

User's Guide

**TRENDNET**<sup>®</sup>



**10-Port 2.5GBASE-T Web Smart+ Switch  
with 2 x 10G SFP+ Slots**

**TEG-30102WS**

## Table of Contents

<b>Product Overview .....</b>	<b>1</b>
Package Contents .....	1
Features .....	1
Product Hardware Features.....	2
Application Diagram .....	4
<b>Switch Installation .....</b>	<b>5</b>
Desktop Hardware Installation .....	5
Rack Mount Hardware Installation.....	5
Basic Installation .....	6
Connect additional devices to your switch.....	7
<b>Configure your switch .....</b>	<b>8</b>
Access your switch management page.....	8
Switch Info .....	8
View your switch status information .....	8
System .....	10
Set your system information .....	10
Set your IPv4 settings .....	11
Create and assign IPv4 address interfaces to VLANs .....	12
Adding IPv4 Static ARP entries.....	13
Creating IPv4 Static Routes.....	14
Set your IPv6 settings .....	15
Create and assign IPv6 address interfaces to VLANs .....	16
Add IPv6 neighbors .....	17
Creating IPv6 Static Routes.....	18
DNS Settings .....	19
Restrict access to switch management page.....	19
Change administrator password and add accounts.....	20
Enable or disable SNMP and modify idle timeout settings.....	21
Set the switch date and time .....	22
Enable HTTPS/SSL (Secure Socket Layer) management access .....	23

View and setup your switch logging .....	24
Physical Interface.....	25
Configure your switch ports and view port status.....	25
Spanning Tree (STP, RSTP, MSTP).....	27
Configure Spanning Tree Protocol settings .....	27
Configure Spanning Tree Protocol port settings.....	28
Configure Spanning Tree Protocol MST settings (MSTP).....	29
View your Spanning Tree Protocol Instance Information (MSTP) .....	30
Configure Spanning Tree Protocol MST Port Settings (MSTP).....	31
Trunk Config (Link Aggregation) .....	31
Configure port trunk settings .....	31
View your trunk group status information .....	32
Configure your port priority .....	33
Mirroring .....	33
Configure port mirror settings.....	33
Loopback Detection.....	34
Enable loopback detection .....	34
Static Unicast .....	35
Add static unicast entries to the switch .....	35
Static Multicast.....	36
Add static multicast entries to the switch .....	36
IGMP Snooping.....	37
Configure IGMP Snooping Settings.....	37
Configure IGMP Snooping Port Settings.....	38
Configure IGMP Snooping Table VLAN parameters.....	38
Configure IGMP Snooping Port Settings.....	39
Configure IGMP Snooping Address Entry .....	40
Configure IGMP Snooping Profile Settings .....	40
MLD Snooping .....	41
Configure MLD Snooping Settings .....	41
Configure MLD Snooping Table VLAN parameters .....	41

Configure MLD Snooping Port Settings.....	42	Configure parameters for RMON events.....	68
Configure MLD Snooping Address Entry.....	43	Voice VLAN .....	69
Configure MLD Snooping Profile Settings.....	43	Create a Voice VLAN .....	70
Bandwidth Control.....	44	Configure Voice VLAN OUI settings .....	71
Configure Storm Control.....	44	Security .....	72
Set Ingress Rate Limiting.....	44	Configure Port Access Control .....	72
Set Egress Rate Limiting .....	45	Configure Port Access Settings .....	73
VLAN .....	45	Create Dial-In Users (Local Authentication Method).....	75
Add, modify, and remove VLANs .....	45	Add RADIUS Servers (RADIUS Authentication Method) .....	76
Configure VLAN Port Settings .....	47	Add TACACS+ Servers (TACACS+ Authentication Method).....	77
View the switch VLAN dynamic forwarding table.....	48	Destination MAC Filter .....	78
Create a private VLAN.....	48	Denial of Service (DoS) .....	79
View the current VLAN database.....	49	ARP Inspection .....	80
Asymmetric VLAN .....	49	Port Security Control .....	81
QoS (Quality of Service).....	51	DHCP Snooping.....	82
Set CoS priority settings.....	51	Enable DHCP Snooping .....	82
Set Port Priority .....	52	Enable DHCP Snooping .....	83
Set DSCP (Differentiated Services Code Point) Class Mapping settings .....	52	Set Trusted Interfaces.....	83
Set the Scheduling Algorithm .....	53	DHCP Server.....	84
SNMP .....	54	Enable DHCP Server .....	84
Set the SNMP Engine ID.....	54	DHCP VLAN Settings .....	84
Configure the SNMP View Table.....	54	DHCP Exclude IP Address.....	84
Configure the SNMP Group Access Table .....	55	DHCP Pool .....	86
Configure the SNMP User/Group Table.....	56	DHCP Relay .....	86
Configure the SNMP Community Table .....	57	DHCP Relay General Settings.....	86
Configure the SNMP Trap Management.....	58	LLDP (Link-Layer Discovery Protocol) .....	87
Access Control Config .....	59	Enable and configure LLDP .....	87
Configure Policy Settings .....	59	View LLDP Neighbor Information .....	89
Configure Rate Control .....	64	Statistic .....	89
RMON .....	64	View Traffic Information Statistics.....	89
Enable RMON.....	64	View Error Information Statistics.....	90
Configure parameters for RMON Ethernet statistics.....	65	<b>Switch Maintenance .....</b>	<b>91</b>
Configure parameters for RMON history control settings.....	66		
Configure parameters for RMON alarms.....	67		

- Upgrade your switch firmware ..... 91
  - Firmware Upgrade via HTTP Settings ..... 91
  - Firmware Upgrade via TFTP Settings ..... 92
- Backup and restore your switch configuration settings ..... 92
  - Backup/Restore via HTTP Settings ..... 92
  - Backup/Restore via TFTP Settings ..... 93
- Cable Diagnostics Test ..... 94
- Reboot/Reset to factory defaults ..... 95
- Network Connectivity Test (Ping Tool) ..... 96
- Technical Specifications.....97**
- Troubleshooting.....99**
- Appendix ..... 100**

## Product Overview



**TEG-30102WS**

## Package Contents

In addition to your switch, the package includes:

- Quick Installation Guide
- Power cord
- RJ-45 to RS-232 console cable (1m / 3.28 ft.)
- Rackmount kit

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 10-Port 2.5GBASE-T Web Smart+ Switch with eight 2.5GBASE-T ports and two 10G SFP+ slots, model TEG-30102WS, delivers advanced management features with an 80Gbps switching capacity. The TEG-30102WS is equipped with 2.5GBASE-T RJ-45 ports that provide higher gigabit speeds capable of up to 2.5Gbps over existing Cat5e or better cabling. This rack mountable IPv6 ready switch comes with an intuitive web-based interface. Advanced traffic management controls include IP routing, VLAN, QoS, access controls, link aggregation, troubleshooting, and SNMP monitoring, making this a powerful solution for SMB networks.

## Hardware Design

Provides 8 x 2.5GBASE-T ports and 2 x 10G SFP+ slots for high-speed network connections, and 1U rack mount design.

## 2.5GBASE-T Technology

Connect 2.5GBASE-T supported devices at 2.5Gbps for increased throughput over existing Cat5e or better cabling

## Smart Fans

Smart fans save energy by auto-adjusting the fan speed and use based on cooling needs

## IP Routing

Supports up to 32 IPv4/IPv6 static routes

## Network Management

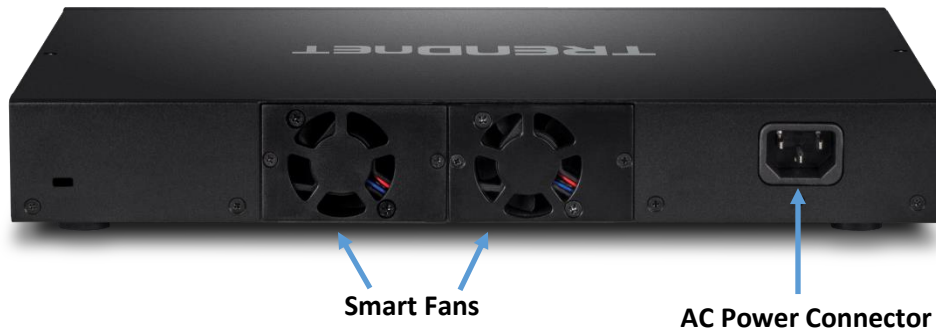
A broad range of network configurations are supported by: link aggregation, VLAN, bandwidth controls, IGMP, loopback detection, port mirroring, QoS, per port MAC restriction, and dynamic ARP inspection

## Troubleshooting

Traffic statistics and a convenient cable diagnostic test aid in network troubleshooting

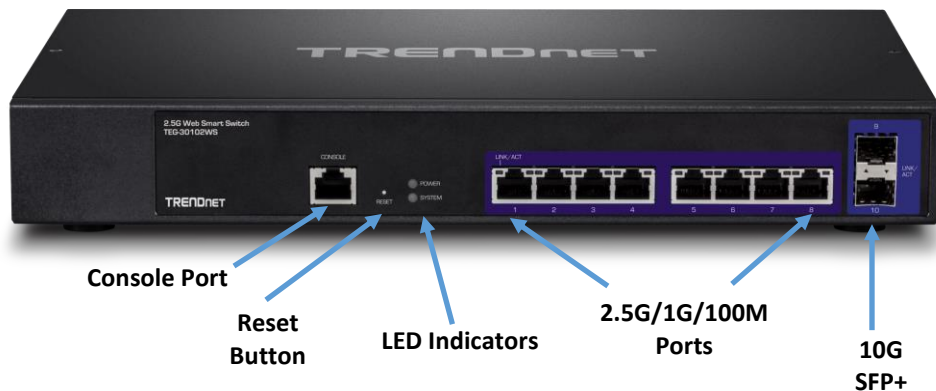
## Product Hardware Features

### Rear View



- **AC Power Connector** – Connect the AC power cord to the connector and the other side into a power outlet. (Input: 100~240VAC, 50/60Hz)

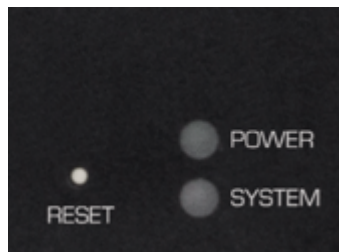
### Front View



- **Smart Fan** – Smart fans will automatically adjust speed based on temperature and switch usage. The smart fans are hot swappable.

- **Reset Button** – Press and hold this button for 10 seconds and release to reset the switch to factory defaults. The System LED will flash rapidly (orange) and turn solid (orange) to indicate the reset procedure was successful.
- **Console Port** – Connect the included RJ-45 to RS-232 cable access the command line interface. The command line management interface does not provide full command line management access to all features, only basic features such as modifying the administrator password and switch IP address.
- **Reset Button** – Press and hold this button for 10 seconds and release to reset the switch to factory defaults. The System LED will flash rapidly (orange) and turn solid (orange) indicating the reset procedure was successful. If using the hardware reset button to reset to factory default, the system LED will remain orange until the first device reboot.
- **2.5 Gigabit Ports (1-8)** – Connect network devices at 2.5G/1G/100M speeds.
- **SFP+ slots (9-10)** – Supports optional 10G SFP+ mini-GBIC modules.

• Diagnostic LED Indicators



• Power LED

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

• System LED

On (Green)	:	Solid - device ready and operating normally. Flashing – Firmware upgrade process
On (Orange)	:	Flashing – device is booting up, not ready. Also, will flash when resetting device to factory default. Solid – device LED will remain in this state when resetting to factory default through HW reset button, and will turn green after first reboot. *If the System LED is flashing or on solid (orange) after normal switch operation, flashing will indicate an issue with the smart fan, solid will indicate an issue with switch.



• 2.5G/1G/100M Ports (1-8)

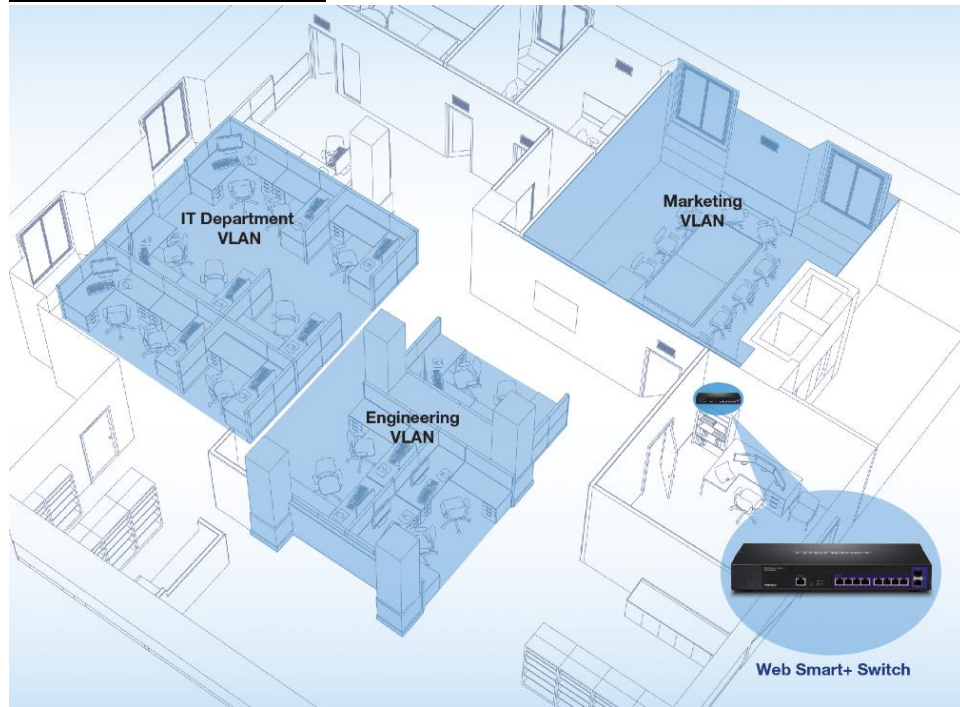
- **Link/Activity:** The upper left LED indicator above the Ethernet port

On (Green)	:	Solid – Device is connected at 2.5G speed. Blinking – Data transmission/activity at 2.5G speed.
On (Orange)	:	Solid – Device is connected at 1G/100Mbps speed. Blinking – Data transmission/activity at 1G/100Mbps speed.
Off	:	No link.

• SFP+ Slots (9-10)

On (Green)	:	Solid - Device is connected at 10G speed. Blinking – Data transmission/activity at 10G speed.
Off	:	No link

## Application Diagram



The WebSmart switch is installed a server room within an EIA standard-size, 19-inch rack. The 2.5G web smart switch is providing 2.5G connectivity and VLAN support to existing network infrastructure.



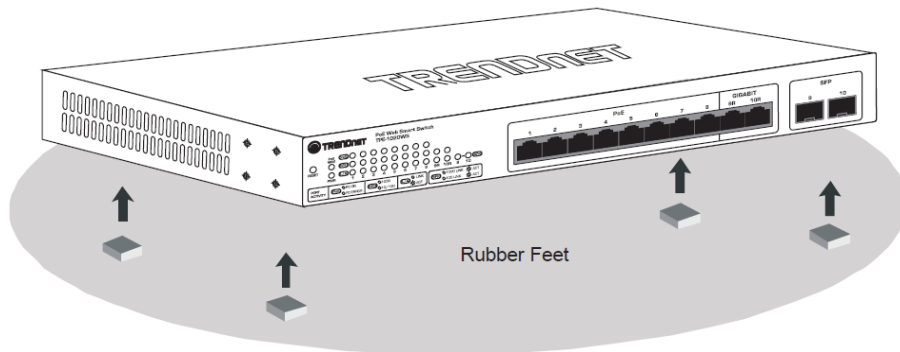
## Switch Installation

### Desktop Hardware Installation

The site where you install the hub stack may greatly affect its performance. When installing, consider the following pointers:

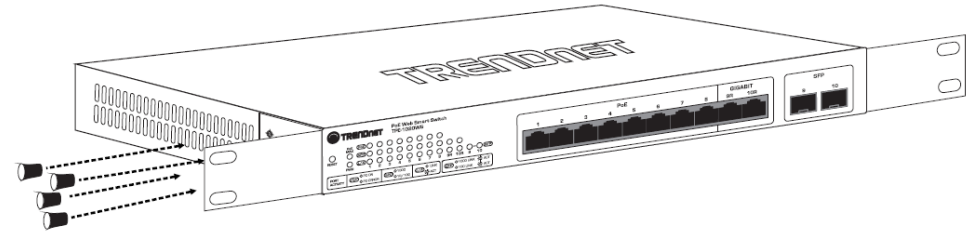
**Note:** The switch model may be different than the one shown in the example illustrations.

- Install the Switch in a fairly cool and dry place.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 10cm of space at the front and rear of the hub for ventilation.
- Install the Switch on a sturdy, level surface that can support its weight, or in an EIA standard-size equipment rack. For information on rack installation, see the next section, Rack Mounting.
- When installing the Switch on a level surface, attach the rubber feet to the bottom of each device. The rubber feet cushion the hub and protect the hub case from scratching.

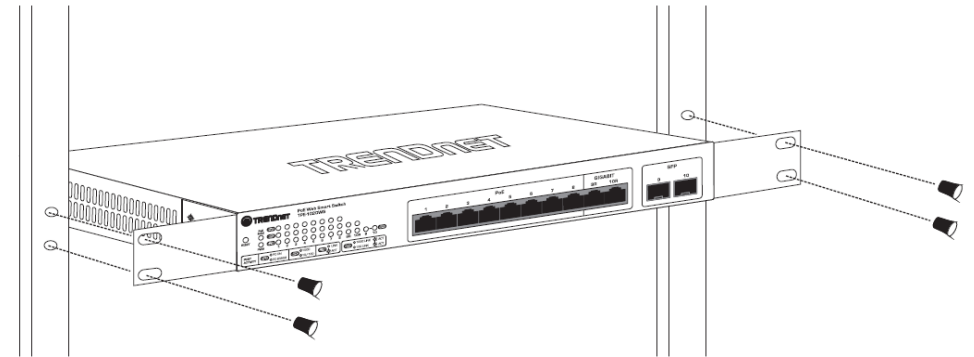


### Rack Mount Hardware Installation

The switch can be mounted in an EIA standard-size, 19-inch rack, which can be placed in a wiring closet with other equipment. Attach the mounting brackets at the switch's front panel (one on each side), and secure them with the provided screws.

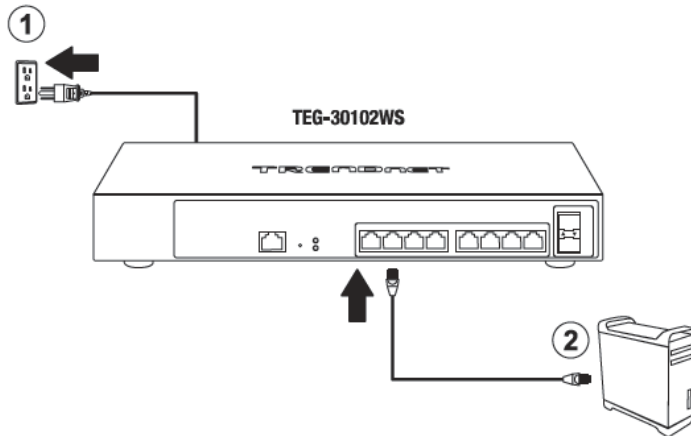


Then, use screws provided with the equipment rack to mount each switch in the rack.



**Note:** The look of the switch may be different than what is actually displayed.

## 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**.



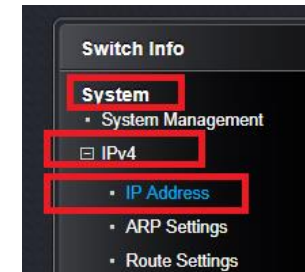
5. Enter the User Name and Password, and then click **Login**. By default:

User Name: **admin**

Password: **admin**

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

6. Click **System**, then click **IPv4**, click **IP Address**, and in the first entry, click **Modify**.



### IPv4 Address Table

Interface	IP Address	Subnet Mask	Link Status	Action
VLAN 1	192.168.10.200	255.255.255.0	Up	<b>Modify</b> Delete

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.

8. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

9. Click **Save Settings to Flash (button)**, then click **OK**.

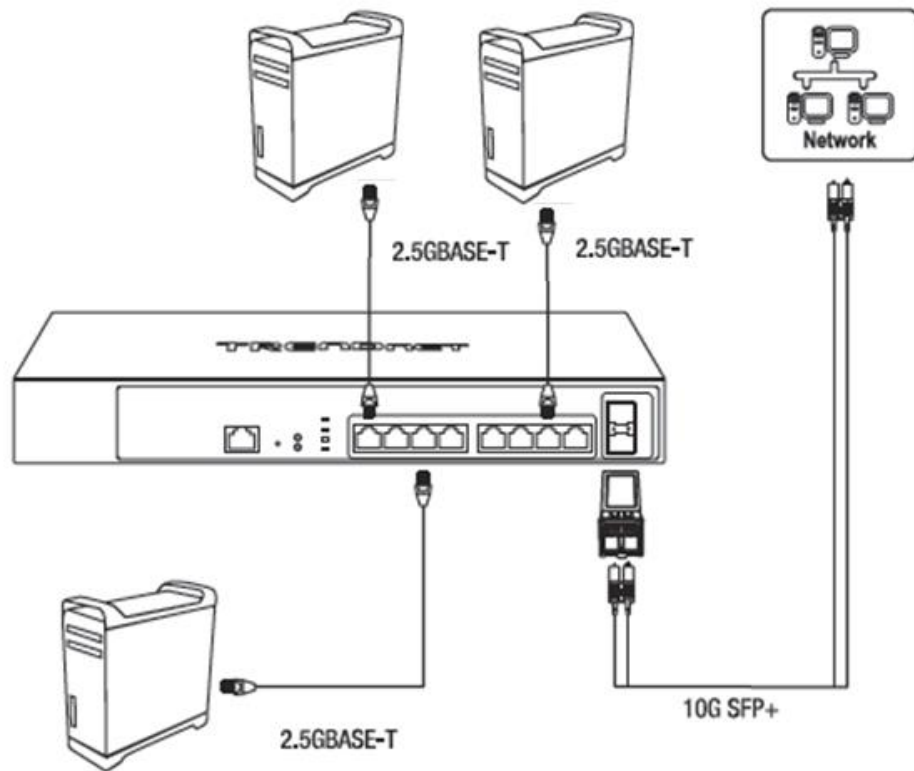
**Note:** Once the settings are saved, you can connect the switch to your network.

**Save Settings to Flash**

## Connect additional devices to your switch

You can connect additional computers or other network devices to your switch using Ethernet cables to connect them to one of the available 2.5G Ports (1-8). 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.

**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.



## 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 H/W version, RAM/Flash size, administration information, IPv4 and IPv6 information.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 13).
2. Click on **Switch 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),0 hr(s),31 min(s),33 sec(s)
Runtime Image:	1.00.16
Boot Loader:	1.00.01

#### Hardware Information

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

**Hardware Information**

Version:	v1.0R
DRAM Size:	512 MB
Flash Size:	128 MB
Temperature:	48 °C
Fan Status:	FAN1:Normal, FAN2:Normal

**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.

**System MAC Address**

MAC Address:	02:00:C1:9F:94:7A
--------------	-------------------

## 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 11).
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 Description** - Specifies the Switch model. You cannot change this parameter.
- **System Object ID** - Indicates the unique SNMP MIB object identifier that identifies the switch model. You cannot change this parameter.
- **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.

Management	
System Description:	TEG-30102WS
System Object ID:	1.3.6.1.4.1.28866.2.38
System Name:	<input type="text"/>
System Location:	<input type="text"/>
System Contact:	<input type="text"/>

4. Click **Apply**.

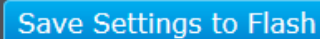


5. Click **Save Settings to Flash (menu)**.



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

**Note:** This step saves all configuration changes to the NV-RAM to ensure that the changes are permanent. If you do not complete this step, rebooting or power cycling the switch will lose all of your current configuration changes.



## Set your IPv4 settings

System > IPv4 > IP Address

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

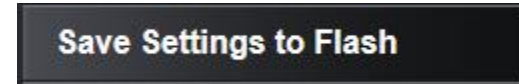
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System, IP Address**, and in the IPv4 address table for the VLAN1 interface, click on **Modify**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.
  - **Interface:** Displays the VLAN interface the IP interface settings are assigned.
  - **MAC Address:** Displays the switch MAC address information.
  - **IP Address:** Enter the new switch IP address. (e.g. 192.168.200.200)
  - **Subnet Mask:** Enter the new switch subnet mask. (e.g. 255.255.255.0)
  - **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 Auto Configuration:** If you need to automatically update the switch configuration files via a remote server, the DHCP Auto Configuration feature is available for this purpose via the DHCP server. Your IP address settings must enable the DHCP client so that this feature can operate with your DHCP server.

Modify IPv4 Address	
Interface:	VLAN 1
MAC Address:	02:00:C1:70:9B:13
IP Address:	192 . 168 . 10 . 200
Subnet Mask:	255 . 255 . 255 . 0
System IP Mode:	Static ▼
DHCP Auto Configuration:	Disabled ▼

4. Click **Apply**.



5. Click **Save Settings to Flash (menu)**.



6. Click **Save Settings to Flash (button)**, 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.



**Note:** Default IPv4 gateway IP address must be specified under System > IPv4 > Route Settings. For example: If your default gateway/router IP is 192.168.200.1, you would need to add a new static route below to specify the default gateway to use to access other IPv4 networks.

IPv4 Route Settings	
IPv4 Network Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Gateway IP Address:	192 . 168 . 200 . 1
<input type="button" value="Add"/>	

**Create and assign IPv4 address interfaces to VLANs**

System > IPv4 > IP Address

This section also allows you to create additional IP interfaces for different IP networks for IP routing and assign them to a specific VLAN interfaces. First, you must create a new VLAN under Bridge > VLAN > Tagged VLAN settings. Afterwards, you can assign an IP interface to the new VLAN.

1. Log into your switch management page (see [“Access your switch management page”](#) on page 11).

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

3. Enter a **VLAN ID** for the new VLAN. (2-4094)

In the example, we will use VLAN ID 50 and VLAN Name VLAN50.

- **VLAN ID:** 50
- **VLAN Name:** Enter text to describe the purpose of the VLAN, ex “VLAN50”.
- **Management VLAN:** Enabled allows management access to the switch management page from this VLAN/IP interface. Disabled denies management access to the switch management page from this VLAN/IP interface.

Tagged VLAN Settings	
VLAN ID:	50 (2-4094)
VLAN Name:	VLAN50 (32 characters limit)
Management VLAN:	Enabled

4. Select the ports to assign to this VLAN and click **Apply**.

In this example, assign ports 3 and 4 as untagged members of VLAN 50.

Static Tagged										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static Untagged										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Not Member										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply Clear Reset to Default

5. Click on **System**, **IPv4**, and **IP Address**.

To assign a new IPv4 address interface to the new VLAN, under **IPv4 Address Setup**, in the **Interface VLAN** field, enter the VLAN ID to assign the IPv4 address interface and click **Add**.

In this example, we will assign an IPv4 interface to VLAN 50.

IPv4 Address Setup	
Interface VLAN :	50 (1-4094)
Add	

The new IPv4 interface and VLAN will appear in the table. Click **Modify** to edit the IPv4 interface address settings. When creating an IP address interface (IPv4 or IPv6), an entry is automatically created for both IPv4 and IPv6 address tables.

IPv4 Address Table				
Interface	IP Address	Subnet Mask	Link Status	Action
VLAN 1	192.168.10.221	255.255.255.0	Up	Modify Delete
VLAN 50	0.0.0.0	0.0.0.0	Down	Modify Delete



For new IPv4 address interface, enter the **IP Address**, and **Subnet Mask** to assign to the VLAN and click **Apply**.

In the example, we will assign an IPv4 address of 192.168.50.200 and subnet mas of 255.255.255.0.

Modify IPv4 Address	
Interface:	VLAN 50
MAC Address:	02:00:C1:45:CE:DB
IP Address:	192 . 168 . 50 . 200
Subnet Mask:	255 . 255 . 255 . 0
System IP Mode:	Static ▾
DHCP Auto Configuration:	Disabled ▾
<b>Apply</b>	

Under **System > IPv4 > IP Address**, you will see the updated IPv4 address interface assigned to VLAN 50.

The VLAN with the assigned IPv4 address interface can now be used for IP routing purposes. You can repeat the steps to create additional VLANs and assign other IPv4 address interfaces.

IPv4 Address Table				
Interface	IP Address	Subnet Mask	Link Status	Action
VLAN 1	192.168.10.221	255.255.255.0	Up	<b>Modify</b> <b>Delete</b>
VLAN 50	192.168.50.200	255.255.255.0	Down	<b>Modify</b> <b>Delete</b>

6. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

7. Click **Save Settings to Flash (button)**, 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**

### Adding IPv4 Static ARP entries

*System > IPv4 > ARP Settings*

This section also allows you to create static ARP entries which may reduce some network overhead by creating entries for hosts that will consistently communicate to the switch in the current network environment. This will prevent the need for additional ARP requests and replies over the network.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, click **IPv4**, and click **ARP Settings**.
3. Review the settings for the static ARP configuration below and click **Add** to add the static ARP entry to the ARP table.

**Interface VLAN:** Enter the VLAN ID that the static ARP entry will reside.

**ARP IPv4 Address:** Enter the IPv4 address for the static ARP entry.

**Link Layer MAC Address:** Enter the MAC address for the static ARP entry.

IPv4 ARP Settings	
Interface VLAN	<input type="text"/> (1-4094)
ARP IPv4 Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Link Layer MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> (XX:XX:XX:XX:XX:XX)
<b>Add</b>	

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

### Creating IPv4 Static Routes

System > IPv4 > Route Settings

The switch supports IPv4 static IP routing which can be used to route traffic between multiple IP subnets.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, click **IPv4**, and click **Route Settings**.
3. Review the IPv4 Route Settings below. After you have entered all of the parameters for the static route, click **Add** to add to the IPv4 Route table.
  - **IPv4 Network Address:** Enter the IPv4 destination network address. (e.g. 192.168.200.0)
  - **Subnet Mask:** Enter the IPv4 subnet mask of the destination network. (e.g. 255.255.255.0)
  - **Gateway IP Address:** Enter the IPv4 gateway address used to reach the destination network. (e.g. 192.168.10.254)

IPv4 Route Settings	
IPv4 Network Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gateway IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="button" value="Add"/>	

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## Set your IPv6 settings

System > IPv6 > IPv6 Address

Use the **IPv6 System Settings** page to configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch via all of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front-panel ports through which traffic is switched or routed.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, **IPv6**, **IPv6 Address**, and in the IPv6 address table for the VLAN1 interface, click on **Modify**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.
  - **IPv6 State:** By default, the IPv6 interface is disabled. The IPv6 address for the IPv6 network interface is set in auto configuration mode if this option is enabled. The default value is Disable. Auto configuration can be enabled only when DHCPv6 is not enabled on any of the management interfaces.
  - **IPv6 Unicast Address / Prefix Length:** The IPv6 Unicast Address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address. Add the IPv6 prefix and prefix length to the IPv6 System Settings interface. (e.g. fc00::2/64)
  - **DHCPv6 Client:** To configure the switch to automatically obtain its IPv6 address configuration settings from a DHCPv6 server on your network.
  - **Link Local Address Settings:** A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need globally unique addresses to communicate. IPv6 devices must not forward packets that have link-local source or destination addresses to other links.

Modify IPv6 Address	
Interface:	VLAN 1
IPv6 State:	Enabled ▾
DHCPv6 Client:	Disabled ▾
IPv6 Unicast Address / Prefix Length:	fc00::1/64 (e.g.:3710::1/64)
Link Local Address / Prefix length	fe80::c1ff:fe4b:a3b1/64

- **NS Retransmit Time Settings:** A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The field is 1~3600 seconds. The default setting is 1 second.

NS Retransmit Time Settings	
NS Retransmit Time:	1 sec (1-3600)

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

**Note:** Default IPv6 gateway IP address must be specified under System > IPv6 > Route Settings.

**Create and assign IPv6 address interfaces to VLANs**

System > IPv6 > IPv6 Address

This section also allows you to create additional IP interfaces for different IPv6 networks for IP routing and assign them to a specific VLAN interfaces. First, you must create a new VLAN under Bridge > VLAN > Tagged VLAN settings. Afterwards, you can assign an IP interface to the new VLAN.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).

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

3. Enter a **VLAN ID** for the new VLAN. (2-4094)

In the example, we will use VLAN ID 50 and VLAN Name VLAN50.

- **VLAN ID:** 50
- **VLAN Name:** Enter text to describe the purpose of the VLAN, ex “VLAN50”.
- **Management VLAN:** Enabled allows management access to the switch management page from this VLAN/IP interface. Disabled denies management access to the switch management page from this VLAN/IP interface.

Tagged VLAN Settings	
VLAN ID:	50 (2-4094)
VLAN Name:	VLAN50 (32 characters limit)
Management VLAN:	Enabled

4. Select the ports to assign to this VLAN and click **Apply**.

In this example, assign ports 3 and 4 as untagged members of VLAN 50.

Static Tagged										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Static Untagged										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply Clear Reset to Default

5. Click on **System**, **IPv6**, and **IPv6 Address**.

To assign a new IPv4 address interface to the new VLAN, under **IPv4 Address Setup**, in the **Interface VLAN** field, enter the VLAN ID to assign the IPv4 address interface and click **Add**.

In this example, we will assign an IPv4 interface to VLAN 50.

IPv6 Address Setup	
Interface VLAN :	50 (1-4094)
Add	

The new IPv6 interface and VLAN will appear in the table. Click **Modify** to edit the IPv6 interface address settings. By default, all IPv6 address interfaces are disabled.

IPv6 Address Table				
Interface	IPv6 State	IPv6 Unicast Address / Prefix Length	DHCPv6 Client	Action
VLAN 1	Disabled		Disabled	Modify Delete
VLAN 50	Disabled		Disabled	Modify Delete

For new IPv6 address interface, set **IPv6 State** to Enabled, and enter the **IPv6 Unicast Address / Prefix Length** to assign to the VLAN and click **Apply**.

In this example, we will assign fc50::2/64 IPv6 address interface to VLAN 50.

Modify IPv6 Address	
Interface:	VLAN 50
IPv6 State:	Enabled ▾
DHCPv6 Client:	Disabled ▾
IPv6 Unicast Address / Prefix Length:	fc50::2/64 (e.g.:3710::1/64)
Link Local Address / Prefix length	
<input type="button" value="Apply"/>	

Under **System > IPv6 > IPv6 Address**, you will see the updated IPv4 address interface assigned to VLAN 50 in the table.

The VLAN with the assigned IPv6 address interface can now be used for IP routing purposes. You can repeat the steps to create additional VLANs and assign other IPv6 address interfaces.

IPv6 Address Table				
Interface	IPv6 State	IPv6 Unicast Address / Prefix Length	DHCPv6 Client	Action
VLAN 1	Disabled		Disabled	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
VLAN 50	Enabled	fc50::2/64	Disabled	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

6. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

7. Click **Save Settings to Flash** (button), 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 IPv6 neighbors

*System > IPv6 > Neighbor Settings*

This settings allows you to manually define IPv6 supported neighboring devices on your network.


1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, **IPv6**, and click on **Neighbor Settings**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.
  - **Interface VLAN:** Sets the value of the VLAN
  - **Neighbor IPv6 Address:** Specifies the neighbor IPv6 address.
  - **Link Layer MAC Address:** Specifies the link layer MAC address.
 Click **Add** to save the entry to the list.

IPv6 Neighbor Settings	
Interface VLAN	<input type="text" value=""/> (1-4094)
Neighbor IPv6 Address:	<input type="text" value=""/>
Link Layer MAC Address	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> (XX:XX:XX:XX:XX:XX)
<input type="button" value="Add"/>	

- You can type in the specific address and click **Find** to find the entry to modify or click **Delete** or delete the address. 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.

IPv6 Neighbor Table				
Interface	Neighbor IPv6 Address	Link Layer MAC Address	State	Action
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	All ▾	<input type="button" value="Find"/> <input type="button" value="Delete"/>
Page 1/1 <input type="button" value="First Page"/> <input type="button" value="Previous Page"/> <input type="button" value="Next Page"/> <input type="button" value="Last Page"/> Page <input type="text" value=""/> <input type="button" value="GO"/>				

4. Click **Save Settings to Flash (menu)**.

A dark grey rectangular button with the text "Save Settings to Flash" in white.

5. Click **Save Settings to Flash (button)**, 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.

A blue rectangular button with the text "Save Settings to Flash" in white.

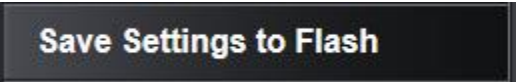
### Creating IPv6 Static Routes

System > IPv6 > Route Settings

The switch supports IPv6 static IP routing which can be used to route traffic between multiple IPv6 subnets.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, click **IPv6**, and click **Route Settings**.
3. Review the IPv6 Route Settings below. After you have entered all of the parameters for the static route, click **Add** to add to the IPv6 Route table.
  - **IPv6 Network Address / Prefix Length:** Enter the IPv6 destination network address and prefix. (e.g. *fc10::/64*)
  - **IPv6 Nexthop Address:** Enter the IPv6 gateway address used to reach the destination IPv6 network. (e.g. *fc00::1*)

4. Click **Save Settings to Flash (menu)**.

A dark grey rectangular button with the text "Save Settings to Flash" in white.

5. Click **Save Settings to Flash (button)**, 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.

A blue rectangular button with the text "Save Settings to Flash" in white.

**DNS Settings***System > DNS Settings*

This section allows you to connect to a specific DNS server with a specific IP address.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, and click on **DNS Settings**.
3. Review the settings.
  - DNS IPv4 Server – Input the IPv4 IP address where you want the switch to connect to.
  - DNS IPv6 Server – Input the IPv6 IP address where you want the switch to connect to.

**Note:** You can enter both the IPv4 and IPv6 IP addresses, or you can enter either one.

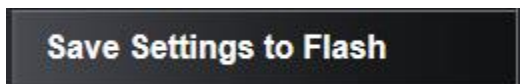
**DNS Server Settings**

DNS IPv4 Server:	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/>
DNS IPv6 Server:	<input style="width: 100%;" type="text"/>

4. Click **Apply**.



5. Click **Save Settings to Flash** (menu).



6. Click **Save Settings to Flash** (button), 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.

**Restrict access to switch management page***System > IP Access List*

This section allows you to define or restrict access to the switch management page to a list of specific IP addresses.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, and click on **IP Access List**.
3. Review the settings.

First, enter the IPv4 or IPv6 address to allow access and click **Add** for each entry.

**IP Address Settings**

IP Address:	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> <input checked="" type="radio"/> IPv4
	<input style="width: 100%;" type="text"/> <input type="radio"/> IPv6
<input type="button" value="Add"/>	

For each entry, the access list will populate. You can click **Delete** next to the entry to delete the entry or **Delete All** to delete all entries in the table.

<b>IP Access List table</b>		<b>Delete All</b>
Index	Accessible IP	Action
1	192.168.10.15	<input type="button" value="Delete"/>

When you have completed entering the IPv4 and IPv6 address entries, click the **IP Restriction Status** drop-down list at the top and select **Enabled**, then click **Apply**.

**IP Access List**

IP Restriction Status: Disabled ▾

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

**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 11).
2. Click on **System**, and click on **Administration**.
3. Review the settings.

To change the administrator password, in the "admin" entry in the table, click on **Modify**. **Note:** This default administrator account cannot be deleted.

**Administration table**

Index	User Name	Password	Action
1	admin	*****	<b>Modify</b>

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.

**Modify Administration**

Entry number:

User Name:

Password:

Confirm Password:

To create additional administrative user accounts:

- **User Name:** Enter the user name of the new account.
- **Password:** Enter the password for the new account and enter the password again the **Confirm Password** field to verify. Then, click **Add** to add to the table. For additional user accounts, you will be provided the option to **Modify** or **Delete** to remove the account.

**Note:** The password consists of up to 20 alphanumeric characters.



Administration Settings	
User Name:	<input type="text"/> (Maximum length is 20)
Password:	<input type="password"/> (Maximum length is 20)
Confirm Password:	<input type="password"/>
<input type="button" value="Add"/>	

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

### Enable or disable SNMP and modify idle timeout settings

System > User Interface

This section explains how to enable SNMP on the switch and modify the switch management page idle timeout settings.

**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 11).

2. Click on **System**, and click on **User Interface**.

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

- **SNMP Agent:** 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.
- **Telnet Agent:** Click the drop-down list to one of the following options
  - **Enabled** - When you enable this parameter, the Telnet agent is active. You can manage the switch remotely with Telnet network management.
  - **Disabled** - when you enable this parameter, the Telnet agent is inactive.
- **SSH Agent:** Click the drop-down list to one of the following options.
  - **Enabled** - When you enable this parameter, the SSH agent is active. You can manage the switch with SSH-agent helper program and the switches private MIB.
  - **Disabled** - when you enable this parameter, the SSH agent is inactive.
- **Web Server Status** - Displays the current SNMP status.

Status Settings	
SNMP Agent:	Enabled ▼
Telnet Agent:	Disabled ▼
SSH Agent:	Disabled ▼
Web Server Status:	Enabled
<input type="button" value="Apply"/>	

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

Timeout Settings	
Web Idle Timeout:	<input type="text" value="60"/> Min. (3-60)
<input type="button" value="Apply"/>	

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

### Set the switch date and time

System > System Time

This section allows you to set the switch time and date settings. Please note if using an SNTP server to sync time and date settings, please make sure the IP address, default gateway settings, and DNS settings are configured correctly, otherwise, the switch will not be able to reach the SNTP server to obtain time and date settings.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, and click on **System Time**.
3. Review the settings. Click **Apply** to save changes.
  - **Clock Mode** - Displays if system time and date is set manually **Local Time** or obtained automatically from a network time server **SNTP**.
  - **Current Time** – Displays the current system time and date.
  - **Time Zone** – Displays the current system time zone.

Clock Mode:	Local Time
Current Time:	2 Jan 2009 06:18:23
Time Zone:	

- **Clock Mode:** Select **Local Time** to manually configure your date and time settings or select **SNTP** to configure your switch to automatically obtain settings from a network time server.

### Date/Time Settings

Clock Mode:	Local Time <input type="button" value="v"/>
-------------	---

- **Local Time** – Allows you to manually set the time settings. If selecting this option, under **Local Time Settings**, manually enter your date and time settings.
  - **Date Settings** – Enter your date settings (YYYY/MM/DD).
  - **Time Settings** – Enter your time settings (HH:MM:SS)

Local time Settings	
Date Settings:	<input type="text" value="2009"/> / <input type="text" value="1"/> / <input type="text" value="2"/> (YYYY:MM:DD)
Time Settings:	<input type="text" value="06"/> : <input type="text" value="18"/> : <input type="text" value="23"/> (HH:MM:SS)

- **SNTP** – Allows you to configure your switch to pull time and date settings automatically from a network time server. If selecting this option, under **Simple Network Time Protocol (SNTP) Settings**, enter your time server settings.
  - **SNTP Primary Server** – Enter the primary network time server IPv4, IPv6 address, or the Domain name.
  - **SNTP Secondary Server** – Enter the secondary network time server IPv4 or IPv6 address.
  - **Time Zone** – Click the drop-down list to select your time zone.

Simple Network Time Protocol (SNTP) Settings										
SNTP Primary Server:	0	.	0	.	0	.	0	.	0	IPv4
SNTP Secondary Server:	0	.	0	.	0	.	0	.	0	IPv4
Time Zone:	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London									

4. Click **Apply**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

### Enable HTTPS/SSL (Secure Socket Layer) management access

System > SSL Settings

By default, your switch management page can be accessed using standard web HTTP protocol which is unsecure. Enabling HTTPS/SSL management access allows access to the switch management page using secure encrypted communication which prevents unauthorized users from intercepting user name and password credentials. Typically, the switch is accessed within the local network only by system administrators which does not necessarily require additional security. It is recommended to only enable this feature, if allowing switch management access from other networks or over the Internet.

**Note:** Once HTTPS/SSL management access is enabled, HTTP management access will be disabled forcing all access to the switch management page using secure encryption communication only.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **System**, and click on **SSL Settings**.

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

- **SSL Status:**

- **Enabled** – Enables HTTPS/SSL management access and disables HTTP unsecured mode.
- **Disabled** – Disabled HTTPS/SSL management access and enabled HTTP unsecured mode. (Default setting).

SSL Settings	
SSL Status:	Disabled

If enabling SSL management access, you will need to access the switch management page using **HTTPS** instead of **HTTP**. (e.g. <https://192.168.10.200/>)



Click **Continue, Proceed to this website**, and accept the certificate if prompted.

 **Continue to this website (not recommended).**

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## View and setup your switch logging

System > System Log Settings

The system log is designed to monitor the operation the switch by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **System**, and click on **System Log Settings**.
3. Review the settings. Click **Apply** to save changes.

- **Time Stamp**

- **Enable** - Each event message recorded in the log will have a time stamp.
- **Disable** - No time stamp will be included with the event messages.

- **Message Buffered Size** - Enter the message buffer size. (Range: 1-200)

- **Syslog** - Allows you to send device logging to an external log (Syslog) server for troubleshooting or monitoring.

- **Syslog Status** –

- **Enable** – Enable syslog and in the **Syslog Server IP** section, enter the IPv4 or IPv6 address of the external syslog server to send logging.
- **Disable** – Disable syslog functionality.

- **Facility** - Click the drop-down list and which facility to store the logging. (Options: local0 – local7)

**Note:** You can define the facility to store logging on your external syslog server. This helps to ensure you have separate logging sections for different devices.

- **Logging Level** – Click the drop-down list to select what level of event messages that will be logged.
  - **0 Emergency** - The system is unusable.
  - **1 Alert** - Action must be taken immediately.
  - **2 Critical** - Critical conditions are displayed.
  - **3 Error** - Error conditions are displayed.
  - **4 Warning** - Warning conditions are displayed.
  - **5 Notice** - Normal but significant conditions are displayed.
  - **6 Informational** - Informational messages are displayed
  - **7 Debug** - Debug-level messages are displayed.

System Log Settings	
Time Stamp:	Enabled ▾
Message Buffered Size:	50 (1-200)
Syslog Status:	Disabled ▾
Syslog Server IP:	0 . 0 . 0 . 0 <input checked="" type="radio"/> IPv4 <input type="text"/> <input checked="" type="radio"/> IPv6
Facility:	local0 ▾
Logging Level:	Info ▾

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

## Physical Interface

### Configure your switch ports and view port status

#### Physical Interface

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

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. 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 Ctrl**, settings to all ports at the same time.
  - **Trunk** - This parameter indicates the trunk group number. A number in this column indicates that the port has been added to a trunk using static or dynamic 802.3ad LACP link aggregation.
  - **Type** - This parameter indicates the port type. On the Switch, the port type is 2500TX for 10/100/1000/2.5GBase-T twisted-pair ports (1 through 8, 9R and 10R) and 100FX or 1000TX for the SFP ports (9 and 10) for copper or fiber SFP type.
  - **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:

- **Ignore** -This parameter applies to the **All** row only and indicates that the **Admin. Status** field must be set individually for each port.
- **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:
  - **Ignore** -This parameter indicates that the **All** setting does not apply to the **Mode** field. In other words, each port is set individually.
  - **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.
  - **Auto (2500F)** -This parameter indicates the port is configured for 2500Mbps operation in Auto-Negotiation full duplex mode.
  - **Auto (1000F)** -This parameter indicates the port is configured for 1000Mbps operation in Auto-Negotiation full duplex mode.
  - **Auto (100F)** - This parameter indicates that the port is configured for 100Mbps operation in Auto-Negotiation full duplex mode.

**Note:** Ports 1-8 can only function in auto negotiation mode 2500F/1000F/100F. 10G SFP+ slots can be set to Auto, 10g/Full, or 1000/Full operation.

**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.
  - The only valid setting for the SFP ports is Auto-Negotiation.
- **Jumbo:** This parameter indicates whether or not jumbo frames can be accepted by the switch. You may want to activate jumbo frames when your switch will transmit video and audio files. The possible values are:
    - **Ignore** -This parameter indicates that the **All** setting does not apply to the **Jumbo** field. In other words, each port is set individually.
    - **Enabled** -This parameter indicates the port is permitted to accept jumbo frames.
    - **Disabled** -This parameter indicates the port is not permitted to accept jumbo frames.
- Note:** When **QoS** is enabled on a port, the **Jumbo frame** parameter can not be enabled.
- **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:
    - **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	Trunk	Type	Link Status	Admin. Status	Mode	Jumbo	Flow Ctrl	Action
All	-	-	-	Ignore ▼	Ignore ▼	Ignore ▼	Ignore ▼	Apply
1	---	2500TX	Up	Enabled ▼	Auto (100F) ▼	Enabled ▼	Disabled ▼	Apply
2	---	2500TX	Up	Enabled ▼	Auto (1000F) ▼	Enabled ▼	Disabled ▼	Apply
3	---	2500TX	Down	Enabled ▼	Auto ▼	Disabled ▼	Disabled ▼	Apply

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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.

## Spanning Tree (STP, RSTP, MSTP)

### Configure Spanning Tree Protocol settings

Bridge > Spanning Tree > Protocol Settings

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 11).
2. Click on **Bridge**, then click on **Spanning Tree**.
3. Review the settings. Click **Apply** to save changes.
  - **Global STP Status:** 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.
  - **Protocol Version:** 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.
    - **MSTP** – Enables Multiple STP 802.1s on the device.
  - **Bridge Priority:** The **Bridge Priority** has a range 0 to 61440 in increments of 4096. To make this easier for you, the Web Management Utility divides the range into increments. You specify the increment that represents the desired bridge priority value.
  - **Maximum Age:** The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds

- **Hello Time:** The Hello Time is frequency with which the root bridge sends out a BPDU.
- **Forward Delay:** The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.
- **Transmit Hold Count:** The Transmit Hold Count specifies the maximum number of BPDUs that the bridge can send per second. Its range is 1 - 10.
- **Max Hop Count:** The Max Hop Count is a parameter set in a BPDU packet when it originates. It is decremented by 1 each time it is retransmitted by the next bridge. When the Hop Count value reaches zero, the bridge drops the BPDU packet. Its range is 6 - 40 hops.

Spanning Tree Protocol Settings	
Global STP Status:	Enabled ▾
Protocol Version:	RSTP ▾
Bridge Priority:	32768 ▾
Maximum Age:	20 <small>Sec. (6-40)</small>
Hello Time:	2 <small>Sec. (1-10)</small>
Forward Delay:	15 <small>Sec. (4-30)</small>
Transmit Hold Count:	6 <small>(1-10)</small>
Max Hop Count:	20 <small>(6-40)</small>

Note : Enabling Spanning Tree will cause the system to temporarily stop responding

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

Root Information	
Root Bridge:	80:00:02:00:c1:45:ce:db
Root Cost:	0
Root Maximum Age:	20
Root Forward Delay:	15
Root Port:	0

**Configure Spanning Tree Protocol port settings**

Bridge > Spanning Tree > Port Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **Spanning Tree**, and click on **Port Settings**.
3. Review the settings. For each entry, click **Apply** to save changes.

- **STP Status:** Indicates if spanning tree protocol is active or not on the port. Select one of the following choices from the pull-down menu:
  - **Enable** - The spanning tree protocol is enabled on the port.
  - **Disabled** - The spanning tree protocol is disabled on the port. Enable Disable

*Note: BPDU passthrough must be disabled for all ports under Physical interface for STP can be enabled.*
- **Priority:** Indicates the port priority. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost.
 

The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 1 lists the values that are valid.

**Valid Port Priority Values**

Step	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Port Priority	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240

- **Admin Cost (0 = Auto):** The administratively assigned value for the contribution of this port to the path cost of paths towards the spanning tree root. Writing a value of '0' assigns the automatically calculated default Path Cost value to the port. If the default Path Cost is being used, this object returns '0' when read.

- **External Cost:** This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Define a value between **1** and **200000000** to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. The default port cost: 100Mbps port = 200000. Gigabit port = 20000.
- **State** – Displays the current port spanning tree state.
  - **Blocking** - A blocking state does not allow network traffic to be sent or received on a the port except for BPDU data. A port with a higher path cost to the root bridge than another on the switch causes a switching loop and is placed in the blocking state by the Spanning Tree algorithm. The port's state may change to the forwarding state if the other links in use fail and the Spanning Tree algorithm determines the port may transition to the forwarding state.
  - **Listening** - This state occurs on a port during the convergence process. The port in the listening state processes BPDUs and awaits new information that would cause the port to return to the blocking state.
  - **Learning** - While the port does not yet forward frames (packets), in this state the port does learn source addresses from frames received and adds them to the filtering (switching) database.
  - **Forwarding** - A port that both receives and sends data. This indicates normal operation. STP continues to monitor the port for incoming BPDUs that indicate the port should return to the blocking state to prevent a loop.
  - **Disabled** - This state is not strictly part of STP. However, a network administrator can manually disable a port.
- **Edge:** Indicates if a port is connected to an edge device in the network topology or not. Selecting the **Forcetrue** parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Selecting the **Forcefalse** parameter indicates that the port does not have edge port status. Selecting the **Auto** parameter indicates that the port have edge port status or not have edge port status automatically. The default setting for this parameter is **Auto**.



- **P2P:** Choosing the **Forcetrue** parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex.

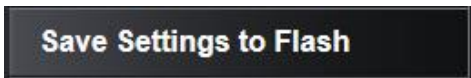
Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A P2P value of **Forcefalse** indicates that the port cannot have P2P status. **Auto** allows the port to have P2P status whenever possible and operate as if the P2P status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were **Forcefalse**.

The default setting for this parameter is **Auto**.

- **Restricted Role:** Toggle between **True** and **False** to set the restricted role state of the packet. If set to **True**, the port will never be selected to be the Root port. The default value is **False**.
- **Restricted TCN:** Toggle between **True** and **False** to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change. If set to **True**, it stops the port from propagating received TCN and to other ports. The default value is **False**.

Port Settings										
Port	STP Status	Priority	Admin Cost (0 = Auto)	External Cost	State	Edge	P2P	Restricted Role	Restricted TCN	Apply
All	Ignore ▼	Ignore ▼		-	-	Ignore ▼	Ignore ▼	Ignore ▼	Ignore ▼	Apply
1	Enabled ▼	128 ▼	0	200000	forwarding	Auto ▼	Auto ▼	False ▼	False ▼	Apply
2	Enabled ▼	128 ▼	0	20000	forwarding	Auto ▼	Auto ▼	False ▼	False ▼	Apply

4. Click **Save Settings to Flash** (menu).



5. Click **Save Settings to Flash** (button), 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 Protocol MST settings (MSTP)

Bridge > Spanning Tree > MST Settings

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Bridge**, click on **Spanning Tree**, and click on **MST Settings**.
3. Review the settings. For each section, click **Apply** to save changes.

#### MST Configuration Identification Settings

- **Configuration Name:** A configured name set on the switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP.
- **Revision Level (0-65535):** This value, together with the configuration name, and identical vlans mapped for STP instance IDs identifies the MST region configured on the switch.

MST Configuration Identification Settings	
Configuration Name:	02-00-c1-9f-94-7a
Revision Level:	0 (0-65535)

#### MST Instance Settings

- **MSTI ID (1 - 7):** Displays the MSTI ID associated with the VID List. The possible field range is 1-7.
- **VID List (1 - 4094):** Displays the VID List. Click **Add** to add into MST Table below.
- **Priority:** Enter the new priority in the Priority field. The user may set a priority value between **0-61440**.

MST Instance Settings	
MSTI ID:	<input type="text"/> * (1-7)
VID List:	<input type="text"/> (1-4094)
Priority:	<input type="text" value="0"/> ▼

- **MST Table:** Make changes to the table entry, and click **Apply** modify or click **Delete** to remove the ID entry.

MST Table			
MSTI ID	VID List	Priority	Action
CIST	<input type="text" value="1-4094"/>	<input type="text" value="32768"/> ▼	<input type="button" value="Apply"/> <input type="button" value="Delete"/>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

### View your Spanning Tree Protocol Instance Information (MSTP)

*Bridge > Spanning Tree > Instance Information*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **Spanning Tree**, and click on **Instance Information**.
3. View your MSTP instance information.

- **MSTI ID** – Specifies the instance to which the VLAN is assigned.
- **Internal Root Cost** – Specifies the intra-region cost to reach the CIST Regional Root.
- **Root Port** – Indicates the selected instance's root port.
- **Regional Root Bridge** – Displays the ID of the regional root bridge.
- **Designated Bridge** – Displays the ID of the bridge that connects the link or shared LAN to the root.
- **Instance Priority** – Specifies the selected spanning tree instance device priority. The field range is 0-61440. The field default is 32768.

Instance Information					
MSTI ID	Internal Root Cost	Root Port	Regional Root Bridge	Designated Bridge	Instance Priority
CIST	0	2	80:00:02:00:c1:9f:94:7a	10:00:d8:eb:97:f8:b7:53	32768

**Configure Spanning Tree Protocol MST Port Settings (MSTP)**

Bridge > Spanning Tree > MST Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **Spanning Tree**, and click on **MST Port Settings**.
3. Review the settings. For each entry, click **Apply** to save changes.
  - **Select MST Port** – Click the drop-down to select which MST port to configure.

**MST Port Settings**

Select MST Port

- **MST Port Info** - The MST Port Information page provides user to configure the MSTP Interface settings.
  - **Admin Path Cost (0 = Auto)** - This is the port cost used by MSTP when calculating path cost to the root bridge.
  - **Priority** - This is the port priority used by MSTP in calculating path costs when two ports on the switch have the same port cost.

MST Port Info							
MSTI ID	Designated Bridge	Internal Path Cost	Admin Path Cost (0 = Auto)	Priority	State	Role	Action
CIST	00:00:01:02:03:04:05	20000	<input type="text" value="0"/>	128	Forwarding	Designated	<input type="button" value="Apply"/>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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.

**Trunk Config (Link Aggregation)**

**Configure port trunk settings**

Bridge > Trunk Config > Trunking

The trunking function enables the cascading of two or more ports for a combined larger total bandwidth. Up to 4 trunk groups may be created. 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.

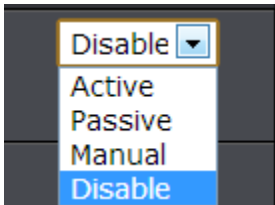
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **Trunk Config**, and click on **Trunking**.
3. Review the settings. For each trunk group, click **Apply** to save changes.

For each Trunk ID/Group, check the port numbers to add for each trunk group.

Trunk ID 1:	1	2	3	4	5	6	7	8	9	10
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Click the drop-down list and select one of the following options.

- **Active** - The specific aggregator will broadcast and respond to LACPDU (LACP Data Unit) packets. This setting enables the dynamic LACP feature for the trunk.
- **Passive** - The specific aggregator will not broadcast LACPDU packets, but it will respond to them. This setting disables the LACP feature for the trunk
- **Manual** - Enables static port trunking and disables the LACP feature for the trunk. (Static link aggregation).
- **Disable** - Disables the static port trunk and disables the LACP feature.



4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

### View your trunk group status information

*Bridge > Trunk Config > LACP Group Status*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **Trunk Config**, and click on **LACP Group Status**.
3. View your trunk group status information.
  - **System Priority** - Preassigned setting that cannot be modified. This value applies to the switch.
  - **System ID** - MAC address value assigned to the individual switch. This value cannot be modified.
  - **Group: #** The ID number of the trunk (link aggregation group).

#### LACP Group Status

System Priority:	32768
System ID:	00:01:02:03:04:05
Group: 1	This group doesn't exist
Group: 2	This group doesn't exist

**Configure your port priority**

Bridge > Trunk Config > Port Priority

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **Bridge**, click on **Trunk Config**, and click on **Port Priority**.

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

To assign a port higher priority within a trunk group, find the port number and in the priority column, enter a priority value 0-65535 (65535 being the highest priority).

Port Priority Settings	
Port	Priority (0-65535)
1	<input type="text" value="32768"/>
2	<input type="text" value="32768"/>
3	<input type="text" value="32768"/>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

**Mirroring****Configure port mirror settings**

Bridge > 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 11).

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

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

- **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.)

**Mirroring Settings**

Status:	<input type="text" value="Enabled"/>
Mirror Target Port:	<input type="text" value="1"/>

Check the port to monitor or copy information 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.

Mirroring Port Settings										
Ingress Port:										
	1	2	3	4	5	6	7	8	9	10
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress Port:										
	1	2	3	4	5	6	7	8	9	10
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## Loopback Detection

### Enable loopback detection

Bridge > 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 11).
2. Click on **Bridge** 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	
State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Loopback Detection Global Settings	
Interval	<input type="text" value="2"/> sec (1-32767)
Recover Time	<input type="text" value="60"/> sec (0 or 60-1000000, 0 is Disabled)

In the Loopback Detection table, select one of the **Loopback Detection State** choices from the drop down menu:

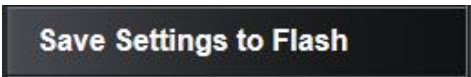
**Ignore:** This parameter indicates that the setting in the **All** row do not apply to the **Loopback Detection State** field. In other words, each port is set individually.

- **Enabled:** This selection enables the Loopback Detection feature for each port. This state must be enabled along with the **State** 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** instead of **Ignore**, 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 State	Loop Status	Action
All	Ignore ▾	-	Apply
1	Disabled ▾	Normal	Apply
2	Disabled ▾	Normal	Apply
3	Disabled ▾	Normal	Apply

4. Click **Save Settings to Flash (menu)**.



5. Click **Save Settings to Flash (button)**, 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.



## Static Unicast

### Add static unicast entries to the switch

Bridge > 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 11).
2. Click on **Bridge** 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.

### Static Unicast Address Settings

802.1Q VLAN:  (1-4094)

MAC Address:  :  :  :  :  :

---

### Port Member Settings

Port Member									
1	2	3	4	5	6	7	8	9	10
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

802.1Q VLAN (Free entries:256, Total entries:0) <span style="float:right">Delete All</span>			
VLAN Index	MAC Address	Port Members	Action
<< 802.1Q VLAN Static Unicast Address Table is empty >>			
Page 0/0	<a href="#">First Page</a>	<a href="#">Previous Page</a>	<a href="#">Next Page</a> <a href="#">Last Page</a> Page <input type="text"/> <a href="#">GO</a>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## Static Multicast

Add static multicast entries to the switch

Bridge > 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 11).
2. Click on **Bridge** 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.

Static Multicast Address Settings										
802.1Q VLAN:	<input type="text"/> (1-4094)									
Group MAC Address :	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>									
Group Member										
	1	2	3	4	5	6	7	8	9	10
<a href="#">All</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



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.

802.1Q VLAN (Free entries:256, Total entries:0) <span style="float: right;">Delete All</span>			
VLAN ID	MAC Address	Group Members	Action
<< Static multicast address table is empty >>			
Page 0/0 <span>First Page</span> <span>Previous Page</span> <span>Next Page</span> <span>Last Page</span> Page <input type="text"/> <span>GO</span>			

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## IGMP Snooping

### Configure IGMP Snooping Settings

Bridge > IGMP Snooping > Basic Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **IGMP Snooping**, and click on **Basic Settings**.
3. To enable IGMP Snooping, select **Enabled** from the drop down menu under **IGMP Snooping Global State**.

### IGMP Snooping Global State

Global State : Enabled ▾

4. Click **Apply**.

**Apply**

5. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

6. Click **Save Settings to Flash (button)**, 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**

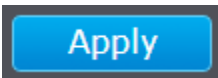
### Configure IGMP Snooping Port Settings

Bridge > IGMP Snooping > Port Settings

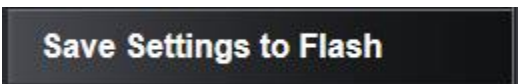
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **IGMP Snooping**, and click on **Port Settings**.
3. Review the settings.
  - **Static Router Port – Enable or Disable** will allow the switch to connect directly to the static router IP address.
  - **Fast Leave** – This allows the switch to send information to the last member of the host.
    - **Enable:** Enable will enable IGMP Snooping Fast Leave
    - **Disable:** Disable will not have IGMP Snooping Fast Leave
  - **Filter Profile** – This allows the switch to filter the types of data that goes through switch

IGMP Snooping Port Settings					
Port	Router Port Status	Static Router Port	Fast Leave	Filter Profile	Action
All		Ignore ▾	Ignore ▾	Ignore ▾	Apply
1	static	Enable ▾	Enable ▾	<None> ▾	Apply
2	none	Disable ▾	Disable ▾	<None> ▾	Apply

4. Click **Apply**.

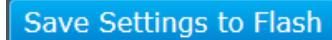


5. Click **Save Settings to Flash (menu)**.



6. Click **Save Settings to Flash (button)**, 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 Table VLAN parameters

Bridge > IGMP Snooping > Basic Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge** and click on **IGMP Snooping**.
3. Review the settings. Click **Apply** to save the settings.
  - **Status** – Click the drop-down list and select **Enabled** to enable the IGMP snooping feature or **Disabled** to disable the feature.
  - **Querier Election** – Click the drop-down list and select **Enabled** to enable the Querier Election or **Disabled** to disable this feature.
  - **Compatibility** – Click the drop-down to select Auto (automatically detect which IGMP version to use) or force the use of a specific IGMP version.
  - **Querier Interval** – Enter the amount of time you want your switch to send IGMP queries.
  - **Max Response Time** – Enter the maximum response time in seconds that client can wait before responding to a query.
  - **Robustness Variable** – Enter the robustness value used to determine the number of times to send a message.

Modify IGMP Snooping Settings	
Interface:	VLAN 1
Status:	Disabled ▾
Querier Election:	Enabled ▾
Compatibility:	Auto ▾
Query Interval:	125 Sec. (60-600)
Max Response Time:	10 Sec. (10-25)
Robustness Variable:	2 times (2-255)
Last Member Query Interval:	1 Sec. (1-25)

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## Configure IGMP Snooping Port Settings

Bridge > IGMP Snooping > Port Settings

- Log into your switch management page (see "[Access your switch management page](#)" on page 11).
- Click on **Bridge, IGMP Snooping, and Port Settings**.
- Review the settings. Click **Apply** to save the settings.
  - Static Router Port** – Select Enable for this option to assign a port as a static router port for IGMP snooping.
  - Fast Leave** – Select Enable to enable the fast leave function on specified port.
  - Filter Profile** – Profile tables can be created to allow or deny a specified range of multicast addresses. The multicast address range can be created under Bridge > IGMP Snooping > Address Entry and assigned to profile table to permit or deny under Bridge > IGMP Snooping > Profile Table.

IGMP Snooping Port Settings					
Port	Router Port Status	Static Router Port	Fast Leave	Filter Profile	Action
All		Ignore ▾	Ignore ▾	Ignore ▾	<b>Apply</b>
1	none	Disable ▾	Disable ▾	<None> ▾	<b>Apply</b>
2	none	Disable ▾	Disable ▾	<None> ▾	<b>Apply</b>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

**Configure IGMP Snooping Address Entry**

Bridge > IGMP Snooping > Address Entry

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **IGMP Snooping**, and click on **Address Entry**.
3. Review the settings.
  - **Address Entry Name:** Enter the entry ID.
  - **Start IPv4 Multicast Address:** Enter the starting IPv4 Address for the IPv4 Multicast Address
  - **End IPv4 Multicast Address:** Enter the final IPv4 Address for IPv4 Multicast Address

IGMP Snooping Address Entry Settings	
Address Entry Name	<input type="text"/>
Start IPv4 Multicast Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
End IPv4 Multicast Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

4. Click **Apply**.

Apply

5. Click **Save Settings to Flash (menu)**.

Save Settings to Flash

6. Click **Save Settings to Flash (button)**, 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

**Configure IGMP Snooping Profile Settings**

Bridge > IGMP Snooping > Profile Table

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **IGMP Snooping**, and click on **Address Entry**.
3. Select **Enable** or **Disabled** from the drop down menu to enable/disable IGMP Snooping Profile and click apply when completed.

IGMP Snooping Profile Settings	
Global State :	Enabled ▼

4. Enter the **Profile Name** and **Product Description** and click Add when completed.

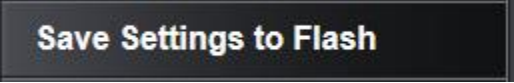
IGMP Snooping Profile Settings	
Profile Name	<input type="text"/>
Profile Description	<input type="text"/>

5. You can review your settings under the IGMP Snooping Profile Table.

4. Click **Apply**.



5. Click **Save Settings to Flash** (menu).



6. Click **Save Settings to Flash** (button), 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.

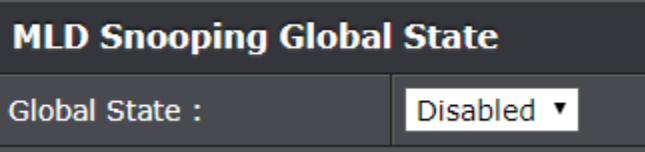


## MLD Snooping

### Configure MLD Snooping Settings

Bridge > MLD Snooping > Basic Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **MLD Snooping**, and click on **Basic Settings**.
3. To enable IGMP Snooping, select **Enabled** from the drop down menu under **MLD Snooping Global State**.



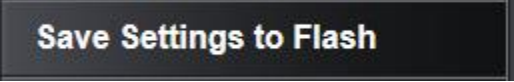
Global State :

Disabled ▼

4. Click **Apply**.



5. Click **Save Settings to Flash** (menu).



6. Click **Save Settings to Flash** (button), 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 MLD Snooping Table VLAN parameters

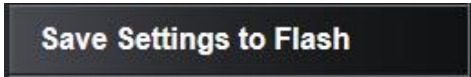
Bridge > MLD Snooping > Basic Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge** and click on **IGMP Snooping**.
3. Review the settings. Click **Apply** to save the settings.
  - **Status** – Click the drop-down list and select **Enabled** to enable the IGMP snooping feature or **Disabled** to disable the feature.
  - **Querier Election** – Click the drop-down list and select **Enabled** to enable the Querier Election or **Disabled** to disable this feature.
  - **Compatibility** – Click the drop-down to select Auto (automatically detect which IGMP version to use) or force the use of a specific IGMP version.
  - **Querier Interval** – Enter the amount of time you want your switch to send IGMP queries.

- **Max Response Time** – Enter the maximum response time in seconds that client can wait before responding to a query.
- **Robustness Variable** – Enter the robustness value used to determine the number of times to send a message.

Modify MLD Snooping Settings	
Interface:	VLAN 1
Status:	Disabled ▾
Querier Election:	Enabled ▾
Compatibility:	Auto ▾
Query Interval:	125 Sec. (60-600)
Max Response Time:	10 Sec. (10-25)
Robustness Variable:	2 times (2-255)
Last Listener Query Interval:	1 Sec. (1-25)

4. Click **Save Settings to Flash (menu)**.



5. Click **Save Settings to Flash (button)**, 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 MLD Snooping Port Settings

Bridge > MLD Snooping > Port Settings

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Bridge**, click on **MLD Snooping**, and click on **Port Settings**.

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

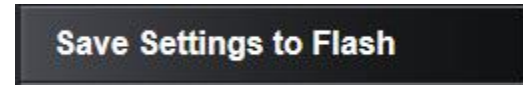
- **Static Router Port** – Select Enable for this option to assign a port as a static router port for IGMP snooping.
- **Fast Leave** – Select Enable to enable the fast leave function on specified port.
- **Filter Profile** – Profile tables can be created to allow or deny a specified range of multicast addresses. The multicast address range can be created under Bridge > MLD Snooping > Address Entry and assigned to profile table to permit or deny under Bridge > MLD Snooping > Profile Table.

MLD Snooping Port Settings					
Port	Router Port Status	Static Router Port	Fast Leave	Filter Profile	Action
All		Ignore ▾	Ignore ▾	Ignore ▾	Apply
1	none	Disable ▾	Disable ▾	<None> ▾	Apply
2	none	Disable ▾	Disable ▾	<None> ▾	Apply

4. Click **Apply**.



5. Click **Save Settings to Flash (menu)**.



6. Click **Save Settings to Flash (button)**, 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.



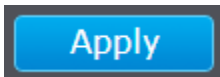
**Configure MLD Snooping Address Entry***Bridge > MLD Snooping > Address Entry*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **MLD Snooping**, and click on **Address Entry**.
3. Review the settings.
  - **Address Entry Name:** Enter the entry ID.
  - **Start IPv6 Multicast Address:** Enter the starting IPv4 Address for the IPv4 Multicast Address
  - **End IPv6 Multicast Address:** Enter the final IPv4 Address for IPv4 Multicast Address

**MLD Snooping Address Entry Settings**

Address Entry Name	<input type="text"/>
Start IPv6 Multicast Address:	<input type="text"/>
End IPv6 Multicast Address:	<input type="text"/>

4. Click **Apply**.



5. Click **Save Settings to Flash (menu)**.



6. Click **Save Settings to Flash (button)**, 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 MLD Snooping Profile Settings***Bridge > MLD Snooping > Profile Table*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **MLD Snooping**, and click on **Address Entry**.
3. Select **Enable** or **Disabled** from the drop down menu to enable/disable MLD Snooping Profile and click apply when completed.

**MLD Snooping Profile Settings**Global State : 

4. Enter the **Profile Name and Product Description** and click Add when completed.

**MLD Snooping Profile Settings**

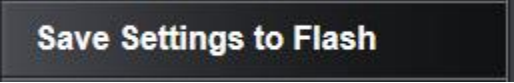
Profile Name	<input type="text"/>
Profile Description	<input type="text"/>

5. You can review your settings under the MLD Snooping Profile Table.

4. Click **Apply**.



5. Click **Save Settings to Flash** (menu).



6. Click **Save Settings to Flash** (button), 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.



## Bandwidth Control

### Configure Storm Control

Bridge > Bandwidth Control > Storm Control

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

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **Bandwidth Control**, and click on **Storm Control**.
3. Review the settings for each port. Click **Apply** to save the settings.
  - **DLF (Destination Lookup Failure)** – Click the drop-down list and select **Enabled** to enable DLF storm control.
  - **Broadcast** – Click the drop-down list and select **Enabled** to enable broadcast storm control.
  - **Multicast** – Click the drop-down list and select **Enabled** to enable multicast storm control.

- **Threshold** – Enter the pps (packets per second) threshold.

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

Storm Control Settings					
Port	DLF	Broadcast	Multicast	Threshold	Action
All	Ignore ▾	Ignore ▾	Ignore ▾	1pps x <input type="text"/> (10-13128147)	<a href="#">Apply</a>
1	Disabled ▾	Disabled ▾	Disabled ▾	1pps x <input type="text"/> 500 (10-13128147)	<a href="#">Apply</a>
2	Disabled ▾	Disabled ▾	Disabled ▾	1pps x <input type="text"/> 500 (10-13128147)	<a href="#">Apply</a>

4. Click **Save Settings to Flash** (menu).

5. Click **Save Settings to Flash** (button), 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

Bridge > 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 11).
2. Click on **Bridge**, click on **Bandwidth Control**, and click on **Ingress Rate Limiting**.
3. Review the settings for each port. Click **Apply** to save the settings.
  - **Bandwidth** – Enter the ingress rate limit value.
  - **Status** – Click the drop-down list and select **Enabled** to enable ingress rate limiting or select **Disabled** to disable ingress rate limiting.

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



Ingress Rate Limiting Settings			
Bandwidth = 1kbps x rate limit			
Port	Bandwidth	Status	Action
All	1kbps x <input type="text" value="500"/> (10-13128147)	Ignore ▾	<a href="#">Apply</a>
1	1kbps x <input type="text" value="500"/> (10-13128147)	Enabled ▾	<a href="#">Apply</a>
2	1kbps x <input type="text" value="500"/> (10-13128147)	Disabled ▾	<a href="#">Apply</a>

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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 Egress Rate Limiting

Bridge > 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 11).

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

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

- **Bandwidth** – Enter the egress rate limit value.
- **Status** – Click the drop-down list and select **Enabled** to enable egress rate limiting or select **Disabled** to disable egress rate limiting.

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

Egress Rate Limiting Settings			
Bandwidth = 1kbps x rate limit			
Port	Bandwidth	Status	Action
All	1kbps x <input type="text" value="500"/> (100-13107100)	Ignore ▾	<a href="#">Apply</a>
1	1kbps x <input type="text" value="500"/> (100-13107100)	Disabled ▾	<a href="#">Apply</a>
2	1kbps x <input type="text" value="500"/> (100-13107100)	Disabled ▾	<a href="#">Apply</a>

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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.

### VLAN

#### Add, modify, and remove VLANs

Bridge > 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 11).

2. Click on **Bridge**, 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.
- **Management VLAN** – Click the drop-down list and select **Enabled** to allow access to the switch management page through the new VLAN. If you want to restrict management access through this VLAN, select **Disabled**.

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

Tagged VLAN Settings	
VLAN ID:	<input type="text" value=""/> (2-4094)
VLAN Name:	<input type="text" value=""/> (32 characters limit)
Management VLAN:	Disabled ▾

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

**Tagged/Untagged/Not Member VLAN Ports**

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

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

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

Static Tagged										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

Static Untagged										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

Not Member										
	1	2	3	4	5	6	7	8	9	10
All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.*

Tagged VLAN Table				
VLAN ID	Name	VLAN Type	Management	VLAN Action
1	DefaultVLAN	Permanent	Enabled	<input type="button" value="Modify"/>

Page 1/1     Page

*Note: If a port does not belong to any VLAN, its PVID will be changed to default VLAN ID.*

4. Click **Save Settings to Flash (menu)**.

### Save Settings to Flash

5. Click **Save Settings to Flash (button)**, 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

### Configure VLAN Port Settings

Bridge > VLAN > Port Settings

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

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **VLAN**, and click on **Port Settings**.
3. Review the settings for each port. Click **Apply** to save settings.
  - **PVID** – Enter the port VLAN ID. **Note:** Required for untagged VLAN ports.
  - **Acceptable Frame Type** – Click the drop-down list and select which type of frames can be accepted.
    - **All** – The port can accept all frame types.
    - **Tagged** – The port can accept tagged frames only. Untagged frames are discarded.
    - **Untagged** – The port can accept untagged frames and frames with tagged priority information only such as 802.1p.
  - **Ingress Filtering** – Click the drop-down list and select **Enabled** to enable ingress filtering or **Disabled** to disable ingress filtering.

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

Port Settings			
Port	PVID	Acceptable Frame Types	Ingress Filtering
All	<input type="text"/>	Ignore ▾	Ignore ▾
1	<input type="text" value="1"/>	All ▾	Enabled ▾
2	<input type="text" value="1"/>	All ▾	Enabled ▾

4. Click **Save Settings to Flash (menu)**.
5. Click **Save Settings to Flash (button)**, then click **OK**.

### View the switch VLAN dynamic forwarding table

Bridge > VLAN > Dynamic 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 11).
2. Click on **Bridge**, click on **VLAN**, and click on **Dynamic 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.

Dynamic Forwarding Table Settings					
Port:	All	<input type="button" value="Refresh"/>			
Dynamic Forwarding Table					
ID	VID	Port	MAC Address	Type	VLAN Mode
1	1	5	00-14-D1-26-E4-76	Dynamic	802.1Q
2	1	1	D0-AE-EC-4E-E1-B0	Dynamic	802.1Q
Page 1/1 <input type="button" value="First Page"/> <input type="button" value="Previous Page"/> <input type="button" value="Next Page"/> <input type="button" value="Last Page"/> Page <input type="text" value=""/> <input type="button" value="GO"/>					

### Create a private VLAN

Bridge > VLAN > Private VLAN

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. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs.

The following guidelines apply when configuring private VLANs: The default VLAN 1 cannot be a private VLAN. The management VLAN 4095 cannot be a private VLAN. The management port cannot be a member of a private VLAN. IGMP Snooping must be disabled on isolated VLANs. Each secondary port's (isolated port and community ports) PVID must match its corresponding secondary VLAN ID. Ports within a secondary VLAN cannot be members of other VLANs. All VLANs that make up the private VLAN must belong to the same Spanning Tree Group.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **VLAN**, and click on **Private VLAN**.
3. To configure Private VLAN Settings, perform the following procedure:
  - Select Private VLAN status from the **Status** radio button choices that you want to change.
    - **Enable**: Enable Private VLAN settings.
    - **Disable**: Disable Private VLAN settings.
  - Press **Apply** for changes to take effect.
  - Set the **Source Port** to one of the following choices from the pull-down menu: All, 01 – 10.

- Click on the **Forwarding Ports** ratio button that applies to your configuration.
- Click **Apply**.

### Private VLAN Settings

State:  Enabled  Disabled

**Apply**

---

### Port Select

Source Port:

Forwarding Ports:

	1	2	3	4	5	6	7	8	9	10
<b>Clear</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Apply**

---

### Port List

Port	Port Map
1	1-10
2	1-10
3	1-10
4	1-10
5	1-10
6	1-10
7	1-10
8	1-10
9	1-10
10	1-10

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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.

### View the current VLAN database

*Bridge > VLAN > VLAN Current Database*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **VLAN**, and click on **Private VLAN**.
3. View the current VLAN database in the table.

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.

### 802.1Q Tagged VLAN

VLAN ID	VLAN Name	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	DefaultVLAN	1	1-10	1-10	permanent

Page 1/1 **First Page** **Previous Page** **Next Page** **Last Page** Page  **GO**

### Asymmetric VLAN

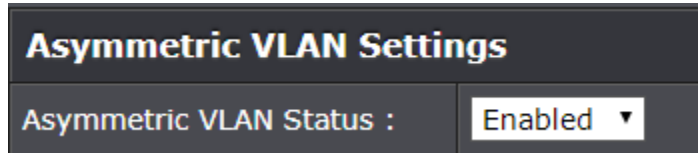
*Bridge > VLAN > Asymmetric VLAN*

Enabling asymmetric VLAN will you to create VLANs with overlapping untagged VLAN member ports for specific applications.

Asymmetric VLAN is a feature that restricts traffic on VLAN trunk ports. Below is a step on enabling and disabling the feature.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **VLAN**, and click on **Asymmetric VLAN**.

3. Select **Enable** or **Disable** from the drop down menu under Asymmetric VLAN.



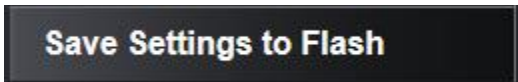
Asymmetric VLAN Settings

Asymmetric VLAN Status : Enabled ▾

4. Click **Apply**.



5. Click **Save Settings to Flash** (menu).



6. Click **Save Settings to Flash** (button), 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.



## 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

Bridge > QoS > CoS

**Note:** Before mapping the CoS priorities and the egress queues, you must disable the **Jumbo frame** parameter on each port. When **Jumbo frames** are enabled, COS cannot be enabled.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Bridge**, click on **QoS** and click on **CoS**.
3. Review the settings. Click **Apply** to save the settings.
  - Select **Enabled** in the **QoS Status** field.
  - For each **Traffic Class** whose queue you want to change, click on the **CoS Table** (Low, Medium, High, or Highest) radio button that applies to your configuration.

CoS	
QoS Status:	Disabled ▾
Traffic Class:	Queue
CoS Table	
Priority	Queue ID
0	1 ▾
1	0 ▾
2	2 ▾
3	3 ▾
4	4 ▾
5	5 ▾
6	6 ▾
7	7 ▾

4. Click **Save Settings to Flash** (menu).

Save Settings to Flash

5. Click **Save Settings to Flash** (button), 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

### Set Port Priority

Bridge > 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 11).
2. Click on **Bridge**, click on **QoS** and click on **Port Priority**.
3. For each port whose priority you want to change, select a priority (0-7) in the **User Priority** column. Click **Apply** to save the settings.

Port Priority Table		
Port	User Priority	Action
All	0 <input type="text"/>	<input type="button" value="Apply"/>
1	0 <input type="text"/>	<input type="button" value="Apply"/>
2	0 <input type="text"/>	<input type="button" value="Apply"/>

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

### Set DSCP (Differentiated Services Code Point) Class Mapping settings

Bridge > 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 11).
2. Click on **Bridge**, 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.



**DSCP Class Mapping Settings**

DSCP Mapping:

**DSCP Class Mapping Table**

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

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

### Set the Scheduling Algorithm

Bridge > QoS > Scheduling Algorithm

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

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

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

- **Strict Priority** - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues.
- **WRR (Weighted Round Robin)** - 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.

### Scheduling Algorithm Settings

Scheduling Algorithm

4. For **Weighted Round Robin** whose queue you want to change, select the weight level (Low, Medium, High, Highest) for each Queue ID.

5. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

6. Click **Save Settings to Flash** (button), 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**

## SNMP

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.

### Set the SNMP Engine ID

SNMP > Engine ID

The SNMP Engine ID screen allows network managers to define the SNMP Engine ID or to assign the default Engine ID to SNMP.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **SNMP** and click on **Engine ID**.
3. Review the settings. Click **Apply** to save the settings.
  - **Engine ID (10-64 Hex Characters)** – Enter the local device Engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. The Engine ID must be defined before SNMP is enabled.
  - **Reset to Default** – Use the device-generated Engine ID (**Reset to Default** will override any entry in the **Engine ID** field).

SNMP Engine ID Settings	
Engine ID:	<input type="text" value="800070c203000102030405"/> *

4. Click **Save Settings to Flash (menu)**.
5. Click **Save Settings to Flash (button)**, 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 SNMP View Table

SNMP > View Table

The SNMP View table specifies the MIB object access criteria for each View Name. If the View Name is not specified on this page, then it has access to all MIB objects. You can specify specific areas of the MIB that can be accessed or denied based on the entries in this table. You can create and delete entries in the View table.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **SNMP** and click on **View Table**.
3. Review the settings.

### Creating SNMP View Table Entries

This procedure explains how to create entries in the SNMP View Table.

- Enter the **View Name**. This entry must be pre-defined on the SNMP User/Group page.
- Enter the **Subtree OID**.
- Enter the **View Type**. Choose from the following options, and then click **Add**.
  - **Included:** This selection allows the specified MIB object to be included in the view.
  - **Excluded:** This selection blocks the view of the specified MIB object.

SNMP View Settings	
View Name:	<input type="text"/> * (32 characters limit)
Subtree OID:	<input type="text"/> *
View Type:	<input type="text" value="included"/> ▼

### Modifying SNMP View Table Entries

If you need to modify an entry in the View Table page, you must first delete the entry and then re-enter it.

### Deleting SNMP View Table Entries

In the **Action** column of the table, click **Delete** for the View table entry that you want to remove.

SNMP View Table			
View Name	Subtree OID	View Type	Action
ReadWrite	1	Included	Delete

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

### Configure the SNMP Group Access Table

SNMP > Group Access Table

The SNMP View Names are defined in the SNMP Group Access table and are based on the User and Group Names

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **SNMP** and click on **Group Access Table**.
3. Review the settings.

### Creating SNMP View Names

Before you can create an SNMP View name, you must define a Group Name using the SNMP User/Group page.

- Enter the **Group Name**. This entry must be pre-defined on the SNMP User/Group page.
- Enter the **Read View Name**. This name is an optional field. It can be up to 31 characters in length.
- Enter the **Write View Name**. This name is an optional field. It can be up to 31 characters in length.
- Enter the **Notify View Name**. This name is an optional field. It can be up to 31 characters in length.
- From the **Security Model** pull-down menu, select **v3**.
- Enter the **Security Level** from the pull-down menu. The selection options are:
  - **NoAuthNoPriv:** This selection is the appropriate selection when no **Auth-Protocol** or **Priv-Protocol** (no encryption) are selected on the SNMP User/Group page.
  - **AuthNoPriv:** Choose this selection when encryption has been enabled but only the **Auth-Protocol** has a password assigned and the **Priv-Protocol** has been selected as **none** on the SNMP User/Group page.
  - **AuthPriv:** When the **Auth-Protocol** or **Priv-Protocol** have been enabled, choose this selection.
- Click the **Add** button.

SNMP Group Access Settings	
Group Name:	<input type="text"/> *
	(32 characters limit)
Read View Name:	<input type="text"/> (32 characters limit)
Write View Name:	<input type="text"/> (32 characters limit)
Notify View Name:	<input type="text"/> (32 characters limit)
Security Model:	v1 ▾
Security Level:	NoAuthNoPriv ▾

### Modifying SNMP View Names

If you need to modify an entry in the SNMP Group Access page, you must first delete the entry and then re-enter it.

### Deleting SNMP View Names

In the **Action** column of the table, click **Delete** for the **View Name** that you want to remove.

**Note:** The views corresponding to the **ReadOnly** and **ReadWrite** Group Names are default values and cannot be removed.

SNMP Group Access Table						
Group Name	Read View	Write View	Notify View	Security Model	Security Level	Action
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	Delete

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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 SNMP User/Group Table

SNMP > SNMP User/Group

An SNMP User Name and Group Name definition is the basis for all the other SNMP tables. You can create and delete View Names by following the procedures in the following sections:

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **SNMP** and click on **SNMP User/Group**.
3. Review the settings.

### Creating SNMP User and Group Names

**Note:** There are no default User Names or Group Names defined for SNMP.

- Type a new **User Name**. Enter a name up to 32 characters in length.
- Type a new **Group Name**. Enter a name up to 32 characters in length.
- From the **SNMP Version** pull down menu, select **v3**. The **encryption** check-box becomes active.
  - Check the **encryption** check-box. The **Auth-Protocol**, **Priv-Protocol**, and associated password fields become active.
- Select one of the following choices for the **Auth-Protocol** field:
  - **MD5** - The MD5 authentication protocol. SNMP Users are authenticated with the MD5 authentication protocol after a message is received.
  - **SHA** - The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.
- Enter the password for the **Auth-Protocol**.
- Select one of the following choices for the **Priv-Protocol** field:
  - **DES** - Specifies DES encryption scrambles the SNMP data so that outside observers are prevented from seeing the data content.
  - **none** - Specifies no encryption is applied to SNMP data.

- Click **Add**. The new User Name and Group Name are displayed on the SNMP User/Group page.

SNMP User/Group Settings		
User Name:	<input type="text"/> *	(32 characters limit)
Group Name:	<input type="text"/> *	(32 characters limit)
SNMP Version:	v1 ▾	<input type="checkbox"/> encrypted
Auth-Protocol:	MD5 ▾	Password: <input type="text"/>
Priv-Protocol:	DES ▾	Password: <input type="text"/>

#### Modifying SNMP User and Group Names

If you need to modify an entry in the **SNMP User/Group** page, you must first delete the entry and then re-enter it.

#### Deleting SNMP User and Group Names

In the **Action** column of the table, click **Delete** for the **User Name** and **Group Name** that you want to remove.

SNMP User/Group Table					
User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

- Click **Save Settings to Flash (menu)**.
- Click **Save Settings to Flash (button)**, 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 SNMP Community Table

SNMP > Community Table

A community string has attributes for controlling who can use the string and what the string will allow a network management station to do on the switch. The Web Management Utility does not provide any default community strings. You must first define an SNMP User and Group Name on the SNMP User/Group page and then define a Community Name on the SNMP Community Table page.

- Log into your switch management page (see "[Access your switch management page](#)" on page 11).
- Click on **SNMP** and click on **SNMP User/Group**.
- Review the settings.

#### Create SNMP Community Settings

- Enter a new **Community Name**. A name can be up to 31 characters in length.
- Enter a **User Name(View Policy)** that has been previously defined. This name must match one of the User Names displayed on the **SNMP User/Group** page. If you enter a user name that has not been pre-defined on the SNMP User/Group page, the Community entry is displayed, but the agent/manager communication fails.
- Click **Add**. The values of the new **Community Name** and **User Name** are displayed.

SNMP Community Settings	
Community Name:	<input type="text"/> *
	(32 characters limit)
User Name (View Policy):	<input type="text"/> *
	(32 characters limit)

#### Modify SNMP Community Settings

If you need to modify a Community Table entry, you must first delete the entry by using the procedure below and then re-enter it with the modification by creating a new Community table entry.

**Delete SNMP Community Settings**

- To delete a **Community Name**, click **Delete** next to the entry in the table that you want to remove.
- The deleted **Community Name** is no longer displayed in the Community table. No confirmation message is displayed.

SNMP View Table		
Community Name	User Name(View Policy)	Action
private	ReadWrite	Delete
public	ReadOnly	Delete

- Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

- Click **Save Settings to Flash (button)**, 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**

**Configure the SNMP Trap Management**

*SNMP > Trap Management*

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.

- Log into your switch management page (see "[Access your switch management page](#)" on page 11).
- Click on **SNMP** and click on **Trap Management**.
- Review the settings.

**Create Trap Host Table Entry**

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

- Enable trap management by selecting the radio button next to **Enabled** at the top of the page. By default, trap management is enabled.
- Enter the **Host IP Address** for the management device that is to receive the SNMP traps.
- Enter the **SNMP Version**, either **v1**, **v2c**, or **v3** 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.
- Click **Add**. The new host is added to the table.

Trap Management Global Settings	
Trap:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<input type="button" value="Apply"/>	
Add Host Table	
Host IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> <input checked="" type="radio"/> IPv4 <input type="text"/> <input type="radio"/> IPv6
SNMP Version:	v1 <input type="button" value="v"/>
Community Name/User Name:	<input type="text"/> * (32 characters limit)
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

### Modify a Trap Host Table Entry

If you need to modify an SNMP Trap entry, you must first delete the entry by using the procedure below and then re-enter it with the modification by creating a new SNMP trap.

### Delete a Trap Host Table Entry

To delete an entry in the host table, click **Delete** next to the entry in the table that you want to remove. The Host table entry is removed from the table. No confirmation message is displayed.

Trap Management Table			
Host Ip Address	SNMP Version	Community Name/User Name	Action
<< snmp trap management list is empty >>			

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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.

## Access Control Config

Access Control configuration allows you to control different aspects of the Ethernet traffic as it enters the switch ports and is process through the Switch. You can specify what traffic is permitted or denied to flow through the switch by setting up specific filter criteria at an ingress port. You can also manage the switching priority of Ethernet packets. All of this is done by specifying policies that define the filtering and priority behavior.

### Configure Policy Settings

*Access Control Config > Policy Settings*

The Policy Settings page allows you to specify the filtering criteria for one policy. You can create, modify or delete a Policy by following the procedures in the following sections:

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Access Control Config** and click on **Policy Settings**.
3. Review the settings.

Choose the type of policy to create:

- **Add ETYPE**
- **Add ARP**
- **Add IPv4**
- **Add IPv6**

**Note:** Please note that when adding polices, it is important to note that the rule/policy order of priority in which the rules/policies are evaluated by the switch, 1 being the highest priority.

Policy Type				
Policy type:	<input type="button" value="Add ETYPE"/>	<input type="button" value="Add ARP"/>	<input type="button" value="Add IPv4"/>	<input type="button" value="Add IPv6"/>

### Add ETYPE

To add an ETYPE policy, use the following procedure:

- Click **Add ETYPE**, The **Policy Settings** page.
- Enter a number in the **Policy Index** field. The **Policy Index** is a unique number within the range of 1 – 256 which identifies the policy. This field is mandatory.
- Enter a number in the **VLAN ID** field. A unique number identifying a VLAN ranging from 1 to 4094.
- Enter a number in the **802.1p Priority** field. Enter the priority level of the frame ranging from 0 – 7.
- Choose the parameters to add for the policy, and enter data one or more of the parameters required for your policy. They are listed here:
  - **Source MAC Address** - Specifies the source MAC address. The format is xx.xx.xx.xx.xx.xx.
  - **MAC Address Mask** - Indicates mask for the Source MAC Address. The format is xx.xx.xx.xx.xx.xx.
  - **Destination MAC Address** - Specifies the destination MAC address. The format is xx.xx.xx.xx.xx.xx.
  - **MAC Address Mask** - Indicates mask for the Destination MAC Address. The format is xx.xx.xx.xx.xx.xx.
  - **Ether Type** - Indicates the protocol of the Ethernet frame protocol ranging from 0600 to FFFF.
  - **Policy Action** – Indicates if the policy will be **Permitted** or **Denied**.
  - **Policy Action:** In the **Permit/Deny** field, use the pull down menu to select one of the following parameters:
    - **Deny** - This selection drops ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP**.
    - **Permit** - This selection allows ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP** to be processed by the switch.

**Note:** You must enter a selection for **Deny/Permit** field even if the Profile Action ID that you have entered ignores both the **Replaced-DSCP** and **Replaced-CoS** fields.

- **Rate Control Index:** The Rate Control Index is a unique number within the range of 1 - 65535. This field is mandatory and must match a Port List Index that has been previously entered on the **Policy Index**.
- **Ingress Port List:** Select the interface for which you want to display data.
- Click **Add** to add the policy to the Policy Table.

Policy Index:	<input type="text" value=""/>	(1-256)		
VLAN ID:	<input type="text" value=""/>	(1-4094)	802.1p Priority:	<input type="text" value=""/>
Source MAC Address:	<input type="text" value=""/>	:	MAC Address Mask:	<input type="text" value="11 : 11 : ed : : :"/>
Destination MAC Address:	<input type="text" value=""/>	:	MAC Address Mask:	<input type="text" value=" : : : : :"/>
Ether Type:	0x <input type="text" value=""/>	(0600-FFFF, Excluding: 0806, 0800, 86DD)		
Policy Action:	<input type="text" value="Permit"/>		Rate Control Index:	<input type="text" value="None"/>
Ingress Port List:	<input type="text" value=""/>	(e.g. 1,3,5-8)		



### Add ARP

To add an ARP policy, use the following procedure:

- Click **Add ARP**, The **Policy Settings** page.
- Enter a number in the **Policy Index** field. The **Policy Index** is a unique number within the range of 1 – 256 which identifies the policy. This field is mandatory.
- Enter a number in the **VLAN ID** field. A unique number identifying a VLAN ranging from 1 to 4094.
- Enter a number in the **802.1p Priority** field. Enter the priority level of the frame ranging from 0 – 7.
- Choose the parameters to add for the policy, and enter data one or more of the parameters required for your policy. They are listed here:
  - **Source MAC Address** - Specifies the source MAC address. The format is xx.xx.xx.xx.xx.xx.
  - **MAC Address Mask** - Indicates mask for the Source MAC Address. The format is xx.xx.xx.xx.xx.xx.
  - **ARP / RARP**: In the field, use the pull down menu to select one of the following parameters
    - **Any**: This selection allows the switch to automatically choose **ARP** or **RARP**
    - **ARP**: This selection allows the sender's IP address to communicate to the target's MAC address
    - **RARP**: This selection allows the sender's Mac address to communicate to the target's IP address
  - **Request / Reply**: In the field, use the pull down menu to select one of the following parameters
    - **Any**: This selection allows the switch to automatically chose **Reply** or **Request**
    - **Request**: This selection allows the target device to request from the source
    - **Reply**: This selection allows the target device to only reply to the source
  - **Sender IP Address** - Specifies the IP address of the sender
  - **Mask Length** – Indicates the length of the Sender IP Address ranging from 1 – 32

- **Target IP Address** - Specifies the IP address of the sender
  - **Mask Length** – Indicates the length of the Sender IP Address ranging from 1 – 32
  - **Policy Action** – Indicates if the policy will be **Permitted** or **Denied**.
  - **Policy Action**: In the **Permit/Deny** field, use the pull down menu to select one of the following parameters:
    - **Deny** - This selection drops ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP**.
    - **Permit** - This selection allows ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP** to be processed by the switch.
- Note: You must enter a selection for **Deny/Permit** field even if the Profile Action ID that you have entered ignores both the **Replaced-DSCP** and **Replaced-CoS** fields.*
- **Rate Control Index**: The Rate Control Index is a unique number within the range of 1 - 65535. This field is mandatory and must match a Port List Index that has been previously entered on the **Policy Index**.
  - **Ingress Port List**: Select the interface for which you want to display data.

Policy Index:	<input type="text" value=""/>	(1-256)		
VLAN ID:	<input type="text" value=""/>	(1-4094)	802.1p Priority:	<input type="text" value=""/>
Source MAC Address:	<input type="text" value=""/>		MAC Address Mask:	<input type="text" value=""/>
ARP / RARP:	<input type="text" value="RARP"/>		Request / Reply:	<input type="text" value="Any"/>
Sender IP Address:	<input type="text" value=""/>		Mask Length:	<input type="text" value=""/>
Target IP Address:	<input type="text" value=""/>		Mask Length:	<input type="text" value=""/>
Policy Action:	<input type="text" value="Permit"/>		Rate Control Index:	<input type="text" value="None"/>
Ingress Port List:	<input type="text" value=""/>	(e.g. 1,3,5-8)		

### Add IPv4

To add an IPv4 policy, use the following procedure:

- Click **Add IPv4**, The **Policy Settings** page.
- Enter a number in the **Policy Index** field. The **Policy Index** is a unique number within the range of 1 – 256 which identifies the policy. This field is mandatory.

- Enter a number in the **VLAN ID** field. A unique number identifying a VLAN ranging from 1 to 4094.
- Enter a number in the **802.1p Priority** field. Enter the priority level of the frame ranging from 0 – 7.
- Choose the parameters to add for the policy, and enter data one or more of the parameters required for your policy. They are listed here:
  - **IP Protocol** – Select from the drop down menu the type of IP Protocol (**TCP, UDP, ICMP, Other or Any**) and fill in the unique number identifying the range of 1 – 255
  - **DSCP**: The DSCP (Differentiated Services Code Point) value in the IP header ranging from 0 - 63
  - **IPv4 Source IP Address** - Specifies the IPv4 Source IP address.
  - **Mask Length** – Indicates the length of the Sender IP Address ranging from 1 – 32
  - **IPv4 Destination IP Address** - Specifies the IPv4 Destination IP address.
  - **Mask Length** – Indicates the length of the Sender IP Address ranging from 1 – 32
  - **ICMP Type** – The ICMP (Internet Control Message Protocol) value ranging from 1 – 255
  - **ICMP Code** – The ICMP (Internet Control Message Protocol) value ranging from 1 – 255
  - **Source Layer 4 Port** – Indicates the source layer 4 port ranging from 1 – 65535
  - **Destination Layer 4 Port** – Indicates the destination layer 4 port ranging from 1 – 65535
  - **Policy Action**: In the **Permit/Deny** field, use the pull down menu to select one of the following parameters:
    - **Deny** - This selection drops ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP**.
    - **Permit** - This selection allows ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP** to be processed by the switch.

- **Policy Action**: In the **Permit/Deny** field, use the pull down menu to select one of the following parameters:
  - **Deny** - This selection drops ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP**.
  - **Permit** - This selection allows ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP** to be processed by the switch.
- Note:** You must enter a selection for **Deny/Permit** field even if the Profile Action ID that you have entered ignores both the **Replaced-DSCP** and **Replaced-CoS** fields.*
- **Rate Control Index**: The Rate Control Index is a unique number within the range of 1 - 65535. This field is mandatory and must match a Port List Index that has been previously entered on the **Policy Index**.
- **Ingress Port List**: Select the interface for which you want to display data.

Policy Index:	<input type="text" value=""/>	(1-256)		
VLAN ID:	<input type="text" value=""/>	(1-4094)	802.1p Priority:	<input type="text" value=""/>
			(0-7)	
IP Protocol:	ICMP ▾	<input type="text" value=""/>	DSCP:	<input type="text" value=""/>
		(1-255)		(0-63)
IPv4 Source IP Address:	<input type="text" value=""/>	.	<input type="text" value=""/>	.
	<input type="text" value=""/>	.	<input type="text" value=""/>	.
	<input type="text" value=""/>	.	<input type="text" value=""/>	<input type="text" value=""/>
Mask Length:	<input type="text" value=""/>			(1-32)
IPv4 Destination IP Address:	<input type="text" value=""/>	.	<input type="text" value=""/>	.
	<input type="text" value=""/>	.	<input type="text" value=""/>	.
	<input type="text" value=""/>	.	<input type="text" value=""/>	<input type="text" value=""/>
Mask Length:	<input type="text" value=""/>			(1-32)
ICMP Type:	<input type="text" value=""/>		ICMP Code:	<input type="text" value=""/>
	(1 - 255)			(1 - 255)
Source Layer 4 Port:	<input type="text" value=""/>		Destination Layer 4 Port:	<input type="text" value=""/>
	(1-65535)			(1-65535)
Policy Action:	Permit ▾		Rate Control Index:	None ▾
Ingress Port List:	<input type="text" value=""/> (e.g. 1,3,5-8)			

**Add IPv6**

To add an IPv6 policy, use the following procedure:

- Click **Add IPv6**, The **Policy Settings** page.
- Enter a number in the **Policy Index** field. The **Policy Index** is a unique number within the range of 1 – 256 which identifies the policy. This field is mandatory.
- Enter a number in the **VLAN ID** field. A unique number identifying a VLAN ranging from 1 to 4094.

- Enter a number in the **802.1q Priority** field. Enter the priority level of the frame ranging from 0 – 7.
- Choose the parameters to add for the policy, and enter data one or more of the parameters required for your policy. They are listed here:
  - **IP Protocol** – Select from the drop down menu the type of IP Protocol (**TCP, UDP, ICMP, Other or Any**) and fill in the unique number identifying the range of 1 – 255
  - **DSCP**: The DSCP (Differentiated Services Code Point) value in the IP header ranging from 0 – 63
  - **IPv6 Source IP Address** - Specifies the IPv6 Source IP address
  - **Prefix Length** - Indicates the length of the Source IP ranging from 1-32.
  - **ICMP Type** – The ICMP (Internet Control Message Protocol) value ranging from 1 – 255
  - **ICMP Code** – The ICMP (Internet Control Message Protocol) value ranging from 1 – 255
  - **Source Layer 4 Port** - Indicates the source layer 4 port ranging from 1 - 65535.
  - **Destination Layer 4 Port** - Indicates the destination layer 4 port ranging from 1 - 65535.
  - **Policy Action**: In the **Permit/Deny** field, use the pull down menu to select one of the following parameters:
    - **Deny** - This selection drops ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP**.
    - **Permit** - This selection allows ingress packets that conform to the specified **Replaced-CoS** or **Replaced-DSCP** to be processed by the switch.
  - Note:** You must enter a selection for **Deny/Permit** field even if the Profile Action ID that you have entered ignores both the **Replaced-DSCP** and **Replaced-CoS** fields.*
  - **Replaced-CoS**: Enter a number in the **Replaced-CoS** field ranging from 0 to 7. This field indicates the CoS level of interest. This field is not mandatory and you may elect to leave it blank
  - **Replaced-DSCP**: Enter a number in the **Replaced-DSCP** field within the range of 0 to 63. This field indicates the DSCP level of interest. This field is not mandatory and you may elect to leave it blank.

- **Rate Control Index**: The Rate Control Index is a unique number within the range of 1 - 65535. This field is mandatory and must match the **Rate Control Settings** page.
- **Ingress Port List**: Select the interface for which you want to display data.
- Click **Add** to add the policy to the Policy Table.

Policy Index:	<input type="text"/> (1-256)	802.1q Priority:	<input type="text"/> (0-7)
VLAN ID:	<input type="text"/> (1-4094)	DSCP:	<input type="text"/> (0-63)
IP Protocol:	ICMP <input type="text"/> (1-255)	Prefix Length:	<input type="text"/> (1-32, LSB only)
IPv6 Source IP Address:	<input type="text"/>	ICMP Code:	<input type="text"/> (1 - 255)
ICMP Type:	<input type="text"/> (1 - 255)	Destination Layer 4 Port:	<input type="text"/> (1-65535)
Source Layer 4 Port:	<input type="text"/> (1-65535)	Policy Action:	Permit <input type="text"/>
Ingress Port List:	<input type="text"/> (e.g. 1,3,5-8)		

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 of the entries in the table. 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.

**Policy Table** Delete All

Free Entries : 200

Total Entries : 0

Index	Classifier	Sequence	Deny/Permit	CoS	DSCP	Rate Control	Port List	St
<< Policy table is empty >>								

Page 0/0 First Page Previous Page Next Page Last Page Page  GO

4. Click **Save Settings to Flash** (menu).

Save Settings to Flash

5. Click **Save Settings to Flash (button)**, 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

### Configure Rate Control

Access Control Config > Rate Control

The Policy Settings page allows you to specify the filtering criteria for one policy. You can create, modify or delete a Policy by following the procedures in the following sections:

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Access Control Config** and click on **Rate Control Settings**.
3. Review the settings below for the rate control configuration table and click **Apply** after configuring the settings. After the new committed rate setting have been configured, they will take effect in the access control configuration policies.
  - **Index** – This is the index number reference used when configuring the access control configuration policy.
  - Enter a number in the **New Committed Rate** column ranging from 0 to 500000.

Rate Control Table		
Index	New Committed Rate	Current Committed Rate
1	10 pps ▾ x <input type="text"/> (0 - 500000)	10 pps
2	10 pps ▾ x <input type="text"/> (0 - 500000)	10 pps

4. Click **Save Settings to Flash (menu)**.

Save Settings to Flash

5. Click **Save Settings to Flash (button)**, 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

### RMON

The RMON (Remote Monitoring) MIB is used with SNMP applications to monitor the operations of network devices. The Switch supports the four RMON MIB groups listed here:

- **Statistic** group— This group is used to view port statistics remotely with SNMP programs.
- **History** group— This group is used to collect histories of port statistics to identify traffic trends or patterns.
- **Event** group— This group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed.
- **Alarm** group— This group is used to create alarms that trigger event log messages or SNMP traps when statistics thresholds are exceeded.

You can use your SNMP Network Management System (NMS) software and the RMON section of the MIB tree to view the RMON statistics, history and alarms associated with specific ports. Since RMON uses the SNMP agent for communicating with your NMS software, the SNMP Agent must be enabled and the SNMP feature must be configured on your switch. Since RMON works in conjunction with the SNMP agent, the SNMP agent must be enabled for the RMON feature to be active.

### Enable RMON

RMON > Global Settings

This section allows you to enable or disable RMON functionality.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **RMON** and click on **Global Settings**.

- Click the **RMON Status** drop-down list and select **Enabled** to enable RMON. Click **Apply** to save settings.

**RMON Global Settings**

RMON Status

- Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

- Click **Save Settings to Flash (button)**, 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**

### Configure parameters for RMON Ethernet statistics

RMON > Statistics

You can remotely view individual port statistics with RMON by using your SNMP NMS software and the RMON portion of the MIB tree.

- Log into your switch management page (see "[Access your switch management page](#)" on page 11).
- Click on **RMON** and click on **Statistics**.
- Review the settings.
  - Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
  - Port:** This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.

- Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

Click **Add** to add the entry to the table.

**Ethernet Statistics Settings**

Index:  \* (1-65535)

Port:  \*

Owner:  (32 characters limit)

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.

**Ethernet Statistics Table**

Index	Port	Drop Events	Octets	Packets	Broadcast Packets	Multicast Packets	Owner	Action
<< Table is empty >>								

Page 0/0     Page

- Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

- Click **Save Settings to Flash (button)**, 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**

### Configure parameters for RMON history control settings

RMON > History

RMON histories are snapshots of port statistics. They are taken by the switch at predefined intervals and can be used to identify trends or patterns in the numbers or types of ingress packets on the ports on the switch. The snapshots can be viewed with your SNMP NMS software with the history group of the RMON portion of the MIB tree.

A history group is divided into buckets. Each bucket stores one snapshot of statistics of a port. A group can have from 1 to 50 buckets. The more buckets in a group, the more snapshots it can store.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **RMON** and click on **History**.
3. Review the settings.
  - **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
  - **Port:** This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.
  - **Buckets Requested:** This parameter defines the number of snapshots of the statistics for the port. Each bucket can store one snapshot of RMON statistics. Different ports can have different numbers of buckets. The range is 1 to 50 buckets.
  - **Interval:** This parameter specifies how frequently the switch takes snapshots of the port's statistics. The range is 1 to 3600 seconds (1 hour). For example, if you want the switch to take one snapshot every minute on a port, you specify an interval of sixty seconds.
  - **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

Click **Add** to add the entry to the table.

History Control Settings	
Index:	<input type="text"/> * (1-65535)
Port:	<input type="text"/> *
Buckets Requested:	<input type="text"/> (1-50)
Interval:	<input type="text"/> (1-3600 secs)
Owner:	<input type="text"/> (32 characters limit)

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 of the entries in the table. 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.

History Control Table							Delete All
Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	Action	
<< Table is empty >>							
Page 0/0	First Page	Previous Page	Next Page	Last Page	Page <input type="text"/>	GO	

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

## Configure parameters for RMON alarms

### RMON > Alarms

RMON alarms are used to generate alert messages when packet activity on designated ports rises above or falls below specified threshold values. The alert messages can take the form of messages that are entered in the event log on the switch or traps that are sent to your SNMP NMS software or both.

RMON alarms consist of two thresholds. There is a rising threshold and a falling threshold. The alarm is triggered if the value of the monitored RMON statistic of the designated port exceeds the rising threshold. The response of the switch is to enter a message in the event log, send an SNMP trap, or both. The alarm is reset if the value of the monitored statistic drops below the falling threshold.

The frequency with which the switch samples the thresholds of an alarm against the actual RMON statistic is controlled by a time interval parameter. You can adjust this interval for each alarm.

Here are the three components that comprise RMON alarms:

- **RMON statistics group:** A port must have an RMON statistics group configured if it is to have an alarm. When you create an alarm, you specify the port to which it is to be assigned not by the port number, but rather by the ID number of the port's statistics group.
- **RMON event:** An event specifies the action of the Switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the Switch, send an SNMP trap to an SNMP workstation, or both. Since there are only three possible actions and since events can be used with more than one alarm, you probably will not create more than three events.
- **Alarm:** The last component is the alarm itself. It defines the port statistic to be monitored and the rising and falling thresholds that trigger the switch to perform an event. The thresholds of an alarm can have the same event or different events. The switch supports up to eight alarms.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **RMON** and click on **Alarm**.
3. Review the settings.
  - **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
  - **Interval:** This parameter specifies the time (in seconds) over which the data is sampled. Its range is 1 to 2147483647 seconds.
  - **Variable:** This parameter specifies the RMON MIB object that the event is monitoring.
  - **Sample type:** This parameter defines the type of change that has to occur to trigger the alarm on the monitored statistic. There are two choices from the pull-down menu - Delta value and Absolute value. Delta value- setting compares a threshold against the difference between the current and previous values of the statistic. Absolute value- setting compares a threshold against the current value of the statistic.
  - **Rising Threshold:** This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes greater than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647.
  - **Falling Threshold:** This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes less than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647.
  - **Rising Event Index:** This parameter specifies the event index for the rising threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in "Events".
  - **Falling Event Index:** This parameter specifies the event index for the falling threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in "Events".
  - **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

Click **Add** to add the entry to the table.

RMON Alarm Settings	
Index:	<input type="text"/> * (1-65535)
Interval:	<input type="text"/> (1-2^31-1 secs)
Variable:	<input type="text"/> *
Sample type:	Absolute value ▾
Rising Threshold:	<input type="text"/> * (0-2^31-1)
Falling Threshold:	<input type="text"/> * (0-2^31-1)
Rising Event Index:	<input type="text"/> (1-65535)
Falling Event Index:	<input type="text"/> (1-65535)
Owner:	<input type="text"/> (32 characters limit)

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 of the entries in the table. 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.

RMON Alarm Table <span style="float: right;">Delete All</span>									
Free Entries : 256									
Total Entries : 0									
Index	Interval	Variable	Sample Type	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Action
<< Table is empty >>									
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Page 0/0</span> <span>First Page</span> <span>Previous Page</span> <span>Next Page</span> <span>Last Page</span> <span>Page <input type="text"/></span> <span>GO</span> </div>									

4. Click **Save Settings to Flash** (menu).

5. Click **Save Settings to Flash** (button), 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 parameters for RMON events

RMON > Event

An event specifies the action of the switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP workstation, or both. Since there are only three possible actions and since events can be used with more than one alarm, you probably will not create more than three events - one for each of the three actions.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **RMON** and click on **Event**.
3. Review the settings.

- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Description:** This parameter specifies a text description of the event that you are configuring.
- **Type:** This parameter specifies where to log the event when it occurs. The choices are to log a message in the event log of the Switch, send an SNMP trap to the SNMP NMS software, or both.
- **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.



Click **Add** to add the entry to the table.

RMON Event Settings	
Index:	<input type="text"/> * (1-65535)
Description:	<input type="text"/> * (32 characters limit)
Type:	None ▼
Owner:	<input type="text"/> (32 characters limit)

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 of the entries in the table. 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.

RMON Event Table							Delete All
Free Entries : 256							
Total Entries : 0							
Index	Description	Type	Community	Owner	Last Time Sent	Action	
<< Table is empty >>							
Page 0/0	First Page	Previous Page	Next Page	Last Page	Page <input type="text"/>	GO	

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

## Voice VLAN

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

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

### CoS with Voice VLAN

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

### Organization Unique Identifier (OUI)

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

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

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

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

### Dynamic Auto-Detection vs Static Ports

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

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

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

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

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

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

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

### Create a Voice VLAN

Voice VLAN > 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 11).
2. Click on **Voice VLAN** and click on **Voice VLAN 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.
  - **Aging Time** - This parameter indicates the amount of time, in hours, after the last IP phone's OUI was received on a port, after which this

port will be removed from the voice VLAN. The range is 1 to 120 hours.

- **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.

### Voice VLAN Status

Voice VLAN:  Enabled  Disabled

Note: Disable will reset the settings to factory default and turn off the function.

---

### Voice VLAN Global Settings

VLAN ID:

Aging Time:  (1-120 hours)

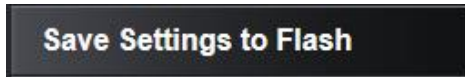
CoS:

- In the table at the bottom of the page, the voice VLAN **Auto- Detection** status is defined. From the **Auto-Detection** column, select one of the port rows and then one of the following choices from the pull-down menu:
  - **Ignore** - This parameter indicates that the setting in the **All** row does not apply to the **Dynamic Vlan Status** field. In other words, each port is set individually.
  - **Enable** - The voice VLAN **Auto-Detection** feature is activated for the port row selected.
  - **Disable** - The voice VLAN **Auto-Detection** feature is active for the port row selected.

**Note:** The voice VLAN Auto-Detection feature can only be enabled on "Not Member" ports of the voice VLAN. Member ports cannot have the voice VLAN Auto-Detection feature enabled. The **Status** column displays **Static** for the member ports

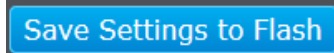
Voice VLAN Table			
Port	Auto Detection	Status	Action
All	Ignore	-	Apply
1	Disabled	None	Apply
2	Disabled	None	Apply

4. Click **Save Settings to Flash (menu)**.



5. Click **Save Settings to Flash (button)**, 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

Voice VLAN > Voice VLAN OUI Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Voice VLAN** and click on **Voice VLAN OUI Settings**.
3. Review the settings.

Use the following procedure to configure voice VLAN OUIs:

- 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 16 OUIs.

Voice VLAN OUI Settings		
	Description	Telephony OUI
User defined OUI:	<input type="text"/>	<input type="text"/> : <input type="text"/> : <input type="text"/> : 00 : 00 : 00 (XX:XX:XX:XX:XX:XX)
Note: 16 maximum user defined OUI allowed.		

**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.

Voice VLAN OUI Table				
ID	Description	Telephony OUI	OUI Mask	Action
<< Voice VLAN OUI List is empty >>				

4. Click **Save Settings to Flash (menu)**.
5. Click **Save Settings to Flash (button)**, 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.

**Security**

This chapter contains information about the Port-based security features and the procedures for setting this feature.

**Configure Port Access Control**

*Security > Port Access Control*

This section contains information and configuration procedures for the Port-based Access Control. Port-based Network Access Control (IEEE 802.1x) is used to control who can send traffic through and receive traffic from a switch port. With this feature, the switch does not allow an end node to send or receive traffic through a port until the user of the node logs on by entering a user name and password.

This feature can prevent an unauthorized individual from connecting a computer to a port or using an unattended workstation to access your network resources. Only those users to whom you have assigned a user name and password are able to use the switch to access the network.

This feature can be used with one of two authentication methods:

- The RADIUS authentication protocol requires that a remote RADIUS server is present on your network. The RADIUS server performs the authentication of the user name and password combinations.
- The Dial-in User (local) authentication method allows you to set up the authentication parameters internally in the switch without an external server. In this case, the user name and password combinations are entered in the associated with an optional VLAN when they are defined. Based on these entries, the authentication process is done locally by the Web Management Utility using a standard EAPOL transaction.

**Note:** RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Port Access Control**.

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

Configure the following parameters as required:

- **Port Access Control** – Select **Enabled** to enable port access control or **Disabled** to disable it. **Disabled** is selected by default.
- **Authentication Method** - This parameter indicates the authentication method used by the switch. Select one of the following choices:
  - **RADIUS:** This parameter configures port security for remote authentication. After completing steps, you must configure the “RADIUS Client” section.
  - **Local:** This parameter configures port security for local authentication. After completing steps, you must configure the parameters for “Dial-in User— Local Authentication” section.
  - **TACACS+:** This parameter configures port security for terminal authentication. After completing steps, you must configure the “TACACS+ Settings” section.
- **Re-authentication Status** – Select **Enabled / Disabled** for the re-authentication. **Default** is selected by default.
- **Re-authentication Period** – Input the duration of the re-authentication period from 1 – 3600 seconds.
- **VLAN Assignment** – Select **Enabled / Disabled** for VLAN Assignment
- **Guest VLAN Status** – Select **Enabled / Disabled** for Guest VLAN Status
- **Guest VLAN ID** – Input the VLAN ID for Guests in the range of 1 – 4094
- **Maximum Request** – Input the number of request that can be made in the range of 1 – 255.

Port Access Control Settings	
Port Access Control:	Enabled ▾
Authentication Method:	RADIUS ▾
Re-authentication Status:	Disabled ▾
Re-authentication Period:	3600 Sec. (1-3600)
VLAN Assignment:	Disabled ▾
Guest VLAN Status:	Disabled ▾
Guest VLAN ID:	1 (1-4094)
Maximum Request:	2 (1-255)

#### Configure Port Access Settings

*Security > Port Access Control*

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Security**, click on **Port Access Control** and click on **Settings** under **Port Access Control Settings**.

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

Configure the following parameters as required:

- **Port:** Select which port is needed for the Security setup
- **Port Control** – Select the type of control being used (**Auto, Force Authorized, Force Unauthorized**)
- **Authentication Mode** – Select which authentication method for each port (**802.1X, MAC Based**)
- **Supplicant Mode** – Select the supplicant mode (**Multiple, Single**)

Port Access Settings	
Port:	2 ▼
Port Control:	Force Unauthorized ▼
Authentication Mode:	802.1X ▼
Supplicant Mode:	Multiple ▼

4. To review your configured settings click on the **Configuration Status**

Current Settings Status						
802.1X Port Access:		Disabled				
Authentication Method:		RADIUS				
Port	Port Control	Auth Mode	Supplicant Mode	Auth Status	Authorized MAC Address	Dynamic VLAN List
1	Auto	802.1X	Single	disabled	N/A	
2	Force Unauthorized	N/A	N/A	disabled	N/A	
3	Force Authorized	N/A	N/A	disabled	N/A	

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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.

## Create Dial-In Users (Local Authentication Method)

Security > Dial-in User

Dial-in User feature provides the local authentication server for port security when a remote (RADIUS) server is not available.

The Dial-in User (local) authentication method allows you to set up 802.1x authentication parameters internally in the Switch. In this case, the user name and password combinations are entered with an optional VLAN when they are defined. Based on these entries, the authentication process of a supplicant is done locally by the Switch Management Utility using a standard EAPOL (EAP over LAN) transaction.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Dial-In User**.
3. Review the settings.

To create a dial-in user for local authentication, use the following procedure:

- In the **User Name** field, type a name for the user.
- In the **Password** field, type a password for the user.
- In the **Dynamic VLAN** field, enter the VID of the VLAN which you will allow the user to access. If you enter 0, this field will be ignored.

Click **Add** to add the entry to the table.

Dial-In User Settings	
User Name:	<input type="text"/> (Maximum length is 23)
Password:	<input type="password"/> (Maximum length is 23)
Dynamic VLAN:	<input type="text"/> (1-4094 for VLAN-ID or left blank to disable)

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 of the entries in the table. 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.

Dial-In User Table				Delete All
Free Entries : 64				
Total Entries : 0				
Username	Password	Dynamic VLAN	Action	
< < Dial-in user list is empty > >				
Page 0/0	First Page	Previous Page	Next Page	Last Page
		Page <input type="text"/>	GO	

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

**Add RADIUS Servers (RADIUS Authentication Method)**

Security &gt; RADIUS

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **RADIUS**.
3. Review the settings.
  - **Server Priority** – Enter the RADIUS Server priority (Highest: 1, Lowest: 5).
  - **Server IP Address** –Select IPv4 or IPv6 and set the RADIUS server IP address and enter the IP address of the RADIUS server you would like to add.
  - **Server Port (1 - 65535)** –Set the RADIUS authentic server(s) UDP port. The default port is 1812.
  - **Accounting Port (1 - 65535)** –Set the RADIUS account server(s) UDP port. The default port is 1813.
  - **Shared Secret** – Enter the default authentication and encryption key for RADIUS communication between the device and the RADIUS server.

Click **Add** to add the entry to the table.

RADIUS Settings	
Server Priority:	1 (Highest :1, Lowest :5)
Server IP Address:	0 . 0 . 0 . 0 <input type="radio"/> IPv4 <input type="text"/> <input type="radio"/> IPv6
Server Port:	1812 (1-65535)
Accounting Port:	1813 (1-65535)
Shared Secret:	<input type="text"/> (32 characters limit)

In the list, you can click **Modify** to modify an entry or click **Delete** or delete the entry.

RADIUS Table					
Server Priority	Server IP Address	Server Port	Accounting Port	Shared Secret	Action
< < Radius list is empty > >					

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**



### Add TACACS+ Servers (TACACS+ Authentication Method)

Security > TACACS+

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 5 TACACS+ servers.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server. The user-assigned TACACS+ parameters are applied to newly defined TACACS+ servers. If values are not defined, the system defaults are applied to the new TACACS+ servers.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **TACACS+**.
3. Review the settings.
  - **Server Priority** – Enter the TACACS+ Server priority (Highest: 1, Lowest: 5).
  - **Server IP Address** – Enter the TACACS+ Server IP address.
  - **Server Port** – Enter the port number via which the TACACS+ session occurs. The default port is port 49.
  - **Timeout** – Enter the amount of time (in seconds) the device waits for an answer from the TACACS+ server before retrying the query, or switching to the next server. Possible field values are 1-255. The default value is 5.
  - **Shared Secret** – Enter the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.

Click **Add** to add the entry to the table.

TACACS+ Settings	
Server Priority:	1 (Highest: 1, Lowest: 5)
Server IP Address:	0 . 0 . 0 . 0 <input type="radio"/> IPv4
	<input type="text"/> <input type="radio"/> IPv6
Server Port:	49 (1-65535)
Timeout:	5 (1-255 secs)
Shared Secret:	<input type="text"/> (32 characters limit)

In the list, you can click **Modify** to modify an entry or click **Delete** or delete the entry.

TACACS+ Table					
Server Priority	Server IP Address	Server Port	Timeout	Shared Secret	Action
< < TACACS+ list is empty > >					

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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**

**Destination MAC Filter***Security > Destination MAC Filter*

This section contains an explanation of the Destination MAC Filter feature as well a procedure for configuring it. This section includes the following information:

The Destination MAC Filter feature prevents the switch from forwarding packets to a specified device. On the Destination MAC Filter Page of the Web Management Utility software, enter the MAC address of the device that you want to filter.

After the switch receives a packet, it examines the destination MAC address of the packet. If the destination MAC address matches a MAC address set in the filter, the software prevents the switch from forwarding it and drops the packet.

You may want to block access to a device within your organization. For instance, you may not want users on the Sales group switch to have access to a server on the Accounting group switch. You can enter the MAC address of the Accounting server as a destination MAC address filter on the Sales group switch. When a packet destined for the Accounting server is received by the Sales group switch, the switch drops the packet. The Destination MAC Filter is a subset of the static MAC address.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Destination MAC Filter**.

**Add Destination MAC Filter**

MAC Address :  :  :  :  :  :   
 (e.g. 00:11:ab:cd:ef:22)

3. Enter the **MAC Address** to add to the destination filter table. Click **Add**.

4. The MAC address will be added to the table.

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 of the entries in the table. 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.

Destination MAC Table <span style="float: right;">Delete All</span>	
Free Entries : 40	
MAC Address	Action
< < Destination MAC Filter is empty > >	

5. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

6. Click **Save Settings to Flash (button)**, 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**

## Denial of Service (DoS)

Security > Denial of Service

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

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Denial of Service**.

DoS Setting	
TCP Null Scan: TCP flag bits are zero	Allow ▾
TCP over MAC Multicast / Broadcast	Allow ▾
TCP Flags with FIN-URG-PSH	Allow ▾
TCP Flags with SYN-RST	Allow ▾
TCP/UDP port is zero	Allow ▾
Fragmented ICMP v4	Allow ▾
ARP MAC SA Mismatch (Src-MAC and Sender MAC of ARP Payload)	Allow ▾

3. Next to the DoS item/rule you would like to activate, click the drop-down menu on the right hand side and select **Deny**.

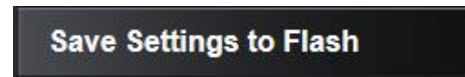


4. Click **Apply** to save the settings.

**Note:** You can click "Reset to Default" to restore all DoS settings to Allow.



5. Click **Save Settings to Flash** (menu).



6. Click **Save Settings to Flash** (button), 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.



**ARP Inspection***Security > ARP Inspection*

This section allows you to create ARP inspection policies for security purposes. The ARP inspection can be set to permit or deny the host based VLAN & port assignment. When ARP inspection is enabled on a specific VLAN or port, the ARP entry must be defined specifically within the ARP inspection static entry table.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security, ARP Inspection**, and click on **Basic Settings**.
3. Review the settings below.

- **Global State:** Selecting Enabled enables the ARP inspection feature on the switch.

### ARP Inspection Global Settings

Global State : Enabled ▼

- **ARP Inspection VLAN Settings** – This will allow you to apply ARP inspection settings to a specific VLAN ID. Click **Add** to add the VLAN to the ARP inspection table.
  - **VLAN ID** – Enter the VLAN ID to apply ARP Inspection.
  - **Log Type** – The log type will define which types of audits to include in the switch system log, permitted ARP entries, denied ARP entries, both permitted & denied (All), or no log entries (None).

### ARP Inspection VLAN Settings

VLAN ID:            (1-4094)

Log Type: None ▼

Click on **Security, ARP Inspection**, and click on **Port Settings**.

Review the settings below and click **Apply** when configuration is completed.

- **State:** Enables ARP inspection on a specific port.
- **Log Type** - The log type will define which types of audits to include in the switch system log, permitted ARP entries, denied ARP entries, both permitted & denied (All), or no log entries (None).
- **Follow VLAN Log Type:** This will follow the VLAN Log Type defined under Security > ARP Inspection > Basic Settings section depending on port VLAN membership and if it has been defined in the table. If no VLAN is match, there will be no logged.

ARP Inspection Port Settings				
Port	State	Log Type	Follow VLAN Log Type	Action
All	Ignore ▼	Ignore ▼	Ignore ▼	<span style="background-color: #007bff; color: white; padding: 2px 5px;">Apply</span>

Click on **Security, ARP Inspection**, and click on **Static Entry Table**.

This section will allow you manually entry static ARP entries.

Enter the VLAN ID, IP address, MAC address and port and click **Add** to add the static ARP entry to the list.

### Add New Static Entry

VLAN ID:            (1-4094)

IPv4 unicast address : . . . .

MAC Address:  : : : : :

---

#### Port Settings

1	2	3	4	5	6	7	8	9	10
●	●	●	●	●	●	●	●	●	●

You can also check the Dynamic Entry Table, and add all dynamic entries discovered to the Static Entry Table list.

**Port Security Control**

Security > Port Security Control

The port security feature allows you to add additional security to your switch by limited the number of MAC addresses learned by each port.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security, Port Security**, and click on **Basic Settings**.
3. Review the settings below and click **Apply** after configuration is completed.
  - **Aging State:** This feature is not required for port security to work but if enabled will allow learned MAC addresses to be deleted after a specific time interval. This will allow the port to learn new MAC addresses in place of the inactive MAC address learned prior.
  - **Aging Time:** The amount of time specified before inactive MAC addresses are deleted from learned MAC address table per port.

Port Security Basic Settings	
Aging State :	Disabled ▾
Aging Time:	3600 (10 - 10000000 seconds)
Hold Time:	300 (10 - 10000000 seconds)

- Click on **Security, Port Security**, and click on **Port Settings**.  
 Review the settings below and click **Apply** when configuration is completed.

- **State:** Enables or disables port security on a specific port..
- **Maximum Allowed** – This number is the maximum number of MAC addresses that can be learned allowed by a specific port before applying the Violation Action/port state.
- **Maximum Violation** – This number is the maximum number of violations that will be allowed before applying the Violation Action/port state.

- **Violation Action** - The resulting action when the maximum allowed violations is reached per port.
  - **Protect** – Drop packets with unknown source addresses until a sufficient number of secure MAC addresses is removed below the maximum value allowed. (Requires aging time)
  - **Restrict** – Drop packets with unknown source addresses until a sufficient number of secure MAC addresses is removed below the maximum value allowed. (Requires aging time)
  - **Shutdown** – Shuts down the port immediately.

Port Security Port Settings					
Port	State	Maximum Allowed (0 - 64)	Maximum Violation (1 - 64)	Violation Action	Action
All	Ignore ▾	0	1	Ignore ▾	Apply
1	Disable ▾	4	4	Protect ▾	Apply
2	Disable ▾	4	4	Protect ▾	Apply

## DHCP Snooping

Here is a summary of the rules to observe when you configure DHCP Snooping:

- A trusted port is connected to one of the following:
  - Directly to the legitimate trusted DHCP Server.
  - A network device relaying DHCP messages to and from a trusted server.
  - Another trusted source such as a switch with DHCP Snooping enabled.
  - Untrusted ports are connected to DHCP clients and to traffic that originates outside of the local area network.
- The VLANs to which the DHCP Snooping feature applies must be specified in the DHCP Snooping VLAN Setting configuration.
- Any static IP addresses on the network must be manually added to the Binding Database.

### Enable DHCP Snooping

DHCP > DHCP Snooping > General Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP Snooping** and click on **General Settings**.
3. Review the settings. Click **Apply** to save the settings.
  - **DHCP Snooping** - Select one of the following radio button choices:
    - **Enabled** - This parameter activates the DHCP Snooping feature.
    - **Disabled** - This parameter de-activates the DHCP Snooping

### DHCP Snooping Global Settings

DHCP Snooping:

Enabled  Disabled

4. Click **Save Settings to Flash (menu)**.

Save Settings to Flash

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

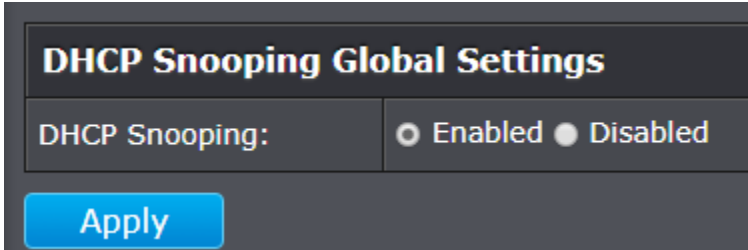
**Note:** This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.

Save Settings to Flash

**Enable DHCP Snooping***DHCP Snooping > VLAN Settings*

In this section, you can enable DHCP Snooping.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP Snooping** and click on **General Settings**.
3. Select **Enabled** to enable DHCP Snooping.



4. Click **Save Settings to Flash (menu)**.
5. Click **Save Settings to Flash (button)**, 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 Trusted Interfaces***DHCP > DHCP Snooping > Trusted Interfaces*

This section allows you to set trusted port interfaces where DHCP servers can be connected allows or denies DHCP server information to be received on those ports.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **DHCP Snooping** and click on **Trusted Interfaces**.

3. Below each port, click the **Check** each port to enable the port as being trusted with the DHCP Snooping feature. To define a port as untrusted for DHCP Snooping, uncheck the box.

**Note:** You can select the row labeled **ALL** to apply settings to all ports.

Trusted Interfaces Settings										
	1	2	3	4	5	6	7	8	9	10
All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

4. Click **Save Settings to Flash (menu)**.

5. Click **Save Settings to Flash (button)**, 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.

## DHCP Server

A DHCP (Dynamic Host Configuration) Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. This relies on DHCP to respond to broadcast queries by clients. DHCP server automatically sends the required network parameters for clients to properly communicate on a network.

### Enable DHCP Server

DHCP > DHCP Server > General Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP**, then click on **DHCP Server**, and click on **General Settings**.
3. Click **Enabled** to enable DHCP Server.

4. Click **Apply** to save the settings.
5. Click **Save Settings to Flash (button)**, 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

## DHCP VLAN Settings

DHCP > DHCP Server > VLAN Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP**, then click on **DHCP Server**, and click on **VLAN Settings**.
3. Input the VLAN numerical value into the field within the range of 1 – 4094.  
**Note:** VLAN needs to be setup first before proceeding with DHCP VLAN.

4. Click **Apply** to save the settings.
5. Click **Save Settings to Flash (button)**, 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

## DHCP Exclude IP Address

DHCP > DHCP Server > Exclude IP Address

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP**, then click on **DHCP Server**, and click on **Exclude IP Address**.
3. Review the settings. Click Add to add the database entry to the table.
  - **Start IP Address:** Enter the starting IP address to exclude from the DHCP server range.



- **End IP Address:** Enter the ending IP address to be excluded from the DHCP server range.

Excluded IP Range Settings							
Start IP Address:	192	.	168	.	10	.	55
End IP Address:	192	.	168	.	10	.	65

In the list, you can **View** an entry or click **Delete** or delete the entry. You can also click **Delete All** to delete all of the entries in the table. 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.

Exclude IP Address Table			Delete All
Start IP Address	End IP Address	Action	
192.168.10.55	192.168.10.65	Delete	

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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.

**DHCP Pool**

DHCP &gt; DHCP Server &gt; Pool


1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP**, then click on **DHCP Server**, and click on **Pool**.
3. Review the settings. Click Add to add the database entry to the table.
  - **Pool Name:** This is used to identify the pool name. The identifier is limited to 16 characters.
  - **IP Address:** Enter the IP address of the DHCP Pool.
  - **Subnet Mast:** Enter the subnet Mask
  - **Default Gateway:** Enter the IP Address of your default gateway.
  - **DNS Server:** Enter the IP address of your DNS server
  - **Lease Time:** Enter the lease time in days, hours, and minutes.

Pool Settings	
Pool Name:	<input type="text"/> (16 characters limit)
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Gateway:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
DNS Server:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Lease Time:	<input type="text"/> : <input type="text"/> : <input type="text"/> (DD:HH:MM)

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 of the entries in the table. 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.

Pool Table					Delete All
Pool Name	IP/Subnet Mask	Default Gateway	DNS Server	Lease Time	Action
trendnet	192.168.10.55/255.255.255.0	0.0.0.0	0.0.0.0	1d0h0m	<a href="#">Modify</a> <a href="#">Delete</a>

4. Click **Save Settings to Flash (menu)**.



5. Click **Save Settings to Flash (button)**, 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.

**DHCP Relay**

A DHCP (Dynamic Host Configuration) Relay allows any host to forward DHCP packets between clients and servers. This allows agents to forward requests and replies between clients and servers when they are not on the same subnet.

**DHCP Relay General Settings**

DHCP &gt; DHCP Relay &gt; General Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **DHCP**, then click on **DHCP Relay**, and click on **General Settings**.
3. Review the settings. Click Apply to save the settings.
  - **DHCP Relay** – Click on **Enabled** or **Disabled** to turn on or turn off DHCP Relay.
  - **Relay Server Address** – Input the IP address of the Relay Server.
  - **Option 82** – Select one of the following choices the menu.
    - **Enabled** – Allows an Option 82 packet to be passed through the switch without being altered
    - **Disabled** – Blocks an Option 82 packet from passing through the switch
  - **Option 82 Policy** – Select one of the following choices from the menu

- **Replace** – Replaces the packet when an Option 82 packet is passed through the switch
- **Keep** – Keeps the Option 82 packet when it passed through the switch
- **Drop** – Drops the Option 82 packet when it is passed through the switch

DHCP Relay Global Settings	
DHCP Relay:	<input type="radio"/> Enabled <input type="radio"/> Disabled
Relay Server Address:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Option 82:	<input type="radio"/> Enabled <input type="radio"/> Disabled
Option 82 Policy:	<input type="radio"/> Replace <input type="radio"/> Keep <input type="radio"/> Drop

4. Click **Save Settings to Flash (menu)**.

**Save Settings to Flash**

5. Click **Save Settings to Flash (button)**, 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.

## LLDP (Link-Layer Discovery Protocol)

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

### Enable and configure LLDP

LLDP > LLDP Global Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **LLDP** and click on **LLDP Global Settings**.

3. Review the settings.

### Enabling or Disabling LLDP

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

LLDP Global Settings	
LLDP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

### Configure the LLDP Settings

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

**Message TX Interval:** Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements. The range is from 5 to 32762 seconds.

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

**LLDP TX Delay:** Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The range is from 1 to 8192 seconds.

Click **Apply** to save the settings.

LLDP Settings	
Message TX Hold Multiplier	<input type="text" value="4"/> (2-10)
Message TX Interval	<input type="text" value="30"/> sec. (5-32768)
LLDP Reinit Delay	<input type="text" value="2"/> sec. (1-10)
LLDP TX Delay	<input type="text" value="2"/> sec. (1-8192)

Note : (LLDP TX Delay) <= (0.25\* (Message TX Interval)) and (Message TX Interval) \* (Message TX Hold Multiplier) < 65535.

#### View LLDP System Information

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

LLDP System Information	
Chassis ID Subtype:	macAddress
Chassis ID:	00:01:02:03:04:05
System Name:	
System Description:	

#### Set LLDP Port State

For each port, click the **State** drop-down list and choose from the following options.

- **Disabled:** Indicates LLDP is disabled on the port. The port cannot receive or transmit LLDP data packets.
- **Enabled:** Indicates LLDP is enabled on the port. The port can receive and transmit LLDP data packets.
- **RxOnly:** Indicates LLDP is enabled on the port. The port can receive LLDP data packets.
- **TxOnly:** Indicates LLDP is enabled on the port. The port can transmit LLDP data packets.

**Note:** You can select the row labeled **ALL** to apply settings to all ports.

Click **Apply** to save the settings.

LLDP Port State Settings		
Port	State	Action
All	<input type="text" value="Disabled"/>	<input type="button" value="Apply"/>
1	<input type="text" value="RxTx"/>	<input type="button" value="Apply"/>
2	<input type="text" value="RxTx"/>	<input type="button" value="Apply"/>

4. Click **Save Settings to Flash** (menu).

**Save Settings to Flash**

5. Click **Save Settings to Flash** (button), 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**

**View LLDP Neighbor Information***LLDP > LLDP Neighbor Information*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **LLDP** and click on **LLDP Neighbor Information**.
3. View the LLDP neighbor information.
  - **Entity:** This parameter is a number assigned to the reporting neighbors in the order that the LLDP information is received from them.
  - **Port:** This parameter specifies the TEG-30102WS local port number where the LLDP information was received.
  - **Chassis ID Subtype:** This parameter describes the Chassis ID subtype of the neighboring network device which is reporting the LLDP information.
  - **Chassis ID:** This parameter is the neighboring device's chassis ID.
  - **Port ID Subtype:** This parameter describes the Port ID subtype of the neighboring network device's port that is connected directly to the TEG-30102WS switch port.
  - **Port ID:** This parameter specifies the neighboring network device's port number from which the LLDP information was transmitted.
  - **Port Description:** This parameter describes the neighboring network device's port.
  - **Show Description:** If you click on this button, a detailed report of the neighboring network device will be displayed.

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.

LLDP Neighbors Information							
Entity	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Normal
Page 0/0 <a href="#">First Page</a> <a href="#">Previous Page</a> <a href="#">Next Page</a> <a href="#">Last Page</a> Page <input type="text"/> <a href="#">GO</a>							

**Statistic**

Statistics provide important information for troubleshooting switch problems at the port level. The Web Management Utility provides a two statistics charts, including Traffic Information and Error Information.

**View Traffic Information Statistics***Statistic > Traffic Information*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Statistic** and click on **Traffic Information**.
3. View the Traffic Information Statistics.
  - **InOctets:** Inbound Octets (Bytes/s), number of inbound octet bits in bytes per second.
  - **InUcastPkts:** Inbound Unicast Packets (Pkts), number of inbound unicast packets in packets per second.
  - **InNUcastPkts:** Inbound Non-unicast Packets (Pkts), number of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
  - **InDiscards:** Inbound Discards (Pkts), number of inbound discarded packets in packets per second.
  - **OutOctets:** Outbound Octets (Bytes/s), rate of outbound octet bits in bytes per second.
  - **OutUcastPkts:** Outbound Unicast Packets (Pkts), number of outbound unicast packets in packets per second.
  - **OutNUcastPkts:** Outbound Non-unicast Packets (Pkts), number of outbound non-unicast (such as broadcast and multicast packets) packets.
  - **OutDiscards:** Outbound Discards (Pkts), number of outbound discarded packets.

**Traffic Information**

Port ID	InOctets	InUcastPkts	InNUcastPkts	InDiscards	OutOctets	OutUcastPkts
All	-	-	-	-	-	-
1	5321840	43919	2720	0	21995888	47105
2	5298680	43693	2721	0	22037654	46883
3	5361571	44230	2794	0	22558152	47532

**View Error Information Statistics**

*Statistic > Error Information*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Statistic** and click on **Traffic Information**.
3. View the Error Information Statistics.
  - **InErrors:** Inbound Errors (Pkts), number of inbound errors in packets per second.
  - **OutErrors:** Outbound Errors (Pkts), number of outbound error packets.
  - **DropEvents:** Drop Events, number of packets dropped.
  - **CRCAAlignErrors:** CRC and Align Errors, number of CRC and Align errors that have occurred.
  - **UndersizePkts:** Undersize Packets (Pkts), number of undersized packets (less than 64 octets) received.
  - **OversizePkts:** Oversize Packets (Pkts), number of oversized packets (over 2000 octets) received.
  - **Fragments:** Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
  - **Collisions:** Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.

**Error Information**

Port ID	InErrors	OutErrors	DropEvents	CRCAAlignErrors	UndersizePkts	OversizePkts	Fr
All	-	-	-	-	-	-	
1	0	0	0	0	0	0	
2	0	0	0	0	0	0	
3	0	0	0	0	0	0	

## 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 router, 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

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Tools**, click on **Firmware Upgrade**, and click **via HTTP**.
3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.

Firmware Upgrade via HTTP Settings	
Image Version:	1.00.16
Firmware File:	<input type="button" value="Choose File"/> No file chosen
Note: System will reset automatically after burning image to flash.	

4. Navigate to the folder on your computer where the unzipped firmware file (.hex) is located and select it.
5. Click **Apply**. If prompted, click **Yes** or **OK**.

Firmware Upgrade via TFTP Settings

Note: Before using this method, you will require a TFTP server. There are third party TFTP server applications available for this function. If you are not familiar with the TFTP protocol, it is recommended to use the HTTP method.

- 1. Log into your switch management page (see "Access your switch management page" on page 11).
2. Click on Tools, click on Firmware Upgrade, and click via TFTP.
3. Make sure your TFTP server is running and note the IP address of your server and firmware file name. The TFTP server should be in the same IP subnet as the switch.
Note: It is recommended to that the firmware file (.hex) is placed in your TFTP server root directory.
4. Review the settings. Click Apply to start the firmware upgrade.
- TFTP Server IP: Enter the IP address of your TFTP server.
- Image File Name: Enter the firmware filename with extension. (.hex)
- Retry Count: Defined the number of time to attempt to pull the firmware file from the TFTP server.

5. Click Apply to start the firmware upgrade.

Form titled 'Firmware Upgrade via TFTP Settings' with fields for Image Version (1.00.10), TFTP Server IP (IPv4/IPv6), Image File Name (64 characters max.), and Retry Count (3). Includes a note: 'Note: System will reset automatically after burning image to flash.'

Backup and restore your switch configuration settings

Tools > Config File 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.

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 11).
2. Click on Tools, click on Configuration File Backup/Restore, and click on via HTTP.
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 11).
2. Click on Tools, click on Configuration File Backup/Restore, and click on via HTTP.
3. Next to Select File, depending on your web browser, click on Browse or Choose File.

Form titled 'File Backup/Restore via HTTP Settings' with a Select File field and a Browse... button. Includes Backup and Restore buttons.

- 4. A separate file navigation window should open.
5. Select the router 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.



### Backup/Restore via TFTP Settings

**Note:** Before using this method, you will require a TFTP server. There are third party TFTP server applications available for this function. If you are not familiar with the TFTP protocol, it is recommended to use the HTTP method.

#### To backup your switch configuration:

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Tools**, click on **Configuration File Backup/Restore**, and click on **via TFTP**.
3. Make sure your TFTP server is running and note the IP address of your server and firmware file name. The TFTP server should be in the same IP subnet as the switch.
4. Review the settings. Click **Backup** to save the configuration file (config.bin) to your local hard drive on your TFTP server root directory.
  - **TFTP Server IP:** Enter the IP address of your TFTP server.
  - **Config File Name:** Enter the configuration file name for the backup. (Default: config.bin)

#### Config File Backup/Restore via TFTP Settings

TFTP Server IP:	<input style="width: 100%;" type="text" value=" . . . ."/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Config File Name:	<input style="width: 100%;" type="text"/> (64 characters max.)

Backup
Restore

#### To restore your switch configuration:

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Tools**, click on **Configuration File Backup/Restore**, and click on **via HTTP**.
3. Make sure your TFTP server is running and note the IP address of your server and configuration file name. The TFTP server should be in the same IP subnet as the switch.
 

**Note:** It is recommended to put the configuration file (config.bin) is placed in your TFTP server root directory.
4. Review the settings. Click **Restore** to restore the switch configuration file (config.bin) from your local hard drive from your TFTP server root directory.
  - **TFTP Server IP:** Enter the IP address of your TFTP server.
  - **Config File Name:** Enter the configuration file name to restore. (Default: config.bin)

#### Config File Backup/Restore via TFTP Settings

TFTP Server IP:	<input style="width: 100%;" type="text" value=" . . . ."/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Config File Name:	<input style="width: 100%;" type="text"/> (64 characters max.)

Backup
Restore

5. Wait for the switch to restore settings.

## Cable Diagnostics Test

Tools > Cable 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 11).

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

Cable Diagnostics Settings	
Port	1 ▾

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

Cable Diagnostics Table		
Port	Test Result	Cable Distance (meters)
1	Pair1:OK	Pair1.2
	Pair2:OK	Pair2.2
	Pair3:OK	Pair3.2
	Pair4:OK	Pair4.2

- **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 Distance:** This parameter specifies the length of the cable connected to the switch port.

## 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 router 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 5-9 seconds and release.
- **Software Method (Switch Management Page):**

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
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:

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

### To reset your switch to factory defaults:

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "[Backup and restore your router configuration settings](#)" on page 44.

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

- **Hardware Method:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button more than 10 seconds and release. Located on the front panel of your switch, see "[Product Hardware Features](#)" on page 6. 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 11).
  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.

**Reboot**

Reboot Type:

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

The switch factory default settings are below.

<b>Administrator User Name</b>	admin
<b>Administrator Password</b>	admin
<b>Switch IP Address</b>	192.168.10.200
<b>Switch Subnet Mask</b>	255.255.255.0

## Network Connectivity Test (Ping Tool)

### Tools > Ping

This chapter provides the procedure to ping a node on your network from the switch. This procedure is useful in determining whether an active link exists between the switch and another network device.

The device you are pinging must be a member of the Default VLAN and within the same local area network as your switch. In other words, the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Tools** and click on **Ping**.
3. Review the settings. Click **Start** to start the network connectivity ping test. After the ping test is activate, you can click **Show Ping Results** to check the ping test result.

**Destination IP Address** - The IP address of the node you want to ping in the IPv4 or IPv6 format.

- **Timeout Value** - Specifies the length of time, in seconds, the switch waits for a response before assuming that a ping has failed.
- **Number of Ping Requests** - Specifies the number of ping requests you want the switch to perform.

Ping Test Settings	
Destination IP Address:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> <input checked="" type="radio"/> IPv4 <input type="text" value=""/> <input type="radio"/> IPv6
Timeout Value:	<input type="text" value="3"/> Sec. (1-5)
Number of Ping Requests:	<input type="text" value="10"/> Times (1-10)

## Technical Specifications

Hardware	
<b>Standards</b>	IEEE 802.1d, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3bz
<b>Device Interface</b>	8 x 2.5GBASE-T ports (100Mbps/1Gbps/2.5Gbps) 2 x 10G SFP+ slots (1Gbps/10Gbps) 1 x RJ-45 console port LED indicators Reset button
<b>Data Transfer Rate</b>	Fast Ethernet: 100Mbps (half duplex), 200Mbps (full duplex) Gigabit Ethernet: 2000Mbps (full duplex) 2.5 Gigabit Ethernet: 5Gbps (full duplex) 10 Gigabit Ethernet: 20Gbps (full duplex)
<b>Performance</b>	Switch fabric: 80Gbps RAM buffer: 2MB MAC address table: 32K entries Jumbo frames: 9KB Forwarding mode: store and forward Forwarding rate: 59.5Mpps (64-byte packet size)
<b>Management</b>	CLI (Console / Telnet / SSHv2) for IP address settings and password configuration only HTTP / HTTPS (SSL v2/3 TLS 1.2) web based GUI SNMP v1, v2c, v3 SNMP trap (Up to 4 receivers) RMON groups 1/2/3/9 Cable diagnostic test Static unicast entries LLDP IPv6 neighbor discovery, IPv6 static IP, and DHCPv6
<b>MIB</b>	MIB II RFC 1213

	Bridge MIB IEEE8021-Q RMON (Group 1,2,3,9) RFC 2819 Interface group MIB using SMIv2 RFC 2863 Multicast group membership discovery MIB RFC 5519 SNMP management frameworks RFC 3411 User-based security model for SNMPv3 RFC 3414 View-based access control model for SNMP RFC 3415 Ethernet-like MIB RFC 3635 802.3 MAU MIB RFC 3636 Entity MIB v3 RFC 4133 Bridge MIB RFC 4188 IP MIB RFC 4293 RADIUS authentication client MIB RFC 4668 RADIUS accounting MIB RFC 4670 LLDP-MIB IEEE802.1AB PAE MIB IEEE802.1X
<b>Spanning Tree</b>	IEEE 802.1D STP (spanning tree protocol) IEEE 802.1w RSTP (rapid spanning tree protocol) IEEE 802.1s MSTP (multiple spanning tree protocol)
<b>Link Aggregation</b>	Static link aggregation and 802.3ad dynamic LACP (Up to 4 groups)
<b>Quality of Service (QoS)</b>	802.1p Class of service (CoS) DSCP (Differentiated Services Code Point) Bandwidth control per port Queue Scheduling: strict priority (SP), deficit weighted round robin (DWRR)
<b>VLAN</b>	Multiple management VLAN assignment Asymmetric VLAN 802.1Q tagged VLAN Up to 32 VLAN groups, ID range 1-4094 Private VLAN Voice VLAN (16 user defined OUIs)

<b>Multicast</b>	IGMP snooping v1, v2, v3 IGMP fast leave Static multicast entries MLD Snooping v1, v2 Up to 1K multicast groups
<b>Port Mirror</b>	One to one Many to one
<b>Storm Control</b>	Broadcast (Min. limit: 10pps) Multicast (Min. limit: 10pps) Destination lookup failure (Min. limit: 10pps)
<b>Access Control</b>	802.1X port-based network access control MAC-based authentication RADIUS (Up to 5 servers) TACACS+ (Up to 5 servers) Local dial in user authentication DHCP IPv4 snooping Duplicated address detection Loopback detection Head-of-line (HoL) blocking prevention Denial of service (DoS) prevention Trusted Host/IP Access List Port Security/MAC address learning restriction (Up to 64 entries per port) Destination MAC filter Static/dynamic ARP inspection
<b>ACL IPv4 &amp; IPv6</b>	MAC address VLAN ID ARP/RARP EtherType ICMP type 1-255

	IP protocol 1-255 TCP/UDP port 1-65535 802.1p DSCP IPv4/IPv6 address Up to 256 entries
<b>Layer 3 Features</b>	IPv4 / IPv6 static routing IP interfaces: Up to 8 Routing table entries: Up to 32 (IPv4 / IPv6) ARP table (up to 1024 entries) DHCP server, relay, option 82 Inter-VLAN routing
<b>Power</b>	Input: 100 – 240V AC, 50/60 Hz Max. Consumption: 27.36W (No PoE load)
<b>Smart Fan / Acoustics</b>	Quantity: 2 (Hot swappable) Noise Level: 41.7 dBA (max.)
<b>MTBF</b>	446,704
<b>Operating Temperature</b>	0° – 50° C (32° – 122° F)
<b>Operating Humidity</b>	Max. 80% non-condensing
<b>Dimensions</b>	330 x 230 x 44.45mm (13 x 9.1 x 1.75 in.) Rack mountable 1U height
<b>Weight</b>	2.33 kg (5.12 lbs.)
<b>Certifications</b>	CE FCC UL

## Troubleshooting

**Q:** I typed <http://192.168.10.200> in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the switch management page?

**Answer:**

1. Check your hardware settings again. See "[Switch Installation](#)" on page 8.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to [Use the following IP address](#) or [Static IP](#)(see the steps below).
4. Make sure your computer is connected to one of the Ethernet switch ports.
5. Since the switch default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

### Windows 7

- 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 15 seconds.

The default IP address of the switch is 192.168.10.200. The default user name and password is "admin".

## Appendix

### How to find your IP address?

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

#### Command Prompt Method

##### **Windows 2000/XP/Vista/7/8/8.1/10**

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 7/8/8.1/10**

- 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.



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,

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.

### Federal Communication Commission Interference Statement

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

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

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

This device complies with Part 15 of the 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.



#### IMPORTANT NOTE:

##### Radiation Exposure Statement:

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

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

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

### RoHS

This product is RoHS compliant.



### Europe – EU Declaration of Conformity

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

- EN60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011 + A2: 2013
- EN 55032: 2012 + AC: 2013 Class A (CISPR32: 2012)
- EN 55024: 2010
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013
- AS/NZS CISPR 32: 2013



#### Directives:

Low Voltage Directive 2014/35/EU

EMC Directive EN 2014/30/EU

RoHS Directive 2011/65/EU

WEEE Directive 2012/19/EU

REACH Regulation (EC) No. 1907/2006

#### CE Mark Warning

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

## Limited Warranty

---

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

### Limited Warranty

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

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

### Limited Lifetime Warranty

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

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

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

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

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

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

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

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

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

shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

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

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

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, 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

2018/03/30



## 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