PAKEDGEDEVICE&SOFTWARE INC.

SX Series Switches

ENTERPRISE-CLASS, FULLY MANAGED SWITCHES WITH POE

USER MANUAL

VERSION 1.1

FCC Declaration of Conformity

Pakedge Device & Software, Inc., 2847 Breakwater Avenue, Hayward, CA, declares under sole responsibility that the SX series switches comply with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. These devices comply with Part 15 of FCC Rules. Operation of the devices is subject to the following two conditions: (1) These devices may not cause harmful interference, and (2) these devices must accept any interference that may cause undesired operation.

WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING WATER. CAUTION: DO NOT OPEN THE UNIT. DO NO PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL. CAUTION: THIS DEVICE MUST BE INSTALLED AND USED IN STRICT ACCORDANCE WITH THE MANUFACTURER'S INSTRUCTIONS AS DESCRIBED IN THE USER DOCUMENTATION THAT COMES WITH THE PRODUCT. WARNING: POSTPONE INSTALLATION UNTIL THERE IS NO RISK OF THUNDERSTORM OR LIGHTNING ACTIVITY IN THE AREA.

Safety Guidelines

Observe the following safety guideline to ensure your own personal safety and to help protect your system from potential damage.

Basic Requirements

1. Keep the device strictly dry while storing, shipping and using;
2. Keep the device from fierce collision;
3. Follow the instructions provided in this manual to install the device;
4. Please contact the specified maintenance staff rather than remove the device on your own if any fault happens.

Environmental Requirements

1. Temperature- Install the switch in a dry area, with ambient temperature between 0 and 40ºC(32 and104ºF). Keep the switch away from heat sources such as direct sunlight, warm air exhausts, hot-air vents, and heaters;
2. Operating humidity -The installation location should have a maximum relative humidity of 90%,non-condensing;
3. Ventilation-Do not restrict airflow by covering or obstructing air inlets on the sides of the switch. Keep it at least10cm free on all sides for cooling. Be sure there is adequate airflow in the room or wiring closet where the switch is installed;
4. Operating conditions-Keep the switch away from nearest source of electromagnetic noise, such as photo copy machines, microwaves, cellphones, etc.

Use Notes

1. Use the provided accessories, such as the cable, mounting kit, etc;
2. Ensure the basic supply voltage standard must be met;
3. Keep the power plug clean and dry in case of electric shock or other dangers;
4. Keep your hands dry while plugging cables;
5. Shutdown the device and power it off before plugging cables;
6. Disconnect the power supply and pull out all cables, such as the power cord, fiber, Ethernet cable, etc.in lightening days;
7. Disconnect the power supply and pull out the plug if the device is out of use for a longtime;
8. Keep the device far from water or other liquids;
9. Contact the specified maintenance staff if any problem occurs;
10. Do not tread on, drag or excessively bend its cable;
11. Do not use worn cables;
12. Do not look the fiber interface in your eyes in case of eye damage;
14. Prevent some matters, such as metals, from entering the device through the ventilation hole;
15. Do not scrape or fray the device's housing shell in case of abnormal operation or human body allergic;
16. Keep the device out of children's reaches.

Cleaning Notes

1. Shutdown the device and pull out all cables before cleaning it;
2. Use soft cloth to clean the device's housing shell.

Environmental Protection

1. Throw the discarded device or batteries into the specified recycling places;
2. Observe local relevant packages, wasted batteries and discarded device processing acts and support recycling action.

CONTENTS

INTRODUCTION

The SX Series 24-port Smart Gigabit PoE Switches provide 24 10/100/1000 Mbps auto-sensing RJ45 ports, 4 1000 Mbps Combo (copper/fiber) ports and one Console port. They support IEEE 802.3af-compliant PDs (15.4W) as well as IEEE802.3at-compliant PDs (30W). In addition, they support VLANs, QoS, DHCP relay, IGMP snooping, ACL, STP, RSTP, MSTP, port mirroring, link aggregation and other features. Aiming at solving the safety problems in LAN, it provides user management classification, management VLAN, ARP attack defense, worm attack defense, DoS attack defense, MAC attack defense, IP+MAC+PORT+VLAN Bind, MAC filter and other safety settings through visual WEB interface operations. With high performance and low cost, they are ideal for residential and enterprise networks.

CUSTOMER SERVICE AND TECHNICAL SUPPORT

Pakedge Device & Software, Inc. is committed to providing you with exceptional support on all of our products. If you wish to speak with one of our representatives, you may contact us at:

Customer Service

Email: **customerservice@pakedge.com**

Phone: **650.385.8701**

Technical Support

Email: **support@pakedge.com**

Phone: **650.385.8703**

Website: **www.pakedge.com**

Visit our website for up-to-date support information.

Please be prepared to provide your product's model and serial number when contacting Pakedge Support. Your model and serial numbers are printed on a label located on the electronic housing.

Pakedge Device & Software, Inc.
3847 Breakwater Avenue
Hayward, CA 94545
USA

Installing

For installation procedures, please refer to the Quick Start Guide that came with the SX switch. You can also visit the dealer portal on our website for all the current manuals and Quick Start Guides.

Note: If you install the switch in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room temperature. Make sure you install the equipment somewhere within the recommended temperature range.

For free-standing installation, make sure that the switch has at least 1.5 in. (3.75cm) of clearance on each side to allow for adequate air flow and cooling.

GETTING TO KNOW YOUR PRODUCT

Package Contents:

- SX Series switch
- Power cord
- Quick Start Guide
- Console Cable
- L-shaped Mounting Kit (2 brackets, screws)

The front panel of the SX switches has several blue LEDs. See Table1 below for more information.

Table 1: Front panel LED explanation from left to right.

LED	Status		Operation
POWER	Blue		The switch is powered on
	Off		The switch is turned off
PoE	Blue		A PoE compliant device is connected to the port
	Off		No PoE compliant device is connected to the port
Ports 1-24	LINK/ACT	Blue	Port is online (link established)
		Flashing Blue	Activity
		Off	No device connected

The rear panel of the SX series switches has several blue LEDs and port connections. See Table 2 below for more information.

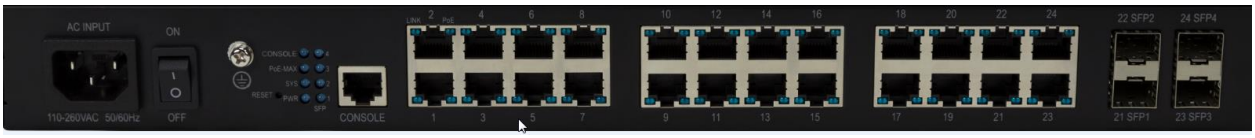


Table 2: Rear panel LED and port connection explanation from left to right.

LED	Status		Operation
RESET	N/A		Reset button. Press and hold for 5 seconds to factory reset the switch
CONSOLE	Blue		Console port is active
	Off		Console port is not active
PoE-Max	Blue		The max PoE budget for the switch has been reached
	Off		The max PoE budget for the switch has not been reached
Sys	Blue		Switch is fully booted
	Flashing Blue		Switch is currently booting
	Off		Switch is powered off
Power	Blue		Switch is powered on
	Off		Switch is powered off
SFP Port 1-4	Blue		SFP port is active
	Off		SFP port is not active
Ports 1-24	Link	Blue	Port is online (link established)
		Off	No device connected
	PoE	Blue	A PoE compliant device is connected to the port
		Off	A PoE compliant device is not connected to the port

Reset Button

To restore factory defaults, press and hold the button for more than 5 seconds when the switch functions correctly. When pressing it for a while, SYS LED will be off and POWER LED is solid. The device will restart and all LEDs will be on. When there booting finished, SYS LED will be blinking, indicating restoring to default factory settings.

Fan

This device has three fans for heat dissipation, one for main board and two for power supply to ensure stable power supply.

Installing the Switch

Installing the Switch in a Rack

To install the switch in a rack, observe the following procedures. To perform this procedure, you need the 19-inch rack-mount kit supplied with switch.

1. Keep the kit well-earthed and stable;
2. Insert the screws provided into the bracket mounting holes to fix brackets on to the switch as shown below.
3. Tighten the screws with the Phillips screwdriver to secure the switch in the rack.

Installing the Switch on a Flat Workbench

If a standard 19-inch rack is not available, place the switch on a clean, flat work bench. Attach the 4 foot pads to corresponding position of the switch bottom to avoid potential sliding and vibration, and ensure good ventilation and proper clearance around the switch for heat dissipation.

⚠**Note**----------

1. Please keep the switch in a dry and well ventilated environment.
2. Keep the work bench stable and well-earthed.
3. Do not restrict airflow covering or obstructing air in lets of the switch. Keep more than 10 centimeters free on all sides for cooling. Be sure there is adequate air flow in the room or wiring closet where the switch is installed.
4. Don’t put heavy articles on the Switch.
5. Make sure there is more than 1.5 centimeters vertical distance free between devices that stack each other.

Connecting SFP fiber combo ports

The small form-factor pluggable (SFP) module is a compact, hot-pluggable transceiver used for optical signal transmission. The module bay is a combo port, sharing a connection with an RJ45 port. Being a combo port, only one type of connection can be active at any given time. For example, both copper and fiber port cannot be used at the same time. If both connectors are plugged in at the same time, the fiber port becomes active. The SFP module accommodates a standard SFP module with an LC connector.

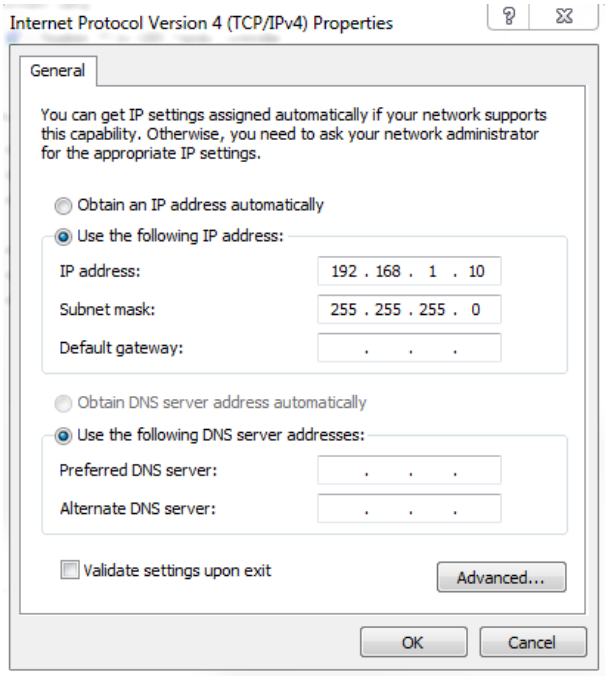
Connecting PoE devices

You may connect PoE powered devices, for example, 802.3at-/802.3af-compliant AP, IP telephone or IP camera, to the switch. By default, the power supply mode is dynamic, PoE power supply is enabled and the power supply standard Is 802.3at.

ACCESSING THE SWITCH

To access the switch's GUI, follow the steps below:

1. If your network currently uses an IP scheme of 192.168.1.X, skip to step 4, otherwise continue to step 2.
2. Plug an Ethernet cable from the switch to your PC.
3. Set your computer to a static IP of 192.168.1.10. The following image is an example of this.

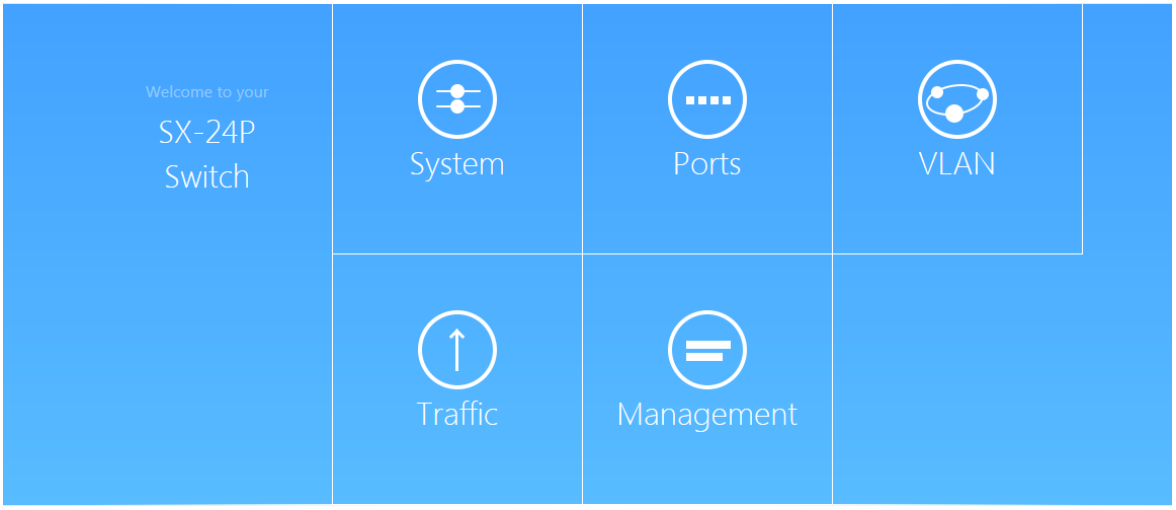


4. Open any internet browser and go to the address http://192.168.1.205. Note: For best results we recommend using Mozilla Firefox as your web browser. If you are using Internet Explorer please use version 9 or newer.
5. Enter the default username **pakedge** and password **pakedges**. Click **Login**.

Note: It is recommended that you change this default password.

DASHBOARD

The dashboard provides frequently used quick links to help with more efficient setup.

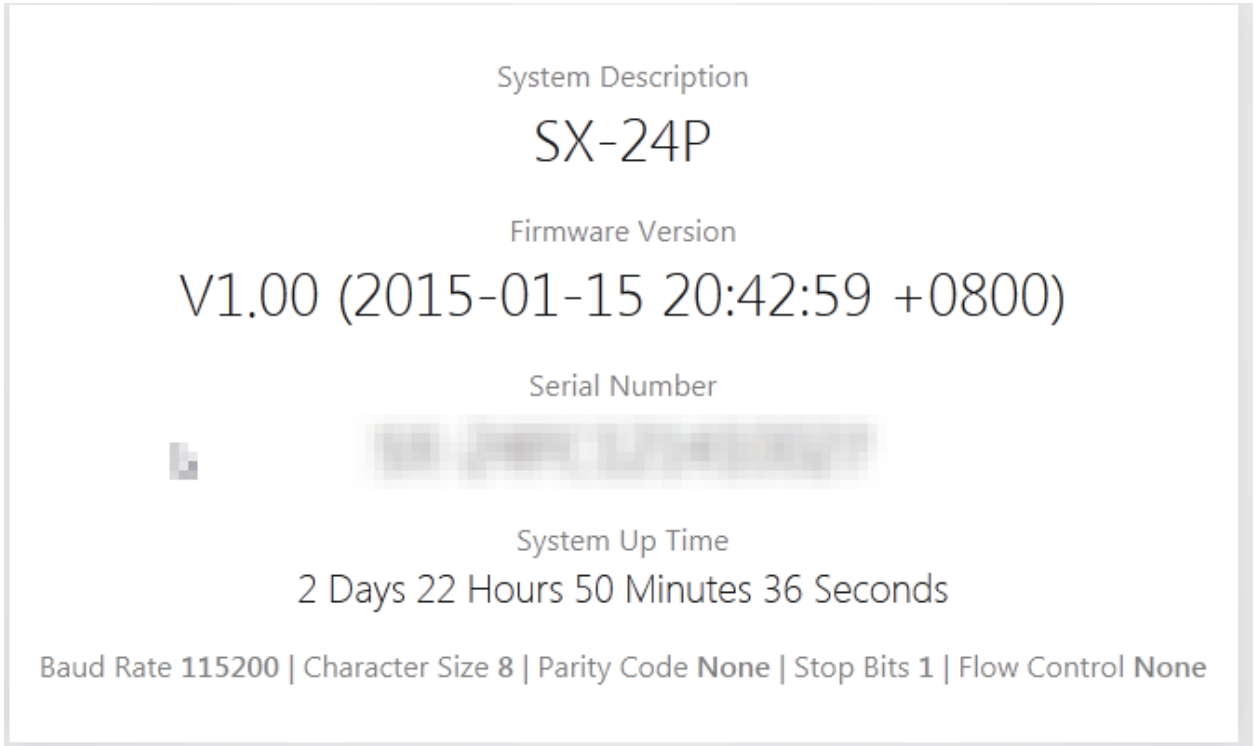


SYSTEM

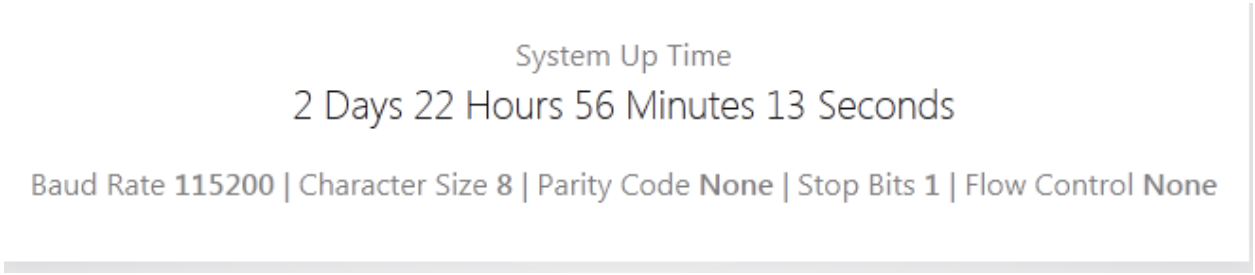
The System section contains the three sub sections System Settings, Security and Time Range Management, each of will be covered next.

BASIC SETTINGS

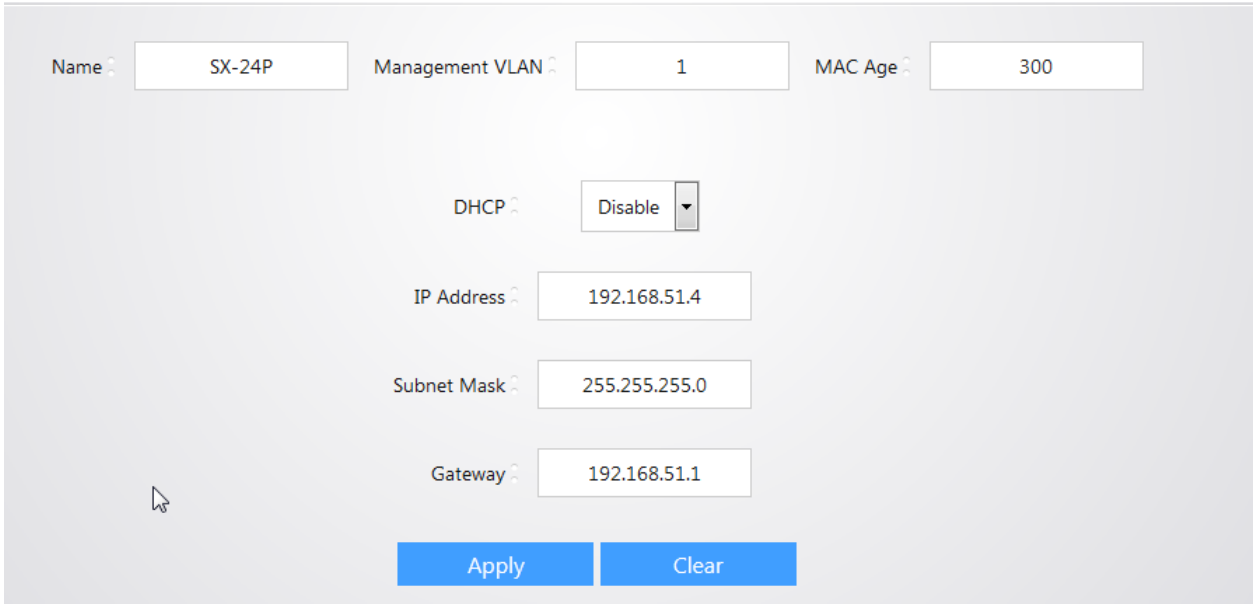
The basic settings page will display the System Description, firmware version, serial number, and system up time.



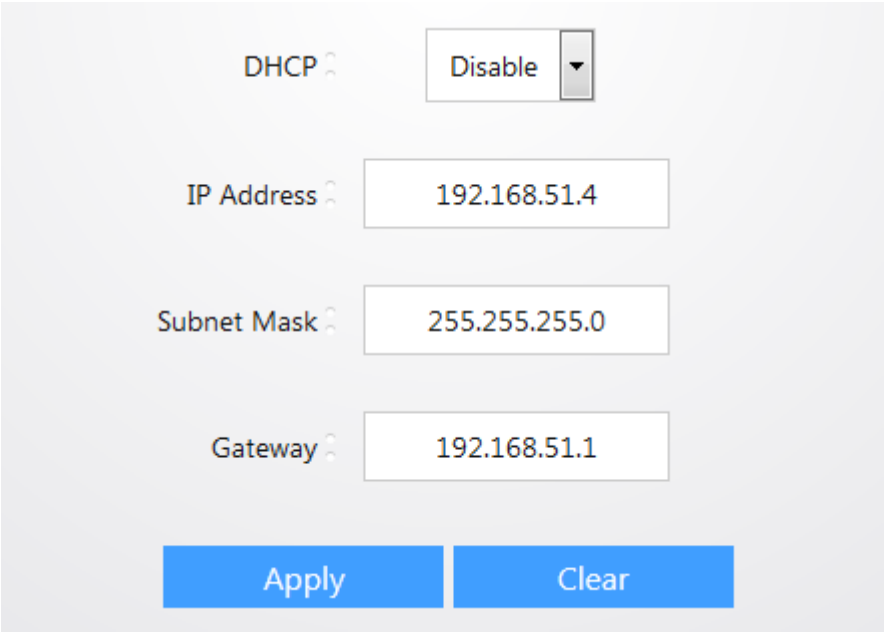
Below the system up time, you will also see the settings to use when consoling into the switch.



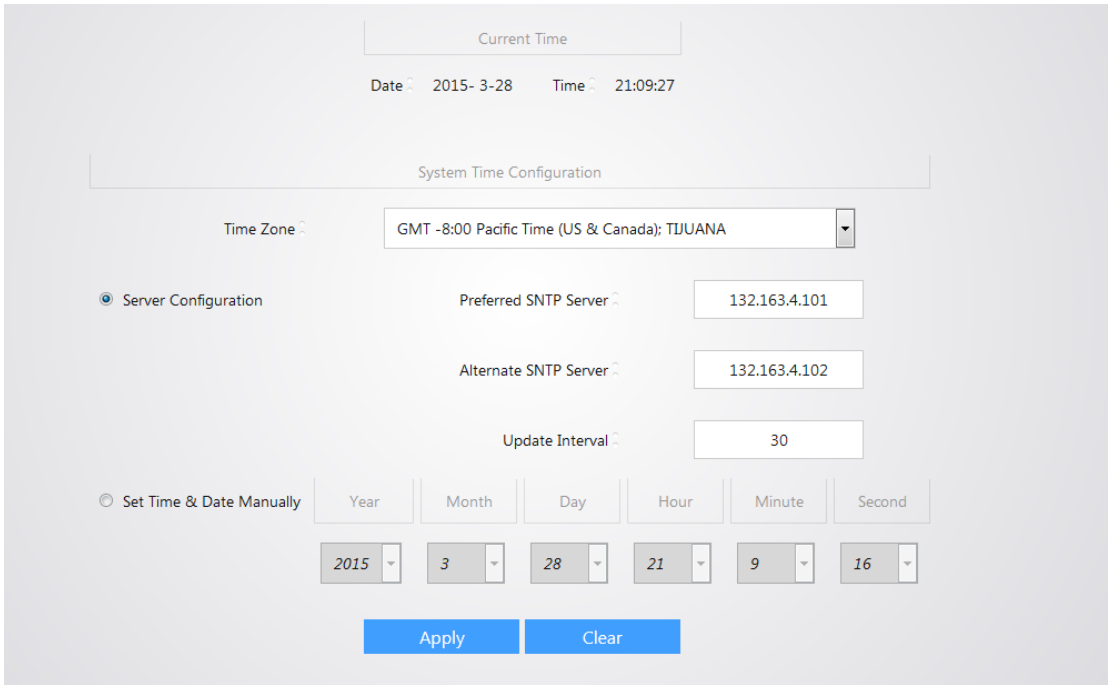
Further down the basic settings page you will find additional settings. The **Name** field indicates the hostname of the switch. The **Management VLAN** indicates the VLAN on which the management GUI of the switch will reside on. The **MAC Age** field indicates how long a mac address that was dynamically learned will be kept in the forwarding table of the switch.



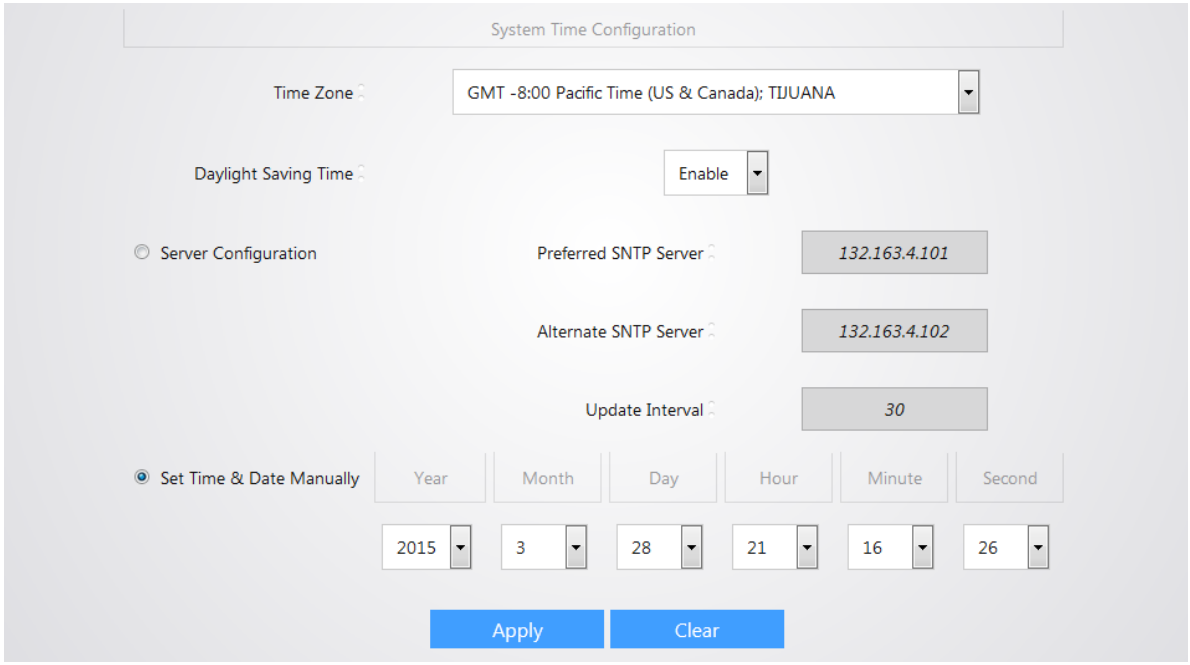
The **DHCP** field can be set to **enable** to allow the switch to obtain its IP address automatically via DHCP. By default, the **DHCP** field is set to disable to allow the switch to use a static IP. To change the IP address of the switch, enter a new IP address into the **IP address** field. You may also change the **subnet mask** and **default gateway** of the switch. Click **Apply** to finalize any setting changes you make on this page.



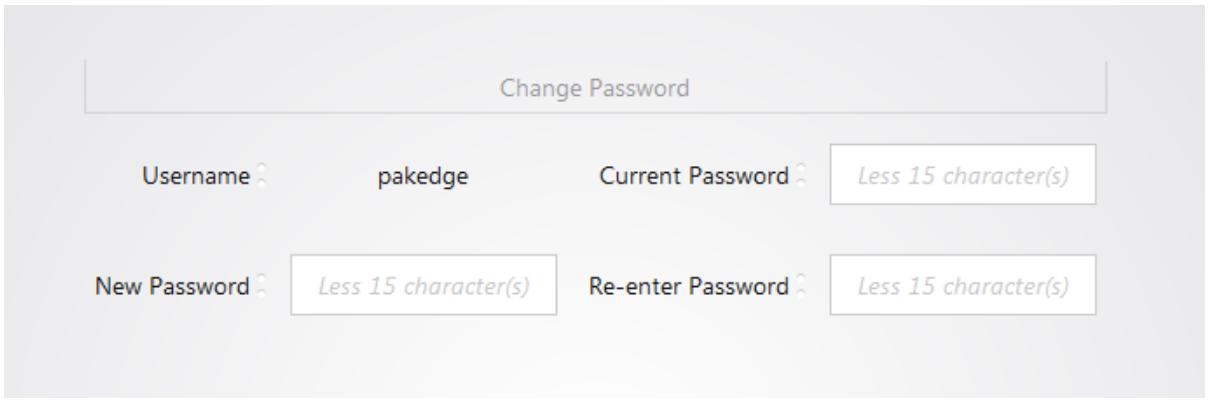
The System time page will display the current time. Use the **Time Zone** drop down menu to set the time zone. Select **Server Configuration** to specify an SNTP server for the switch to use to synchronize its time. You may enter the SNTP server IP address in the **Preferred SNTP Server** field. The **Alternate SNTP Server** provides a backup in case the preferred server is unavailable. The **Update interval** specifies how often the switch will synchronize with the SNTP server.



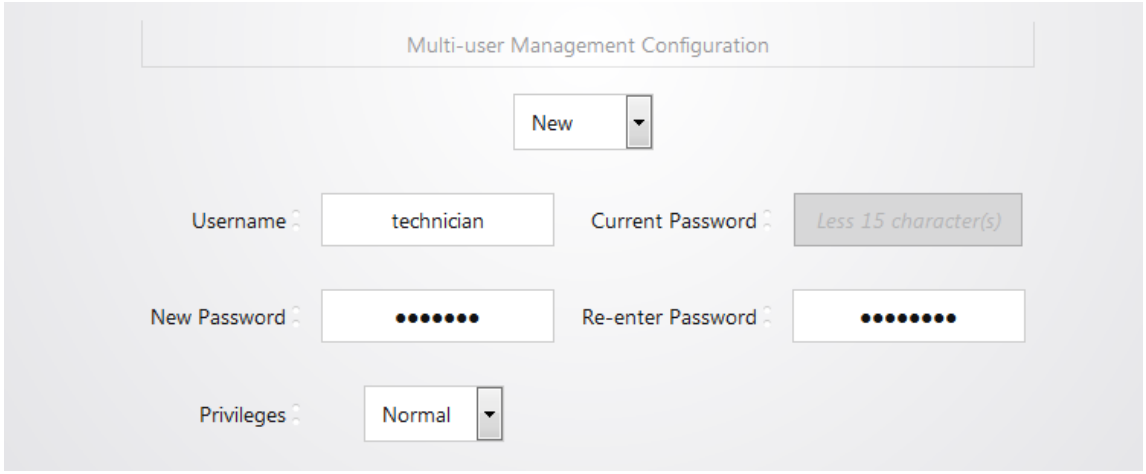
Use the **Set Time & Date Manually** field to manually input the system time. When the system time is manually inputted, you will have an option to enable **Daylight Saving Time**. Set this option to **enable** to have the switch automatically adjust the time when Daylight Savings occurs. Click **Apply** to finalize your settings on this page.



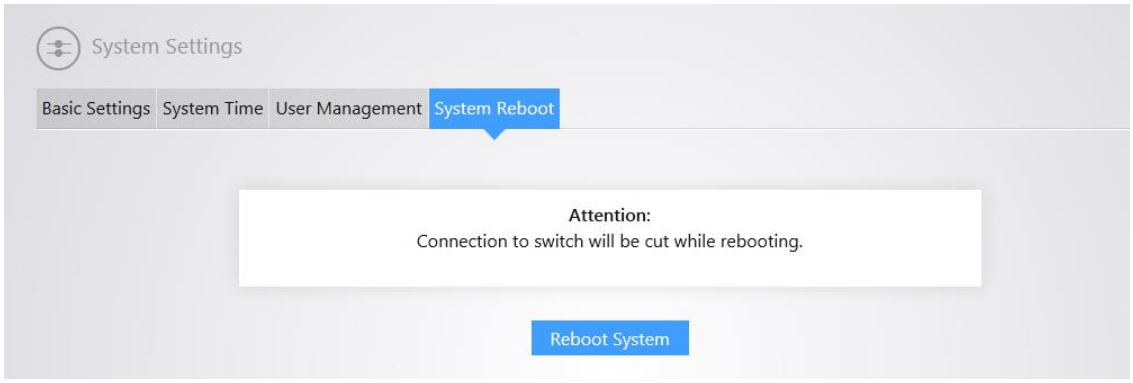
The User Management page allows you to adjust settings to the user accounts that manage the switch. To change the password to the switch, enter the **Current Password** and then enter the **New Password**. You will need to Re-enter the new password. Click **Apply** towards the bottom to finalize the new password.



You can create a new user by New under Multi-user Management Configuration. Enter the new **Username**. Enter a password under the **New Password** field. You will need to re-enter the password to confirm. The **Privileges** field allows you to set a privilege level for the new user. **Normal** privilege will allow a user to log into the switch in read only mode. A **Privileged** user can make changes to the switch. Click **Apply** towards the bottom to finalize your settings.



The System Reboot page allows you to reboot the switch. Click **Reboot System** to perform a reboot.



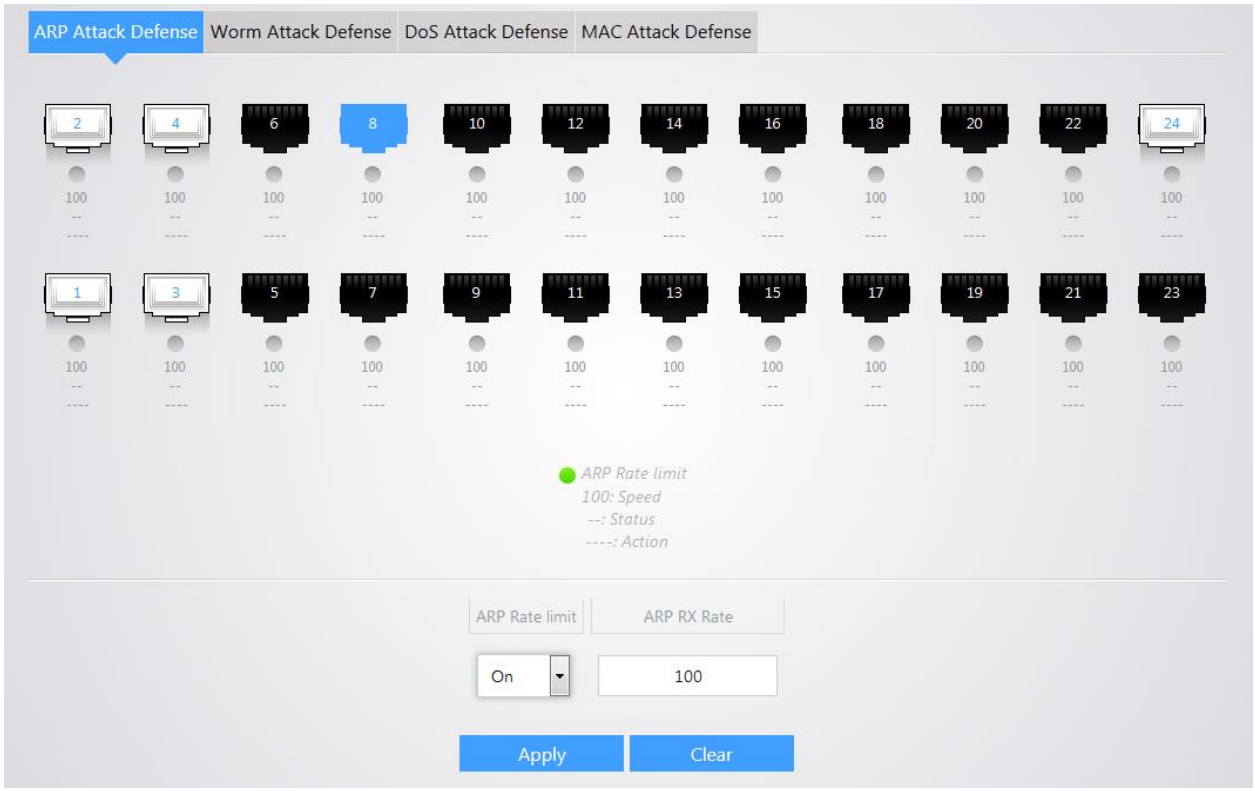
Security

The Attack Defense page has several options for defending against malicious attacks towards on the network.

ARP Attack Defense

If a switch continuously receives an enormous number of ARP messages on a specific port, it will not function properly as CPU is overloaded and, worse still, may break up. ARP rate limit is just designed as a solution to these problems. ARP rate limit enabled ports will enter a protection status and discard all ARP messages received if they exceed the set threshold.

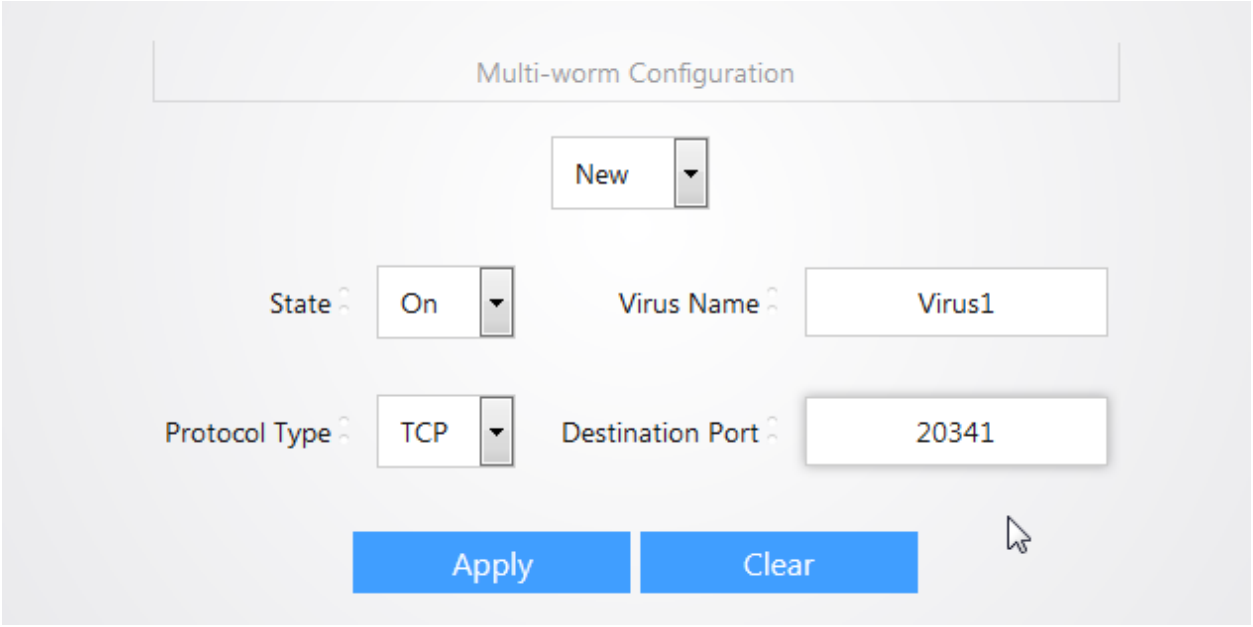
To enable ARP rate limit on a port, select a port, and set the **ARP Rate Limit** to **On**. The **ARP RX Rate** field specifies how the threshold value for ARP messages. Click **Apply** to finalize the settings.



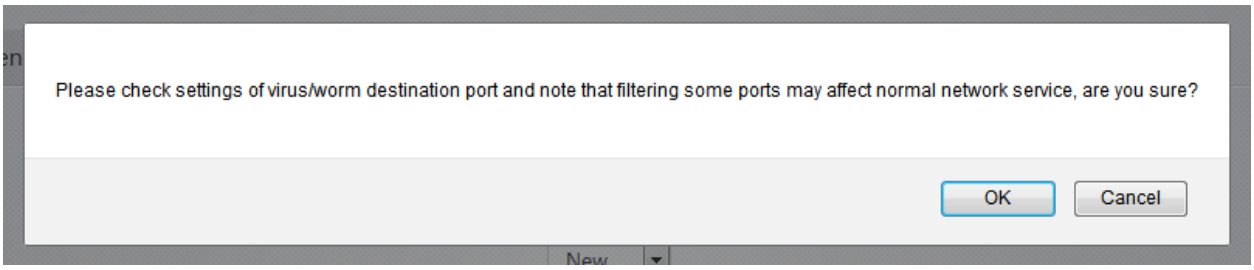
Worm Attack Defense

Worm Attack Defense prevents virus/worm infected PCs being spread to targeted healthy PCs and the whole network by scanning for security failures. Once Worm Attack Defense feature is enabled, the switch directly discards messages that match features of predefined virus so that PC and other network devices will not be infected.

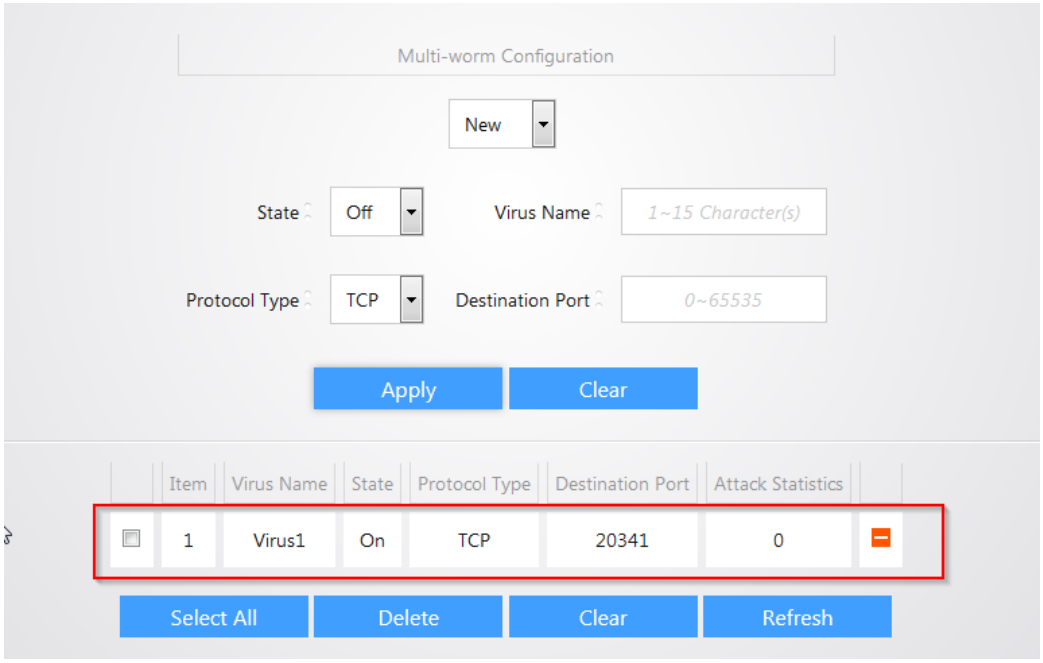
To defend against known viruses, you need to add them to the device and enable the worm attack defense feature. Set the **State** to **On**. Enter a name in the **Virus Name** field. Select the **Protocol Type** that the known virus uses. Set the **Destination Port** number that the virus uses. Click **Apply** to finalize the settings.



You will receive a message stating that network traffic may be affected by enabling this feature. Click **OK**.



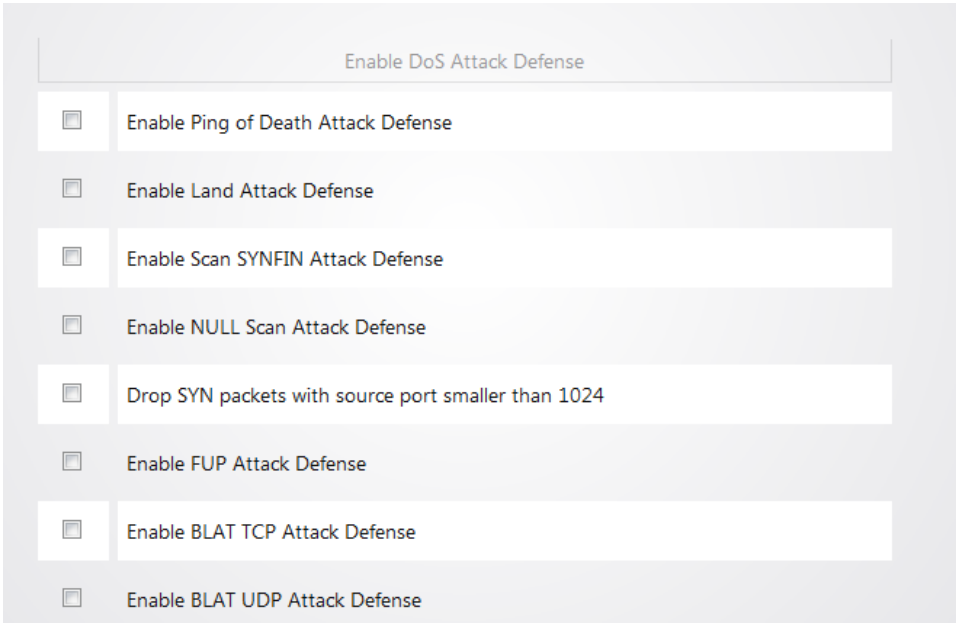
You will see your entry listed at the bottom. You can delete this entry by selecting the check box next to it and clicking **Delete** at the bottom.



DoS Attack Defense

DoS Attack Defense prevents potential attackers from making a machine or network resource unavailable to its intended users by saturating the target machine with large amount of malicious communication requests.

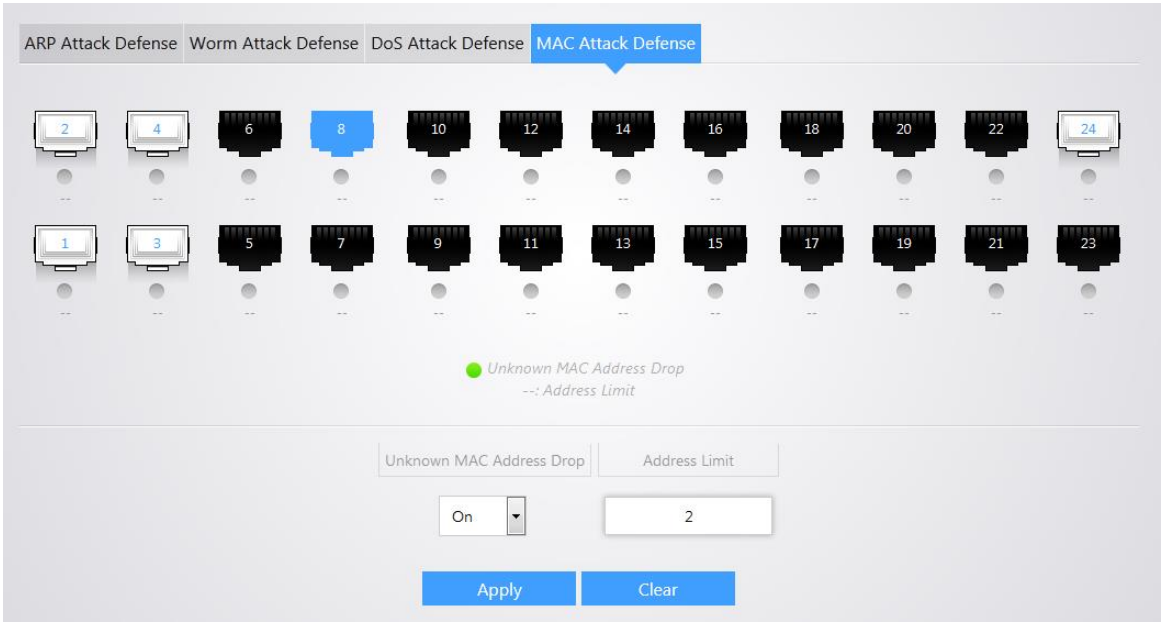
You can enable any of the DoS Attack Defense functions by checking the box and clicking Apply towards the bottom.



MAC Attack Defense

MAC Attack Defense prevents the device from learning large amount of unnecessary source MAC addresses so that forwarding capability will not be degraded due to an oversized MAC address table. The MAC Attack Defense is implemented on the device by limiting the number of MAC addresses that can be learned on each port.

To enable MAC Attack Defense on a port, select a port and set the **Unknown MAC Address Drop** field to **On**. The **Address Limit** field specifies how many mac addresses the switch will keep in its table for that port. Click **Apply** to finalize the settings.

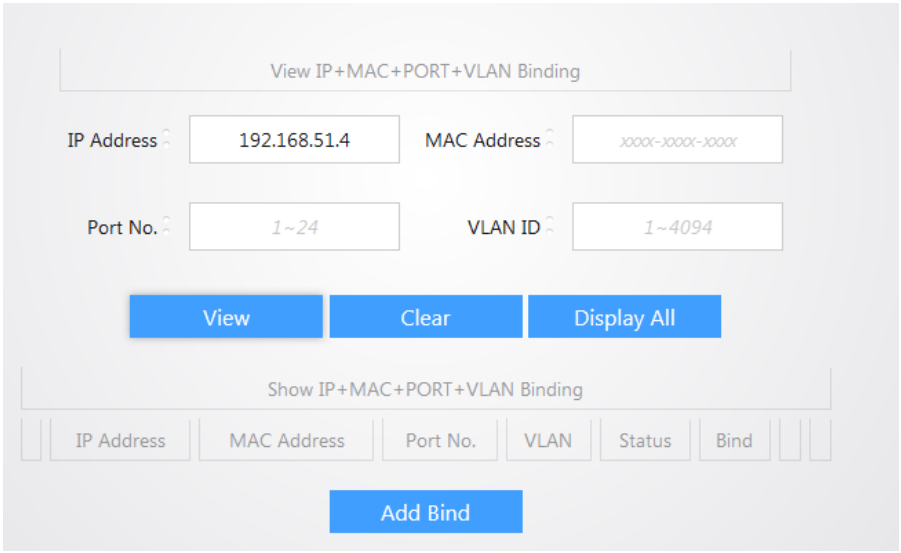


Once enabled, the MAC Attack Defense feature will only allow the specified number of dynamically learned MAC addresses to pass through the port. Any data coming from additional MAC addresses will be dropped.

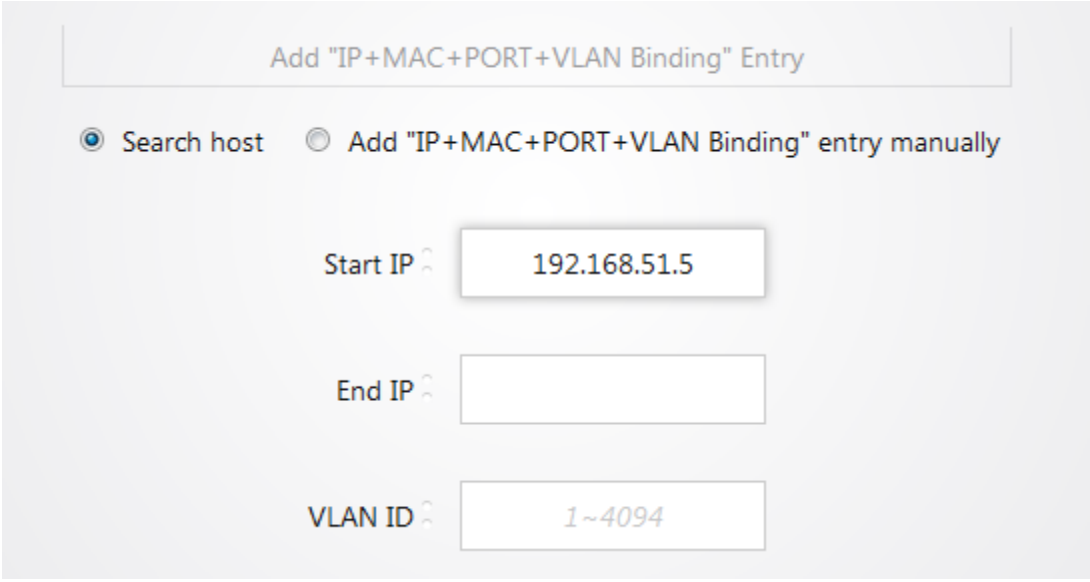
IP Filter

IP+MAC+PORT+VLAN Bind allows you to bind a device to a port on the switch based on IP address, MAC Address, Port Number, or VLAN ID.

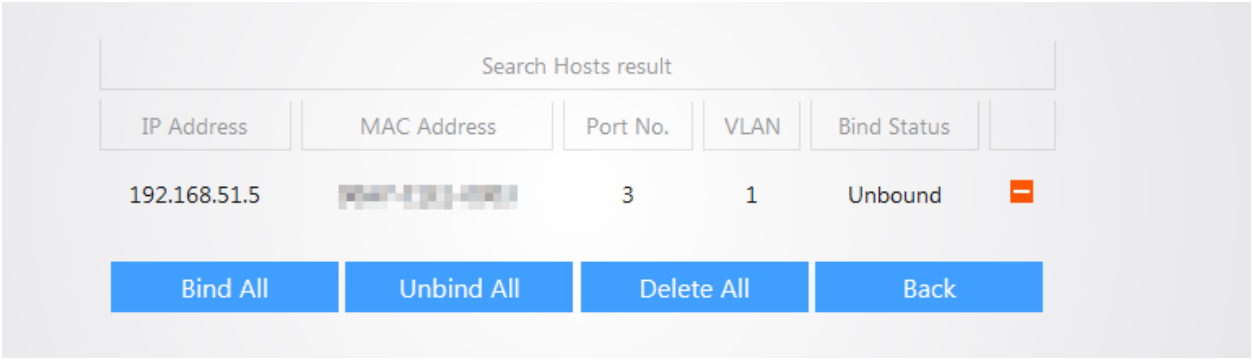
You can view current bindings by entering an IP Address, MAC address, port number or VLAN ID as shown in the following image and clicking on **View**. Any current bindings that match the criteria you entered will be displayed.



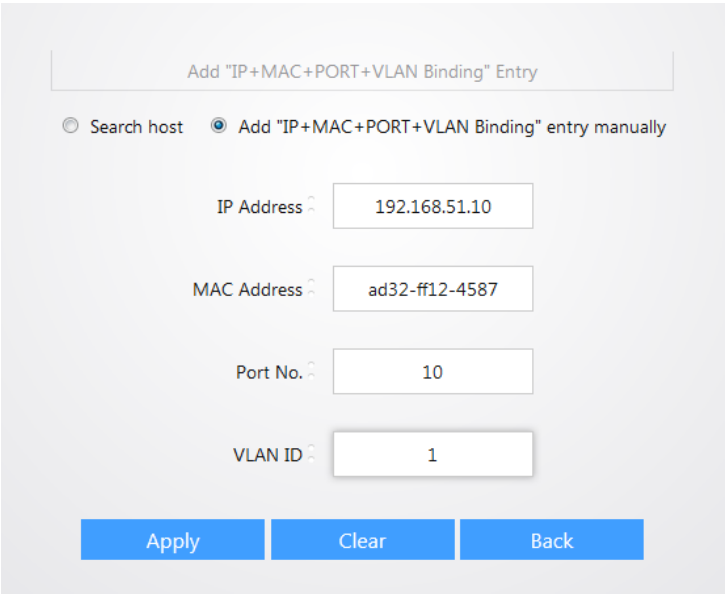
To create a new binding click **Add Bind** towards the bottom. You can enter an **IP address** of the device you want to bind and click **Apply** and the switch will search for that device



Once the switch has found the device, it will display the MAC Address, port number, and VLAN. You can then click **Bind All** to have the switch finalize the binding. The device is now bound to the port it is connected to.

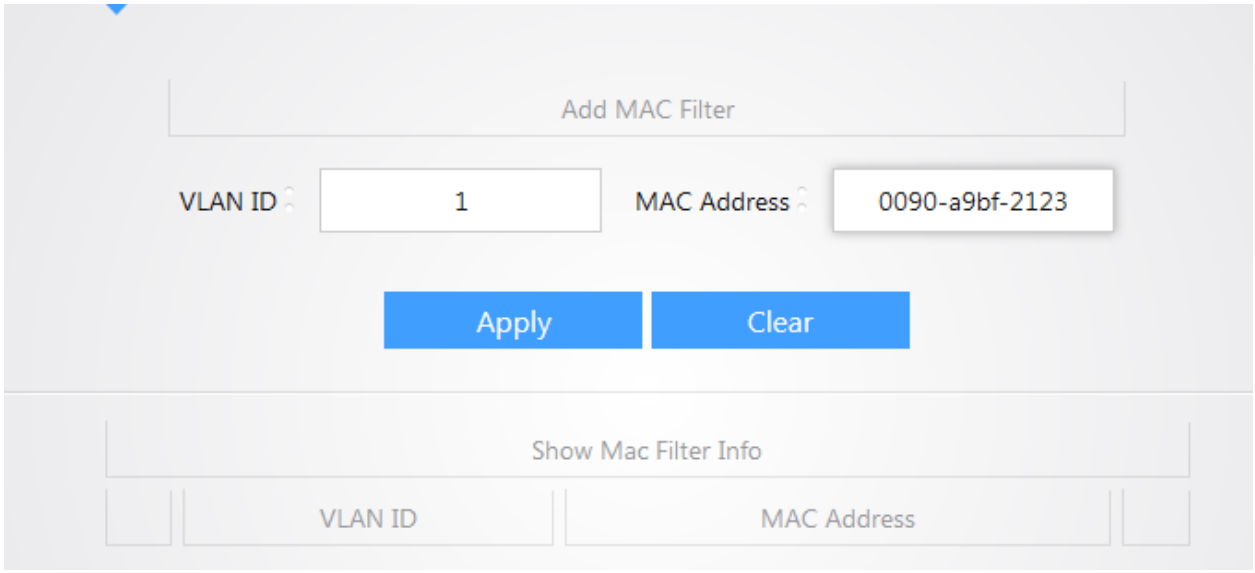


You can manually add an entry and specify the **IP address**, **MAC Address**, **Port Number**, and **VLAN ID**. Click **Apply** to add the entry.



MAC Filter

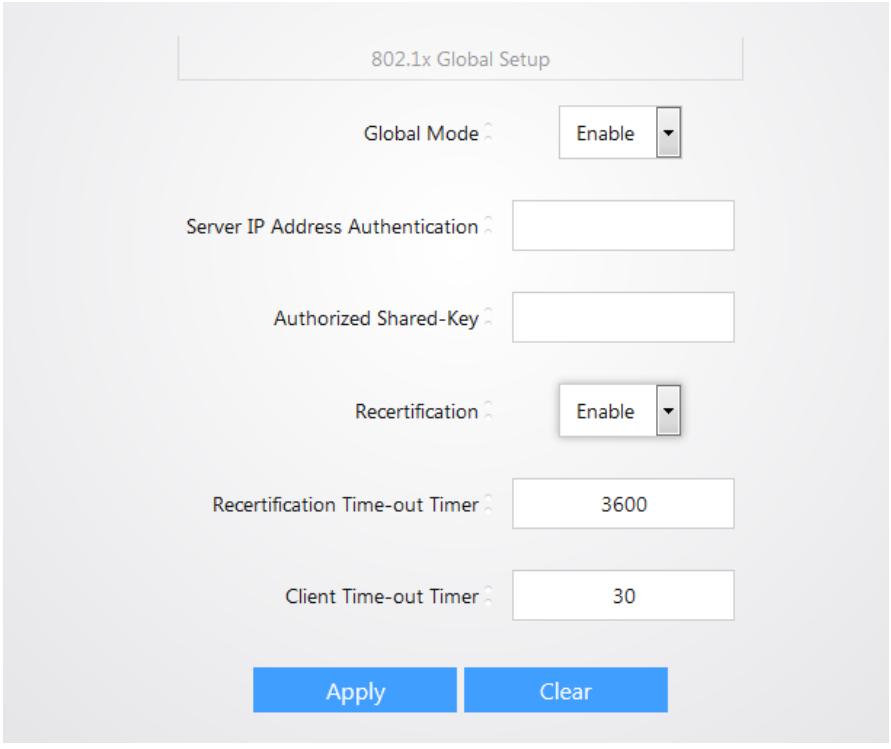
Once MAC filter settings are configured on this device, the device will check source and destination MAC addresses of ingress packets. If source and destination MAC addresses already exist in the MAC filter table, these packets will be discarded. To add an entry, enter the **VLAN ID** and **MAC Address**. Click **Apply** to add it to the switch.



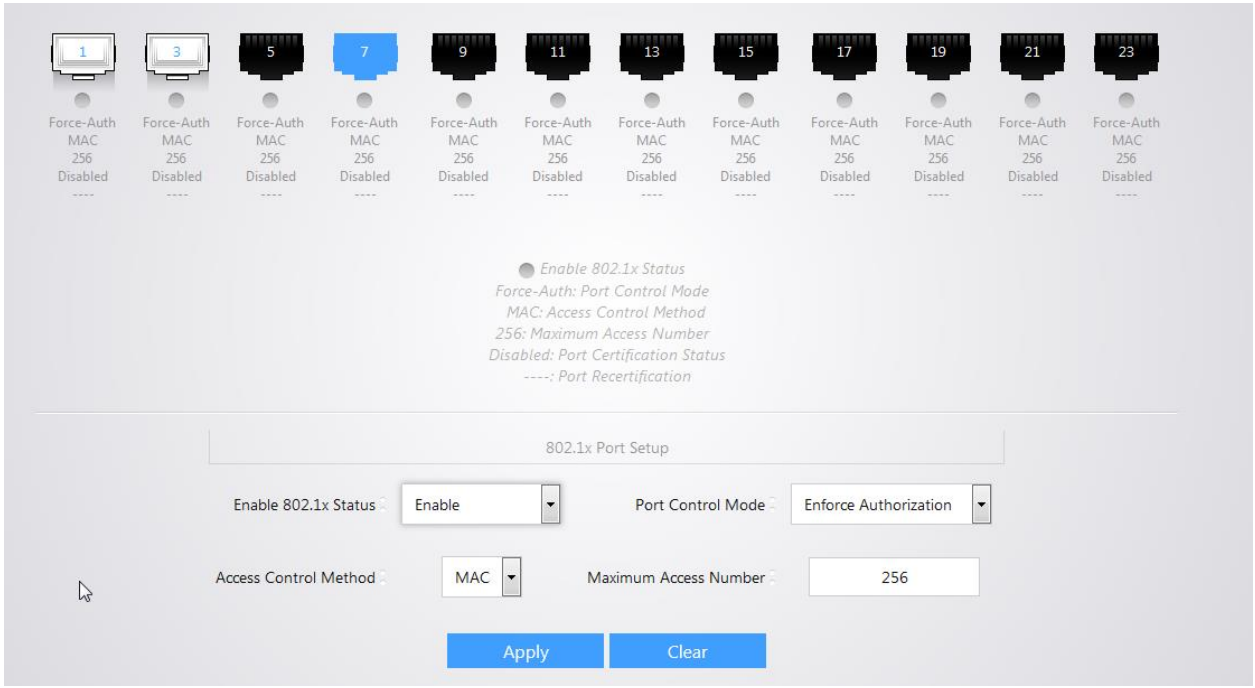
802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices wishing to attach to a LAN or WLAN. IEEE 802.1X defines the encapsulation of EAP over LAN" or EAPOL. 802.1X authentication involves three parties :a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN-though the term “supplicant” is also used interchangeably to refer to the software running on the client that provides credentials for the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as username/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

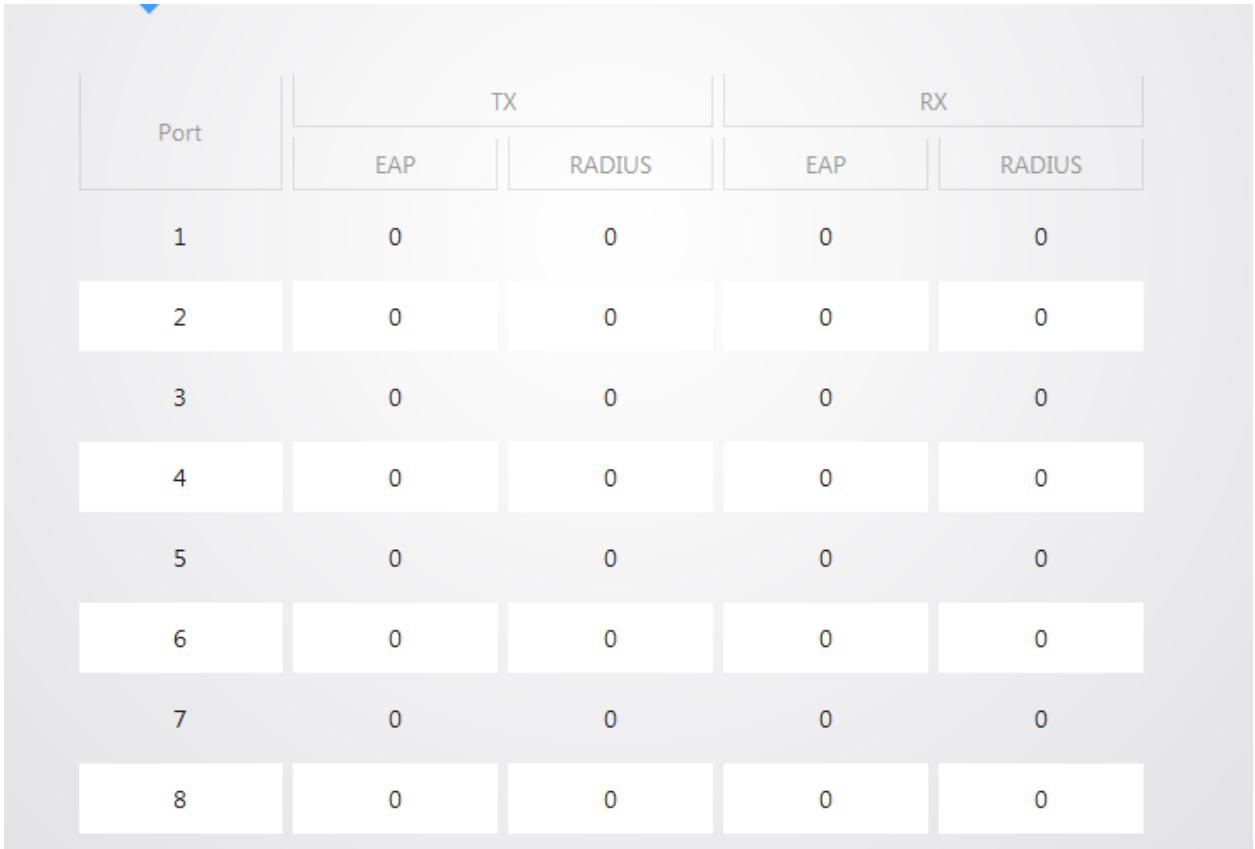
To enable 802.1X set **Global Mode** to **Enable**. The **Server IP Address Authentication** field specifies a valid authentication server on the network. The **Authorized Shared-Key** specifies the shared key that is configured on the server. The **Recertification** field specifies whether to enable or disable re-authentication on all ports. **Recertification Time-out Timer** specifies the interval for a device to initiate an 802.1X re-authentication. The **Client Time-out Timer** field specifies how long the switch will wait for a response on a Request/Challenge request from a client. Click **Apply** to finalize the settings.



The Port setup page allows you to configure individual port settings for 802.1X. Select a port and then you can configure individual port settings towards the bottom. The **Enable 802.1X Status** field specifies whether 802.1X is enabled on a port. **Port Control Mode** specifies whether to enforce authorization or not. The **Access Control Method** specifies whether you are using a port or MAC Address for the control method. **Maximum Access Number** field specifies the maximum number of MAC addresses that may authenticate to a port. Click **Apply** to finalize the settings.



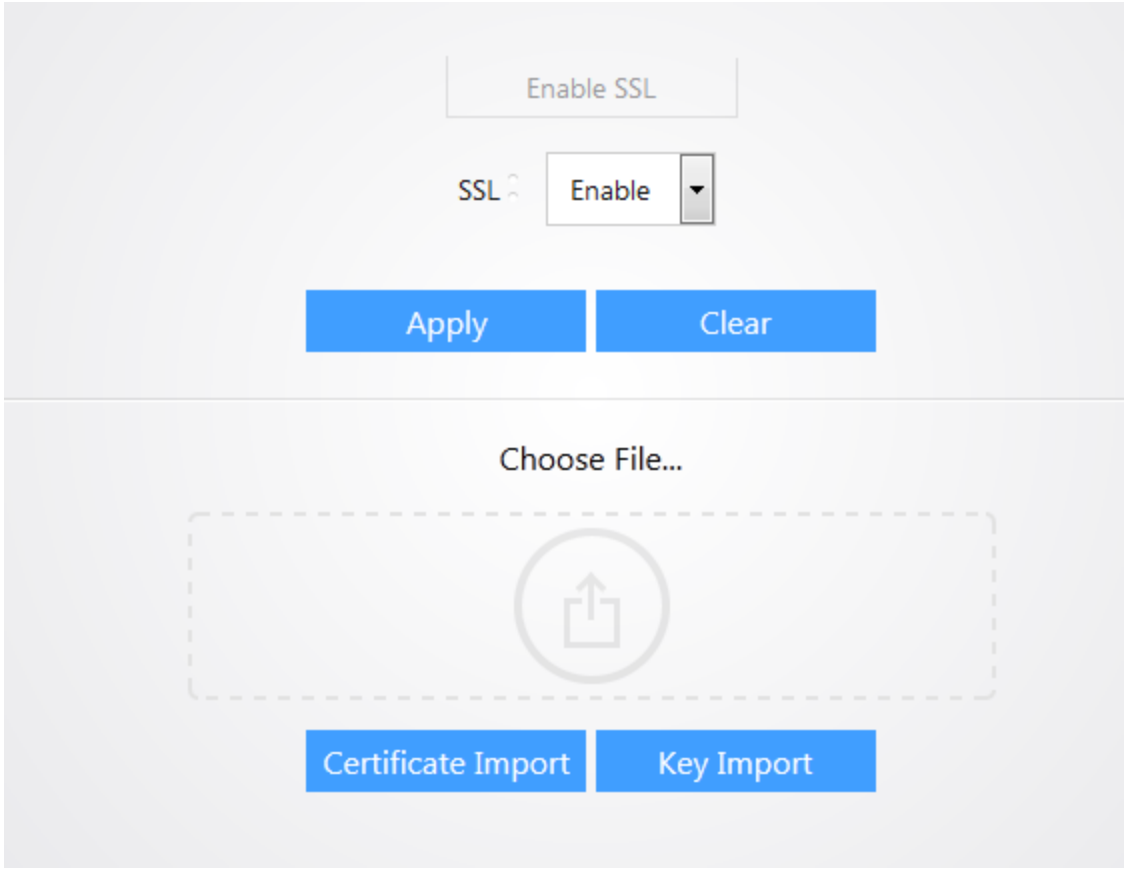
The Port Statistics page will display sent and received data from the authentication server on the network.



Port	TX		RX	
	EAP	RADIUS	EAP	RADIUS
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

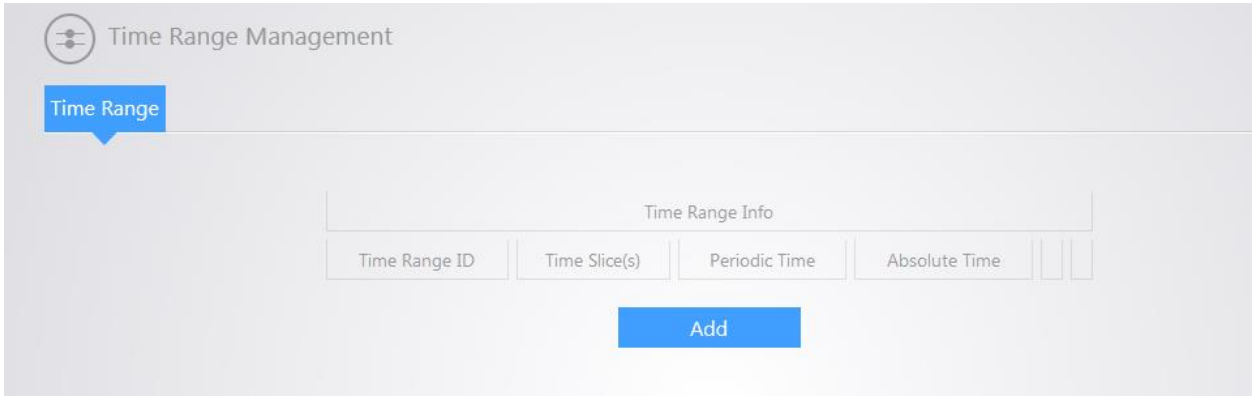
SSL Certificate

SSL Certificate allows you to import an SSL certificate to the switch. Set the **SSL** field to **Enable**. Click **Apply** to finalize the settings. Use the **Certificate Import** and **Key Import** to import certificates and keys into the switch for use with SSL.

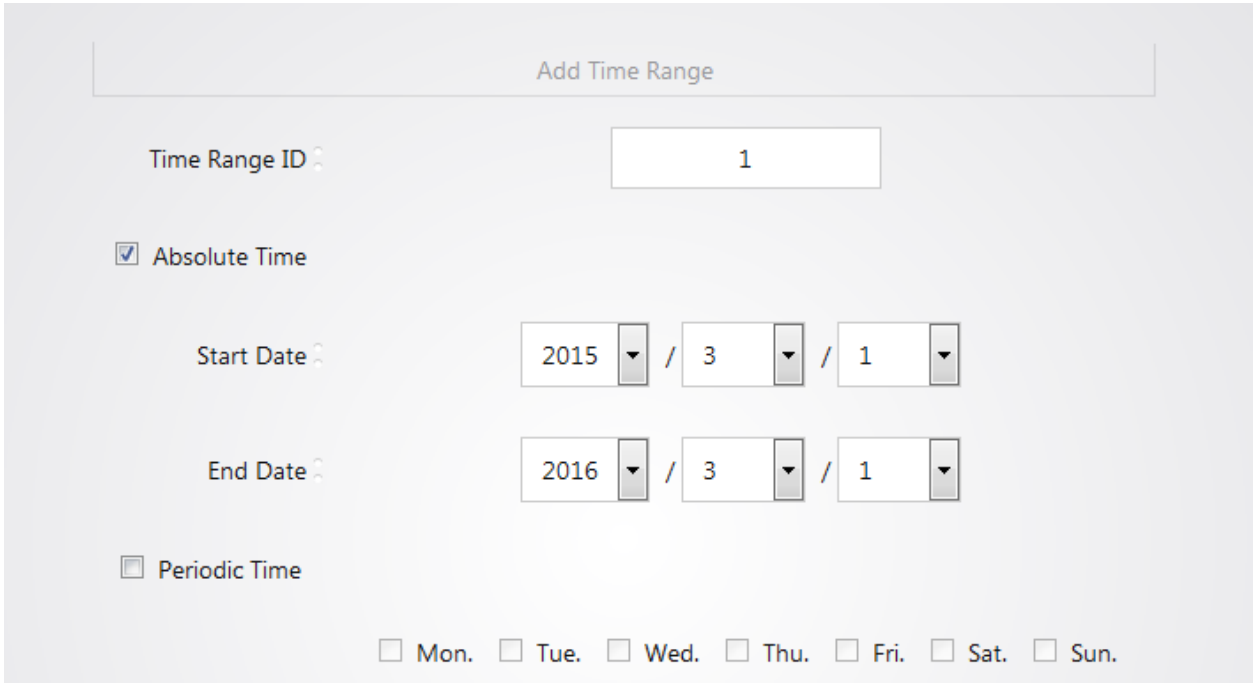


TIME RANGE MANAGEMENT

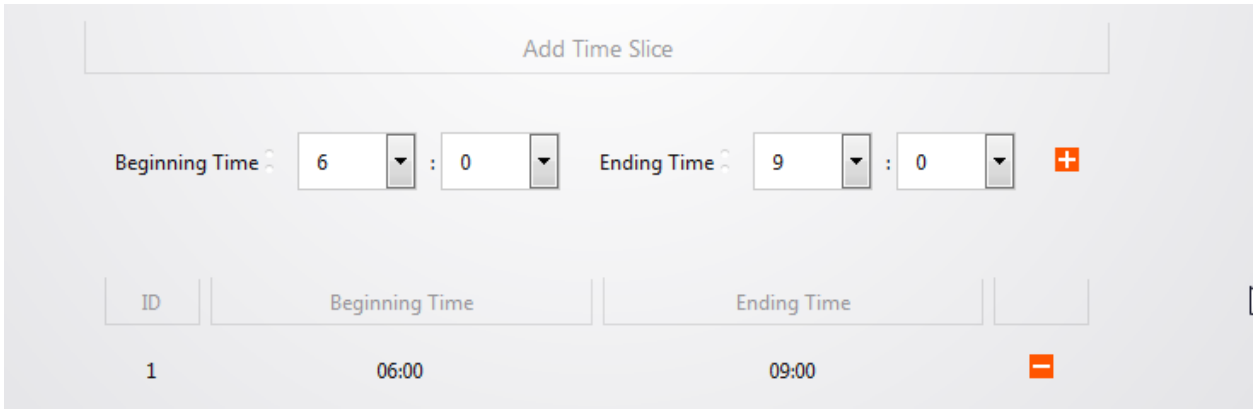
The Time Range Management page allows you to create a schedule that can be applied to ACLs or PoE settings. Click Add to create a new Time Range Entry.



Enter a **Time Range ID**. It can be between 1-100 and is used only for identifying this entry. **Absolute time** allows you to specify a time period for which this entry is active. **Periodic time** allows you to specify which days of the week this entry will be active for.



Towards the bottom, specify a **Beginning Time** and **Ending Time** for this entry. Click the plus symbol next to **Ending Time** to add the time range to this entry. Click **Apply** to finalize the settings.



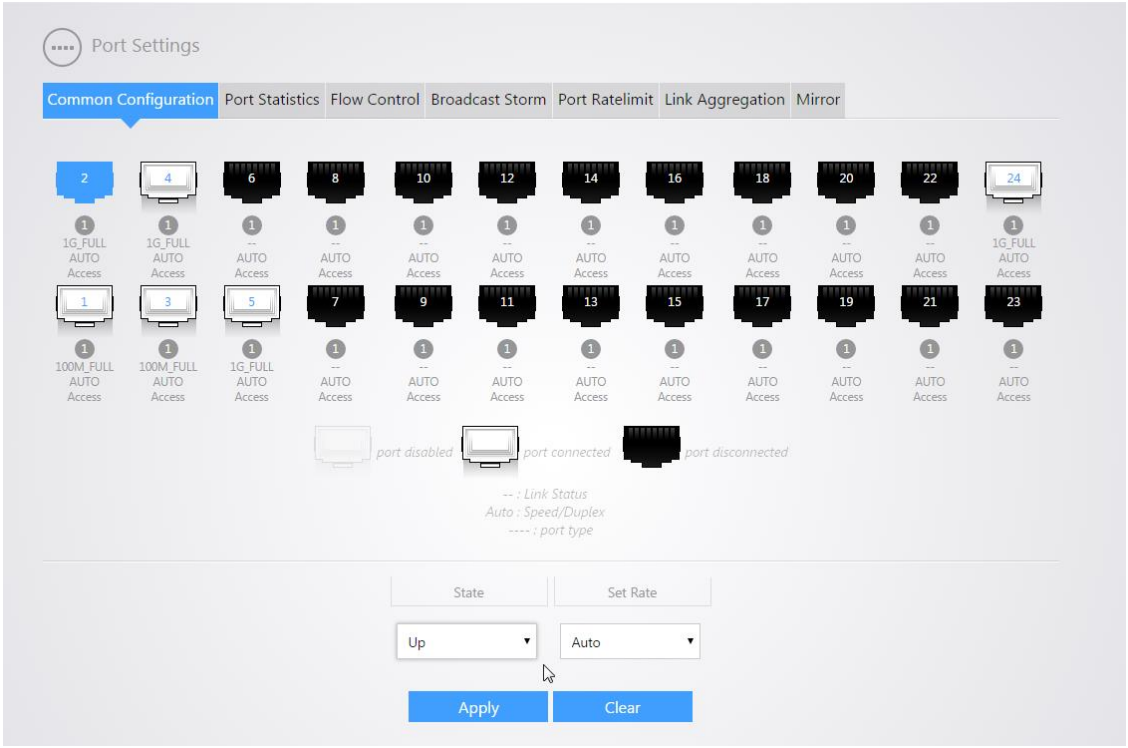
PORTS

The Ports section contains three subsections, each will be covered next.

PORT SETTINGS

Common Configuration

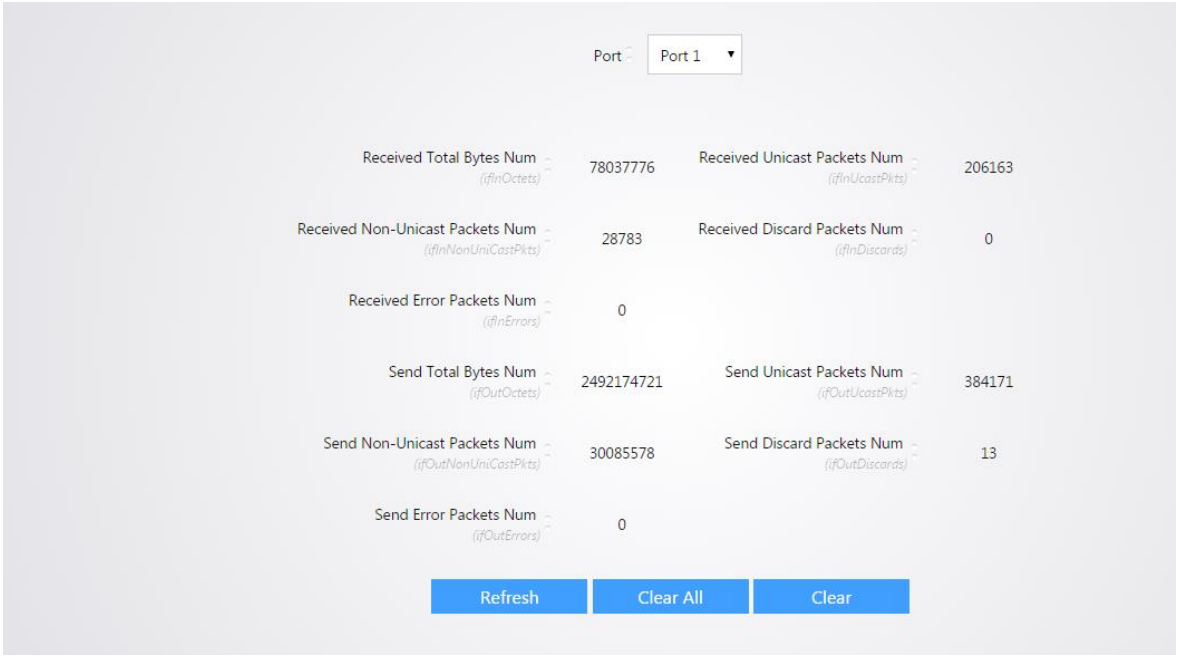
The common configuration page will allow you to change a port state or port speed. You can simply click on a port to highlight it and then change the port **State** or **Set Rate** down below. Click **Apply** to finalize your settings.



You may also select multiple ports at one time. The following image illustrates this.

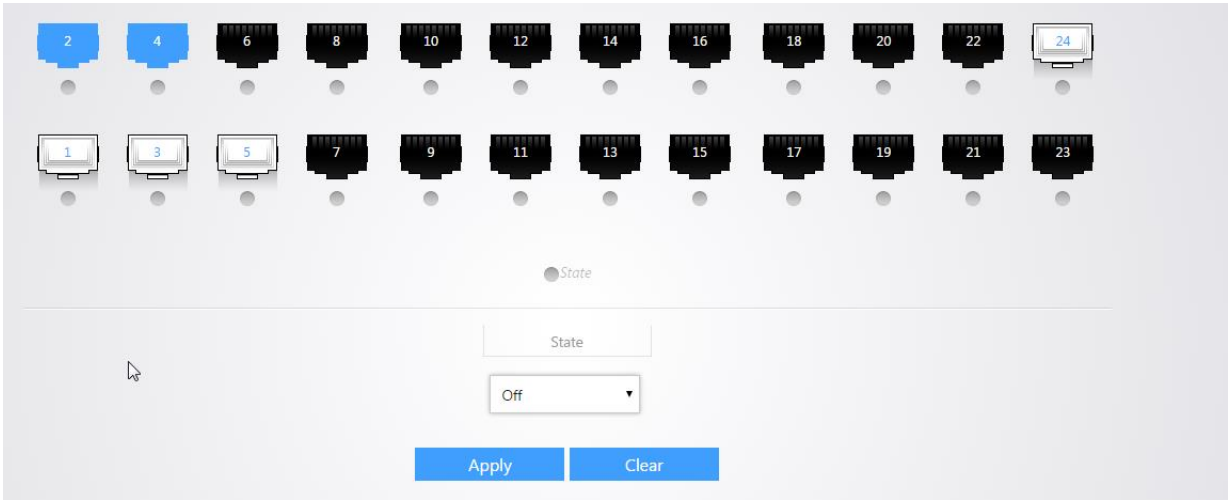
Port Statistics

The port statistics page allows you to see statistics per port. Select a port from the drop down menu towards the top and you will see statistics such as received and sent bytes and even if there are errors on the port. Click **Refresh** to manually update the information on the page. Click **Clear All** to clear the statistics on all ports. Click **Clear** to only clear the statistics of the selected port.



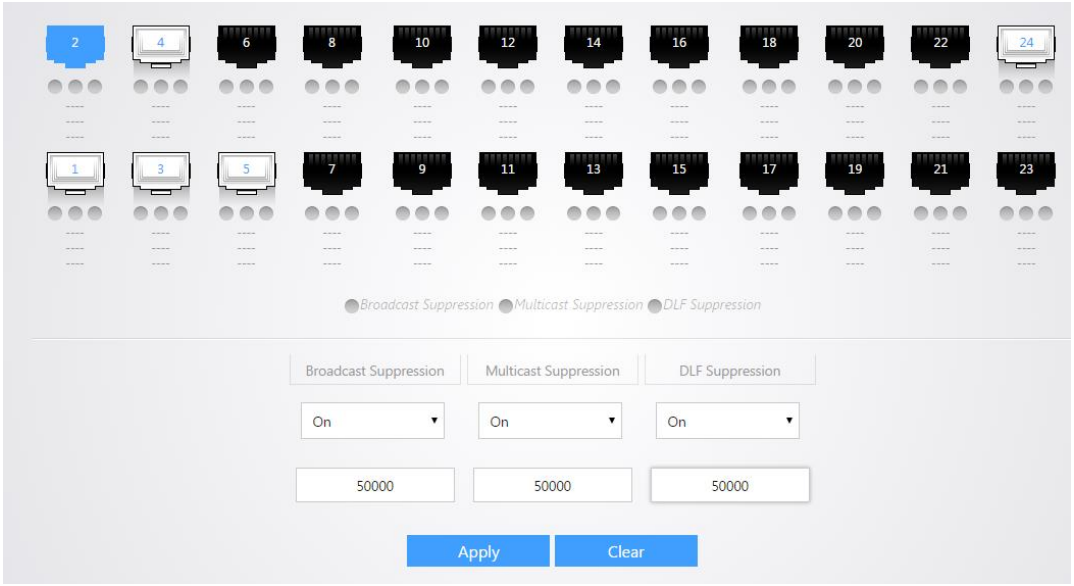
Flow Control

The Flow Control page allows you to enable or disable flow control per port. With flow control enabled on both the switch and its link partner, the switch, when encountering congestion, will send flow control frames to notify the link partner of such; upon receiving such frames, the link partner will temporarily stop sending packets to the switch, thus avoiding packets drop and ensuring a reliable network. Meanwhile, if a certain port receives a Pause frame, it will also stop sending packets out. By default, the flow control feature is disabled. To change the state of flow control select the ports you want to change and then change the **State** down below. Click **Apply** to finalize the settings.



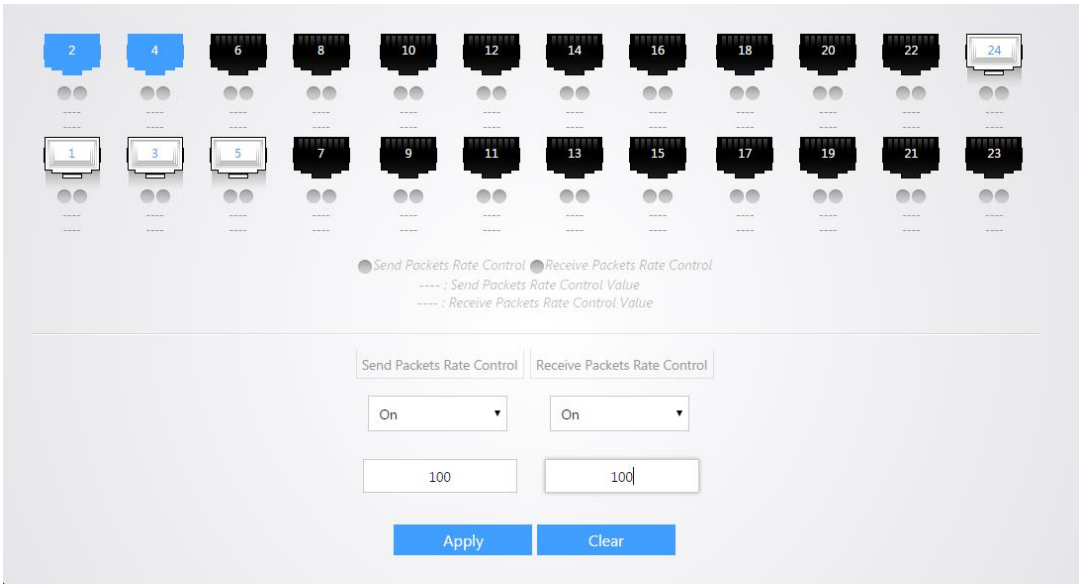
Broadcast Storm

The Broadcast storm page allows you to limit the amount of broadcast or multicast data that is allowed to pass per port. You can also limit the amount of Destination Lookup Failures that the switch is allowed to forward through the switch ports. You can select a port and then set the **Broadcast**, **Multicast** or **DLF suppression** to **On**. Then you will be able to enter a value which defines the amount of data allowed to pass through the port. The value must be in Kbps (kilobits per second). The following image illustrates this. A limit of 50,000 Kbps has been defined for port number two. Click **Apply** to finalize your settings.



Port Ratelimit

The Port Ratelimit page will allow you to define how much data is allowed to pass through a port on the switch. You can select ports and then towards the bottom set the **Send Packets Rate Control** and **Receive Packets Rate Control** to **On**. Then you can enter the amount of data, in megabits per second that the switch should allow to pass through. The following image illustrates this. A limit of 100 mbps has been defined for ports two and four. Click **Apply** to finalize your settings.



Link Aggregation

Link aggregation groups multiple Ethernet ports together in parallel to act as a single logical link. Aggregation-enabled devices treat all physical links (ports) in an aggregation group entirely as a single logical link (port). Member ports in an aggregation group share egress/ingress traffic load, delivering a bandwidth that is multiple of a single physical link. Link aggregation provides redundancy in case one of the links fails, thus reliability could be maintained.

Static Aggregation

For static aggregation, you must manually maintain the aggregation state of the member ports as system does not allow adding a new port or deleting any existing member port. Down to 2 member ports must be included in a single aggregation group. LACP is disabled on the member ports in static LACP mode. Ports in static aggregation group must all be of the same port speed and will stay in forwarding state. In case a certain port is set to a different speed, packets on it will be forwarded at the actual connection speed. The rate of the aggregation group equals the total rate of its member ports.

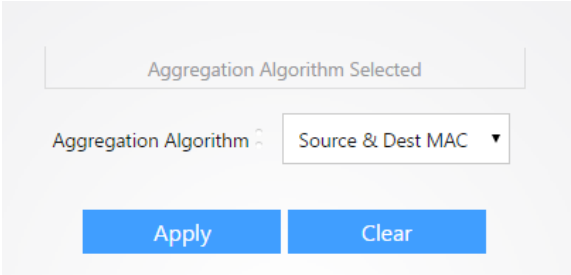
LACP

For LACP aggregation, you must manually maintain the aggregation state of the member ports. Whether ports in LACP group are aggregation ports or not is determined by LLDPBU frame auto-negotiation. Down to 2 member ports must be included in a single aggregation group. LACP is enabled on the member ports in LACP mode. Ports in an LACP aggregation group may stay either in a forwarding status or a blocked status. Ports in LACP aggregation group will be in a forwarding status. If all ports in the aggregation group are not aggregated, only the first port will be in the forwarding status. Ports in forwarding status can send/receive both service packets and LACP frames; ports in blocked status can only send/receive LACP frames.

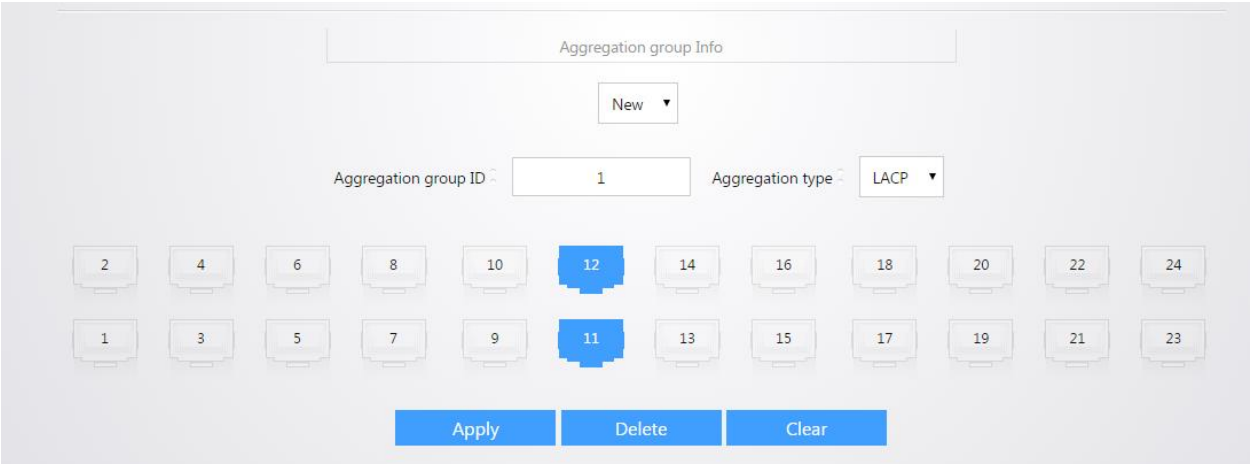
To configure a LACP group, you first must select the aggregation algorithm. The following table describes the different Algorithm options.

Algorithm	Description
Source MAC	Member ports in a link aggregation group share traffic load according to Source MAC addresses.
Dest MAC	Member ports in a link aggregation group share traffic load according to Destination MAC addresses.
Source & Dest MAC	Member ports in a link aggregation group share traffic load according to Source and destination MAC addresses.
Source & Dest IP	Member ports in a link aggregation group share traffic load according to Source and destination IP addresses.

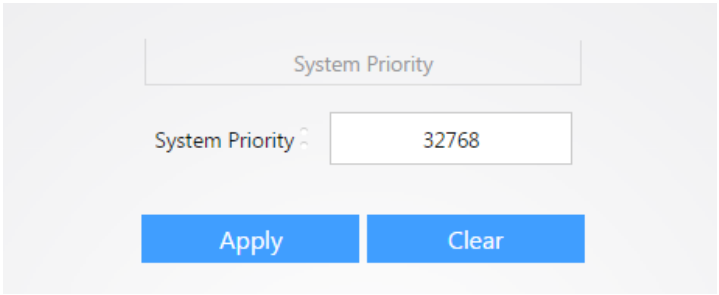
Once you have selected the algorithm you want to use, click **Apply**.



Leave the following drop down menu as **New** and enter an **Aggregation group ID**. Select **LACP** for the Aggregation Type and then select the ports you wish to add to this aggregation group. Click **Apply** to finalize the settings and create the aggregation group.



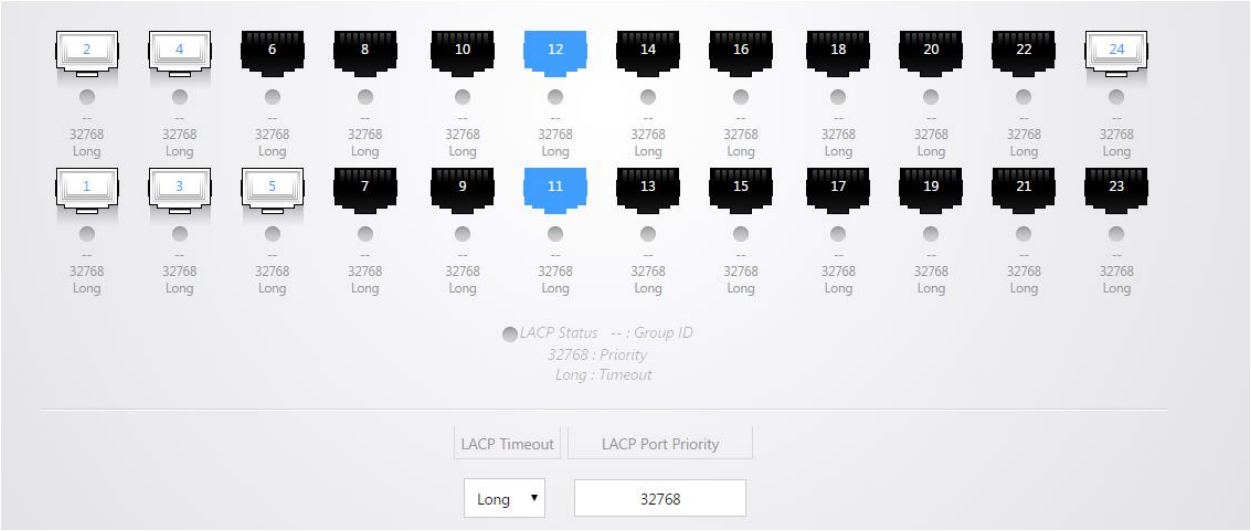
The LACP Protocol page allows you to modify the system priority or the change the LACP timeout setting. To change the **System Priority** you can enter the value you want to use and click **Apply**.



You can modify the **LACP timeout** or **Port Priority** settings. A **Long** timeout indicates that the LACP PDU will be sent every 30 seconds, and the LACP timeout value (when no packet is received from the peer) is 90 seconds. A **Short** timeout indicates that the LACP PDU will send out every 1 second, and the LACP timeout value is 3 seconds.

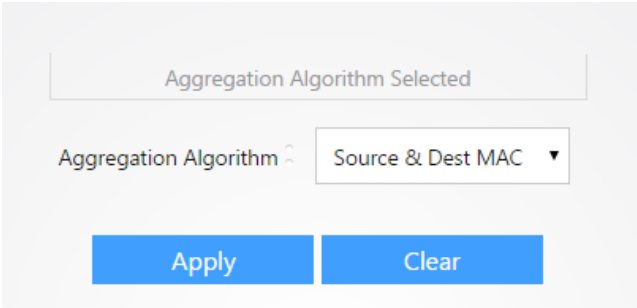
The LACP **port priority** is used to determine which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

You can select multiple ports, and make the changes to the LACP timeout or port priority down below. Click **Apply** to finalize the settings.

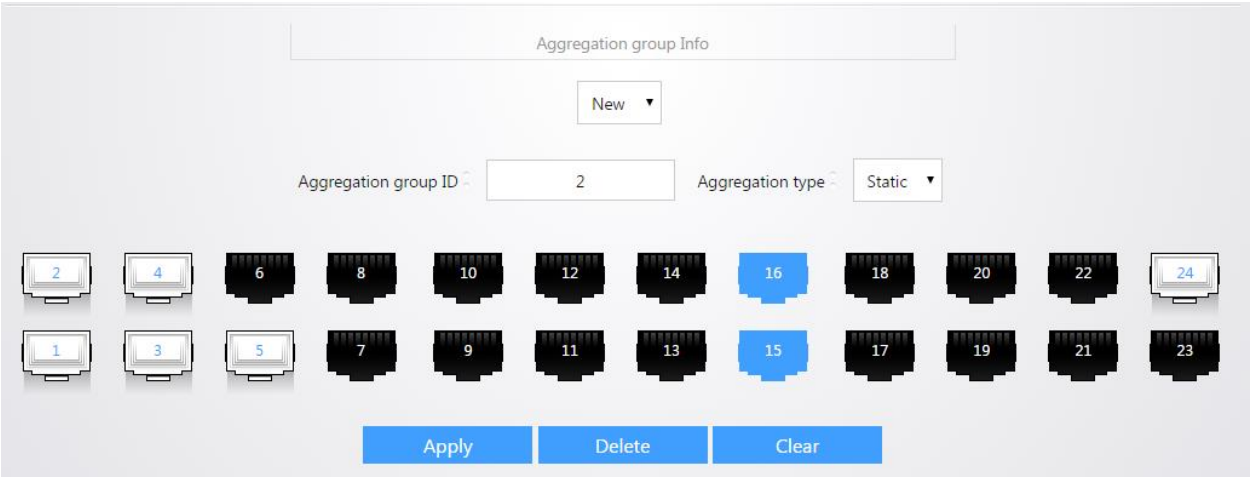


Static Aggregation

To configure a static link aggregation group, you must first select the **Aggregation Algorithm**. Once you have selected the algorithm, click **Apply**.



Leave the following drop down menu as **New** and enter an **Aggregation group ID**. Set the Aggregation Type to **Static**. Select the ports you want to be in the group, and click **Apply**.

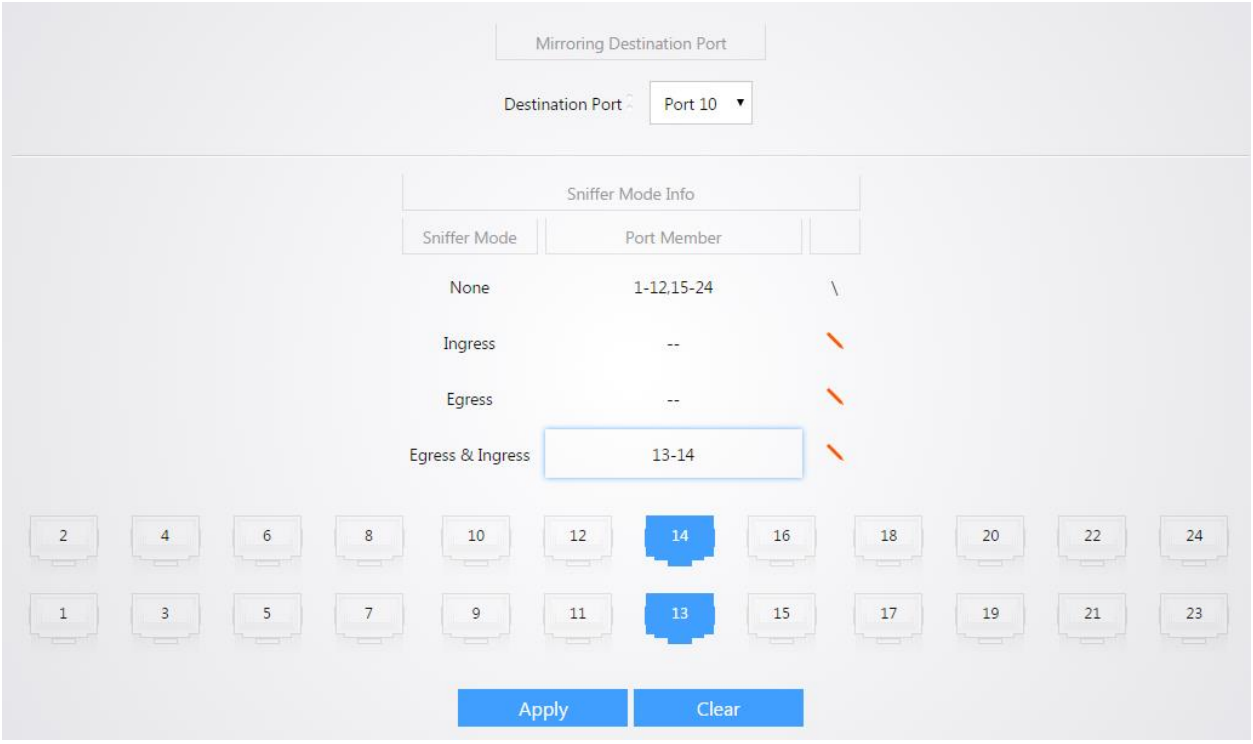


Mirror

Port Mirroring allows you to copy packets on one or more ports to a mirroring destination port. You can attach a monitoring device to the mirroring destination port to view details about the packets passing through the copied port(s). This is useful for network monitoring and troubleshooting purposes. The switch provides local port mirroring functionality, namely, both mirrored ports and mirroring destination ports are located on the same device.

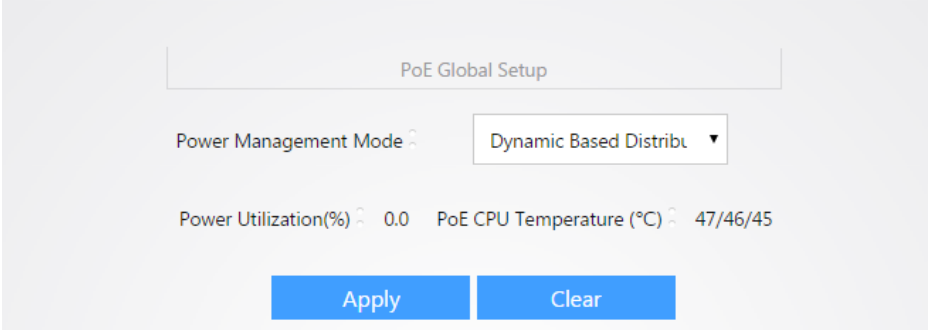
To configure port mirroring, select the **Destination Port**. The destination port is the port which all mirrored data is sent to. You can select **Ingress**, **Egress** or **Egress & Ingress** for the **Sniffer mode**. Ingress mode indicates that only data being received will be mirrored. Egress mode indicates that only data being sent will be mirrored. Egress & ingress indicates that both directions of data are being mirrored to the destination port.

Once you have decided which sniffer mode to use, click the edit icon towards the right and then you will be able to select the ports that you want to mirror data for. The following image illustrates this. Click **Apply** to finalize the settings.



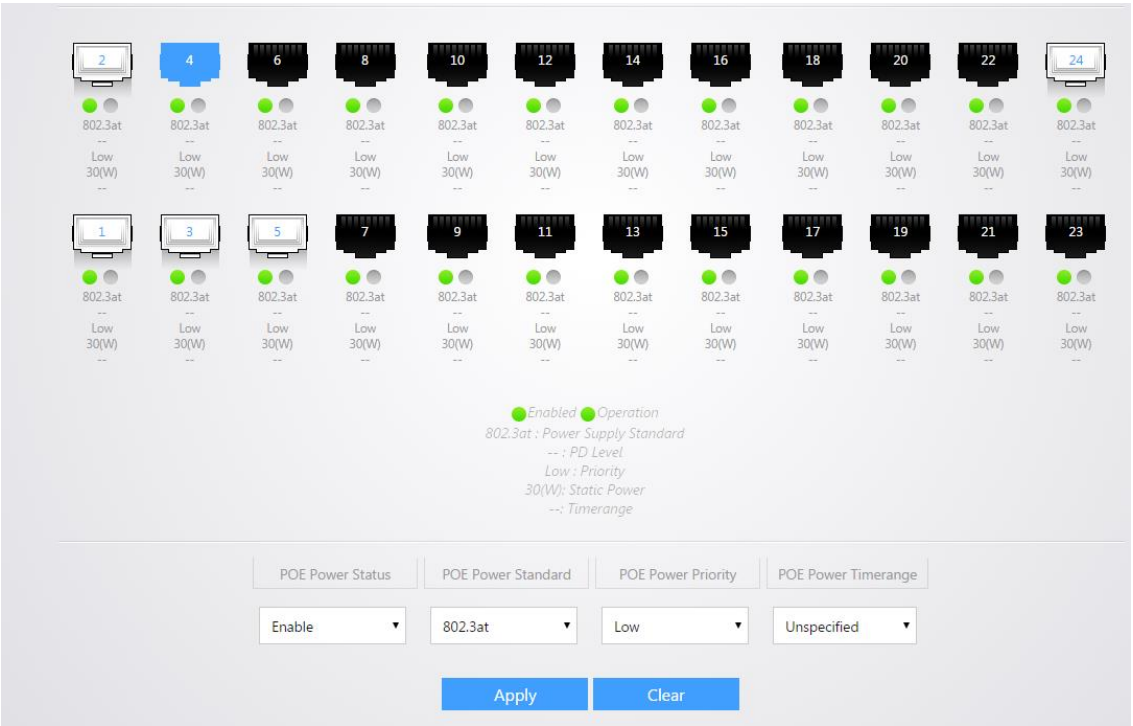
POE

The PoE page allows you to modify power over Ethernet settings. The PoE global Setup configures PoE **Power Management Mode**. When it is **Static**, you can configure power allocation manually. When power supply is connected on the port, part of power will be enforced to be reserved for this port and can't be used by other ports. When it is **Dynamic**, according to actual used power allocation, in full load, power will be allocated by port priority (priority + port number). If the priority is the same, the smaller the port number is, the higher the priority.

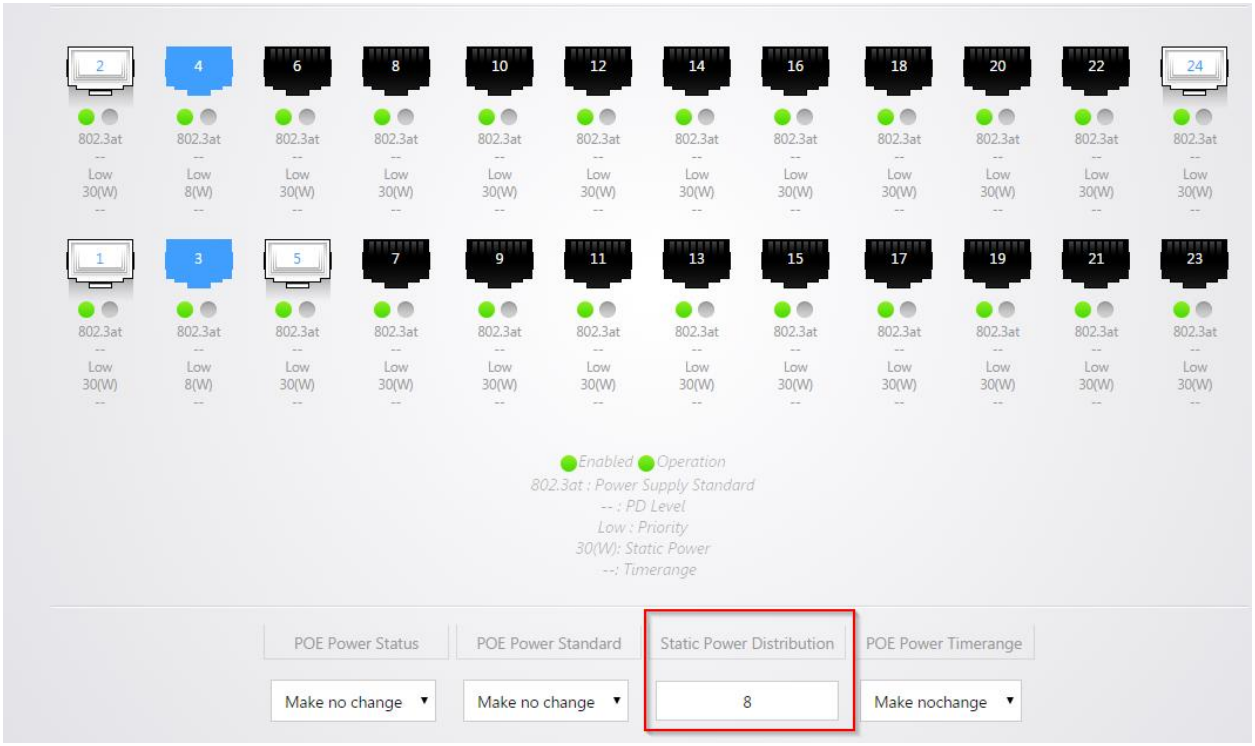


You can select a port and then adjust the following settings below

- **PoE Power Status**: You can disable or enable poe on the port
- **PoE Power Standard**: You can select from 802.3af or 802.3at. 802.3af defines up to 15.4 watts per port. 802.3af defines up to 30 watts per port.
- **PoE Power Priority**: The priority defines which ports have access to available power from the switch. Devices with high priority will have access to available power first.
- **PoE power Timerange**: If you created a time range object under Time Range Management you can select it here and the switch will follow that schedule for enabling and disabling power on the port.

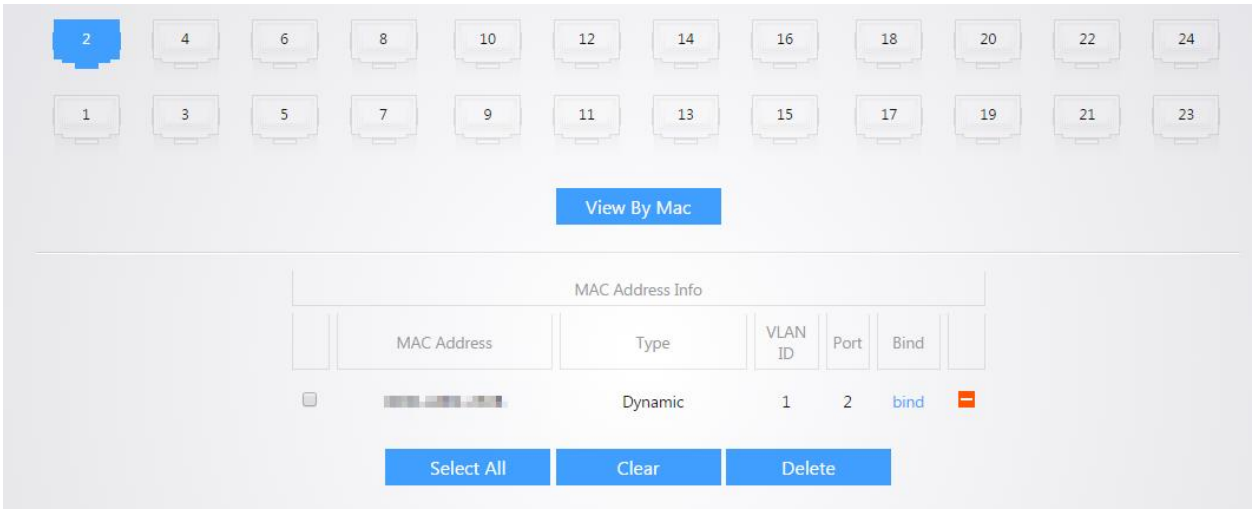


If **Static Based Distribution** is used you will be able to enter the amount of watts that you want the ports on the switch to use. The following image illustrates this. Click **Apply** to finalize any settings made on this page.

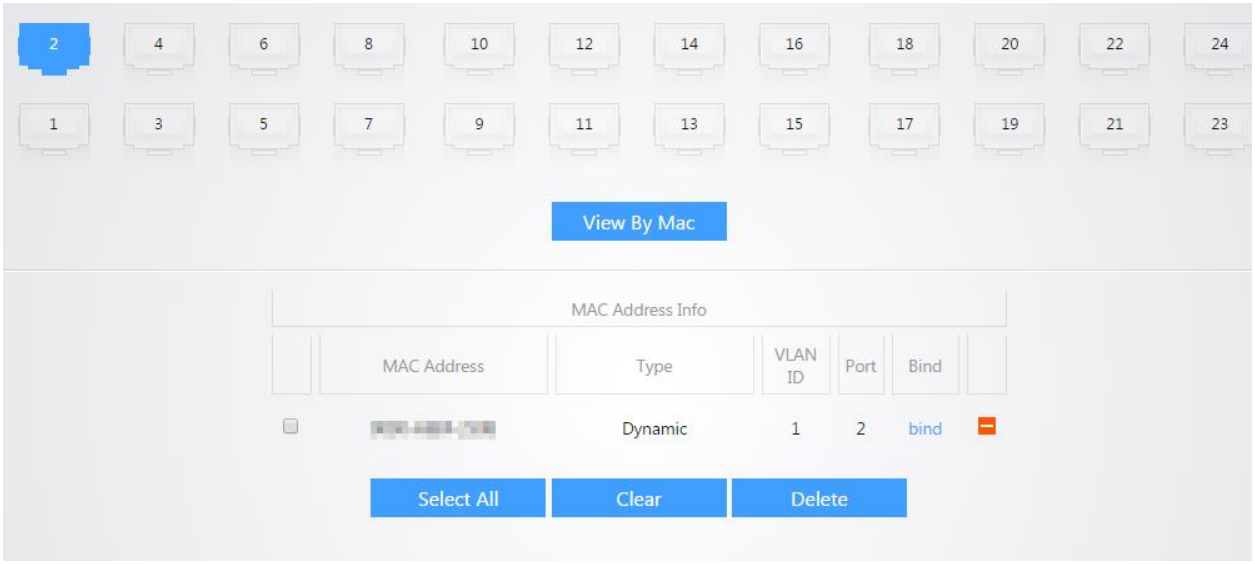


MAC CONTROL

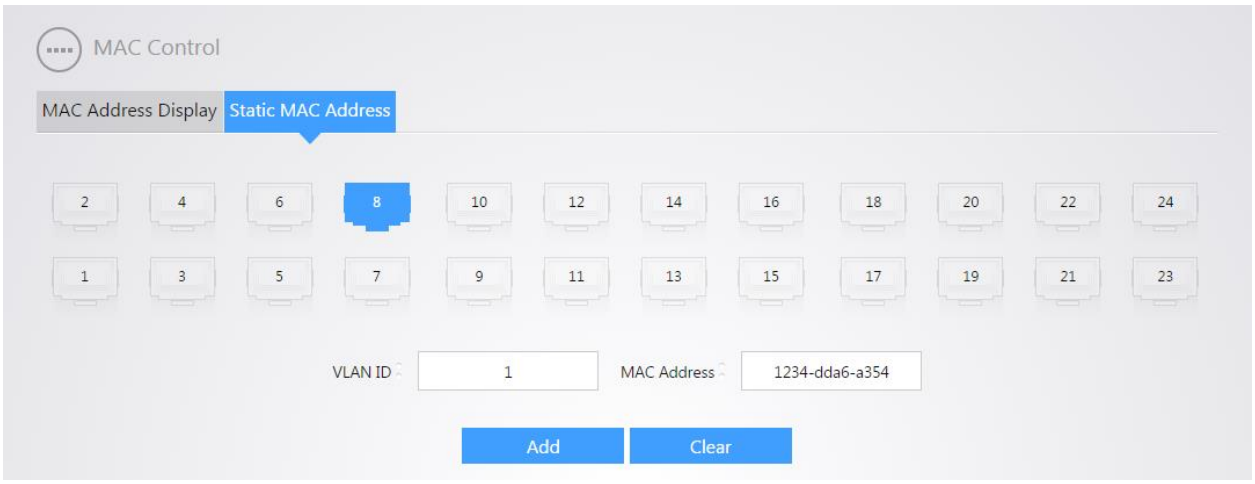
The MAC Address Display page will allow you to view the different mac addresses passing through the ports on the switch. You can click on a port and see the mac address associated with that port. The following image illustrates this.



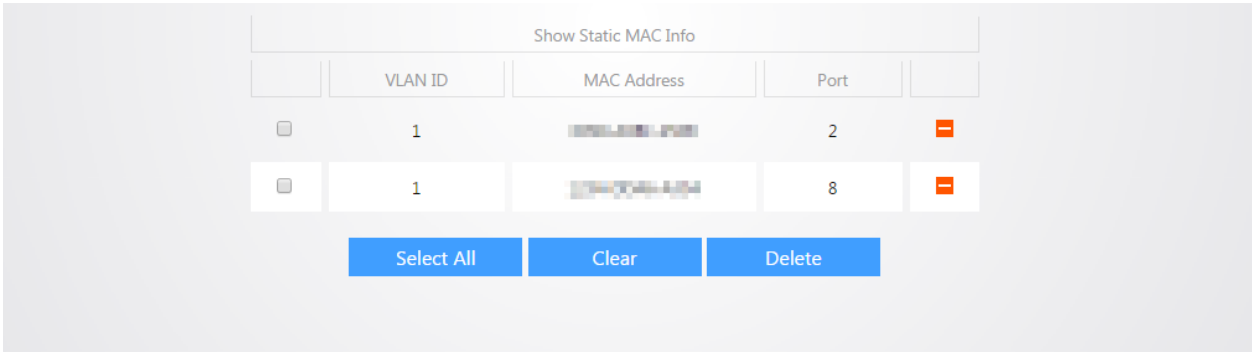
Once you have selected a port, you can click bind on a mac address entry and the switch will bind that mac address to the current port. Data from any other mac address will be denied on that port.



The Static MAC Address page will allow you to bind a mac address to a port on the switch. You can select a port and then enter the **VLAN ID** that the device with the specified mac address will be on along with the **MAC Address**. The following image illustrates an example of this. Click **Add** to add the entry.



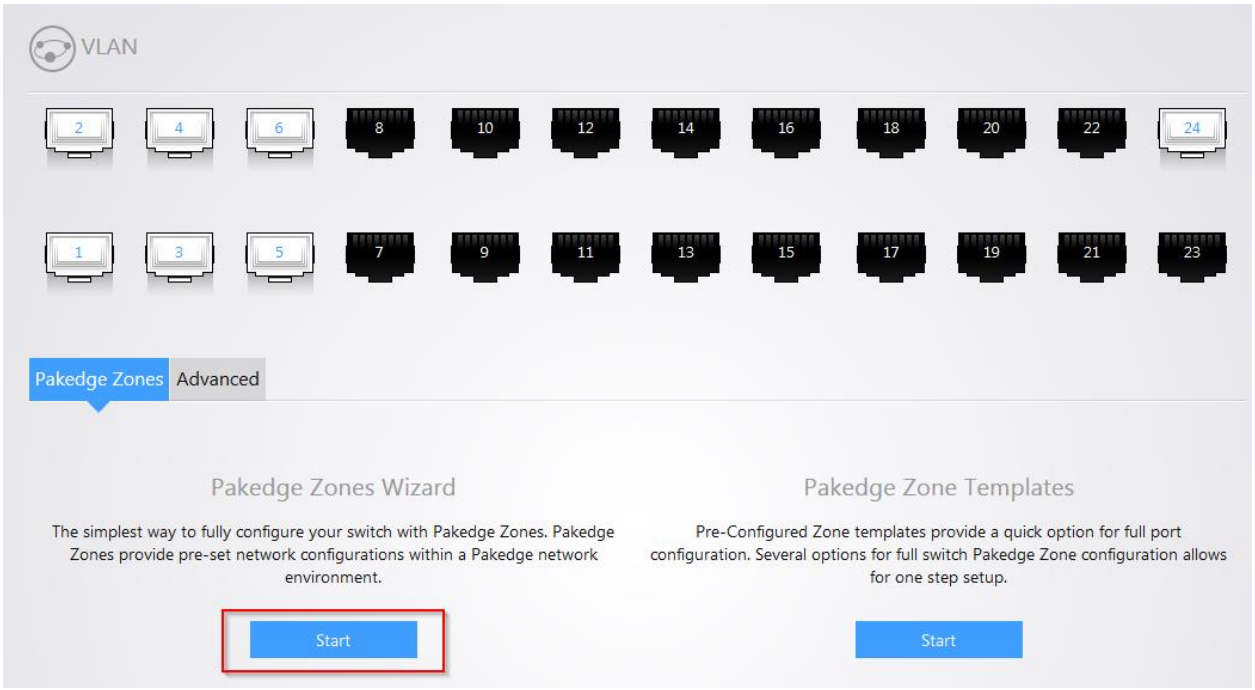
Under **Show Static MAC info**, you can see all existing Mac bindings on the switch. You can delete an entry by selecting the check box next to it and clicking **Delete**.



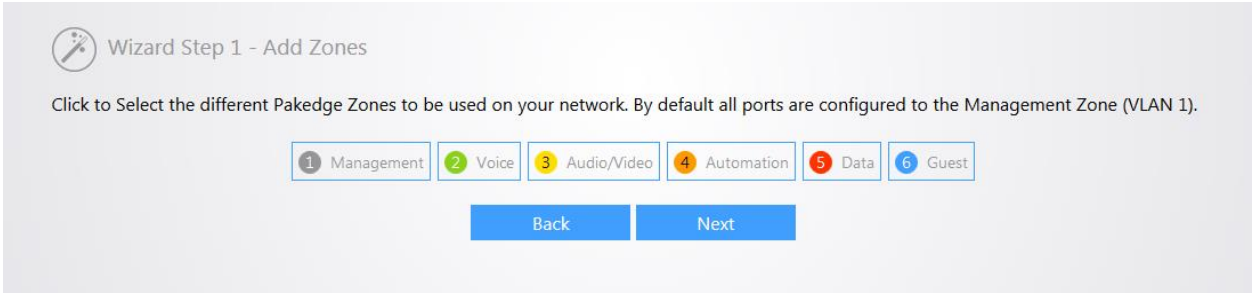
VLANS

A Virtual Local Area Network (VLAN) is a network topology which allows to logically instead of physically segment a LAN into several net segments. A VLAN combines a group of hosts with a common set of requirements logically instead of physically relocating devices or connections. VLANs allow a network to be logically segmented into different broadcast domains. All members in a VLAN are treated as in the same broadcast domain and communicate as if they were on the same net segment, regardless of their physical locations. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated. Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer 3 devices that are able to perform Layer 3 forwarding.

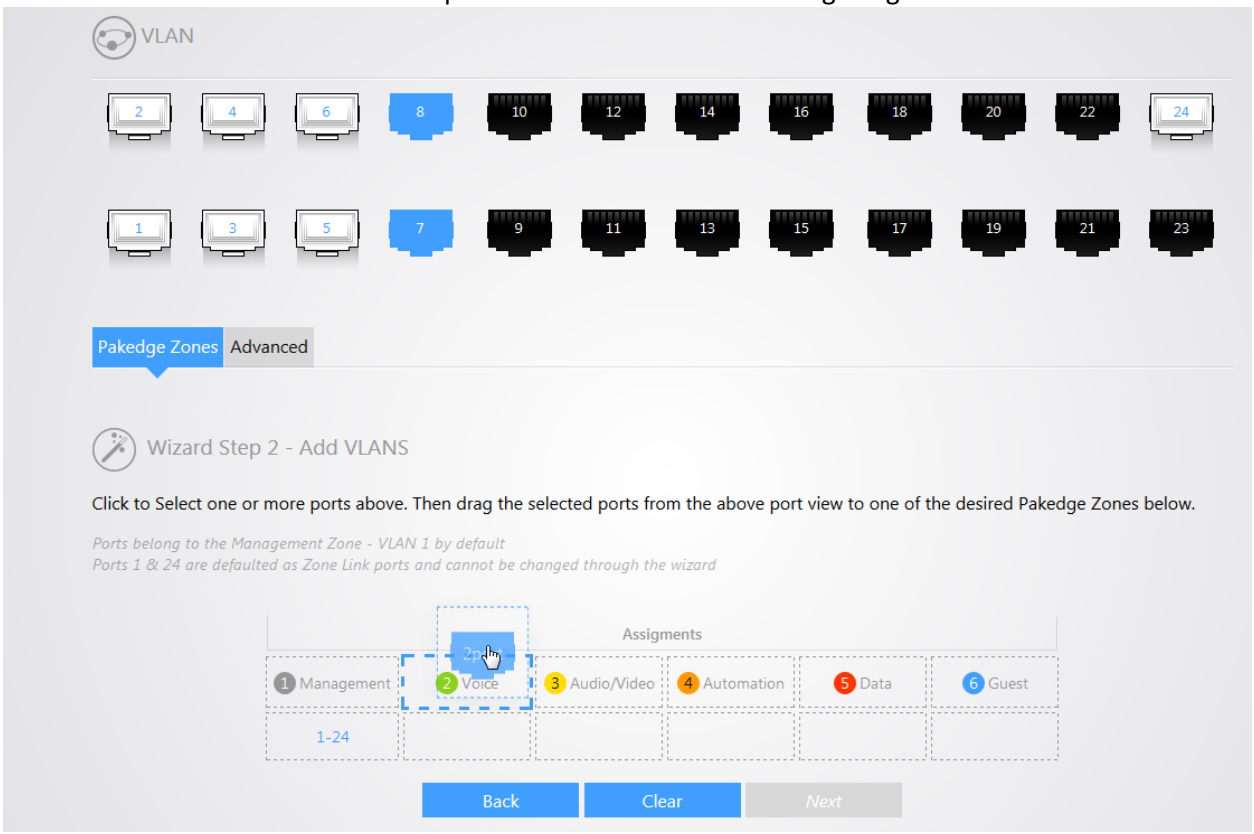
The VLAN configuration page will allow you to use the Pakedge Zone Wizard to setup your different VLANs. Click on **Start** to begin the wizard.



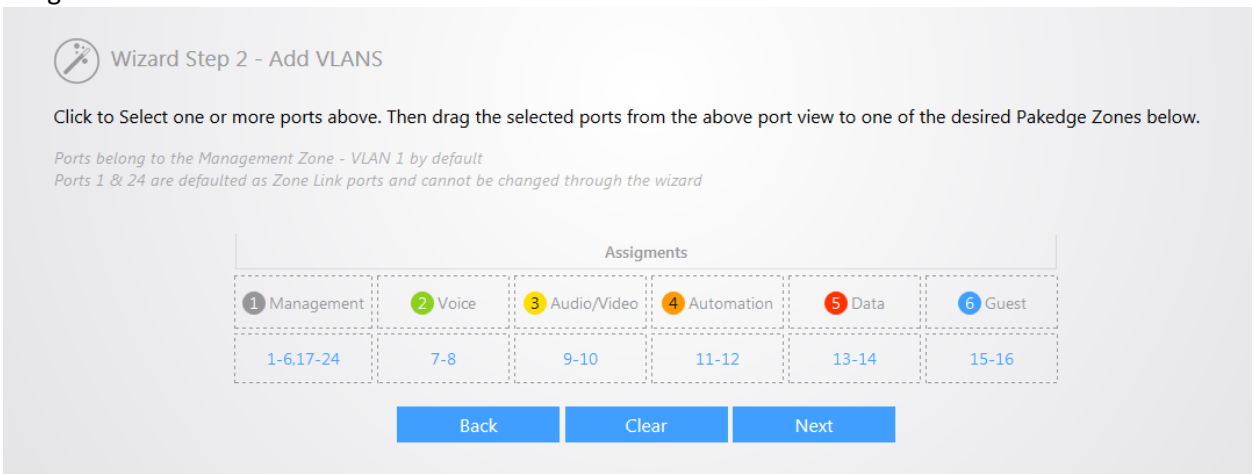
Step 1: Click on the VLANs you would like to use. The following image illustrates this. By default, VLANs 1 through 6 will be available for use. Click **Next**.



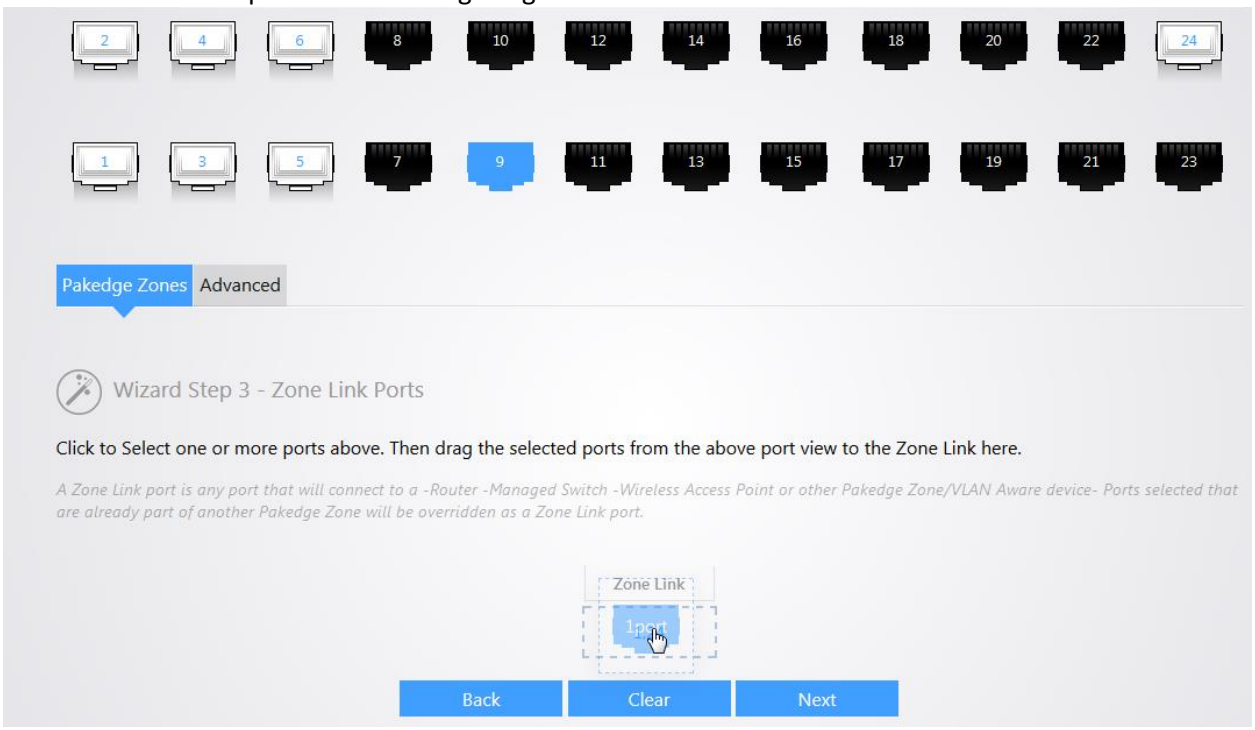
Step 2: Select the ports you wish to add to each VLAN. For example, you can select ports 7 and 8 and then drag them to VLAN 2 to add both of those ports to that VLAN. The following image demonstrates this.



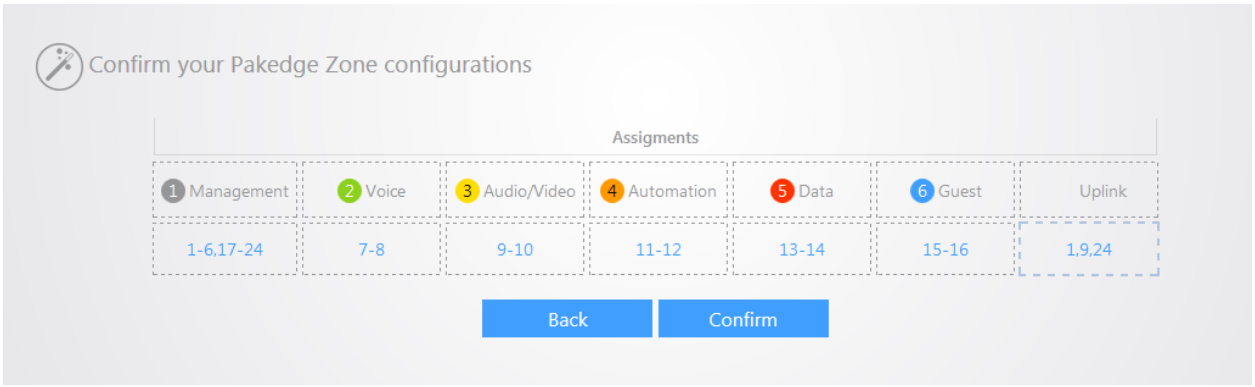
Continue to add the ports for all of your VLANs. When finished, your configuration might look like the following image. Click **Next** to continue.



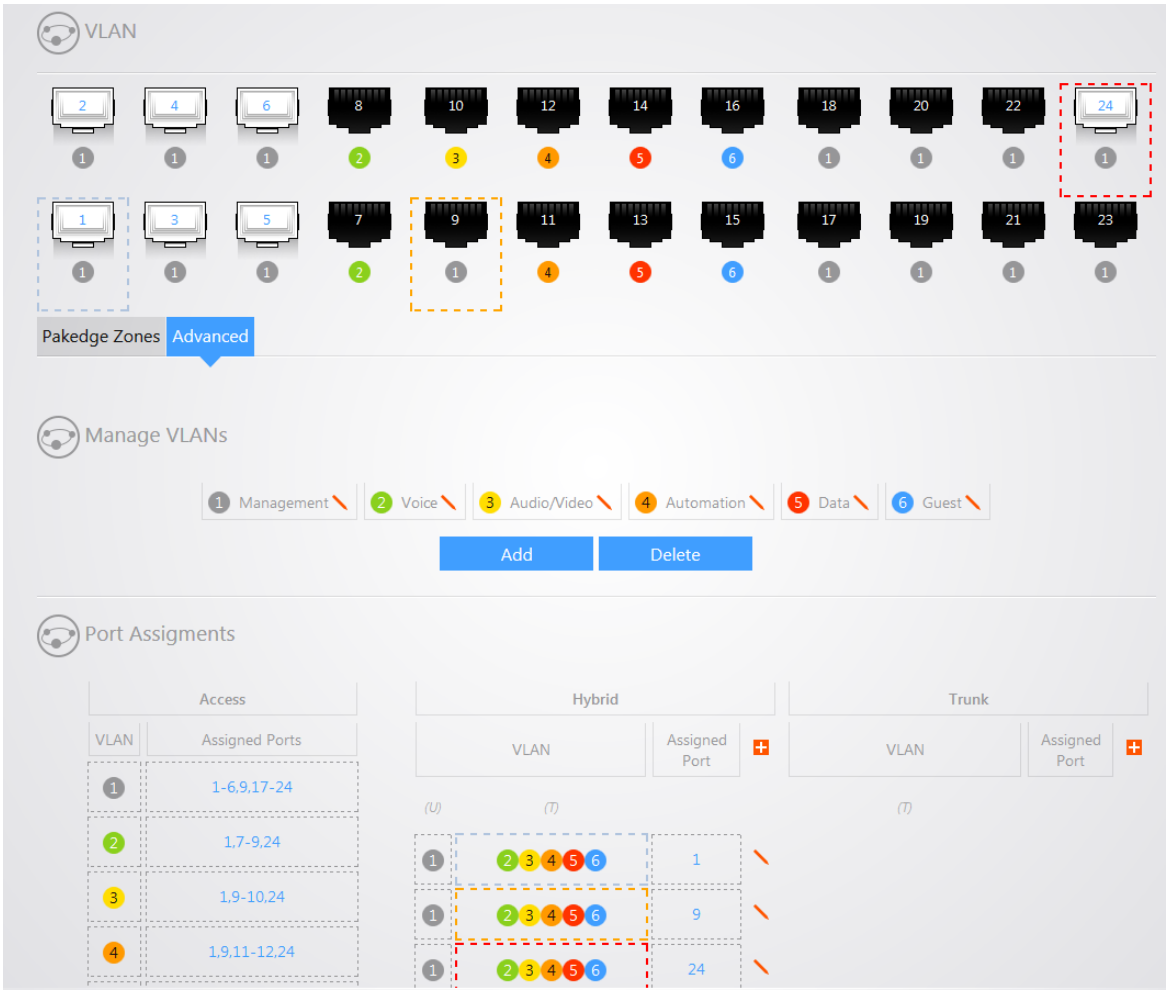
Step 3: Select your zone link ports. The zone link ports are ports that connect to other VLAN aware devices such as Routers, Access Points, and other managed switches. By default, ports 1 and 24 are Zone Link ports. Zone link ports are also known as hybrid ports. You can select another port and drag it down to the Zone Link box to add it as a Zone Link port. The following image illustrates this. Click **Next** to continue.



Click **Confirm** to finalize the settings.

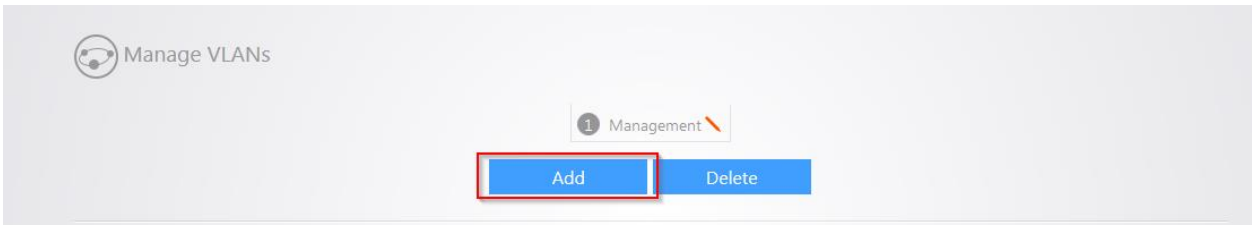


Once the VLAN wizard is complete, you will be taken to the advanced VLAN configuration page.

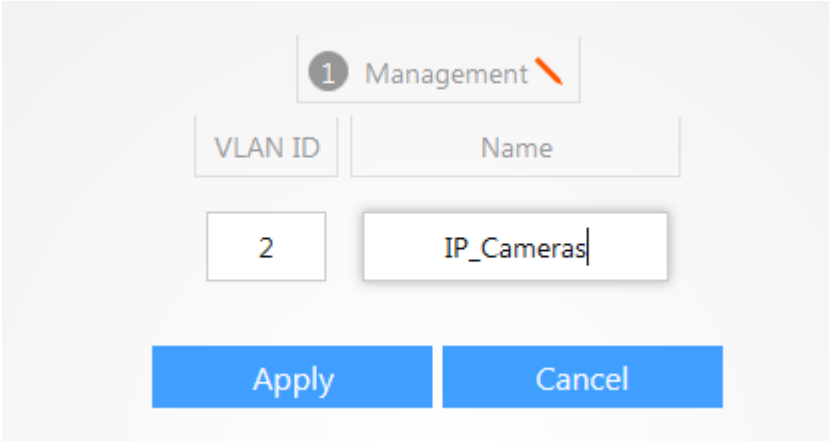


Manually Configuring VLANs

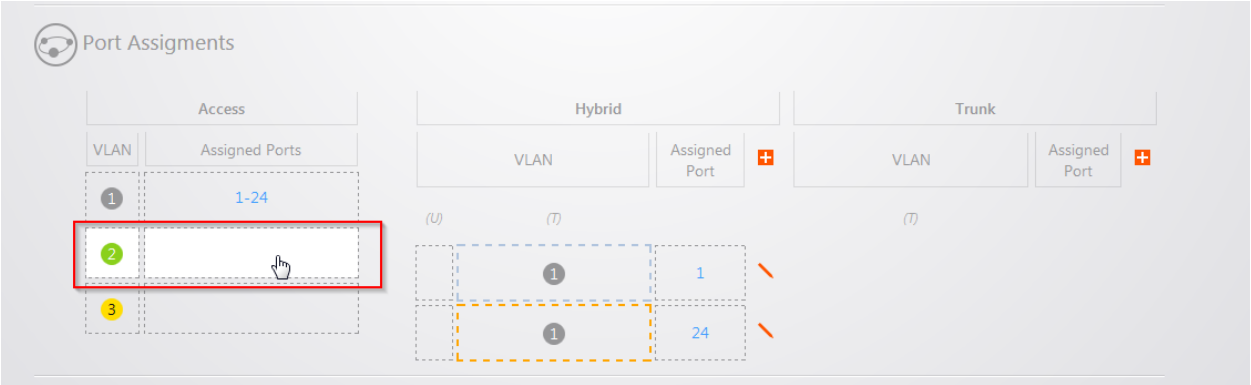
You can manually configure VLANs on the switch using the Advanced VLAN configuration page. Click **Add** to add another VLAN.



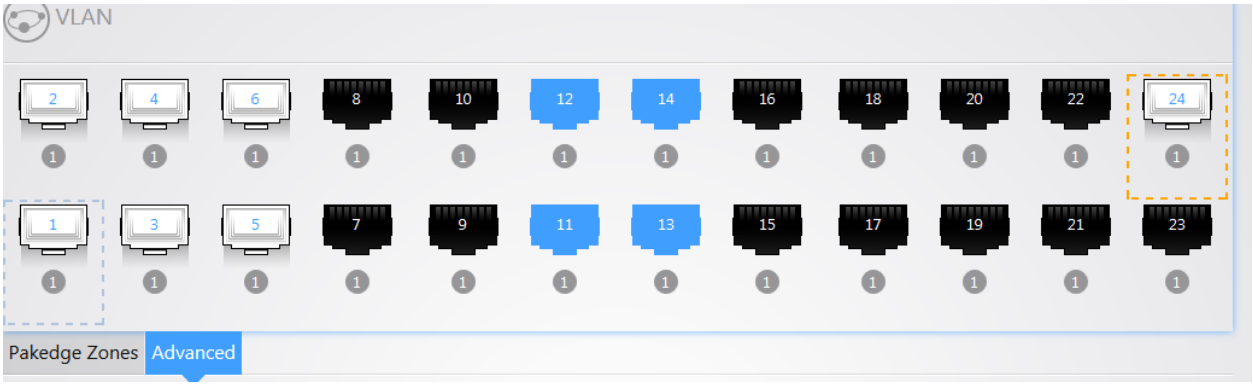
Enter the **VLAN ID** and **Name** for the VLAN and click **Apply**. You can continue adding VLANs in this manner.



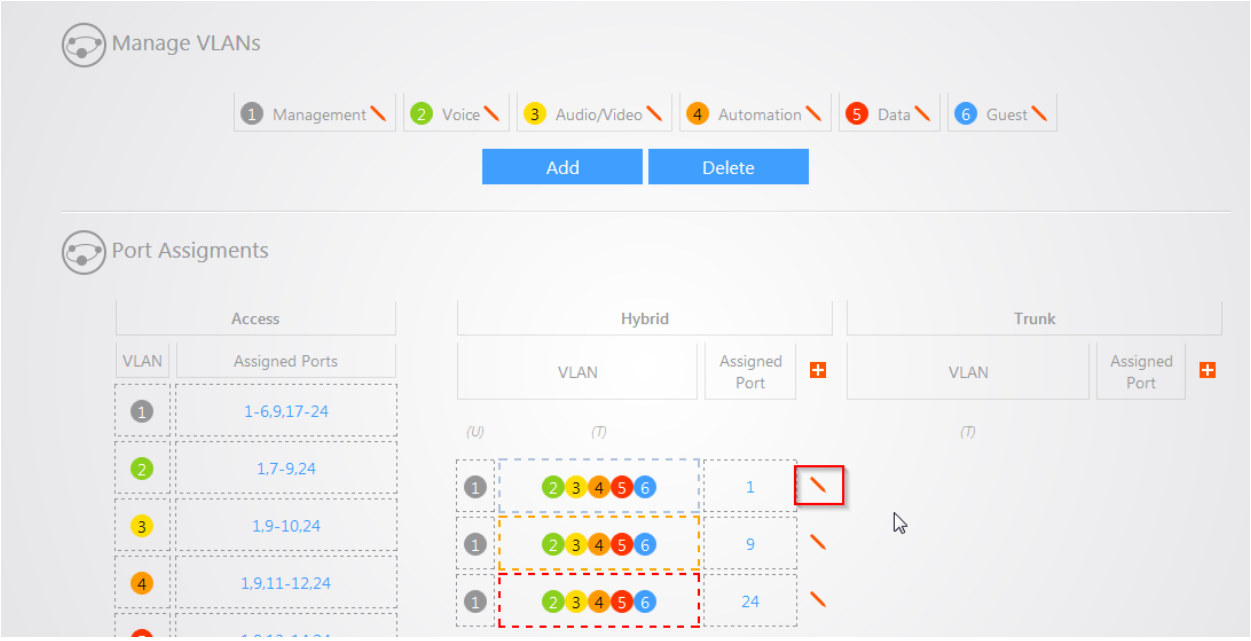
To add ports to a VLAN, click on the VLAN under Port Assignments.



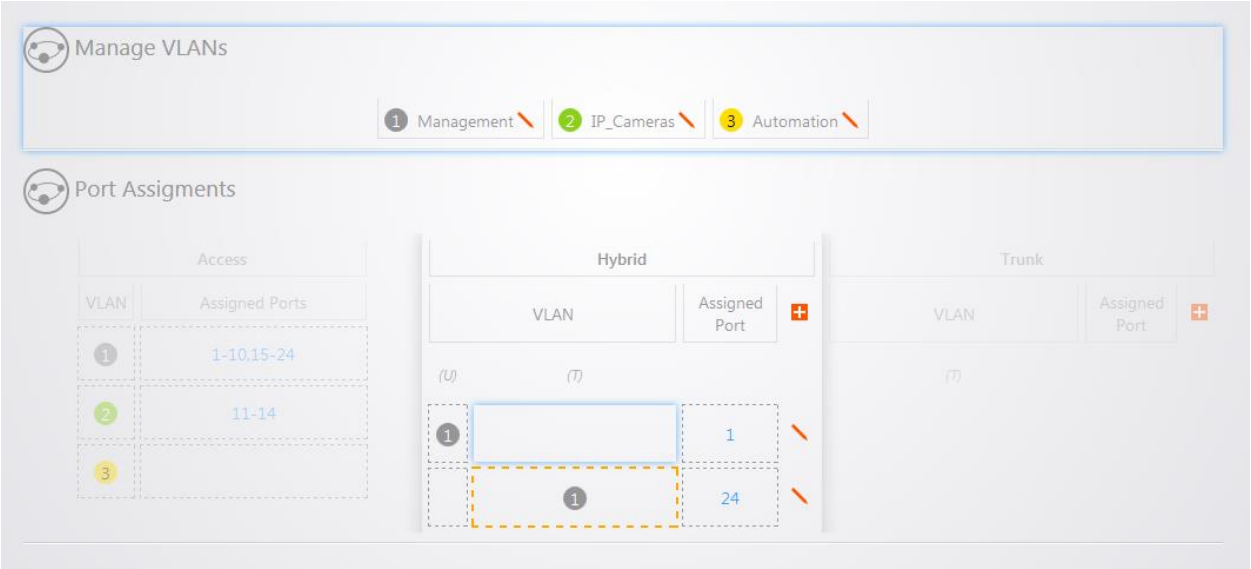
Select the ports you wish to add to this VLAN. Click **Apply** towards the bottom to finalize the settings.



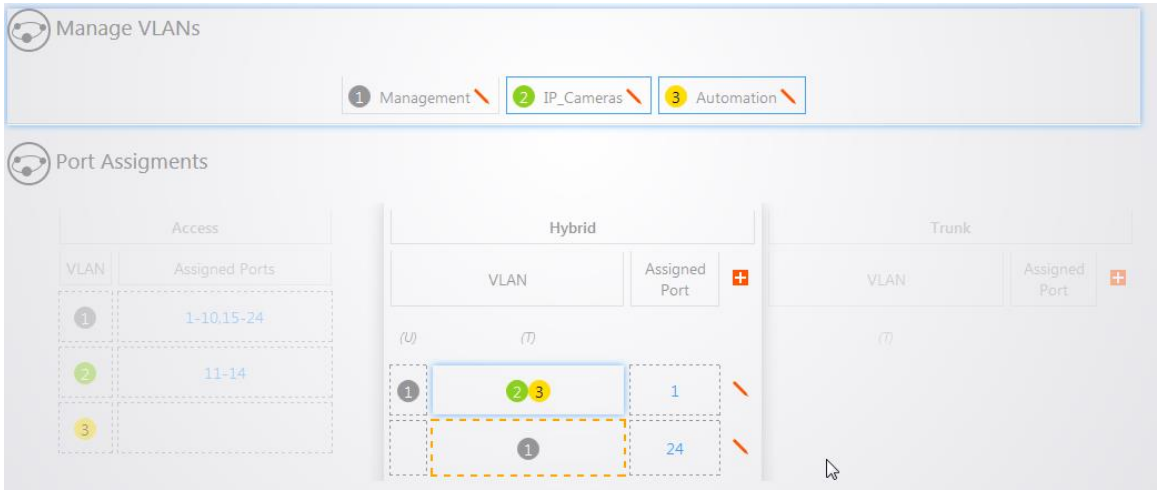
You will also need to configure hybrid ports for VLANs to work properly. By default, ports 1 and 24 are hybrid ports. You will need to add any additional VLANs you configured to the Hybrid ports. To do this, click the edit icon next to one of the Hybrid ports.



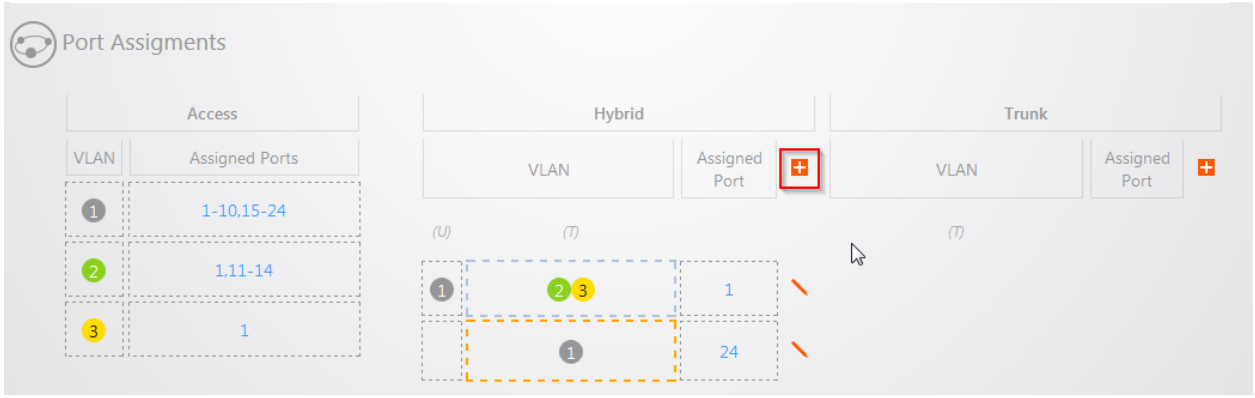
There will be a blue outline around the box under the (U) column. The (U) indicates the VLAN that will have data untagged. Click on VLAN 1 and then VLAN 1 will be populated in the box.



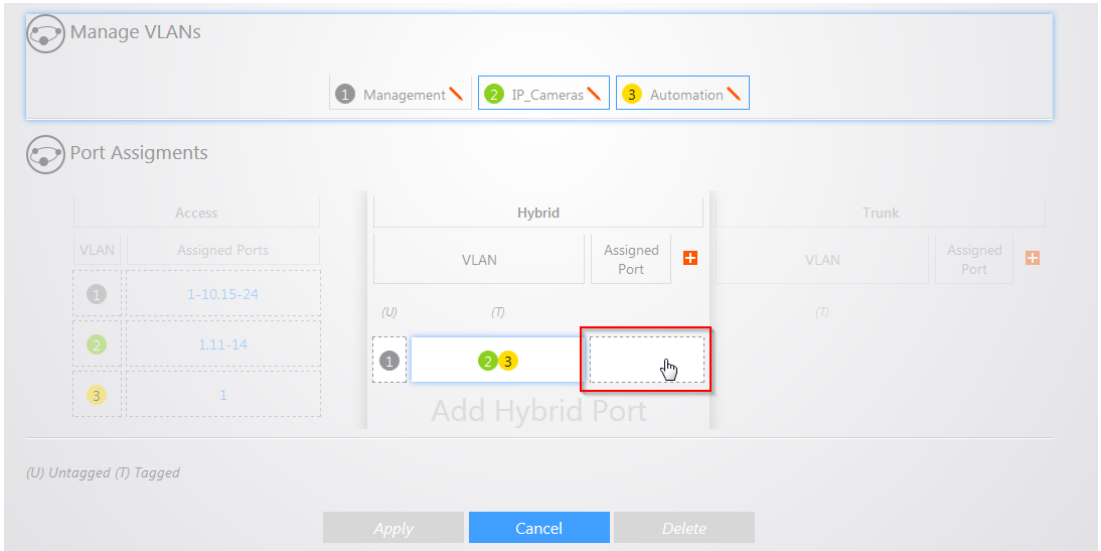
There will then be a blue outline around the box under the (T) column. The (T) indicates the VLANs that will have tagged data. Click on the remaining VLANs to add them to the port. Click **Apply**. Repeat these steps for any other Hybrid ports you need to configure.



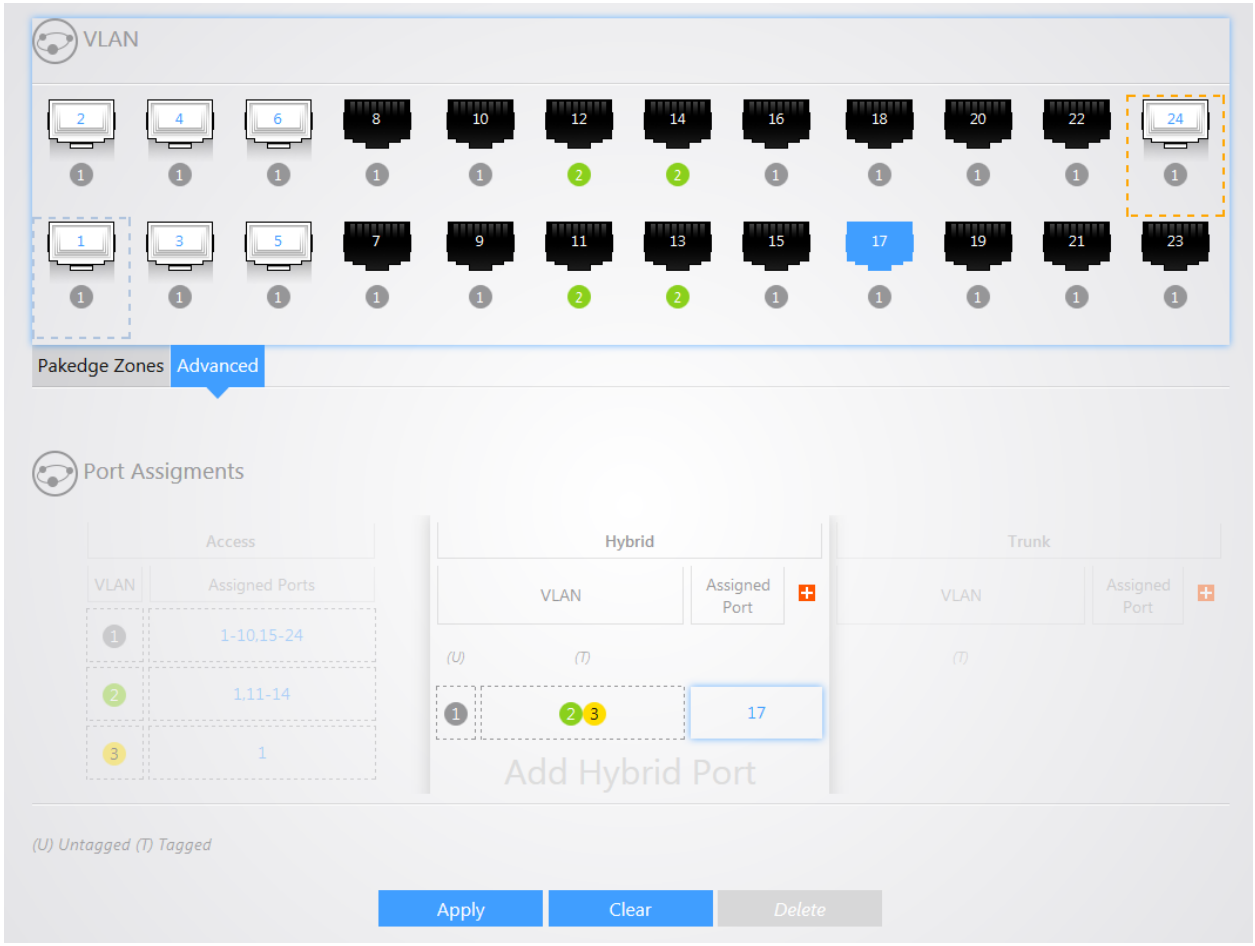
If you need to add another Hybrid port, click the add symbol under the Hybrid section.



Select the VLAN you wish to be untagged (normally VLAN1) and then select the VLANs you wish to tag. Click the **Assigned Port** column.

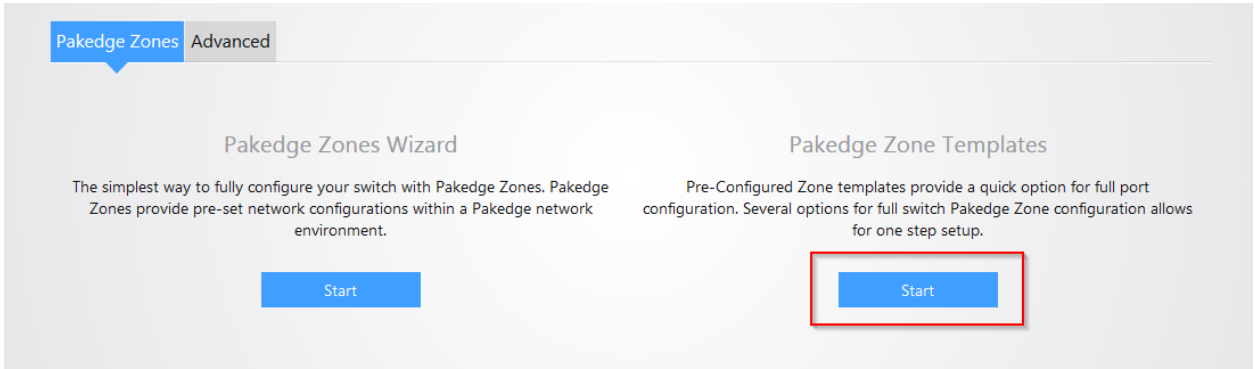


Click the port you want to add as hybrid. Click **Apply** to finalize the settings.

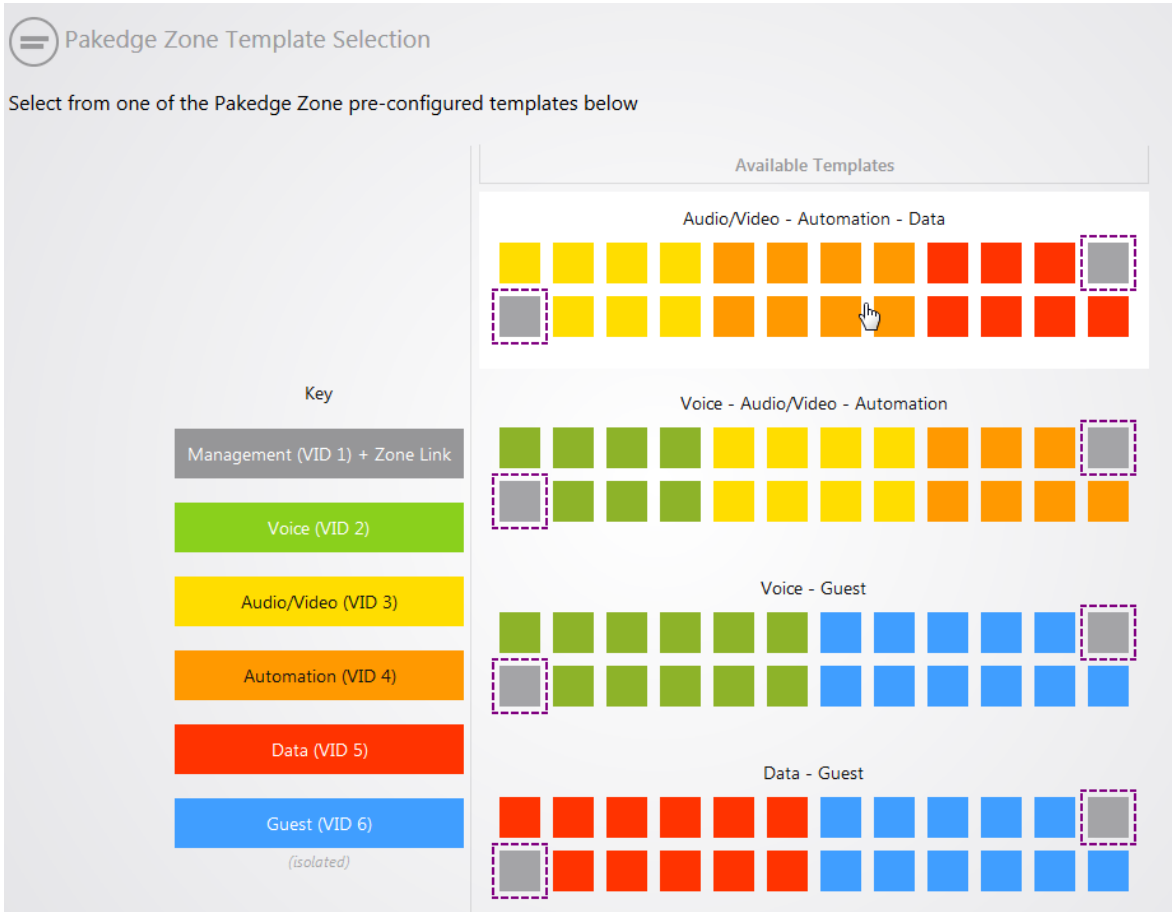


Pakedge Zone Templates

The Pakedge Zone templates allow you to quickly apply a VLAN template to all the ports on the switch. Click **Start** to view the templates.



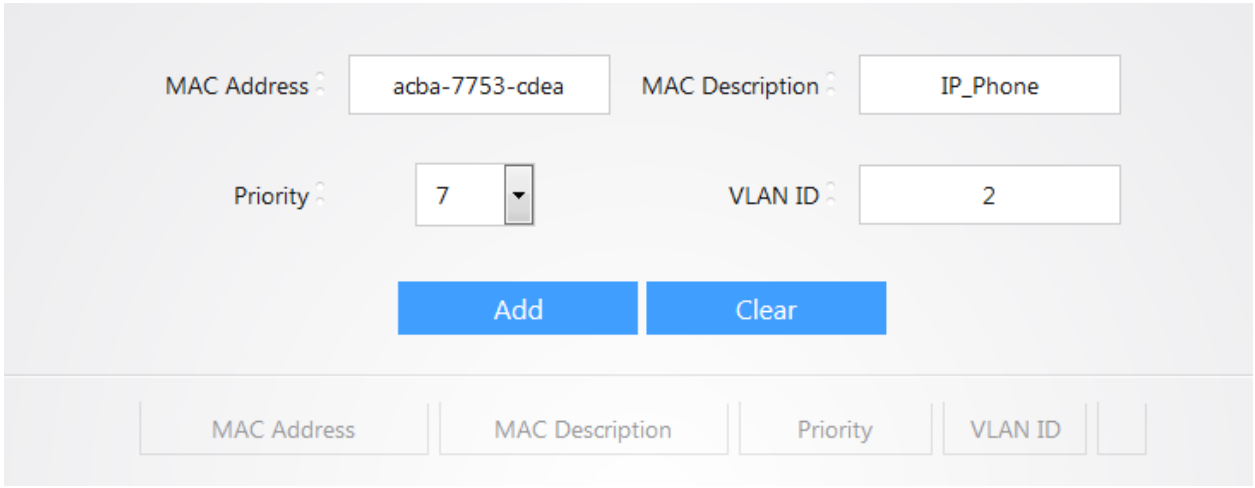
You can select a template and then click **Apply Template** to apply it to all ports on the switch. Use the **Key** on the left hand side to identify which colors correspond to which VLANs.



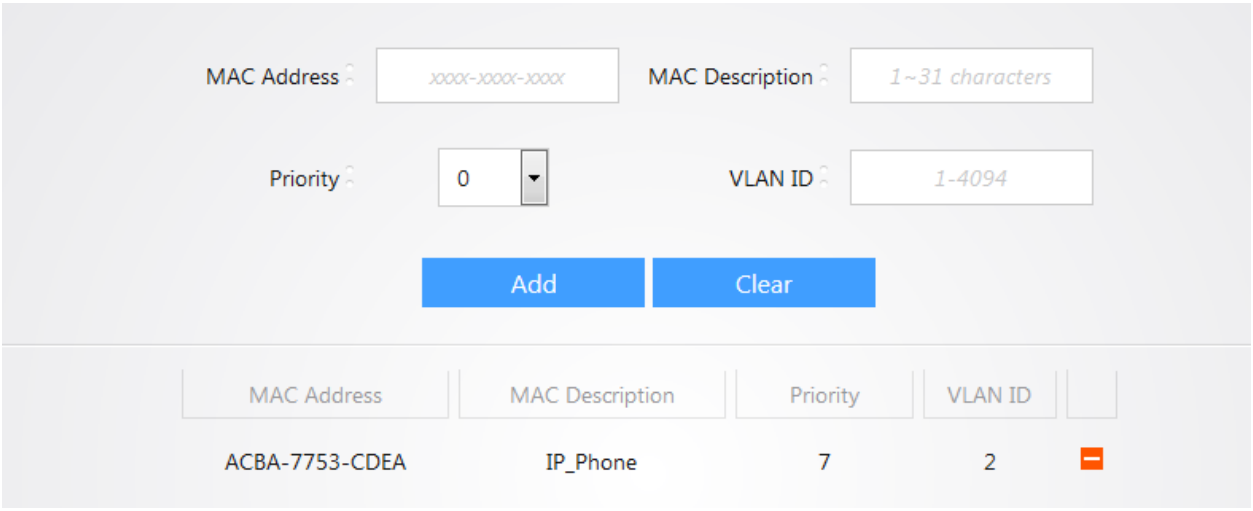
MAC VLAN

MAC VLAN technology is the way to classify VLANs according to the MAC addresses of Hosts. MAC VLAN only takes effect on ingress untagged data. When the port receives an untagged packet, the device, with the matching key words of the packets' source MAC address, will search MAC VLAN entries to obtain the terminal's binding VLAN. In this way, packets of the designated terminal will be forwarded in the designated VLAN. Thus, the user terminal and VLAN will be bound accurately and flexibly.

In the MAC VLAN page, specify a **MAC address** to be put on a VLAN. Enter a **MAC Description**. Specify the **priority**. Enter the **VLAN ID** for the VLAN that you want to place this mac address in. Click **Add**. You can continue to add MAC addresses.



You will see your entry listed down below. To delete your entry click on the red icon.

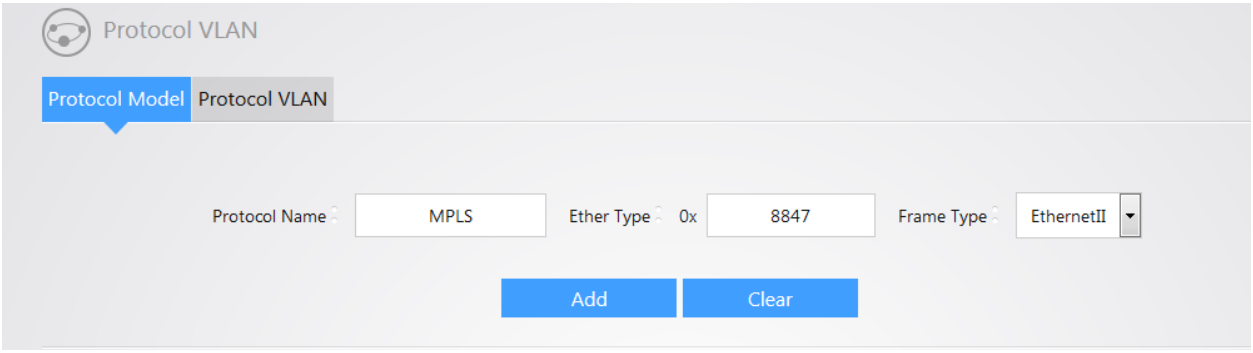


PROTOCOL VLAN

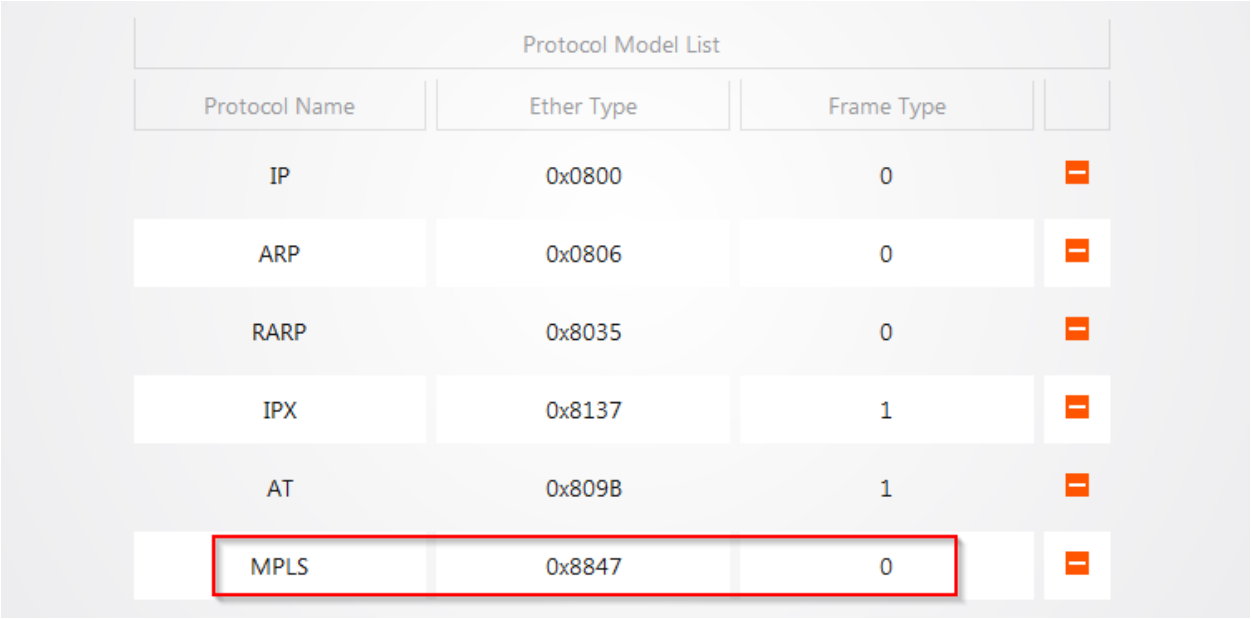
Protocol VLAN, another way to classify VLANs based on network protocol, can bind ToS provided in the network to VLAN to realize the specific service. Through protocol VLAN, the switch can analyze the received untagged packets on the port and match the packets with the user-defined protocol template according to different encapsulation formats and the values of the special fields.

If a packet is matched, the switch will add a corresponding VLAN tag to it automatically and thus the data of specific protocol can be automatically assigned to the corresponding VLAN for transmission. The network administrator can manage network clients based on their specific applications and services through protocol VLAN.

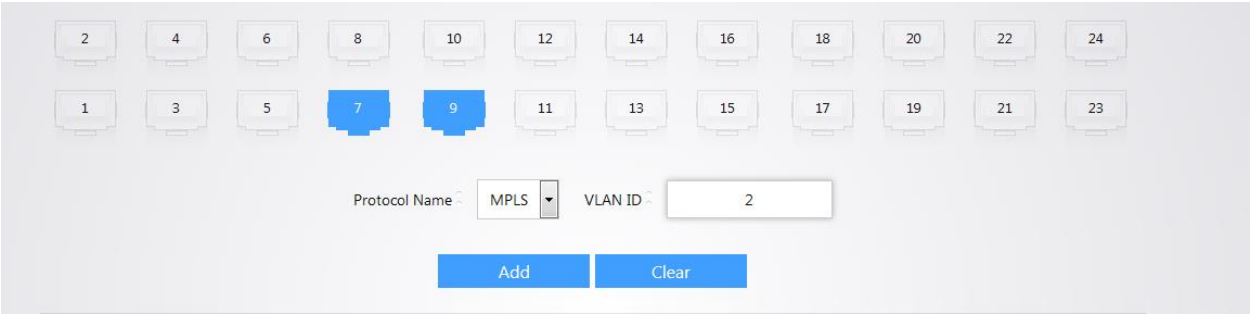
In the protocol VLAN page, specify a **Protocol Name**. Enter the **Ether Type** value and specify the Frame Type. Click **Add** when finished.



You will see your entry in the list below.



On the Protocol VLAN page, select the Protocol from the **Protocol Name** drop down box. Enter the **VLAN ID** that you want this protocol data to be placed on. Select the ports that you want to be members of the Protocol VLAN. Click **Add** to finalize the settings.

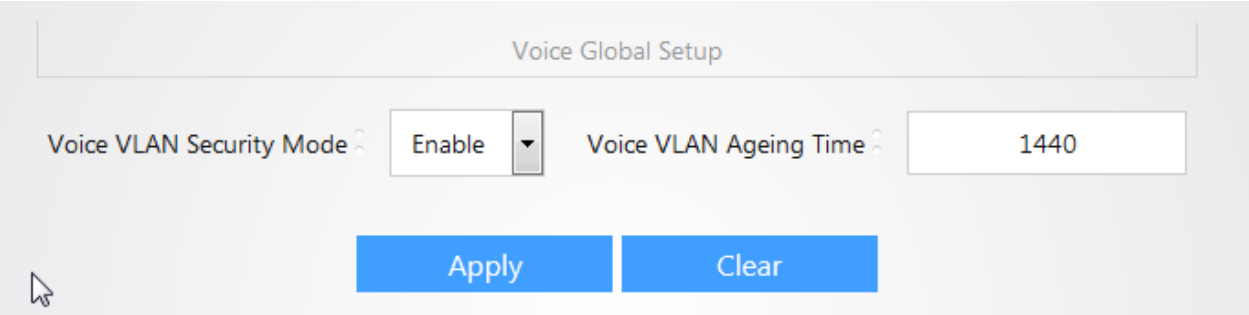


You will see your entry towards the bottom.

VOICE VLAN

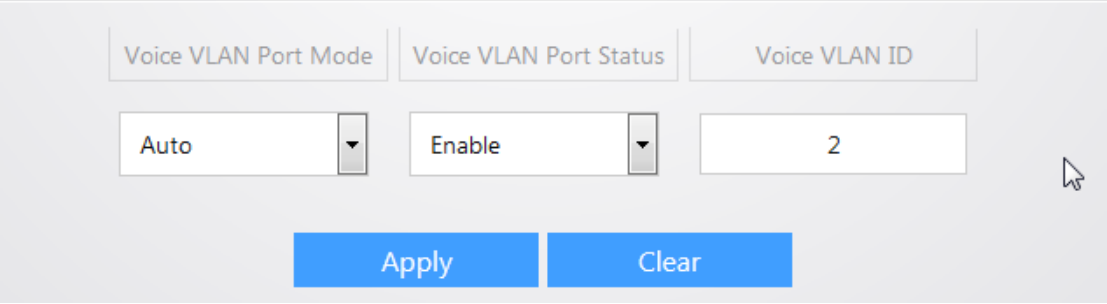
Using Voice VLAN the switch is able to distinguish whether data is voice data or not according to the source MAC fields of the ingress packets. If the source MAC address conforms to the voice device's OUI (Organizationally Unique Identifier) address, the packets will be regarded as voice data flow and the port which has received the voice data flow will automatically join the voice VLAN. Thus, the voice-VLAN-tagged voice traffic of voice devices connected to this port can be transmitted and enjoys higher transmission priority. You can preset OUI address or use the default OUI address as the criteria. An Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. This device supports OUI mask. You can adjust MAC address' matching depth by setting different masks.

To configure Voice VLAN, set the **Voice VLAN Security mode** to **Enabled**. The **Voice VLAN aging time** specifies how long the switch will wait to receive voice data on a port before removing that port from the voice VLAN. This is in seconds. Click **Apply** to enable Voice VLAN.

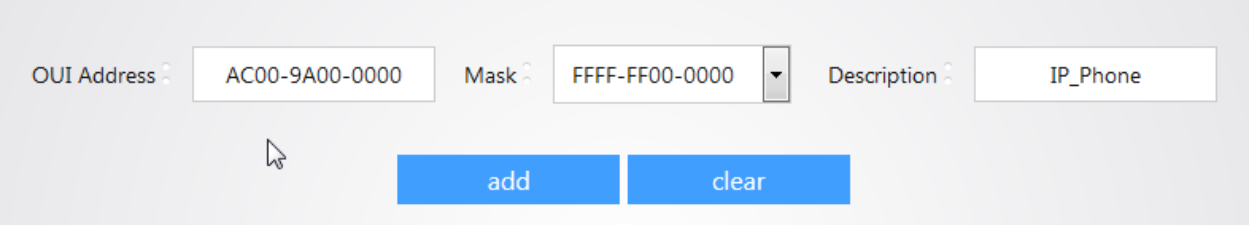


Select the ports that you would like to have the switch listen for voice data. If Voice data is detected, the port will be put into the Voice VLAN.

Down below; set the **Voice VLAN Port Mode**. Auto indicates that the switch will automatically place a port(s) into the Voice VLAN when it detects voice data. Manual indicates that the switch will simply place the port(s) into the Voice VLAN permanently. Set the **Voice VLAN Port Status** to **Enable**. The **Voice VLAN ID** specifies the VLAN that voice data will be placed into. Click **Apply** to finalize the settings.



The OUI setup page allows you to enter the MAC addresses of devices that will be placed on the voice VLAN. Enter the MAC address into the **OUI Address field**. The **Mask** specifies how many bits of the entered MAC address must match in order to be placed in the Voice VLAN. The Mask FFFF-FF00-0000 indicates that the first 24 bits must match. Enter a **Description**. Click **Add** to add your entry.



QOS

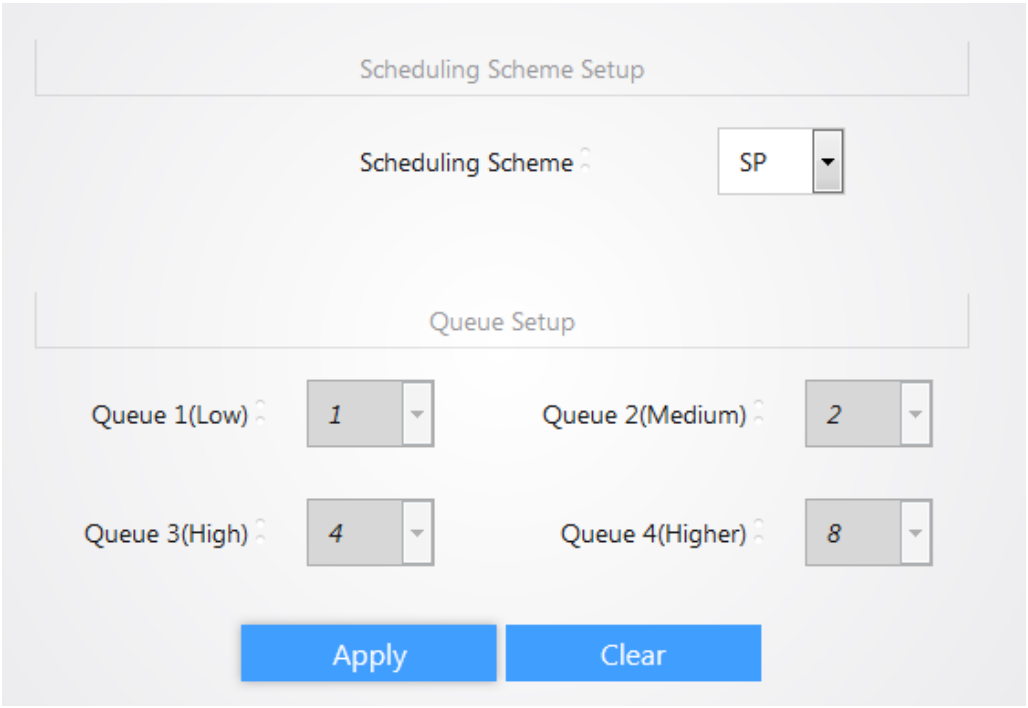
Quality of service is the ability to provide different applications, users, or data flows with different priority, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

The Scheduling Scheme page allows you to specify the Scheduling scheme that will be used for QoS on the switch.

SP: Strict Priority Queuing is specially designed to meet the demands of critical services or applications. Under the SP algorithm, the port strictly prioritizes packets from higher priority queue over those from lower priority queue. Namely, only after packets in highest priority queue are emptied, can packets in lower priority queue be forwarded. Thus High-priority packets are always processed before those of less priority. Medium-priority packets are always processed before low-priority packets. The lowest priority queue would be serviced only when highest priority queues had no packets buffered.

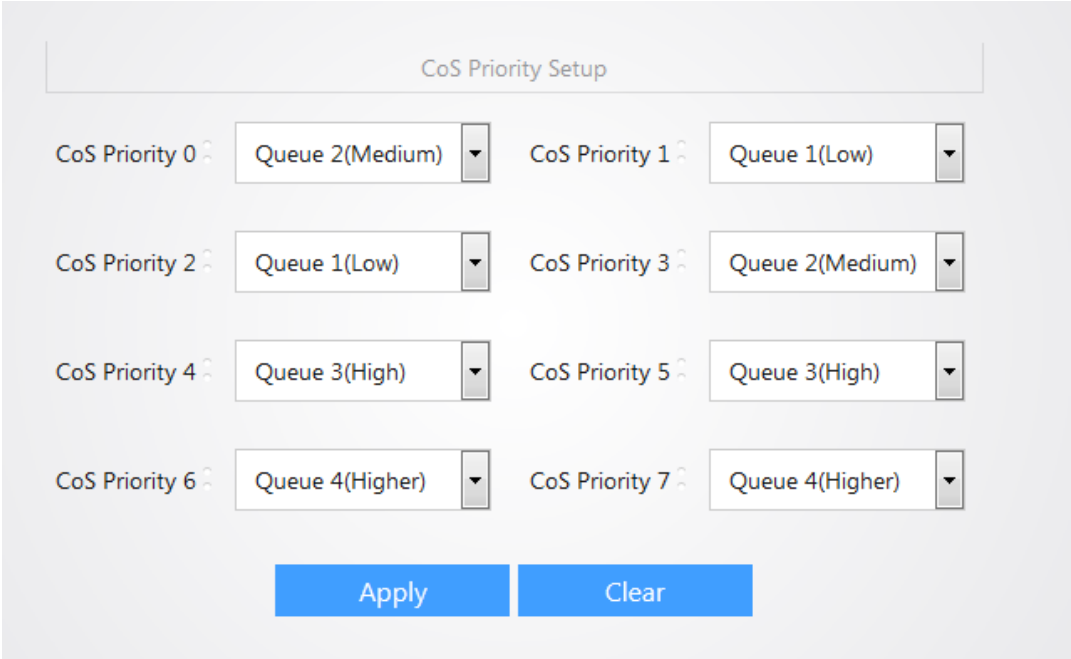
WRR: WRR queue scheduling algorithm ensures every queue a guaranteed service time by taking turns to schedule all queues. The four weight values (namely, Queue 4, Queue 3, Queue 2, Queue 1) indicate the proportion of resources assigned to the four queues respectively. On a 100M port, if you set the weight values of WRR queue-scheduling algorithm to 25, 15, 5 and 5(corresponding to Queue 4, Queue 3, Queue 2, Queue 1 respectively). Then the queue with the lowest priority can be ensured of, at least, 10 Mbps bandwidth.

Click **Apply** to finalize any setting changes on this screen.

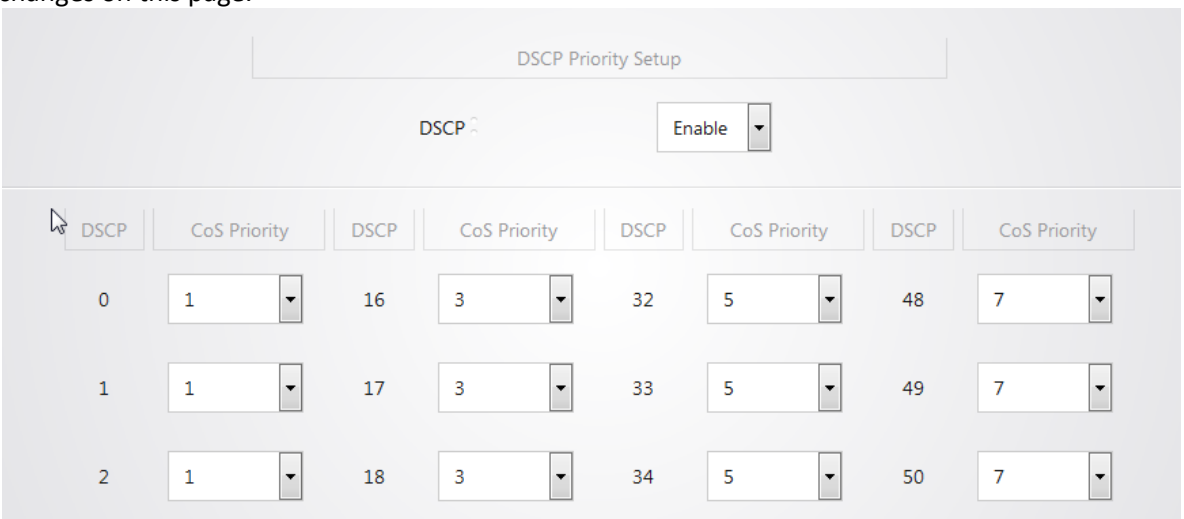


The 802.1P priority, contained in the Ethernet header, is used by QoS disciplines to differentiate traffic on layer 2 where analyzing IP header is not necessary. The 802.1P priority page allows you to specify which queues correspond to which Class of Service (CoS) value.

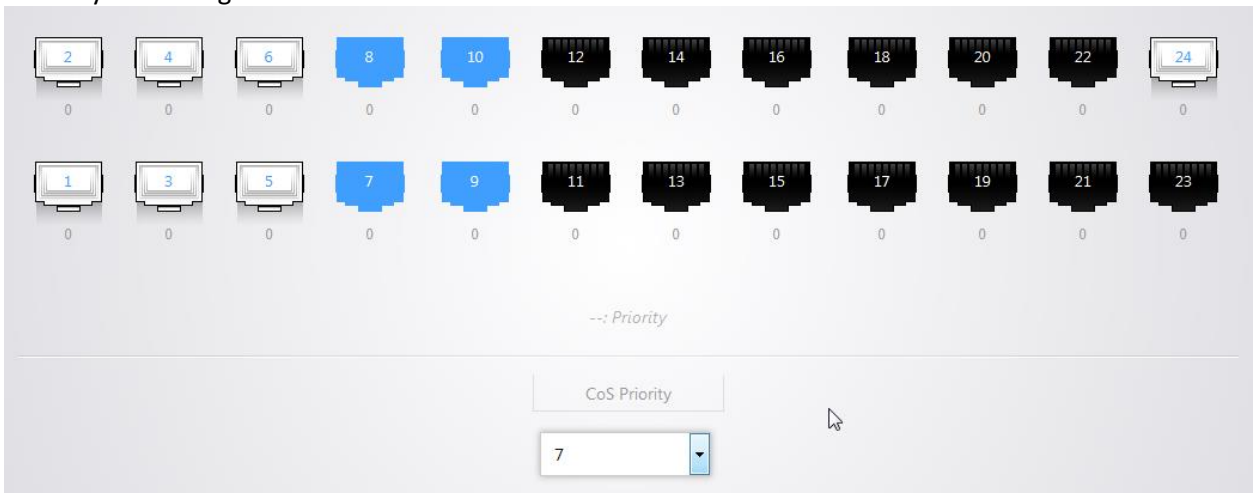
The following image illustrates the default values that are used by the switch. Click **Apply** to finalize any setting changes made on this page.



The DSCP priority resides in the IP header. The ToS field includes 8 bits, among which: The first 3 bits denote the IP priority, with available values ranging from 0 to 7.Bits 3-6 denote the ToS priority, with available values ranging from 0 to 15.The RFC 2474 redefined the IPv4 ToS field as the DS field. The DSCP priority is denoted by the first 6 bits (bits 0 ~ 5), with available values ranging from 0 to 63, while the last 2 bits (bits 6-7) are reserved. The DSCP page allows you to set which DSCP priority maps to which CoS priority. In order to enable DSCP quality of service you must set **DSCP** to **Enable**. Click **Apply** to finalize any setting changes on this page.



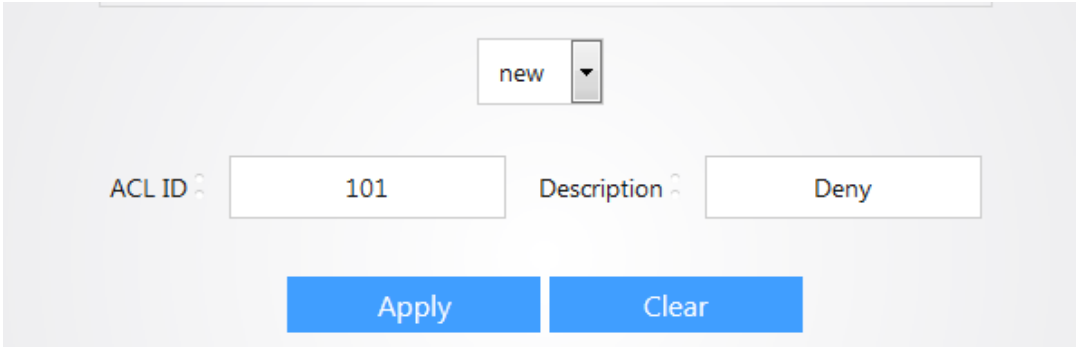
The Port Priority page allows you to define priority on the physical ports of the switch. The available values range from 0 to 7. It is used to determine the forwarding sequence of packets not carrying priority identifiers. Select the ports you want to configure, and then set the **CoS Priority** down below. 0 is the lowest priority and 7 is the highest. Click **Apply** to finalize your settings.



ACL

As traffic increases and network grows, network security appears more and more important. Pack filter can effectively block unauthorized users from accessing network and control traffic volume on the network for the purpose of conserving network resources. An access control list (ACL) implements packet filter via configured rules and operations attached to a packet. When the switch receives a packet, it analyzes the packet using currently applied ACL rules and then handles the packet by preset operations.

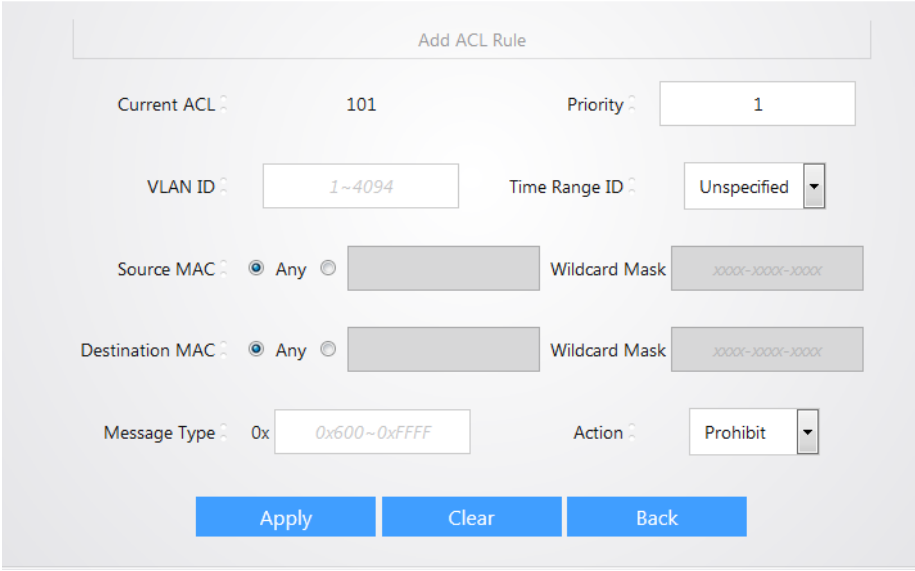
The MAC Based ACL page allows you to define ACLs by MAC address. To create a new ACL, enter an **ACL ID** and **Description**. Click **Apply**.



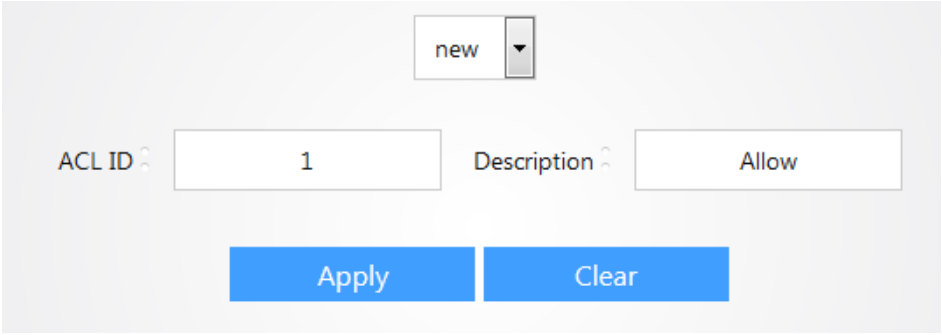
The following table describes the options listed under the ACL Rule page.

Field	Description
Current ACL	Select an existing ACL and specify rules for it.
Priority	Specify a priority for a given rule, which determines match scheduling order. If an ACL has multiple rules, the rule with smallest priority value will be first scheduled for match purpose.

VLAN ID	Specify the VLAN ID of the messages for ACL rules to apply.
Source/Destination MAC	Specify source MAC and destination MAC of packets for a rule to match. Note: If Any is selected, the rule will match and apply to all packets with whatever source MAC/destination MAC.
Message Type	Specify the message type in Hex.
Action	Permit: Allow messages that match existing rules to pass. Prohibit: Discard messages that match existing rules. Rate Limit: Limit forwarding rate of messages that match existing rules (64-1048576kbps). The default action is Prohibit.
Time Range ID	Select time range ID for rule application. Within the set time range, rules will take effect. By default, no time range is specified and ACL rules take effect at any time.

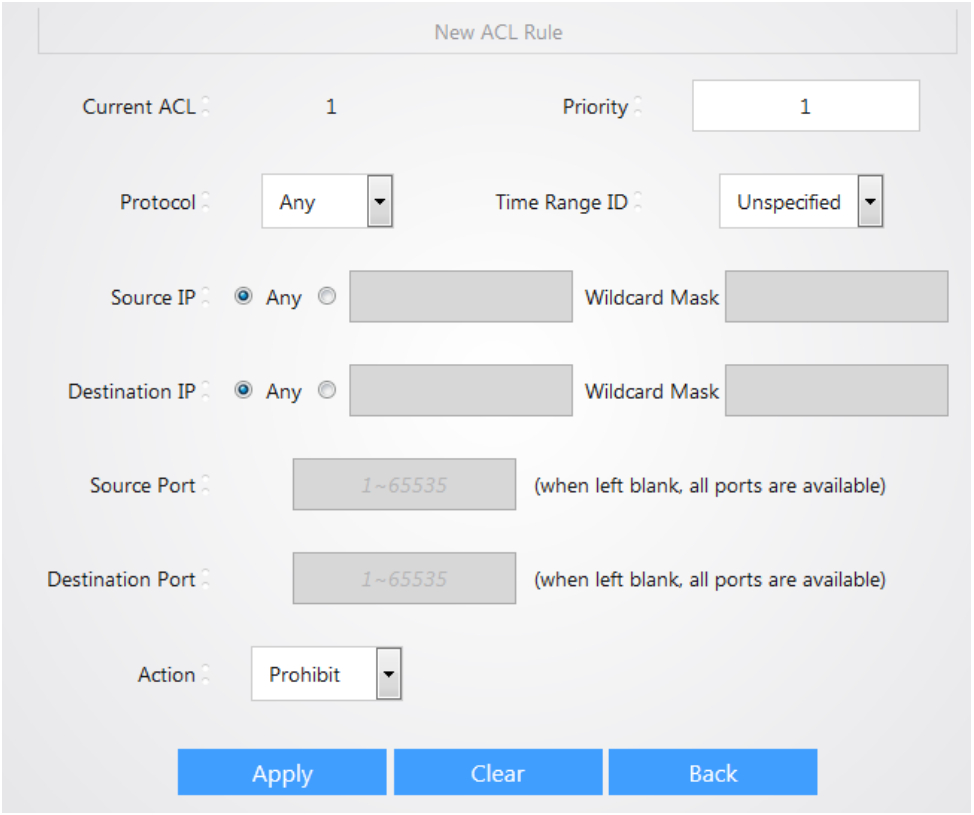


The IP Based ACL allows you to create define ACLs by IP address or Port number. To create a new ACL, enter an **ACL ID** and **Description**. Click **Apply**.

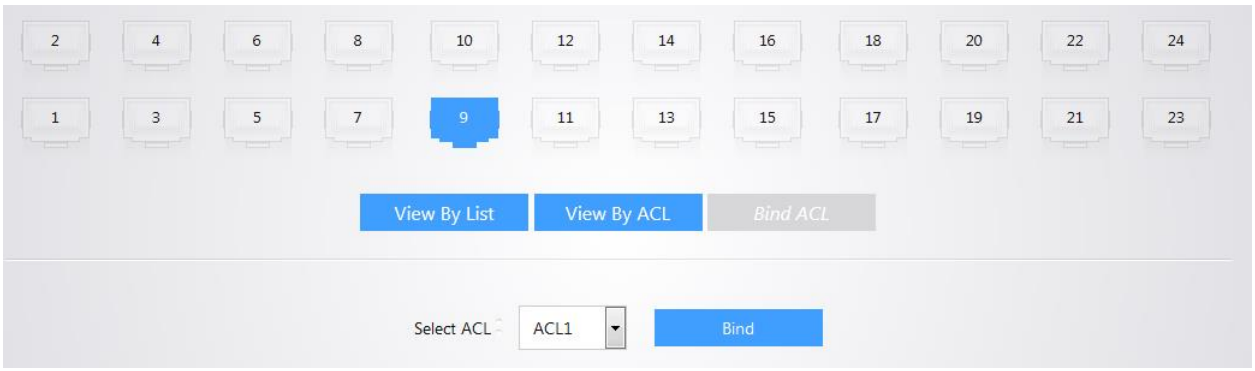


The following table describes the options listed under the ACL Rule page.

Field	Description
Current ACL	Select an existing ACL and specify rules for it.
Priority	Specify a priority for a given rule, which determines match scheduling order. If an ACL has multiple rules, the rule with the smallest priority value will be first scheduled for match purpose.
Protocol	Select a protocol to match.
Source/Destination IP	Specify source IP and destination IP of packets for a rule to match. Note: If Any is selected, the rule will match and apply to all packets with whatever source IP/destination IP.
Source Port	Specify source port number to match TCP/UDP messages. Note: If Any is selected, the rule will match and apply to any source port. Source port is configurable only when TCP or UDP protocol is selected.
Destination Port	Specify destination port number to match TCP/UDP messages. Note: If Any is selected, the rule will match and apply to any destination port. Destination port is configurable only when TCP or UDP protocol is selected.
Action	Specify an action to handle messages: Permit: Allow messages that match existing rules to pass. Prohibit: Discard messages that match existing rules. Rate Limit: Limit forwarding rate of messages that



The Port ACL Binding page allows you to bind an ACL to a port. Simply click **Bind ACL** and then select the port you want to bind the ACL to. Click **Bind** to finalize the settings.



STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. On Ethernet, only a single active path at a time can be maintained between any two network nodes to avoid broadcast storm. However, spare (redundant) links are indispensable to ensure reliability. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, and disable those that are not part of the spanning tree, leaving a single active path between any two network nodes. This is accomplished in the STP. A STP-enabled switch can perform the following tasks:

1. Discover and generate an optimum STP topology.
2. Discover and repair failures on the network; automatically update the network topology for future use. Local topology is generated by computing bridge configurations made by a network administrator. Thus, if configured properly, an optimum topology tree can be generated.

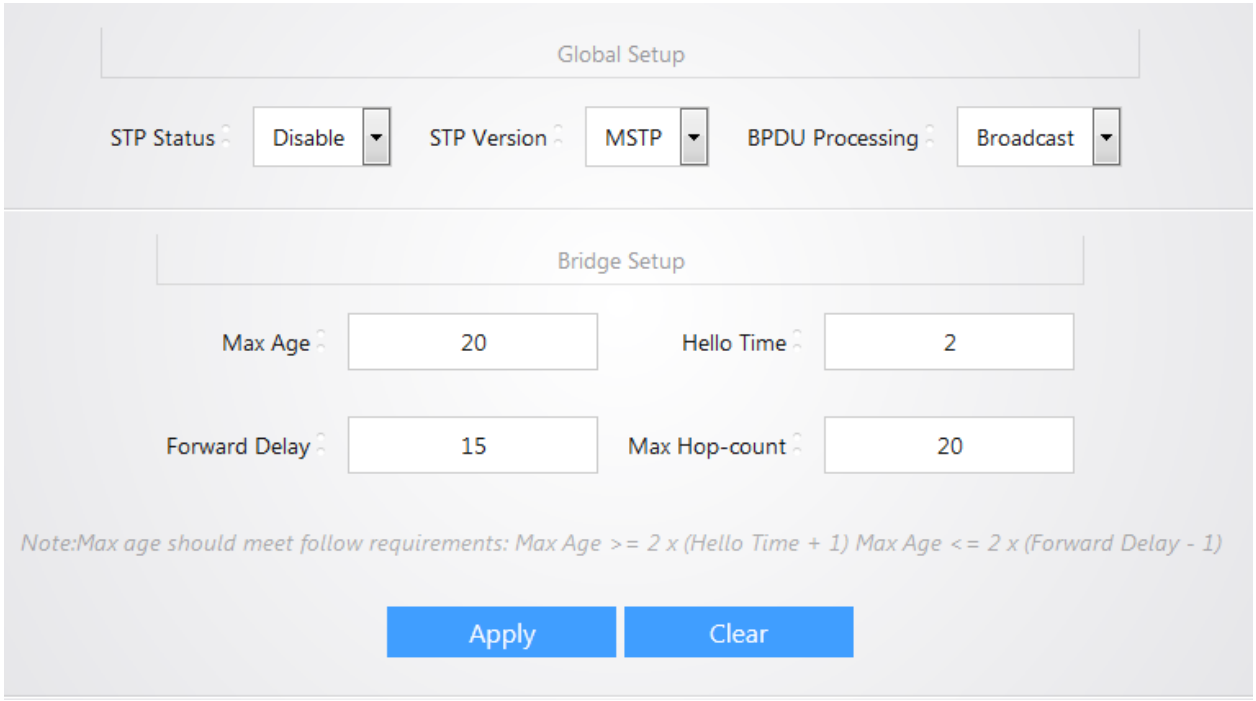
RSTP (Rapid Spanning Tree Protocol) provides significantly faster spanning tree convergence after a topology changes, introducing new convergence behaviors and bridge port roles to do this. RSTP is designed to be backwards-compatible with standard STP. RSTP is typically able to respond to changes within one second while STP can take 30 to 50 seconds to respond to a topology change. RSTP delivers fast transition to forwarding status without relying on timer settings. A RSTP bridge is responsive to other RSTP bridge's link status. The port does not need to wait for the topology to become stable. Edge port and P2P port are introduced to the protocol for faster transition. The explanation of an Edge port and a P2P port is shown below:

Edge port: The edge port is a configurable designation port that is directly connected to a segment where a loop cannot be created. Usually it would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P port: A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration. The three protocols are mutually compatible and no conflicts or network collapses will be caused in spanning tree application.

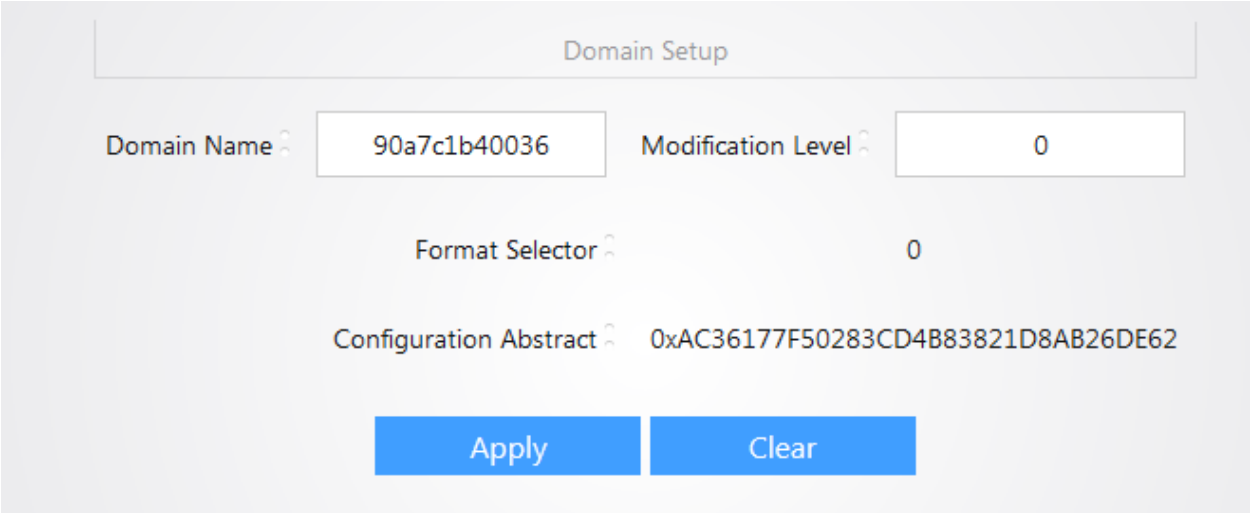
MSTP divides a network into several MST regions. The CST is generated between these MST regions, and multiple spanning trees can be generated in each MST region. Each spanning tree is called an instance. As well as STP, MSTP uses BPDUs to generate spanning tree. The only difference is that the BPDU for MSTP carries the MSTP configuration information on the switches. MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST). Unlike some proprietary per-VLAN spanning tree implementations, MSTP includes all of its spanning tree information in a single BPDU format. Not only does this reduce the number of BPDUs required on a LAN to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP does this by encoding additional region information after the standard RSTP BPDU as well as a number of MSTI messages (from 0 to 64 instances, although in practice many bridges support fewer). Each of these MSTI configuration messages conveys the spanning tree information for each instance. Each instance can be assigned a number of configured VLANs and frames (packets) assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. In order to avoid conveying the entire VLAN to spanning tree mapping in each BPDU, bridges encode an MD5 digest of their VLAN to instance table in the MSTP BPDU. This digest is then used by other MSTP bridges, along with other administratively configured values, to determine if the neighboring bridge is in the same MST region as itself.

The table down below describes the options under the Global Setup page.



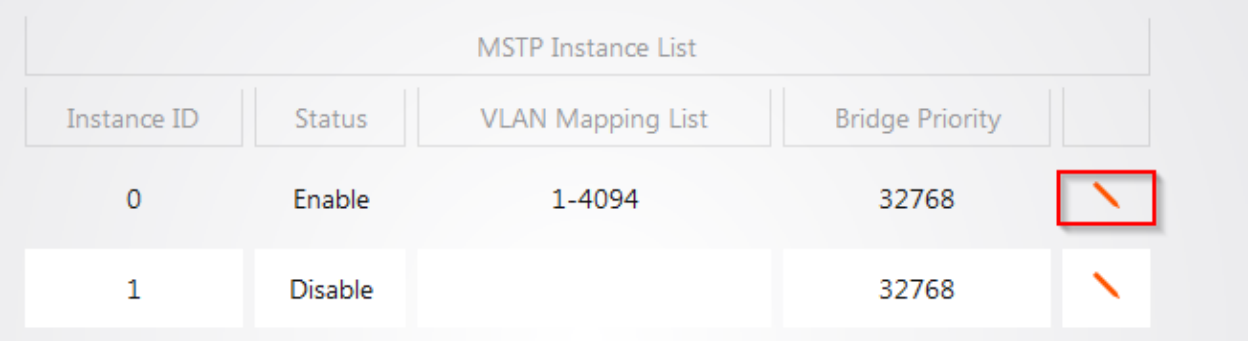
Field	Description
STP Status	Enable/Disable STP globally. By default, the STP feature is disabled.
STP Version	Select the desired version of STP version: MSTP/RSTP/STP compatible to eliminate loops on data link layer. The default is RSTP mode.
BPDU Processing	Select a BPDU processing method: Broadcast/Filter. This option takes effect only if STP is disabled globally. By default, BPDU packets are broadcasted.
Max Age	Config a max aging time for messages. You may choose a time between 6 and 40 seconds. The default value is 20s.
Hello Time	Config the Hello Time. You may choose a time between 1 and 10 seconds. The default value is 2s.
Forward Delay	The latency time for a bridge port to switch from a Listening state to a Learning state or from a Learning state to a Forwarding state. Valid values range from 4 to 30 seconds. The default is 15s.
Max Hop-count	Config max hop-count. In MSTP mode, it decreases by 1 upon every switch. If the received BPDU hop value is 1, this packet will be discarded.

The Table down below describes the options under the Domain Setup.

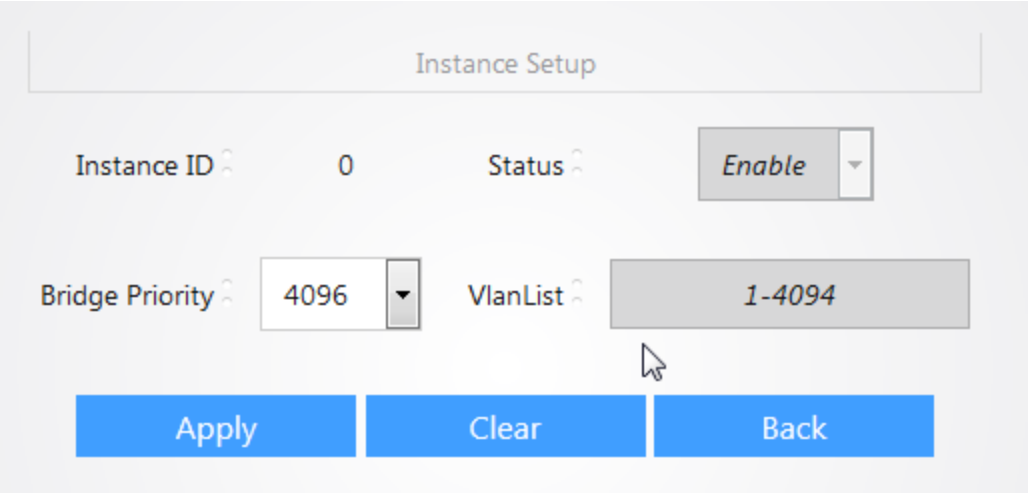


Field	Description
Domain Name	Config switch domain name (32 characters allowed). The default is the device's MAC address.
Modification Level	Config MSTP modification level. Valid range is 0-65535. The default is 0.
Format Selector	Display 0.
Configuration Abstract	A value worked out by VLAN mapping, belonging to an important parameter of the inter-domain calculation.

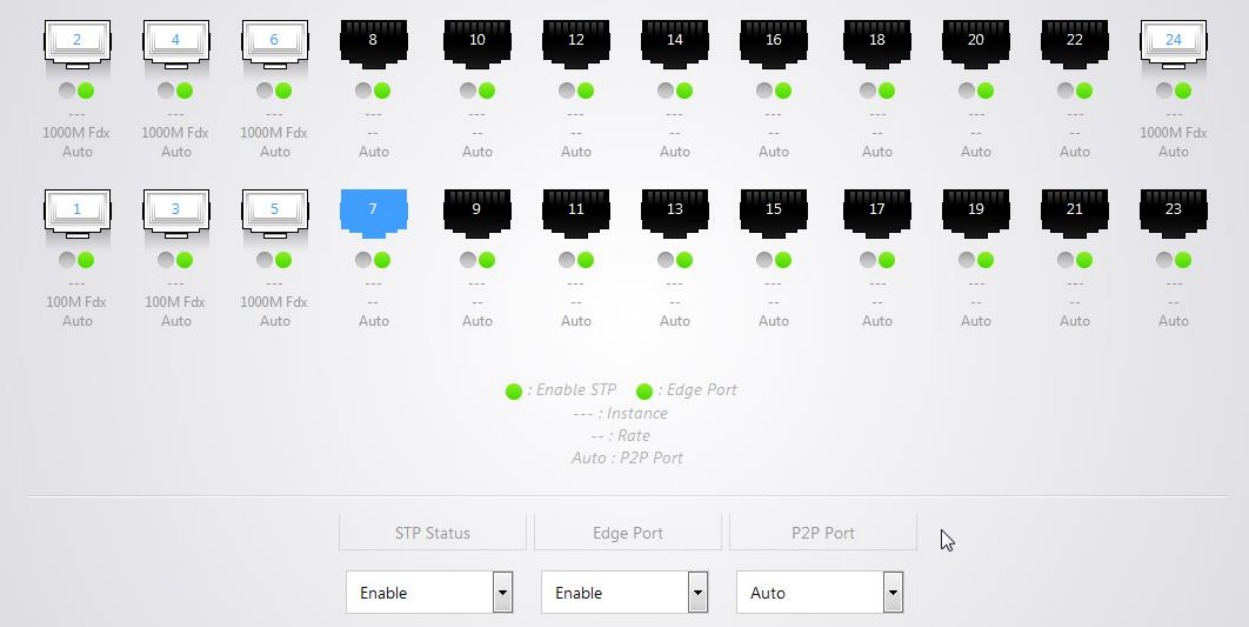
The MSTP Instance page allows you to specify the Bridge priority for each instance of STP running on the network. To edit the first instance, click the edit icon next to Instance ID 0.



Here you select the Bridge Priority for this instance of STP. Click **Apply** when finished.



The Port Setup page allows you to specify which ports should have STP enabled. Ports that are connected to other switches or access points should have STP enabled on them. You can also configure Edge and P2P port settings.

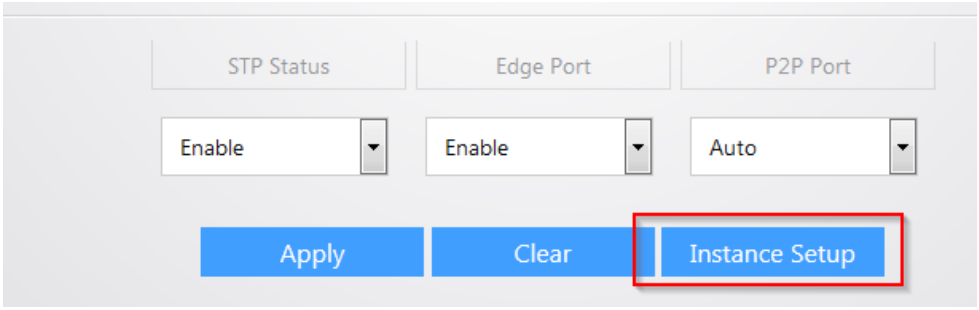


The Table describes the settings listed down below on the Port Setup page.

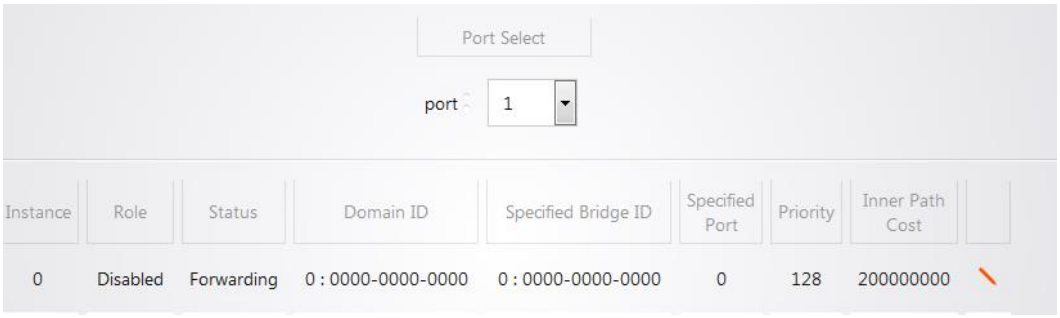
Field	Description
STP Status	Select to enable/disable the STP feature or make no change. By default, the STP feature is disabled. To activate the STP feature, you must enable STP both globally on the entire device and specifically on desired port(s).
Edge Port	An edge port is a port that is connected to the terminal directly. Ports that are designated as edge ports transit rapidly from the blocked state to the forwarding state without delay. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port. By default, all ports are edge ports.

P2P Port	A P2P port is also capable of rapid transition. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports. By default, port establishes a link automatically.

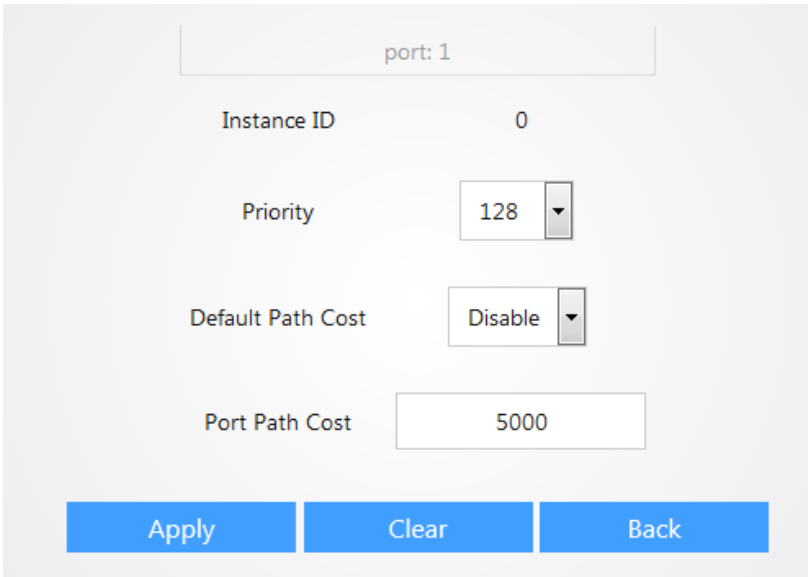
Click **Apply** to finalize any setting changes on the port setup page. The Instance setup page will allow you to specify the path cost of a port. Click **Instance Setup**.



Select a **Port**. Click the edit icon next to **instance 0**.



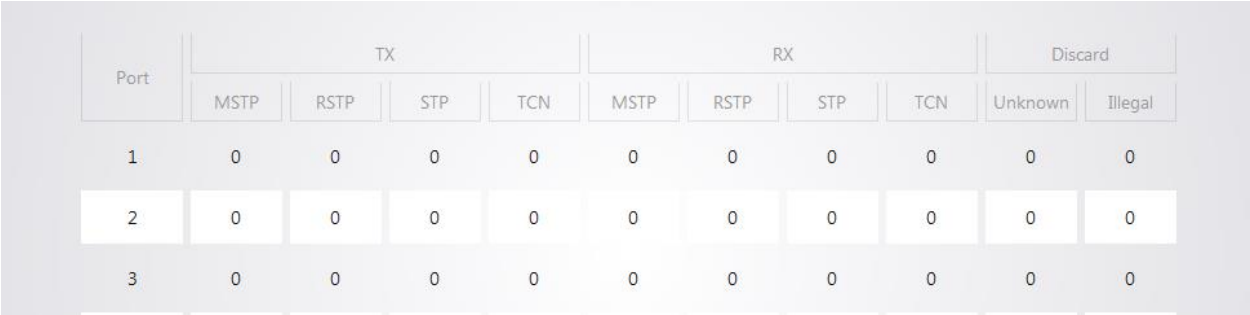
Here you can set the **Priority** and **Port Path Cost**. The table down below describes the settings on this page.



Priority	By default, the port priority is set to 128.

Default Path Cost	Enable/disable port default path cost. You can specify a custom port path cost between 1 and 200,000,000 if you disable the default port path cost. When enabled, port path cost can be configured automatically and 802.1at is supported.
Port Path Cost	The default path cost is 200,000,000. Only if you disable the default path cost option, can path cost be configurable.

The Port Statistics page displays STP information for each port.

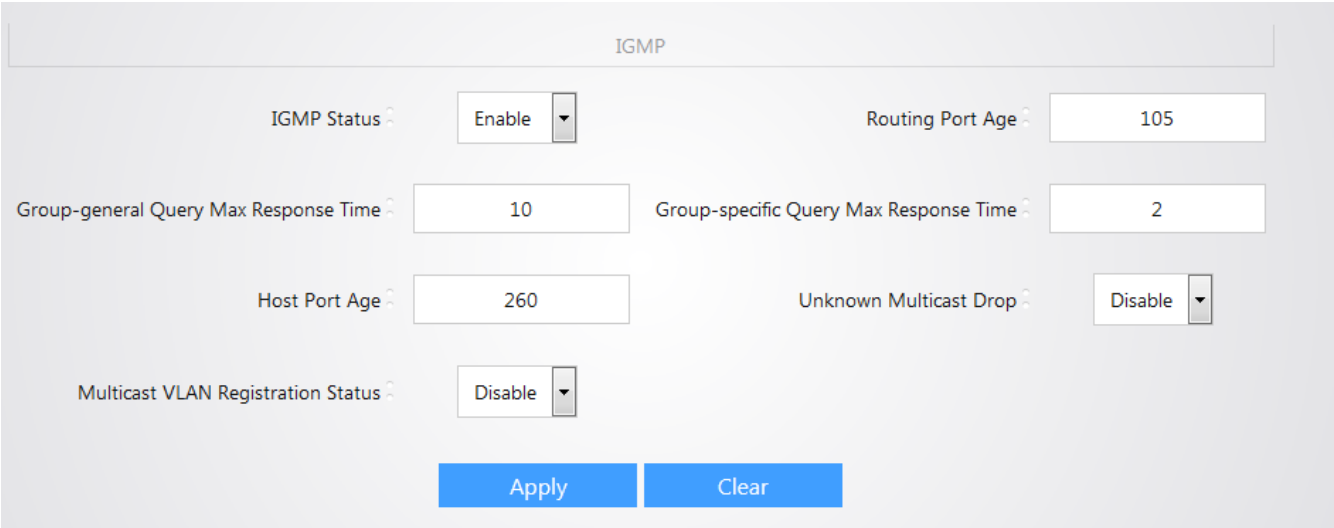


Port	TX				RX				Discard	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0

IGMP

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP snooping, as implied by the name, is a feature that allows a network switch to listen to on the IGMP conversation between hosts and routers. By listening to the conversations between hosts and routers, the switch maintains a map of links which need IP multicast streams. Multicast streams may be filtered from the links which do not solicit them. An IGMP-Snooping-disabled layer-2 device will flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). With IGMP snooping enabled, known multicast traffic will be forwarded to hosts that have explicitly joined the group. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client).

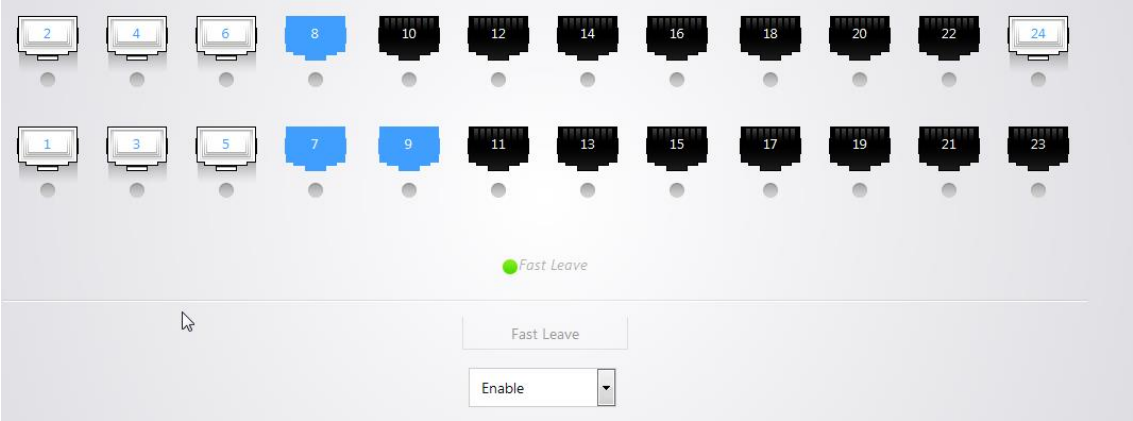
The IGMP page will allow you to configure IGMP snooping settings. The table down below describes the settings displayed on the page. Click Apply to finalize settings on this page.



Field	Description

IGSP Status	Enable/disable the IGMP Snooping feature.
Routing Port Age	Config routing port aging time (1-1000 sec). The default is 105s.
Group-general Query Max Response Time	Config max amount of time in response to group-general query messages (1-25 sec). The default is 10s.
Group-specific Query Max Response Time	Config max amount of time in response to group-specific query messages (1-5 sec). The default is 2s.
Host Port Age	Config host port aging time (200-1000 sec). The default is 260s.
Unknown Multicast Drop	Enable/disable the unregistered multicast discard feature. This feature takes effect only if the IGSP feature has been enabled globally on the device.
Multicast VLAN Status	Enable/Disable multicast VLAN. When multicast VLAN is enabled, multicast VLAN ID becomes configurable and multicast packets can only be forwarded in this VLAN.
Multicast VLAN ID	This option becomes visible when multicast VLAN is enabled. This VLAN ID must already exist in 802.1Q VLAN and only ports in this VLAN can forward multicast packets. Valid range is 1-4094.

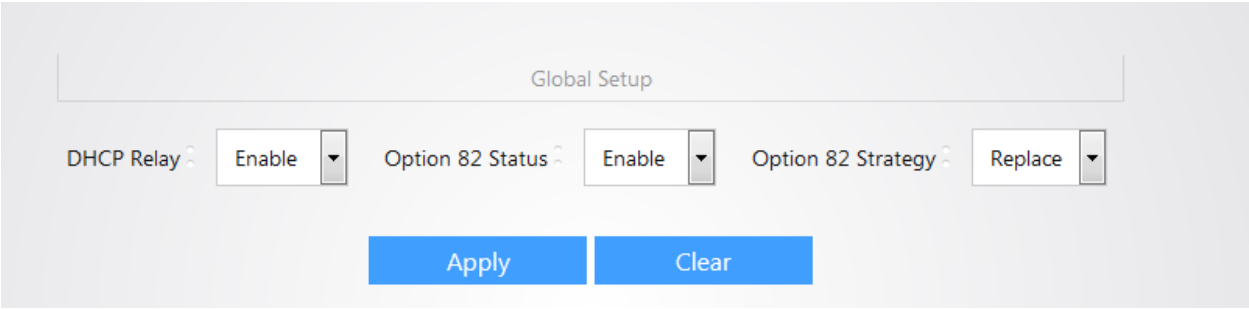
The Fast Leave page allows you to enable fast leave on any of the ports of the switch. Simply select the ports you would like to configure and then configure the Fast Leave option down below. Click Apply to finalize your settings.



DHCP RELAY

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you have to configure the DHCP Relay Agent on the subnet that contains the remote clients, so that it can relay DHCP broadcast messages to your DHCP server.

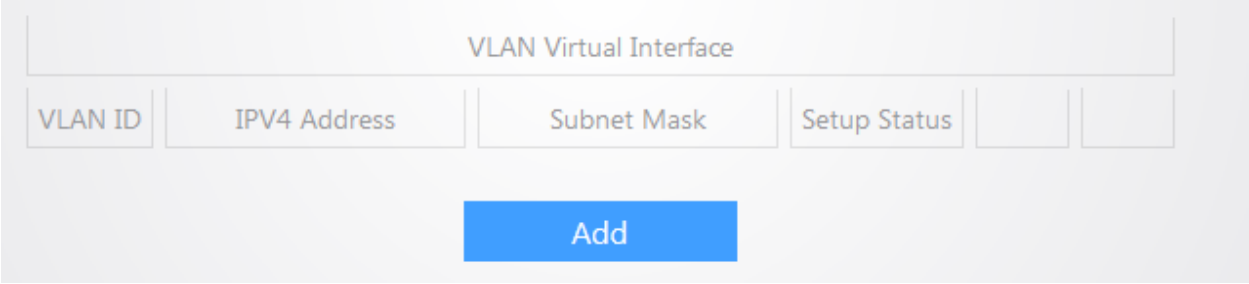
The table further below describes the different settings on this page.



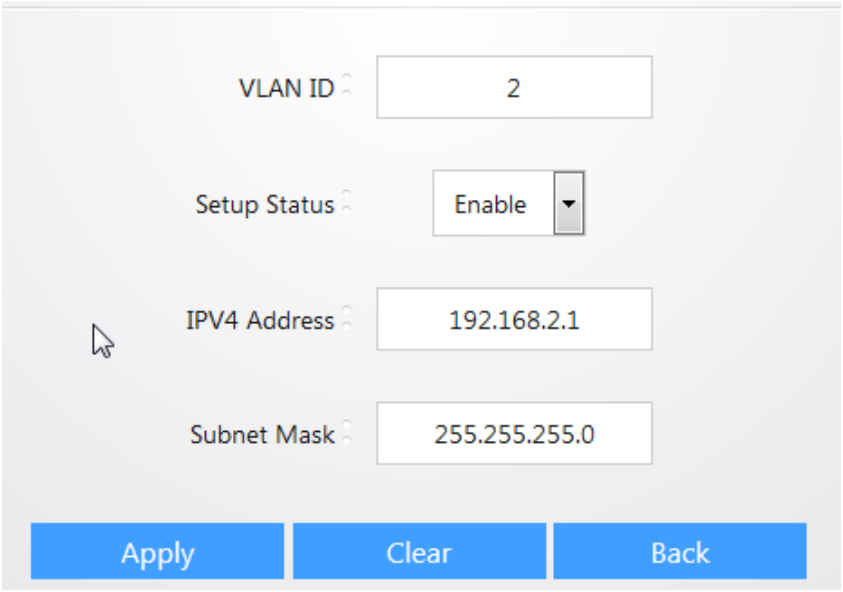
Field	Description
DHCP Relay	Enable/Disable DHCP relay feature. DHCP relay will only take effect when DHCP relay is enabled globally. By default, it is disabled.
Option82 Status	Enable/Disable Option82 feature. Option 82 strategy will only take effect when Option 82 is enabled.

Option82 Strategy	Three strategies are available: replace, keep, drop.

Click **Add** under the Virtual VLAN interface to add an interface for a VLAN on the switch.



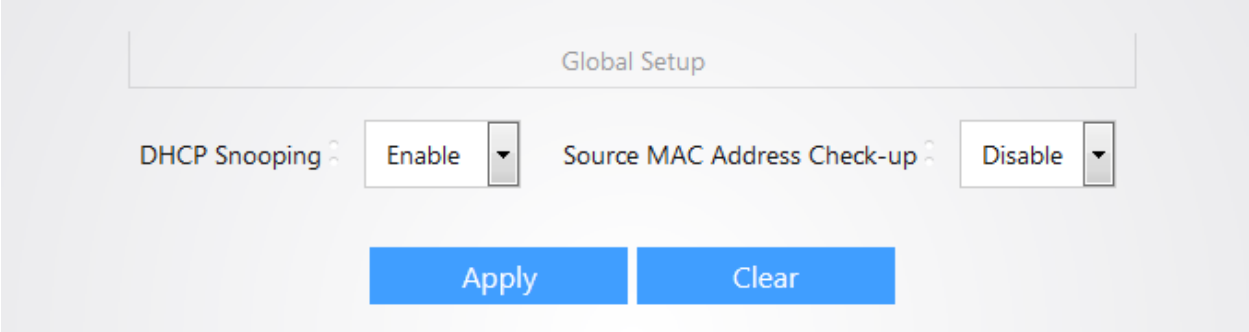
Enter a **VLAN ID** for this interface. Select **Enable** for the Setup Status. Specify a valid IP Address for VLAN 2. Specify a valid Subnet Mask. The following image illustrates this. Click **Apply** to finalize your settings.



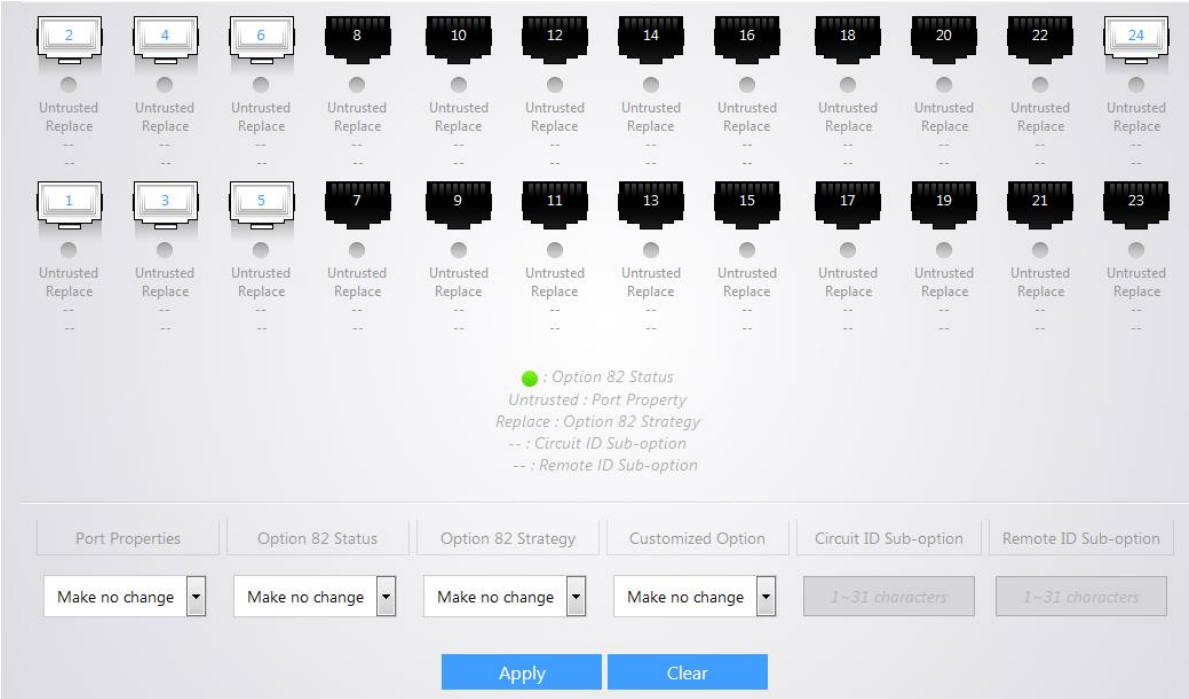
DHCP SNOOPING

In computer networking, DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. If illegal DHCP servers exist in computer networking, DHCP clients might obtain incorrect IP addresses and parameters, thus leading to abnormal communication. In order that DHCP clients obtain IP addresses via legal DHCP servers, trusted ports and untrusted ports are configured. After receiving DHCP-ACK and DHCP-OFFER packets, untrusted ports will discard these packets. Ports which are connected to DHCP servers and other DHCP Snooping devices need to be configured as trusted ports and other ports need to be configured as untrusted ports, so that DHCP clients can only obtain IP addresses from legal DHCP clients.

The DHP Snooping page will allow you to enable and configure the different DHCP Snooping options. Set the DHCP Snooping field to **Enable**. The **Source MAC Address Check-up** specifies whether the source MAC address check-up feature is enabled or not. Click **Apply** to enable the DHCP Snooping feature.



The table further below describes the options in the following image.

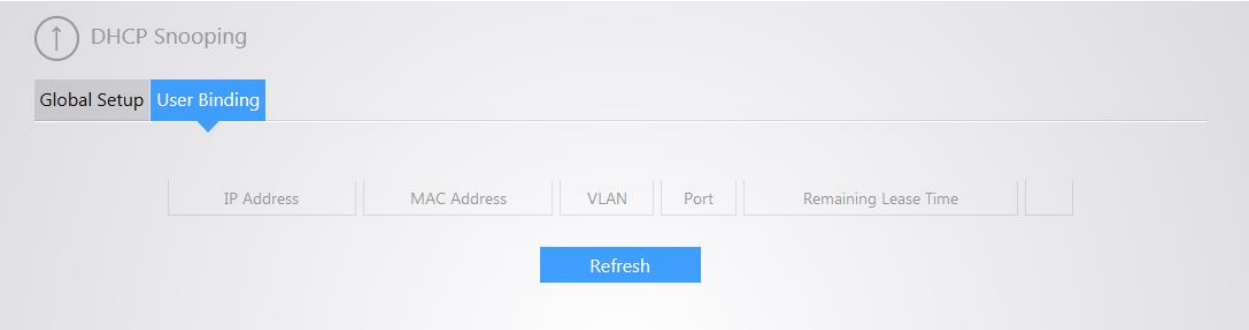


Field	Description
Port	The corresponding port number.
Port Property	Configure the current port's DHCP snooping property.

Option82 Status	Enable/Disable option 82. Option 82 records DHCP clients' location info.

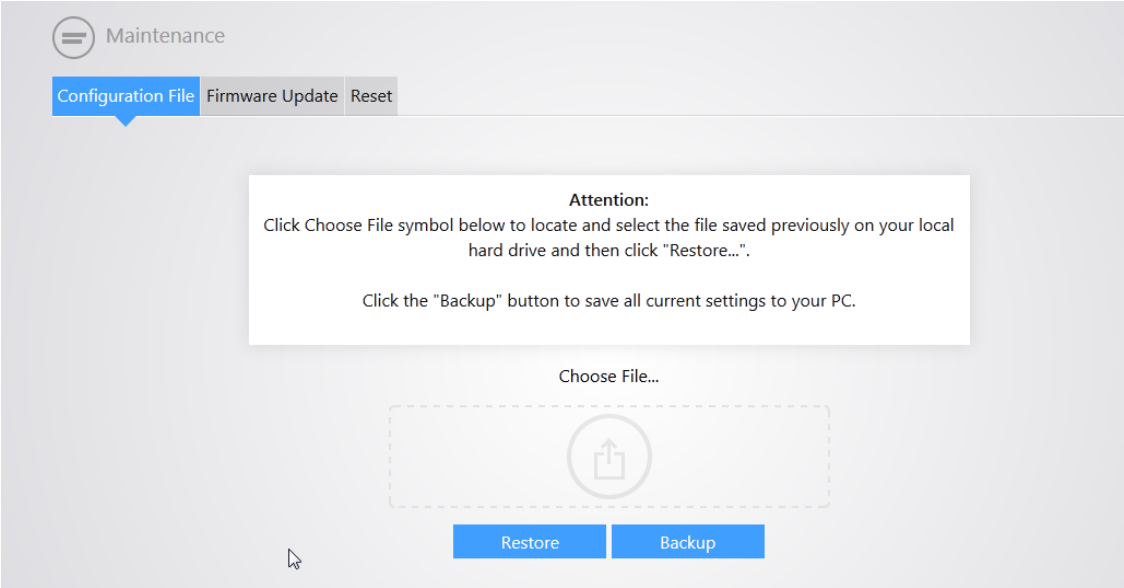
Option82 Strategy	When DHCP snooping receives DHCP packets, it will process these packets according to whether Option 82 included, processing strategy of user configuration and fill pattern, and then forward them to DHCP server. Three strategies are available: replace, keep and drop.
Circuit ID Sub-option	Configure the current port's circuit ID sub-option.
Remote ID Sub-option	Configure the current port's remote ID sub-option.
Back	Click it to go back to port setup page.

The User Binding page will display user binding digits in the list.

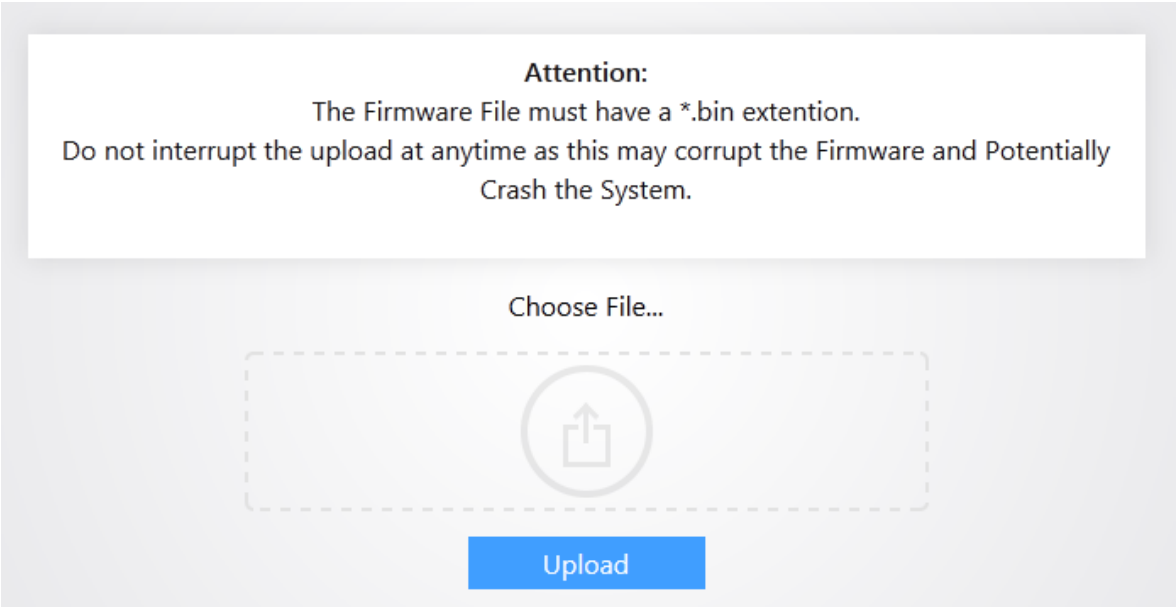


MAINTENANCE

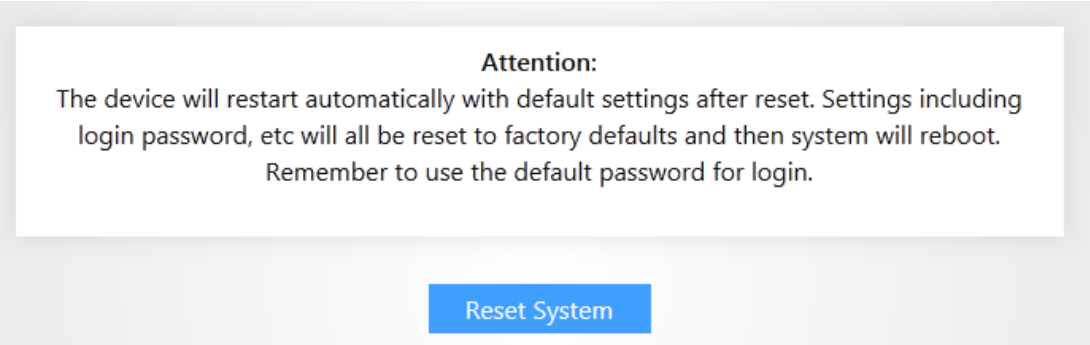
The Maintenance page will allow you to backup/restore configurations, perform firmware updates and factory reset the switch. To create a backup of your configuration, simple click **Backup**. To restore a configuration, click the icon and navigate to your configuration file. Click **Restore**.



The Firmware Update allows you to update the systems firmware. Simply click the icon and browse to the firmware file. Click **Upload**.



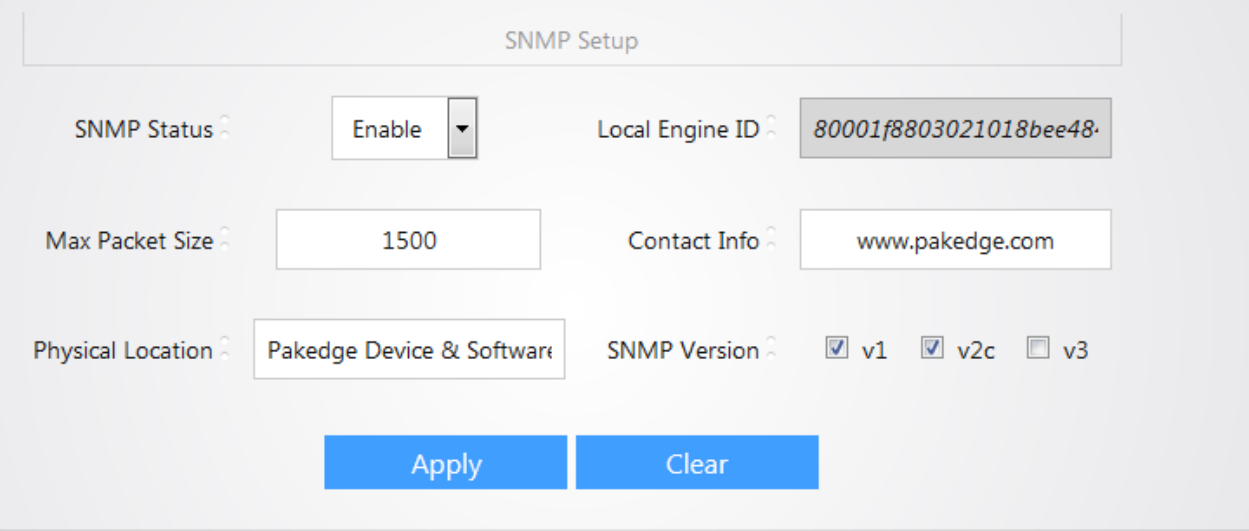
The Reset page will allow you to factory reset the switch. Simply click **Reset System** and the switch will then perform a factory reset.



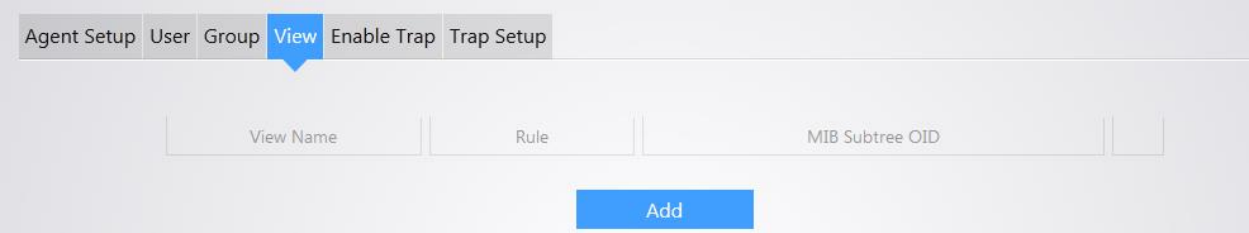
SNMP

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

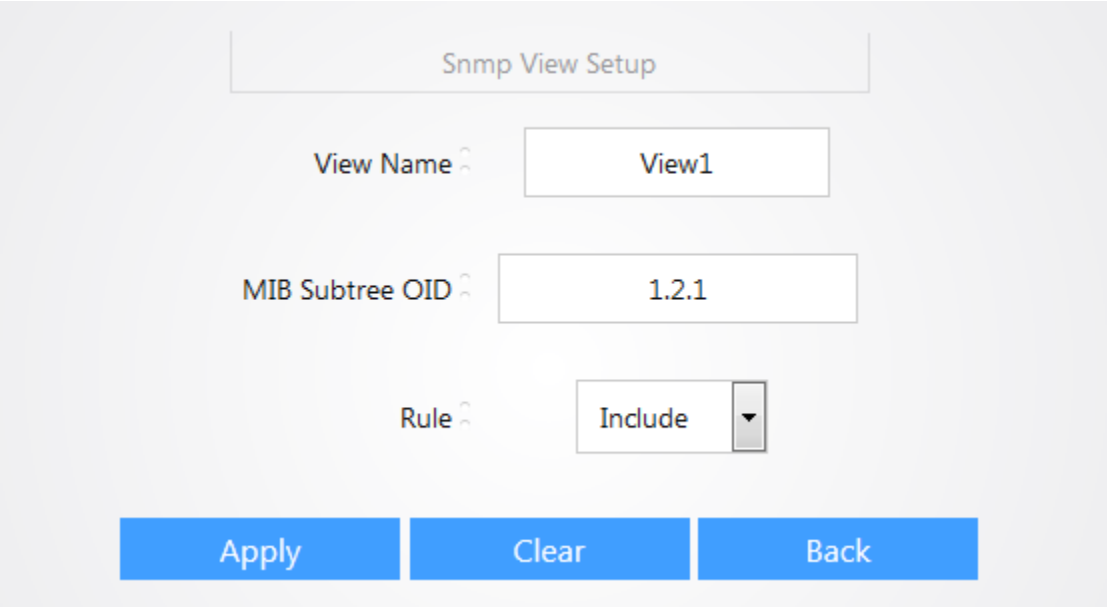
To configure SNMP, set the **SNMP Status** to **Enable**. Specify a **Max Packet Size**, the default is 1500. Enter the **Contact Info** and **Physical Location**. By default, the switch will use SNMP version 1 and 2c. Click **Apply**.



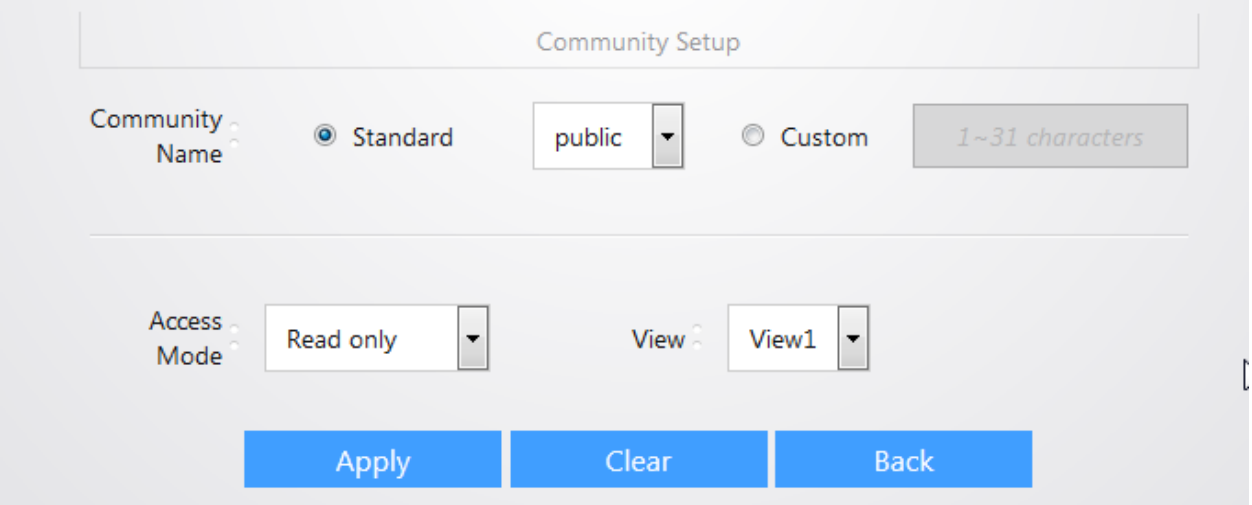
Before you can configure a community name, you must create a view. Click **Add** under the View tab.



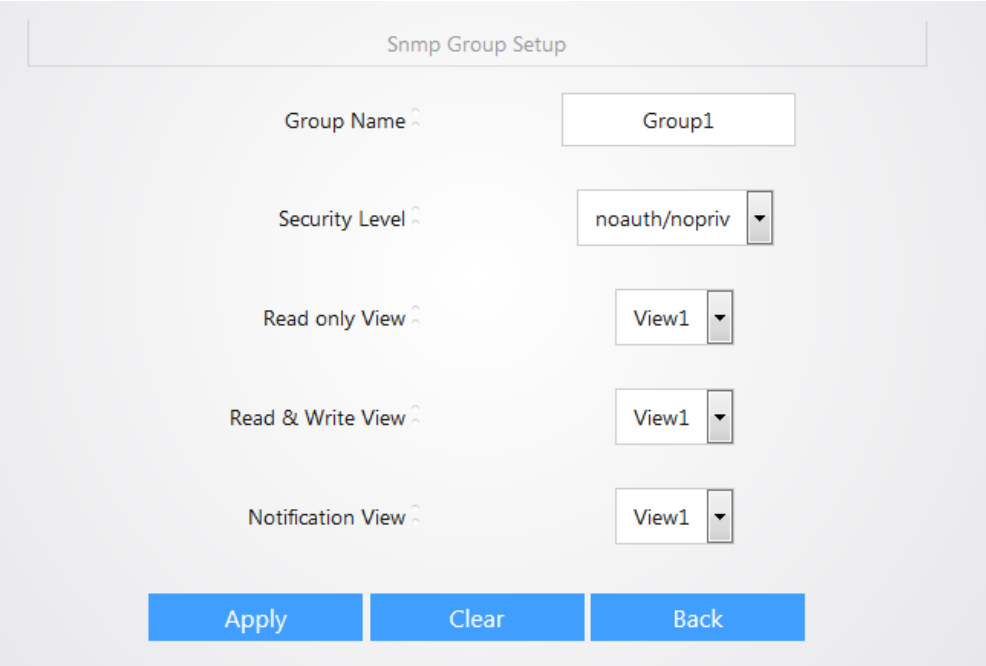
Enter a **View Name**. Enter a **MIB Subtree OID**. Specify a view **Rule**. Click **Apply**.



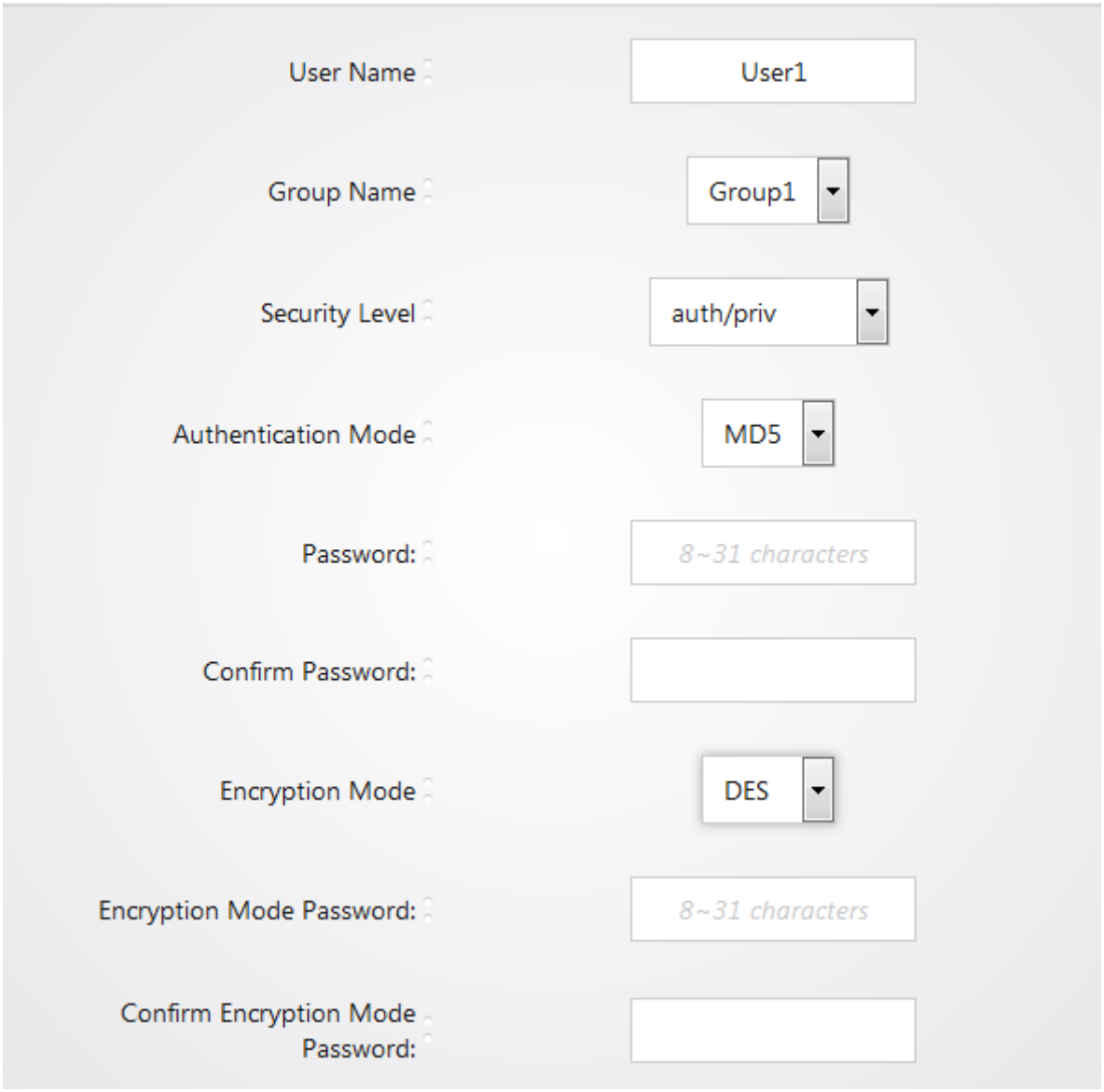
Once the View is created, navigate to the Agent Setup page. Click **Add** towards the bottom to add a community string. Specify a **Community Name**, you can select custom to use a name other than the defaults. Specify an **Access Mode**. Specify a **View**. Click **Apply** to finalize your settings.



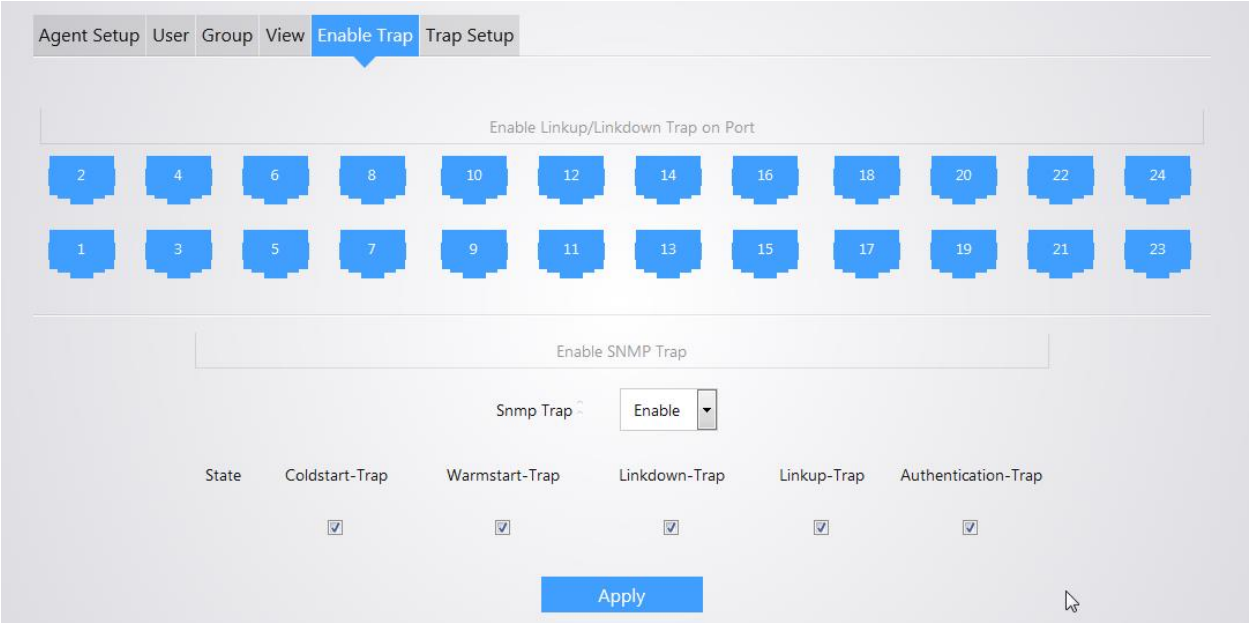
The Group page allows you to create an SNMP group. Specify a **Group Name**. Select a **Security Level**. Specify the **Read only View**, **Read & Write View**, and **Notification View**. Click **Apply** to finalize your settings.



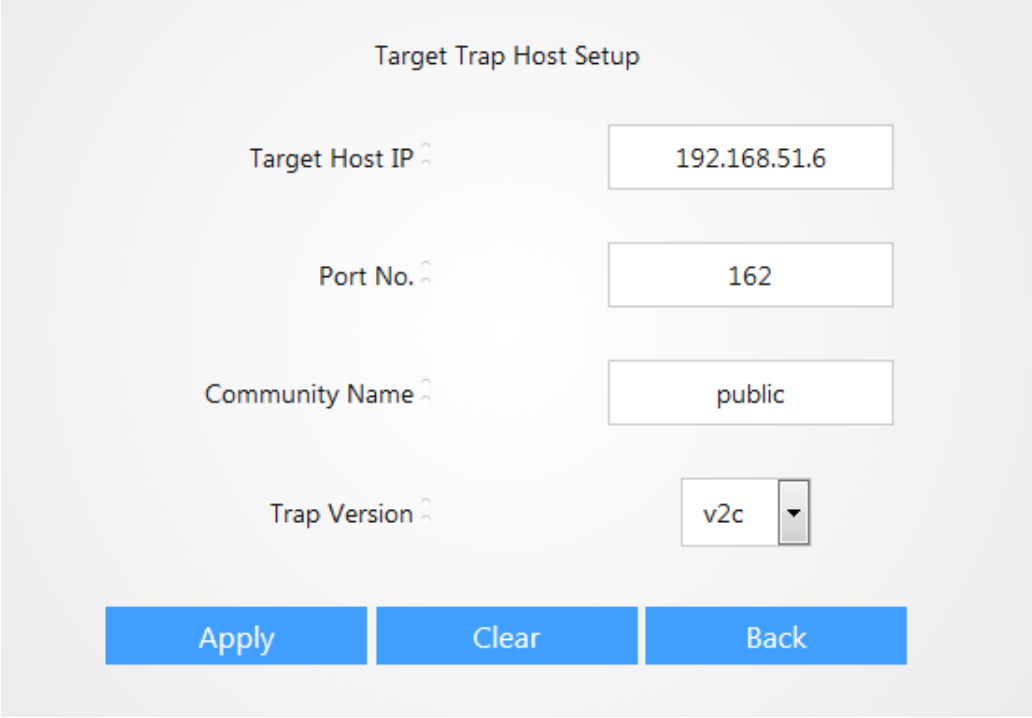
Once you have created an SNMP group, you will be able to create an SNMP user. Specify a **User Name**. Select the **Group Name** and **Security Level** for the user. If security level is set to **auth/priv** you will be able to configure **Authentication Mode** and **Encryption Mode**. Click **Apply** to finalize your settings.



The Enable Trap page allows you specify which ports the switch will send Trap notifications for. By default, all ports are part of the trap notifications. To disable notifications for a port simply select the port and set the **SNMP Trap** to disable.



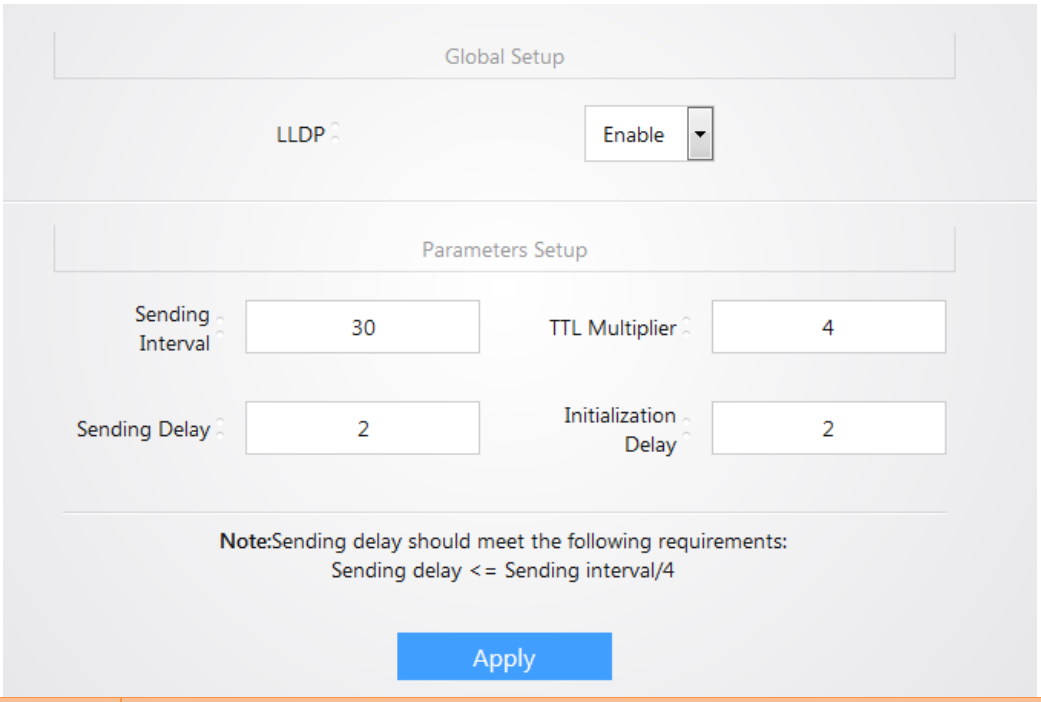
The Trap Setup page allows you to setup where the trap notifications are sent to. Click **Add**. Specify a **Target Host IP**. Enter the **port number** to use when sending the traps. Port 162 is the default port used. Enter a **Community Name** and specify a **Trap Version**. Click **Apply** to finalize your settings.



LLDP

LLDP (Link Layer Discovery Protocol) is a Layer 2 protocol that is used for network devices to advertise their own device information periodically to neighbors on the same IEEE 802 local area network. The advertised information, including details such as device identification, capabilities and configuration settings, is represented in TLV (Type/Length/Value) format according to the IEEE 802.1ab standard, and these TLVs are encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit). The LLDPDU distributed via LLDP is stored by its recipients in a standard MIB (Management Information Base), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

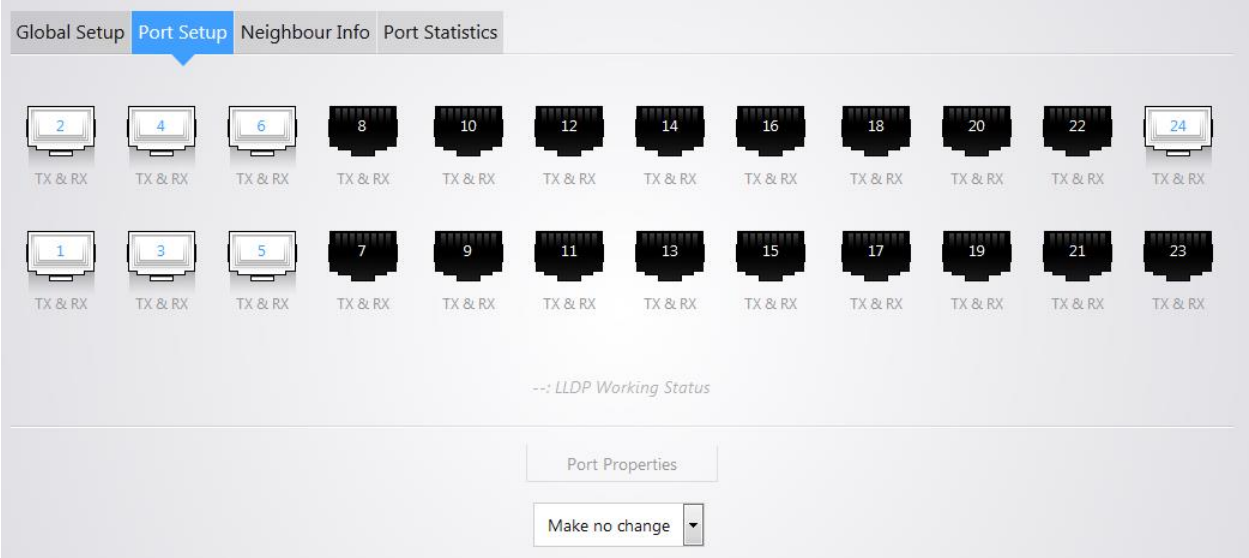
The Table further below describes the options displayed on this page.



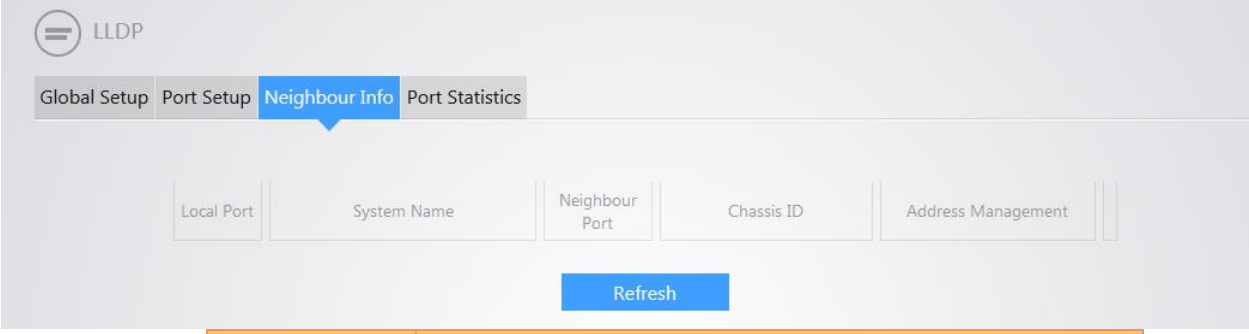
Field	Description
LLDP	Enable/ Disable LLDP feature.
Sending Interval	The interval among each LLDP message (5~32768s).
TTL Multiplier	TTL value is used to configure neighbor info's age time on local devices. TTL = Min (65535, (TTL multiplier × LLDP packet sending time interval)). Through adjusting TTL multiplier, you can control this device info's age time on the neighboring device (2~10s).
Sending Delay	When local configurations change, each LLDP packet will be sent after one sending delay time (1~8192s and <= sending time interval/4).
Initialization Delay	To avoid constant port initialization caused by frequent changes of working mode, you can configure port initialization delay time. When port's working mode changes, the initialization will be delayed for some time (1~10s).

The Port Setup page allows you to configure LLDP port properties. Select a port and you will be able to make any of the following changes:

- **Make no change**: Make no change toward previous configurations. Disable: Disable LLDP feature.
- **TX**: Transmit LLDP packet only. RX: Receive LLDP packet only.
- **TX & RX**: Transmit and receive LLDP packet.

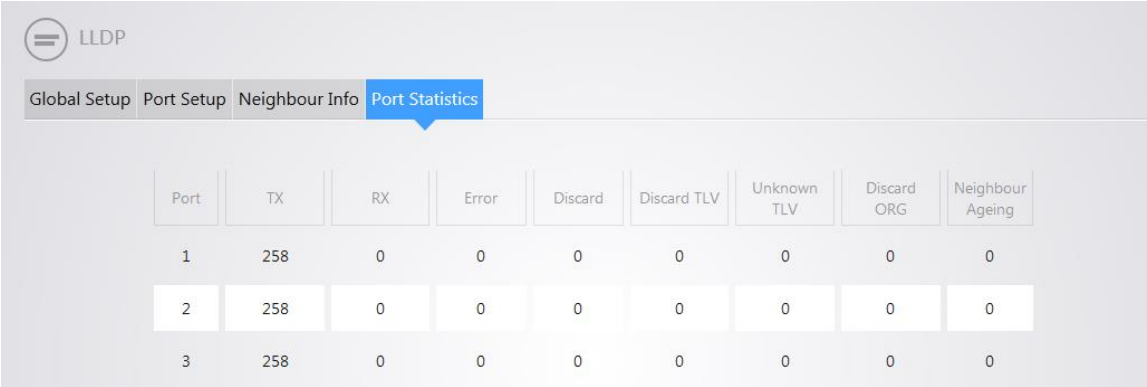


The Neighbour info page will display about devices that were discovered via LLDP. The table further below describes the different options.



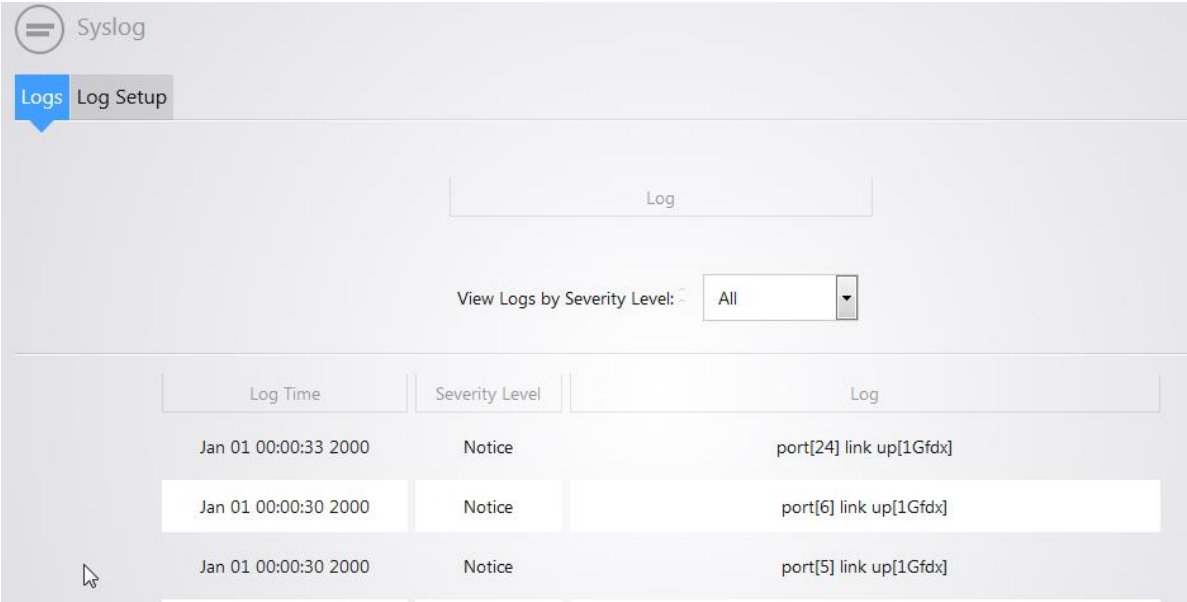
Field	Description
Local Port	Display the port which receives LLDP packet.
System Name	Display the neighboring device's system name.
Neighbor Port	Display the port which sends LLDP packets on the neighboring device.
Chassis ID	Display the MAC address of the neighboring device.
Address Management	Display the management IP address of the neighboring device.

The Port Statistics page will display LLDP statistics on each port.



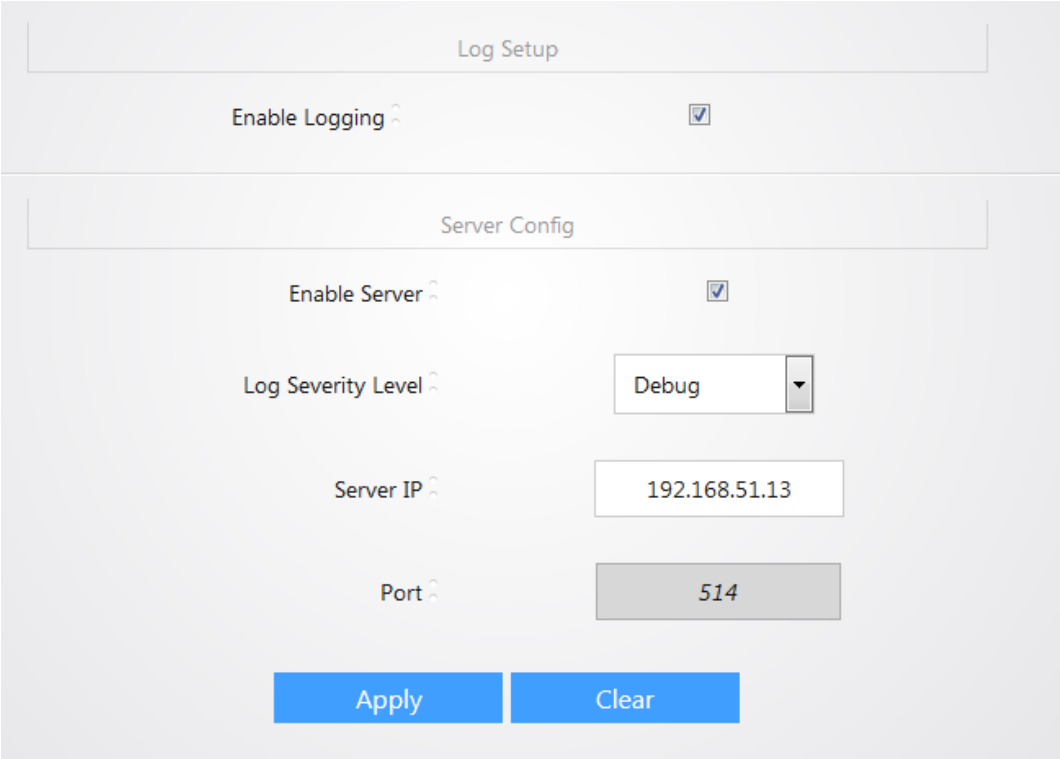
SYSLOG

The Syslog page displays logs from the switch. The table further below describes the different Severity level of logs the switch will display.



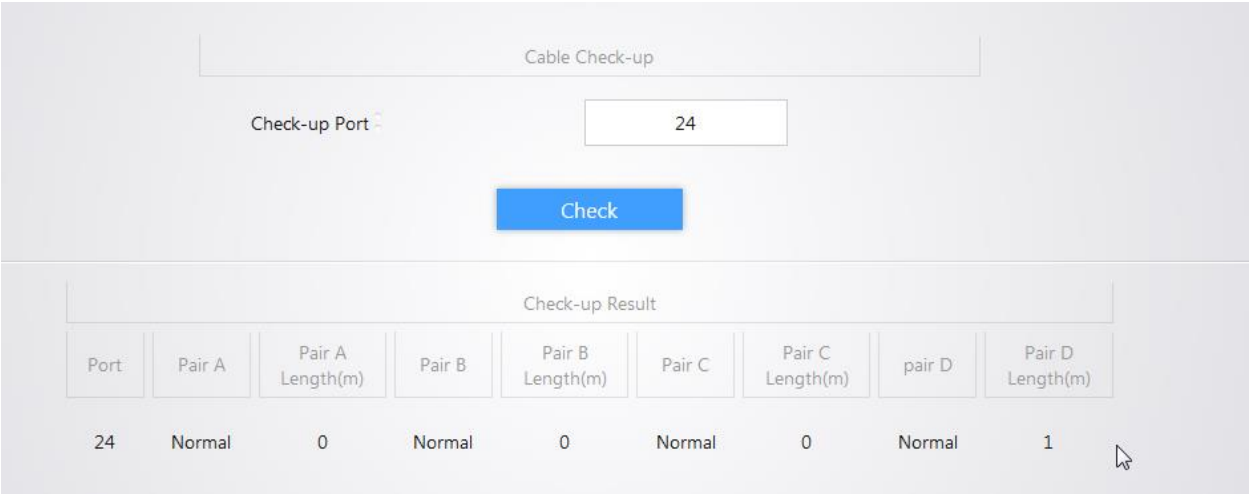
Severity	Level	Description
Emergency	1	The system is unusable
Alert	2	Action must be taken immediately
Critical	3	Critical conditions
Error	4	Error conditions
Warning	5	Warning conditions
Notice	6	Normal but significant conditions
Informational	7	Informational messages
Debug	8	Debug-level messages

The Log Setup page allows you to input a Syslog Server IP address to collect logs. Check the **Enable Logging** box. Check the **Enable Server** box. Select a **Log Severity Level**. Enter a **Server IP address**. Click **Apply** to finalize your settings.

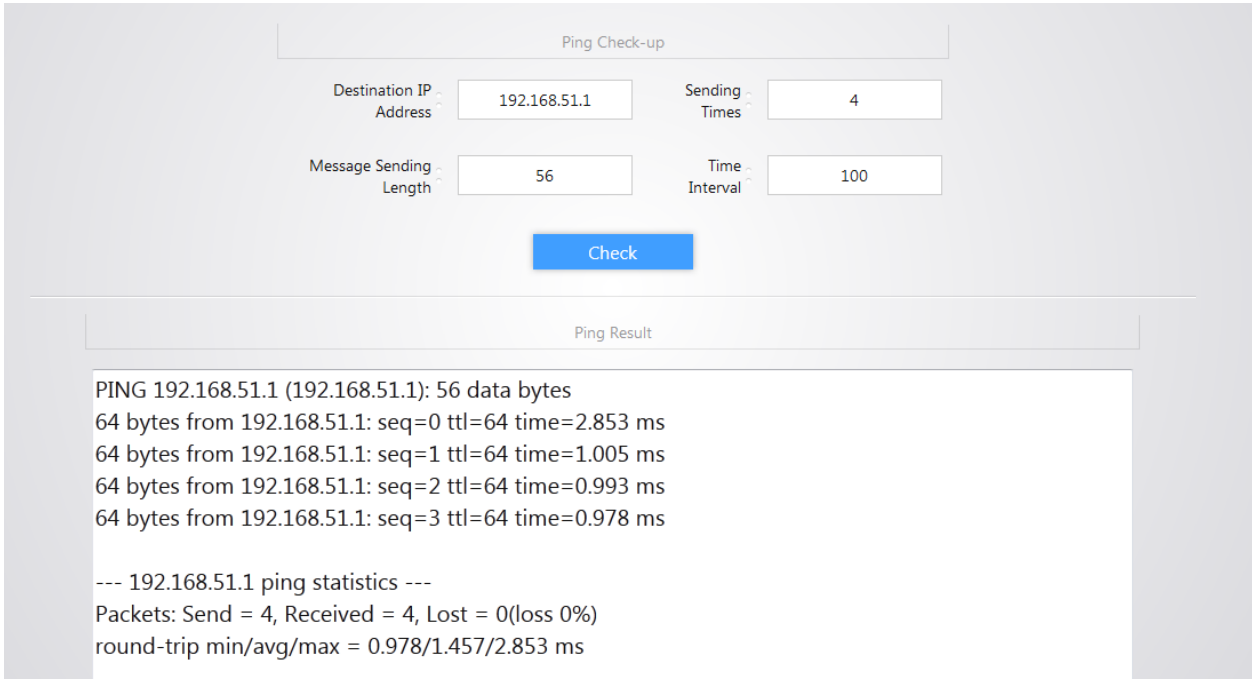


NETWORK DIAGNOSTICS

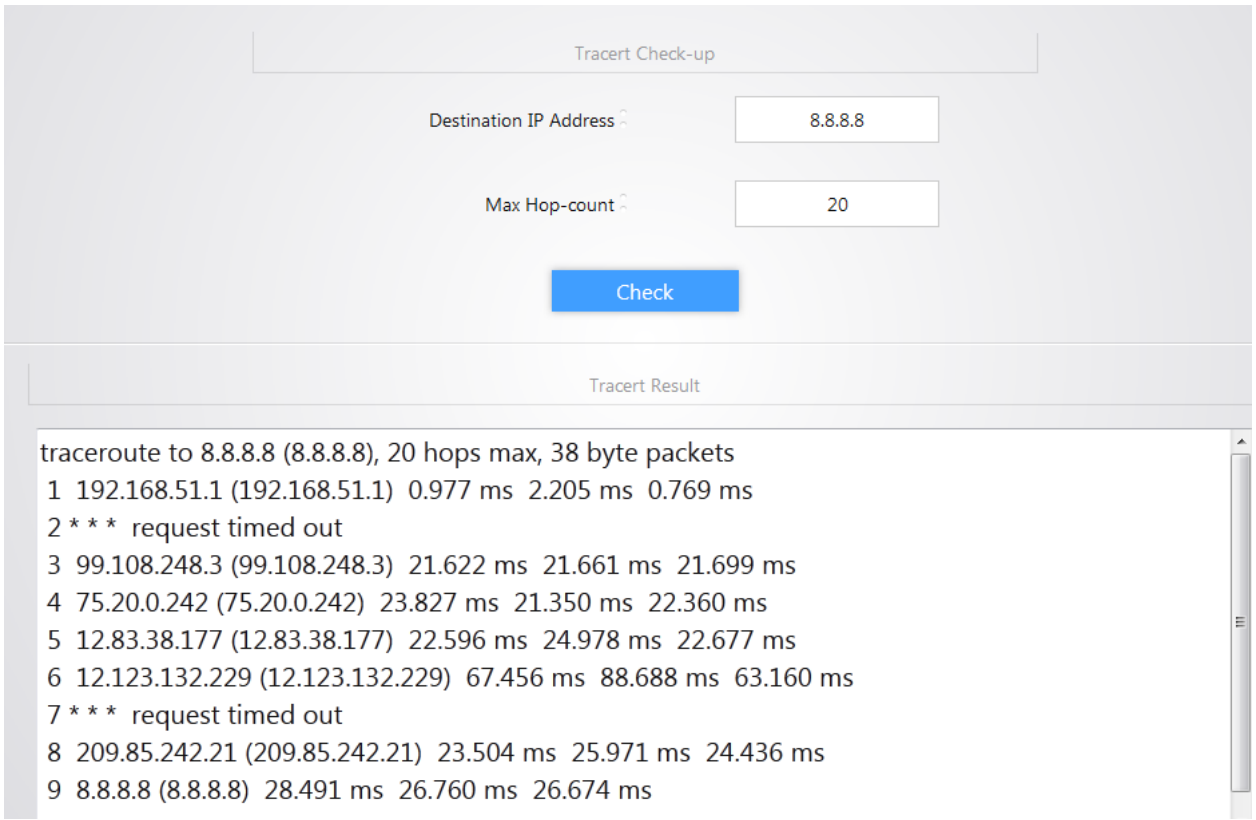
The Network Diagnostics page will allow you to perform cable checks, pings, and trace routes. Simply enter a port number into the **Check-up Port** field and click **Check**. The switch will then check to see if the cable is good.



The Ping page will allow you to ping an IP address from the switch. Simply enter an IP address and click **Check**.



The Trace route page allows you to perform a trace route to an IP address. Simply enter a **Destination IP Address** and **Max Hop-count** and click **Check**.



APPENDIX A – TECHNICAL SUPPORT

Please visit our website for up-to-date support information:

Website: www.pakedge.com
Email: support@pakedge.com

CONTACT INFORMATION:
Pakedge Device & Software Inc.
3847 Breakwater Avenue
Hayward, CA 94545-3606

APPENDIX B – SPECIFICATIONS

Item	Specification
Input Voltage	100 - 240VAC 50/60Hz 6A
Power Consumption	About 15W(no load); About 390W(full load);
PoE	24 10/100/1000Mbps auto-sensing, PoE-capable RJ45 ports with up to 30W on each;
Interface	24 RJ45 10/100/1000 auto-sensing Giga switching ports; 4 1000Mbps SFP ports;
Management Interface	One Console port
Operating Temperature	0℃ - 40℃
Storage Temperature	-40℃ - 70℃
Operating Humidity	10% - 90% RH, non-condensing
Storage Humidity	5% - 90% RH, non-condensing
Safety	UL 60950-1 CAN/CSAC22.2 No 60950-1 IEC 60950-1 EN 60950-1/A11 AS/NZS 60950-1 EN 60825-1 EN 60825-2
EMC	EN 55024;1998+A1:2001+A2:2003 EN 55022:2006 ICES-003:2004 EN 61000-3-2:2000+A1:2001+A2:2005 EN 61000-3-3:1995+A1:2001+A2:2005 AS/NZS CISPR 22:2004 FCC PART 15:2005 ETSI EN 300 386 V1.3.3:2005
MTBF	> 100,000h
Dimension	440mm * 284mm * 44mm
Weight	< 7.5kg
Features	Specification
Switch Volume (Full Duplex)	56Gbps
Packet Forwarding	35.7Mpps

MAC Address Table	8K

VLAN	1. VLAN distribution based on ports. Up to 24 can be configured; 2. IEEE 802.1Q VLAN. Up to 128 can be configured; 3. Protocol VLAN. Up to 16 can be configured; 4. MAC VLAN. Up to 64 can be configured; 5. Voice VLAN;
DHCP	DHCP Snooping, DHCP Relay, and DHCP Client
Multicast	1. IGMP Snooping V1/V2; 2. Up to 128 can be configured; 3. Fast leave;
Broadcast Storm Constrain	1. Broadcast storm constrain based on ports; 2. Multicast storm constrain based on ports; 3. Unknown unicast storm constrain based on ports;
STP	1. IEEE 802.1d STP; 2. IEEE 802.1w FSTP; 3. IEEE 802.1s MSTP protocol. In MSTP mode, up to 16 STP instances can be configured; 4. Edge port; 5. P2P port; 6. STP BPDU packets statistics;
ACL	1. MAC ACL. Up to 100 entries can be configured; 2. IPv4 ACL. Up to 100 entries can be configured; 3. Time range limit;
Safety	1. ARP attack defense, worm attack defense, DoS attack defense and MAC attack defense; 2.User grading management and SSL certification; 3. Management VLAN; 4. IP+MAC+PORT+VLAN Bind. Up to 200 entries can be configured; 5. Interface isolation;
MAC Filter	1. Unicast MAC filter; 2. Up to 1000 entries can be configured;
QoS	1. 802.1P port trust mode; 2. IP DSCP port trust mode; 3. Bandwidth control; 4. Up to 4-queue QoS mapping;
Certification	1. IEEE 802.1X based on ports; 2. IEEE 802.1X based on MAC; 3. Up to 256 MAC can be certificated;
Upgrade	TFTP (Trivial File Transfer Protocol)

Management	1. Telnet configuration; 2. Console interface configuration; 3. SNMP (Simple Network Management Protocol); 4. WEB;
PoE	1. IEEE 802.3at and IEEE 802.3af; 2. Maximum power consumption: 385W;
Maintenance	Ping\Tracert\Cable check-up;

APPENDIX C – LIMITED WARRANTY

SX Series

Congratulations on your purchase of a Pakedge Device & Software product! Pakedge designs and manufactures the finest home networking products. With proper installation, setup, and care, you should enjoy many years of unparalleled performance. Please read this consumer protection plan carefully and retain it with your other important documents.

This is a LIMITED WARRANTY as defined by the U.S. Consumer Product Warranty and Federal Trade Commission Improvement Act.

What Is Covered Under the Terms of This Warranty?

SERVICE LABOR: Pakedge will pay for service labor by an approved Pakedge service center when needed as a result of manufacturing defect for a period of **three (3) year** from the effective date of delivery to the end user.

PARTS: Pakedge will provide new or rebuilt replacement parts for parts that fail due to defects in materials or workmanship for a period of **three (3) year** from the effective date of delivery to the end user. Such replacement parts are then subsequently warranted for the remaining portion (if any) of the original warranty period.

What Is Not Covered Under the Terms of This Warranty?

This warranty only covers failure due to defects in materials and workmanship that occur during normal use and does not cover normal maintenance. This warranty does not cover any appearance item; any damage to living structure; failure resulting from accident (for example: flood, electrical shorts, insulation); misuse, abuse, neglect, mishandling, misapplication, faulty or improper installation or setup adjustments; improper maintenance, alteration, improper use of any input signal and/or power, damage due to lightning or power line surges, spikes and brownouts; damage that occurs during shipping or transit; or damage that is attributed to acts of God.

The foregoing limited warranty is the sole warranty of Pakedge and applicable only to Products sold as new by Authorized Dealers. The remedies provided herein are in lieu of a) any and all other remedies and warranties, whether expressed, implied or statutory, including but not limited to, any implied warranty of merchantability, fitness for a particular purpose or non-infringement, and b) any and all obligations and liabilities of Pakedge for damages including but not limited to incidental, consequential or special damages, or any financial loss, lost profits or expense, or loss of network connection arising out of or in connection with the purchase, use or performance of the Product, even if Pakedge has been advised of the possibility of such damages.

CAUTION: DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM IMPROPER INSTALLATION OR SETUP IS SPECIFICALLY EXCLUDED FROM COVERAGE UNDER THIS WARRRANTY. IT IS IMPERATIVE THAT

INSTALLTION AND SETUP WORK BE PERFORMED ONLY BY AN AUTHORIZED PAKEDGE DEALER TO PROTECT YOUR RIGHTS UNDER THIS WARRANTY. THIS WILL ALSO ENSURE THAT YOU ENJOY THE FINE PERFORMANCE YOUR PAKEDGE PRODUCT IS CAPABLE OF PROVIDING.

Rights, Limits, and Exclusions

Pakedge limits its obligation under any implied warranties under state laws to a period not to exceed the warranty period. There are no express warranties. Pakedge also excludes any obligation on its part for incidental or consequential damages related to the failure of this product to function properly. Some states do not allow limitations on how long an implied warranty lasts, and some states do not allow the exclusion or limitation of incidental or consequential damages. In this case, the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

Effective Warranty Date

This warranty begins on the effective date of delivery to the end user. For your convenience, keep the original bill of sale as evidence of the purchase date from your authorized dealer.

Important- Warranty Registration

Please register your product at www.pakedge.com. It is imperative that Pakedge knows how to reach you promptly if we should discover a safety problem or product update for which you must be notified. In addition, you may be eligible for discounts on future upgrades as new networking standards come about.

To Obtain Service, Contact Your Pakedge Dealer.

Repairs made under the terms of the Limited Warranty covering your Pakedge product will be performed by an Authorized Pakedge Service Center. These arrangements must be made through the selling Pakedge Dealer. If this is not possible, contact Pakedge directly for further instructions. Prior to returning a defective Product directly to Pakedge, you must obtain a Return Material Authorization number and shipping instructions. Return shipping costs will be the responsibility of the owner.

For additional information about this warranty, visit our website:

Pakedge Device & Software Inc.
3847 Breakwater Avenue
Hayward, CA 94545-3606
U.S.A.

877-274-6100

Email: support@pakedge.com

www.pakedge.com

pakedgedevice&software inc.

3847 Breakwater Avenue

Hayward, CA 94545

U.S.A

Visit Us At:

www.pakedge.com