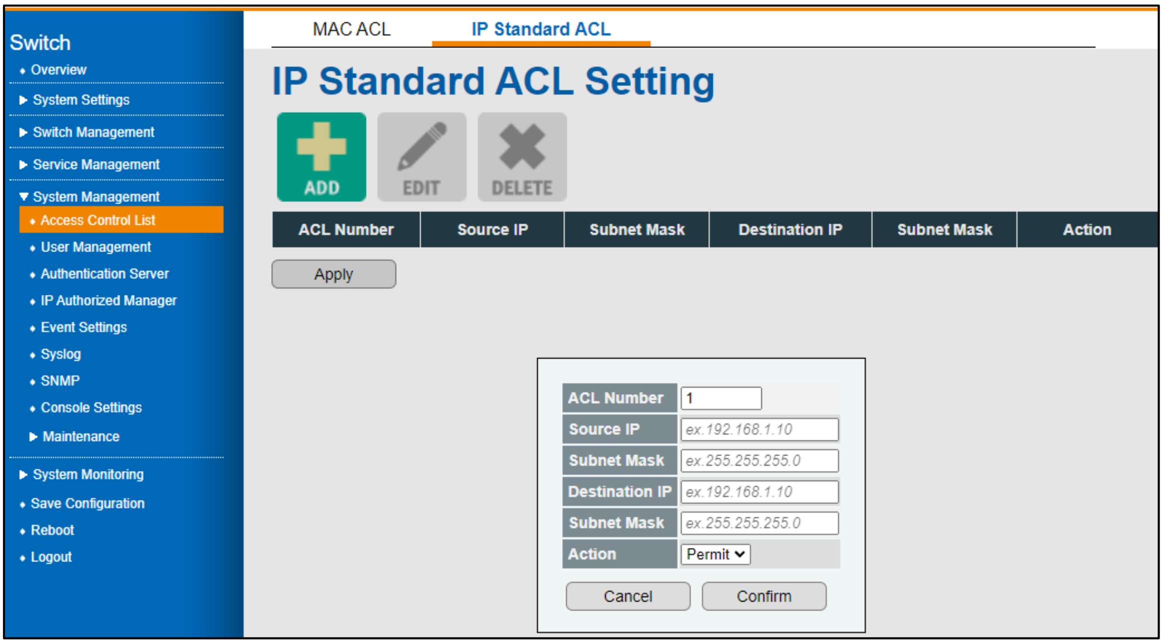
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Access Control List** > **IP Standard ACL**. The GUI screen displays the Interface Standard ACL Setting menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



IP Standard ACL Setting

ACL Number	Source IP	Subnet Mask	Destination IP	Subnet Mask	Action

ACL Number	1
Source IP	ex.192.168.1.10
Subnet Mask	ex.255.255.255.0
Destination IP	ex.192.168.1.10
Subnet Mask	ex.255.255.255.0
Action	Permit

Figure 37 System Management > Access Control List > IP Standard ACL Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **EDIT** to delete an existing configuration.
ACL number	Specify the number to identify the entry.
Source IP	Specify the source IP address for the entry.
Subnet mask	Specify the subnet mask address for the entry.
Destination IP	Specify the destination IP address for the entry.
Subnet mask	Specify the subnet mask address of the destination IP entry.
Action	Permit (default): Frames matching ACE can be forwarded and learned. Deny: Frames matching ACE are dropped.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.2. User Management

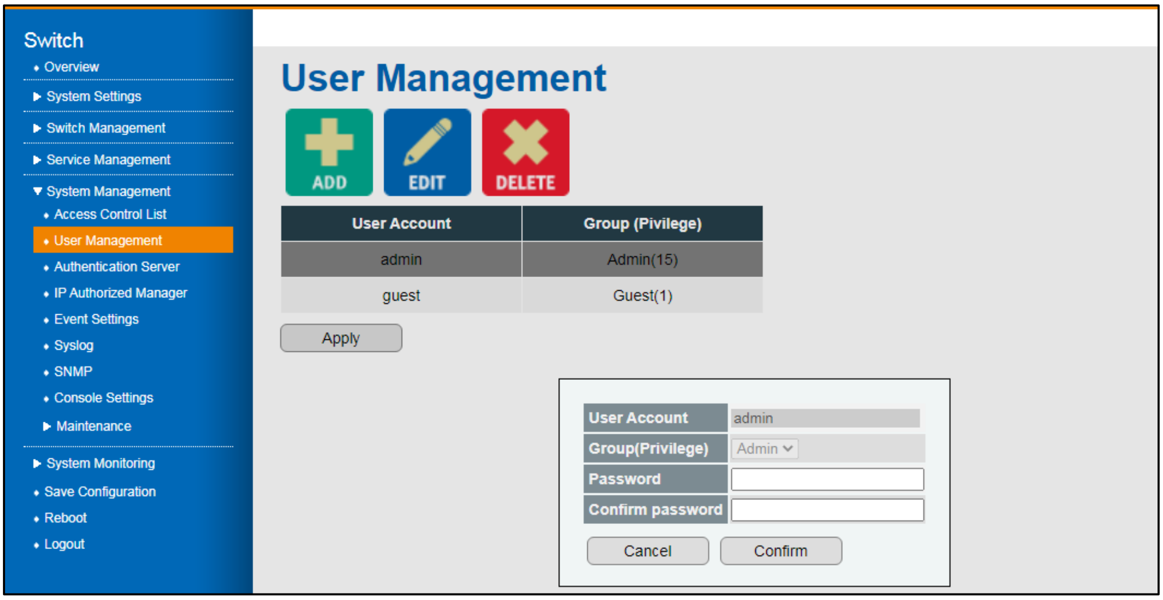
To configure the settings, see the following steps:

Log in to the interface, see Accessing the Web Interface.

1 - Click **System Management** > **User Management**. The GUI screen displays the User Management menu.

2 - Select the fields to be configured to define the settings.

3 - Click **Apply**.



User Account	Group (Pivilege)
admin	Admin(15)
guest	Guest(1)

User Account	admin
Group(Privilege)	Admin
Password	
Confirm password	

Figure 39 System Management > User Management Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **EDIT** to delete an existing configuration.
User account	Specify the name of the user entry.
Group (Privilege)	Specify a user privilege. Available privileges: Admin and Guest.
Password	Specify the password for the user entry.
Confirm password	Specify the password by re-entering it to confirm.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.3. Authentication Server

Client authentication is handled by the authentication server function. In addition to validating the client's identity, the authentication server also informs the switch whether the client is authorized to access LAN and switch services. Because the switch acts as a proxy, the authentication service is transparent to the client. Two authentication methods are available: RADIUS or TACACS+.

3.6.3.1. RADIUS

By using Remote Access Dial-In User Service (RADIUS), networks can be securely protected from unauthorized access. JetNet series switches send all user authentication and network service access information to a central RADIUS server that contains all user authentication and network service access information.

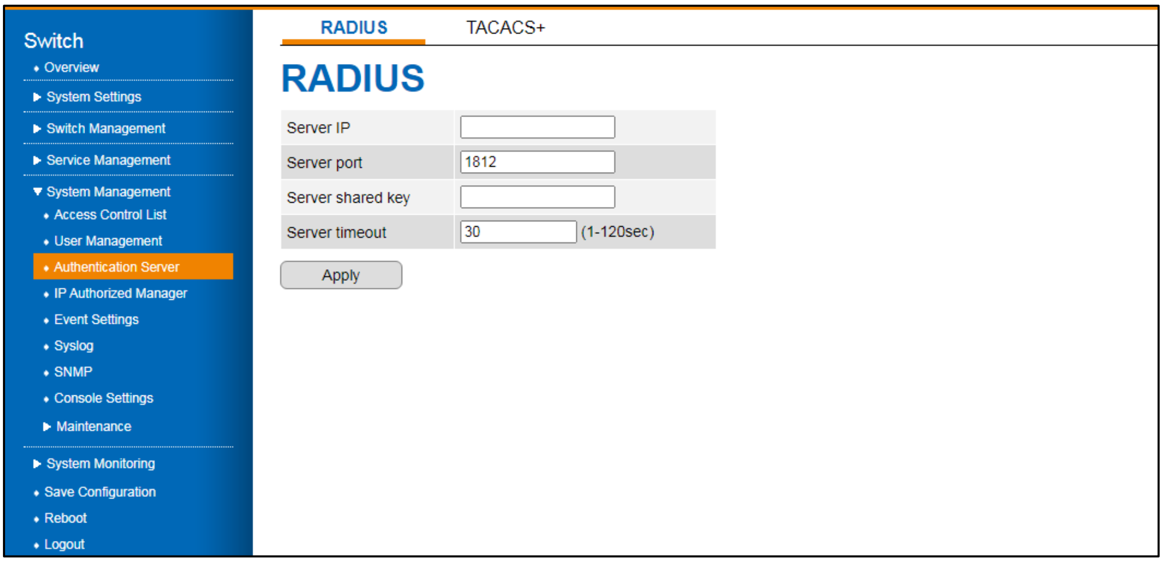
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Authentication Server** > **RADIUS**. The GUI screen displays the RADIUS menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



RADIUS

Server IP	
Server port	1812
Server shared key	
Server timeout	30 (1-120sec)

Figure 40 System Management > Authentication Server > RADIUS Menu.

Item	Description
Server IP	Specify the IP address of the RADIUS server.
Server port	Specify the UDP port of the RADIUS server.

Item	Description
Server shared key	Specify the password (shared key) to authenticate access between the switch and the RADIUS server.
Server timeout	Specify the period of time in seconds (1 to 120 sec.) to define the response for authentication before dropping the request.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.3.2. TACACS+

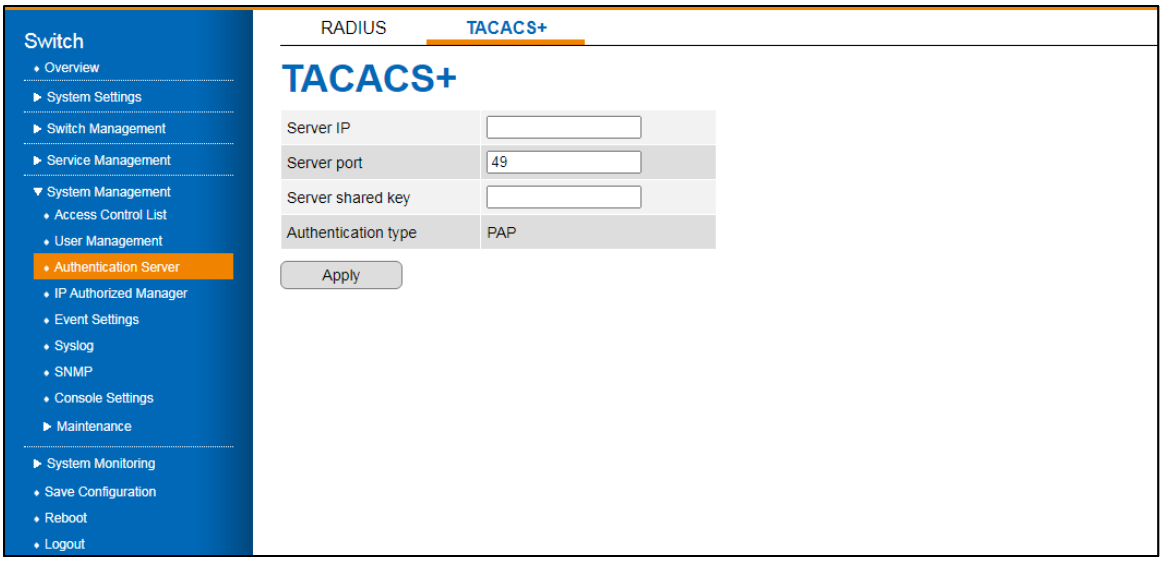
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Authentication Server** > **TACACS+**. The GUI screen displays the TACACS+ menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



TACACS+

Server IP	
Server port	49
Server shared key	
Authentication type	PAP

Figure 41 System Management > Authentication Server > TACACS+ Menu

Item	Description
Server IP	Specify the TACACS+ server IP address.
Server port	Specify the TACACS+ server port.
Server shared key	Specify the authentication key.
Authentication type	Displays the authentication type: PAP.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.
- We recommend a redundant connection between a switch stack and the TACACS+ server. This is to help ensure that the TACACS+ server remains accessible in case one of the connected stack members is removed from the switch stack.

3.6.4. IP Authorized Manager

Using the Authorized IP Manager feature, users can access the switch through the network based on their IP addresses. The following methods are supported:

- SNMP versions 1, 2 and 3
- Telnet
- HTTP

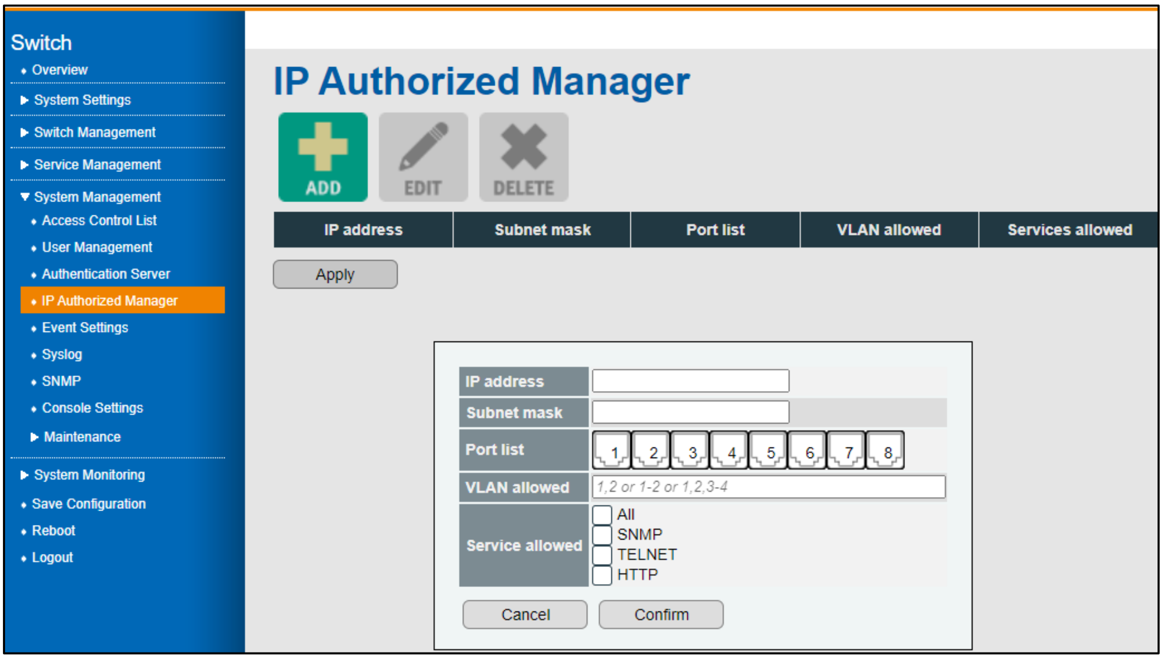
Whenever the Authorized IP managers feature is configured on the switch, it takes precedence over local passwords, TACACS+, and RADIUS. The switch must authorize the IP address of a networked management device before it can authenticate the device using any other security features.
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **IP Authorized Manager**. The GUI screen displays the IP Authorized Manager menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



IP Authorized Manager

IP address	Subnet mask	Port list	VLAN allowed	Services allowed

IP address	
Subnet mask	
Port list	1 2 3 4 5 6 7 8
VLAN allowed	1,2 or 1-2 or 1,2,3-4
Service allowed	□ All □ SNMP □ TELNET □ HTTP

Figure 42 System Management > IP Authorized Manager Menu

Item	Description
ADD	Click **ADD** to create a configuration. The Configuration menu is displayed.
EDIT	Click **EDIT** to modify an existing configuration.
DELETE	Click **EDIT** to delete an existing configuration.
IP address	Specify the IP address of an authorized manager.
Subnet Mask	Specify the subnet mask of the authorized manager.
Port list	Specify the port(s) accessible by the authorized manager entry.
VLAN allowed	Specify the VLAN entry in which access is authorized.
Service allowed	Specify the authorized manager access method: All, SNMP, Telnet, HTTP.
Cancel	Click **Cancel** to exit the screen without saving.
Confirm	Click **Confirm** to exit the screen and save the settings.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.5. Event Settings

System events are related to the overall function of the switch. The Event Settings describes events that can be monitored through the system log function.

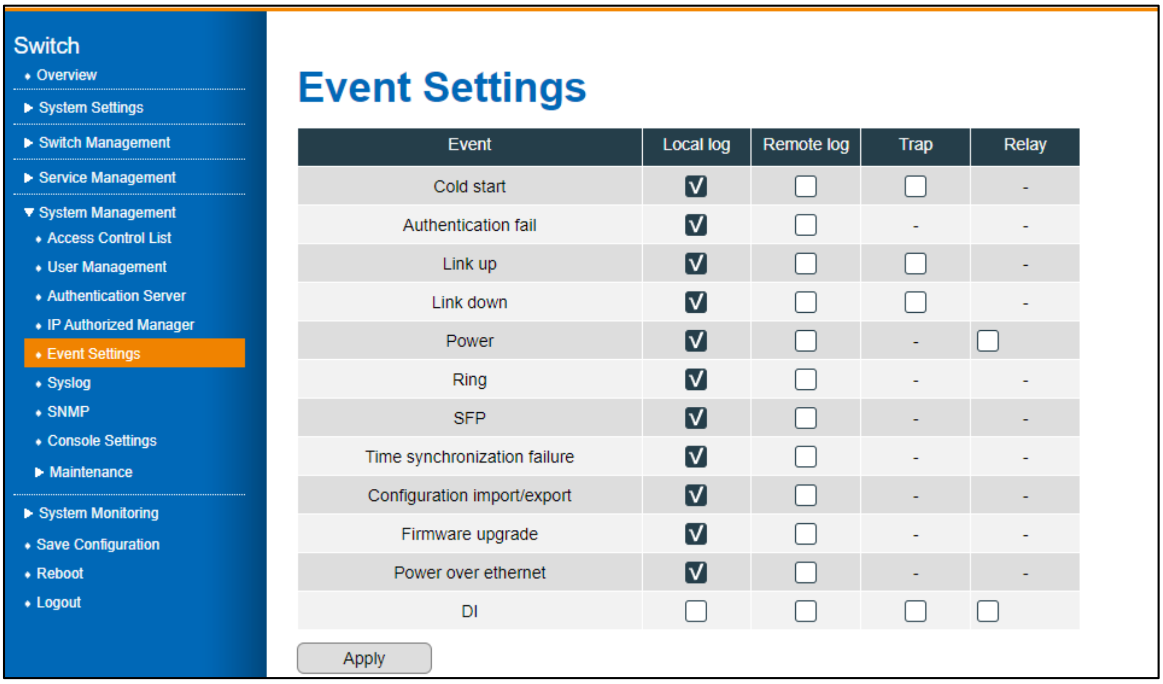
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Event Settings.** The GUI screen displays the Event Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Event Settings

Event	Local log	Remote log	Trap	Relay
Cold start	☑	□	□	-
Authentication fail	☑	□	-	-
Link up	☑	□	□	-
Link down	☑	□	□	-
Power	☑	□	-	□
Ring	☑	□	-	-
SFP	☑	□	-	-
Time synchronization failure	☑	□	-	-
Configuration import/export	☑	□	-	-
Firmware upgrade	☑	□	-	-
Power over ethernet	☑	□	-	-
DI	□	□	□	□

Figure 43 System Management > Event Settings Menu

Item	Description
Cold start	Specify to receive local, remote and trap logs. Event: Power is cut off and then reconnected.
Authentication fail	Specify to receive local and remote logs. Event: An incorrect password, SNMP Community String is entered.
Link up	Specify to receive local, remote and trap logs. Event: The port is connected to another device
Link down	Specify to receive local, remote and trap logs. Event: The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down)

Item	Description
Power	Specify to receive local, remote, and relay logs. Event: Power (AC, DC1, DC2 or Any) failure.
Ring	Specify to receive local and remote logs. 1. Ring status is Normal. 2. Ring port is down. 3. Ring port is down on other switch. 4. Non-ring port receives ring packet. 5. Ring is disabled.
SFP	Specify to receive local and remote logs. Event: SFP transceiver is overheating or outside of set TX/RX power limits.
Time synchronization failure	Specify to receive local and remote logs. Event: Access to NTP Server failure.
Configuration import/export	Specify to receive local and remote logs. Event: Importing/exporting configuration process failure.
Firmware upgrade	Specify to receive local and remote logs. Event: Firmware upgrade failure.
Power over Ethernet	Specify to receive PoE logs. Event: local and remote status
DI	Specify to receive event logs to pre-defined address. Events: Local log, remote log, trap, relay.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.6. Syslog

With the JetNet series, system administrators can monitor switch events remotely by using the system log. In remote mode, you must assign the IP address of the System Log server. The events you select in Event Settings are sent to the specified System Log server.

To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Syslog.** The GUI screen displays the Syslog menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.

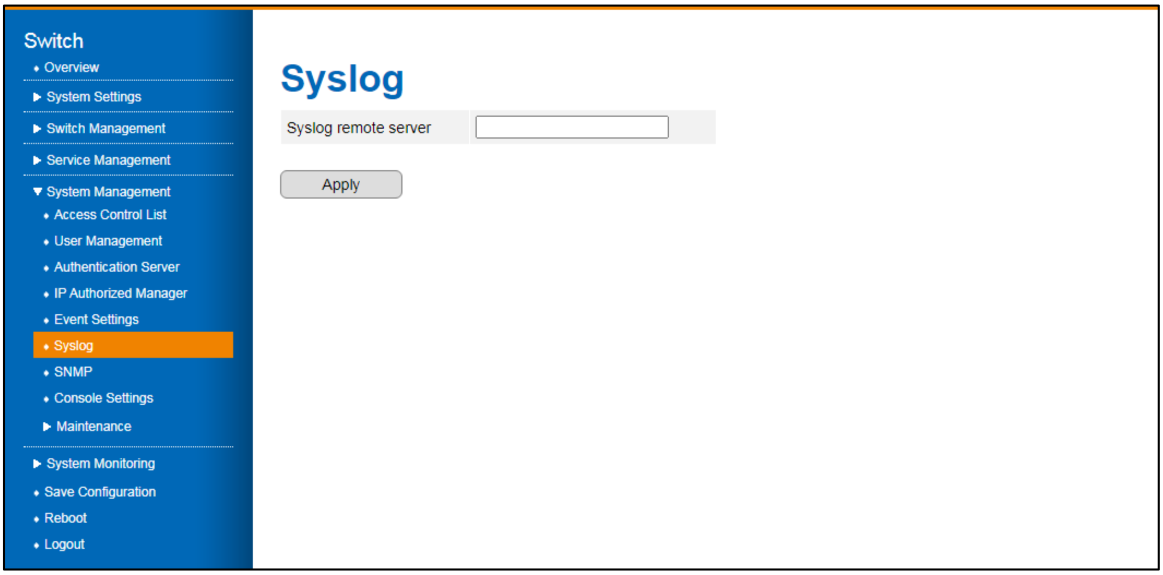


Figure 44 System Management > Syslog

Item	Description
Syslog remote server	Specify the remote server IP address.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.7. SNMP

SNMP is a protocol used to exchange management information between network devices. It is a member of the TCP/IP protocol suite. JetNet series supports SNMP v1/ v2c and v3.

An SNMP-managed network consists of two main components: agents and a manager. An agent is a management software module that resides on a managed switch. It is responsible for translating local management information from managed devices into SNMP-compatible formats. The manager is the console connected to the network.

3.6.7.1.SNMP Setting

Here the user can select either MD5 (Message-Digested algorithm 5) or SHA (Secure Hash Algorithm). MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. JetNet series provide two (2) user authentication protocols: MD5 and SHA.

You will need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.

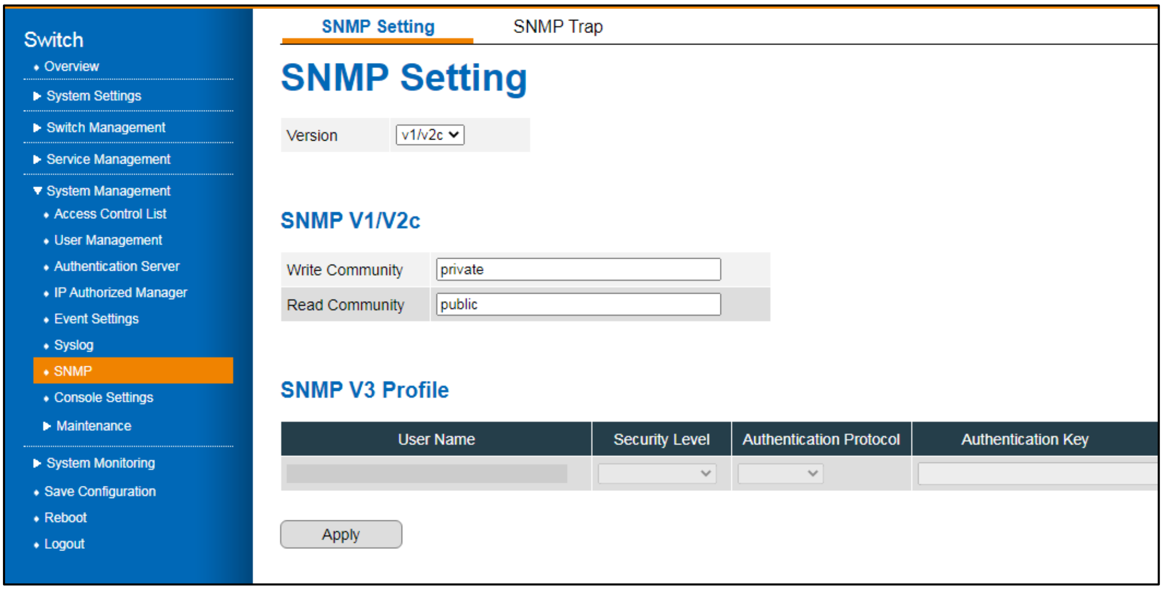
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **SNMP**. The GUI screen displays the SNMP Setting menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



SNMP Setting

Version: v1/v2c

SNMP V1/V2c

Write Community: private

Read Community: public

SNMP V3 Profile

User Name	Security Level	Authentication Protocol	Authentication Key

Figure 45 System Management > SNMP > SNMP Setting Menu

Item	Description
SNMP setting	
Version	Specify the version to support: v1/v2c or v3.
SNMP V1/V2c	
Write community	Specify the write community string: • public for read-only • private for read-write • secret for read-write-all
Read community	Specify the read community string: • public for read-only • private for read-write • secret for read-write-all
SNMP V3 profile	
User name	Specify the user for authentication.
Security level	Specify the permitted level of security: None, Authentication, Privacy.

Item	Description
Authentication protocol	Specify the authentication protocol to use on the interface. Options include: • None – no method is selected • MD5 - Specifies the Message-Digest 5 algorithm, a cryptographic hash function with a 128-bit value. • SHA - The Secure Hash Algorithm specifies related cryptographic hash functions. MD5 was succeeded by SHA. • SHA-256 - cryptographic SHA function that outputs a 256-bit value. • SHA-384 - cryptographic SHA function that outputs a 384-bit value. • SHA-512 - cryptographic SHA function that outputs a 512-bit value.
Authentication key	Specify a key to use while authenticating the packet.
Privacy protocol	Specify the protocol to use for encryption of SNMP v3 messages to ensure confidentiality of data. Options include: • None: no encryption is selected. • DES: encryption using 168-bit key size. • AES-CFB128: encryption using 128-bit key size.
Privacy key	Specify the unique authentication key to use while authenticating encryption.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.7.2.SNMP Trap

An SNMP Trap is a notification feature defined in the SNMP protocol that can be read by any SNMP management application, so you don't have to install any special applications.

You can enable SNMP traps, configure the IP address and community name of the SNMP Trap server, as well as specify the version of the trap. SNMP predefined standard traps and predefined traps are updated after configuration.

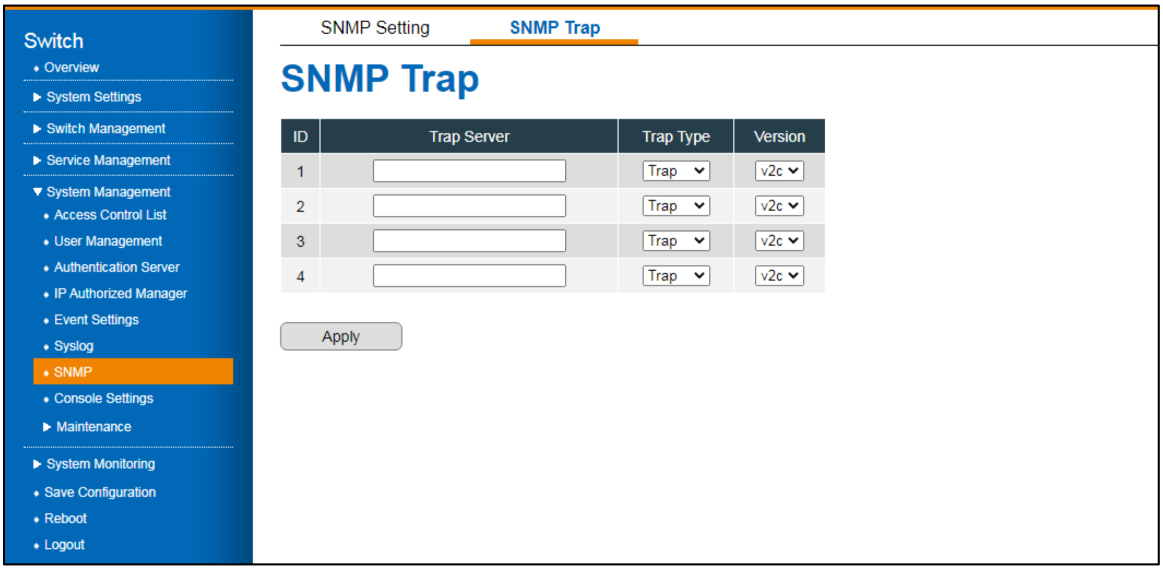
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **SNMP** > **SNMP Trap**. The GUI screen displays the SNMP Trap menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



SNMP Trap

ID	Trap Server	Trap Type	Version
1		Trap	v2c
2		Trap	v2c
3		Trap	v2c
4		Trap	v2c

Figure 46 System Management > SNMP > SNMP Trap Menu

Item	Description
ID	Displays the ID number of the trap entry.
Trap server	Specify the IP address of the trap server IP.
Trap type	Specify the notification flow type of the protocol. Trap: an unacknowledged notification to the SNMP manager. Inform: a notification from SNMP agent to the SNMP manager.
Version	Specify the version type of the trap: Options include: v1, v2c.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.8. Console Settings

With the JetNet series Industrial Managed Switch, you can configure your switch in-band or out-of-band. In cases where a network connection is not available, configuring the switch via an RS-232 console cable is supported. This is an out-of-band management approach.

The in-band management allows remote management of the switch over a network.

Remote management can be accomplished via Telnet or web-based management. All you need is the device's IP address and you can access its embedded HTTP web pages or Telnet console remotely.

The following section provides management of the supported access methods available on the JetNet series.

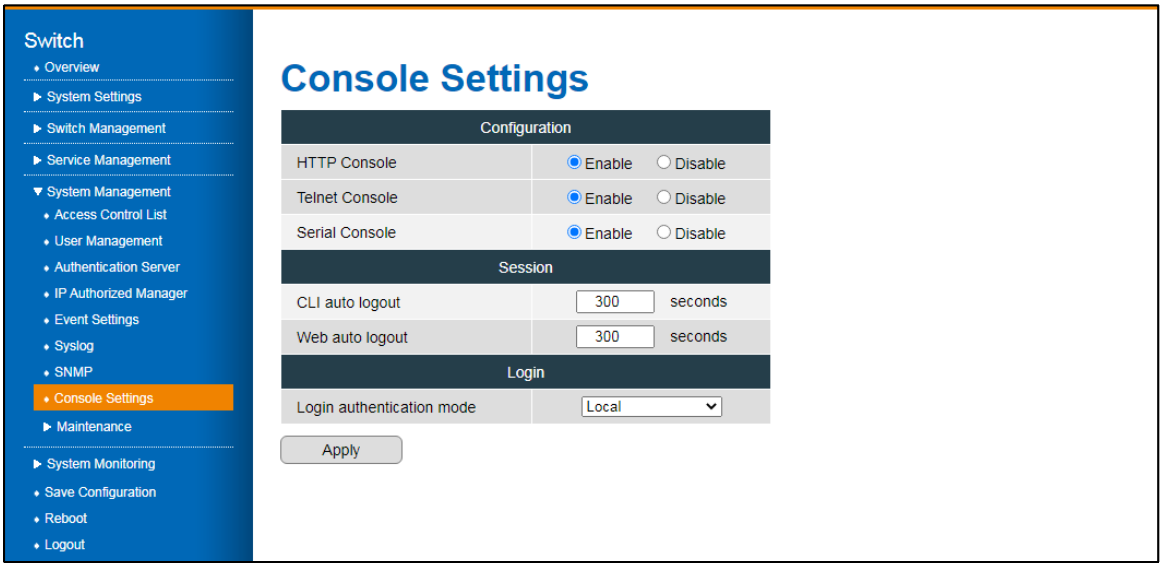
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Console Settings**. The GUI screen displays the Console Settings menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Console Settings

Configuration	
HTTP Console	● Enable ○ Disable
Telnet Console	● Enable ○ Disable
Serial Console	● Enable ○ Disable
Session	
CLI auto logout	300 seconds
Web auto logout	300 seconds
Login	
Login authentication mode	Local

Figure 47 System Management > Console Settings Menu

Item	**Description**
Configuration	
HTTP console	Specify enable (default) or disable to provide users with HTTP console access.
Telnet console	Specify enable (default) or disable to provide users with Telnet console access.
Serial console	Specify enable (default) or disable to provide users with Serial console access.
Session	
CLI auto logout	Specify the inactive timeout period before a CLI user is logged out. The default is 300 seconds.
Web auto logout	Specify the inactive timeout period before a Web user is logged out. The default is 3600 seconds.
Login	
Login authentication mode	Specify the authentication mode which can access the console. Options include: Local (default), RACIUS – Local, TACACS+ - Local.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.9. Maintenance

3.6.9.1.Load Factory Default

The switch can be reset to its original factory default settings through the use of the Load Factory Default function.

To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Maintenance** > **Load Factory Default**. The GUI screen displays the Load Factory Default menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.

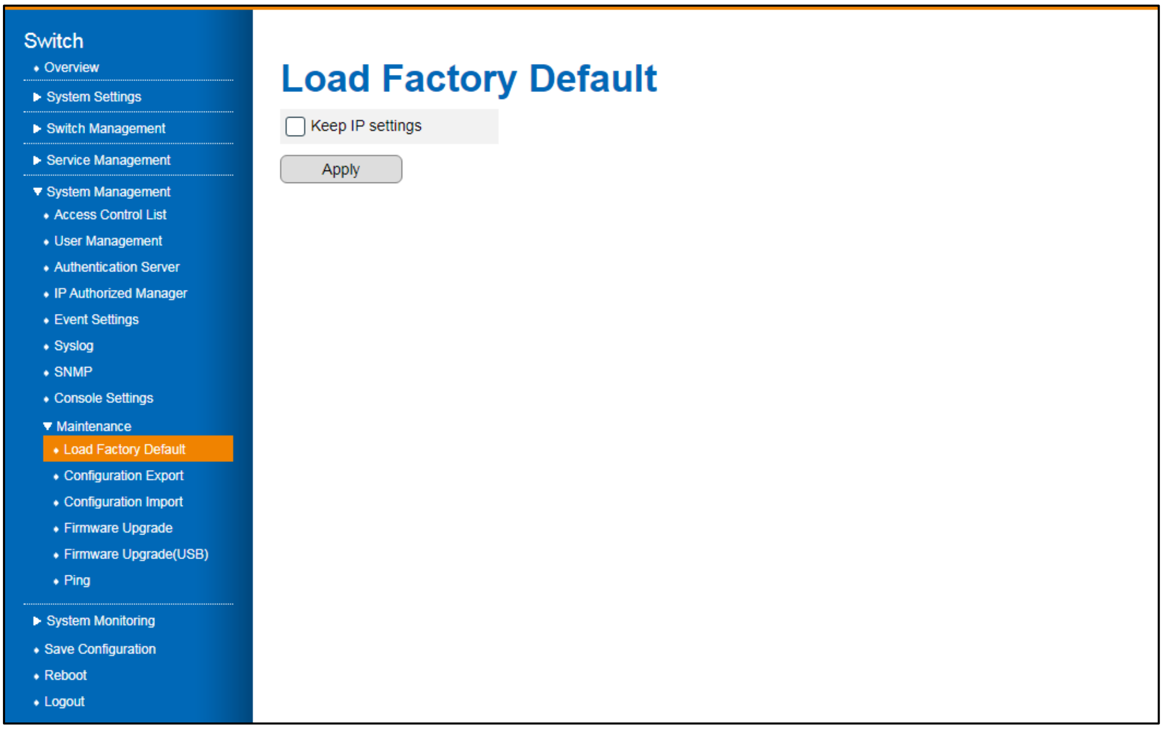


Figure 48 System Management > Maintenance > Load Factory Default Menu

Item	Description
Keep IP settings	Specify to exempt system IP settings from the factory reset process.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.6.9.2. Configuration Export

In addition to updating the system setting, you can also export settings to an external file.

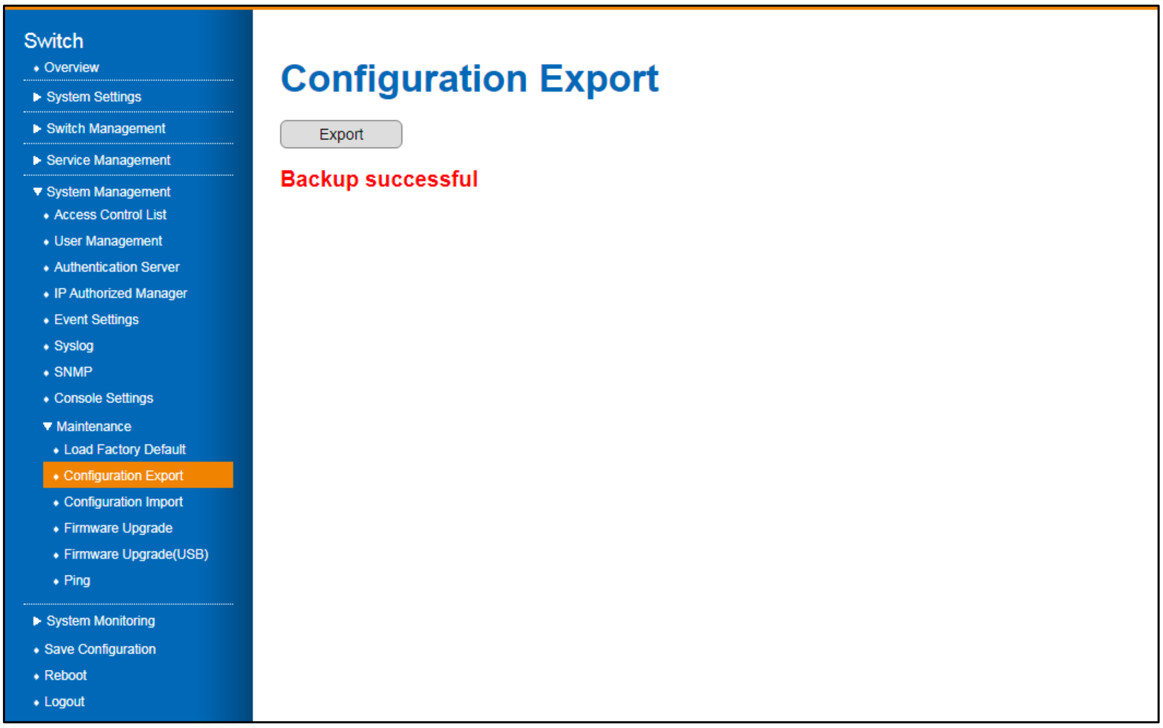
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Maintenance** > **Configuration Export**. The GUI screen displays the Configuration Export menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Backup successful

Figure 49 System Management > Maintenance > Configuration Export Menu

Item	Description
Export	Click **Export** to download the current buffered configuration settings to a *.conf file, such as *JetNet5200-xx-xx.conf*.

3.6.9.3. Configuration Import

Once a configuration file is created through the Export function or obtained from an administrator, you can import the systems settings. After the file is imported, the system is updated a **Restore successful** message displays.

To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Maintenance** > **Configuration Import**. The GUI screen displays the Configuration Import menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.

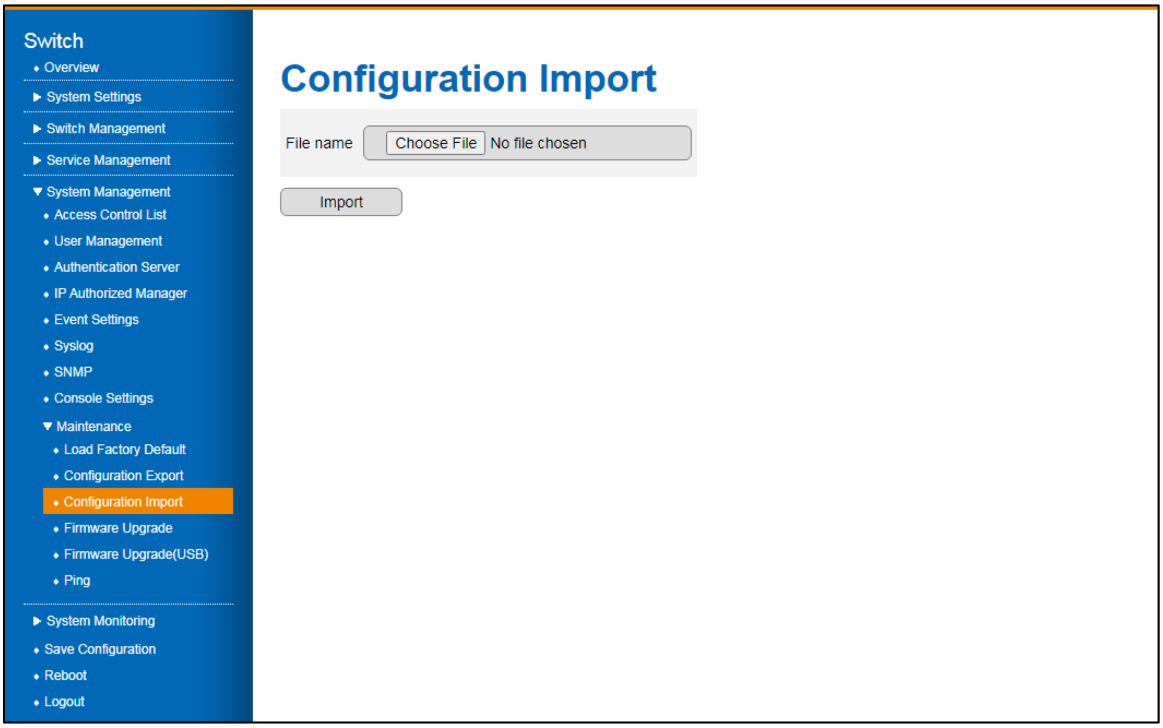


Figure 50 System Management > Maintenance > Configuration Import Menu

Item	Description
Choose File	Click **Choose File** to select a previously saved configuration file (*.conf file) to import in the device.
Import	Click **Import** to load the selected file into the device.

3.6.9.4. Firmware Upgrade

With the Firmware Upgrade feature, you can update your switch to the latest firmware. The latest firmware is available on Beijer's website. It includes new features, bug fixes, and other software updates. A release note will also be provided. We recommend that the switch be installed on the customer site using the latest firmware. When updating the system's firmware, the new firmware overwrites the current image. After uploading the new firmware, the system will automatically reboot. If upgrading remotely, ensure all users are notified prior to starting the upgrade process. To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Management** > **Maintenance** > **Firmware Upgrade**. The GUI screen displays the Firmware Upgrade Import menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.

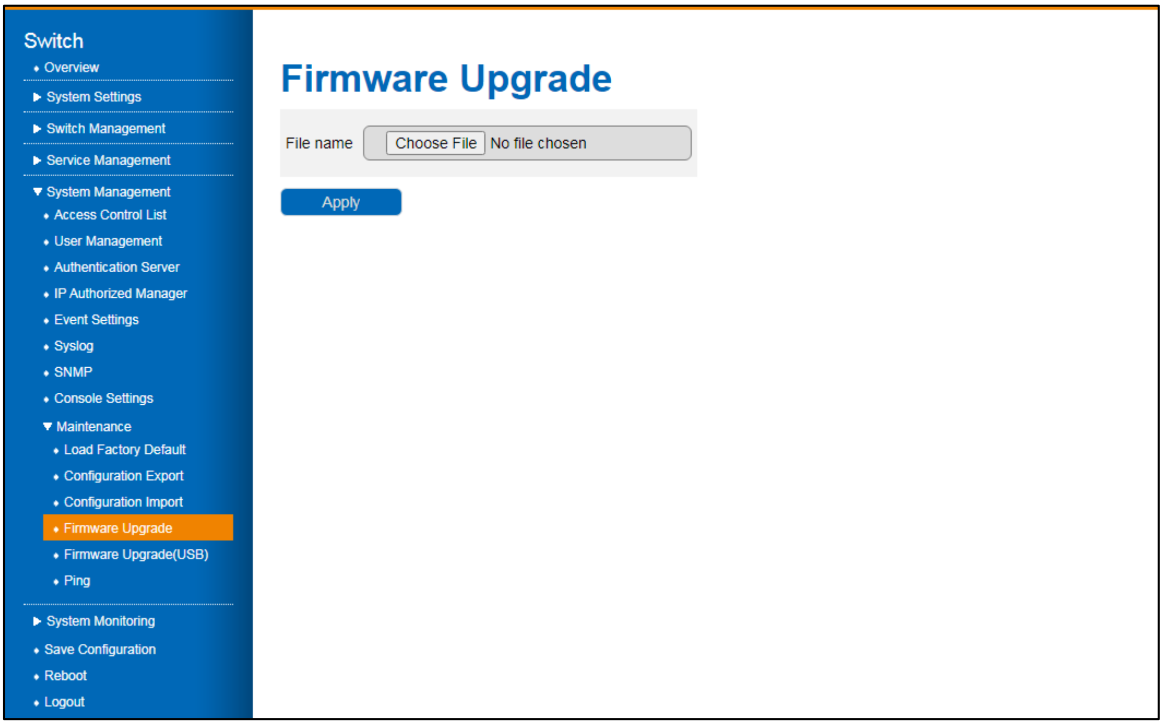


Figure 51 System Management > Maintenance > Firmware Upgrade Menu

Item	Description
File name	Click **Choose File** to select a firmware file (*.bin file) to upgrade the device. **Note!** System reboots automatically after firmware upgrade. If upgrading remotely, ensure all users are notified prior to starting the upgrade process.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

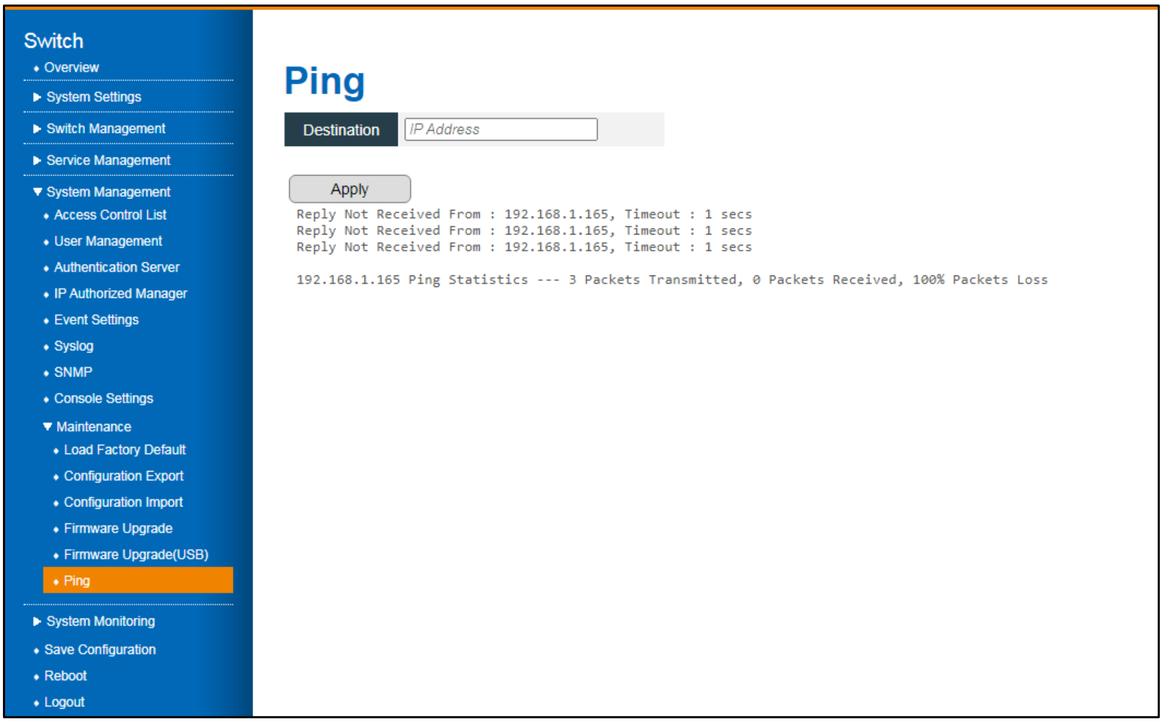
3.6.9.5. Ping

The ping command sends a sequence of ICMP echo request packets to the specified host. It is one of the simplest and most commonly used troubleshooting tools.

Ping prints a special character for each packet indicating whether the router received the corresponding echo reply.

To configure the settings, see the following steps:

- Log in to the interface, see Accessing the Web Interface.
- Click **System Management** > **Maintenance** > **Ping**. The GUI screen displays the Ping menu.
- Select the fields to be configured to define the settings.
- Click **Apply**.



```
Reply Not Received From : 192.168.1.165, Timeout : 1 secs
Reply Not Received From : 192.168.1.165, Timeout : 1 secs
Reply Not Received From : 192.168.1.165, Timeout : 1 secs

192.168.1.165 Ping Statistics --- 3 Packets Transmitted, 0 Packets Received, 100% Packets Loss
```

Figure 51 System Management > Maintenance > Ping Menu

Item	Description
Destination	Specify the IP address to transmit an echo request packet.
Apply	Click **Apply** on the main menu to save the configuration changes. The Configuration changes screen displays.

3.7. System Monitoring

System Logs allow system administrators to monitor switch events.

3.7.1. System Logs

In this page, you will find the most recent entries in the Switch's internal log. Log entries are listed in chronological order (the most recent entries will be at the bottom of the list).

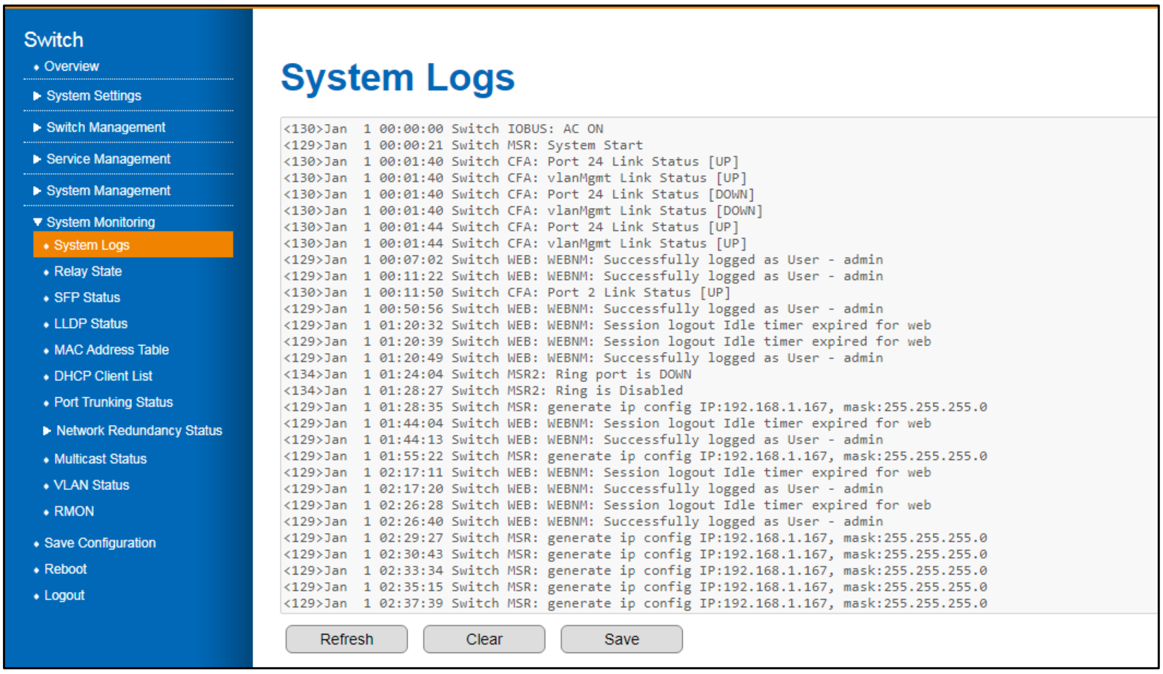
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **System Logs**. The GUI screen displays the System Logs menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



```
<130>Jan  1 00:00:00 Switch IOBUS: AC ON
<129>Jan  1 00:00:21 Switch MSR: System Start
<130>Jan  1 00:01:40 Switch CFA: Port 24 Link Status [UP]
<130>Jan  1 00:01:40 Switch CFA: vlanMgmt Link Status [UP]
<130>Jan  1 00:01:40 Switch CFA: Port 24 Link Status [DOWN]
<130>Jan  1 00:01:40 Switch CFA: vlanMgmt Link Status [DOWN]
<130>Jan  1 00:01:44 Switch CFA: Port 24 Link Status [UP]
<130>Jan  1 00:01:44 Switch CFA: vlanMgmt Link Status [UP]
<129>Jan  1 00:07:02 Switch WEB: WEBNM: Successfully logged as User - admin
<129>Jan  1 00:11:22 Switch WEB: WEBNM: Successfully logged as User - admin
<130>Jan  1 00:11:50 Switch CFA: Port 2 Link Status [UP]
<129>Jan  1 00:50:56 Switch WEB: WEBNM: Successfully logged as User - admin
<129>Jan  1 01:20:32 Switch WEB: WEBNM: Session logout Idle timer expired for web
<129>Jan  1 01:20:39 Switch WEB: WEBNM: Session logout Idle timer expired for web
<129>Jan  1 01:20:49 Switch WEB: WEBNM: Successfully logged as User - admin
<134>Jan  1 01:24:04 Switch MSR2: Ring port is DOWN
<134>Jan  1 01:28:27 Switch MSR2: Ring is Disabled
<129>Jan  1 01:28:35 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
<129>Jan  1 01:44:04 Switch WEB: WEBNM: Session logout Idle timer expired for web
<129>Jan  1 01:44:13 Switch WEB: WEBNM: Successfully logged as User - admin
<129>Jan  1 01:55:22 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
<129>Jan  1 02:17:11 Switch WEB: WEBNM: Session logout Idle timer expired for web
<129>Jan  1 02:17:20 Switch WEB: WEBNM: Successfully logged as User - admin
<129>Jan  1 02:26:28 Switch WEB: WEBNM: Session logout Idle timer expired for web
<129>Jan  1 02:26:40 Switch WEB: WEBNM: Successfully logged as User - admin
<129>Jan  1 02:29:27 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
<129>Jan  1 02:30:43 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
<129>Jan  1 02:33:34 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
<129>Jan  1 02:35:15 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
<129>Jan  1 02:37:39 Switch MSR: generate ip config IP:192.168.1.167, mask:255.255.255.0
```

Figure 51 System Monitoring > System Logs Menu

Item	Description
Refresh	Click to refresh the System Logs entry list.
Clear	Click to delete the System Logs entry list.
Save	Click to download a .txt file of the currently available system logs.

3.7.2. Relay State

The JetNet series come with 1 digital output, commonly referred to as Relay Output. It has relay contacts that are open during normal operation and closed if a fault is detected. The settings can be customized in the fault Relay State if a power outage, a link failure, a ping failure, or a super ring topology change occurs.

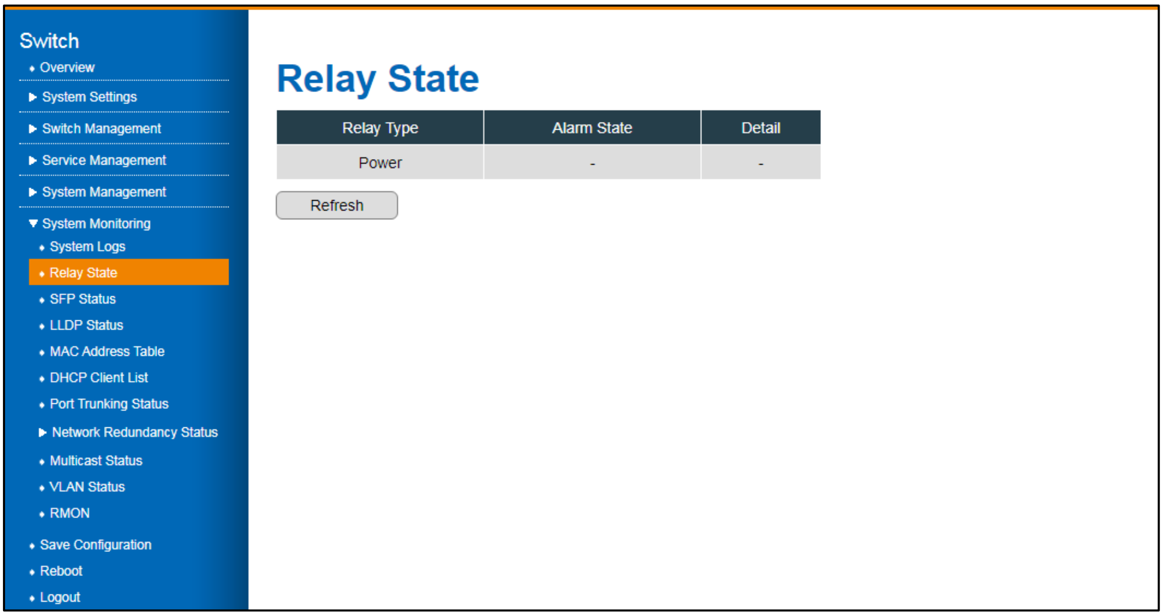
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **Relay State**. The GUI screen displays the Relay State menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Relay State

Relay Type	Alarm State	Detail
Power	-	-

Refresh

Figure 51 System Monitoring > Relay State Menu

Item	Description
Relay Type	Displays the fault relay state. Options include: system and port events.
Alarm State	Displays the status of the instance. Options include: • Normal: Monitoring events are all normal. • Abnormal: An abnormal monitoring event.
Detail	Display abnormal monitoring events: AC or DC1, DC2.
Refresh	Click to refresh the Relay State entry listing.

3.7.3. LLDP Status

The LLDP Status screen enables the viewing of discovered network neighbors as well as the corresponding information.

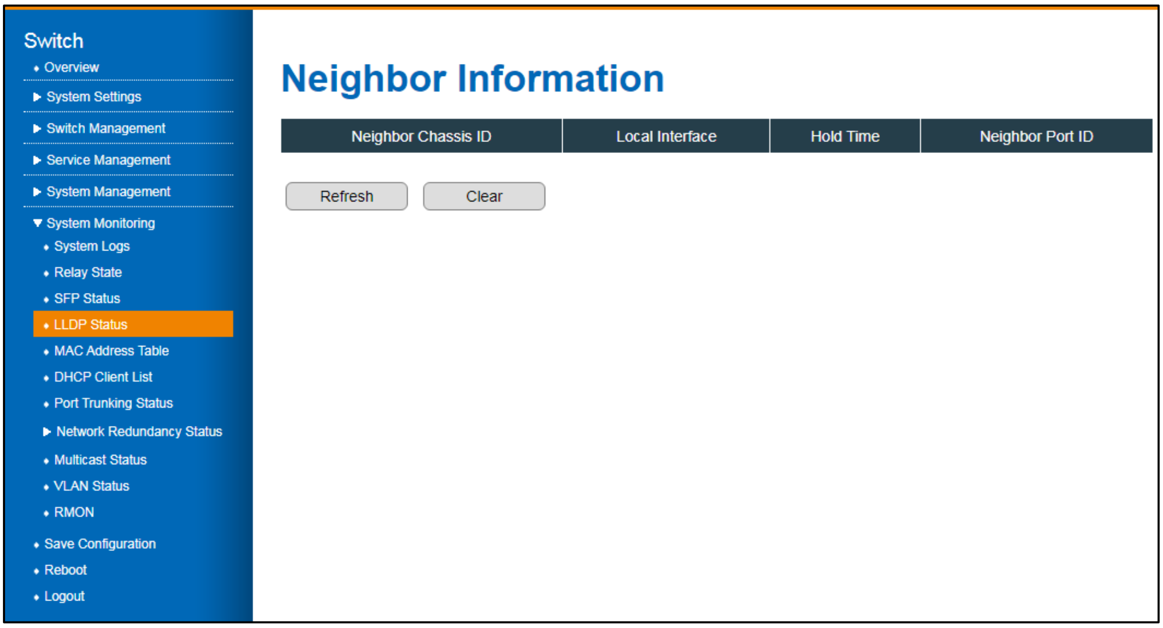
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **Neighbor Information**. The GUI screen displays the Neighbor Information menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Neighbor Information

Neighbor Chassis ID	Local Interface	Hold Time	Neighbor Port ID

Figure 51 System Monitoring > LLDP Status Menu

Item	Description
Neighbor Chassis ID	Displays the discovered neighboring device ID.
Local Interface	Displays the IP address that is advertised from the interface.
Hold Time	Displays the Time to Live timer. The LLDP state expires once the LLDP is not received by the hold time.
Neighbor Port ID	Displays the discovered neighboring port ID.
Refresh	Click to refresh the Neighbor Information entry listing.
Clear	Click to clear the entry list.

3.7.4. MAC Address Table

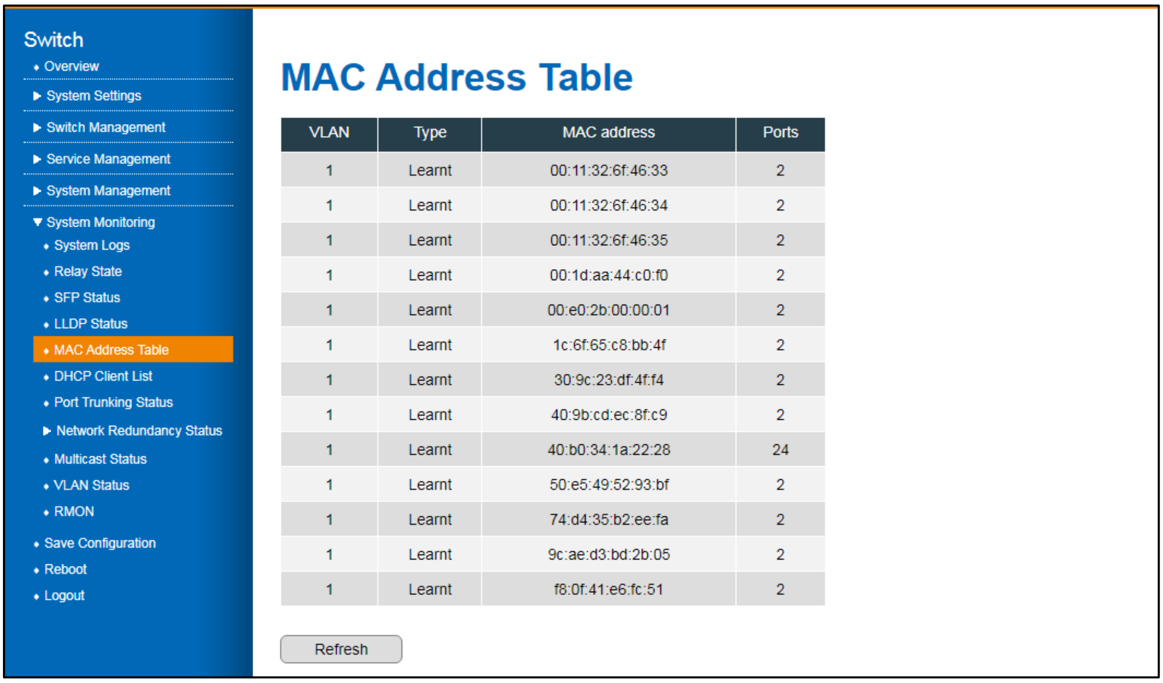
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **MAC Address Table**. The GUI screen displays the MAC Address Table menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



MAC Address Table

VLAN	Type	MAC address	Ports
1	Learnt	00:11:32:6f:46:33	2
1	Learnt	00:11:32:6f:46:34	2
1	Learnt	00:11:32:6f:46:35	2
1	Learnt	00:1d:aa:44:c0:f0	2
1	Learnt	00:e0:2b:00:00:01	2
1	Learnt	1c:6f:65:c8:bb:4f	2
1	Learnt	30:9c:23:df:4f:f4	2
1	Learnt	40:9b:cd:ec:8f:c9	2
1	Learnt	40:b0:34:1a:22:28	24
1	Learnt	50:e5:49:52:93:bf	2
1	Learnt	74:d4:35:b2:ee:fa	2
1	Learnt	9c:ae:d3:bd:2b:05	2
1	Learnt	f8:0f:41:e6:fc:51	2

Figure 51 System Monitoring > MAC Address Table Menu

Item	Description
VLAN	Displays the VLAN ID of the interface.
Type	Displays the status of used or unused entries: Learnt, Static.
MAC address	Displays the advertised MAC address of the chassis entry.
Ports	Displays the member ports assigned to the chassis interface.
Refresh	Click to refresh the MAC Address listing.

3.7.5. DHCP Client List

The Dynamic Host Configuration Protocol (DHCP) client table list displays the address bindings.

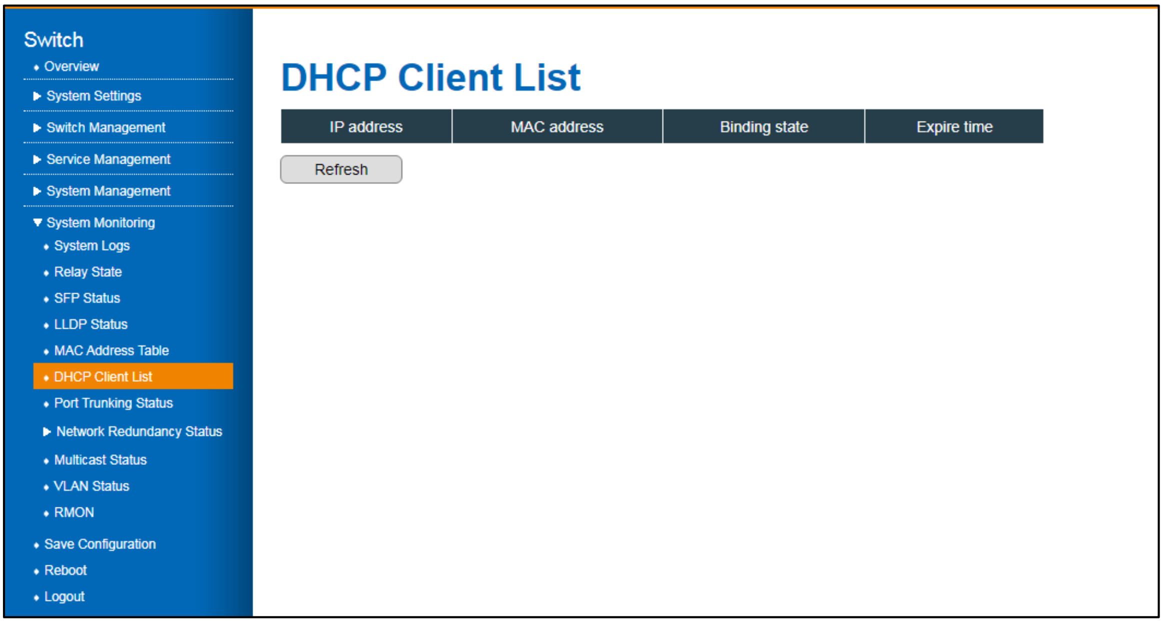
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **DHCP Client List**. The GUI screen displays the DHCP Client List menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



DHCP Client List

IP address	MAC address	Binding state	Expire time

Figure 51 System Monitoring > DHCP Client List Menu

Item	Description
IP address	Displays the IP address of the specified client.
MAC address	Displays the MAC address of the specified client.
Binding state	Displays the state of the address binding
Expire time	Displays the number of seconds in which the lease of the interface expires.
Refresh	Click to refresh the DHCP Client listing.

3.7.6. Port Trunking Status

The Port Trunking Status screen allows for viewing

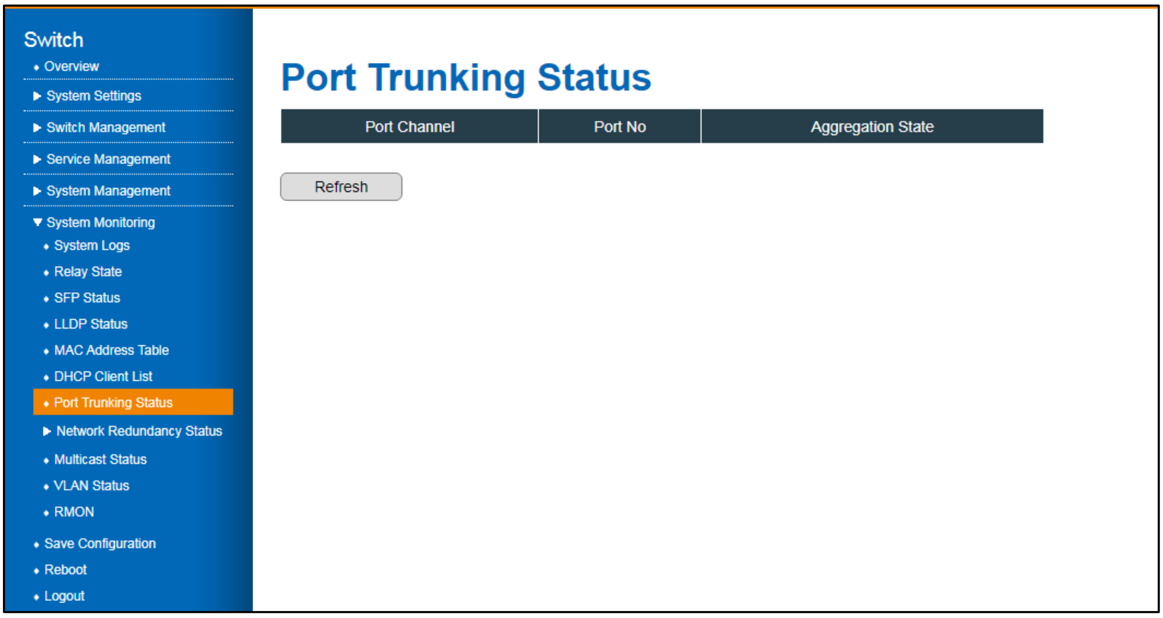
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **Port Trunking Status**. The GUI screen displays the Port Trunking Status menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Port Trunking Status

Port Channel	Port No	Aggregation State

Refresh

Figure 51 System Monitoring > Port Trunking Status Menu

Item	Description
Port Channel	Displays the ring control channel of the LAG.
Port No	Displays the member ports of the LACP group.
Aggregation State	Displays the aggregate state of the interface. • Aggregation: Port is a potential candidate for aggregation. • Individual: Port can be operated only as an individual link. • Sync: Port is allocated to the correct LA group which is associated with a compatible port channel whose identity is consistent with the Actor System ID and Port Channel ID. System ID and Port Channel ID are synced with partner information. • Collecting: Port is enabled to collect incoming frames and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Distributing: Port is enabled to distribute outgoing frames. • Defaulted: Port is configured to use the defaulted operational partner information that is administratively configured for the partner. • Expired: PDUs are not received from partner in certain time period.
Refresh	Click to refresh the Port Trunking listing.

3.7.7. Network Redundancy Status

3.7.7.1. Spanning Tree

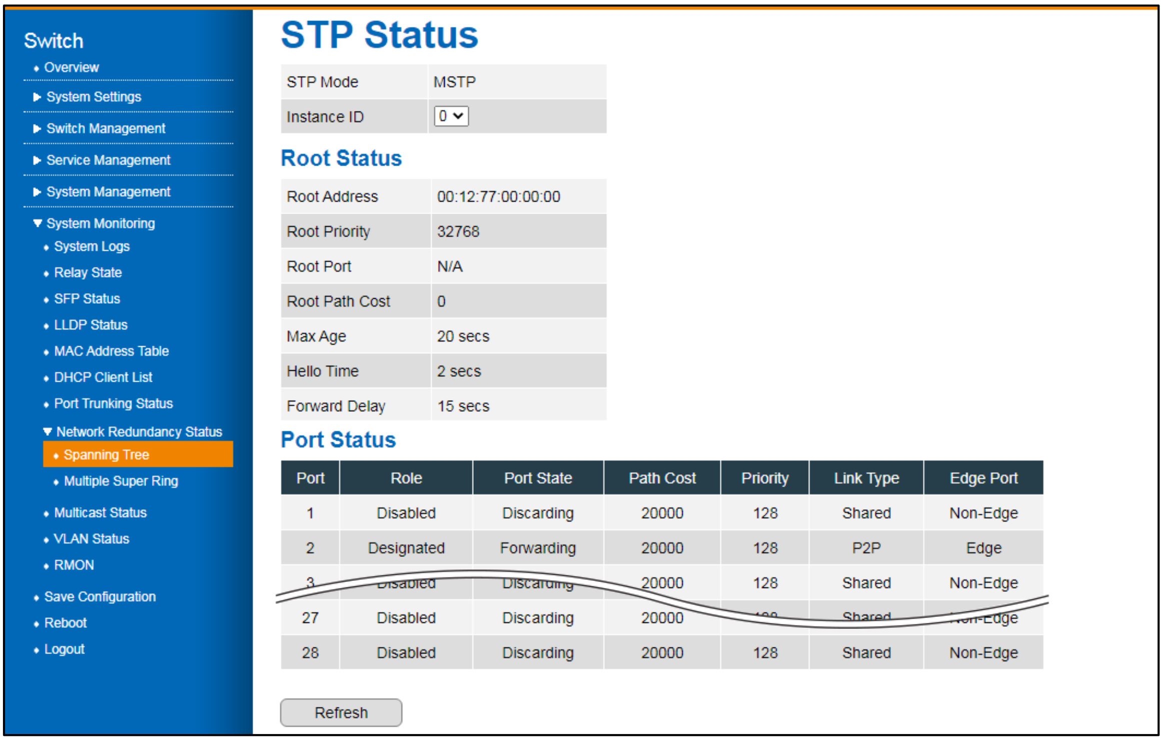
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **Network Redundancy Status** > **Spanning Tree**. The GUI screen displays the Spanning Tree menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



STP Status

STP Mode	MSTP
Instance ID	0

Root Status

Root Address	00:12:77:00:00:00
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 secs
Hello Time	2 secs
Forward Delay	15 secs

Port Status

Port	Role	Port State	Path Cost	Priority	Link Type	Edge Port
1	Disabled	Discarding	20000	128	Shared	Non-Edge
2	Designated	Forwarding	20000	128	P2P	Edge
3	Disabled	Discarding	20000	128	Shared	Non-Edge
27	Disabled	Discarding	20000	128	Shared	Non-Edge
28	Disabled	Discarding	20000	128	Shared	Non-Edge

Figure 51 System Monitoring > Network Redundancy Status > Spanning Tree Menu

Item	Description
STP Mode	Displays the STP mode. Options: STP, RSTP, MSTP, and disable.
Instance ID	Displays the instance ID of the interface. Range: 1 to 15.
Root Status	
Root Address	Displays the instance root address.
Root Priority	Displays the set root priority of the bridge for the selected instance.
Root Port	Displays the root port of the selected instance.
Root Path Cost	Displays the root path cost of the selected instance.

Item	Description
Max Age	Displays the interval (seconds) for the wait period without receiving a configuration message, before attempting to redefine its own configuration.
Hello Time	Displays the interval (seconds) that a Root Bridge waits between configuration messages.
Forward Delay	Displays the interval (seconds) for the wait period in which a bridge remains in a learning state before forwarding packets.
Port Status	
Port	Displays the interface ID of the selected port.
Role	Displays the role of the port that was assigned by STP to provide STP paths. Options include: Disabled: The port is not participating in Spanning Tree Designated: Connects the bridge to the LAN, providing the lowest cost path from the LAN to the Root Bridge.
Port State	Displays the current STP state of a port.
Path Cost	Displays the port contribution to the root path cost.
Priority	Displays the port priority for the specified interface and instance.
Link Type	Displays the link type of the instance. The values can be: • Point-to-Point – Specifies that the port is treated as if it is connected to a point-to-point link. • SharedLan – Specifies that the port is treated as if it is having a shared media connection. The values can be set directly or as Auto for the switch to decide about the point-to-point status, in the field Admin Point to Point provided in the screen Port Status Configuration.
Edge Port	Displays whether or not the port is directly connected to the end stations.
Refresh	Click to refresh the Spanning Tree listing.

3.7.7.2.Multiple Super Ring

The Multiple Super Ring screen provides access to the configuration settings of the ring instances

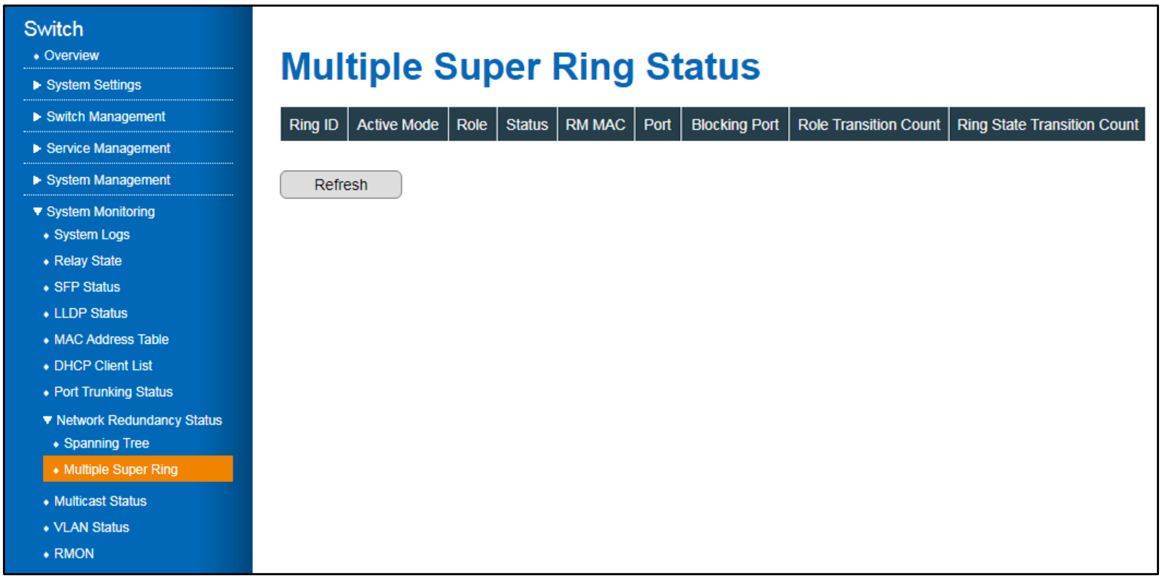
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **Network Redundancy Status** > **Multiple Super Ring**. The GUI screen displays the Multiple Super Ring Status menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



Multiple Super Ring Status

Ring ID	Active Mode	Role	Status	RM MAC	Port	Blocking Port	Role Transition Count	Ring State Transition Count

Figure 51 System Monitoring > Network Redundancy Status > Multiple Super Ring Menu

Item	Description
Ring ID	Displays the ring instance ID.
Active Mode	Displays MSR, activated in Ring or Super Chain mode.
Role	Displays whether the switch role: RM or nonRM.
Status	Displays the status of the instance. Options include: • Normal: redundancy is approved. • Abnormal: link status is broken.
RM MAC	Displays the MAC address of Ring Master of this Ring.
Port	Displays the configured port for the instance.
Blocking Port	Displays the RM blocked port.
Role Transition Count	Displays the number of times the switch has changed its Role from nonRM to RM or from RM to nonRM.
Ring State Transition Count	Displays the number of times the Ring status has been transformed between Normal and Abnormal state.
Refresh	Click to Refresh the Multi Super Ring Status listing.

3.7.8. Multicast Status

The Multicast Status screen displays the MAC address and VLAN learning and forwarding properties for the configured interfaces.

To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **Multicast Status**. The GUI screen displays the MAC Based Multicast Forwarding Table menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.

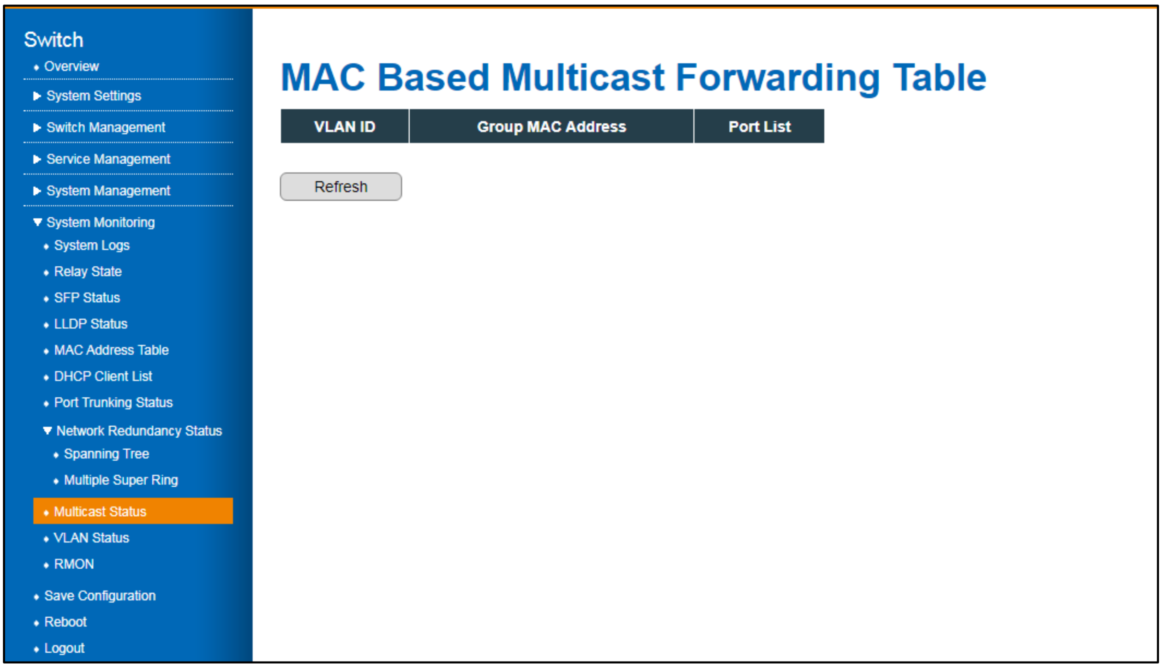


Figure 51 System Monitoring > Multicast Status Menu

Item	Description
VLAN ID	Displays the VLAN ID of the interface.
Group MAC Address	Displays the MAC address used for the group of hosts to process frames intended for multicasting.
Port List	Displays the member port(s) configured to the interface.
Refresh	Click to refresh the MAC Based Multicast Forwarding Table listing.

3.7.9. VLAN Status

The VLAN Status screen displays the current settings of the VLAN interface(s).

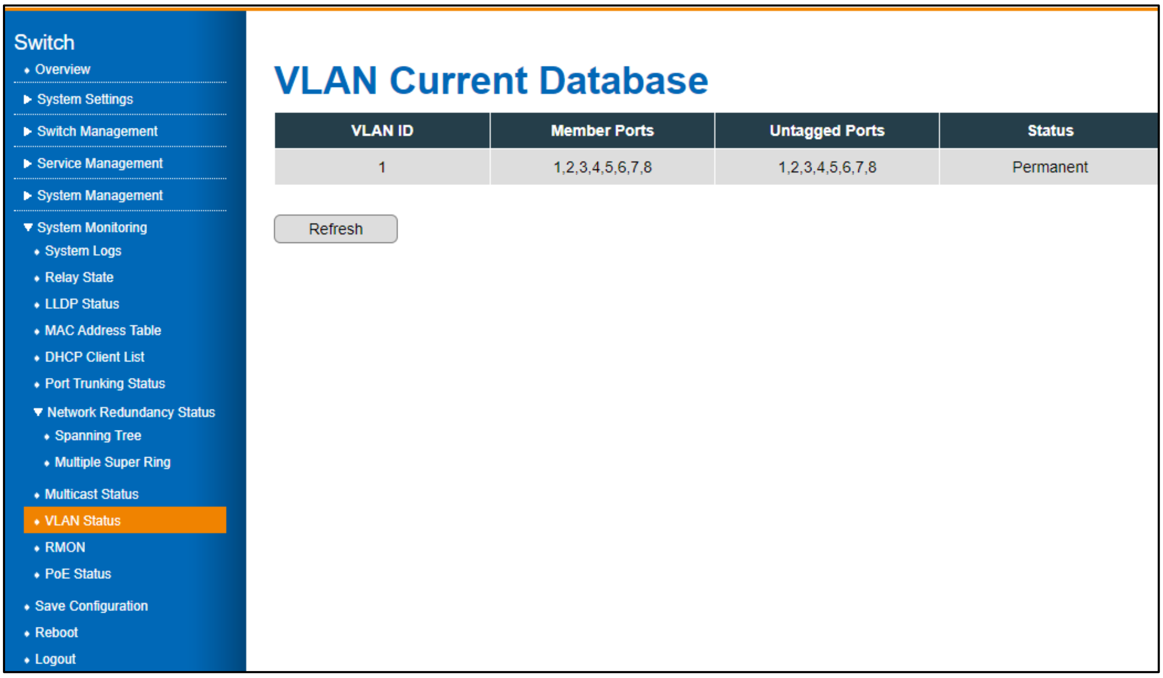
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **VLAN Status**. The GUI screen displays the VLAN Current Database menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



VLAN Current Database

VLAN ID	Member Ports	Untagged Ports	Status
1	1,2,3,4,5,6,7,8	1,2,3,4,5,6,7,8	Permanent

Figure 51 System Monitoring > VLAN Status Menu

Item	Description
VLAN ID	Displays the VLAN ID of the interface.
Member Ports	Displays the member ports specified as tagged egress ports.
Untagged Ports	Displays the member ports specified as untagged egress ports.
Status	Displays the status of the ports.
Refresh	Click to refresh the VLAN Current Database listing.

3.7.10. RMON

The RMON screen displays detailed information regarding packet sizes and information regarding physical layer errors.

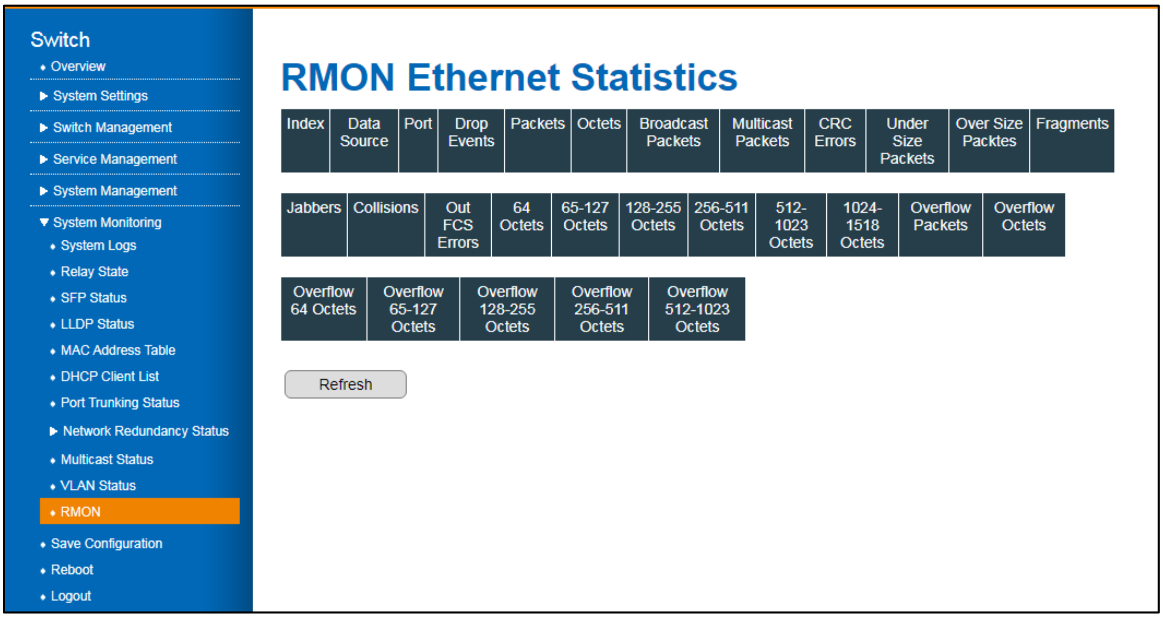
To configure the settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **RMON**. The GUI screen displays the RMON Ethernet Statistics menu.

3 - Select the fields to be configured to define the settings.

4 - Click **Apply**.



RMON Ethernet Statistics

Index	Data Source	Port	Drop Events	Packets	Octets	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packtes	Fragments

Jabbers	Collisions	Out FCS Errors	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets	Overflow Packets	Overflow Octets

Overflow 64 Octets	Overflow 65-127 Octets	Overflow 128-255 Octets	Overflow 256-511 Octets	Overflow 512-1023 Octets

Figure 51 System Monitoring > RMON Ethernet Statistics Menu

Item	Description
Index	Displays the index of the interface representing the RMON probe.
Data Source	Displays the Ethernet subnetwork that is the data source of the interface.
Port	Displays the port number of the interface.
Drop Events	Displays the number of packets that were dropped.
Packets	Displays the number of packets received, which includes bad packets, Multicast packets, and Broadcast packets.
Octets	Displays the number of octets received, which includes bad packets and FCS octets and excludes framing bits.
Broadcast Packets	Displays the number of good broadcast packets received, excluding Multicast packets.

Item	Description
Multicast Packets	Displays the number of good Multicast packets received.
CRC Errors	Displays the number of CRC errors that have occurred.
Under Size Packets	Displays received number of undersized packets (less than 64 octets).
Over Size Packets	Displays the number of oversized packets (over 1518 octets) received.
Fragments	Displays the number of fragments (packets with less than 64 octets, excluding framing bits--including FCS octets) received
Jabbers	Displays the number of received packets, longer than 1632 octets.
Collisions	Displays the number of collisions received.
Out FCS Errors	Displays the number of FC octet errors.
64 Octets	Displays the number of frames, containing 64 octets that were received.
65-127 Octets	Displays the number of frames, containing 65 to 127 octets that were received.
128-255 Octets	Displays the number of frames, containing 128 to 255 octets that were received.
256-511 Octets	Displays the number of frames, containing 256 to 511 octets that were received.
512-1023 Octets	Displays the number of frames, containing 512 to 1023 octets that were received.
1024-1518 Octets	Displays the number of frames, containing 1024 to 1518 octets that were received.
Overflow Packets	Displays the number of frames, containing nonconforming packets of the first bucket that were received.
Overflow Octets	Displays the number of overflow octets.
Overflow 64 Octets	Displays the number of overflow packets which are 64 octets in length.
Overflow 65-127 Octets	Displays the number of total number of overflow packets which are between 65 and 127 octets in length.
Overflow 128-255 Octets	Displays the number of total number of overflow packets which are between 128 and 255 octets in length.
Overflow 256-511 Octets	Displays the number of total number of overflow packets which are between 512 and 1023 octets in length.
Overflow 512-1023 Octets	Displays the number of total number of overflow packets which are between 512 and 1023 octets in length.
Overflow 1024-1518 Octets	Displays the number of total number of overflow packets which are between 1024 and 1518 octets in length.
Refresh	Click to refresh the RMON Ethernet Statistics listing.

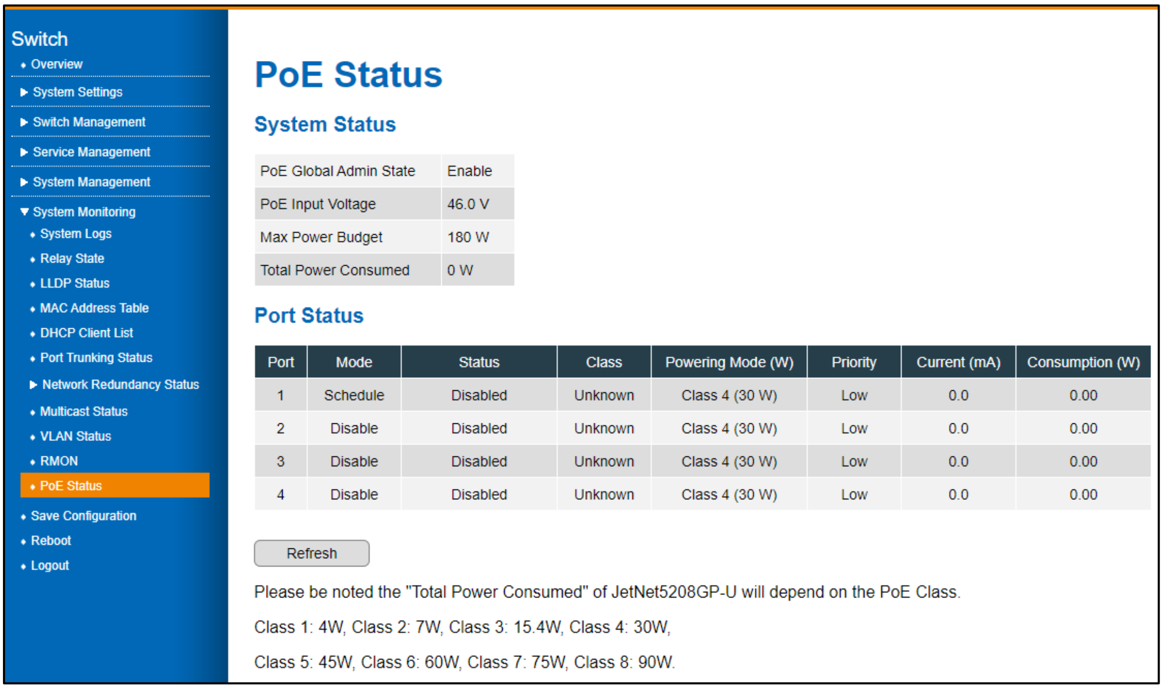
3.7.11. PoE Status

A managed switch can be enabled with Power over Ethernet (PoE), which allows it to provide power to end devices connected on the other side of its Ethernet ports called Powered Devices (PD). End devices that are located in areas without power will benefit from this.

To view the PoE status settings, see the following steps:

1 - Log in to the interface, see Accessing the Web Interface.

2 - Click **System Monitoring** > **PoE Status**. The GUI screen displays the PoE Status screen. The System and Port status information is displayed.



PoE Status

System Status

PoE Global Admin State	Enable
PoE Input Voltage	46.0 V
Max Power Budget	180 W
Total Power Consumed	0 W

Port Status

Port	Mode	Status	Class	Powering Mode (W)	Priority	Current (mA)	Consumption (W)
1	Schedule	Disabled	Unknown	Class 4 (30 W)	Low	0.0	0.00
2	Disable	Disabled	Unknown	Class 4 (30 W)	Low	0.0	0.00
3	Disable	Disabled	Unknown	Class 4 (30 W)	Low	0.0	0.00
4	Disable	Disabled	Unknown	Class 4 (30 W)	Low	0.0	0.00

Please be noted the "Total Power Consumed" of JetNet5208GP-U will depend on the PoE Class.

Class 1: 4W, Class 2: 7W, Class 3: 15.4W, Class 4: 30W,

Class 5: 45W, Class 6: 60W, Class 7: 75W, Class 8: 90W.

Figure 51 System Monitoring > PoE Status Screen

Item	Description
System Status	Displays the following status fields: • PoE global Admin, enabled or disabled • PoE input voltage • Max power budget • Total power consumed

Item	Description
Port Status	Displays the following port status fields: • Port • Mode • Status • Class • Powering Mode (W) • Priority • Current (mA) • Consumption (W)
Refresh	Click to refresh the PoE Status listings.

Note: The Total Power Consumed is dependent on the PoE Class.

Class 1: 4W	Class 2: 7W	Class 3: 15.4
Class 4: 30W	Class 5: 45W	Class 6: 60W
Class 7: 75W	Class 8: 90W	

3.8. Save Configuration

The Save Configuration screen allows you to save any configuration to Flash. The Save Configuration allows you to save any configuration you just made to Flash. By powering off your switch without using the Save Configuration function, the new settings will be lost. After selecting **Save Configuration**, click **Save** to save the changes.

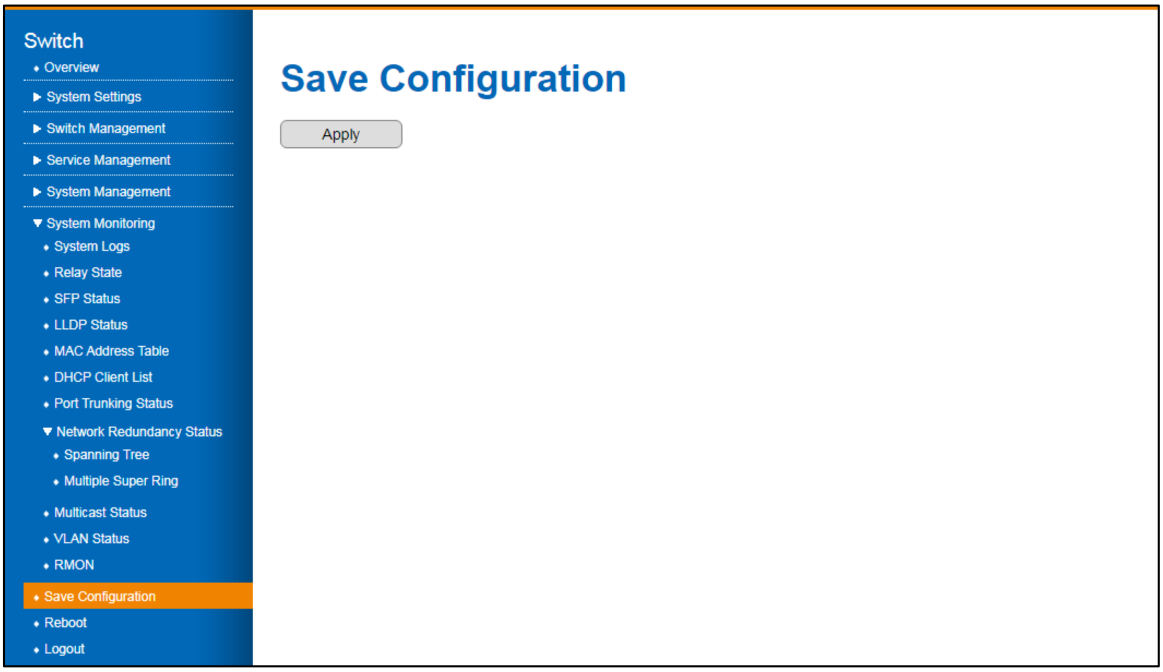


Figure 66 Save Configuration

Item	Description
Apply	Click **Apply** to save the setting permanently to the system’s flash.

3.9. Reboot

The Reboot screen allows for a reboot of the device. Some of the feature changes require you to reboot the system. Click on Reboot to reboot your device.

Note: Any settings not permanently saved to the system's flash will be deleted. Use the Save Configuration function to save any settings before rebooting the system.

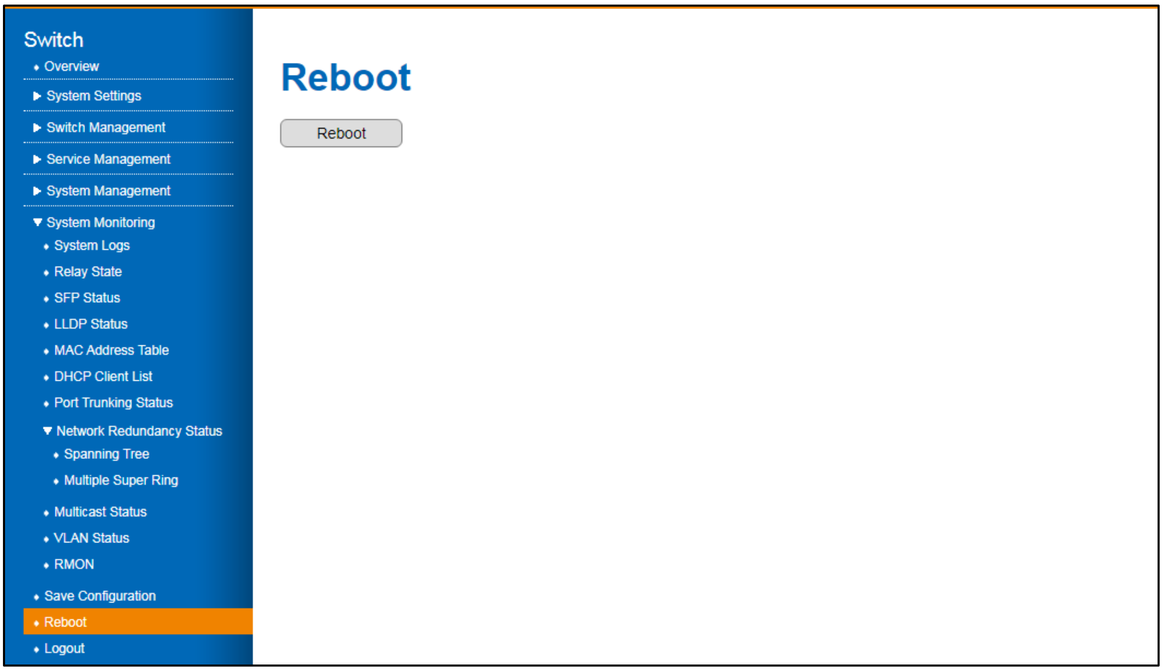


Figure 51 System Monitoring > Reboot Menu

Item	Description
Refresh	Click **Reboot** to initiate a reset of the system.

3.10. Logout

By default, the system logs out after 300 seconds of inactivity. You can change this default value as described in the Console Settings Session Timeout section.

From the main menu, click **Logout** to logout the current profile.