User's Guide

TRENDnet®

Managed Industrial L2 Switch Series

Contents

Product Overview

TI-RG262i / TI-RP262i

TRENDnet's Industrial Gigabit L2 Managed Rackmount Switch Series offers advanced layer 2 managed features with enhanced traffic controls to meet the evolving demands of today's SMB networks. Each industrial layer 2 rackmount switch is equipped with an IP30 rated metal enclosure, designed to withstand a high degree of vibration and shock, while operating within a wide temperature range of -40° – 70° C (-40° – 158° F) for industrial environments. Our industrial layer 2 rackmount switch models feature copper gigabit ports for high-speed device connections, as well as SFP slots that support 100/1000Base-FX SFP modules for long distance fiber networking applications. These industrial layer 2 rackmount switches feature a fanless design that eliminates operating noise and lowers energy consumption.

These Industrial Gigabit L2 Managed Rackmount Switch Series provides an intuitive web-based management interface. Each TRENDnet industrial layer 2 rackmount switch supports advanced traffic management controls, troubleshooting, and SNMP monitoring. Advanced managed switch features include LACP to group ports together and increase bandwidth between switches, VLANs for segmenting and isolating virtual LAN groups, QoS to prioritize traffic, port bandwidth controls, SNMP monitoring, and more, making each TRENDnet industrial layer 2 rackmount switch a powerful solution for SMB networks.

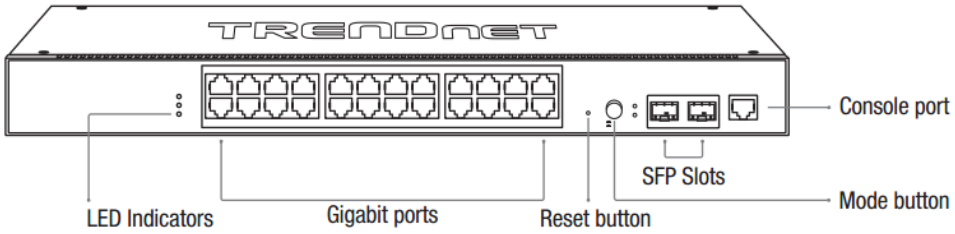
Package Contents

In addition to your switch, the package includes:

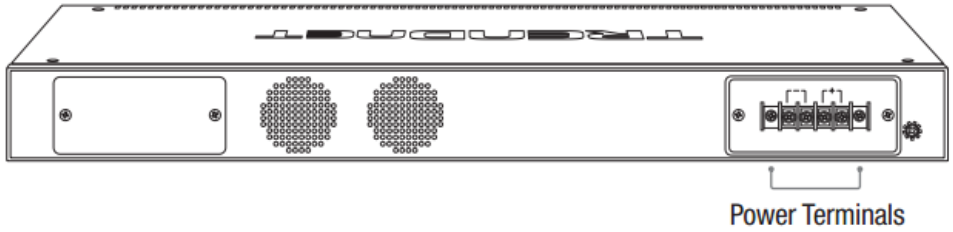
- Quick Installation Guide
- Console cable (RJ-45 to RS-232)
- Rackmount Kit

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

Front View



Rear View



- **LED Indicators –** Indicators on the left display **ALM**, **PWR**, and **POST** status. LEDs on each port show the status of the port based on the mode selected using the **Mode Button**.
- **Mode Button (TI-RP262i only) –** Press the mode button to change the **left** LED indicator on each port to display Speed, or PoE Mode. When button is depressed it will display PoE, when not pressed it will indicate if 1000Mbps.
- **Gigabit Ethernet PoE+ Ports (1-24) –** Connect either network PoE+ or non-PoE devices.
- **Reset Button –** Press and hold the button for less than 5 seconds to reboot, or more than 5 seconds to reset to factory default.
- **SFP Ports (25-26) –** Supports optional 1000BASE-SX/LX mini-GBIC modules for uplink or downlink connections.
- **Console Port –** The console port is a female RJ-45, use the included RJ-45 male to RS-232 serial DB-9 female console cable.
- **Power Terminals –** Using proper gauge wire, terminate the leads from your power supply to these power terminals to power your switch.

LED Indicators

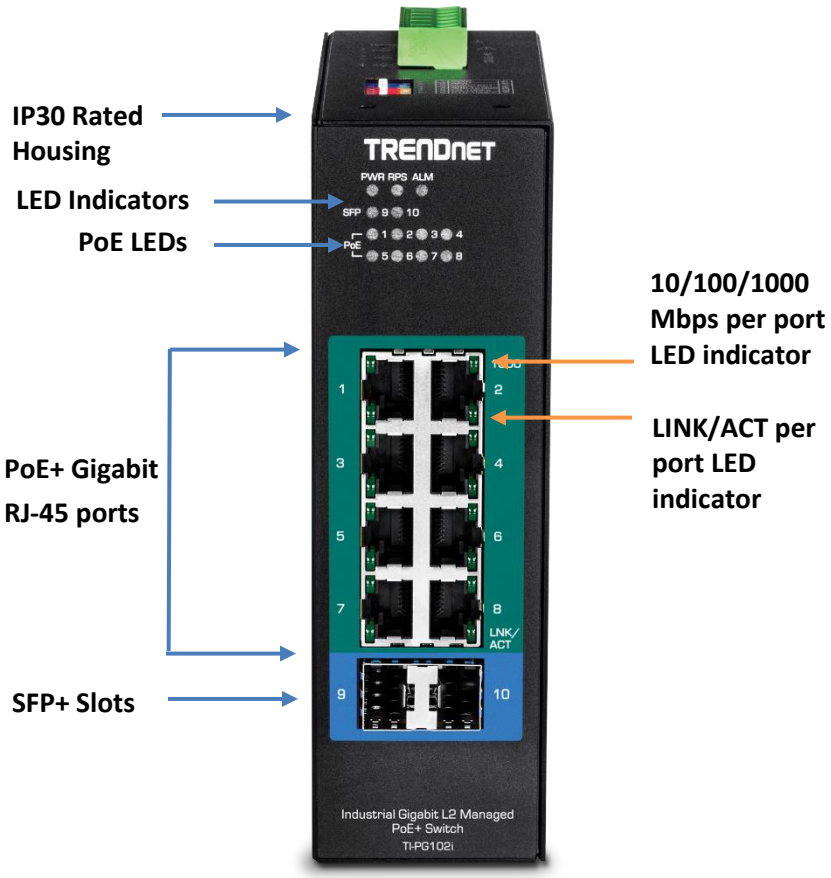
LED	State	Status
PWR (Green)	ON	When the PWR LED is on, the device is using the primary power input source.
	OFF	Primary power input source is off, disconnected, or has failed.
ALM (Red)	ON	Indicates alarm has been triggered on DIP switch settings and signal sent out through ALM terminals on terminal block to third party alarm device.
	OFF	No alarm triggered.
POST (Green)	ON	Device is ready and completed boot process.
	OFF	Device is not ready.
SFP Slot 6 (Green)	ON	SFP link is connected.
	BLINKING	Data is transmitting/receiving.
	OFF	SFP link is disconnected.
PoE Ports 1-4 (Green) (TI-RP262i only)	ON	PoE supplied to Ethernet port.
	OFF	No PoE supplied to Ethernet port.
Ports 1-5 1000M (Green)	ON	Ethernet port is connected.
10/100M (Off)	BLINKING	Data is transmitting/receiving.
	OFF	Ethernet port is not connected.

- **Ports 1-4 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes. Supports Auto MDI-X and capable of delivering up to 30W (802.3at PoE+) per port.
- **Port 5 -** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes. Supports Auto MDI-X
- **SFP Port 6 –** Designed to operate at Gigabit speeds.
- **Reset/Reboot Button –** Push the button for 10 seconds and release to reset the switch to factory defaults. Push the button for 3 seconds and release to reboot.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)

Note: *For any unused ports or SFP ports, it is recommended to leave the rubber plugs installed during operation.*

TI-PG102i / TI-PG102i-M

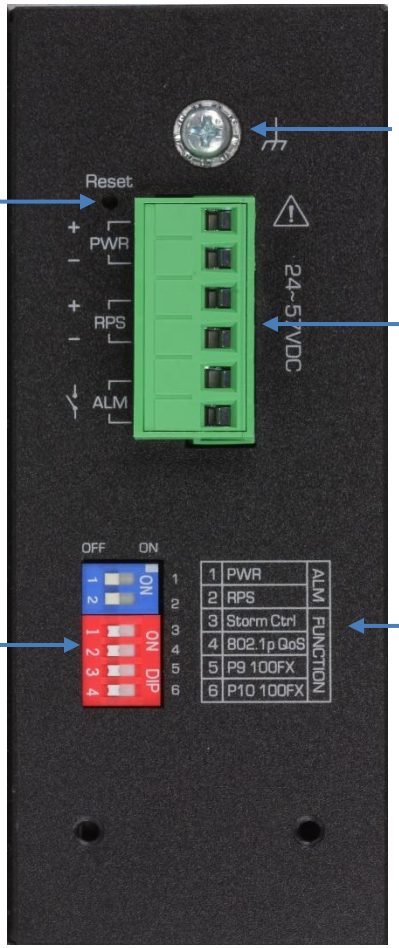
Front View



LED	Status	Function
PWR	OFF	Terminal block PWR failure or disconnected
	ON	Terminal block PWR is connected
RPS	OFF	Terminal block RPS failure or disconnected
	ON	Terminal block RPS is connected
ALM (Red)	OFF	No alarm setup
	ON	PWR/RPS failure or disconnected
PoE (Ports 1 – 8)	OFF	No PoE power supplied
	ON	PoE power is supplied to connected device
10/100/ 1000Mbps (Ports 1 – 8)	OFF	Link speed established at 10Mbps or 100Mbps
	ON	Link speed established at 1000Mbps
LINK/ACT (Ports 1 – 8)	OFF	No link/port is disconnected
	ON	Port connection is established
	Blinking	Data transmission
SFP 9-10	OFF	No link/SFP is disconnected
	ON	SFP link is established
	Blinking	Data transmission

- **PoE+ Ports 1-8 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes while simultaneously providing power to supported PoE devices. Supports Auto MDI-X.
- **SFP Ports 9-10 –** Designed to operate at Gigabit or 100Mbps speeds.
- **Reset Button –** Push the button for 5-10 seconds and release to reset.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)

Top View



Ground point

Reset Button

6-pin terminal block (PWR, RPS, ALM)

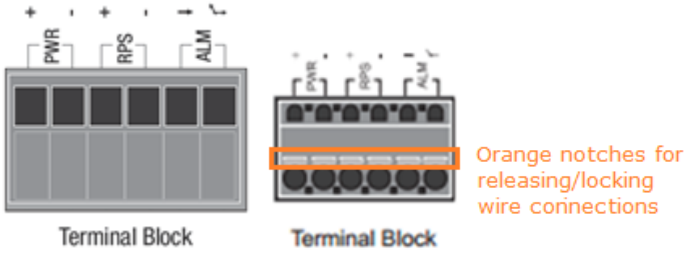
DIP Switches

DIP switch definition

Please note power supply is sold separately

Supported power supplies: TI-S12024 (120W), TI-S24048 (240W), TI-S48048 (480W). Lower wattage power supplies may be used but may result in decreased PoE power budget*

6-pin Removable Terminal Block

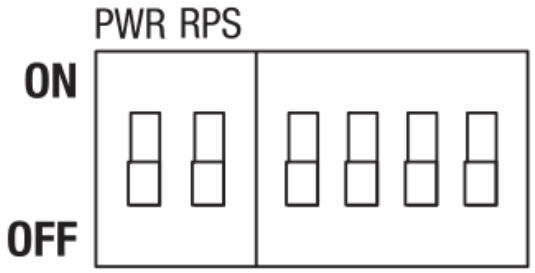


Note: Turn off the power before connecting modules or wires.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Input/Output	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

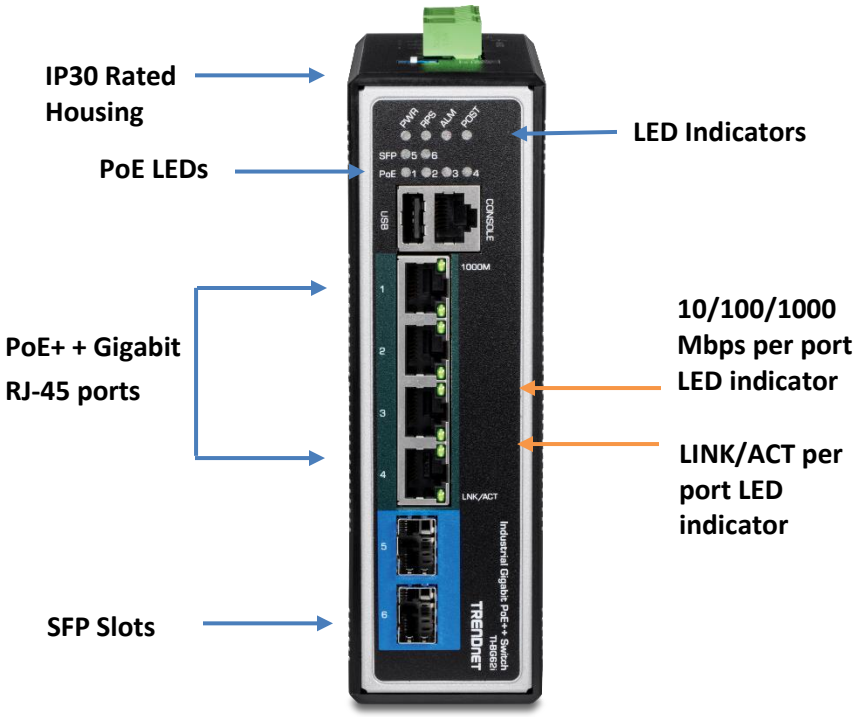
ALM DIP Switches

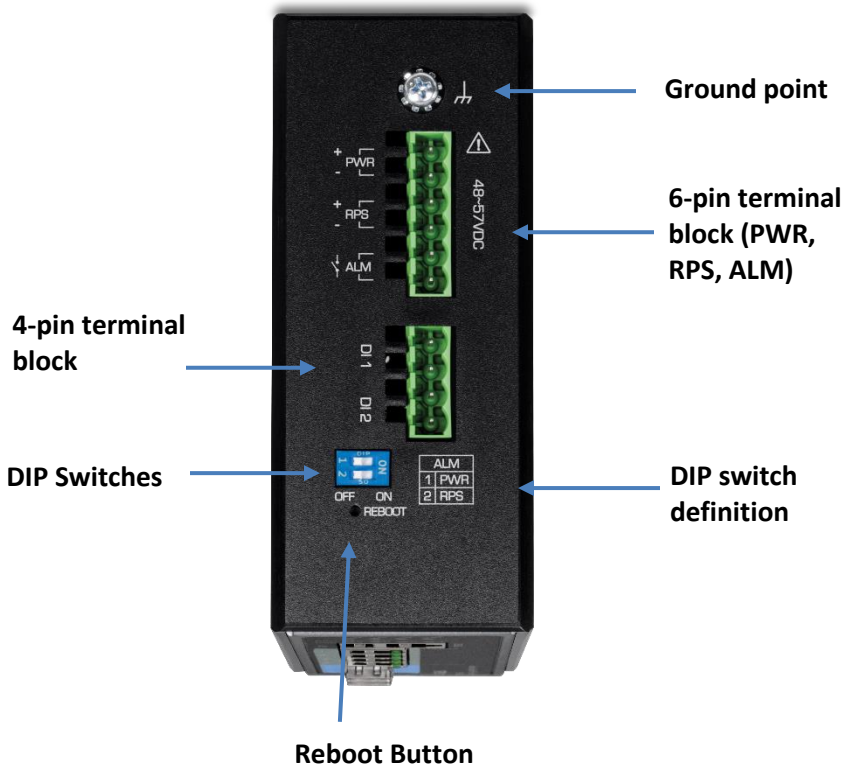


Switch	Status	Function
1	OFF	Disable alarm relay for PWR power input
	ON	Enable alarm relay for power failure on PWR power input
2	OFF	Disable alarm relay for RPS power input
	ON	Enable alarm relay for power failure on RPS power input
3	OFF	Storm control managed by switch configuration
	ON	Enable storm control (Broadcast and DLF rate set to 300pps) Takes precedence over storm control switch configuration
4	OFF	802.1p QoS managed by switch configuration
	ON	Enable 802.1p QoS on ports 1 and 2 (Set CoS priority to tag 4 on ports 1 and 2) Takes precedence over 802.1p QoS switch configuration
5	OFF	Port 9 SFP set to Gigabit speed full duplex
	ON	Port 9 SFP set to 100Mbps speed full duplex
6	OFF	Port 10 SFP set to Gigabit speed full duplex
	ON	Port 10 SFP set to 100Mbps speed full duplex

TI-BG62i

Front View





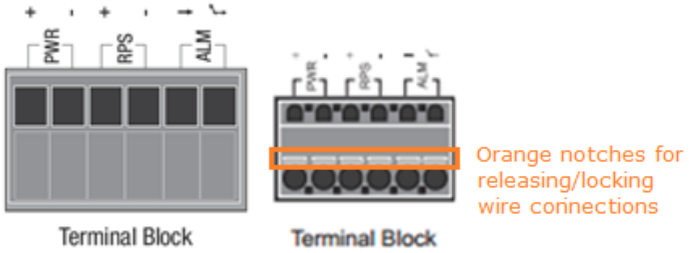
- **PoE++ Ports 1-4 –** Connect either network PoE++ or non-PoE devices.
- **SFP Ports 5-6 –** Designed to operate at Gigabit or 100Mbps speeds.
- **Reset Button –** Push the button for 5-10 seconds and release to reset.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)

Top View

Please note power supply is sold separately

****Supported power supplies: TI-S12024 (120W), TI-S24048 (240W), TI-S48048 (480W). Lower wattage power supplies may be used but may result in decreased PoE power budget****

6-pin Removable Terminal Block

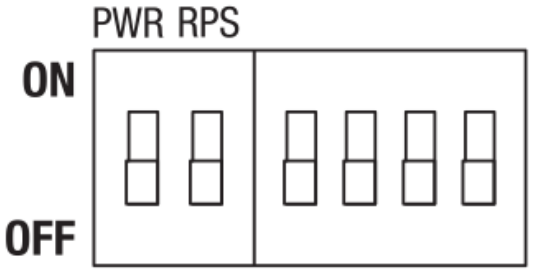


Note: Turn off the power before connecting modules or wires.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Input/Output	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

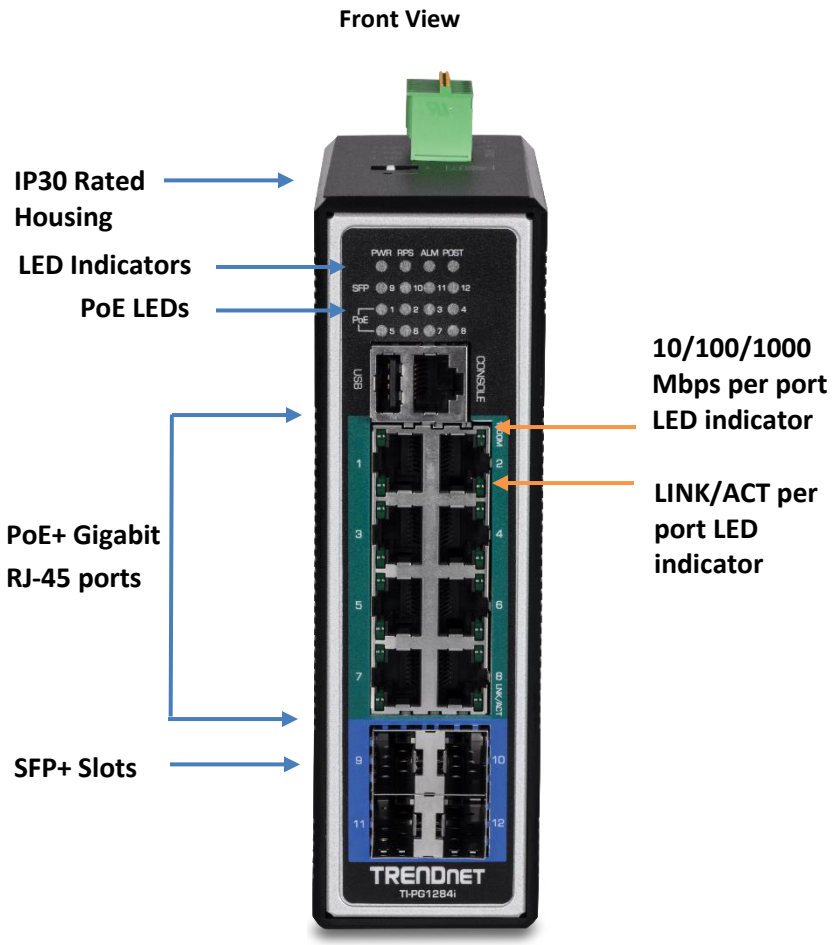
ALM DIP Switches



Switch	Status	Function
1	OFF	Disable alarm relay for PWR power input
	ON	Enable alarm relay for power failure on PWR power input
2	OFF	Disable alarm relay for RPS power input
	ON	Enable alarm relay for power failure on RPS power input

TI-PG1284i

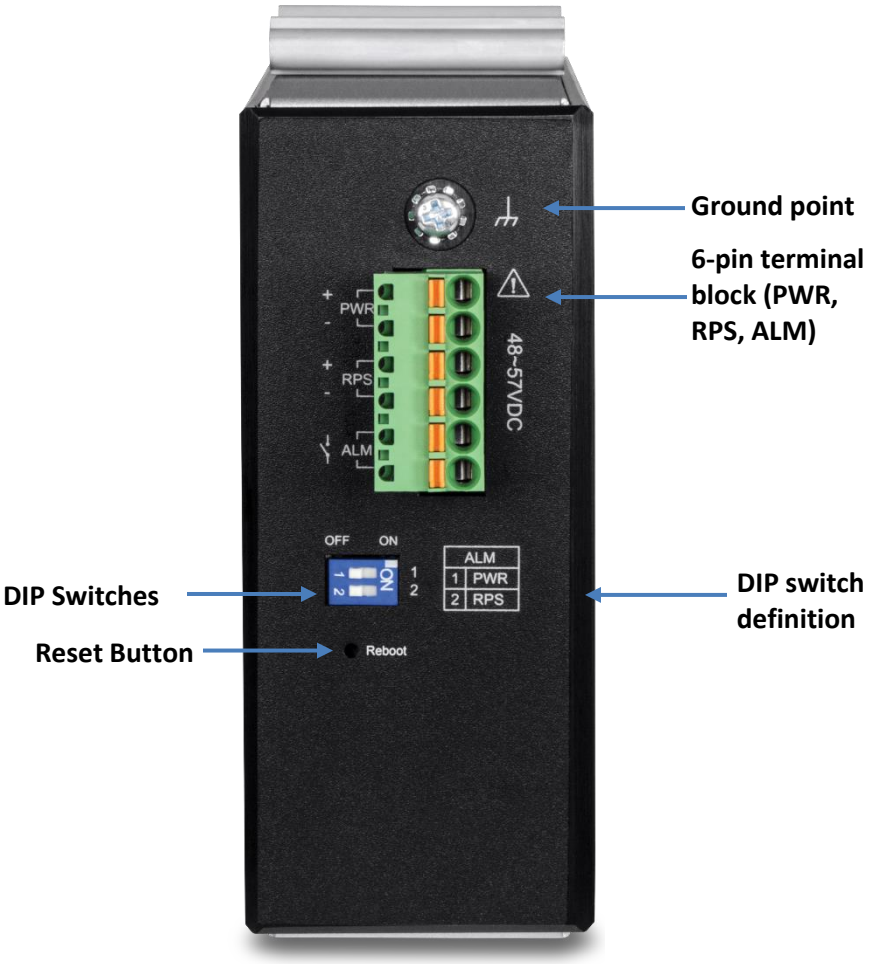
Front View



PWR (Green)	**ON**: Terminal block PWR is connected
	OFF: Terminal block PWR failure
RPS (Green)	**ON**: Terminal block RPS is connected
	OFF: Terminal block RPS failure
ALM (Red)	**ON**: PWR/RPS failure
	OFF: No alarm setup
POST (Green)	**ON**: Device system ready
	Blinking: System is getting ready
	OFF: Device system not ready
10/100/1000 Mbps (Green)	**ON**: Network speed at 1000 Mbps
	OFF: Network speed at 10/100 Mbps
LINK/ACT (Green)	**ON**: Port connection is established
	Blinking: Data is transmitting/receiving
	OFF: Port disconnected
SFP Slots 9 - 12 (Green)	**ON**: SFP port link-up at 1000 Mbps
	Blinking: Data is transmitting/receiving
	OFF: Port disconnected
PoE Ports 1 - 8 (Green)	**ON**: PoE/PoE+ device is connected
	OFF: No PoE power output or no PoE device connected

- **PoE+ Ports 1-8 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes while simultaneously providing power to supported PoE devices. Supports Auto MDI-X.
- **SFP Ports 9-12 –** Designed to operate at Gigabit or 100Mbps speeds.
- **Reset Button –** Push the button for 5-10 seconds and release to reset.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)

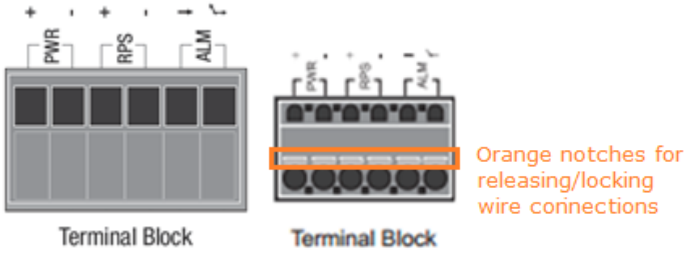
Top View



Please note power supply is sold separately

****Supported power supplies: TI-S12024 (120W), TI-S24048 (240W), TI-S48048 (480W). Lower wattage power supplies may be used but may result in decreased PoE power budget****

6-pin Removable Terminal Block

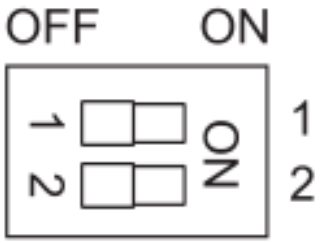


Note: Turn off the power before connecting modules or wires.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Input/Output	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

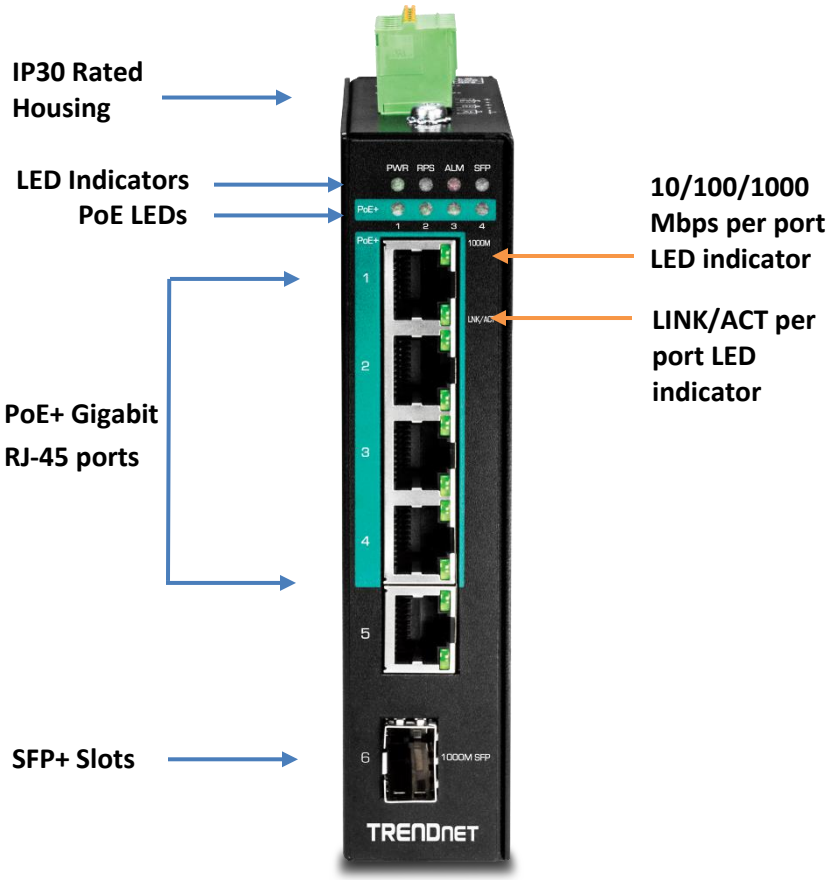
ALM DIP Switches



Switch	Status	Function
1	OFF	Disable alarm relay for PWR power input
	ON	Enable alarm relay for power failure on PWR power input
2	OFF	Disable alarm relay for RPS power input
	ON	Enable alarm relay for power failure on RPS power input

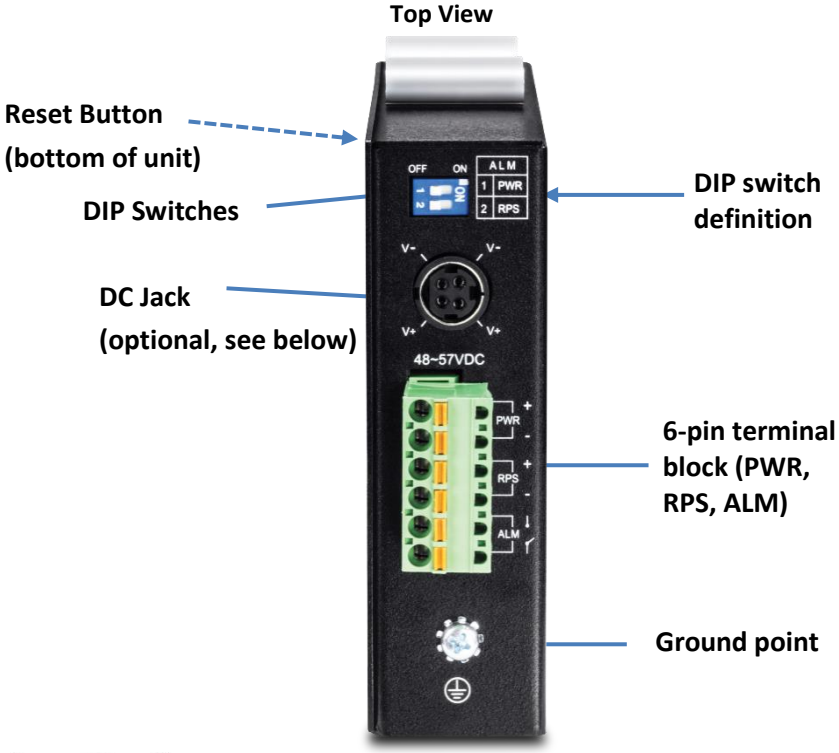
TI-PG541i

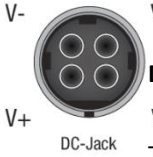
Front View



PWR	**ON**: Terminal block PWR is connected
	OFF: No power or power source connected incorrectly
RPS	**ON**: Terminal block RPS is connected
	OFF: Terminal block RPS fail
ALM (Red)	**ON**: PWR/RPS failure
	OFF: No alarm setup
10/100/1000 Mbps	**ON**: Network speed at 1000 Mbps
	OFF: Network speed at 10/100 Mbps
LINK/ACT	**ON**: Port connection is established
	Blinking: Data is transmitting/receiving
	OFF: Port disconnected
SFP Slot 6	**ON**: SFP port link-up at 1000 Mbps
	Blinking: Data is transmitting/receiving
	OFF: Port disconnected
PoE Ports 1 - 4	**ON**: PoE/PoE+ device is connected
	OFF: No PoE power output or no PoE device connected

- **PoE+ Ports 1-5 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes while simultaneously providing power to supported PoE devices. Supports Auto MDI-X.
- **SFP Port 6 –** Designed to operate at Gigabit or 100Mbps speeds.
- **Reset Button –** Push the button for 5-10 seconds and release to reset.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)





DC Jack Input for External Power Adapter

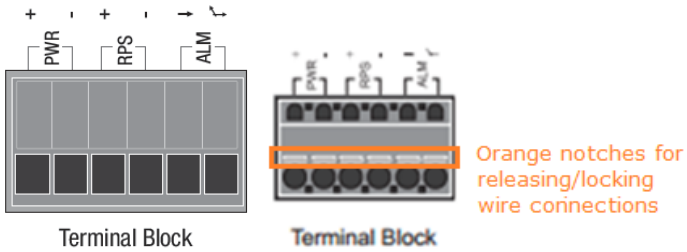
The device includes a DC Jack for an external power adapter and can also be used as an additional redundant power supply (RPS) input.

Please ensure that the external power adapter is supplying 48VDC @ 120W or above. 130W for max. PoE+ power. **Please note power adapter is sold separately (model: 48VDC3000)**

Please note power supply is sold separately

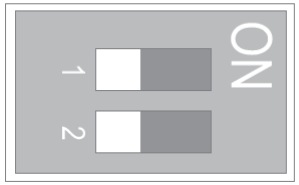
****Supported power supplies: TI-S12024 (120W), TI-S24048 (240W), TI-S48048 (480W). Lower wattage power supplies may be used but may result in decreased PoE power budget****

6-pin Removable Terminal Block



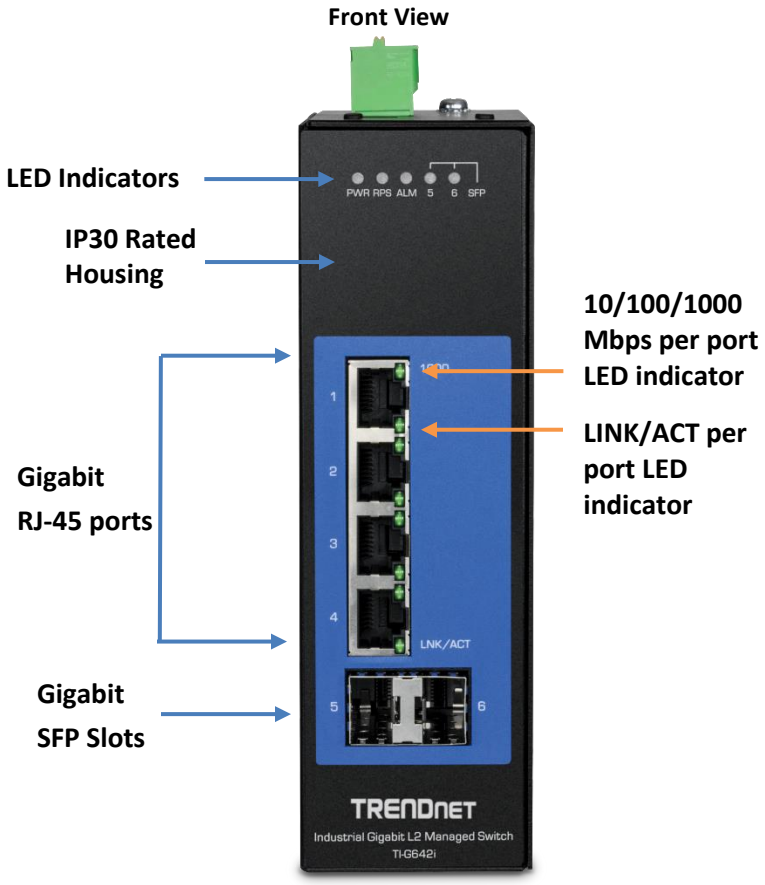
Input/Ouput	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Please ensure that the external power supply is supplying within the range of 48VDC ~ 57VDC @ 120W or above. 130W for max. PoE+ power. **Please note power supply is sold separately (model: TI-24048)** Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Please ensure that the external power supply is supplying within the range of 48VDC ~ 57VDC @ 120W or above. 130W for max. PoE+ power. **Please note power supply is sold separately (model: TI-24048)** Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

ALM DIP Switches



DIP No	Name	State	Status
1	PWR	ON	Primary power input source alarm trigger enabled.
		OFF	Primary power input source alarm trigger disabled.
2	RPS	ON	Redundant power input source alarm trigger enabled.
		OFF	Redundant power input source alarm trigger disabled.

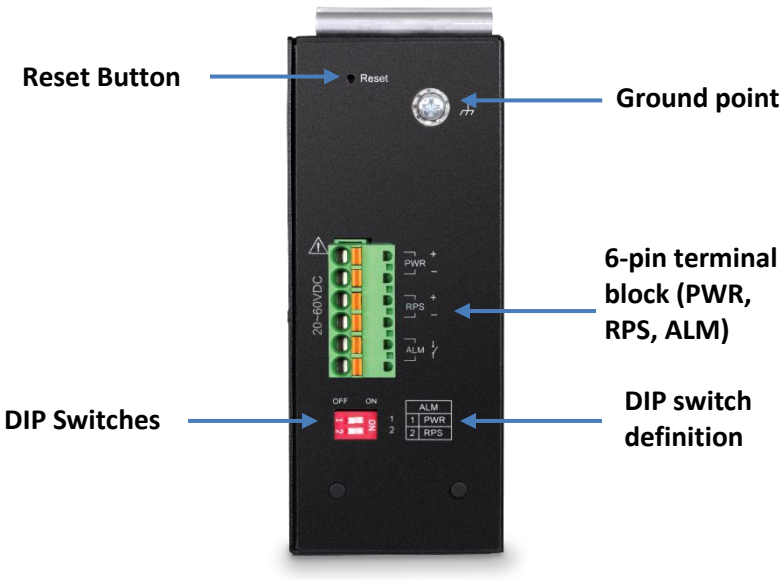
Non-PoE
TI-G642i



LED	Status	Function
PWR	OFF	Terminal block PWR failure or disconnected
	ON	Terminal block PWR is connected
RPS	OFF	Terminal block RPS failure or disconnected
	ON	Terminal block RPS is connected
ALM (Red)	OFF	No alarm setup
	ON	PWR/RPS failure or disconnected
10/100/ 1000Mbps (Ports 1 – 4)	OFF	Link speed established at 10Mbps or 100Mbps
	ON	Link speed established at 1000Mbps
LINK/ACT (Ports 1 – 4)	OFF	No link/port is disconnected
	ON	Port connection is established
	Blinking	Data transmission
SFP 5 – 6	OFF	No link/SFP is disconnected
	ON	SFP link is established
	Blinking	Data transmission

- **Ports 1-4 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes. Supports Auto MDI-X.
- **SFP Ports 5-6 –** Designed to operate at Gigabit speeds.
- **Reset Button –** Push the button for 3 seconds and release to reset to factory defaults.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)

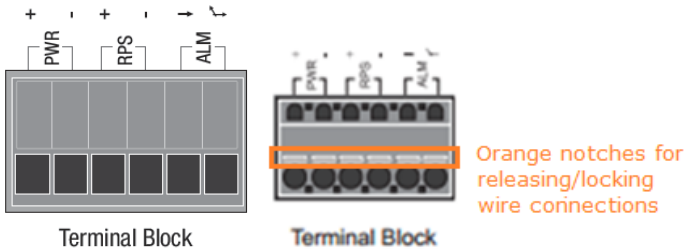
Top View



Please note power supply is sold separately

****Supported power supplies: TI-M6024, TI-S12024 (120W), TI-S24048 (240W) ****

6-pin Removable Terminal Block

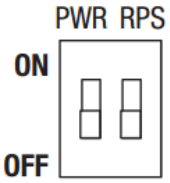


Note: Turn off the power before connecting modules or wires.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

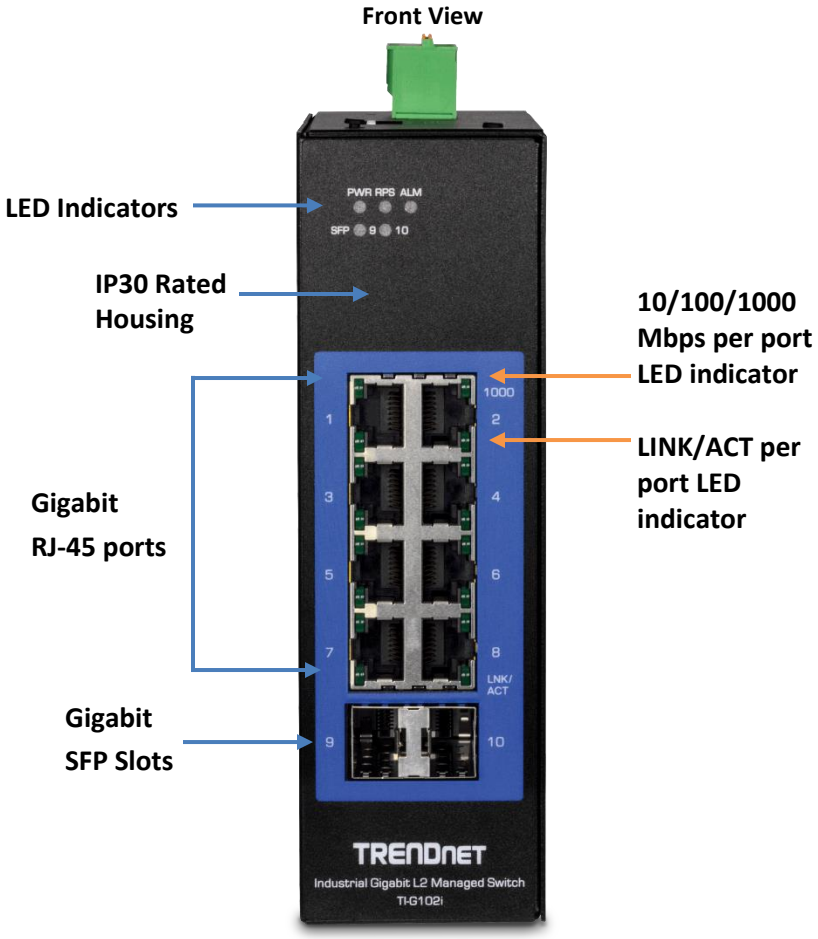
Input/Output	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

ALM DIP Switches



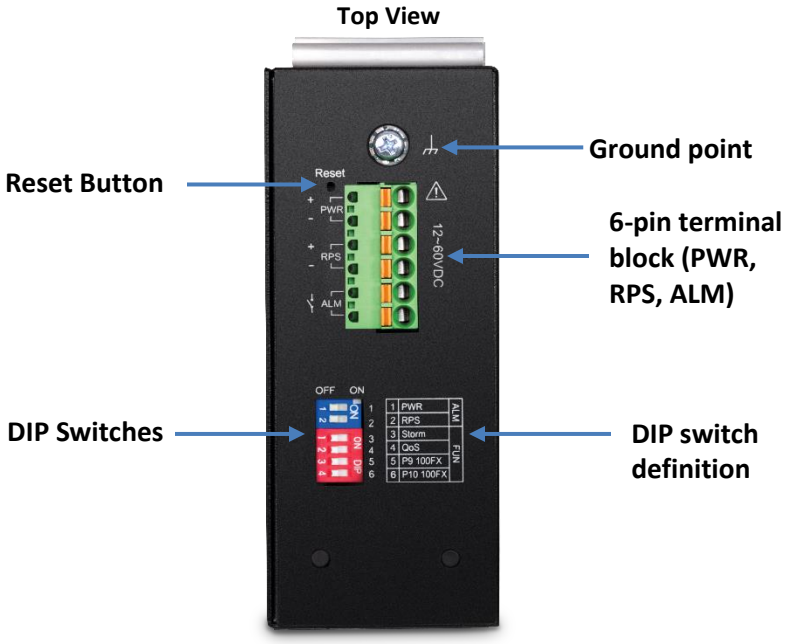
Switch	Status	Function
1	OFF	Disable alarm relay for PWR power input
	ON	Enable alarm relay for power failure on PWR power input
2	OFF	Disable alarm relay for RPS power input
	ON	Enable alarm relay for power failure on RPS power input

TI-G102i



LED	Status	Function
PWR	OFF	Terminal block PWR failure or disconnected
	ON	Terminal block PWR is connected
RPS	OFF	Terminal block RPS failure or disconnected
	ON	Terminal block RPS is connected
ALM (Red)	OFF	No alarm setup
	ON	PWR/RPS failure or disconnected
10/100/ 1000Mbps (Ports 1 – 8)	OFF	Link speed established at 10Mbps or 100Mbps
	ON	Link speed established at 1000Mbps
LINK/ACT (Ports 1 – 8)	OFF	No link/port is disconnected
	ON	Port connection is established
	Blinking	Data transmission
SFP 9 – 10	OFF	No link/SFP is disconnected
	ON	SFP link is established
	Blinking	Data transmission

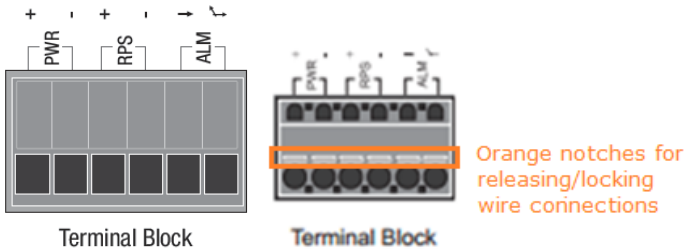
- **Ports 1-8 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes. Supports Auto MDI-X.
- **SFP Ports 9-10 –** Designed to operate at Gigabit or 100Mbps speeds.
- **Reset Button –** Push the button for 3 seconds and release to reset to factory defaults.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)



Please note power supply is sold separately

****Supported power supplies: TI-M6024, TI-S12024 (120W), TI-S24048 (240W) ****

6-pin Removable Terminal Block

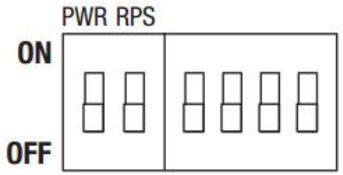


Note: Turn off the power before connecting modules or wires.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Input/Output	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

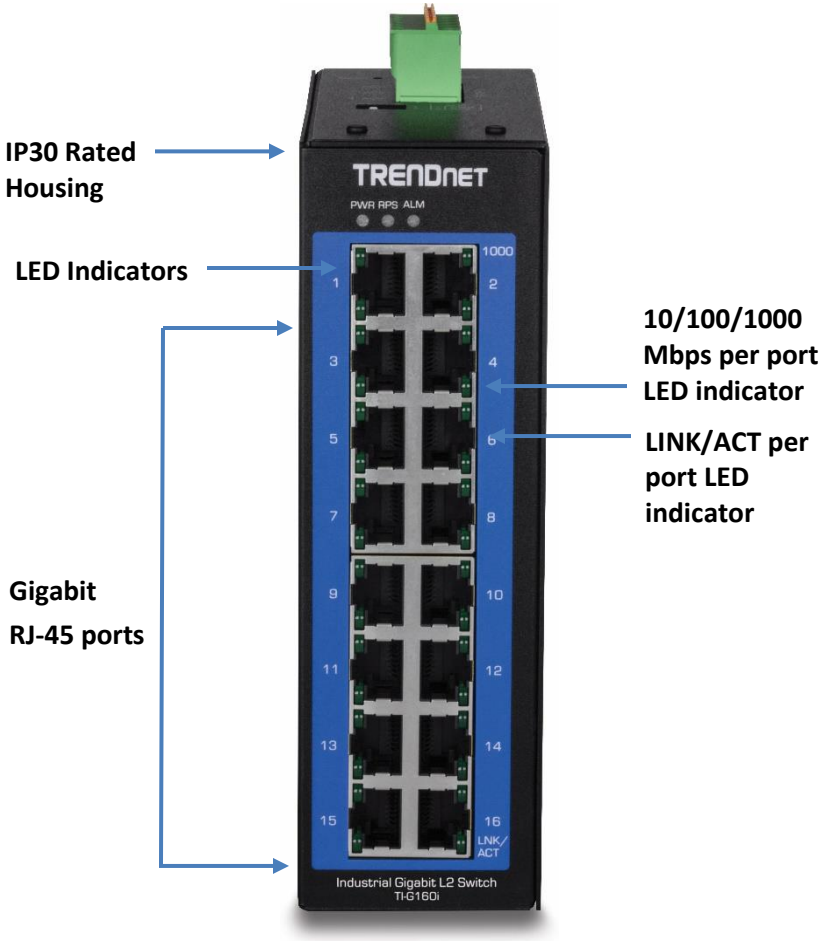
ALM DIP Switches



Switch	Status	Function
1	OFF	Disable alarm relay for PWR power input
	ON	Enable alarm relay for power failure on PWR power input
2	OFF	Disable alarm relay for RPS power input
	ON	Enable alarm relay for power failure on RPS power input
3	OFF	Storm control managed by switch configuration
	ON	Enable storm control (Broadcast and DLF rate set to 300pps) Takes precedence over storm control switch configuration
4	OFF	802.1p QoS managed by switch configuration
	ON	Enable 802.1p QoS on ports 1 and 2 (Set CoS priority to tag 4 on ports 1 and 2) Takes precedence over 802.1p QoS switch configuration
5	OFF	Port 9 SFP set to Gigabit speed full duplex
	ON	Port 9 SFP set to 100Mbps speed full duplex
6	OFF	Port 10 SFP set to Gigabit speed full duplex
	ON	Port 10 SFP set to 100Mbps speed full duplex

TI-G160WS / TI-G160i

Front View

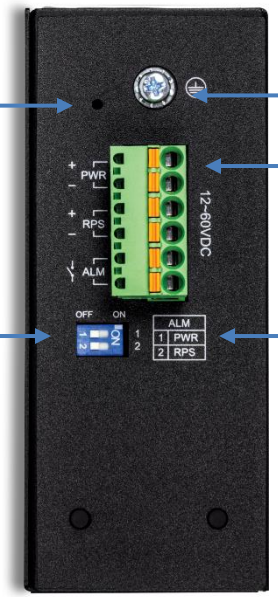


LED Indicators

PWR	**ON**: Terminal block PWR is connected
	OFF: Terminal block PWR failure
RPS	**ON**: Terminal block RPS is connected
	OFF: Terminal block RPS failure
ALM (Red)	**ON**: PWR/RPS failure
	OFF: No alarm setup
10/100/1000 Mbps	**ON**: Network speed at 1000 Mbps
	OFF: Network speed at 10/100 Mbps
LINK/ACT	**ON**: Port connection is established
	Blinking: Data is transmitting/receiving
	OFF: Port disconnected

- **Ports 1-16 –** Designed to operate at 10Mbps, 100Mbps, or Gigabit speed in both half-duplex and full-duplex transfer modes. Supports Auto MDI-X.
- **Reset Button –** Push the button for 3 seconds and release to reset to factory defaults.
- **Grounding point/screw** – The switch chassis can also be connected to a known ground point for additional safety and protection. (grounding wire not included)

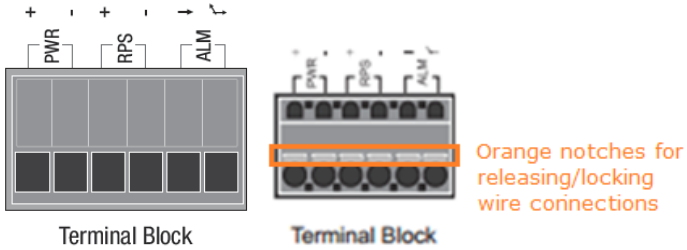
Top View



Please note power supply is sold separately

****Supported power supplies: TI-M6024, TI-S12024 (120W), TI-S24048 (240W) ****

6-pin Removable Terminal Block

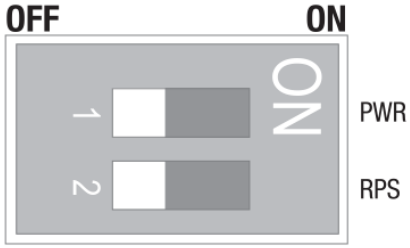


Note: Turn off the power before connecting modules or wires.

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Input/Output	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
RPS Input (+) & (-)	Connects redundant power source (ex. external power supply) to power the device. Device will obtain power from this input secondary priority if primary power input is not available or has failed. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange notches in order release the wiring connections. While holding in released position, insert the wiring into the connection inputs from the external power supply and release the orange notch to lock in the wire connections. Device supports overload current protection and reverse polarity protection.
ALM Output	Connects external alarm and sends output signal if fault is detected based on DIP switch settings. Supports an output with current carrying capacity of 1A @ 24V DC.

ALM DIP Switches



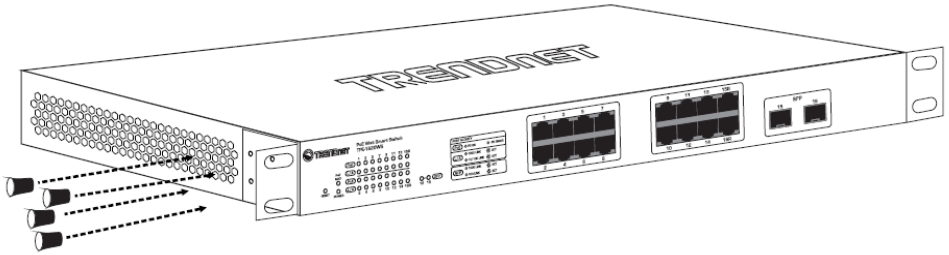
PWR	**ON**: Primary power alarm enabled
	OFF: Primary power alarm disabled
RPS	**ON**: Redundant power alarm enabled
	OFF: Redundant power alarm disabled

Switch Installation

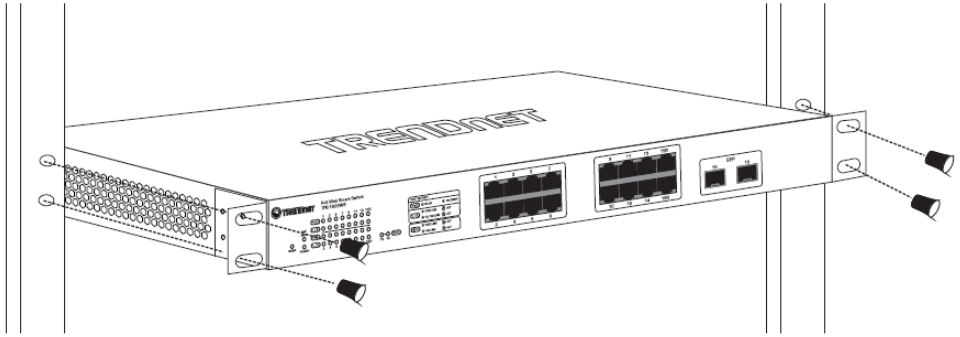
Rack Mount Hardware Installation

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.



DIN-Rail Installation

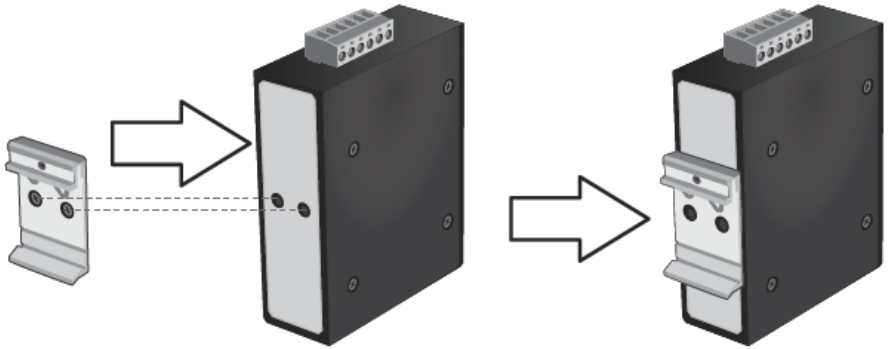
The site where the switch will be installed may greatly affect its performance. When installing, consider the following pointers:

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

- Install the switch in the appropriate location. Please refer to the technical specifications at the end of this manual for the acceptable operating temperature and humidity ranges.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Install the switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- Leave at least 10cm of space at the front and rear of the switch for ventilation.

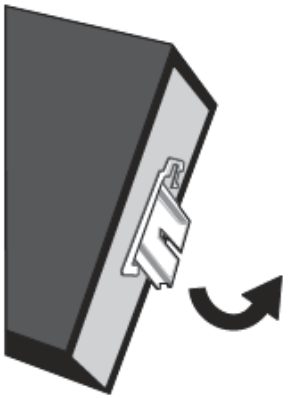
Fasten the DIN-Rail bracket to the rear of the switch using the included fasteners/screws.
Note: *The DIN-Rail bracket may already be installed to your switch when received.*

The movable clip at the top of the DIN-Rail bracket should be on top.



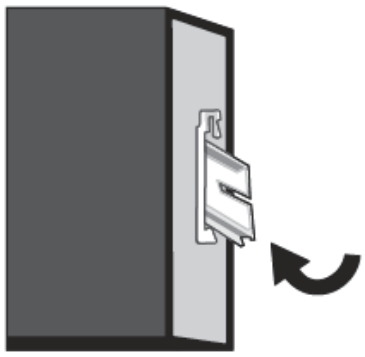
The switch can be installed to a 35mm (W) DIN-Rail located in cabinet, rack, or enclosure.

To mount the switch to a DIN-Rail using the attached DIN-Rail bracket, position the switch in front of the DIN-Rail and hook the bracket over the top of the rail.
Then rotate the switch downward towards the rail until your hear a click indicating the bracket is secure and locked into place.



Mounting the unit

To unmount the switch from the DIN-Rail, slightly pull the switch downwards to clear the bottom of the DIN-Rail and rotate away from DIN-Rail to unmount.



Releasing the unit

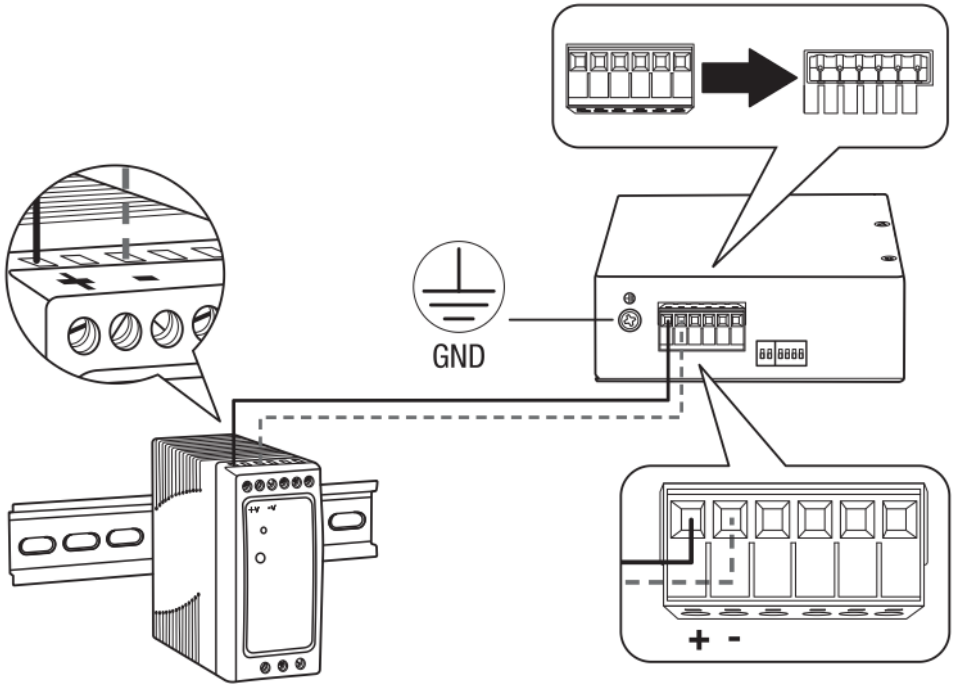
Install power supply connections

Connect the power supply (sold separate, e.g. TRENDnet TI-S24048) to the switch terminal block as shown below.

***Optional**: The switch chassis can also be connected to a known ground point for additional safety and protection (grounding wire not included).*

***Note:** Polarities V+ and V- should match between power supply and connections to switch terminal block.*

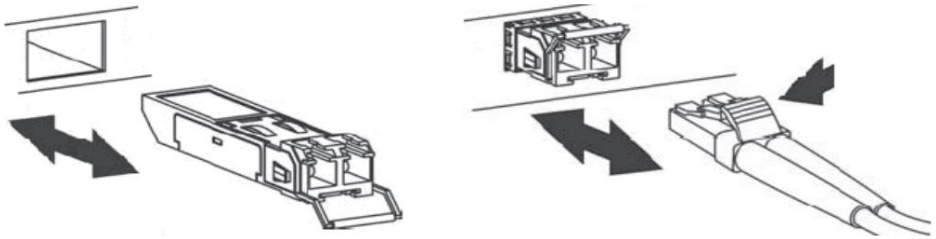
***Note:** The models in the image may be different than your specific model.*



SFP Transceiver/Optical Cable Installation

1. Remove the rubber plug from the SFP port.

   Note: *For any unused ports or SFP ports, it is recommended to leave the rubber plugs installed during operation.*
2. Slide the selected SFP module into the selected SFP slot (Make sure the SFP module is aligned correctly with the inside of the slot)
3. Insert and slide the module into the SFP slot until it clicks into place.
4. Remove any rubber plugs that may be present in the SFP module's slot.
5. Align the fiber cable's connector with the SFP module's mouth and insert the connector
6. Slide the connector in until a click is heard
7. If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module



To properly connect fiber cabling*:* Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Note: When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Setup Wizard

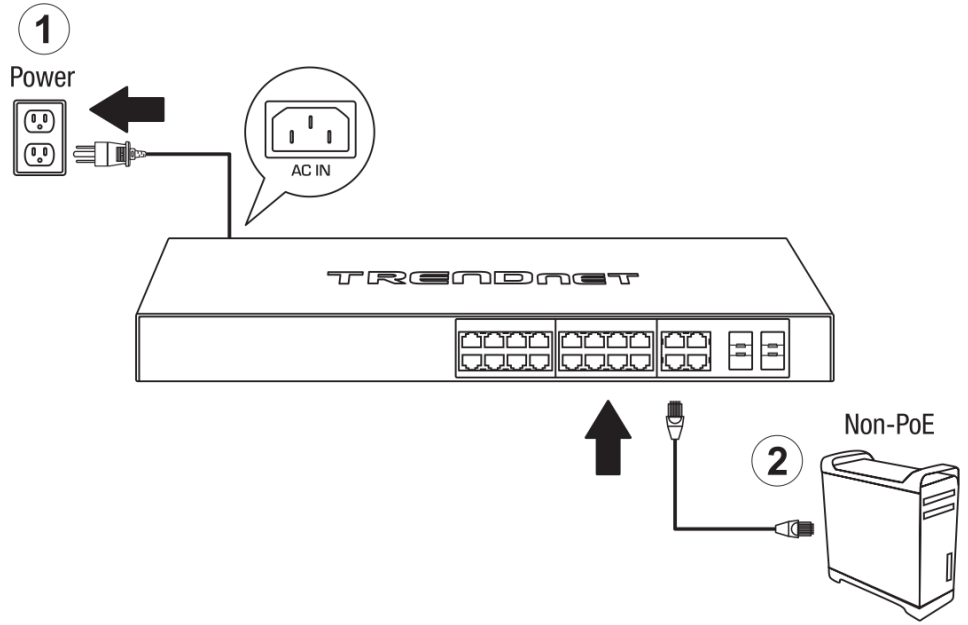
When the switch is reset to factory defaults, the setup wizard will appear on the first login to guide through the initial setup process.

Note: Configuration with TRENDnet Hive Cloud Management requires an existing network with Internet access and DHCP server for automatic IP addressing. The switch must be configured to reach the Internet in order to connect to your TRENDnet Hive Cloud Management account.

Note: The setup wizard must be completed through the web interface. The CLI command line interface is unavailable until the wizard is complete.

Initial Setup

1. Connect the switch as shown in the diagram below:



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.

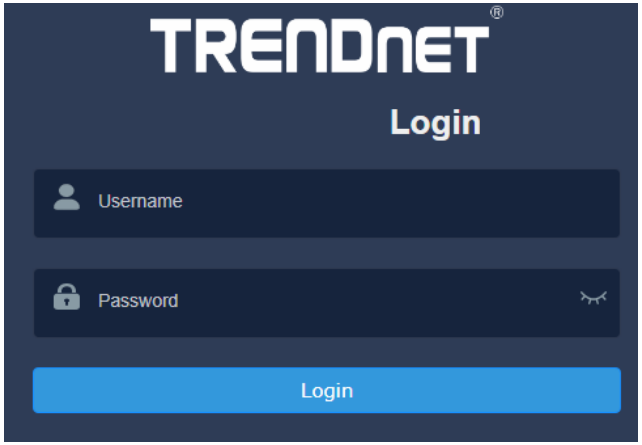
3. Open your web browser, and type the IP address of the switch in the address bar, and then press **Enter**. The default IP address is **192.168.10.200**.

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

User Name: **admin**

Password: **admin**

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



5. Click **Next** on the **Switch Setup Wizard**.

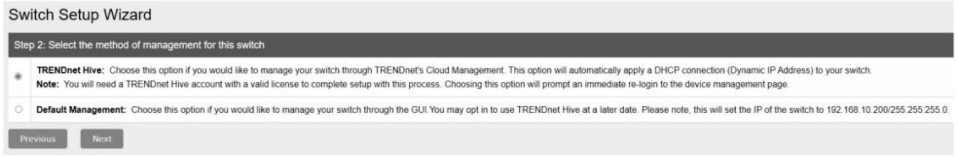
6. You can change the switch administrator password by typing in the new password in the fields provided, then click Next.

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

7. Select the method of management and click **Next**:

-TRENDnet Hive: Manage your switch with TRENDnet's Cloud Management. This option will automatically apply a DHCP connection to your switch.

-Default Management: Manage your switch through the GUI. You may opt-in to use TRENDnet Hive at a later date.



8. Proceed to the following sections depending on the selection above.

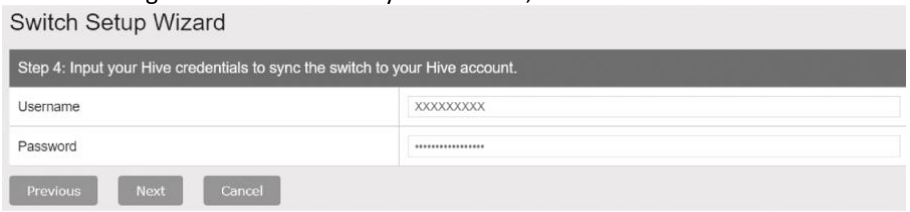
TRENDnet Hive

Follow these steps if you have selected TRENDnet Hive in the setup wizard.

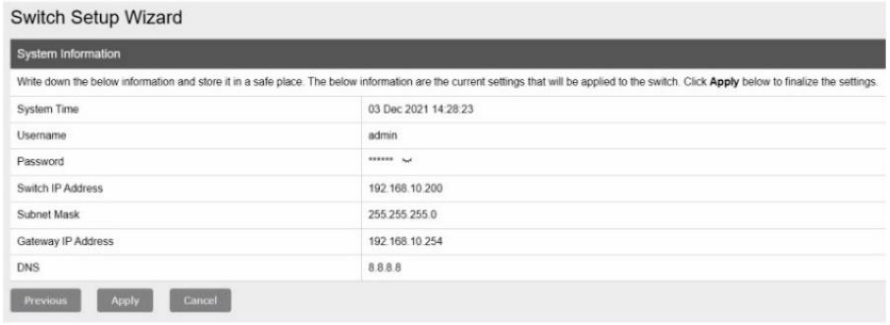
1. Change your computer's network adapter settings to obtain an IP address automatically, as the TRENDnet Hive option automatically applies a DHCP connection to your switch.

2. Select your **Time Zone**, then click **Next**.

3. Enter the user account credentials for your TRENDnet Hive Cloud Management account to register the switch with your account, then click **Next**.



4. The summary page will display all of the configuration settings that were applied through the setup wizard. Click **Apply** to complete the setup wizard.
Note: *You may want to note the new password and IP address settings for local management access to the switch.*

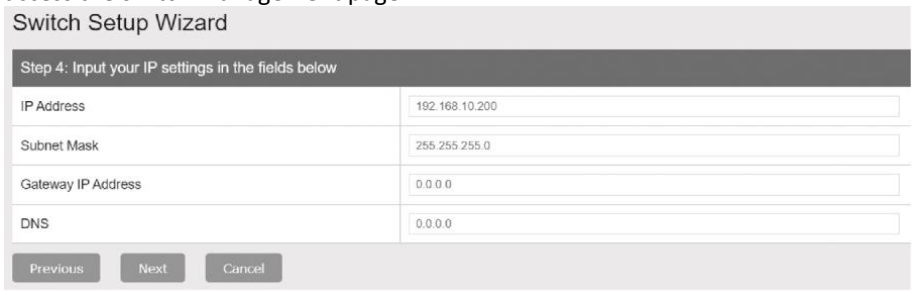


5. To verify the switch is now successfully registered with your TRENDnet Hive Cloud Management account, the Hive button in the top right will be green to indicate successful registration.

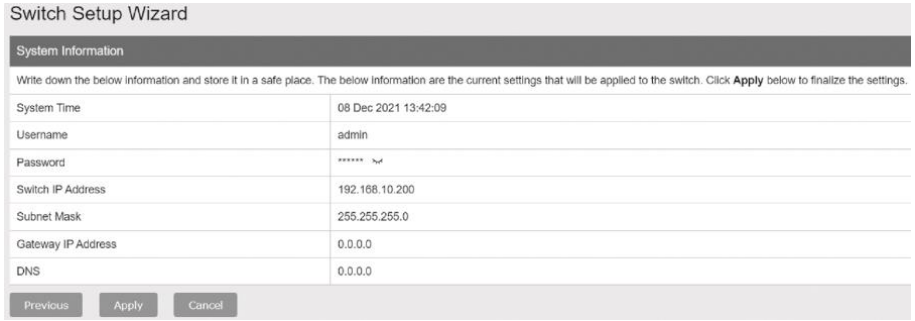
Default Management
Follow these steps if you have selected Default Management in the setup wizard.

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

2. Configure the switch IP address, subnet mask, gateway IP address, and DNS settings to match the requirements of your existing network using the fields provided, then click **Next**.
Note: If the switch IP address settings are changed to a different IP network subnet such as 192.168.1.x, 192.168.2.x, etc. your computer's network adapter settings will need to be changed match the new IP address settings configured on the switch in order to access the switch management page.



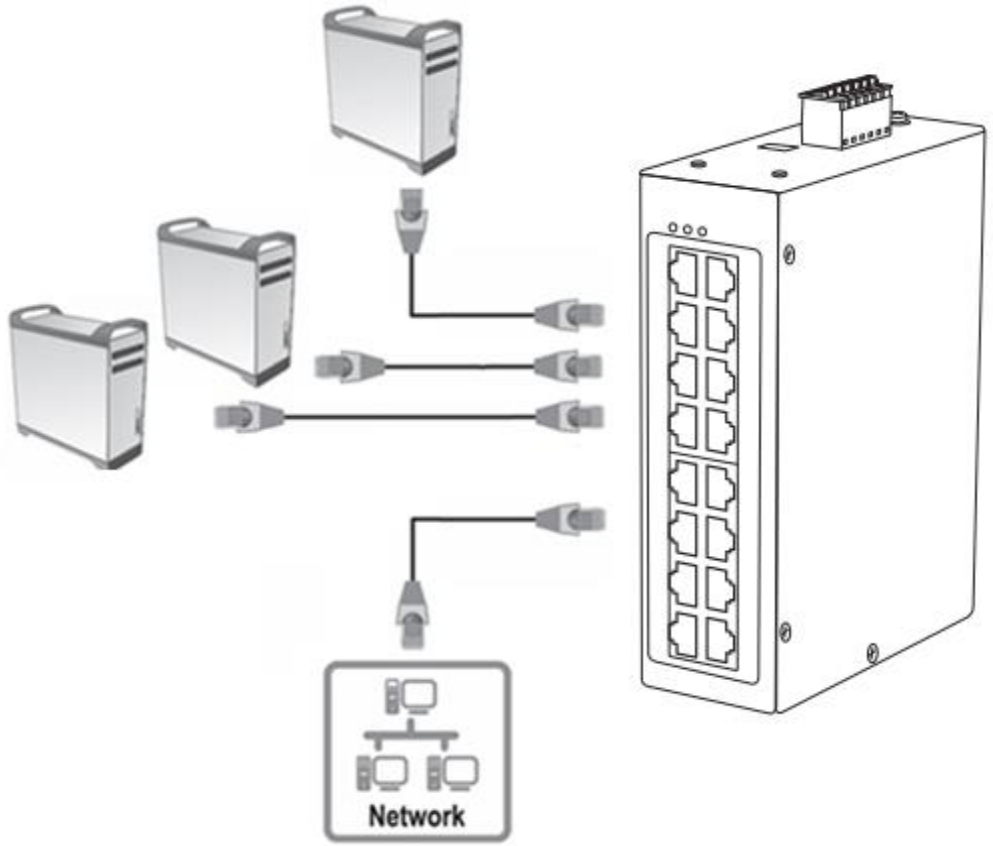
3. The summary page will display all of the configuration settings that were applied through the setup wizard. Click **Apply** to complete the setup wizard.
Note: *You may want to note the new password and IP address settings for local management access to the switch.*



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 Ports. Check the status of the LED indicators on the front panel of your switch to ensure the physical cable connection from your computer or device.

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.*

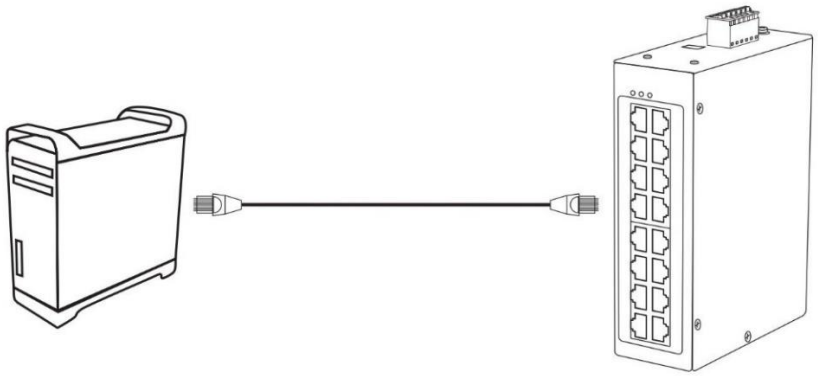


Accessing switch management interfaces

Access your switch command line interface

Note: *The system may be managed using the Telnet or SSH protocol. Throughout this user's guide, the term "CLI Configuration" will be used reference access through the command line interface.*

1. Connect your computer to one of the available Ethernet ports and make sure your computer and switch are assigned to an IP address with the same IP subnet. For select models, you may also use the console port.



2. On your computer, run the terminal emulation program (ex. HyperTerminal, TeraTerm, Putty, etc.) and set the program to use the Telnet protocol and enter the IP address assigned to the switch. The default IP address of the switch is 192.168.10.200 / 255.255.255.0. For models with a console port, the port parameters are 38400 baud, 8-bits, no parity, 1 stop bit.

3. The terminal emulation window should display a prompt for user name and password.

Enter the user name and password. By default:

Console User Name: **admin**
Note: *User Name and Password are case sensitive.*
Enable Mode/Privileged Exec User Name: **admin**
Enable Mode/Privileged Exec Password: **admin**

Setting	Default Value
Default Username	admin
Default Password	admin

Setting	Default Value
IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	admin

CLI Command Modes and Example Commands

Node	Command	Description
enable	show hostname	Displays the system's hostname.
configure	reboot	Reboots the system.
eth0	ip address A.B.C.D/M	Configures a static IP and subnet mask for the switch.
interface	show	Displays the current port configuration.
vlan	show	Displays the current VLAN configuration.

The Node type:

- enable

  Its command prompt is **"[DEVICE_NAME]*#".***

  It means these commands can be executed in this command prompt.

- configure

  Its command prompt is **"[DEVICE_NAME]*(config)#".***

  It means these commands can be executed in this command prompt.

  In ***Enable*** code, executing command "***configure terminal***" enter the configure node.

  [DEVICE_NAME]# configure terminal

- eth0

  Its command prompt is **"[DEVICE_NAME]*(config-if)#".***

  It means these commands can be executed in this command prompt.

  In ***Configure*** code, executing command "***interface eth0***" enter the eth0 interface node.

  [DEVICE_NAME](config)#interface eth0

  [DEVICE_NAME](config-if)#

- interface

  Its command prompt is **"[DEVICE_NAME]*(config-if)#".***

  It means these commands can be executed in this command prompt.

  In ***Configure*** code, executing command "***interface gigaethernet1/0/5***" enter the interface port 5 node.

  Or

  In ***Configure*** code, executing command "***interface fastethernet1/0/5***" enter the interface port 5 node.

  Note: depend on your port speed, gigaethernet1/0/5 for gigabit Ethernet ports and fastethernet1/0/5 for fast Ethernet ports.

  [DEVICE_NAME](config)#interface gigaethernet1/0/5

  [DEVICE_NAME](config-if)#

- vlan

  Its command prompt is **"[DEVICE_NAME]*(config-vlan)#".***

  It means these commands can be executed in this command prompt.

  In ***Configure*** code, executing command "***vlan 2***" enter the vlan 2 node.

  Note: where the "2" is the vlan ID.

  [DEVICE_NAME](config)#vlan 2

  [DEVICE_NAME](config-vlan)#

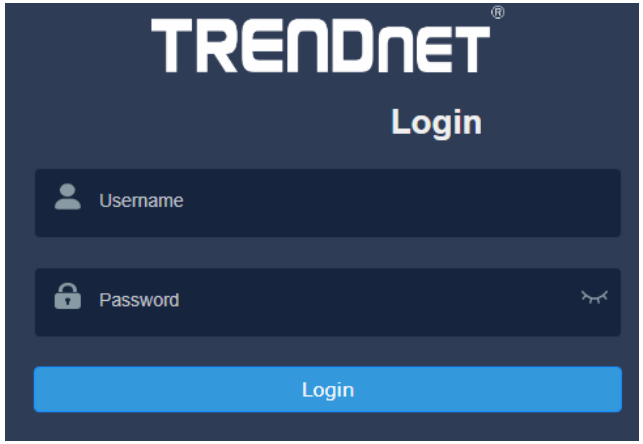
Access your switch web management page

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

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

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

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



Dashboard

View your switch status information

Dashboard

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

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

2. Click on **Dashboard**.

Switch Information

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

Switch Information	
System Uptime:	1 day(s),0 hr(s),44 min(s),26 sec(s)
Runtime Image:	3.01.004
Boot Loader:	1.00.014

Hardware Information

- **DRAM Size:** Displays your switch RAM memory size.
- **Flash Size:** Displays your switch Flash memory size.

Hardware Information	
DRAM Size:	256 MB
Flash Size:	32 MB

Administration Information

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

Administration Information	
System Name:	
System Location:	
System Contact:	

System MAC Address, IPv4 Information

- **Serial Number:** Displays the serial number of the switch
- **MAC Address:** Displays the switch system MAC address.
- **IP Address** – Displays the current IPv4 address assigned to your switch.
- **Subnet Mask** – Displays the current IPv4 subnet mask assigned to your switch.
- **Default Gateway** – Displays the current gateway address assigned to your switch.

System Serial Number, MAC Address, IPv4	
Serial Number:	CA0J2W1000001
MAC Address:	00-AD-24-A2-D3-FD
IP Address:	192.168.10.200
Subnet Mask:	255.255.255.0
Default Gateway:	

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

IPv6 Information	
IPv6 Unicast Address / Prefix Length:	
IPv6 Default Gateway:	
Link Local Address / Prefix length:	

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.

Automatic Network Features	
IPv4 DHCP Client Mode:	Disabled
IPv6 DHCP Client Mode:	Disabled

System Information

Switch View

View your switch status information

Dashboard > Switch View

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

2. Click on **Dashboard**, then click on **Switch View.** The switch view shows the ports that are connected.

3. Review the settings below.

- **Port:** Designates the port number that is displayed.
- **Throughput:** Current throughput being used for the specified port
- **Loopback Detection:** Displays the loopback detection status
- **Distance:** Displays the estimated length of the cable measured in meters

Port	Throughput	Loopback Detection	Distance
1	0 Mbps	Normal	
2	0 Mbps	Normal	
3	0 Mbps	Normal	

Real-time Statistics

View your switch status information

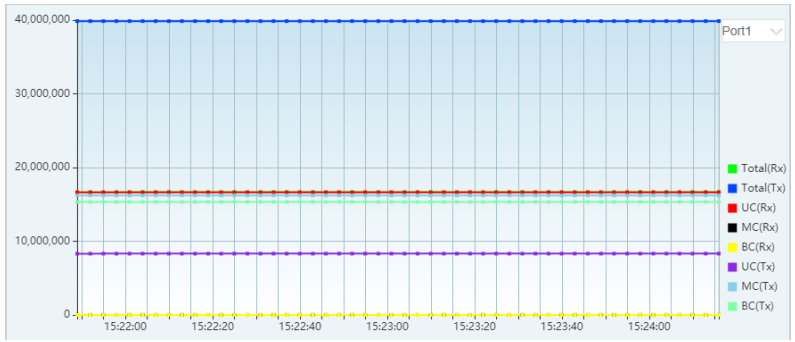
Dashboard > Real-time Statistics

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

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

3. Select the port from the drop down menu to review the current settings.

- **Total(Rx):** The total number of packets received
- **Total(TX):** The total number of packets transmitted
- **UC (Rx):** The number of Unicast packets received
- **MC(Rx):** The number of Multicast packets received
- **BC(Rx):** The number of Broadcast packets received
- **UC(Tx):** The number of Unicast packets transmitted
- **MC(Tx):** The number of Multicast packets transmitted
- **BC(Tx):** The number of Broadcast packets transmitted



Topology Map

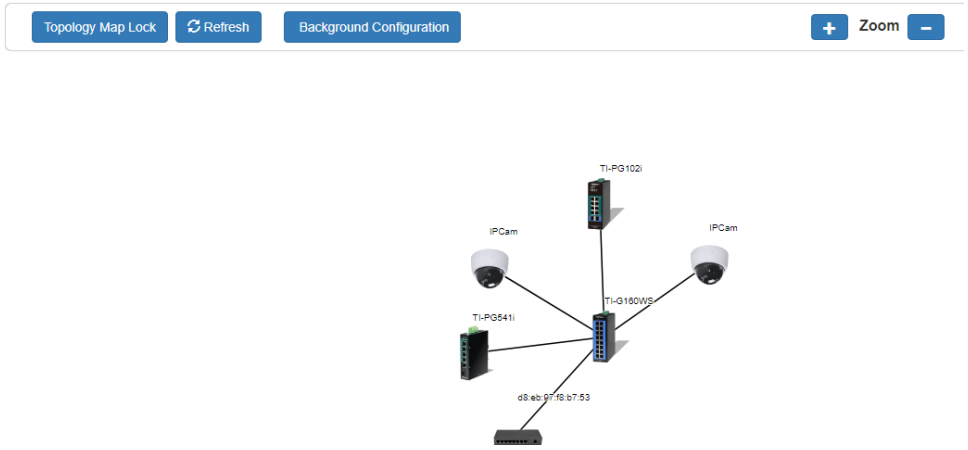
View the topology of your network

Dashboard > Topology Map

The topology map displays a basic view of the current network topology and device inter-connections. Devices can be automatically discovered and added with the LLDP and ONVIF protocols, or can be manually entered into the switch database. The topology map/netlite view is only available through the web management page.

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

2. Click on **Dashboard**, then click on **Topology Map.** Review the topology map.



To add devices into the map, refer to the **Network > Manual Registration**, **Network > ONVIF**, and **Network > LLDP** sections of this manual.

System

System Management

Set your system information

System > System Management

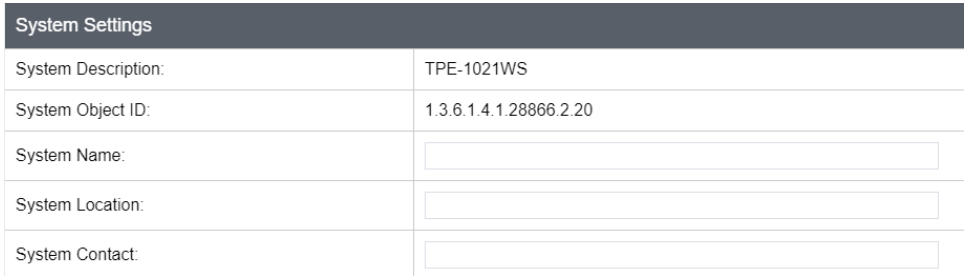
This section explains how to assign a name, location, and contact information for the switch. This information helps in identifying each specific switch among other switches in the same local area network. Entering this information is optional.

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

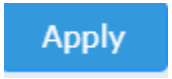
2. Click on **System**, and click on **System Management**.

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

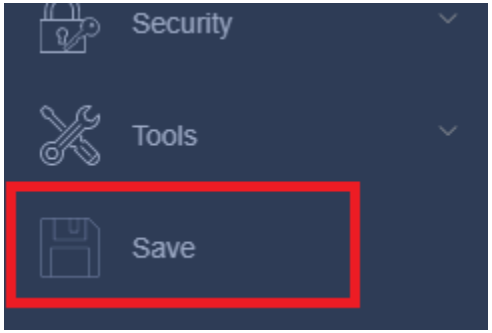
- **System Description** - Specifies the Switch model. You cannot change this parameter.
- **System Object ID** - Indicates the unique SNMP MIB object identifier that identifies the switch model. You cannot change this parameter.
- **System Name** - Specifies a name for the switch, the name is optional 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.



4. Click **Apply**.



5. At the bottom of the left-hand panel, click **Save**.

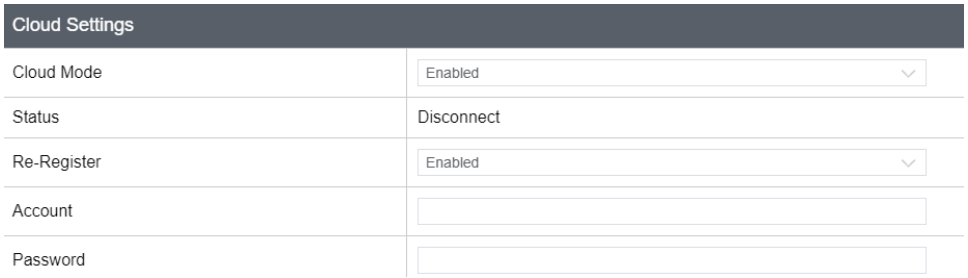


Cloud Settings

System > Cloud Settings

This section allows you to setup your device for TRENDnet's Cloud Management (Hive). With TRENDnet Hive, you will be able to manage and monitor your device through the TRENDnet Cloud portal remotely.

1. Log into your switch management page (see "Access your switch management page on page 5").
2. Click on **System,** and then **Cloud Settings.**
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.



- **Cloud Mode:** Select **Enabled** to connect the device to TRENDnet Hive, and **Disabled** to disable connection.
- **Status:** Displays the current connection status between the device and TRENDnet Hive
- **Re-Register:** Select **Enabled** to sync your device with your TRENDnet Hive account, and **Disabled** to disable the sync.
- **Account:** Enter your TRENDnet Hive account username
- **Password:** Enter your TRENDnet Hive account password

Note: Connecting your device to the cloud will lock all configurations to be managed by the cloud. To configure your device locally, please **Disable** your connection to the cloud.

(CLI commands)

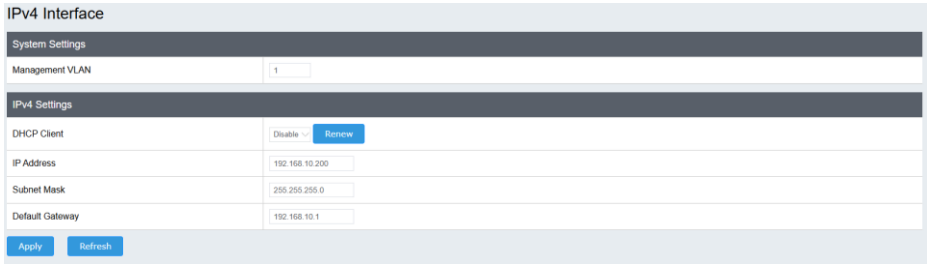
L3 Feature

IPv4 Interface

System > L3 Feature > IPv4 Interface

This section allows you to change your switch IPv4 address settings and additionally specify the management VLAN. 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.

1. Log into your switch management page (see "Access your switch management page on page 5").
2. Click on **System**, **L3 Feature**, and then **IPv4 Interface**.
3. To change the IPv4 IP address associated with a specific VLAN, click on **Edit** within the lower table**.**



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

- **Management VLAN**: Enter the VLAN that the switch can be managed from
- **DHCP Client**: Select **Disabled** to statically assign an IP address and subnet mask, select **Enabled** to automatically request one from your network's DHCP server. DHCP is required for Hive cloud connection.
- **IP Address**: Enter the new switch IP address you would like to statically assign. (e.g. *192.168.200.200*)
- **Subnet Mask**: Enter the new switch subnet mask. (e.g. *255.255.255.0*)
- **Default Gateway**: Enter the new switch default gateway IP

6. At the bottom of the left-hand panel, click **Save**.

CLI Commands

Node	Command	Description
configure	interface eth0	Enters the ETH0 interface node.
eth0	show	Displays the current configuration of ETH0.
eth0	ip address A.B.C.D/M	Configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	Configures the system's default gateway.
eth0	ip dhcp client (disable|enable|renew)	Configures the DHCP client. Disable: Set to use a static IP address Enable & Renew: Enable the DHCP client
eth0	management vlan VLANID	Configures the management VLAN.

Example:

- Enter the ETH0 interface node.
  [DEVICE_NAME](config)#interface eth0
  [DEVICE_NAME](config-if)#

- Enable the DHCP Client.
  [DEVICE_NAME](config-if)#ip dhcp client enable

- Configure a static IP address and a default gateway.
  [DEVICE_NAME](config-if)#ip address 192.168.10.200/24
  [DEVICE_NAME](config-if)#ip address default-gateway 192.168.10.1

IPv4 ARP Aging Time

System > L3 Feature > IPv4 ARP Aging Time

This section allows you to set the timeout for the switch's ARP Table per each configured VLAN.

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

2. Click on **System**, **L3 Feature**, and then **IPv4 ARP Aging Time**.

3. Click on **Edit** to change the value, then click **Apply**.

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

Set your IPv6 settings

System > L3 Feature > IPv6 Interface

Internet Protocol version 6 (IPv6) is a new IP protocol designed to replace IP version 4 (IPv4). The IPv6 address protocol meets the current requirements of new applications and the never ending growth of the Internet. The IPv6 address space makes more addresses available but it must be approached with careful planning. Successful deployment of IPv6 can be achieved with existing IPv4 infrastructures. With proper planning and design, the transition between IP version 4 and 6 is possible today as well.

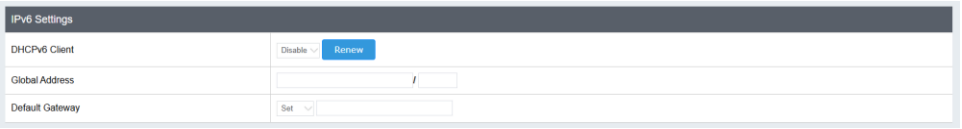
Use the **IPv6 Interface** page to configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch via all of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration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

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

2. Click on **System**, **L3 Feature**, and then **IPv6 Interface**.

3. To create a new entry per VLAN, type the VLAN number you would like to create, then click **Add**. To view a specific VLAN ID's configuration, enter the VLAN ID into the **Interface VLAN** field and then click **Find**.

4. To change the IPv6 IP address associated with a specific VLAN, click on **Detail** within the lower table**.**



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

- **DHCPv6 Client:** Select **Enabled** to automatically obtain the IPv6 address from the DHCP server on the network, select **Disabled** to manually specify an IPv6 Address.
- **IPv6 Address**: Enter the full IPv6 address you would like to specify for this connection.
- **Default Gateway**: Enter the default gateway for this connection.

6. At the bottom of the left-hand panel, click **Save**.

DNS

Set your DNS server settings

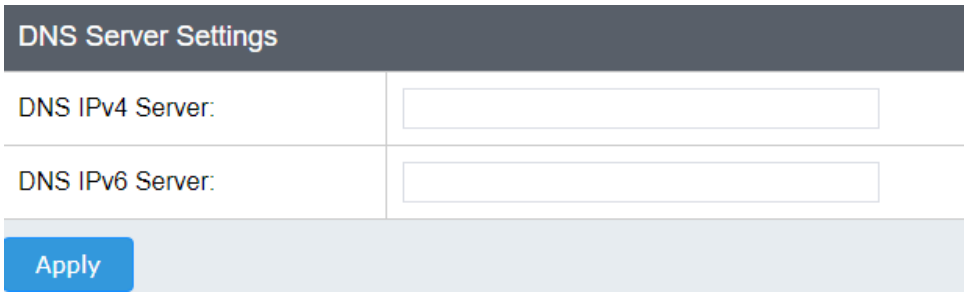
System > DNS

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

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

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

3. Enter your **DNS IPv4 Server** address and/or **DNS IPv6 Server** address in the provided fields then click **Apply**.



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

IP Access List

Restrict access to switch management page

System > IP Access List

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

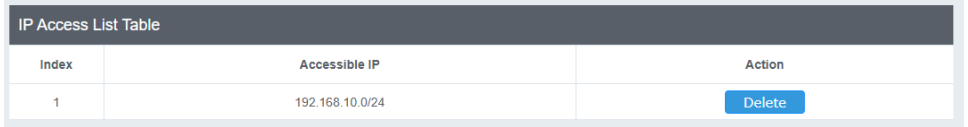
1. Log into your switch management page (see "Access your switch management page on page 5").

2. Click on **System**, and click on **IP Access List**.

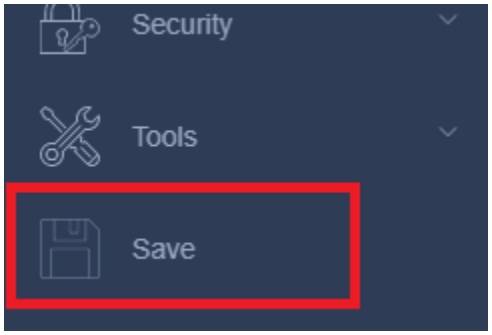
3. Review the settings.

Enter the IPv4 or IPv6 address to allow access and click **Add** for each entry. Make sure to enter your current IP address to prevent lockouts.

For each entry, the access list will populate. You can click **Delete** next to the entry to delete the entry.



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



Administration

Change administrator password and add accounts

System > Administration

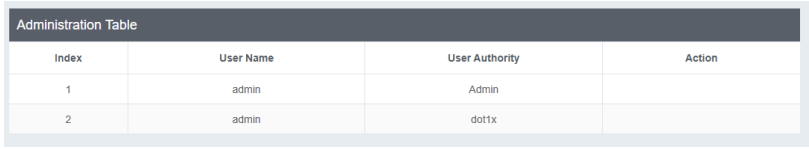
This section explains how to change the administrator password create additional administrative user accounts for access to the switch management page.

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

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

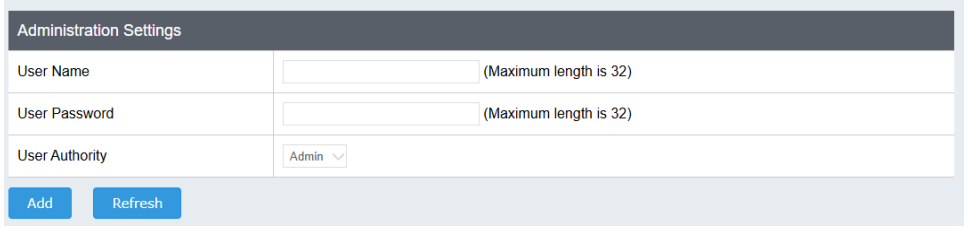
3. Review the settings.

To change the administrator password, in the "admin" entry in the table, click on **Modify.** ***Note:*** *This default administrator account and the "dot1x" account cannot be deleted.*



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 32 characters.*

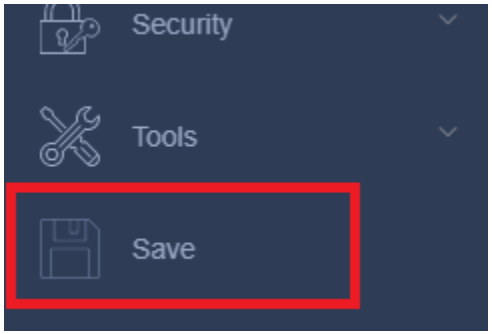


To create additional administrative user accounts:

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

  Note: *The password consists of up to 32 characters.*

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



CLI Commands

Node	Command	Description
enable	show user account	Displays the current user accounts on the switch.
configure	add user USER_ACCOUNT PASSWORD (normal|admin)	Adds a new user account with the specified password and account type.
configure	delete user USER_ACCOUNT	Deletes a present user account. The default admin and "dot1x" accounts cannot be deleted.

Example:

[DEVICE_NAME]#configure terminal

[DEVICE_NAME](config)#add user q q admin

[DEVICE_NAME](config)#add user 1 1 normal

System Time

Set the switch date and time

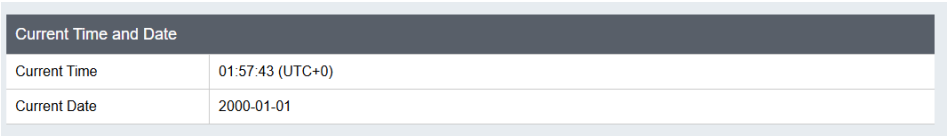
System > System Time

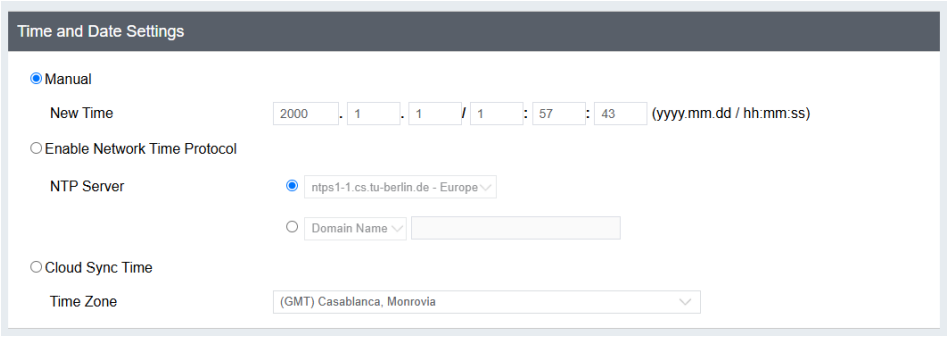
1. Log into your switch management page (see "Access your switch management page" on page 5).

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

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

- **Current Time –** Displays the current system time.
- **Current Date –** Displays the current system date.

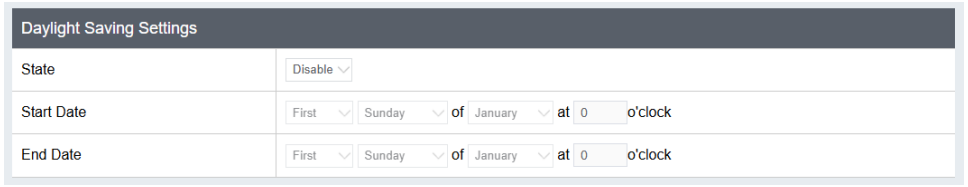




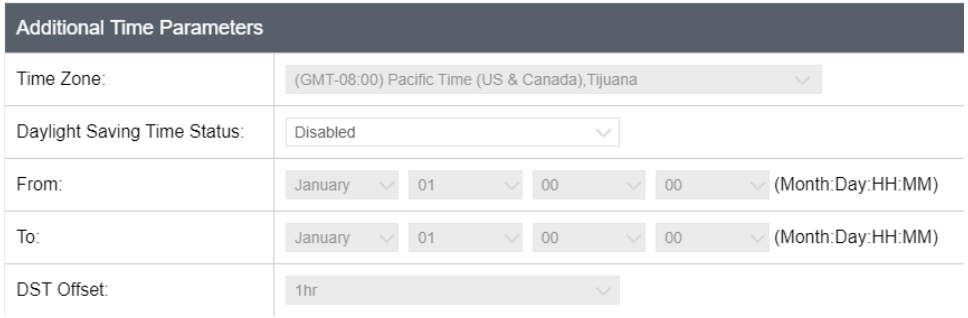
- **Manual –** Allows you to manually set the time settings. If selecting this option, manually enter your date and time settings in **New Time**.
- **Enable Network Time Protocol –** Allows you to configure your switch to pull time and date settings automatically from a network time server. If selecting this option, choose from a dropdown of default entries, or enter your desired time server settings.

Note: *Please note that in order for the switch to communicate to Internet SNTP time servers, the switch must have valid IPv4/IPv6 address settings including a default gateway address for Internet access. Additionally, if using a domain name, the switch must be configured with valid DNS server settings in order to resolve host/domain names.*

- **Cloud Sync Time –** Allows you to configure your switch to pull time and date settings automatically from the cloud. This is the only option when using TRENDnet Hive cloud management.
  - **Time Zone –** Select the local time zone.

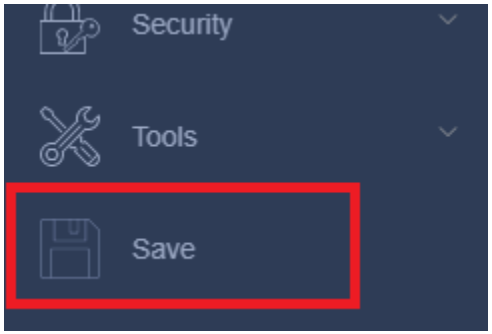


- **Daylight Saving Settings** – Allows you to configure additional Daylight Saving Time parameters.
  - **State:** Click the drop-down list to enable or disable Daylight Savings.
  - **Start Date:** Set the daylight savings start date and time.
  - **End Date:** Set the daylight savings end date and time.
  - **DST Offset:** Click the drop-down list to set the time offset based on respective time zone.



4. When finished, click **Apply** to save changes.

5. At the bottom of the left-hand panel, click **Save**.



CLI Commands

Node	Command	Description
enable	show time	Displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. *hour*: 0-23 *min*: 0-59 *sec*: 0-59 Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time.
configure	time date YEAR/MONTH/DAY	Sets the current date on the Switch. *year*: 1970- *month*: 1-12 *day*: 1-31
configure	time daylight-saving-time	Enables the daylight saving time feature.
configure	time daylight-saving-time start-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH OCLOCK	Sets the start date for Daylight Saving Time. For Example: first Sunday 4 0 (AM:0 1st Sunday in April)
configure	time daylight-saving-time end-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH OCLOCK	Sets the end date for Daylight Saving Time. For Example: Last Sunday 10 18 (PM: 6 Last Sunday in October)
configure	no time daylight-saving-time	Disables daylight saving time.
configure	time ntp-server IP_ADDRESS	Sets the IP address of your time server.
configure	no time ntp-server	Disables the NTP server.
configure	time timezone VALUE	Sets the timezone using the UTC offset. Valid value: -1200 to 1200.

Example:

[DEVICE_NAME](config)#*time ntp-server 192.5.41.41*
[DEVICE_NAME](config)#*time timezone +0800*
[DEVICE_NAME](config)#*time ntp-server enable*
[DEVICE_NAME](config)#time daylight-saving-time start-date first Monday 6 0
[DEVICE_NAME](config)#time daylight-saving-time end-date last Saturday 10 0

SSL

Enable HTTPS/SSL (Secure Socket Layer) management access

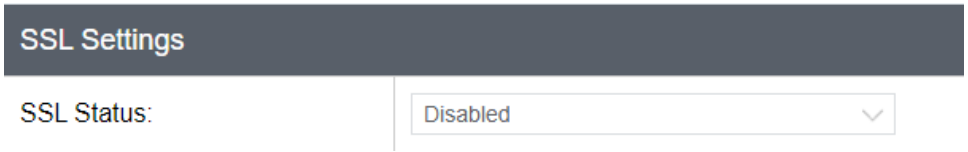
System > SSL By default, your switch management page can be accessed using standard web HTTP protocol which is unsecure. Enabling HTTPS/SSL management access allows access to the switch management page using secure encrypted communication which prevents unauthorized users from intercepting user name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

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

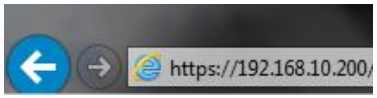
1. Log into your switch management page (see "Access your switch management page on page 5").

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

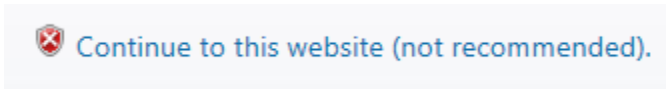
3. Review the settings. Click **Apply** to save changes.
   - **SSL Status:**
     - **Enabled –** Enables HTTPS/SSL management access and disables HTTP unsecured mode.
     - **Disabled** – Disabled HTTPS/SSL management access and enabled HTTP unsecured mode. (Default setting).



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

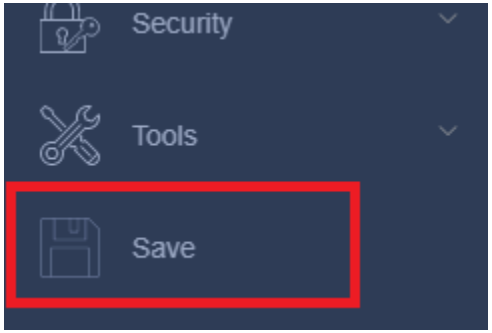


Click **Continue, Proceed to this website**, and accept the certificate if prompted.



You may update the SSL certificate at **System > Upgrade SSL Certificate** to eliminate this prompt.

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



SSH

Enable SSH (Secure Shell) management access

System > SSH

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

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

3. Review the settings. Click **Apply** to save changes.
   - **SSH Status:**
     - **Enabled –** Enables SSH management access.
     - **Disabled** – Disabled SSH management access.
   - **Port:** Set the port number to use for SSH management access

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

CLI Commands

Node	Command	Description
configure	ssh server	Enables SSH management access.
configure	no ssh server	Disables SSH management access.

Telnet

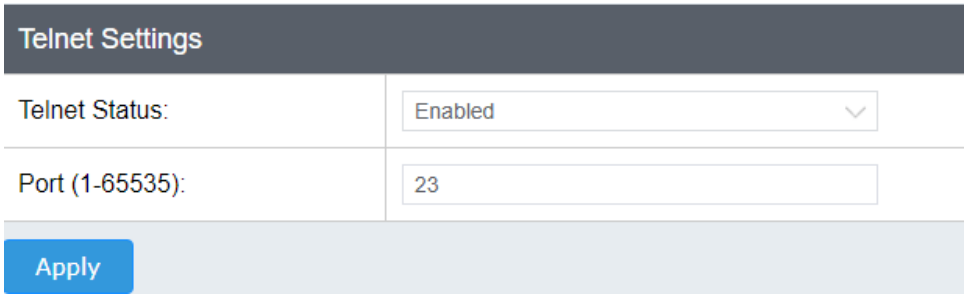
Enable Telnet management access

System > Telnet

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

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

3. Review the settings. Click **Apply** to save changes.
   - **Telnet Status:**
     - **Enabled –** Enables Telnet management access.
     - **Disabled** – Disabled Telnet management access.
   - **Port:** Set the port number to use for Telnet management access



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

CLI Commands

Node	Command	Description
configure	telnet server	Enables Telnet management access.
configure	no telnet server	Disables Telnet management access.

System Log

View and setup your switch logging

System > System Log

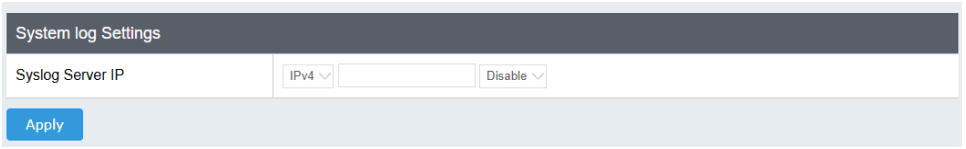
The system log is designed to monitor the operation the switch by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

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

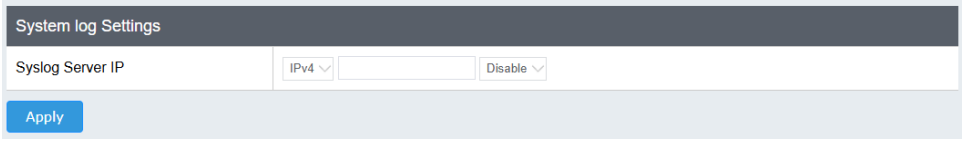
2. Click on **System**, and click on **System Log**.

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

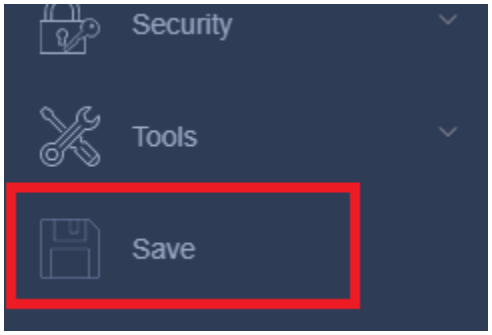
- **Syslog Server IP** – Enter the IP of the Syslog server.



- **Log Level** – Click the drop-down list to select what level of event messages that will be logged.
  - **1 Alert** - Action must be taken immediately.
  - **2 Critical** - Critical conditions are displayed.
  - **3 Error** – Non-critical error conditions are displayed.
  - **4 Warning** - Warning conditions are displayed.
  - **5 Notice** - Notices are displayed.
  - **6 Info** - Informational messages are displayed.



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



CLI Commands

Node	Command	Description
enable	show syslog	Displays all of the entire log messages recorded on the switch.
enable	show syslog level LEVEL	Displays all of the entire log messages and their respective log levels.
enable	show syslog server	Displays the syslog configuration.
configure	syslog (disable|enable)	Disables/enables the syslog option.
configure	syslog ip IPADDR	Configures the syslog server's IP address.

SNMP

Settings

System > SNMP > Settings

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

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

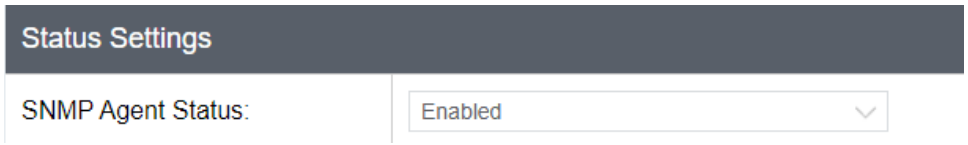
Note: *If you disable the SNMP on the switch, the switch will not be manageable via SNMP using MIBs.*

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

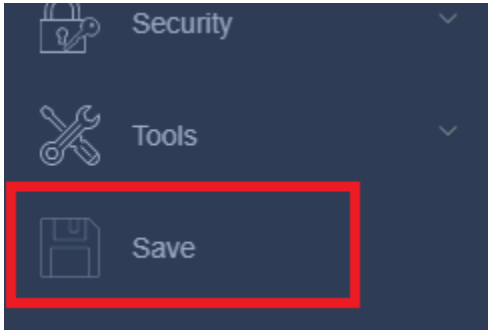
2. Click on **System**, click on **SNMP**, and click on **Settings**.

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

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



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



CLI Configuration

Node	Command	Description
interface	power efficient-ethernet auto	Enables EEE on the specified interface.
interface	no power efficient-ethernet auto	Disables EEE on the specified interface.

View

System > SNMP > View

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

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

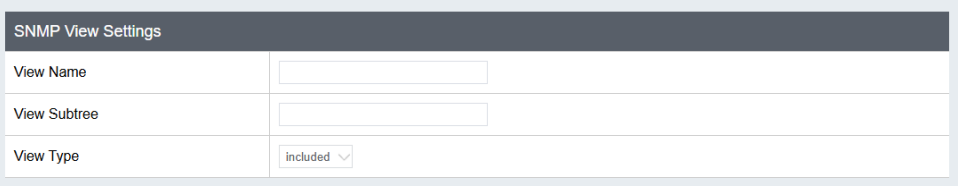
2. Click on **System**, click on **SNMP**, and click on **View**.

3. Review the settings.

Creating SNMP View Table Entries

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

- Enter the **View Name**. This entry must be pre-defined on the SNMP User/Group page.
- Enter the **View Subtree.**
- 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.

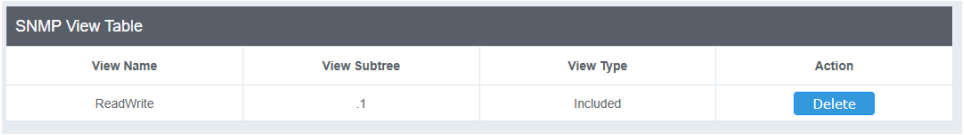


Modifying SNMP View Table Entries

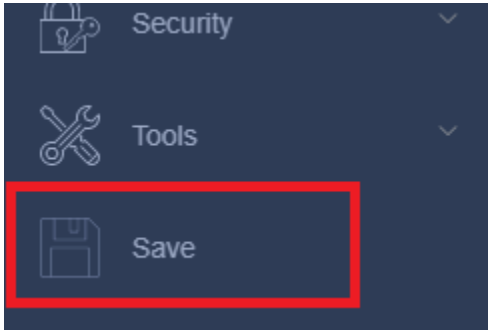
If you need to modify an entry in the View Table page, you must first delete the entry and then re-enter it.

Deleting SNMP View Table Entries

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



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



Group

System > SNMP > Group

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

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

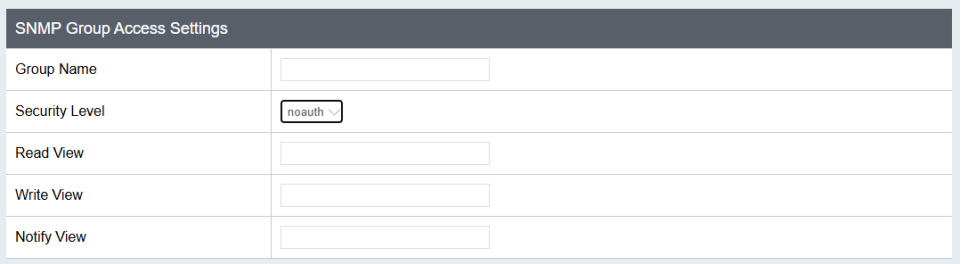
2. Click on **System**, click on **SNMP**, and click on **Group**.

3. Review the settings.

Creating SNMP View Names

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

- Enter the **Group Name**. This entry must be pre-defined on the SNMP User/Group page.
- Enter the **Read View Name**. This name is an optional field. It can be up to 31 characters in length.
- Enter the **Write View Name**. This name is an optional field. It can be up to 31 characters in length.
- Enter the **Notify View Name**. This name is an optional field. It can be up to 31 characters in length.
- Enter the **Security Level** from the pull-down menu. The selection options are:
  - **NoAuth:** This selection is the appropriate selection when no **Auth-Protocol** or **Priv-Protocol** (no encryption) are selected on the SNMP User/Group page.
  - **Auth:** 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.
  - **Priv:** When the **Auth-Protocol** or **Priv-Protocol** have been enabled, choose this selection.
- Click the **Add** button.



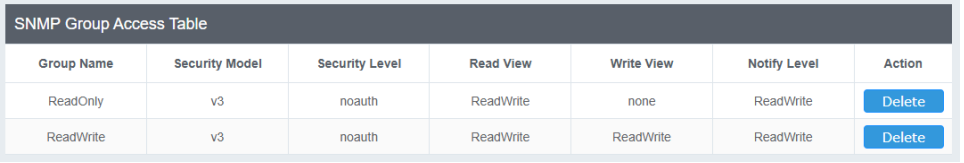
Modifying SNMP View Names

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

Deleting SNMP View Names

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

Note: *The views corresponding to the **ReadOnly** and **ReadWrite Group Names** are shown as examples only. They are not present on a factory default configuration.*



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

User

System > SNMP > User

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

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

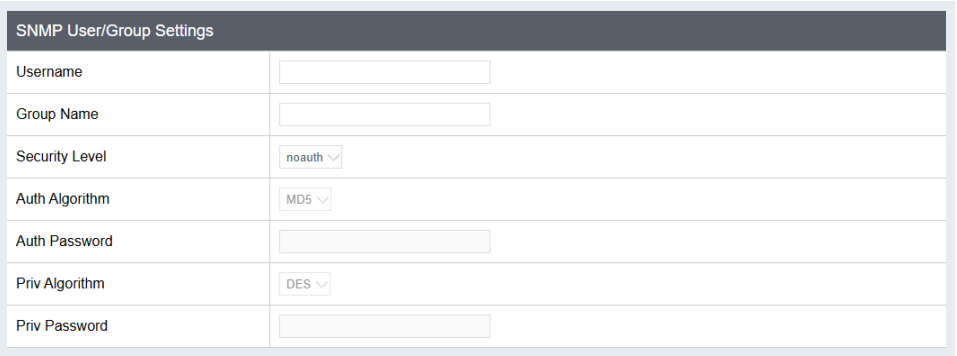
2. Click on **System**, click on **SNMP**, and click on **User**.

3. Review the settings.

Creating SNMP User and Group Names

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

- Type a new **User Name**. Enter a name up to 32 characters in length.
- Type a new **Group Name**. Enter a name up to 32 characters in length.
- Select the **Security Level** desired.
  - **Auth** - The **Auth Algorithm** and its associated password field become active.
  - **Priv** - The **Auth Algorithm**, **Priv Algorithm**, and associated password fields become active.
- Select one of the following choices for the **Auth Algorithm** 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.
- Select one of the following choices for the **Priv Algorithm** field:
  - **DES** – Specifies that DES encryption will be applied to SNMP data.
  - **AES** - Specifies that AES encryption will be applied to SNMP data.
- Enter a password for each of the selected options**.**
- Click **Add**. The new User Name and Group Name are displayed on the SNMP User/Group page.

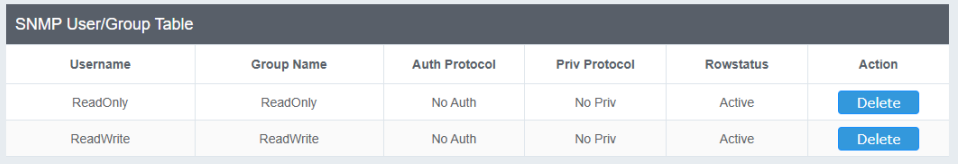


Modifying SNMP User and Group Names

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

Deleting SNMP User and Group Names

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



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

Community

System > SNMP > Community

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.

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

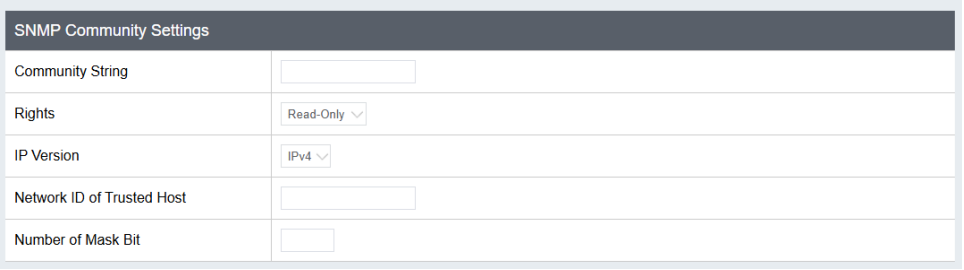
2. Click on **System**, click on **SNMP**, and click on **Community**.

3. Review the settings.

Create SNMP Community Settings

- Enter a new **Community Name**. A name can be up to 32 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.

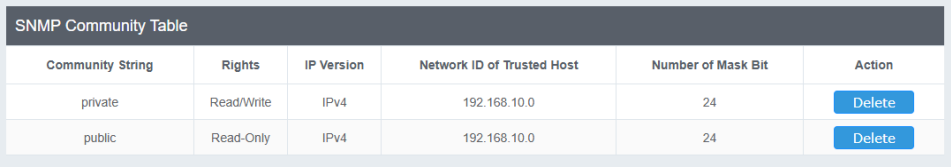


Modify SNMP Community Settings

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

Delete SNMP Community Settings

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



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

Trap Receiver

System > SNMP > Trap Receiver

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

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

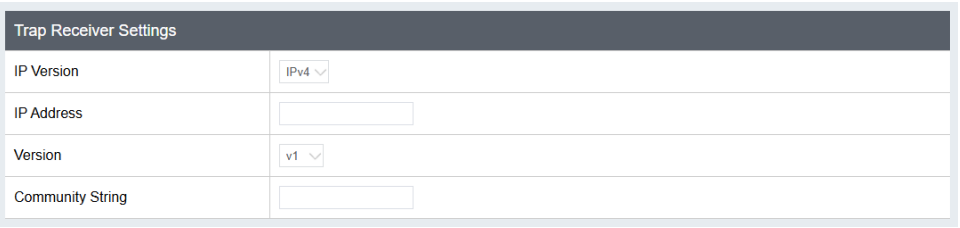
2. Click on **System**, click on **SNMP**, and click on **Trap Receiver**.

3. Review the settings.

Create Trap Host Table Entry

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

- Enter the **Host IP Address** for the management device that is to receive the SNMP traps.
- Enter the **SNMP Version**, either **v1** or **v2c**, that is configured for the host management device.
- Enter a **Community String** that you have defined previously in the SNMP Community table. The **Community String** must correlate with one of the communities displayed on the SNMP Community Table page. If you enter a **Community String** 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.

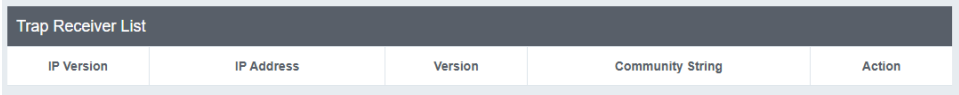


Modify a Trap Host Table Entry

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

Delete a Trap Host Table Entry

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



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

Trap Event

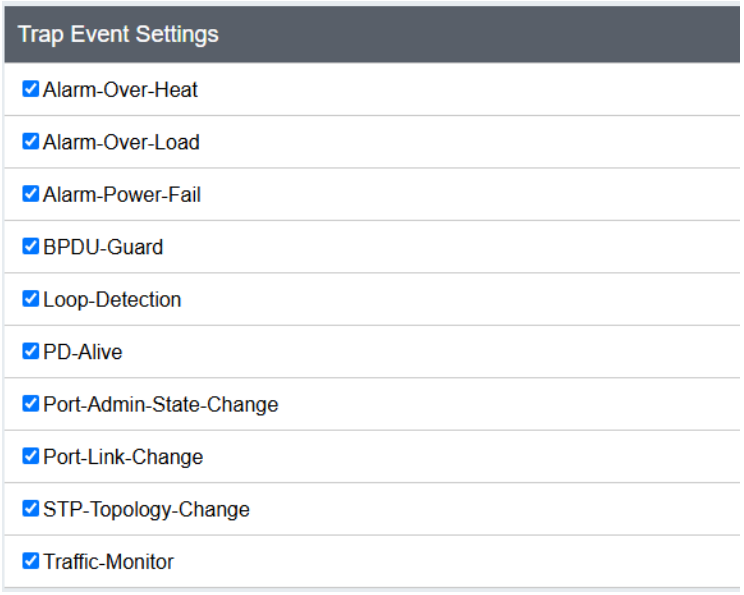
System > SNMP > Trap Event

You can select which events to monitor through SNMP here.

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

2. Click on **System**, click on **SNMP**, and click on **Trap Event**.

3. Review the settings.



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

Trap Port Event

System > SNMP > Trap Port Event

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

2. Click on **System**, click on **SNMP**, and click on **Trap Port Event**.

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

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

CLI Commands

Node	Command	Description
enable	show snmp	Displays the current SNMP configuration.
configure	snmp community STRING (ro|rw) trusted-host IPADDR	Configures the SNMP community name.
configure	snmp (disable|enable)	Disables/enables SNMP.
configure	snmp system-contact STRING	Configures contact information for the system.
configure	snmp system-location STRING	Configures the location information for the system.
configure	snmp system-name STRING	Configures a name for the system. (The system name is same as the host name)

configure	snmp trap-receiver IPADDR VERSION COMMUNITY	Specifies the device that will receive SNMP traps from the switch.

RMON

Settings

System > RMON > Settings

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.

Statistics

System > 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.

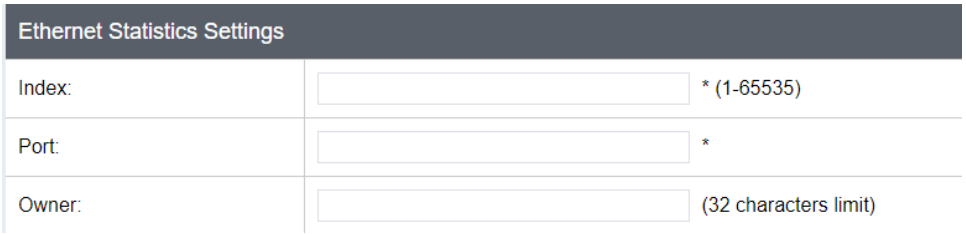
1. Log into your switch management page (see "Access your switch management page on page 5").

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

3. Review the settings.

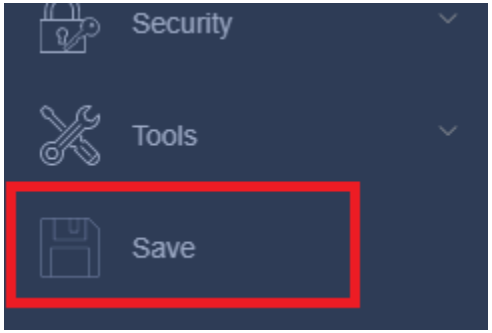
- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Port:** This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.
- **Owner:** This parameter is used to identify the person who created an entry. 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.



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

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



History

System > RMON > History

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

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

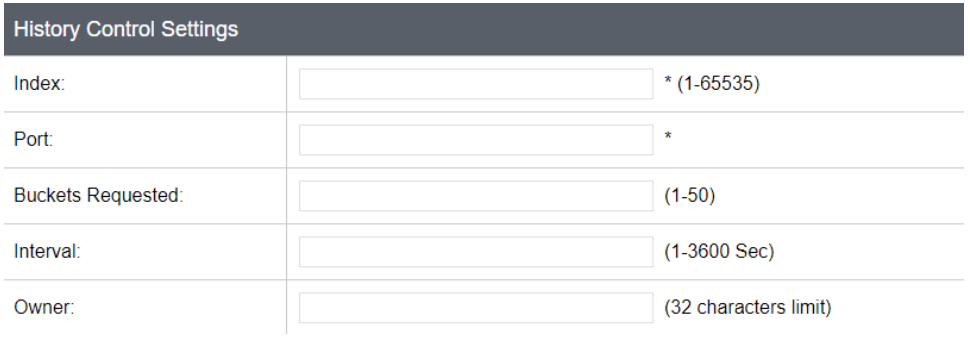
1. Log into your switch management page (see "Access your switch management page on page 5").

2. Click on **System**, click on **RMON,** and click on **History**.

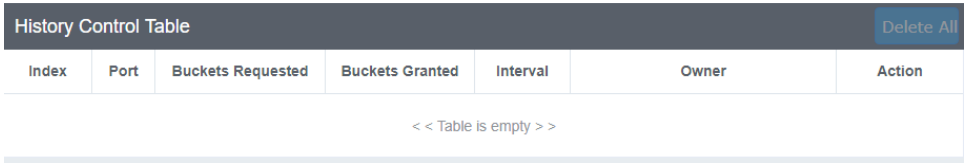
3. Review the settings.

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

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



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



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

Alarms

System > RMON > Alarms

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

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

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

Here are the three components that comprise RMON alarms:

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

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

2. Click on **System**, click on **RMON,** and click on **Alarm**.

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

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

RMON Alarm Settings		
Index:		* (1-65535)
Interval:		(1-2^31-1 Sec)
Variable:		*
Sample type:	Absolute value	
Rising Threshold:		* (0-2^31-1)
Falling Threshold:		* (0-2^31-1)
Rising Event Index:		(1-65535)
Falling Event Index:		(1-65535)
Owner:		(32 characters limit)

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

5. At the bottom of the left-hand panel, click **Save.**

6. Select the Config you would like to save the settings to, click **Save Settings to Flash**, then click **OK.**

Events

System > RMON > Event

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

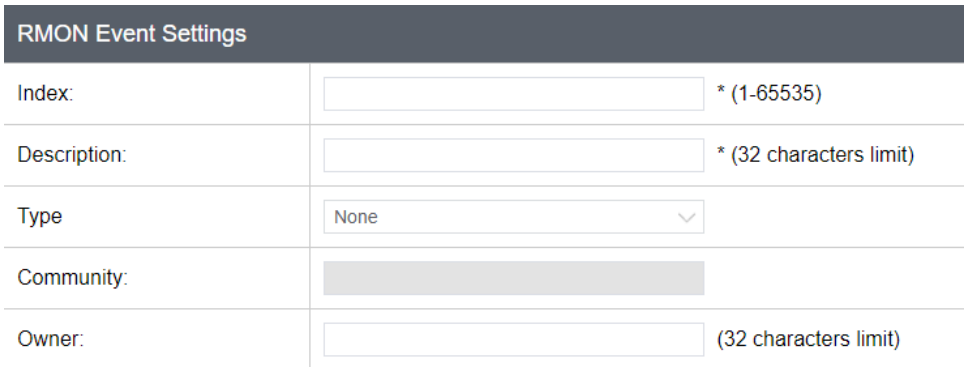
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System**, click on **RMON,** and click on **Event**.

3. Review the settings.

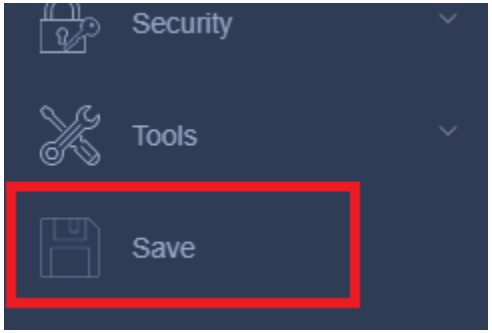
- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Description:** This parameter specifies a text description of the event that you are configuring.
- **Type:** This parameter specifies where to log the event when it occurs. The choices are to log a message in the event log of the Switch, send an SNMP trap to the SNMP NMS software, or both.
- **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.



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

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



CLI Commands

Node	Command	Description
enable	show rmon statistics	Displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	Clears the RMON statistics of the specified interface(s).

Statistics

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.

Traffic

System > Statistics > Traffic

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

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

3. View the Traffic Information Statistics.

- **InOctets:** Inbound Octets (Bytes/s), number of inbound octet bits in bytes per second.
- **InUcastPkts:** Inbound Unicast Packets (Pkts), number of inbound unicast packets in packets per second.
- **InNUcastPkts:** Inbound Non-unicast Packets (Pkts), number of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
- **InDiscards:** Inbound Discards (Pkts), number of inbound discarded packets in packets per second.
- **OutOctets:** Outbound Octets (Bytes/s), rate of outbound octet bits in bytes per second.
- **OutUcastPkts:** Outbound Unicast Packets (Pkts), number of outbound unicast packets in packets per second.
- **OutNUcastPkts:** Outbound Non-unicast Packets (Pkts), number of outbound non-unicast (such as broadcast and multicast packets) packets.
- **OutDiscards:** Outbound Discards (Pkts), number of outbound discarded packets.
- **Apply:** Click the **Apply** button to clear port specific Traffic information.
- **Refresh:** Click the Refresh button to update table with newest traffic information.

Port ID	In Octets	In Ucast Pkts	In NUcast Pkts	In Discards	Out Octets	Out Ucast Pkts	Out NUcast Pkts	Out Discards	Clear
All	-	-	-	-	-	-	-	-	Apply
1	2636022...	1860979	1853	1632	120267950	868432	4113	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	1255383...	895604	4176	34	2641130432	1888701	208	0	Apply
9	0	0	0	0	0	0	0	0	Apply
10	0	0	0	0	0	0	0	0	Apply

Error

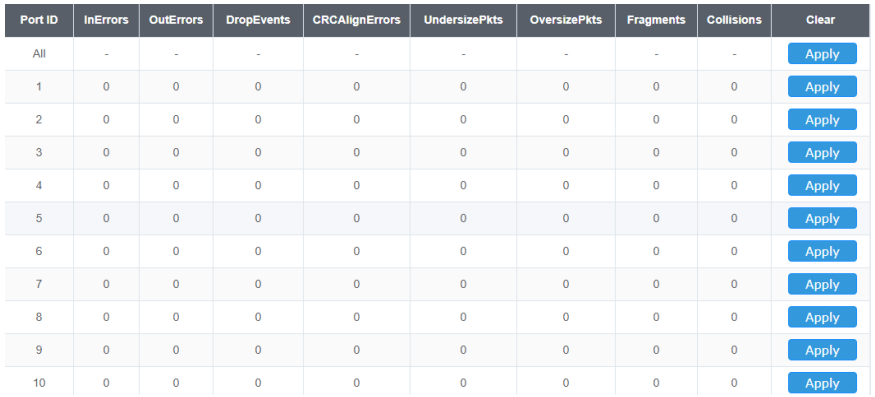
System > Statistic > Error

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

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

3. View the Error Information Statistics.

- **InErrors:** Inbound Errors (Pkts), number of inbound errors in packets per second.
- **OutErrors:** Outbound Errors (Pkts), number of outbound error packets.
- **DropEvents:** Drop Events, number of packets dropped.
- **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.
- **Apply:** Click the Apply button to clear port specific Traffic information.
- **Refresh:** Click the Refresh button to update table with newest traffic 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
9	0	0	0	0	0	0	0	0	Apply
10	0	0	0	0	0	0	0	0	Apply

CLI Commands

Node	Command	Description
enable	show port-statistics	Displays the statistics of all active ports.

IEEE 802.3az EEE

Enable IEEE 802.3az Power Saving Mode

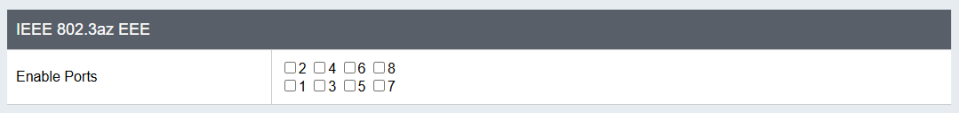
System > IEEE 802.3az EEE

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

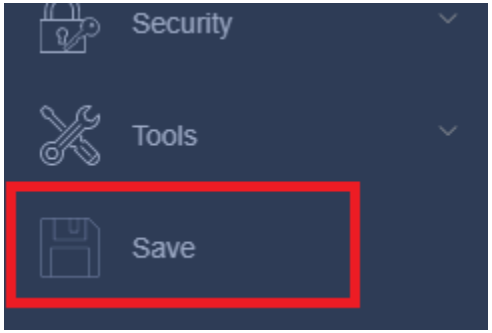
1. Log into your switch management page (see "Access your switch management page on page 5").

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

3. Check the boxes to enable the power saving feature for their respective ports and click **Apply** to save the settings.



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



CLI Commands

Node	Command	Description
interface	power efficient-ethernet auto	Enables EEE on the specified interface.
interface	no power efficient-ethernet auto	Disables EEE on the specified interface.

Mail Alarm

System > Mail Alarm

This feature sends an e-mail trap to a predefined administrator when certain events occur. The events are listed below:

- System Reboot: The system has been rebooted.
- Port Link Change: A port has been connected/disconnected.
- Configuration Change: The switch configuration has been changed.
- Firmware Upgrade: The system firmware was upgraded.
- User Login: A user has logged in to the management interface.
- Port Blocked: A port was blocked by Loopback Detection or BPDU Guard.

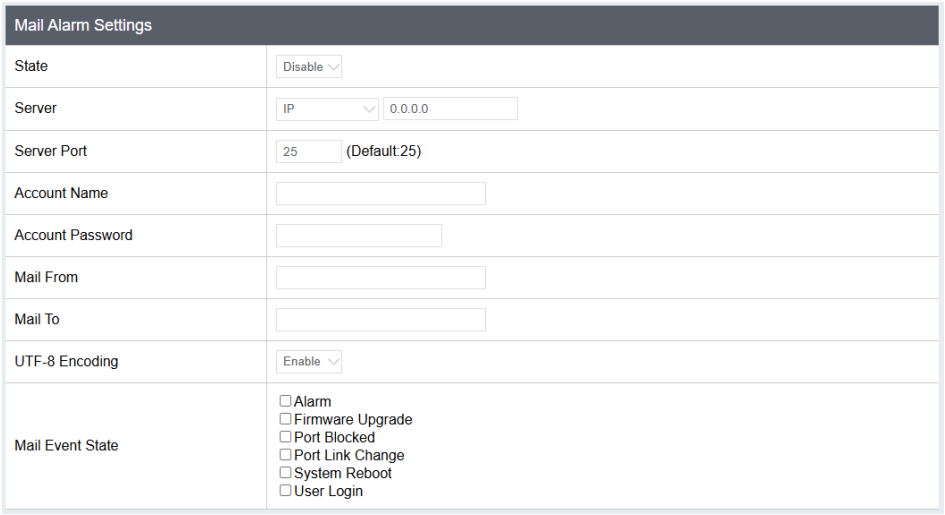
Configure the Mail Alarm feature as follows:

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

2. Click on **System** and click on **Mail Alarm**.

3. Review the settings. Click **Apply** to save changes.
   - **State: Enable** or **Disable** this feature.
   - **Server:** Enter the location of the mail server.
   - **Server Port:** Enter the port of the mail server (default 25).
   - **Account Name/Password:** Enter the email account and password to use for this feature

- **Mail From:** Specify the From: field in the email
- **Mail To:** Specify the To: field in the email
- **UTF-8 Encoding: Enable** or **Disable** the use of UTF-8 encoding in the email
- **Mail Event State:** Select the events to notify via email, as listed above



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

CLI Commands

Node	Command	Description
enable	show mail-alarm	Displays the current Mail Alarm configuration.
configure	mail-alarm (disable|enable)	Disables/enables the Mail Alarm function.
configure	mail-alarm auth-account	Configures the email account used for this function.
configure	mail-alarm mail-from	Configures the From: field in the email.
configure	mail-alarm mail-to	Configures the To: field in the email.
configure	mail-alarm server-ip IPADDR server-port (VALUE|"Default")	Configures the IP address and the TCP port of the email server. Use "Default" for the default SMTP port of 25.
configure	mail-alarm trap-event (reboot|link-change|config.| firmware|login|port-blocked| alarm) (disable|enable)	Configures the events that will cause the switch to send an email alert.

Monitor

View other important information about the switch here.

Alarm

System > Monitor > Alarm

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

2. Click on **System**, click on **Monitor**, and click on **Alarm**.

3. View the Alarm information.
   - **State:** Indicates the current alarm state.
   - **Alarm Reason(s):** Indicates the reason that the alarm is active

Alarm Information	
State	No Alarm.
Alarm Reason(s)	

(for some models)

The states of the DIP-Switches can also be reviewed here:

DIP-switch Settings			
DIP-switch	Status	DIP-switch	Status
Storm	Disable	QoS	Disable
P9 100Fx	Disable	P10 100Fx	Disable

CLI Commands

Node	Command	Description
enable	show alarm-info	Displays alarm information.

Port Utilization

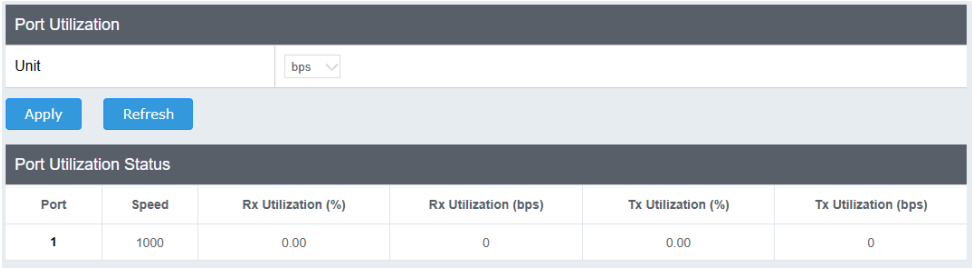
System > Monitor > Port Utilization

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

2. Click on **System**, click on **Monitor**, and click on **Port Utilization**.

3. View the port utilization statistics.

- **Units:** Display the below Tx/Rx statistics in bps, Kbps, or Mbps.
- **Rx Utilization (%):** Average receive rate percentage.
- **Rx Utilization (bps):** Average receive rate in bits per second. Units of measurement can be specified in the drop-down above.
- **Rx Utilization (%):** Average transmit rate percentage.
- **Rx Utilization (bps):** Average transmit rate in bits per second. Units of measurement can be specified in the drop-down above.



CLI Commands

Node	Command	Description
enable	show port-utilization	Displays the utilization of all active ports.

SFP Information

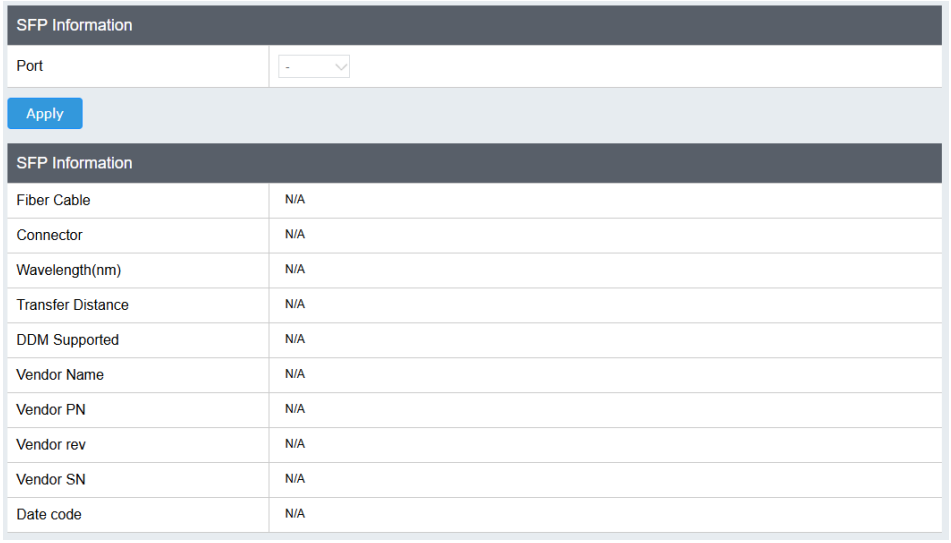
(models with SFP ports only)

System > Monitor > SFP Information

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

2. Click on **System**, click on **Monitor**, and click on **SFP Information**.

3. View the port utilization statistics.



CLI Commands

Node	Command	Description
enable	show sfp info port PORT_ID	Displays the information of the currently installed SFP module in the specified port.
enable	show sfp ddmi port PORT_ID	Displays the monitoring status of the currently installed SFP module in the specified port.

Traffic Monitor

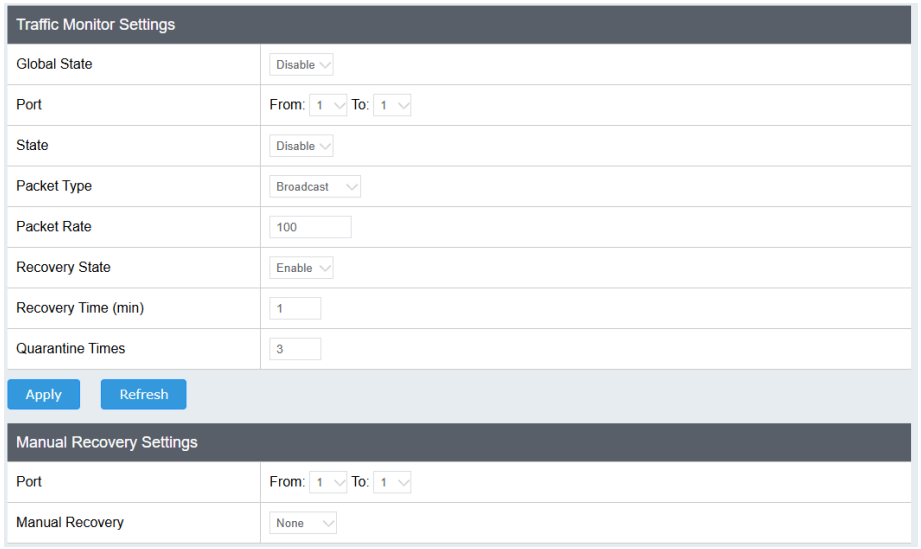
System > Monitor > Traffic Monitor

This feature monitors the rate at which packets enter the switch. If the packet rate exceeds the specified rate, the port will be blocked, and can be unblocked automatically after an optional recovery time.

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

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

3. Review the settings. Click **Apply** to save changes.
   - **Global State: Enable** or **Disable** the traffic monitor function.
   - **Port:** Specifies the range of port(s) to apply the following settings to.
   - **State: Enable** or **Disable** the traffic monitor function for the specified port(s).
   - **Packet Type:** Specify the packet type which you want to monitor.
   - **Packet Rate:** Enter the maximum packet rate for the specified port(s).
   - **Recover State: Enable** or **Disable** the recovery function for the specified port(s).
   - **Recovery Time:** Configures the recovery time for the traffic monitor function for the specified port(s) when the recovery function is enabled.



CLI Configuration

Node	Command	Description
enable	show traffic-monitor	Displays the traffic monitor configuration and current status.
configure	traffic-monitor (disable|enable)	Enables/disables the traffic monitor function.
interface if-range	traffic-monitor (disable|enable)	Enables/disables the traffic monitor on the specified port port.
interface if-range	traffic-monitor rate RATE_LIMIT type (bcast|mcast|bcast+mcast)	Configures the packet rate and packet type for the traffic monitor on the specified port. bcast – Broadcast packet. mcast – Multicast packet.
interface if-range	traffic-monitor recovery (disable|enable)	Enables/disables the recovery function on the specified port.

interface if-range	traffic-monitor recovery time VALUE	Configures the recovery time on the specified port.

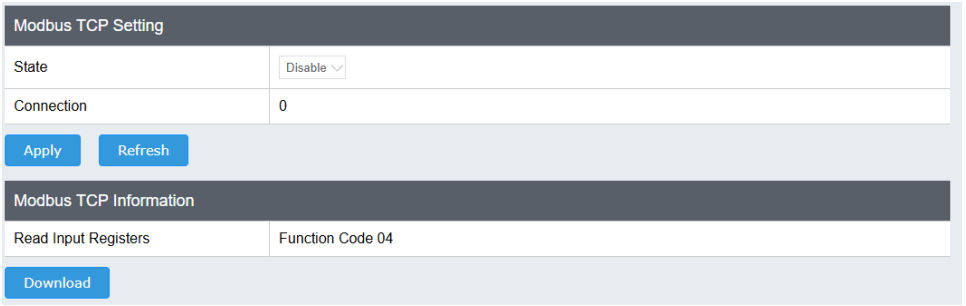
Modbus

System > Modbus

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

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

3. Review the settings. Click **Apply** to save changes.
   - **State: Enable** or **Disable** Modbus capability.
   - **Download:** Downloads the supported Modbus registers to a file on your local machine.



CLI Commands

Node	Command	Description
enable	show modbus	Displays the current Modbus configuration.
configure	modbus (disable|enable)	Disables/enables the Modbus function.

Auto Provision

System > Auto Provision

You can set up the switch to download configuration files and firmware updates automatically from a remote server.

When enabled, place a file on the server called "ModelName_Autoprovision.txt" (i.e. "TI-PG102i_Autoprovision.txt") that should contain the following:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=(the specified FW ver)
Firmware_Image_File=(name of FW file)
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=(name of configuration file)
Global_Configuration_Reboot=0
Specific_Configuration_State=0
Specific_Configuration_Reboot=0
```

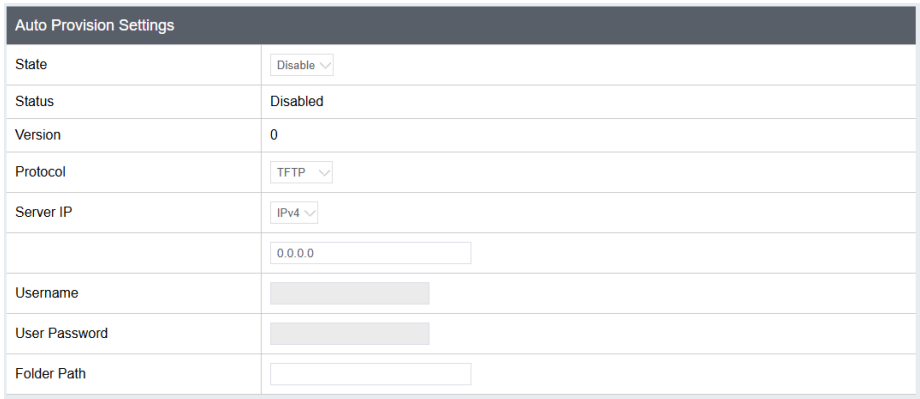
The switch will then perform the following procedure:

1. The switch will download the above autoconfiguration file.
2. If AUTO_PROVISION_VER is bigger than current auto provision version, do step 3; otherwise, wait 24 hours and go back to step 1.
3. If `Firmware_Upgrade_State=1`, do step 4; otherwise, do step 6.
4. If `Firmware_Version` is different than the current firmware version, download and update the firmware using `Firmware_Image_File`.
5. After the firmware is updated and `Firmware_Reboot=1`, reboot the switch.
6. If `Global_Configuration_State=1`, download `Global_Configuration_File` and update configuration; otherwise, do step 8.
7. After configuration update and `Global_Configuration_Reboot=1`, reboot the switch.
8. If `Specific_Configuration_State=1`, download the specific configuration file (named "Model_Name _" with the switch's MAC address, i.e. "TI-PG102i_***00e04c8196b9.txt***") and update configuration.
9. After configuration update and `Specific_Configuration_Reboot=1`, reboot the switch.
10. The auto provision procedure is complete.

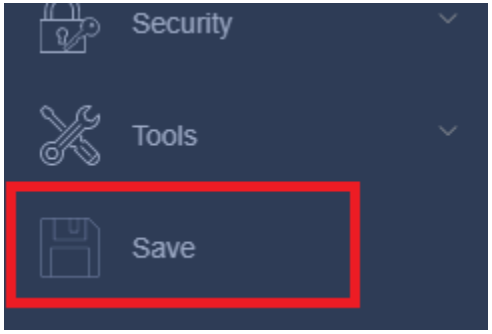
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **System** and click on **Auto Provision**.

3. Review the settings. Click **Apply** to save changes.
   - **State: Enable** or **Disable** Auto Provision.
   - **Protocol:** Select the protocol used on the remote server
   - **Server IP:** Enter the IP of the remote server
   - **Username:** Enter the username used for authentication.
   - **User Password:** Enter the password used for authentication.
   - **Folder Path:** Enter the folder/directory in which the auto provision file is located.



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



Network

Physical Interface

Configure Physical Interfaces

Network > Physical Interface

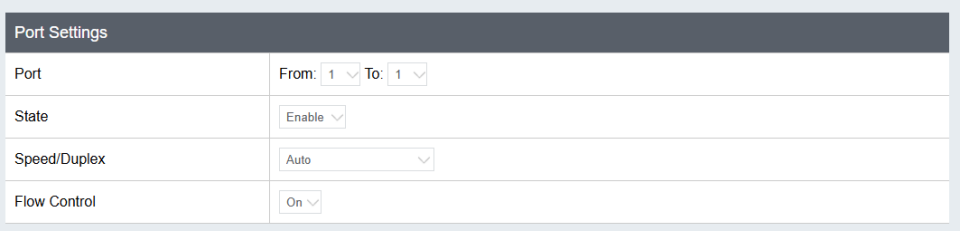
This section allows you to configure the physical port parameters such as speed, duplex, flow control, and jumbo frames. This section also reports the current link status of each port and negotiated speed/duplex. Additionally you will be able to set your BPDU ports for Spanning Tree Configuration and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

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

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

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

- **Port -** Specifies the port number. Select the range of ports to apply the new settings to with the **From** and **To** drop-down list.



- **State:** This parameter indicates the operating status of the port. You can use this parameter to enable or disable a port. You may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. You can enable the port to resume normal operation after the problem has been fixed. You can also disable an unused port to secure it from unauthorized connections. The possible values are:
  - **Ignore** -This parameter applies to the **All** row only and indicates that the **Admin. Status** field must be set individually for each port.
  - **Enabled** - This parameter indicates the port is able to send and receive Ethernet frames.
  - **Disabled** - This parameter indicates the port is not able to send and receive Ethernet frames.
- **Speed/Duplex:** This parameter indicates the speed and duplex mode settings for the port. You can use this parameter to set the speed and duplex mode of a port. The possible settings are:
  - **Ignore** -This parameter indicates that the **All** setting does not apply to the **Mode** field. In other words, each port is set individually.
  - **Auto** -This parameter indicates the port is using Auto-Negotiation to set the operating speed and duplex mode. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "1000/F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.
  - **1000/Full** -This parameter indicates the port is configured for 1000Mbps operation in full-duplex mode.
  - **100/Full** -This parameter indicates the port is configured for 100Mbps operation in full-duplex mode.
  - **10/Full** -This parameter indicates the port is configured for 10Mbps operation in full-duplex mode.
  - **100/Half** -This parameter indicates the port is configured for 100Mbps operation in half-duplex mode.
  - **10/Half** -This parameter indicates the port is configured for 10Mbps operation in half-duplex mode.

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

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

- **Flow Control:** Flow Control, This parameter reflects the current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:
    - **Ignore** - This parameter indicates that the **All** setting does not apply to the **Flow Control** field. In other words, each port is set individually.
    - **Enabled** - This parameter indicates that the port is permitted to use flow control.
    - **Disabled** - This parameter indicates that the port is not permitted to use flow control.
- **Link Status -** This parameter indicates the status of the link between the port and the end node connected to the port. The possible values are:
    - **Up** -This parameter indicates a valid link exists between the port and the end node.
    - **Down** -This parameter indicates the port and the end node have not established a valid link.

Port Status

Port	State	Speed/Duplex	Flow Control	Link Status
1	Enabled	Auto	On	1000M / Full / On
2	Enabled	Auto	On	Link Down
3	Enabled	Auto	On	Link Down
4	Enabled	Auto	On	Link Down
5	Enabled	Auto	On	Link Down
6	Enabled	Auto	On	Link Down
7	Enabled	Auto	On	Link Down

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

Spanning Tree

Protocol

Network > Spanning Tree > Protocol

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

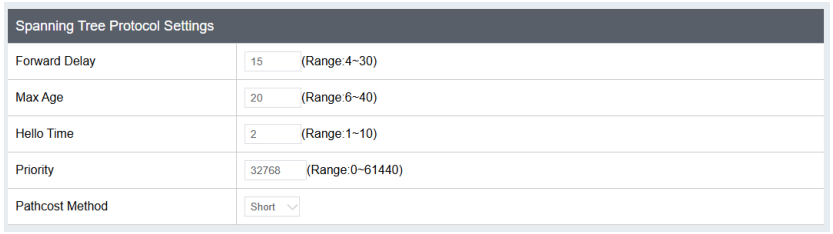
1. Log into your switch management page (see "Access your switch management page on page 5").

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

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

- **Global STP Status:** Select the STP state on the device. The possible field values are:
    - **Disable** – Disables STP on the device. This is the default value.
    - **Enable** – Enables STP on the device.
- **Protocol Version:** Specifies the Spanning Tree Protocol (STP) mode to enable on the switch. The possible field values are:
    - **STP** – Enables STP 802.1d on the device.
    - **RSTP** – Enables Rapid STP 802.1w on the device. This is the default value.
    - **MSTP** – Enables Multiple STP 802.1s on the device.
- **Forward Delay:** The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.
- **Maximum Age:** The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds
- **Hello Time:** The Hello Time is frequency with which the root bridge sends out a BPDU.
- **Bridge Priority:** Enter the desired priority value within the range of 0 - 61440.

- **Pathcost Method:** Select **Short** or **Long** path first method



Port

Network > Spanning Tree > Port

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

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

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

- **Active:** Indicates if spanning tree protocol is active or not on the port. Select one of the following choices from the pull-down menu:
  - **Enable** - The spanning tree protocol is enabled on the port.
  - **Disabled** - The spanning tree protocol is disabled on the port.
- **Role:** The current role of the port. For display purposes only Can be **Alternated**, **Designated**, **Root**, **Backup**, or **None**
- **Path cost:** Specify the path cost of using this port. The recommended values for this option depend on the link speed as shown below:

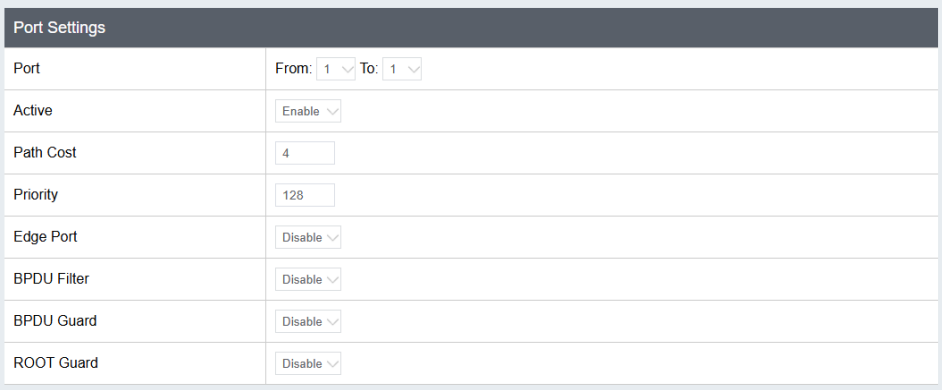
	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

- **Priority:** Indicates the port priority. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost. The range for port priority is 0 to 240.
- **Status –** Displays the current port spanning tree status.
  - **Blocking** - A blocking state does not allow network traffic to be sent or received on a the port except for BPDU data. A port with a higher path

cost to the root bridge than another on the switch causes a switching loop and is placed in the blocking state by the Spanning Tree algorithm. The port's state may change to the forwarding state if the other links in use fail and the Spanning Tree algorithm determines the port may transition to the forwarding state.

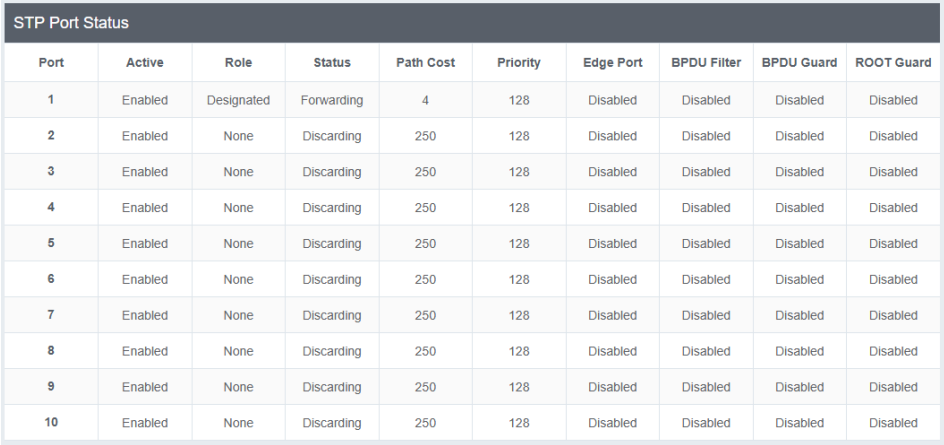
- **Listening** - This state occurs on a port during the convergence process. The port in the listening state processes BPDUs and awaits new information that would cause the port to return to the blocking state.
- **Learning** - While the port does not yet forward frames (packets), in this state the port does learn source addresses from frames received and adds them to the filtering (switching) database.
- **Forwarding** - A port that both receives and sends data. This indicates normal operation. STP continues to monitor the port for incoming BPDUs that indicate the port should return to the blocking state to prevent a loop.
- **Disabled** - This state is not strictly part of STP. However, a network administrator can manually disable a port.

- **Edge:** Mark this port as an edge port, which does not have any other bridges connected to it.
- **BPDU Filter:** Filter BPDUs from being sent or received by the port.
- **BPDU Guard:** When this option is turned on, and the switch receives a BPDU packet, the switch port will be automatically disabled and must be reenabled manually.
- **ROOT Guard:** Mark this port as a Designated port and prevent other switches connected to this switch from becoming the STP root.



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

The current STP status for each port is listed in the table below:



CLI Commands

Node	Command	Description
enable	show spanning-tree active	Displays the spanning tree information for all active port(s)

enable	show spanning-tree blockedports	Displays the spanning tree information for all blocked port(s)
enable	show spanning-tree port detail PORT_ID	Displays the spanning tree information for the specified port.
enable	show spanning-tree statistics PORT_ID	Displays the spanning tree information for the specified port.
enable	show spanning-tree summary	Displays a summary of port states and configuration of the spanning tree
enable	clear spanning-tree counters [PORT_ID]	Clears the spanning-tree statistics for the specified port, or all ports if none is specified.
configure	spanning-tree (disable | enable)	Disables/enables the spanning tree function.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	Configures the bridge times for the STP algorithm (forward-delay,max-age,hello-time).
configure	no spanning-tree algorithm-timer	Resets the bridge times for the STP algorithm (forward-delay,max-age,hello-time) to defaults.
configure	spanning-tree forward-time <4-30>	Configures the bridge forward delay time (sec).
configure	no spanning-tree forward-time	Resets the bridge forward-delay time to defaults.
configure	spanning-tree hello-time <1-10>	Configures the bridge hello time(sec).
configure	no spanning-tree hello-time	Resets the bridge hello time to defaults.
configure	spanning-tree max-age<6-40>	Configures the bridge message max-age time(sec).
configure	no spanning-tree max-age	Resets the bridge message max-age time to defaults.
configure	spanning-tree mode (rstp|stp)	Configures the spanning tree mode.
configure	spanning-tree pathcost method (short|long)	Configures the pathcost method used for STP pathfinding.
configure	spanning-tree priority<0-61440>	Configures the system STP priority.
configure	no spanning-tree priority	Resets the system STP priority to defaults.
interface / if-range	spanning-tree (disable|enable)	Enables/disables STP for the specified port(s).
interface / if-range	spanning-tree bpdufilter (disable|enable)	Enables/disables the BDPU Filter for the specified port(s).
interface / if-range	spanning-tree bpduguard (disable|enable)	Enables/disables the BDPU Guard function for the specified port(s).
interface / if-range	spanning-tree rootguard (disable|enable)	Enables/disables the BPDU Root guard port setting for the specified port(s).
interface / if-range	spanning-tree edge-port (disable|enable)	Enables/disables the edge port setting for the specified port(s).
interface / if-range	spanning-tree cost VALUE	Configures the path cost for the specified port(s). Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface / if-range	no spanning-tree cost	Resets the path cost for the specified port(s) to defaults.
interface /	spanning-tree port-priority <0-240>	Configures the port priority for the specified port(s).

if-range		Default: 128.
interface / if-range	no spanning-tree port-priority	Resets the port priority for the specified port(s) to defaults.

Trunk

The trunking function enables the cascading of two or more ports for a combined larger total bandwidth. Up to 3 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.*

Settings

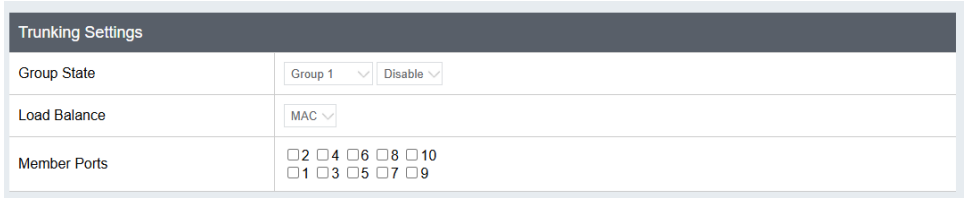
Network > Trunk > Settings

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

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

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

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



For the **Load Balance** policy, select whether to use the **MAC** or **IP** of the hosts for trunking.

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

CLI Commands

Node	Command	Description
enable	show link-aggregation	Displays the current trunk configuration.
configure	link-aggregation [GROUP_ID] (disable | enable)	Disables/enables the trunk on the specified trunk group.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	Adds the specified port(s) to a specified trunk group.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	Removes the specified port(s) from a specified trunk group.

Status

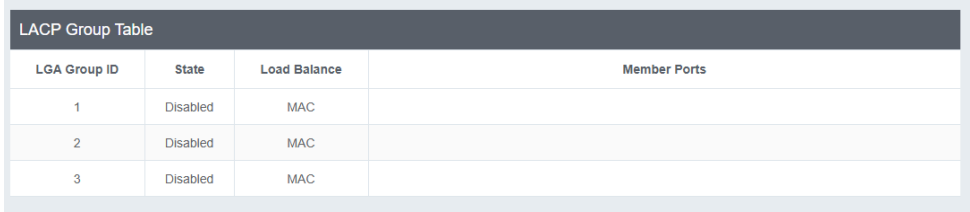
Network > Trunk > Status

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

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

3. View your trunk group status information.

- **LGA Group ID –** Displays the trunk group ID.
- **State –** Indicates whether the trunk group is active.
- **Load Balance –** The current load balance policy for the trunk group.
- **Member Ports –** List of ports in the trunk group.



Port Priority

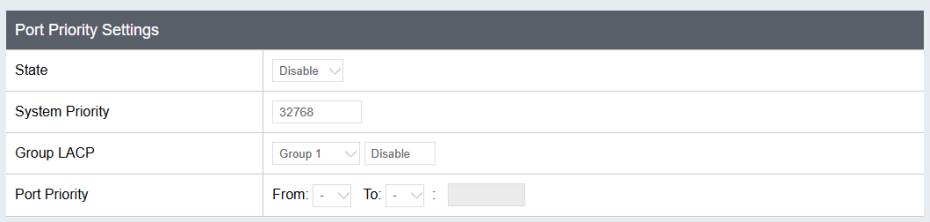
Network > Trunk > Port Priority

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

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

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

To assign a port higher priority within a trunk group, select the LACP group and port range, and in the priority field, enter a value from 0-32768 (32768 being the highest priority).



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

CLI Commands

Node	Command	Description
enable	show lacp counters [GROUP_ID]	Displays the LACP counters for the specified group, or all groups if none is specified.
enable	show lacp internal [GROUP_ID]	Displays the LACP internal information for the specified group, or all groups if none is specified.
enable	show lacp neighbor [GROUP_ID]	Displays the LACP neighbor's information for the specified group, or all groups if none is specified.
enable	show lacp port_priority	Displays the port priority for the trunk.
enable	show lacp sys_id	Displays the actor's and partner's system ID.
configure	lacp (disable | enable)	Disables/enables the LACP function.
configure	lacp GROUP_ID (disable | enable)	Disables/enables LACP on the specified trunk group.
configure	clear lacp counters [PORT_ID]	Clears the LACP statistics for the specified port, or all ports if none is specified.
configure	lacp system-priority<1-65535>	Configures the LACP system priority. Note: The default value is 32768.
configure	no lacp system-priority	Resets the LACP system priority to defaults.
interface / if-range	lacp port_priority <1-65535>	Configures the priority for the specified port. Note: The default value is 32768.
interface / if-range	no lacp port_priority	Resets the priority for the specified port to defaults.

Mirroring

Configure port mirror settings

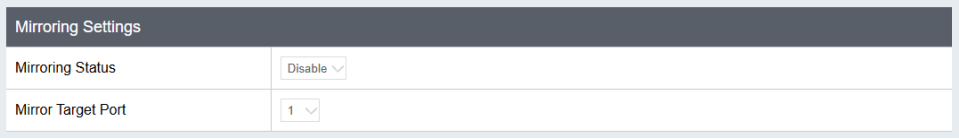
Network > Mirroring

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

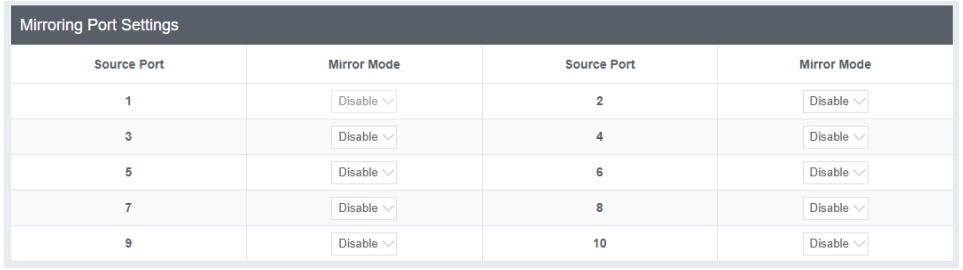
1. Log into your switch management page (see "Access your switch management page on page 5").

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

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



Select the port(s) to monitor or copy information from.



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

CLI Commands

Node	Command	Description
enable	show mirror	Displays the current port mirroring configuration.
configure	mirror (disable|enable)	Disables/enables port mirroring.
configure	mirror destination port PORT_ID	Specifies the monitor port for the port mirror.
configure	mirror source ports PORT_LIST mode *(both|ingress|egress)*	Adds a port or a range of ports as the source ports of the port mirror.
configure	no mirror source ports PORT_LIST	Removes a port or a range of ports from the source ports of the port mirroring.

Loopback Detection

Enable loopback detection

Network > Loopback Detection

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

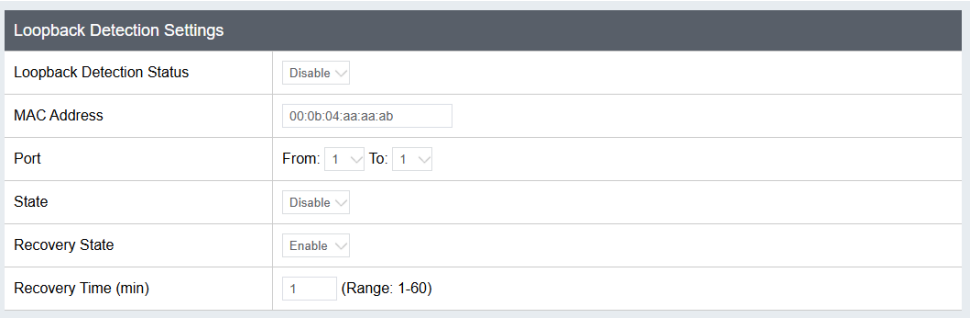
1. Log into your switch management page (see "Access your switch management page on page 5").

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

3. Review the settings.

- **Loopback Detection Status** – Select **Enabled** to enable the loopback detection feature. Select **Disabled** to disabled the loopback detection feature.
- **MAC Address** – Specifies the MAC address that will receive the special loopback detection packets.
- **Interval –** Defines the interval your switch will check for loops.
- **Recovery Time –** Defines the time period when connectivity will be restored to a port where a loop was previously detected and blocked.

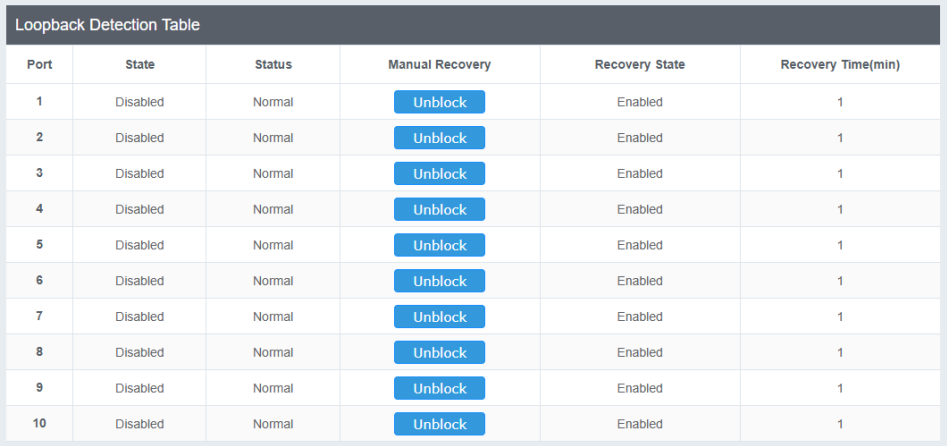
Click **Apply** to save changes.



In the Loopback Detection table, select one of the **Loopback Detection Status** choices from the pull down menu:
Ignore: This parameter indicates that the setting in the **All** row do not apply to the **Loopback Detection Status** 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 **Status** field at the top of the page before this feature can be active on the selected port.
- **Disabled:** This selection disables the Loopback Detection feature on the selected port.
- ***Note:*** *In the **All** row when you select **Enable** or **Disable** instead of **Ignore**, the selection applies to all of the Switch ports.*

In case a port is inadvertently blocked, click the **Unblock** button to unblock the port.



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

CLI Commands

Node	Command	Description
enable	show loop-detection	Displays the current loopback detection configuration.

configure	loop-detection (disable | enable)	Disables/enables loopback detection.
configure	loop-detection address MACADDR	Configures the destination MAC that will receive the special loopback detection packets.
configure	no loop-detection address	Clears the destination MAC setting and resets it to defaults.
interface / if-range	loop-detection (disable | enable)	Disables/enables loopback detection on the specified port.
interface	no shutdown	Unblocks the port blocked by loopback detection.
interface / if-range	loop-detection recovery (disable | enable)	Enables/disables the recovery function.
interface / if-range	loop-detection recovery time VALUE	Configures the recovery time before the port is automatically unblocked.

Static Unicast

Add static unicast entries to the switch

Network > Static Unicast

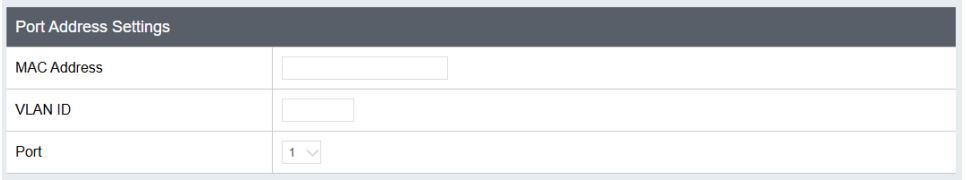
In this section, you can add static unicast entries to the switch configuration.

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

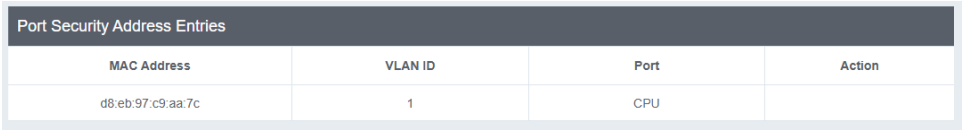
2. Click on **Network** and click on **Static Unicast**.

3. Review the settings.
   - **MAC Address** – Enter the MAC address of the device to add.
   - **VLAN ID** – 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.*
   - **Port –** Select the port where the MAC address will reside.

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



In the list, you can click **Modify** to modify an entry or click **Delete** or delete the entry**.** You cannot delete the default CPU port entry.



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

CLI Commands

Node	Command	Description
enable	show mac-address-table aging-time	Displays the current MAC address table age time.
enable	show mac-address-table (static|dynamic)	Displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	Displays information of a specific MAC.
enable	show mac-address-table port PORT_ID	Displays the current unicast address entries learnt by the specified port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	Configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan VLANID	Removes a static unicast entry from the address table.
configure	clear mac address-table dynamic	Clears all of the dynamic address entries from the switch.

Static Multicast

Add static multicast entries to the switch

Network > Static Multicast

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

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

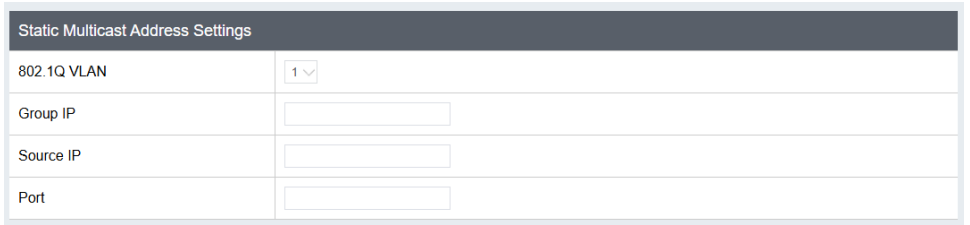
2. Click on **Network** and click on **Static Multicast**.

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

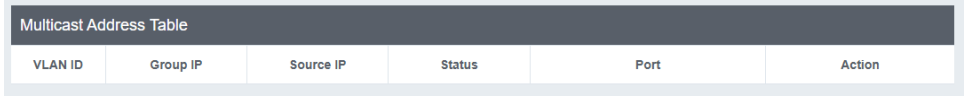
     Note: *By default, all switch ports are part of the default VLAN, VLAN ID 1.*
   - **Source IP** – Enter the multicast source IP address.
   - **Group IP** – Enter the multicast group IP address.
   - **Port –** Enter the port(s) where the multicast address will reside.

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

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



In the list, you can click **Delete** to delete the entry**.**



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

CLI Commands

Node	Command	Description
enable	show mac-address-table multicast	Displays the current static/dynamic multicast address entries.
configure	mac-address-table multicast MACADDR vlan VLANID ports PORTLIST	Command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	Removes a static multicast entry from the address table.

IGMP Snooping

Settings

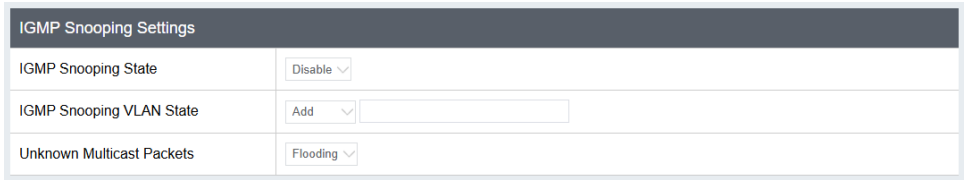
Network > IGMP Snooping > Settings

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

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

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

- **State** – Click the drop-down list and select **Enabled** to enable the IGMP snooping feature or **Disabled** to disable the feature.
- **VLAN State –** Click the drop-down list to **Add** or **Delete** the entered VLAN.
- **Unknown Multicast Packets –** Click the drop-down list to select whether to **Drop** or pass (**Flooding**) unknown multicast packets
- .
- **Fast Leave Status** – Click the drop-down list and select **Enabled** to enable the Fast Leave Status or **Disabled** to disable this feature
- **Querier Interval** – Enter the amount of time you want your switch to send IGMP queries.
- **Max Response Time**- Specifies the maximum time before sending a response report.
- **Robustness Variable**- Enter a variable for the expected packet loss on a subnet. The robustness variable should be set to a larger value if higher packet loss is expected.
- **Last Member Query Interval** - Set the response time for group queries sent in response to leave messages.
- **Router Timeout** - **Enter** the maximum time duration without router messages before the router timeout.



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.

IGMP Snooping State	
IGMP Snooping State	Disabled
Enabled on VLAN	None
Unknown Multicast Packets	Flooding

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

Port Settings

Network > IGMP Snooping > Port Settings

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

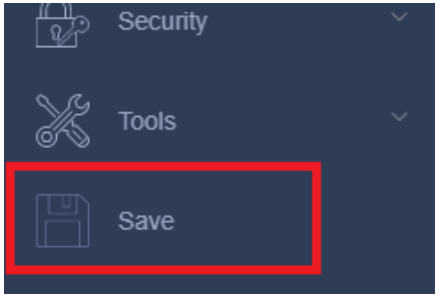
2. Click on **Network**, click on **IGMP Snooping**, and click on **Router Port**.

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

- **Port -** Specifies the range of ports to apply the following settings to.
- **Querier Mode –** Click the drop-down list to **Add** or **Delete** the entered VLAN.
- **Immediate Leave Status** – Click the drop-down list and select **Enabled** to enable the Immediate Leave Status or **Disabled** to disable this feature.
- **Group Limit** – Click the drop-down list and select **Enabled** to enable the Immediate Leave Status or **Disabled** to disable this feature

Port Settings	
Port	From: 1 To: 1
Querier Mode	Auto
Immediate Leave	Disable
Group Limit	266

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



CLI Commands

Node	Command	Description
enable	show igmp-snooping	Displays the current IGMP snooping configuration.
enable	show igmp-counters	Displays the current IGMP snooping counters.
enable	show igmp-counters (port|vlan)	Displays the current IGMP snooping counters per port/VLAN.
configure	igmp-snooping (disable | enable)	Disables/enables IGMP snooping.
configure	igmp-snooping vlan VLANID	Enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANID	Disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop|flooding)	Configures the process for unknown multicast packets when IGMP snooping is enabled. *drop:* Drop all of the unknown multicast packets.
interface	igmp-querier-mode (auto|fixed|edge)	Specifies whether and under what conditions the specified port(s) is considered an IGMP query port. (Default:auto)
interface	igmp-immediate-leave	Enables the immediate leave function for the specific interface.
interface	no igmp-immediate-leave	Disables the immediate leave function for the specific interface.

Bandwidth Control

Storm Control

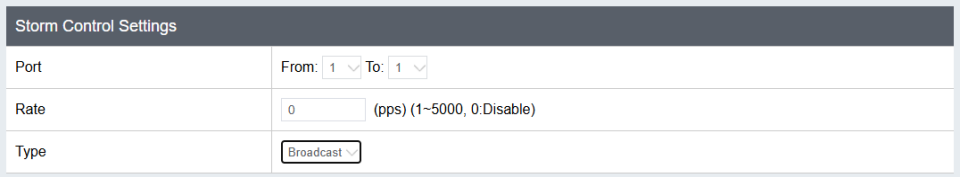
Network > Bandwidth Control > Storm Control

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

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

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

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Port -** Specifies the range of ports to apply the following settings to.
   - **Rate** – Enter the pps (packets per second) threshold.
   - **Type** – Click the drop-down list to select either **Broadcast**, **Multicast**, or **DLF (Destination Lookup Failure)**.



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

CLI Commands

Node	Command	Description
enable	show storm-control	Displays the current storm control configuration.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	Enables and sets the bandwidth limit for broadcast or multicast or DLF packets.

configure	no storm-control type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	Disables the bandwidth limit for broadcast or multicast or DLF packets.

Ingress Rate Limiting

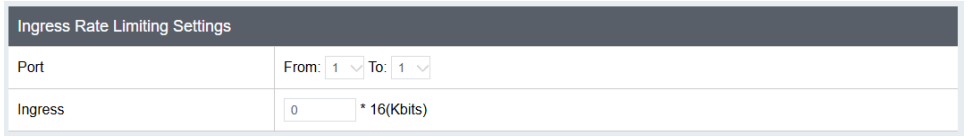
Network > Bandwidth Control > Ingress Rate Limiting

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

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

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

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Port -** Specifies the range of ports to apply the following settings to.
   - **Ingress** – Enter the ingress rate limit value.



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

CLI Commands

Node	Command	Description
enable	show bandwidth-limit	Displays the current rate control configurations.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	Enables and sets the bandwidth limit for incoming packets.
configure	no bandwidth-limit ingress ports PORTLISTS	Disables the bandwidth limit for incoming packets.

Egress Rate Limiting

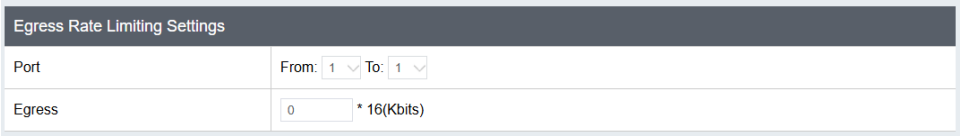
Network > Bandwidth Control > Egress Rate Limiting

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

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

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

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Port -** Specifies the range of ports to apply the following settings to.
   - **Egress** – Enter the egress rate limit value.



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

CLI Commands

Node	Command	Description
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	Enables and sets the bandwidth limit for outgoing packets.
configure	no bandwidth-limit egress ports PORTLISTS	Disables the bandwidth limit for outgoing packets.

VLAN

Settings

Network > VLAN > Settings

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

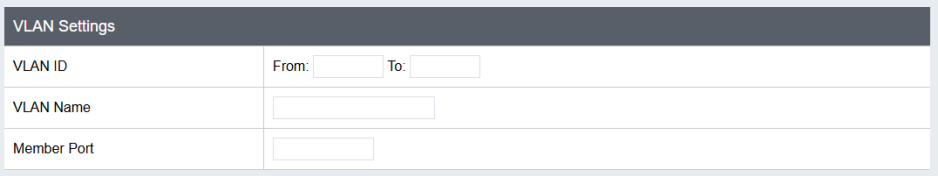
VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having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

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

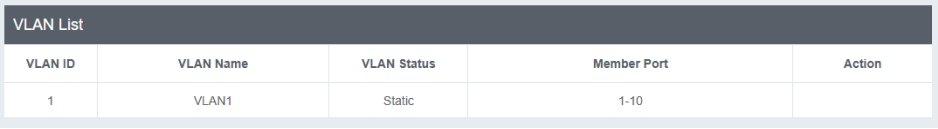
2. Click on **Network**, click on **VLAN,** and click on **Settings**.

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

     Note: *By default, the default VLAN VID 1 is set as the Management VLAN.*
   - **Port -** Enter the port(s) to assign the new VLAN(s) to.



In the list, you can click **Delete** to delete the entry. You cannot delete the default VLAN1.



Tagged

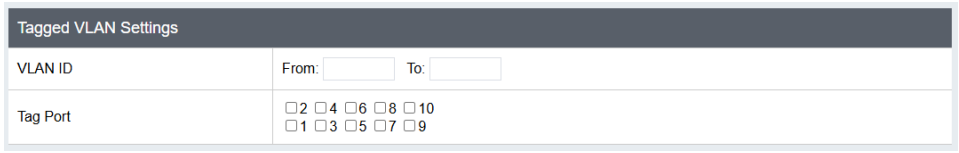
Network > VLAN > Tagged

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.

Enter the VLAN(s) and select the ports to add as tagged members to the new VLAN.



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

Click **Apply** to save the changes to the VLAN.

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

Port

Network > VLAN > Port

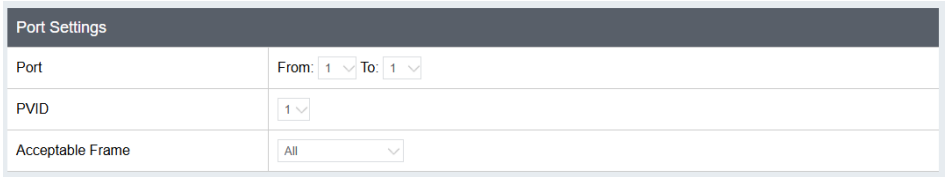
In this section, you can modify the port VID settings, acceptable frame types, and ingress filtering.

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

2. Click on **Bridge**, click on **VLAN,** and click on **Port Settings**.

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

- **Port –** Specifies the range of ports to apply the following settings to.
- **PVID –** Enter the port VLAN ID. ***Note:*** *Required for untagged VLAN ports.*
- **Acceptable Frame Type** – Click the drop-down list and select which type of frames can be accepted.
  - **All** – The port can accept all frame types.
  - **Tagged** – The port can accept tagged frames only. Untagged frames are discarded.
  - **Untagged** – The port can accept untagged frames and frames with tagged priority information only such as 802.1p.



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

Dynamic

Network > VLAN > Dynamic

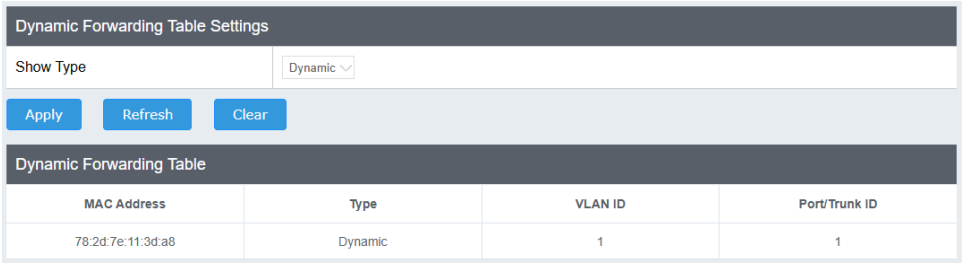
This section allows you to view the VLAN forwarding table with dynamically generated forwarding table entries as devices more devices are connected to your switch.

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

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

3. By default, dynamic forwarding entries for all ports are listed. You can click the **Show Type** drop-down list to view the forwarding tables of different types (i.e. **Static**, **Port**, or **MAC**).

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.



Private

Network > VLAN > Private

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

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

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

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

3. To configure Private VLAN Settings, perform the following procedure:
   - Set the **Source Port** range from the pull-down menu.
   - Click on the **Forwarding Ports** checkboxes that applies to your configuration.
   - Click **Apply.**

In the table, the numbered columns represent the **Forwarding Ports** that the port listed on the **Port** column is allowed to forward ports to.

Port List								
Port	1	2	3	4	5	6	7	8
1	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓	✓	✓
7	✓	✓	✓	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓	✓	✓	✓

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

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.*

Settings

Network > Voice VLAN > Settings

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

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

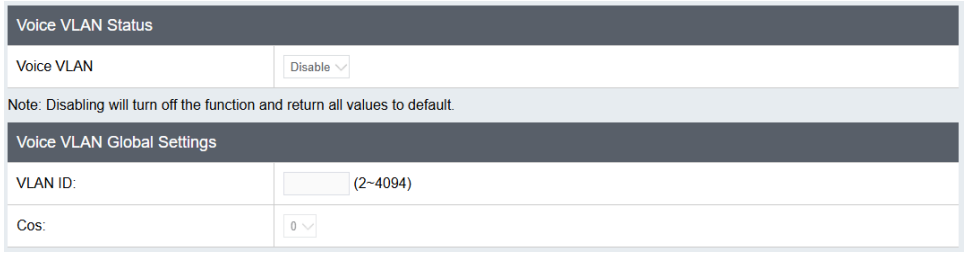
2. Click on **Network**, click on **Voice VLAN,** and click on **Settings**.

3. Review the settings.

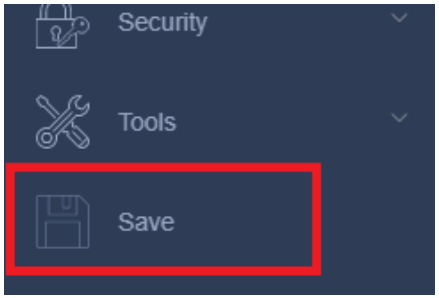
Use the following procedure to configure voice VLAN:

- From the **Voice VLAN** field at the top of the page, select one of the following radio button choices:
  - **Enable -** The voice VLAN feature is active. The other parameter fields in the voice VLAN Global Settings section become active and are eligible for data to be entered.
  - **Disable** - The voice VLAN feature is inactive. The other parameter fields in the voice VLAN Global Settings section become inactive and are greyed out so that data cannot be entered.
- In the Voice VLAN Global Settings section, enter the configuration information for the following parameters:
  - **VLAN ID** - This parameter is the tagged VLAN ID that has been configured in "Tagged VLAN Configuration". It is a pull-down menu showing the tagged VLAN IDs that have been defined.
  - **Aging Time** - This parameter indicates the amount of time, in hours, after the last IP phone's OUI was received on a port, after which this port will be removed from the voice VLAN. The range is 1 to 120 hours.
  - **CoS** - This parameter is CoS priority level assigned to the voice data packets received on each voice VLAN port. For the **COS** priority to be effective, QoS must be **Enabled**.

Click **Apply** to save the settings.



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



OUI

Network > Voice VLAN > OUI

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

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

3. Review the settings.

Use the following procedure to configure voice VLAN OUIs:

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

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

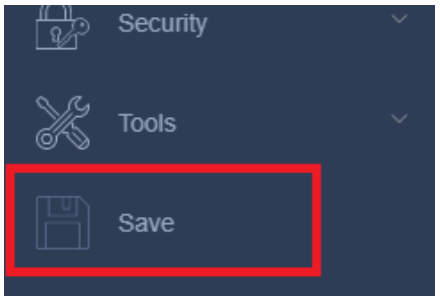
Modify OUI Setting

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

Delete OUI Setting

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

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



LLDP

Enable and configure LLDP

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network and to store data that is learned about other devices. Devices discovered through LLDP can be added to the Topology Map (**Dashboard > Topology Map**).

Settings

Network > LLDP > Settings

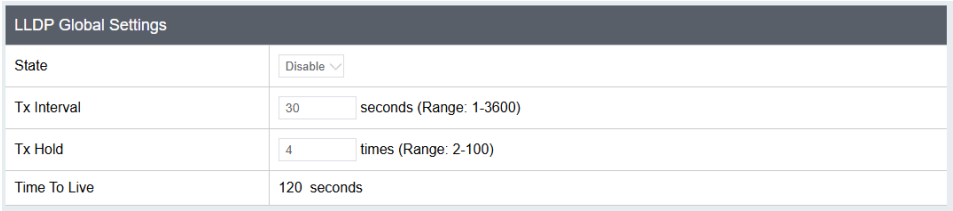
1. Log into your switch management page (see "Access your switch management page on page 5").

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

3. Review the settings.

Enabling or Disabling LLDP

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



The following settings can be set:

- **Tx Interval –** Specifies the interval between LLDP advertisements.
- **Tx Hold –** Specifies the multiplier of **Tx Interval** to provide the Time To Live (TTL) that the switch advertises to the neighbors.

MED Port Settings

Network > LLDP > MED Port Settings

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

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

3. Configure the MED port settings. Click **Apply** to save.

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

LLDP Statistics Information

Network > LLDP > LLDP Statistics Information

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

2. Click on **Network**, click on **LLDP,** and click on **LLDP Statistics Information.**

3. View the LLDP Statistics Information. Click **Clear** to clear the counters.

Neighbor

Network > LLDP > Neighbors

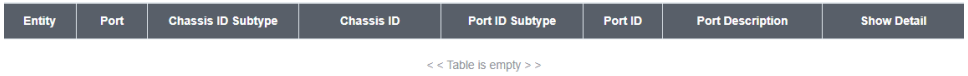
1. Log into your switch management page (see "Access your switch management page on page 5").

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

3. View the LLDP neighbor information.
   - **Entity:** This parameter is a number assigned to the reporting neighbors in the order that the LLDP information is received from them.
   - **Port:** This parameter specifies the 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 Detail:** 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.



CLI Commands

Node	Command	Description
enable	show lldp	Displays the LLDP configuration.
enable	show lldp neighbor	Displays all of the ports' neighbor information.
configure	lldp (disable|enable)	Globally enables/disables the LLDP function.
configure	lldp tx-interval	Configures the interval between the transmission of LLDP packets.
configure	lldp tx-hold	Configures the tx-hold time which determines the TTL of the LLDP packet. (TTL=tx-hold * tx-interval)
interface	lldp-agent (disable|enable|rx-only|tx-only)	Configures the LLDP agent function. disable – Disable the LLDP on the specific port. enable – Transmit and Receive the LLDP packet on the specific port. tx-only – Transmit the LLDP packet on the specific port only. rx-only – Receive the LLDP packet on the specific port.

MAC VLAN

MAC VLAN

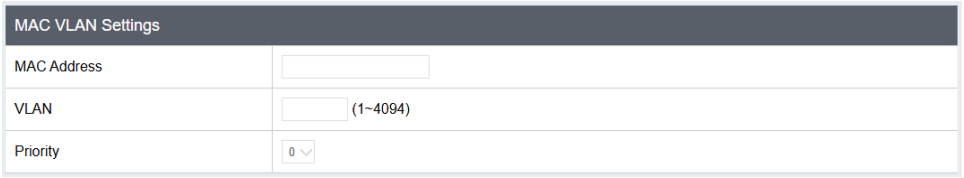
Network > MAC VLAN

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

2. Click on **Network** and click on **MAC VLAN**.

3. Configure the MAC VLAN. Click **Add** to save.

- **MAC Address –** Enter the MAC Address to add to the VLAN
- **VLAN ID –** Assign a VLAN ID
- **Description –** Enter a Description.



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

Protocol VLAN

Network > Protocol VLAN

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

2. Click on **Network** and click on **Protocol VLAN**.

3. Configure the Protocol VLAN. Click **Apply** to save.

- **Frame Type –** Select a frame type from the drop down.
- **Ethernet Type –** Assign an Ether Type from 0000 to FFFF.
- **VLAN –** Assign a VLAN to the profile.
- **Priority –** Select a priority level from the dropdown menu

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

Manual Registration

Network > Manual Registration

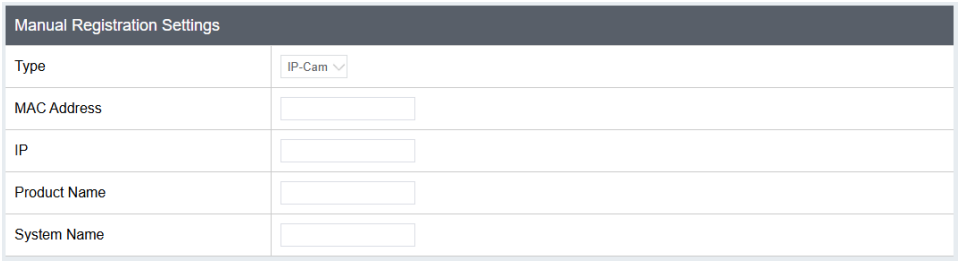
Devices that cannot be discovered automatically by LLDP or ONVIF for the Topology Map can be added here.

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

2. Click on **Network** and click on **Manual Registration**.

3. Configure the new device entry. Click **Apply** to save.

- **Type –** Select from IP-Cam, PLC, Switch, or PC from the drop down.
- **MAC Address –** Enter the MAC Address of the device.
- **IP –** Enter the IP Address of the device.
- **Product Name/System Name –** Enter a descriptive name for the device.



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

5. Navigate to the Topology Map (**Dashboard > Topology Map**) to find the newly added device.

ONVIF

Network > ONVIF

The ONVIF protocol can be used to discover and add devices automatically for the Topology Map.

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

2. Click on **Network** and click on **ONVIF**.

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

- **State – Enable** or **Disable** ONVIF on this switch.
- **Tx Interval –** Specify the interval in which the switch sends out ONVIF discovery packets.

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

5. Navigate to the Topology Map (**Dashboard > Topology Map**) to find the newly added devices.

ERPS

The ITU-T G.8032 **E**thernet **R**ing **P**rotection **S**witching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 **Ethernet Ring Protection (ERP)** protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

The Ethernet ring protection functionality includes the following:

- Loop avoidance
- The use of learning, forwarding, and Filtering Database (FDB mechanisms

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the **ring protection link (RPL)** and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the **RPL owner** node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible for unblocking its end of the RPL, unless the RPL has failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, **the RPL neighbour** node, may also participate in blocking or unblocking its end of the RPL.

The Ethernet rings could support a multi-ring/ladder network that consists of conjoined Ethernet rings by one or more interconnection points. The protection switching mechanisms and protocol defined in this Recommendation shall be applicable for a multi-ring/ladder network, if the following principles are adhered to:

- R-APS channels are not shared across Ethernet ring interconnections;
- on each ring port, each traffic channel and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet ring protection control process (ERP control process) of only one Ethernet ring;
- Each major ring or sub-ring must have its own RPL.

In an Ethernet ring, without congestion, with all Ethernet ring nodes in the idle state (i.e., no detected failure, no active automatic or external command and receiving only "NR, RB" R-APS messages), with less than 1200 km of ring fibre circumference and fewer than 16 Ethernet ring nodes, the switch completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link shall be less than **50 ms**.

The ring protection architecture relies on the existence of an **APS protocol** to coordinate ring protection actions around an Ethernet ring.

The Switch supports up to **six** rings.

Guard timer – All ERNs use a guard timer. The guard timer prevents the possibility of forming a closed loop and prevents ERNs from applying outdated R-APS messages. The guard timer activates when an ERN receives information about a local switching request, such as after a switch fail (SF), manual switch (MS), or forced switch (FS). When this timer expires, the ERN begins to apply actions from the R-APS it receives. This timer cannot be manually stopped.

Wait to restore (WTR) timer – The RPL owner uses the WTR timer. The WTR timer applies to the revertive mode to prevent frequent triggering of the protection switching due to port flapping or intermittent signal failure defects. When this timer expires, the RPL owner sends a R-APS (NR, RB) through the ring.

Wait to Block (WTB) timers – This wait-to-block timer is activated on the RPL owner. The RPL owner uses WTB timers before initiating an RPL block and then reverting to the idle state after operator-initiated commands, such as for FS or MS conditions, are entered. Because multiple FS commands are allowed to co-exist in a ring, the WTB timer ensures that the clearing of a single FS command does not trigger the re-blocking of the RPL. The WTB timer is defined to be 5 seconds longer than the guard timer, which is enough time to allow a reporting ERN to transmit two R-APS messages and allow the ring to identify the latent condition. When clearing a MS command, the WTB timer prevents the formation of a closed loop due to the RPL owner node applying an outdated remote MS request during the recovery process.

Hold-off timer – Each ERN uses a hold-off timer to delay reporting a port failure. When the timer expires, the ERN checks the port status. If the issue still exists, the failure is reported. If the issue does not exist, nothing is reported.

ERPS revertive and non-revertive switching

ERPS considers revertive and non-revertive operation. In revertive operation, after the condition(s) causing a switch has cleared, the traffic channel is restored to the working transport entity, i.e. blocked on the RPL. In the case of clearing of a defect, the traffic channel reverts after the expiry of a WTR timer, which is used to avoid toggling protection states in case of intermittent defects. In non-revertive operation, the traffic channel continues to use the RPL, if it is not failed, after a switch condition has cleared.

Control VLAN:

The pure ERPS control packets domain only, no other packets are transmitted in this vlan to guarantee no delay for the ERPS. So when you configure a Control VLAN for a ring, the vlan should be a new one. The ERPS will create this control vlan and its member ports automatically. The member port should have the Left and Right ports only.

In ERPS, the control packets and data packets are separated in different vlans.

The control packets are transmitted in a vlan which is called the Control VLAN.

Instance:

For ERPS version 2, the instance is a profile specifies a control vlan and a data vlan or multiple data vlans for the ERPS. In ERPS, it can separate the control packets and data packets in different vlans. The control packets is in the Control VLAN and the data packets can be in one or multiple data vlan. And then user can assign an instance to an ERPS ring easily.

In ERPS version 1, if a port is blocked by ERPS, all packets are blocked.

In ERPS version 2, if a port is blocked by a ring of ERPS, only the packets belong to the vlans in the instance are blocked.

Notice:

Control VLAN and Instance:

In CLI or Web configurations, there are the Control VLAN and the Instance settings.

If the Control VLAN is configured for a ring and you want to configure an instance for the ring. The control vlan of the instance must be same as the Control VLAN; otherwise, you will get an error. If you still want to use this instance, you can change the Control VLAN to same as the control vlan of the instance first. And then configures the instance.

Configure ERPS Settings

Network > ERPS > Settings

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

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

3. In the **Global State** drop-down, click on **Enable** to enable this feature.

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

- **Ring ID –** Configures the ring ID. The Valid value is from 1 to 255.
- **State –** Enables/ disables the ring state.
- **Ring Name –** Configures the ring name.(Up to 32 characters)
- **Revertive –** Enables / disables the revertive mode.
- **Instance –** Configures the instance for the ring. The Valid value is from 0 to 30. 0-Disable means the ERPS is running in version 1. The control VLAN of the instance should be same as below Control VLAN.
- **Control VLAN –** Configures the Control VLAN which is the ERPS control packets domain for the ring.
- **Version –** Configures the version for the ring.
- **Hold-off Timer –** Configures the Hold-off time for the ring. The Valid value is from 0 to 10000 (ms).
- **WTR Timer –** Configures the WTR time for the ring. The Valid value is from 5 to 12 (min).
- **MEL –** Configures the Control MEL for the ring. The Valid value is from 0 to 7. The default is 7.
- **Guard Timer –** Configures the Guard time for the ring. The Valid value is from 10 to 2000 (ms).
- **Left Port –** Configures the left port and its type for the ring. The valid port type is one of Owner, Neighbor or Normal.
- **Right Port –** Configures the right port and its type for the ring. The valid port type is one of Owner, Neighbor or Normal.

ERPS Ring Settings	
Ring ID	(1~255)
State	Disable
Ring Name	
Revertive	Enable
Instance	0 (0:Default, 0~30)
Ring Type	Major-ring
Control VLAN	(1~4094)
Version	v2
Holdoff Timer (ms)	0 (0~10000)
WTR Timer (sec)	300 (5~720)
MEL	7 (0~7)
Guard Timer (ms)	500 (10~2000)
Left Port	None Normal
Right Port	None Normal

5. At the bottom of the left-hand panel, click **Save**.

ERPS Ring Instance

Network > ERPS > Ring Instance

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

2. Click on **Network**, click on **ERPS**, and click on **Ring Instance**.

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

- **Instance –** Configures the instance ID. The valid value is from 1 to 31.
- **Control VLAN –** Configures the control vlan for the instance. The valid value is from 1 to 4094.
- **Data VLAN –** Configures the data vlan for the instance. The valid value is from 1 to 4094. It can be one or multiple vlans.

ERPS Instance Settings	
Instance	(1~30)
Control VLAN	(1~4094)
Data VLAN	(Multiple VLAN List, e.g. 1,2,5,10)

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

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.

CoS

Set CoS priority settings

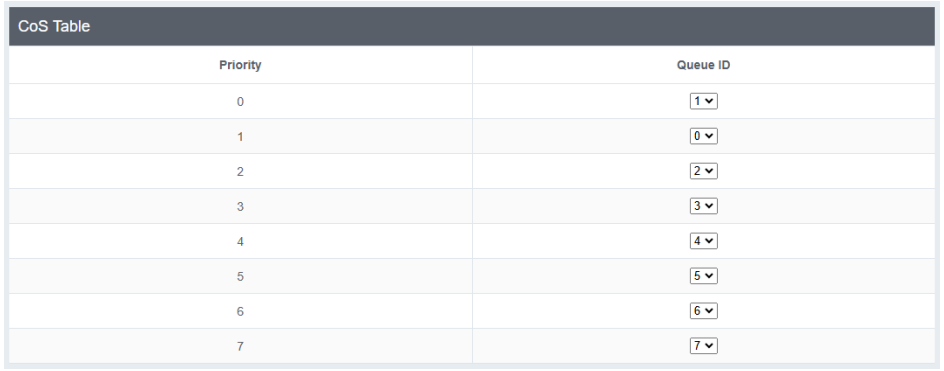
QoS > CoS

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

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

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

3. In **QoS Status**, select **Enabled** and then click **Apply**.
   - For each **Priority** who's Queue ID you want to change, select the appropriate Queue ID in the drop-down that applies to your configuration.
4. Review the settings. Click **Apply** to save the settings.



5. At the bottom of the left-hand panel, click **Save**.

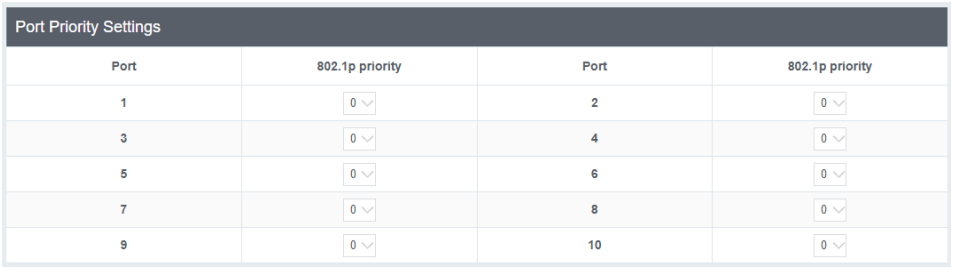
Port Priority

Set Port Priority

QoS > Port Priority

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

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



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

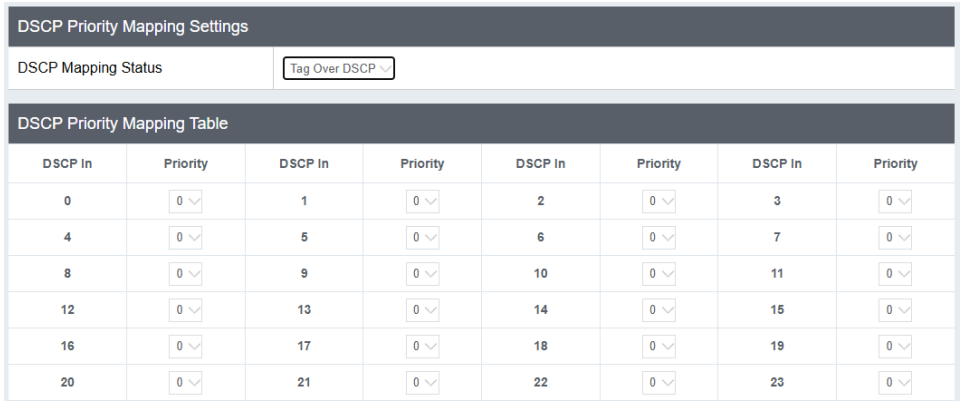
DSCP

Set DSCP (Differentiated Services Code Point) Class Mapping settings

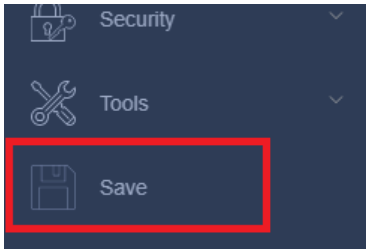
QoS > DSCP

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

1. Log into your switch management page (see "Access your switch management page on page 5").
2. Click on **QoS** and click on **DSCP**.
3. For each DSCP In value that is relevant to your configuration, select a Queue ID in the **Priority** column. Select a mode in the **DSCP Mapping** drop-down list. Click **Apply** to save the settings.
   - **Tag Over DSCP –** 802.1p tags take priority over DSCP.
   - **DSCP Over Tag –** DSCP takes priority over 802.1p tags.



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



Scheduling Algorithm

Set the Scheduling Algorithm

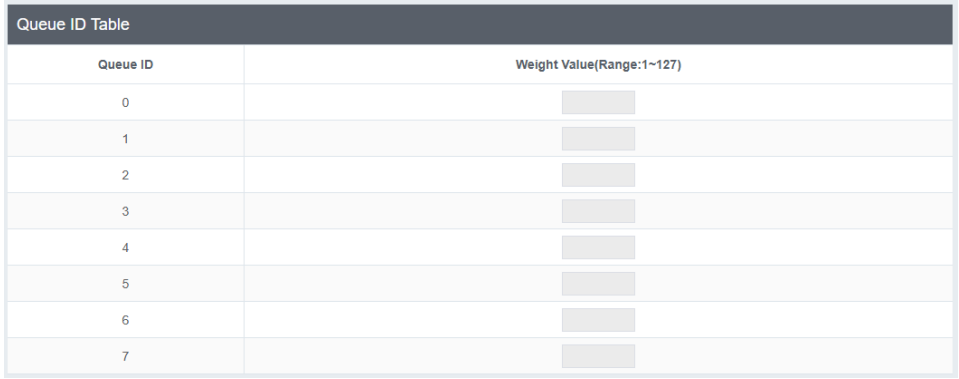
QoS > Scheduling Algorithm

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

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

3. Review the settings. Click **Apply** to save the settings.
   - **High First (SPQ)** - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues. Also known as Strict Priority.
   - **Weighted Round Robin (WRR)** - 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.
   - **Weighted Fair Queuing (WFQ)** - a.

For WRR and WFQ modes, the weight of each queue can be specified in the table below:



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

CLI Commands

Node	Command	Description
enable	show queue cos-map	Displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	Displays the current QoS scheduling mode.
configure	queue cos-map PRIORITY QUEUE_ID	Configures the 802.1p priority map.
configure	no queue cos-map	Resets the 802.1p priority map to default.
configure	qos mode high-first	Configures the QoS scheduling mode to high_first (Strict Priority).
configure	qos mode wfq-queue	Configures the QoS scheduling mode to Weighted Fair Queuing.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	Configures the QoS scheduling mode to Weighted Round Robin with the corresponding weights for each queue.
interface	default-priority	Specifies the default priority value for untagged packets received by the port. Default: 0.
interface	no default-priority	Resets the default priority for the specific port to default (0).
enable	show diffserv	Displays the DSCP configuration.
configure	diffserv (disable|enable)	Disables/enables DSCP.
configure	diffserv dscp VALUE priority VALUE	Sets the DSCP-to-IEEE 802.1q mapping for the specified priority queue.

PoE (Power over Ethernet)

(PoE models only)

Power over Ethernet

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

Power Sourcing Equipment (PSE)

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

Powered Device (PD)

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

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

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

Power Budget

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

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

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

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

Configure PoE settings

PoE > Power over Ethernet

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

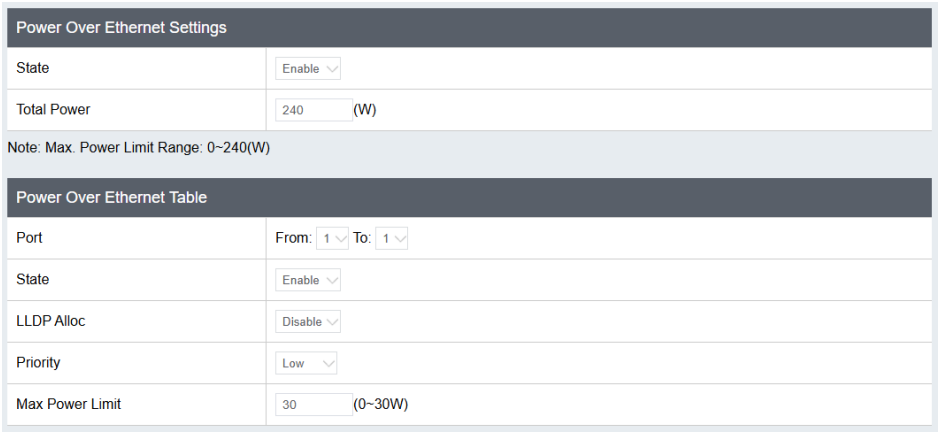
2. Click on **PoE** and click on **Power over Ethernet.**

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

- **State – Enable** or **Disable** PoE globally for all ports.
- **Total Power** – Specify the total power budget for the entire switch in watts.

In Power Over Ethernet Table:

- **Port –** Specifies the range of ports to apply the following settings to.
- **State** - To activate or deactivate PoE on a specific port, select **Enable** or **Disable**. By default the PoE feature is enabled on all switch ports.
- **LLDP Alloc** – Allow the use of LLDP to advertise and negotiate PoE capabilities.
- **Priority** - Indicates the port priority: Low, High, or Critical.
- **Max Power Limit** – Define the maximum power consumption for the specified port(s).



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

CLI Commands

Node	Command	Description
enable	show poe	Displays the PoE configuration and status.
enable	show poe schedule port PORT_ID	Displays the PoE port schedule configuration.
configure	poe (disable | enable)	Disables/enables the PoE function. When disabled, all ports will not supply power.
configure	poe total-power	Configures the PoE budget, the total amount of power that the switch can support.
interface	poe (disable|enable)	Enables/disables PoE on the specified port.
interface	poe priority (critical|high|low)	Configures the PoE priority for the specified port. • critical: The highest priority. • high: The middle priority. • low: The lowest priority.

Time Range

Configure PoE Time Range

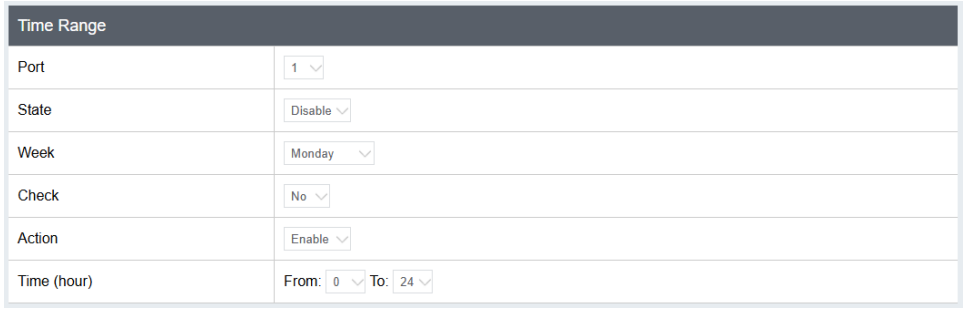
PoE > Time Range

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

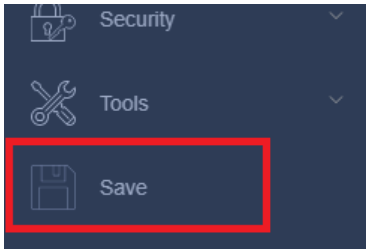
2. Click on **PoE** and click on **Time Range.**

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

- **Port –** Specifies the range of ports to apply the following settings to.
- **State – Enable** or **Disable** PoE globally for all ports.
- **Week –** Set the day that the PoE time range will be applied.
- **Check –** Set whether this feature is active for the specified port(s).
- **Action –**Specify the action to take during the specified time range.
- **Time (hour) –** Set the start and end time of the PoE time range.



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



PD Alive Check

Configure PD Alive Check

PoE > PD Alive

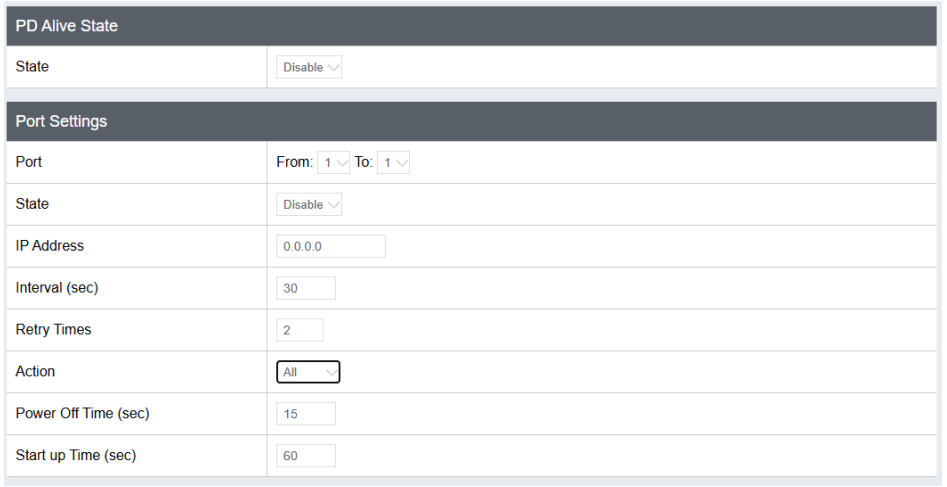
PD Alive Check is used to check the connection between the switch and the device connected to it. The switch sends a ping, and if the device does not respond, the switch will try to revive the device by doing a power cycle of the connected device.

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

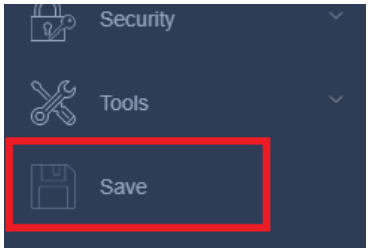
2. Click on **PoE** and click on **PD Alive.**

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

- **State:** Select **Enabled** to enable PD Alive check and **Disabled** to disable it
- **Port:** Specifies the range of ports to apply the following settings to.
- **State (Port Settings):** Select **Enabled** to enable PD Alive Check for the selected port and **Disabled** to disable it
- **IP Address:** Enter the IP address of the device that is connected to the port
- **Interval:** Enter the desired time for how often the switch will send a ping to the connected device
- **Retry Times:** Enter the amount of times the switch will try to send a ping before power cycling
- **Action:** Select **Reboot** to power cycle the device, **Alarm** to send a notification, or **All** to reset and notify.
- **Power Off Time:** Enter the desired time for the switch to turn off the power before sending power again.
- **Start Up Time:** Enter the time it takes for your PD device to boot up. If the entered time is too short, the switch will keep powering on and off the device.



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



Power Delay

Configure Power Delay

PoE > Power Delay

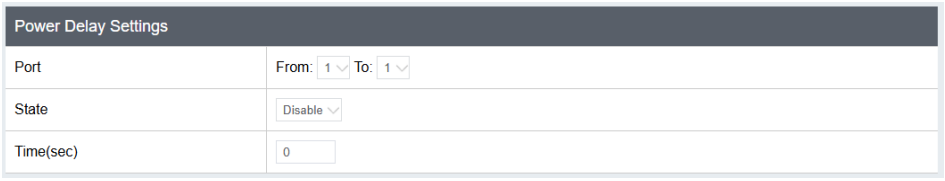
Power Delay is used to delay supplying PoE power to certain ports after switch startup.

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

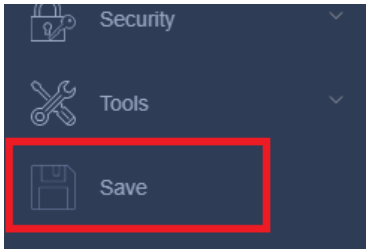
2. Click on **PoE** and click on **PD Alive.**

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

- **Port:** Specifies the range of ports to apply the following settings to.
- **State:** Select **Enabled** to enable Power Delay for the selected port and **Disabled** to disable it
- **Time:** Enter the desired time that the switch will wait after a reboot before supplying PoE to the port



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



Security

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

Port Security Global Settings

Configure Port Access Control

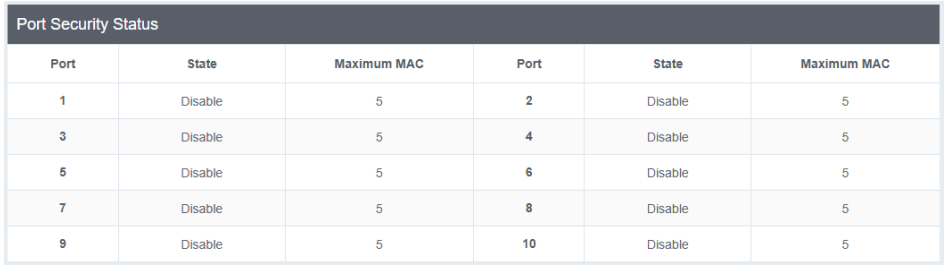
Security > Port Security > Port Settings

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

2. Click on **Security,** click on **Port Security** and click on **Port Settings**.

3. Review the settings for each port. Click **Apply** to save the settings.
   - **Port Security: Enable** or **Disable** Port Security globally for all ports.
   - **Port:** Select the port(s) you wish to set
   - **State:** Select the **Enabled** to enable Security Port Settings or **Disabled** to disable it
   - **Maximum MAC:** Input the number of MAC addresses the switch can store for this port.

4. You may review the settings that was made in the table below



5. At the bottom of the left-hand panel, click **Save**.

Port Security Address Settings

Configure Port Security Address Settings

Security > Port Security > Port Address Settings

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

2. Click on **Security,** click on **Port Security** and click on **Port Address Settings**.

3. Input the desired Port Security System Settings and click **Apply** to save the settings.
   - **MAC Address:** Enter the MAC Address
   - **VID:** Enter the VID
   - **Port:** Select the desired port

DHCP Snooping

Settings

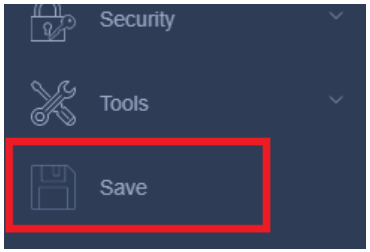
DHCP Snooping > Settings

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

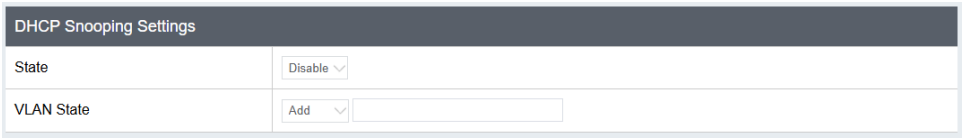
- A trusted port is connected to one of the following:
  - Directly to the legitimate trusted DHCP Server.
  - A network device relaying DHCP messages to and from a trusted server.
  - Another trusted source such as a switch with DHCP Snooping enabled.
  - Untrusted ports are connected to DHCP clients 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.

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

2. Click on **Security**, click on **DHCP Snooping,** and click on **Settings**.



3. Review the settings. Click **Apply** to save the settings.
   - **State** - Select one of the following radio button choices:
     - **Enabled** - This parameter activates the DHCP Snooping feature.
     - **Disabled** - This parameter de-activates the DHCP Snooping
   - **VLAN State -** Enter the VLAN(s) to add to or remove from DHCP Snooping



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

Interfaces

Security > DHCP Snooping > Interfaces

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

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

2. Click on **Security**, click on **DHCP Snooping,** and click on **Interfaces**.

3. Review the settings.
   - **Port:** Specifies the range of port(s) to apply the following settings to.
   - **Trust:** Set this to **Yes** to add them to the trusted ports list.
   - **Maximum Host Count:** Set the maximum number of hosts allowed per port.

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

Binding

Security > DHCP Snooping > Binding

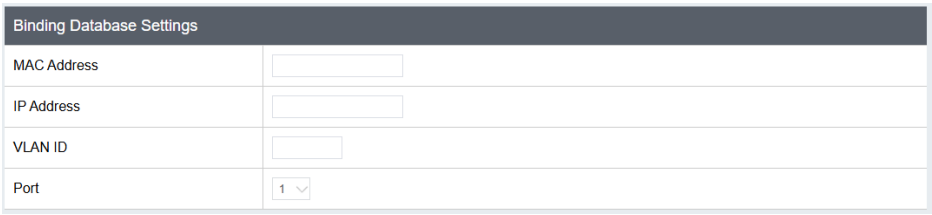
The Binding Database displays learned and statically assigned MAC

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.

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

2. Click on **Security**, click on **DHCP Snooping**, and click on **Binding**.

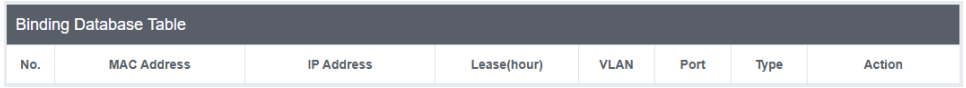
3. Review the settings. Click **Add** to add the database entry to the table.
   - **MAC Address** - Enter the host's MAC Address.
   - **IP Address** - Enter the static IP Address assigned to the host.
   - **VLAN ID** - Enter the host's VLAN ID.
   - **Port** - Enter the port number where the host is connected.



In the list, you can click **Delete** or delete the entry**.**

- **MAC Address:** This parameter shows the host's MAC Address.
- **IP Address:** This parameter is the IP Address assigned by the DHCP server to the DHCP client.
- **Lease:** This parameter is the time that IP address assignment by the DHCP server is valid.
- **VLAN:** This parameter shows the host's VLAN ID of which the DHCP client is a member.

- **Port:** This parameter is the port number where the DHCP client is connected.
- **Type:** This parameter indicates the following:
- **Static-** The host IP Address is statically assigned.



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

DHCP Options

Security > DHCP Snooping > Interfaces

You can set the circuit information that sent when the switch forwards a DHCP request as a DHCP relay.

When you enable DHCP Options on the switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote-ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit-ID suboption).
- If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server **echoes** the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch **removes** the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

Option Frame Format:

Code	Len	Agent Information Field					
82	N	i1	i2	i3	i4	…	iN

The Agent Information field consists of a sequence of SubOpt/Length/Value tuples for each sub-option, encoded in the following manner:

Sub-Option	Len	Sub-Option Value					
1	N	s1	s2	s3	s4	…	sN

DHCP Agent Sub-option	Sub-Option Description Code
1	Agent Circuit ID Sub-option
2	Agent Remote ID Sub-option

Circuit ID Sub-option Format:

Sub-Option Type	Length	Information
0x01		Circuit Form

Remote ID Suboption Frame Format:

Sub-Option Type	Length	Type	Length	Mac Address
0x02	8	0	6	6

Circuit Form:

The circuit form is a flexible architecture. It allows user to combine any information or the system configurations into the circuit sub-option.

The Circuit Form is a string format. And its maximum length is 100 characters.

The keyword, %SPACE, will be replaced with a space character.

The other keywords get system configurations from the system and then replace the keyword and its leading code in the Circuit form. Eventually, the content of the circuit form is part of the payload on the DHCP option 82 packet.

Rules:

- The keyword must have a leading code '%'. For example: *%HOSTNAME*.
- If there are any characters following the keywords, you must add '+' between the keyword and character. For example: *%HOSTNAME+/*.
- If there are any characters before the keyword, you must add '+' between the character and the keyword. For example: *Test+%HOSTNAME*.

Keyword:

HOSTNAME -Add the system name into the Circuit sub-option..

SPACE -Add a space character.

SVLAN -Add the service provider VLAN ID into the Circuit sub-option.

If the service provider VLAN is not defined, the system will return PVLAN.

CVLAN -Add the customer VLAN ID into the Circuit sub-option.

If the CVLAN is not defined, the system returns 0.

PORT -Add the transmit port ID into the Circuit sub-option.

FRAME -Add the frame ID into the Circuit sub-option.

The frame ID is configured with the CLI command, "dhcp-options option82 circuit_frame VALUE". Or GUI Circuit Frame.

SHELF -Add the shelf ID into the Circuit sub-option.

The shelf ID is configured with the CLI command, "dhcp-options option82 circuit_shelf VALUE". Or GUI Circuit Shelf.

SLOT -Add the slot ID into the Circuit sub-option.

The slot ID is configured with the CLI command, "dhcp-options option82 circuit_slot VALUE". Or GUI Circuit Slot.

For Example:

HOSTNAME=[YOUR_DEVICE_NAME].

SVLAN=44.

CVLAN=32.

CircuitForm=RD+%SPACE+Department+%SPACE+%HOSTNAME+%SPACE+%PORT+_+%SVLAN+.+%CVLAN

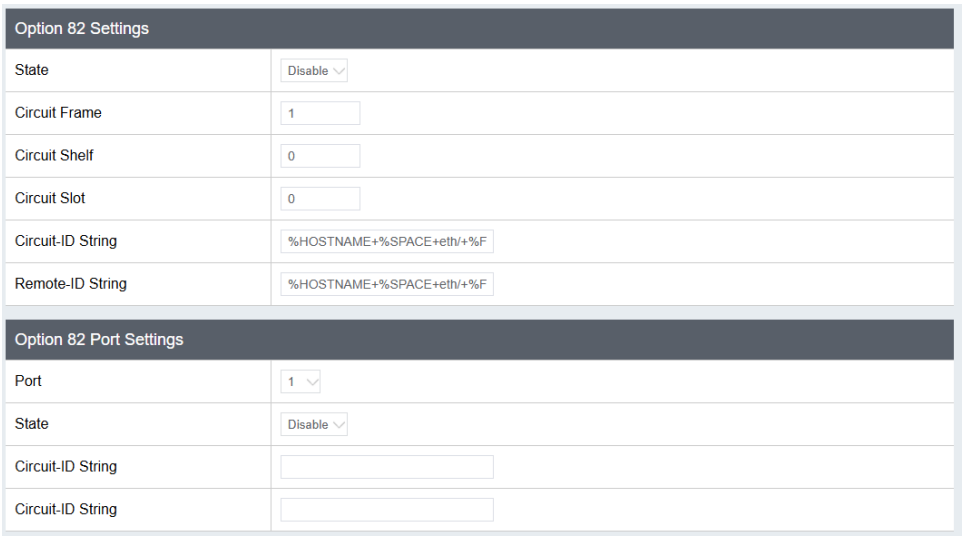
The circuit sub-option result is: RD Department [YOUR_DEVICE_NAME] 1_44.32

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

2. Click on **Security**, click on **DHCP Snooping,** and click on **DHCP Options**.

3. Review the settings.

- **State** – Enable or Disable the DHCP Options feature.
- **Circuit Frame, Circuit Shelf, Circuit Slot** - Enter the IDs for these sub-options.
- **Circuit-ID String** - Enter the desired Circuit-ID String.
- **Remote-ID String** - Enter the desired Remote-ID String.
- **Port** – Select the port to apply DHCP Options to.
- **Circuit-ID String (Port Settings)** - Enter the desired Circuit-ID String for this port.
- **Circuit-ID String (Port Settings, bottom-most)** - Enter the desired Remote-ID String for this port.



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

DHCP Relay

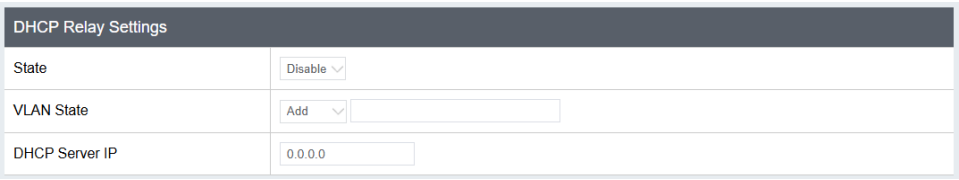
Security > DHCP Relay

This feature allows you to forward all DHCP request packets to a single DHCP server even if the DHCP server is on a different network segment.

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

2. Click on **Security** and click on **DHCP Relay**.

3. Review the settings. Click **Apply** to save the settings.
   - **State** – Enable or Disable the DHCP Relay feature.
   - **VLAN State** - Enter the VLAN(s) to enable the DHCP Relay on.
   - **DHCP Server IP** - Enter the IP address of the DHCP server.



ARP Inspection

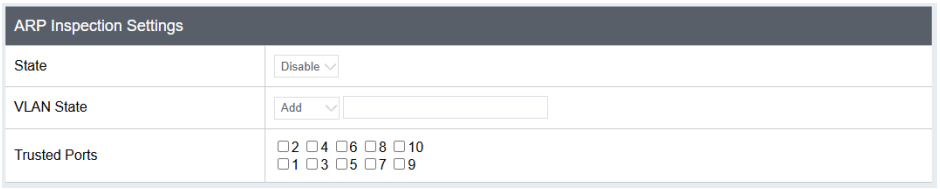
Settings

Security > ARP Inspection > Port Settings

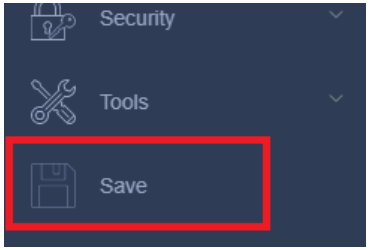
1. Log into your switch management page (see "Access your switch management page on page 5").

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

3. Enable the feature by selecting **Enable** in **State**, then add the desired VLAN(s) and select the ports to mark as trusted. Click **Apply** to save the settings.



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



ARP Filter Table

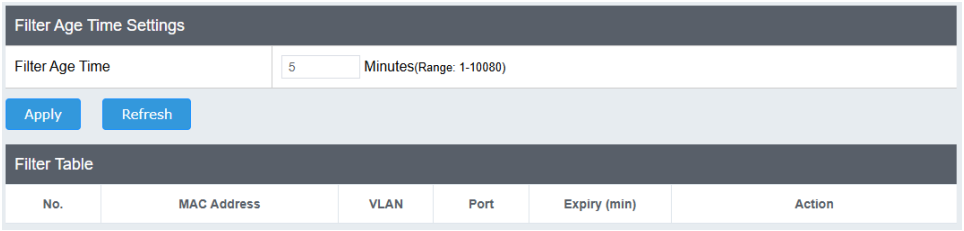
Security > ARP Inspection > Filter Table

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

2. Click on **Security**, click on **Dynamic ARP Inspection,** and click on **ARP Inspection Validation**.

3. Review the settings and the filter table. Click **Apply** to save the settings.

- **Filter Age Time** – Specify the expiration time of filter entries



You can click **Delete** to remove the Filter entry immediately.

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

ACL

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.

Add ACL Entries

Security > ACL > Access Profile List

The ACL Configuration Wizard page allows for simple configuration of ACL profiles and rules.

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

2. Click on **Security,** click on **ACL**, and click on **Access Profile List**.

3. Click **Add Profile**, and review the settings. Click **Apply** to save the settings.

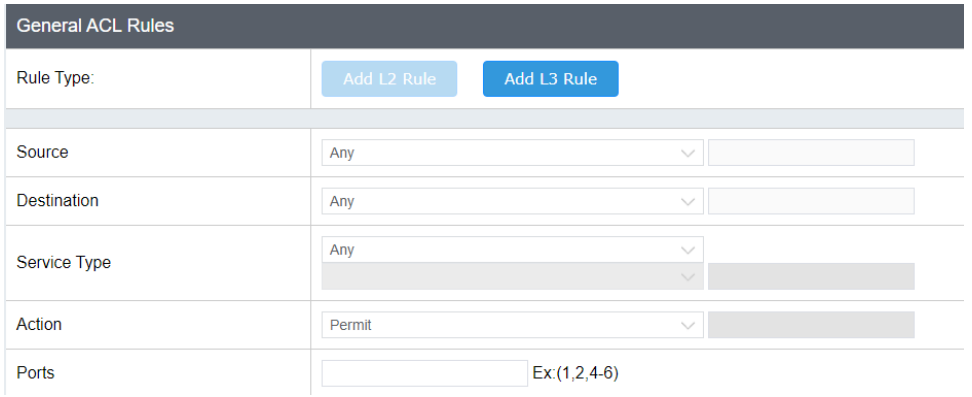
ACL Configuration Wizard

Create an ACL rule by selecting the appropriate fields.

- **Source-** Defines the access packet origin.
  - **Any-** Indicates ACL action will be taken on packets from any source.
  - **MAC Address –** Indicates ACL action will be taken on packets from the specified MAC address.
  - **IPv4 Address-** Indicates ACL action will be taken on packets from the specified IPv4 source address.
  - **IPv6 Address-** Indicates ACL action will be taken on packets from the specified IPv6 address.
- **Destination-** Defines the access packet destination.
  - **Any-** Indicates ACL action will be taken on packets to any destination.
  - **MAC Address –** Indicates ACL action will be taken on packets to the specified MAC address.

- **IPv4 Address-** Indicates ACL action will be taken on packets to the specified IPv4 source address.
- **IPv6 Address-** Indicates ACL action will be taken on packets to the specified IPv6 address.

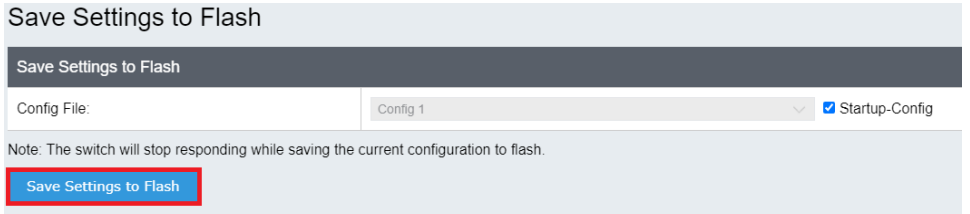
- **Service Type-** Defines the type of service.
  - **Any-** Indicates the ACL action will be taken on packets of all types of service.
  - **EtherType-** Specifies EtherType packet filtering.
  - **ICMP All-** Specifies ICMP packet filtering.
  - **IGMP-** Specifies IGMP packet filtering.
  - **TCP All-** Specifies TCP packet filtering.
  - **TCP Source Port-** Matches packet to corresponding TCP Source Port.
  - **TCP Destination Port-** Matches packet to corresponding TCP Destination Port.
  - **UDP All-** Specifies UDP packet filtering.
  - **UDP Source Port-** Matches packet to the corresponding UDP Source Port.
  - **UDP Destination Port-** Matches packet to the corresponding UDP Destination Port.
- **Action-** Defines the ACL action linked to the rule criteria.
  - **Permit-** This selection allows ingress packets that conform to the specified ACL criteria.
  - **Deny-** This selection drops ingress packets that conform to the specified ACL criteria.
  - **Rate Limiting-** Activates rate limiting if all ACL criteria are met.
  - **Replace 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.
- **Ports-** Defines the ports to be configured.



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

5. Select the Config you would like to save the settings to, then click **Save Settings to Flash,.**

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



Access Profile List

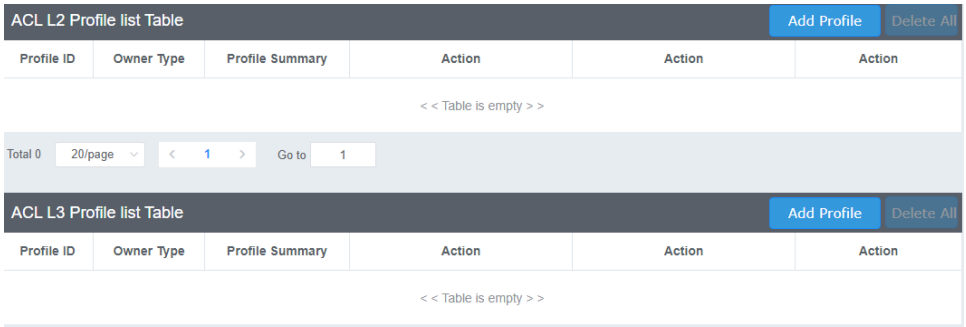
Security > ACL > Access Profile List

The Access Profile List allows users to view the active ACL profiles.

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

2. Click on **Security,** click **ACL,** and click on **Access Profile List**.

In the list, you can click **Show Details** to view the ACL Profile details, click **Edit/New Rules** to edit or create rule details, or delete the entry**.** You can also click **Delete All** to delete all of the entries in the table.



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

5. Select the Config you would like to save the settings to, then click **Save Settings to Flash.**

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

ACL Finder

Security > ACL > ACL Finder

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

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

2. Click on **Security**, click on **ACL,** and click on **ACL Finder**.

3. The ACL Finder contains the following fields.

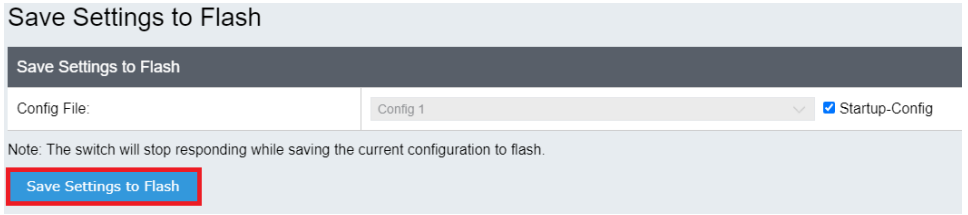
- **Profile Type-** Select the Profile type for the drop-down search bar
- **Profile ID-** Defines the Profile ID for the drop-down search bar
- **Ports-** Defines the port number search bar.
- **Profile ID-** Indicates the Profile ID.
- **Access ID-** Indicates the Access ID.
- **Profile Type-** Indicates the profile type.
- **Summary-** Displays the ACL rule summary.
- **Status-** Displays the ACL rule status.
- **Action-** Includes the **Delete** button for removing ACL rules.

4.View the active poicies by clicking on the **Access ID** number.

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

5. Select the Config you would like to save the settings to, then click **Save Settings to Flash.**

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



Tools

Firmware Upgrade

Upgrade your switch's firmware

Tools > Firmware Upgrade

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

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

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

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

Please note the following:

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

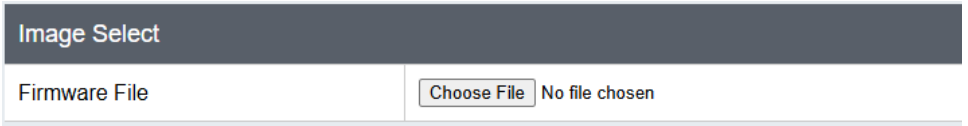
Firmware Upgrade via HTTP Settings

Tools > Firmware Upgrade

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

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

3. Depending on your web browser, click **Browse** or **Choose File**.



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

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

CLI Commands

Node	Command	Description
configure	archive download-fw <URL PATH>	Initiates a firmware update with a firmware file from a remote server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Config Backup Restore

Config Backup/Restore

Tools > Configuration > Backup/Restore

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

Backup/Restore via HTTP Settings

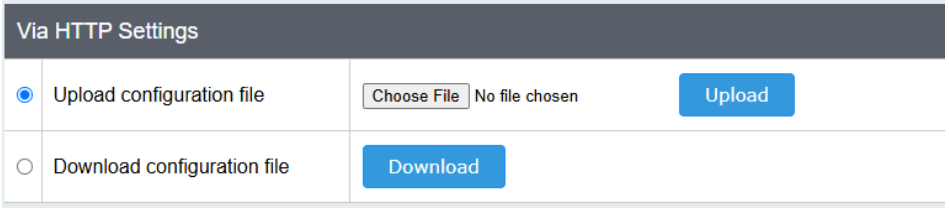
To backup your switch configuration:

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

2. Click on **Tools**, click on **Configuration** and click on **Backup/Restore**, under **via HTTP**.

3. Click **Download** to save the configuration file (config.bin) to your local hard drive.

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



To restore your switch configuration:

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

2. Click on **Tools**, click on **Configuration** and click on **Backup/Restore**, under **via HTTP**.

3. Next to **Upload configuration file,** depending on your web browser, click on **Browse** or **Choose File**.

4. A separate file navigation window should open.

5. Select the switch configuration file to restore and click **Upload**. (Default Filename: *config.bin*). If prompted, click **Yes** or **OK**.

6. Wait for the switch to restore settings.

CLI Commands

Node	Command	Description
enable	show config-change-status	Displays any changes made to the default configuration.
configure	write memory	Writes the current running configuration to the configuration file.
configure	archive download-config <URL PATH>	Downloads a new copy of the configuration file from the specified location and replaces the currently running configuration. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	Uploads a copy of the current configuration file to the specified location.

Reboot

Reboot/Reset to factory defaults

Tools > Reboot

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

To reboot your switch:

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

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

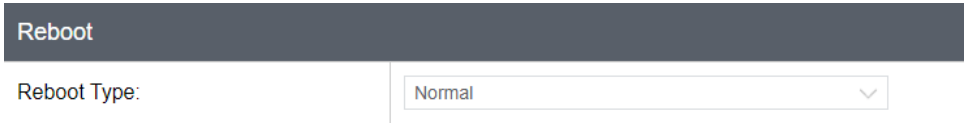
There are two methods that can be used to reboot your switch.

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

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

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

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



To reset your switch to factory defaults:

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

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

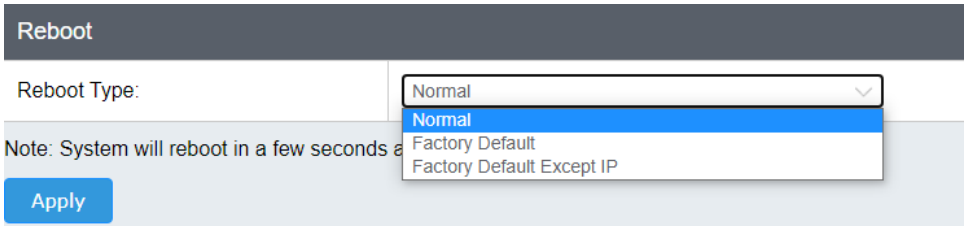
- **Hardware Method:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button more than 6 seconds and release. Located on the front panel of your switch, see "Product Hardware Features" on page 2. Use this method if you are encountering difficulties with accessing your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

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

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

3. Click the **Reboot Type** drop-down list and select from one of the following options

- **Factory Default:** Resets all switch configuration settings to factory defaults including the IP address.
- **Factory Default Except Network:** Resets all switch configuration settings to factory defaults and leaves the current IP address configuration.



After reboot, use these settings to access the setup wizard:

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

CLI Commands

Node	Command	Description
configure	reboot	Reboots the system.
configure	reload default-config	Initiates a factory reset. **Note:** The system will reboot automatically to take effect the configuration. Due to firmware limitations, once you reset the switch to factory defaults, you must log in to the web interface for the first time to complete the setup wizard. The CLI will be inoperative during this time.

Ping Watchdog

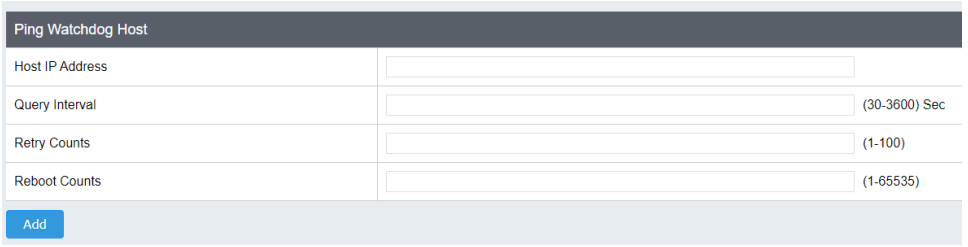
Gateway Monitor

Tools > Ping Watchdog

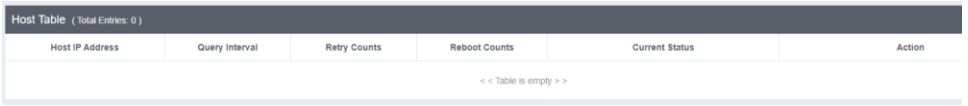
This feature allows the switch to reboot automatically when it loses connection to a specified host. This is done by continually pinging the host until a certain number of pings has failed.

1. Log into your switch management page (see "Access your switch management page on page 5").
2. Click on **Tools** and click on **Ping Watchdog.**
3. Review the settings
   - **Host IP Address** - Specifies the IP address of the host
   - **Query Interval** - Specifies the length of time, in seconds, the switch will ping the host
   - **Retry Counts** - Specifies the number of ping failures before the switch is rebooted
   - **Reboot Counts** - Specifies the maximum number of reboots allowed

Click **Add** to add the entry to the table. Select **Enable** in **Global Status** to enable the feature.



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

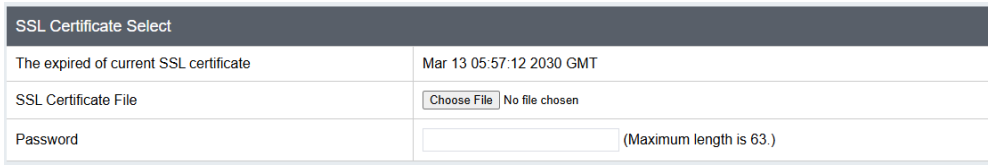


Upgrade SSL Certificate

Tools > Upgrade SSL Certificate

You can update the SSL certificate for the switch's web management page.

1. Log into your switch management page (see "Access your switch management page on page 5").
2. Click on **Tools** and click on **Upgrade SSL Certificate.**
3. Depending on your web browser, click **Browse** or **Choose File**.



4. Navigate to the folder on your computer where the SSL certificate is located.

5. Enter the **Password** for the certificate.

6. Click **Upgrade** to update the certificate. You may need to log in to the switch again after this step.

Technical Specifications (Non-PoE Models)

	TI-G642i (v1.xR)	TI-G102i (v1.xR)	TI-G160WS / TI-G160i (v1.xR)	TI-RG262i (v1.0R)
Device Interface	LED indicators and reset button			
	4 x Gigabit ports	8 x Gigabit ports	16 x Gigabit ports	24 x Gigabit ports
	2 x Gigabit SFP slots			2 x SFP slots
	DIP switches (DIN Rail only) and LED Mode select button (PoE only)			
Data Transfer Rate	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)			
	Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)			
	Gigabit Ethernet: 2000 Mbps (full duplex)			
	1G SFP: 2000 Mbps (full duplex)			
Switch fabric	12 Gbps	20 Gbps	32 Gbps	52 Gbps
RAM buffer	128 MB			512 KB
MAC Address Table	8K entries			
Jumbo Frames	10 Kbytes			
Forwarding	18.9 Mpps (64-byte packet size)	14.88 Mpps (64-byte packet size)	23.8 Mpps (64-byte packet size)	38.7 Mpps (64-byte packet size)
HOL Blocking Prevention	HOL Blocking Prevention supported on all models			
Power Input	External power supply (20 - 60V DC)	External power supply (12 - 60V DC)		External power supply (48 - 57V DC)
Power Consumption	12 W (max.)	13 W (max.)	12 W (max.)	20 W (max.)
PoE Type	N/A			
PoE Budget	N/A			

	TI-G642i (v1.xR)	TI-G102i (v1.xR)	TI-G160WS / TI-G160i (v1.xR)	TI-RG262i (v1.0R)
Fan Quantity	Fanless			
Noise Level	N/A (fanless)			
Operating Temperature	-40° – 70° C (-40° – 158° F)			
Operating Humidity	Max. 95% non-condensing			
Dimensions	160 x 120 x 50mm (6.3 x 4.72 x 1.97 in.)			440 x 284 x 44mm (17.32 x 11.18 x 1.7 in.)
	DIN-Rail mount			Rack mountable 1U height
Weight	720 g (1.59 lbs.)	884g (1.95 lbs.)		3.46kg (7.62 lbs.)
Certifications	CE			
	FCC			
Warranty	Lifetime			
Package Contents	In addition to the switch, the package contents include the following:			
	Quick Installation Guide			
	DIN rail mounting bracket			Rack mount kit
MTBF	125,932 hours	113,378 hrs.	177,143 hours	127,076 hours

Technical Specifications (PoE Models)

	TI-PG1284i (v2.xR)	TI-PG541i (v1.xR)	TI-PG102i / TI-PG102i-M (v1.xR)	TI-RP262i (v1.xR)	TI-BG6i (v1.xR)
Device Interface	LED indicators and reset button				
	8 x Gigabit PoE+ ports	4 x Gigabit PoE+ ports	8 x Gigabit PoE+ ports	24 x Gigabit PoE+ ports	4 x Gigabit PoE+ ports
	4 x Gigabit SFP ports	1 x Gigabit port	2 x Gigabit SFP ports	2 x SFP ports	2 x SFP ports
	1 x Console port (RJ-45)	1 x Gigabit SFP port		1 x Console port (RJ-45)	
	1 x USB port				
Data Transfer Rate	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)				
	Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)				
	Gigabit Ethernet: 2000 Mbps (full duplex)				
	1G SFP: 2000 Mbps (full duplex)				
Switch fabric	24 Gbps	12 Gbps	20 Gbps	52 Gbps	12Gbps
RAM buffer	1.5 MB	128MB	512KB	512 KB	1.5MB
MAC Address Table	16K entries	8K	8K	8K	16K
Jumbo Frames	10 KB				
Forwarding	17.9 Mpps (64-byte packet size)	8.93 Mpps (64-byte packet size)	14.88 Mpps (64-byte packet size)	38.7 Mpps (64-byte packet size)	8.9 Mpps (64-byte packet size)
HOL Blocking Prevention	HOL Blocking Prevention supported on all models				
Power Input	External power supply (48 - 57V DC)		External power supply (24 - 57V DC)	External power supply (48 - 57V DC)	External power supply (48 - 57V DC)
Power Consumption	258W (max.)	130 W (max.)	12 W (max.)	705 W (max.)	380W W (max.)
PoE Type	IEEE 802.3at: Up to 30W per port				802.3bt: Up to 95 W per port
PoE Budget	240W	120W	240W	685W	360W

	TI-PG1284i (v2.xR)	TI-PG541i (v1.xR)	TI-PG102i / TI-PG102i-M (v1.xR)	TI-RP262i (v1.xR)	TI-BG6i (v1.xR)
Fan Quantity	Fanless				
Noise Level	N/A (fanless)				
Operating Temperature	-40° – 70° C (-40° – 158° F)				
Operating Humidity	Max. 95% non-condensing				
Dimensions	160 x 120 x 50mm (6.3 x 4.72 x 1.97 in.)	135 x 120 x 31mm (5.31 x 4.72 x 1.22 in.)	160 x 120 x 50mm (6.3 x 4.72 x 1.97 in.)	440 x 310 x 44mm (17.3 x 12.3 x 1.7 in.)	170 x 118 x 50mm (6.69 x 4.65 x 1.97 in.)
	DIN-Rail mount			Rack mountable 1U height	DIN-Rail mount
Weight	946g (2.12 lbs.)	528g (1.17 lbs.)	930g (2.05 lbs.)	3.58kg (7.89 lbs.)	956g (2.1 lbs.)
Certifications	CE				
	FCC				
Warranty	Lifetime				
Package Contents	In addition to the switch, the package contents include the following:				
	Quick Installation Guide				
	DIN rail mounting bracket			Rack mount kit	DIN rail mounting bracket
MTBF	561,724 hours	435,909 hours	562,234 hours	127,076 hours	379,100 hours

Troubleshooting

Q: I typed http://192.168.10.200 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the switch management page?
Answer:
1. Check your hardware settings again. See "Switch Installation" on page 7.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Use the following IP address* or *Static IP* (see the steps below).
4. Make sure your computer is connected to one of the Ethernet switch ports.
5. Since the switch default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

Windows 7/8.1/10

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

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

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

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

Windows Vista

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

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

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

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

Windows XP/2000

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

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

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

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

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

Q: If my switch IP address is different than my network's subnet, what should I do?
Answer:
You should still configure the switch first. After all the settings are applied, go to the switch configuration page, click on Basic, click General Settings and change the IP address of the switch to be within your network's IP subnet. Click Save in the top right to save the IP settings to the NV-RAM.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7/8.1/10

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

MAC OS X

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

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

Graphical Method

MAC OS 10.6/10.5

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

MAC OS 10.4

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

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

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

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

Windows 7/8.1/10

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

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

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

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

Windows Vista

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

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

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

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

Windows XP/2000

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

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

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

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

MAC OS 10.4/10.5/10.6

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

b. Click the **Network** icon.

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

d. Select and view your Ethernet connection.

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

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

f. Restart your computer.

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

How to find your MAC address?

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

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

In MAC OS 10.4,

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

In MAC OS 10.5/10.6,

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

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

Windows 2000/XP/Vista/7/8.1/10

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.

2. In the dialog box, type ***cmd*** to bring up the command prompt.

3. In the command prompt, type ***ping <ip_address>*** with the *<ip_address>* being the IP address you want ping and check for connectivity.

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

C:\Users>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.

2. Double-click on **Terminal** to launch the command prompt.

3. In the command prompt, type ***ping –c <#> <ip_address>*** with the *<#> ping being the number of time you want to ping and* the *<ip_address>* being the IP address you want ping and check for connectivity.

Example: *ping –c 4 192.168.10.100*

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

Radiation Exposure Statement:

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

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

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

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

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

- **EN 55032: 2015 + AC: 2016 (Class A)**
- **EN 55024: 2010 + A1: 2015**
- **EN 61000-4-2: 2009**
- **EN 61000-4-3: 2006 + A1: 2008 + A2: 2010**
- **EN 61000-4-4: 2012**
- **EN 61000-4-5: 2014**
- **EN 61000-4-6: 2014 + AC 2015**
- **EN 61000-4-8: 2010**
- **Regulation (EC) No. 1275/2008, No. 801/2013**

Directives:

EMC Directive 2014/30/EU

RoHS Directive 2011/65/EU

REACH Regulation (EC) No. 1907/2006

CE Mark Warning

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

Limited Warranty

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

Limited Warranty

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

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

Limited Lifetime Warranty

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PWP07172015v3 2018/09/15

TRENDnet®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA