User's Guide

TRENDnet®

5-Port Gigabit PoE++ Powered Managed Switch with PoE Passthrough

TPE-B541

Table of Contents

Thank you for purchasing your new TRENDnet PoE-Powered Switch!

Please note: The scope of this user's guide encompasses multiple products with varying features. Images, artwork, and other specificities including port count, interfaces etc. may not be identical to the model you purchased. Please consult the specific model specifications for your unit for a full list of supported features.

PoE-Powered Switch Product Overview

TPE-B541 Overview

TPE-B541

Package Contents

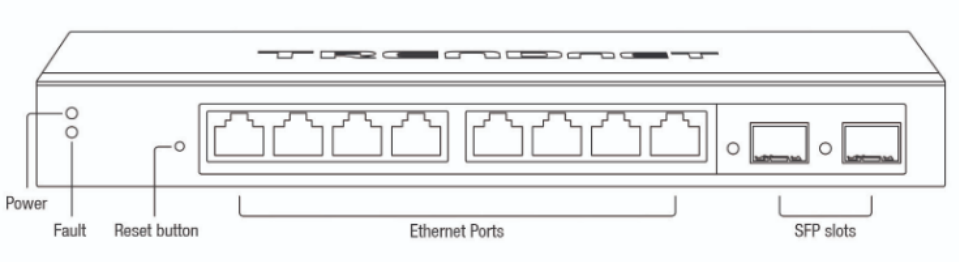
In addition to your switch, the package includes:

- Quick Installation Guide

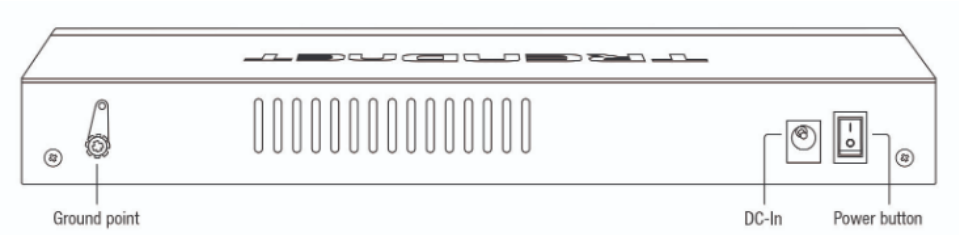
If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

TPE-B541 Hardware Features

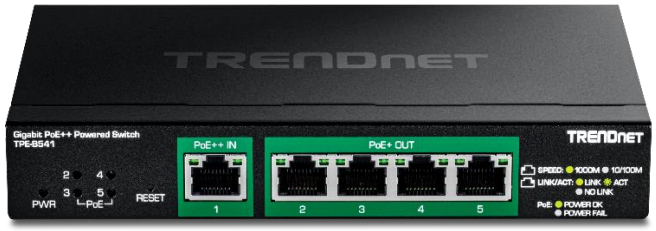
Front View



Rear View



- **Power and PoE LEDs** – LED indicators for power and PoE status.
- **Reset Button –** Press and hold the button 1~3 seconds and release to reboot the device. Pressing the button more than 5 seconds will reset the switch to factory defaults. The ports LEDs will turn off to indicate that the reset was initiated.
- **PoE In Ports (1) –** Connect a PoE-powered network cable to power this switch.
- **Ethernet Ports (2-5) –** Connect either network PoE+ or non-PoE devices at 1Gbps / 100Mbps / 10Mbps speed.



Diagnostic LEDs

Power LED

On	:	When the Power LED is on, the device is receiving power.
Off	:	When the Power LED is off, the power source is not connected or the device is not receiving power.

PoE LEDs

On	:	When the PoE LED is on, the port is supplying PoE power.
Off	:	When the PoE LED is on, the port is not supplying PoE power.

Ethernet Port LEDs (1-5)

Left on	:	When the LED is on, the respective port is connected to a 1Gbps Ethernet network.
Right on	:	When the LED is on, the respective port is connected an Ethernet network.
Right Blinking	:	When the LED is blinking green, the port is transmitting or receiving data on the network.
Left Off	:	When the LED is off, and the right LED is on, the respective port is connected to a 10/100Mbps Ethernet network
All Off		When the LED is off, the respective port is disconnected.

Setup Wizard

When the switch is reset to factory defaults, the setup wizard will appear on the first login to guide through the initial setup process.

1. Assign a static IP address to your computer's network adapter in the subnet of 192.168.10.x (e.g. 192.168.10.25) and a subnet mask of 255.255.255.0.

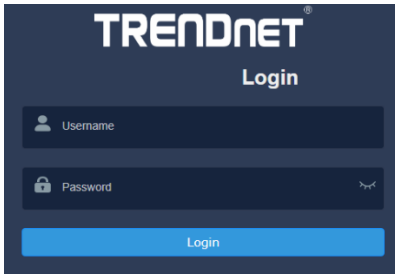
2. Open your web browser, and type the IP address of the switch in the address bar, and then press Enter. The default IP address is 192.168.10.200.

3. Enter the User Name and Password, and then click **Login.** By default:

User Name: **admin**

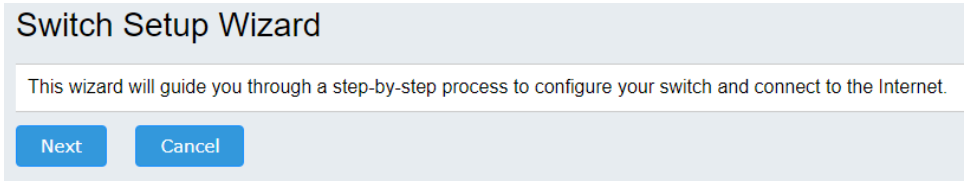
Password: **admin**

Note: *User name and password are case sensitive.*



4. Select **Next** to move onto the next screen

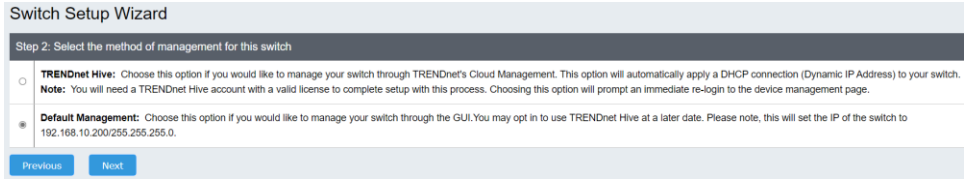
Note*: If the switch setup wizard does not appear, you can click the setup wizard button in the top right section of the switch management page to access the switch setup wizard.*



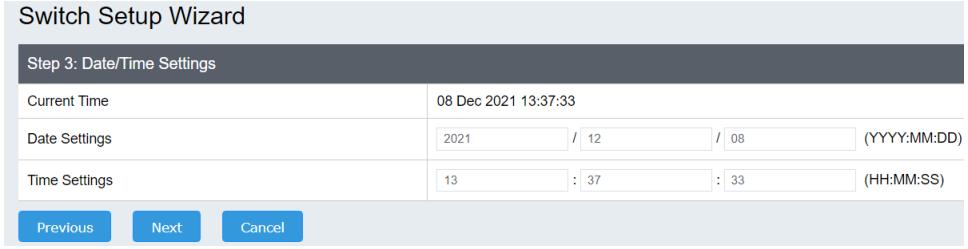
5. Change your login password and click **Next**. The default password is **admin**.

Note: If entering a new password, please note that you will need to use the new password when logging into the switch management page for local management access moving forward.

6. For the method of management, select Default Management.

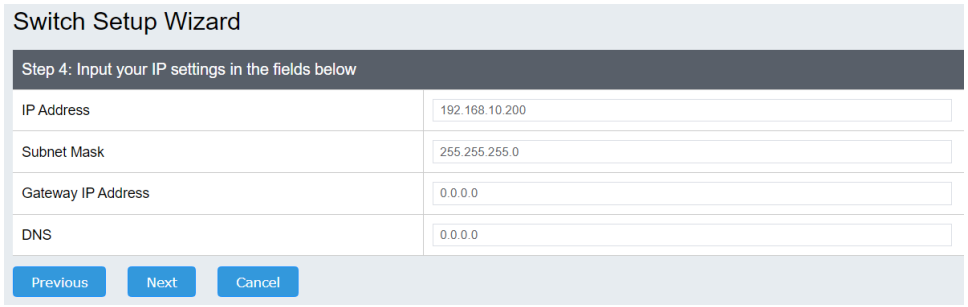


7. Configure the switch date and time settings, then click Next.



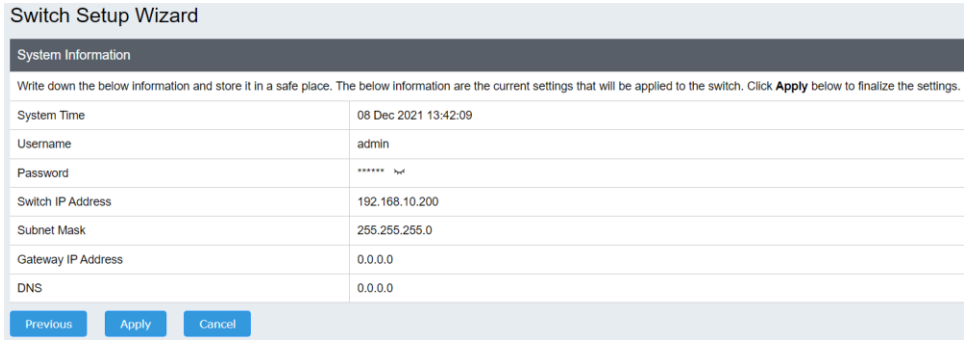
8. Configure the switch IP address, subnet mask, gateway IP address, and DNS settings to match the requirements of your existing network using the fields provided, then click Next.

Note: If the switch IP address settings are changed to a different IP network subnet such as 192.168.1.x, 192.168.2.x, etc. your computer's network adapter settings will need to be changed match the new IP address settings configured on the switch in order to access the switch management page.



9. The summary page will display all of the configuration settings that were applied through the setup wizard. Click Apply to complete the setup wizard.

Note: You may want to note the new password and IP address settings for local management access to switch.

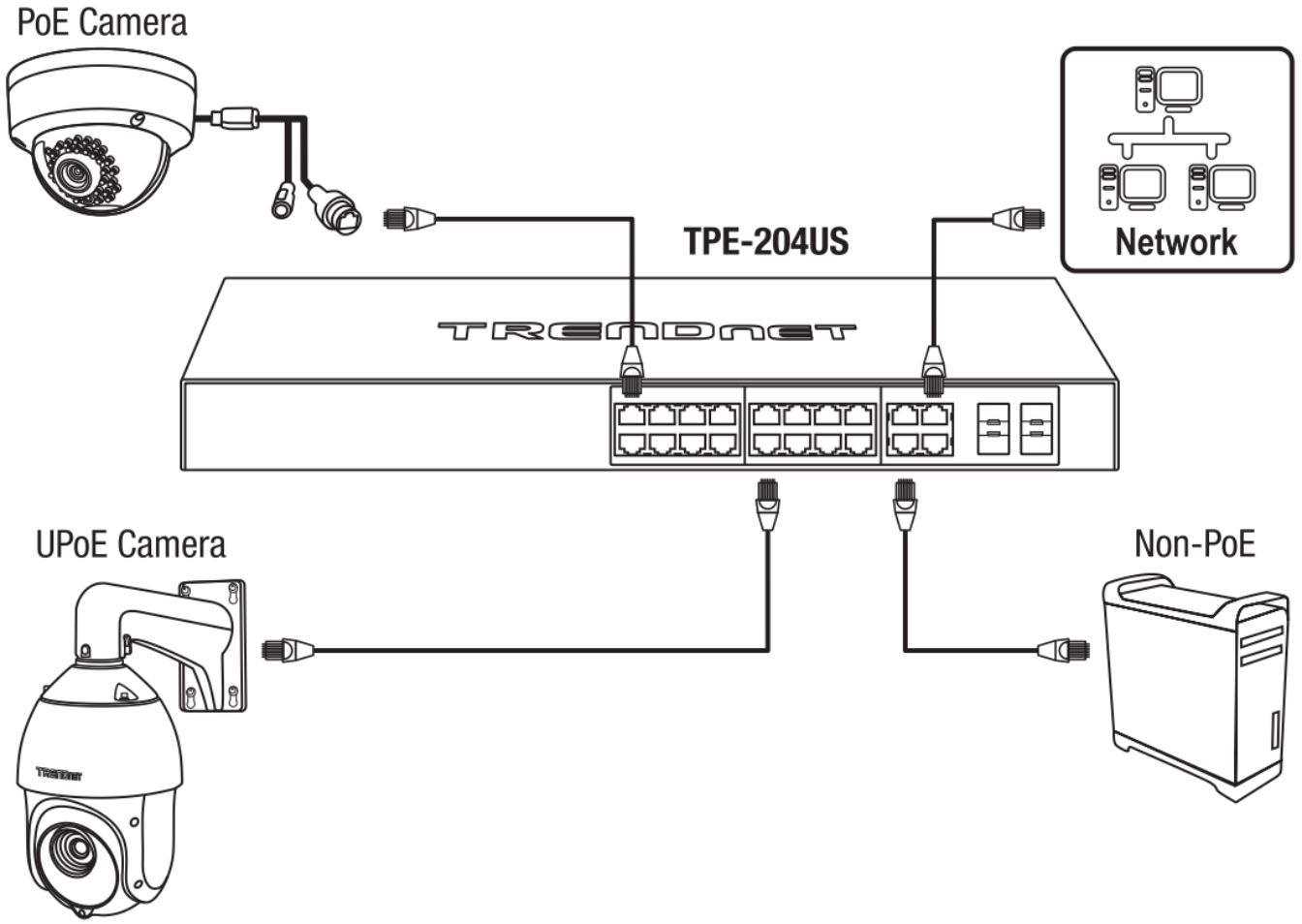


Connect additional devices to your switch

You can connect computers or other network devices to your switch using Ethernet cables to connect them to one of the available Gigabit Ethernet Ports, Gigabit Ethernet PoE Ports, Gigabit Ethernet PoE+ Ports, Gigabit Ethernet PoE++ Ports, or SFP Ports. Check the status of the LED indicators on the front panel of your switch to ensure the physical cable connection from your computer or device. You can use either the Gigabit Ethernet ports or SFP connections as network uplinks. (SFP modules sold separately)

Note: *If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured properly within the network subnet your switch is connected.*

Note: *Your switch model may be different than the one shown in the example illustrations.*



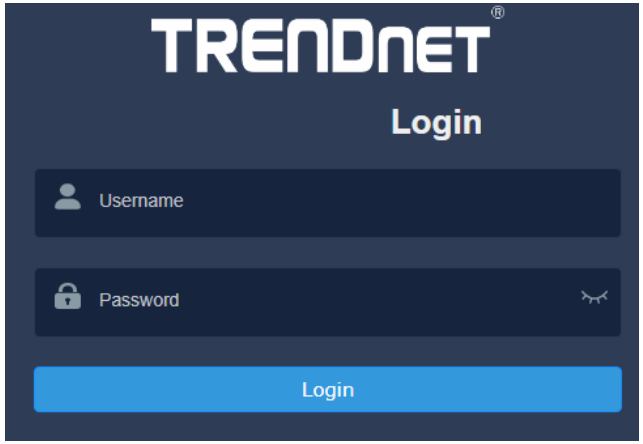
Access your switch management page

Note: *Your switch default management IP address http://192.168.10.200 is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide. Throughout this user's guide, the term Web Configuration will be used to reference access from web management page.*

1. Open your web browser and go to its IP address (default: http://192.168.10.200). Your switch will prompt you for a user name and password.

2. Enter the user name and password. By default:

   User Name: **admin**
   Password: **password**
   Note: *User Name and Password are case sensitive.*



Dashboard

View your switch status information

Dashboard

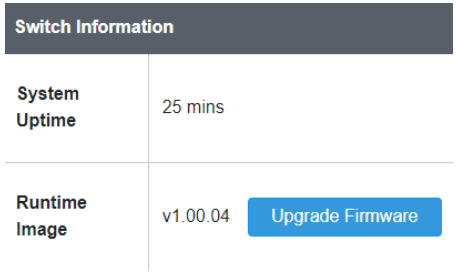
You may want to check the general system information of your switch such as firmware version, boot loader information and system uptime. Other information includes H/W version, RAM/Flash size, administration information, IPv4 and IPv6 information.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Dashboard**.

Switch Information

- **System Uptime** – The duration your switch has been running continuously without a restart/power cycle (hard or soft reboot) or reset.
- **Firmware:** The current software or firmware version your switch is running.
- **Boot Loader** – The current boot loader version your switch is running.



Hardware Information

- **DRAM Size:** Displays your switch RAM memory size.
- **Flash Size:** Displays your switch Flash memory size.
- **Fan Status:** Displays the current status of your switch's fan
- **Hardware Version:** Displays your switch's current hardware version

Hardware Information	
DRAM Size	256 KB
Flash Size	32 MB
Fan Status	None
Hardware Version	v1.00.00

Administration Information

- **System Description** – Displays the identifying system name of your switch. This information can be modified under the **System** section.
- **System Location** - Displays the identifying system location of your switch. This information can be modified under the **System** section.
- **System Contact –** Displays the identifying system contact or system administrator of your switch. This information can be modified under the **System** section.

Administration Information	
System Description	TPE-B541
System Location	Default Location
System Contact	Default Contact

System MAC Address, IPv4 Information

- **Serial No:** Displays the serial number of the switch
- **MAC Address:** Displays the switch system MAC address.
- **IP Address** – Displays the current IPv4 address assigned to your switch.
- **Subnet Mask** – Displays the current IPv4 subnet mask assigned to your switch.
- **Default Gateway** – Displays the current gateway address assigned to your switch.

System Information	
Serial NO.	EP4D5A1000001
MAC Address	78:2D:7E:23:A9:DA
IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	

IPv6 Information

- **Voice VLAN:** Displays if your switch has Voice VLAN enabled or disabled
- **Jumbo Frames:** Displays the size of Jumbo Frames that is supported.
- **IGMP Snooping:** Displays if your switch has IGMP Snooping enabled or disabled
- **STP:** Displays the current status of STP
- **LLDP:** Displays the current status ofLLDP

Feature Status	
Voice VLAN	OFF
Jumbo Frames	1518
IGMP Snooping	OFF
STP	ON
LLDP	ON

Automatic Network Features

- **QoS:** Displays if your switch has QoS enabled or disabled
- **DoS:** Displays if your switch has DoS enabled or disabled
- **IPv4 DHCP Client Mode:** Displays if your switch IPv4 address setting is set to DHCP client.

- **IPv6 DHCP Client Mode:** Displays if your switch IPv6 address setting is set to DHCP client.

Feature Status	
QoS	ON
DoS	OFF
IPv4 DHCP Client Mode	STATIC
Total PoE Usage	0.0% (0/40W)

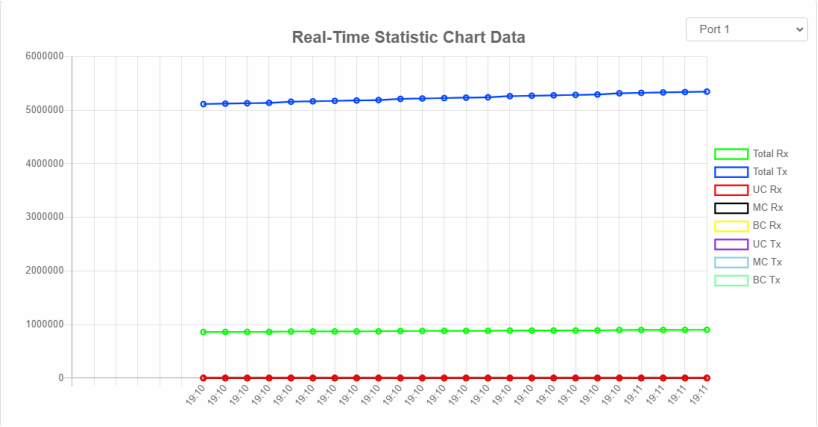
Real-time Statistics

View your switch status information

Dashboard > Real-time Statistics

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Dashboard**, then click on **Real-time Statistics.** The switch view shows the ports that are connected. Select **Status**, **Duplex, Speed,** or **PoE** to display which ports are currently using the selected feature.



3. Select the port from the drop down menu to review the current settings.
   - **Total(Rx):** The total number of packets received
   - **Total(TX):** The total number of packets transmitted
   - **UC (Rx):** The number of Unicast packets received
   - **MC(Rx):** The number of Multicast packets received
   - **BC(Rx):** The number of Broadcast packets received
   - **UC(Tx):** The number of Unicast packets transmitted
   - **MC(Tx):** The number of Multicast packets transmitted
   - **BC(Tx):** The number of Broadcast packets transmitted

System

System Settings

Set your system information

System > System Settings

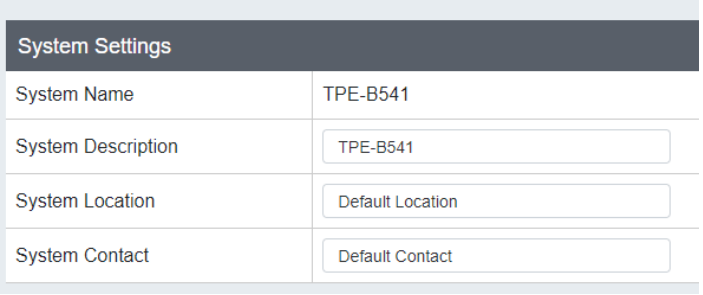
This section explains how to assign a name, location, and contact information for the switch. This information helps in identifying each specific switch among other switches in the same local area network. Entering this information is optional.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System**, and click on **System Management**.

3. Review the settings. When you have completed making changes, click **Apply** to save the settings.

- **System Name** - Specifies the Switch model. You cannot change this parameter.
- **System Description** - Specifies a name for the switch, the name is optional and may contain up to 255 characters.
- **System Location** - Specifies the location of the switch. The location is optional and may contain up to 255 characters.
- **System Contact** - Specifies the name of the network administrator responsible for managing the switch. This contact name is optional and may contain up to 255 characters.



4. Click **Apply**.

Note: *Clicking Apply will save all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

IP Settings

System > System Settings > IP Settings

This section allows you to change your switch IPv4 address settings and additionally create and assign the aforementioned address to VLANs. Typically, the IP address settings should be changed to match your existing network subnet in order to access the switch management page on your network.

Default Switch IPv4 Address: 192.168.10.200

Default Switch IPv4 Subnet Mask: 255.255.255.0

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System**, **System Settings**, and then **IP Settings**.

4. To change the IPv4 IP address associated with a specific VLAN, select the VLAN ID from the drop down menu under **VLAN**.

5. Review the settings. When you have completed making changes, click **Apply** to save the settings.

- **VLAN**: Select the VLAN ID you wish to configure. .
- **Address**: Enter the new switch IP address you would like to statically assign. (e.g. *192.168.200.200*)
- **Subnet Mask**: Enter the new switch subnet mask. (e.g. *255.255.255.0*)
- **Default Gateway**: Enter the IP address of your gateway device (ie: router)
- **DNS Servers 1 / DNS Servers 2**: Enter the IP address of a DNS server to use. (ie: 8.8.8.8 for Google's DNS server)
- **Configuration**: Select **Static** to statically assign an IP address and subnet mask, select **DHCP** to automatically request one from your networks DHCP server.

6. At the top right of the screen, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

System Time

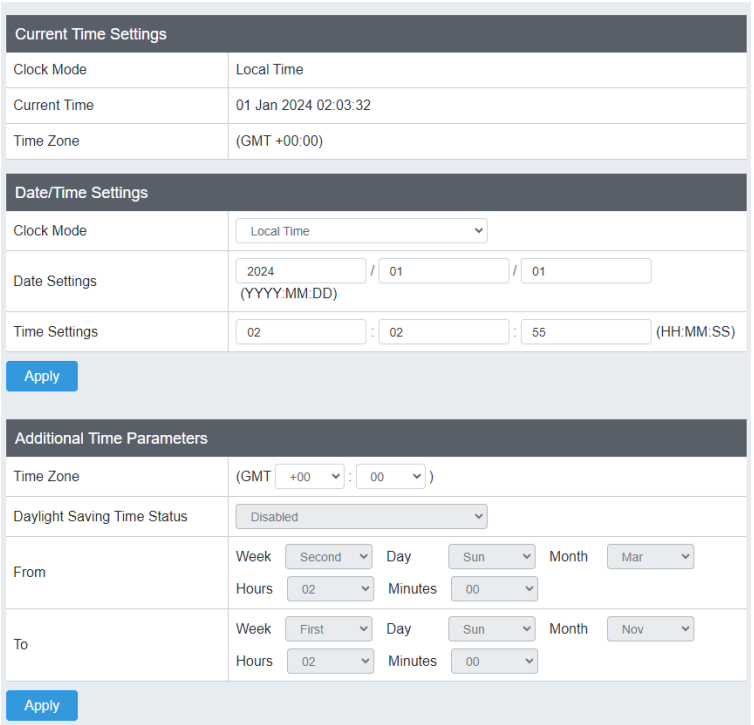
System > System Settings > System Time

This setting allows you to configure your IPv4/IPv6 DNS server settings for the purpose or resolving hostnames. For example, when specifying your SNTP server time settings via domain name, the switch will not be able to resolve the SNTP domain name specified until you configure the switch DNS server setting.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System**, then click on **System Settings,** and click on **System Time**.

3. Review the settings below and click **Apply** to save your settings.



- **Current Time:** Displays the current time that is saved on your switch
- **Date/Time Settings:** Manually input the current date and time
- **Time Zone:** Sets the current time zone you are in
- **Daylight Savings Time:** Enable to set if daylight savings is on and disable if it is not currently in daylight savings

4. At the top right of the screen, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Administration

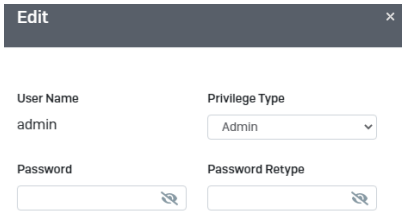
Changing login credentials

System > Administration

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network** and click on **Administration**. Click on **Modify** to open the administration settings page.

3. Review the settings below and click apply to save the changes to your flash
   - **Password:** Set the password for this new username
   - **Confirm Password:** Re-type your password.



System Logs

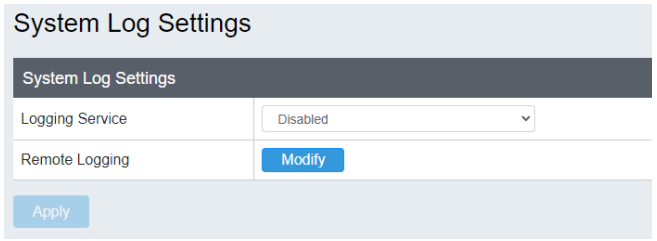
Settings

System > System Log

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System** and click on **System Log**.

3. Select **Enabled** to enable logs, or **Disabled** to disable this feature.



Remote Logging

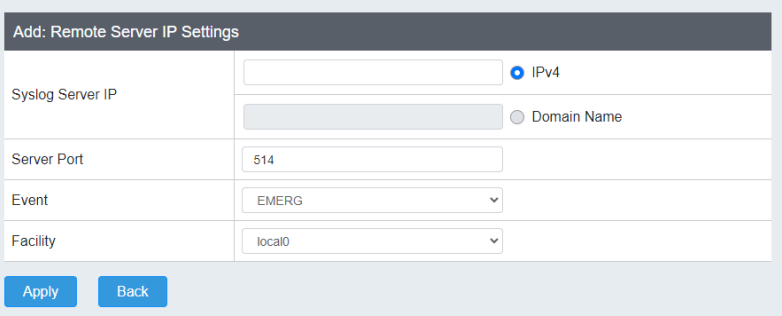
System > System Log

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System** and click on **System Log**. Click **Modify** in **Remote Logging** to enable this feature.

3. Review the settings and click **Apply** to save the changes to the Flash.

- **Syslog Server IP:** Enter the IP address of the location you want the log files to go to.
- **Server Port:** Enter the port number of the IP address
- **Event:** Select what type of log events will be sent to the IP Address
- **Facility:** Select the facility that the event will be logged as



Statistics

Statistics provide important information for troubleshooting switch problems at the port level.

View Statistics

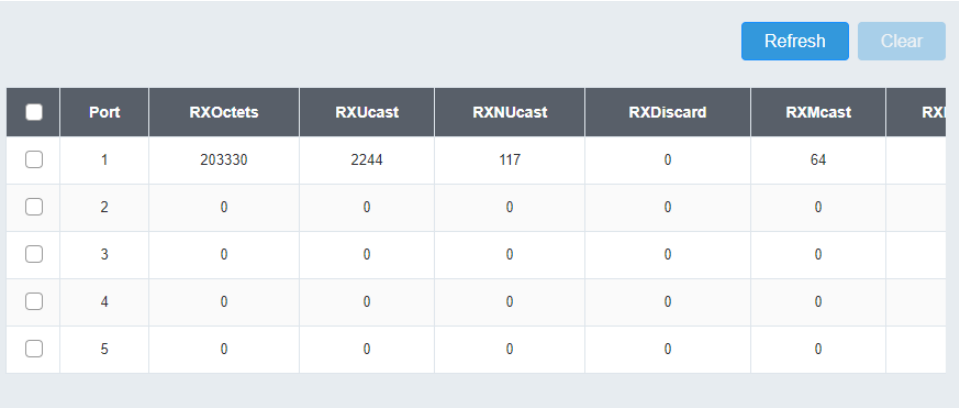
System > Statistics

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System** and click on **Statistics**

3. View the Traffic Information Statistics.

- **Port ID:** The port number where the information is being displayed.
- **RxOctets:** Receive Octets, number of received octets (8-bit chunks).
- **RxUcasts:** Receive Unicast Packets (Pkts), number of received unicast packets.
- **RxNUcasts:** Receive Non-unicast Packets (Pkts), number of received non-unicast packets (such as broadcast and multicast packets).
- **RxDiscard:** Received Discards (Pkts), number of received packets discarded.
- **RxMcast:** Receive Multicast Packets (Pkts), number of received multicast packets.
- **RxBcast:** Receive Broadcast Packets (Pkts), number of received broadcast packets.
- **RxError:** Receive errors (Pkts), number of received error packets.
- **TxOctets:** Transmit Octets, number of transmitted octets (8-bit chunks).
- **TxUcasts:** Transmit Unicast Packets (Pkts), number of transmitted unicast packets.
- **TxNUcasts:** Transmit Non-unicast Packets (Pkts), number of transmitted non-unicast packets (such as broadcast and multicast packets).
- **TxDiscard:** Transmit Discards (Pkts), number of transmitted packets discarded.
- **TxMcast:** Transmit Multicast Packets (Pkts), number of transmitted multicast packets.
- **TxBcast:** Transmit Broadcast Packets (Pkts), number of transmitted broadcast packets.
- **TxError:** Transmit errors (Pkts), number of transmitted error packets.
- **Clear:** Click the Apply button to clear port specific Traffic information.
- **Refresh:** Click the Refresh button to update table with newest traffic information.



MAC Address Table

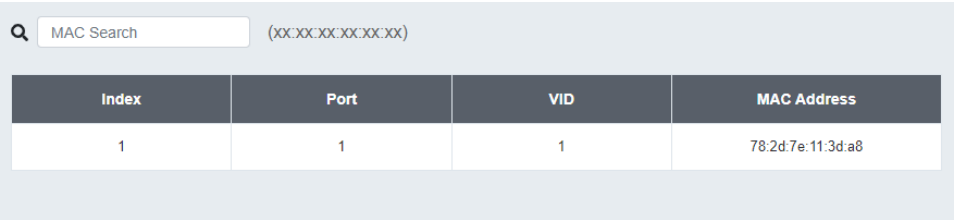
Dynamic MAC Address

System > MAC Address Table > Dynamic MAC Address

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System**, click on **MAC Address Table,** and click on **Dynamic MAC Address.**

3. The table currently displays the MAC address of devices connected to the switch.



MAC Aging Time

System > MAC Address Table > MAC Aging Time

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System**, click on **MAC Address Table,** and click on **MAC Aging Time.**

3. Enter the duration in seconds for MAC Aging Table

IEEE 802.3az EEE

Enable IEEE 802.3az Power Saving Mode

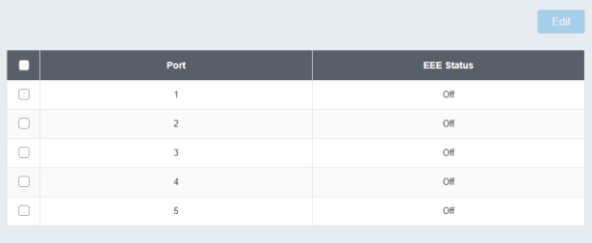
System > EEE

The IEEE 802.3 EEE standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be IEEE802.3az EEE compliance. By default, the switch disabled the IEEE 802.3az EEE function. Users can enable this feature via the IEEE802.3az EEE setting page.

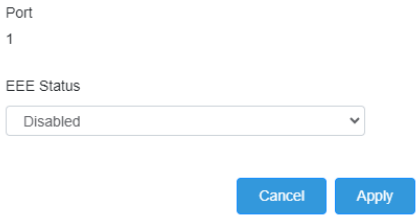
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Tools** and click on **EEE**.

3. Select the port you would like to turn on or off the IEEE 802.3az. To select all the ports, click the box on the top left. Click **Edit** to modify the options.



4. Select **Enable** or **Disabled** from the drop down menu to turn on or turn off the IEEE 802.3az settings for the selected ports.



5. Click the **Apply** button to save the settings to the flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Network

Physical Interface

Configure Physical Interfaces

Network > Physical Interface

This section allows you to configure the physical port parameters such as speed, duplex, flow control, and jumbo frames. This section also reports the current link status of each port and negotiated speed/duplex. Additionally you will be able to set your BPDU ports for Spanning Tree Configuration and EAP ports for 802.1x port-based authentication configuration.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **Physical Interface,** and click on **Port**.

3. Review the settings. Click **Apply** to save changes.

- **Port -** Specifies the port number. The All value indicates ports 1 through 10 on the Switch. You cannot change this parameter. You can use the **All** column value in the **Port** column to apply**, Mode, Flow Control,** and **Description** settings to all ports at the same time.

  - **Link Status -** This parameter indicates the status of the link between the port and the end node connected to the port. The possible values are:
  - **Link up** -This parameter indicates a valid link exists between the port and the end node.
  - **Link down** -This parameter indicates the port and the end node have not established a valid link.

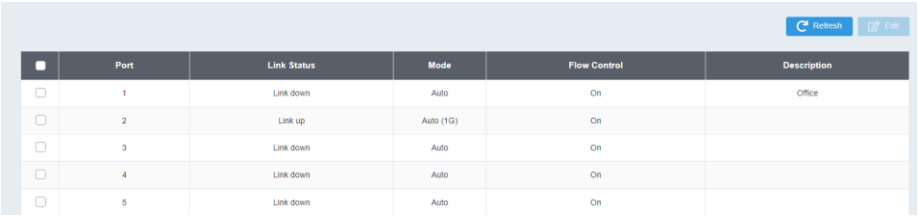
- **Mode:** This parameter indicates the speed and duplex mode settings for the port. You can use this parameter to set the speed and duplex mode of a port. The possible settings are:
  - **Auto** -This parameter indicates the port is using Auto-Negotiation to set the operating speed and duplex mode. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "1000/F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.
  - **1000/Full** -This parameter indicates the port is configured for 1000Mbps operation in full-duplex mode.
  - **100/Full** -This parameter indicates the port is configured for 100Mbps operation in full-duplex mode.
  - **10/Full** -This parameter indicates the port is configured for 10Mbps operation in full-duplex mode.

- **100/Half** -This parameter indicates the port is configured for 100Mbps operation in half-duplex mode.
- **10/Half** -This parameter indicates the port is configured for 10Mbps operation in half-duplex mode.
- **10/Half** -Disables this port.

Note: *When selecting a* ***Mode*** *setting, the following points apply:*

- *When a twisted-pair port is set to Auto-Negotiation, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch.*
- *A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.*

- **Flow Control:** This parameter reflects the current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:
  - **Enabled** - This parameter indicates that the port is permitted to use flow control.
  - **Disabled** - This parameter indicates that the port is not permitted to use flow control.
  - **Description**: This parameter offers the ability to name the device that's connected to it



Mirroring

Network > Physical Interface > Mirror

Port mirroring allows you to monitor the ingress and egress traffic on a port by having the traffic copied to another port where a computer or device can be set up to capture the data for monitoring and troubleshooting purposes.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, then click on **Physical Interface**, and click on **Mirror**.

3. Review the settings. Click **Apply** to save changes.
   - **Edit** – Click to edit the selected session ID.
   - **Session State** – Click the drop-down and list and select one of the following options:
   - **Enable** - This parameter activates the Port Mirroring feature and the rest of the configuration parameters become active on the page.
   - **Disable** - This parameter de-activates the Port Mirroring feature and the rest of the configuration parameters become inactive on the page.
   - **Destination Port** – Click the drop-down and list and select the port to send the copied ingress/egress packets/data. (*e.g. Computer or device* with *packet capture or data analysis program.)*

Check the port to monitor or copy inormation from. (Source)

To copy data received on a specific port, select the port number(s) under the **Ingress Port** section or you could click **All** to copy data received on all ports.

To copy data transmitted on specific port, select the port number under the **Egress Port** section or you could click **All** to copy data transmitted on all ports.

4. At the right hand panel, click the check mark to save your settings.

5. At the top right of the screen, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Jumbo Frames

Network > Physical Interface > Jumbo Frames

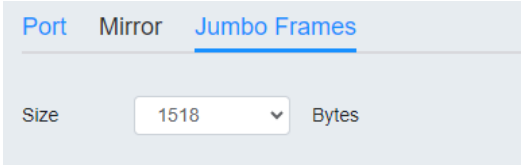
This section lets you input the size of the Jumbo Frames that can be accepted by the switch.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, then click on **Physical Interface**, and click on **Jumbo Frames**.

3. Enter the size of the Jumbo Frames to be accepted by the switch (in Bytes).

Note: *The value of the Jumbo Frames needs to be between 1518 and 9216 Bytes. By default the value is **1518** Bytes.*



4. Click **Reset** to reset the size of the Jumbo Frames to its default value. To save your new Jumbo Frame size, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

VLAN Settings

802.1Q VLAN

Network > VLAN Settings > 802.1Q

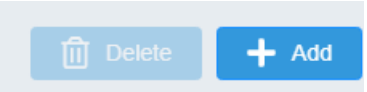
A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **VLAN Settings,** and click on **802.1Q**.

3. Click on **Add** to create a new VLAN.

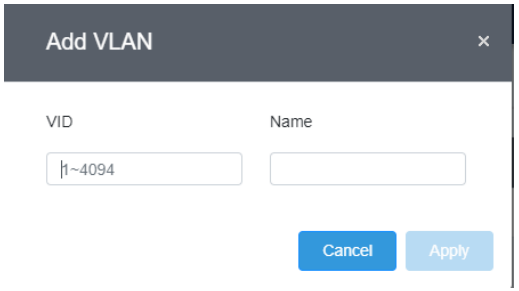


3. Review the settings.

- **VID –** Enter the VLAN ID for the new VLAN.
- **Name** – Enter the VLAN name.

Note: *By default, the default VLAN VID 1 is set as the Management VLAN.*

- **Cancel –** Deletes the current settings
- **Apply** – Apply the new settings



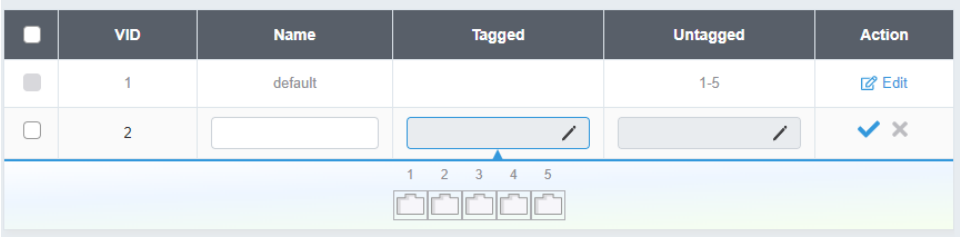
In the sections **Static Tagged, Static Untagged,** and **Not Member**, you can add the type of VLAN ports to add to the new VLAN (Tagged or Untagged) and assign ports that are not members (Forbidden) of the new VLAN.

Tagged/Untagged/Not Member VLAN Ports

On a port, the tag information within a frame is examined when it is received to determine if the frame is qualified as a member of a specific tagged VLAN. If it is, it is eligible to be switched to other member ports of the same VLAN. If it is determined that the frame's tag does not conform to the tagged VLAN, the frame is discarded.

Since these VLAN ports are VLAN aware and able to read VLAN VID tagged information on a frame and forward to the appropriate VLAN, typically tagged VLAN ports are used for uplink and downlink to other switches to carry and forward traffic for multiple VLANs across multiple switches. Tagged VLAN ports can be included as members for multiple VLANs. Computers and other edge devices are not typically connected to tagged VLAN ports unless the network interface on these device can be enabled to be VLAN aware.

Select the tagged VLAN ports to add to the new VLAN.



Untagged VLAN ports are used to connect edge devices (VLAN unaware) such as computers, laptops, and printers to a specified VLAN. It is required to modify the Port VID settings accordingly for untagged VLAN ports under Bridge > VLAN > Port Settings. (e.g. If the VID for the VLAN is 2, the PVID should also be set to 2)

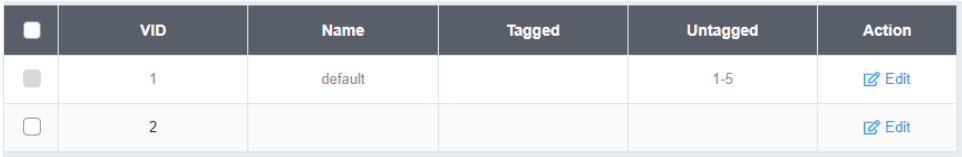
Select the untagged VLAN ports to add to the new VLAN.

Select the Forbidden ports to restrict from the new VLAN.

Click **Apply** to save the new VLAN to the table.

In the list, you can click **Edit** to modify an entry

Note: *The default VLAN VID1 cannot be removed.*



4. At the top of the right hand panel, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

PVID & Ingress Filter

Network > VLAN Settings > PVID & Ingress Filter

In this section, you can modify the port VID settings, acceptable frame types, and ingress filtering.

1. Log into your switch management page (see "Access your switch management page" on page 5).

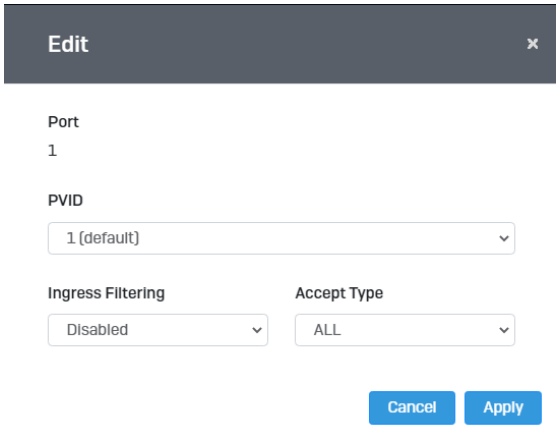
2. Click on **Network**, click on **VLAN Settings,** and click on **PVID & Ingress Filter**.

3. Select the port would like to modify and click **Edit** to modify an entry.

4. Review the settings for each port. Click **Apply** to save settings.

- **Port** – Displays the selected port
- **PVID –** Select the correct VLAN ID. ***Note:*** *Required for untagged VLAN ports.*
- **Ingress Filtering** –Click the drop-down list and select **Enabled** to enable ingress filtering or **Disabled** to disable ingress filtering.
- **Acceptable Frame Type** – Click the drop-down list and select which type of frames can be accepted.
- **All** – The port can accept all frame types.
- **Tagged** – The port can accept tagged frames only. Untagged frames are discarded.
- **Untagged**– The port can accept untagged frames and frames with tagged priority information only such as 802.1p.

Note: *Modifying settings in the row marked* ***All****, will apply the settings to all ports.*



4. At the bottom, click **Apply** to save the changes made.

Spanning Tree

Protocol

Network > Spanning Tree > Global Settings > STP

Spanning Tree Protocol (STP) provides network topology for any arrangement of bridges/switches. STP also provides a single path between end stations on a network, eliminating loops. Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

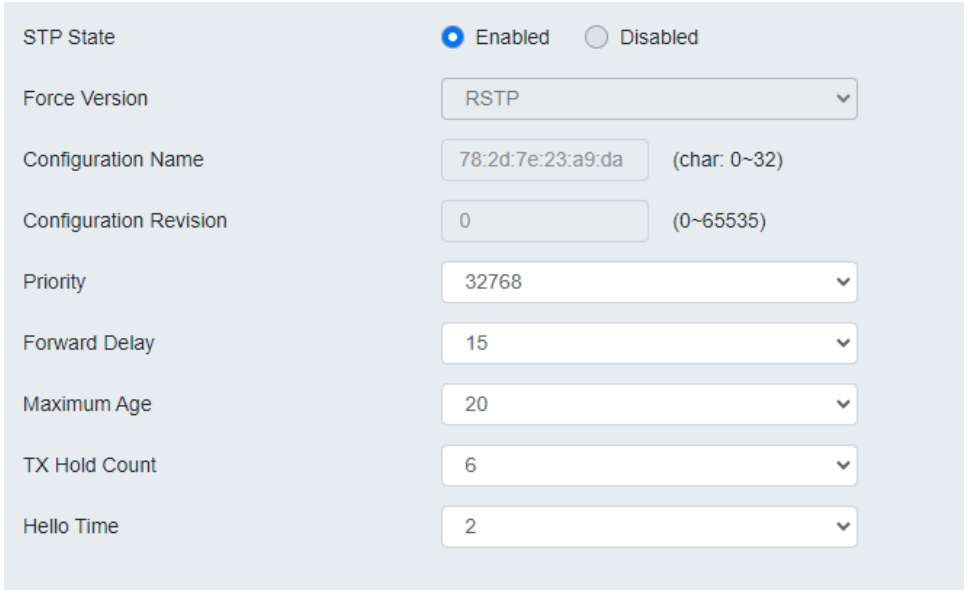
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **STP**.

3. Review the settings. Click **Apply** to save changes.

- **STP State:** Select **Enabled** to Enable Spanning Tree Protocol, or **Disabled** to disable STP.
- **Force Version:** Select **MSTP** or **RSTP** from the drop-down menu
- **Configuration Name:** Name the current STP

- **Configuration Revision:** Assign a revision number
- **Priority:** The **Priority** has a range 0 to 61440 in increments of 4096. To make this easier for you, the Web Management Utility divides the range into increments. You specify the increment that represents the desired bridge priority value.
- **Forward Delay:** The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.
- **Maximum Age:** The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds
- **TX Hold Count:** The Transmit Hold Count specifies the maximum number of BPDUs that the bridge can send per second. Its range is 1 - 10.
- **Hello Time:** The Hello Time is frequency with which the root bridge sends out a BPDU.



4. At the top right panel, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

Root Bridge Information

Network > Spanning Tree > Global Settings > Root Bridge Information

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **Root Bridge Information**.

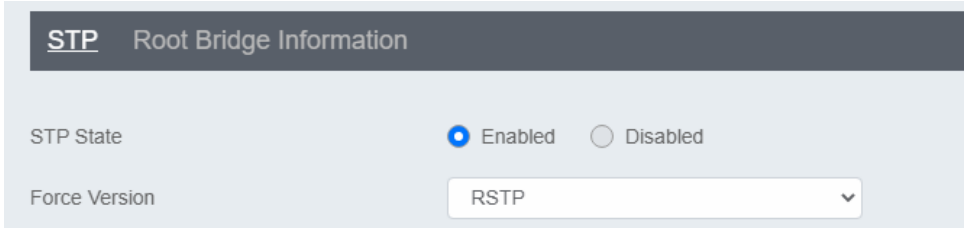
3. Displays the current settings made under STP.

RSTP Port Settings

Network > Spanning Tree > RSTP Port Settings

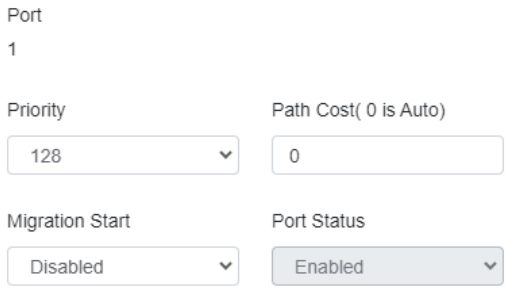
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **STP**.



3. Click on **RSTP Port Settings** and select the port(s) to configure and click **Edit**.

4. Review the settings and click **Apply** to save your changes.



- **Priority:** Indicates the port priority. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost. The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 1 lists the values that are valid.
- **Path Cost:** This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. The default port cost: 100Mbps port = 200000. Gigabit port = 20000.
- **Edge Port Conf/Oper:** Indicates if a port is connected to an edge device in the network topology or not. Select **Yes** designates the port is an edge port, and **No** to designate the port is not an edge port.
- **P2P MAC Conf/Oper:** P2P ports are similar to edge ports, however, they are restricted in that a P2P port must operate in full-duplex. **Auto** allows the port to have P2P status whenever possible and operate as if the P2P status were true. Selecting **Yes** indicates a P2P shared link is available. Selecting **No** means the port cannot maintain a P2P link.
- **Migration: Enabled** indicates the port is configured to accept RSTP and **Disabled** indicates the port is not configured to accept RSTP.
- **Status:** Select **Enabled** to enable the status to be shown or **Disabled** to disable this feature.

IGMP Snooping

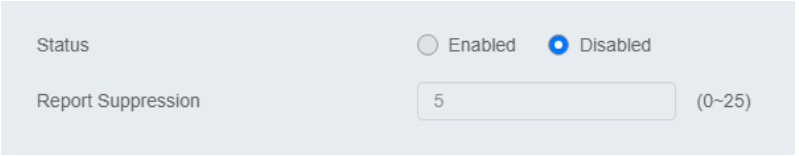
Global Settings

Network > IGMP Snooping > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **IGMP Snooping**, and click on **Global Settings**.

3. Review the settings. Click **Apply** to save the settings.
   - **Status** – Select **Enabled** to enable the IGMP snooping feature or **Disabled** to disable the feature.
   - **Report Suppression** – Enter the time suppression interval between 0 – 25.



VLAN Settings

Network > IGMP Snooping > VLAN Settings

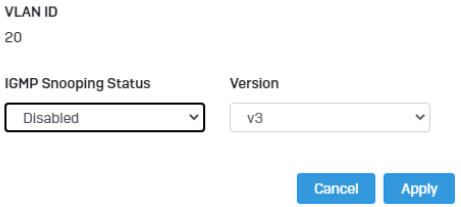
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **IGMP Snooping**, and click on **VLAN Settings**.

3. Select the VLAN ID to configure

4. Review the settings. Click **Apply** to save the settings.

- **IGMP Snooping Status –** Click the drop-down list and select **Enabled** to enable the IGMP snooping or **Disabled** to disable the feature
- **Version –** Click the drop-down list and select IGMP version



Querier Settings

Network > IGMP Snooping > Querier Settings

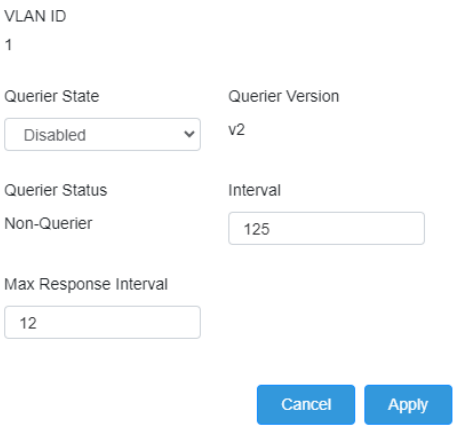
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **IGMP Snooping**, and click on **Querier Settings**.

3. Select the VLAN ID to configure

4. Review the settings. Click **Apply** to save the settings.

- **Querier State –** Click the drop-down list and select **Enabled** to enable the Querier Status or **Disabled** to disable this feature.
- **Interval** – Enter the amount of time you want your switch to send IGMP queries.
- **Max Response Interval**- Specifies the maximum time before sending a response report.
- **Startup Query Counter** – Enter the amount to start the query counter
- **Startup Query Interval** – Enter the amount of time to start the query counter



Loopback Detection

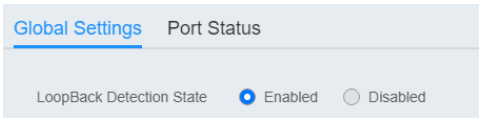
Global Settings

Network > Loopback Detection > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **Loopback Detection**, and click on **Global Settings**.

3. Select **Enabled** to enable loopback detection, or **Disabled** to disable this feature



4. At the top right panel, click the **Apply** button to save the changes to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

Voice VLAN

This chapter contains a description of the Switch's Voice VLAN feature and the procedures to create, modify, and delete a voice VLAN configuration.

The Voice VLAN feature is specifically designed to maintain high quality, uninterrupted voice traffic through the switch. When talking on a voice over IP phone, a user expects to have no interruptions in the conversation and excellent voice quality. The Voice VLAN feature can be configured to meet these requirements.

CoS with Voice VLAN

The Voice VLAN CoS parameter maintains the voice quality between the ingress and egress ports of the switch. CoS must be enabled for the Voice VLAN CoS priority to take effect. The CoS priority level that you config is applied to voice traffic on all ports of the voice VLAN. Normally, most (non-Voice) Ethernet traffic transverses the switch through lower order egress queues. To avoid delays and interruptions in the voice data flow, the CoS priority level assigned to the voice VLAN should be mapped to a higher order queue and the scheduling algorithm should be set to Strict Priority. These settings ensure that the voice data packets are processed before other types of data so that the voice quality is maintained as the voice data passes through the switch.

Organization Unique Identifier (OUI)

Each IP phone manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is imbedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of an IP phone in the first three complete bytes of its MAC address.

Typically, you will find that all of the IP phones you are installing have the same OUI in common. The switch identifies a voice data packet by comparing the OUI information in the packet's source MAC address with an OUI table that you configure when you initially set up the voice VLAN. This is important when the Auto-Detection feature for a port and is a dynamic voice VLAN port.

When you are configuring the voice VLAN parameters, you must enter the complete MAC address of at least one of your IP phones. An "OUI Mask" is automatically generated and applied by the Web Management Utility software to yield the manufacturer's OUI. If the OUI of the remaining phones from that manufacturer is the same, then no other IP phone MAC addresses need to be entered into the configuration.

However, it is possible that you can find more than one OUI from the same manufacturer among the IP phones you are installing. It is also possible that your IP phones are from two or more different manufacturers in which case you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP phones being installed, then one MAC address representing each individual OUI must be configured in the voice VLAN. You can enter a total of 10 OUIs.

Dynamic Auto-Detection vs Static Ports

Prior to configuring the voice VLAN, you must configure a tagged VLAN which is the basis for the voice VLAN configuration. The VLAN must be configured with one or more tagged or untagged ports that will serve as the voice VLAN uplink/downlink. By default, a tagged or untagged port is a static member of a tagged VLAN. The ports that you choose to configure as dynamic Auto-Detection ports

must be connected directly to an IP phone. When you initially define the ports of a tagged VLAN for your voice VLAN configuration, they must be configured as a "Not Member" ports. The "Not Member" ports are eligible to dynamically join the voice VLAN when voice data is detected with a predefined OUI in the source MAC address. The port will leave the voice VLAN after a specified timeout period. This port behavior is configured with the voice VLAN Auto-Detection feature.

For the Auto-Detection feature to function, your IP phone(s) must be capable of generating 802.1Q packets with imbedded VLAN ID tags. You must manually configure your IP phone(s) for the same VLAN ID as the switch's voice VLAN ID. When voice data is detected on one of the "Not Member" ports, the packets from the IP phone will contain the voice VLAN ID so they are switched within the switch's voice VLAN.

One or more ports in your voice VLAN must be configured as Static tagged or untagged members. Static VLAN members are permanent member ports of the voice VLAN and there is no dependency on the configuration of the devices connected to the ports. These ports might be connected to other voice VLAN network nodes such as other Ethernet switches, a telephone switch, or a DHCP server. The voice VLAN Auto-Detection feature cannot be enabled on Static tagged or tagged ports.

Note: *Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID. This insures that all untagged packets entering the port are switched within the voice VLAN as the voice data passes through the switch.*

If the IP phone(s) that you are installing cannot be configured with a VLAN ID, then the switch ports should be configured as Static tagged ports within the voice VLAN.

Note: *Link Layer Discovery Protocol for Media Endpoint Devices (LLDP- MED) is not supported on the switch. Each IP phone that is VLAN aware should be manually configured for the VLAN ID that matches your voice VLAN ID. Each of the voice VLAN ports connected to an IP phone should be configured as "Not Member" ports of the tagged VLAN.*

Global Settings

Network > Voice VLAN > Global Settings

Note: *Prior to configuring your voice VLAN, you must first configure a tagged VLAN. This VLAN will be used as a basis for your voice VLAN.*

1. Log into your switch management page (see "Access your switch management page" on page 5).

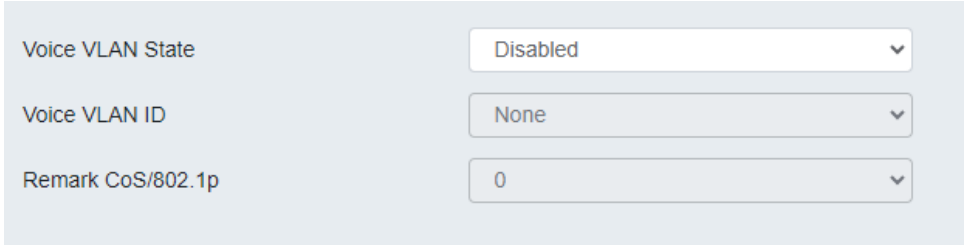
2. Click on **Network**, click on **Voice VLAN,** and click on **Global Settings**.

3. Review the settings.

Use the following procedure to configure voice VLAN:

- **Voice VLAN State –** Select **Disabled** to disable this feature, or **Auto** to allow this feature to be automatically enable and disable or set it to **OUI** to use pre-selected OUI VLANs
- **Voice VLAN ID** - This parameter is the tagged VLAN ID that has been configured in "Tagged VLAN Configuration". It is a pull-down menu showing the tagged VLAN IDs that have been defined.
- **VLAN Priority Tag** – This parameter sets the priority of the VLAN. The priority is configured through the pull-down menu.
- **Remark CoS / 802.1p** - This parameter is CoS priority level assigned to the voice data packets received on each voice VLAN port. For the **COS** priority to be effective, **802.1p Remark** must be **Enabled**.

4. Click **Apply** to save the settings.



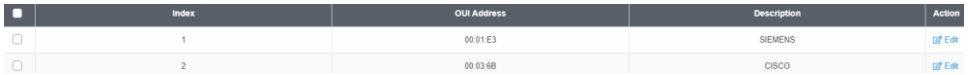
OUI Settings

Network > Voice VLAN > OUI Settings

1. Log into your switch management page (see "Access your switch management page" on page 5).

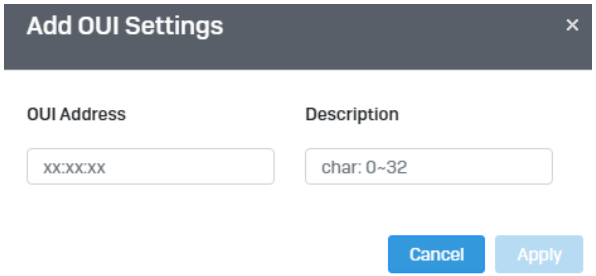
2. Click on **Network**, click on **Voice VLAN,** and click on **OUI Settings**.

3. Select from the table to use a pre-defined OUI. To modify a pre-defined OUI, click **Edit** on the far right of the table. To delete an OUI from this table, select the OUI Index and click **Delete.**



4. To add a new OUI to the table, click on **Add**.

5. Input the **OUI Address** and the name of your OUI. Click **Apply** to save it to the OUI settings table.



LLDP

Enable and configure LLDP

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network and to store data that is learned about other devices.

Settings

Network > LLDP > Global Settings

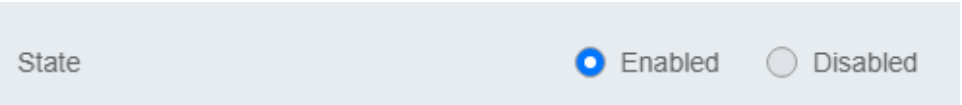
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **LLDP,** and click on **Settings**.

3. Review the settings.

Enabling or Disabling LLDP

- From the **LLDP** parameter, select one of the following radio button choices and click **Apply** to save the settings.
- **Enable:** The LLDP feature is active.
- **Disable:** The LLDP feature is inactive.



Configure the LLDP Parameter Settings

Transmission Interval: Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements. The range is from 5 to 32767 seconds.

Holdtime Multiplier: Sets the hold multiplier value. The hold time multiplier is multiplied by the transmit interval to give the Time To Live (TTL) that the switch advertises to the neighbors. The range is from 2 to 10.

Reinitialization Delay: Sets the reinitialization delay, which is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is from 1 to 10 seconds.

Transmit Delay: Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The range is from 1 to 8191 seconds.

Click **Apply** to save the settings.

View LLDP System Information

Network > LLDP > Local Device

- **Chassis ID Subtype:** This parameter describes the Chassis ID subtype which is "macAddress". You cannot change this parameter.
- **Chassis ID:** This parameter lists the MAC Address of the switch. You cannot change this parameter.
- **System Name:** This parameter lists the System Name of the switch. You can assign the system name from **System Settings.**

- **System Description:** This parameter lists the product name of the switch. You cannot change this parameter
- **Capabilities Supported:** This parameter lists the capabailities that can be supported. You cannot change this parameter.
- **Capabilities Enabled:** This parameter lists the capabilities that are enabled. You cannot change this parameter.
- **Port ID Subtype:** This parameter lists the Port ID. This parameter cannot be changed.

Entity	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Detail

< < Table is empty > >

Multicast Filtering

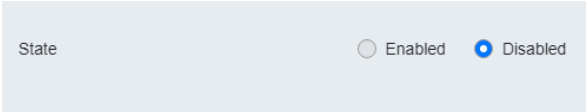
Enable Multicast Filtering

Network > Multicast Filtering

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network** and click on **Multicast Filtering**.

3. Select **Enabled** to enable this feature or **Disabled** to disable Multicast Filtering



4. At the top right panel, click the **Apply** button to save the changes to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

QoS (Quality of Service)

When a port on an Ethernet switch becomes oversubscribed, its egress queues contain more packets than the port can handle in a timely manner. In this situation, the port may be forced to delay the transmission of some packets, resulting in the delay of packets reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Minor delays are often of no consequence to a network or its performance. But there are applications, referred to as delay or time sensitive applications, which can be impacted by packet delays. Voice transmission and video conferences are two examples. If packets carrying data in either of these cases are delayed from reaching their destination, the audio or video quality may suffer.

This is where Cost of Service (CoS) is of value. It allows you to manage the flow of traffic through a switch by having the switch ports give higher priority to some packets, such as delay sensitive traffic, over other packets. This is referred to as prioritizing traffic.

Global Settings

Set QoS settings

QoS > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **QoS** and click on **Global Settings**.

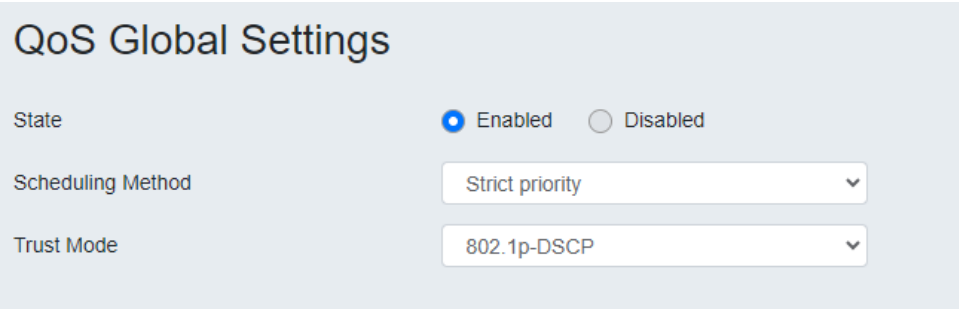
3. Select **Enabled** to enable QoS and **Disabled** to disable this feature.

4. Set the scheduling method:

- **Strict Priority** - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues.
- **WRR (Weighted RoundRobin)** - The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic.

4. Select the Trust Mode:

- **DSCP –** Priority of packets is based on the ToS (Types of Service) field in the IP header
- **802.1p –** Priority of packets is based off of the PRI value.
- **802.1p –** DSCP -



Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

DSCP Mapping

Set DSCP (Differentiated Services Code Point) Class Mapping settings

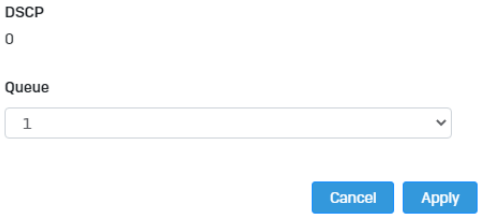
QoS > DSCP Mapping

If you choose to use the DSCP tags in your Access Control policy configuration, each DSCP value (0-63) that is relevant to your configuration needs to be mapped to one of the eight egress queues. The default queue for all DSCP values is 1. To assign the queue mappings to the DSCP values, perform the following procedure.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **QoS** and click on **DSCP Mapping**.

3. Select the relevant DSCP value to configure and click **Edit** to modify the Queue ID for the selected DSCP value. Click **Apply** to save the settings.



Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

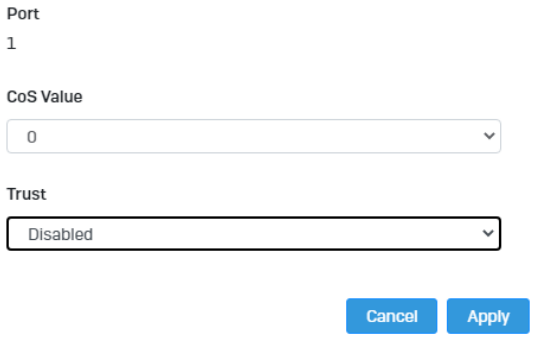
Port CoS

Set Port Priority

QoS > Port CoS

The Port Priority values are assigned to an untagged frame at ingress for internal processing in the switch. This procedure explains how to change the default mappings of port priorities to the User Priority. This is set at the switch level. You cannot set this at the per-port level. To change the port priority mappings, perform the following procedure.

1. Log into your switch management page (see "Access your switch management page" on page 5).
2. Click on **QoS** and click on **Port CoS**.
3. For each port whose priority you want to change, select a priority (0-7, Ignore) in the **CoS Value**. Click **Apply** to save the settings.



4. At the bottom of the left hand panel, click **Apply**.

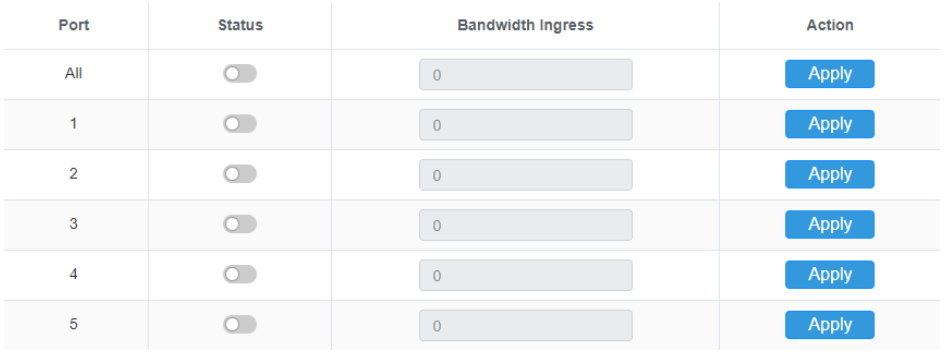
Bandwidth Control

Bandwidth Control

Network > Bandwidth Control

This section allows you to configure the DLF (Destination Lookup Failure), broadcast, and multicast storm settings for each switch port.

1. Log into your switch management page (see "Access your switch management page" on page 5).
2. Click on **QoS**, click on **Bandwidth Control**, and either **Ingress Rate Limiting** or **Egress Rate Limiting**.
3. Select the port to modify and click the **Edit** button.



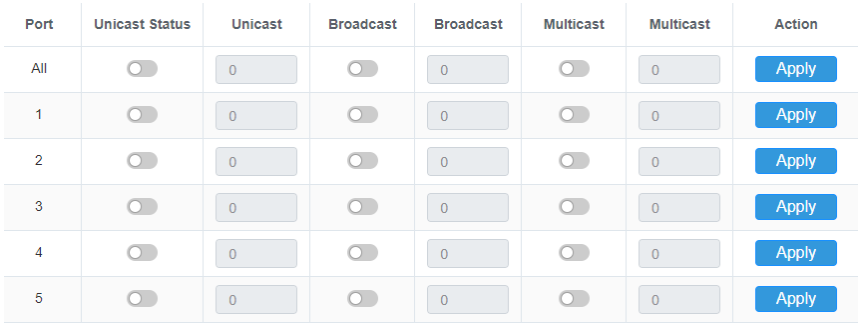
4. Review the settings below and click **Apply** to save your settings.
   - **Status –** Click to **Enable** or **Disable** this feature.
   - **Bandwidth** Ingress - Enter the ingress rate limit value.
   - **Bandwidth** Ingress **–** Enter the egress rate limit value.

Storm Control

Network > Bandwidth Control > Storm Control

1. Log into your switch management page (see "Access your switch management page" on page 5).
2. Click on **QoS**, click on **Storm Control**
3. Review the settings for each port. Click **Apply** to save the settings.
   - **Status** – Click to **Enable** or **Disable** this feature for each type of control.

- **Broadcast** – Click the empty box to enable Broadcast and enter the limit value for broadcast in kbps.
- **Multicast** – Click the empty box to enable Multicast and enter the limit value for broadcast in kbps.
- **Unicast** – Click the empty box to enable Unicast and enter the limit value for broadcast in kbps.



PoE (Power over Ethernet)

Power over Ethernet

The main advantage of PoE is that it can make installing a network easier. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE compatible devices wherever they are needed without having to worry about whether there is power source nearby.

Power Sourcing Equipment (PSE)

A device that provides PoE to other network devices is referred to as power sourcing equipment (PSE). The Gigabit Web Smart PoE+ Switch is a PSE device which provides DC power to the network cable and functions as a central power source for other network devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

PD Classes PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The Gigabit Web Smart PoE+ Switch supports all five classes.

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	34.2W	12.85W to 25.5W

Power Budget

Power budget is the maximum amount of power that the PoE switch can provide at one time to the connected PDs. Port Prioritization As long as the total power requirements of the PDs is less than the total available power of the switch, it can supply power to all of the PDs.

However, when the PD power requirements exceed the total available power, the switch denies power to some ports based on a process called port prioritization.

The ports on the PoE switch are assigned to one of three priority levels. These levels and descriptions are listed in Table 3. Without enough power to support all the ports set to the same priority level at one time, the switch provides power to the ports based on the port number, in ascending order. For example, when all of the ports in the switch are set to the low priority level and the power requirements are exceeded on the switch, port 1 has the highest priority level, port 2 has the next highest priority level and so forth.

Priority Level	Description
Critical	This is the highest priority level. Ports set to the Critical level are guaranteed to receive power before any of the ports assigned to the other priority levels.
High	Ports set to the High level receive power only when all the ports assigned to the Critical level are already receiving power.
Low	This is the lowest priority level. Ports set to the Low level receive power only when all the ports assigned to the Critical and High levels are already receiving power. This level is the default setting.

Configure PoE Budget

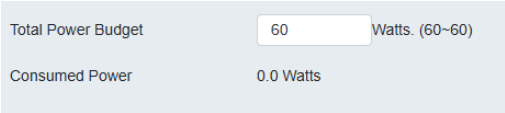
PoE > Power Budget

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **PoE** and click on **Power Budget.**

3. Enter the max PoE budget of the switch. The total consumed wattage is also shown.

Note: By default, the PoE budget is set to 240W (maximum budget).



4. Click **Apply** to save your settings to the flash.

Configure PoE Port Settings

PoE > PoE Port Settings

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **PoE** and click on **PoE Port Settings.**

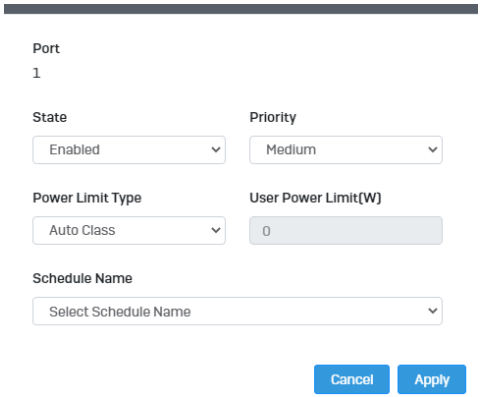
3. Review the settings for each port.

- **State** - The PoE port status is given as follows:
  - **ON** - The port is supplying PoE power.
  - **OFF** - The port is not supplying PoE power.
- **Priority** - Indicates the port priority: Low, High, or Critical.
- **Power Limit Type** – Indicates the power limit by class or power limit defined by the user.
- **User Power Limit(W) –** Set the power limit that the PD is allowed to consume
- **Status –** Displays the current PoE status
- **Class** - The PoE class is indicated the class of the PD. N/A is displayed when the port is not supplying power
- **Output Voltage(V)** - Indicates the Voltage in volts as measured at the port when the port is supplying power to the PD.
- **Output Current(mA)** - Indicates the Current in milliamps that the port is supplying to the PD.
- **Output Power(mW)** - Indicates the Power in milliwatts that the port is supplying power to the PD.

4. To modify the settings, select the port and click **Edit**. Review the settings below and click **Apply** to save your settings to the flash.

- **State –** Select **Enabled** to enable PoE on this port or **Disabled** to disable PoE from the selected port.

- **Priority –** Set the priority of this port.
- **Power Limit Type –** Select **Auto Class** for the switch to determine the amount of power need to power your PD or **User defined** to manually define the amount of power your PD device needs.
- **Schedule Name** – Select the schedule rule to follow.
  Note: *In order to set the schedule, the "Time Range" must first be configured.*



4. Click **Apply** to save your settings to the flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Security

Denial of Service

Denial of Service (DoS)

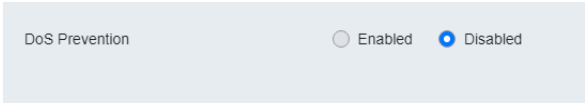
Security > DoS

The switch has built-in DoS prevention features to restrict specific type of traffic associated denial of service attacks on your network. By default, all of the DoS settings are set to Allow, which allow any type of traffic to pass through the switch. Setting one of the items to Deny will set the switch to check for traffic matching the selected item and deny any traffic matching the rule. On the other hand, setting one of rules to Deny may deny a specific type of traffic that may prevent traffic essential to running your network such as devices in load balancing configuration using virtual IP addresses (Ex. If ARP MAC SA Mismatch is set to Deny, it may cause devices in load balance configuration using shared virtual IP addresses communication issues essential for network server load balancing.) For additional security, you can set these rules to Deny as necessary.

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Security** and click on **DoS**

3. Select **Enabled** to enable DoS or **Disabled** to disable DoS.



4. Click **Apply** to save the settings to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Tools

Firmware Upgrade

Upgrade your switch's firmware

Tools > Firmware Upgrade

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet switch model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. http://www.trendnet.com/downloads/

In addition, it is also important to verify if the latest firmware version is newer than the one your switch is currently running. To identify the firmware that is currently loaded on

your switch, log in to the switch, click on the System Info section or click on Tools and click on Firmware Upgrade. The firmware used by the switch is listed as Runtime Image or Image Version. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.

2. Unzip the file to a folder on your computer.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your switch.

Firmware Upgrade via HTTP Settings

Tools > Firmware > Firmware Upgrade

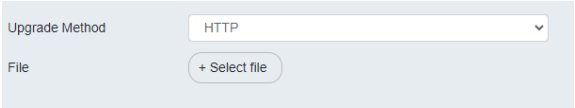
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Tools**, click on **Firmware**, and click on **Firmware Upgrade**.

3. Select the firmware **Upgrade Method** (HTTPS or TFTP).

4. Select the **Image** you would like to upgrade to.

5. Select the location of the file by clicking **Select file.**



6. Navigate to the folder on your computer where the unzipped firmware file (*.imag*) is located and select it.

5. Click **Apply**. If prompted, click **Yes** or **OK**.

Config Backup Restore

Config Backup/Restore

Tools > Firmware > Backup/Restore

You may have added many customized settings to your switch and in the case that you need to reset your switch to default, all your customized settings would be lost and would require you to manually reconfigure all of your switch settings instead of simply restoring from a backed up switch configuration file. The configuration will be backed up or restored only to the currently used image.

Backup/Restore via HTTP Settings

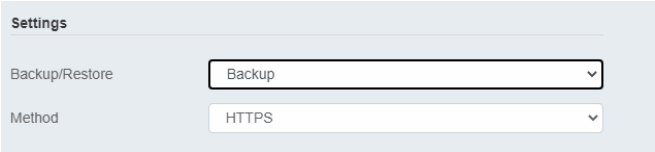
To backup your switch configuration:

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Tools**, click on **Firmware** and click on **Backup/Restore**.

3. Click **Backup** to save the configuration file (.cfg) to your local hard drive. **Startup-config** refers to the configuration that was used to startup this switch.

Note: *If prompted, choose the location on your local hard drive. If you are not prompted, the configuration file (.cfg) will be saved to your default downloads folder.*



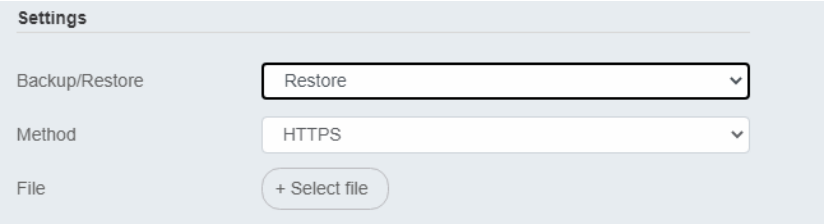
To restore your switch configuration:

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Tools**, click on **Firmware** and click on **Backup/Restore**.

3. Select **Restore** under **Backup/Restore**

Next to **Select File,** depending on your web browser, click on **Browse** or **Choose File**.



4. A separate file navigation window should open.

5. Select the switch configuration file to restore and click **Restore**. (Default File Extension: *.cfg*). Click **Apply** to restore the settings,

6. Wait for the switch to restore settings.

Reboot

Reboot/Reset to factory defaults

Tools > Reboot

This section provides the procedures for rebooting or resetting the switch to factory default settings.

To reboot your switch:

You may want to reboot your switch if you are encountering difficulties with your switch and have attempted all other troubleshooting.

Note: *You may want to save the settings to flash before reboot the switch under Save Settings to Flash (menu) > Save Settings to Flash (button). If you have not saved your current configuration settings to flash first, the configuration changes will be lost after a reboot.*

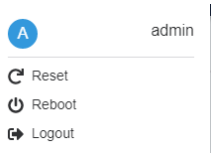
There are two methods that can be used to reboot your switch.

- **Hardware Method:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button between 1~5 seconds and release.
- **Software Method (Switch Management Page):**

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on your profile in the top right corner**.**

3. Click **Reboot** drop-down list. Wait for the switch complete the rebooting process.



To reset your switch to factory defaults:

You may want to reset your switch to factory defaults if you are encountering difficulties with your switch and have attempted all other troubleshooting. Before you reset your switch to defaults, if possible, you should backup your switch configuration first, see "Backup/Restore" on page 88.

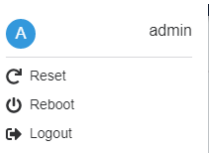
There are two methods that can be used to reset your switch to factory defaults.

- **Hardware Method:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button more than 6 seconds and release. Located on the front panel of your switch, see "Product Hardware Features" on page 2. Use this method if you are encountering difficulties with accessing your switch management page.
- **Software Method (Switch Management Page):**

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on your profile in the top right corner.

3. Click **Reset** from the drop-down list. Clicking **Reset,** will automatically reset the switch back to its factory default settings.



The switch's factory default settings are below.

Administrator User Name	admin
Administrator Password	admin
Switch IP Address	192.168.10.200
Switch Subnet Mask	255.255.255.0

Hardware Features and Specifications

Standards

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3x
- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3bt
- IEEE 802.1d
- IEEE 802.1p
- IEEE 802.1q
- IEEE 802.1w

Device Interface

- 1 x Gigabit PoE++ in port
- HTTP Web based GUI
- Backup/Restore Configuration
- Upload Firmware

Spanning Tree

- IEEE 802.1D STP (Spanning Tree protocol)
- IEEE 802.1w RSTP (Rapid Spanning Tree protocol)

Quality of Service (QoS)

- Port-based QoS
- 802.1p Class of Service (CoS)
- Bandwidth Control/Rate Limiting per port (Min. Limit: 16Kbps)
- Queue Scheduling: Strict Priority (SP), Weighted Fair Queueing (WFQ)

VLAN

- Port-based VLAN
- 802.1Q Tagged VLAN
- 4 x Gigabit PoE+ out port
- LED indicators
- Wall mount

Data Transfer Rate

- Ethernet: 10Mbps (half duplex), 20Mbps (full duplex)
- Fast Ethernet: 100Mbps (half duplex), 200Mbps (full duplex)
- Gigabit: 2Gbps (full duplex)

Performance

- Data RAM Buffer: 512KB
- Switching Fabric: 10Gbps
- MAC Address Table: 8K entries
- Jumbo Frame: 10KB
- Forwarding rate: 7.44Mpps (64-byte packet size)

Management

- Up to 32 VLAN groups, ID Range 1-4094
- VLAN port isolation
- Voice VLAN (8 user defined OUIs)

Multicast

- IGMP Snooping v1/2
- Block unknown multicast source

Port Mirror

- RX, TX, or Both
- One to one
- Many to one

Storm Control

- Broadcast (Min. Limit: 16Kbps)
- Multicast (Min. Limit: 16Kbps)
- Loopback Detection

Special Features

- PoE++ Powered
- Auto-Negotiation

Power

- IEEE 802.3bt Type 4 (90W), IEEE 802.3bt Type 3 (60W), or IEEE 802.3at (30W), PoE input only (no external power supply)
- IEEE 802.3bt Type 4 PoE PD Class 8
- IEEE 802.3bt Type 3 PoE PD Class 5
- IEEE 802.3at Type 2 PoE PD Class 4
- IEEE 802.3af Type 1 PoE PD Class 0
- Max. consumption: 7.31W (no PoE)

PoE

- 60W PoE budget with IEEE 802.3bt Type 4 (90W) input power
- 50W PoE budget with IEEE 802.3bt Type 3 (60W) input power
- 21W PoE budget with IEEE 802.3at (30W) input power

MTBF

- 503,726 hours @ 25°C

Operating Temperature

- 0° – 40° C (32° – 104° F)

Operating Humidity

- Max. 90% non-condensing

Dimensions

- 170 x 105 x 28mm (4.21 x 4.13 x 1.10 in.)

Weight

- 450g (15.9 oz.)

Certifications

- CE
- FCC
- LVD

Warranty

- Lifetime

Package Contents

- TPE-B541
- Quick Installation Guide

Quick Installation Guide Troubleshooting

Q: I typed http://192.168.10.200 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the switch management page?
Answer:
1. Check your hardware settings again. See "Switch Installation" on page 8.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Use the following IP address* or *Static IP* (see the steps below).
4. Make sure your computer is connected to one of the Ethernet switch ports.
5. Since the switch default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

Windows 7/8.1/10/11

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: If my switch IP address is different than my network's subnet, what should I do?
Answer:
You should still configure the switch first. After all the settings are applied, go to the switch configuration page, click on System, click IPv4 Setup and change the IP address of the switch to be within your network's IP subnet. Click Apply, then click OK. Then click Save Settings to Flash (menu) and click Save Settings to Flash to save the IP settings to the NV-RAM.

Q: I changed the IP address of the switch, but I forgot it. How do I reset my switch?
Answer:
Using a paper clip, push and hold the reset button on the rear of the switch and release after 6~10 seconds.
The default IP address of the switch is 192.168.10.200. The default user name and password is "admin".

Appendix

How to find your IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Command Prompt Method

Windows 7/8.1/10/11

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type ***cmd*** to bring up the command prompt.
3. In the command prompt, type ***ipconfig /all*** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type ***ipconfig getifaddr <en0 or en1>*** to display the wired or wireless IP address settings.

Note: en0 *is typically the wired Ethernet and* ***en1*** *is typically the wireless Airport interface.*

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to configure your network settings to use a static IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Windows 7/8.1/10/11

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.

b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.

c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon

b. Right-click the **Local Area Connection** icon and the click **Properties**.

c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.

b. Click the **Network** icon.

c. From the **Location** drop-down list, select **Automatic**.

d. Select and view your Ethernet connection.

In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

e. Configure TCP/IP to use a static IP.
In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Manually** and assign your network adapter a static IP address. Then click the **Apply Now** button.
In MAC 10.5/10.6, from the **Configure** drop-down list, select **Manually** and assign your network adapter a static IP address . Then click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7/8.1/10/11,

Your computer MAC addresses are also displayed in this window, however, you can type ***getmac –v*** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

How do I use the ping tool to check for network device connectivity?

Windows 7/8.1/10/11

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type ***cmd*** to bring up the command prompt.
3. In the command prompt, type ***ping <ip_address>*** with the *<ip_address>* being the IP address you want ping and check for connectivity.

Example: Usage of ping command and successful replies from device.

```
C:\Users>ping 192.168.10.100
Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type ***ping –c <#> <ip_address>*** with the *<#> ping being the number of time you want to ping and* the *<ip_address>* being the IP address you want ping and check for connectivity.

Example: *ping –c 4 192.168.10.100*

Federal Communication Commission Interference Statement

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

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

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

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 2004/108/EC and 2006/95/EC.

- **EN IEC 62368-1: 2020 + A11: 2020**
- **EN 55032: 2015 + A1: 2020**
- **EN 55035: 2017 + A11: 2020**
- **ASNZS CISPR 32: 2015+AMD1:2020**

Directives:

EMC Directive 2014/30/EC
RoHS Directive 2011/65/EU
RoHS 3 Directive 2015/863/EU
WEEE Directive 2012/19/EU
REACH Regulation (EC) No. 1907/2006
Low Voltage Directive 2014/35/EC

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use, or (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation, a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet

prepaid, insured and packaged appropriately for safe shipment. International customers shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Visit http://www.trendnet.com/gpl or the support section on http://www.trendnet.com and search for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please visit http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP07172015v3 2019/08/08

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at http://www.trendnet.com/register

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA