

User's Guide

TRENDNET®



8-Port Gigabit Web Smart Switch

TEG-082WS

Contents

PRODUCT OVERVIEW	2	INSTALLATION.....	102
FEATURES.....	2	USING THE UTILITY.....	103
FRONT VIEW.....	3	DISCOVERY LIST.....	104
LED INDICATORS.....	3	DEVICE SETTING.....	105
REAR VIEW	5	MAIN MENU OPTIONS	106
PACKAGE CONTENTS.....	5	TECHNICAL SPECIFICATIONS	108
SWITCH INSTALLATION.....	5	TROUBLESHOOTING.....	110
DESKTOP HARDWARE INSTALLATION.....	5	APPENDIX.....	111
RACK MOUNT HARDWARE INSTALLATION.....	6	HOW TO FIND YOUR IP ADDRESS?	111
BASIC INSTALLATION	6	HOW TO FIND YOUR MAC ADDRESS?	118
CONNECT ADDITIONAL DEVICES TO YOUR SWITCH.....	8	REGULATIONS.....	119
CONFIGURE YOUR SWITCH	9	FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT.....	119
ACCESS YOUR SWITCH MANAGEMENT PAGE	9	ROHS.....	119
SWITCH INFO	9	EUROPE – EU DECLARATION OF CONFORMITY.....	120
SYSTEM.....	11	LIMITED WARRANTY	121
PHYSICAL INTERFACE.....	22		
BRIDGE.....	26		
SNMP	56		
ACCESS CONTROL CONFIG.....	63		
RMON.....	69		
VOICE VLAN	75		
SECURITY.....	79		
DESTINATION MAC FILTER.....	84		
DHCP SNOOPING.....	86		
LLDP (LINK-LAYER DISCOVERY PROTOCOL)	90		
STATISTIC.....	93		
SWITCH MAINTENANCE.....	94		
SAVE SETTINGS TO FLASH.....	101		
WEB SMART SWITCH MANAGEMENT UTILITY.....	102		
SYSTEM REQUIREMENTS	102		

Product Overview



TEG-082WS

Features

TRENDnet's fanless 8-Port Gigabit Web Smart Switch, model TEG-082WS, offers 8 x Gigabit ports, 2 x shared SFP slots, a built-in power supply, and a 16 Gbps switching capacity. This IPv6 ready switch offers advanced traffic management, troubleshooting, access control, energy saving GREENnet, and monitoring features at a reduced cost.

Hardware Design

Provides 8 x Gigabit ports, 2 x shared SFP slots, a 16 Gbps switching capacity, a built-in power supply, and rackmount brackets

Fanless

Fanless design reduces energy consumption and operating noise

IPv6 Ready

This switch supports IPv6 configuration and IPv6 neighbor discovery

Traffic Management

A broad range of network configurations are supported by: 802.3ad link aggregation, Asymmetric VLAN, 802.1Q VLAN, Voice VLAN, Private VLAN, Bandwidth Controls, GVRP, IGMP v1-v3, 802.1p Class of Service (CoS), Spanning Tree (STP, RSTP, and MSTP), and QoS queue scheduling

Troubleshooting

Real time traffic comparison charts, error group charts, and a convenient cable diagnostic test aid in rapid troubleshooting

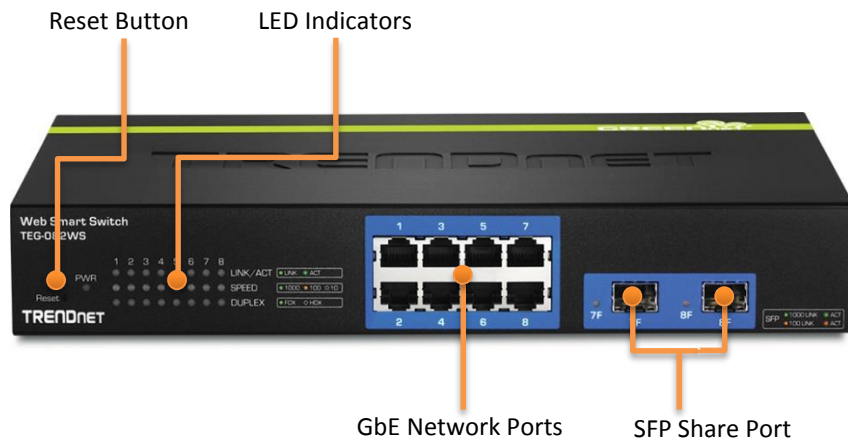
Access Controls

Features such as ACL, SSL, MAC/port filtering, Denial of Service controls, 802.1X, TACACS+, and RADIUS are compatible with layered network access controls

Monitoring

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

Front View



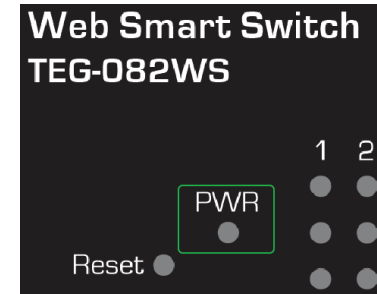
Interfaces

Reset Button	Press and hold this button for 10 seconds and release to reset the switch to factory defaults.
Gigabit Ethernet Ports (1-8)	Connect network devices and can be used for uplink or downlink connections. Ports 7 and 8 are shared with SFP slots 7F and 8F and will be disabled when SFP slots (7F, 8F) are in use.
SFP slots (7F, 8F)	Supports optional 100 or 1000BASE-SX/LX mini-GBIC modules.

LED Indicators

Power (PWR) LED

On	The TEG-082WS is powered on.
Off	The TEG-082WS is not powered.



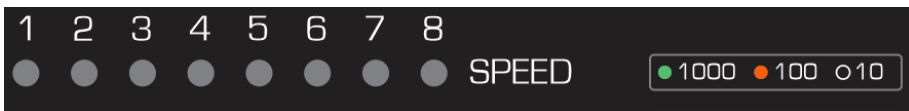
Link/ACT LED (per port)

On	The respective port is successfully connected to an Ethernet network.
Blinking	The port is transmitting or receiving data on the Ethernet network.
Off	No link.



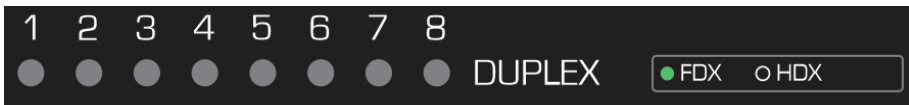
Speed LED (per port)

Green	When respective LED shows in solid green LED, the port is connected to a 1000Mbps Gigabit Ethernet network.
Amber	When respective LED shows in solid amber, the port is connected to a 100Mbps Ethernet network.
Off	When the LINK LED is on and Speed LED is off, the respective port is connected to a 10Mbps Ethernet network.



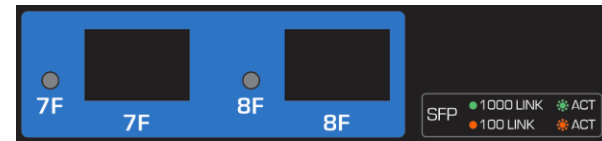
Duplex (per port)

On	Full duplex Ethernet
Off	Half duplex Ethernet



Shared SFP Slots (7F, 8F)

Solid Green	The port is inserted mini-GBIC Gigabit module and gigabit link is established.
Blink in Green	Traffic is passing through this SPF port with gigabit link.
Solid Amber	The port is inserted mini-GBIC 100Mbps module and 100M link is established.
Blink in Amber	Traffic is passing through this SPF port with 100Mbps link.
Off	No link



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)

Package Contents

TEG-082WS package includes:

- TEG-082WS
- Multi-Language Quick Installation Guide
- CD-ROM (Utility and User's Guide)
- Power cord (1.8 m / 6 ft.)
- Rack mount hardware

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

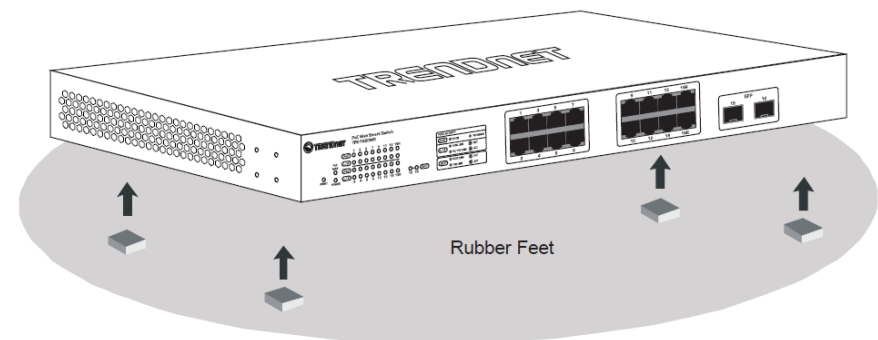
Switch Installation

Desktop Hardware Installation

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

Note: The model showing in illustrations may be different to the one you have.

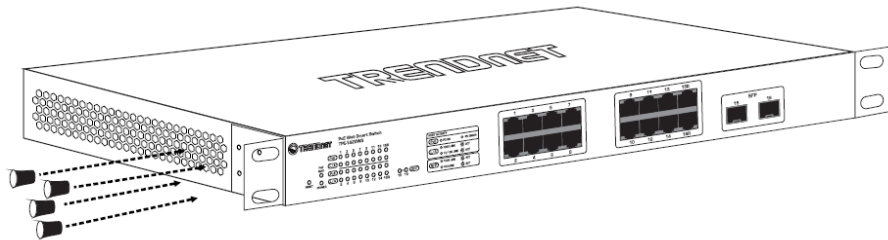
- Install the Switch in a fairly cool and dry place.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 10cm of space at the front and rear of the hub for ventilation.
- Install the Switch 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.



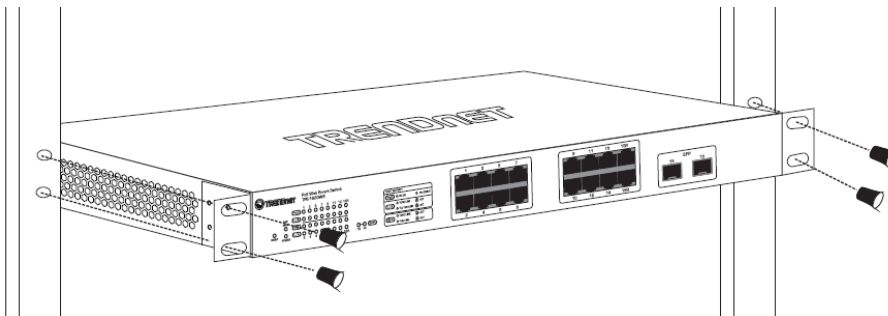
Rack Mount Hardware Installation

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.

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



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

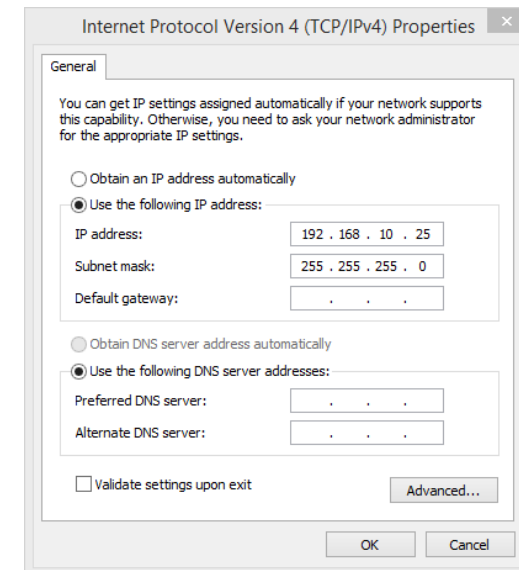


Basic Installation

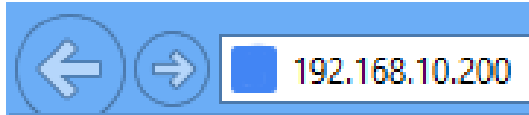
1. Power on your TEG-082WS and connect your computer to the switch.



2. 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.



- Open your web browser, and enter the IP address of the switch, and then press **Enter**. The default IP address is 192.168.10.200.



- Enter the User Name and Password, and then click **Login**. The default username is **admin** and the password is **admin** as well. The username and password are case sensitive, please enter them in all lower cases.

 A screenshot of the TEG-082WS LOGIN page. At the top left is an ID card icon. The title "TEG-082WS LOGIN" is centered. Below the title are two input fields: "User Name:" with the text "admin" and "Password:" with five dots. A blue "LOGIN" button is located at the bottom right.

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

 A screenshot of the IPv4 Setup configuration page. On the left is a sidebar menu with "System" selected. The main area is titled "IPv4 Setup" and contains the following fields:

System MAC Address:	00:14:D1:2D:18:DE
System IP Address:	192 . 168 . 10 . 200
System Subnet Mask:	255 . 255 . 255 . 0
System Default Gateway:	0 . 0 . 0 . 0
System IP Mode:	Static

 A blue "Apply" button is at the bottom.

- 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.

To store the change to flash memory so you can access the same switch management IP address, please follow the instruction below.

- Click **Save Settings to Flash** on the bottom of the menu.

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

- Click **Save Settings to Flash** button, then click **OK**.

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

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 Gigabit Ethernet 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.

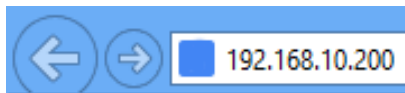


Configure your switch

Access your switch management page

Note: Your switch default management IP address <http://192.168.10.200>. You can manage the TEG-082WS websmart switch using Internet web browser on your choice. (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, or Opera™).

1. Open your web browser and enter the IP address of the switch, such as <http://192.168.10.200>. Your switch will prompt you for a user name and password.



9. Enter the User Name and Password, and then click **Login**. The default username is **admin** and the password is **admin** as well. The username and password are case sensitive, please enter them in all lower cases.

TEG-082WS LOGIN

User Name:	<input style="width: 80%;" type="text" value="admin"/>
Password:	<input style="width: 80%;" type="password" value="••••"/>

Switch Info

You'll landing on Switch Info page when login to the web management GUI. You can view your switch status information here.

Switch Info	Switch Information																																														
System	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="2">Switch Information</th> </tr> <tr> <td>System Up For:</td> <td>6 day(s),7 hr(s),31 min(s),26 sec(s)</td> </tr> <tr> <td>Runtime Image:</td> <td>1.00.02</td> </tr> <tr> <td>Boot Loader:</td> <td>1.00.04</td> </tr> <tr> <th colspan="2">Hardware Information</th> </tr> <tr> <td>DRAM Size:</td> <td>128 MB</td> </tr> <tr> <td>Flash Size:</td> <td>16 MB</td> </tr> <tr> <th colspan="2">Administration Information</th> </tr> <tr> <td>System Name:</td> <td></td> </tr> <tr> <td>System Location:</td> <td></td> </tr> <tr> <td>System Contact:</td> <td></td> </tr> <tr> <th colspan="2">System MAC Address, IPv4 Information</th> </tr> <tr> <td>MAC Address:</td> <td>00:14:D1:2D:18:DE</td> </tr> <tr> <td>IP Address:</td> <td>192.168.10.200</td> </tr> <tr> <td>Subnet Mask:</td> <td>255.255.255.0</td> </tr> <tr> <td>Default Gateway:</td> <td>0.0.0.0</td> </tr> <tr> <th colspan="2">IPv6 Information</th> </tr> <tr> <td>IPv6 Unicast Address / Prefix Length:</td> <td></td> </tr> <tr> <td>IPv6 Default Gateway:</td> <td></td> </tr> <tr> <td>Link Local Address / Prefix length:</td> <td></td> </tr> <tr> <th colspan="2">Automatic Network Features</th> </tr> <tr> <td>IPv4 DHCP Client Mode:</td> <td>Disabled</td> </tr> <tr> <td>IPv6 DHCP Client Mode:</td> <td>Disabled</td> </tr> </table>	Switch Information		System Up For:	6 day(s),7 hr(s),31 min(s),26 sec(s)	Runtime Image:	1.00.02	Boot Loader:	1.00.04	Hardware Information		DRAM Size:	128 MB	Flash Size:	16 MB	Administration Information		System Name:		System Location:		System Contact:		System MAC Address, IPv4 Information		MAC Address:	00:14:D1:2D:18:DE	IP Address:	192.168.10.200	Subnet Mask:	255.255.255.0	Default Gateway:	0.0.0.0	IPv6 Information		IPv6 Unicast Address / Prefix Length:		IPv6 Default Gateway:		Link Local Address / Prefix length:		Automatic Network Features		IPv4 DHCP Client Mode:	Disabled	IPv6 DHCP Client Mode:	Disabled
Switch Information																																															
System Up For:	6 day(s),7 hr(s),31 min(s),26 sec(s)																																														
Runtime Image:	1.00.02																																														
Boot Loader:	1.00.04																																														
Hardware Information																																															
DRAM Size:	128 MB																																														
Flash Size:	16 MB																																														
Administration Information																																															
System Name:																																															
System Location:																																															
System Contact:																																															
System MAC Address, IPv4 Information																																															
MAC Address:	00:14:D1:2D:18:DE																																														
IP Address:	192.168.10.200																																														
Subnet Mask:	255.255.255.0																																														
Default Gateway:	0.0.0.0																																														
IPv6 Information																																															
IPv6 Unicast Address / Prefix Length:																																															
IPv6 Default Gateway:																																															
Link Local Address / Prefix length:																																															
Automatic Network Features																																															
IPv4 DHCP Client Mode:	Disabled																																														
IPv6 DHCP Client Mode:	Disabled																																														
Physical Interface																																															
Bridge																																															
SNMP																																															
Access Control Config																																															
RMON																																															
Voice VLAN																																															
Security																																															
DHCP Snooping																																															
LLDP																																															
Statistic																																															
Tools																																															
Save Settings to Flash																																															

Switch 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.

Hardware Information

DRAM Size: Displays your switch RAM memory size.

Flash Size: Displays your switch Flash memory size.

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.

System MAC Address, IPv4 Information

MAC Address: Displays the switch system MAC address.

IP Address: Displays the current IPv4 address assigned to your switch.

Subnet Mask: Displays the current IPv4 subnet mask assigned to your switch.

Default Gateway: Displays the current gateway address assigned to your switch.

IPv6 Information

IPv6 Unicast Address / Prefix Length: Displays the current IPv6 address and prefix assigned to your switch.

IPv6 Default Gateway: Displays the current IPv6 default gateway address assigned to your switch.

Link Local Address / Prefix Length: Displays the current Link Local address and prefix length assigned to your switch.

Automatic Network Features

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

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

System

System Management

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.

Management	
System Description:	TEG-082WS
System Object ID:	1.3.6.1.4.1.28866.2.26
System Name:	<input type="text"/>
System Location:	<input type="text"/>
System Contact:	<input type="text"/>

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Management

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.

Set your IPv4 settings

System > IPv4 Setup

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

The screenshot shows the 'IPv4 Setup' configuration page. On the left is a navigation menu with 'System' expanded to show 'IPv4 Setup' selected. The main content area is titled 'IPv4 Setup' and contains the following fields:

- System MAC Address:** 00:14:D1:2D:18:DE
- System IP Address:** 10 . 10 . 10 . 22
- System Subnet Mask:** 255 . 255 . 255 . 0
- System Default Gateway:** 10 . 10 . 10 . 254
- System IP Mode:** DHCP (selected in a dropdown menu)

An 'Apply' button is located at the bottom of the configuration area.

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

IPv4 Setup

System MAC Address: Displays the switch MAC address information.

System IP Address: Enter the new switch IP address. (Default: 192.168.10.200)

System Subnet Mask: Enter the new switch subnet mask. (e.g. 255.255.255.0)

System Default Gateway: Enter the default gateway IP address. (e.g. 192.168.10.1 or typically your router/gateway to the Internet).

System IP Mode: Click the drop-down list and select Static to manually specify your IP address settings or DHCP to allow your switch to obtain IP address settings automatically from a DHCP server on your network.



Set your IPv6 settings

System > IPv6 System Settings

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.

Switch Info System <ul style="list-style-type: none"> ▪ System Management ▪ IPv4 Setup ▪ IPv6 System Settings ▪ IPv6 Neighbor Settings ▪ DNS Settings ▪ IP Access List ▪ Administration ▪ User Interface ▪ System Time ▪ SSL Settings ▪ DHCP Auto Configuration ▪ System Log Settings Physical Interface Bridge SNMP Access Control Config RMON Voice VLAN	<h3 style="text-align: center;">IPv6 System Settings</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">IPv6 State:</td> <td style="padding: 5px;"><input type="button" value="Disabled"/></td> </tr> <tr> <td style="padding: 5px;">DHCPv6 Client:</td> <td style="padding: 5px;"><input type="button" value="Disabled"/></td> </tr> <tr> <td style="padding: 5px;">IPv6 Unicast Address / Prefix Length:</td> <td style="padding: 5px;"><input type="text" value=""/> <small>(e.g.:3710::1/64)</small></td> </tr> <tr> <td style="padding: 5px;">IPv6 Static Gateway:</td> <td style="padding: 5px;"><input type="text" value=""/> <small>(e.g.:3710::9)</small></td> </tr> <tr> <td style="padding: 5px;">IPv6 Dynamic Gateway:</td> <td style="padding: 5px;"><input type="text" value=""/></td> </tr> </table> <p style="text-align: center;"><input type="button" value="Apply"/></p> <h3 style="text-align: center;">NS Retransmit Time Settings</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">NS Retransmit Time:</td> <td style="padding: 5px;"><input type="text" value="1"/> sec <small>(1-3600)</small></td> </tr> </table> <p style="text-align: center;"><input type="button" value="Apply"/></p> <h3 style="text-align: center;">Link Local Address Settings</h3> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Automatic Link Local Address:</td> <td style="padding: 5px;"><input type="button" value="Disabled"/></td> </tr> <tr> <td style="padding: 5px;">Link Local Address / Prefix length:</td> <td style="padding: 5px;"><input type="text" value=""/> <small>(e.g.:FE80::6/10)</small></td> </tr> </table> <p style="text-align: center;"><input type="button" value="Apply"/></p>	IPv6 State:	<input type="button" value="Disabled"/>	DHCPv6 Client:	<input type="button" value="Disabled"/>	IPv6 Unicast Address / Prefix Length:	<input type="text" value=""/> <small>(e.g.:3710::1/64)</small>	IPv6 Static Gateway:	<input type="text" value=""/> <small>(e.g.:3710::9)</small>	IPv6 Dynamic Gateway:	<input type="text" value=""/>	NS Retransmit Time:	<input type="text" value="1"/> sec <small>(1-3600)</small>	Automatic Link Local Address:	<input type="button" value="Disabled"/>	Link Local Address / Prefix length:	<input type="text" value=""/> <small>(e.g.:FE80::6/10)</small>
IPv6 State:	<input type="button" value="Disabled"/>																
DHCPv6 Client:	<input type="button" value="Disabled"/>																
IPv6 Unicast Address / Prefix Length:	<input type="text" value=""/> <small>(e.g.:3710::1/64)</small>																
IPv6 Static Gateway:	<input type="text" value=""/> <small>(e.g.:3710::9)</small>																
IPv6 Dynamic Gateway:	<input type="text" value=""/>																
NS Retransmit Time:	<input type="text" value="1"/> sec <small>(1-3600)</small>																
Automatic Link Local Address:	<input type="button" value="Disabled"/>																
Link Local Address / Prefix length:	<input type="text" value=""/> <small>(e.g.:FE80::6/10)</small>																

IPv6 System Settings

IPv6 State: The IPv6 address for the IPv6 network interface is set in auto configuration mode if this option is enabled. The default value is. Auto configuration can be enabled only when DHCPv6 is not enabled on any of the management interfaces.

DHCPv6 Client: This option only displays when DHCPv6 is enabled.

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.

IPv6 Static Gateway: Specifies the corresponding Gateway of the IP address entered into the field.

IPv6 Dynamic Gateway: To configure the switch to automatically obtain its IP configuration from a DHCP server on your network.

NS Retransmit Time Settings

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

Link Local Address Settings

Automatic Link Local Address: A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

Link Local Address/Prefix length: Enter the Link Local Address/Prefix Length.

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80/10 and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless auto configuration 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.

Click **Apply** to apply the change to the switch.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

DNS Settings

System > DNS Settings

Some of the smart switch services requires name resolution services to finish its job, such as SNMP service. Setup the DNS server settings here for name resolution.

DNS Server Settings

DNS IPv4 Server: Specifies the IPv4 DNS server address.

DNS IPv6 Server: Specifies the IPv6 DNS server address.

Click **Add** to save the entry to the list.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Add IPv6 neighbors

System > IPv6 Neighbor Settings

These settings allow you to manually define IPv6 supported neighboring devices on your network.

IPv6 Neighbor Settings

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.

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

IP Access List

IP Restriction Status: Enable or disable Access Control List. Default: Disabled

IP Address Settings

IP Address: Enter the IPv4 or IPv6 address and then click **Add** to create an access list entry.

IP Access List Table

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.

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**.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Administration table			
Index	User Name	Password	Action
1	admin	*****	Modify

To create additional administrative user accounts

Administration Settings

User Name: Enter the user name of the new account.

Password: Enter the password for the new account

Confirm Password: Enter the password again for verification.

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

Click **Add** to add the new administrator.

Changing the administrator password

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. The index 1 **admin** user on the administration table is the default administrator. You can modify the password, but you cannot remove it.*

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Status Settings

- SNMP Agent:** Click the drop-down list to one of the following options.
- **Enabled:** The SNMP agent is active. You can manage the switch with SNMP network management software and the switch's private MIB.
 - **Disabled:** The SNMP agent is inactive.

Web Server Status: Displays the current SNMP status.

Timeout Settings

Web Idle Timeout: Enter the idle period in minutes, when the switch will automatically log out an idled user from the switch management page. Default: 10 min.

Group Interval: The IGMP group timeout interval. Default: 120 sec.

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Set the switch date and time

System > System Time

Switch Info	System Time
System <ul style="list-style-type: none"> System Management IPv4 Setup IPv6 System Settings IPv6 Neighbor Settings DNS Settings IP Access List Administration User Interface System Time SSL Settings DHCP Auto Configuration System Log Settings 	<p>Current Time Settings</p> <p>Clock Mode: Local Time</p> <p>Current Time: 1 Jan 2009 16:35:41</p> <p>Time Zone:</p>
	<p>Date/Time Settings</p> <p>Clock Mode: Local Time</p>
	<p>Local time Settings</p> <p>Date Settings: 2009 / 1 / 1 (YYYY:MM:DD)</p> <p>Time Settings: 16 : 57 : 59 (HH:MM:SS)</p>
	<p>Simple Network Time Protocol (SNTP) Settings</p> <p>SNTP Primary Server: 0 . 0 . 0 . 0 IPv4</p> <p>SNTP Secondary Server: 0 . 0 . 0 . 0 IPv4</p> <p>SNTP Poll Interval: 1 Min.(1-60)</p> <p>Time Zone: (GMT-08:00) Pacific Time (US & Canada),Tijuana</p>
	<p>Additional Time Parameters</p> <p>Daylight Saving Time Status: Disabled</p> <p>From: January 01 00 00 (Month:Day:HH:MM)</p> <p>To: January 01 00 00 (Month:Day:HH:MM)</p> <p>DST Offset: 1 hr</p> <p>Apply</p>
Physical Interface	
Bridge	
SNMP	
Access Control Config	
RMON	

Current Time Settings

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.

Date/Time Settings

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.

SNTP
Local Time

Local Time Settings

Date Settings: Enter your date settings (YYYY/MM/DD).

Time Settings: Enter your time settings (HH:MM:SS)

When select the clock mode to **Local Time**, enter the date and time manually here.

Simple Network Time Protocol (SNTP) Settings

SNTP Primary Server: Select the format of the URL you want to enter for SNTP server address. Enter the primary network time server IPv4, IPv6 address or domain name.

Domain Name ▾
IPv4
IPv6
Domain Name

SNTP Secondary Server: Select the format of the URL you want to enter for SNTP server address. Enter the secondary network time server IPv4, IPv6 address or domain name.

SNTP Poll Interval: Enter the interval time when your switch will update the time and date settings with the time server. Default: 1 min.

Time Zone Click the drop-down list to select your time zone.

When select the clock mode to **SNTP**, enter the SNTP server information here.

Click **Apply** to apply the change to the switch

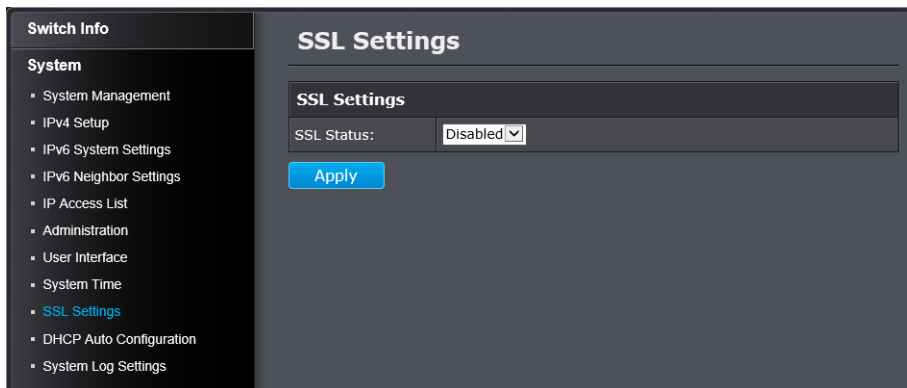
Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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 transmit files with clear text over the network. Enabling HTTPS/SSL management access allows access to the switch management page using encrypted communication prevents your data been eavesdropped by unauthorized user.

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.

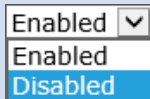


Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

SSL Settings

SSL Status: Enable or disable HTTPS/SSL management access or to HTTP clear text mode. Default: Disabled.



Note: When SSL is enabled, you need to access the switch management page using HTTPS instead of HTTP. (e.g. <https://192.168.10.200>)

Enable DHCP Auto Configuration

System > DHCP Auto Configuration

If you need to synchronize the switch configuration file on remote server, the DHCP Auto Configuration feature is available for this purpose via the DHCP server. Your IP address settings must be enabled to the DHCP client so that this feature can operate with your DHCP/TFTP server.

DHCP Auto Configuration Settings

Auto Configuration State: Enable/Disable Auto Configuration from DHCP/TFTP server. Default: Disabled.

Enabled	▼
Enabled	
Disabled	

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

System Log Settings

Time Stamp: Enable/Disable the time stamp on log entry. Default: Enabled.

Enabled
Disabled
Disabled ▾

Message Buffered Size: Enter the message buffer size. Default: 50 entries, Range: 1-200.

Syslog Status: Enable/ Disable to store the logs on remote log server. Default: Enabled.

Enabled
Disabled
Disabled ▾

Syslog Server IP: Enter the IPv4 or IPv6 address of the external syslog server to send logging.

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.

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Switch Info

System

Physical Interface

Bridge

SNMP

Access Control Config

RMON

Voice VLAN

Security

DHCP Snooping

LLDP

Statistic

Tools

Save Settings to Flash

Physical Interface

Physical Interface Table											
Port	Trunk	Type	Link Status	Admin. Status	Mode	Jumbo	Flow Ctrl	EAP	BPDU	Action	
All	-	-	-	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Apply	
1	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
2	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
3	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
4	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
5	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
6	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
7(1)	---	1000TX	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
7(2)	---	100FX	Down	Enabled ▾	100/Full ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
7(3)	---	1000X	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
8(1)	---	1000TX	Up	Enabled ▾	Auto (1000F) ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
8(2)	---	100FX	Down	Enabled ▾	100/Full ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	
8(3)	---	1000X	Down	Enabled ▾	Auto ▾	Enabled ▾	Disabled ▾	Disabled ▾	Enabled ▾	Apply	

Notes:
1. All ports mode setting is only used for copper.
2. All media type of combo port will be consistent for Jumbo, EAP and BPDU state.

Physical Interface Table

Port: Specifies the port number. The All value indicates ports 1 through 8 on the Switch. The port number 7 and 8 are Gigabit and SFP shared ports. Only one interface will be activated at the same time. When SFP and Gigabit connection coexist, the SFP will take the priority.

- (1) Gigabit Port
- (2) SFP with 100FX module
- (3) SFP with 1000X module

Trunk: This cell displays the trunk status with 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 cell displays the port type. On the Switch, the port type is 1000TX for 10/100/1000Base-T twisted-pair ports (1-8) and 100FX or 1000X for the SFP ports (7F-8F) for copper or fiber SFP type.

Link Status: This cell displays the network link status of the port. The possible values are:

- Up: This value indicates a valid link exists between the port and the end node.
- Down: This value 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.

Ignore
Enabled

Enabled
Disabled
Disabled ▾

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **Admin Status** is not changing. If you select **Enabled** then

click on **Apply** for all ports, **Admin Status** on all ports will be set to **Enabled**.

Each Port:

- Enabled: This port is enabled to send and receive Ethernet frames.
- Disabled: This port is disabled and cannot send and receive Ethernet frames.

*Note: Click **Apply** in the end of the row to apply the change.*

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.

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **Mode** is not changing. If you set to certain mode then click on **Apply** for all ports, the **Mode** on all ports will be set to the same value.

Each Port:

- 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, "1000F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.
 - Auto (1000F): This parameter indicates the port is configured for 1000Mbps operation in Auto-Negotiation mode.
 - 1000/Full -This parameter indicates the port is configured for 1000Mbps operation in full-duplex mode.
 - 100/Full -This parameter indicates the port is configured for 100Mbps operation in full-duplex mode.

- 10/Full -This parameter indicates the port is configured for 10Mbps operation in full-duplex mode.
- 1000/Half -This parameter indicates the port is configured for 1000Mbps operation in half-duplex mode.
- 100/Half -This parameter indicates the port is configured for 100Mbps operation in half-duplex mode.
- 10/Half -This parameter indicates the port is configured for 10Mbps operation in half-duplex mode.

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

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

*Note: Click **Apply** in the end of the row to apply the change.*

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.

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **Jumbo** setting is not changing. If you select **Enabled** or **Disabled** then click on **Apply** for all ports, **Jumbo** setting on all ports will be set to the same value on **Enabled** or **Disabled**.

Each Port:

- **Enabled:** This port is enabled to send and receive Jumbo frames.
- **Disabled:** This port is disabled and cannot send and receive Jumbo frames.

Note:

- 1) Click **Apply** in the end of the row to apply the change.
- 2) When QoS is enabled on a port, the Jumbo frame parameter cannot be enabled.

Flow Ctrl: Flow Control, This parameter shows 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.

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **Flow Control** setting is not changing. If you select **Enabled** or **Disabled** then click on **Apply** for all ports, **Flow Control** setting on all ports will be set to the same value on **Enabled** or **Disabled**.

Each Port:

- **Enabled:** This port is enabled to proceed the flow control.
- **Disabled:** This port is disabled and not doing flow control.

*Note: Click **Apply** in the end of the row to apply the change.*

EAP: This number shows the current Extensible Authentication Protocol (EAP) setting on the port.

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **EAP** setting is not changing. If you select **Enabled** or **Disabled** then click on **Apply** for all ports, **EAP** setting on all ports will be set to the same value on **Enabled** or **Disabled**.

Each Port:

Enabled: This port is enabled to send and receive EAP packets.

Disabled: This port is disabled and will not send and receive EAP packets.

*Note: Click **Apply** in the end of the row to apply the change.*

BPDU: This parameter shows the current BPDU setting on the port.

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **BPDU** setting is not changing. If you select **Enabled** or **Disabled** then click on **Apply** for all ports, **BPDU** setting on all ports will be set to the same value on **Enabled** or **Disabled**.

Each Port:

Enabled: This port is enabled to pass BPDU frames through the switch and broadcast them through all other ports.

Disabled: This port is disabled and the switch will not pass BPDU frames through the switch. With RSTP or STP enabled, the switch will receive BPDU frames and process them according to the spanning tree protocol.

*Note: Click **Apply** in the end of the row to apply the change.*

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Bridge

The Bridge session covers most of the web smart switch features including spanning tree, trunk configuration, IGMP snooping, bandwidth control, VLAN, VGRP, and QoS.

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.

Spanning Tree Protocol Settings

Global STP Status:

Protocol Version:

Bridge Priority:

Maximum Age: Sec. (6-40)

Hello Time: Sec. (1-10)

Forward Delay: Sec. (4-30)

Transmit Hold Count: (1-10)

Max Hop Count: (6-40)

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

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

Spanning Tree Protocol Settings

Global STP Select the STP state on the device.

- Status:**
- **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.

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.

Root Information

Root Bridge: The root bridge ID in the spanning tree.

Root Cost: The connection cost on the root port

Root Maximum Age: The aging timeout for the root port.

Age:

Root Forward Delay: The forward delay timer before packet forwarding.

Root Port: The port number been assigned as root port.

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure Spanning Tree Protocol port settings

Bridge > Spanning Tree > Port Settings

Port	STP Status	Priority	Admin Cost (0 = Auto)	External Cost	State	Edge	P2P	Restricted Role	Restricted TCN	Migrate	Apply
All	Ignore	Ignore		-	-	Ignore	Ignore	Ignore	Ignore	Restart	Apply
1	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
2	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
3	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
4	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
5	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
6	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
7	Enabled	128	0	20000	Disabled	Auto	Auto	False	False	Restart	Apply
8	Enabled	128	0	20000	Forwarding	Auto	Auto	False	False	Restart	Apply

Port Settings

STP Status: Indicates if spanning tree protocol is active or not on the port.

Ignore
Enabled
Disabled

All Ports:

If you select **Ignore** and click on **Apply** for all ports, the **STP Status** setting is not changing. If you select **Enabled** or **Disabled** then click on **Apply** for all ports, **STP Status** setting on all ports will be set to the same value on **Enabled** or **Disabled**.

Each Port:

- **Enable:** The spanning tree protocol is enabled on the port.
- **Disabled:** The spanning tree protocol is disabled on the port. Enable Disable

*Note: Click **Apply** in the end of the row to apply the change. BPDU pass-through 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.

0
16
32
48
64
80
96
112
128
144
160
176
192
208
224
240

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, select a desired value.

*Note: Click **Apply** in the end of the row to apply the change. If you select **Ignore** on **All Ports** and click on **Apply** for all ports, the **Admin Cost** setting is not changing. If you set the value then click on **Apply** for all ports, The **Admin Cost** will be set to the same value.*

Admin Cost (0 = Auto): The administratively assigned value for the contribution of this port to the path cost of a port. 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 200,000,000 to determine the external cost. The default port cost: 100Mbps port = 200,000. Gigabit port = 20,000.

State: Displays the current port spanning tree state.

- **Blocking:** A blocking state does not allow network traffic to be sent or received on 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:** A port with STP disabled does not participate in STP. 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** to assign 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** 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

Ignore
ForceTrue
ForceFalse
Auto

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

*Note: Click **Apply** in the end of the row to apply the change. If you select **Ignore on All Ports** and click on **Apply** for all ports, the **Admin Cost** setting is not changing. If you set the value then click on **Apply** for all ports, The **Admin Cost** will be set to the same value.*

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.

Migrate: Indicates if the port is configured to accept RSTP and STP BPDUs.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure Spanning Tree Protocol MST settings (MSTP)

Bridge > Spanning Tree > MST Settings

Switch Info

System

Physical Interface

Bridge

- Spanning Tree
 - Protocol Settings
 - Port Settings
 - MST Settings**
 - Instance Information
 - MST Port Settings
- Trunk Config
 - Mirroring
 - Loopback Detection
 - Static Unicast
 - Static Multicast
- IGMP Snooping
- Bandwidth Control
- VLAN
- GVRP
- QoS

MST Settings

MST Configuration Identification Settings

Configuration Name: 0014d12d18de

Revision Level: 0 (0-65535)

Apply

MST Instance Settings

MSTI ID: * (1-31)

VID List: (1-4094)

Priority: 0

Add

MST Table

MSTI ID	VID List	Priority	Action
CIST	1-4094	32768	Apply Delete

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: This value, together with the configuration name, and identical VLAN mapped for STP instance IDs identifies the MST region configured on the switch. Range: 0 to 65535.

MST Instance Settings

MSTI ID: Displays the MSTI ID associated with the VLAN ID. Range: 1 to 31.

VID List: Displays the VLAN ID associated with MSTI. Click **Add** to add the VLAN and MSTI association on MST table. Range: 0 to 4094.

Priority: Select a priority in the **Priority** field. The user may set a priority value between 0 and 61440.

MST Table

MSTI ID: Displays the MSTI ID associated with the VLAN ID.

VID List: Displays the VLAN ID associated with MSTI. Click **Apply** to change the VID List value on an entry. Range: 0 – 4094.

Priority: Select a priority in the **Priority** field. The user may set a priority value between 0 and 61440. Click **Apply** to apply the change.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Click **Apply** to apply the change to the switch

View your Spanning Tree Protocol Instance Information (MSTP)

Bridge > Spanning Tree > Instance Information

Instance Information

MSTI ID	Internal Root Cost	Root Port	Regional Root Bridge	Designated Bridge	Instance Priority
CIST	0	0	80:00:00:14:D1:2D:18:DE	80:00:00:14:D1:2D:18:DE	32768
1	0	0	00:00:00:14:D1:2D:18:DE	00:00:00:14:D1:2D:18:DE	0

Instance Information**MSTI ID:** Specifies the ID of MSTI.**Internal Root Cost:** Root cost to the root bridge**Root Port:** Root port of the specific instance.**Regional Root Bridge:** The bridge connected with root port.**Designated Bridge:** The bridge connected with designated port.**Instance Priority:** Priority of the instance.

Configure Spanning Tree Protocol MST Port Settings (MSTP)

Bridge > Spanning Tree > MST Settings

MST Port Settings

Select MST Port: 01

MST Port Info

MSTI ID	Designated Bridge	Internal Path Cost	Admin Path Cost (0 = Auto)	Priority	State	Role	Action
CIST	80:00:00:14:D1:2D:18:DE	123	123	128	Disabled	Disabled	Apply
1	80:00:00:14:D1:2D:18:DE	20000	0	128	Disabled	Disabled	Apply

MST Port Settings**Select MST Port:** Click the drop-down to select which MST port to configure.**MST Port Info****MSTI ID:** MSTI identification number**Designated Bridge:** The bridge connects to the designated ports.**Internal Path Cost:** The path cost to the designated bridge.**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.**State:** STP port forwarding state**Role:** The port role in the STP: root port, designated port, backup port, or disabled port.**Action:** Click **Apply** to apply the change to the MST port

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

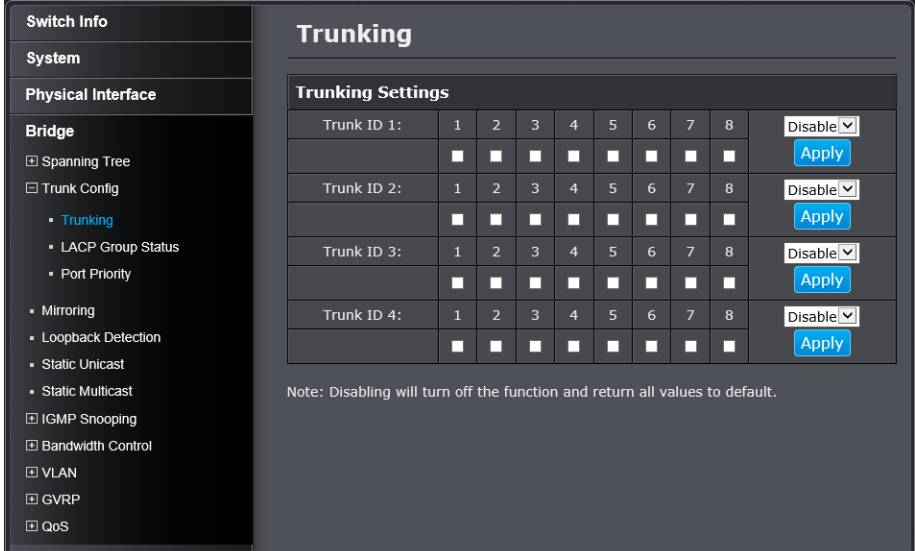
Trunk Configuration (Link Aggregation)

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, each supporting up to 8 ports. Add a trunking Name and select the ports to be trunked together, and click Apply to activate the selected trunking groups.

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



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

Note: Disabling will turn off the function and return all values to default.

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

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.

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

View your trunk group status information

Bridge > Trunk Config > LACP Group Status

LACP Group Status	
System Priority:	32768
System ID:	00:14:D1:2D:18:DE
Group: 1	This group doesn't exist
Group: 2	This group doesn't exist
Group: 3	This group doesn't exist
Group: 4	This group doesn't exist

LACP Group Status

System Priority: Pre assigned 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 trunk group (link aggregation group) ID number and status.

Configure your port priority

Bridge > Trunk Config > Port Priority

Port	Priority (0-65535)
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Port Priority Status

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.

Port Priority Settings

Port: The port number

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

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.

Mirroring Settings

Status: Click the drop-down menu and select one of the following options:

- **Enabled:** This parameter activates the Port Mirroring feature and the rest of the configuration parameters become active on the page.

- **Disabled:** 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 Port Settings

Ingress Port: 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.

Egress Port: 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Switch Info

System

Physical Interface

Bridge

- Spanning Tree
- Trunk Config
 - Trunking
 - LACP Group Status
 - Port Priority
- Mirroring
- Loopback Detection**
- Static Unicast
- Static Multicast
- IGMP Snooping
- Bandwidth Control
- VLAN
- GVRP
- QoS

Loopback Detection

Loopback Detection Settings

State: Enabled Disabled

Loopback Detection Global Settings

Interval: sec (1-32767)

Recover Time: sec (0 or 60-1000000, 0 is Disabled)

Note: Disabling will turn off the function and return all values to default.

[Apply](#)

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	Disabled	Normal	Apply
5	Disabled	Normal	Apply
6	Disabled	Normal	Apply
7	Disabled	Normal	Apply
8	Disabled	Normal	Apply

Loopback Detection Settings

State: Select **Enabled** to enable the loopback detection feature. Select **Disabled** to disabled the loopback detection feature.

Loopback Detection Global Settings

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 apply the change to the switch

Loopback Detection Table

Port: The network port number on the switch

Loopback Detection State: Select one of the Loopback **Detection State** selections 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.

Loop Status: Display the current loopback status.

Action: Next to each entry, click **Apply** to apply the change of the port.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Static Unicast

Add static unicast entries to the switch

Bridge > Static Unicast

Static Unicast Address Table

Static Unicast Address Settings

802.1Q VLAN: (1-4094)

MAC Address:

Port Member Settings

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

802.1Q VLAN (Free entries:256, Total entries:0)

VLAN Index	MAC Address	Port Members	Action
<< 802.1Q VLAN Static Unicast Address Table is empty >>			

Page 0/0 Page

Static Unicast Address 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 Settings

Port Member: Select the port where the MAC address will reside.

*Note: Click **Apply** to apply the change.*

802.1Q VLAN

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Static Multicast

Add static multicast entries to the switch

Bridge > Static Multicast

Static Multicast Address 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 1).

MAC Address: Enter the MAC address of the device to add.

Group Member Settings

Group Member: Select the port where the MAC address will reside.

*Note: Click **Apply** to apply the change.*

802.1Q VLAN

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

IGMP Snooping

Configure IGMP Snooping Settings

Bridge > IGMP Snooping > IGMP Snooping Settings

Switch Info	IGMP Snooping Settings						
System							
Physical Interface							
Bridge	IGMP Snooping Settings						
<input type="checkbox"/> Spanning Tree <input type="checkbox"/> Trunk Config <ul style="list-style-type: none"> <input type="checkbox"/> Mirroring <input type="checkbox"/> Loopback Detection <input type="checkbox"/> Static Unicast <input type="checkbox"/> Static Multicast <input type="checkbox"/> IGMP Snooping <ul style="list-style-type: none"> IGMP Snooping Settings <input type="checkbox"/> IGMP Snooping Router Port 	Status: <input type="text" value="Disabled"/>						
<input type="checkbox"/> Bandwidth Control <input type="checkbox"/> VLAN <input type="checkbox"/> GVRP <input type="checkbox"/> QoS	Age-Out Timer: <input type="text" value="250"/> Sec. (130-153025)						
SNMP	Querier Status: <input type="text" value="Disabled"/>						
Access Control Config	Query Interval: <input type="text" value="125"/> Sec. (60-600)						
	Max Response Time: <input type="text" value="10"/> Sec. (10-25)						
	Robustness Variable: <input type="text" value="2"/> Sec. (2-255)						
	Last Member Query Interval: <input type="text" value="1"/> Sec. (1-25)						
	Router Timeout: <input type="text" value="250"/> Sec. (120-1200)						
	Note: The Host Timeout will be computed automatically in Querier Enabled by (Robustness Variable * Query Interval + Max Response Time).						
	<input type="button" value="Apply"/>						
	Multicast Group Entries (Free entries:256, Total entries:0)						
	<table border="1"> <thead> <tr> <th>VLAN ID</th> <th>Multicast Group Address</th> <th>Member Ports</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="text-align: center;"><< IGMP Snooping multicast address table is empty >></td> </tr> </tbody> </table>	VLAN ID	Multicast Group Address	Member Ports	<< IGMP Snooping multicast address table is empty >>		
VLAN ID	Multicast Group Address	Member Ports					
<< IGMP Snooping multicast address table is empty >>							

IGMP Snooping Settings

Status: Click the drop-down list and select **Enabled** to enable the IGMP snooping feature or **Disabled** to disable the feature.

Age-Out Timer: Enter the amount of time in seconds that you want your switch to wait before it purges an inactive dynamic MAC address.

Querier Status: Click the drop-down list and select **Enabled** to enable the Querier Status or **Disabled** to disable this feature.

Query Interval: Enter the amount of time you want your switch to send IGMP queries.

Max Response Time: When a host receives the query packet, it starts counting to a random value, less than the maximum response time. When this timer expires, host replies with a report, provided that no other host has responded yet.

Robustness Variable: Adjust the robustness variable to compensate the packet loss.

Last Member Query Interval: The timer to define the window of time to collect member response.

Router Timeout: The timer to maintain a valid router.

Multicast Group Entries

The table below displays the static multicast address groups defined in your switch for reference and can be modified on under **Bridge > Static Multicast** or dynamically updated with the active multicast address groups.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure IGMP Snooping Router Ports

Bridge > IGMP Snooping > IGMP Snooping Router Port

802.1Q VLAN			
VLAN ID	Static Router Port	Dynamic Router Port	Action
1	N/A	N/A	Modify

In the VLAN ID router port list, you can configure your Static and Dynamic Router ports. IGMP Snooping Router Port configured manually is a **Static Router Port**, and a **Dynamic Router Port** is dynamically configured by the Switch when a query control message is received. To modify an entry, click **Modify** to add statically add router ports.

Modify IGS Static Router Port

IGS Static Router Port Settings

802.1Q VLAN ID:

Static Router Port

	1	2	3	4	5	6	7	8
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"/>

Check the static router ports to add and click **Apply** to save the settings.

*Note: You can click on **All** to add all ports. Clicking **Restore** will restore the static router port settings to default.*

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Port	DLF	Broadcast	Multicast	Threshold	Action
All	Ignore	Ignore	Ignore	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
1	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
2	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
3	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
4	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
5	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
6	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
7	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>
8	Disabled	Disabled	Disabled	64pps x <input type="text" value="22194"/> (1-22194)	<input type="button" value="Apply"/>

Storm Control Settings

Port: The port ID you want to implement the storm control.

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.

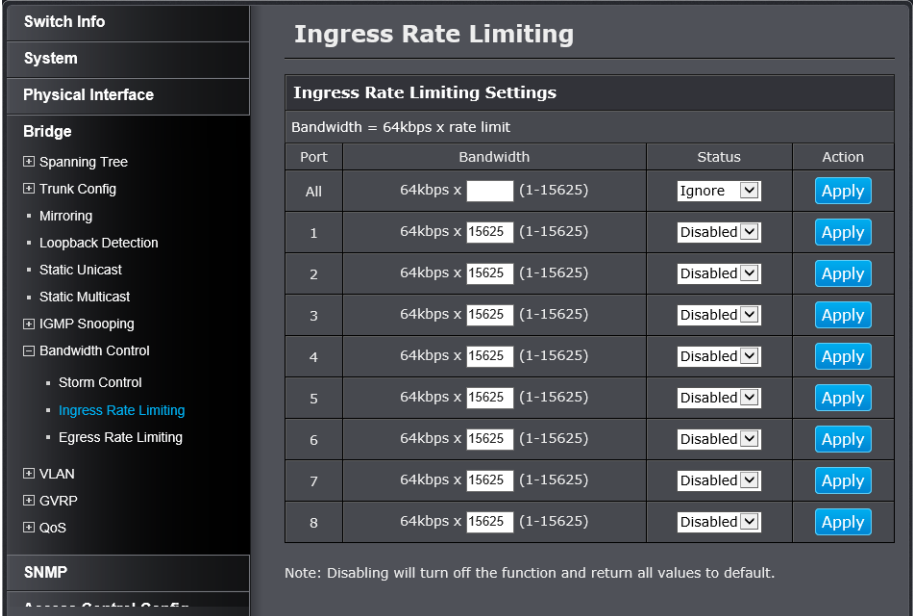
Action: Modifying settings in the row marked **All**, will apply the settings to all ports. Click **Apply** to apply the change.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Set Ingress Rate Limiting

Bridge > Bandwidth Control > Ingress Rate Limiting

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



Ingress Rate Limiting Settings			
Bandwidth = 64kbps x rate limit			
Port	Bandwidth	Status	Action
All	64kbps x <input type="text" value="15625"/> (1-15625)	Ignore <input type="text" value="v"/>	<input type="button" value="Apply"/>
1	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
2	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
3	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
4	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
5	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
6	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
7	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>
8	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled <input type="text" value="v"/>	<input type="button" value="Apply"/>

Note: Disabling will turn off the function and return all values to default.

Ingress Rate Limiting Settings

Port: The port number.

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.

Action: Modifying settings in the row marked **All**, will apply the settings to all ports. Click **Apply** to apply the change.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Set Egress Rate Limiting

Bridge > Bandwidth Control > Egress Rate Limiting

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

Egress Rate Limiting

Bandwidth = 64kbps x rate limit

Port	Bandwidth	Status	Action
All	64kbps x <input type="text" value=""/> (1-15625)	Ignore	Apply
1	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
2	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
3	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
4	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
5	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
6	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
7	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply
8	64kbps x <input type="text" value="15625"/> (1-15625)	Disabled	Apply

Note: Disabling will turn off the function and return all values to default.

Egress Rate Limiting Settings

Port: The port number.

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.

Action: Modifying settings in the row marked **All**, will apply the settings to all ports. Click **Apply** to apply the change.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Tagged VLAN

Tagged VLAN Settings

VLAN ID: (2-4094)

VLAN Name: (32 characters limit)

Management VLAN:

Static Tagged

	1	2	3	4	5	6	7	8
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"/>

Static Untagged

	1	2	3	4	5	6	7	8
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"/>

Not Member

	1	2	3	4	5	6	7	8
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"/>

[Apply](#) [Clear](#) [Reset to Default](#)

Tagged VLAN Table

VLAN ID	Name	VLAN Type	Management	VLAN Action
1	DefaultVLAN	Permanent	Enabled	Modify

Page 1/1 [First Page](#) [Previous Page](#) [Next Page](#) [Last Page](#) Page [GO](#)

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

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.

Tagged VLAN 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.

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.

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)

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

Tagged VLAN 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: VLAN 1 is the default VLAN and cannot be removed.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure VLAN Port Settings

Bridge > VLAN > Port Settings

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

The screenshot shows the 'Port Settings' configuration page. On the left is a navigation menu with options like Mirroring, Loopback Detection, Static Unicast, Static Multicast, IGMP Snooping, Bandwidth Control, VLAN (with sub-options like Tagged VLAN, Port Settings, Forwarding Table Mode, Dynamic Forwarding Table, Private VLAN, VLAN Current Database), GVRP, QoS, SNMP, Access Control Config, RMON, Voice VLAN, and Security. The main area is titled 'Port Settings' and contains a table:

Port	PVID	Acceptable Frame Types	Ingress Filtering	Action
All	<input type="text"/>	Ignore	Ignore	Apply
1	<input type="text"/>	All	Enabled	Apply
2	<input type="text"/>	All	Enabled	Apply
3	<input type="text"/>	All	Enabled	Apply
4	<input type="text"/>	All	Enabled	Apply
5	<input type="text"/>	All	Enabled	Apply
6	<input type="text"/>	All	Enabled	Apply
7	<input type="text"/>	All	Enabled	Apply
8	<input type="text"/>	All	Enabled	Apply

Port Settings

Port: The port number.

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 & Priority Tagged:** 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.

Action: Modifying settings in the row marked **All**, will apply the settings to all ports. Click **Apply** to apply the change.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure the VLAN Forwarding Table Mode

Bridge > VLAN > Forwarding Table Mode

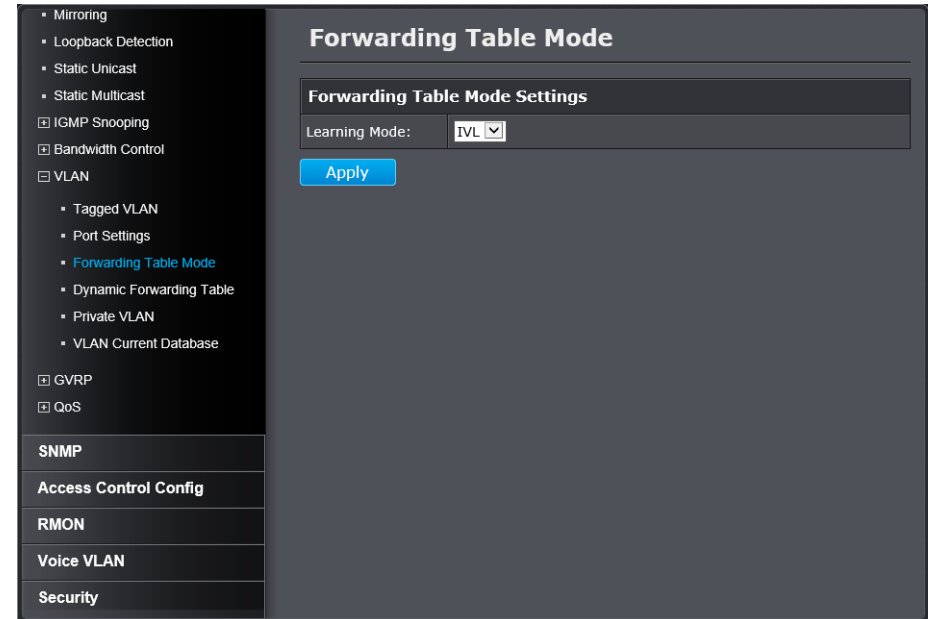
This section allows you to configure your switch to standard 802.1Q VLAN mode (IVL) or Asymmetric VLAN mode (SVL). Asymmetric VLAN allows the configuration of overlapping untagged VLAN ports in order to create VLAN groups. It is recommended to use the standard 802.1Q VLAN mode when possible.

IVL – Independent VLAN Learning

SVL – Shared VLAN Learning

Please note the following when switching between forwarding table modes:

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



Note: The default mode is IVL.

Click **Apply** to apply the change to the switch

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Dynamic Forwarding Table

Dynamic Forwarding Table Settings

Port:

Dynamic Forwarding Table

ID	VID	Port	MAC Address	Type
1	1	8	00-00-00-00-00-11	Dynamic
2	1	8	00-11-32-0D-61-76	Dynamic
3	1	8	00-14-D1-CD-67-80	Dynamic
4	1	8	44-19-B7-09-A5-88	Dynamic
5	1	8	B8-C7-5D-E2-FC-11	Dynamic
6	1	8	D8-EB-97-D3-97-63	Dynamic

Page 1/1 Page

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

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

Create a private VLAN

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.

Private VLAN

Private VLAN Settings

State: Enabled Disabled

Apply

Port Select

Source Port: 01

Forwarding Ports:

	1	2	3	4	5	6	7	8
Clear	<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	1-8
2	1-8
3	1-8
4	1-8
5	1-8
6	1-8
7	1-8
8	1-8

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

To configure Private VLAN Settings, perform the following procedure:

- Change the **Private VLAN Settings** by clicking the **State** radio button choices that you want to change.
 - **Enable:** Enable Private VLAN settings.
 - **Disable:** Disable Private VLAN settings.
 Press **Apply** to make the changes to take effect.
- Set the Source Port to on port 1 – 8.
- Click on the **Forwarding Ports** radio button that applies to your configuration.
- Click **Apply**.

View the current VLAN database

Bridge > VLAN > VLAN Database

VLAN Current Database

802.1Q Tagged VLAN

VLAN ID	VLAN Name	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	DefaultVLAN	1	1-8	1-8	permanent

Page 1/1 [First Page](#) [Previous Page](#) [Next Page](#) [Last Page](#) Page [GO](#)

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.

GVRP (GARP VLAN Registration Protocol)

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches.

With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

Bridge > GVRP > GVRP Global Settings

GVRP Global Settings

GVRP Global Settings

GVRP Status:

[Apply](#)

Click the GVRP Status drop-down list and select **Enabled** to activate GVRP or **Disabled** to deactivate GVRP. Click **Apply** to save the settings.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Set GVRP port settings

Bridge > GVRP > Port Settings

This section will allow you to select which ports will have GVRP enabled or will be restricted from using GVRP.

Port	Dynamic Vlan Status	Restricted VLAN Registration	Action
All	Ignore	Ignore	Apply
1	Enabled	Disabled	Apply
2	Enabled	Disabled	Apply
3	Enabled	Disabled	Apply
4	Enabled	Disabled	Apply
5	Enabled	Disabled	Apply
6	Enabled	Disabled	Apply
7	Enabled	Disabled	Apply
8	Enabled	Disabled	Apply

GVRP Port Settings

Port: The port number on the switch.

Dynamic Vlan Status This parameter defines the GVRP status of the port. From the Dynamic Vlan Status field, select 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.

- **Enabled:** The Dynamic Vlan is activated for the port row selected.
- **Disabled:** The Dynamic VLAN is de-active for the respective port.

Restricted VLAN Registration

This parameter controls if the VLAN registration on the port is restricted or not.

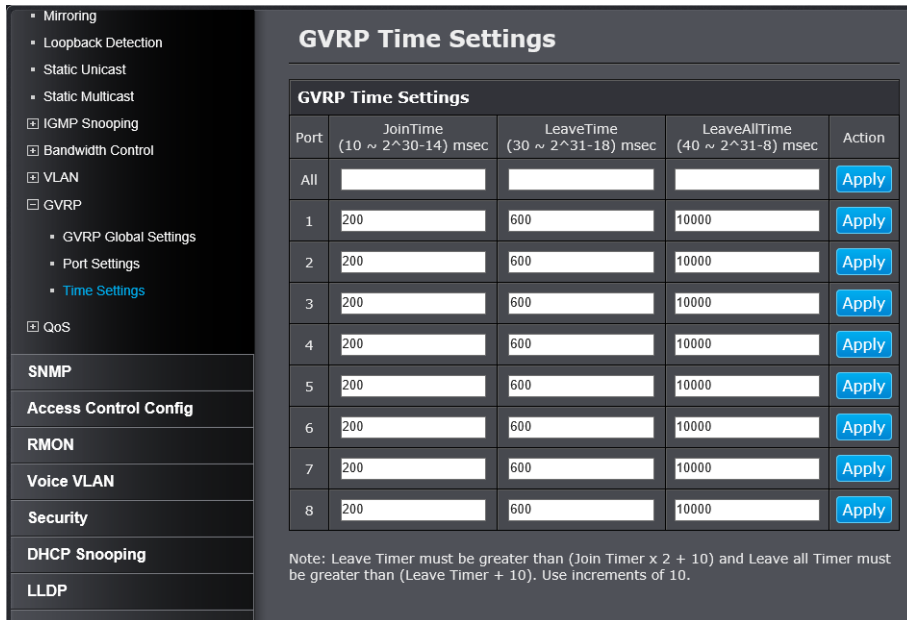
- **Ignore:** This parameter indicates that the setting in the All row does not apply to the Restricted VLAN Registration field. In other words, each port is set individually.
- **Enable:** The Restricted VLAN Registration is active for the port row selected.
- **Disable:** The Restricted VLAN Registration is de-active for the port row selected.

Action: Modifying settings in the row marked **All**, will apply the settings to all ports. Click **Apply** to apply the change.

Set GVRP time settings

Bridge > GVRP > Time Settings

This section will allow you to define the GARP Join, Leave, and Leave All Time for each port.



Port	JoinTime (10 ~ 2 ³⁰ -14) msec	LeaveTime (30 ~ 2 ³¹ -18) msec	LeaveAllTime (40 ~ 2 ³¹ -8) msec	Action
All	<input type="text"/>	<input type="text"/>	<input type="text"/>	Apply
1	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
2	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
3	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
4	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
5	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
6	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
7	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply
8	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="10000"/>	Apply

Note: Leave Timer must be greater than (Join Timer x 2 + 10) and Leave all Timer must be greater than (Leave Timer + 10). Use increments of 10.

Note: The GARP LeaveTime must be greater than (GARP JoinTimer x 2 + 10) and the GARPLLeaveAllTime must be greater than (GARP LeaveTime + 10). The acceptable input values are multiples of 10. If you try to enter a value that is not a multiple of 10, the value is rimmed down to the multiple of 10.

GVRP Time Settings

Port: The port number on the switch.

JoinTime: This parameter is the GARP Join Timer. Its range is 10 - 1073741810 milli-seconds.

LeaveTime: This parameter is the GARP Leave Timer. Its range is 30 - 2147483630 milli-seconds. This timer must be set in relation to the GVRP Join Timer according to the following equation:

- $\text{GARPLLeaveTimer} \geq (\text{GARPJoinTimer} \times 2) + 10$

LeaveAllTime: This parameter is the GARP Leave All Timer. Its range is 30 - 2147483630 milli-seconds. This timer must be set in relation to the GVRP Leave Timer according to the following equation:

- $\text{GARPLLeaveAllTimer} > (\text{GARPLLeaveTimer} + 10)$

Action: Modifying settings in the row marked **All**, will apply the settings to all ports. Click **Apply** to apply the change.

Note: To ensure compatibility between network devices, you need to configure the same values for the GARP Join Timer, GARP Leave Timer, and GARP Leave All Timer on all participating GVRP devices in your network.

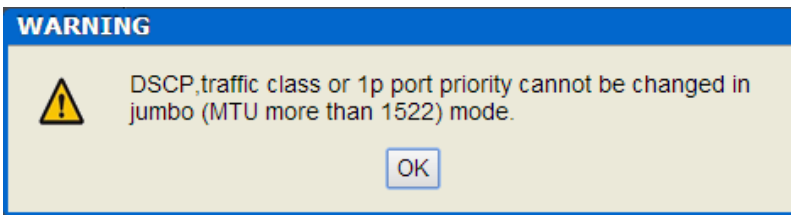
Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.



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.

Set CoS priority settings

Bridge > QoS > CoS

CoS

QoS Status:

Traffic Class:

CoS Table

0	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
1	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
2	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
3	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
4	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
5	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
6	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>
7	Low : <input type="radio"/>	Medium : <input type="radio"/>	High : <input type="radio"/>	Highest : <input type="radio"/>

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

Apply

CoS Settings

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.

After you have completed this mapping process, select **Enabled** in the **QoS Status** field.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Port	User Priority	Action
All	0	Apply
1	0	Apply
2	0	Apply
3	0	Apply
4	0	Apply
5	0	Apply
6	0	Apply
7	0	Apply
8	0	Apply

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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

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

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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Set the Scheduling Algorithm

Bridge > QoS > Scheduling Algorithm

The screenshot shows the 'Scheduling Algorithm' configuration page. On the left is a navigation menu with the following items: Mirroring, Loopback Detection, Static Unicast, Static Multicast, IGMP Snooping, Bandwidth Control, VLAN, GVRP, QoS (expanded to show CoS, Port Priority, DSCP, Scheduling Algorithm, and IPv6 Traffic Class Priority Settings), SNMP, Access Control Config, RMON, Voice VLAN, and Security. The 'Scheduling Algorithm' item is highlighted. The main content area is titled 'Scheduling Algorithm' and contains a 'Scheduling Algorithm Settings' section. This section has a 'Scheduling Algorithm' dropdown menu currently set to 'Strict Priority' and an 'Apply' button below it.

Select your scheduling algorithm and then click **Apply** to save the settings.

Schedule Algorithm 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure the IPv6 Traffic Class Priority Settings

Bridge > QoS > IPv6 Traffic Class Priority Settings

IPv6 Traffic Class Global Settings: Select **Enabled** or **Disabled**. Click **Apply** to save the settings.

IPv6 Traffic Class Settings

IPv6 Traffic Class: Specify the value of IPv6 class. Range: 0 – 255.

Class ID: Defines the priority assigned to the port. The priorities are Highest, High, Medium and Low.

Click **Add** to add the traffic class setting entry to the table.

On the **IPv6Traffic Class Table**, 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Set your **Engine ID** and then click **Apply** to apply the settings.

SNMP Engine ID Settings

Engine ID: Enter the local device **Engine ID**. The value is a hexadecimal string. Each byte in the hexadecimal character strings is two hexadecimal digits. The **Engine ID** must be defined before SNMP is enabled. (10 - 64 Hexadecimal digits)

Reset: Clear up the **Engine ID** value

Reset to Default: Use the device-generated **Engine ID** (Reset to Default will override any entry in the **Engine ID** field).

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

SNMP View Table

SNMP View Settings

View Name: *
(32 characters limit)

Subtree OID: *

OID Mask: *

View Type: ▼

SNMP View Table

View Name	Subtree OID	OID Mask	View Type	Action
ReadWrite	1	1	Included	<input type="button" value="Delete"/>

To creating SNMP View Table Entries:

- Enter the **View Name**. This value must be pre-defined on the SNMP User/Group page.
- Enter the Subtree OID.
- Enter "1" for the OID Mask.

- 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.

To modify an SNMP View Table Entry:

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

To deleting SNMP View Table Entry:

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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**.

SNMP Group Access Settings

Group Name: *
(32 characters limit)

Read View Name: (32 characters limit)

Write View Name: (32 characters limit)

Notify View Name: (32 characters limit)

Security Model:

Security Level:

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

To create 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.

To modify a SNMP View Name:

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

To delete a SNMP View Name:

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.*

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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:

SNMP User/Group Settings

User Name: * (32 characters limit)

Group Name: * (32 characters limit)

SNMP Version: v1 encrypted

Auth-Protocol: MD5 Password:

Priv-Protocol: DES Password:

SNMP User/Group Table

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
ReadOnly	ReadOnly	v1	None	None	<input type="button" value="Delete"/>
ReadOnly	ReadOnly	v2c	None	None	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	v1	None	None	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	v2c	None	None	<input type="button" value="Delete"/>

To create a SNMP User and Group Name:

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

- Type a new **User Name**. Enter a name up to 31 characters in length.
- Type a new **Group Name**. Enter a name up to 31 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.

To modify a SNMP User and Group Name:

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

To delete a SNMP User and Group Name:

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

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

To create **SNMP Community Setting**

- 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

*Note: **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.

To modify a SNMP Community Setting

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.

To delete a SNMP Community Setting

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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

The screenshot shows the 'Trap Management' configuration page. On the left is a sidebar with navigation options: Physical Interface, Bridge, SNMP (with sub-items: Engine ID, View Table, Group Access Table, SNMP User/Group, Community Table, Trap Management), Access Control Config, RMON, Voice VLAN, Security, DHCP Snooping, LLDP, Statistic, Tools, and Save Settings to Flash. The main content area is titled 'Trap Management' and includes:

- Trap Management Global Settings:** A 'Trap' status set to 'Enabled' with an 'Apply' button.
- Add Host Table:** Fields for 'Host IP Address' (with IPv4 and IPv6 radio buttons), 'SNMP Version' (set to v1), and 'Community Name/User Name' (with a 32-character limit). 'Add' and 'Reset' buttons are present.
- Trap Management Table:** A table with columns: Host Ip Address, SNMP Version, Community Name/User Name, and Action. The table is currently empty, showing '<< snmp trap management list is empty >>'.

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

The new host is added to the table.

To 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.

To 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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:

Choose the type of policy to create:

- Add L2+IPv4
- Add IPv6

Note: Please note that when adding policies, 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.

Add L2+IPv4

To add an L2+IPv4 policy, use the following procedure:

- Click **Add L2+ 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 – 65535 which identifies the policy. This field is mandatory.
- 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.
 - **Source MAC Mask Length:** Indicates the length of the Source MAC Mask ranging from 1- 48.
 - **Destination MAC Address:** Specifies the destination MAC address. The format is xx.xx.xx.xx.xx.xx.
 - **Destination MAC Mask Length:** Indicates the length of the Destination MAC Mask ranging from 1 - 48.
 - **VLAN ID:** A unique number identifying a VLAN ranging from 1 to 4094.
 - **802.1p Priority:** 802.1p priority level of the frame ranging from 0 to 7.
 - **Ether Type:** Indicates the protocol of the Ethernet frame protocol ranging from 0000 to FFFF.
 - **Protocol:** Indicates the packet protocol ranging from 0 to 255.
 - **Source IP Address:** Specifies the source IP address.
 - **Source IP Mask Length:** Specifies the mask length of the source IP address ranging from 0 to 32.
 - **Destination IP Address:** Specifies the destination IP address.
 - **Destination IP MAC Mask Length:** Specifies the mask length of the destination IP address ranging from 0 to 32.

- **DSCP:** The DSCP (Differentiated Services Code Point) value in the IP header ranging from 0 to 63.
- **Source Layer 4 Port:** Indicates the source layer 4 port ranging from 1 to 65535.
- **Destination Layer 4 Port:** Indicates the destination layer 4 port ranging from 1 - 65535.
- **Policy Sequence:** Enter a number in the Policy Sequence field. The Policy Sequence must be a unique number within the range of 1 - 65535. This field is mandatory.
- **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 to 65535. This field is mandatory and must match a Port List Index that has been previously entered on the Policy Index.
- **Port List:** Select the interface for which you want to display data.
- Click **Add** to add the policy to the **Policy Table**.

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 – 65535 which identifies the policy. This field is mandatory.
- 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:
 - **VLAN ID:** A unique number identifying a VLAN ranging from 1 to 4094.
 - **802.1p Priority:** 802.1p priority level of the frame ranging from 0 to 7.
 - **Protocol:** Indicates the packet protocol ranging from 0 to 255.
 - **IPv6 Source IP Address:** Specifies the IPv6 Source IP address.
 - **Prefix Length:** Indicates the length of the Source IP ranging from 1 to 128.
 - **IPv6 Destination IP Address:** Specifies the IPv6 Destination IP address.
 - **Prefix Length:** Indicates the length of the Destination IP ranging from 1 to 128.
 - **Source Layer 4 Port:** Indicates the source layer 4 port ranging from 1 to 65535.
 - **Destination Layer 4 Port:** Indicates the destination layer 4 port ranging from 1 to 65535.
 - **Policy Sequence:** Enter a number in the Policy Sequence field. The Policy Sequence must be a unique number within the range of 1 to 65535. This field is mandatory.
 - **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.
- **Port List:** Select the interface for which you want to display data.
- Click **Add** to add the policy to the Policy Table.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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:

Rate Control Settings

Rate Control Settings

Index: (1-65535)

Committed Rate: 64kbps x (1-15625)

[Add](#)

Rate Control Table [Delete All](#)

Free Entries : 248

Total Entries : 0

Index	Committed Rate	Action
<< Rate Control table is empty >>		

Page 0/0 [First Page](#) [Previous Page](#) [Next Page](#) [Last Page](#) Page [GO](#)

- Enter a number in the Index field. The Index is a unique number within the range of 1–65535 which identifies the policy. This field is mandatory.
- Enter a number in the Committed Rate column ranging from 1 to 15625.
- Click **Add** to add the rate control settings to the **Rate Control Table**.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

View your policy database

[Access Control Config > Policy Database](#)

Allows you to view current policies assigned to each port by Index or Sequence.

Click the **Select Port** drop-down list to select the port you would like to view associated with the selected port. Then select the order to sort **Index** or **Sequence**.

Note: The Any option will display policies for all ports.

View the active policies associated with the specified port.

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:

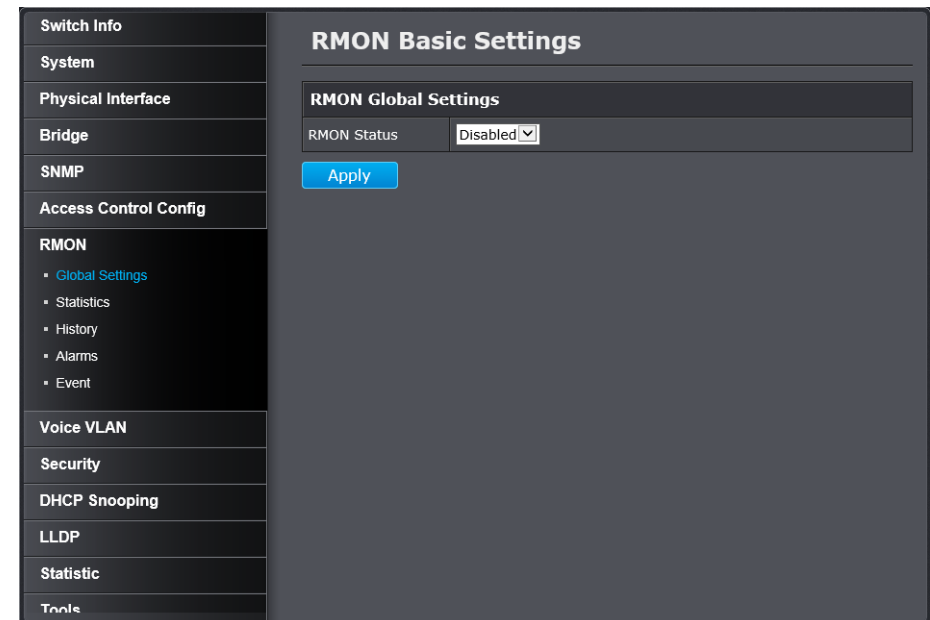
- **Statistic group:** This group is used to view port statistics remotely with SNMP programs.
- **History group:** This group is used to collect histories of port statistics to identify traffic trends or patterns.
- **Event group:** This group is used with alarms to define the actions of the switch 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.



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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

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

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Ethernet Statistics 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.

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.

History Control 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.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure parameters for RMON alarms

RMON > Alarm

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.

RMON Alarm 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.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

RMON Event 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.

Community: This parameter specifies the community where you want to send the SNMP trap.

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.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Voice VLAN Settings

Voice VLAN Status

Voice VLAN: Enabled Disabled

Note: Disabling will turn off the function and return all values to default.

Voice VLAN Global Settings

VLAN ID:

Aging Time: (1-120 hours)

CoS:

[Apply](#)

Voice VLAN Table

Port	Auto Detection	Status	Action
All	Ignore	-	Apply
1	Disabled	None	Apply
2	Disabled	None	Apply
3	Disabled	None	Apply
4	Disabled	None	Apply
5	Disabled	None	Apply
6	Disabled	None	Apply
7	Disabled	None	Apply
8	Disabled	None	Apply

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 apply the settings.
- 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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure Voice VLAN OUI settings

Voice VLAN > Voice VLAN OUI 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 10 OUIs.

Modify OUI Setting

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

Delete OUI Setting

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

Switch Info	<h3>Port Access Control Settings</h3> <div> <p>Port Access Control Settings</p> <p>NAS ID: <input type="text" value="Nas1"/> (16 characters max)</p> <p>Port Access Control: <input type="text" value="Disabled"/></p> <p>Authentication Method: <input type="text" value="Local"/></p> <p><input type="button" value="Apply"/> <input type="button" value="Settings"/> <input type="button" value="Configuration Status"/></p> </div>
System	
Physical Interface	
Bridge	
SNMP	
Access Control Config	
RMON	
Voice VLAN	
Security	
▪ Port Access Control	
▪ Dial-in User	
▪ RADIUS	
▪ TACACS+	
▪ Destination MAC Filter	
▪ Denial of Service	
DHCP Snooping	
LLDP	
Statistic	

Configure the following parameters as required:

- **NAS ID:** This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.
- **Port Access Control:** This parameter enables or disables **Port Access Control**. Select one of the following choices from the pull down menu:
 - **Enable:** The **Port Access Control** feature is activated.
 - **Disable:** The **Port Access Control** feature is de-activated.

- **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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

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.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Add RADIUS Servers (RADIUS Authentication Method)

Security > RADIUS

The screenshot shows the RADIUS configuration page. On the left is a sidebar with a navigation menu. The main area is titled 'RADIUS' and contains two sections: 'RADIUS Settings' and 'RADIUS Table'.

RADIUS Settings

- Server Priority: 1 (Highest :1, Lowest :5)
- Server IP Address: 0 . 0 . 0 . 0 (IPv4 selected, IPv6 unselected)
- Server Port: 1812 (1-65535)
- Accounting Port: 1813 (1-65535)
- Shared Secret: (32 characters limit)

There is an 'Add' button below the settings.

RADIUS Table

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

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

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

RADIUS 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: Set the RADIUS authentic server(s) UDP port. The default port is 1812. Range: 1 – 65535.

Accounting Port: Set the RADIUS account server(s) UDP port. The default port is 1813. Range: 1 – 65535.

Shared Secret: Enter the default authentication and encryption key for RADIUS communication between the device and the RADIUS server.

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.

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.

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

TACACS+ Settings

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.

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

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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.

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

Apply Reset to Default

Select the DoS rule you want to activate, click the drop-down menu on the right hand side and select **Deny**.

Click **Apply** to apply the settings.

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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 Snooping > General Settings

Switch Info	<h3>General Settings</h3> <div style="border: 1px solid #ccc; padding: 5px;"> <p>DHCP Global Settings</p> <p>DHCP Snooping: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>General Settings</p> <p>Pass Through Option 82: <input type="text" value="Disabled"/></p> <p>Verify MAC Address: <input type="text" value="Enabled"/></p> <p>Backup Database: <input type="text" value="Disabled"/></p> <p>Database Update Interval: <input type="text" value="1200"/> (600-86400)(Sec)</p> <p>DHCP Option 82 Insertion: <input type="text" value="Disabled"/></p> <p style="text-align: center;">Apply</p> </div>
System	
Physical Interface	
Bridge	
SNMP	
Access Control Config	
RMON	
Voice VLAN	
Security	
DHCP Snooping <ul style="list-style-type: none"> ▪ General Settings ▪ VLAN Settings ▪ Trusted Interfaces ▪ Binding Database 	
LLDP	
Statistic	
Tools	

DHCP Snooping Global Settings

Enabled: This parameter activates the DHCP Snooping feature.

Disabled: This parameter de-activates the DHCP Snooping.

DHCP Snooping General Settings

Pass Through Option 82: Select one of the following choices from the pull-down 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.

Verify MAC Address: Select one of the following choices from the pull-down menu:

- **Enabled:** The MAC address of each ingress ARP packet is validated when compared against the Binding Table entries. Invalid ARP packets are discarded.
- **Disabled:** The MAC address of each ingress ARP packet is not validated against the Binding Table. All ARP packets are forwarded through the switch without regard to the IP and MAC Address information in the packet header.

Backup Database: select one of the following choices from the pull-down menu:

- **Enabled:** The Web Management Utility Software saves a backup copy of the Binding Table to flash at a specified interval (Database Update Interval) of time.
- **Disabled:** The Web Management Utility Software does not save a backup copy of the Binding Table to flash.

Database Update Interval: Enter the database update interval. The range of this interval is 600 to 86400 seconds.

DHCP Option 82 Insertion: select one of the following choices from the pull-down menu:

- **Enabled:** The Web Management Utility software inserts the DHCP Option 82 information into the DHCP packets.
- **Disabled:** The Web Management Utility software does not insert the DHCP Option 82 information into the DHCP packets.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

DHCP Snooping over VLAN

DHCP Snooping > VLAN Settings

In this section, you can define an existing VLAN to apply DHCP snooping.

In the field, enter the existing VLAN ID to apply DHCP Snooping. Then click **Add** to add the VLAN entry to the table.

On 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.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Set Trusted Interfaces

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.

Port	Trust	Action
All	Ignore	Apply
1	Enabled	Apply
2	Enabled	Apply
3	Enabled	Apply
4	Enabled	Apply
5	Enabled	Apply
6	Enabled	Apply
7	Enabled	Apply
8	Enabled	Apply

Next to each port, click the Trust drop-down list and select one of the following options.

- **Disabled:** This parameter defines the port as untrusted for the DHCP Snooping feature.
- **Enabled:** This parameter defines the port as trusted for the DHCP Snooping feature.

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Configure Binding Database

DHCP Snooping > Binding Database

The Binding Database displays learned and statically assigned MAC

Address and IP Address information for each host on the local area network. Dynamically assigned IP addresses from the DHCP server will automatically populate the table on the Binding Database page as they are assigned by the server. Statically assigned IP addresses are entered manually by entering the host's address information and clicking on the Add button.

Binding Database Settings

MAC Address: Enter the host's MAC Address.

IP Address: Enter the static IP Address assigned to the host.

VLAN: Enter the host's VLAN ID.

Port: Enter the port number where the host is connected.

Type: Because the IP Address being entered is static, you must select Static.

Lease Time: Enter the time that IP address assignment is valid. The range is 10 to 4294967295 seconds.

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

On 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.

Binding Database Table

MAC Address: This parameter shows the host's MAC Address.

VLAN ID: This parameter shows the host's VLAN ID of which the DHCP client is a member.

IP Address: This parameter is the IP Address assigned by the DHCP server to the DHCP client.

Port: This parameter is the port number where the DHCP client is connected.

Type: This parameter indicates the following:

- **Learned:** The host IP Address is dynamically assigned by the DHCP server.
- **Static:** The host IP Address is statically assigned. See "Static IP Addresses" on page 300 for more information.

Lease Time: This parameter is the time that IP address assignment by the DHCP server is valid.

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

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

Switch Info	LLDP Global Settings
System	
Physical Interface	
Bridge	
SNMP	
Access Control Config	
RMON	
Voice VLAN	
Security	
DHCP Snooping	
LLDP	
<ul style="list-style-type: none"> LLDP Global Settings LLDP Neighbors Information 	
Statistic	
Tools	
Save Settings to Flash	

LLDP Global Settings

LLDP Enabled Disabled

[Apply](#)

LLDP Settings

Message TX Hold Multiplier: (2-10)

Message TX Interval: sec. (5-32768)

LLDP Reinit Delay: sec. (1-10)

LLDP TX Delay: sec. (1-8192)

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

[Apply](#)

LLDP System Information

Chassis ID Subtype: macAddress

Chassis ID: 00:14:D1:2D:18:DE

System Name:

System Description: TEG-082WS

LLDP Port State Settings

Port	State	Action
All	Disabled	Apply
1	RxTx	Apply
2	RxTx	Apply
3	RxTx	Apply
4	RxTx	Apply
5	RxTx	Apply
6	RxTx	Apply
7	RxTx	Apply
8	RxTx	Apply

LLDP Global Settings**Enabled:** The LLDP feature is active.**Disabled:** The LLDP feature is inactive.**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 1 to 10 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 apply the settings.**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 Port State Settings****Port:** The port number on the switch.**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.***Action:** Click **Apply** to apply the settings.Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

View LLDP Neighbor Information

LLDP > LLDP Neighbor Information

LLDP Neighbors 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 switch 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 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 Normal: 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.

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

Statistic Information										
Traffic Information										
Port ID	InOctets	InUcastPkts	InNUcastPkts	InDiscards	OutOctets	OutUcastPkts	OutNUcastPkts	OutDiscards	Clear	
All	-	-	-	-	-	-	-	-	-	Apply
1	0	0	0	0	0	0	0	0	0	Apply
2	0	0	0	0	0	0	0	0	0	Apply
3	0	0	0	0	0	0	0	0	0	Apply
4	0	0	0	0	0	0	0	0	0	Apply
5	0	0	0	0	0	0	0	0	0	Apply
6	0	0	0	0	0	0	0	0	0	Apply
7	0	0	0	0	0	0	0	0	0	Apply
8	91434222	11610	528322	0	30926562	14745	226649	0	0	Apply

< Refresh >

Traffic Information

Port ID: The port ID on the switch

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.

View Error Information Statistics

Statistic > Error Information

Port ID	InErrors	OutErrors	DropEvents	CRCAlignErrors	UndersizePkts	OversizePkts	Fragments	Collisions	Clear
All	-	-	-	-	-	-	-	-	Apply
1	0	0	0	0	0	0	0	0	Apply
2	0	0	0	0	0	0	0	0	Apply
3	0	0	0	0	0	0	0	0	Apply
4	0	0	0	0	0	0	0	0	Apply
5	0	0	0	0	0	0	0	0	Apply
6	0	0	0	0	0	0	0	0	Apply
7	0	0	0	0	0	0	0	0	Apply
8	0	0	0	0	0	0	0	0	Apply

Error Information

Port ID: The port ID on the switch

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.

CRCAlignErrors: 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.

Switch Maintenance

Upgrade your switch firmware

Tools > Firmware Upgrade

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

In addition, it is also important to verify if the latest firmware version is newer than the one your switch is currently running. To identify the firmware that is currently loaded on your switch, log in to the switch, click on the **System Info** section or click on **Tools** and click on **Firmware Upgrade**. The firmware used by the switch is listed as **Runtime Image** or **Image Version**. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.

- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your switch.

Firmware Upgrade via HTTP Settings

The screenshot shows the 'Firmware Upgrade via HTTP' settings page. On the left is a navigation menu with categories: Switch Info, System, Physical Interface, Bridge, SNMP, Access Control Config, RMON, Voice VLAN, Security, DHCP Snooping, LLDP, Statistic, Tools, and Firmware Upgrade. Under 'Tools', 'Firmware Upgrade' is expanded to show 'via HTTP' and 'via TFTP'. 'Config File Backup/Restore' is also visible. The main content area is titled 'Firmware Upgrade via HTTP' and contains a table with 'Image Version: 1.00.02' and 'Firmware File:' with a 'Browse...' button. Below the table is a note: 'Note: System will reset automatically after burning image to flash.' and an 'Apply' button.

Firmware Upgrade via HTTP Settings	
Image Version:	1.00.02
Firmware File:	<input type="text"/> Browse...

Note: System will reset automatically after burning image to flash.

1. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.
2. Navigate to the folder on your computer where the unzipped firmware file (.hex) is located and select it.
3. Click **Apply**. If prompted, click **Yes** or **OK**.

Firmware Upgrade via TFTP Settings

Note: Before using this method, a TFTP server is required alive on the network. The TFTP server has to be in the same subnet. Please place the firmware file (.hex) on the root directory of your TFTP server. If you are not familiar with the TFTP protocol, it is recommended to use the HTTP method.

The screenshot shows the 'Firmware Upgrade via TFTP' configuration page. On the left is a navigation menu with categories: Switch Info, System, Physical Interface, Bridge, SNMP, Access Control Config, RMON, Voice VLAN, Security, DHCP Snooping, LLDP, Statistic, and Tools. Under Tools, 'Firmware Upgrade' is expanded to show 'via HTTP' and 'via TFTP' (selected). Below this is 'Config File Backup/Restore'. The main content area is titled 'Firmware Upgrade via TFTP Settings' and contains the following fields:

- Image Version: 1.00.02
- TFTP Server IP: [IP Address] IPv4 (selected) / IPv6
- Image File Name: [Text Field] (64 characters max.)
- Retry Count: 3

A note states: 'Note: System will reset automatically after burning image to flash.' An 'Apply' button is at the bottom.

Firmware Upgrade via TFTP Settings

Image Version: The firmware version now is running on the switch.

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.

Click **Apply** to start the firmware upgrade.

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

The screenshot shows the 'Config File Backup/Restore via HTTP' configuration page. The left navigation menu is similar to the previous page, but 'Config File Backup/Restore' is expanded to show 'via HTTP' (selected) and 'via TFTP'. The main content area is titled 'File Backup/Restore via HTTP Settings' and contains:

- Select File: [Text Field] Browse...
- Backup button
- Restore button

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. Depending on your web browser, click on **Browse** or **Choose File**.
2. A separate file navigation window should open.
3. Select the configuration file to restore and click **Restore**. (Default Filename: config.bin). If prompted, click **Yes** or **OK**.
4. Wait for the switch to restore settings.

Backup/Restore via TFTP Settings

Note: Before using this method, a TFTP server is required alive on the network. The TFTP server has to be in the same subnet. Please place the firmware file (.hex) on the root directory of your TFTP server. If you are not familiar with the TFTP protocol, it is recommended to use the HTTP method.

1. 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.
2. 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)

To restore your switch configuration:

1. 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.

2. 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 for the backup. (Default: config.bin)
3. 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.

The screenshot shows the 'Cable Diagnostics' section of a network switch's GUI. On the left is a navigation menu with options like SNMP, Access Control Config, RMON, Voice VLAN, Security, DHCP Snooping, LLDP, and Tools. The 'Tools' section is expanded, showing 'Cable Diagnostics' as the selected option. The main content area is titled 'Cable Diagnostics' and contains a 'Cable Diagnostics Settings' section with a 'Port' dropdown menu set to '1' and a 'Test Now' button. Below this is a 'Cable Diagnostics Table' with columns for 'Port', 'Test Result', 'Cable Fault Distance (meters)', and 'Cable Length (meters) [in range]'. A note explains the test's purpose and provides three key points: 1. 'N/A' for cable length means it's not available due to link speed or cable quality. 2. 'Cable Fault Distance' is +/- 2 meters. 3. The test identifies fault length from the switch.

Note:

1. If the cable length displays N/A, it means that the cable length is Not Available. This 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 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.

Select the port you want to proceed cable test. Then click on **Test Now**. The results will be displayed in the Cable Diagnostic Table below.

Cable Diagnostics Table

Port: The port number of the switch.

Test Result: Displays the diagnostic results for each pair in the cable. One of the following cable status parameters is displayed:

- **OK:** There is no problem detected with the cable.
- **Open in Cable:** There is an open wire within the cable.
- **Short in Cable:** Two wires are shorted together within the cable.
- **Cross talk in Cable:** There is crosstalk detected between one pair of wires and another pair within the cable.

Cable Fault Distance: This parameter specifies the distance from the switch port to the cable fault.

Cable Length: This parameter specifies the length of the cable connected to the switch port.

Enable IEEE 802.3az Power Saving Mode

Tools > IEEE 802.3az EEE

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

The screenshot shows the web interface for configuring IEEE 802.3az EEE. On the left, a sidebar menu lists various configuration sections: SNMP, Access Control Config, RMON, Voice VLAN, Security, DHCP Snooping, LLDP, Statistic, Tools, and Save Settings to Flash. The 'Tools' section is expanded, showing options like Firmware Upgrade, Config File Backup/Restore, Cable Diagnostics, IEEE 802.3az EEE (highlighted), Reboot, and Ping. The main content area is titled 'IEEE 802.3az EEE' and contains a sub-section 'IEEE 802.3az EEE Settings'. It features a label 'IEEE 802.3az Energy Efficient Ethernet Status:' followed by a dropdown menu currently set to 'Disabled'. Below this is a blue 'Apply' button.

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

Go **Save Settings to Flash** section to save the change on the flash to make sure the change is permanent.

Reboot/Reset to factory defaults

Tools > Reboot

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

The screenshot shows the 'Factory Default Reset' page. The left sidebar menu is similar to the previous screenshot, but 'Tools' is expanded to 'Reboot'. The main content area is titled 'Factory Default Reset' and contains a sub-section 'Reboot'. It features a label 'Reboot Type:' followed by a dropdown menu currently set to 'Normal'. Below this is a blue 'Apply' button. A note below the button states: 'Note: System will reboot in a few seconds after pressing the Apply button.'

To reboot your switch:

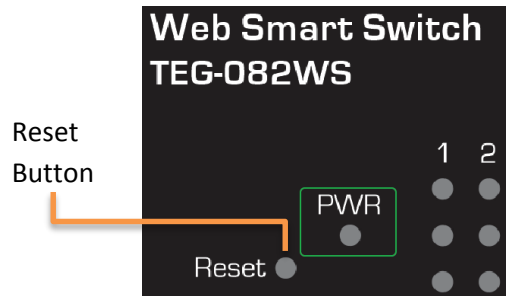
You may want to make your switch restart as a clean and fresh without changing the switch configuration. Select **Reboot Type to Normal** and then click on **Apply** to reboot the switch. Wait for the switch complete the rebooting process.

*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.*

To reset your switch to factory defaults:

To reset the switch configurations to factory defaults you can proceed with hardware reset-to-default, or with the web GUI. Hardware reset has the same effect to “reboot the switch to factory default” selection in this session.

- **Hardware Reset-to-Default:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button more than 10 seconds and then release. Located on the front panel of your switch. Wait for the switch complete the rebooting process.



- **With Web GUI:** You can choose reset to **Factory Default** or **Factory Default Except IP**. If you select **Factory Default Except IP**, all the configurations will be set to the factory defaults, but the switch management IP remains the same.

Default Settings

Management IP: 192.168.10.200

Admin user name: admin

Password: admin

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.

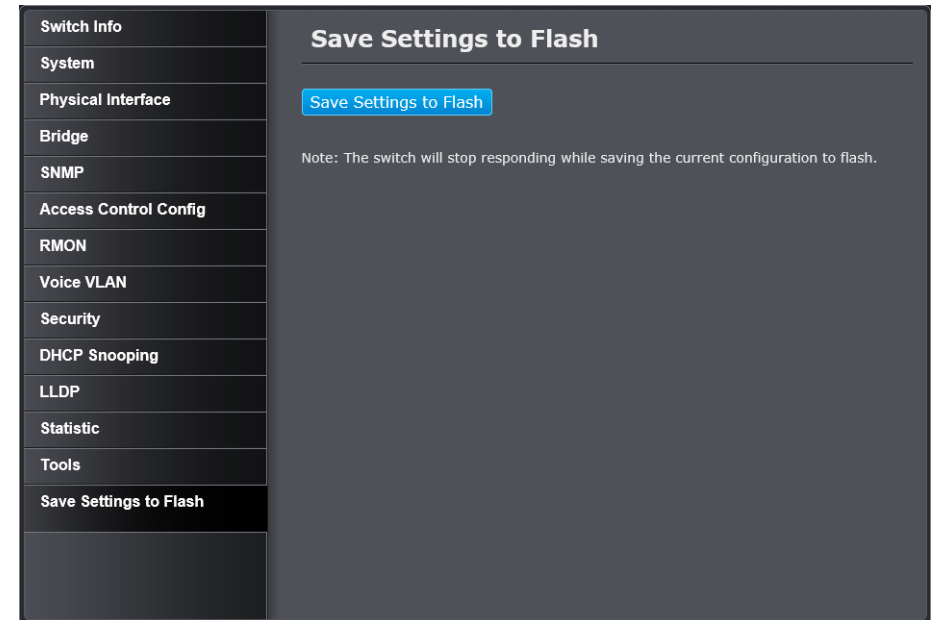
PING Test Settings

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 Pings Requests: Specifies the number of ping requests you want the switch to perform.

Click **Start** to start the network connectivity ping test. After the ping test, click **Show Ping Results** to check the ping test result.

Save Settings to Flash***Save Settings to Flash***


The screenshot shows a web interface for saving settings to flash. On the left is a vertical menu with the following items: Switch Info, System, Physical Interface, Bridge, SNMP, Access Control Config, RMON, Voice VLAN, Security, DHCP Snooping, LLDP, Statistic, Tools, and Save Settings to Flash. The 'Save Settings to Flash' item is highlighted. The main content area is titled 'Save Settings to Flash' and contains a blue button labeled 'Save Settings to Flash'. Below the button is a note: 'Note: The switch will stop responding while saving the current configuration to flash.'

Click **Save Settings to Flash** button to save the change on the flash to make sure the change is permanent.

Web Smart Switch Management Utility

The **TRENDnet Management Utility** allows you to do the following:

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

System Requirements

Operating System: Windows® 8.1, Windows8, Windows 7, Windows Vista, or Windows XP

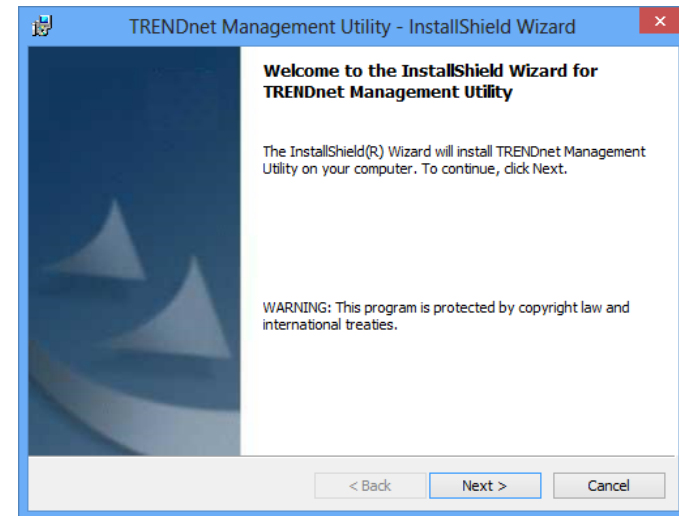
Installation

1. Insert the included CD-ROM into your computer's CD-ROM drive.
2. At the CD Autorun Prompt window, click **Run Autorun.exe**.

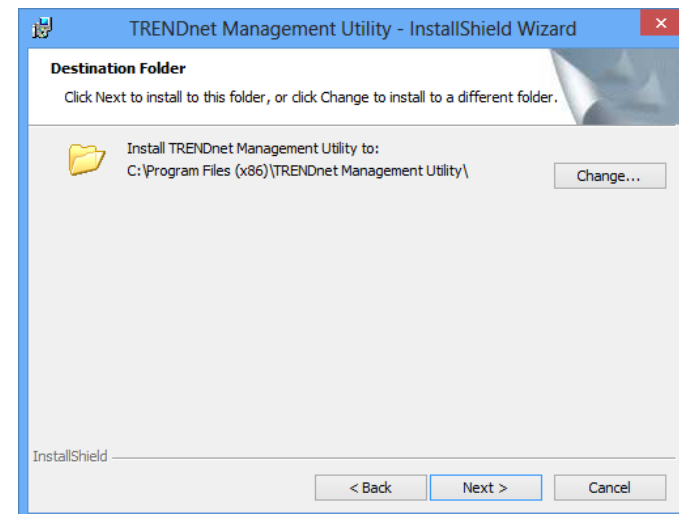
Note: If the Autorun prompt does not appear automatically, open the CD contents and double-click Autorun.exe.

3. At the CD-ROM main menu, click Install Utility.

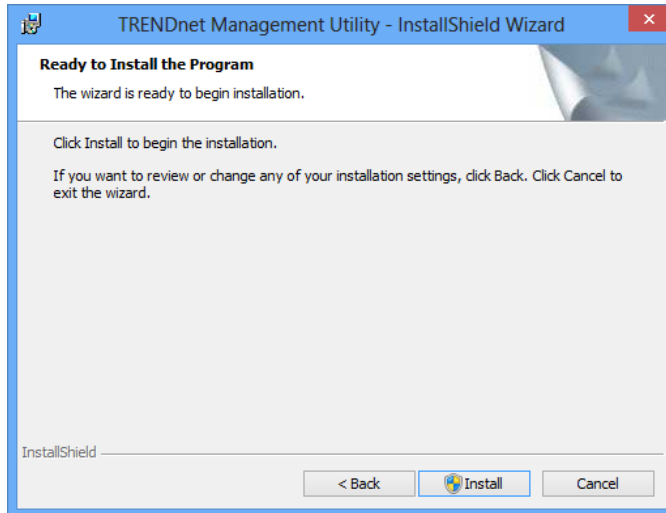
4. At the Utility installation window, click **Next**.



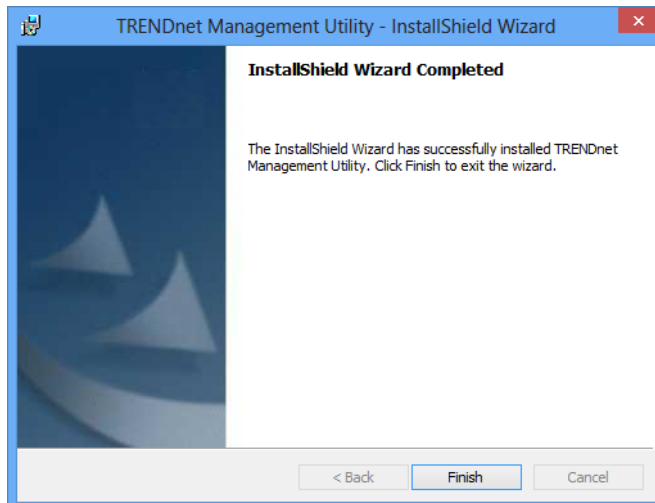
5. At the Install Location installation window, click **Next**.



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



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



Using the Utility

Launching the Utility

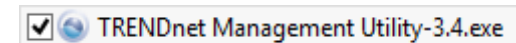
Upon completing the software installation, a desktop shortcut is automatically created.

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



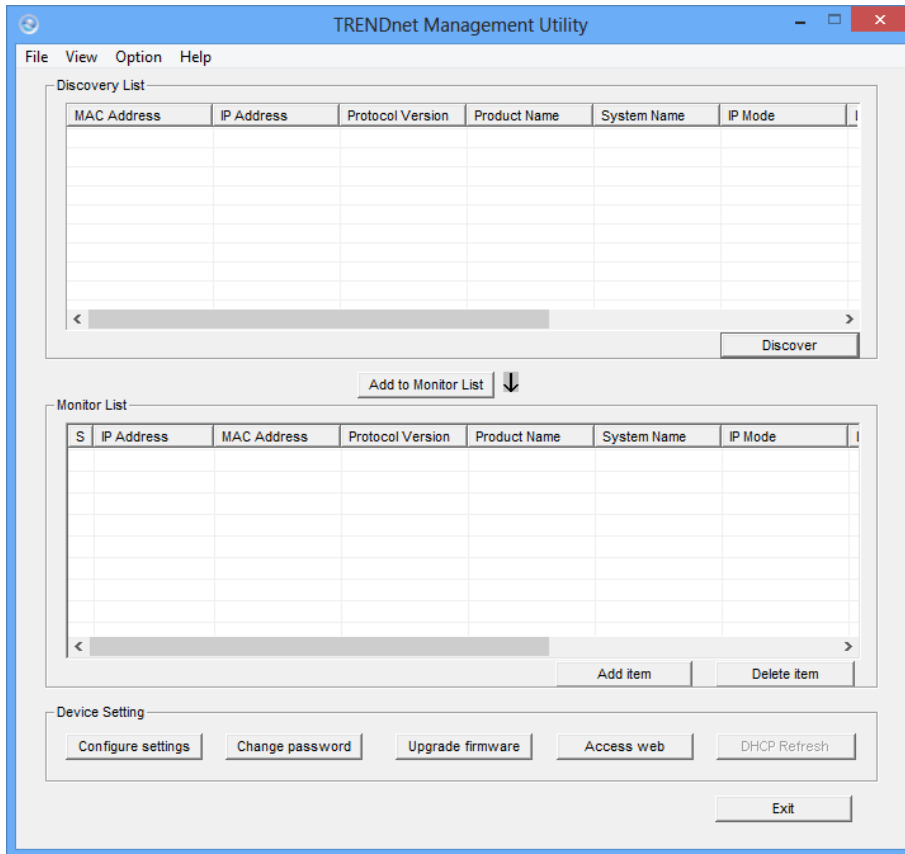
You can also launch the utility from the Start Menu programs.

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



Discovery List

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



Click on the **Discovery** button, you can list all the Web Smart Management switches in the discovery list.

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

Discovery List

MAC Address: Shows the device MAC Address.

IP Address: Shows the current IP address of the device.

Protocol version: Shows the version of the Utility protocol.

Product Name: Shows the device product name.

System Name: Shows the appointed device system name.

IP Mode: Shows the DHCP status of the device.

Location: Shows where the device is located.

Subnet Mask: Shows the Subnet Mask set of the device.

Gateway: Shows the Gateway set of the device.

Group Interval: The IGMP group interval time.

Monitor List

S: Shows the system symbol of the Web-Smart device, represent for device system is not alive.

IP Address: Shows the current IP address of the device.

MAC Address: Shows the device MAC Address.

Protocol version: Shows the version of the Utility protocol.

Product Name: Shows the device product name.

System Name: Shows the appointed device system name.

IP Mode: Shows the DHCP status of the device.

Location: Shows where the device is located.

Subnet Mask: Shows the Subnet Mask set of the device.

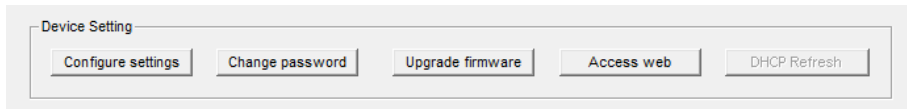
Gateway: Shows the Gateway set of the device.

Group Interval: The IGMP group interval time.

Add Item: To add a device to the **Monitor List** manually, enter the IP Address of the device that you want to monitor.

Delete Item: To delete the device in the **Monitor List**.

Device Setting



Configuration Setting:

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

S	IP Address	MAC Address	Protocol Version	Product Name	System Name	IP Mode
	192.168.10.200	0014d12d18de	2.001.006	TEG-082WS		Static

Select the device in the Discovery list or Monitor List and press **Configure settings** button, then it will appear, after entering the data that you want to change, you must enter the password and then click on **Set** to switch configuration. The default password of TRENDnet Web Smart Switches is **admin**.

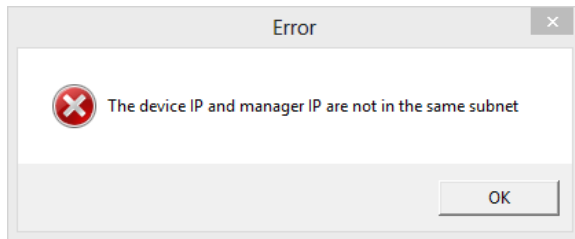
Password Change:

You can use this **Password Change** when you need to change the password, fill in the password needed in the dialog box and then click on **Set** button to proceed the password change.

Firmware Upgrade:

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

Note: Make sure your computer is in the same sub net with the switch management IP. Otherwise, you are going to have this error message.



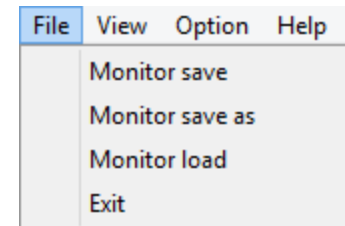
Access Web:

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

DHCP Refresh:

Click on the **DHCP Refresh** button to refresh IP address of selected device form DHCP server. (Only applies if Web Smart switch IP address settings are set to DHCP).

Main Menu Options



In the **File** tab, you can find **Monitor Save**, **Monitor Save As**, **Monitor Load** and **Exit** actions to choose.

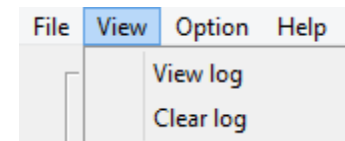
File Tab

Monitor Save: To record the setting of the Monitor List to the default, when you open the Web Management Utility next time, it will auto load the default recorded setting.

Monitor Save As: To record the setting of the Monitor List in appointed filename and file path.

Monitor Load: To manually load the setting file of the Monitor List.

Exit: To exit the Web Management Utility.

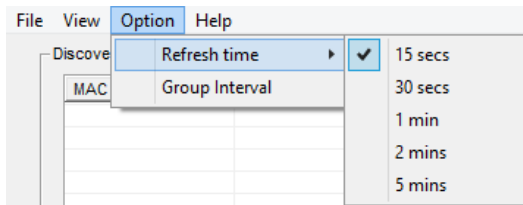


In the **View** tab, there are **view log** and **clear log** actions to choose.

View Tab

View Log: To show the event of the Web Management Utility and the device.

Clear Log: To clear the log.

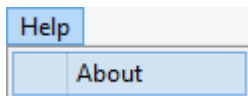
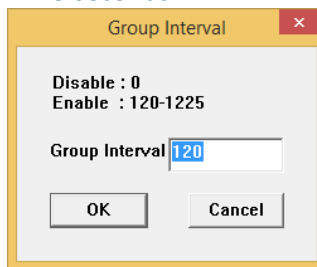


In the **Option** tab, you can set the **Refresh Time** and **Group Interval**.

Option Tab

Refresh Time: This function helps you to refresh the time of monitoring the device. Choose 15 secs, 30 secs, 1 min, 2 min and 5 min to select the time of monitoring.

Group Interval: This is IGMP group interval. The range is from 120 to 1225 seconds.



In the **Help** tab, you can find the utility information with **About** action, it will show out the version of the Web Management Utility.



Technical Specifications

Hardware

- Standards:**
- IEEE 802.1D
 - IEEE 802.1Q
 - IEEE 802.1S
 - IEEE 802.1X
 - IEEE 802.1p
 - IEEE 802.1w
 - IEEE 802.3
 - IEEE 802.3u
 - IEEE 802.3x
 - IEEE 802.3z
 - IEEE 802.1ab
 - IEEE 802.3ab
 - IEEE 802.3ad
 - IEEE 802.3az

- Interface:**
- 8 x Gigabit Ports (Ports 1-8)
 - 2 x Shared SFP Slots (shared with ports 7-8)
 - LED indicators
 - Reset button

- Cabling Network:**
- 10Base-T: UTP/STP Cat. 5 cable (100 m)
 - 100Base-TX: UTP/STP Cat. 5, 5e cable (100 m)
 - 1000Base-T: UTP/STP Cat 5e, 6 cable (100 m)

- Mini-GBIC:**
- LC (Multi-Mode): 50/125um~62.5/125um
 - LC (Single Mode): 9/125um~10/125um

Buffer Memory: 1MB

Filtering Address Table: 16K MAC address entries

Switch: Up to 16Gbps

Fabric/Capacity:

Forwarding Rate: 11.9 M pps (64-byte packet size)

LED Display: • PWR (Power): Green

- Speed: 10Mbps (Off), 100Mbps (Orange), Gigabit (Green)
- Link/Activity: Connected (Solid Green), Activity (Blinking Green)
- Duplex: Full-duplex (Solid Green), Half-duplex (off)
- SFP: 10 (Off), 100Mbps (Orange), Gigabit (Green)
 - 10/100Mbps Activity (Blinking Orange)
 - Gigabit Activity (Blinking Green)

Power Input: 100~240VAC, 50/60Hz internal power supply

Power Consumption: 13.8W (max.)

Fan/Acoustics: Fanless design

Dimensions: 280 x 180 x 44 mm (11 x 7.1 x 1.7 in.)
19 in. width rack mountable (with rack mount hardware installed with 1U height.)

Weight: 1.5 kg (3.4 lbs)

Operating Temperature: 0° - 45° C (32° ~ 113° F)

Storage: -10° - 70° C (14° - 158° F)

Humidity: Max. 90% (non-condensing)

Software

- Management:**
- HTTP/HTTPS (SSL v2/3 TLS) Web based GUI
 - SNMP v1, v2c, v3
 - RMON v1
 - Static Unicast MAC Address
 - Enable/disable 802.3az Power Saving
 - LLDP
 - Virtual Cable Test

- IPv6: IPv6 Neighbor Discovery, IPv6 Static IP, DHCPv6, Auto configuration

- MIB:**
- MIB II RFC 1213
 - Bridge MIB RFC 1493
 - Bridge MIB Extension RFC 2674
 - SNMPv2 MIB RFC 1907
 - Ethernet Interface MIB RFC 1643
 - Ethernet –like MIB RFC 2863
 - Interface Group MIB RFC 2233
 - MIB Traps Convention RFC 1215
 - RMON MIB RFC 1757, RFC 2819
 - 802.1p MIB RFC 2674
 - RADIUS Client Authentication MIB RFC 2618
 - LLDP-MIB IEEE 802.1ab
 - Ping MIB RFC 2925, RFC 4560

- Spanning Tree:**
- 802.1d STP (Spanning Tree Protocol)
 - 802.1w RSTP (Rapid Spanning Tree Protocol)
 - 802.1s MSTP (Multiple Spanning Tree Protocol)

- Link Aggregation**
- Static Link Aggregation
 - 802.3ad Dynamic LACP

- Quality of Service:**
- 802.1p Class of Service (CoS)
 - DSCP (Differentiated Services Code Point)
 - Bandwidth Control per port
 - Queue Scheduling: Strict Priority, Weighted Round Robin (WRR)

- VLAN:**
- Multiple management VLAN assignment
 - Asymmetric VLAN
 - 802.1Q Tagged VLAN
 - Dynamic GVRP
 - Up to 256 groups, ID Range 1-4094
 - Private VLAN (Protected Ports)
 - Voice VLAN (10 user defined OUIs)

- Multicast:**
- IGMP Snooping v1, v2, v3 (per VLAN)
 - Static Multicast Address
 - Up to 256 multicast entries

Port Mirror: RX, TX, or both

- Access Control:**
- 802.1X Port-Based Network Access Control, RADIUS, TACACS+
 - Local Dial In User Authentication
 - DHCP Snooping (per VLAN)
 - Loopback Detection
 - Duplicated Address Detection
 - Denial of Service (DoS)

- ACL IPv4 L2-L4 & IPv6:**
- MAC Address
 - VLAN ID
 - Ether Type (IPv4 only)
 - IP Protocol 0-255
 - TCP/UDP Port 1-65535
 - 802.1p
 - DSCP (IPv4 only)
 - IPv6 Address (IPv6 only)

Flow Control 802.3x Flow Control for Full-Duplex and back pressure for Half-Duplex

Firmware Update Support TFTP firmware update, TFTP backup and restore, via Web Browser

Utility OS Compatibility Windows® 8.1, Windows® 8, Windows® 7, Windows® Vista, Windows® XP, Windows® 2003/2008 Server.

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?

A:

1. Check your hardware settings again.
2. Make sure the Power and port Link/Activity lights are lit.
3. Make sure your network adapter TCP/IP settings are set to use the static IP.
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

Q:

If my switch IP address is different than my network's subnet, what should I do?

A:

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?

A:

Using the TRENDnet Samrt Switch Management Utility to find your smart switch. Or, you can reset your smart switch to factory default.

To reset the smart switch, 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?

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.

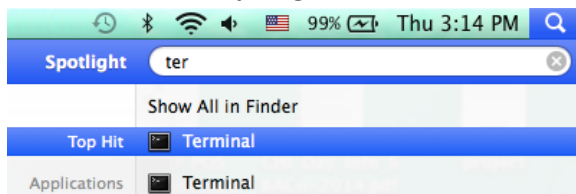
Command Line

Windows 2000/XP/Vista/7

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. Enter **Terminal** in **Spotlight** to look for the **Terminal** app.

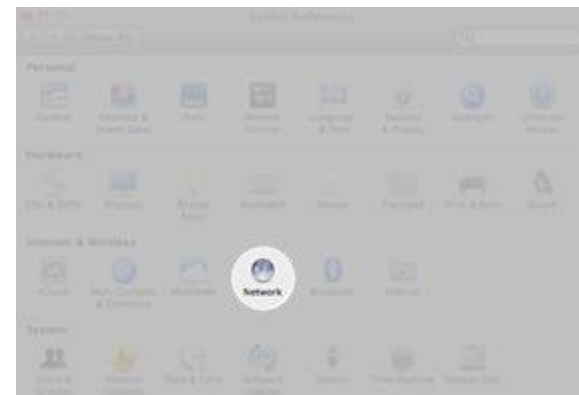
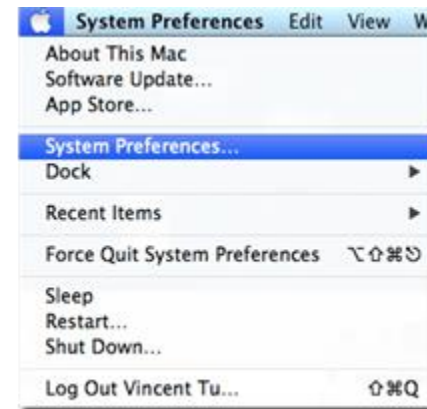


2. Click on **Terminal** to launch the command prompt.
3. In the command prompt, enter `ifconfig` to display all network interface status on your MAC.

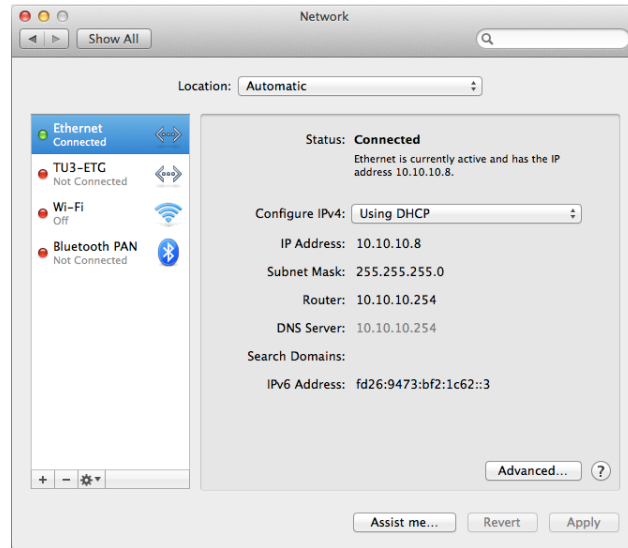
Graphic User Interface

MAC OS X

1. Click the **Apple logo** in the top-left corner of your screen. Click on **System Preferences...**. In the Internet and Wireless section, click on **Network**.



2. Select the network card you want to configure on the left banner and the network adapter status is showing here.

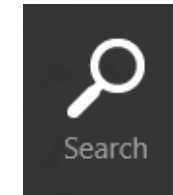


How to setup a static IP address on your computer's network card

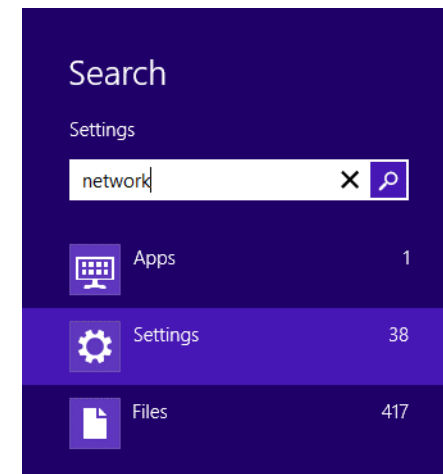
Note: Before setup, make sure that you have a unique static IP address available which will not cause the network address collision.

Windows 8

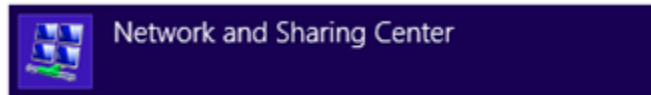
1. Open the Charms bar by moving the mouse to the top right corner of the screen or press the **Windows Key + C** and click on Search.



2. Type "network" in the search box and click Settings to focus your search.



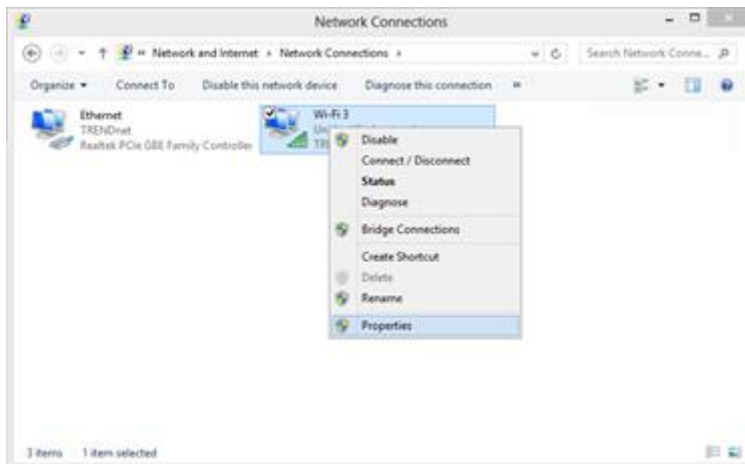
3. Choose **Network and Sharing Center**



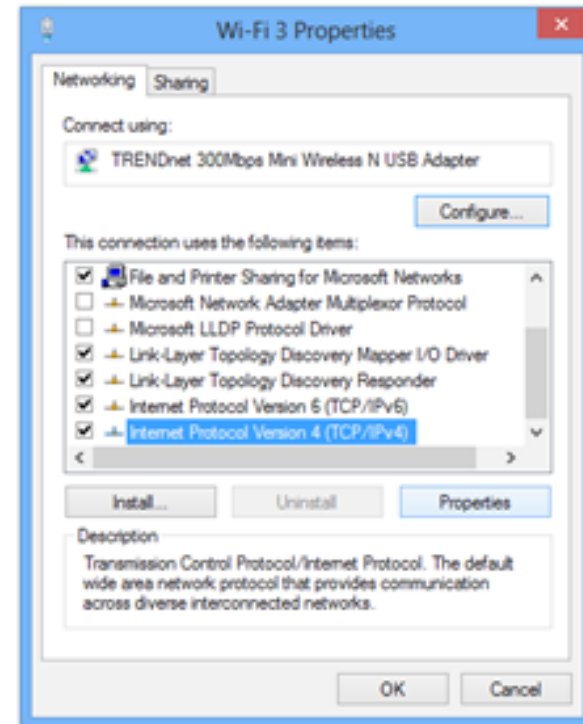
4. Click **Change adapter settings** on the left-hand side.



5. Click **Properties** on the selected network adapter.



6. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.

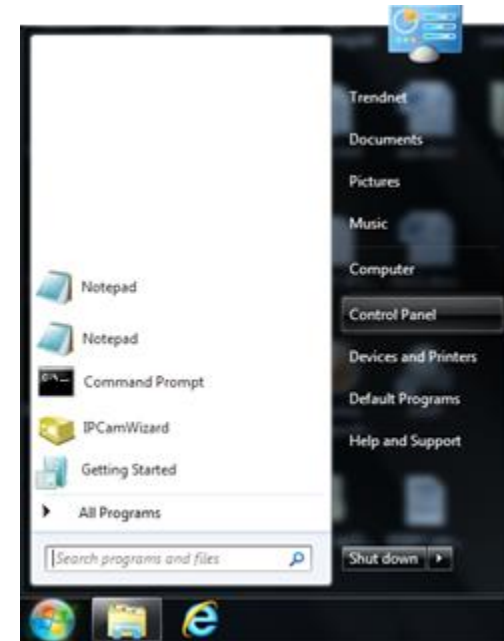


- Click **Use the following address** and enter the static IP address and related information. For setting up the TEW-737HRE, you can enter 192.168.10.10 as your IP address, 255.255.255.0 as the Subnet mask. Leave the other fields blank. Click **OK** to apply the changes.



Windows 7

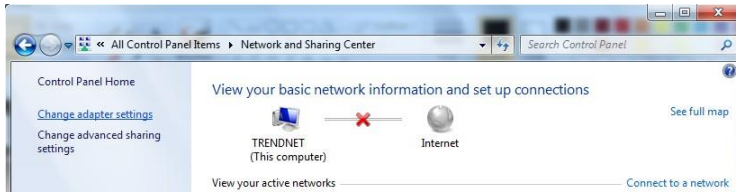
- Click **Control Panel** from the **Start** menu.



- Type "network" in the search box to focus your selection. Click on **Network and Sharing Center**



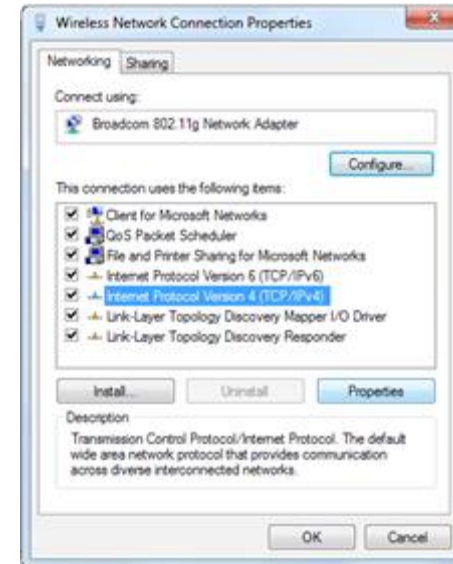
3. Click **Change adapter settings** on the left-hand side.



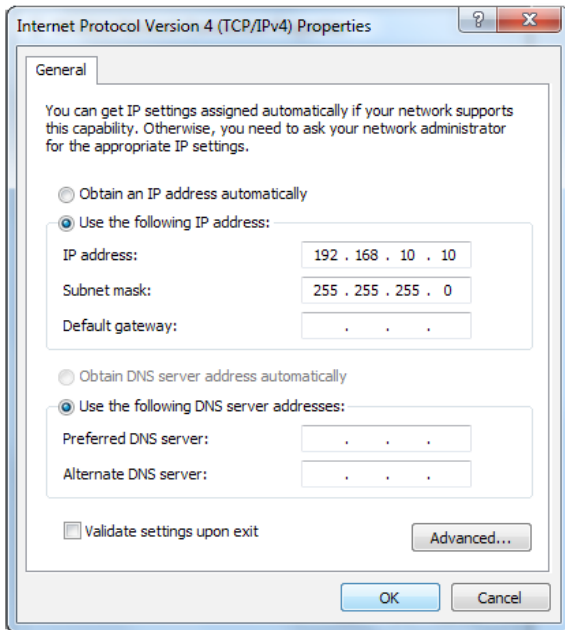
4. Click **Properties** on the selected network adapter.



5. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click Properties

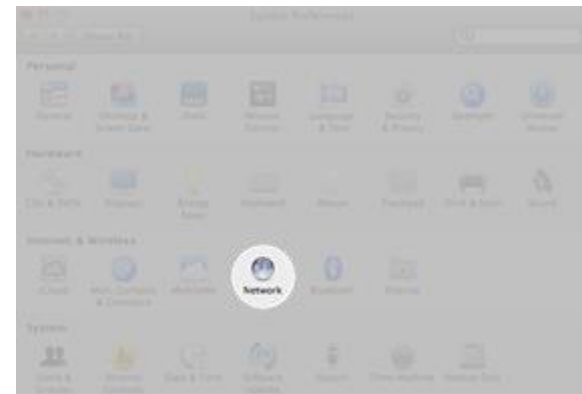
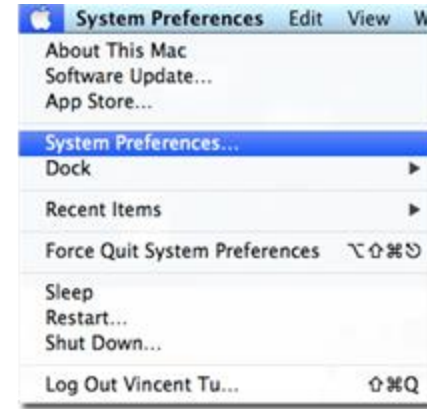


- Click Use the following address and enter the static IP address and related information. For setting up the TEW-737HRE, you can enter 192.168.10.10 as the IP address, 255.255.255.0 as the Subnet mask. Leave other fields blank. Click OK to apply the changes.



OS X

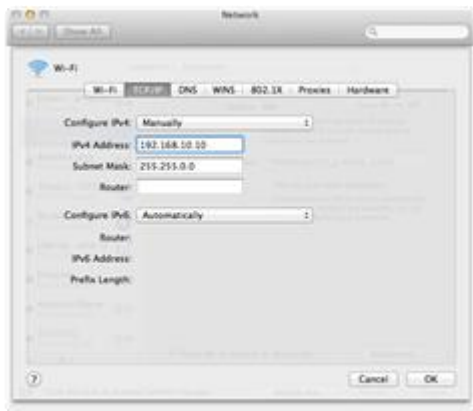
- Click the **Apple logo** in the top-left corner of your screen. Click on **System Preferences...**. In the Internet and Wireless section, click on **Network**.



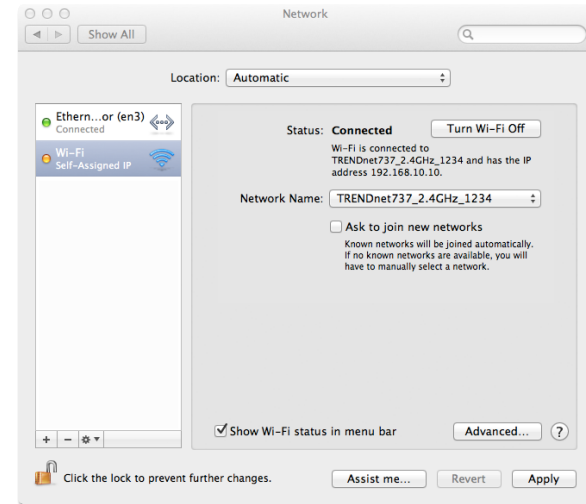
4. Select the network card you want to configure on the left banner (e.g. Wi-Fi). Click **Advanced**.



5. Choose TCP/IP. In Configure IPv4, select Manually. Input the static IP address, subnet mask, and your router IP address. (In order to setup the TEW-737HRE, you can put in 192.168.10.10 as the IP address, 255.255.255.0 as the subnet mask and leave router in blank. Click **OK** to exit advanced setup.



6. Click **Apply** to apply the changes.



How to find your MAC address?

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.

MAC OS X

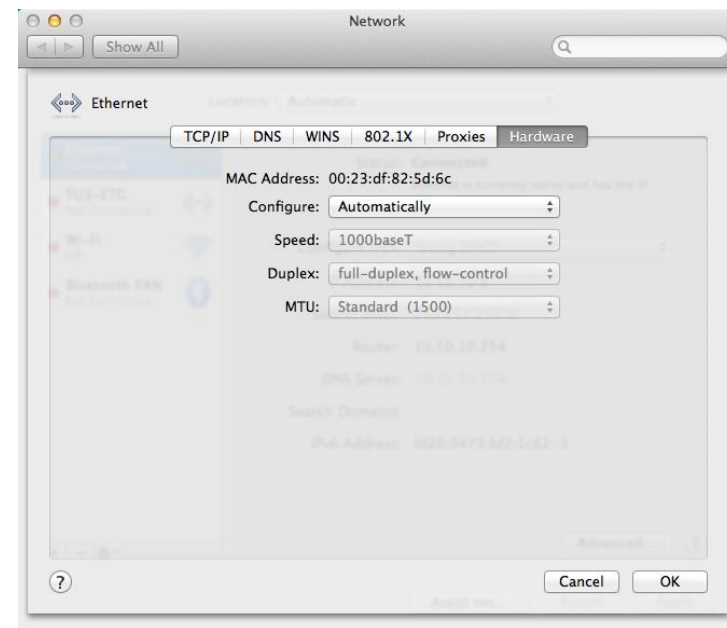
1. Click the **Apple logo** in the top-left corner of your screen. Click on **System Preferences...** . In the Internet and Wireless section, click on **Network**.



2. Select the network card you want to configure on the left banner (e.g. Wi-Fi). Click **Advanced**.



3. Click **Hardware** to find out the MAC address of the network adapter.



Regulations

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:

FCC 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.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

This device complies with the essential requirements of the Directive 2004/108/EC and 2006/95/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the Directive 2004/108/EC and 2006/95/EC:

- EN60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011
- AS/NZS CISPR 22: 2009 Class A
- EN 55022: 2010 Class A
- EN 55024: 2010
- EN 61000-3-2: 2006 + A1: 2009 + A2: 2009 Class A
- EN 61000-3-3: 2008



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.

Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEG-082WS je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2004/108/ES a 2006/95/ES.
Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEG-082WS overholder de væsentlige krav og øvrige relevante krav i direktiv 2004/108/EF og 2006/95/EF.
Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEG-082WS in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2004/108/EG und 2006/95/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEG-082WS vastavust direktiivi 2004/108/EÜ ja 2006/95/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, TRENDnet, declares that this TEG-082WS is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC and 2006/95/EC.
Español [Spanish]	Por medio de la presente TRENDnet declara que el TEG-082WS cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2004/108/CE y 2006/95/CE.

Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΤΡΕΝΔΝΕΤ ΔΗΛΩΝΕΙ ΟΤΙ ΤΕΓ-082WS ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2004/108/ΕΚ, 2006/95/ΕΚ κλπ.
Français [French]	Par la présente TRENDnet déclare que l'appareil TEG-082WS est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2004/108/CE, 2006/95/CE et.
Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEG-082WS è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2004/108/CE e 2006/95/CE.
Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TEG-082WS atbilst Direktīvas 2004/108/EK un 2006/95/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEG-082WS atitinka esminius reikalavimus ir kitas 2004/108/EB ir 2006/95/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEG-082WS in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2004/108/EG en 2006/95/EG.
Malti [Maltese]	Hawn hekk, TRENDnet, jiddikjara li dan TEG-082WS jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2004/108/KE u 2006/95/KE.
Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEG-082WS megfelel a vonatkozó alapvető követelményeknek és az 2004/108/EK és a 2006/95/EK irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEG-082WS jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2004/108/WE i 2006/95/.
Português [Portuguese]	TRENDnet declara que este TEG-082WS está conforme com os requisitos essenciais e outras disposições da Directiva 2004/108/CE e 2006/95/CE.
Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEG-082WS v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2004/108/ES in 2006/95/ES.
Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TEG-082WS spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2004/108/ES a 2006/95/ES.
Suomi [Finnish]	TRENDnet vakuuttaa täten että TEG-082WS tyyppinen laite on direktiivin 2004/108/EY ja 2006/95/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar TRENDnet att denna TEG-082WS står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2004/108/EG och 2006/95/EG.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

- TEG-082WS – 3 Years Warranty

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 (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. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

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").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look 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 go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.

August 1, 2014

TEG-082WS User's Guide V1.0



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