User's Guide

TRENDnet®

5-Port Gigabit EdgeSmart PoE+ Switch

TPE-TG50ES

Contents

Product Overview 1

Package Contents 1

Features 1

Product Hardware Features..... 2

Basic Installation 3

Connect additional devices to your switch 5

Configure your switch 6

Access your switch management page..... 6

Switch Info 6

View your switch status information 6

System 8

Set your system information 8
Set your IPv4 settings 9
Change administrator password and add accounts..... 10
Change Web idle login timeout settings..... 11
Enable or Disable SNMP 11
Set the SNMP Community Settings..... 12
Configure the SNMP Trap Management..... 13
View Statistics 14
View Traffic Information Statistics..... 14
Enable IEEE 802.3az Power Saving Mode 14

Network 15

Configure Physical Interfaces..... 15
Configure Spanning Tree (STP, RSTP)..... 16
Configure Spanning Tree Protocol port settings..... 17
Configure port trunk settings (Trunk/Link Aggregation) 18
Configure port mirror settings..... 19
Enable loopback detection 20
Add static unicast entries to the switch..... 21
Add static multicast entries to the switch 22
Configure IGMP Snooping Settings..... 23
Configure IGMP Snooping Group Settings..... 23
Configure Storm Control..... 24
Set Ingress Rate Limiting..... 24
Set Egress Rate Limiting..... 25
Add, modify, and remove VLANs..... 25
Configure VLAN Port Settings 27
Configure the VLAN forwarding Table 27
View the switch VLAN Dynamic forwarding table 28
Create a private VLAN..... 28
Create a Voice VLAN 30
Configure Voice VLAN OUI settings 30

QoS (Quality of Service)..... 32

Set CoS priority settings..... 32
Set Port Priority 32
Set DSCP (Differentiated Services Code Point) Class Mapping settings 33
Set the Scheduling Algorithm 33

PoE Configuration 35

Configure PoE settings..... 36
Configure PoE settings..... 36

Switch Maintenance 38

Upgrade your switch firmware..... 38

Firmware Upgrade via HTTP Settings 38

Backup and restore your switch configuration settings 39

Backup/Restore via HTTP Settings..... 39

Cable Diagnostics Test 39

Reboot/Reset to factory defaults 40

Using the EdgeSmart Switch Management Utility 41

System Requirements..... 41

Installation 41

Using the Utility 43

Launching the Utility..... 43
Discovery List 44

© Copyright 2018 TRENDnet. All Rights Reserved.

Monitor List 44
Device Setting 45
Main Menu Options 46

Technical Specifications.....47

Troubleshooting.....49

Appendix 50

© Copyright 2018 TRENDnet. All Rights Reserved.

Product Overview

TPE-TG50ES

Package Contents

In addition to your switch, the package includes:

- Quick Installation Guide
- Power Brick (48V DC, 0.8A)
- Power cord

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

Features

TRENDnet's 5-Port Gigabit EdgeSmart PoE+ Switch, model TPE-TG50ES, is a cost-effective desktop managed switch solution for high-speed gigabit PoE+ applications. This 5-port smart PoE+ switch features the most commonly used managed switch features, reducing unnecessary switch complexity. The web-based management interface offers features for traffic control, LACP, RSTP, VLAN, QoS, and monitoring. TRENDnet's TPE-TG50ES provides four gigabit PoE+ ports for connecting devices such as wireless access points, IP cameras, and VoIP handsets.

Ports

Four gigabit PoE+ ports and one gigabit port provide a 10Gbps switching capacity on this 5-port smart PoE+ switch

Compact Design

With a compact and lightweight metal housing design, this desktop PoE managed switch is also well-suited for wall mount installations

Network Management

The web-based management interface offers features for loopback detection, RSTP, LACP, VLAN, IGMP Snooping, and QoS

Monitoring

SNMP, SNMP Trap, and Port Mirroring support administrator monitoring solutions

Troubleshooting

Traffic statistics and a convenient cable diagnostic test

Fanless

Desktop PoE managed switch with fanless design is ideal for quiet environments that require silent operation

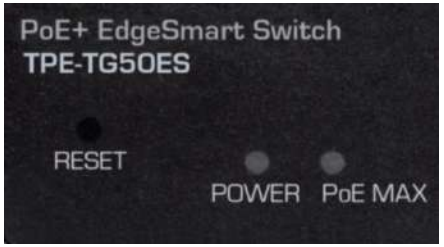
© Copyright 2018 TRENDnet. All Rights Reserved.

Product Hardware Features

Front View

Rear View

- **Reset Button –** Press and hold the button 1~5 seconds and release to reboot the device. Pressing the button more than 6 seconds will reset the switch to factory defaults. The ports LEDs will display Amber and then turn off to indicate that the reset was initiated.
- **Gigabit Ethernet PoE+ Ports (1-4) –** Connect either PoE+ or non-PoE devices.
- **Gigabit Ethernet Port (5) –** Connect a non-PoE device.



Diagnostic LEDs

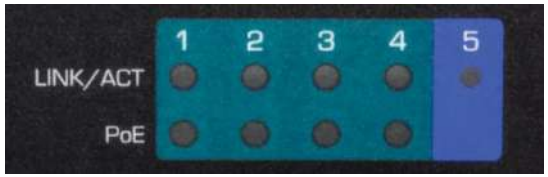
- **Power LED**

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

- **PoE MAX (Power over Ethernet Max.)**

On	When reaching near the max PoE power budget provided 64W or above, the LED will turn on and the system will not provide power additional PD (PoE client devices) after max PoE budget is reached.
Off	When the PoE power provided is below the 57W PoE power budget.

© Copyright 2018 TRENDnet. All Rights Reserved.



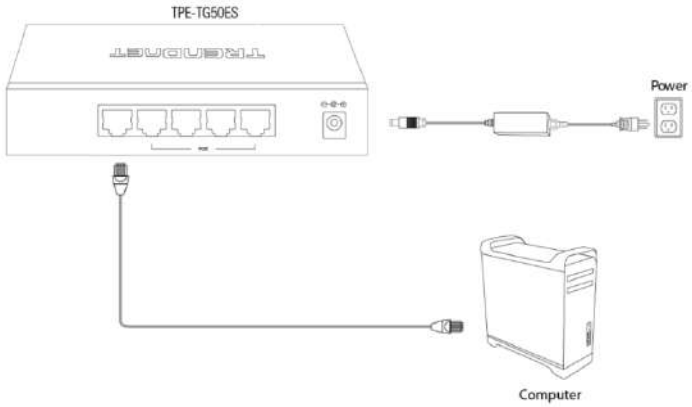
- **Link/Activity (1-5)**

Top Row LED	Green on:	When the Green LED is on, the respective port is connected to a 1Gbps Ethernet network.
	Amber on:	When the Amber LED lights on, the respective port is connected to a 10/100Mbps Ethernet network.
	Green Blinking:	When the LED is blinking green, the port is transmitting or receiving data on the network at 1Gbps speed.
	Amber Blinking:	When the LED is blinking amber, the port is transmitting or receiving data on the network at 10/100Mbps speed.
	Off	When the LED is off, the respective port is disconnected.

- **PoE (1-4)**

Bottom Row LED	Green on:	When the Green LED is on, the connected device is receiving power.
	Amber on:	When the Amber LED lights on, the connected PoE device is not receiving power. The cause is either insufficient power budget, or due to **Class/PowerLimit** restrictions in the PoE configurations.
	Off:	When the LED is off, the respective port is either not connected to a PoE device or is disconnected.

Basic Installation



3. 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.

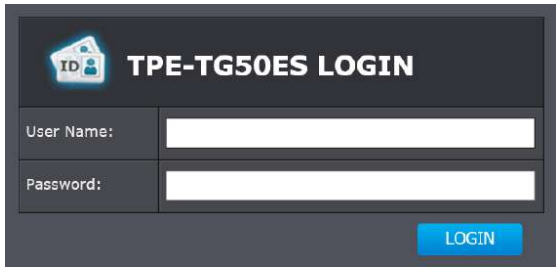
4. Open your web browser, and type the IP address of the switch in the address bar, and then press **Enter**. The default IP address is **192.168.10.200**.

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

User Name: **admin**

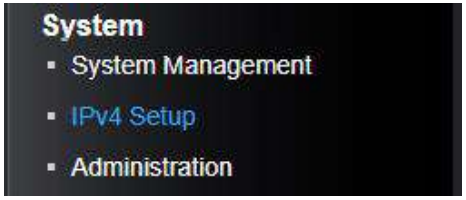
Password: **admin**

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



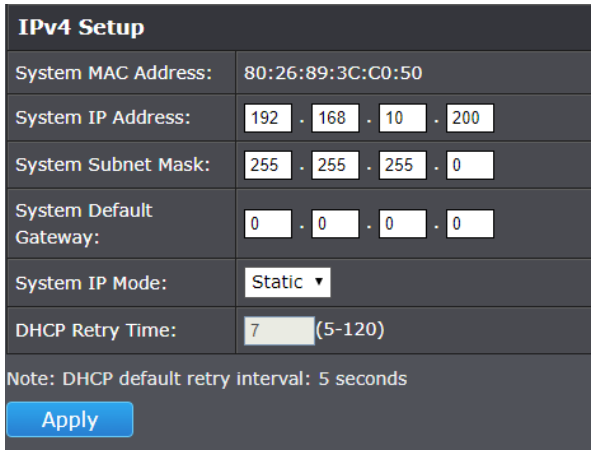
© Copyright 2018 TRENDnet. All Rights Reserved.

6. Click **System** and then click **IPv4 Setup**.



7. Configure the switch IP address settings to be within your network subnet, then click **Apply.**

Note: *You may need to modify the static IP address settings of your computer's network adapter to IP address settings within your subnet in order to regain access to the switch.*



5. In the left hand panel, click on **Save**

6. Click **Save Settings to Flash**, then click **OK.**

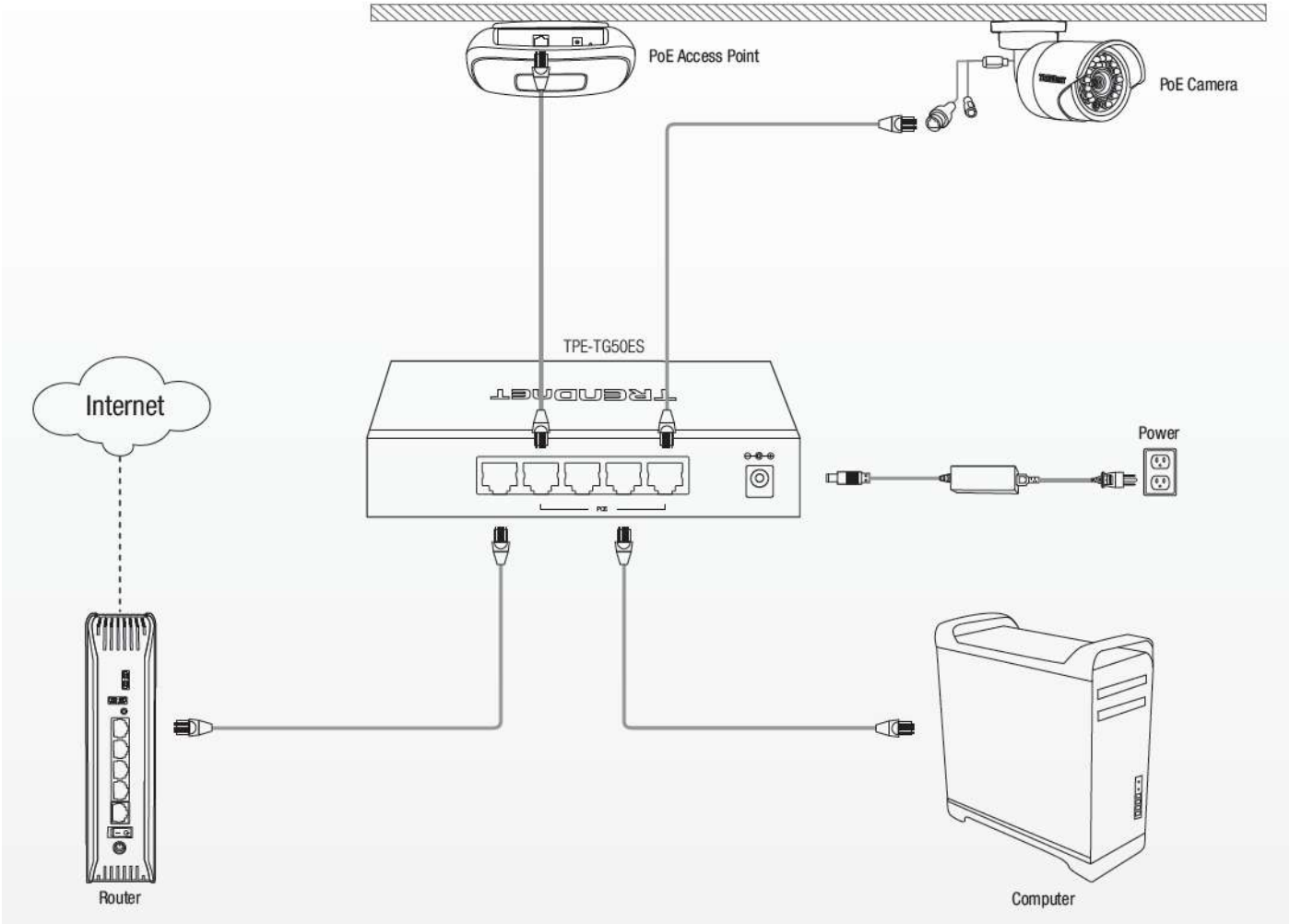
Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

© Copyright 2018 TRENDnet. All Rights Reserved.

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 PoE+ Ports (1-4) / Gigabit Ethernet Port (5). 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 the Gigabit Ethernet ports as network uplinks.

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.*



© Copyright 2018 TRENDnet. All Rights Reserved.

Configure your switch

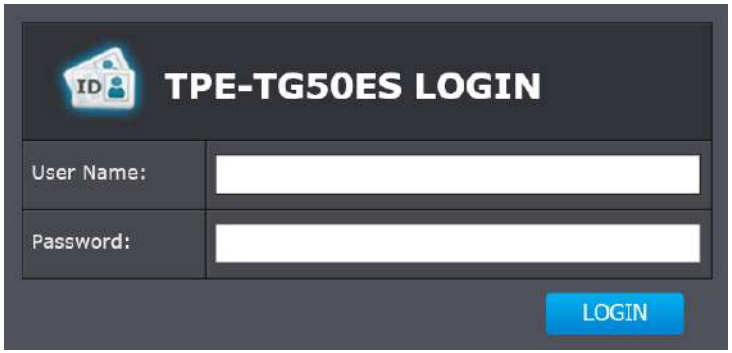
Access your switch management page

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.*

1. Open your web browser and go to the IP address 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: **admin**
   Note: *User Name and Password are case sensitive.*



Switch Info

View your switch status information

Switch Info

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 administration information, System MAC Address, IPv4 Information and Automatic Network Features information.

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **System Info**.

System Information

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

Switch Information	
System Up For:	0 day(s),5 hr(s),14 min(s),58 sec(s)
Runtime Image:	1.00.005
Boot Loader:	1.00.004

© Copyright 2018 TRENDnet. All Rights Reserved.

Administration Information

- **System Name** – 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 Name:	
System Location:	
System Contact:	

System MAC Address, IPv4 Information

- **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 MAC Address, IPv4 Information	
MAC Address:	00:01:02:03:04:05
IP Address:	192.168.10.200
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0

Automatic Network Features

- **IPv4 DHCP Client Mode:** Displays if your switch IPv4 address setting is set to DHCP client.

Automatic Network Features	
IPv4 DHCP Client Mode:	Disabled

© Copyright 2018 TRENDnet. All Rights Reserved.

System

Set your system information

System > System Management

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.

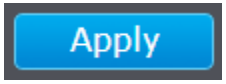
1. Log into your switch management page (see "Access your switch management page" on page 6).

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 a name for the switch, the name is optional and may contain up to 15 characters.
- **System Location** - Specifies the location of the switch. The location is optional and may contain up to 30 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 30 characters.

4. Click **Apply**.



5. In the left hand panel, click on **Save**

6. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Set your IPv4 settings

System > IPv4 Setup

This section allows you to change your switch IPv4 address settings. 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

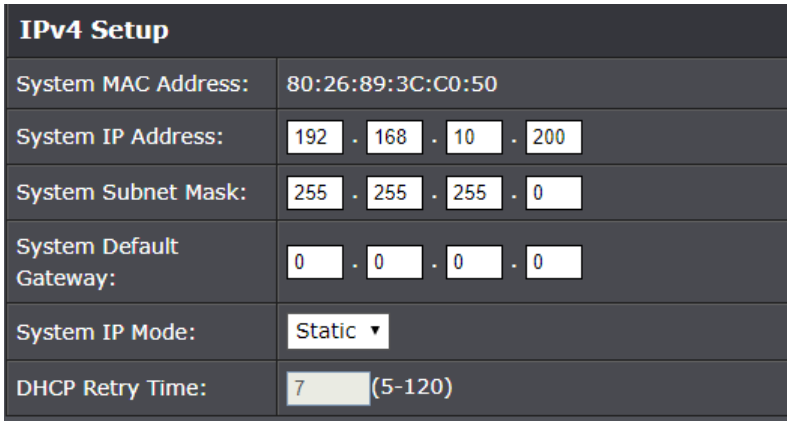
Default Switch IPv4 Subnet Mask: 255.255.255.0

1. Log into your switch management page (see "Access your switch management page" on page 6).

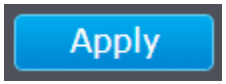
2. Click on **System**, and click on **IPv4 Setup**.

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

- **System MAC Address:** Displays the switch MAC address information.
- **System IP Address:** Enter the new switch IP address. (e.g. *192.168.200.200*)
- **System Subnet Mask:** Enter the new switch subnet mask. (e.g. *255.255.255.0*)
- **System Default Gateway:** Enter the default gateway IP address. (e.g. 192.168.200.1 or typically your router/gateway to the Internet).
- **System IP Mode:** Click the drop-down list and select **Static** to manually specify your IP address settings or **DHCP** to allow your switch to obtain IP address settings automatically from a DHCP server on your network.
- **DHCP Retry Time:** Enter the number of seconds your device will retry to connect to a DHCP server.



4. Click **Apply**.



5. In the left hand panel, click on **Save**

6. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Change administrator password and add accounts

System > Administration

This section explains how to change the administrator password create additional administrative user accounts for access to the switch management page.

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

3. Review the settings.

In the **Password** field, enter the new password and enter the new password again the **Confirm Password** field to verify. Then, click **Apply**.

Note: *The password consists of up to 12 alphanumeric characters.*

Administration Settings	
Old Password:	(Maximum length is 20)
New Password:	(Maximum length is 20)
Confirm Password:	

To create additional administrative user accounts:

- **Old Password:** Enter the old password
- **New Password:** Enter the new password you wish to change it to
- **Confirm Password:** Enter the password again to confirm the change

  Note: *The password consists of up to 12 alphanumeric characters.*

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Change Web idle login timeout settings

System > Timeout

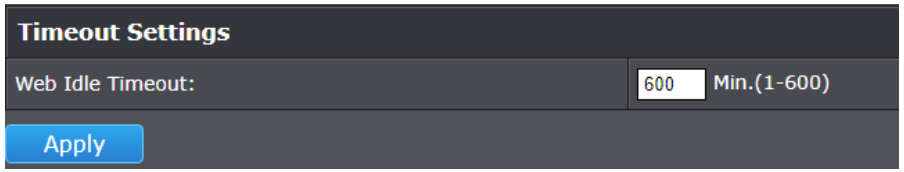
This section explains how to modify the switch management page idle timeout settings.

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

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

- **Web Idle Timeout -** Enter the idle period in minutes, when the switch will automatically log out a user from the switch management page.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK.**

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.*

Enable or Disable SNMP

System > SNMP > Global Settings

You can manage a switch by viewing and configuring the management information base (MIB) objects on the device with the Simple Network Management Program (SNMP). This chapter describes how to configure SNMP. A Group Name, IP address of the switch and at least one community string is the minimum required to manage the switch using SNMP.

Note: *If you disable the SNMP on the switch, the switch will not be manageable via SNMP using MIBs.*

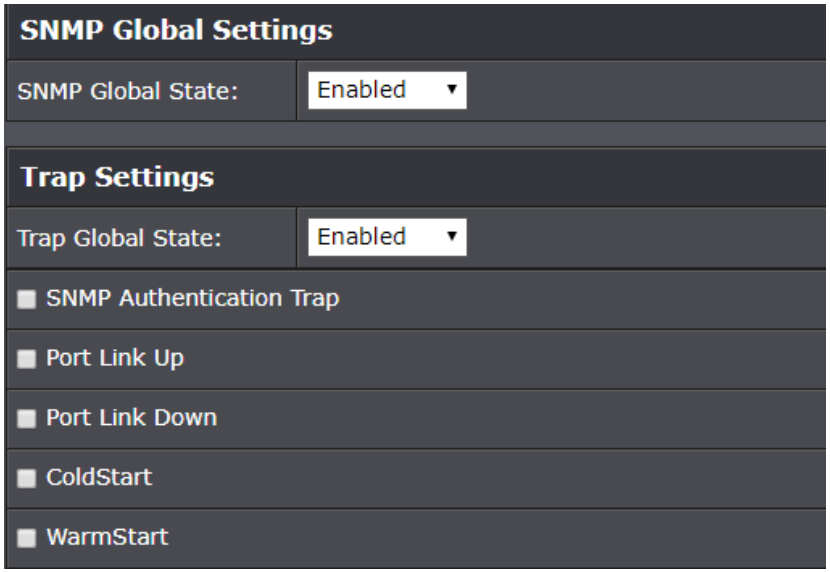
1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **System**, click on **SNMP**, and click on **Global Settings**.

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

- **SNMP Global State:** Click the drop-down list to one of the following options.
  - **Enabled** - When you enable this parameter, the SNMP agent is active. You can manage the switch with SNMP network management software and the switch's private MIB.
  - **Disabled** - When you enable this parameter, the SNMP agent is inactive.
- **SNMP Trap Global State**: Select **Enabled** from the drop down menu
  - **SNMP Authentication Trap:** Enable this to turn on SNMP trap for your network
  - **Port Link Up:** Enable this to turn on SNMP trap settings for uplink ports
  - **Port Link Down:** Enable this to turn on SNMP trap settings for downlink ports
  - **ColdStart:** Enable this to turn on SNMP ColdStart function for switch power reboot alert.
  - **WarmStart:** Enable this to turn on SNMP WarmStart function for switch software reboot.

© Copyright 2018 TRENDnet. All Rights Reserved.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK.**

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.*

Set the SNMP Community Settings

System > SNMP > Community Table Settings

The SNMP Community Table Settings screen allows network managers to define the SNMP Community Name and the access right

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **System**, click on **SNMP**, and click on **Community Table Settings.**.

3. Review the settings. Click **Apply** to save the settings.
   - **Access Right:** Assign users the level of access from the drop down menu
   - **Community Nsme:** Input the name of this SNMP community.

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Configure the SNMP Trap Management

System > SNMP > Host Settings

A Host IP address is used to specify a management device that needs to receive SNMP traps sent by the switch. This IP address is associated with the SNMP Version and a valid Community Name in the Host table of the switch.

1. Log into your switch management page (see "Access your switch management page" on page 6).

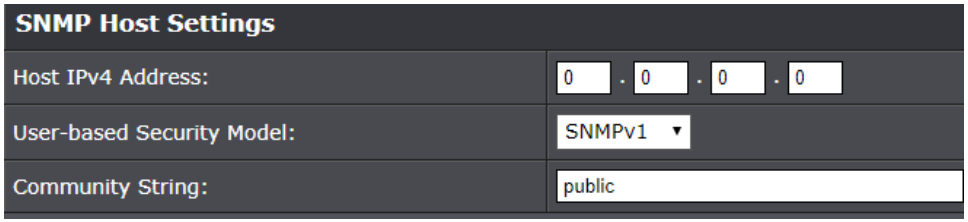
2. Click on **System**, click on **SNMP**, and click on **Host Settings**.

3. Review the settings.

Create Trap Host Table Entry

Use the following procedure to create a trap Host table entry:

- Enter the **Host IP Address** for the management device that is to receive the SNMP traps.
- Select the **SNMP Version**, either **v1** or **v2c**, that is configured for the host management device.
- Enter a **Community Name** that you have defined previously in the SNMP Community table. The **Community Name** must correlate with one of the communities displayed on the SNMP Community Table page. If you enter a **Community Name** that has not been pre-defined, the Trap Host entry is displayed, but agent/manager communication fails.



4. Click **Apply**. The new host is added to the table.

5. In the left hand panel, click on **Save**

6. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

View Statistics

System > Statistics

Statistics provide important information for troubleshooting switch problems at the port level. The statistics traffic information support normal packets and Error packets information.

View Traffic Information Statistics

System > Statistics > Traffic

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

3. View the Traffic Information Statistics.
   - **Port ID:** The port number where the information is being displayed.
   - **TxOK:** Outbound traffic (Packets/s), number of outbound bytes per second
   - **TxErr:** Outbound traffic (Packets/s), number of error outbound bytes per second
   - **RxOK:** Inbound traffic (Packets/s), number of outbound bytes per second
   - **RxErr:** Inbound traffic (Packets/s), number of error outbound bytes per second
   - **Clear:** Click the Apply button to clear port specific Traffic information.
   - **Refresh:** Click the Refresh button to update table with newest traffic information.

Traffic Information

Port ID	TxOK	TxErr	RxOK	RxErr	Clear
All	-	-	-	-	Apply
1	0	0	0	0	Apply
2	0	0	0	0	Apply
3	0	0	0	0	Apply
4	5	0	7	0	Apply
5	0	0	0	0	Apply

Enable IEEE 802.3az Power Saving Mode

System > IEEE 802.3az 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 6).

2. Click on **Tools** and click on **IEEE 802.3az EEE**.

3. Click the **IEEE 802.3az EEE Status** drop-down list and select **Enabled** to enable the power saving feature and click **Apply** to save the settings.

IEEE 802.3az EEE Settings

IEEE 802.3az EEE Status:	Disabled

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Network

Configure Physical Interfaces

Network > Physical Interface

This section allows you to configure the physical port parameters such as speed, duplex, and flow control. This section also reports the current link status of each port and negotiated speed/duplex.

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

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** row value in the **Port** column to apply **Admin Status, Mode, Jumbo, Flow Contrl, EAP, BPDU** 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:
  - **Up** -This parameter indicates a valid link exists between the port and the end node.
  - **Down** -This parameter indicates the port and the end node have not established a valid link.
- **Admin. Status:** This parameter indicates the operating status of the port. You can use this parameter to enable or disable a port. You may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. You can enable the port to resume normal operation after the problem has been fixed. You can also disable an unused port to secure it from unauthorized connections. The possible values are:
  - **Enabled** - This parameter indicates the port is able to send and receive Ethernet frames.
  - **Disabled** - This parameter indicates the port is not able to send and receive Ethernet frames.
- **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.

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 Ctrl:** 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:

© Copyright 2018 TRENDnet. All Rights Reserved.

- **Ignore** - This parameter indicates that the **All** setting does not apply to the **Flow Control** field. In other words, each port is set individually.
- **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.

Physical Interface Table

Port	Link Status	Admin. Status	Mode	Flow Ctrl	Action
All	-	Disabled	Auto	Disabled	Apply
1	Down	Enabled	Auto	Disabled	Apply
2	Down	Enabled	Auto	Disabled	Apply
3	Down	Enabled	Auto	Disabled	Apply

5. In the left hand panel, click on **Save**

6. Click **Save Settings to Flash**, then click **OK.**

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.*

Configure Spanning Tree (STP, RSTP)

Network > Spanning Tree > Protocol

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.

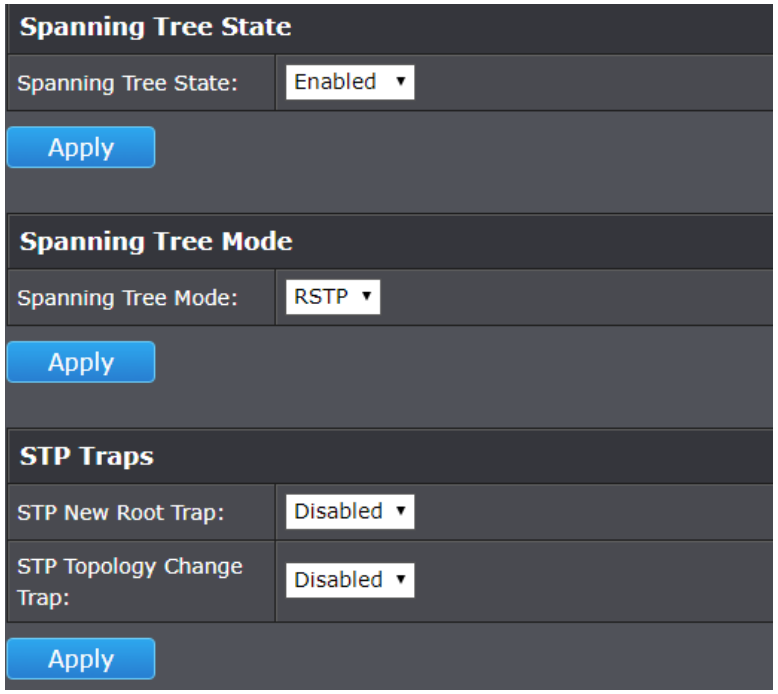
1. Log into your switch management page (see "Access your switch management page on page 6").

2. Click on **Network**, click on **Spanning Tree,** and click on **Protocol**.

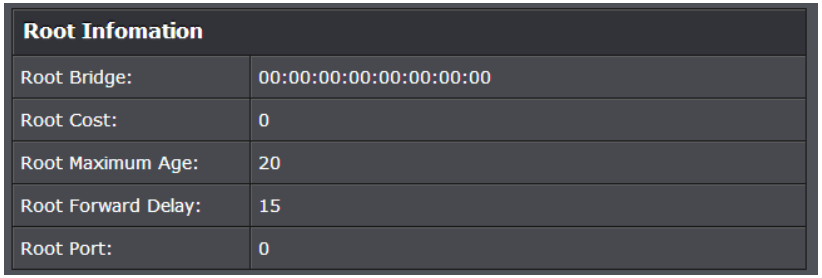
3. Review the settings. Click **Apply** to save changes.

- **Spanning Tree State:** Select the STP state on the device. The possible field values are:
  - **Disable** – Disables STP on the device. This is the default value.
  - **Enable** – Enables STP on the device.
- **Spanning Tree Mode:** Specifies the Spanning Tree Protocol (STP) mode to enable on the switch. The possible field values are:
  - **STP** – Enables STP 802.1d on the device.
  - **RSTP** – Enables Rapid STP 802.1w on the device. This is the default value.
- **STP New Root Traps:** Select the STP Root Trap on the device. The possible field values are:
  - **Disable** – Disables STP Root Trap on the device. This is the default value.
  - **Enable** – Enables STP Root Trap on the device.
- **STP Topology Change:** Select the STP Topology Change on the device. The possible field values are:
  - **Disable** – Disables STP Topology Change on the device. This is the default value.
  - **Enable** – Enables STP Topology Change on the device.

© Copyright 2018 TRENDnet. All Rights Reserved.



In addition, this section also displays the spanning tree root information.



Root Infomation	
Root Bridge:	00:00:00:00:00:00:00:00
Root Cost:	0
Root Maximum Age:	20
Root Forward Delay:	15
Root Port:	0

Configure Spanning Tree Protocol port settings

Network > Spanning Tree > RSTP Port Settings

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **Spanning Tree**, and click on **RSTP Port Settings**.

3. Review the settings. For each entry, click **Apply** to save changes.
   - **Port:** Indicates the port number (1-8)
   - **Port Fast:** Select the spanning tree protocol for each port
     - **Network:** Automatically lets the device determine the type of device that is connected to the port
     - **Disable:** Disable port fast on a particular port.
     - **Edge:** Indicates that this port is connected to an Edge device.

Port Settings			
Port	Port Fast	State	Action
All	Network	-	Apply
1	Disabled	Link down	Apply
2	Edge	Link down	Apply

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK.**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Configure port trunk settings (Trunk/Link Aggregation)

Network > Trunk

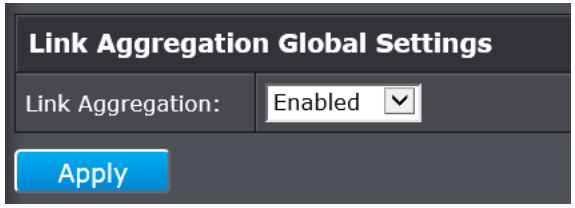
The trunking function enables the cascading of two or more ports for a combined larger total bandwidth. Only 1 trunk group may be created, each supporting up to 4 ports. Add a trunking Name and select the ports to be trunked together, and click Apply to activate the selected trunking groups.

Important Note: *Do not connect the cables of a port trunk to the ports on the switch until you have configured the ports on both the switch and the end nodes. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.*

1. Log into your switch management page (see "Access your switch management page" on page 6).

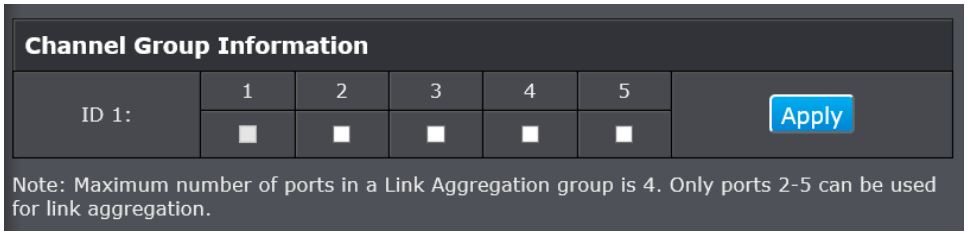
2. Click on **Network**, and click on **Trunk**.

3. Select **Enabled** from the drop down menu under **Link Aggregation Global Settings.**



3. Review the settings. For each trunk group, click **Apply** to save changes.

For each Trunk ID/Group, select the number of ports to add to each Trunk ID and click **Apply**.



5. In the left hand panel, click on **Save**

6. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Configure port mirror settings

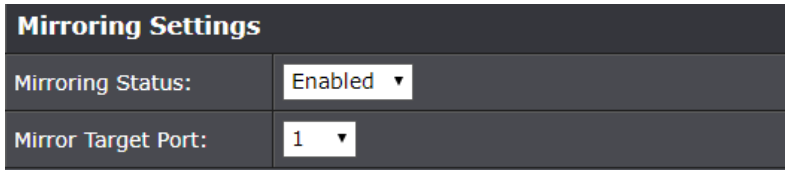
Network > Mirroring

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 6).

2. Click on **Network**, and click on **Mirroring**.

3. Review the settings. Click **Apply** to save changes.
   - **Mirroring Status** – 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.
   - **Mirror Target 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.)*



   - **Frame Type:** Click the drop-down menu and select one of the following options
     - **Ingress:** This parameter allows configuration of the inbound traffic to the selected port.
     - **Egress:** This parameter allows configuration of the outbound traffic to the selected port.
     - **Ingress/Egress:** This parameter allows configuration of the inbound and outbound traffic to the selected port.

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

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

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Enable loopback detection

Network > Loopback Detection

The loopback detection feature allows the switch to detect and prevent disruption from loops that occur on uplink or downlink switches directly connected to your switch.

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network** and click on **Loopback Detection**.

3. Review the settings.

- **State** – Select **Enabled** to enable the loopback detection feature. Select **Disabled** to disabled the loopback detection feature.
- **Interval –** Defines the interval your switch will check for loops.
- **Recover Time –** Defines the time period when connectivity will be restored to a port where a loop was previously detected and blocked.

Click **Apply** to save changes.

Loopback Detection Settings		
Loopback Detection Status:	Enabled	
Loopback Detection Time Settings		
Interval:	2	sec(1-32767)
Recover Time:	60	sec(0 or 60-1000000, 0 is Disabled)

In the Loopback Detection table, select one of the **Loopback Detection Status** choices from the pull down menu:

- **Enabled:** This selection enables the Loopback Detection feature for each port. This state must be enabled along with the **Status** field at the top of the page before this feature can be active on the selected port.
- **Disabled:** This selection disables the Loopback Detection feature on the selected port.
- ***Note:*** *In the **All** row when you select **Enable** or **Disable**, the selection applies to all of the Switch ports.*

Next to each entry modified, under the **Action** column, click **Apply** to save the changes.

Loopback Detection Table			
Port	Loopback Detection Status	Loop Status	Action
All	Ignore	-	Apply
1	Disabled	Normal	Apply
2	Disabled	Normal	Apply
3	Disabled	Normal	Apply

4. In the left hand panel, click on **Save**

Save

5. Click **Save Settings to Flash**, then click **OK**

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.*

Save Settings to Flash

© Copyright 2018 TRENDnet. All Rights Reserved.

Add static unicast entries to the switch

Network > Static Unicast

In this section, you can add static unicast entries to the switch configuration.

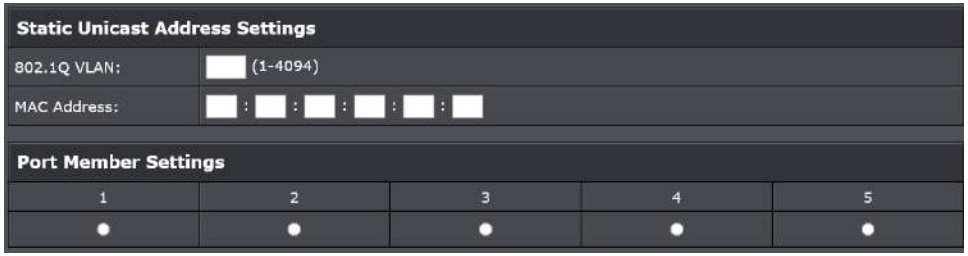
1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network** and click on **Static Unicast**.

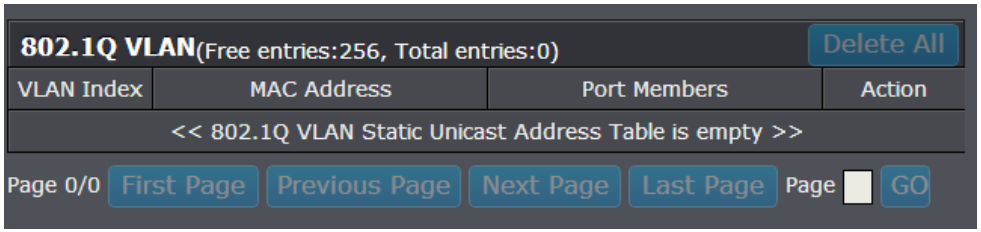
3. Review the settings.

- **802.1Q VLAN** – Enter the VLAN ID where the MAC address will reside.
  Note: *By default, all switch ports are part of the default VLAN, VLAN ID 1.*
- **MAC Address** – Enter the MAC address of the device to add.
- **Port Member –** Select the port where the MAC address will reside.

Click **Apply** to add the Static Unicast entry to the list.



In the list, you can click **Modify** to modify an entry or click **Delete** or delete the entry**.** You can also click **Delete All** to delete all the entries in the list. If the entries span multiple pages, you can navigate page number in the **Page** field and click **Go** or you can click **First, Previous, Next,** and **Last Page** to navigate the pages.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Add static multicast entries to the switch

Network > Static Multicast

In this section, you can add static multicast entries to the switch configuration.

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

3. Review the settings.

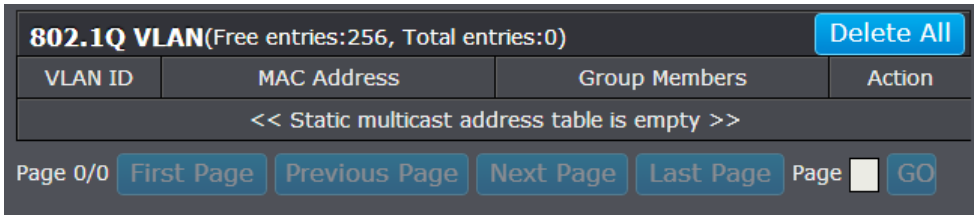
- **802.1Q VLAN** – Enter the VLAN ID where the multicast group MAC address will reside.

  Note: *By default, all switch ports are part of the default VLAN, VLAN ID 1.*
- **MAC Address** – Enter the multicast group MAC address.
- **Group Member –** Check the port(s) where the MAC address will reside.

  Note: *You can click **All** to select all ports.*

Click **Apply** to add the Static Multicast Group entry to the list.

In the list, you can click **Modify** to modify an entry or click **Delete** or delete the entry**.** If the entries span multiple pages, you can navigate page number in the **Page** field and click **Go** or you can click **First, Previous, Next,** and **Last Page** to navigate the pages.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

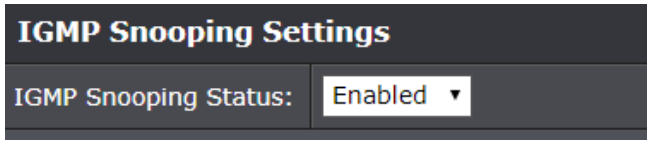
Configure IGMP Snooping Settings

Network > IGMP Snooping > Settings

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

3. To enable IGMP Snooping, select **Enable** from the drop down menu under **IGMP Snooping Status** and click **Apply.**



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

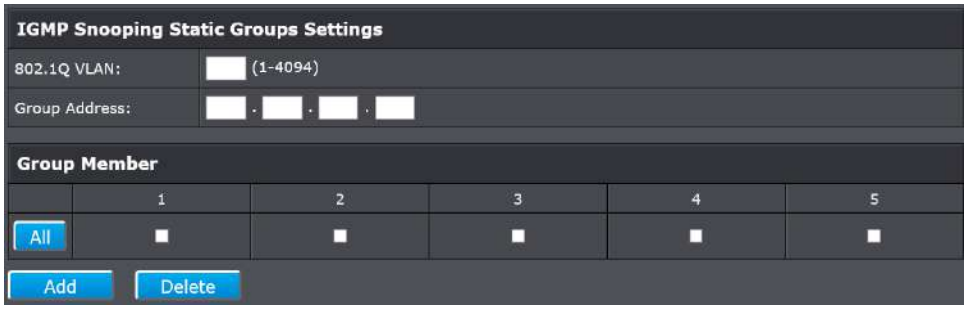
Configure IGMP Snooping Group Settings

Network > IGMP Snooping > Group Settings

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

3. Review the settings and click **Add** to save the settings.
   - **802.1Q VLAN:** Input the 802.1Q VLAN ID
   - **Group Address:** Input the Group Address for the VLAN ID
   - **Group Member:** Select the ports to be included in this group and click **Add.**. For all ports, click **All** and click **Add** to all ports the ports to this VLAN ID



In addition, the table shows the IGMP group entries. To delete a specific entry, click the **Delete** button to delete the specified Group ID.

© Copyright 2018 TRENDnet. All Rights Reserved.

Configure Storm Control

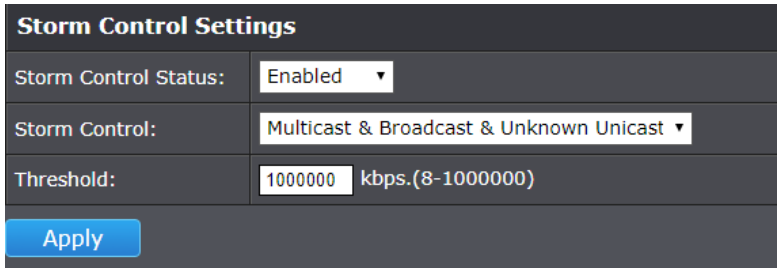
Network > Bandwidth Control > Storm Control

This section allows you to configure the storm control threshold.

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **Bandwidth Control,** and click on **Storm Control**.

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Storm Control Status** – Click the drop-down list and select **Enabled** to enable Storm Control.
   - **Storm Control** – Select from the type of Unicast traffic to allow: **Multicast & Broadcast & Unknown Unicast, Multicast & Broadcast,** and **Broadcast** only.
   - **Threshold** – Enter the kbit/s (kilobits per second) threshold.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

Set Ingress Rate Limiting

Network > Bandwidth Control > Ingress Rate Limiting

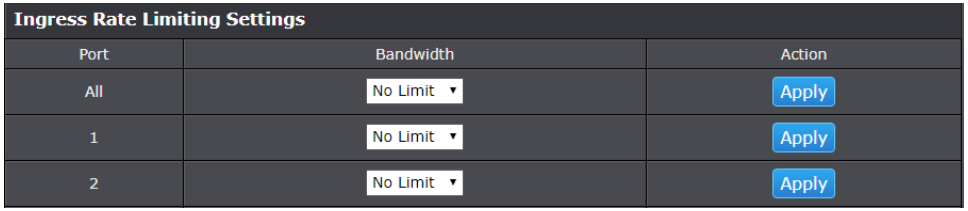
This section allows you to set the ingress (receive) rate for each switch port.

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **Bandwidth Control,** and click on **Ingress Rate Limiting**.

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Bandwidth** – Select the ingress rate limit value from the drop down menu.

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



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Set Egress Rate Limiting

Network > Bandwidth Control > Egress Rate Limiting

This section allows you to set the egress (transmit) rate for each switch port.

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **Bandwidth Control,** and click on **Egress Rate Limiting**.

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Bandwidth** – Select the egress rate limit value from the drop down menu.

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

Egress Rate Limiting Settings

Port	Bandwidth	Action
All	No Limit	Apply
1	No Limit	Apply
2	No Limit	Apply

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

Add, modify, and remove VLANs

Network > VLAN > Tagged VLAN

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 6).

2. Click on **Network**, click on **VLAN,** and click on **Tagged VLAN**.

3. Review the settings.
   - **VLAN ID –** Enter the VLAN ID for the new VLAN.
   - **VLAN Name** – Enter the VLAN name.

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

Tagged VLAN Settings

VLAN ID:	(2-4094)
VLAN Name:	(Name should be less than 10 characters)

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.

© Copyright 2018 TRENDnet. All Rights Reserved.

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)

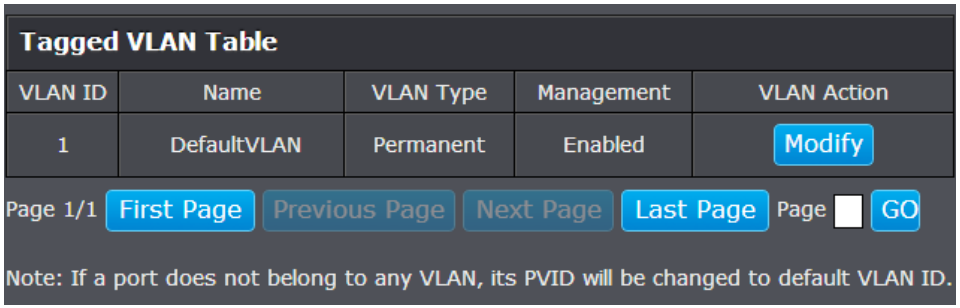
Select the untagged VLAN ports to add to the new VLAN.

Select the not member ports to restrict from the new VLAN.

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

In the list, you can click **Modify** to modify an entry or click **Delete** or delete the entry**.** If the entries span multiple pages, you can navigate page number in the **Page** field and click **Go** or you can click **First, Previous, Next,** and **Last Page** to navigate the pages.

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



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Configure VLAN Port Settings

Network > VLAN > Port

In this section, you can modify the port VID settings, acceptable frame types, and ingress filtering. In order to modify these settings, you must first add VLANs before set up (see "Add, modify, and remove VLANs" on page 32).

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **VLAN,** and click on **Port**.

3. Review the settings for each port. Click **Apply** to save settings.
   - **PVID –** Enter the port VLAN ID. ***Note:*** *Required for untagged VLAN ports.*

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

Configure the VLAN forwarding Table

Network > VLAN > Forwarding

This section allows you to configure your switch to standard 802.1Q VLAN mode (IVL) or Asymmetric VLAN mode (SVL). Asymmetric VLAN allows the configuration of overlapping untagged VLAN ports in order to create VLAN groups. It is recommended to use the standard 802.1Q VLAN mode when possible.

IVL – Independent VLAN Learning

SVL – Shared VLAN Learning (also known as asymmetric VLAN)

Please note the following when switching between forwarding table modes:

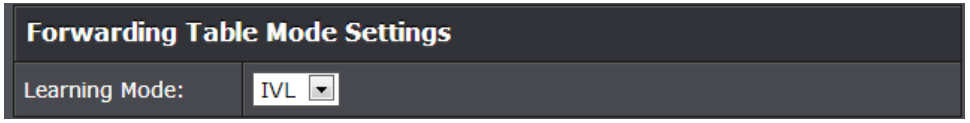
- FDB (Forwarding Database) will be cleared.
- Static Unicast Address entries will be cleared.
- Static Multicast Address entries will be cleared.
- 802.1X authenticated records will be cleared.
- IGMP Snooping multicast group addresses will be cleared
- When using SVL mode, Voice VLAN will not be supported.
- When using SVL mode, the VID field on 802.1Q-VLAN mode will be displayed as "N/A".

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **VLAN,** and click on **Forwarding**.

3. Click the learning mode drop-down list to select the forwarding table mode and click **Apply** to save settings.

Note*: The default mode is IVL.*



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

View the switch VLAN Dynamic forwarding table

Network > VLAN > Forwarding Table

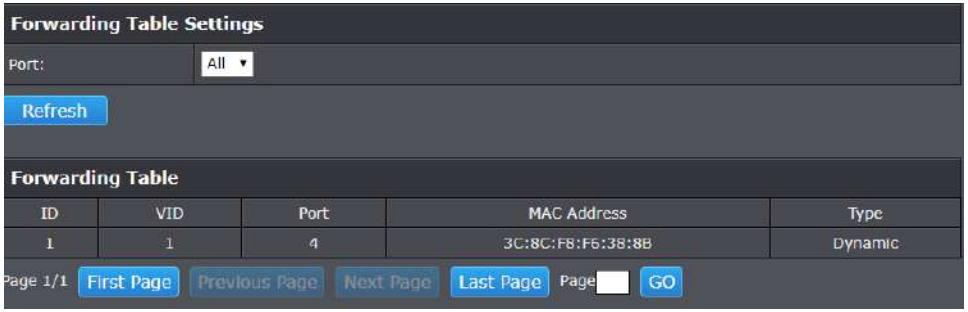
This section allows you to view the VLAN forwarding table with dynamically generated forwarding table entries as devices more devices are connected to your switch.

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **VLAN,** and click on **Forwarding Table**.

3. By default, forwarding entries for all ports are listed. You can click the **Port** drop-down list to select a specific port to view only the forwarding entries for the selected port.

If the entries span multiple pages, you can navigate page number in the **Page** field and click **Go** or you can click **First, Previous, Next,** and **Last Page** to navigate the pages.



Create a private VLAN

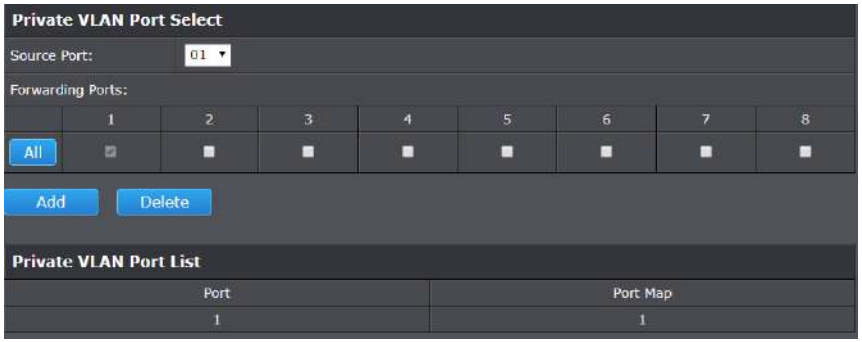
Network > VLAN > Private

The private VLAN feature allows you to create a more secure VLAN that is completely isolated to its members and cannot communicate with other VLANs

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **Network**, click on **VLAN,** and click on **Private**.

3. To configure Private VLAN Settings, perform the following procedure:
   - Select the **Source Port** to one of the following choices from the pull-down menu: All, 01 – 08
   - Click on the **Forwarding Ports** ratio button that applies to your configuration.
   - Click **Add.**



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Configuring Voice VLANs

Network > 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 13 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.

© Copyright 2018 TRENDnet. All Rights Reserved.

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.*

Create a Voice VLAN

Network > Voice VLAN > 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 6).

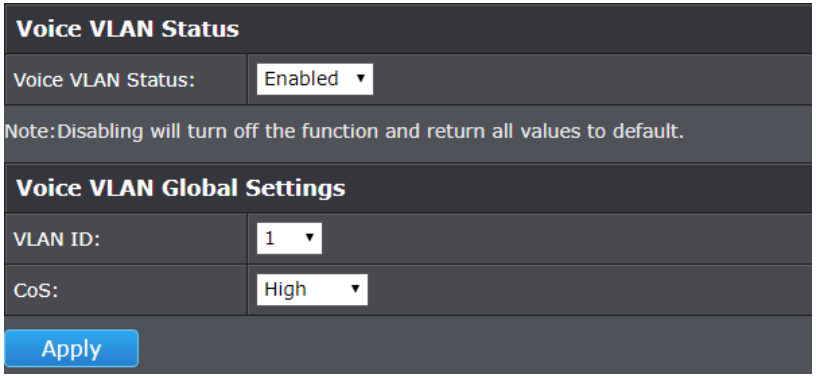
2. Click on **Network**, click on **Voice VLAN,** and click on **Settings**.

3. Review the settings.

Use the following procedure to configure voice VLAN:

- From the **Voice VLAN** field at the top of the page, select one of the following radio button choices:
  - **Enable -** The voice VLAN feature is active. The other parameter fields in the voice VLAN Global Settings section become active and are eligible for data to be entered.
  - **Disable** - The voice VLAN feature is inactive. The other parameter fields in the voice VLAN Global Settings section become inactive and are greyed out so that data cannot be entered.
- In the Voice VLAN Global Settings section, enter the configuration information for the following parameters:
  - **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.
  - **CoS** - 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, QoS must be **Enabled**.

Click **Apply** to save the settings.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

Configure Voice VLAN OUI settings

Network Voice VLAN > OUI

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

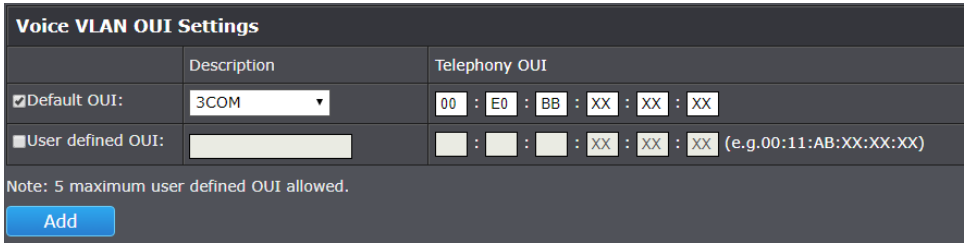
3. Review the settings.

© Copyright 2018 TRENDnet. All Rights Reserved.

Use the following procedure to configure voice VLAN OUIs:

- **Default OUI:** Select from the drop down menu for a list of pre-defined Telephony OUIs.
- **User defined OUI:** Enter a text description that helps you identify the manufacturer's OUI in the **User Defined OUI - Description** field. This parameter can be up to 20 characters in length. Enter the MAC address in the **User Defined OUI - Telephony OUI** field of one of the IP phones with the manufacturer's OUI.
- Click **Add**. The new OUI entry is displayed in the table at the bottom of the page.

  Note: *If you find more than one OUI among the IP phones you are installing, enter one MAC address that represents each individual OUI. You can enter a total of 10 OUIs.*

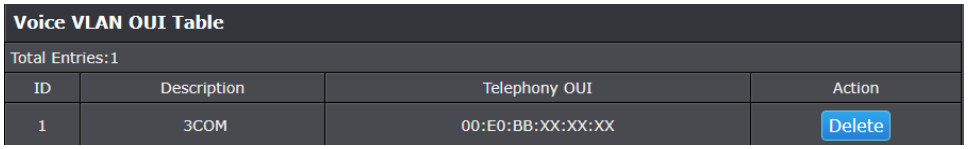


Modify OUI Setting

To modify or delete an OUI, it must be first be deleted and then re-created.

Delete OUI Setting

To delete a specific OUI that had already been entered in the table at the bottom of the page, click on **Delete** in the **Action** column of the table. The specific OUI will be deleted from the table.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

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.

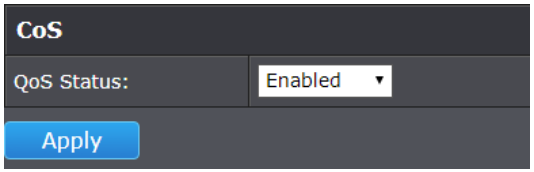
Set CoS priority settings

QoS > CoS

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **QoS** and click on **CoS**.

3. In **QoS Status**, select **Enabled** and then click **Apply**.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

Set Port Priority

QoS > Port Priority

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 6).

2. Click on **QoS** and click on **Port Priority**.

3. For each port whose priority you want to change, select a priority (Low-Highest) in the **User Priority** column. Click **Apply** to save the settings.

4. In the left hand panel, click on **Save**

© Copyright 2018 TRENDnet. All Rights Reserved.

5. Click **Save Settings to Flash**, then click **OK**

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.*

Set DSCP (Differentiated Services Code Point) Class Mapping settings

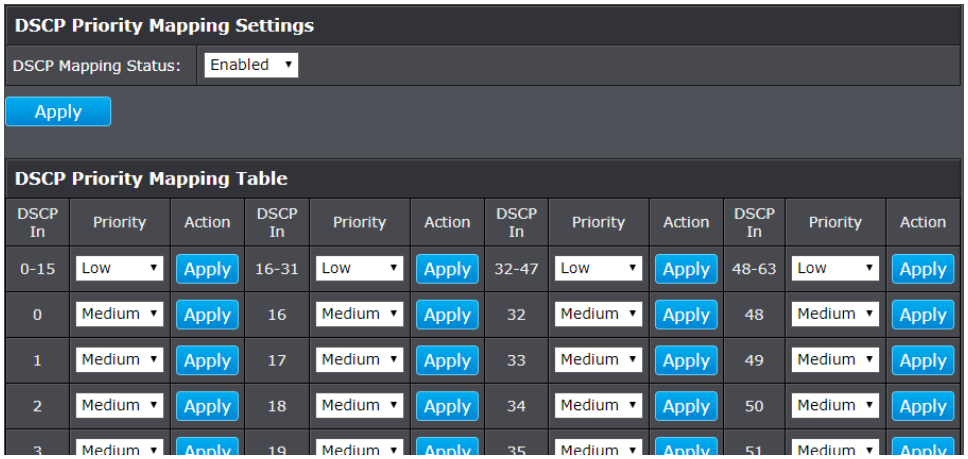
QoS > DSCP

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 four egress queues(Low, Medium, High, or Highest). The default queue for all DSCP values is 0.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 6).

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

3. For each DSCP In value that is relevant to your configuration, select a queue (Low, Medium, High, or Highest) in the **Queue** column. Select **Enabled** in the **DSCP Mapping** drop-down list. Click **Apply** to save the settings.



4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

Set the Scheduling Algorithm

QoS > Scheduling Algorithm

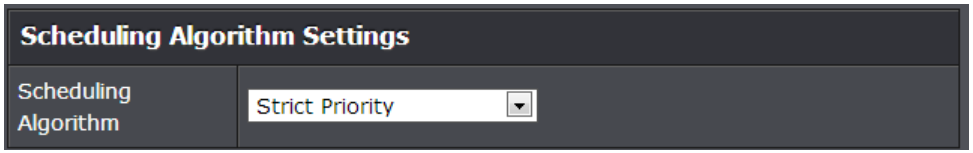
1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **QoS** and click on **Scheduling Algorithm**.

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

© Copyright 2018 TRENDnet. All Rights Reserved.

- **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. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

PoE Configuration

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	25.5W to 38.9W

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.

© Copyright 2018 TRENDnet. All Rights Reserved.

Configure PoE settings

PoE > Power over Ethernet

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **PoE** and click on **Power over Ethernet.**

A PoE System Power Status page displays PoE statistical information such as total PoE budget, PoE power used, and remaining PoE budget.

Power Over Ethernet System Power Status	
Power Budget:	31.0 W
Power Used:	0.0 W
Power Left:	31.0 W
The percentage of system power supplied:	0 %

Configure PoE settings

PoE > PoE Configuration

1. Log into your switch management page (see "Access your switch management page" on page 6).

2. Click on **PoE** and click on **PoE Configuration.**

3. Review the settings for each port. Next to each port entry, click **Apply** to save the settings.

- **Port** - Indicates the port with a specific PoE status and that you are configuring.
  Note: *You can **Enable** the row labeled **ALL** to apply settings to all ports.*
- **Admin** - To activate or deactivate PoE on a specific port, select **Enable** or **Disable**. By default the PoE feature is enabled on all switch ports.
- **Status** - The PoE port status is given as follows:
  - **Power ON** - The port is supplying PoE power.
  - **Power OFF** - The port is not supplying PoE power.
- **Classification** - The PoE class is indicated the class of the PD. N/A is displayed when the port is not supplying power.
- **Priority** - Indicates the port priority: Low, High, or Critical.
- **PowerLimit** – Indicates the power limit by class or power limit defined by the user.
- **UserDef** – After **UserDef** is selected in the **PowerLimit** cell, users can define the maximum power consumption for a specific port.
  Note: *The User Defined power limit ranges between 1.0 and 30.0 watts.*
- **Legacy Support –** When **Legacy Support** is enabled, the port sends out Passive PoE requirements to the device connected to the port.
  Note: *Doing so, may damage the device connected to the devices' ports.*
- **Power(W)** - Indicates the Power in watts that the port is supplying power to the PD.
- **Voltage (V)** - Indicates the Voltage in volts as measured at the port when the port is supplying power to the PD.

© Copyright 2018 TRENDnet. All Rights Reserved.

- **Current (mA)** - Indicates the Current in milliamps that the port is supplying to the PD.

PoE Configuration Table

Port	Admin	Status	Classification	Priority	PowerLimit	UserDef (1000-30000mW)	Legacy Support	Power (W)	Voltage (V)	Current (mA)	Action
All	Disabled	-	-	Low	Auto		Disabled	-	-	-	Apply
1	Enabled	POWER OFF	N/A	High	Auto		Disabled	0.0	0.0	0.0	Apply
2	Enabled	POWER OFF	N/A	High	Auto		Disabled	0.0	0.0	0.0	Apply

4. In the left hand panel, click on **Save**

5. Click **Save Settings to Flash**, then click **OK**

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.*

© Copyright 2018 TRENDnet. All Rights Reserved.

Switch Maintenance

Upgrade your switch 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.

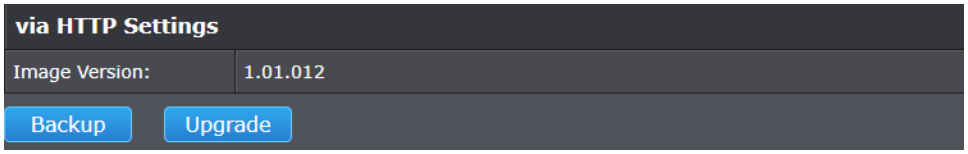
Firmware Upgrade via HTTP Settings

Tools > Firmware Upgrade

1. Log into your switch management page (see "Access your switch management page" on page 6).

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

3. Depending on your web browser, in the **via HTTP Settings** section, click **Upgrade** and click **Ok** on the prompt.



4. Wait for the 15 seconds and click continue.

5. Click **Browse** or **Choose File** and navigate to the folder on your computer where the unzipped firmware file (*.bin*) is located and select it.

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

© Copyright 2018 TRENDnet. All Rights Reserved.

Backup and restore your switch configuration settings

Tools > Configuration > 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

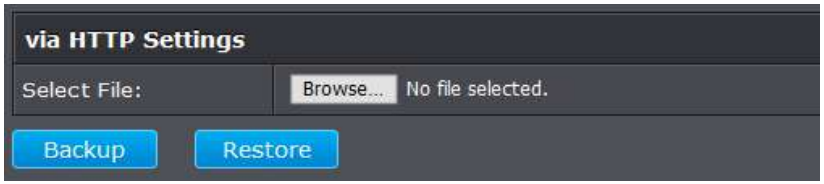
To backup your switch configuration:

1. Log into your switch management page (see "Access your switch management page" on page 6).
2. Click on **Tools**, and click on **Configuration.**
3. Click **Backup** to save the configuration file (config.bin) to your local hard drive.

Note: *If prompted, choose the location on your local hard drive. If you are not prompted, the configuration file (config.bin) 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 6).
2. Click on **Tools**, click on **Configuration**.
3. 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 Filename: *config.bin*). If prompted, click **Yes** or **OK**.
6. Wait for the switch to restore settings.

Cable Diagnostics Test

Tools > Diagnostics

The switch provides a basic cable diagnostic tool in the GUI for verifying the pairs in copper cabling and estimated distance for troubleshooting purposes.

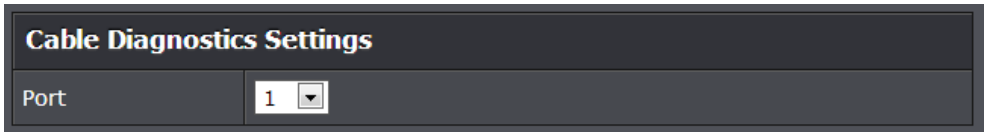
Note:

1. If the cable length displays N/A, it means that the cable length is Not Available. The may be due to the port being unable to determine the estimated cable length. If length is displayed as "N/A" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or of bad in quality.

2. The deviation of "Cable Fault Distance" is +/- 2 meters. No cable may be displayed in the table when the cable is less than 2 meters in length.

3. The test also measures the cable fault and identifies the fault in length according to the distance from the switch.

1. Log into your switch management page (see "Access your switch management page" on page 6).
2. Click on **Tools** and click on **Diagnostic**.
3. Click on the **Port** drop-down list to select which port to run the cable diagnostic and click **Test Now** to run the test.



© Copyright 2018 TRENDnet. All Rights Reserved.

The results will be displayed in the **Cable Diagnostic Table** below.

Cable Diagnostics Table

Port	Test Result	Cable Fault Distance(meters)
4	Pair1:Cross talk in Cable Pair2:OK Pair3:OK Pair4:Cross talk in Cable	Pair1:N/A Pair2:N/A Pair3:N/A Pair4:N/A

- **Test Results:** Displays the diagnostic results for each pair in the cable. One of the following cable status parameters is displayed:
  - **OK:** There is no problem detected with the cable.
  - **Open in Cable:** There is an open wire within the cable.
  - **Short in Cable:** Two wires are shorted together within the cable.
  - **Cross talk in Cable:** There is crosstalk detected between one pair of wires and another pair within the cable.
- **Cable Fault Distance:** This parameter specifies the distance from the switch port to the cable fault.

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 6).

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

3. Click the **Reboot Type** drop-down list and select **Normal** and click **Apply** to initiate a reboot. Wait for the switch complete the rebooting process.

Reboot

Reboot Type: Normal

Note: System will reboot in a few seconds after pressing the Apply button.

© Copyright 2018 TRENDnet. All Rights Reserved.

To reset your switch to factory defaults:

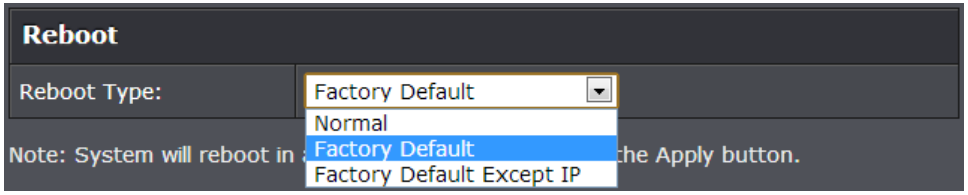
You may want to reset your switch to factory defaults if you are encountering difficulties with your switch and have attempted all other troubleshooting. Before you reset your switch to defaults, if possible, you should backup your switch configuration first, see "Backup and restore your switch configuration settings" on page 82.

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 6).
2. Click on **Tools** and click on **Reboot.**
3. Click the **Reboot Type** drop-down list and select from one of the following options
   - **Factory Default:** Resets all switch configuration settings to factory defaults including the IP address.
   - **Factory Default Except IP:** Resets all switch configuration settings to factory defaults and leaves the current IP address configuration.



The switch 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

Using the EdgeSmart Switch Management Utility

The Web Smart Management Utility allows you to do the following:

- You can easily discover all TRENDnet edgesmart switches on your network using the discover feature.
- You can modify the IP address settings, change the admin password, and upgrade firmware for multiple switches.

System Requirements

Operating System: Windows® 10 (32/64-bit), 8 (32/64-bit), Windows 7 (32/64-bit), Vista (32/64-bit), or XP (32/64-bit)

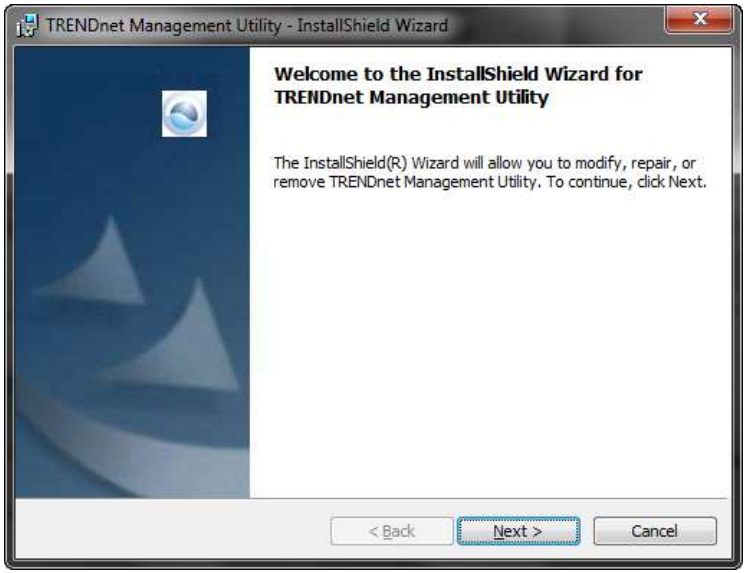
Installation

1. Download the utility from www.trendnet.com/support.

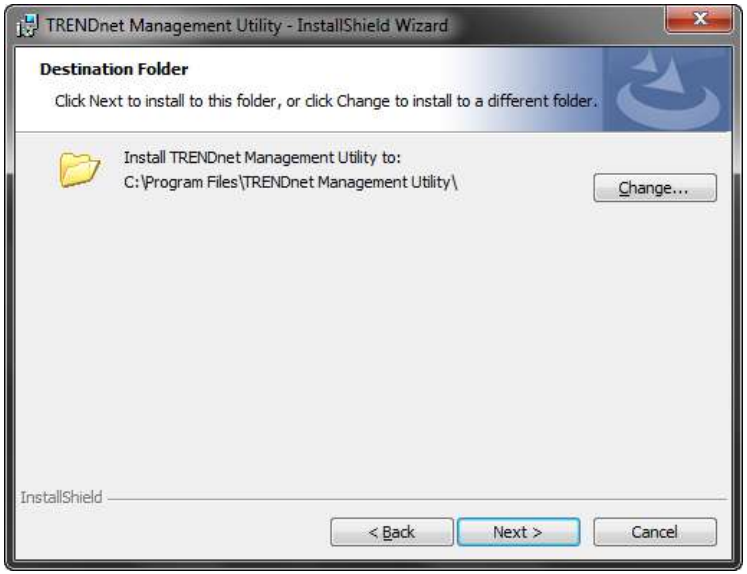
2. Extract the files from the zip file and run the **TRENDnet Management Utility-3.5.4.exe** file.

3. At the Utility installation window, click **Next**.

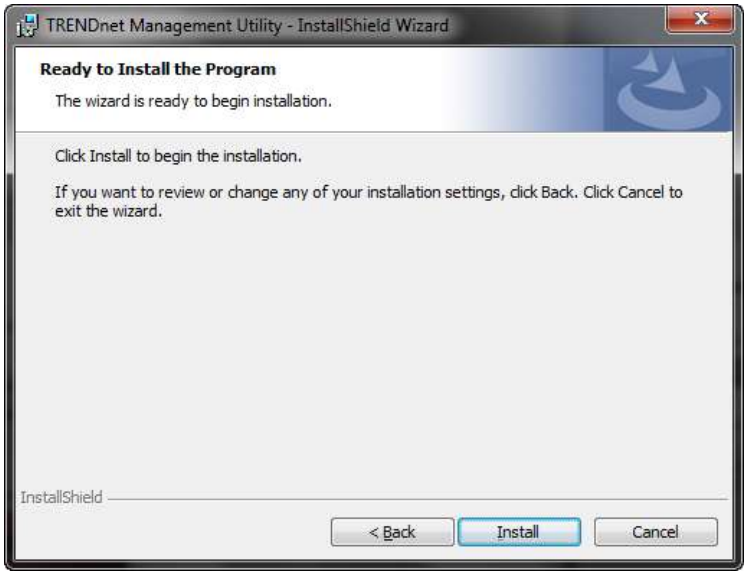
© Copyright 2018 TRENDnet. All Rights Reserved.



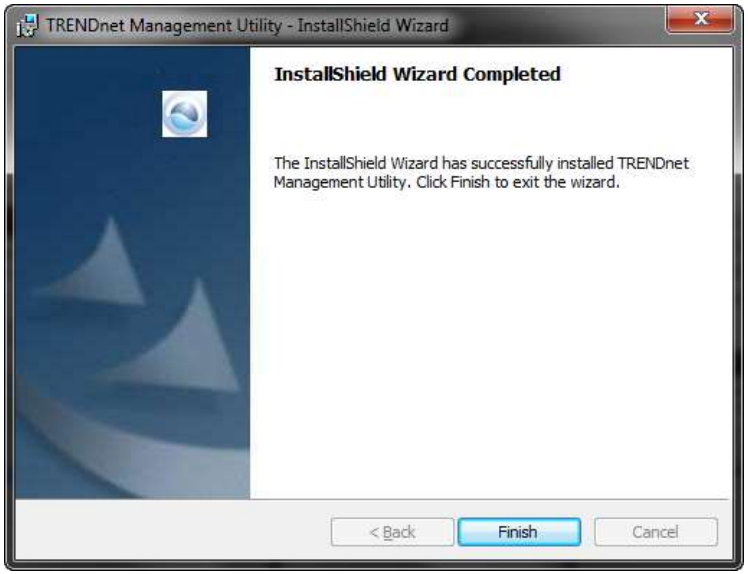
4. At the Install Location installation window, click **Next.**



5. At the Installation, click **Install**.



6. In the Completion window, click **Finish**.



© Copyright 2018 TRENDnet. All Rights Reserved.

Using the Utility

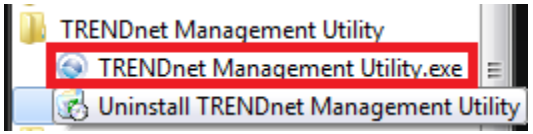
Launching the Utility

Upon completing the software installation, a desktop shortcut is automatically created.

Double-click the icon to start the utility or open the utility if it is already running. Closing the utility will exit the application. You can also click **Exit** at the bottom of the utility user interface to exit the application.

You can also launch the utility from the Start Menu programs.

Start > Programs (or All Programs) > TRENDnet Management Utility > TRENDnet Management Utility.exe



© Copyright 2018 TRENDnet. All Rights Reserved.

Discovery List

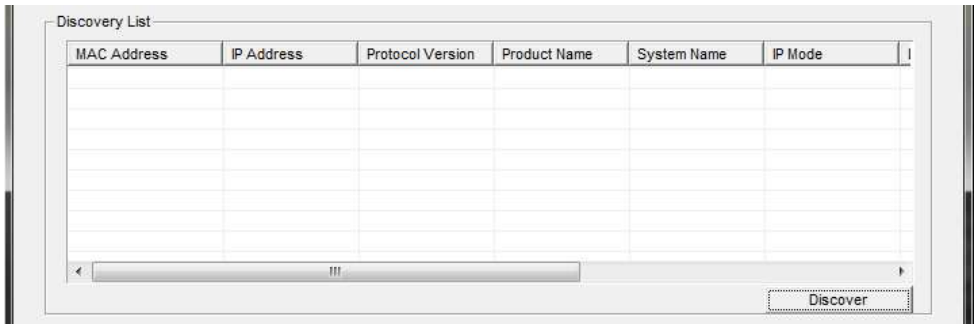
This is the list where you can discover all the Web management devices in your network.

By pressing the ***"Discovery"*** button, you can list all the Web Smart Management switches in the discovery list.

Double click or press the ***"Add to monitor list"*** button to select a device from the Discovery List to the Monitor List.

System word definitions in the Discovery List:

- ***MAC Address:*** Shows the device MAC Address.
- ***IP Address:*** Shows the current IP address of the device.
- ***Protocol version:*** Shows the version of the Utility protocol.
- ***Product Name:*** Shows the device product name.
- ***System Name:*** Shows the appointed device system name.
- ***IP Mode:*** Shows the DHCP status of the device.
- ***Location:*** Shows where the device is located.
- ***Subnet Mask:*** Shows the Subnet Mask set of the device.
- ***Gateway:*** Shows the Gateway set of the device.
- ***Group Interval:***

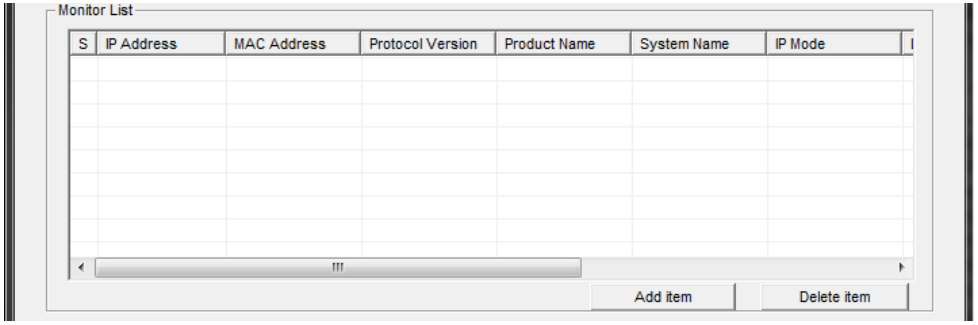


Monitor List

All the Web Smart switches in the Monitor List can be monitored; you can also receive the trap and show the status of the device.

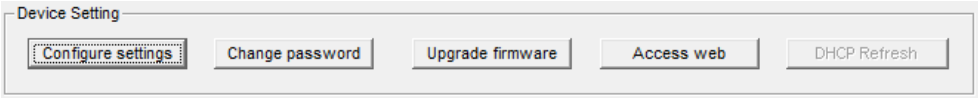
System word definitions in the Monitor List:

- ***S:*** Shows the system symbol of the Web-Smart device, ☒ represent for device system is not alive.
- ***IP Address:*** Shows the current IP address of the device.
- ***MAC Address:*** Shows the device MAC Address.
- ***Protocol version:*** Shows the version of the Utility protocol.
- ***Product Name:*** Shows the device product name.
- ***System Name:*** Shows the appointed device system name.
- ***IP Mode:*** Shows the DHCP status of the device.
- ***Location:*** Shows where the device is located.
- ***Subnet Mask:*** Shows the Subnet Mask set of the device.
- ***Gateway:*** Shows the Gateway set of the device.
- ***Group Interval:***
- ***Add Item:*** To add a device to the Monitor List manually, enter the IP Address of the device that you want to monitor.
- ***Delete Item:*** To delete the device in the Monitor List.



© Copyright 2018 TRENDnet. All Rights Reserved.

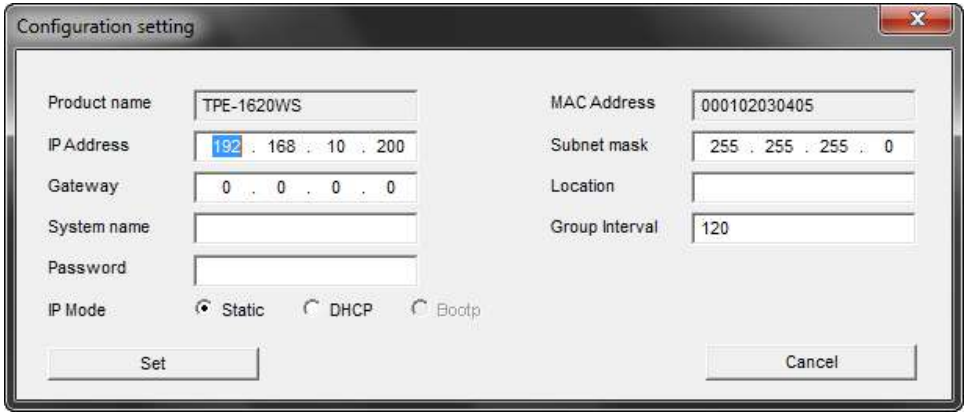
Device Setting



You can set the device by using the function key in the Device Setting Dialog box.

Configuration Setting: In this Configuration Setting, you can set the IP Address, Subnet Mask, Gateway, Group Interval, System name, Location and IP Mode.

Select the device in the Discovery list or Monitor List and press this button, then the Configuration Setting window will appear, after entering the data that you want to change, you must enter the password and press the "Set" to process the data change immediately. The default password of TRENDnet Web Smart Switches is ***"admin"***.



Password Change: You can use this Password Change when you need to change the password, fill in the password needed in the dialog box and press ***"Set"*** button to proceed the password change immediately.

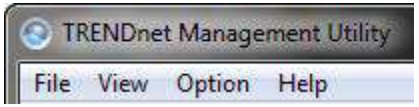
Firmware Upgrade: When the device has a new function, there will be a new firmware to update the device, use this function to update.

Access Web: Double click the device in the Monitor List or select a device in the Monitor List and press this ***"Web Access"*** button to access the device in Web browser.

DHCP Refresh: Press this ***"DHCP Refresh"*** button to refresh IP address of selected device form DHCP server. (Only applies if Web Smart switch IP address settings are set to DHCP).

© Copyright 2018 TRENDnet. All Rights Reserved.

Main Menu Options



In the ***"File TAB"***, there are Monitor Save, Monitor Save As, Monitor Load and Exit.

- ***Monitor Save:*** To record the setting of the Monitor List to the default, when you open the Web Management Utility next time, it will auto load the default recorded setting.
- ***Monitor Save As:*** To record the setting of the Monitor List in appointed filename and file path.
- ***Monitor Load:*** To manually load the setting file of the Monitor List.
- ***Exit:*** To exit the Web Management Utility.

In the ***"View TAB"***, there are view log and clear log function, this function will help you to show trap setting.

- ***View Log:*** To show the event of the Web Management Utility and the device.
- ***Clear Log:*** to clear the log.

In the ***"Option TAB"***, there are Refresh Time and Group Interval

- ***Refresh Time:*** *This function helps you to refresh the time of monitoring the device. Choose 15 secs, 30 secs, 1 min, 2 min and 5 min to select the time of monitoring.*
- ***Group Interval:*** **120~1225**

In the ***"Help TAB"***, there is About function, it will show out the version of the Web Management Utility.

© Copyright 2018 TRENDnet. All Rights Reserved.

Technical Specifications

Standards

- IEEE 802.1d
- IEEE 802.1w
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab
- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3az

Device Interface

- 4 x Gigabit PoE+ ports
- 1 x Gigabit port
- LED indicators
- Reset button

Data Transfer Rate

- Ethernet: 10Mbps (half duplex), 20Mbps (full duplex)
- Fast Ethernet: 100Mbps (half duplex), 200Mbps (full duplex)
- Gigabit: 2000Mbps (full duplex)

Performance

- Packet Buffer: 125KB
- Switch Fabric: 10Gbps
- MAC Address Table: 2K entries
- Forwarding rate: 7.44Mpps (64-byte packet size)
- Jumbo Frame: 9KB

Management

- HTTP Web based GUI
- SNMP v1, v2c
- Cable diagnostic test
- Backup/Restore Configuration
- Upload Firmware

Spanning Tree

- IEEE 802.1d STP (spanning tree protocol)
- IEEE 802.1w RSTP (rapid spanning tree protocol)

Link Aggregation

- Static link aggregation (only 1 group)

Quality of Service (QoS)

- Port-based QoS
- 802.1p Class of Service (CoS)
- Bandwidth Control/Rate Limiting per port (Min. Limit: 8Kbps)
- Queue Scheduling: Strict Priority (SP), Weighted Fair Queueing (WFQ)

VLAN

- Port-based VLAN
- 802.1Q Tagged VLAN
- Up to 32 VLAN groups, ID Range 1-4094
- Private VLAN

© Copyright 2018 TRENDnet. All Rights Reserved.

- Asymmetric VLAN
- Voice VLAN (5 user defined OUIs)

Multicast

- IGMP Snooping v1/2/3
- Block unknown multicast source
- Up to 32 multicast groups

Port Mirror

- One to one
- Many to one

Storm Control

- Broadcast (Min. Limit: 8Kbps)
- Multicast (Min. Limit: 8Kbps)
- Loopback Detection

Special Features

- PoE+ support
- Enable/disable 802.3az Power Saving
- Wall mountable

Power

- Input: 110-240V AC, 50/60Hz, 0.75A
- Output: 48V DC, 0.8A external power adapter
- Max. consumption: 34W

PoE

- PoE budget: 31W
- PoE Mode A: Pins 1,2 for power and pins 3,6 for power

MTBF

- 2,942,586 hours

Operating Temperature

- 0° – 40° C (32° – 104° F)

Operating Humidity

- Max. 90% non-condensing

Dimensions

- 150 x 98 x 28mm (5.9 x 3.86 x 1.1 in.)

Weight

- 380g (13.4 oz.)

Certifications

- CE
- FCC

Warranty

- Lifetime

© Copyright 2018 TRENDnet. All Rights Reserved.

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 4.
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

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 front 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".

© Copyright 2018 TRENDnet. All Rights Reserved.

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 2000/XP/Vista/7/8.1/10

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

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.

© Copyright 2018 TRENDnet. All Rights Reserved.

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,

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.

© Copyright 2018 TRENDnet. All Rights Reserved.

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

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

WARNING: Any changes or modifications 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

- EN 62368-1: 2014
- EN 55032:2015 +AC:2016 (CISPR32:2015/COR1:2016) (Class A)
- EN 61000-3-2:2014
- EN 61000-3-3:2013
- EN 55024:2010+A1:2015

Directives:

EMC Directive 2014/30/EU
RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
REACH Regulation (EC) No. 1907/2006
Low Voltage Directive 2014/35/EU
Ecodesign Directive 2009/125/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.

© Copyright 2018 TRENDnet. All Rights Reserved.

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

© Copyright 2018 TRENDnet. All Rights Reserved.

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 2018/08/06

© Copyright 2018 TRENDnet. All Rights Reserved.

TRENDnet®

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

Copyright ©2018. All Rights Reserved. TRENDnet.