User's Guide

TRENDnet®

6-Port Hardened Industrial Gigabit PoE+ Layer 2 Managed DIN-Rail Switch

TI-PG541i

Contents

Product Overview

TI-PG541i

Package Contents

In addition to your switch, the package includes:

- Quick Installation Guide
- CD-ROM (User's Guide)

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

Please note power adapter is sold separately (model: 48VDC3000)
Please note power supply is sold separately (model: TI-24048).

Features

TRENDnet's 6-Port Hardened Industrial Gigabit PoE+ Layer 2 Managed DIN-Rail Switch, model TI-PG541i, has four Gigabit PoE+ ports, one Gigabit port, one Gigabit SFP slot and a 120W PoE budget. The switch is equipped with an IP30 rated metal enclosure and designed to withstand a high degree of vibration, shock, protection against ESD/EMI/surge, and operate within a wide temperature range (- 40 – 70 °C (- 40 - 158 °F)) for harsh environments. L2 management include features such as PoE port control, VLAN, multicast, and QoS which allow for network integration flexibility.

Industrial Hardened Design

Equipped with a rugged IP30 rated enclosure and designed to withstand a high degree of vibration, shock, protection against ESD/EMI/surge, and operate with a wide temperature range (- 40 – 70 °C (- 40 - 158 °F)) for harsh environments.

Integration Flexibility

Managed features include PoE control, VLAN, IGMP snooping, QoS, RMON, SNMP trap, and syslog for monitoring and flexible network integration.

Fault Tolerance

Features dual redundant power inputs (Primary and RPS) from external power sources and an output alarm relay to indicate the event of input power failure

Full PoE+ Power Budget

Supplies up to 30 Watts of PoE/PoE+ power per port (ports 1-4 802.3at/802.3af) with a 120 Watt PoE power budget

Network Ports and Capacity

4 x Gigabit PoE+ ports, 1 x Gigabit Port, and 1 x Gigabit SFP slot allow for a 12Gbps switching capacity

Integrated DIN-Rail Mount

IP30 rated metal enclosure with integrated DIN-rail mounting hardware

Full PoE Control Per Port

PoE control features include enabling/disabling PoE and class, power priority, PD alive check, scheduling, and power delay per port using CLI or web management.

L2 Management

Managed features include 802.1Q, MAC-Based VLAN, IGMP v1/2/3 Snooping, per port bandwidth control/802.1p/DSCP/Queue Scheduling (SP/WFQ/WRR), and Storm Control for flexible network integration.

System Monitoring

Monitoring features include SNMPv1/v2c, MIB support, SNMP trap, RMON Groups (1, 2, 3, 9), SMTP alert, syslog, and port mirroring.

Redundant Power

Dual redundant power inputs (primary and RPS) with overload current protection

Alarm Output

Alarm relay output triggered by power failure of primary and/or redundant power (DIP switch)

Jumbo Frame

Sends larger packets, or Jumbo Frames (up to 10K)

Wide Temperature

Hardened switch is rated for an operating temperature range of - 40 to 70 °C (-40 to 158 °F)

Electro Magnetic Compliance

Complies with IEC61000-6-2 EMC generic standard immunity for industrial environments

Shock and Vibration Resistant

Rated for shock (IEC 60068-2-27), freefall (IEC 60068-2-32), and vibration (IEC 60068-2-6)

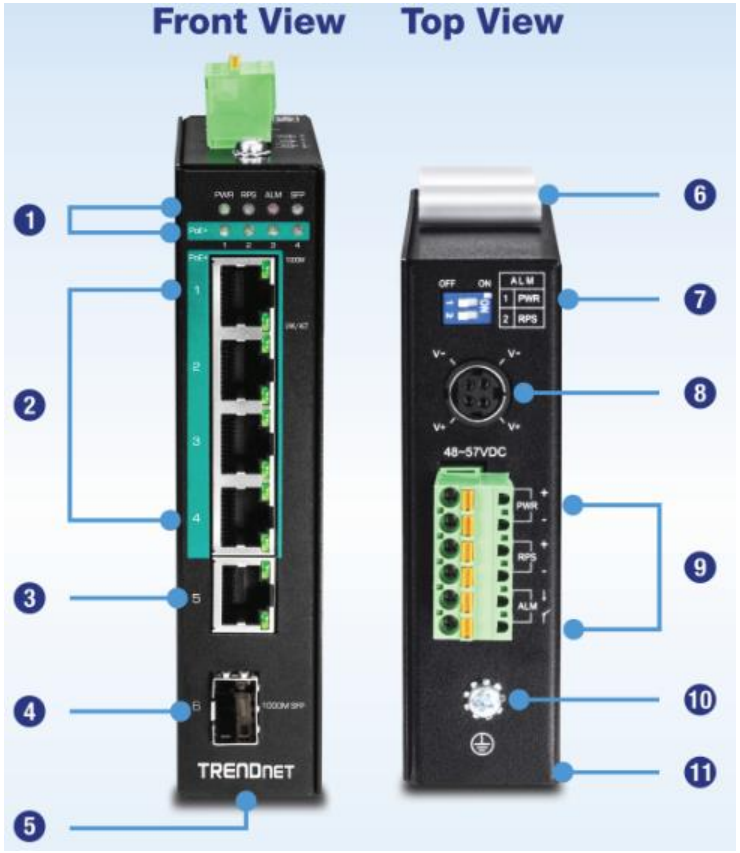
LED Indicators

LED indicators convey power, redundant power, alarm, SFP, PoE, and network port status

Grounding Point

Grounding point protects equipment from external electrical surges

Product Hardware Features



1. LED indicators
2. Gigabit PoE+ ports
3. Gigabit port
4. Gigabit SFP slot
5. Reset button
6. Integrated DIN-Rail mount
7. DIP switches
8. DC Power connector (power adapter sold separately: model 48VDC3000)
9. 6-pin terminal block (power supply sold separately: model TI-S24048)
10. Grounding point
11. Hardened IP30 rated metal switch

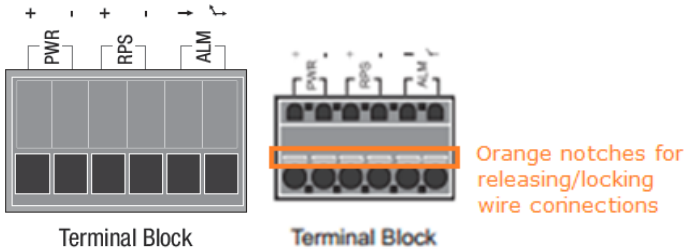
LED Indicators

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.
RPS (Green)	ON	When the RPS LED lights on, the device is using the redundant power input source.
	OFF	Redundant 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)	ON	PoE supplied to Ethernet port.
	OFF	No PoE supplied to Ethernet port.
Ports 1-5 1000M (Green)	ON	Ethernet port is connected.
	BLINKING	Data is transmitting/receiving.
10/100M (Off)	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 Slot 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 slots, it is recommended to leave the rubber plugs installed during operation.*

6-pin Removable Terminal Block

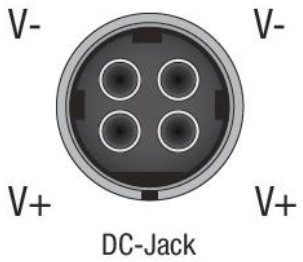


Input/Ouput	Function
PWR Input (+) & (-)	Connects primary power source (ex. external power supply) to power the device. Device will obtain power from this input first priority if available. Please make sure to power supplies are turned off before wiring in. Use a flat-head screw driver to push the orange 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.

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.

DC Jack Input for External Power Adapter

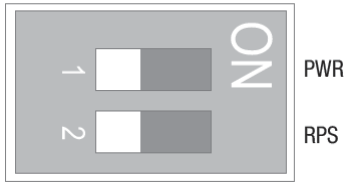


The device includes a DC Jack for an external power adapter and can also be used as an additional redundant power supply (RPS) input.

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)

ALM DIP Switches

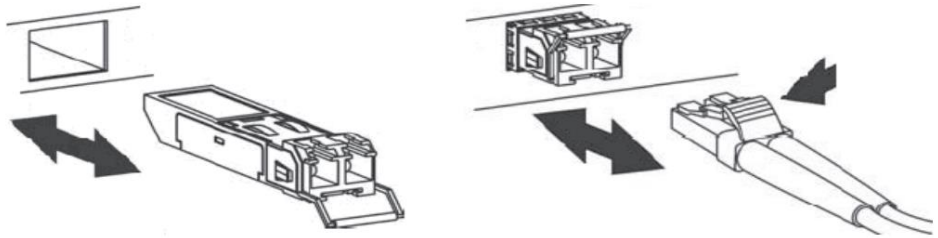


DIP No	Name	State	Status
1	PWR	ON	Primary power input source alarm trigger enabled.
		OFF	Primary power input source alarm trigger disabled.
2	RPS	ON	Redundant power input source alarm trigger enabled.
		OFF	Redundant power input source alarm trigger disabled.

SFP Transceiver/Optical Cable Installation

1. Remove the rubber plug from the SFP slot.

   Note: *For any unused ports or SFP slots, 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.

Switch Installation

DIN-Rail Installation

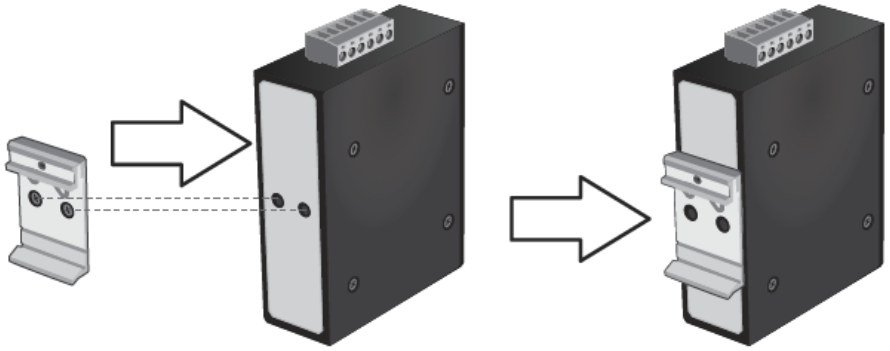
The site where the switch will be installed may greatly affect its performance. When installing, consider the following pointers:

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.

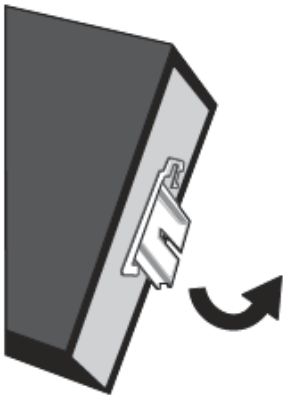
Fasten the DIN-Rail bracket to the rear of the switch using the included fasteners/screws.
Note: *The DIN-Rail bracket may already be installed to your switch when received.*

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



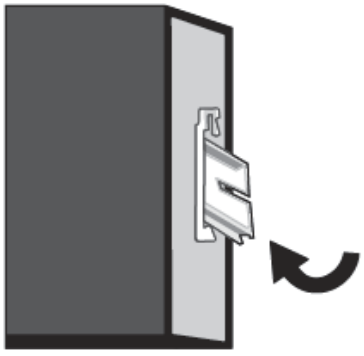
The switch can be installed to a 35mm (W) DIN-Rail located in cabinet, rack, or enclosure.

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.



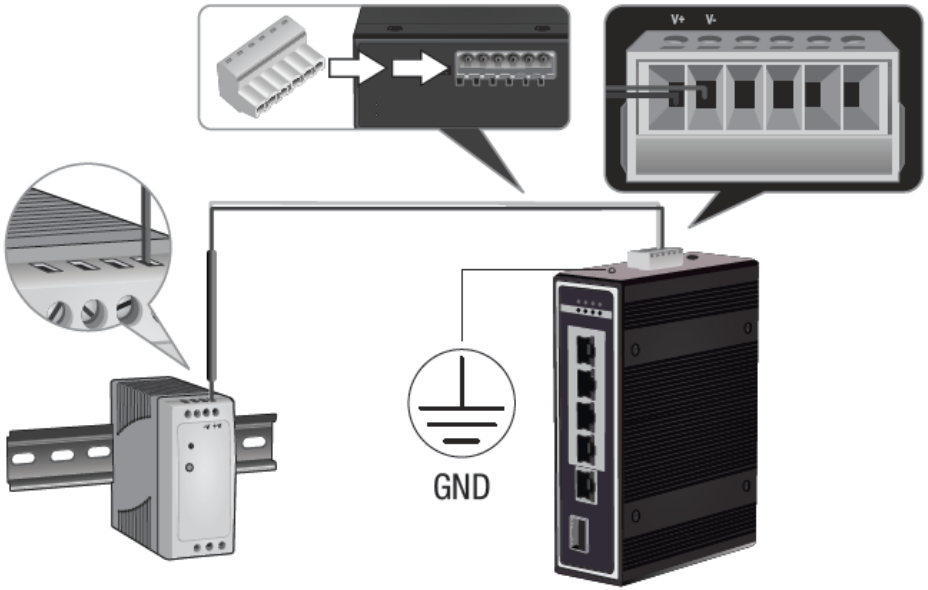
Releasing the unit

Install power supply connections

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

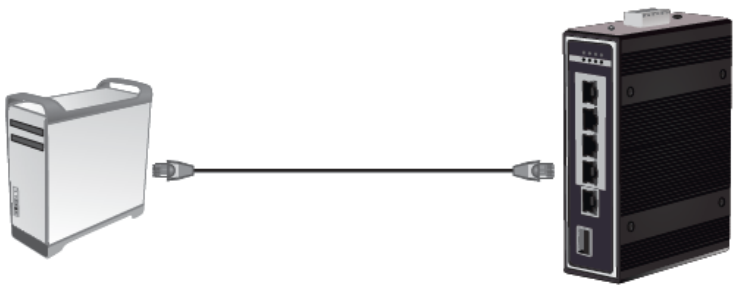
Note: *Polarities V+ and V- should match between power supply and connections to switch terminal block.*

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



Basic IP Configuration

1



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.

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

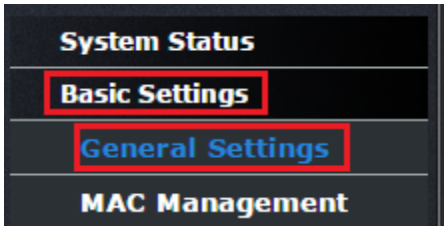
5. Enter the User Name and Password, and then click **Login.** By default:

User Name: **admin**

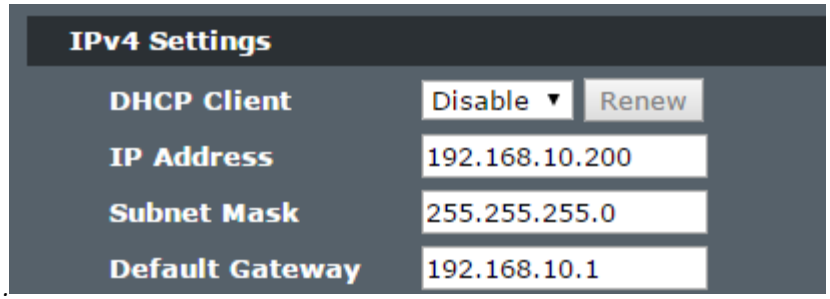
Password: **admin**

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

6. Click **Basic Settings** and then click **General Settings**.



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



8. Click **Save** at the top right.

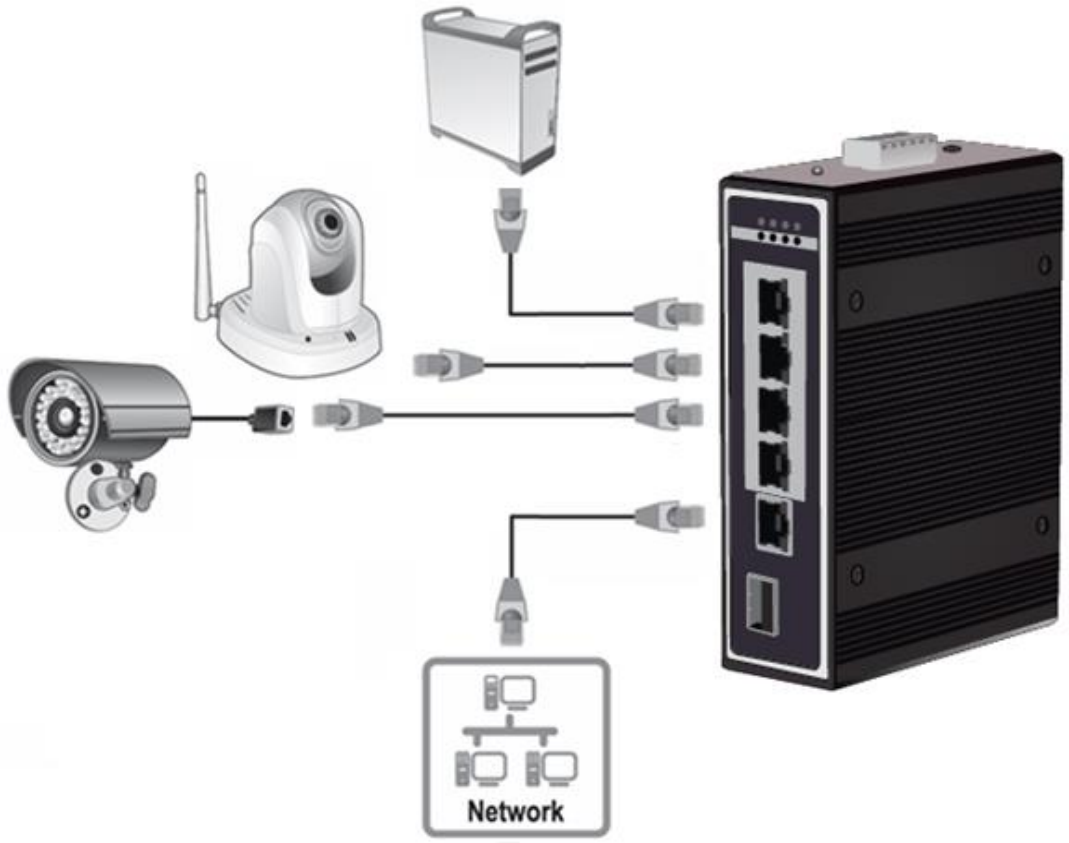
9. When confirmation message appears click **OK.**

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

Connect additional devices to your switch

You can connect additional computers or other network devices to your switch using Ethernet cables to connect them to one of the available Gigabit PoE+ Ports (1-8). Check the status of the LED indicators on the front panel of your switch to ensure the physical cable connection from your computer or device.

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



Accessing switch management interfaces

Access your switch command line interface

Note: *The system may be managed using the Telnet protocol. The Telnet protocol is enabled by default. 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.

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.

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

Node	Command	Description
enable	show hostname	This command displays the system's network name.
configure	reboot	This command reboots the system.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
interface	show	This command displays the current port configurations.
vlan	show	This command displays the current VLAN configurations.

The Node type:

- enable

  Its command prompt is "***TI-PG541I#".***

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

- configure

  Its command prompt is "***TI-PG541I(config)#".***

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

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

  TI-PG541I# configure terminal

- eth0

  Its command prompt is "***TI-PG541I(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.

  TI-PG541I(config)#interface eth0

  TI-PG541I(config-if)#

- interface

  Its command prompt is "***TI-PG541I(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.

  TI-PG541I(config)#interface gigaethernet1/0/5

  TI-PG541I(config-if)#

- vlan

  Its command prompt is "***TI-PG541I(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.

  TI-PG541I(config)#vlan 2

  TI-PG541I(config-vlan)#

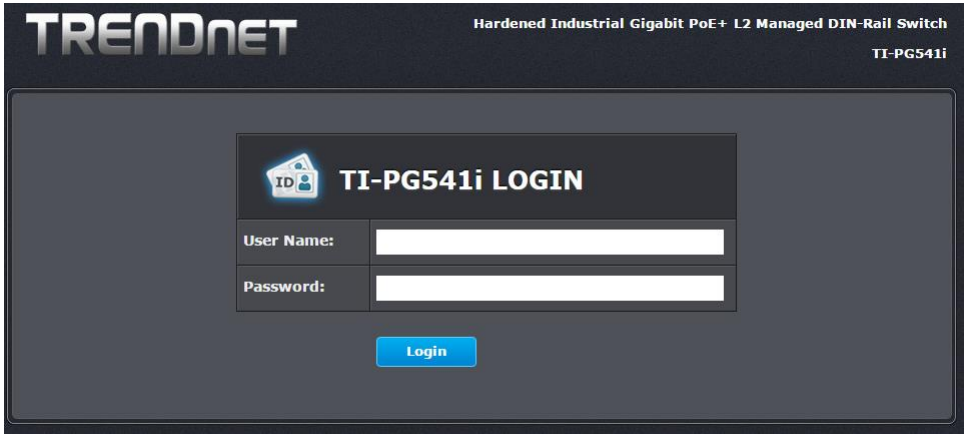
Access your switch web management page

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 Conifiguration will be used to reference access from web management page.*

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

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

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



Parameter	Description
User ID	Enter the user name.
Password	Enter the password.

Default:

User name: admin

Password: admin

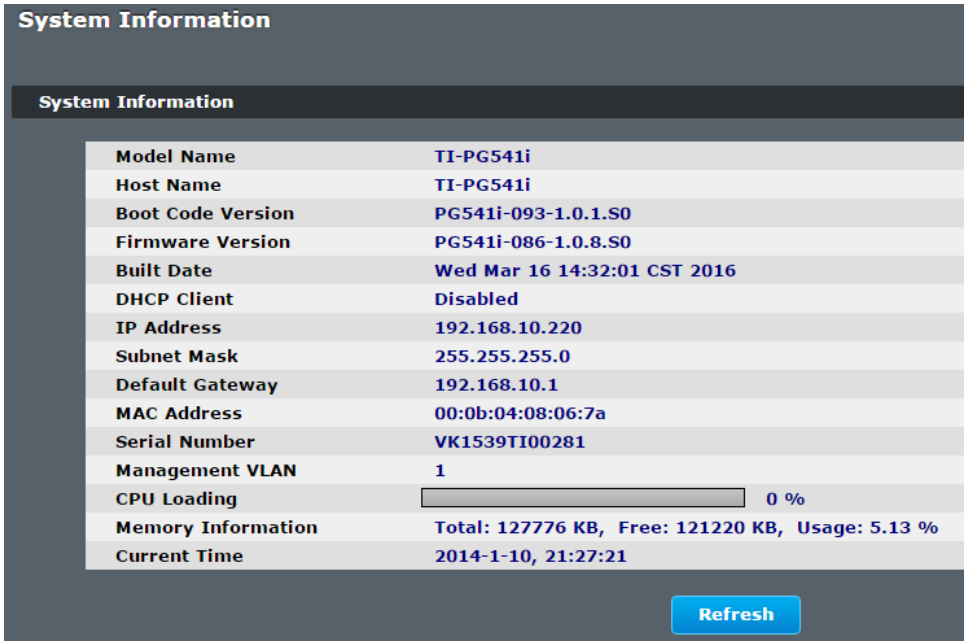
System Information

CLI Configuration

Node	Command	Description
enable	show hostname	This command displays the system's network name.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system's CPU loading and memory information.
enable	show uptime	This command displays the system up time.

Web Configuration

System Status > System Information



Parameter	Description
Model Name	This field displays the model name of the Switch.
Host name	This field displays the name of the Switch.
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the firmware version.
Built Date	This field displays the built date of the firmware.
DHCP Client	This field displays whether the DHCP client is enabled on the Switch.

IP Address	This field indicates the IP address of the Switch.
Subnet Mask	This field indicates the subnet mask of the Switch.
Default Gateway	This field indicates the default gateway of the Switch.
MAC Address	This field displays the MAC (Media Access Control) address of the Switch.
Serial Number	The serial number assigned by manufacture for identification of the unit.
Management VLAN	This field displays the VLAN ID that is used for the Switch management purposes.
CPU Loading	This field displays the percentage of your Switch's system load.
Memory Information	This field displays the total memory the Switch has and the memory which is currently available (**Free**) and occupied (**Usage**).
Current Time	This field displays current date (yyyy-mm-dd) and time (hh:mm:ss).
Refresh	Click this to update the information in this screen.

Basic Settings

General Settings

System

Management VLAN

To specify a VLAN group which can access the Switch.

- The valid VLAN range is from 1 to 4094.
- If you want to configure a management VLAN, the management VLAN should be created first and the management VLAN should have at least one member port.

Host Name

The **hostname** is same as the SNMP system name. Its length is up to 64 characters.

The first 16 characters of the hostname will be configured as the CLI prompt.

Default Settings

The default Hostname is TI-PG541I

The default DHCP client is disabled.

The default Static IP is 192.168.10.200

Subnet Mask is 255.255.255.0

Default Gateway is 0.0.0.0

Management VLAN is 1.

CLI Commands

Node	Command	Description
configure	Reboot	This command reboots the system.
configure	hostname STRINGS	This command sets the system's network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
eth0	Show	This command displays the eth0 configurations.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	This command configures the system default gateway.
eth0	ip dhcp client (disable|enable|renew)	This command configures a DHCP client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCP client to get an IP address from DHCP server.

eth0	management vlan VLANID	This command configures the management vlan.

Example: The procedures to configure an IP address for the Switch.

✓ To enter the configure node.

TI-PG541I#configure terminal

TI-PG541I(config)#

✓ To enter the ETH0 interface node.

TI-PG541I(config)#interface eth0

TI-PG541I(config-if)#

✓ To get an IP address from a DHCP server.

TI-PG541I(config-if)#ip dhcp client enable

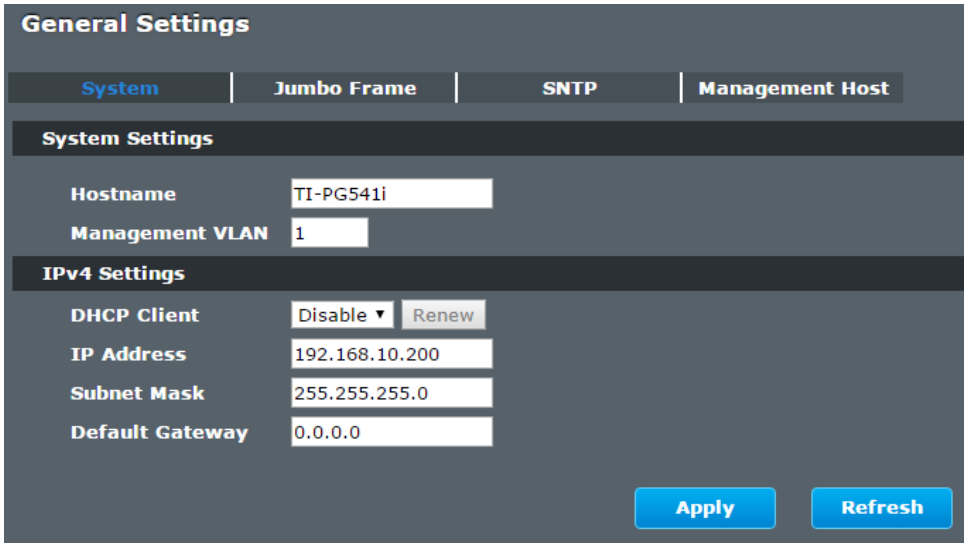
✓ To configure a static IP address and a gateway for the Switch.

TI-PG541I(config-if)#ip address 192.168.202.111/24

TI-PG541I(config-if)#ip address default-gateway 192.168.202.1

Web Configuration

Basic Settings > General Settings > System



IP Address	Configures a IPv4 address for your Switch in dotted decimal notation. For example, 192.168.10.200.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.10.1.

Jumbo Frame

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a network. The bigger the frame size, the better the performance.

Notice:

The jumbo frame settings will apply to all ports.

If the size of a packet exceeds the jumbo frame size, the packet will be dropped.

The available values are 10240, 9216, 1522, 1536, 1552.

Default Settings

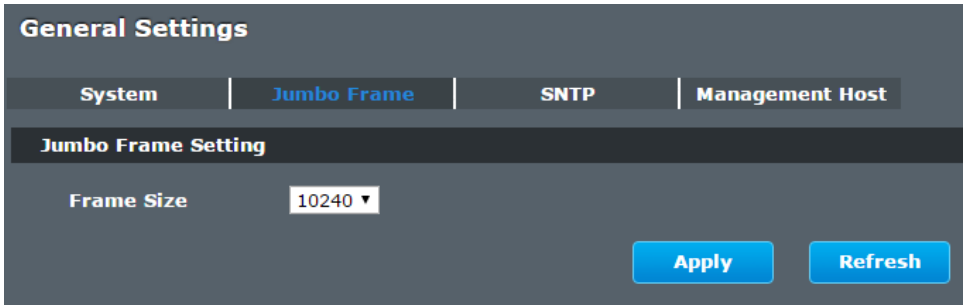
The default jumbo frame is 10240 bytes.

CLI Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240|9216|1522|1536|1552)	This command configures the maximum number of bytes of frame size.

Web Configuration

Basic Settings > General Settings > Jumbo Frame



Parameter	Description
Frame Size	This field configures the maximum number of bytes of frame size for specified port(s).
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

SNTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the **Simple Network Time Protocol** (**SNTP**). NTP provides Coordinated Universal Time (UTC). No information about time zones or daylight saving time is transmitted; this information is outside its scope and must be obtained separately.

UDP Port: 123.

Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

Note:

1. The SNTP server always replies the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
4. If no SNTP reply packets, the Switch will retry every 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

Default Settings

Current Time:

Time: 0:3:51 (UTC)

Date: 1970-1-1

Time Server Configuration:

Time Zone : +00:00

IP Address: 0.0.0.0

DayLight Saving Time Configuration:

State : disabled

Start Date: None.

End Date : None.

CLI Configuration

Node	Command	Description
enable	show time	This command 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	This command enables the daylight saving time.
configure	time daylight-saving-time start-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH OCLOCK	This command sets the start date for the 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	This command sets the end date for the Daylight Saving Time. For Example: Last Sunday 10 18 (PM: 6 Last Sunday in October)

configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of your time server.
configure	no time ntp-server	This command disables the NTP server settings.
configure	time timezone VALUE	Selects the time difference between UTC (formerly known as GMT) and your time zone. Valid value: -1200 to 1200.

Example:

TI-PG541I(config)#*time ntp-server 192.5.41.41*

TI-PG541I(config)#*time timezone +0800*

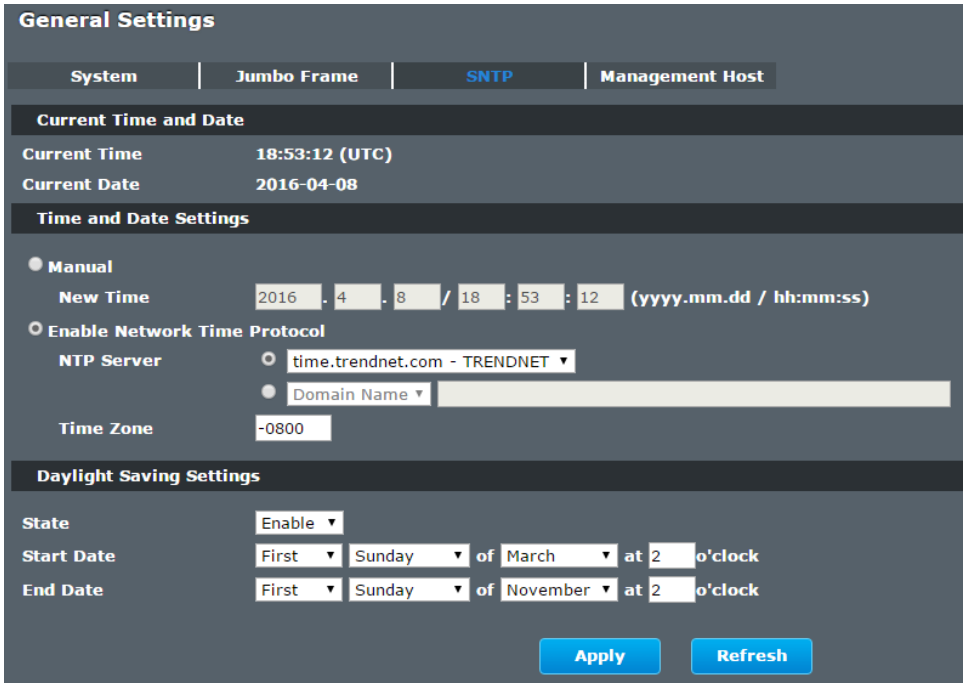
TI-PG541I(config)#*time ntp-server enable*

TI-PG541I(config)#time daylight-saving-time start-date first Monday 6 0

TI-PG541I(config)#time daylight-saving-time end-date last Saturday 10 0

Web Configuration

Basic Settings > General Settings > SNTP



Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.

New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then appear in the **Current Date** and **Current Time** fields after you click **Apply**.
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address or type the domain name of your time server. The Switch searches for the timeserver for up to 60 seconds.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Settings	
State	Select **Enable** if you want to use Daylight Saving Time. Otherwise, select **Disable** to turn it off.
Start Date	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Management Host

The feature limits the hosts which can manage the Switch. That is, any hosts can manage the Switch via **telnet** or **web browser**. If user has configured one or more management host, the Switch can be managed by these hosts only. The feature allow user to configure management IP up to 3 entries.

Default Settings

The default is none, any host can manage the Switch via telnet or web browser.

CLI Configuration

Node	Command	Description
enable	show interface eth0	The command displays the all of the interface *eth0* configurations.

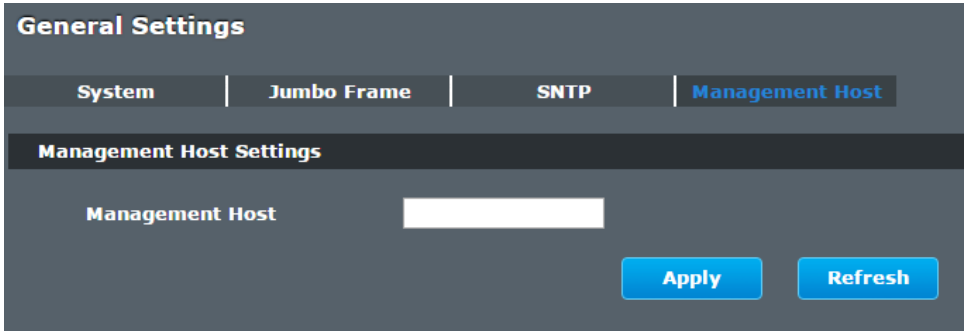
eth0	show	The command displays the all of the interface *eth0* configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example:

TI-PG541I#configure terminal
TI-PG541I(config)#interface eth0
TI-PG541I(config-if)#management host 192.168.200.106

Web Configuration

Basic Settings > General Settings > Management Host



Parameter	Description
Management Host	This field configures the management host.
Apply	Click this button to take effect the settings.
Refresh	Click this button to begin configuring this screen afresh.

Management Host List	
No.	This field displays a sequential number for each management host.
Management Host	This field displays the management host.
Action	Click the Delete button to remove the specified entry.

MAC Management

Dynamic Address:

The MAC addresses are learnt by the switch. When the switch receives frames, it will record the source MAC, the received port and the VLAN in the address table with an age time. When the age time is expired, the address entry will be removed from the address table.

Static Address:

The MAC addresses are configured by users. The static addresses will not be aged out by the switch; it can be removed by user only. The maximum static address entry is up to 256.

The **MAC Table** (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's MAC Table. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1. The Switch examines the received frame and learns the port from which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learnt in the **MAC Table**.
   - If the Switch has already learnt the port for this MAC address, then it forwards the frame to that port.
   - If the Switch has not already learnt the port for this MAC address, then the frame is flooded to all ports. If too much port flooding, it may lead to network congestion.
   - If the Switch has already learnt the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

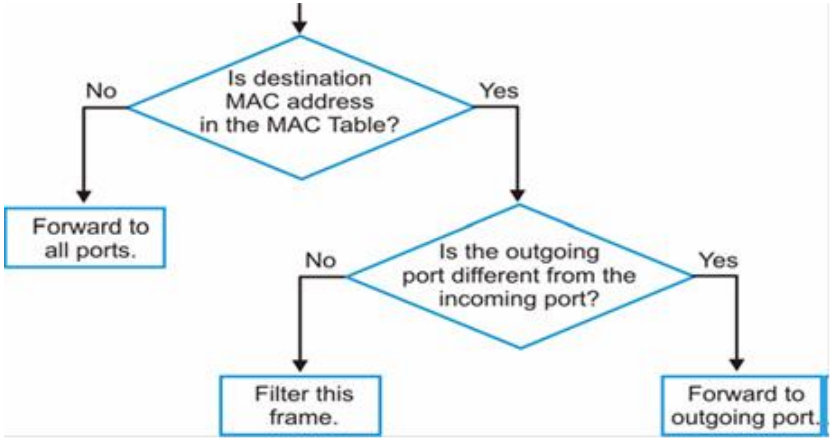


Figure MAC Table Flowchart

Default Settings

The default MAC address table age time is 300 seconds.
The Maximum static address entry is 256.

Static MAC Settings

CLI Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current MAC address table age time.
enable	show mac-address-table (static|dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	This command displays information of a specific MAC.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries learnt by the specific port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	This command configures a static unicast entry.

configure	no mac-address-table static MACADDR vlan VLANID	This command removes a static unicast entry from the address table.
configure	clear mac address-table dynamic	This command clears the dynamic address entries.

Example:

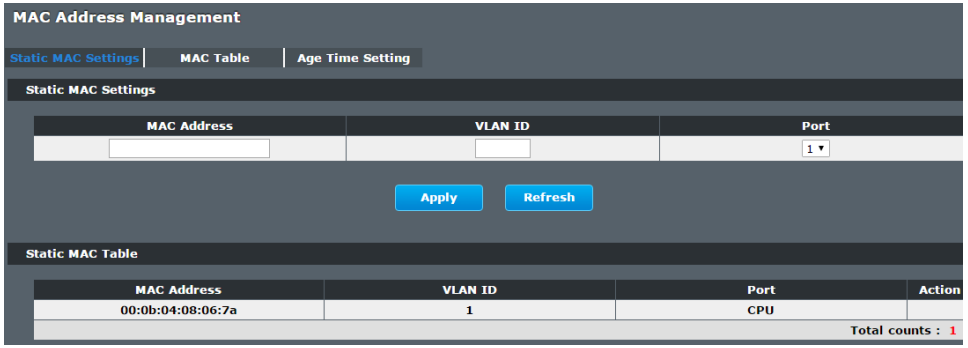
TI-PG541I(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1

Web Configuration

Basic Settings > MAC Management > Static MAC Settings

Static MAC

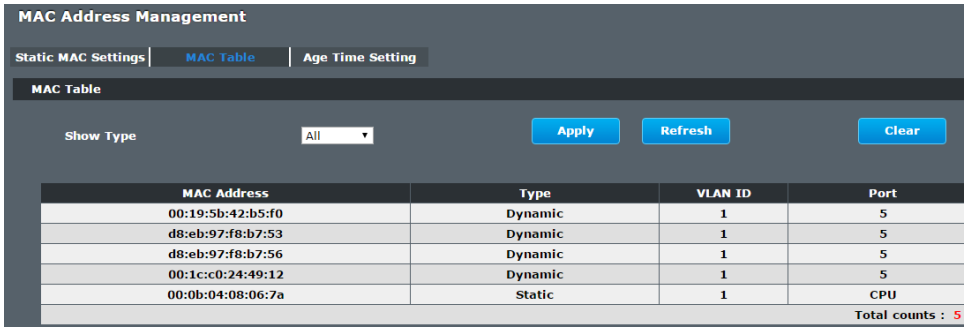
A static Media Access Control (MAC) address is an address that has been manually entered in the MAC address table, and do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port, so this may reduce the need for broadcasting.



Parameter	Description
Static MAC Settings	
MAC Address	Enter the MAC address of a computer or device that you want to add to the MAC address table.
	Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Port	Enter the port number to which the computer or device is connected.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Static MAC Table	
MAC Address	This field displays the MAC address of a manually entered MAC address entry.
VLAN ID	This field displays the VID of a manually entered MAC address entry.
Port	This field displays the port number of a manually entered MAC address entry. The MAC address with port CPU means the Switch's MAC addresses itself.
Action	Click **Delete** to remove this manually entered MAC address entry from the MAC address table. You cannot delete the Switch's MAC address from the static MAC address table.

MAC Table

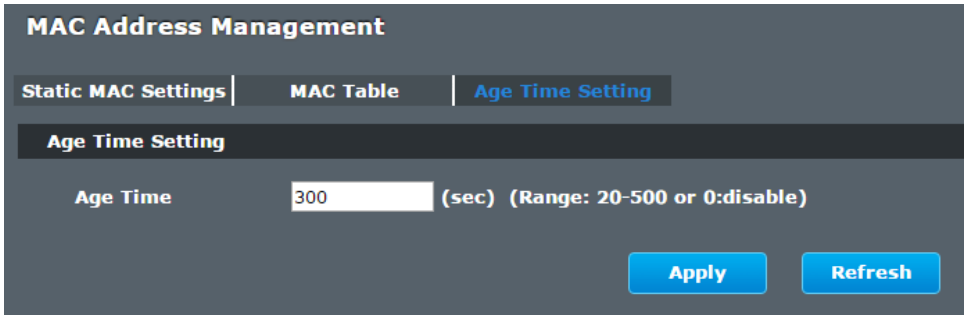
Basic Settings > MAC Management > MAC Table



Parameter	Description
Show Type Apply	Select **All, Static**, **Dynamic or Port** and then click **Apply** to display the corresponding MAC address entries on this screen.
Refresh	Click this to update the information in the MAC table.
MAC Address	This field displays a MAC address.
Type	This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic).
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Port	This field displays the port number the MAC address entry is associated. It displays CPU if it is the entry for the Switch itself. The CPU means that it is the Switch's MAC.
Total Counts	This field displays the total entries in the MAC table.

Age Time Settings

Basic Settings > MAC Management > Age Time Settings



Parameter	Description
Age Time	Configure the age time; the valid range is from 20 to 500 seconds. The default value is 300 seconds.
Apply	Click Apply to take effect the settings.
Refresh	Click this to update the information in the MAC table.

Port Mirror

Port-based Mirroring

The Port-Based Mirroring is used on a network switch to send a copy of network packets sent/received on one or a range of switch ports to a network monitoring connection on another switch port (**Monitor to Port**). This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic. Users can monitor the selected ports (**Source Ports**) for egress and/or ingress packets.

Source Mode:

Ingress : The received packets will be copied to the monitor port.

Egress : The transmitted packets will be copied to the monitor port.

Both : The received and transmitted packets will be copied to the monitor port.

Note:

1. The monitor port cannot be a trunk member port.
2. The monitor port cannot be ingress or egress port.
3. If the Port Mirror function is enabled, the Monitor-to Port can receive mirrored packets only.
4. If a port has been configured as a source port and then user configures the port as a destination port, the port will be removed from the source ports automatically.

Default Settings

Mirror Configurations:

State : Disable

Monitor port : 1

Ingress port(s) : None

Egress port(s) : None

CLI Configuration

Node	Command	Description
enable	show mirror	This command displays the current port mirroring configurations.
configure	mirror (disable|enable)	This command disables / enables the port mirroring on the switch.
configure	mirror destination port PORT_ID	This command specifies the **monitor port** for the port mirroring.
configure	mirror source ports PORT_LIST mode *(both|ingress|egress)*	This command **adds** a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	This command **removes** a port or a range of ports from the source ports of the port mirroring.

Example:

TI-PG541I#*configure terminal*

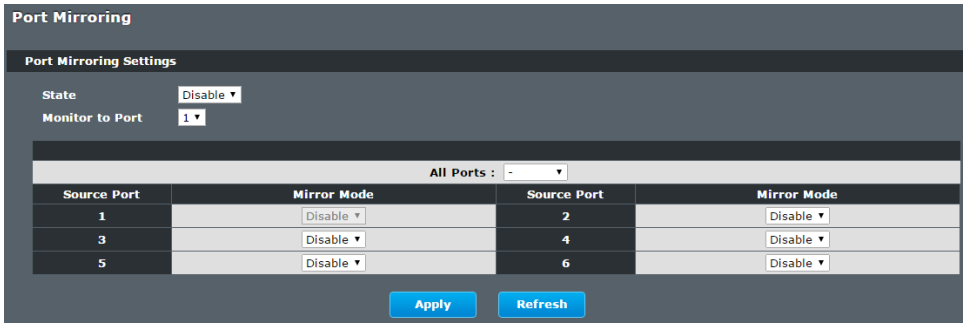
TI-PG541I(config)#mirror enable

TI-PG541I(config)#mirror destination port 2

TI-PG541I(config)#mirror source ports 3-5 mode both

Web Configuration

Basic Settings > Port Mirroring



Parameter	Description
State	Select **Enable** to turn on port mirroring or select **Disable** to turn it off.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port	This field displays the number of a port.
Mirror Mode	Select **Ingress**, **Egress** or **Both** to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select **Disable** to not copy any traffic from the specified source ports to the monitor port.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

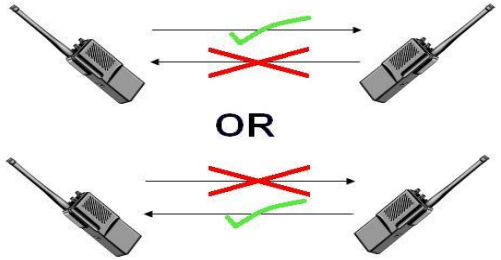
Port Settings

- Duplex mode

A *duplex* communication system is a system composed of two connected parties or devices that can communicate with one another in both directions.

Half Duplex:

A *half-duplex* system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.



Full Duplex:

A *full-duplex*, or sometimes *double-duplex* system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time.

- Loopback Test

A loopback test is a test in which a signal in sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. One type of loopback test is performed using a special plug, called a **wrap plug** that is inserted in a port on a communications device. The effect of a wrap plug is to cause transmitted (output) data to be returned as

received (input) data, simulating a complete communications circuit using a single computer.

- Auto MDI-MDIX

Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used or the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto". Auto-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

- Auto Negotiation

Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode.

If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using **half duplex** mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

- Flow Control

A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses.IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill and resend later.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Note: 1000 Base-T doesn't support force mode.

- Cable Test.

This feature determines the quality of the cables, shorts, and cable impedance mismatch, bad connectors, termination mismatch, and bad magnetics. The feature can work on the copper Ethernet cable only.

Default Settings

The default port Speed & Duplex is auto for all ports.

The default port Flow Control is Off for all ports.

General Settings

CLI Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none | mac)	This command tests the loopback mode of operation for the specific port.
interface	flowcontrol (off | on)	This command disables / enables the flow control for the port.
interface	speed (auto|10-full||10-half|100-full|100-half|1000-full)	This command configures the speed and duplex for the port.
interface	shutdown	This command disables the specific port.
interface	no shutdown	This command enables the specific port.
interface	description STRINGs	This command configures a description for the specific port.
interface	no description	This command configures the default port description.
interface	cable test	This command diagnostics the Ethernet cable and shows the broken distance.
interface	clean cable-test result	This command cleans the test result of the Ethernet cable test.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a description for the specific ports.
if-range	no description	This command configures the default port description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto|10-full||10-half|100-full|100-half|1000-full)	This command configures the speed and duplex for the port.

Example:

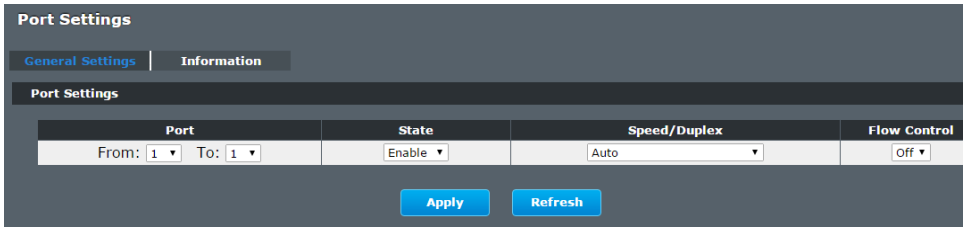
TI-PG541I#*configure terminal*

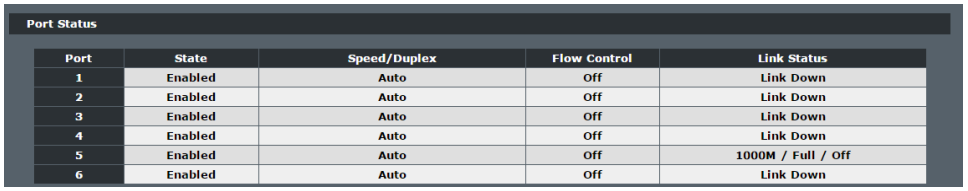
TI-PG541I(config)#*interface gi1/0/1*

TI-PG541I(config-if)#*speed auto*

Web Configuration

Basic Settings > Port Settings > General Settings

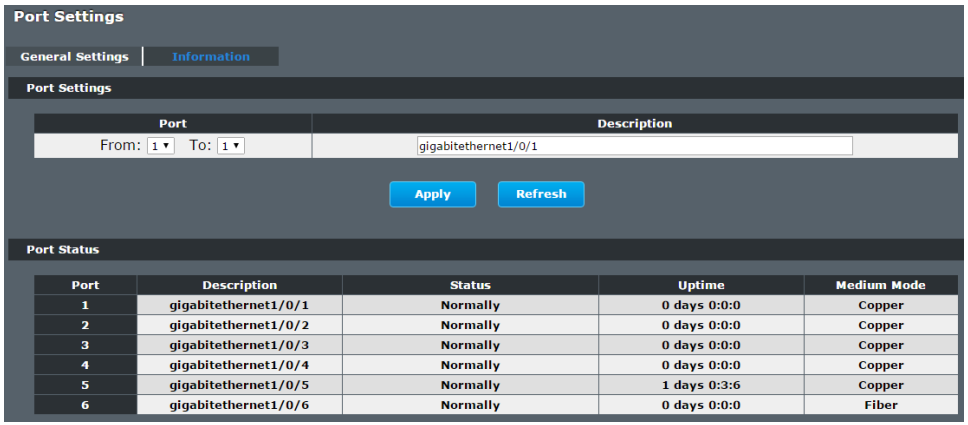




Parameter	Description
Port	Select a port or a range ports you want to configure on this screen.
State	Select **Enable** to activate the port or **Disable** to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: • **Auto** • **10 Mbps / Full Duplex** • **10 Mbps / Half Duplex** • **100 Mbps / Full Duplex** • **100 Mbps / Half Duplex** • **1000 Mbps / Full Duplex**
Flow Control	Select **On** to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select **Off** to disable it.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port	This field displays the port number.
State	This field displays whether the port is enabled or disabled.
Speed/Duplex	This field displays the speed either **10M**, **100M** or **1000M** and the duplex mode **Full** or **Half**.
Flow Control	This field displays whether the port's flow control is **On** or **Off**.
Link Status	This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays **Link Down** if the port is disabled or not connected to any device.

Information

Basic Settings > Port Settings > Information



Parameter	Description
Port	Select a port or a range ports you want to configure on this screen.
Description	Configures a meaningful name for the port(s).
Port Status	
Port	This field displays the port number.
Description	The meaningful name for the port.
Status	The field displays the detail port status if the port is blocked by some protocol.
Uptime	The sustained time from last link up.
Medium Mode	The current working medium mode, copper or fiber, for the port.

Advanced Settings

Bandwidth Control

QoS

Each egress port can support up to 8 transmit queues. Each egress transmit queue contains a list specifying the packet transmission order. Every incoming frame is forwarded to one of the 8 egress transmit queues of the assigned egress port, based on its priority. The egress port transmits packets from each of the 8 transmit queues according to a configurable scheduling algorithm, which can be a combination of Strict Priority (SP) and/or Weighted Round Robin (WRR).

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue.

The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

Priority : 0 1 2 3 4 5 6 7
Queue : 2 0 1 3 4 5 6 7

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the four hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

QoS Enhancement

You can configure the Switch to prioritize traffic even if the incoming packets are not marked with IEEE 802.1p priority tags or change the existing priority tags based on the criteria you select. The Switch allows you to choose one of the following methods for assigning priority to incoming packets on the Switch:

- **802.1p Tag Priority** - Assign priority to packets based on the packet's 802.1p tagged priority.
- **Port Based QoS** - Assign priority to packets based on the incoming port on the Switch.
- **DSCP Based QoS** - Assign priority to packets based on their Differentiated Services Code Points (DSCPs).

Note: Advanced QoS methods only affect the internal priority queue mapping for the Switch. The Switch does not modify the IEEE 802.1p value for the egress frames. You can choose one of these ways to alter the way incoming packets are prioritized or you can choose not to use any QoS enhancement setting on the Switch.

802.1p Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Ethernet Packet:

6	6	2	42-1496	4
DA	SA	Type / Length	Data	FCS

6	6	4	2	42-1496	4
DA	SA	802.1Q Tag	Type / Length	Data	FCS

802.1Q Tag:

2 bytes	2 bytes		
Tag Protocol Identifier (TPID)	Tag Control Information (TCI)		
16 bits	3 bits	1 bit	12 bits
TPID (0x8100)	Priority	CFI	VID

- Tag Protocol Identifier (TPID): a 16-bit field set to a value of **0x8100** in order to identify the frame as an IEEE 802.1Q-tagged frame.
- Tag Control Information (TCI)
  - Priority Code Point (PCP): a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level from **0 (lowest) to 7 (highest)**, which can be used to prioritize different classes of traffic (voice, video, data, etc.).
  - Canonical Format Indicator (CFI): a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to zero for Ethernet switches. CFI is used for compatibility between Ethernet and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be bridged to an untagged port.
  - VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame doesn't belong to any VLAN; in this case the 802.1Q tag specifies only a priority and is referred to as a **priority tag.** A value of hex 0xFFF is reserved for implementation use. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs. On bridges, VLAN 1 is often reserved for management.

Priority Levels

PCP: Priority Code Point.

PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, <100ms latency
5	5	Video, < 10ms latency
6	6	Internetwork Control
7	7 (highest)	Network Control

DiffServ (DSCP)

Differentiated Services or **DiffServ** is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (**QoS**) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service (**GS**) to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

Differentiated Services Code Point (**DSCP**) is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

When using the DiffServ priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Version	IHL	**Type of Service**	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	

Source Address	
Destination Address	
Options	Padding

Example Internet Datagram Header

IP Header Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence at time of high load). The major choice is a three way tradeoff between low-delay, high-reliability, and high-throughput.

Bits 0-2: Precedence.
Bit 3: 0 = Normal Delay, 1 = Low Delay.
Bits 4: 0 = Normal Throughput, 1 = High Throughput.
Bits 5: 0 = Normal Reliability, 1 = High Reliability.
Bit 6-7: Reserved for Future Use.

```
  0   1   2   3   4   5   6   7
+-----+-----+-----+-----+-----+-----+-----+-----+
|  PRECEDENCE   | D | T | R | 0 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Precedence
111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

The use of the Delay, Throughput, and Reliability indications may increase the cost (in some sense) of the service. In many networks better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases at most two of these three indications should be set.

The type of service is used to specify the treatment of the datagram during its transmission through the internet system. Example mappings of the internet type of service to the actual service provided on networks such as AUTODIN II, ARPANET, SATNET, and PRNET is given in "Service Mappings".

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only.

If the actual use of these precedence designations is of concern to a particular network, it is the responsibility of that network to control the access to, and use of, those precedence designations.

DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	1	0	2	0
60	0	31	0	62	0
63	0				

Example:

IP Header

DSCP=50 ➔ 45 **C8** . . .

Queuing Algorithms

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

- **Strict-Priority (SPQ)**

  The packets on the high priority queue are always service firstly.

- **Weighted round robin (WRR)**

  Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

  Weighted Round Robin (WRR) scheduling uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

Default Settings

QoS mode : High First (SPQ)

The mappings of the Priority to Queue are:

PRIO 0 ==> COSQ 2
PRIO 1 ==> COSQ 0
PRIO 2 ==> COSQ 1
PRIO 3 ==> COSQ 3
PRIO 4 ==> COSQ 4
PRIO 5 ==> COSQ 5
PRIO 6 ==> COSQ 6
PRIO 7 ==> COSQ 7

The DiffServ is disabled on the switch.

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
00	0	01	0	02	0	03	0
04	0	05	0	06	0	07	0
08	0	09	0	10	0	11	0
12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0
20	0	21	0	22	0	23	0
24	0	25	0	26	0	27	0
28	0	29	0	30	0	31	0
32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0
40	0	41	0	42	0	43	0
44	0	45	0	46	0	47	0
48	0	49	0	50	0	51	0
52	0	53	0	54	0	55	0
56	0	57	0	58	0	59	0
60	0	61	0	62	0	63	0

Note: If the DiffServ is disabled, the 802.1p tag priority will be used.

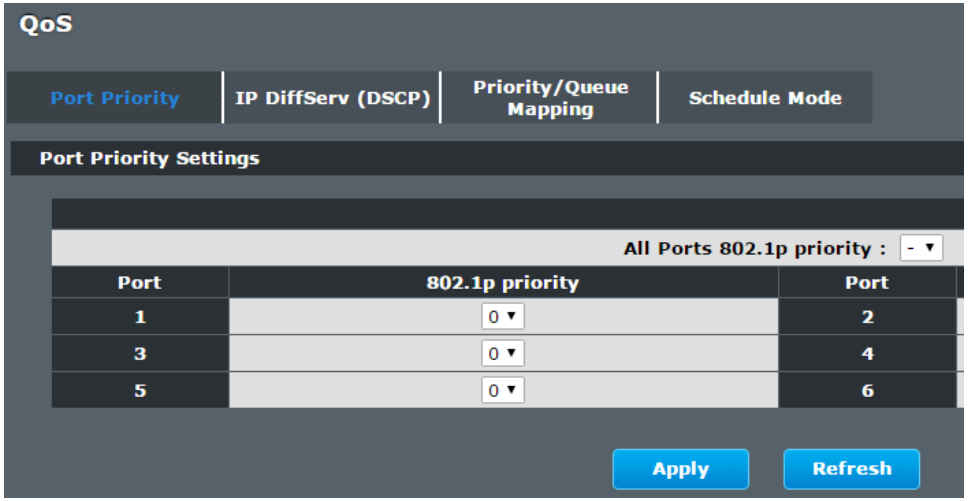
CLI Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	This command displays the current QoS scheduling mode of IEEE 802.1p.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping to the service queue.
configure	no queue cos-map	This command configures the 802.1p priority mapping to the service queue to default.
configure	qos mode high-first	This command configures the QoS scheduling mode to high_first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wfq-queue	This command configures the QoS scheduling mode to Weighted Fair Queuing.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command configures the QoS scheduling mode to Weighted Round Robin.
interface	default-priority	This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to default (0).
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv	This command disables / enables the DiffServ function. (disable|enable)
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

Web Configuration

Port Priority

Advanced Settings > Bandwidth Control > QoS

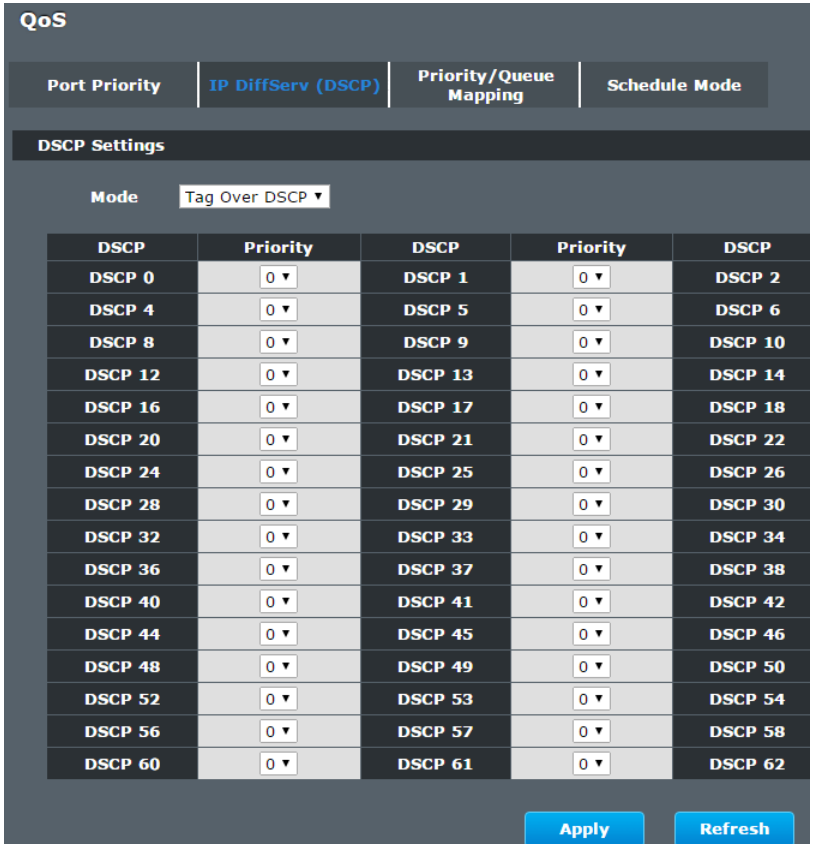


Parameter	Description
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	This field displays the number of a port.
802.1p Priority	Select a priority for packets received by the port. Only packets without 802.1p priority tagged will be applied the priority you set here.

Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

IP DiffServ (DSCP)

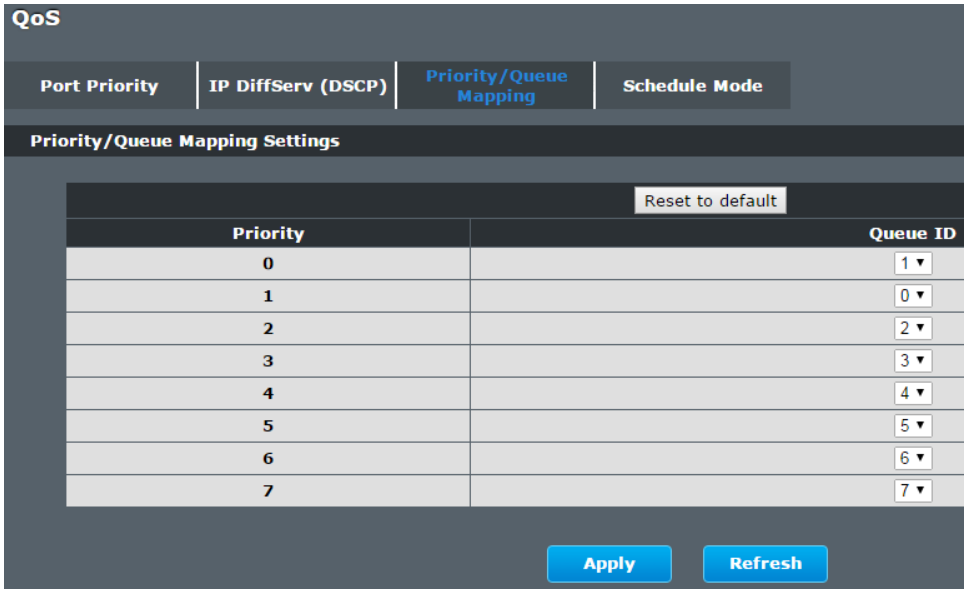
Advanced Settings > Bandwidth Control > IP DiffServ (DSCP)



Parameter	Description
Mode	"Tag Over DSCP" or "DSCP Over Tag". "Tag Over DSCP" means the 802.1p tag has higher priority than DSCP.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Priority/Queue Mapping

Advanced Settings > Bandwidth Control > Priority/Queue Mapping

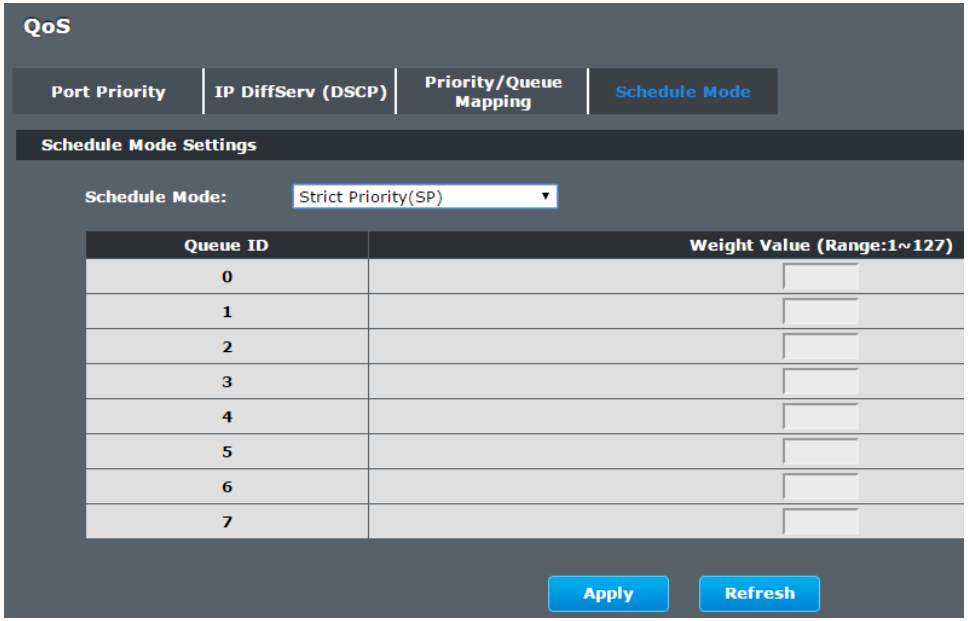


Parameter	Description
Reset to Default	Click this button to reset the priority to queue mappings to the defaults.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Queue ID	Select the number of a queue for packets with the priority level.

Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Schedule Mode

Advanced Settings > Bandwidth Control > Schedule



Parameter	Description
Schedule Mode	Select **Strict Priority** (SP) or **Weighted Round Robin** (**WRR**). Note: Queue weights can only be changed when **Weighted Round Robin** is selected. **Weighted Round Robin** scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Queue ID	This field indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.
Weight Value	You can only configure the queue weights when **Weighted Round Robin** is selected. Bandwidth is divided across the different traffic queues according to their weights.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Rate Limitation

Storm Control

A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate.

Storm Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The **Rate** is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.

Storm Control unit : pps.

Default Settings

Broadcast Storm Control : 300pps.
Multicast Storm Control : None.
DLF Storm Control : 300pps.

CLI Configuration

Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation.
configure	no storm-control type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command disables the bandwidth limit for broadcast or multicast or DLF packets.

Example:

TI-PG541I#configure terminal

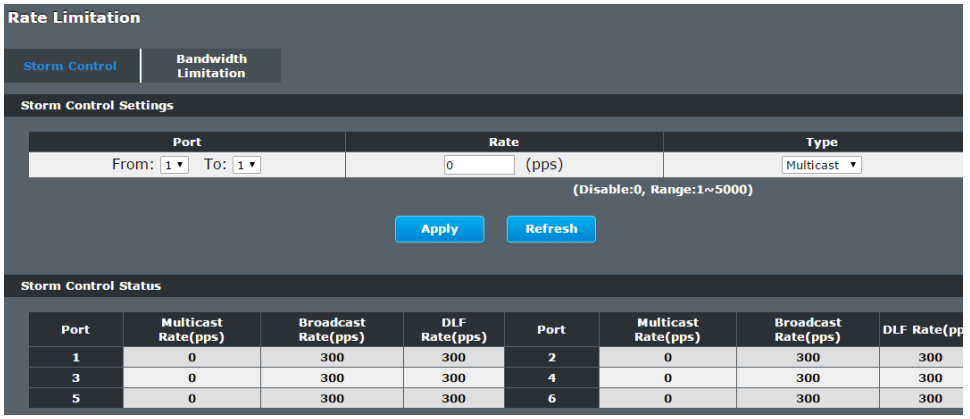
TI-PG541I(config)#storm-control rate 1 type broadcast ports 1-6

TI-PG541I(config)#storm-control rate 1 type multicast ports 1-6

TI-PG541I(config)#storm-control rate 1 type DLF ports 1-6

Web Configuration

Advanced Settings > Bandwidth Control > Rate Limitation > Storm Control



Parameter	Description
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the **Type** field) per second the Switch can receive per second.
Type	Select **Broadcast** - to specify a limit for the amount of broadcast packets received per second. **Multicast** - to specify a limit for the amount of multicast packets received per second. **DLF** - to specify a limit for the amount of DLF packets received per second.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Bandwidth Limitation

The rate limitation is used to control the rate of traffic sent or received on a network interface.

Rate Limitation unit: Mbs.

Default Settings

All ports' Ingress and Egress rate limitation are disabled.

CLI Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current rate control configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for outgoing packets and set the limitation.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the bandwidth limit for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for incoming packets and set the limitation.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the bandwidth limit for incoming packets.

Example:

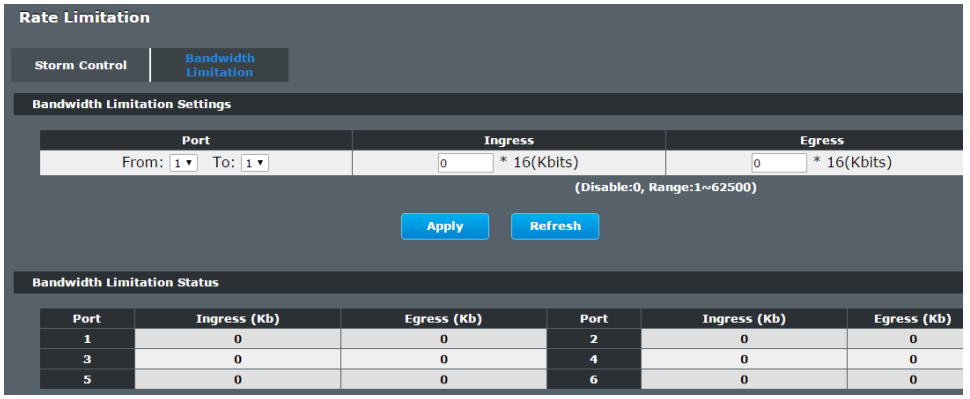
TI-PG541I#configure terminal

TI-PG541I(config)#bandwidth-limit egress 1 ports 1-6

TI-PG541I(config)#bandwidth-limit ingress 1 ports 1-6

Web Configuration

Advanced Settings > Bandwidth Control > Rate Limitation > Bandwidth Limitation



Parameter	Description
Port	Selects a port that you want to configure.
Ingress	Configures the rate limitation for the ingress packets.
Egress	Configures the rate limitation for the egress packets.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

IGMP Snooping

IGMP Snooping

The IGMP snooping is for multicast traffic. The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first VLANs that send IGMP packets. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

Immediate Leave

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN. (Immediate Leave is only supported on IGMP Version 2 hosts).

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Fast Leave

The switch allow user to configure a delay time. When the delay time is expired, the switch removes the interface from the multicast group.

Last Member Query Interval

Last Member Query Interval: The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP specific query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

IGMP Querier

There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router **with a lower IP address**, it MUST become a Non-Querier on that network. If a router has not heard a Query message from another router for [Other Querier Present Interval], it resumes the role of Querier. Routers periodically [Query Interval] send a General Query on each attached network for which this router is the Querier, to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] in order to quickly and reliably determine membership information. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max Response Time of [Query Response Interval].

Port IGMP Querier Mode

- **Auto:**

The Switch uses the port as an IGMP query port if the port receives IGMP query packets.

- **Fixed:**

The Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). The Switch always forwards the client's **report/leave** packets to the port.

Normally, the port is connected to an IGMP server.

- **Edge:**

The Switch does not use the port as an IGMP query port. The IGMP query packets received by this port will be dropped.

Normally, the port is connected to an IGMP client.

Note: The Switch will forward the IGMP join and leave packets to the query port.

Configurations:

Users can enable/disable the IGMP Snooping on the Switch. Users also can enable/disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the Switch is disabled, the IGMP Snooping is disabled on all VLANs even some of the VLAN IGMP Snooping are enabled.

Default Settings

If received packets are not received after 400 seconds, all multicast entries will be deleted.

The default global IGMP snooping state is disabled.

The default VLAN IGMP snooping state is disabled for all VLANs.

The unknown multicast packets will be dropped.

The default port Immediate Leave state is disabled for all ports.

The default port Querier Mode state is auto for all ports.

The IGMP snooping Report Suppression is disabled.

Notices: There are a global state and per VLAN states. When the global state is disabled, the IGMP snooping on the Switch is disabled even per VLAN states are enabled. When the global state is enabled, user must enable per VLAN states to enable the IGMP Snooping on the specific VLAN.

CLI Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
enable	show igmp-counters	This command displays the current IGMP snooping counters.
enable	show igmp-counters (port|vlan)	This command displays the current IGMP snooping counters per port or per vlan.
configure	igmp-snooping (disable | enable)	This command disables / enables the IGMP snooping on the switch.
configure	igmp-snooping vlan VLANID	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANID	This command disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop|flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. *drop:* Drop all of the unknown multicast packets.
interface	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well.

		(Default:auto)
interface	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific interface.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific interface.

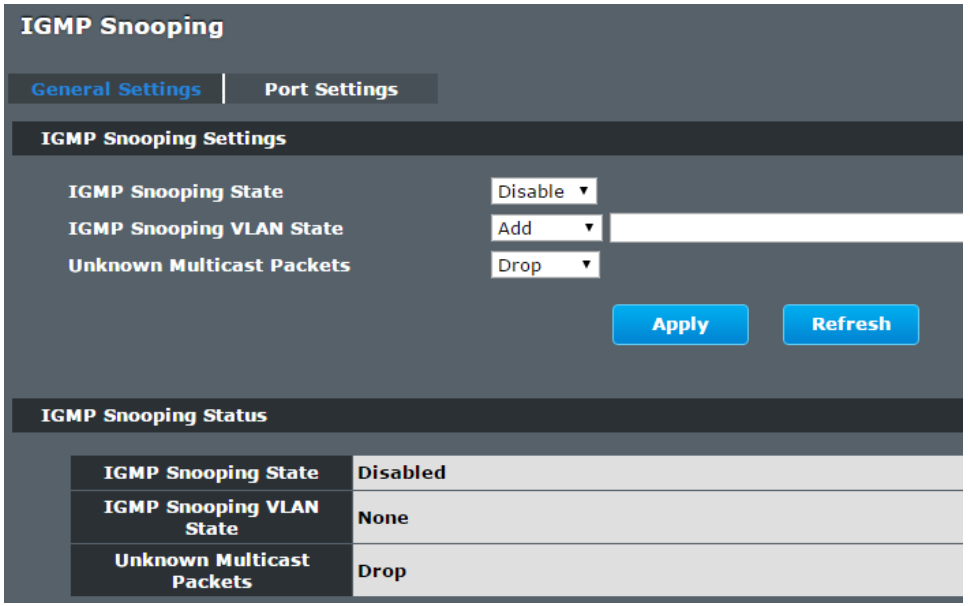
Example:

TI-PG541I(config)#*igmp-snooping enable*
TI-PG541I(config)#*igmp-snooping vlan 1*
TI-PG541I(config)#*interface 1/0/1*
TI-PG541I(config-if)#*igmp-immediate-leave*
TI-PG541I(config-if)#igmp-querier-mode fixed
TI-PG541I(config-if)#igmp-snooping group-limit 20

Web Configuration

General Settings

Advanced Settings > IGMP Snooping > IGMP Snooping > General Settings

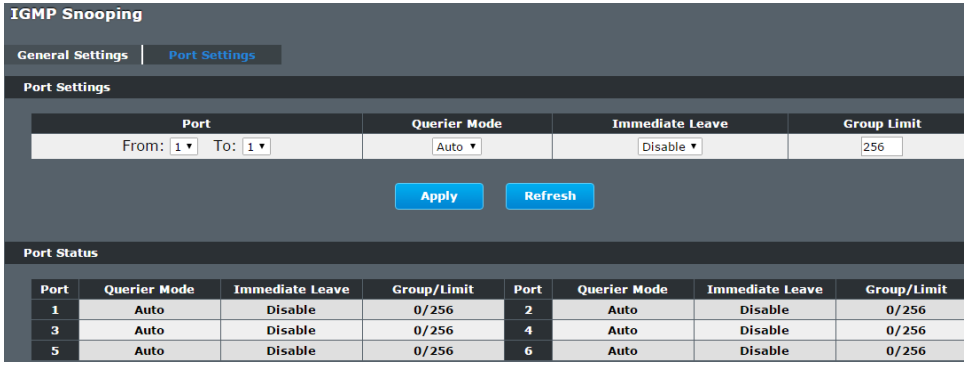


Parameter	Description
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate the feature.
IGMP Snooping VLAN State	Select **Add** and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select **Delete** and enter VLANs on which to have the Switch not perform IGMP snooping.
Unknown Multicast Packets	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.

Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
IGMP Snooping State	This field displays whether IGMP snooping is globally enabled or disabled.
IGMP Snooping VLAN State	This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet.
Unknown Multicast Packets	This field displays whether the Switch is set to discard or flood unknown multicast packets.

Port Settings

Advanced Settings > IGMP Snooping > IGMP Snooping > Port Settings



Parameter	Description
Querier Mode	Select the desired setting, **Auto**, **Fixed**, or **Edge**. **Auto** means the Switch uses the port as an IGMP query port if the port receives IGMP query packets. **Fixed** means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). **Edge** means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch does not forward IGMP join or leave packets to this port.
Immediate Leave	Select individual ports on which to enable immediate leave.
Group Limit	Configures the maximum group for the port or a range of ports.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
Port	The port ID.
Querier Mode	The Querier mode setting for the specific port.
Immediate Leave	The Immediate Leave setting for the specific port.
Group Counts	The current joining group count and the maximum group count.

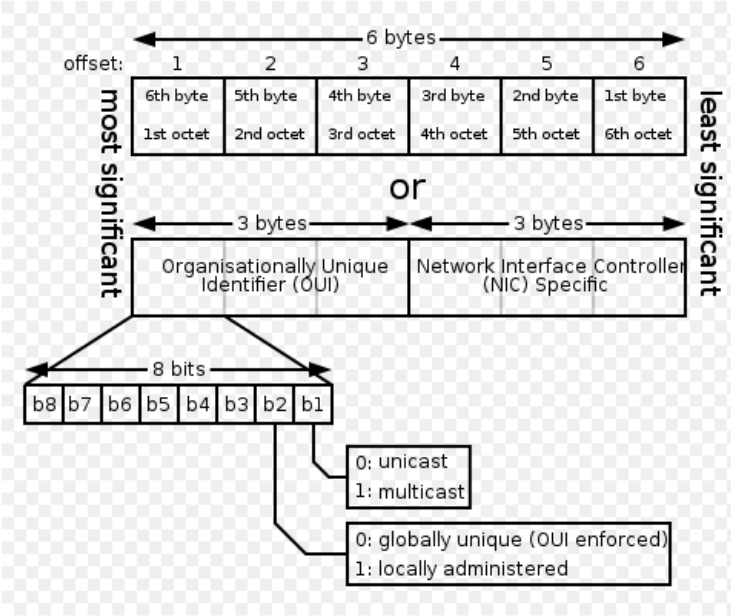
Multicast Address

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4.

The IANA owns the OUI MAC address 01:00:5e, therefore multicast packets are delivered by using the Ethernet MAC address range 01:00:5e:00:00:00 - 01:00:5e:7f:ff:ff. This is 23 bits of available address space.

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.



IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) AllSPFRouters address. Used to send Hello packets to all OSPF routers on a network segment
224.0.0.6	The OSPF AllDRouters address. Used to send OSPF routing information to OSPF designated routers on a network segment

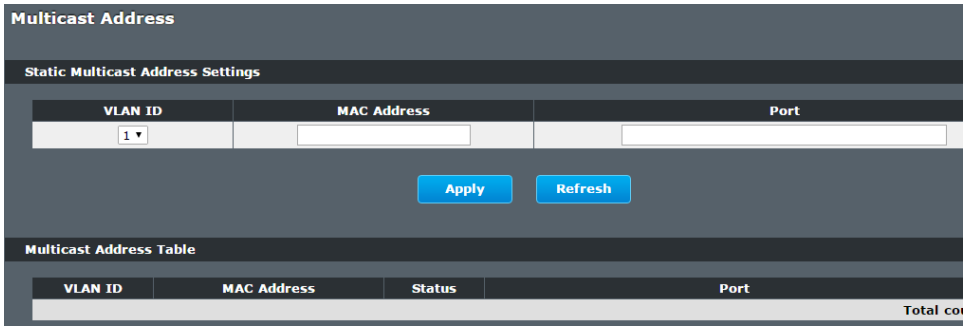
224.0.0.9	The RIP version 2 group address, used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment
224.0.0.10	EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment
224.0.0.13	PIM Version 2 (Protocol Independent Multicast)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 (Internet Group Management Protocol)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address
224.0.0.252	Link-local Multicast Name Resolution address
224.0.1.1	Network Time Protocol address
224.0.1.39	Cisco Auto-RP-Announce address
224.0.1.40	Cisco Auto-RP-Discovery address
224.0.1.41	H.323 Gatekeeper discovery address

CLI Configuration

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

Web Configuration

Advanced Settings > IGMP Snooping > Multicast Address



Parameter	Description
VLAN ID	Configures the VLAN that you want to configure.
MAC Address	Configures the multicast MAC which will not be aged out. Valid format is hh:hh:hh:hh:hh:hh.
Port	Configures the member port for the multicast address.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

VLAN

Port Isolation

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the port's private domain is not allowed. It will ignore the packets' tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.

Example: If you want to allow port-1 and port-3 to talk to each other, you must configure as below:

TI-PG541I(config)#interface 1/0/1
TI-PG541I(config-if)#port-isolation ports 3
TI-PG541I(config-if)#exit
; Allow the port-1 to send its ingress packets to port-3.

TI-PG541I(config)#interface 1/0/3
TI-PG541I(config-if)#port-isolation ports 1
TI-PG541I(config-if)#exit
; Allow the port-3 to send its ingress packets to port-1

CLI Configuration

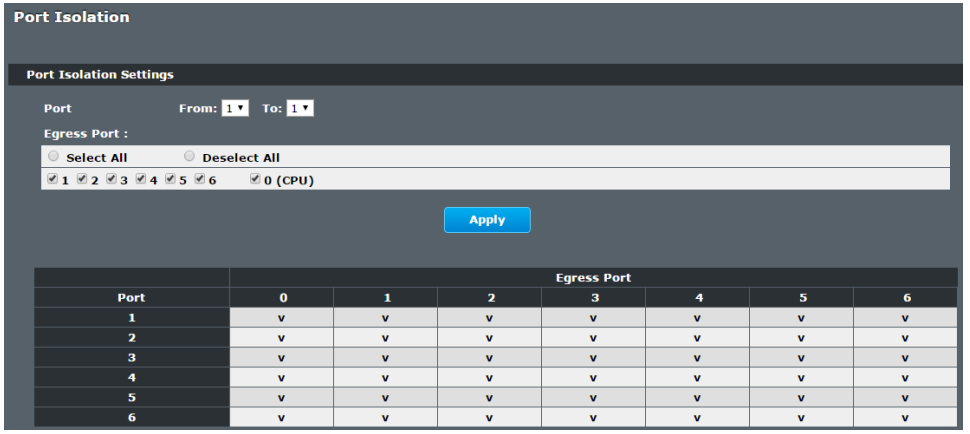
Node	Command	Description
enable	show port-isolation	This command displays the current port isolation configurations.
		"V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.
interface	port-isolation ports PORTLISTS	This command configures a port or a range of ports to egress traffic from the specific port.
interface	no port-isolation	This command configures all ports to egress traffic from the specific port.

Example:

TI-PG541I(config)#interface 1/0/2
TI-PG541I(config-if)#port-isolation ports 3-6

Web Configuration

Advanced Settings > VLAN > Port Isolation



Parameter	Description
Port	Select a port number to configure its port isolation settings.

	Select **All Ports** to configure the port isolation settings for all ports on the Switch.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves. Selecting a port as an outgoing port means it will communicate with the port currently being configured.
Select All/ Deselect All	Click **Select All** to mark all ports as egress ports and permit traffic. Click **Deselect All** to unmark all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
Port Isolation Status	"V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.

802.1Q VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VID- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 bytes	3 bits	1 bit	12 bits

- Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

- 802.1Q Port base VLAN

With port-based VLAN membership, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members of the same VLAN. The network administrator typically performs the

VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN without the intervention of a Layer 3 device.

The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is a member of a subnet and that the device should be able to talk to all other members of the subnet by simply sending information to the cable segment. The switch is responsible for identifying that the information came from a specific VLAN and for ensuring that the information gets to all other members of the VLAN. The switch is further responsible for ensuring that ports in a different VLAN do not receive the information.

This approach is quite simple, fast, and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If port-to-VLAN association is done with an application-specific integrated circuit (ASIC), the performance is very good. An ASIC allows the port-to-VLAN mapping to be done at the hardware level.

Default Settings

The default PVID is 1 for all ports.

The default Acceptable Frame is All for all ports.

All ports join in the VLAN 1.

Notice: The maximum VLAN group is 4094.

CLI Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command configures the vlan name to default. Note: The default vlan name is "VLAN"+vlan_ID, VLAN1, VLAN2,…
vlan	add PORTLISTS	This command adds a port or a range of ports to the vlan.
vlan	fixed PORTLISTS	This command assigns ports for permanent member of the vlan.
vlan	no fixed PORTLISTS	This command removes all fixed member from the vlan.
vlan	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no tagged PORTLISTS	This command removes all tagged member from the vlan.
vlan	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.

vlan	no untagged PORTLISTS	This command removes all untagged member from the vlan.
interface	acceptable frame type (all|tagged|untagged)	This command configures the acceptable frame type. all - acceptable all frame types. tagged - acceptable tagged frame only. untagged – acceptable untagged frame only.
interface	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
interface	no pvid	This command configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	This command configures 1 for the port default VLAN ID.
configure	vlan range STRINGS	This command configures a range of vlans.
configure	no vlan range STRINGS	This command removes a range of vlans.
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the vlans.
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the vlans.
vlan-range	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the vlans.
vlan-range	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the vlans.

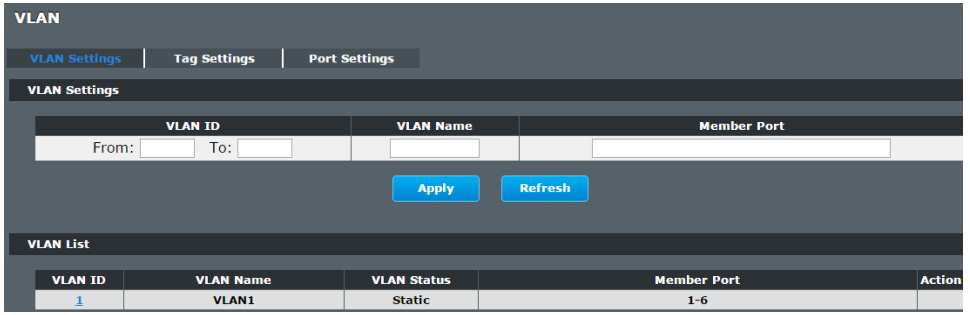
Example:

TI-PG541I#configure terminal
TI-PG541I(config)#vlan 2
TI-PG541I(config-vlan)#fixed 1-6
TI-PG541I(config-vlan)#untagged 1-3

Web Configuration

VLAN Settings

Advanced Settings > VLAN > VLAN > VLAN Settings

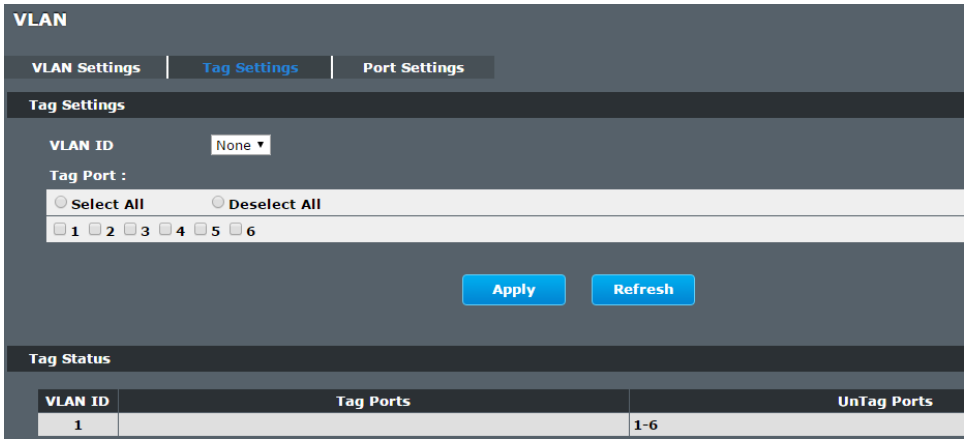


Parameter	Description
VLAN ID	Enter the VLAN ID for this entry; the valid range is between 1 and 4094.
VLAN Name	Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be the combination of the digit or the

	alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
Member Port	Enter the port numbers you want the Switch to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
VLAN List	
VLAN ID	This field displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	This field displays the name of the VLAN.
VLAN Status	This field displays the status of the VLAN. **Static** or **Dynamic** (802.1Q VLAN).
Member Port	This field displays which ports have been assigned as members of the VLAN. This will display **None** if no ports have been assigned.
Action	Click **Delete** to remove the VLAN. The VLAN 1 cannot be deleted.

Tag Settings

Advanced Settings > VLAN > Tag Settings

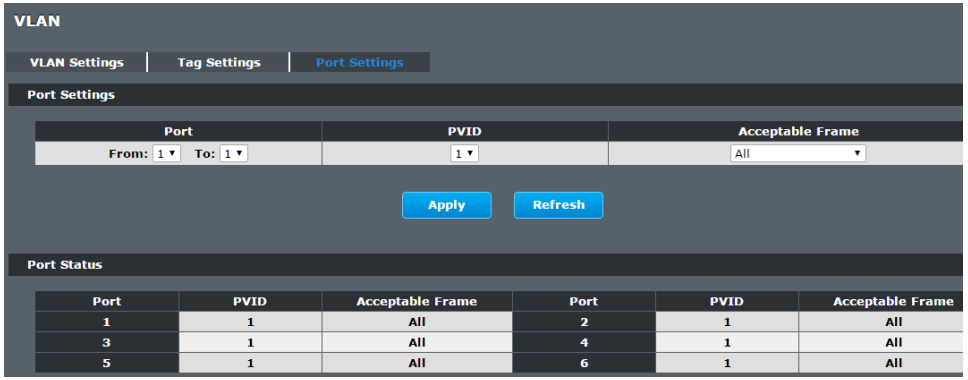


Parameter	Description
VLAN ID	Select a VLAN ID to configure its port tagging settings.
Tag Port	Selecting a port which is a member of the selected VLAN ID will make it a tag port. This means the port will tag all outgoing frames transmitted with the VLAN ID.
Select All	Click **Select All** to mark all member ports as tag ports.
Deselect All	Click **Deselect All** to mark all member ports as untag ports.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Tag Status	
VLAN ID	This field displays the VLAN ID.
Tag Ports	This field displays the ports that have been assigned as tag ports.

Untag Ports	This field displays the ports that have been assigned as untag ports.

Port Settings

Advanced Settings > VLAN > VLAN > Port Settings



Parameter	Description
Port	Select a port number to configure from the drop-down box. Select **All** to configure all ports at the same time.
PVID	Select a **PVID** (Port VLAN ID number) from the drop-down box.
Acceptable Frame	Specify the type of frames allowed on a port. Choices are **All**, **VLAN Untagged Only** or **VLAN Tagged Only**. - Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. - Select **VLAN Tagged Only** to accept only tagged frames on this port. All untagged frames will be dropped. - Select **VLAN Untagged Only** to accept only untagged frames on this port. All tagged frames will be dropped.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

Port Status	
Port	This field displays the port number.
PVID	This field displays the Port VLAN ID number.
Acceptable Frame	This field displays the type of frames allowed on the port. This will either display **All** or **VLAN Tagged Only or VLAN Untagged Only.**

MAC-based VLAN

The MAC base VLAN allows users to create VLAN with MAC address. The MAC address can be the leading three or more bytes of the MAC address.

For example, 00:01:02 or 00:03:04:05 or 00:01:02:03:04:05.

When the Switch receives packets, it will compare MAC-based VLAN configures. If the SA is matched the MAC-based VLAN configures, the Switch replace the VLAN with user configured and them forward them.

For example:

Configurations: 00:01:02, VLAN=23, Priority=2.

The packets with SA=00:01:02:xx:xx:xx will be forwarded to VLAN 22 member ports.

Notices: The 802.1Q port base VLAN should be created first.

CLI Configuration

Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan VLANID priority <0-7>	This command creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.

configure	no mac-vlan entry STRINGS	This command deletes a mac-vlan entry.
configure	no mac-vlan all	This command deletes all of the mac-vlan entries.

Example:

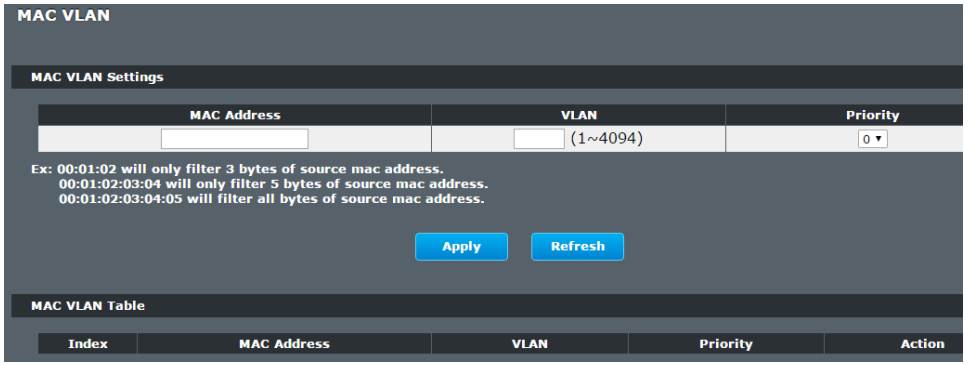
TI-PG541I(config)#mac-vlan 00:01:02:03:04 vlan 111 priority 1

TI-PG541I(config)#mac-vlan 00:01:02:22:04 vlan 121 priority 1

TI-PG541I(config)#mac-vlan 00:01:22:22:04:05 vlan 221 priority 1

Web Configuration

Advanced Settings > VLAN > MAC VLAN



Parameter	Description
MAC Address	Configures the leading three or more bytes of the MAC address.
VLAN	Configures the VLAN.
Priority	Configures the 802.1Q priority.
Action	Click the "Delete" button to delete the protocol VLAN profile.

EEE (Energy Efficient Ethernet)

The Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

Notice: This feature is for Ethernet copper ports only.

Default Settings

All ports' EEE states are disabled.

CLI Configuration

Node	Command	Description
enable	show interface [IFNAME]	This command displays the current port configurations.
interface	power efficient-ethernet auto	The command enables EEE on the specified interface. When EEE is enabled, the device advertises and auto negotiates EEE to its link partner.
interface	no power efficient-ethernet auto	The command disables EEE on the specified interface.

Example:

TI-PG541I#*configure terminal*

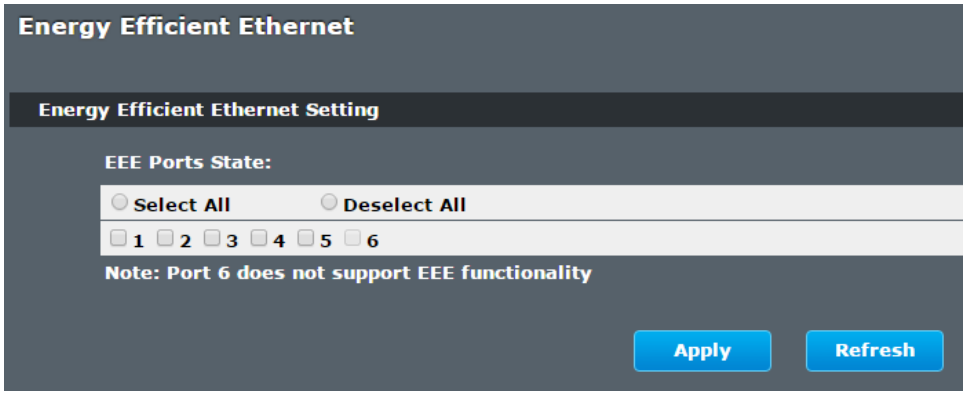
TI-PG541I(config-if)#interface gigabitethernet1/0/1

TI-PG541I(config-if)#power efficient-ethernet auto

TI-PG541I(config-if)#no power efficient-ethernet auto

Web Configuration

Advanced Settings > EEE



Parameter	Description
EEE Port State	Click a port to enable IEEE 802.3az Energy Efficient Ethernet on that port.
Select All	Click this to enable IEEE 802.3az Energy Efficient Ethernet across all ports.
Deselect All	Click this to disable IEEE 802.3az Energy Efficient Ethernet across all ports.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.

Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802® LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Default Settings

The LLDP on the Switch is disabled.

Tx Interval : 30 seconds.
Tx Hold : 4 times.
Time To Live : 120 seconds.

Port	Status	Port	Status
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable

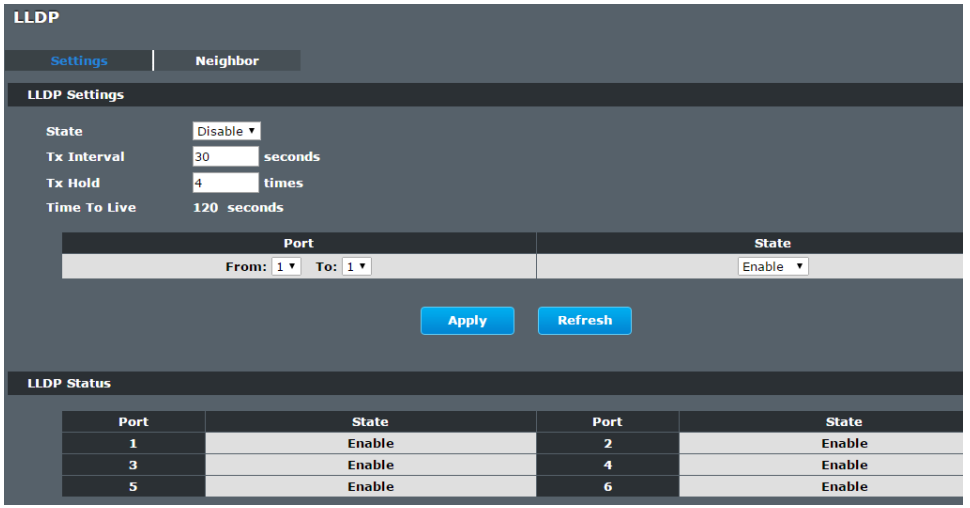
CLI Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all of the ports' neighbor information.

configure	lldp (disable|enable)	This command globally enables / disables the LLDP function on the Switch.
configure	lldp tx-interval	This command configures the interval to transmit the LLDP packets.
configure	lldp tx-hold	This command configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
interface	lldp-agent (disable|enable|rx-only|tx-only)	This command 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.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.

Web Configuration

Advanced Settings > LLDP > Settings

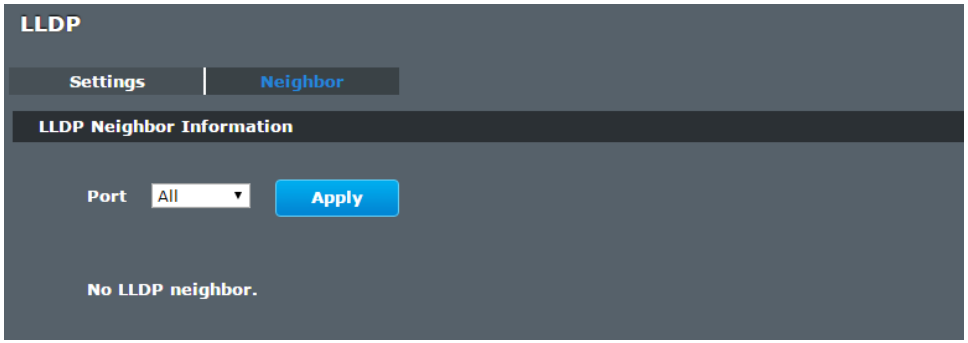


Parameter	Description
State	Globally enables / disables the LLDP on the Switch.
Tx Interval	Configures the interval to transmit the LLDP packets.
Tx Hold	Configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
Time To Live	The hold time for the Switch's information.
Port	The port range which you want to configure.
State	Enables / disables the LLDP on these ports.
LLDP Status	
Port	The Port ID.

State	The LLDP state for the specific port.

Neighbor

Advanced Settings > LLDP > Neighbor



Parameter	Description
Port	Select the port(s) which you want to display the port's neighbor information.
Local Port	The local port ID.
Remote Port ID	The connected port ID.
Chassis ID	The neighbor's chassis ID.
System Name	The neighbor's system name.
System Description	The neighbor's system description.
System Capabilities	The neighbor's capability.
Management Address	The neighbor's management address.
Time To Live	The hold time for the neighbor's information.

PoE (Power over Ethernet)

Power over Ethernet or **PoE** technology describes a system to pass electrical power safely, along with data, on Ethernet cabling. PoE requires category 5 cable or higher for high power levels, but can operate with category 3 cable for low power levels. Power can come from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a midspan power supply.

The original **IEEE 802.3af-2003** PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.

The updated **IEEE 802.3at-2009** PoE standard also known as **PoE+** or **PoE plus**, provides up to 25.5 W of power. Some vendors have announced products that claim to comply with the 802.3at standard and offer up to 51 W of power over a single cable by utilizing all four pairs in the Cat.5 cable. Numerous non-standard schemes had been used prior to PoE standardization to provide power over Ethernet cabling. Some are still in active use.

PSE: Power sourcing equipment (PSE) is a device such as a switch that provides ("sources") power on the Ethernet cable.

PD: A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through a 10/100 Mbps Ethernet port.

Standard PoE parameters and comparison

Property	802.3af (802.3at Type 1)	802.3at Type 2
Power available at PD	12.95 W	25.50 W per mode
Maximum power delivered by	15.40 W	30.00 W per mode
PSE		
Voltage range (at PSE)	44.0 - 57.0 V	50.0 - 57.0 V
Voltage range (at PD)	37.0 - 57.0 V	42.5 - 57.0 V
Maximum current	350 mA	600 mA per mode
Maximum cable resistance	20 Ω (Category 3)	12.5 Ω (Category 5)
Power management	Three power class levels negotiated at initial connection	Four power class levels negotiated at initial connection or 0.1 W steps negotiated continuously
Dreading of maximum cable ambient operating temperature	None	5°C with one mode (two pairs) active, 10°C with two modes (four pairs) simultaneously active
Supported cabling	Category 3 and Category 5	Category 5
Supported modes	Mode A (endspan), Mode B (midspan)	Mode A, Mode B, Mode A and Mode B operating simultaneously

Power Devices

Class	Usage	Power levels available: Classification current [mA]	Power range [Watt]	Class description
0	Default	0 - 4	0.44 - 12.94	Classification unimplemented
1	Optional	9 - 12	0.44 - 3.84	Very Low power
2	Optional	17 - 20	3.84 - 6.49	Low power
3	Optional	26 - 30	6.49 - 12.95	Mid power
4	Reserved	36 - 44	12.95 - 25.50	High power

For IEEE 802.3at (type 2) devices class 4 instead of Reserved has a power range of 12.95 - 25.5 W.

PoE Specification

The port 1 ~ 4 supports the PoE function.

Total-power: The maximum power which the switch can support to the PDs.

Schedule: The Switch allows user to arrange a week schedule to enable or disable the PoE for the specific ports.

Default Settings

State : Disabled
Total Power(W) : 0

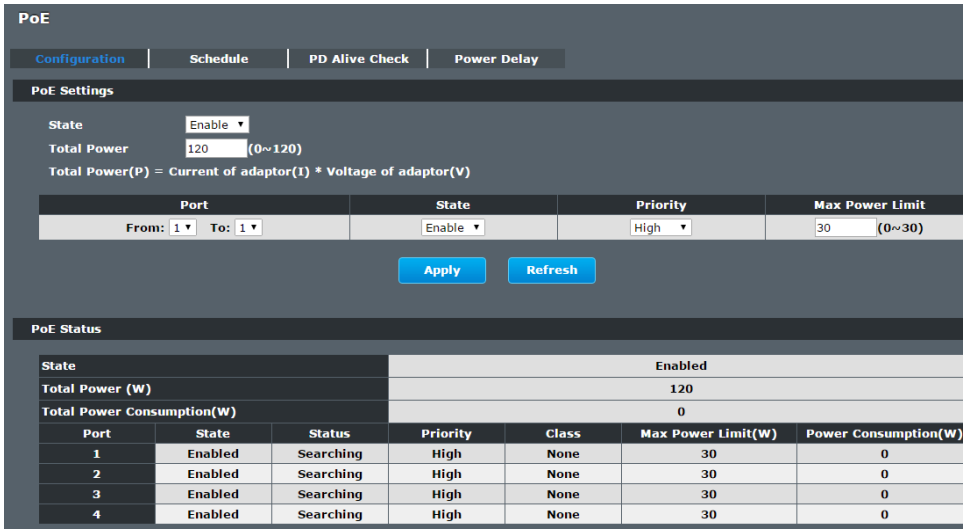
Port	State	Status	Priority
1	Disabled	Disabled	High
2	Disabled	Disabled	High
3	Disabled	Disabled	High
4	Disabled	Disabled	High

CLI Configuration

Node	Command	Description
enable	show poe	This command displays the PoE configurations and status.
enable	show poe schedule port PORT_ID	This command displays the PoE port schedule configurations.
configure	poe (disable | enable)	This command disables or enables the global PoE for the Switch.
configure	poe total-power	This command configures the total power which the Switch can support.
interface	poe (disable|enable)	This command enables or disables the PoE function on the specific port.
interface	poe priority (critical|high|low)	This command configures the priority of the PoE function for the specific port. ● critical : The highest priority. ● high : The middle priority. ● low : The lowest priority.

Web Configuration

Advanced Settings > PoE > Configuration



Parameter	Description
PoE Mode	Selects the PoE mode, classification or consumption. **Classification** - Allocated power according to class (0 to 4). **Consumption** - Allocated power according to the actual need of each PD.
Port	Selects a port or a range of ports that you want to configure the PoE function.
State	Selects **Enable** to enable the PoE function on the specific port. Selects **Disable** to disable the PoE function on the specific port.
Priority	Selects **Critical / High / Low** priority for the specific port.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

PoE Mode	Displays the current PoE mode.
Total Power	Displays the total power that the Switch supports.
Total Consuming Power	Displays the total consuming power for all of the PDs.
External Power Module	Displays the status of the external power module.
Port	Display the Port No.
State	Displays the PoE state for the specific port.
PD Priority	Displays the PoE priority for the specific port.
Class	The field displays the class mode which the PSE negotiate with the PD on the specific port.
Consuming Power(mW)	Displays the consuming power for the specific port.
Power Allocated(mW)	Displays the power allocated for the specific port.
Current Status(mA)	Displays the current status for the specific port.

PoE Schedule

The function has a global *state* configuration. If the global state configuration is disabled. The Switch will not perform the schedule function. If the global state is enabled, the Switch will check every port's configurations.

If the port's *check* configuration is NO for a specific day, the Switch will not perform action for the specific port. If the port's *check* configuration is YES for a specific day, the Switch will check the *Start time* and *End Time*. If the current time is in the interval between *Start time* and *End Time,* the Switch will perform the *action* configuration. If the *action* is ENABLE, the Switch will send power to the port. If the current time is not in the interval between *Start time* and *End Time,* the Switch will not send power to the port.

Port:

Schedule State: Disabled

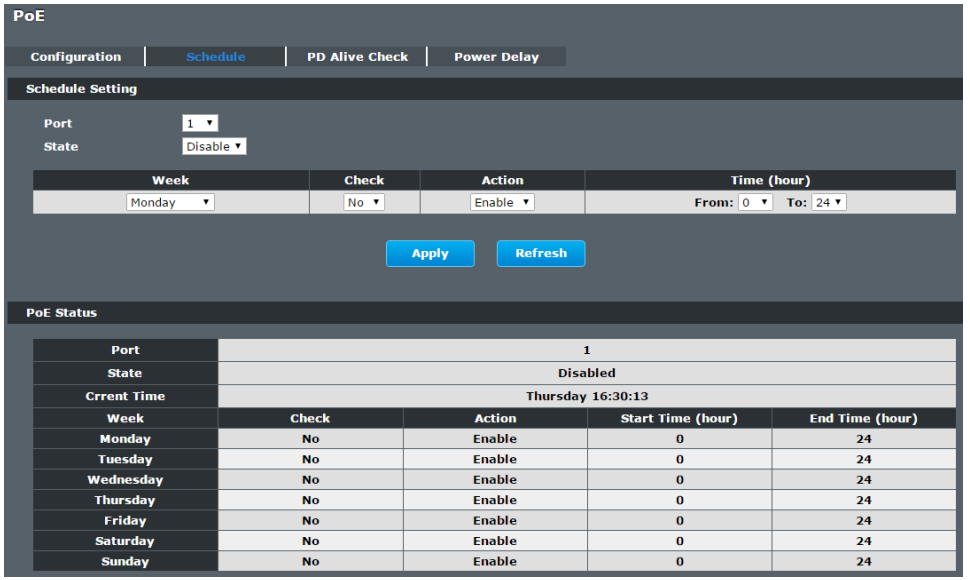
Week	Check	Action	Start Time(hour)	End Time(hour)
Monday	No	Enable	0	24
Tuesday	No	Enable	0	24
Wednesday	No	Enable	0	24
Thursday	No	Enable	0	24
Friday	No	Enable	0	24
Saturday	No	Enable	0	24
Sunday	No	Enable	0	24

CLI Configuration

Node	Command	Description
enable	show poe schedule port PORT_ID	This command displays the PoE port schedule configurations.
interface	poe schedule (disable|enable)	This command disables or enables the PoE schedule on the specific port.
interface	poe schedule week (Sun|Mon|Tue|Wed|Thu|Fri|Sat) check (yes|no)	This command enables or disables the PoE schedule on the specific day.
interface	poe schedule week (Sun|Mon|Tue|Wed|Thu|Fri|Sat) start-time VALUE end-time VALUE action (enable|disable)	This command configures the PoE schedule start-time and end-time on a specific day on the specific port. Users can enable or disable the PoE on the time period.

Web Configuration

Advanced Settings > PoE > Schedule



Parameter	Description
Port	Selects a port that you want to configure the PoE schedule function.
Week	Select a week day that you want to configure the schedule.
Check	Enables or Disables the PoE schedule on the specific port for a defined time period.
Time (Hour)	

PD Alive Check

The function has a global *state* configuration. If the global state configuration is enabled. The Switch will check the configurations of every port.

If the port's *state* is enabled, the Switch will send keep-a-live probe packet every *interval* time. If the host cannot respond when the keep-a-live probe packet count is over the *retry times*, the Switch performs the *action, reboot/alarm/all* to the Power Device, depending on the port's configuration.

Power OFF Time (sec):

When PD has been rebooted, the PoE port restored power after the specified time.

Default:15, range: 3-120 sec.

Start up Time (sec):

When PD has been start up, the Switch will wait Start up time to do PoE Auto Checking. Default: 60, range: 30-600 sec.

Interval Time (sec):

Device will send checking message to PD each interval time.

Default: 30, range: 10-120 sec.

Action:

The action when the failure detection.

All: Send an alarm message to inform the administrator and then reboot the PD.

Alarm: Just send an alarm message to inform the administrator.

None: Keep Ping the remote PD but does nothing further.

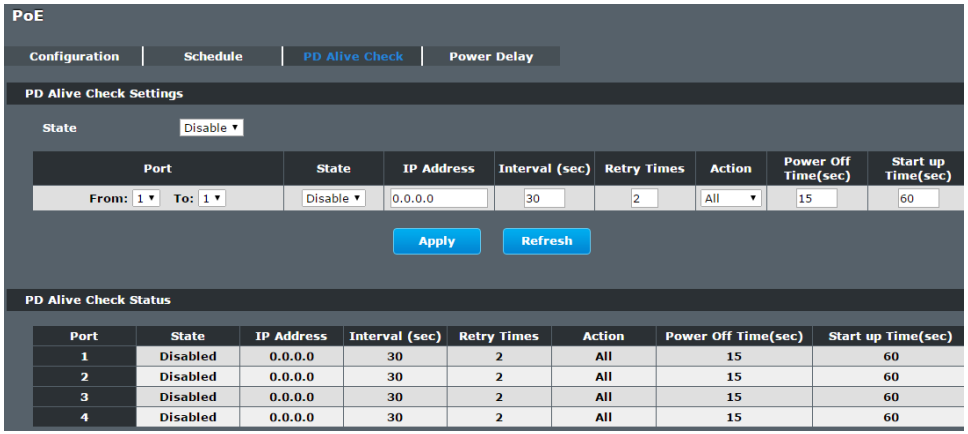
Reboot: Cut off the power of the PoE port, make PD rebooted.

CLI Configuration

Node	Command	Description
enable	show pd-alive	This command displays the configuration of the PD Alive Check.
configure	pd-alive (disable|enable)	This command disables or enables the global PD Alive Check for the Switch.
Interface	pd-alive action (reboot|alarm|all|none)	This command configures the action when the system detects that the host cannot respond the keep-a-live probe packet.
Interface	pd-alive interval VALUE	This command configures the interval to send the keep-a-live probe packets to check if the host is still alive for the specific port.
Interface	pd-alive ip IP_ADDR	This command configures the Host IP address which connects to the specific port.
Interface	pd-alive retry-time VALUE	This command configures the retry times when no response from the host for the keep-a-live probe packet for the specific port.
Interface	pd-alive power-off-time VALUE startup-time VALUE	This command configures the power-off time and startup time.

Web Configuration

Advanced Settings > PoE > PD Alive Check



Parameter	Description
State	Enables/Disables the PD Alive Check.
Port	Selects a port or a range of ports which you want to configure.
State	Enables/Disables the PD Alive Check for the specific port(s).
IP Address	Specifies the Host IP address which connects to the port.
Interval	The interval to send the packet probes to check if the host is still alive.
Retry Time	The retry times when no response from the host for the keep-a-live probe packet.
Action	The action to the Power Device when the system detects that the Power Device cannot respond the keep-a-live probe packet. The options have Reboot / Alarm / All /None.
Power Off Time	When PD has been rebooted, the PoE port restored power after the Power Off Time time.
Start Up Time	The Switch waits the Start Up Time to do PoE Auto Checking when the PD is rebooting.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

Power Delay

The Power Delay allows the user to setting the delay time of power providing after device rebooted.

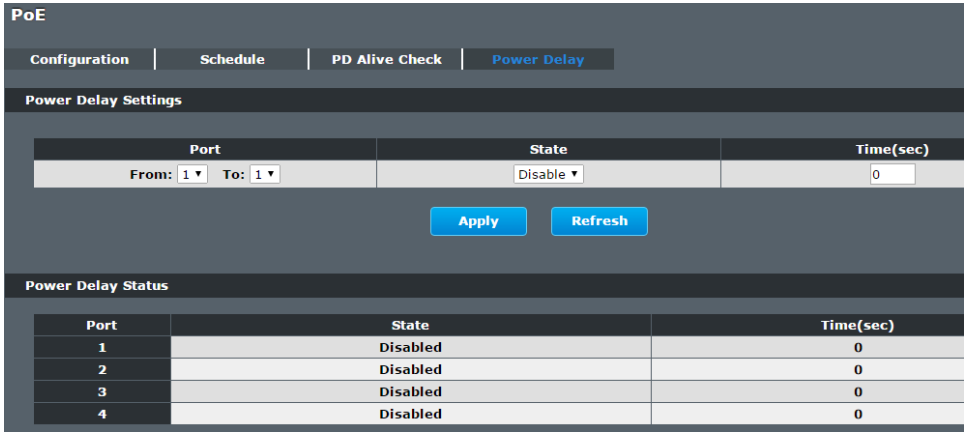
CLI Configuration

Node	Command	Description
enable	show poe power-delay	This command displays the PoE power delay configurations.
interface	poe power-delay (enable|disable)	This command enables / disables of the Power Delay function for the specific port.
interface	poe power-delay time VALUE	This command configures the delay time of the Power Delay for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	poe power-delay (enable|disable)	This command enables / disables of the Power Delay function for the range of ports.

if-range	poe power-delay time VALUE	This command configures the delay time of the Power Delay for the range of ports.

Web Configuration

Advanced Settings > PoE > Power Delay



Parameter	Description
Port	Selects a port or a range of ports which you want to configure.
State	Enables/Disables the PoE Power Delay for the specific ports.
Time	The delay time for the specific ports.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Power Delay Status	
Port	The port ID.
State	The PoE power delay state for the port.
Time	The PoE power delay time for the port.

Notice: The high priority port should have low value for power delay.

Monitor

Alarm

The feature displays if there are any abnormal situation need process immediately.

Notice: The Alarm DIP Switch allow users to configure if send alarm message when the corresponding event occurs.

For Example:

P1: ON, The Switch will send alarm message when port 1 is link down.

PWR: ON, The Switch will send alarm message when the main power supply disconnect.

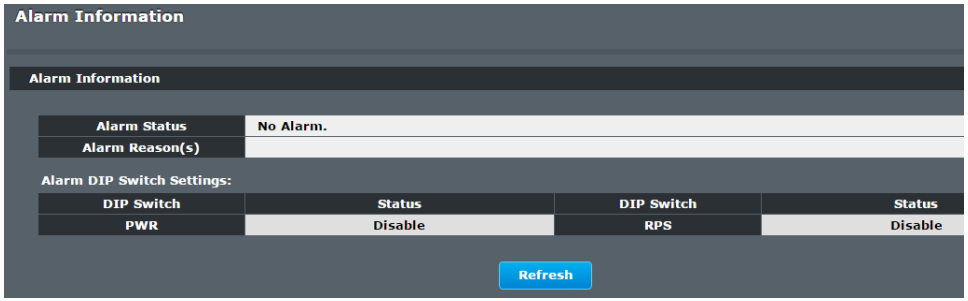
RPS: ON, The Switch will send alarm message when the redundant power supply disconnect.

CLI Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

Web Configuration

Monitor > Alarm



Parameter	Description
Alarm Information	
Alarm Status	This field indicates if there is any alarm events.
Alarm Reason(s)	This field displays all of the detail alarm events.
Alarm DIP Switch Settings	
DIP Switch	The field displays the DIP Switch name.
Status	The field indicates the DIP Switch current status.

Port Statistics

This feature helps users to monitor the ports' statistics, to display the link up ports' traffic utilization only.

CLI Configuration

Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

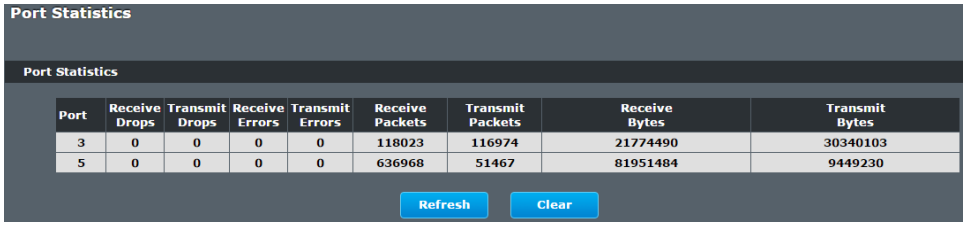
Example:

TI-PG541I#show port-statistics

	Packets		Bytes		Errors		Drops	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
3	1154	2	108519	1188	0	0	0	0

Web Configuration

Monitor > Port Statistics



Parameter	Description
Port	Select a port or a range of ports to display their statistics.
Rx Packets	The field displays the received packet count.
Tx Packets	The field displays the transmitted packet count.
Rx Bytes	The field displays the received byte count.
Tx Bytes	The field displays the transmitted byte count.
Rx Errors	The field displays the received error count.
Tx Errors	The field displays the transmitted error count.
Rx Drops	The field displays the received drop count.
Tx Drops	The field displays the transmitted drop count.
Refresh	Click this button to refresh the screen quickly.

Port Utilization

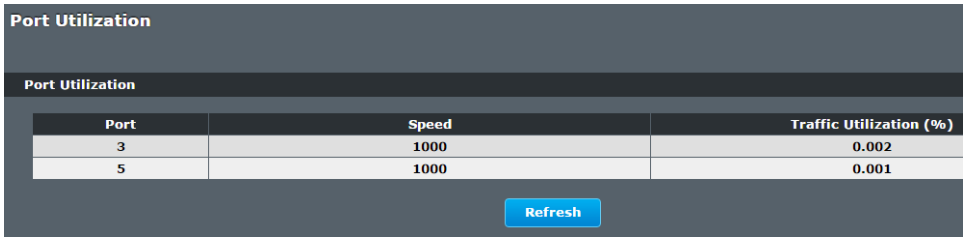
This feature helps users to monitor the ports' traffic utilization, to display the link up ports' traffic utilization only.

CLI Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

Web Configuration

Monitor > Port Utilization



Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Speed	The current port speed.
Utilization	The port traffic utilization.
Refresh	Click this button to refresh the screen quickly.

RMON Statistics

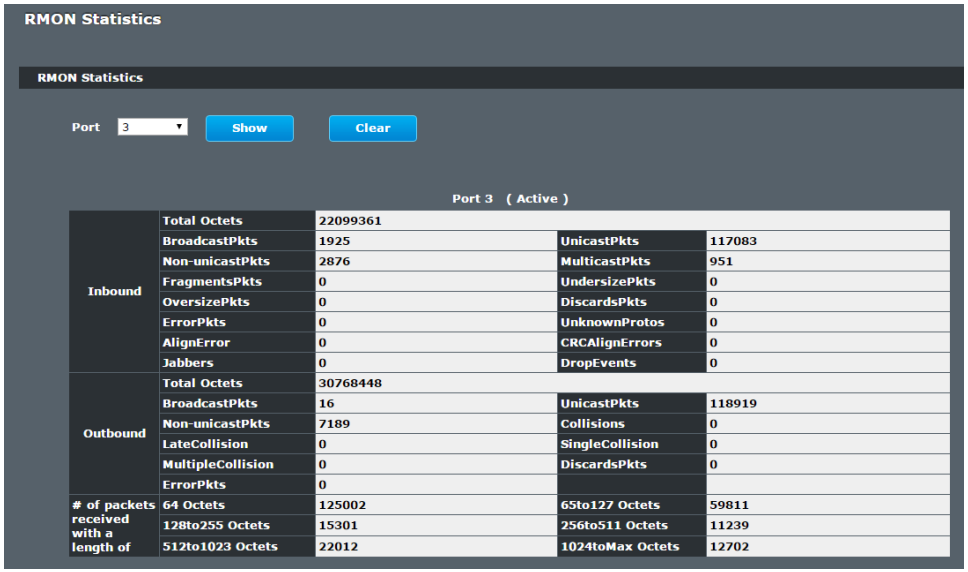
This feature helps users to monitor or clear the port's RMON statistics.

CLI Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears one port's or all ports' RMON statistics.

Web Configuration

Monitor > RMON Statistics



Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Show	Show them.
Clear	Clear the RMON statistics for the port or a range of ports.

Traffic Monitor

The function can be enabled / disabled on a specific port or globally be enabled disabled on the Switch.

The function will monitor the broadcast / multicast / broadcast and multicast packets rate. If the packet rate is over the user's specification, the port will be blocked. And if the recovery function is enabled, the port will be enabled after recovery time.

Default Settings

Port	State	Packet Status	Packet Type	Rate(pps)	Recovery State	Time(min)
1	Disabled	Normal	Bcast	1000	Enabled	1
2	Disabled	Normal	Bcast	1000	Enabled	1
3	Disabled	Normal	Bcast	1000	Enabled	1
4	Disabled	Normal	Bcast	1000	Enabled	1
5	Disabled	Normal	Bcast	1000	Enabled	1
6	Disabled	Normal	Bcast	1000	Enabled	1

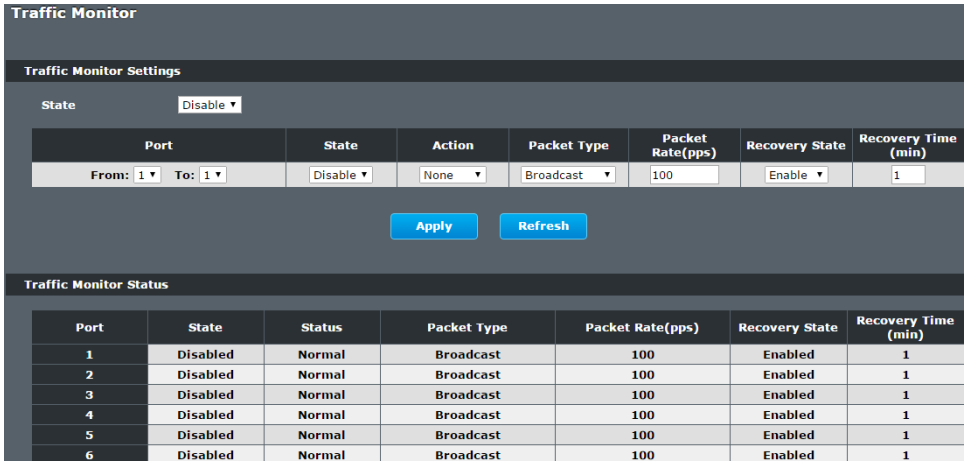
CLI Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the traffic monitor configurations and current status.
configure	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the Switch.
interface	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the port.
interface	traffic-monitor rate RATE_LIMIT type (bcast|mcast|bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet. mcast – Multicast packet.

interface	traffic-monitor recovery (disable|enable)	This command enables / disables the recovery function for the traffic monitor on the port.
interface	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the port.
if-range	traffic-monitor rate RATE_LIMIT type (bcast|mcast|bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet. mcast – Multicast packet.
if-range	traffic-monitor recovery (disable|enable)	This command enables / disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.

Web Configuration

Monitor > Traffic Monitor



Parameter	Description
State	Globally enables / disables the traffic monitor function.
Port	The port range which you want to configure.
State	Enables / disables the traffic monitor function on these ports.
Action	Unblock these ports.
Packet Type	Specify the packet type which you want to monitor.
Packet Rate	Specify the packet rate which you want to monitor.
Recover State	Enables / disables the recovery function for the traffic monitor function on these ports.
Recovery Time	Configures the recovery time for the traffic monitor function on these ports.(Range: 1 – 60 minutes)

Management

SNMP

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Support below MIBs:

- RFC 1157 A Simple Network Management Protocol
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 Ethernet Interface MIB
- RFC 1757 RMON Group 1,2,3,9

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is "public" for both SNMP v1 and SNMP v2c before SNMP v3 is enabled. Once SNMP v3 is enabled, the communities of SNMP v1 and v2c have to be unique and cannot be shared.

Network ID of Trusted Host:

The IP address is a combination of the Network ID and the Host ID.

Network ID = (Host IP & Mask).

User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0

Note: Allow user to configure the community string and rights only.

User configures the Community String and the Rights and the Network ID of Trusted Host=0.0.0.0, Subnet Mask=0.0.0.0. It means that all hosts with the community string can access the Switch.

Default Settings

- SNMP : disabled.
- System Location : TI-PG541I. (Maximum length 64 characters)
- System Contact : None. (Maximum length 64 characters)
- System Name : None. (Maximum length 64characters)
- Trap Receiver : None.
- Community Name : None.
- The maximum entry for community : 3.
- The maximum entry for trap receiver : 5.

CLI Configuration

Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro|rw) trusted-host IPADDR	This command configures the SNMP community name.
configure	snmp (disable|enable)	This command disables/enables the SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command configures a name for the system. (The System Name is same as the host name)

configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver's configurations, including the IP address, version (v1 or v2c) and community.

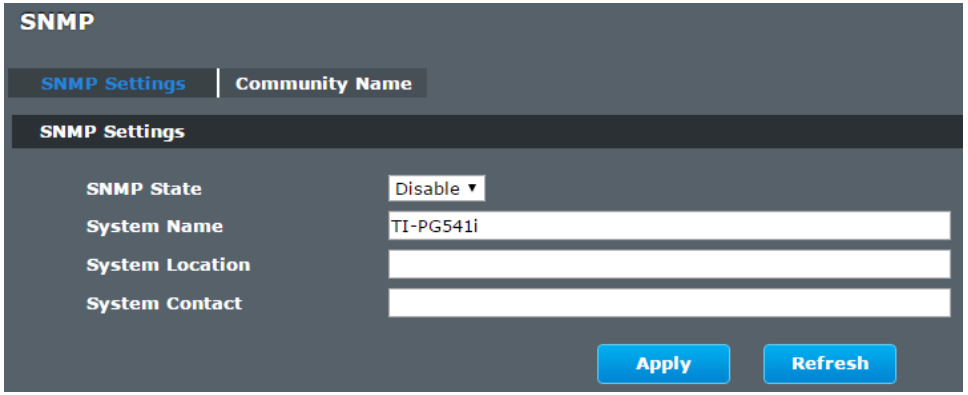
Example:

TI-PG541I#configure terminal
TI-PG541I(config)#snmp enable
TI-PG541I(config)#snmp community public rw trusted-host 192.168.200.106/24
TI-PG541I(config)#snmp trap-receiver 192.168.200.106 v2c public
TI-PG541I(config)#snmp system-contact IT engineer
TI-PG541I(config)#snmp system-location Branch-Office

Web Configuration

SNMP Setting

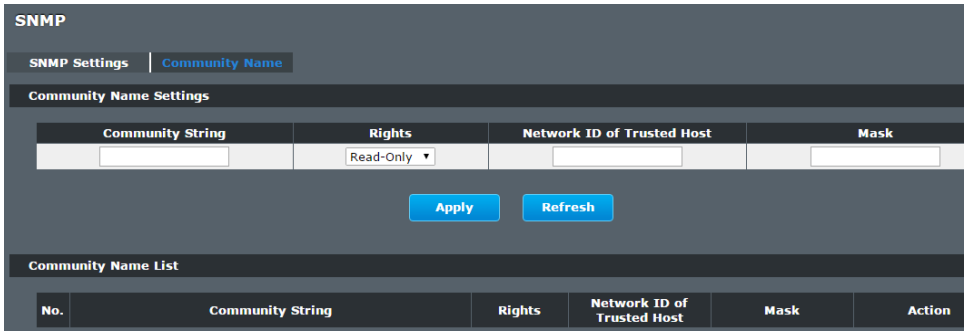
Management > SNMP > SNMP > SNMP Settings



Parameter	Description
SNMP State	Select **Enable** to activate SNMP on the Switch. Select **Disable** to not use SNMP on the Switch.
System Name	Type a System Name for the Switch. (The System Name is same as the host name)
System Location	Type a System Location for the Switch.
System Contact	Type a System Contact for the Switch.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.

Community Name

Management > SNMP > SNMP > Community Name



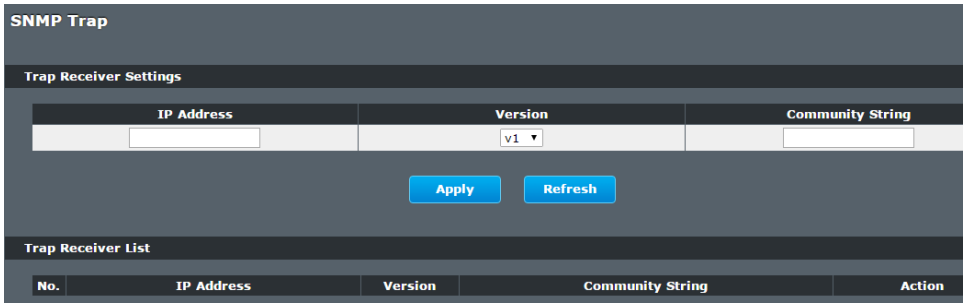
Parameter	Description
Community String	Enter a Community string, this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.

Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example 255.255.255.0.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Community Name List	
No.	This field indicates the community number. It is used for identification only. Click on the individual community number to edit the community settings.
Community String	This field displays the SNMP community string. An SNMP community string is a text string that acts as a password.
Right	This field displays the community string's rights. This will be **Read Only** or **Read Write**.
Network ID of Trusted Host	This field displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Subnet Mask	This field displays the subnet mask for the IP address of the remote SNMP management station.
Action	Click **Delete** to remove a specific Community String.

SNMP Trap

Web Configuration

Management > SNMP > SNMP Trap



Parameter	Description
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. **v1** or **v2c**.
Community String	Specify the community string used with this remote trap station.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Trap Receiver List	
No.	This field displays the index number of the trap receiver entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the remote trap station.
Version	This field displays the version of Simple Network Management Protocol in use. **v1** or **v2c**.

Community String	This field displays the community string used with this remote trap station.
Action	Click **Delete** to remove a configured trap receiver station.

Mail Alarm

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

- System Reboot : The system warn start or cold start.
- Port Link Change : A port link up or down.
- Configuration Change : The system configurations in the NV-RAM have been updated.
- Firmware Upgrade : The system firmware image has been updated.
- User Login : A user login the system.
- Port Blocked : A port is blocked by looping detection or BPDU Guard.

Default Settings

Mail-Alarm Configuration:

State : Disabled.
Server IP : 0.0.0.0
Server Port : 25
Mail From :
Mail To :

Trap Event Status:

System Reboot : Disabled.
Port Link Change : Disabled.
Configuration Change : Disabled.
Firmware Upgrade : Disabled.
User Login : Disabled.
Port Blocked : Disabled.
Alarm : Disabled.

Reference

Default Ports	Server	Authentication	Port
SMTP Server (Outgoing Messages)	Non-Encrypted	AUTH	25 (or 587)
	Secure (TLS)	StartTLS	587
	Secure (SSL)	SSL	465
POP3 Server (Incoming Messages)	Non-Encrypted	AUTH	110
	Secure (SSL)	SSL	995
Googlemail - Gmail	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.gmail.com	SSL	465
	smtp.gmail.com	StartTLS	587
POP3 Server (Incoming Messages)	pop.gmail.com	SSL	995
Outlook.com	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.live.com	StartTLS	587
POP3 Server (Incoming Messages)	pop3.live.com	SSL	995
Yahoo Mail	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.mail.yahoo.com	SSL	465

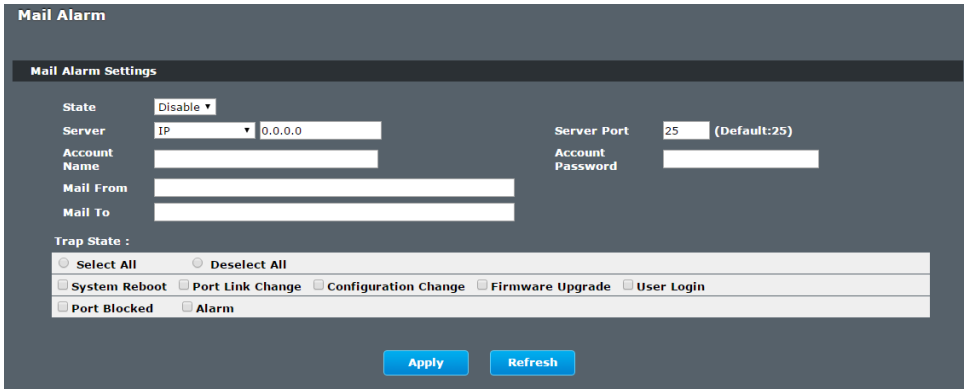
POP3 Server (Incoming Messages)	pop.mail.yahoo.com	SSL	995
Yahoo Mail Plus	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	plus.smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	plus.pop.mail.yahoo.com	SSL	995

CLI Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the Mail Alarm configurations.
configure	mail-alarm (disable|enable)	This command disables / enables the Mail Alarm function.
configure	mail-alarm auth-account	This command configures the Mail server authentication account.
configure	mail-alarm mail-from	This command configures the mail sender.
configure	mail-alarm mail-to	This command configures the mail receiver.
configure	mail-alarm server-ip IPADDR server-port VALUE	This command configures the mail server IP address and the TCP port.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the mail server IP address and configures 25 as the server's TCP port.
configure	mail-alarm trap-event (reboot|link-change|config.| firmware|login|port-blocked| alarm) (disable|enable)	This command disables / enables mail trap events.

Web Configuration

Management > Mail Alarm



Parameter	Description
State	Enable / disable the Mail Alarm function.
Server IP	Specifies the mail server's IP address.
Server Port	Specifies the TCP port for the SMTP.
Account Name	Specifies the mail account name.
Account Password	Specifies the mail account password.
Mail From	Specifies the mail sender.
Mail To	Specifies the mail receiver.
Trap State	Enables / disables the mail trap event states.

Maintenance

CLI Configuration

Node	Command	Description
enable	show config-change-status	This command displays the configurations status if there are default values.
configure	reboot	This command reboots the system.
configure	reload default-config	This command copies a default-config file to replace the current one. **Note:** The system will reboot automatically to take effect the configurations.
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP 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
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server.
configure	archive download-fw <URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP 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

Example:

TI-PG541I#*configure terminal*

TI-PG541I(config)#*interface eth0*

TI-PG541I(config-if)#*ip address 172.20.1.101/24*

TI-PG541I(config-if)#*ip address default-gateway 172.20.1.1*

TI-PG541I(config-if)#*management vlan 1*

Enable the DHCP client function for the switch.

- TI-PG541I#*configure terminal*
- TI-PG541I(config)#*interface eth0*
- TI-PG541I(config-if)#*ip dhcp client enable*

TI-PG541I#show config-change-status

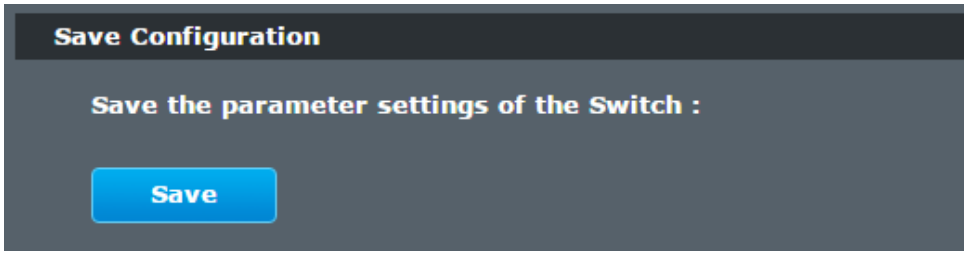
The user configuration file is default.

The configurations have been modified.

Web Configuration

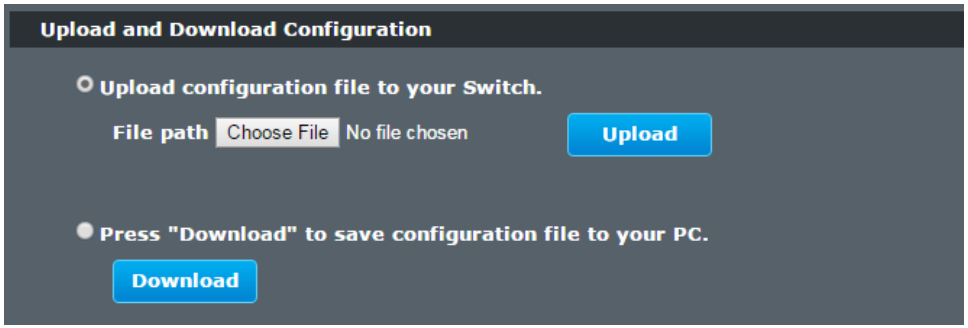
Management > Maintenance > Configuration

Save Configuration



Press the Save button to save the current settings to the NV-RAM (flash).

Upload / Download Configuration to /from a your server



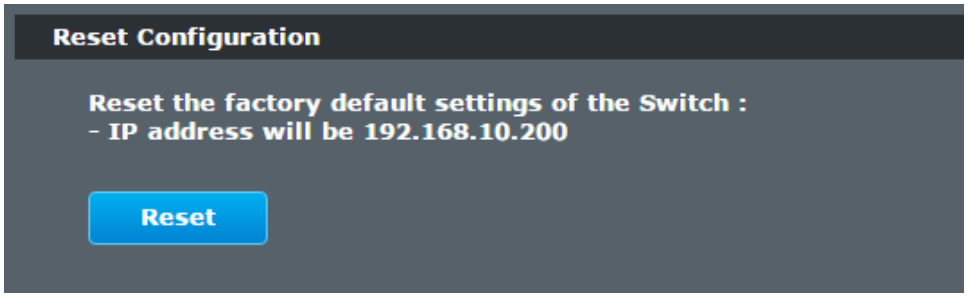
Follow the steps below to save the configuration file to your PC.

- Select the "Press "Download" to save configurations file to your PC".
- Click the "Download" button to start the process.

Follow the steps below to load the configuration file from your PC to the Switch.

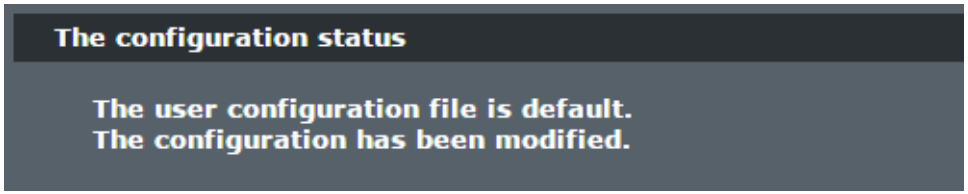
- Select the "Upload configurations file to your Switch".
- Select the full path to your configuration file.
- Click the Upload button to start the process.

Reset the factory default settings of the Switch



Press the Reset button to set the settings to factory default configuration.

The configuration status



Display the configuration status of recorded in the NV-RAM.

Notice:

If the user has changed any configurations, the message displays "The configurations have been modified!" Otherwise, the message "The configurations are default values."

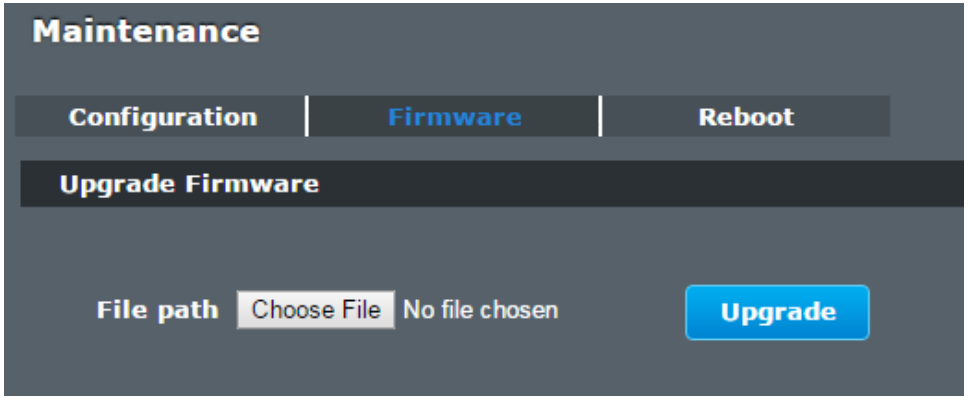
There are two conditions will change message from "The configurations have been modified!" to "The configurations are default values."

1. Click "Reset configuration" in web management or do cli command, reload default-config.
2. Click "Upload configuration" in web management or do cli command, "archive download-config xxx".

Firmware

Management > Maintenance > Firmware

Type the path and file name of the firmware file you wish to upload to the Switch in the **File path** text box or click **Browse** to locate it. Click **Upgrade** to load the new firmware.

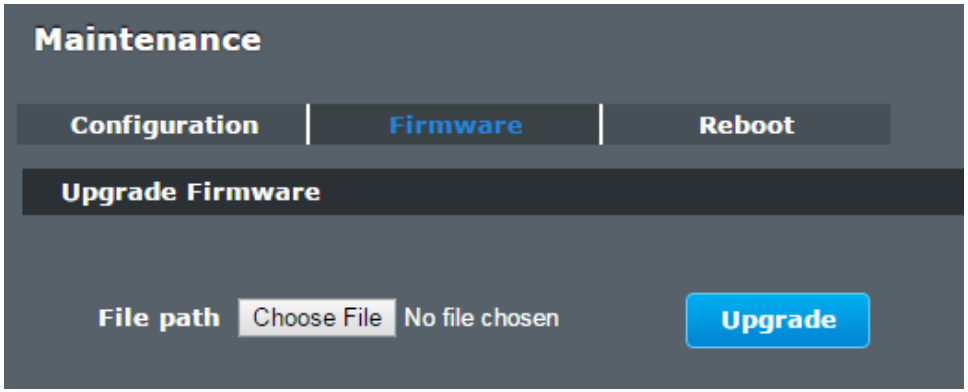


Reboot

Management > Maintenance > Reboot

Reboot allows you to restart the Switch without physically turning the power off.

Follow the steps below to reboot the Switch.



- In the **Reboot** screen, click the **Reboot** button. The following screen displays.

- Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

System Log

The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, **Alert / Critical / Error / Warning / Notice / Information.** The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the Switch file system. If the syslog server's IP address has been configured, the Switch will send a copy to the syslog server.

The log message file is limited in 4KB size. If the file is full, the oldest one will be replaced.

CLI Configuration

Node	Command	Description
enable	show syslog	The command displays the entire log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.

enable	show syslog server	The command displays the syslog server configurations.
configure	syslog (disable|enable)	The command disables / enables the syslog function.
configure	syslog ip IPADDR	The command configures the syslog server's IP address.

Example:

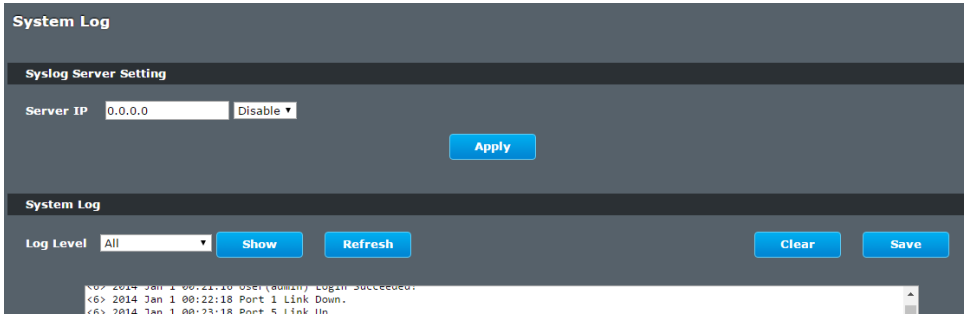
TI-PG541I#configure terminal

TI-PG541I(config)#syslog-server ipv4-ip 192.168.200.106

TI-PG541I(config)#syslog-server enable

Web Configuration

Management > System Log



Parameter	Description
Server IP	Enter the Syslog server IP address in dotted decimal notation. For example, 192.168.1.1. Select **Enable** to activate switch sent log message to Syslog server when any new log message occurred.
Log Level	Select **Alert/Critical/Error/Warning/Notice/Information** to choose which log message to want see.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

User Account

The Switch allows users to create up to 6 user account. The user name and the password should be the combination of the digit or the alphabet. The last admin user account cannot be deleted. Users should input a valid user account to login the CLI or web management.

User Authority:

The Switch supports two types of the user account, admin and normal. The **default** user's account is **username (admin) / password (admin)**.

- admin - read / write.
- normal - read only.

; Cannot enter the privileged mode in CLI.

; Cannot apply any configurations in web.

The Switch also supports backdoor user account. In case of that user forgot their user name or password, the Switch can generate a backdoor account with the system's MAC. Users can use the new user account to enter the Switch and then create a new user account.

Default Settings

Maximum user account : 6.

Maximum user name length : 32.

Maximum password length : 32.

Default user account for privileged mode : admin / admin.

Notices

The Switch allows users to create up to 6 user account.

The user name and the password should be the combination of the digit or the alphabet.

The last admin user account cannot be deleted.

The maximum length of the username and password is 32 characters.

CLI Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal|admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

Example:

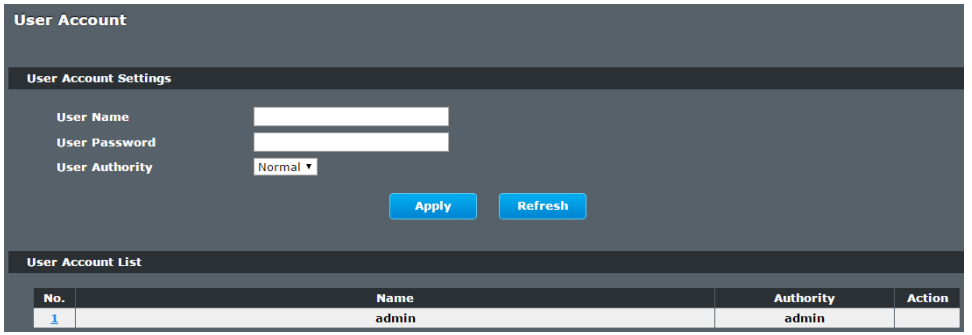
TI-PG541I#configure terminal

TI-PG541I(config)#add user q q admin

TI-PG541I(config)#add user 1 1 normal

Web Configuration

Management > User Account



Parameter	Description
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates: **admin** (read and write) or **normal** (read only) for this user account.
Apply	Click **Apply** to add/modify the user account.
Refresh	Click **Refresh** to begin configuring this screen afresh.
User Account List	
No.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
User Password	This field displays the password.
User Authority	This field displays the associated group.
Action	Click the **Delete** button to remove the user account. Note: You cannot delete the last admin accounts.

Technical Specifications

Standards

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

Device Interface

- 4 x Gigabit PoE+ ports
- 1 x Gigabit port
- 1 x Gigabit SFP slot
- 6-pin removable terminal block (primary/RPS power inputs & alarm relay output)
- Optional power adapter input (adapter sold separately)
- DIP switch (Alarm for Primary/RPS power)
- LED indicators

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)
- SX/LX: 2000 Mbps (full-duplex)

Performance

- Switch fabric: 12 Gbps
- RAM buffer: 128 MB
- MAC address table: 8K entries
- Jumbo frames: 10 KB
- Forwarding rate: 8.93 Mpps (64-byte packet size)

Management

- CLI (Telnet)
- HTTP web based GUI
- SNMP v1, v2c
- SNMP trap
- RMON groups 1, 2, 3, 9
- Enable/disable 802.3az power saving
- LLDP
- SNTP
- SMTP alert
- Syslog
- Port statistics/utilization
- Traffic monitor
- Trusted host
- Port mirror (Ingress, Egress, Both)
- Storm control (Multicast, DLF, Broadcast)

MIB

- MIB II RFC 1213
- Bridge MIB RFC 1493
- Ethernet Interface MIB RFC 1643
- RMON MIB RFC 1757
- Power Ethernet MIB RFC 3621

Quality of Service (QoS)

- 802.1p Class of Service (CoS)
- DSCP (Differentiated Services Code Point)
- Bandwidth control per port
- Queue Scheduling: Strict Priority (SP), Weighted Fair Queuing (WFQ), Weighted Round Robin (WRR)

VLAN

- 802.1Q tagged VLAN
- MAC-based VLAN
- Port isolation
- Up to 256 VLAN groups, ID range 1-4094

Multicast
- IGMP snooping v1, v2, v3
- Static multicast address
- Up to 256 multicast entries

Special Features
- CLI & web based management
- Full power PoE+
- Wide operating temperature range
- Dual redundant power inputs
- Alarm relay triggered by power failure
- Surge/ESD protection

Power
- PWR (Primary) terminal input: 48 – 57V DC (TI-S12048 sold separately)
- RPS (Redundant) terminal input: 48 – 57V DC (TI-S12048 sold separately)
- Consumption: 10 W (max.), 130 W (max.) with PoE+ fully loaded

Optional Power Adapter (48VDC3000 sold separately)
- Input: 100 - 240 V AC, 50/60 Hz, 2 A
- Output: 48 V DC, 3.34 A 160 watts max.

Optional Power Supply (TI-S24048 sold separately)
- Input: 100-240 V AC, 50/60 Hz, 1.8 A 125-370 V DC
- Output: 240 Watts, 48 V, 5 A
- DIN-rail: TS-35/7.5 or 15
- Operating Temperature: - 25 to 70 °C (- 13 to 158 °F)

PoE
- PoE budget: 120W
- Up to 15W per port for PoE
- Up to 30W per port for PoE+
- Mode A: Pins 1, 2 (V+) and pins 3, 6 (V-)
- PoE enable/disable per port setting, priority, scheduling, power delay, and PD alive check

Enclosure
- IP30 rated metal enclosure
- DIN-Rail Mount
- Grounding Point
- ESD (Ethernet) Protection: 8KV DC
- Surge (Power) Protection: 6KV DC

MTBF
- 180,136 hrs @ 65 °C
- 435,905 hrs @ 25 °C

Operating Temperature
- - 40 – 70 °C (- 40 - 158 °F)

Operating Humidity
- Max. 95% non-condensing

Dimensions
- 135 x 120 x 31 mm (5.31 x 4.72 x 1.22 in.)

Weight
- 528 g (1.17 lbs.)

Certifications
- CE
- FCC
- Shock (IEC 60068-2-27)
- Freefall (IEC 60068-2-32)
- Vibration (IEC 60068-2-6)

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 System, click IPv4 Setup and change the IP address of the switch to be within your network's IP subnet. Click Apply, then click OK. Then click Save Settings to Flash (menu) and click Save Settings to Flash to save the IP settings to the NV-RAM.

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 55011: 2009 + A1: 2010 (Group 1, Class A)**
- **EN 55022: 2010 + AC: 2011 (Class A)**
- **EN 55024: 2010**
- **EN 61000-3-2: 2014**
- **EN 61000-3-3: 2013**

Directives:

EMC Directive 2004/108/EC and EN 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.

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TI-PG541I je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/30/EU a 2004/108/ES.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TI-PG541I overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/30/EU og 2004/108/EF.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TI-PG541I in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/30/EU, und 2004/108/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TI-PG541I vastavust direktiivi 2014/30/EU ja 2004/108/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, TRENDnet, declares that this TI-PG541I is in compliance with the essential requirements and other relevant provisions of Directive 2014/30/EU and 2004/108/EC.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TI-PG541I cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/30/EU, 2004/108/CE y.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑTRENDnet ΔΗΛΩΝΕΙ ΟΤΙTI-PG541IΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ, 2014/30/EU, 2004/108/ΕΚ και.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TI-PG541I est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/30/UE et 2004/108/CE.
it Italiano[Italian]	Con la presente TRENDnet dichiara che questo TI-PG541I è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/30/EU e 2004/108/CE.
Latviski [Latvian]	AršoTRENDnetdeklarē, ka TI-PG541I atbilstDirektīvas 2014/30/EU un 2004/108/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.
Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TI-PG541I atitinka esminius reikalavimus ir kitas 2014/30/EU ir 2004/108/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TI-PG541I in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/30/EU en 2004/108/EG.
mt Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TI-PG541I jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/30/EU u 2004/108/KE.
hu Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TI-PG541Imegfelel a vonatkozó alapvetõ követelményeknek és az 2014/30/EU, irányelv és a 2004/108/EK irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym TRENDnet oświadcza, że TI-PG541I jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/30/EU i 2004/108/WE.
pt Português [Portuguese]	TRENDnet declara que este TI-PG541I está conforme com os requisitos essenciais e outras disposições da Directiva 2014/30/EU, e 2004/108/CE.
sl Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TI-PG541I v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/30/EU, in 2004/108/ES.
Slovensky [Slovak]	TRENDnettýmtovyhlasuje, že TI-PG541Ispĺňazákladnépožiadavky a všetkypríslušnéustanoveniaSmernice 2014/30/EU a 2004/108/ES.
fi Suomi [Finnish]	TRENDnet vakuuttaa täten että TI-PG541I tyyppinen laite on direktiivin 2014/30/EU ja 2004/108/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TI-PG541I står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/30/EU, och 2004/108/EG.

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 2016/04/15

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