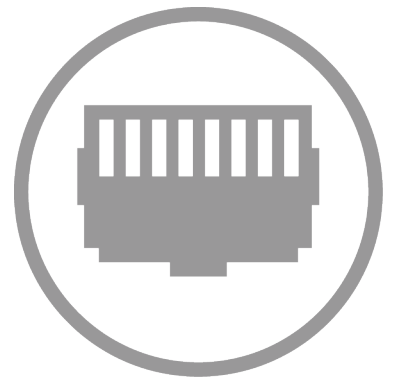


pakedge® 

SX-8P

Enterprise-AV, Smart Managed Switches

User Guide



This device complies with Part 15 of conditions:

following two

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

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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 NOT 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. CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT. 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 40°C (32 and 104°F). 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 least 10cm 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. Shut down 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	5
Customer service and technical support	5
Accessing the Switch	8
Dashboard.....	9
System.....	9
Basic Settings	10
Ports	16
Port Settings.....	16
PoE	24
MAC Control.....	26
VLANs	27
Voice VLAN.....	33
Traffic menu	35
QoS.....	36
STP.....	41
IGMP	45
Maintenance	49
SNMP.....	50
LLDP.....	51
Syslog	53
Network Diagnostics	54
Appendix A – Technical Support	56
Appendix B – Specifications	57
Appendix C – Limited Warranty	59

INTRODUCTION

The SX Series 8-port Smart Gigabit Switches provide 8 10/100/1000 Mbps auto-sensing RJ45 ports, 1 1000 Mbps Dedicated fiber port, 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, IGMP snooping, STP, RSTP, port mirroring, link aggregation and many 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, MAC filter and other safety settings through visual WEB interface operations. With high performance and low cost, they are ideal for residential and enterprise AV 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
- Mounting Kit (2 side brackets, 1 face bracket, 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	
SFP	Blue	Port is online (link established)	
	Flashing Blue	Activity	
	Off	No device connected	
Ports 1-8	PoE	Blue	PoE in use
		Flashing Blue	PoE error
		Off	No PoE in use
Ports 1-8	LINK/ACT	Blue	Port is online (link established)
		Flashing Blue	Activity
		Off	No device connected
PWR	Blue	The switch is powered on	
	Off	The switch is turned off	
SYS	Blue	The switch has booted	
	Flashing Blue	The switch is booting	

The rear panel of the SX Series switches provides all inputs for a clean installation. See Table 2 below for more information.

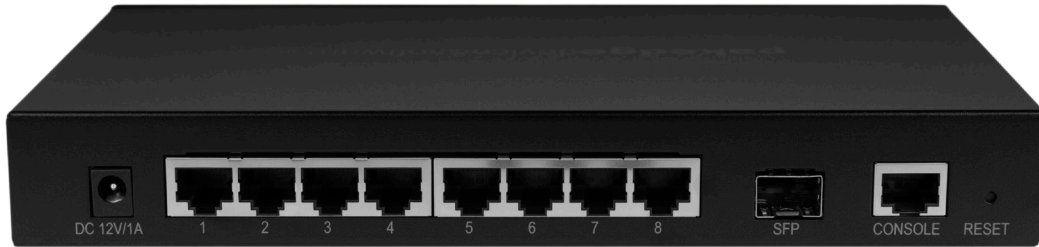


Table 2: Rear panel port connection explanation from left to right.

Input	Description
Power	Power adapter input
Ports 1-8	RJ45 PoE/PoE+ ports
SFP Port	1G SFP port
CONSOLE	RJ45 console port
RESET	Reset button. Press and hold for 10 seconds to factory reset the switch

Reset Button

To restore factory defaults, press and hold the button for more than 10 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.



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.

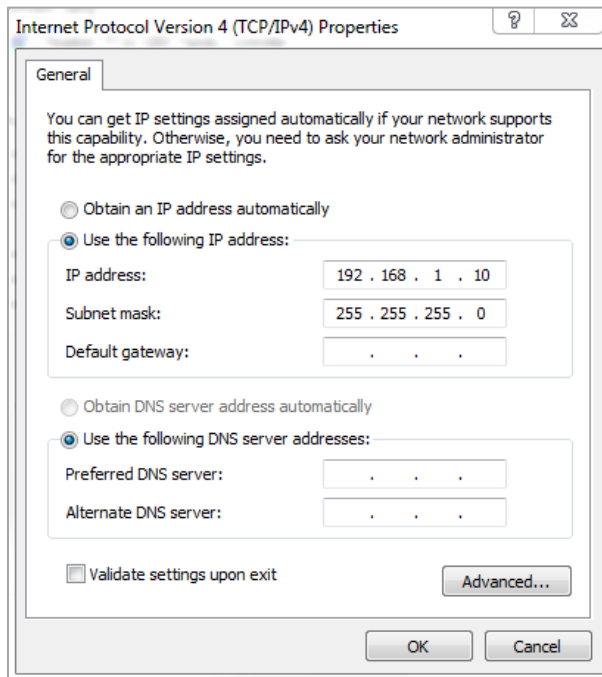
Connecting SFP fiber port

The small form-factor pluggable (SFP) module is a compact, hot-pluggable transceiver used for optical signal transmission. The module bay is a standalone port, making it the “9th” port on the switch. The SFP module accommodates a standard 1G SFP module with an LC connector.

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.



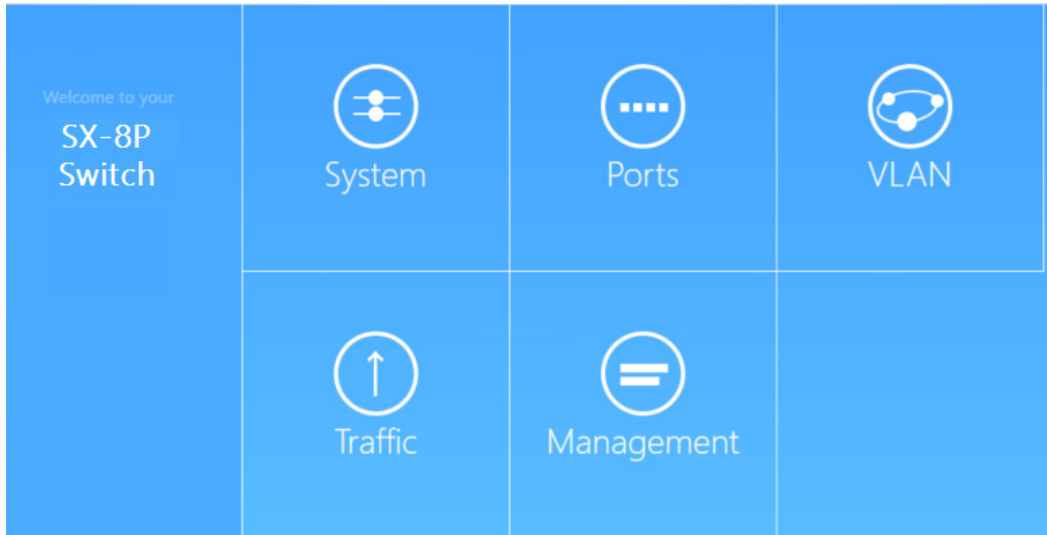
4. Open any Internet browser and go to the address <http://192.168.1.205>. Note: For best results we recommend using Mozilla Firefox as your web browser. If you are using Internet Explorer, please use version 9 or newer.
5. Enter the default username **pakedge** and password **pakedges**. Click **Login**.



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

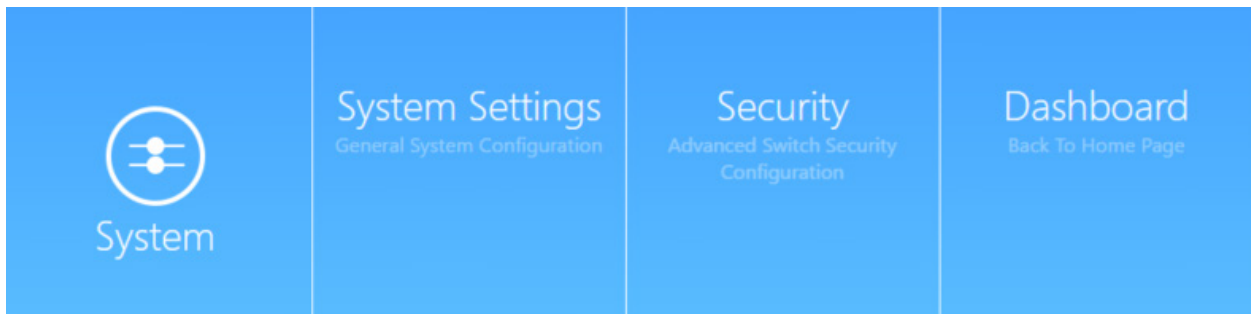
DASHBOARD

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



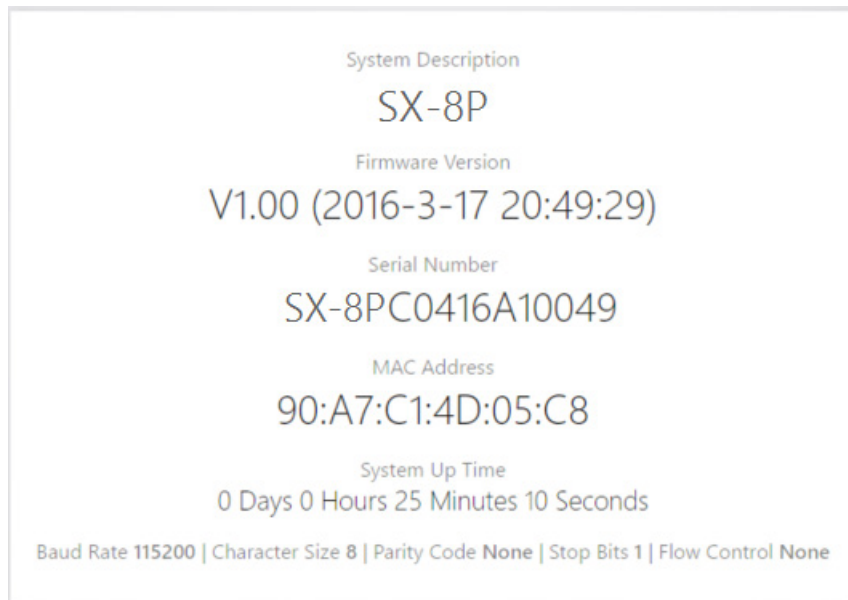
SYSTEM

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



BASIC SETTINGS

The System Settings page's *Basic Settings* page will display the System Description, firmware version, serial number, and system up time.



System Description
SX-8P

Firmware Version
V1.00 (2016-3-17 20:49:29)

Serial Number
SX-8PC0416A10049

MAC Address
90:A7:C1:4D:05:C8

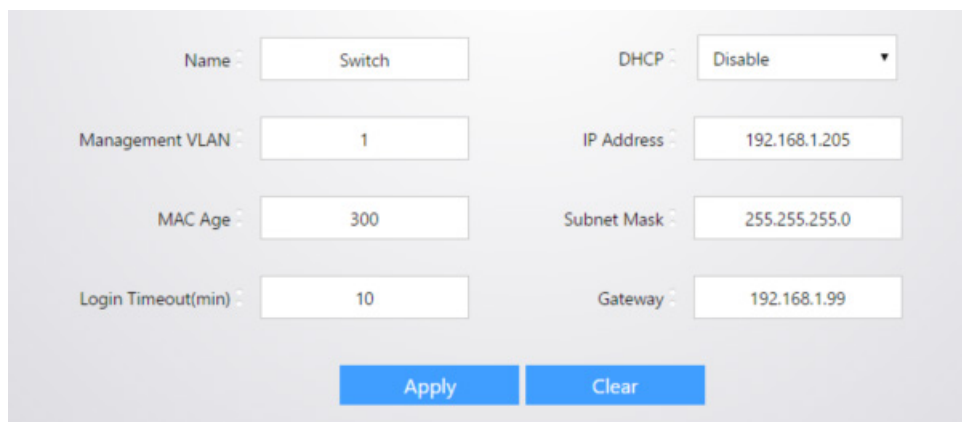
System Up Time
0 Days 0 Hours 25 Minutes 10 Seconds

Baud Rate 115200 | Character Size 8 | Parity Code None | Stop Bits 1 | Flow Control None

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

Baud Rate 115200 | Character Size 8 | Parity Code None | Stop Bits 1 | Flow Control None

Further down the basic settings page you will find additional settings.



Name	Switch	DHCP	Disable
Management VLAN	1	IP Address	192.168.1.205
MAC Age	300	Subnet Mask	255.255.255.0
Login Timeout(min)	10	Gateway	192.168.1.99

Apply Clear

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 **Login Timeout(min)** field is the setting for the number of idle minutes before a user is automatically logged out of the web page.

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 **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. Enable **Daylight Saving Time** to have the switch automatically adjust the time when Daylight Savings occurs, and set the dates and times it will take effect. 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. Enter the public SNTP server IP or domain name into the **Server Port** field.

The screenshot shows the 'System Settings' interface with the 'System Time' tab selected. At the top, the current system time is displayed as '2000-01-01 08:38:45'. Below this, the 'Time Zone' is set to 'UTC +8:00'. The 'Daylight Saving Time' checkbox is unchecked. The 'Start' and 'End' dates and times are both set to 'Month: 1', 'Week: First', 'Day: Sun', and 'Hour: 0' and 'Hour: 1' respectively. The 'Server Configuration' section shows 'Preferred SNTP Server' and 'Server Port' fields, with the 'Server Port' field containing the value '123'. The 'Set Time Manually' section has six dropdown menus for Year, Month, Day, Hour, Minute, and Second, with values '2000', '1', '1', '8', '38', and '36' respectively. At the bottom, there are 'Apply' and 'Clear' buttons.

Use the **Set Time & Date Manually** field to manually input the system time. 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.

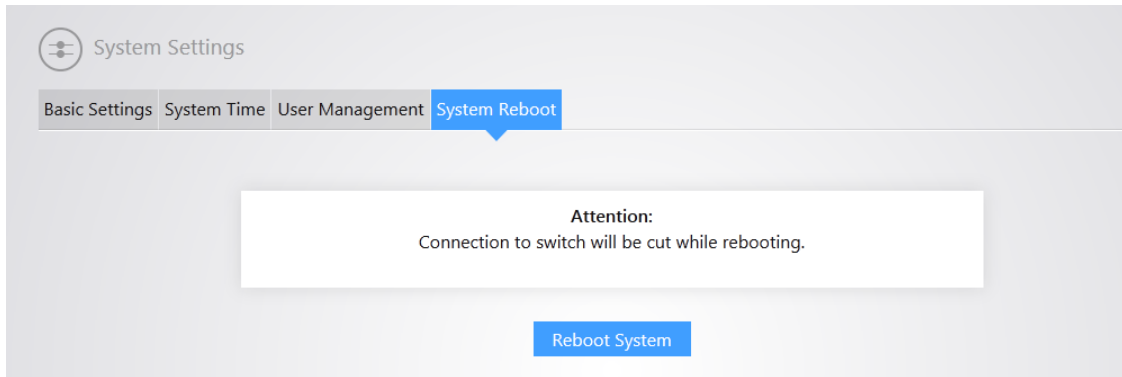
The screenshot shows the 'System Settings' interface with the 'User Management' tab selected. The 'Change Password' section is visible, showing the username 'pakedge' and fields for 'Current Password', 'New Password', and 'Re-enter Password'. Below this is the 'Multi-user Management Configuration' section, which includes a dropdown menu set to 'New', fields for 'Username', 'Current Password', 'New Password', and 'Re-enter Password', and a 'Privileges' dropdown set to 'none'. At the bottom of the page are three buttons: 'Apply', 'Delete', and 'Clear'.

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.

You can create a new user by selecting **New** under *Multi-user Management Configuration*. Enter the new **Username**. Enter a password in 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.

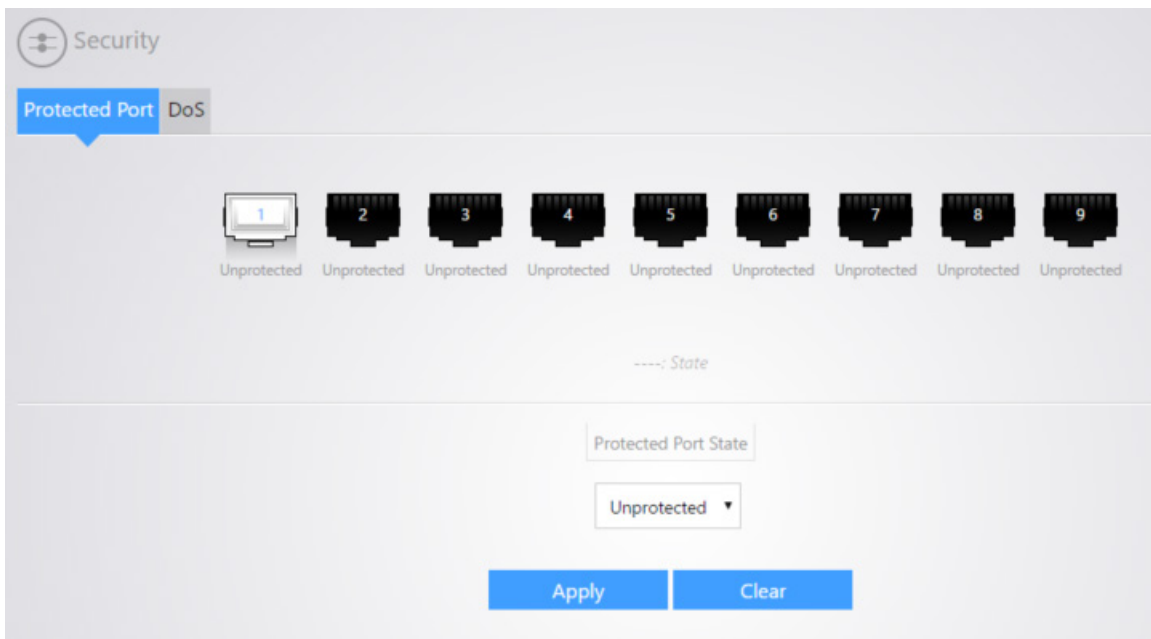
Click **Apply** (at the bottom of the screen) to finalize the settings.

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



Security

Protected Port page



This setting allows the user to prevent the selected ports from communication with each other. Protected ports are allowed to communicate only with unprotected ports. No traffic will be allowed to pass between any two ports both set to “Protected”. To protect a port, click it to select it, then select **Protected** from the **Protected Port State** drop-down menu.

DoS page

Security

Protected Port: DoS

Property: Port Setting

POD: Enable

Land: Enable

UDP Blat: Enable

TCP Blat: Enable

DMAC = SMAC: Enable

Null Scan Attack: Enable

X-Mas Scan Attack: Enable

TCP SYN-FIN Attack: Enable

TCP SYN-RST Attack: Enable

ICMP Fragment: Enable

TCP-SYN: Enable
(Note: Source Port < 1024)

TCP Fragment: Enable
(Note: Offset = 1)

Ping Max Size: Enable IPv4
 Enable IPv6
512 Byte (0 - 65535, default 512)

TCP Min Hdr size: Enable
20 Byte (0 - 31, default 20)

IPv6 Min Fragment: Enable
1240 Byte (0 - 65535, default 1240)

Smurf Attack: Enable
0 Netmask Length (0 - 32, default 0)

Apply Clear

A Denial of Service (DoS) attack is an attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The **Property** section allows activation of the security settings.

POD: Avoids ping of death attack.

Land: Drops the packets if the source IP address is equal to the destination IP address.

UDP Blat: Drops the packets if the UDP source port equals to the UDP destination port.

TCP Blat: Drops the packages if the TCP source port is equal to the TCP destination port.

DMAC = SMAC: Drops the packets if the destination MAC address is equal to the source MAC address.

Null Scan Attack: Drops the packets with NULL scan.

X-Mas Scan Attack: Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.

TCP SYN-FIN Attack: Drops the packets with SYN and FIN bits set.

TCP SYN-RST Attack: Drops the packets with SYN and RST bits set.

ICMP Fragment: Drops the fragmented ICMP packets.

TCP- SYN: Drops SYN packets with sport less than 1024.

TCP Fragment: Drops the TCP fragment packets with offset equals to one.

Ping Max Size: Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.

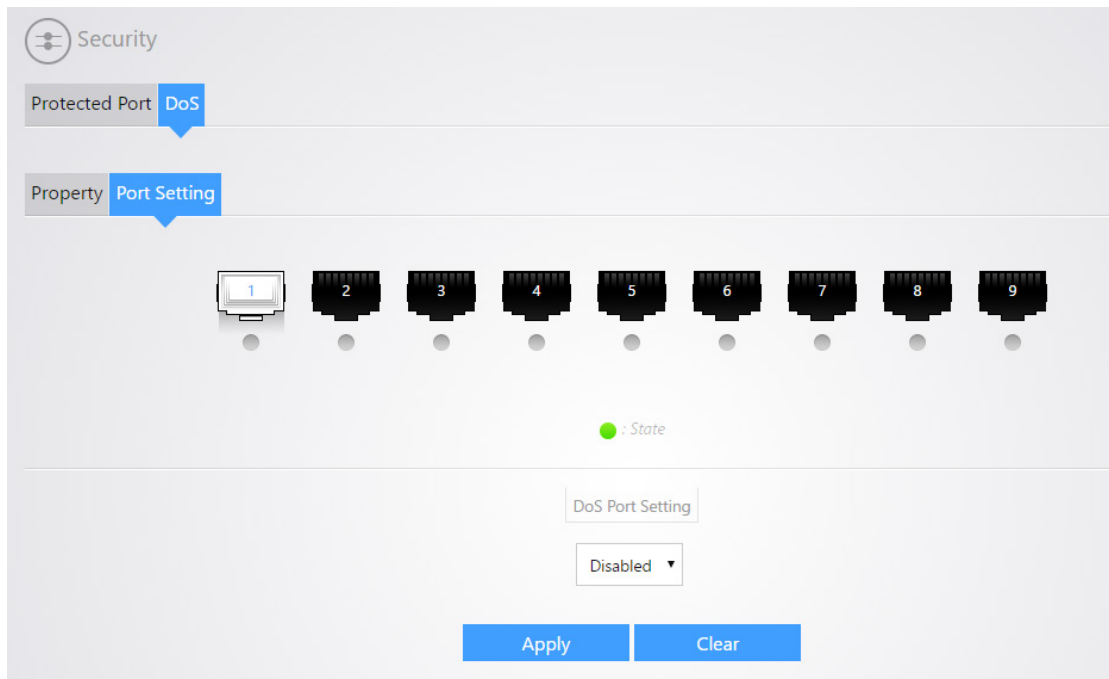
TCP Min Hdr Size: Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.

IPv6 Min Fragment: Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.

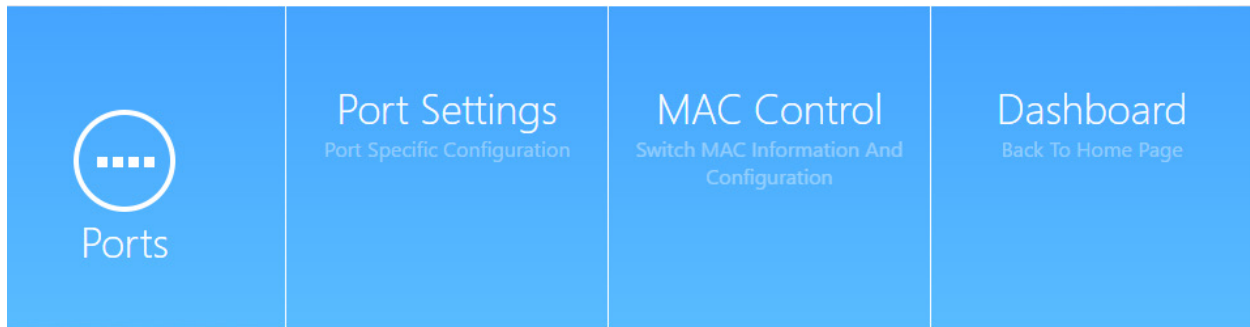
Smurf Attack: Avoids smurf attack. The length range of the netmask is from 0 to 32 bytes, and default length is 0 bytes.

To apply the settings:

1. Click the **Port Setting** tab.
2. Click the ports to apply your DoS settings to, then click **Apply**.



PORTS

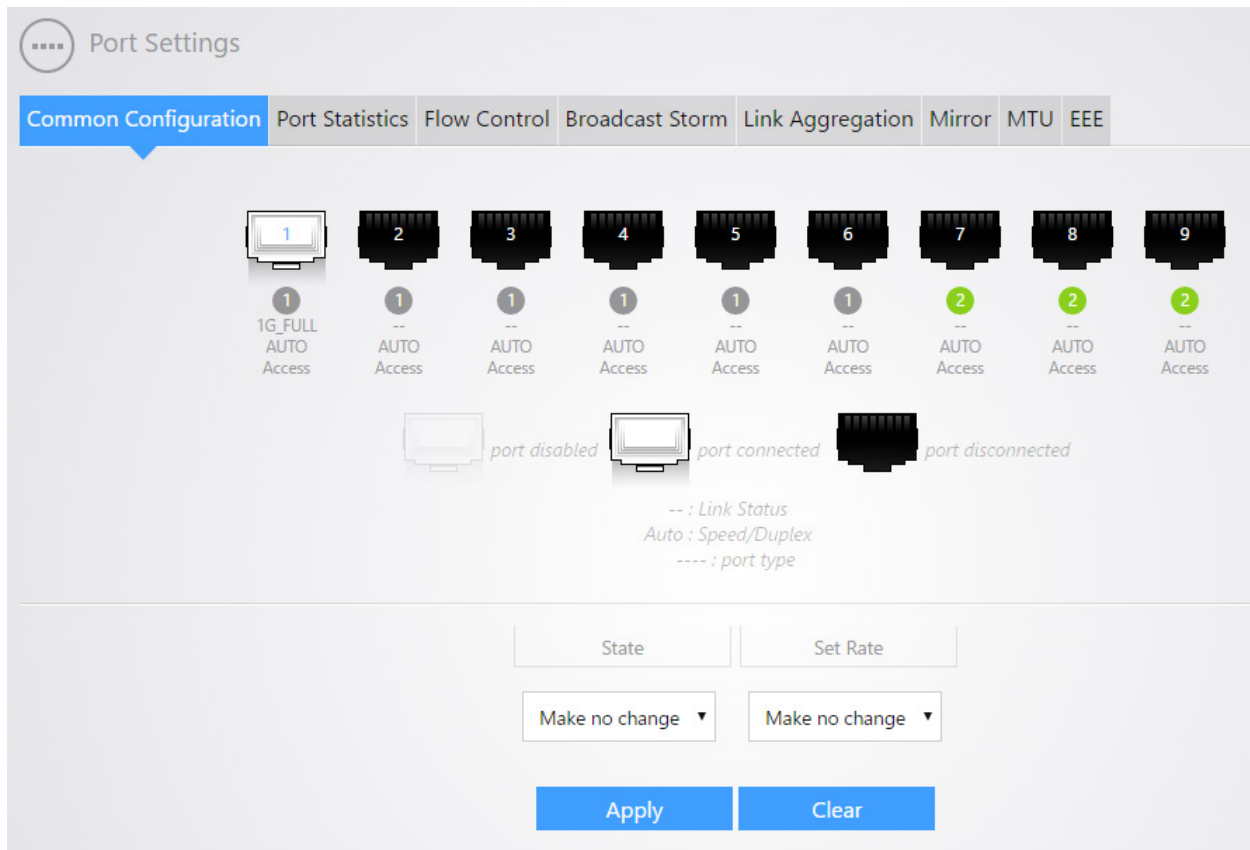


The Ports section contains three subsections. Each will be covered next.

PORT SETTINGS

Common Configuration page

The Common Configuration page will allow you to change a port state or port speed. You can simply click on a port to select it (you can also select multiple ports) and then change the port **State** or **Set Rate** down below. Click **Apply** to finalize your settings.



Port Statistics page

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.

The screenshot shows the 'Port Settings' page with the 'Port Statistics' tab selected. At the top, there are navigation tabs: 'Common Configuration', 'Port Statistics', 'Flow Control', 'Broadcast Storm', 'Link Aggregation', 'Mirror', 'MTU', and 'EEE'. Below these tabs is a row of nine port icons, numbered 1 through 9. Port 1 is highlighted with a white border. Below the port icons, there are two columns of statistics for the selected port (Port 1). Each statistic is followed by a value of 0. The statistics are:

Statistic	Value
Received Total Bytes Num <small>(ifInOctets)</small>	0
Received Unicast Packets Num <small>(ifInUcastPkts)</small>	0
Received Non-Unicast Packets Num <small>(ifInNonUniCastPkts)</small>	0
Received Discard Packets Num <small>(ifInDiscards)</small>	0
Received Error Packets Num <small>(ifInErrors)</small>	0
Send Total Bytes Num <small>(ifOutOctets)</small>	0
Send Unicast Packets Num <small>(ifOutUcastPkts)</small>	0
Send Non-Unicast Packets Num <small>(ifOutNonUniCastPkts)</small>	0
Send Discard Packets Num <small>(ifOutDiscards)</small>	0
Send Error Packets Num <small>(ifOutErrors)</small>	0

At the bottom of the page, there are three blue buttons: 'Refresh', 'Clear All', and 'Clear'.

Flow Control

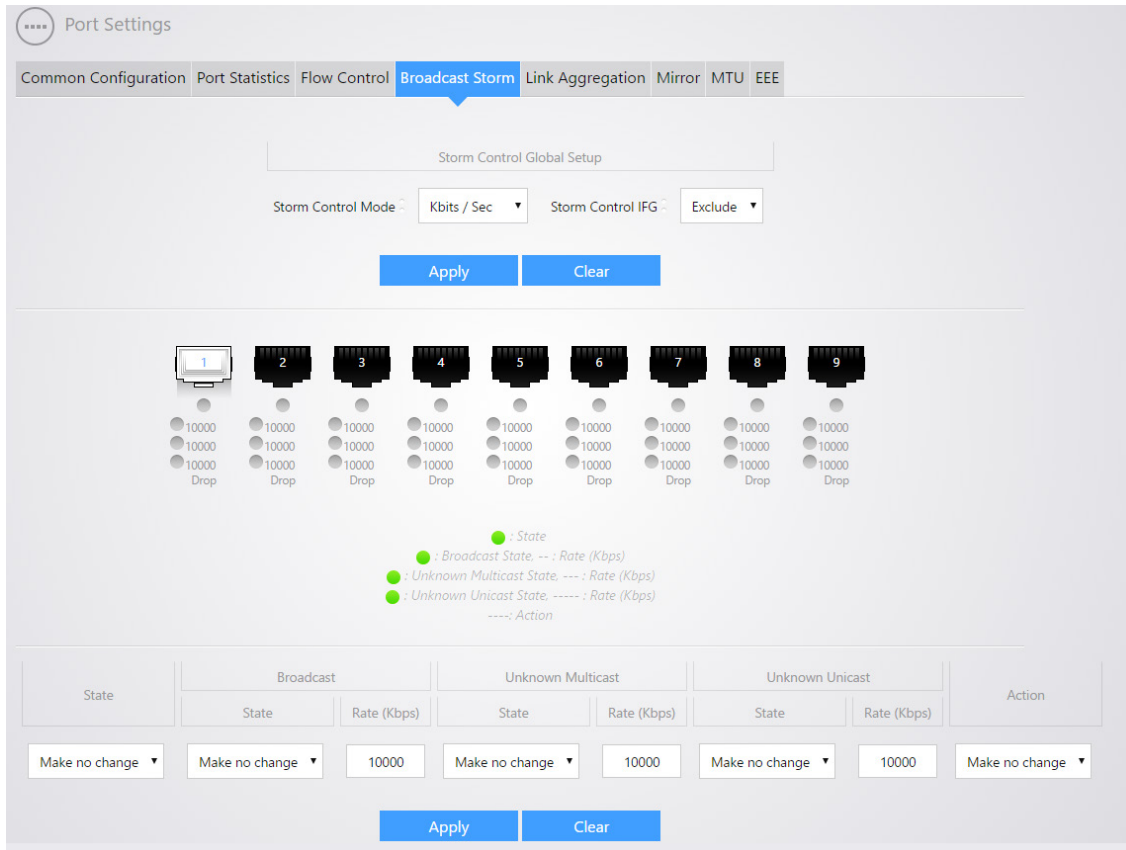
The Flow Control page allows you to enable or disable flow control per port. With flow control enabled on both the switch and its link partner, the switch, when encountering congestion, will send flow control frames to notify the link partner of such; upon receiving such frames, the link partner will 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.

The screenshot displays the 'Port Settings' configuration interface. At the top, there is a breadcrumb 'Port Settings' and a navigation bar with tabs: 'Common Configuration', 'Port Statistics', 'Flow Control' (which is highlighted in blue), 'Broadcast Storm', 'Link Aggregation', 'Mirror', 'MTU', and 'EEE'. Below the tabs, there is a row of nine port icons labeled 1 through 9. Port 1 is highlighted with a white border and a small computer icon. Below the ports, there is a 'State' radio button. Underneath that is a dropdown menu with the text 'Make no change' and a downward arrow. At the bottom of the interface are two blue buttons: 'Apply' and 'Clear'.

Broadcast Storm

The Broadcast storm page allows you to limit the amount of broadcast, multicast, or unicast data that is allowed to pass incoming per port.



The **Storm Control Global Setup** allows you to modify how incoming traffic is calculated for storm control.

Storm Control Mode: Select the unit of storm control.

- **Packet / Sec:** storm control rate calculated by packet
- **Kbits / Sec:** storm control rate calculated by kilobit

Storm Control IFG: Calculates traffic with or w/o preamble (8 bytes) & Inter-Frame Gap (12 bytes) taken into account.

- **Exclude:** exclude the preamble & IFG (20 bytes) when counting ingress storm control rate.
- **Include:** include preamble & IFG (20 bytes) when counting ingress storm control rate.

The Port section allows you to configure individual ports with the desired storm control values.

[Port]: Select the ports to configure.

State: Select the state of setting.

- **Enable:** Enable the storm control function.

Broadcast

- **State:** Enable or Disable the storm control function of Broadcast packet.

- **Rate: Value of storm control rate, Unit:** pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range 16 - 1000000) depends on global mode setting.

Unknown Multicast

- **State:** Enable or Disable the storm control function of Unknown multicast packet.
- **Rate: Value of storm control rate, Unit:** pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range 16 - 1000000) depends on global mode setting.

Unknown Unicast

- **State:** Enable or Disable the storm control function of Unknown unicast packet.
- **Rate: Value of storm control rate, Unit:** pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range 16 - 1000000) depends on global mode setting.

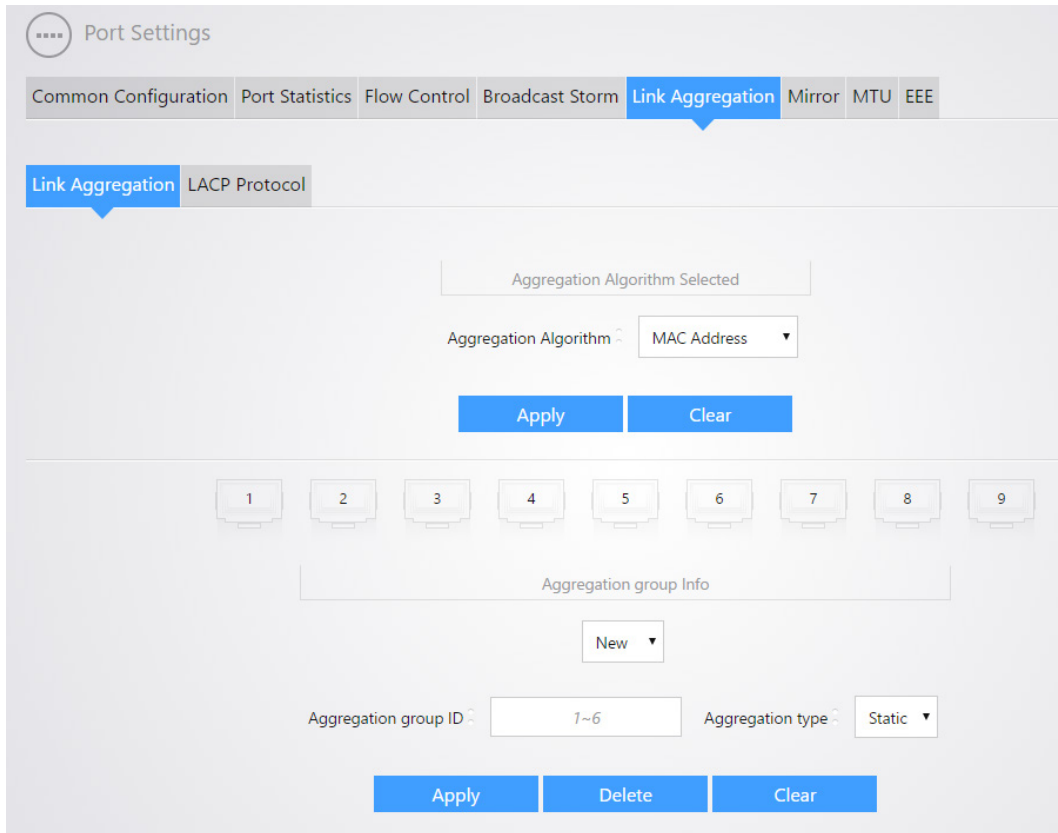
Action: Select the state of setting:

- **Drop:** Packets exceed storm control rate will be dropped.
- **Shutdown:** Port will be shut down when packets exceed storm control rate.

Link Aggregation page

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. Select the type of aggregation in the **Aggregation type** drop-down list.



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

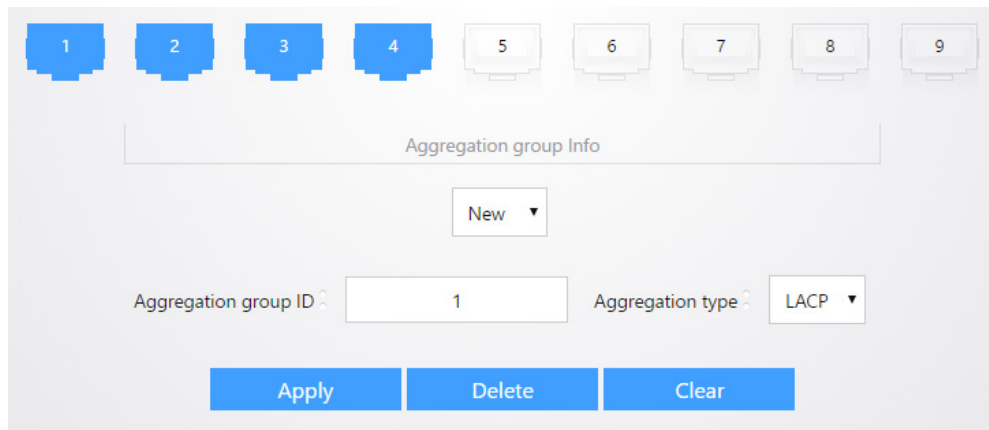
For LACP aggregation, you must manually maintain the aggregation state of the member ports. Whether ports in LACP group are aggregation ports or not is determined by LLDPBU frame auto-negotiation. Down to 2 member ports must be included in a single aggregation group. LACP is enabled on the member ports 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. Select from the following algorithm options:

- **MAC Address:** Member ports in a link aggregation group share traffic load according to Source and Destination MAC addresses.
- **IP Address:** Member ports in a link aggregation group share traffic load according to Source and Destination IP addresses.

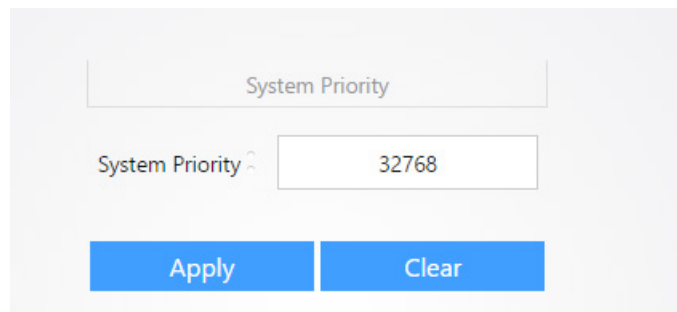
Once you have selected the algorithm you want to use, click **Apply**.

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 screenshot shows a configuration interface for LACP. At the top, there are nine port icons numbered 1 through 9. Ports 1, 2, 3, and 4 are highlighted in blue, indicating they are selected for the aggregation group. Below the port icons is a section titled "Aggregation group Info". Inside this section, there is a dropdown menu currently set to "New". Below the dropdown, there are two input fields: "Aggregation group ID" with the value "1" and "Aggregation type" with the value "LACP". At the bottom of the section, there are three buttons: "Apply", "Delete", and "Clear".

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**.

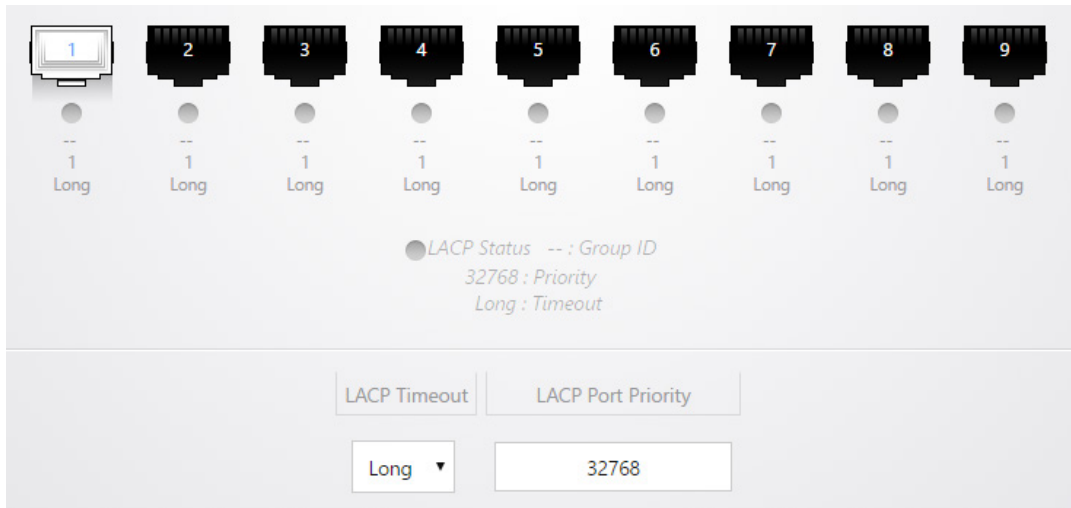


The screenshot shows a configuration interface for System Priority. It features a section titled "System Priority". Below the title, there is an input field labeled "System Priority" containing the value "32768". At the bottom of the section, there are two buttons: "Apply" and "Clear".

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.

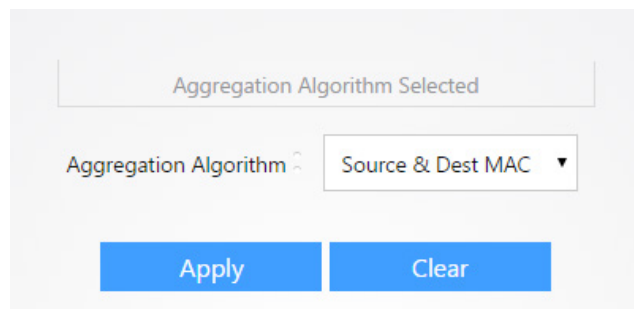
The LACP **port priority** is used to determine which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

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**.



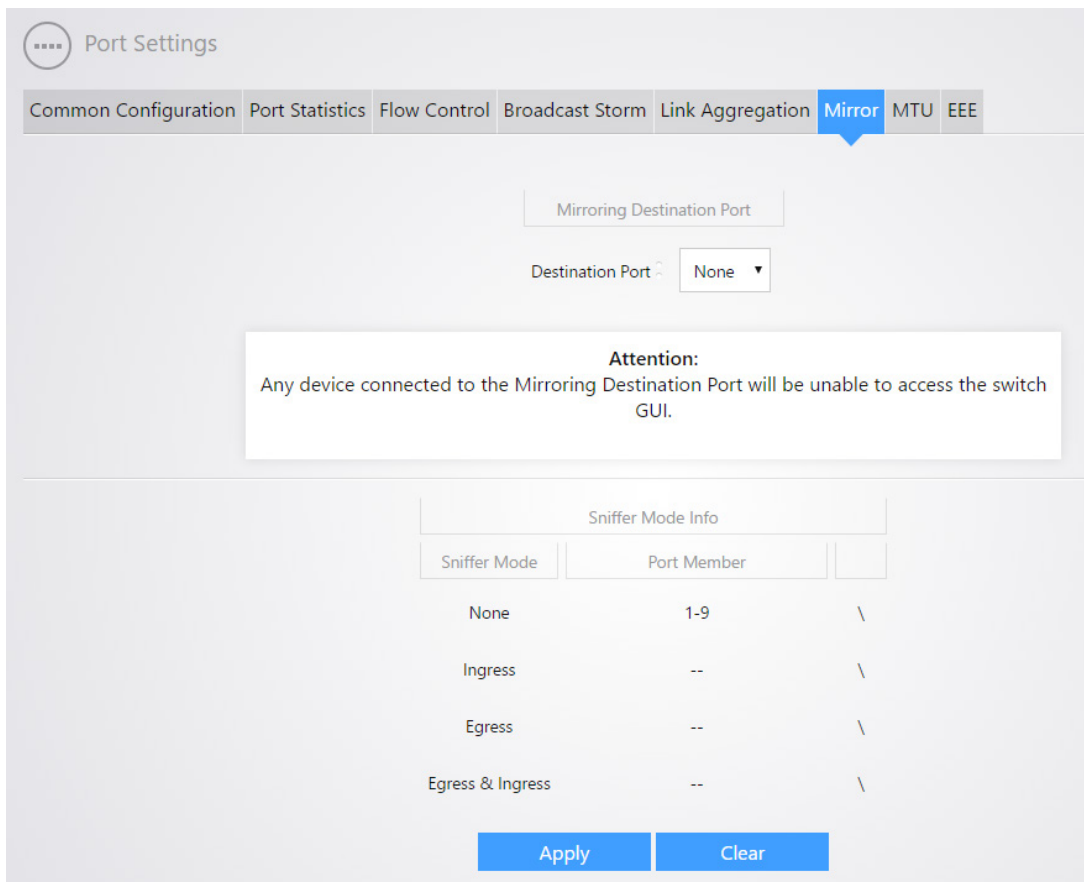
Leave the following drop down menu as **New** and enter an **Aggregation group ID**. Set the Aggregation Type to **Static**. Select the ports you want to be in the group, and click **Apply**.

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.



EEE

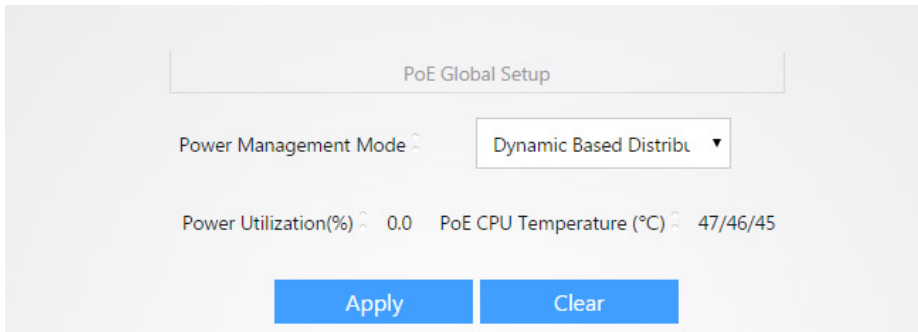
Port: Selected port list

State: Port EEE admin state:

- **Enable:** Enable EEE
- **Disable:** Disable EEE

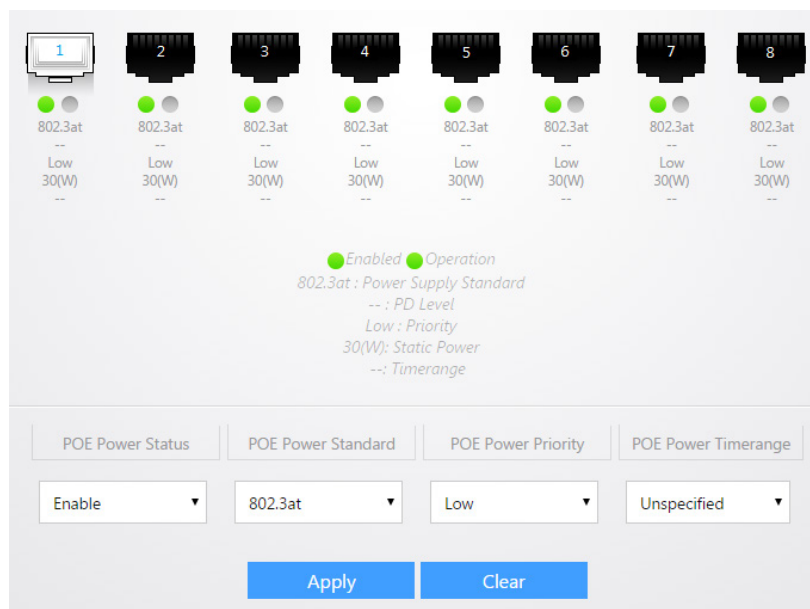
POE

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.

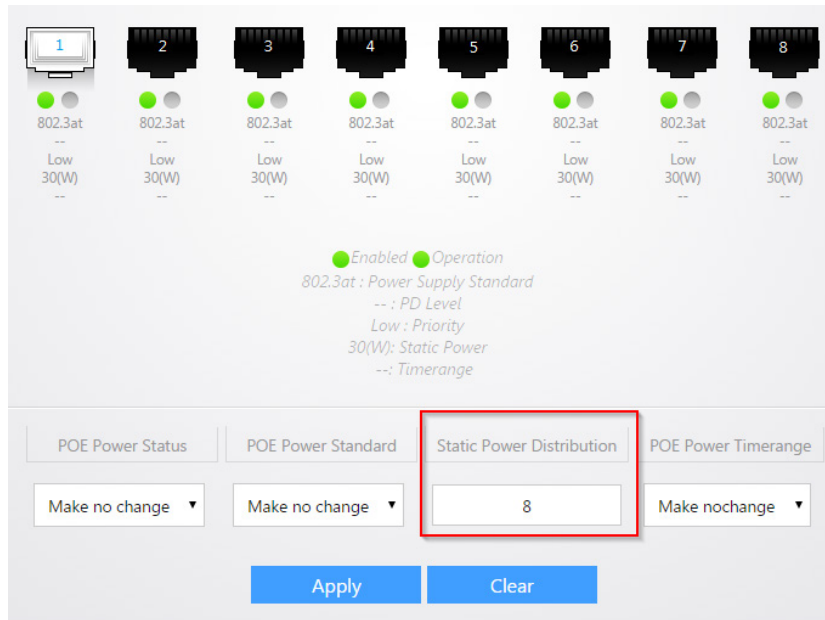


You can select a port and then adjust the following settings below

- **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. 802.3at 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.

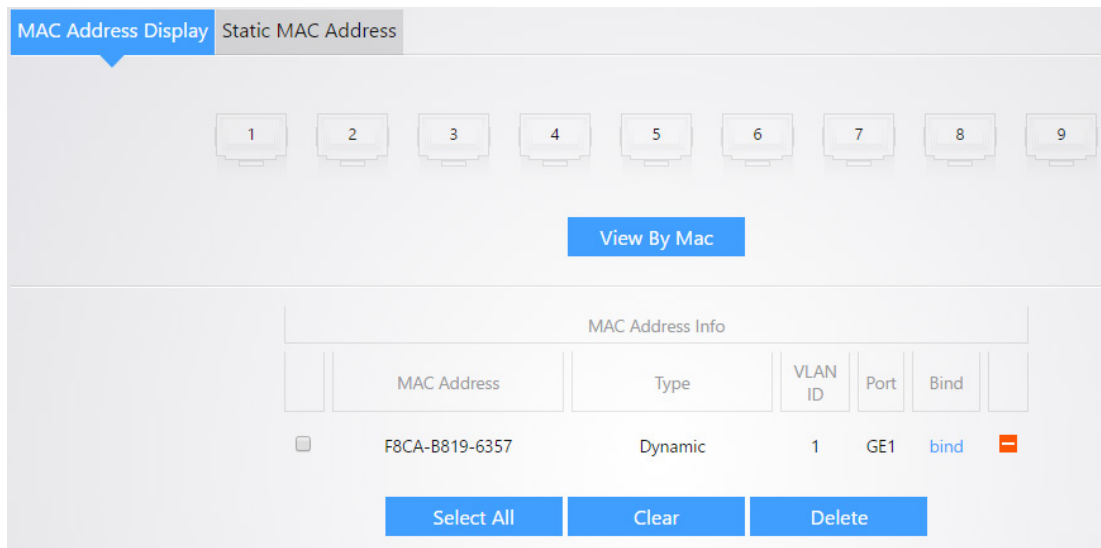


If **Static Based Distribution** is used, you will be able to enter the amount of watts that you want the ports on the switch to use. The following image illustrates this. Click **Apply** to finalize any settings made on this page.



MAC CONTROL

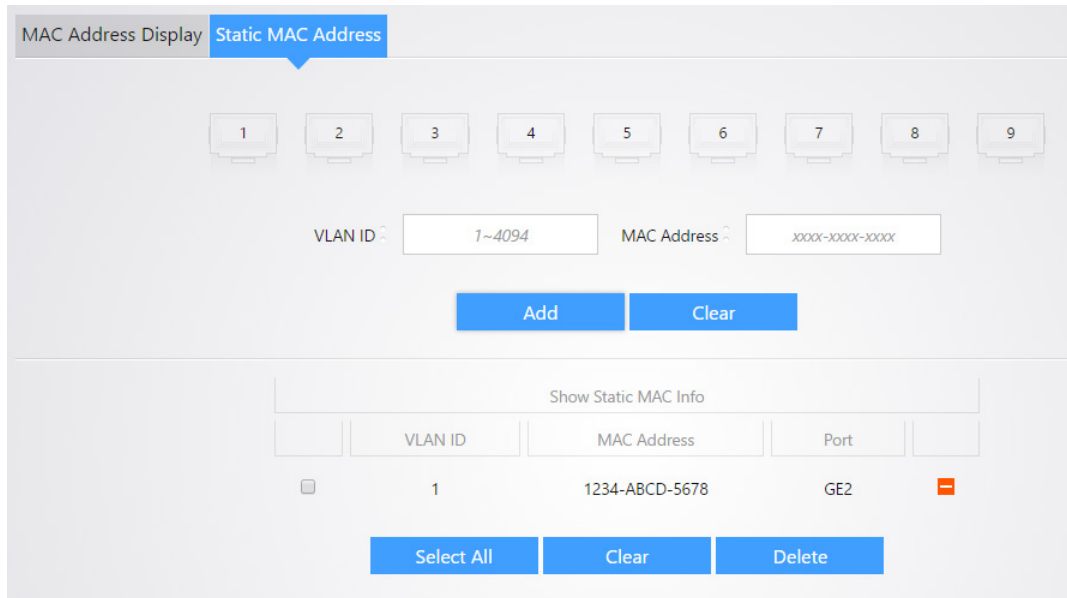
The *MAC Address Display* page will allow you to view the different mac addresses passing through the ports on the switch. You can click on a port and see the mac address associated with that port. The following image illustrates this.



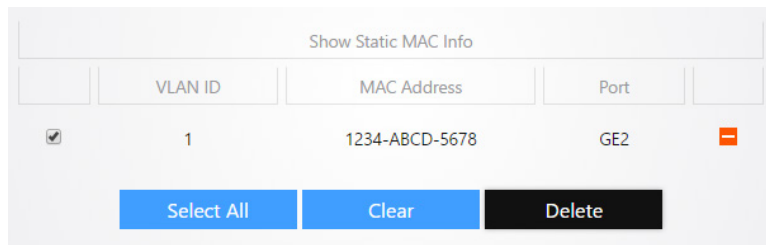
After you have selected a port, you can click **bind** on a mac address entry and the switch will bind that mac address to the current port. Data from any other mac address will be denied on that port.

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**.

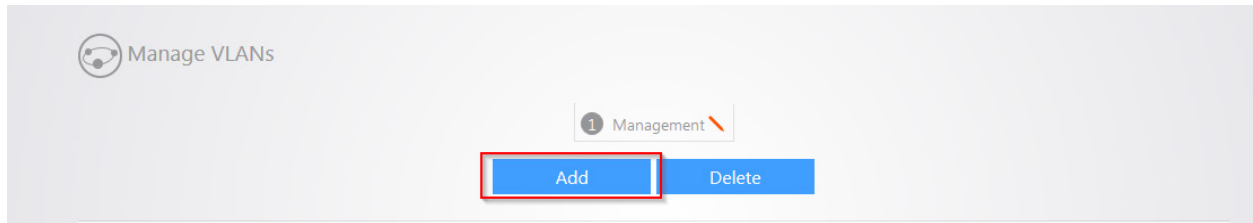


VLANS

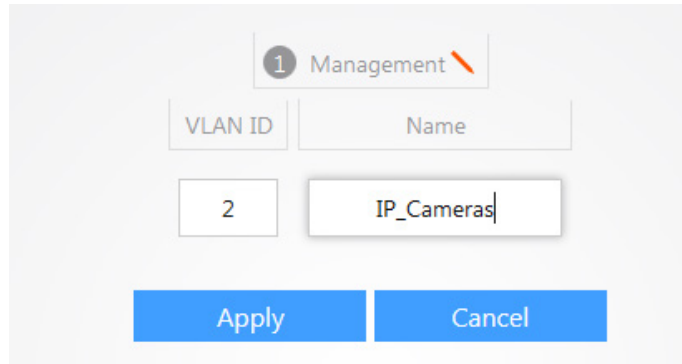
A Virtual Local Area Network (VLAN) is a network topology which allows to logically instead of physically segment a LAN into several net segments. A VLAN combines a group of hosts with a common set of requirements logically instead of physically relocating devices or connections. VLANs allow a network 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.

Manually Configuring VLANs

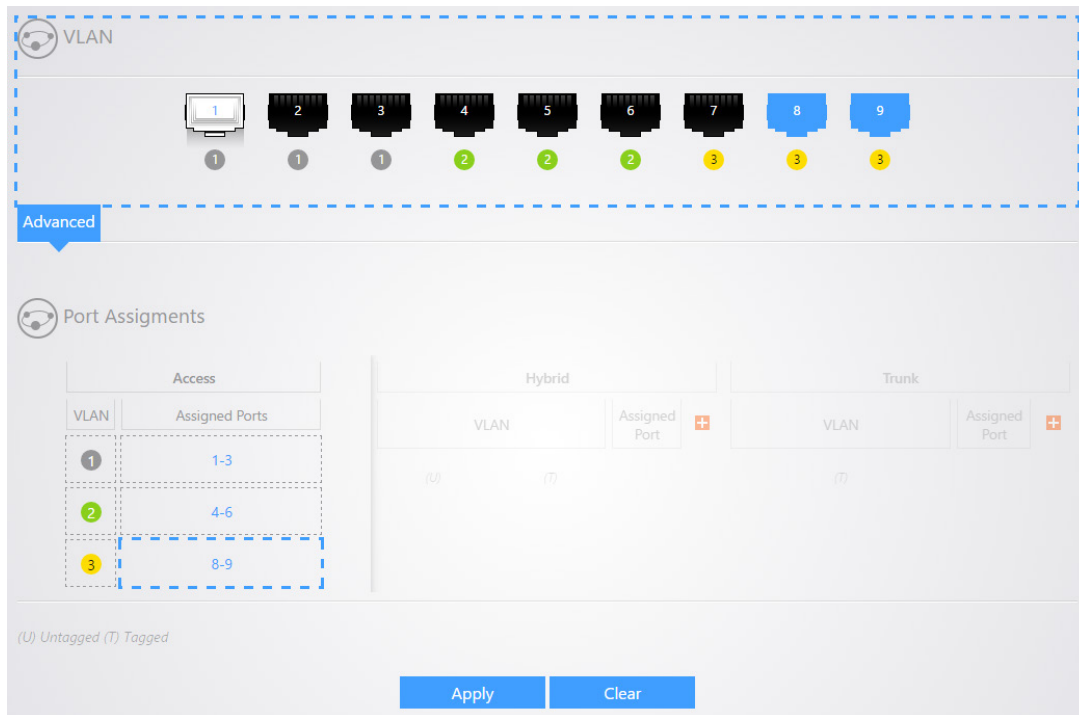
You can manually configure VLANs on the switch using the VLAN *Advanced* configuration tab. Click **Add** to add another VLAN.



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

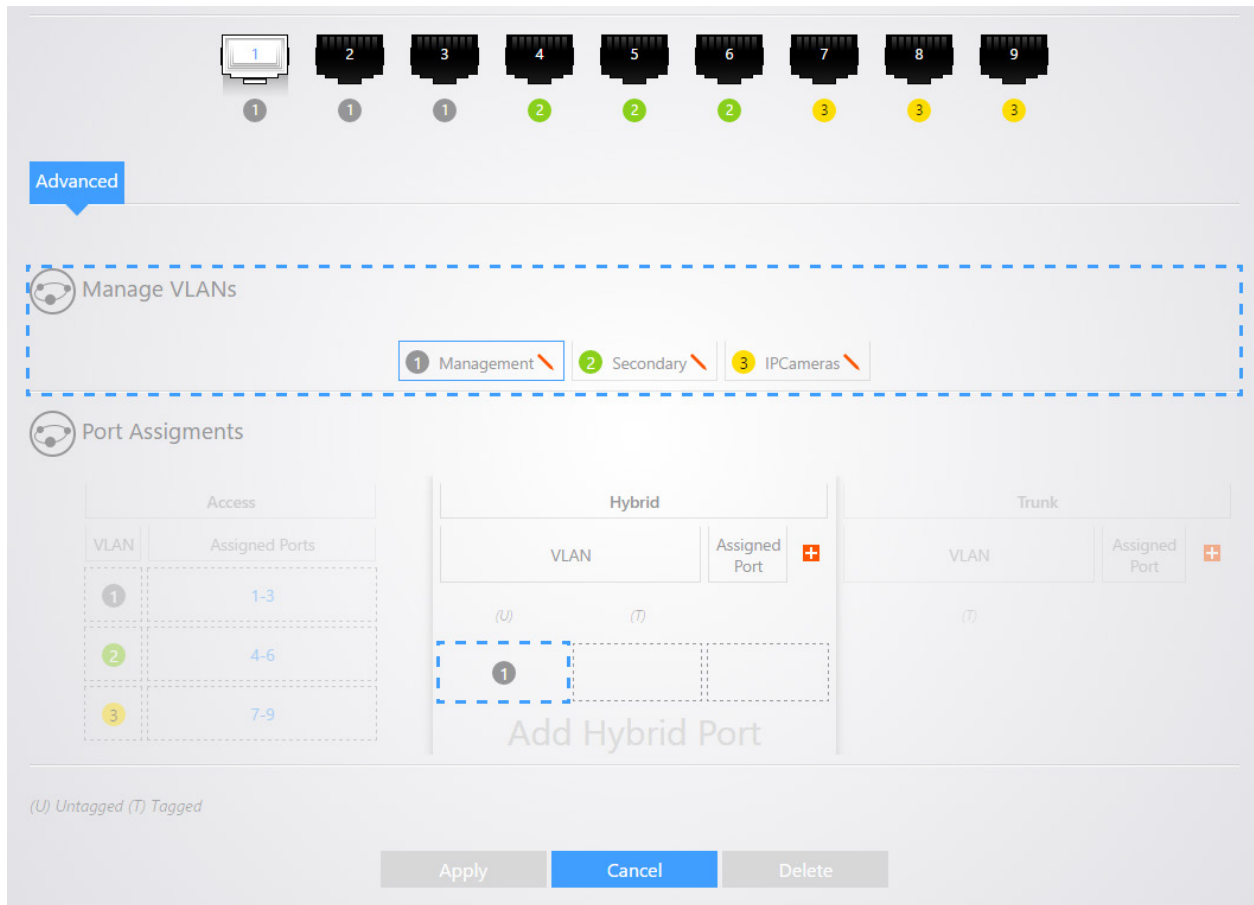


To add ports to a VLAN, click on the VLAN under Port Assignments. **Note:** All ports will belong to VLAN 1 by default.

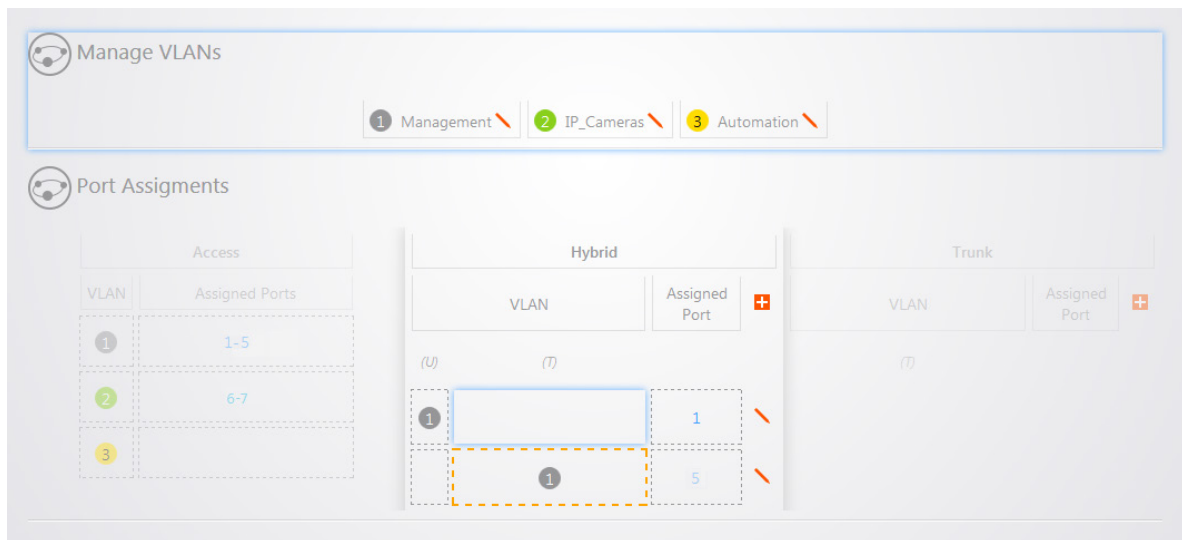


Select the ports you wish to add to this VLAN. Click **Apply** towards the bottom to finalize the settings.

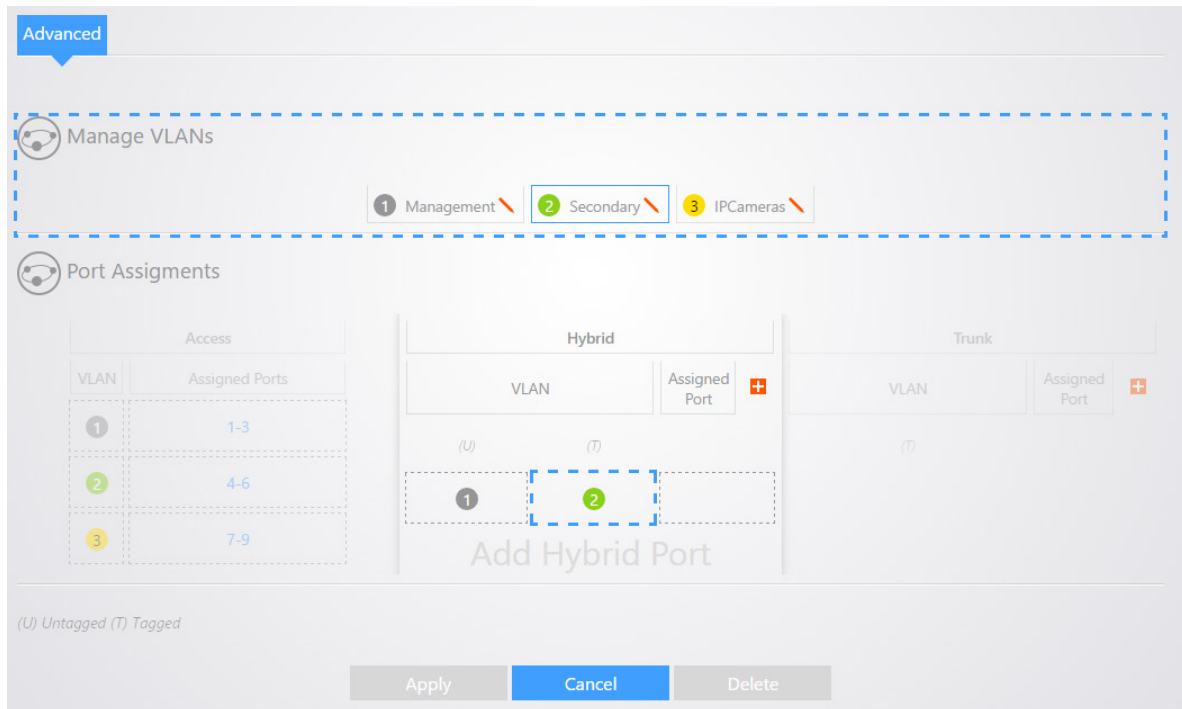
You can also configure Hybrid ports in order to pass tagged VLAN traffic with one Primary Untagged VLAN on a port. You will need to add any additional VLANs you configured to the Hybrid ports. To do this, click the edit icon next to one of the Hybrid ports.



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

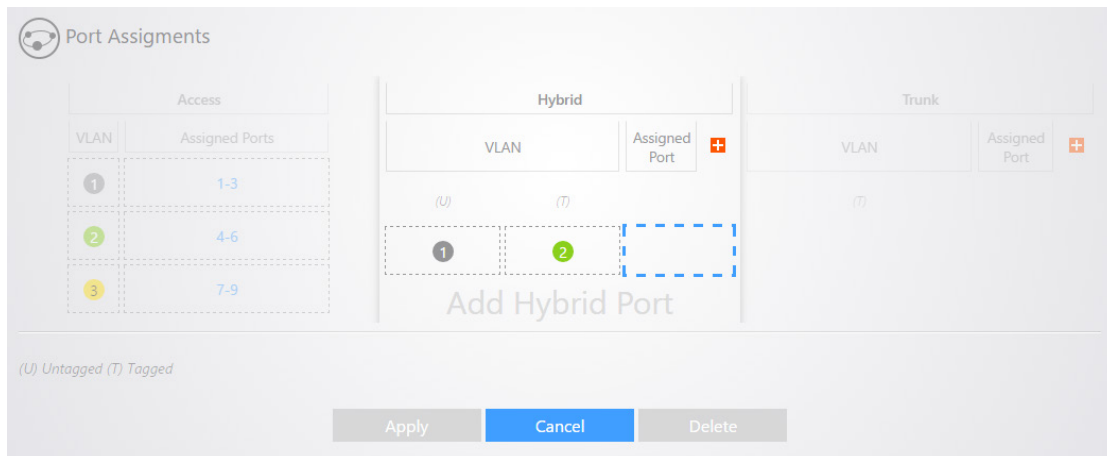


There will then be a blue outline around the box under the (T) column. The (T) indicates the VLANs that will have Tagged data. Click on the remaining VLANs to add them to the port. Click **Apply**. Repeat these steps for any other Hybrid ports you need to configure.



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.

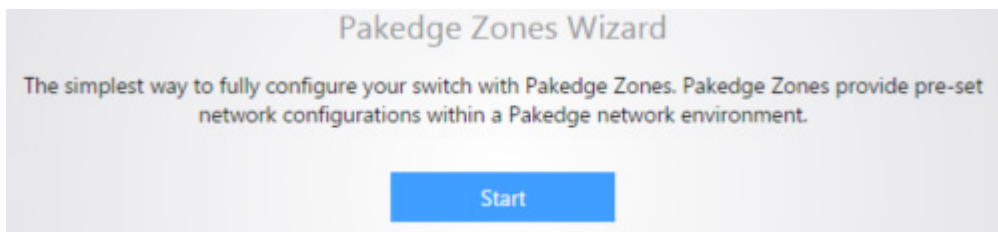


Click the port you want to add as hybrid. Click **Apply** to finalize the settings.

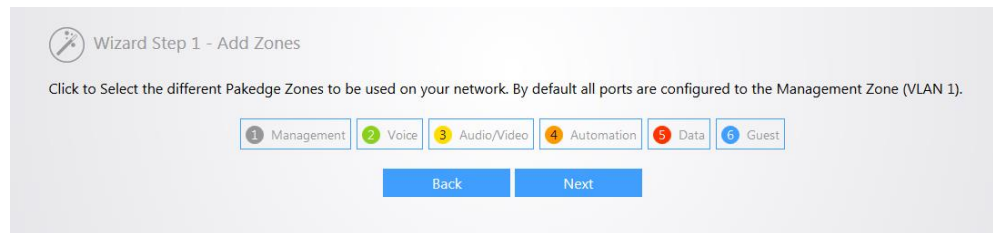
Using the Zone Wizard

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.

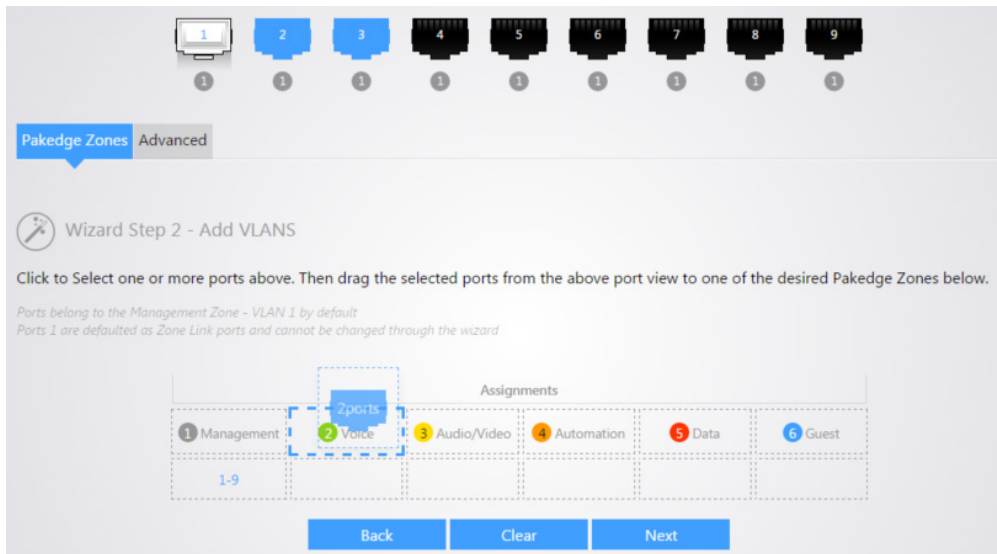
The VLAN configuration page will allow you to use the Pakedge Zone Wizard to setup your different VLANs. Click on **Start** to begin the wizard.



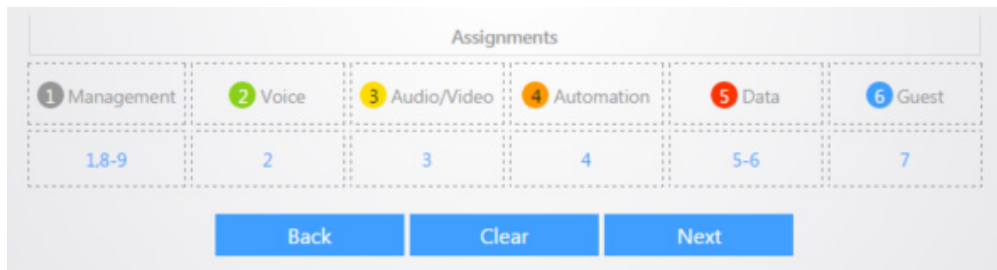
Step 1: Click on the VLANs you would like to use. The following image illustrates this. By default, VLANs 1 through 6 will be available for use. Click **Next**.



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.



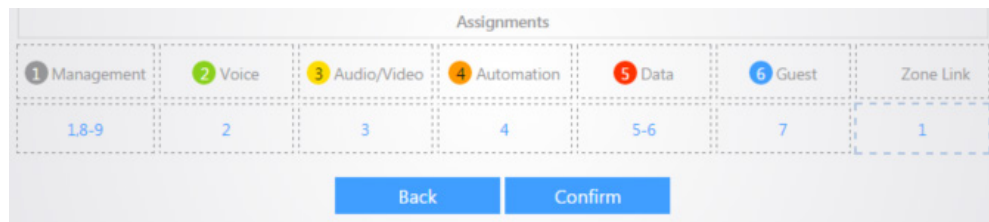
Continue to add the ports for all of your VLANs. When finished, your configuration might look like the following image. Click **Next** to continue.



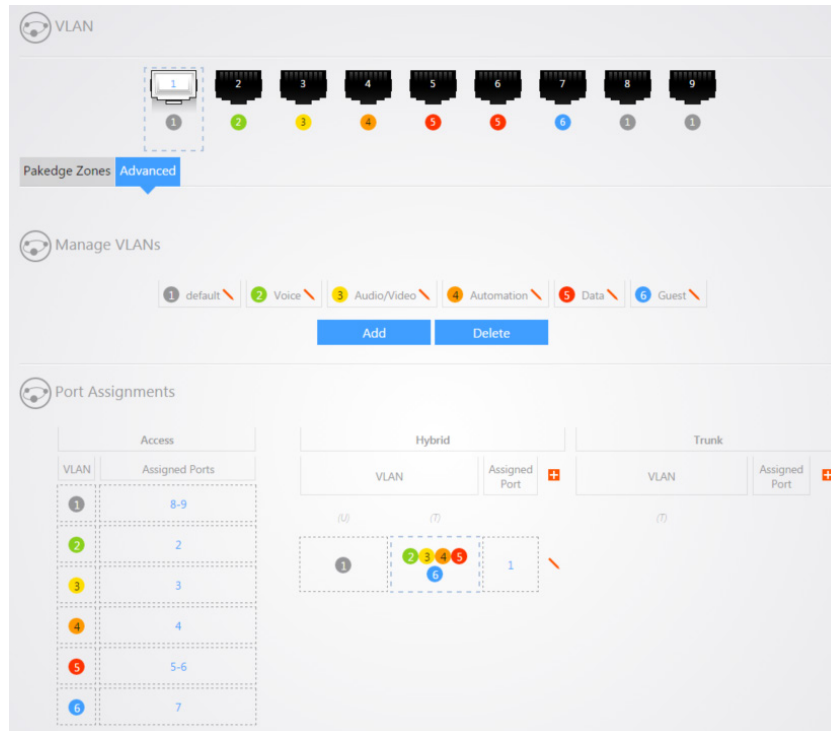
Step 3: Select your zone link ports. The zone link ports are ports that connect to other VLAN aware devices such as Routers, Access Points, and other managed switches. By default, port 1 is a Zone Link ports. Zone link ports are also known as hybrid ports. You can select another port and drag it down 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.



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



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.

Port Setup page

The screenshot displays the 'Port Setup' page with two tabs: 'Port Setup' (active) and 'OUI Setup'. The main section is titled 'Voice Global Setup' and contains the following configuration options:

- Voice VLAN Security Mode: **Disable** (dropdown menu)
- Voice VLAN Ageing Time: **1440** (input field)
- Voice VLAN ID: **None** (dropdown menu)
- CoS / 802.1p Remarking: **Disable** (dropdown menu) and **6** (input field)

Below these options are two buttons: **Apply** and **Clear**.

The next section shows a row of nine port icons, numbered 1 through 9. Port 1 is highlighted with a white border. Below each icon is a radio button labeled 'Auto' and the text 'Voice Packet'.

Below the port icons is a green dot icon with the text 'Voice VLAN Port Status' and 'Voice VLAN QoS Policy'.

The bottom section contains three dropdown menus for 'Voice VLAN Port Mode', 'Voice VLAN Port Status', and 'Voice VLAN QoS Policy', all set to 'Make no change'. Below these are two buttons: **Apply** and **Clear**.

Voice VLAN Security Mode: Set to enable or disable voice VLAN function.

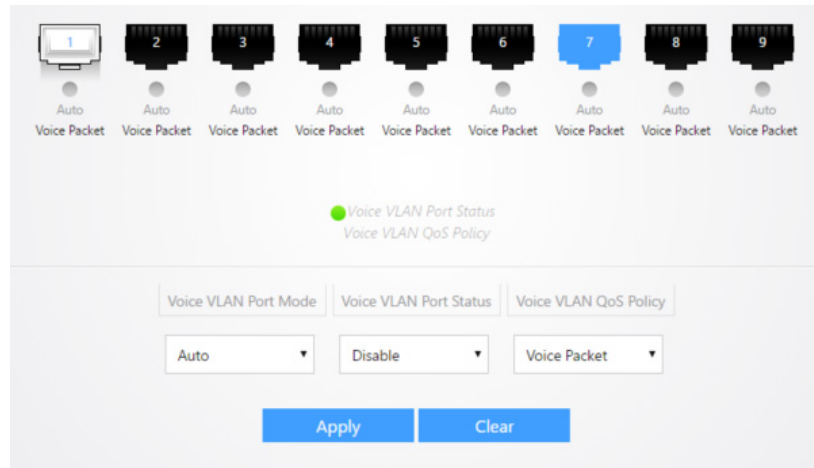
Voice VLAN Aging Time: Input value of aging time. Default is 1440 minutes. A voice VLAN entry will be aged out after this time without any activity.

Voice VLAN ID: Select Voice VLAN ID. Voice VLAN ID cannot be default VLAN (cannot be VLAN 1).

CoS / 802.1p Remarking: Enable or Disable 1p remarking. If enabled, qualified packets will be remarked by this value. Also select a CoS value of VPT. Qualified packets will use this VPT value as Inner CoS priority.

To configure Voice VLAN, set the **Voice VLAN Security mode** to **Enable**. 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, 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.



Port: Select the port to apply configurations to.

Voice VLAN Port Mode: Set Auto/Manual for Voice VLAN on an interface.

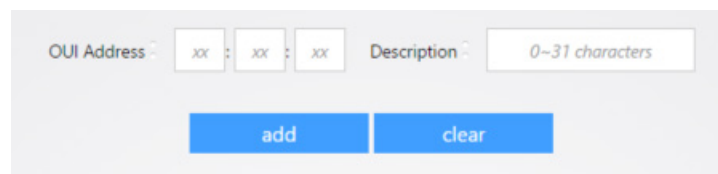
Voice VLAN Port Status: Enable/disable the display of voice VLAN mode.

Voice VLAN QoS Policy: Display voice VLAN remark will effect which kind of packet

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.

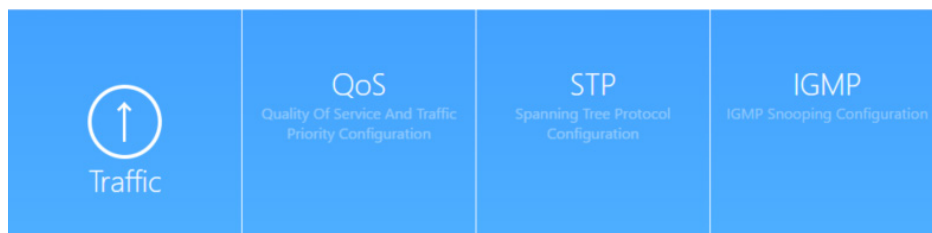
OUI Setup page

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. Enter a **Description**. Click **Add** to add your entry.



TRAFFIC MENU

The *Traffic* menu lets you configure QoS, STP, and IGMP.



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.

QoS Property page

The screenshot shows the QoS Property configuration page. It features a navigation bar with tabs for QoS Property, Queue Scheduling, CoS Mapping, DSCP Mapping, and IP Precedence Mapping. The QoS Property tab is active. The main content area is titled "QoS Property Global Setup" and includes a "State" dropdown menu set to "Disabled" and a "Trust Mode" dropdown menu set to "CoS". Below these are "Apply" and "Clear" buttons. A central section displays nine ports (1-9) with status indicators for CoS, DSCP, and IP Precedence. A legend below the ports defines the indicators: a green dot for CoS State, a red dot for DSCP State, and a blue dot for IP Precedence State. The bottom section is titled "Remarking" and has three sub-sections: "CoS", "Trust", and "IP Precedence". Each sub-section has a "Make no change" dropdown menu. At the bottom are "Apply" and "Clear" buttons.

The *QoS Property* page allows for the configuration of global QoS mode settings and individual ports. It also provides the individual port configurations to specify the type of QoS marking that should be used on each port.

State: Set to enable/disable QoS globally.

Trust Mode: Select QoS trust mode

- **CoS:** Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on the CoS Mapping page.
- **DSCP:** All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP Mapping page. If traffic is not IP traffic, it is mapped to the best effort queue.

- **CoS-DSCP:** Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic.
- **IP Precedence:** Traffic is mapped to queues based on the IP Precedence (first three bits of ToS field, although this has been depreciated for DSCP). The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping

Port: Port name

CoS: Port default CoS priority value for the selected ports

Trust: Port trust state

- **Enabled:** Traffic will follow trust mode in global setting
- **Disabled:** Traffic will always use best efforts

Remarking (CoS): Port CoS remarking admin state:

- **Enabled:** CoS remarking is enabled
- **Disabled:** CoS remarking is disabled

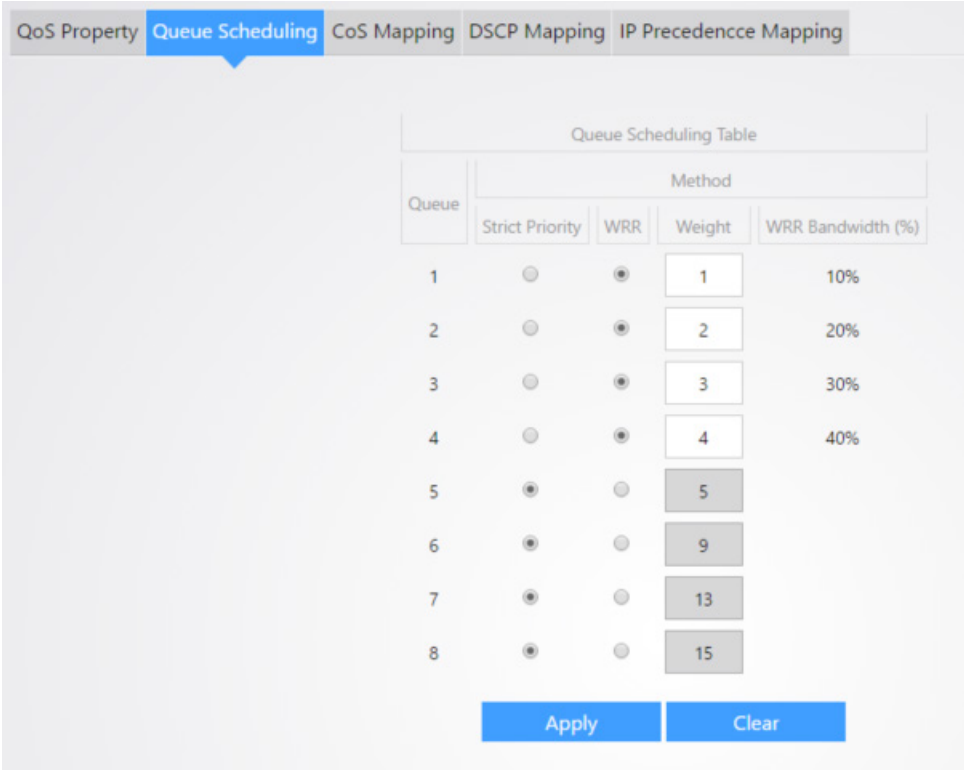
Remarking (DSCP): Port DSCP remarking admin state

- **Enabled:** DSCP remarking is enabled
- **Disabled:** DSCP remarking is disabled

Remarking (IP Precedence): Port IP Precedence remarking admin state

- **Enabled:** IP Precedence remarking is enabled
- **Disabled:** IP Precedence remarking is disabled

Queue Scheduling page



The screenshot shows the Queue Scheduling page with the following configuration:

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input type="radio"/>	<input checked="" type="radio"/>	1	10%
2	<input type="radio"/>	<input checked="" type="radio"/>	2	20%
3	<input type="radio"/>	<input checked="" type="radio"/>	3	30%
4	<input type="radio"/>	<input checked="" type="radio"/>	4	40%
5	<input checked="" type="radio"/>	<input type="radio"/>	5	
6	<input checked="" type="radio"/>	<input type="radio"/>	9	
7	<input checked="" type="radio"/>	<input type="radio"/>	13	
8	<input checked="" type="radio"/>	<input type="radio"/>	15	

Buttons: Apply, Clear

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

- Strict Priority (SP)—Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.
- Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

The queuing modes can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with Queue 8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).

Queue: Queue ID to configure.

Strict Priority: Set queue to strict priority type.

WRR: Set queue to Weight Round Robin type.

Weight: If the queue type is WRR, set the queue weight for the queue (1-127).

WRR Bandwidth: Display of the WRR queue bandwidth percentage.

CoS Mapping page

CoS Priority	Queue
CoS Priority 0	Queue 2
CoS Priority 1	Queue 1
CoS Priority 2	Queue 3
CoS Priority 3	Queue 4
CoS Priority 4	Queue 5
CoS Priority 5	Queue 6
CoS Priority 6	Queue 7
CoS Priority 7	Queue 8

The CoS Mapping table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

Use the CoS Mapping table to remark the CoS/802.1p priority for egress traffic from each queue.

CoS Priority: The CoS Priority level being set

Queue: Select which Queue the CoS priority should be assigned to

DSCP Mapping page

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

D : DSCP P : Cos Priority

priority

Make no change ▾

Apply Clear

The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.

D: DSCP Priority Value in numbered format

P: Priority, the CoS Priority level currently assigned to the DSCP value

Priority: Set the selected DSCP Values with this CoS Priority level

IP Precedence Mapping page

This page allows users to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping.

QoS Property	Queue Scheduling	CoS Mapping	DSCP Mapping	IP Precedence Mapping
IP Precedence Mapping				
IP Precedence 0	Queue 1	IP Precedence 1	Queue 2	
IP Precedence 2	Queue 3	IP Precedence 3	Queue 4	
IP Precedence 4	Queue 5	IP Precedence 5	Queue 6	
IP Precedence 6	Queue 7	IP Precedence 7	Queue 8	
Apply Clear				

IP Precedence: IP Precedence value

Queue: Select a Queue ID for the IP Precedence value

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, 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.

STP Property Setup page

STP

STP Property Setup | Port Setup | Statistics

Global Setup

STP Status: STP Version:

Path Cost: BPDUs Processing:

Bridge Setup

Max Age: Hello Time:

Forward Delay: Tx Hold Count:

Priority:

Note: Max age should meet follow requirements: Max Age >= 2 x (Hello Time + 1) Max Age <= 2 x (Forward Delay - 1)

Specified Root Bridge

Bridge ID: Root Bridge ID:

Root Port: Root Path Cost:

Topology Status: Last Topology Change Time:

STP Status: Enable/Disable the STP on the switch.

STP Version: Specify the STP operation mode.

- **STP:** Enable the Spanning Tree (STP) operation.
- **RSTP:** Enable the Rapid Spanning Tree (RSTP) operation.

Path Cost: Specify the path cost method.

- **Long:** Specifies that the default port path costs are within the range 1-200,000,000.
- **Short:** Specifies that the default port path costs are within the range 1-65,535.

BPDU Processing: Specify the BPDU forward method when the STP is disabled.

- **Filtering:** Filter the BPDU when STP is disabled.
- **Flooding:** Flood the BPDU when STP is disabled.

Max Age: Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.

Hello Time: Specify the STP hello time in second to broadcast its hello message to other bridges by Designated Ports. Its valid range is from 1 to 10 seconds.

Forward Delay: Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.

Tx Hold Count: Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.

Priority: Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.

Port Setup page

The screenshot displays the 'Port Setup' configuration page for STP. It features a header with three tabs: 'STP Property Setup', 'Port Setup' (selected), and 'Statistics'. Below the header, there are nine port configuration cards, numbered 1 through 9. Each card shows a port icon, a green dot indicating STP is enabled, a grey dot indicating it is not an edge port, a path cost of 20000, and a priority of 128. The P2P Port is set to 'Auto'. A legend below the cards explains the symbols: a green dot for 'Enable STP', a grey dot for 'Edge Port', a dashed line for 'Path Cost', a solid line for 'Priority', and 'Auto' for 'P2P Port'. At the bottom, there are five configuration fields: 'STP Status' (Make no change), 'Path Cost' (0), 'Priority' (128), 'Edge Port' (Make no change), and 'P2P Port' (Make no change). 'Apply' and 'Clear' buttons are located at the bottom center.

STP Status: Enable/Disable the STP on the specified port.

Path Cost: Specify the STP path cost on the specified port.

Priority: Specify the STP path cost on the specified port.

Edge Port: Specify the edge mode.

- **Enable:** Force to true state (as link to a host).
- **Disable:** Force to false state (as link to a bridge).

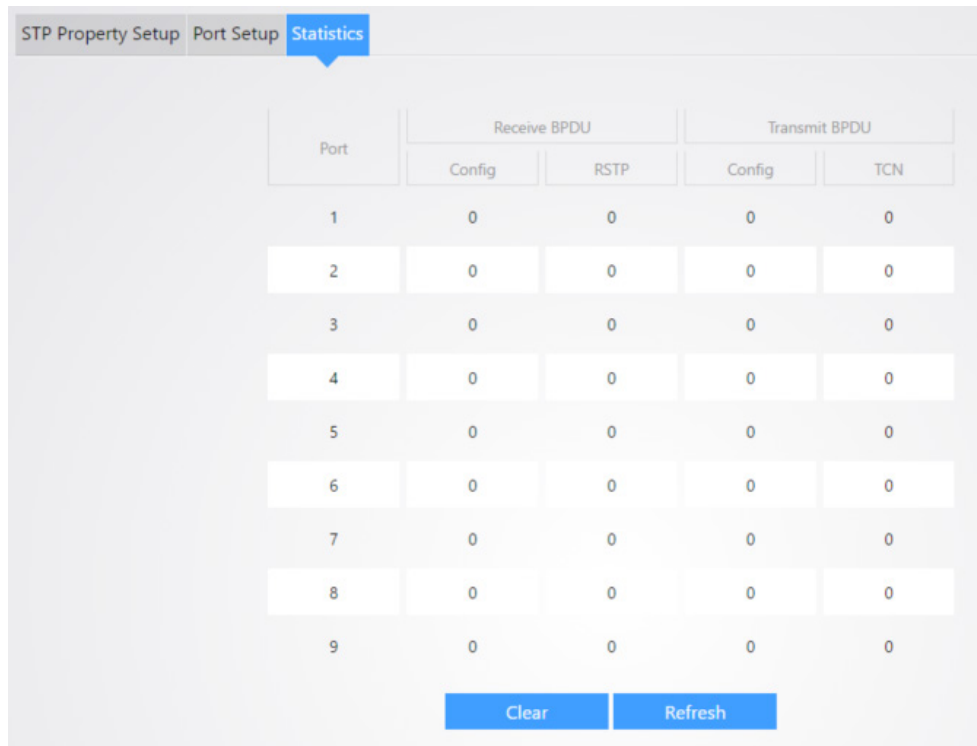
In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.

P2P Port: Specify the Point-to-Point operation mode.

- **Enable:** Force the true state (as link to an RSTP participating switch).
- **Disable:** Force to false state (as link to host).
- **Auto:** Automatically detect based on the duplex setting of the port.

Statistics page

The *Statistics* page displays STP information for each port.



Port	Receive BPDU		Transmit BPDU	
	Config	RSTP	Config	TCN
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
9	0	0	0	0

Clear Refresh

Receive BPDU (Config): The counts of the received CONFIG BPDU.

Receive BPDU (RSTP): The counts of the received TCN BPDU.

Transmit BPDU (Config): The counts of the transmitted CONFIG BPDU.

Transmit BPDU (TCN): The counts of the transmitted TCN BPDU.

IGMP

IGMP Snooping page

ID	VLAN ID	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
1	1	Disable	Enable	2	125	10	2	1	Disable
2	2	Disable	Enable	2	125	10	2	1	Disable
3	3	Disable	Enable	2	125	10	2	1	Disable

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).

State: Set the enabling status of IGMP Snooping functionality

- **Enable:** If Checked Enable IGMP Snooping, else is **Disabled** IGMP Snooping.

Version: Set the IGMP snooping version.

- **IGMPv2:** Only support process IGMP v2 packet.
- **IGMPv3:** Support v3 basic and v2.

Report Suppression: Set the enabling status of IGMP v2 report suppression

- **Enable:** If Checked Enable IGMP Snooping v2 report suppression, else **Disable** the report suppression function.

VLAN: The IGMP entry VLAN ID

Operation Status: The enable status of IGMP snooping VLAN functionality.

Router Port Auto Learn: The enabling status of IGMP snooping router port auto learning.

Query Robustness: The Query Robustness allows tuning for the expected packet loss on a subnet.

Query Interval: The interval of querier to send general query.

Query Max Response Interval: In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.

Last Member Query count: The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

Last Member Query Interval: The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

Immediate leave: The immediate leave status of the group will immediate leave when receive IGMP Leave message.

IGMP Snooping VLAN Settings Edit Page

VLAN: The selected VLAN list.

State: Set the enabling status of IGMP Snooping VLAN functionality

- **Enable:** If Checked Enable IGMP Snooping VLAN, else is Disabled IGMP Snooping VLAN.

Router Port Auto Learn: Set the enabling status of IGMP Snooping router port learning.

- **Enable:** If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.

Immediate leave: Immediate Leave the group when receive IGMP Leave message.

- **Enable:** If checked Enable immediate leave, else disable immediate leave.

Query Robustness: The Admin Query Robustness allows tuning for the expected packet loss on a subnet.

Query Interval: The Admin interval of querier to send general query.

Query Max Response Interval: The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.

Last Member Query Counter: The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

Last Member Query Interval: The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

Operational Status

Status: Operational IGMP snooping status, must both IGMP snooping global and IGMP snooping enable the status will be enable.

Query Robustness: Operational Query Robustness.

Query Interval: Operational Query Interval.

Query Max Response Interval: Operational Query Max Response Interval.

Last Member Query Counter: Operational Last Member Query Count.

Last Member Query Interval: Operational Last Member Query Interval.

IGMP Querier

VLAN: IGMP Snooping querier entry VLAN ID

State: The IGMP Snooping querier Admin State.

Operational Status: The IGMP Snooping querier operational status

Querier Version: The IGMP Snooping querier operational version.

Querier IP: The operational Querier IP address on the VLAN

IGMP Querier VLAN Settings Edit Page

VLAN: The Selected Edit IGMP Snooping querier VLAN List

State: Set the enabling status of IGMP Querier Election on the chose VLANs

- **Enabled:** if checked Enable IGMP Querier else Disable IGMP Querier

Version: Set the query version of IGMP Querier Election on the chose VLANs

- **IGMPv2:** Querier version 2.
- **IGMPv3:** Querier version 3. (IGMP Snooping version should be IGMPv3) .

IGMP Statistics

Receive Packet

Total: Total RX IGMP packet, include ipv4 multicast data to CPU.

Valid: The valid IGMP snooping process packet.

InValid: The invalid IGMP snooping process packet.

Other: The ICMP protocol is not 2, and is not ipv4 multicast data packet.

Leave: IGMP leave packet.

Report: IGMP join and report packet

General Query: IGMP General Query packet

Special Group Query: IGMP Special Group General Query packet

Source-specific Group Query: IGMP Special Source and Group General Query packet

Transmit Packet:

Leave: IGMP leave packet

Report: IGMP join and report packet

General Query: IGMP general query packet include querier transmit general query packet

Special Group Query: IGMP special group query packet include querier transmit special group query packet

Source-specific Group Query: IGMP Special Source and Group General Query packet

Multicast Property

Unknown Multicast Action: Set the unknown multicast action

- **Drop:** Drop the unknown multicast data.
- **Flood:** Flood the unknown multicast data.
- **Router port:** Forward the unknown multicast data to router port.

IPv4: Set the ipv4 multicast forward method.

- **MAC-VID:** Forward method is the Destination MAC and VLAN ID.
- **DIP-VID:** Forward method is the Destination IP and VLAN ID.

Multicast Group

VLAN: The VLAN ID of group.

Group Address: The group IP address.

Member: The member ports of group.

Type: The type of group. Static or Dynamic.

Life(Sec): The life time of this dynamic group.

Multicast Group Add

VLAN: The VLAN ID of group.

Group Address: The group IP address.

Member: The member ports of group.

- **Available Port:** Optional port member
- **Selected Port:** Selected port member

Multicast Router Port


VLAN: The VLAN ID router entry.

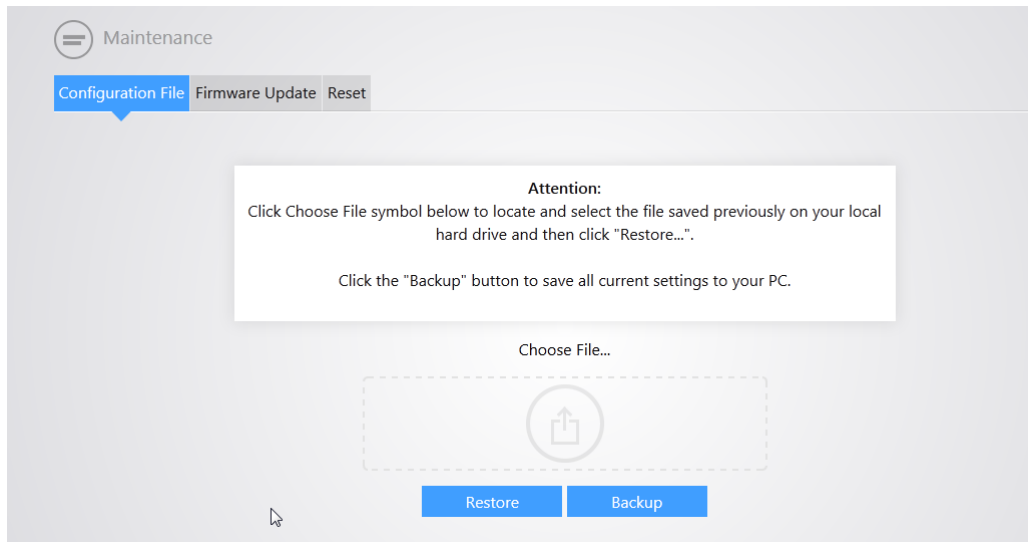
Member: Router Port member.


Life (Sec): The expiry time of the router entry.

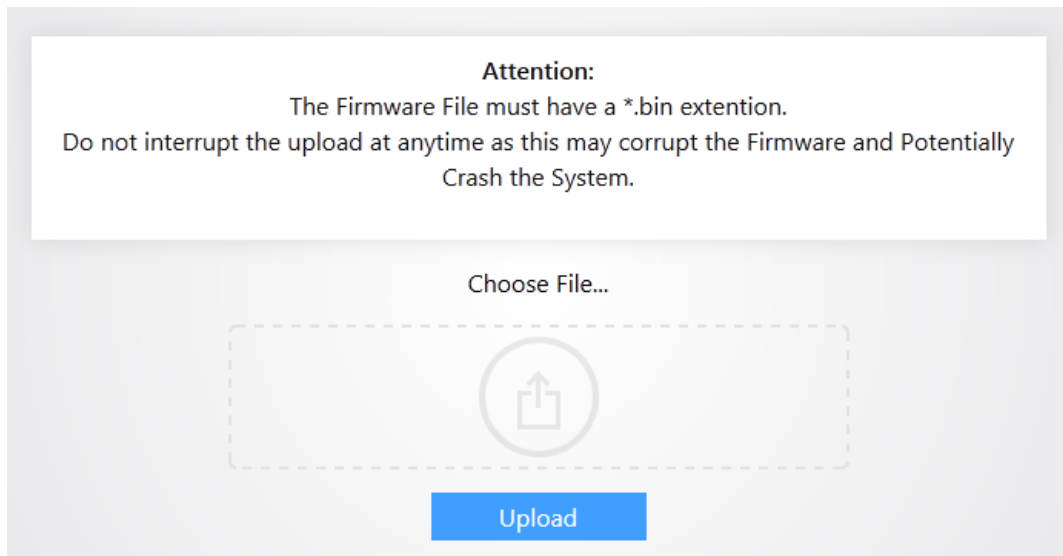
MAINTENANCE

The Management > Maintenance page will allow you to backup/restore configurations, perform firmware updates and factory reset the switch. To create a backup of your configuration, simply click

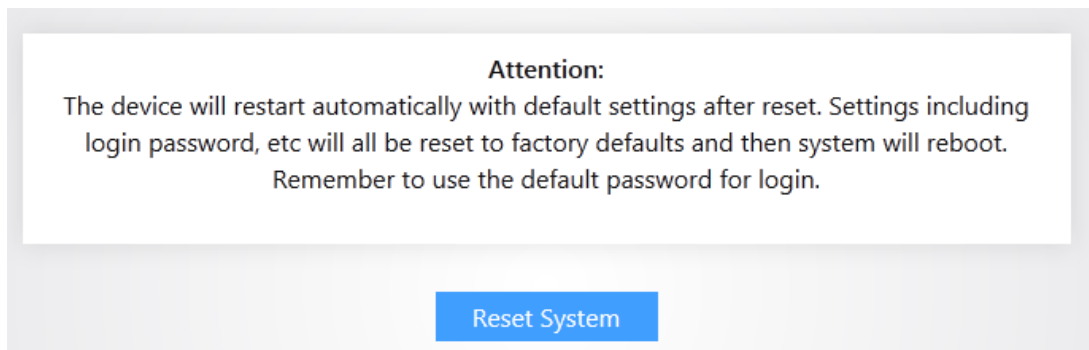
Backup. To restore a configuration, click the  icon and navigate to your configuration file. Click **Restore**.



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.

Community

Community: The SNMP community name. Its maximum length is 20 characters.

Access Right: SNMP access mode

- **Read-Only:** Read only.
- **Read-Write:** Read and write.

Trap Event

Authentication Failure: SNMP authentication failure trap, when community not match or user authentication password not match.

Link Up/Down: Port link up or down trap

Cold Start: Device reboot configure by user trap

Warm Start: Device reboot by power down trap

Notification

Server Address: IP address or the hostname of the SNMP trap recipients.

Version: Specify SNMP notification version

- **SNMPv1:** SNMP Version 1 notification.
- **SNMPv2:** SNMP Version 2 notification.

Type: Notification Type

- **Trap:** Send SNMP traps to the host.
- **Inform:** Send SNMP informs to the host.

Community: SNMP community name for notification.

Trap Event

Authentication Failure: SNMP authentication failure trap, when community not match or user authentication password not match.

Link Up/Down: Port link up or down trap.

Cold Start: Device reboot configure by user trap.

Warm Start: Device reboot by power down trap.

Notification

Server Address: IP address or the hostname of the SNMP trap recipients.

Version: Specify SNMP notification version.

- **SNMPv1:** SNMP Version 1 notification.
- **SNMPv2:** SNMP Version 2 notification.

Type: Notification Type:

- **Trap:** Send SNMP traps to the host.
- **Inform:** Send SNMP informs to the host.:

Community: SNMP community name for notification.

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.

Global Setup

LLDP State: Enable/ Disable LLDP protocol on this switch.

LLDP Handling: Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled.

- **Filtering:** Deletes the packet.
- **Bridging:** (VLAN-aware flooding) Forwards the packet to all VLAN members.
- **Flooding:** Forwards the packet to all ports

TLV Advertise Interval: Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32767 seconds.

Holdtime Multiplier: Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).

Reinitialization Delay: Select the delay before a re-initialization (range 1–10 seconds, default = 2).

Transmit Delay: Select the delay after an LLDP frame is sent (range 1–8191 seconds, default = 3).

Port Setup

Port: Select specified port or all ports to configure LLDP state.

Mode: Select the transmission state of LLDP port interface.

- **Disable:** Disable the transmission of LLDP PDUs.
- **RX Only:** Receive LLDP PDUs only.
- **TX Only:** Transmit LLDP PDUs only.
- **TX And RX:** Transmit and receive LLDP PDUs both.

Neighbor Info

Local Port: Number of the local port to which the neighbor is connected.

Chassis ID Subtype: Type of chassis ID (for example, MAC address).

Chassis ID: Identifier of the 802 LAN neighboring device's chassis.

Port ID Subtype: Type of the port identifier that is shown.

Port ID: Identifier of port.

System Name: Published name of the switch.

Time to Live: Time interval in seconds after which the information for this neighbor is deleted.

Port Statistics

Insertions: The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.

Deletions: The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.

Drops: The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.

Age Outs: The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.

Port: Interface or port number.

Transmit Frame Total: Number of LLDP frames transmitted on the corresponding port.

Receive Frame Total: Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.

Receive Frame Discard: Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.

Receive Frame Error: Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.

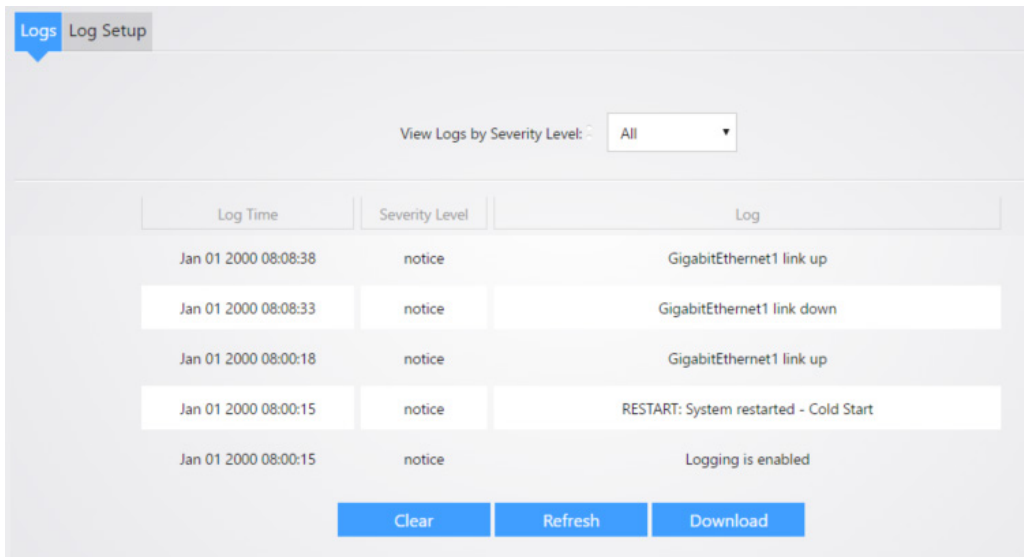
Receive TLV Discard: Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.

Receive TLV Unrecognized: Number of TLVs of LLDP frames that are unrecognized while the LLDP agent is enabled.

Neighbor Timeout: Number of age out LLDP frames.

SYSLOG

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



The screenshot shows a web interface for Syslog. At the top, there are tabs for "Logs" and "Log Setup". Below the tabs, there is a dropdown menu labeled "View Logs by Severity Level:" with "All" selected. The main content is a table with three columns: "Log Time", "Severity Level", and "Log". The table contains five rows of log entries. At the bottom of the table, there are three buttons: "Clear", "Refresh", and "Download".

Log Time	Severity Level	Log
Jan 01 2000 08:08:38	notice	GigabitEthernet1 link up
Jan 01 2000 08:08:33	notice	GigabitEthernet1 link down
Jan 01 2000 08:00:18	notice	GigabitEthernet1 link up
Jan 01 2000 08:00:15	notice	RESTART: System restarted - Cold Start
Jan 01 2000 08:00:15	notice	Logging is enabled

Severity levels

- **Emergency Level 1:** The system is unusable.
- **Alert Level 2:** Action must be taken immediately.

- **Critical Level 3:** Critical conditions.
- **Error Level 4:** Error conditions.
- **Warning Level 5:** Warning conditions.
- **Notice Level 6:** Normal but significant conditions.
- **Informational Level 7:** Informational messages.
- **Debug Level 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.

Port	Pair A	Pair A Length(m)	Pair B	Pair B Length(m)	Pair C	Pair C Length(m)	pair D	Pair D Length(m)
24	Normal	0	Normal	0	Normal	0	Normal	1

Ping page

Destination IP Address: Specify the Hostname/IPv4/IPv6 address for the remote logging server.

Sending Times: Specify the number of ICMP ping requests.

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.

11734 Election Road

Draper, UT 84020

APPENDIX B – SPECIFICATIONS

Item	Specification
Input voltage	100 – 240VAC 50/60 Hz 6A
Power consumption	7W
Interface	8x RJ45 10/100/1000 auto-sensing Giga switching ports with PoE/PoE+ output 1x 1000 Mbps SFP port
PoE power budget	125W
Management interface	1x Console port
Operating temperature	0°C ~ 40°C
Storage temperature	-40° ~ 70°C
Operating humidity	10% - 90% RH, non-condensing
Storage humidity	5% - 90% RH, non-condensing
Certifications	FCC/CE, RoHS
Dimension	228 mm × 128 mm × 31 mm
Weight	5 lbs (2.25 kg)
Features	Specification
Switching capacity	18 Gbps
Packet forwarding	13.3 Mpps
Packet Buffer	4Mbits
MAC address table	8K
VLAN	<ol style="list-style-type: none"> 1. VLAN distribution based on ports. Up to 9 can be configured; 2. IEEE 802.1Q VLAN. Up to 128 can be configured; 3. Voice VLAN;
Multicast	<ol style="list-style-type: none"> 1. IGMP Snooping V2/V3 Basic; 2. Up to 256 entries can be learned; 3. Fast leave 4. Querier
Broadcast storm constrain	<ol style="list-style-type: none"> 1. Broadcast storm constrained based on ports; 2. Multicast storm constrained based on ports; 3. Unknown unicast storm constrained based on ports;
STP	<ol style="list-style-type: none"> 1. IEEE 802.1d STP; 2. IEEE 802.1w RSTP; 3. Edge port; 4. P2P port; 5. STP BPDU packets statistics;

Safety	<ol style="list-style-type: none"> 1. ARP attack defense, worm attack defense, DoS attack defense and MAC attack defense; 2. Interface isolation;
QoS	<ol style="list-style-type: none"> 1. 802.1P port trust mode; 2. IP DSCP port trust mode; 3. IP Precedence port trust mode; 4. Bandwidth control; 5. Up to 8-queue QoS mapping;
Firmware/Configuration Upgrade	TFTP (Trivial File Transfer Protocol) WEB
Management	<ol style="list-style-type: none"> 1. Telnet configuration 2. Console interface configuration 3. SNMP (Simple Network Management Protocol) 4. WEB
Maintenance	Ping\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 WARRANTY. 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.
11734 Election Road
Draper, UT 84020
U.S.A.

877-274-6100

Email: support@pakedge.com

www.pakedge.com



11734 Election Road
Draper, UT 8402045
U.S.A

Visit Us At:

www.pakedge.com

© Pakedge Device & Software Inc. 2017 – All Rights Reserved

DOC-00251-C 2017-06-19 MS