User's Guide

TRENDnet®

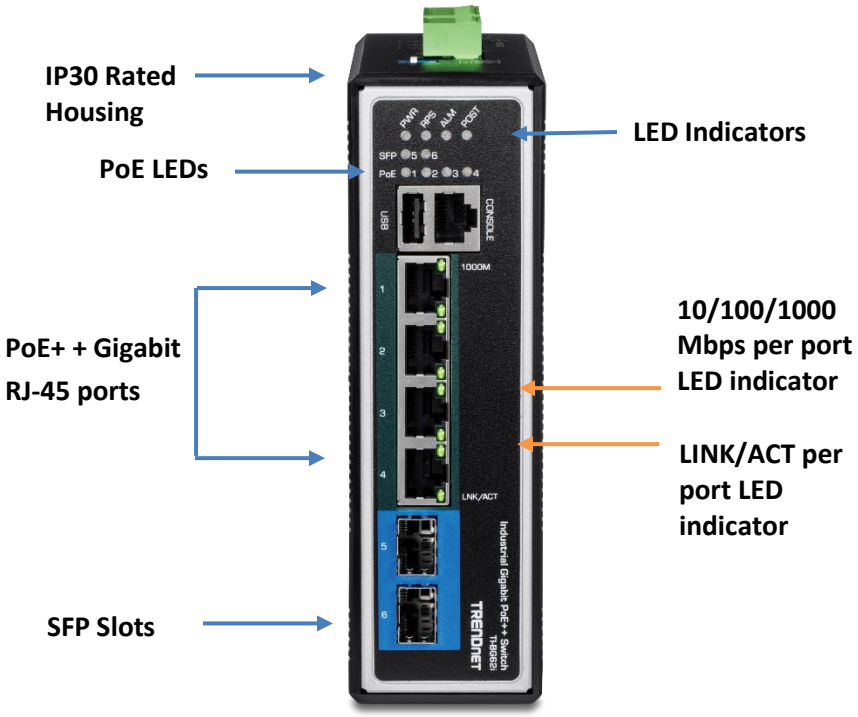
6-Port Industrial Gigabit L2+ Managed PoE++ DIN-Rail Switch

TI-BG62i

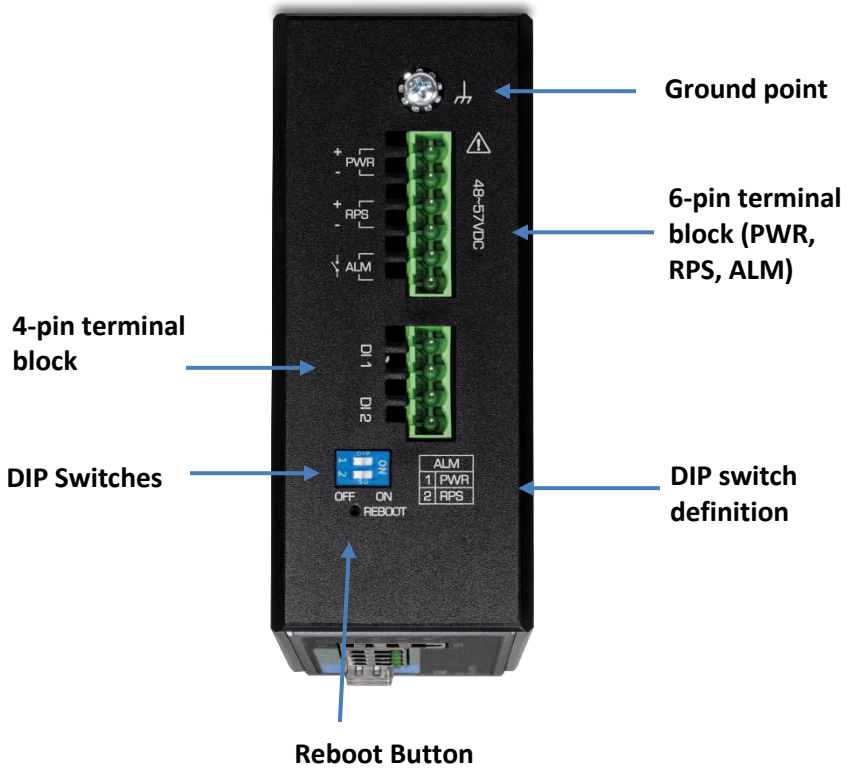
Product Overview

TI-BG62i

Front View



Top View

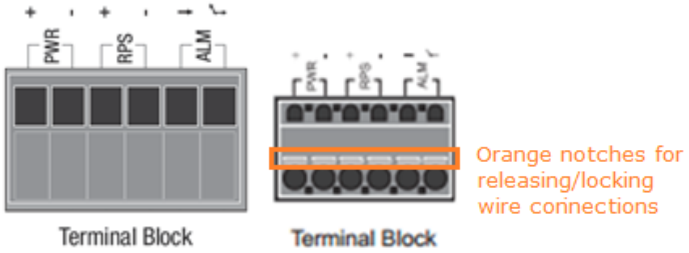


- **PoE++ Ports 1-4 –** Connect either network PoE++ or non-PoE devices.
- **SFP Slot 5-6 –** Designed to operate at Gigabit or 100Mbps speeds.
- **Reset Button –** Push the button for 5-10 seconds and release to reset.
- **Grounding point/screw** – The switch chassis can also be connected to a known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

Please note power supply is sold separately

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

6-pin Removable Terminal Block

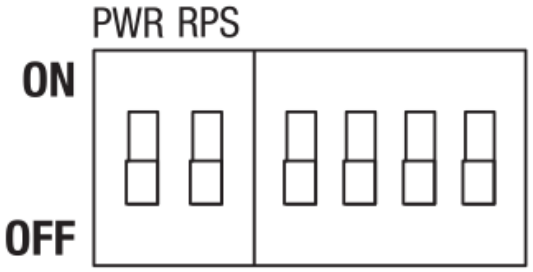


Note: Turn off the power before connecting modules or wires.

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

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

ALM DIP Switches



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

Switch Installation

DIN-Rail Installation

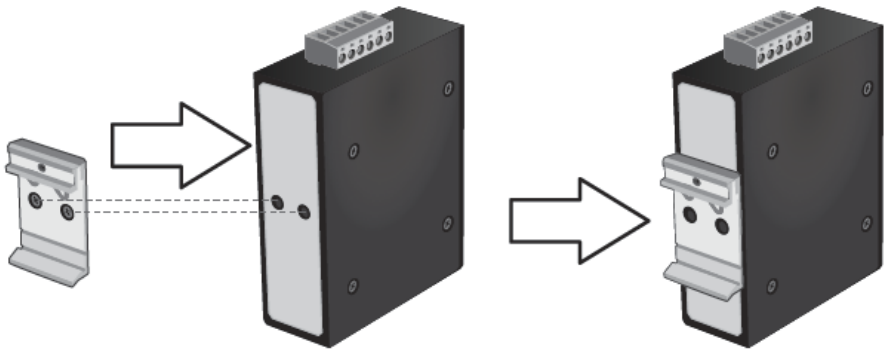
The site where the switch will be installed may greatly affect its performance. When installing, consider the following pointers:

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.

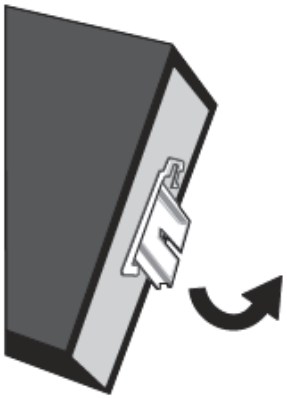
Fasten the DIN-Rail bracket to the rear of the switch using the included fasteners/screws.
Note: *The DIN-Rail bracket may already be installed to your switch when received.*

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



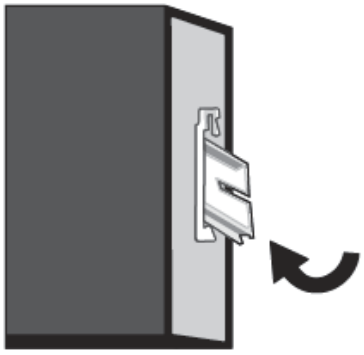
The switch can be installed to a 35mm (W) DIN-Rail located in cabinet, rack, or enclosure.

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

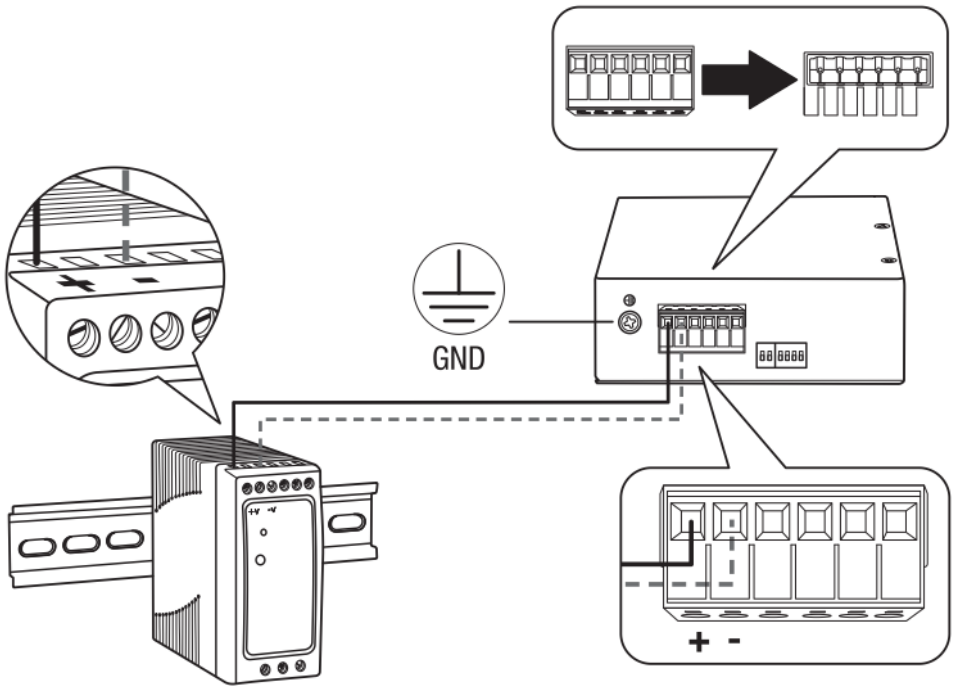
Install power supply connections

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

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

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

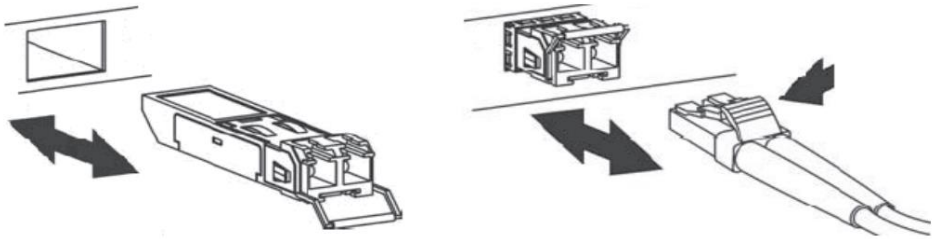
***Note:** The models in the image may be different than your specific model.*



SFP Transceiver/Optical Cable Installation

1. Remove the rubber plug from the SFP 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

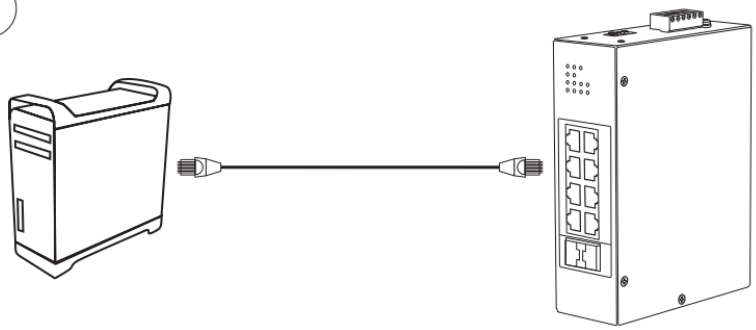


***To properly connect fiber cabling**:* Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through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

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.

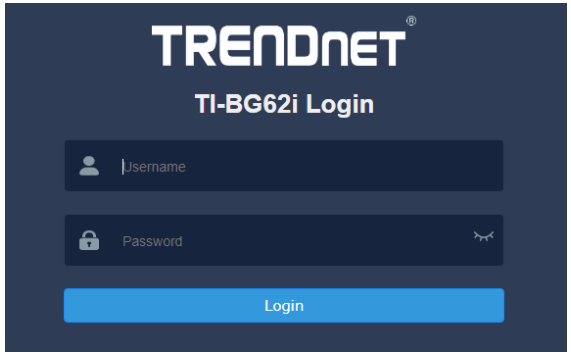
3. Open your web browser, and type the IP address of the switch in the address bar, and then press **Enter**. The default IP address is **192.168.10.200**.

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

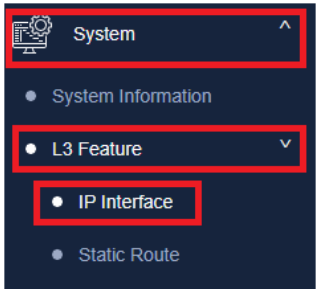
User Name: **admin**

Password: **admin**

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

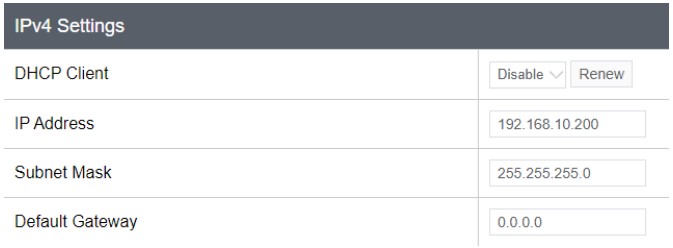


5. Click **System,** click **L3 Feature**, and then click **IP Interface**.



6. 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*



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

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

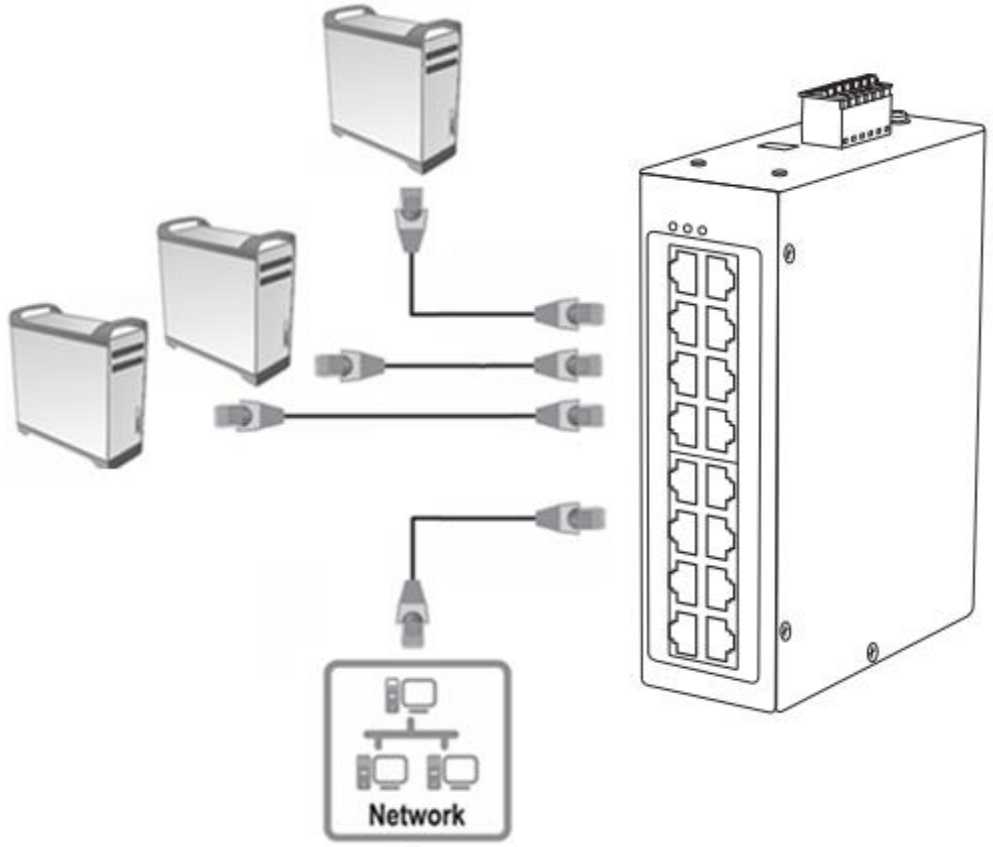
Note: *Once the settings are saved, you can connect the switch to your network.*

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

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

Note*: The switch below may be different than the one you purchased.*

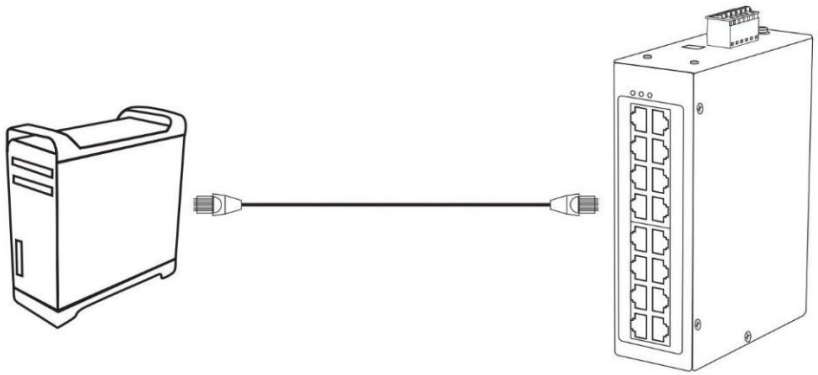


Accessing switch management interfaces

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 **"[DEVICE_NAME]*#".***

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

- configure

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

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

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

  [DEVICE_NAME]# configure terminal

- eth0

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

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

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

  [DEVICE_NAME](config)#interface eth0

  [DEVICE_NAME](config-if)#

- interface

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

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

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

  Or

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

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

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

  [DEVICE_NAME](config-if)#

- vlan

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

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

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

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

  [DEVICE_NAME](config)#vlan 2

  [DEVICE_NAME](config-vlan)#

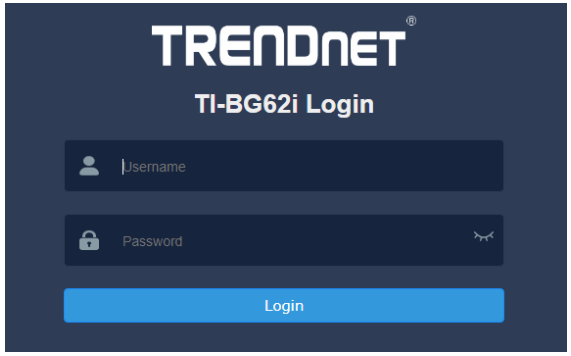
Access your switch web management page

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

1. Open your web browser and go to 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 Name	Enter the user name.
Password	Enter the password.

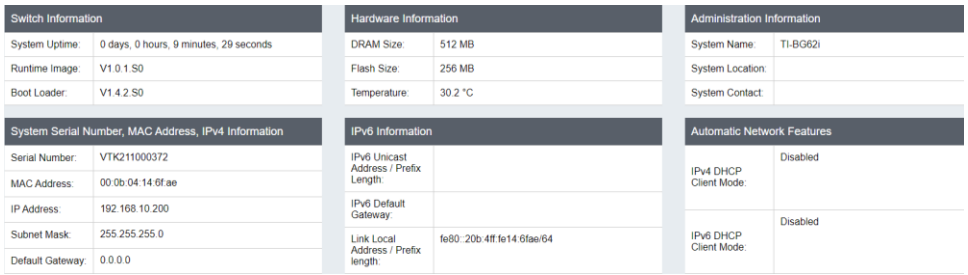
System Information

CLI Configuration

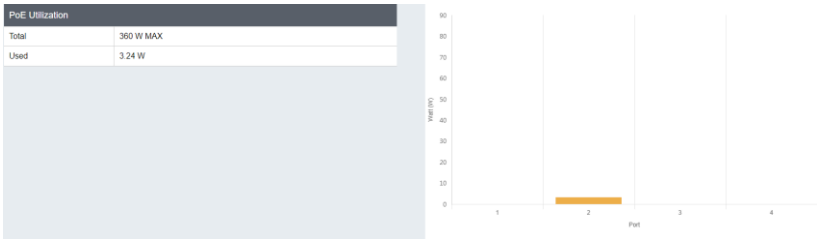
Node	Command	Description
enable	show hostname	This command displays the system's network name.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current 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

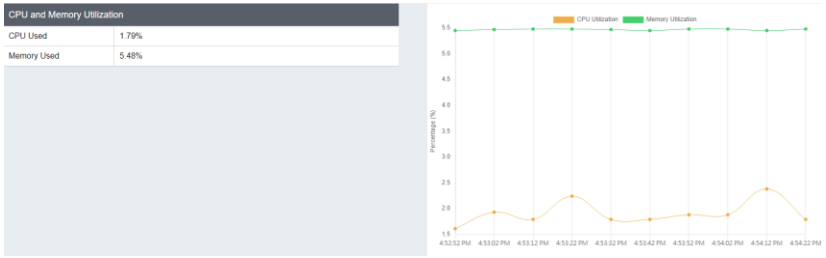
Dashboard > Dashboard



Parameter	Description
System Uptime	This field displays the total time the switch has been on
Runtime Image	This field displays the firmware version of the switch
Boot Loader	This field displays the boot code version.
DRAM Size	The total size of the RAM
Flash Size	This field displays the total size of the Flash.
Temperature	This field displays the current temperature of the switch.
System Name	This field displays the name of the Switch.
System Location	This field displays the location of the switch.
System Contact	This field displays the contact information of the switch.
Serial Number	The serial number assigned by manufacture for identification of the unit.
MAC Address	This field displays the MAC (Media Access Control) address of 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.
IPv6 Unicast Address / Prefix Length	This field indicates the IPv6 Unicast Address.
IPv6 Default Gateway	This field displays the gateway's IPv6 Address.
Link Local Address / Prefix Length	This field displays the local IPv6 Address
IPv4 DHCP Client Mode	This field displays whether the IPv4 DHCP client is enabled on the Switch.
IPv6 DHCP Client Mode	This field displays whether the IPv6 DHCP client is enabled on the Switch.



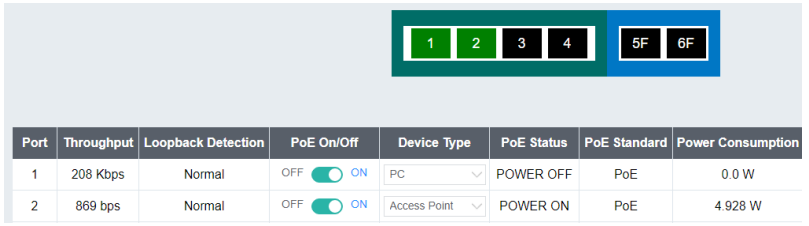
Parameter	Description
Total	This field displays the max budget for PoE in Watts
Used	This field displays the current total wattage used for PoE in Watts



Parameter	Description
CPU Used	This field displays the amount of CPU resources being used
Memory Used	This field displays the amount of memory being used

Switch View

Dashboard > Switch View



Parameter	Description
Throughput	This field displays the current throughput of the port.
Loopback Detection	This field displays the current status of Loopback Detection.
PoE On/Off	Enable and disable the PoE of the connected PD device.
Device Type	This field displays the current type of device connected to this port.
PoE Status	Displays the current PoE status.
PoE Standard	Displays the PoE standard being used.
Power Consumption	Displays the max power consumption in used by the PD device.

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 [YOUR_DEVICE_NAME]

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.

[DEVICE_NAME]#configure terminal

[DEVICE_NAME](config)#

✓ To enter the ETH0 interface node.

[DEVICE_NAME](config)#interface eth0

[DEVICE_NAME](config-if)#

✓ To get an IP address from a DHCP server.

[DEVICE_NAME](config-if)#ip dhcp client enable

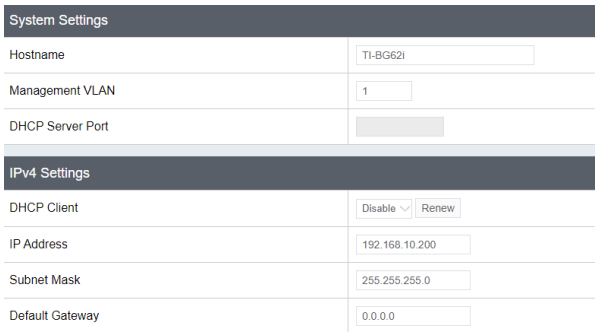
✓ To configure a static IP address and a gateway for the Switch.

[DEVICE_NAME](config-if)#ip address 192.168.202.111/24

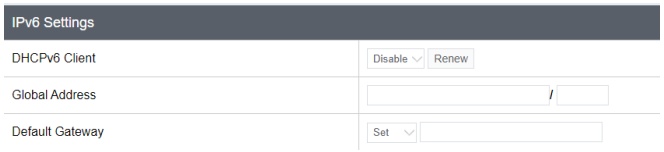
[DEVICE_NAME](config-if)#ip address default-gateway 192.168.202.1

Web Configuration

System > L3 Feature > IP Interface



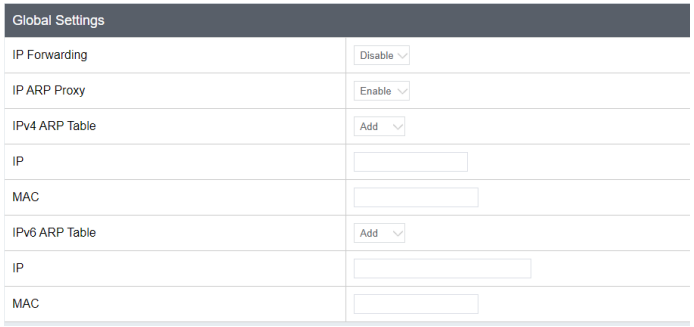
DHCP Client	Sets the switch to DHCP client to receive IP address assigned by the default gateway.
IP Address	Configures a IPv4 address for your Switch in dotted decimal notation. For example, 192.168.10.200.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.10.1.



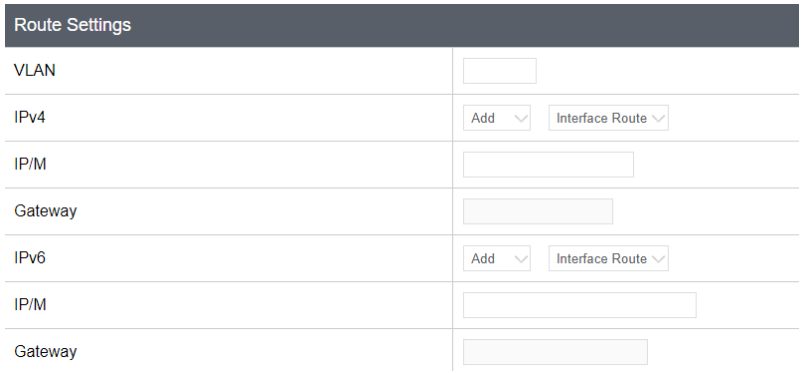
DHCPv6 Client	Sets the switch to enable or disable DHCPv6 client to receive IP address assigned by the default gateway.
Global Address	Configures a IPv6 address for your Switch in dotted decimal notation.
Default Gateway	Enter the default IPv6 address for your gateway

Static Route

System > L3 Feature > Static Route



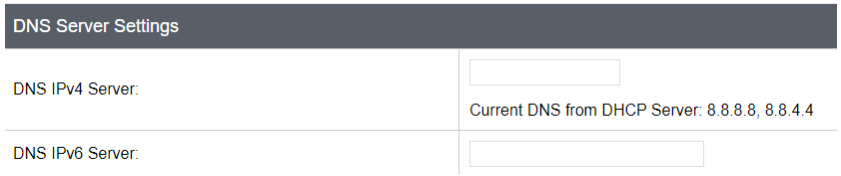
IP Forwarding	Configures the switch to enable or disable IP Forwarding.
IP ARP Proxy	Configures the switch to enable or disable IP ARP Proxy.
IPv4 ARP Table	Configures the switch to add or delete the IPv4 ARP table.
IP	Enter the IP address for the static route.
MAC	Enter the MAC address for the static route.
IPv6 ARP Table	Configures the switch to add or delete the IPv6 ARP table.
IP	Enter the IPv6 IP address for the IPv6 ARP table.
MAC	Enter the MAC address for the IPv6 ARP table.



VLAN	Enter the VLAN ID to route
IPv4	Add or delete the settings.
IP/M	
Gateway	Enter the Gateway address
IPv6	Add or delete the settings for the IPv6
IP/M	
Gateway	Enter the IPv6 gateway address

DNS Server

System > DNS



DNS IPv4 Server	Enter the IP address of the DNS server. ***Note:*** DNS is set to 8.8.8.8 and 8.8.4.4 by default
DNS IPv6 Server	Enter the IP address in IPv6 of the DNS server

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:

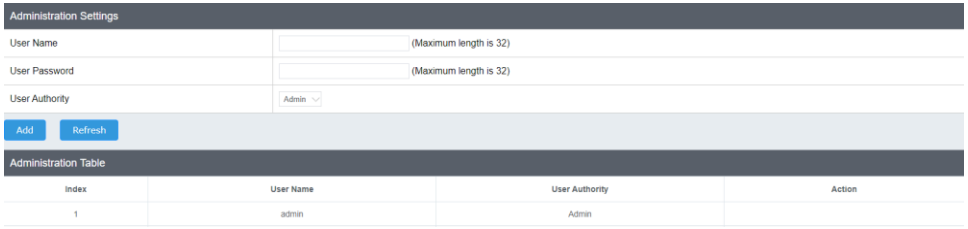
[DEVICE_NAME]#configure terminal

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

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

Web Configuration

System > Administration



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.
Add	Click **Add** to add/modify the user account.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Administration Table	
Index.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
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.

System Time

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:

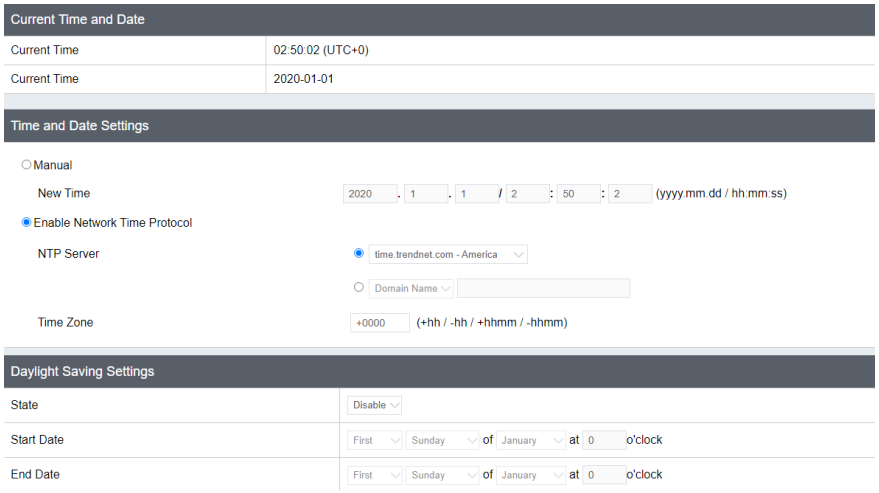
[DEVICE_NAME](config)#*time ntp-server 192.5.41.41*

[DEVICE_NAME](config)#*time timezone +0800*

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

Web Configuration

System > System Time



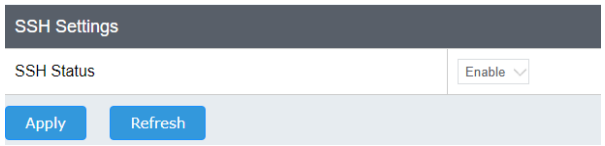
Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.
New Time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

SSH

Enable SSH (Secure Shell) management access

System > SSH

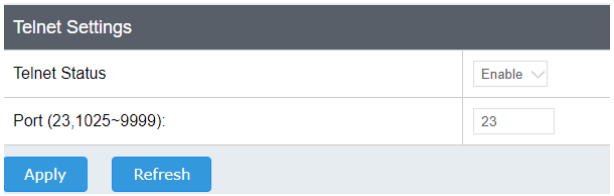


Parameter	Description
SSH Status	Enable or disable SSH via drop down menu
Apply	Click Apply for settings to take effect
Refresh	Click Refresh to begin configuring this screen afresh

Telnet

Enable SSH (Secure Shell) management access

System > Telnet



Parameter	Description
Telnet Status	Enable or disable telnet
Port	Input the port for telnet settings
Apply	Click Apply for settings to take effect
Refresh	Click Refresh to begin configuring this screen afresh

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:

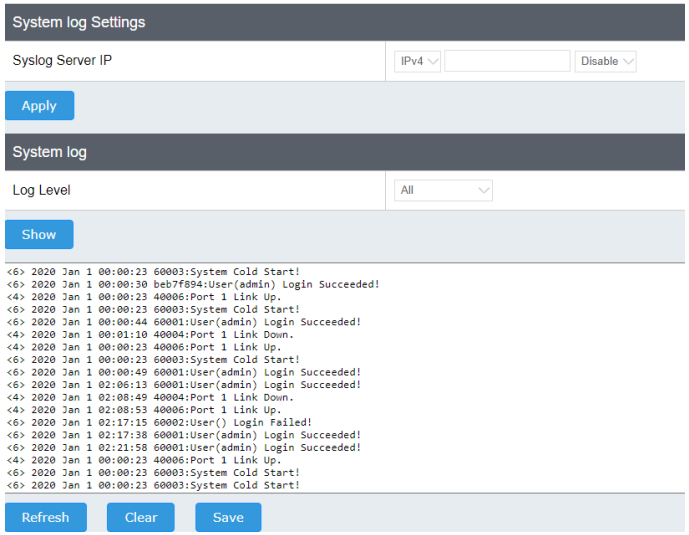
[DEVICE_NAME]#configure terminal

[DEVICE_NAME](config)#syslog-server ipv4-ip 192.168.200.106

[DEVICE_NAME](config)#syslog-server enable

Web Configuration

System > System Log



Parameter	Description
Syslog 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.

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 : [YOUR_DEVICE_NAME]. (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:

[DEVICE_NAME]#configure terminal

[DEVICE_NAME](config)#snmp enable

[DEVICE_NAME](config)#snmp community public rw trusted-host 192.168.200.106/24

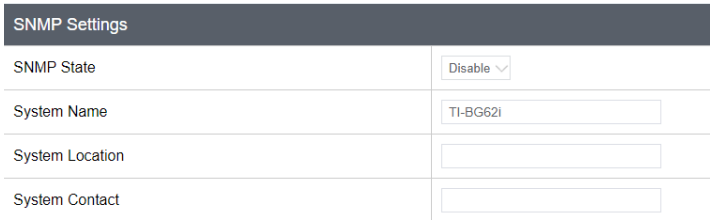
[DEVICE_NAME](config)#snmp trap-receiver 192.168.200.106 v2c public

[DEVICE_NAME](config)#snmp system-contact IT engineer

[DEVICE_NAME](config)#snmp system-location Branch-Office

Web Configuration

System > SNMP > Settings

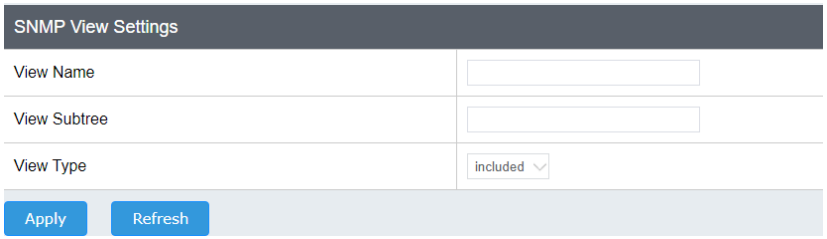


Parameter	Description
SNMP State	Select **Enable** to activate SNMP on the Switch. Select **Disable** to not use SNMP on the Switch.
System Name	Type a System Name for the Switch. (The System Name is same as the host name)
System Location	Type a System Location for the Switch.
System Contact	Type a System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

View Settings

System > SNMP > View

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

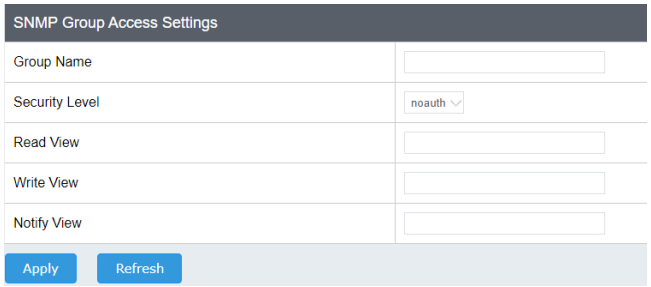


View Name	This entry must be pre-defined on the SNMP User/Group page.
View Subtree	Input the subtree OID
View Type	Select **Included** or **Excluded** as the view type
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.

Group

System > SNMP > Group

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

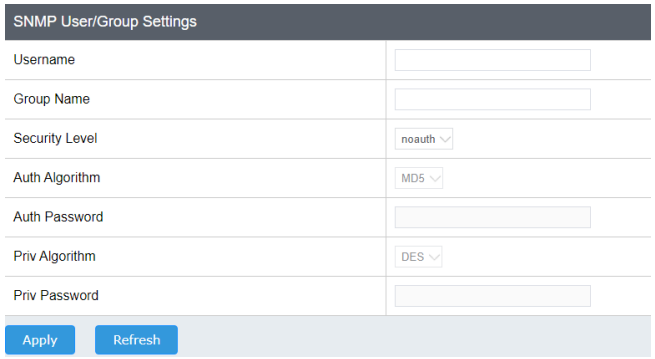


Parameter	Description

Group Name	Enter the group name in this field. The entry must be pre-defined on the SNMP User/Group Page
Security Level	Select from the options from the drop down menu • **NoAuthNoPriv**: This selection is the appropriate selection when no Auth-Protocol or Priv-Protocol (no encryption) are selected on the SNMP User/Group page. • **AuthNoPriv**: Choose this selection when encryption has been enabled but only the Auth-Protocol has a password assigned and the Priv-Protocol has been selected as none on the SNMP User/Group page. • **AuthPriv**: When the Auth-Protocol or Priv-Protocol have been enabled, choose this selection
Read View	Enter the Read View name. This field is optional.
Write View	Enter the Write View name. This field is optional.
Notify View	Enter the Notify View. This field is optional.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

SNMP User/Group

System > SNMP > User

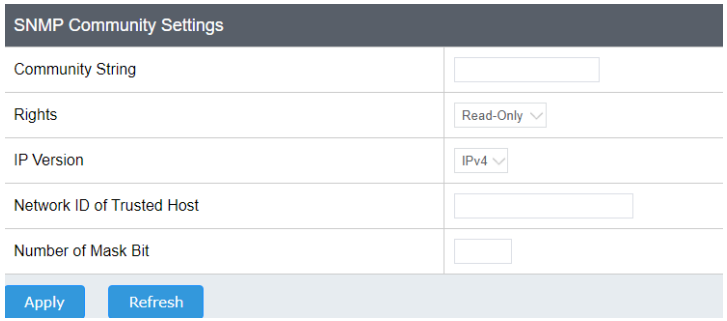


Parameter	Description
Username	Enter a username
Group Name	Enter a group name
Security Level	Select from the options from the drop down menu • **NoAuthNoPriv**: This selection is the appropriate selection when no Auth-Protocol or Priv-Protocol (no encryption) are selected on the SNMP User/Group page. • **AuthNoPriv**: Choose this selection when encryption has been enabled but only the Auth-Protocol has a password assigned and the Priv-Protocol has been selected as none on the SNMP User/Group page. • **AuthPriv**: When the Auth-Protocol or Priv-Protocol have been enabled, choose this selection
Auth Algorithm	Select from the options from the drop down menu • **MD5** - The MD5 authentication protocol. SNMP Users are authenticated with the MD5 authentication protocol after a message is received. • **SHA** - The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

Auth Password	Enter the password for the Auth Protocol
Notify View	Enter the Notify View. This field is optional.
Priv Algorithm	Select from the options from the drop down menu • **DES** - Specifies DES encryption scrambles the SNMP data so that outside observers are prevented from seeing the data content. • **none** - Specifies no encryption is applied to SNMP data.
Priv Password	Enter the password for the Priv Password
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

Community Name

System > SNMP > Community



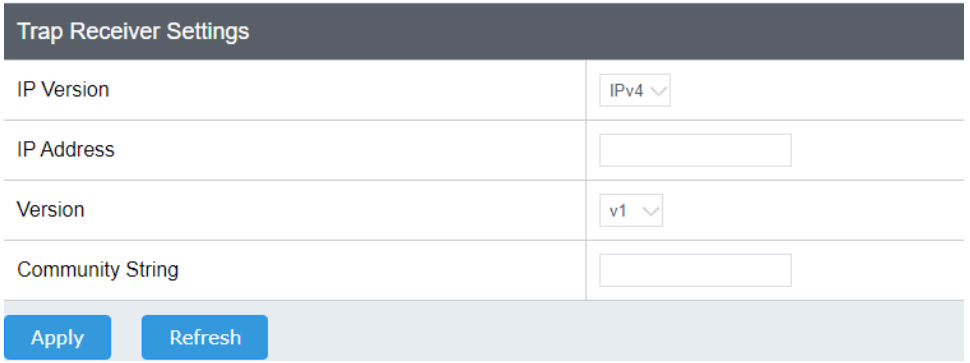
Parameter	Description
Community String	Enter a Community string, this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) 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).
IP Version	Select IPv4 or IPv6 from the drop down menu.
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**.
IP Version	This field displays the IP version
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.

Number of Mask Bit	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

System > SNMP > Trap Receiver



Parameter	Description
IP Version	Select IPv4 or IPv6 from the drop down menu.
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	
IP Version	This field displays the IP version
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.

RMON Statistics

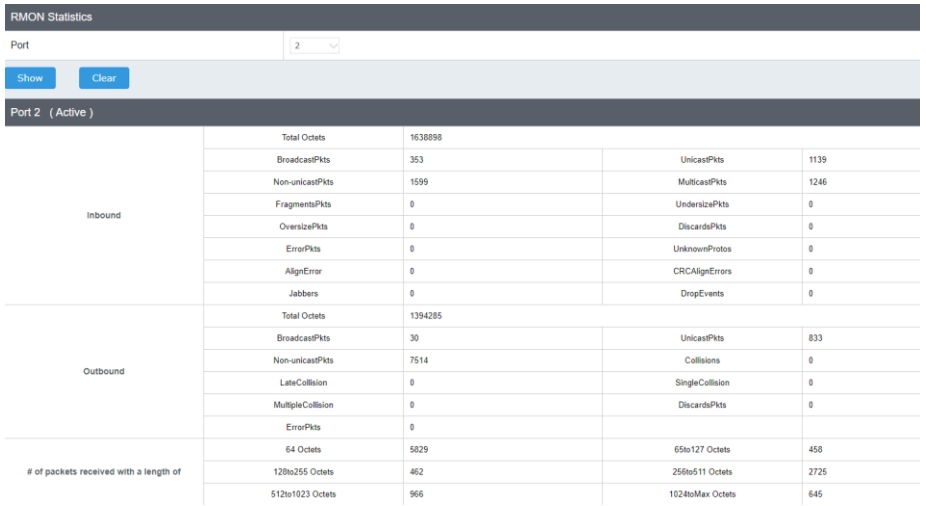
This feature helps users to monitor or clear the port's RMON statistics.

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

System > RMON



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.

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

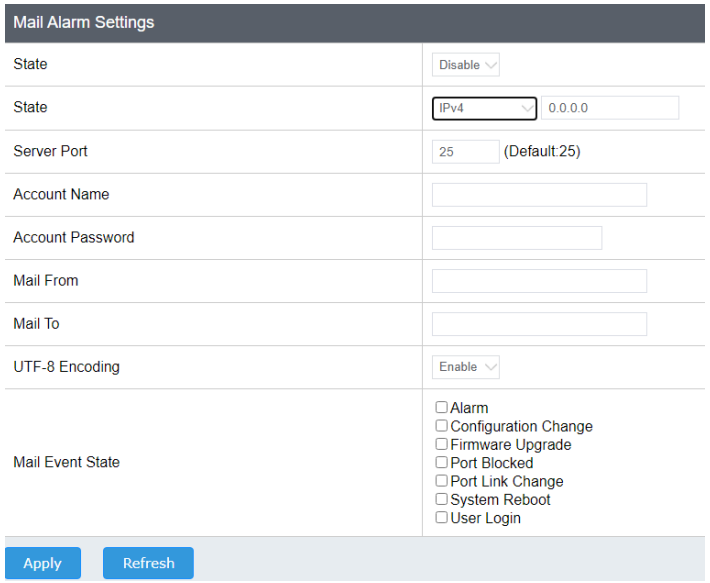
Default Ports	Server	Authentication	Port
SMTP Server (Outgoing Messages)	Non-Encrypted	AUTH	25 (or 587)
	Secure (TLS)	StartTLS	587
	Secure (SSL)	SSL	465
POP3 Server (Incoming Messages)	Non-Encrypted	AUTH	110
	Secure (SSL)	SSL	995
Googlemail - Gmail	Server:	Authentication:	Port:
SMTP Server (Outgoing 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

System > Mail Alarm



Parameter	Description
State	Enable / disable the Mail Alarm function.
State	Specifies the mail server's IP address.
Server Port	Specifies the TCP port for the SMTP. By default the server port is 25.
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.

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.

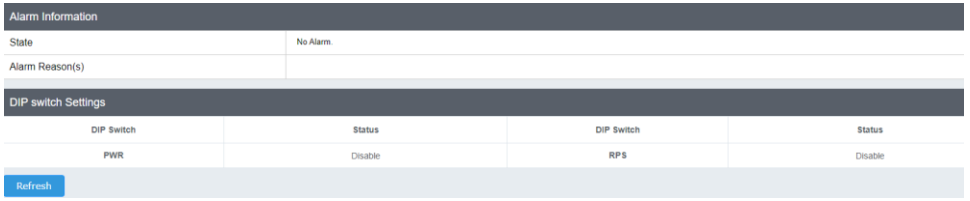
RPS: ON, The Switch will send alarm message when the redundant power supply disconnect.

CLI Configuration

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

Web Configuration

System > Monitor > Alarm

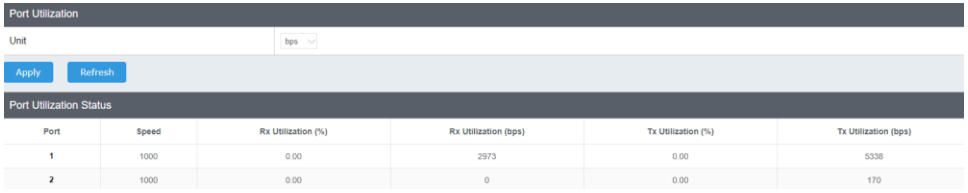


Parameter	Description
Alarm Information	
Alarm State	This field indicates if there is any alarm events.

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 Utilization

System > Monitor > Port Utilization



Parameter	Description
Port Utilization	
Unit	Select the unit of measurement used in Port Utilization Status
Port	This field displays the port number
Speed	This field displays the speed that is currently connected
Rx Utilization (%)	This field displays the percentage data received
Rx Utilization (bps)	This field displays the total data received
Tx Utilization (%)	This field displays the percentage data transmitted
Tx Utilization (bps)	This field displays the percentage data transmitted

SFP Information

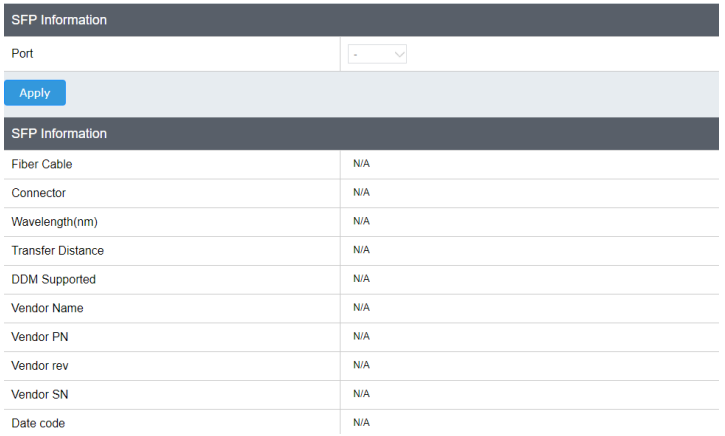
The SFP information allows user to know the SFP module's information, such as vendor name, connector type, revision, serial number, manufacture date, and to know the DDMI information if the SFP modules have supported the DDMI function.

CLI Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmi port PORT_ID	This command displays the SFP DDMI status.

Web Configuration

System > Monitor > SFP Information



Parameter	Description
Port	Select a port number to configure.
Apply	Click Apply to display the SFP information.

Fiber Cable	To indicate if the fiber cable is connected.
Connector	Code of optical connector type.
Wavelength	Displays the wavelength
Transfer Distance	Displays the distance of the fiber cable
DDM Supported	Displays if DDM is supported by the SFP module
Vendor Name	SFP vendor name.
Vendor PN	Part Number.
Vendor rev	Revision level for part number.
Vendor SN	Serial number (ASCII).
Date Code	Manufacturing date code.

Notice: If the fiber cable is not connected, the Rx Power fields are not available.

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	Packet Rate(pps)	Recovery State	Recovery 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
7	Disabled	Normal	Bcast	1000	Enabled	1
8	Disabled	Normal	Bcast	1000	Enabled	1
9	Disabled	Normal	Bcast	1000	Enabled	1
10	Disabled	Normal	Bcast	1000	Enabled	1
11	Disabled	Normal	Bcast	1000	Enabled	1
12	Disabled	Normal	Bcast	1000	Enabled	1
13	Disabled	Normal	Bcast	1000	Enabled	1
14	Disabled	Normal	Bcast	1000	Enabled	1
15	Disabled	Normal	Bcast	1000	Enabled	1
16	Disabled	Normal	Bcast	1000	Enabled	1

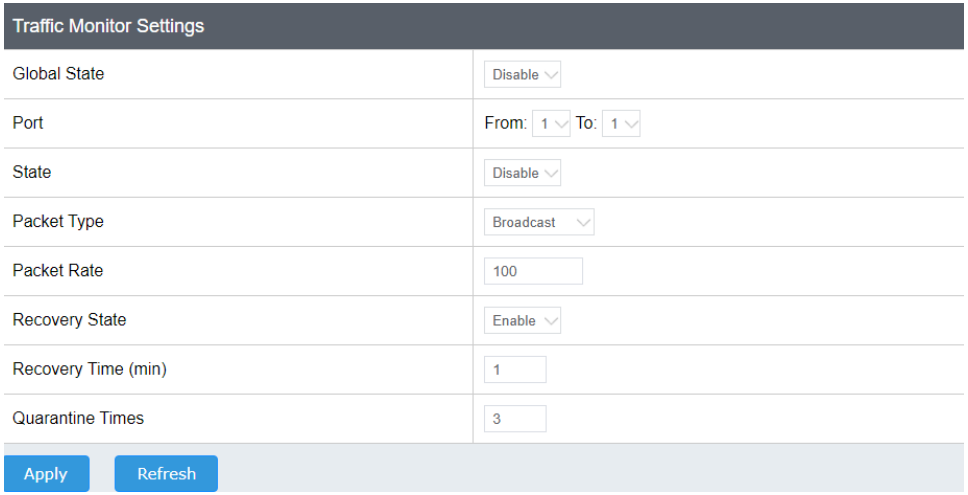
CLI Configuration

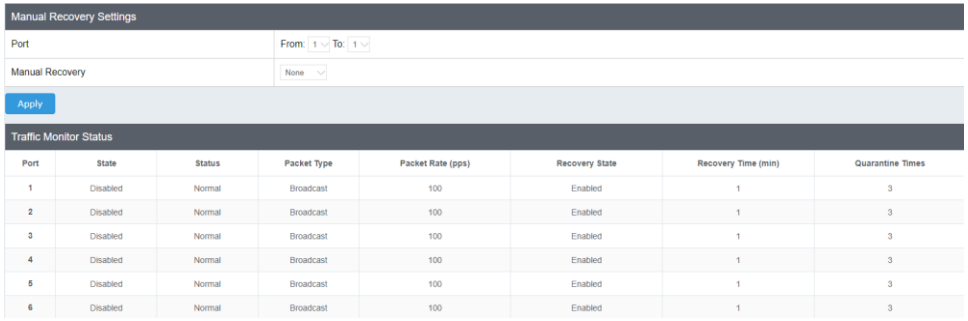
Node	Command	Description
enable	show traffic-monitor	This command displays the traffic monitor configurations and current status.
configure	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the Switch.
interface	traffic-monitor (disable|enable)	This command enables / 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

System > Monitor > Traffic Monitor





Parameter	Description
Global 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.
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)
Quarantine Times	Configures the quarantine times for the traffic monitor function on the selected ports.

Hardware Information

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

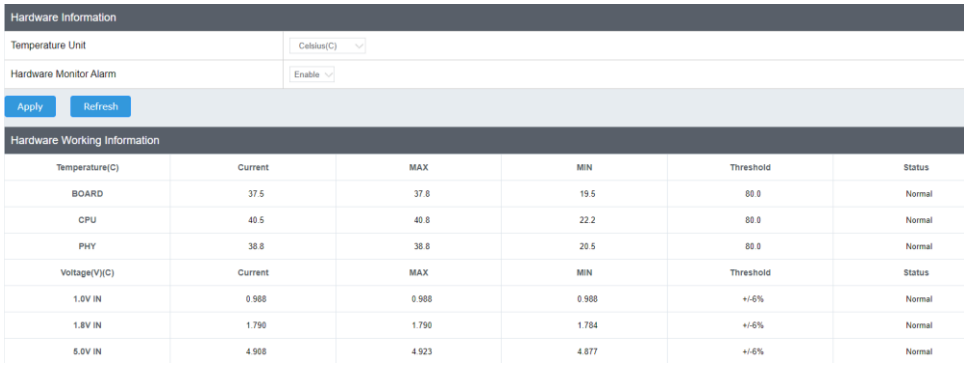
Port	State	Packet Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time(min)
1	Disabled	Normal	Bcast	1000	Enabled	1
2	Disabled	Normal	Bcast	1000	Enabled	1
3	Disabled	Normal	Bcast	1000	Enabled	1
4	Disabled	Normal	Bcast	1000	Enabled	1
5	Disabled	Normal	Bcast	1000	Enabled	1
6	Disabled	Normal	Bcast	1000	Enabled	1
7	Disabled	Normal	Bcast	1000	Enabled	1
8	Disabled	Normal	Bcast	1000	Enabled	1
9	Disabled	Normal	Bcast	1000	Enabled	1
10	Disabled	Normal	Bcast	1000	Enabled	1
11	Disabled	Normal	Bcast	1000	Enabled	1
12	Disabled	Normal	Bcast	1000	Enabled	1
13	Disabled	Normal	Bcast	1000	Enabled	1
14	Disabled	Normal	Bcast	1000	Enabled	1
15	Disabled	Normal	Bcast	1000	Enabled	1
16	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

System > Monitor > Hardware Information



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)

Modbus

MODBUS TCP supports different types of data format for reading. The primary four types of them are:

Data Access Type		Function Code	Function Name	Note
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Not support now
	Internal Bits or Physical Coils	1	Read Coils	Not support now
Word access (16-bit access)	Physical Input Registers	4	Read Input Registers	
	Physical Output Registers	3	Read Holding Registers	Not support now

MODBUS Data Map and Information Interpretation of IE Switches

MODBUS base address of switches is 1001(decimal) for Function Code 4.

Address Offset	Data Type	Interpretation	Description
System Information			
0x0000	1 word	HEX	Vendor ID = 0x0b04
0x0001	16 words	ASCII	Vendor Name = "ABCDEFG Corp." Word 0 Hi byte = 'A' Word 0 Lo byte = 'B' Word 1 Hi byte = 'C' Word 1 Lo byte = 'D' Word 2 Hi byte = 'E' Word 2 Lo byte = 'F' Word 3 Hi byte = 'G'

			Word 3 Lo byte = ' ' Word 4 Hi byte = 'C' Word 4 Lo byte = 'o' Word 5 Hi byte = 'r' Word 5 Lo byte = 'p' Word 6 Hi byte = '.' Word 6 Lo byte = '\0'
0x0020	16 words	ASCII	Product Name = "SWITCH" Word 0 Hi byte = 'S' Word 0 Lo byte = 'W' Word 1 Hi byte = 'I' Word 1 Lo byte = 'T' Word 2 Hi byte = 'C' Word 2 Lo byte = 'H'
0x0040	7 words		Product Serial Number Ex: Serial No=A000000000001
0x0050	12 words	ASCII	Firmware Version=" 8648-999-1.1.0.S0" Word 0 Hi byte = '8' Word 0 Lo byte = '6' Word 1 Hi byte = '4' Word 1 Lo byte = '8' Word 2 Hi byte = '-' Word 2 Lo byte = '9' Word 3 Hi byte = '9' Word 3 Lo byte = '9' Word 4 Hi byte = '-' Word 4 Lo byte = '1' Word 5 Hi byte = '.' Word 5 Lo byte = '1'

			Word 6 Hi byte = '.' Word 6 Lo byte = '0' Word 7 Hi byte = '.' Word 7 Lo byte = 'S' Word 8 Hi byte = '0' Word 8 Lo byte = '\0'
0x0060	16 words	ASCII	Firmware Release Date=" Mon Sep 30 18:51:45 2013"
0x0070	3 words	HEX	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05
0x0080	1 word	HEX	Power 1(PWR) Alarm, DIP switch 1 need ON 0x0000: no alarm 0x0001: input voltage < 44V 0x0002: input voltage > 57V 0x0003: No PWR input
0x0081	1 word	HEX	Power 2(RPS) Alarm, DIP switch 1 need ON 0x0000: no alarm 0x0001: input voltage < 44V 0x0002: input voltage > 57V 0x0003: No RPSinput
0x0090	1 word	HEX	Fault LED Status 0x0000: No

			0x0001: Yes
Port Information			
0x0100 to 0x0109	1 word	HEX	Port 1 to 10 Link Status 0x0000: Link down 0x0001: 10M-Full-FC_ON (FC: Flow Control) 0x0002: 10M-Full-FC_OFF 0x0003: 10M-Half-FC_ON 0x0004: 10M-Half-FC_OFF 0x0005: 100M-Full-FC_ON 0x0006: 100M-Full-FC_OFF 0x0007: 100M-Half-FC_ON 0x0008: 100M-Half-FC_OFF 0x0009: 1000M-Full-FC_ON 0x000A: 1000M-Full-FC_OFF 0x000B: 1000M-Half-FC_ON 0x000C: 1000M-Half-FC_OFF 0xFFFF: No port
0x0200 to 0x0213 (port 1) 0x0220 to 0x0233 (port 2) … 0x0320 to 0x0333 (port 10)	20 words	ASCII	Port 1 to 10 Description Port Description = "100TX,RJ45." Or "1000TX,SFP." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'T' … Word 4 Hi byte = '4' Word 4 Lo byte = '5' Word 5 Hi byte = '.' Word 5 Lo byte = '\0'

0x0400 to 0x0413 (port 1 to 10)	2 words	HEX	Port 1 to 10 Tx Packets Ex: port 1 Tx Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
0x0440 to 0x0453 (port 1 to 10)	2 words	HEX	Port 1 to 10 Rx Packets Ex: port 1 Rx Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
0x0480 to 0x0493 (port 1 to 10)	2 words	HEX	Port 1 to 10 Tx Error Packets Ex: port 1 Tx Error Packet Amount = 0x87654321 Word 0 =8765 Word 1 = 4321
0x04C0 to 0x04D3 (port 1 to 10)	2 words	HEX	Port 1 to 10 Rx Error Packets Ex: port 1 Rx Error Packet Amount = 0x123456 Word 0 = 0012 Word 1 = 3456
STP Information			
0x0500	1 word	HEX	STP Status: 0x0000 : STP is disabled. 0x0001 : STP 0x0002 : RSTP 0x0003 : MSTP
Xpress Ring Information			
0x0501	1 word	HEX	Xpress Ring Status on the Switch: 0x0000 : Disabled. 0x0001 : Enabled

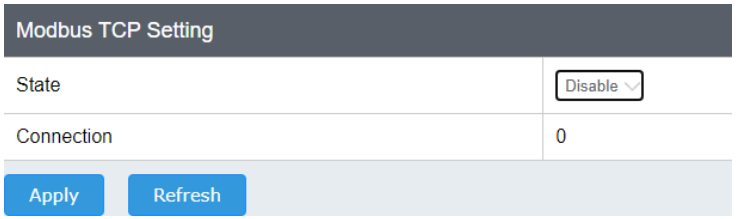
0x0510	1 word	HEX	Status of Xpress-ring1 of the Switch 0x0000 : Disabled 0x0001 : Enabled
0x0511	1 word	HEX	Status of Xpress-ring2 of the Switch 0x0000 : Disabled 0x0001 : Enabled
0x0512	3 word	HEX	Destination MAC of the Xpress-ring1 Word 0 Lo byte = MAC0 Word 0 Hi byte = MAC1 Word 1 Lo byte = MAC2 Word 1 Hi byte = MAC3 Word 2 Lo byte = MAC4 Word 2 Hi byte = MAC5
0x0515	3 word	HEX	Destination MAC of the Xpress-ring2 Word 0 Lo byte = MAC0 Word 0 Hi byte = MAC1 Word 1 Lo byte = MAC2 Word 1 Hi byte = MAC3 Word 2 Lo byte = MAC4 Word 2 Hi byte = MAC5
0x0518	1 word	HEX	Primary Port of the Xpress-ring1 Word 0 Hi byte = Port ID.
0x0519	1 word	HEX	Secondary Port of the Xpress-ring1 Word 0 Hi byte = Port ID.
0x051a	1 word	HEX	Primary Port of the Xpress-ring2 Word 0 Hi byte = Port ID.
0x051b	1 word	HEX	Secondary Port of the Xpress-ring2 Word 0 Hi byte = Port ID.
0x051c	1 word	HEX	Role of Xpress-ring1
			0x0000 : Forwarder 0x0001 : Arbiter
0x051d	1 word	HEX	Role of Xpress-ring2 0x0000 : Forwarder 0x0001 : Arbiter
0x051e	1 word	HEX	Primary Port Status of Xpress-ring1 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking
0x051f	1 word	HEX	Secondary Port Status of Xpress-ring1 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking
0x0520	1 word	HEX	Primary Port Status of Xpress-ring2 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking
0x0521	1 word	HEX	Secondary Port Status of Xpress-ring2 0x0000 : link down 0x0001 : forwarding 0x0002 : blocking

CLI Configuration

Node	Command	Description
enable	show modbus	This command displays the current Modbus configurations.
configure	modbus (disable|enable)	This command disables / enables the Modbus on the switch.

Web Configuration

System > Modbus



Parameter	Description
State	Select this option to enable / disable the Modbus on the Switch.
Apply	Click Apply to save your changes to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

PTP (IEEE-1588 v2)

PTP (Precision Time Protocol) is a distributed protocol to do time synchronization with each other systems in the network.

There are 4 different clocks in PTP:

1. **Ordinary Clock**: Switch communicates with the network by using specified single port. It will be same as grand master clock.
2. **Boundary Clock:** Switch can use multiple ports to communicate with network and each port behaves as ordinary clock. Port is selected as either master or member based on its local clock and data sets.
3. **Transparent Clock:** It forwards all received PTP messages and measures and accumulate delay timers in correction field.
4. **Forward Clock:** It forward all received PTP messages in domain ports.

PTP works in 2 phases:

1. **Establishing hierarchy**: Only ordinary or boundary clocks will have this phase.
   a. Processes all received announce messages by using "Best Master Clock (BMC)" algorithm and identifies itself as either master or member.
2. **Clock Synchronization:**
   a. Master sends "Sync" message to member
   b. Member sends "DReq (Delay Request)" message to master
   c. Master sends "Dresp (Delay Response)" message to member
   d. Member will adjust its clock by using parameters in above messages.

CLI Configuration

Node	Command	Description
Enable	sshow ptp informationhow interface eth0	This command displays PTP global configurations, PTP domain configurations and PTP port configurations
Enable	show ptp domain <Domain-ID>	This command displays specified PTP domain configurations.
Enable	show ptp port <Domain-ID> <Port-ID>	This command displays specified PTP domain and port configurations.
Configure	ptp enable	This command enables PTP.
Configure	No ptp enable	This command disables PTP.
Configure	ptp primary-domain <Domain-ID>	This command configures a specified Domain ID

		as the PTP's primary domain.
Configure	no ptp primary-domain	This command resets the primary domain ID default domain ID (0).
Configure	ptp domain <Domain-ID>	This command creates a specified domain in PTP.
Configure	no ptp domain <Domain-ID>	This command deletes a specified domain ID from PTP.
ptp_config	domain enable	This command enables the PTP domain.
ptp_config	No domain enable	This command disables PTP domain.
ptp_config	clock-mode <ordinary|boundary|transparent|forward>	This command assigns specified clock mode in PTP domain.
ptp_config	no clock-mode	This command deletes existing clock mode of PTP domain and assigns default clock mode (Forward) in PTP domain.
ptp_config	clock-priority1 <Value>	This command assigns specified priority for PTP

		domain dataset's 1st priority.
ptp_config	no clock-priority1	This command deletes existing 1st priority from PTP domain clock and assigns default priority value (128).
ptp_config	clock-priority2 <Value>	This command assigns specified priority for PTP domain dataset's 2nd priority.
ptp_config	no clock-priority2	This command deletes existing 2nd priority from PTP domain clock and assigns default priority value (128).
ptp_config	path-trace	This command enables path trace TLV and adds TLV in list.
ptp_config	No path-trace	This command disables path trace TLV in domain and deletes it from list.
ptp_config	slave	This command enables PTP domain as slave. PTP domain will be act as member in PTP network.
ptp_config	No slave	This command disables PTP domain

		as slave only. Based on clock data sets it can be act as either slave or master.
ptp_config	two-step-clk	This command enables two step clock mode in PTP domain.
ptp_config	No two-step-clk	This command disables two step clock mode and acts as one step clock as default.
ptp_config	exit	This command provides command prompt one step as "config" node.
ptp_config	end	This command provides command prompt as "enable" node.
ptp_config	port <Port-ID>	This command creates port data sets in PTP domain.
ptp_config	No port <Port-ID>	This command deletes port data sets from PTP domain.
ptp_config_port	port enable	This command enables PTP port in domain.
ptp_config_port	No port enable	This command disables PTP port in domain.
ptp_config_port	acceptable-master enable	This command enables PTP port in domain as acceptable master.
ptp_config_port	No acceptable-master enable	This command deletes PTP port in domain from acceptable master list.
ptp_config_port	announce interval <0-4>	This command configures to send periodical announce messages in specified intervals in PTP port.
ptp_config_port	no announce interval	This command deletes existing announce interval from PTP port and adds default interval (1).
ptp_config_port	announce timeout <2-10>	This command configures specified value as announce time in PTP port.
ptp_config_port	no announce timeout	This command deletes existing announce timeout from PTP port and adds default timeout (3).
ptp_config_port	sync interval [-1, 1]	This command configures synchronization

		interval of PTP port as specified value.
ptp_config_port	no sync interval	This command deletes existing synchronization interval from PTP port and adds default value (0).
ptp_config_port	vlan <VLAN LIST>	This command configures specified VLAN list to PTP port.
ptp_config_port	no vlan <VLAN LIST>	This command deletes specified VLAN list from PTP port.
ptp_config_port	exit	This command provides command prompt one step as "ptp_config" node.
ptp_config_port	end	This command provides command prompt as "enable" node.

Example:

- Enabling PTP: This command is used to enable PTP; by default PTP is disabled
  TI-BG62i(config)#ptp enable

- Disabling PTP: This command is used to disable PTP
  TI-BY62i(config)#no ptp enable

- Adding Primary Domain: This command is used to add specified domain ID as primary domain in PTP; By default primary domain ID is 0.
  Ti-BG62i(config)#ptp primary-domain 1

- Deleting Primary Domain: This command is used to delete existing primary domain ID from PTP and adds default domain ID (0) as primary domain ID
  TI-BG62i(config)#no ptp primary-domain

- Creating PTP Domain: This command is used to create a new PTP domain and provies us command prompt as "config-ptp" note.
  TI-BG62i(config)#ptp domain 1

- Deleting Existing PTP Domain: This command is delete existing PTP domain from domain list.
  TI-BG62I(config)#no ptp domain 1

- Enabling PTP Domain: This command is used to enable PTP domain; by default PTP domain is enabled.
  TI-BG62I(config-ptp)#domain enable

- Disabling PTP Domain: This command is used to disable PTP domain.
  TI-BG62I(config-ptp)#no domain enable

- Adding Clock Mode in PTP Domain: This command is used to add clock mode in domain; by default domain is in forward clock mode.
  TI-BG62I(config-ptp)#clk-mode ordinary
  TI-BG62I(config-ptp)#clk-mode boundary
  TI-BG62I(config-ptp)#clk-mode transparent
  TI-BG62I(config-ptp)#clk-mode forward

- Deleting Clock Mode from PTP Domain: This command is used to delete existing clock mode from PTP domain and adds "Forward" mode as domain's clock mode.
  TI-BG62I(config-ptp)#no clk-mode

- Adding 1st Priority in PTP Domain: This command is used to add 1st priority in PTP domain; by default domain's 1st priority is 128.
  TI-BG62I(config-ptp)#clk-priority1 20

- Deleting 1st Priority from PTP Domain: This command is used to delete existing 1st priority from PTP domain and adds 128 as domain's first priority.

TI-BG62I(config-ptp)#no clk-priority1

- Adding 2nd Priority in PTP Domain: This command is used to add 2nd priority in PTP domain; by default domain's 2nd priority is 128.
  TI-BG62I(config-ptp)#clk-priority2 30

- Deleting 2nd Priority from PTP Domain: This command is used to delete existing 2nd priority from PTP domain and adds domain's 2nd priority as 128.
  TI-BG62I(config-ptp)#no clk-priority2

- Enabling Path Trace in PTP Domain: This command is used to enable path trace TLV in PTP domain; by default path trace is disabled.
  TI-BG62I(config-ptp)#path-trace

- Disabling Path Trace from PTP Domain: This command is used to disable path trace from PTP domain.
  TI-BG62I(config-ptp)#no path-trace

- Enabling Slave Mode in PTP Domain: This command is used to enable PTP domain as slave only. In PTP network it will be act as member (slave). By default slave mode is disabled in PTP domain.
  TI-BG62I(config-ptp)#slave

- Disabling Slave Mode from PTP Domain: This command is used to disable slave mode from PTP domain. PTP domain will be act as either Master or Member based on received data sets by using BMC (Best Master Clock) algorithm.
  TI-BG62I(config-ptp)#no slave

- Enabling Two Step Clock in PTP Domain: This command is used to enable two step clock mode in PTP domain; by default two step clock is disabled in domain.
  TI-BG62I(config-ptp)#two-step-clk

- Disabling Two Step Clock from PTP Domain: This command is used to disable two step clock mode from PTP domain.
  TI-BG62I(config-ptp)#no two-step-clk

- Creating PTP Port in Domain: This command is used to create PTP port in domain with default values and it provides us "config-ptp-port" command prompt.
  TI-BG62I(config-ptp)#port 1
  TI-BG62I(config-ptp-port)#

- Deleting PTP Port from Domain: This command is used to delete PTP port from Domain.
  TI-BG62I(config-ptp)#no port 1

- Enabling PTP Port: This command is used to enable PTP port; by default PTP port is disabled.
  TI-BG62I(config-ptp-port)#port enable

- Disabling PTP Port: This command is used to disable PTP port.
  TI-BG62I(config-ptp-port)#no port enable

- Enabling Acceptable Master in PTP Port: This command is used to enable acceptable master mode in PTP port; by default it is disabled.
  TI-BG62I(config-ptp-port)#acceptable-master enable

- Disabling Acceptable Master in PTP port: This command is used to disable acceptable maser mode in PTP port.
  TI-BG62I(config-ptp-port)#no acceptable-master enable

- Adding Announce Interval in PTP port: This command is used to add announce interval in PTP port; by default announce interval value in PTP port is 1
  TI-BG62I(config-ptp-port)#announce interval 2

- Deleting Announce Interval from PTP Port: This command is used to delete existing announce interval from PTP port and adds 1 (default value) as announce interval in PTP port.
  TI-BG62I(config-ptp-port)#no announce interval
- Adding Announce Timeout in PTP Port: This command is used to add specified value as announce timeout in PTP port; by default announce timeout value is 3.
  TI-PG1284I(config-ptp-port)#announce timeout 3

- Deleting Announce Timeout from PTP Port: This command is used to delete existing announce timeout value from PTP port and adds 3 (default value) as announce timeout in PTP port.
  TI-PG1284I(config-ptp-port)#no announce timeout

- Adding Synchronous Interval in PTP Port: This command is used to add specified value synchronous interval in PTP port; by default synchronous interval is 0.
  TI-PG1284I(config-ptp-port)#sync interval 1

- Deleting Synchronous Interval from PTP Port: This command is used to delete existing synchronous interval from PTP port and adds 0 (default value) as synchronous interval.
  TI-PG1284I(config-ptp-port)#no sync interval

- Adding VLAN List into PTP Port: This command is used to add specified VLAN list into PTP port; by default there is no VLAN list in PTP port.
  TI-PG1284I(config-ptp-port)#vlan 1-10

- Deleting VLAN List from PTP Port: This command is used to delete specified VLAN list from PTP port.
  TI-PG1284I(config-ptp-port)#no vlan 5-6

- Displays All PTP Configurations: This command is used to display all existing PTP configurations.
  TI-PG1284I#show ptp information
  PTP Status: Disable
  PTP Primary Domain: 0(Default)

Domain ID: 1

Domain Status: Disabled
Slave Mode: Disabled
Path Trace Mode: Disabled
Clock Mode: Forward(Default)
Two Step Clock Mode: Disabled
Clock Priority_1: 128(default)
Clock Priority_2: 128(default)
Port ID: 1
Port Status: Disabled
Announce Interval: 3
Announce Timeout: 4
Delay Interval: 0(Default)
Sync Interval: 1
Acceptable Master Status: Enabled
VLAN IDs: None

- Displays PTP Domain Configurations: This command is used to display specified PTP domain configurations.
  TI-PG1284I#show ptp domain 1

Domain ID: 1

Domain Status: Disabled
Slave Mode: Disabled
Path Trace Mode: Disabled
Clock Mode: Forward (Default)
Two Step Clock Mode: Disabled
Clock Priority_1: 128(default)
Clock Priority_2: 128(default)

Port ID: 1
Port Status: Disabled
Announce Interval: 3
Announce Timeout: 4
Delay Interval: 0(Default)
Sync Interval: 1
Acceptable Master Status: Enabled
VLAN IDs: None

- Displays PTP Port Configurations: This command is used to display specified PTP port configurations.

TI-PG1284I#show ptp port 1 1
Port ID: 1
Port Status: Disabled
Announce Interval: 3
Announce Timeout: 4
Delay Interval: 0(Default)
Sync Interval: 1
Acceptable Master Status: Enabled

VLAN IDs: None

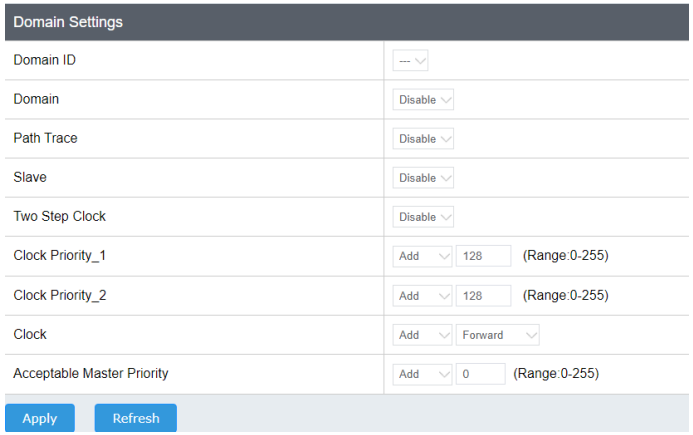
Web Configuration

System > PTP > General Settings

Parameter	Description
PTP State	Enables / Disables the global PTP state.
Domain ID	Creates / Removes a Domain.
Primary Domain	Configure the primary domain.
PTP Status	
PTP Status	The current global PTP state.
PTP Primary Domain	The primary domain.

Domain Settings

System > PTP > Domain Settings

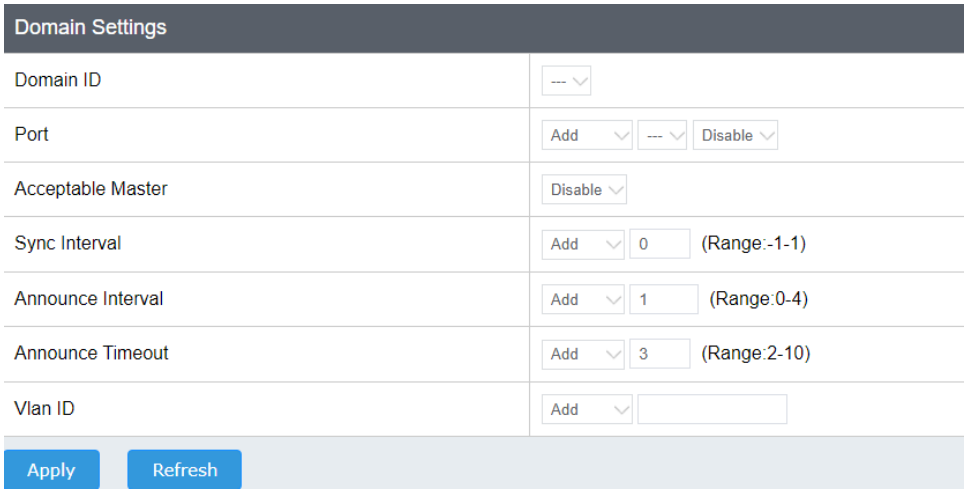


Parameter	Description
Domain ID	Creates / Removes a Domain.
Path Trace	The current path track mode of the domain.
Slave	The current slave mode of the domain.
Two Step Clock	The current Two Step clock mode of the domain.
Clock Priority_1	Configures a priority for PTP domain dataset's 1st priority. The default priority value is 128.
Clock Priority_2	Configures a priority for PTP domain dataset's 2nd priority. The default priority value is 128.
Clock	Ordinary Clock - Switch communicates with the network by using specified single port. It will be same as grand master clock. Boundary Clock - Switch can use multiple ports to communicate with network and each port behaves as ordinary clock. Port is selected as either master or member based on its local clock and data sets. Transparent Clock - It forwards all received PTP messages and measures and accumulate delay timers in correction field. Forward Clock - It forward all received PTP messages in domain ports.

Acceptable Master Priority	Enable - enables PTP port in domain as acceptable master. Disable - deletes PTP port in domain from acceptable master list.

Port Settings

System > PTP > Port Settings



Parameter	Description
Domain ID	
Port	
Acceptable Master	Enable - enables PTP port in domain as acceptable master. Disable - deletes PTP port in domain from acceptable master list.
Sync Interval	Add - configures synchronization interval of PTP port as specified value. Default - deletes existing synchronization interval from PTP port and adds default value (0).
Announce Interval	Add - configures to send periodical announce messages in specified intervals in PTP port. Default - deletes existing announce interval from PTP port and adds default interval (1).
Announce Timeout	Add - configures specified value as announce time in PTP port. Default - deletes existing announce timeout from PTP port and adds default timeout (3).
VLAN ID	Add - configures specified VLAN list to PTP port. Remove - deletes specified VLAN list from PTP port.

Auto Provision

Auto provision is a service that service provider can quickly, easily and automatically configure remote device or doing firmware upgrade at remote side.

1. When the Auto Provision is enabled, the Switch will download the auto provision information file from the auto provision server first.

The file name is followed below naming rule:

Model_Name_Autoprovision.txt

For Example: ***SWITCH*_Autoprovision.txt**

The contents of the file are listed below:

AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=8648P-999-1.1.0.S0
Firmware_Image_File=8648P-999-1.1.0.S0.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=8648P-999-1.1.0.S0.save
Global_Configuration_Reboot=0
Specific_Configuration_State=0

Specific_Configuration_Reboot=0

2. If AUTO_PROVISION_VER is biggest than current auto provision version, do step 3; otherwise, wait 24 hours and go back to step 1.
3. If the Firmware_Upgrade_State =1, do step 4; otherwise, do step 6.
4. If the Firmware_Version is difference than current firmware version, download the Firmware_Image_File and upgrade firmware.
5. If upgrade firmware succeeded and Firmware_Reboot=1, let reboot_flag=1.
6. If the Global_Configuration_State =1, download the Global_Configuration_File and upgrade configuration; otherwise, do step 8.
7. If upgrade configutation succeeded and Global_Configuration_Reboot =1, let reboot_flag=1.
8. If the Specific_Configuration_State =1, download the specific configuration file and upgrade configuration; otherwise do step 10. The naming is "Model_Name _" with 12-bit MAC digits ,example for following is "INS-8648P***_00e04c8196b9.txt***"
9. If upgrade configutation succeeded and Specific_Configuration_Reboot =1, let reboot_flag=1.
10. If reboot_flag=1, save running configuration and reboot the switch; otherwise, wait 24 hours and go back to step 1.

Default Settings

Auto provision configuration profile:

Active: Disable
Version: 0
Protocol: FTP
FTP user/pwd: /
Folder:
Server address:

CLI Configuration

Node	Command	Description
enable	show auto-provision	This command displays the current auto provision configurations.
configure	auto-provision	This command enters the auto-provision node.
auto-provision	show	This command displays the current auto provision configurations.
auto-provision	active (enable|disable)	This command enables/disables the auto provision function.
auto-provision	server-address IPADDR	This command configures the auto provision server's IP.
auto-provision	protocol (tftp|http|ftp)	The command configurations the upgrade protocol.
auto-provision	FTP-user username STRING password STRING	The command configurations the username and password for the FTP server.
auto-provision	folder STRING	The command configurations the folder for the auto provision server.
auto-provision	no folder	The command configurations the folder to default.
auto-provision	no FTP-user	The command configurations the username and password to default.

Web Configuration

System > Auto Provision

Auto Provision Settings	
State	Disable
Status	Disabled
Version	0
Protocol	TFTP
Server IP	IPv4
	0.0.0.0
Username	
User Password	
Folder Path	

Parameter	Description
State	Select Enable or Disable Auto Provision
Status	Displays the current status of Auto Provision
Version	Displays the current version
Protocol	Select the type of protocol for Auto Provision
Server IP	Enter the IP Address for the Server IP
Username	Input the username
User Password	Input the Password
Folder Path	Input the folder path

Physical Interface

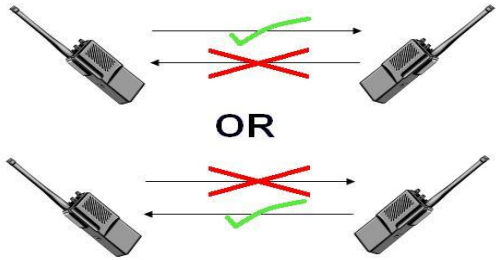
Port Settings

- 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:

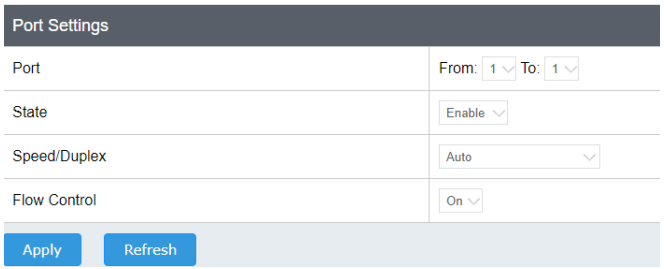
[DEVICE_NAME]#*configure terminal*

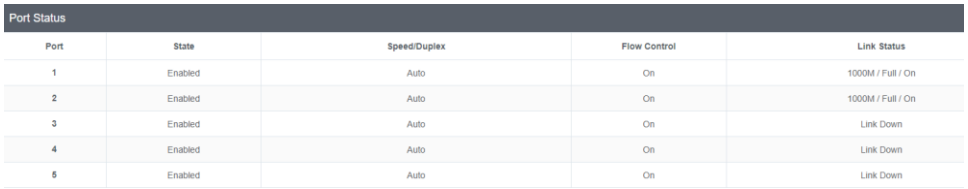
[DEVICE_NAME](config)#*interface gi1/0/1*

[DEVICE_NAME](config-if)#*speed auto*

Web Configuration

Network > Physical 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.

Spanning Tree Protocol

STP/RSTP

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multi Spanning Tree Protocol

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.

In STP, the port states are Blocking, Listening, Learning, Forwarding.

In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this document, "STP" refers to both STP and RSTP.

STP Terminology

- The root bridge is the base of the spanning tree.
- Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

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

- On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.
- For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

Forward Time (Forward Delay):

This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.

Max Age:

This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Hello Time:

This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

PathCost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge, the slower the media, the higher the cost.

How STP Works?

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed. Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

802.1D STP

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under the OSI layer-2. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

The Spanning Tree Protocol (STP) is defined in the IEEE Standard 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges

(typically Ethernet switches), and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

STP switch port states

- Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
- Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
- Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
- Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

802.1w RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

RSTP bridge port roles:

- Root - A forwarding port that is the best port from Nonroot-bridge to Rootbridge
- Designated - A forwarding port for every LAN segment
- Alternate - An alternate path to the root bridge. This path is different than using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

Edge Port:

They are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

Forward Delay:

The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).

Transmission Limit:

This is used to configure the minimum interval between the transmissions of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The range is from 1 to 10 seconds.

Hello Time:

Set the time at which the root switch transmits a configuration message. The range is from 1 to 10 seconds.

Bridge priority:

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device.

Port Priority:

Set the port priority in the switch. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240.

Path Cost:

The valid value is from 1 to 200000000. Higher cost paths are more likely to be blocked by STP if a network loop is detected.

BPDU Guard:

This is a per port setting. If the port is enabled in BPDU guard and receive any BPDU, the port will be set to disable to avoid the error environments. User must enable the port by manual.

BPDU Filter:

It is a feature to filter sending or receiving BPDUs on a switch port. If the port receives any BPDUs, the BPDUs will be dropped.

Notice:

If both of the BPDU filter and BPDU guard are enabled, the BPDU filter has the high priority.

Root Guard:

The Root Guard feature forces an interface to become a designated port to prevent surrounding switches from becoming a root switch. In other words, Root Guard provides a way to enforce the root bridge placement in the network. The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature receives a superior BPDU, it moves the port into a rootinconsistent state (effectively equal to a listening state), thus maintaining the current Root Bridge status. The port can be moved to forwarding state if no superior BPDU received by this port for three hello times.

Default Settings:

STP/RSTP:		disabled.
STP/RSTP mode:		RSTP.
Forward Time:		15 seconds.
Hello Time:		2 seconds.
Maximum Age:		20 seconds.
System Priority:		32768.
Transmission Limit:		3 seconds.
Per port STP state:		enabled.
Per port Priority:		128.
Per port Edge port:		disabled.
Per port BPDU filter:		disabled.
Per port BPDU guard:		disabled.
Per port BPDU Root guard:		disabled.
Per port Path Cost:		depend on port link speed.
Example: Bandwidth	->	STP Port Cost Value
10 Mbps	->	100
100 Mbps	->	19
1 Gbps	->	4
10 Gbps	->	2

CLI Configuration

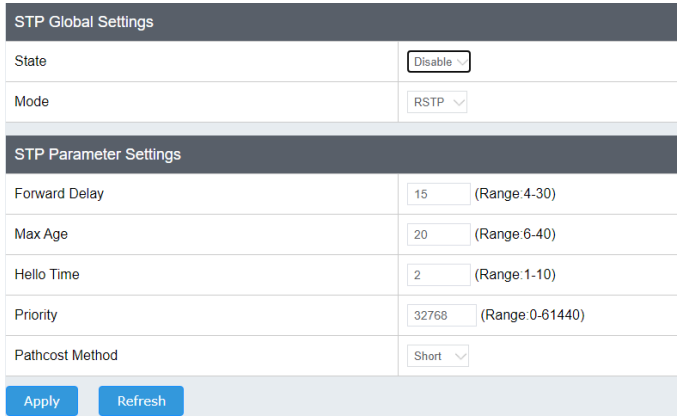
Node	Command	Description
enable	show spanning-tree active	This command displays the spanning tree information for only active port(s)

enable	show spanning-tree blockedports	This command displays the spanning tree information for only blocked port(s)
enable	show spanning-tree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree summary	This command displays the summary of port states and configurations
enable	clear spanning-tree counters	This command clears spanning-tree statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears spanning-tree statistics for a specific port.
configure	spanning-tree (disable | enable)	This command disables / enables the spanning tree function for the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (forward-delay,max-age,hello-time).
configure	no spanning-tree algorithm-timer	This command configures the default values for forward-time & max-age & hello-time.
configure	spanning-tree forward-time <4-30>	This command configures the bridge forward delay time (sec).
configure	no spanning-tree forward-time	This command configures the default values for forward-time.
configure	spanning-tree hello-time <1-10>	This command configures the bridge hello time(sec).
configure	no spanning-tree hello-time	This command configures the default values for hello-time.
configure	spanning-tree max-age<6-40>	This command configures the bridge message max-age time(sec).
configure	no spanning-tree max-age	This command configures the default values for max-age time.
configure	spanning-tree mode (rstp|stp)	This command configures the spanning mode.
configure	spanning-tree pathcost method (short|long)	This command configures the pathcost method.
configure	spanning-tree priority<0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree (disable|enable)	This command configures enables/disables the STP function for the specific port.
interface	spanning-tree bpdufilter (disable|enable)	This command configures enables/disables the bpdufilter function for the specific port.
interface	spanning-tree bpduguard (disable|enable)	This command configures enables/disables the bpduguard function for the specific port.
interface	spanning-tree rootguard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
interface	spanning-tree edge-port (disable|enable)	This command enables/disables the edge port setting for the specific port.
interface	spanning-tree cost VALUE	This command configures the cost for the specific port.

		Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	spanning-tree (disable|enable)	This command configures enables/disables the STP function for the specific port.
if-range	spanning-tree bpdufilter (disable|enable)	This command configures enables/disables the bpdufilter function for the specific port.
if-range	spanning-tree bpduguard (disable|enable)	This command configures enables/disables the bpduguard function for the specific port.
if-range	spanning-tree rootguard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning-tree edge-port (disable|enable)	This command enables/disables the edge port setting for the specific port.
if-range	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range:
		16-bit based value range 1-65535, 32-bit based value range 1-200000000.
if-range	no spanning-tree cost	This command configures the path cost to default for the specific port.
if-range	spanning-tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
if-range	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

Web Configuration

Network > Spanning Tree > Protocol

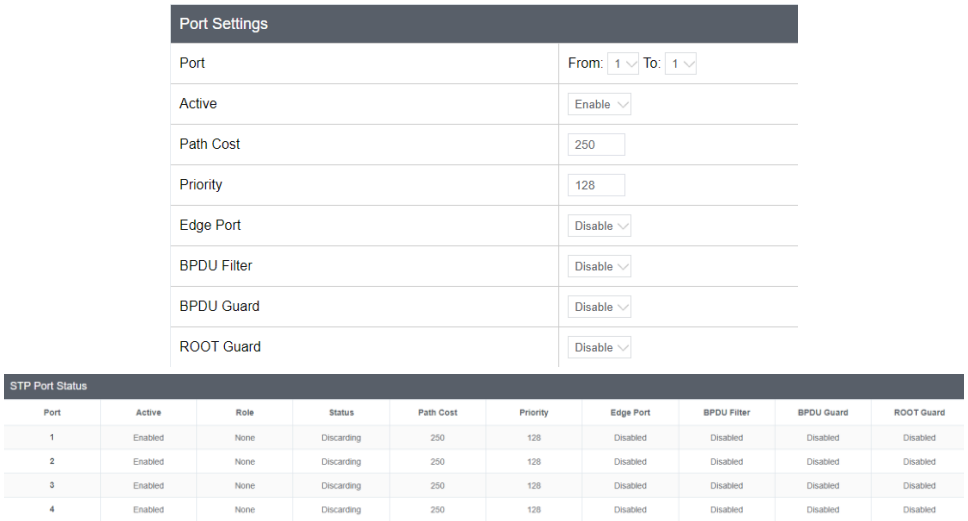


Parameter	Description
State	Select **Enabled** to use Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), or Multi Spanning Tree Protocol (MSTP)

Mode	Select to use either Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), or Multi Spanning Tree Protocol (MSTP).
Forward Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Priority	Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Enter a value from 0~61440. The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
Pathcost Method	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.

Port Parameters

Advanced Settings > Spanning Tree > Port



Parameter	Description
Port	Selects a port that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.

BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.
Port Status	
Active	The state of the STP function.
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filter function.
BPDU Guard	The state of the BPDU guard function.
ROOT Guard	The state of the BPDU Root guard function.

Link Aggregation

Static Trunk

Link Aggregation (Trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports. The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

Default Settings:

The default group Link Aggregation state is disabled for all groups.

The default group Link Aggregation load balance is source MAC and destination MAC for all groups.

Maximum link aggregation group: 6

Maximum port in link aggregation group: 8

CLI Configuration

Node	Command	Description
enable	show link-aggregation	The command displays the current trunk configurations.
configure	link-aggregation [GROUP_ID] (disable | enable)	The command disables / enables the trunk on the specific trunk group.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	The command adds ports to a specific trunk group.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	The commands delete ports from a specific trunk group.

Example:

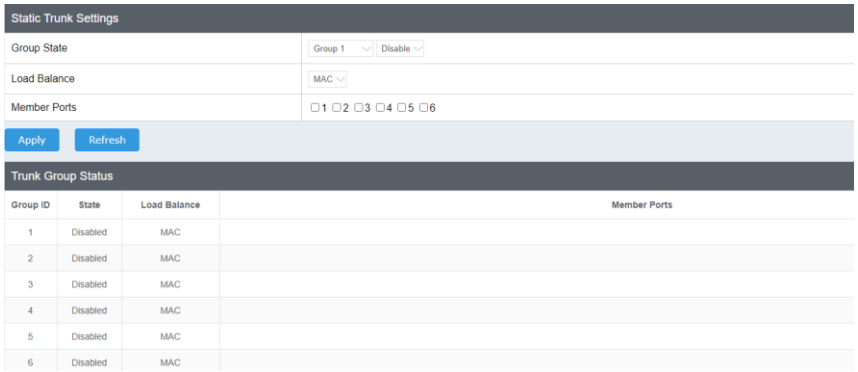
[DEVICE_NAME]#*configure terminal*

[DEVICE_NAME](config)#*link-aggregation 1 enable*

[DEVICE_NAME](config)#*link-aggregation 1 ports 1-4*

Web Configuration

Network > Trunk > Settings



Parameter	Description
Group State	Select the group ID to use for this trunk group, that is, one logical link containing multiple ports. Select **Enable** to use this static trunk group.
Load Balance	Configures the load balance algorithm for the specific trunk group.
Member Ports	Select the ports to be added to the static trunk group.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
Trunk Group Status	
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
State	This field displays if the trunk group is enabled or disabled.
Load Balance	This field displays the load balance policy for the trunk group.
Member Ports	This field displays the assigned ports that comprise the static trunk group.

LACP

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention.

Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, and duplex mode and flow control settings.
- Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

System Priority:

The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP), the smaller the number, the higher the priority level.

System ID:

The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

Administrative Key:

The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:

- Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium.
- Configuration restrictions that you establish.

Port Priority:

The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Default Settings:

The default System Priority is 32768.

The default group LACP state is disabled for all groups.

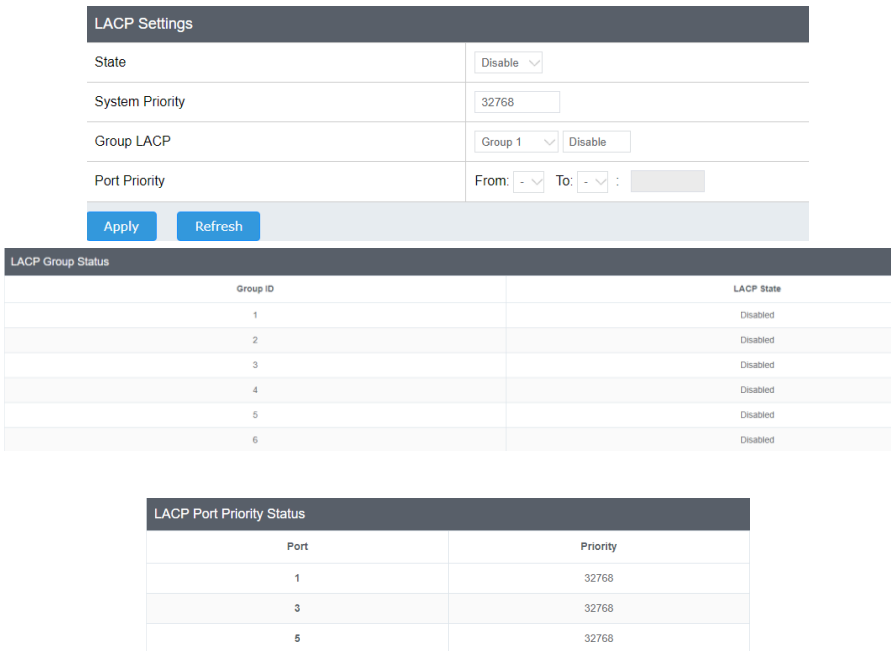
CLI Configuration

Node	Command	Description
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor's information for the specific group or all groups.
enable	show lacp port_priority	This command displays the port priority for the LACP.
enable	show lacp sys_id	This command displays the actor's and partner's system ID.
configure	lacp (disable | enable)	This command disables / enables the LACP on the switch.
configure	lacp GROUP_ID (disable | enable)	This command disables / enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority<1-65535>	This command configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default for the system priority for the LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port. Note: The default value is 32768.
interface	no lacp port_priority	This command configures the default for the priority for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	lacp port_priority <1-65535>	This command configures the priority for the specific ports. Note: The default value is 32768.
if-range	no lacp port_priority	This command configures the default for the priority for the specific ports.

Web Configuration

Link Aggregation Settings

Network > Trunk > Port Priority



Parameter	Description
State	Select **Enable** from the drop down box to enable Link Aggregation Control Protocol (LACP). Select **Disable** to not use LACP.
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group LACP	Select a trunk group ID and then select whether to **Enable** or **Disable** Group Link Aggregation Control Protocol for that trunk group.
Port Priority	Select a port or a range of ports to configure its (their) LACP priority.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
LACP Group Status	
Group ID	The field identifies the LACP group ID.
LACP State	This field displays if the group has LACP enabled.
LACP Group Status	
Port	The field identifies the port ID.
Priority	The field identifies the port's LACP priority.

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:

[DEVICE_NAME]#*configure terminal*

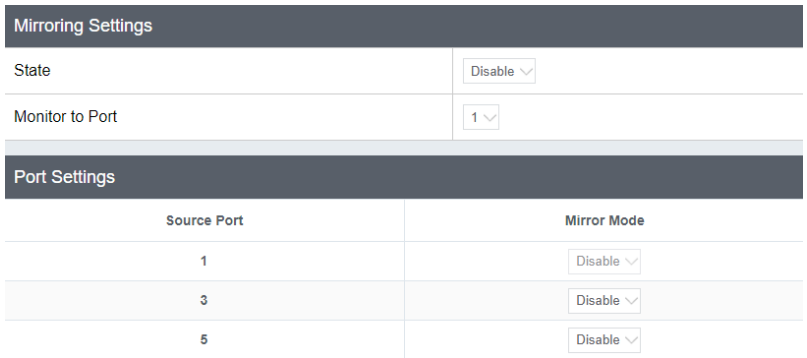
[DEVICE_NAME](config)#mirror enable

[DEVICE_NAME](config)#mirror destination port 2

[DEVICE_NAME](config)#mirror source ports 3-5 mode both

Web Configuration

Network > 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.

Loop Detection

Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

The loop detection function sends probe packets periodically to detect if the port connect to a network in loop state. The Switch shuts down a port if the Switch detects that probe packets loop back to the same port of the Switch.

Loop Recovery:

When the loop detection is enabled, the Switch will send one probe packets every two seconds and then listen this packet. If it receives the packet at the same port, the Switch will disable this port. After the time period, ***recovery time*****,** the Switch will enable this port and do loop detection again.

The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.

Default Settings

The default global Loop-Detection state is disabled.

The default Loop Detection Destination MAC is **00:0b:04:AA:AA:AB**

The default Port Loop-Detection state is disabled for all ports.

The default Port Loop-Detection status is unblocked for all ports.

The loop detection on the Switch is disabled.

Loop Detection Destination MAC=00:0b:04:aa:aa:ab

Port	State	Status	Recovery State	Time	Port	State	Status	Recovery State	Time
1	Disabled	Normal	Enabled	1	2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1	4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1	6	Disabled	Normal	Enabled	1
7	Disabled	Normal	Enabled	1	8	Disabled	Normal	Enabled	1
9	Disabled	Normal	Enabled	1	10	Disabled	Normal	Enabled	1
11	Disabled	Normal	Enabled	1	12	Disabled	Normal	Enabled	1
13	Disabled	Normal	Enabled	1	14	Disabled	Normal	Enabled	1
15	Disabled	Normal	Enabled	1	16	Disabled	Normal	Enabled	1

CLI Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable | enable)	This command disables / enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default (00:0b:04:AA:AA:AB).

interface	loop-detection (disable | enable)	This command disables / enables the loop detection on the port.
interface	no shutdown	This command enables the port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable | enable)	This command enables / disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	loop-detection (disable | enable)	This command disables / enables the loop detection on the ports.
if-range	loop-detection recovery (disable | enable)	This command enables / disables the recovery function on the port.
if-range	loop-detection recovery time VALUE	This command configures the recovery period time.

Example:

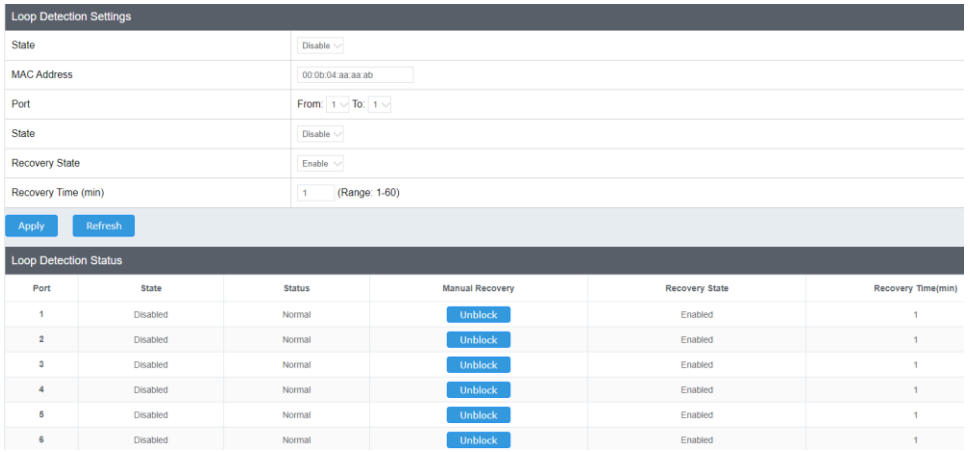
[DEVICE_NAME](config)*#loop-detection enable*

[DEVICE_NAME](config)*#interface 1/0/1*

[DEVICE_NAME](config-if)*#loop-detection enable*

Web Configuration

Network > Loop Detection



Parameter	Description
State	Select this option to enable loop guard on the Switch.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select **Enable** to use the loop guard feature on the Switch.
Recovery State	Select **Enable** to reactivate the port automatically after the designated recovery time has passed.
Recovery Time	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Loop Detection Status	

Port	This field displays a port number.
State	This field displays if the loop guard feature is enabled.
Status	This field displays if the port is blocked.
Manual Recovery	Manually recover from the loop
Recovery State	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

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.

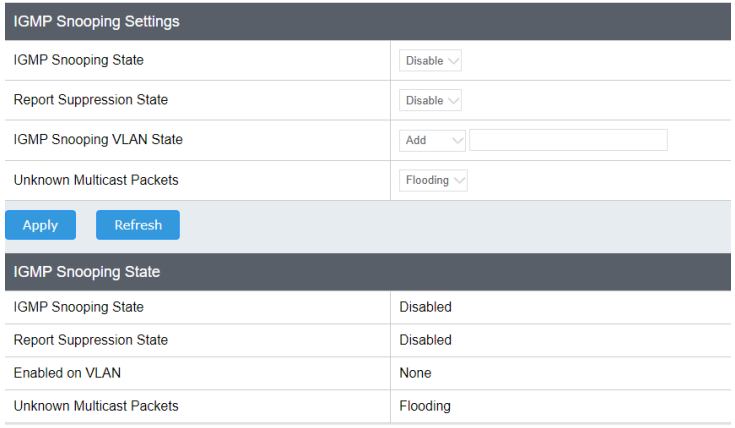
Example:

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

Web Configuration

General Settings

Network > IGMP Snooping > Settings

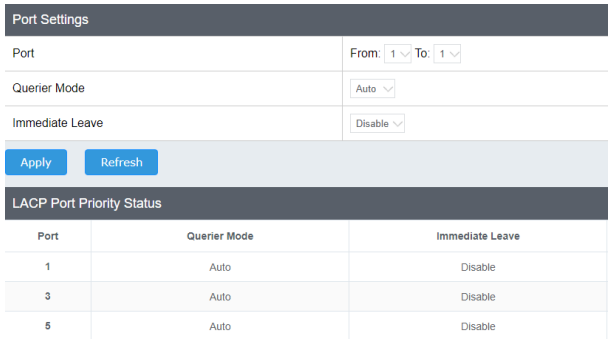


Parameter	Description
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate the feature.
Report Suppression State	Select **Enable** to allow the IGMP Snooping to report the suppression state. Select **Disable** to deactivate this 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

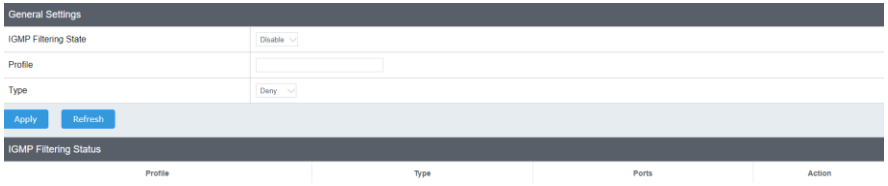
Network > IGMP Snooping > Port Settings



Parameter	Description
Port	Select the range of the port.
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.

IGMP Filtering

Network > IGMP Filtering > General Settings

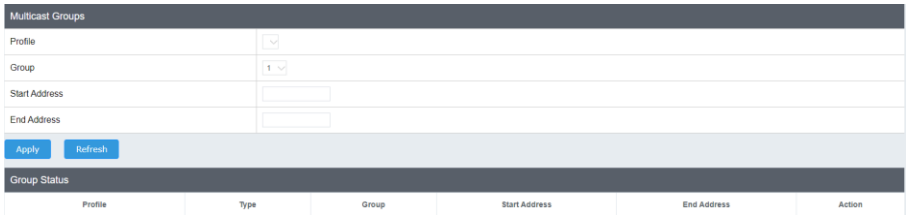


Parameter	Description
IGMP Filtering State	Select **Enabled** to enable IGMP Filtering, and **Disabled** to disable this feature
Profile	Enter the name of the IGMP Filtering group.

Type	Select **Permit** to allow the traffic through and **Deny** to deny the traffic
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
IGMP Filtering Status	
Profile	Displays the name of the profile
Type	Displays the traffic permission
Port	The port ID.
Action	Click **Delete** to remove the profile from the database

Multicast Groups

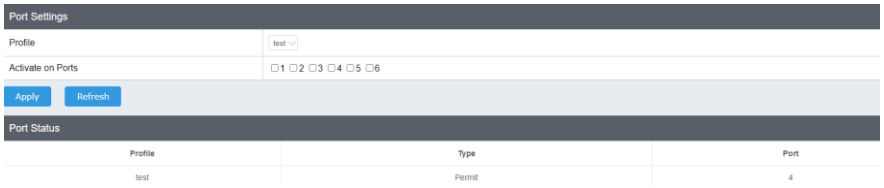
Network > IGMP Filtering > Multicast Groups



Parameter	Description
Profile	Select the profile created from General Settings
Group	Select the group from the drop down menu
Start Address	Input the beginning range of the IP address
End Address	Input the ending range of the IP address
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
Group Status	
Profile	Displays the name of the profile
Type	Displays the traffic permission
Group	Displays the Group ID
Start Address	Displays the beginning range of the IP address
End Address	Displays the end range of the IP address
Action	Click **Delete** to remove the profile from the database

IGMP Filtering: Port Settings

Network > IGMP Filtering > Port Settings



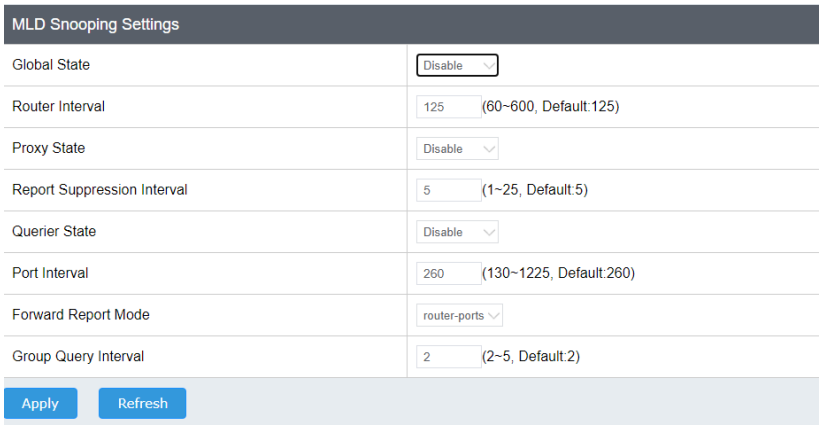
Parameter	Description
Profile	Select the profile created from General Settings
Group	Select the group from the drop down menu

Activate on Ports	Select the ports to activate IGMP filtering
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
Port Status	
Profile	Displays the name of the profile
Type	Displays the traffic permission
Port	Display the port that the setting is activated on

MLD Snooping

MLD Snooping Settings

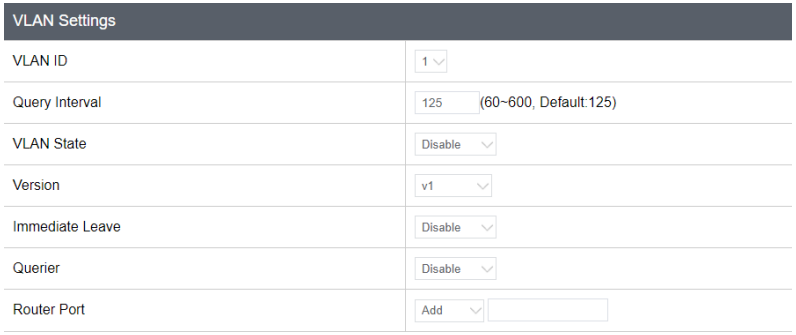
Network > MLD Snooping > General Settings



Parameter	Description
Global State	Select **Enabled** to enable MLD Snooping or **Disable** to deactivate this feature
Router Interval	Input the router interval
Proxy State	Select **Enabled** to enable Proxy State in MLD Snooping or **Disable** to deactivate this feature
Report Suppression Interval	Input the report suppression interval
Querier State	Select **Enabled** to enable Querier State in MLD Snooping or **Disable** to deactivate this feature
Port Interval	Input the port interval level
Forward Report Mode	Select **all-ports** to forward reports in all ports or **router-ports** to only forward ports from the router
Group Query Interval	Input the query interval group

MLD Snooping VLAN Settings

Network > MLD Snooping > VLAN Settings



Parameter	Description

VLAN ID	Select the VLAN ID to apply to the MLD Snooping
Query Interval	Input the Query Interval
VLAN State	Select **Enabled** to enable the MLD Snooping in this VLAN State and **Disable** to deactivate this feature
Version	Select the MLD Snooping version to use
Immediate Leave	Select **Enabled** to enable Immediate Leave in MLD Snooping or **Disable** to deactivate this feature
Querier	Select **Enabled** to enable Querier in MLD Snooping or **Disable** to deactivate this feature
Router Port	Select **Add** to add the router port or **Delete** to delete the port. The port number can be input in the field box.

MVR

MVR

MVR refers to Multicast VLAN Registration that enables a media server to transmit multicast stream in a single multicast VLAN while clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join/leave message to a receiver port. The receiver port belonging to one of the multicast groups can receive multicast stream from media server. Without support of MVR, the Multicast stream from media server and subscriber must reside in the same VLAN.

- Source ports: The Stream source ports.
- Receiver ports: The Client ports.
- Tagged ports: Configure the tagged ports for source ports or receiver ports.

MVR Mode

- **Dynamic Mode:**
  If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will be forwarded to a multicast router through its source port. Multicast router knows which multicast groups exist on which interface dynamically.
- **Compatible mode:**
  If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will not be transmitted to a multicast router.

Operation Mode

- **Join Operation:**
  A subscriber sends an IGMP report message to the switch to join the appropriate multicast. The next depends on whether the IGMP report matches the switch configured multicast MAC address. If it matches, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of MVLAN.
- **Leave Operation:**
  Subscriber sends an IGMP leave message to the switch to leave the multicast. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another subscriber in the VLAN, subscriber must respond within the max response time. If there is no subscriber, the switch would eliminate this receiver port.
- **Immediate Leave Operation:**
  Subscriber sends an IGMP leave message to the switch to leave the multicast. Subscribers do not need to wait for the switch CPU to send an IGMP group-specific query through the receiver port VLAN. The switch will immediately eliminate this receiver port.

Figure-1:

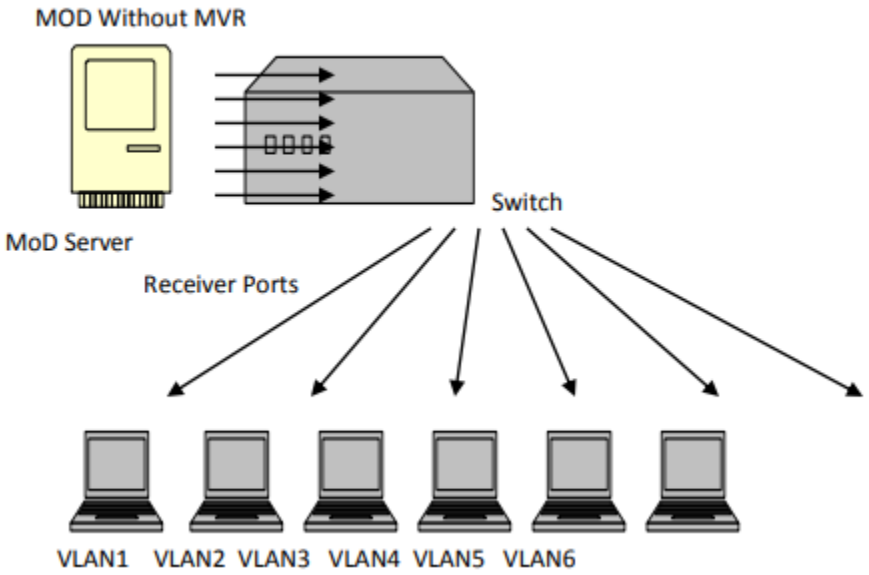
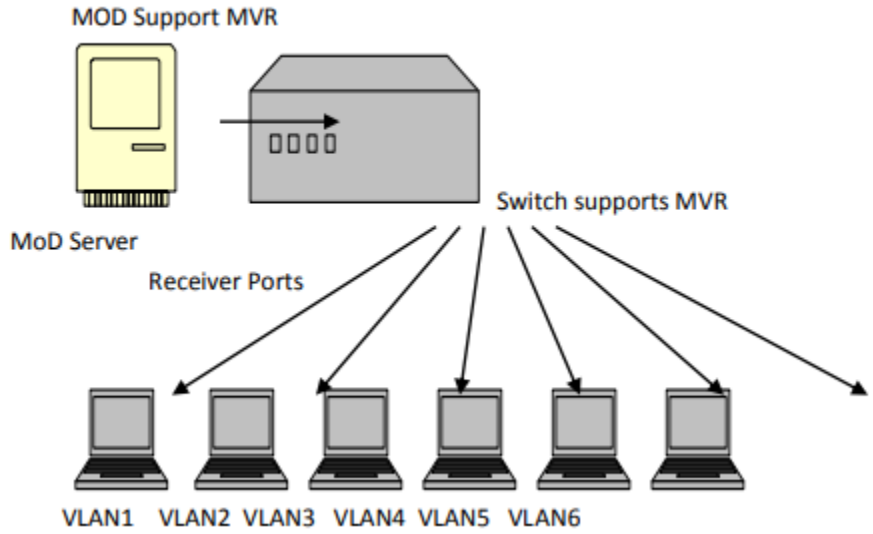


Figure-2:



Default Settings

There is no MVR VLAN.

Default configuration for a new MVR:

MVR VLAN Information

- VLAN ID: 2
- Name: MVR2
- Active: Enabled
- Mode: Dynamic
- Source Port(s): None
- Receiver Port(s): None
- Tagged Port(s): None

The Switch allows user to create up to 250 groups.

The Switch allows user to create up to 16 MVRs.

Notices

- IGMP snooping and MVR can be independently enabled.
- IGMP snooping and MVR use the same IGMP timers.
- MVR can recognize IGMPv3 reports.
- About the IGMPv3 report, switch doesn't treat those group records with the following group record types as membership reports. Those group record types are MODE_IS_INCLUDE, CHANGE_TO_INCLUDE_MODE, ALLOW_NEW_SOURCES and BLOCK_OLD_SOURCES.
- Don't use the group address X.0.0.1 for your multicast stream. It is because the system detects and records the 224.0.0.1 for dynamic querier port. The group address X.0.0.1 may conflict with 224.0.0.1.
- Because the lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. When you configure group address, the Switch compares the lower 23 bits only.
- CLI command "group 1 start-address 224.1.1.1 6", it creates 6 groups. That is, one IP, one group.
- The MVR name should be the combination of the digit or the alphabet.
- The group name should be the combination of the digit or the alphabet.

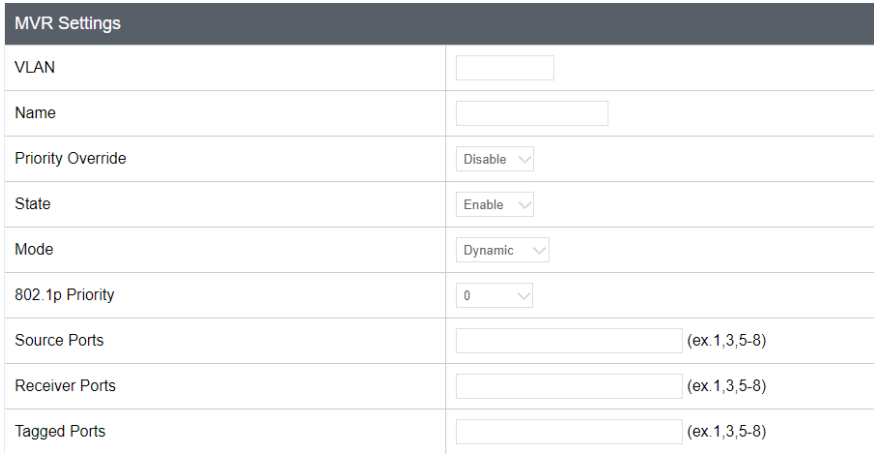
CLI Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLANID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current IGMP snooping configurations
configure	mvr VLANID	This command configures the MVR configurations for the specific VLAN.
configure	No mvr VLANID	This command disables the MVR configurations for the specific VLAN.
MVR	group NAME	This command configures a group configuration for the MVR.
MVR	No group NAME	This command removes the group
		configurations from the MVR.
MVR	inactive	This command disables the MVR settings.
MVR	No inactive	This command enables the MVR settings.
MVR	mode (dynamic|compatible)	This command configures the mode for the MVR. Dynamic: Sends IGMP report to all MVR source ports in the multicast VLAN. Compatible: Sets the Switch not to send IGMP report.
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command sets the receiver port(s). Normally the source ports are connected to the streaming client.
MVR	no receiver-port PORTLIST	This command removes a port or range of ports from the receiver port(s).
MVR	source-port PORTLIST	This command sets the source port(s). Normally the source ports are connected to the streaming server.
MVR	no source-port PORTLIST	This command removes a port or range of ports from the source port(s).
MVR	tagged PORTLIST	This command sets the tagged port(s). Same as the VLAN tagged port.
MVR	No tagged PORTLIST	This command removes a port or range of ports from the tagged port(s).
MVR	priority-override (disable|enable)	This command enables/disables the multicast priority override.

Web Configuration

MVR Settings

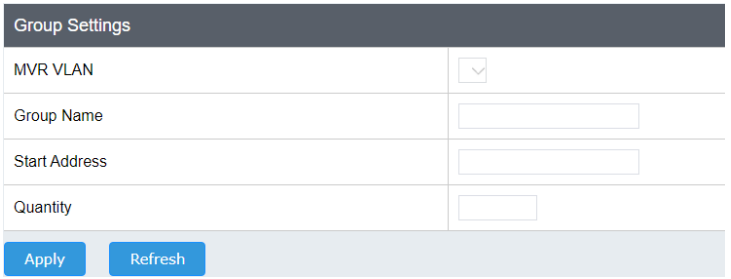
Network > MVR > MVR Settings



Parameter	Description
VLAN	Configures a VLAN
Name	Configures a name for the MVR.
Priority Override	Enable / Disable for the priority override
State	Enables / Disables the MVR
Mode	Configures the mode for the MVR.
802.1p Priority	The priority for these multicast group packets.
Source Ports	Configures the source port(s) for the MVR. Normally the source ports are connected to the streaming server.
Receiver Ports	Configures the receive port(s) for the MVR. Normally the source ports are connected to the streaming client
Tagged Ports	Configures the tagged port(s) for the MVR. Same as the VLAN tagged port

Group Settings

Network > MVR > Group Settings



Parameter	Description
MVR VLAN	Select a MVR VLAN.
Group Name	Configures the group name.
Start Address	Configures the multicast start address.
Quantity	Configures the quantity of the multicast address.

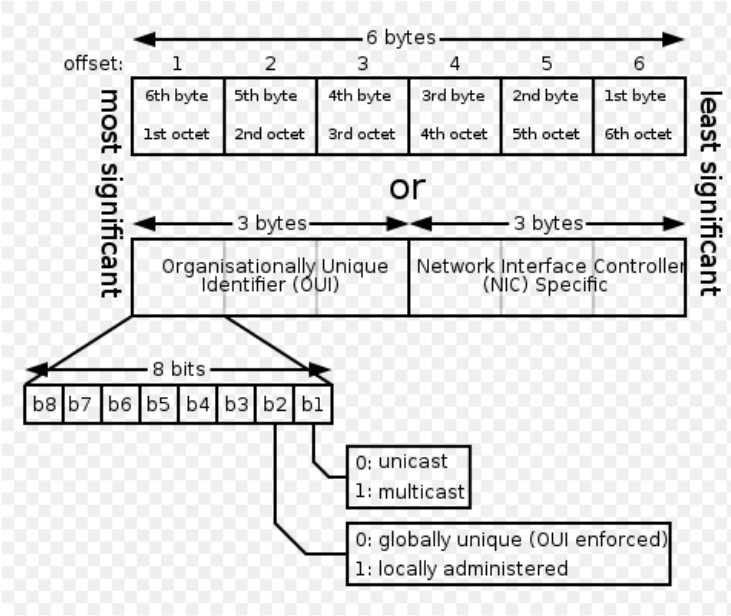
Multicast Address

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

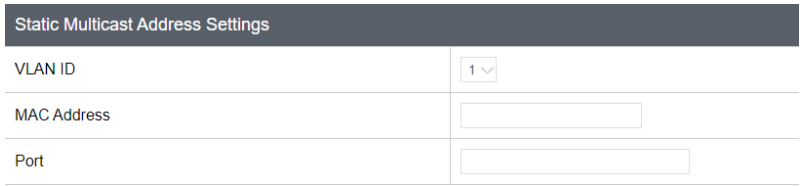
224.0.0.9	The RIP version 2 group address, used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment
224.0.0.10	EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment
224.0.0.13	PIM Version 2 (Protocol Independent 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

Network > Static Multicast



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.

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

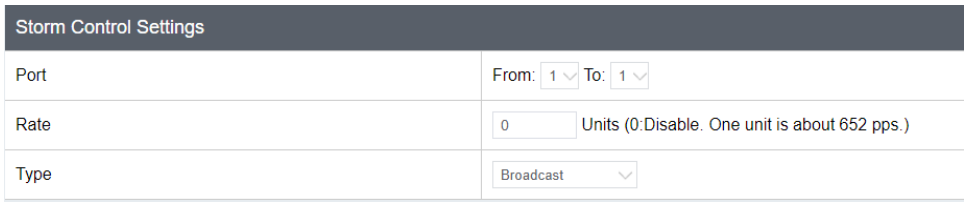
Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast 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:

[DEVICE_NAME]#configure terminal
[DEVICE_NAME](config)#storm-control rate 1 type broadcast ports 1-6
[DEVICE_NAME](config)#storm-control rate 1 type multicast ports 1-6
[DEVICE_NAME](config)#storm-control rate 1 type DLF ports 1-6

Web Configuration

Network > Bandwidth Control > 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:

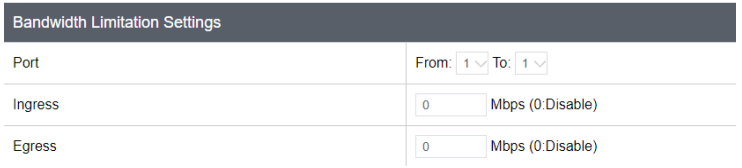
[DEVICE_NAME]#configure terminal

[DEVICE_NAME](config)#bandwidth-limit egress 1 ports 1-6

[DEVICE_NAME](config)#bandwidth-limit ingress 1 ports 1-6

Web Configuration

Network > Bandwidth Control > Rate Limiting

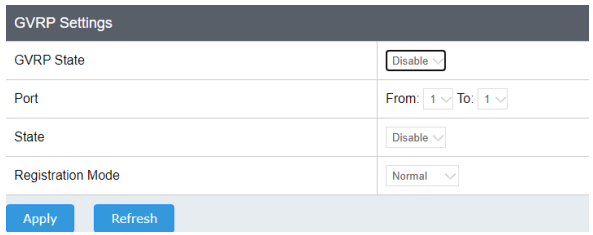


Parameter	Description
Port	Selects a port that you want to configure.
Ingress	Configures the rate limitation for the ingress packets.
Egress	Configures the rate limitation for the egress packets.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

GVRP

Web Configuration

Network > GVRP > GVRP

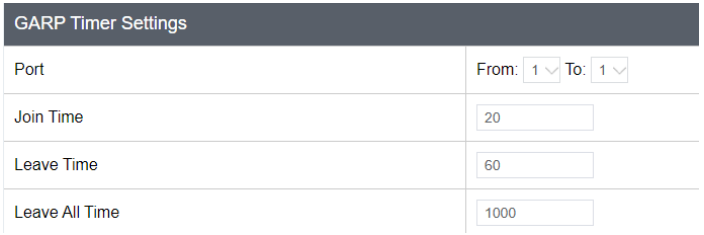


Parameter	Description

GVRP State	Select **Enable** to enable GVRP and **Disable** to disable this feature
Port	Select the range of port to apply this change to
State	Select **Enable** to enable the state and **Disable** to disable this feature
Registration Mode	Select Normal or Forbidden for this GVRP
Apply	Click Apply to apply the settings
Refresh	Click Refresh to refresh the page

GVRP TImer Web Configuration

Network > GVRP > GVRP Timer



Parameter	Description
Port	Select the range of port to apply this change to
Join Time	Input the Join Time
Leave Time	Input the Leave Time
Leave All Time	Input the Leave All Time

VLAN

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.

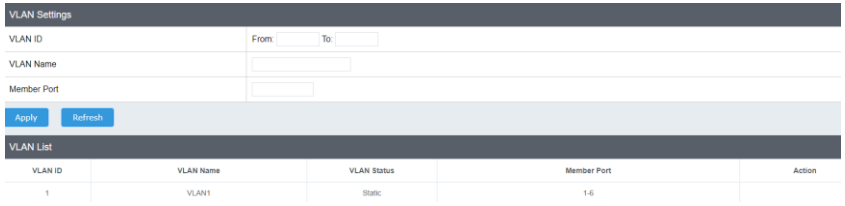
Example:

[DEVICE_NAME]#configure terminal
[DEVICE_NAME](config)#vlan 2
[DEVICE_NAME](config-vlan)#fixed 1-6
[DEVICE_NAME](config-vlan)#untagged 1-3

Web Configuration

VLAN Settings

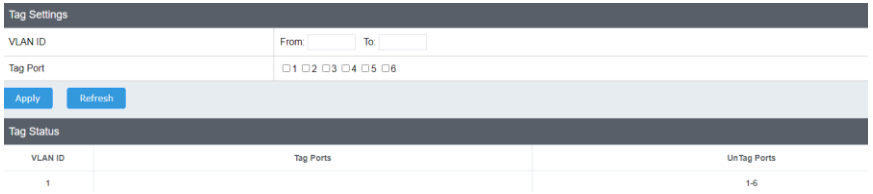
Network > VLAN > Settings



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

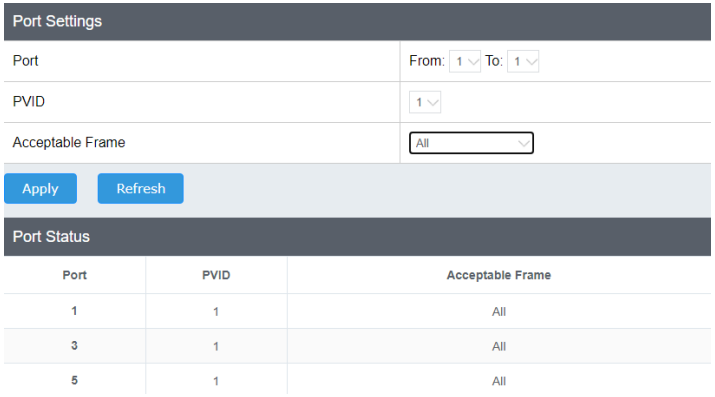
Network > VLAN > Tagged



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.
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

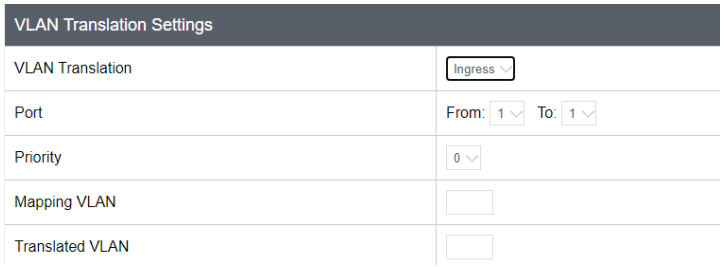
Network > VLAN > Port



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.**

Port Settings

Network > VLAN > VLAN Translation



Parameter	Description
VLAN Translation	Select **Ingress** or **Egress** for your VLAN Translation
Port	Select the range of port to apply the VLAN translation to
Priority	Select the priority level from 0 – 7
Mapping VLAN	Input the Mapping VLAN
Translated VLAN	Input the Translated VLAN

Q-in-Q

Q-in-Q tunneling is also known as VLAN stacking. Both of them use 802.1q double tagging technology. Q-in-Q is required by ISPs (Internet Service Provider) that need

Transparent LAN services (TLS), and the service provider has their own set of VLAN, independent of customer VLANs. Typically, each service provider VLAN interconnects a group of sites belonging to a customer. However, a service provider VLAN could also be shared by a set of customers sharing the same end points and quality of service requirements of the VLAN. Double tagging is considered to be a relatively simpler way of implementing transparent LAN. This is accomplished by encapsulating Ethernet Frame. A second or outer VLAN tag is inserted in Ethernet frames sent over the ingress PE (Provider Edge). This VLAN tag corresponds to the VLAN of the Service Provider (SP). When the frame reaches the destination PE, the SP VLAN is stripped off. The DA of the encapsulated frame and the VLAN ID are used to take further L2 decisions, similar to an Ethernet frame arriving from a physical Ethernet port. The SP VLAN tag determines the VPLS (Virtual Private LAN Service) membership. Double tagging aggregates multiple VLANs within another VLAN and provides a private, dedicated Ethernet connection between customers to reach their subnet transparently across multiple networks. Thus service providers can create their own VLANs without interfering with customer VLANs by using double tagging. This allows them to connect customers to ISPs and ASPs (Application Service Provider).

The ports that are connected to the service provider VLANs are called tunnel ports, and the ports that are connected to the customer VLANs are called access (subscriber/customer) ports. When a port is configured as tunnel port, all the outgoing packets on this port will be sent out with SPVLAN (SPVID and 1p priority) tag. The incoming packet can have two tags (SPVLAN + CVLAN), one tag (SPVLAN or CVLAN), or no tag. In all cases, the packet is sent out with a SPVLAN tag. When a port is configured as an access port, the incoming traffic can have only a CVLAN (CVID and 1p priority) tag or no tag. Hence, all the packets that are being sent out of access ports will be untagged or single tagged (CVLAN). When a port is configured as a normal port, it will ignore the frames with double tagging.

Double Tagging Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

TPID	Priority	VID

TPID (Tag Protocol Identifier) is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. The value of this field is 0x8100 as defined in IEEE 802.1Q. Other vendors may use a different value, such as 0x9100.

Tunnel TPID is the VLAN stacking tag type the Switch adds to the outgoing frames sent through a Tunnel Port of the service provider's edge devices.

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for. "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. SP VID is the VID for the second or outer (service provider's) VLAN tag. CVID is the VID for the first or inner (Customer's) VLAN tag.

The frame formats for an untagged Ethernet frame; a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) are shown as following.

DA: Destination Address

SA: Source Address

Tunnel TPID: Tag Protocol Identifier added on a tunnel port

P: 802.1p priority

VID: VLAN ID

Len or Etype: Length or Ethernet frame type

Data: Frame data

FCS: Frame Check Sequence

VLAN Stacking Port Roles

Each port can have three VLAN stacking "roles", Normal, Access Port and Tunnel Port.

- ✓ Select Normal for "regular" (non-VLAN stacking) IEEE 802.1Q frame switching.

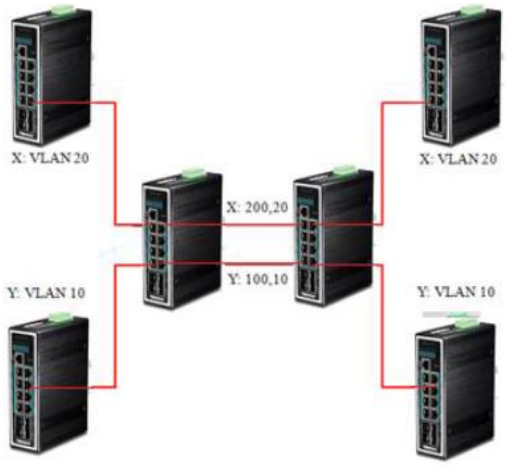
- ✓ Select Access Port for ingress ports on the service provider's edge devices. The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.
- ✓ Select Tunnel Port for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

NOTE: In order to have the double tagged frames switching correctly, user has to configure a service provider's VLAN (SPVLAN) on the Q-in-Q switch. Then, the double tagged frames can be switched according to the SP VID. The SPVLAN should include all the related Tunnel and Access ports. Also, user has to configure the Tunnel posts as tagged ports and the Access ports as untagged ports.

Port-based Q-in-Q

Q-in-Q encapsulation is to convert a single tagged 802.1Q packet into a double tagged Q-in-Q packet. The Q-in-Q encapsulation can be based on port or traffic. Port-based Q-in-Q is to encapsulate all the packets incoming to a port with the same SPVID outer tag. The mode is more inflexible.

In the following example figure, both X and Y are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 100 to distinguish customer X and tag 200 to distinguish customer Y at edge device A and then stripping those tags at edge device B as the data frames leave the network.



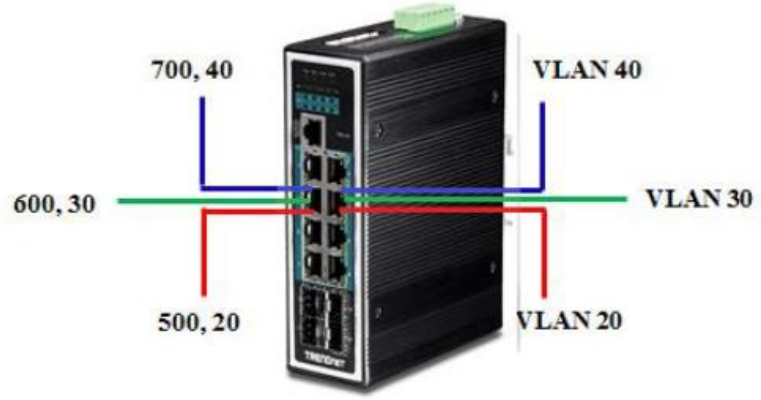
This example shows how to configure switch A with ports 1 on the Switch to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to service provider's VID of 100 (ports are connected to customer Y network). This example also shows how to set the priority for port 1 to 3 and port 7 to 4.

TI-BG62I(config)# vlan-stacking port-based
TI-BG62I(config)# vlan-stacking tpid-table index 2 value 88a8
TI-BG62I(config)# vlan 10
TI-BG62I(config-vlan)# fixed 7,8
TI-BG62I(config-vlan)# tagged 7
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 100
TI-BG62I(config-vlan)# fixed 7,8
TI-BG62I(config-vlan)# tagged 8
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 20
TI-BG62I(config-vlan)# fixed 1,2
TI-BG62I(config-vlan)# tagged 1

TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 200
TI-BG62I(config-vlan)# fixed 1,2
TI-BG62I(config-vlan)# tagged 2
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# interface gigaethernet1/0/1
TI-BG62I(config-if)# vlan-stacking port-based role access
TI-BG62I(config-if)# vlan-stacking spvid 200
TI-BG62I(config-if)# vlan-stacking priority 3
TI-BG62I(config)# interface gigaethernet1/0/2
TI-BG62I(config-if)# vlan-stacking port-based role tunnel
TI-BG62I(config-if)# vlan-stacking tunnel-tpid index 2
TI-BG62I(config)# interface gigaethernet1/0/7
TI-BG62I(config-if)# vlan-stacking port-based role access
TI-BG62I(config-if)# vlan-stacking spvid 100
TI-BG62I(config-if)# vlan-stacking priority 4
TI-BG62I(config)# interface gigaethernet1/0/8
TI-BG62I(config-if)# vlan-stacking port-based role tunnel
TI-BG62I(config-if)# vlan-stacking tunnel-tpid index 2
TI-BG62I(config-if)# exite
TI-BG62I(config)# exit
TI-BG62I# show vlan-stacking
TI-BG62I# show vlan-stacking tpid-table
TI-BG62I# show vlan-stacking portbased-qinq

Selective Q-in-Q

The traffic based Q-in-Q is also called Selective Q-in-Q. Selective Q-in-Q allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags. In the Selective Q-in-Q mode, switch performs traffic classification for the traffic incoming to a port based on the VLAN ID. When a user uses different VLAN IDs for different services, traffic can be classified according to the VLAN ID. For example, the VLAN ID 20 for surfing on the internet by PC, VLAN ID 30 for IPTV and VLAN ID 40 for VIP customers. After receiving user data, the switch labels the traffic of surfing on the Internet by PC with 500 as a SPVID outer tag, IPTV with 600, and VIP customers with 700.



This following example shows how to configure ports 3 on the Switch to tag incoming frames with the different service provider's VID and priority.

TI-BG62I(config)# vlan-stacking selective
TI-BG62I(config)# vlan-stacking tpid-table index 6 value 9100
TI-BG62I(config)# vlan 20
TI-BG62I(config-vlan)# fixed 3,4
TI-BG62I(config-vlan)# tagged 3
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 30
TI-BG62I(config-vlan)# fixed 3,4
TI-BG62I(config-vlan)# tagged 3
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 40
TI-BG62I(config-vlan)# fixed 3,4
TI-BG62I(config-vlan)# tagged 3
TI-BG62I(config-vlan)# exit

```
TI-BG62I(config)# vlan 500
TI-BG62I(config-vlan)# fixed 3,4
TI-BG62I(config-vlan)# tagged 4
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 600
TI-BG62I(config-vlan)# fixed 3,4
TI-BG62I(config-vlan)# tagged 4
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan 700
TI-BG62I(config-vlan)# fixed 3,4
TI-BG62I(config-vlan)# tagged 4
TI-BG62I(config-vlan)# exit
TI-BG62I(config)# vlan-stacking selective-qinq rule1
TI-BG62I(config-qinq)# cvids 20
TI-BG62I(config-qinq)# priority 2
TI-BG62I(config-qinq)# spvid 500
TI-BG62I(config-qinq)# access-ports 3
TI-BG62I(config-qinq)# tunnel-ports 4
TI-BG62I(config-qinq)# active
TI-BG62I(config-qinq)# show
TI-BG62I(config-qinq)# exit
TI-BG62I(config)# vlan-stacking selective-qinq rule2
TI-BG62I(config-qinq)# cvids 30
TI-BG62I(config-qinq)# priority 5
TI-BG62I(config-qinq)# spvid 600
TI-BG62I(config-qinq)# access-ports 3
TI-BG62I(config-qinq)# tunnel-ports 4
TI-BG62I(config-qinq)# active
TI-BG62I(config-qinq)# show
TI-BG62I(config-qinq)# exit
TI-BG62I(config)# vlan-stacking selective-qinq rule3
TI-BG62I(config-qinq)# cvids 40
TI-BG62I(config-qinq)# priority 7
TI-BG62I(config-qinq)# spvid 700
TI-BG62I(config-qinq)# access-ports 3
TI-BG62I(config-qinq)# tunnel-ports 4
TI-BG62I(config-qinq)# active
TI-BG62I(config-qinq)# show
TI-BG62I(config-qinq)# exit
TI-BG62I(config)# interface interface 1/0/4
TI-BG62I(config-if)# vlan-stacking tunnel-tpid index 6
TI-BG62I(config-if)# exit
TI-BG62I(config)# exit
TI-BG62I# show vlan-stacking
TI-BG62I# show vlan-stacking tpid-table
TI-BG62I# show vlan-stacking selective-qinq
```

Default Setting: VLAN Stacking is disabled.

CLI Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current vlan-stacking type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
configure	vlan-stacking (disable|port-based|selective)	This command disables the vlan stacking or enables the vlan-stacking with port-based or selective on the switch.

configure	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile with the name.
configure	no vlan-stacking selective-qinq STRINGS	This command removes the selective Q-in-Q profile with the name.
configure	vlan-stacking tpid-table index <2-6> value STRINGS	This command configures TPID table.
Interface	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
Interface	vlan-stacking port-based role (tunnel|access|normal)	This command sets VLAN stacking port role.
Interface	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
Interface	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.
configure	interface range gigabitethernet1/0/ ORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel|access|normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.
qinq	active	This command enables the selective Q-in-Q profile.

Qinq	inactive	This command disables the selective Q-in-Q profile.
Qinq	cvid VLANID	This command specifies the customer's VLAN range on the incoming packets.
Qinq	spvid VLANID	This command sets the service provider's VLAN ID for outgoing packets in selective Q-in-Q.
Qinq	priority <0-7>	This command sets priority in selective Q-in-Q.
Qinq	access-ports PORTLISTS	This command specifies the access ports to apply the rule.
Qinq	tunnel-ports PORTLISTS	This command specifies the tunnel ports to apply the rule.
Qinq	End	The command exits the CLI Q-in-Q node and enters the CLI enable node.
Qinq	exit	The command exits the CLI Q-in-Q node and enter the CLI configure node.
Qinq	Show	The command shows the current selective Q-in-Q profile configurations.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel|access|normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.

Web Configuration

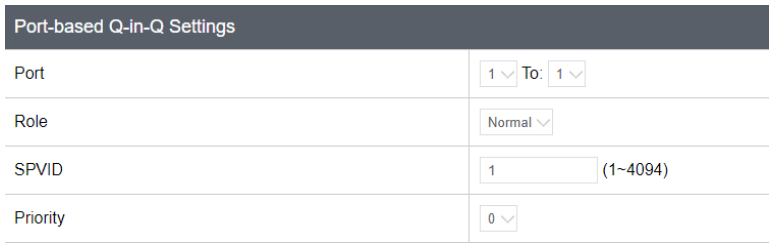
VLAN Stacking

Network > Q-in-Q > VLAN Stacking

Parameter	Description
Action	Select one of the three modes, Disable or Port-Based or Selective for the VLAN stacking.
Tunnel TPID Index	Selects the table index.
TPID	TPID Configures the TPID.
Port	Selects a port or a range of ports which you want to configure.
Tunnel TPID Index	Configures the index of the TPID Table for the specific ports.

Port Based Q-in-Q

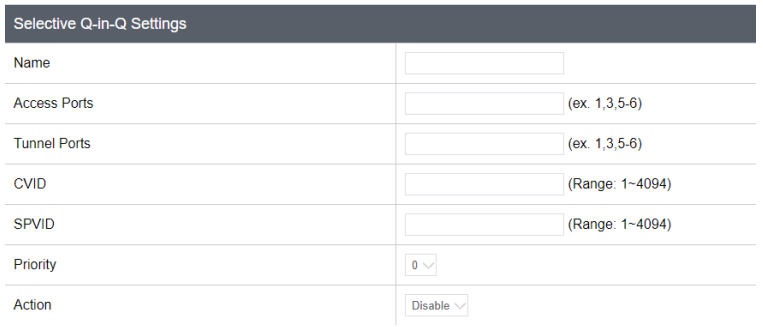
Network > Q-in-Q > Port Based Q-in-Q



Parameter	Description
Port	Selects a port or a range of ports which you want to configure.
Role	Selects one of the three roles, Normal and Access and Tunnel, for the specific ports.
SPVID	Configures the service provider's VLAN.
Priority	Configures the priority for the specific ports.

Selective Q-in-Q

Network > Q-in-Q > Selective Q-in-Q



Parameter	Description
Name	Configures the selective Q-in-Q profile name.
Access Points	Configures a port or a range of ports for the access points.
Tunnel Ports	Configures a port or a range of ports for the tunnel ports.
CVID	Configures a customer's VLAN.
SPVID	Configures a service provider's VLAN.

Priority	Configures an 802.1Q priority for the profile.
Action	Enables / Disables the profile.

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.

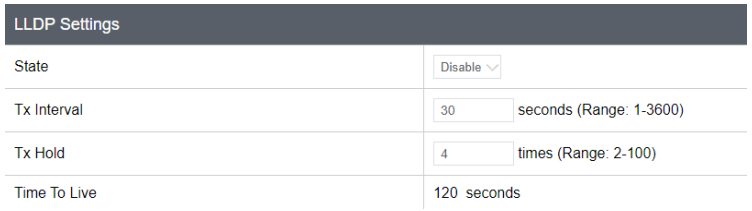
Port	Status	Port	Status
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable
13	Enable	14	Enable
15	Enable	16	Enable

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

Network > LLDP



Parameter	Description
State	Globally enables / disables the LLDP on the Switch.
Tx Interval	Input the Tx Interval
Tx Hold	Input the Tx Hold

MAC 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:

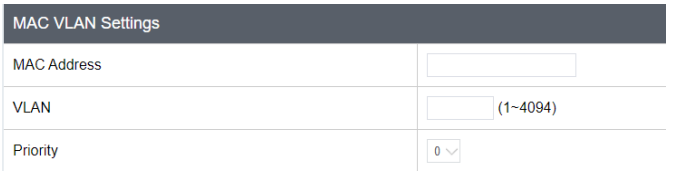
[DEVICE_NAME](config)#mac-vlan 00:01:02:03:04 vlan 111 priority 1

[DEVICE_NAME](config)#mac-vlan 00:01:02:22:04 vlan 121 priority 1

[DEVICE_NAME](config)#mac-vlan 00:01:22:22:04:05 vlan 221 priority 1

Web Configuration

Network > 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.

Protocol-based VLAN

The Protocol based VLAN allows users to create VLAN with packet frame type. The packet frame type can be one of the three frame types: EthernetII, NonLLC-SNAP and LLC-SNAP. If configuring the Ethernet II frame type, the configuration will be more detail with the ethernet type.

When the user configures the protocol VLAN as LLC-SNAP, VLAN:22, ports list: 1-3.

If the Switch receives packets with LLC-SNAP frame type from port 1 to 3, the packets' VLAN will be replaced with VLAN 22 and 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 protocol-vlan	This command displays the all of the protocol-vlan configurations.
configure	protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with ethernetII frame type.
configure	protocol-vlan frame-type nonLLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with nonLLC-SNAP frame type.
configure	protocol-vlan frame-type LLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with LLC-SNAP frame type.
configure	no protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID	This command deletes a protocol-vlan entry with ethernetII frame type.
configure	no protocol-vlan frame-type nonLLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with nonLLC-SNAP frame type and vlan.
configure	no protocol-vlan frame-type LLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with LLC-SNAP frame type and vlan.
configure	no protocol-vlan all	This command deletes all of the protocol-vlan entries.

Example:

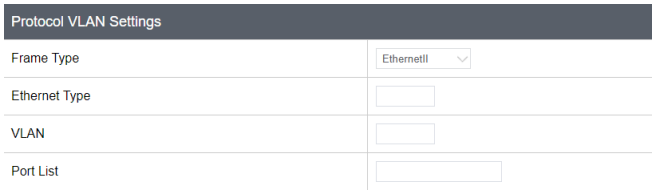
TI-BG62I(config)#protocol-vlan frame-type LLC-SNAP vlan 12 ports 1-2

TI-BG62I(config)#protocol-vlan frame-type nonLLC-SNAP vlan 13 ports 3-4

TI-BG62I(config)#protocol-vlan frame-type ethernetII ether-type 0800 vlan 14 ports 1-2

Web Configuration

Network > Protocol VLAN



Parameter	Description

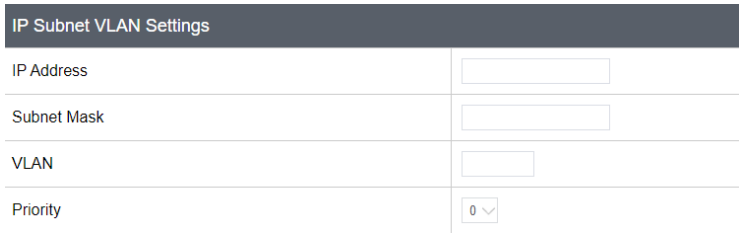
Frame Type	Select one of three frame types, "EthernetIU" and "NonLLC-SNAP" and "LLC-SNAP".
Ethernet Type	Input the Ethernet type for the EthernetII frame type.
VLAN	Configure the VLAN ID.
Port List	Configure the member ports.

IP Subnet VLAN

IP Subnet based VLANs assigns all computers with the same subnet to the same VLAN.

Web Configuration

Network > IP Subnet VLAN



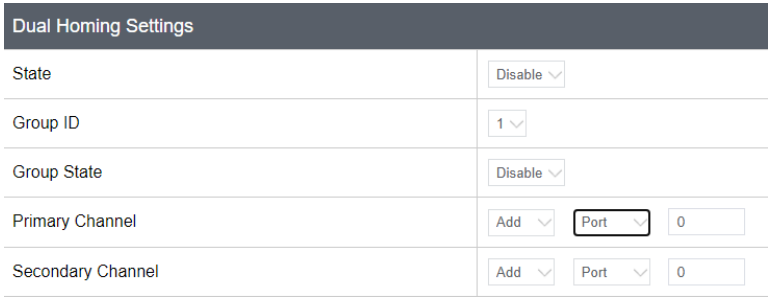
Parameter	Description
IP Address	Input the address of the VLAN
Subnet Mask	Input the subnet mask to assign the appropriate devices
VLAN	Input the VLAN ID
Priority	Set the priority level

Dual Homing

Dual Homing creates a redundant back-up connection in case of failure on one of the ports.

Web Configuration

Network > Dual Homing



Parameter	Description
State	Select Enable to enable this feature and Disable to disable this feature
Group ID	Select the Group ID to modify
Group State	Select Enable to enable all configurations in this group or disable to disable it.
Primary Channel	Select "Add" or "Reset" , "Port" or "Trunk" and input the port number for the primary channel
Secondary Channel	Select "Add" or "Reset" , "Port" or "Trunk" and input the port number for the primary channel

Xpress Ring

The Xpress-Ring is a fast-acting, self-healing ring recovery technology that enables networks to recover from link failure within 10ms.

Fast Link Recovery and Ring Redundancy are important features for increasing the reliability of non-stop systems.

If the network is planned correctly with an arbiter Switch and ring ports, the network will recover from any segment failure within a very short time.

There are two roles (Forwarder and Arbiter) of the Switch in the Xpress-Ring. There is one and only one Switch is the Arbiter Switch and the others are the forwarder Switch.

One of the ring ports of the Arbiter Switch will be set to blocking state. When one of the ring connections is broken, the blocked port will be set to forwarding state.

Default Settings

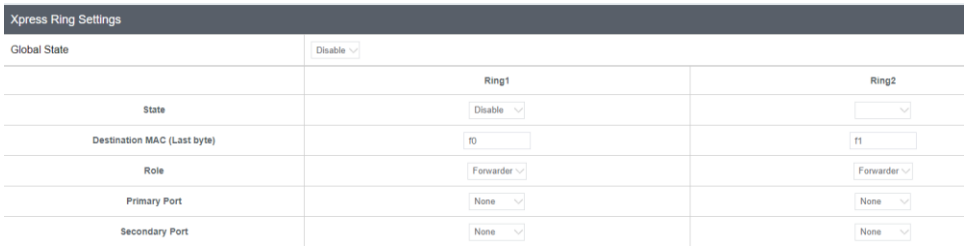
Xpress-Ring Configurations:
The global Xpress Ring state is: Disabled.
Ring 1: State : Disabled.
Destination MAC : 01:80:c2:ff:ff:f0.
Role : Forwarder.
Primary Port : None.
Secondary Port : None.
Ring 2: State : Disabled.
Destination MAC : 01:80:c2:ff:ff:f1.
Role : Forwarder.
Primary Port : None.
Secondary Port : None.

Configuration

Node	Command	Description
enable	show xpress-ring	This command displays the current XpressRing configurations.
configure	xpress-ring (disable|enable)	This command enables/disables the Xpress-Ring on the Switch
Configure	Xpress-ring ring (RING1 | RING2) state (disable | emable)	This command enables/disables the ring on the Switch
Configure	Xpress-ring-ring (RING1|RING2) last-byte- destination-mac Value	This command configuresthe last byte of the destination MAC for the ring on the Switch
	Xpress-ring ring (RING|RING2) role (forwarder|arbiter)	This command configures the role (forwarder/arbiter) for the ring on the Switch
Configure	Xpress-ring ring (RING1|RING2) primary port PORTID	This command configures the primary port for the ring on the Switch **Note** *If the global xpress ring is disabled or ring state is disabled, you can input 0 to the reset the primary port*
Configures	Xpress-ring-ring (RING1|RING2) secondary port PORTID	This command configures the secondary port for the ring on the Switch. Notice: If the global express ring is disabled or ring state is disabled, you can input 0 to reset the primary porty

Web Configuration

Network > Xpress Ring



Parameter	Description
State	Select Enable to enable this feature and Disable to disable this feature

Destination MAC	Select the Group Input the MAD address of the destination
Role	Configures the role for the ring
Primary Port	Configure the primary port for the ring
Secondary Port	Configures the secondary port for the rig

Xpress Ring Status

	Ring1	Ring2
State	Disabled	Disabled
Destination MAC	01:80:c2:ff:ff:f0	01:80:c2:ff:ff:f1
Role	Forwarder	Forwarder
Primary Port	N/A (No connection)	N/A (No connection)
Secondary Port	N/A (No connection)	N/A (No connection)

Parameter	Description
State	Displays if the Xpress Ring is enabled or disabled
Destination Mac	the destination MAC for the ring
Role	The current role of the ring
Primary Port	The current primary port and its status
Secondary Port	The current secondary port and its status

Notices

An Xpress ring can have one Arbiter only.

- A switch can join one or two Xpress Ring.
- Every Switch can be a Forwarder or Arbiter in an Xpress Ring.
- The two adjacent Xpress Rings should not use a same destination multicast MAC.
- If you want to enable the STP (RSTP) and Xpress Ring on a Switch, you should disable the STP (RSTP) on the Xpress Ring's member ports.
- If you want to enable the Loop Detection and Xpress Ring on a Switch, you should disable the Loop Detection on the Xpress Ring's member ports.
- If you want to enable the Broadcast Storm and Xpress Ring on a Switch, you should disable the Braodcast Storm on the Xpress Ring's member ports.
- If there are old devices (for example: INS-803A) to join the Xpress-Ring, they can join as a forwarder only.

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:

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

[DEVICE_NAME](config)#interface 1/0/3
[DEVICE_NAME](config-if)#port-isolation ports 1
[DEVICE_NAME](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:

[DEVICE_NAME](config)#interface 1/0/2

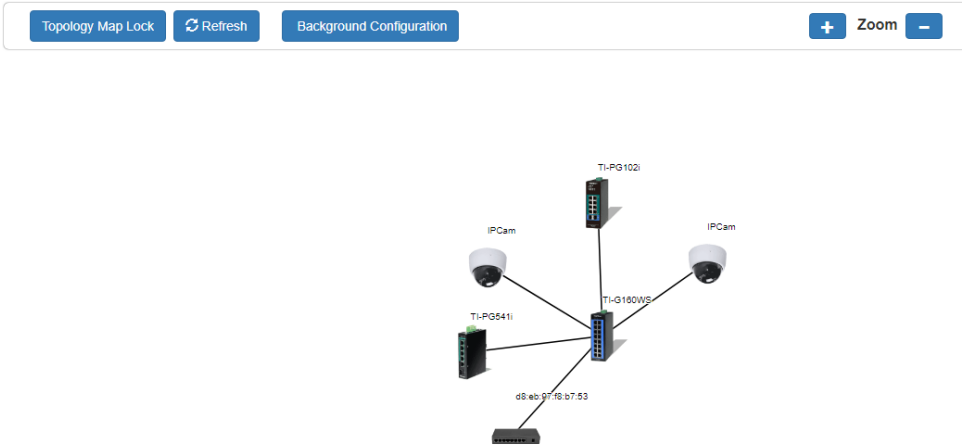
[DEVICE_NAME](config-if)#port-isolation ports 3-6

Toplogy Map

The topology map displays a basic view of the current network topology and device inter-connections. Devices are discovered via LLDP and ONVIF protocols, or can be manually entered which will be added to the device display. The topology map/netlite view is only available through the web GUI configuration page.

Web Configuration

Network > Topology Map



Parameter	Description
Topology Map Lock	When map is unlocked, you can freely drag the connected devices to a different locations of the map view. When the map is locked, devices are locked into their current viewing position and right-clicking the devices may allow for other web accessible/ configurable options depending on the device. Also, all of the current devices will remain on the map even if they are disconnected until the topology map is unlocked.
Refresh	Manually refresh the topology map/netlite page.
Background Configuration	Modify the background color of the topology map or upload a background image.
Zoom	Zoom in or out of the topology map/netlite viewing page.

Manual Registration

Network > Manual Registration

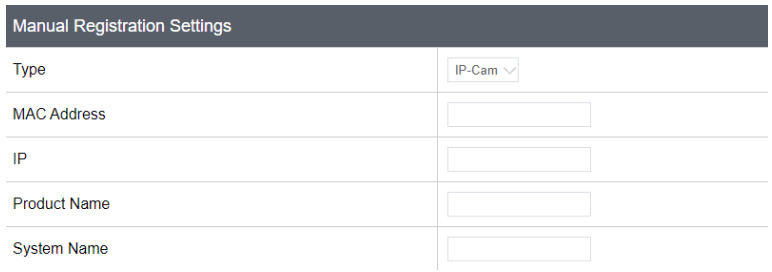
If devices do not support LLDP and ONVIF, user has to enter the details of it by manually under manual registration. The function supports three type, IP-Cam, PLC and Switch.

For devices which do not support ONVIF or LLDP, User can input the device's MAC address and then the Switch will discover the device and display it on the Topology/Netlite Map in the Topology map web GUI page.

Node	Command	Description
enable	show netlite-device	This command displays the netlite-device whose MAC are manually entered
configure	netlite-device type ipcam mac	This command adds a MAC address of an IP-cam to display on netlite.
configure	netlite-device type plc mac	This command adds a MAC address of a PLC to display on netlite.
configure	netlite-device type switch mac	This command binds the MAC address to a particular port
configure	no netlite-device mac	This command removes device from netlite..

Web Configuration

Network > Manual Registration



Parameter	Description
Type	Select the type of device to display on Topology/Netlite map. IP-Cam, PLC, or Switch.
MAC Address	Enter the MAC address of the device to add to the topology map. (00:11:22:aa:bb:cc)
IP	Enter the IP address of the device to add to the topology map.
Product Name	Enter the device name
System Name	Enter the system name

ONVIF

Network > ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

The Switch use ONVIF to discovery if there is ONVIF device connected to the Switch.

The page show the detail information about ONVIF settings and ONVIF devices connected to the Switch. The Switch displays ONVIF devices up to total port count, IEN-8428PL shows upto 10 ONVIF devices connected to it. If one or more ONVIF devices are connected to the same port it displays the last ONVIF device gets connect to it.

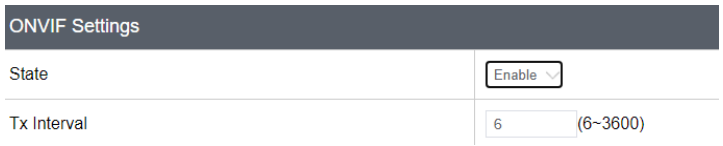
Important

Node	Command	Description
enable	show onvif	This command displays the onvif configurations.
enable	show onvif neighbor	This command displays all of the ports' neighbor information.
configure	onvif enable	This command enables onvif function on the Switch.
configure	onvif tx-interval	This command configures the interval to transmit the onvif packets.
configure	onvif binding-ports	This command binds the MAC address to a particular port
configure	no onvif tx-interval	This command configures the onvif packets transmit interval to the default value

configure	no onvif binding-ports	This command binds the MAC address to a particular port

Web Configuration

Management > Device Management > ONVIF



Parameter	Description
State	Globally enables / disables the ONVIF on the Switch.
Tx Interval	Sets the interval time in seconds when to send transmit ONVIF packets.

ERPS (Ethernet Ring Protection Switching)

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

The Ethernet ring protection functionality includes the following:

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

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

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

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

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

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

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

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

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

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

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

ERPS revertive and non-revertive switching

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

Control VLAN:

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

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

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

Instance:

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

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

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

Notice:

Control VLAN and Instance:

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

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

CLI Configuration

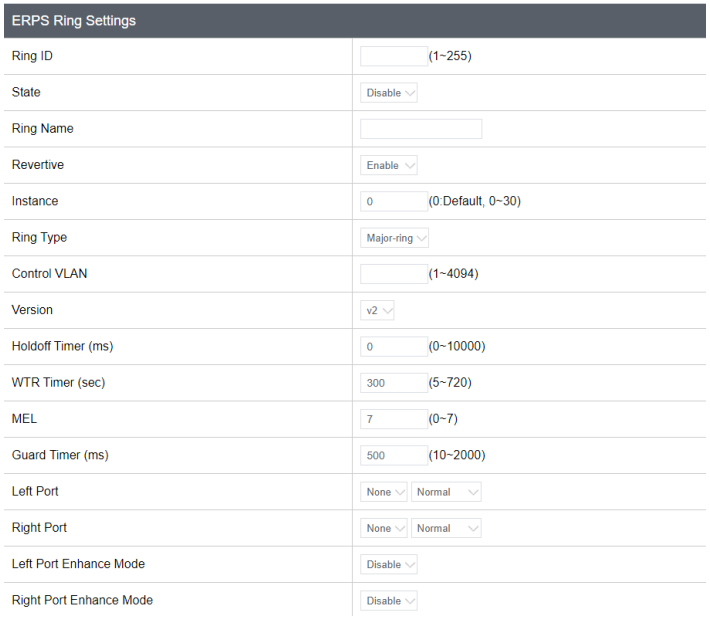
Node	Command	Description
enable	show erps	This command displays the ERPS configurations.
enable	show erps instance	This command displays the ERPS instance configurations.
enable	show erps instance INSTANCE_ID	This command displays the specific ERPS instance configurations.
configure	erps enable	This command enables the global ERPS on the Switch.
configure	no erps enable	This command disables the global ERPS on the Switch.
configure	erps ring-id VALUE	This command creates an ERPS ring and its ID and enter ERPS node.

configure	erps instance	This command enters the instance configure node.
configure	no erps ring-id VALUE	This command creates an ERPS ring and enter ERPS node to configure detail ring configurations.
erps-ring	show	This command displays the configurations of the ring.
erps-ring	control-vlan	This command configures a control-vlan for the ERPS ring.
erps-ring	guard-timer	This command configures the Guard Timerfor the ERPS ring. (default:500ms)
erps-ring	holdoff-timer	This command configures the Hold-off Timer for the ERPS ring. (default:0 ms)
erps-ring	left-port PORTID type [owner|neighbor|normal]	This command configures the left port and type for the ERPS ring.
erps-ring	mel VALUE	This command configures a Control MEL for the ERPS ring.
erps-ring	name STRING	This command configures a name for the ERPS ring.
erps-ring	revertive	This command configures the revertive mode for the ERPS ring.
erps-ring	no revertive	This command configures the non-revertive mode for the ERPS ring.
erps-ring	right-port PORTID type [owner|neighbor|normal]	This command configures the right port and type for the ERPS ring.
erps-ring	ring enable	This command enables the ring.
erps-ring	no ring enable	This command disables the ring.
erps-ring	version	This command configures a version for the ERPS ring.
erps-ring	wtr-timer	This command configures the WTR Timer for the ERPS ring. (default: 5 minutes)
config-erps-inst	instance INSTANCE_ID control-vlan VLAN_ID data-vlan VLAN_ID	This command configures a new instance and specifies its control vlan and data vlan.
config-erps-inst	no instance INSTANCE_ID	This command removes an instance.
config-erps-inst	show	This command displays all of the instance configurations.

Web Configuration

Ring Settings

Network > ERPS > Settings



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

Parameter	Description
Ring ID	The ring ID.
Ring Name	The ring name.

State	The ring state.
Revertive	The ring revertive mode.
Control VLAN	The ring Control VLAN.
Version	The protocol version on the ring.
Holdoff Timer	The Hold-off time.
WTR Timer	The WTR time.
MEL	The Control MEL.
Guard Timer	The Guard time.
Left Port	The left port.
Left Port Type	The left port type.
Right Port	The right port.
Right Port Type	The right port type.
WTB Timer	The WTB time.
Ring Status	The current ring status.
Left Port Status	The current left port status.
Right Port Status	The current right port status.

Instance Settings

Network > ERPS > Ring Instance

Parameter	Description
Instance Settings	
Instance	Configures the instance ID. The valid value is from 1 to 31.
Control VLAN	Configures the control vlan for the instance. The valid value is from 1 to 4094.
Data VLAN	Configures the data vlan for the instance. The valid value is from 1 to 4094. It can be one or multiple vlans.
Instance Status	
Instance	The instance ID.
Control VLAN	The control vlan of the instance.
Data VLAN	The data vlan of the instance.

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.

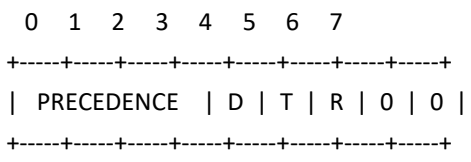
Bits 0-2: Precedence.

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.



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 (disable|enable)	This command disables / enables the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

Web Configuration

CoS

QoS > CoS

Priority/Queue Mapping Settings

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

Parameter	Description
Show 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.

802.1p

QoS > Port Priority

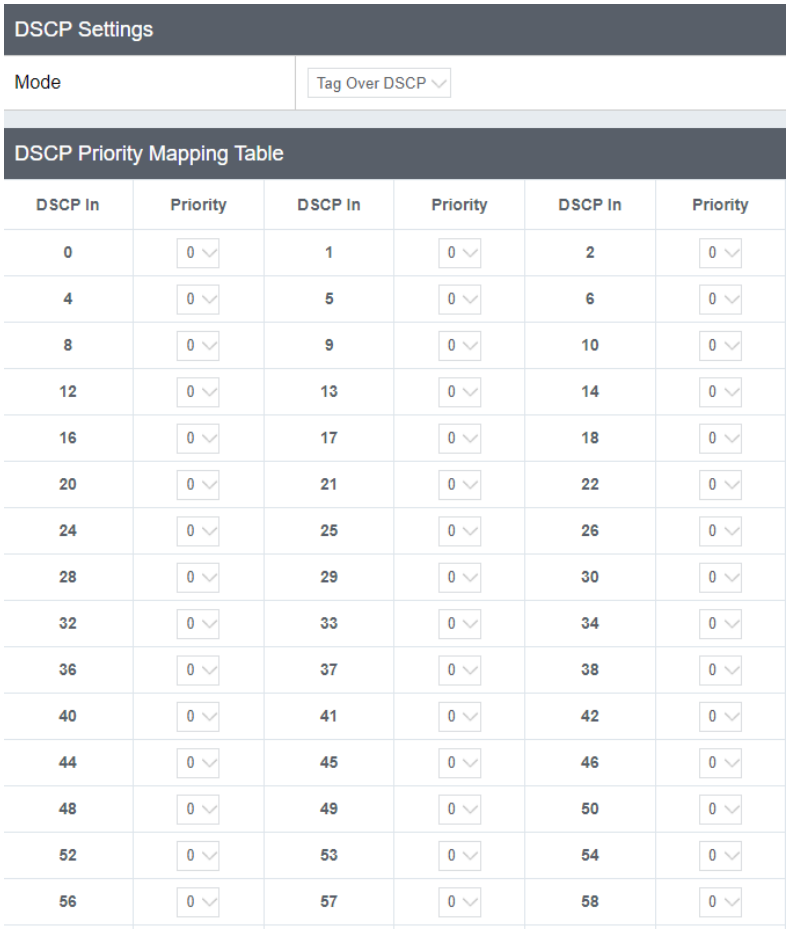
Port Priority Settings

Port	802.1p priority	Port	802.1p priority
1	0	2	0
3	0	4	0
5	0	6	0

Parameter	Description
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.

DSCP

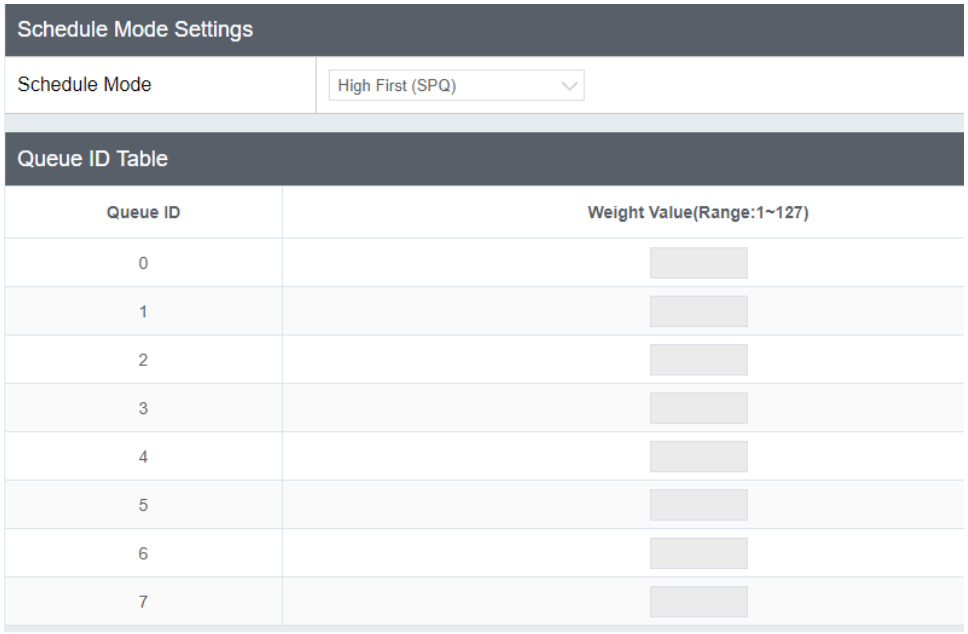
QoS > DSCP



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.

Scheduling Algorithm

QoS > Scheduling Algorithm



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.

Power over Ethernet

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

Power Sourcing Equipment (PSE)

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

Powered Device (PD)

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

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

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	34.2W	12.85W to 25.5W
5	45W	40W
6	60W	51W
7	75W	62W
8	99W	71.3W

Power Budget

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

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

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

Priority Level	Description
Critical	This is the highest priority level. Ports set to the Critical level are guaranteed to receive

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

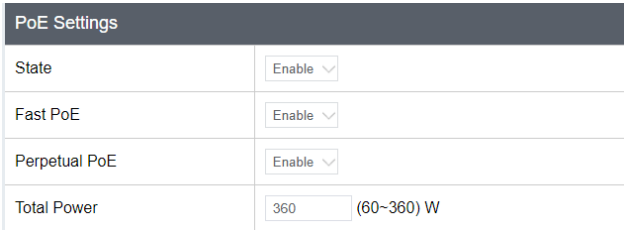
CLI Configuration

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.

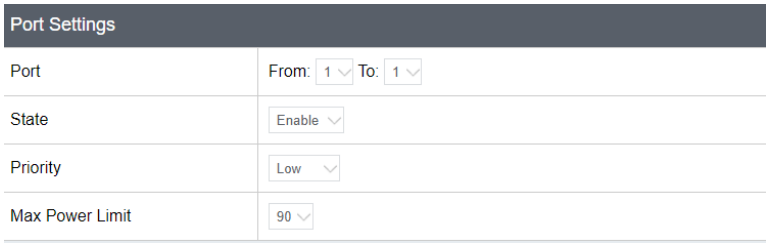
Web Configuration

Power over Ethernet

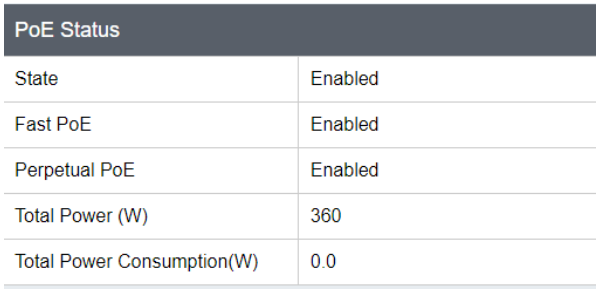
Advanced Settings > VLAN > Port Isolation



Parameter	Description
State	Selects **Enable** to enable the PoE function Selects **Disable** to disable the PoE function
Fast PoE	Select **Enable** to enable Fast PoE to deliver power to PD devices as soon as the switch is powered on Select **Disable** to disable this function
Perpetual PoE	Select **Enable** to enable this function to distribute PoE even when the switch reboots Select **Disable** to disable this function
Total Power	Input the maximum total PoE budget



Parameter	Description
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.
Max Power Limit	Select the maximum power output per port (in watts)
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh



PoE Status	
State	Enabled
Fast PoE	Enabled
Perpetual PoE	Enabled
Total Power (W)	360
Total Power Consumption(W)	0.0

Parameter	Description
State	Displays the PoE status
Fast PoE	Displays the status of Fast PoE
Perpetual PoE	Displays if the status of Perpetual PoE
Total Power	Total available PoE budget left
Total Power Consumption (W)	Displays the total power consumption

PoE Port Status						
Port	State	Status	Priority	Class	Max Power Limit(W)	Power Consumption(W)
1	Enabled	Searching	Low	None	90	0.0
2	Enabled	Searching	Low	None	90	0.0
3	Enabled	Searching	Low	None	90	0.0
4	Enabled	Searching	Low	None	90	0.0

Port	Display the Port No.
State	Displays the PoE state for the specific port.
Status	Displays the status of the PoE port
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.
Max Power Limit (W)	Displays the max power output available for the port
Power Consumption (W)	Displays the current consumption by 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.

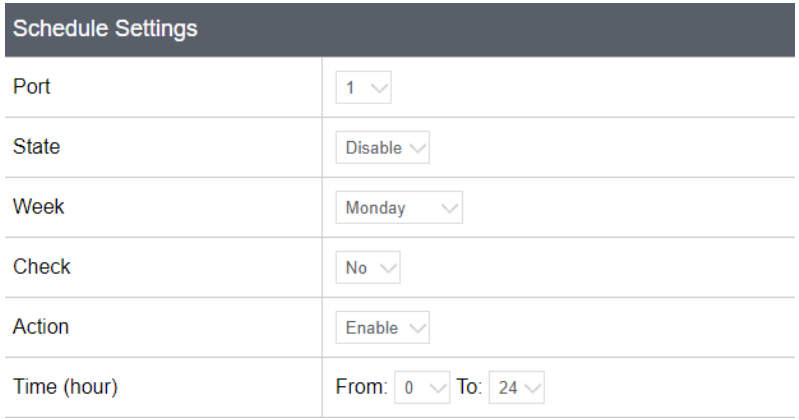
If the port's check configuration is NO for a specific day, the Switch will not perform action for the specific port. If the port's check configuration is YES for a specific day, the Switch will check the Start time and End Time. If the current time is in the interval between Start time and End Time,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

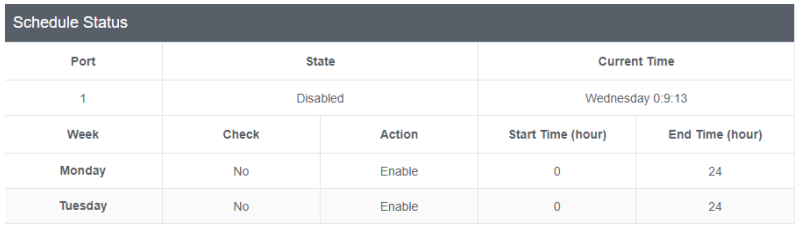
CLI Configuration

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

PoE > Time Range





Parameter	Description
Port	Selects a port that you want to configure the PoE schedule function.
State	Select Enable to enable this rule, or disable this rule
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.
Action	Select Enable to turn PoE on or Disable to turn off PoE for the selected rule
Time (Hour)	Select the time (in hours) to start and stop the schedule.

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.

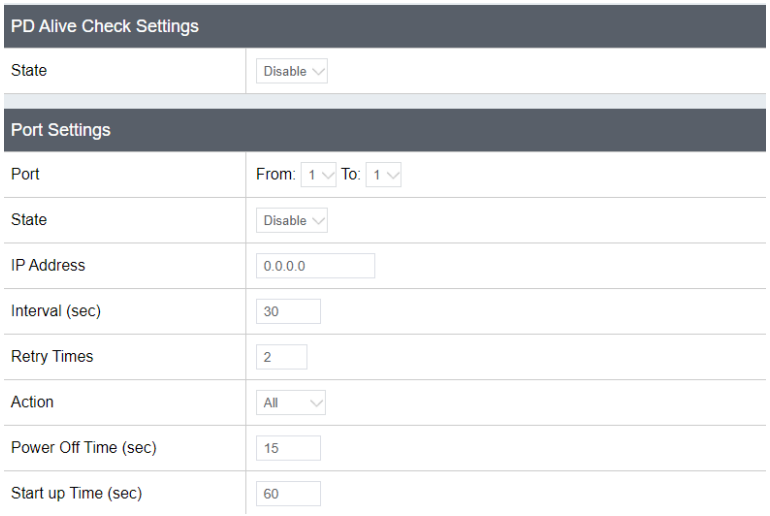
Reboot: Cut off the power of the PoE port, make PD rebooted.

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

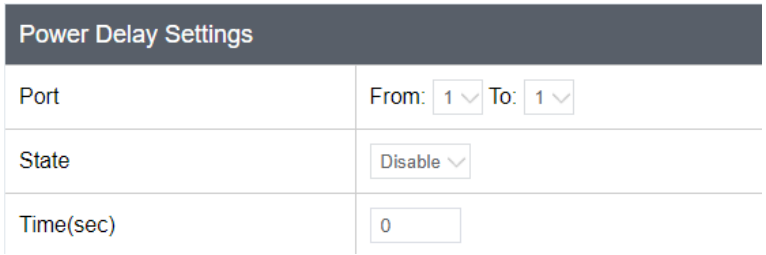
PoE > PD Alive



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-alive 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

PoE > Power Delay



Parameter	Description
Port	Select a port number to configure
State	Enables/Disables the Power Delay for the specific port(s).
Time (sec)	Set time duration of when to send PoE power for the selected port

Port Security

The Switch will learn the MAC address of the device directly connected to a particular port and allow traffic through. We will ask the question: "How do we control who and how many can connect to a switch port?" This is where port security can assist us. The Switch allow us to control which devices can connect to a switch port or how many of them can connect to it (such as when a hub or another switch is connected to the port).

Let's say we have only one switch port left free and we need to connect five hosts to it. What can we do? Connect a hub or switch to the free port! Connecting a switch or a hub to a port has implications. It means that the network will have more traffic. If a switch or a hub is connected by a user instead of an administrator, then there are chances that loops will be created. So, it is best that number of hosts allowed to connect is restricted at the switch level. This can be done using the "port-security limit" command. This command configures the maximum number of MAC addresses that can source traffic through a port.

Port security can sets maximum number of MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped. It can be use MAC table to check it. The static MAC addresses are included for the limit.

Note: If you configure a port of the Switch from disabled to enabled, all of the MAC learned by this port will be clear.

Default Settings

The port security on the Switch is disabled.

The Maximum MAC per port is 5.

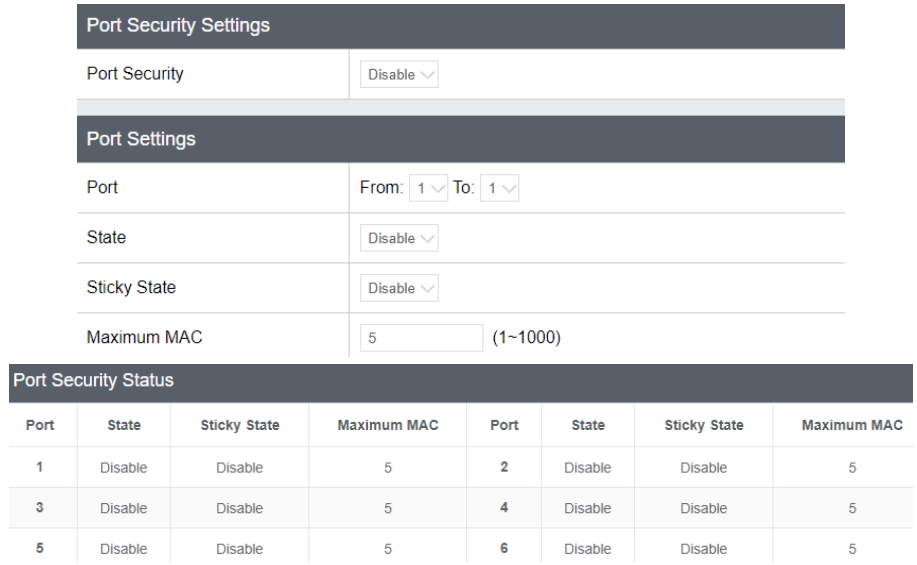
The port state of the port security is disabled.

CLI Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
configure	port-security (disable|enable)	This command enables / disables the global port security function.
interface	port-security (disable|enable)	This command enables / disables the port security function on the specific port.
interface	port-security limit VALUE	This command configures the maximum MAC entries on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	port-security (disable|enable)	This command enables / disables the port security function for the specified ports
if-range	port-security limit VALUE	This command configures the maximum MAC entries for the specified ports.

Web Configuration

Security > Port Security > Port Settings

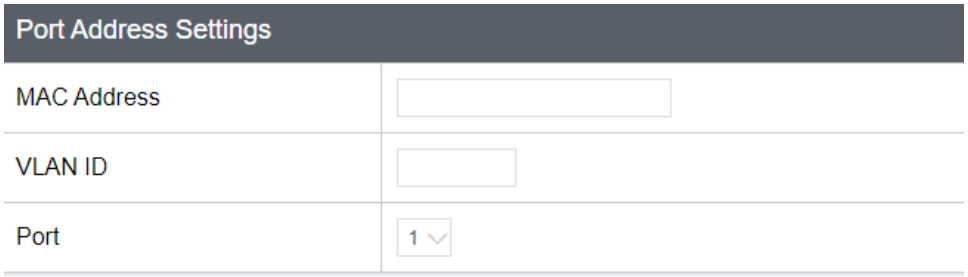


Parameter	Description
Port Security Settings	
Port Security	Select **Enable/Disable** to permit Port Security on the Switch.
Port	Select a port number to configure.
State	Select **Enable/Disable** to permit Port Security on the port.
Sticky State	Select **Enable/Disable** to sticky learning of non-static MAC addresses
Maximum MAC	The maximum number of MAC addresses allowed per interface. The acceptable range is 1 to 30.
Port Security Status	

Port	This field displays a port number.
State	This field displays if Port Security is **Enabled** or **Disabled**
Maximum MAC	This field displays the maximum number of MAC addresses

Port Address Settings

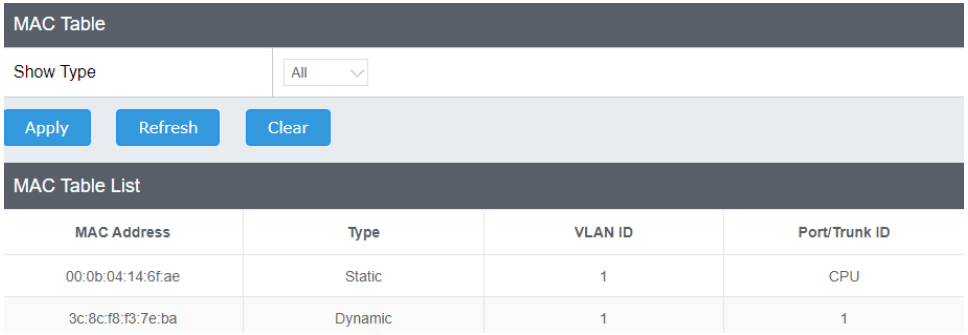
Security > Port Security > Port Address Settings



Parameter	Description
MAC Address	Enter the MAC Address
VLAN ID	Enter the VID
Port	Select the port.

MAC Table

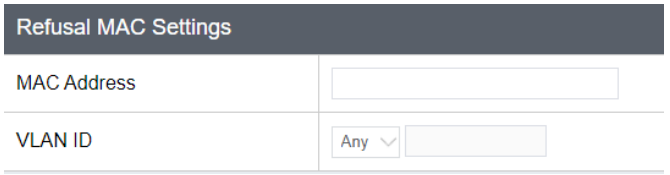
Security > Port Security > MAC Table



Parameter	Description
Show Type	Select from the menu to display the type of filter

Refusal MAC

Security > Refusal MAC



Parameter	Description
MAC Address	Enter the MAC Address
VLAN ID	Select the VLAN ID location to refuse access

IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the

interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports.

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.

The IP Source Guard features include below functions:

1. DHCP Snooping.
2. DHCP Binding table.
3. ARP Inspection.
4. Blacklist Filter. (arp-inspection mac-filter table)

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You can use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The DHCP snooping binding database contains the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- ✓ A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from the untrusted port.
- ✓ A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match any of the current bindings.

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again.

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN.
3. Configure trusted and untrusted ports.
4. Configure static bindings.

Note:

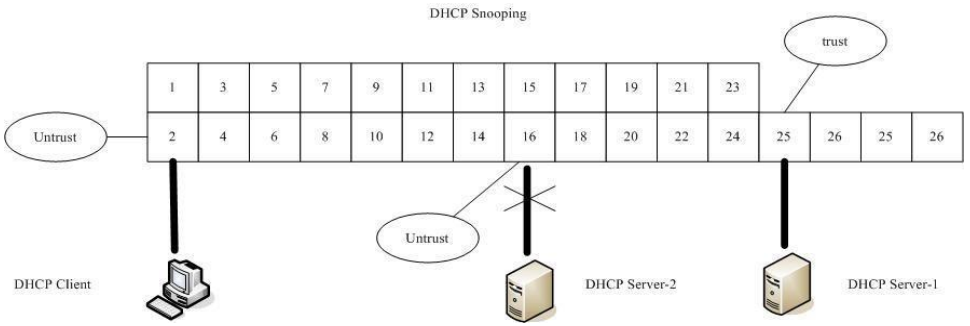
The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

If the port link down, the entries learned by this port in the DHCP snooping binding table will be deleted.

You must enable the global DHCP snooping and DHCP Snooping for vlan first.

The main purposes of the DHCP Snooping are:

1. Create and maintain binding table for ARP Inspection function.
2. Filter the DHCP server's packets that the DHCP server connects to an untrusted port.



The DHCP server connected to an un-trusted port will be filtered.

Default Settings

The DHCP snooping on the Switch is disabled.

The DHCP snooping is enabled in VLAN(s): None.

Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
1	no	32	2	no	32
3	no	32	4	no	32
5	no	32	6	no	32
7	no	32	8	no	32
9	no	32	10	no	32
11	no	32	12	no	32
13	no	32	14	no	32
15	no	32	16	no	32

Notices

- There are a global state and per VLAN states.

When the global state is disabled, the DHCP 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 DHCP Snooping on the specific VLAN.

VLAN 1: port 1-10.
DHCP Client-1: connect to port 3.
DHCP Server: connect to port 1.

Procedures:

1. Default environments:
   A. DHCP Client-1: ipconfig /release
   B. DHCP Client-1: ipconfig /renew
   ➔ DHCP Client-1 can get an IP address.

2. Enable the global DHCP Snooping.
   A. **[DEVICE_NAME](**config)#*dhcp-snooping*
   B. DHCP Client-1: ipconfig /release
   C. DHCP Client-1: ipconfig /renew
   ➔ DHCP Client-1 can get an IP address.

3. Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.
   A. **[DEVICE_NAME](**config)#*dhcp-snooping*
   B. **[DEVICE_NAME](**config)#*dhcp-snooping vlan 1*
   C. DHCP Client-1: ipconfig /release
   D. DHCP Client-1: ipconfig /renew
   ➔ DHCP Client-1 cannot get an IP address.
   ; Because the DHCP server connects to a un-trust port.

4. Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.
   A. **[DEVICE_NAME](**config)#*dhcp-snooping*
   B. **[DEVICE_NAME](**config)#*dhcp-snooping vlan 1*
   C. **[DEVICE_NAME](**config)#*interface gi1/0/1*
   D. **[DEVICE_NAME](**config-if)#*dhcp-snooping trust*
   E. DHCP Client-1: ipconfig /release
   F. DHCP Client-1: ipconfig /renew
   ➔ DHCP Client-1 can get an IP address.

5. If you configure a static host entry in the DHCP snooping binding table, and then you want to change the host to DHCP client, the host will not get a new IP from DHCP server, and then you must delete the static host entry first.

CLI Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current DHCP snooping configurations.
configure	dhcp-snooping (disable|enable)	This command disables/enables the DHCP snooping on the switch.
configure	dhcp-snooping vlan VLANID	This command enables the DHCP snooping function on a VLAN or range of VLANs.
configure	no dhcp-snooping vlan VLANID	This command disables the DHCP snooping function on a VLAN or range of VLANs.
configure	dhcp-snooping server IPADDR	This command configures a valid DHCP server.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.
interface	no dhcp-snooping host	This command configures the maximum host count to default for the specific port.
interface	dhcp-snooping trust	This command configures the trust port for the specific port.
interface	no dhcp-snooping trust	This command configures the un-trust port for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.

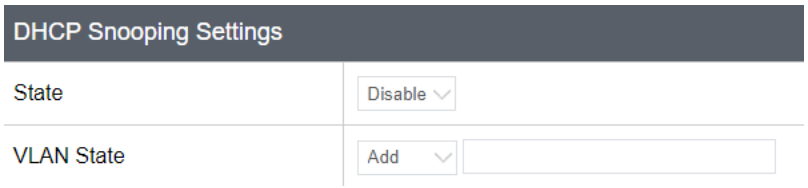
if-range	dhcp-snooping host	This command configures the maximum host count for the specific ports.
if-range	no dhcp-snooping host	This command configures the maximum host count to default for the specific ports.
if-range	dhcp-snooping trust	This command configures the trust port for the specific ports.
if-range	no dhcp-snooping trust	This command configures the un-trust port for the specific ports.

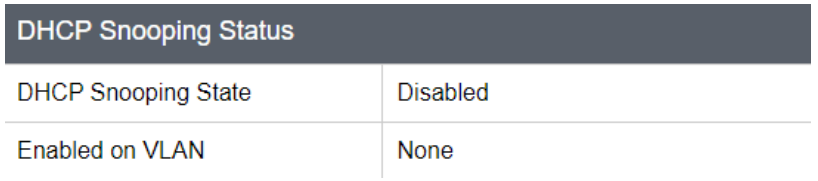
Example:

[DEVICE_NAME]#*configure terminal*
[DEVICE_NAME](config)*#dhcp-snooping enable*
[DEVICE_NAME](config)*#dhcp-snooping vlan 1*
[DEVICE_NAME](config)*#interface 1/0/1*
[DEVICE_NAME](config-if)*#dhcp-snooping trust*

DHCP Snooping

Security > DHCP Snooping > Settings

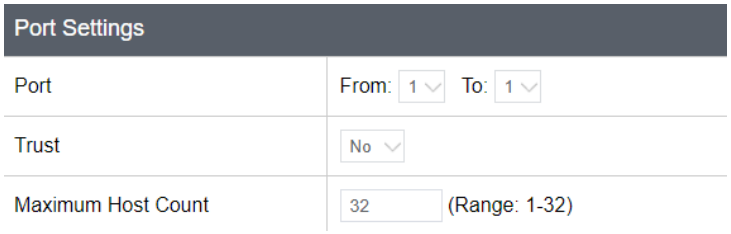




Parameter	Description
State	Select **Enable** to use DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLANs and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports. Select **Disable** to not use DHCP snooping.
VLAN State	
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
DHCP Snooping Status	
DHCP Snooping State	This field displays the current status of the DHCP snooping feature, **Enabled** or **Disabled**.
Enabled on VLAN	This field displays the VLAN IDs that have DHCP snooping enabled on them. This will display **None** if no VLANs have been set.

DHCP Snooping Interfaces

Security > DHCP Snooping > Interfaces



Port Status

Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
1	NO	32	2	NO	32
3	NO	32	4	NO	32
5	NO	32	6	NO	32

Parameter	Description
Port	Select a port number to modify its maximum host count.
Trust	Configures the specific port if it is a trust port.
Maximum Host Count	Enter the maximum number of hosts (1-32) that are permitted to simultaneously connect to a port.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

DHCP Snooping Binding Table

Security > DHCP Snooping > Binding

Parameter	Description
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Type	This field displays how the Switch learned the binding. **Static**: This binding was learned from information provided manually by an administrator. **Dynamic**: This binding was learned by snooping DHCP packets.

DHCP Server Screening

Security > DHCP Snooping > Server Screening

Parameter	Description
IP Address	This field configures the valid DHCP server's IP address.
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Server Screening List	
No.	This field displays the index number of the DHCP server entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the DHCP server.
Action	Click Delete to remove a configured DHCP server.

DHCP Options

DHCP Options, formally known as DHCP Options 82 is the "DHCP Relay Agent Information Option". Option 82 was designed to allow a DHCP Relay Agent to insert circuit specific information into a request that is being forwarded to a DHCP server. Specifically the option works by setting two sub-options: Circuit ID and Remote ID.

The DHCP option 82 is working on the DHCP snooping or/and DHCP relay. The switch will monitor the DHCP packets and append some information as below to the DHCPDISCOVER and DHCPREQUEST packets. The switch will remove the DHCP Option 82 from the DHCPOFFER and DHCPACK packets. The DHCP server will assign IP domain to the client dependent on these information.

The maximum length of the information is 32 characters.

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

When you enable the DHCP snooping information option 82 on the switch, this sequence of events occurs:

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

Option Frame Format:

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

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

Sub-Option	Len	Sub-Option Value

1	N	s1	s2	s3	s4	…	sN

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

Circuit ID Sub-option Format:

Sub-Option Type	Length	Information
0x01		Circuit Form

Remote ID Suboption Frame Format:

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

Circuit Form:

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

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

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

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

Rules:

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

Keyword:

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

SPACE -Add a space character.

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

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

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

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

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

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

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

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

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

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

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

For Example:

HOSTNAME=[YOUR_DEVICE_NAME].

SVLAN=44.

CVLAN=32.

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

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

Default Settings:

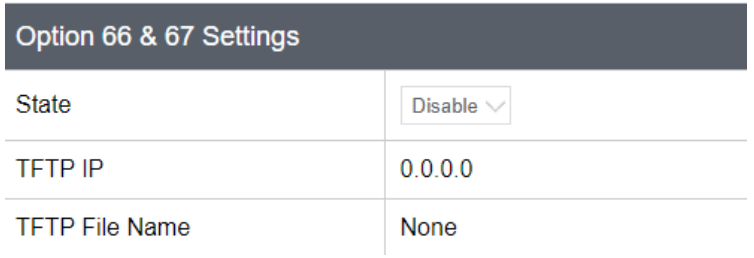
DHCP Option 82 state: disabled.
Circuit Frame: 1.
Circuit Shelf: 0.
Circuit Slot: 0.
Circuit ID String:
%HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN
Remote ID String:
%HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN

CLI Configuration

Node	Command	Description
enable	show dhcp-options	This command displays the DHCP options configurations.
configure	dhcp-options option82 (disable | enable)	This command disables / enables the DHCP option 82 on the Switch.
configure	dhcp-options option82 circuit_id	This command configures the information of the circuit ID sub-option.
configure	dhcp-options option82 remote_id	This command configures the information of the remote ID sub-option.
configure	dhcp-options option82 circuit_frame VALUE	This command configures the frame ID for the circuit sub-option.
configure	dhcp-options option82 circuit_shelf VALUE	This command configures the shelf ID for the circuit sub-option.
configure	dhcp-options option82 circuit_slot VALUE	This command configures the slot ID for the circuit sub-option.

DHCP Options 66 & 67

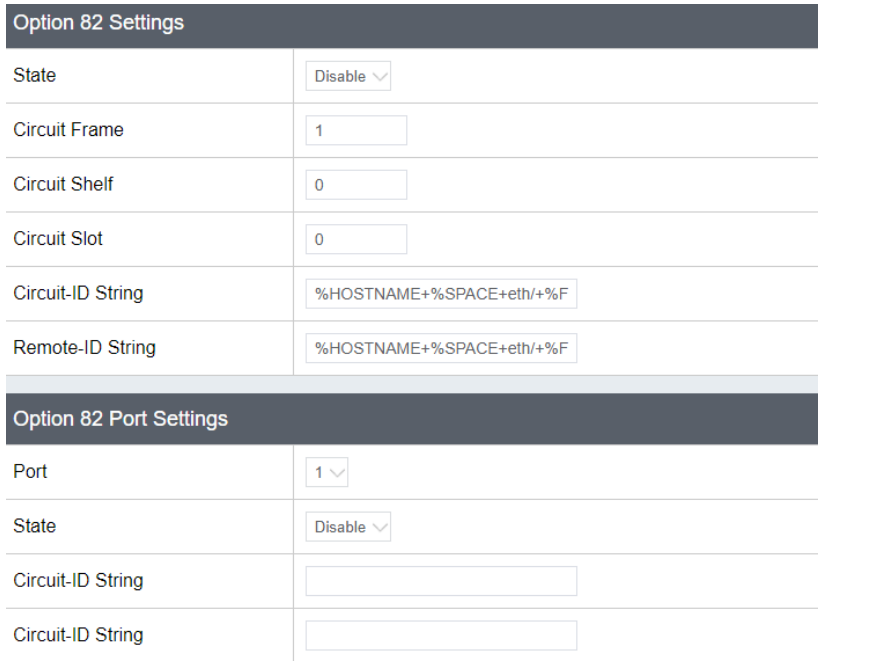
Security > DHCP Options > Option 66 & 67

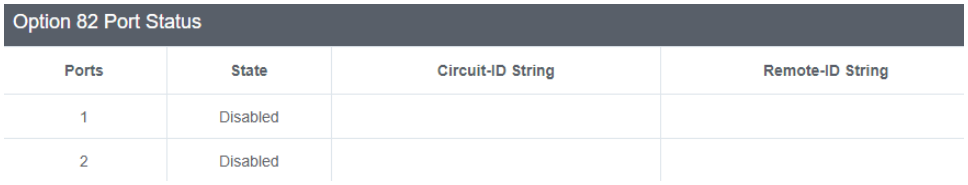


Parameter	Description
State	Select this option to enable / disable the DHCP option 66 & 67 on the Switch.
TFTP IP	Displays the IP address
TFTP File Name	Displays the file name

DHCP Options 82

Security > DHCP Options > Option 82





Parameter	Description
State	Select this option to enable / disable the DHCP option 82 on the Switch.
Circuit Frame	The frame ID for the circuit sub-option.
Circuit Shelf	The shelf ID for the circuit sub-option.
Circuit Slot	The slot ID for the circuit sub-option.
Circuit-ID String	The String of the circuit ID sub-option information.
Remote-ID String	The String of the remote ID sub-option information.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
DHCP Option 82 Port Settings	
Port	The Port ID.
Curcuit-ID String	The String of the circuit ID sub-option information for the specific port.
Remote-ID String	The String of the remote ID sub-option information for the specific port.
DHCP Option 82 Port Status	
	The field displays all of the ports' configurations.

DHCP Relay

Because the *DHCPDISCOVER* message is a broadcast message, and broadcasts only cross other segments when they are explicitly routed, you might have to configure a DHCP Relay Agent on the router interface so that all DHCPDISCOVER messages can be forwarded to your DHCP server. Alternatively, you can configure the router to forward DHCP messages and BOOTP message. *In a routed network, you would need DHCP Relay Agents if you plan to implement only one DHCP server.*

The DHCP Relay that either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet.

Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. A router for such a subnet receives the DHCP broadcasts, converts them to unicast (with a destination MAC/IP address of the configured DHCP server, source MAC/IP of the router itself). The field identified as the **GIADDR** in the main DHCP page is populated with the IP address of the interface on the router it received the DHCP request on. The DHCP server uses the GIADDR field to identify the subnet the device and select an IP address from the correct pool. The DHCP server then sends the DHCP OFFER back to the router via unicast which then converts it back to a broadcast and out to the correct subnet containing the device requesting an address.

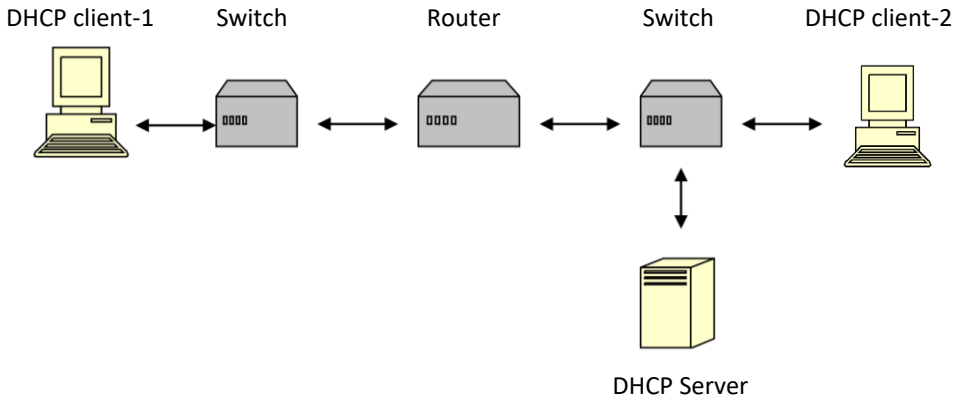
Configurations:

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

Applications:

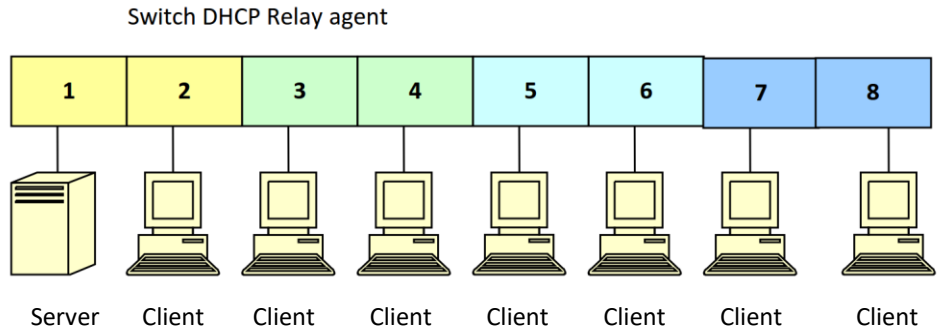
- Application-1 (Over a Router)

  The DHCP cleint-1 and DHCP client-2 are located in different IP segments. But they allocate IP address from the same DHCP server.



- Application-2 (Local in different VLANs)

  The DHCP cleint-1 and DHCP client-2 are located in different VLAN. But they allocate IP address from the same DHCP server.



VLAN 1: port 1, 2 (Management VLAN)
VLAN 2: port 3, 4
VLAN 3: port 5, 6
VLAN 4: port 7, 8

DHCP Server ➔ Port 1.
DHCP Client ➔ Port 2, 3, 4, 5, 6, 7, 8.

Result: Hosts connected to port 2,3,4,5,6,7,8 can get IP from DHCP server.

Note: The DHCP Server must connect to the management VLAN member ports.
The DHCP Relay in management VLAN should be enabled.

Default Settings:

The default global DHCP relay state is disabled.
The default VLAN DHCP relay state is disabled for all VLANs.
The default DHCP server is 0.0.0.0

CLI Configuration

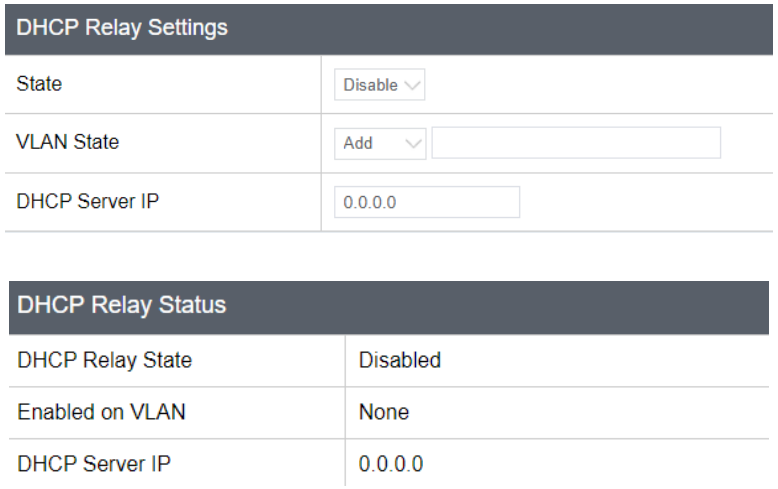
Node	Command	Description
enable	show dhcp relay	This command displays the current DHCP relay configurations.
configure	dhcp relay (disable | enable)	This command disables/enables the DHCP relay on the switch.
configure	dhcp relay vlan VLAN_RANGE	This command enables the DHCP relay function on a VLAN or a range of VLANs.
configure	no dhcp relay vlan VLAN_RANGE	This command disables the DHCP relay function on a VLAN or a range of VLANs.
configure	dhcp helper-address IP_ADDRESS	This command configures the DHCP server's IP address.
configure	no dhcp helper-address	This command removes the DHCP server's IP address.

Example:

[DEVICE_NAME]#*configure terminal*
[DEVICE_NAME](config)#*interface eth0*
[DEVICE_NAME](config-if)#*ip address 172.20.1.101/24*
[DEVICE_NAME](config-if)#*ip address default-gateway 172.20.1.1*
[DEVICE_NAME](config)#*dhcp relay enable*
[DEVICE_NAME](config)#*dhcp relay vlan 1*
[DEVICE_NAME](config)#*dhcp helper-address 172.20.1.1*

Web Configuration

Advanced Settings > DHCP Relay



Parameter	Description
State	Enables / disables the DHCP relay for the Switch.
VLAN State	Enables / disables the DHCP relay on the specific VLAN(s).
DHCP Server IP	Configures the DHCP server's IP address.

ARP Inspection

Dynamic ARP inspection is a security feature which validates ARP packet in a network by performing IP to MAC address binding inspection. Those will be stored in a trusted database (the DHCP snooping database) before forwarding. Dynamic ARP intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before it updates the local ARP cache or before it forwards the packet to the appropriate destination.

Trusted and untrusted port

- This setting is independent of the trusted and untrusted setting of the DHCP snooping.
- The Switch does not discard ARP packets on trusted ports for any reasons.
- The Switch discards ARP packets on un-trusted ports if the sender's information in the ARP packets does not match any of the current bindings.
- Normally, the trusted ports are the uplink port and the untrusted ports are connected to subscribers.

Configuration:

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

Default Settings

The ARP Inspection on the Switch is disabled.

The age time for the MAC filter is 5 minutes.

ARP Inspection is enabled in VLAN(s): None.

Port	Trusted	Port	Trusted
1	no	2	no
3	no	4	no
5	no	6	no
7	no	8	no
9	no	10	no
11	no	12	no
13	no	14	no
15	no	16	no

Notices

There are a global state and per VLAN states.

- ✓ When the global state is disabled, the ARP Inspection 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 ARP Inspection on the specific VLAN.

CLI Configuration

Node	Command	Description
enable	show arp-inspection	This command displays the current ARP Inspection configurations.
configure	arp-inspection (disable | enable)	This command disables/enables the ARP Inspection function on the switch.
configure	arp-inspection vlan VLANID	This command enables the ARP Inspection function on a VLAN or range of VLANs.
configure	no arp-inspection vlan VLANID	This command disables the ARP Inspection function on a VLAN or range of VLANs.
interface	arp-inspection trust	This command configures the trust port for the specific port.
interface	no arp-inspection trust	This command configures the un-trust port for the specific port.

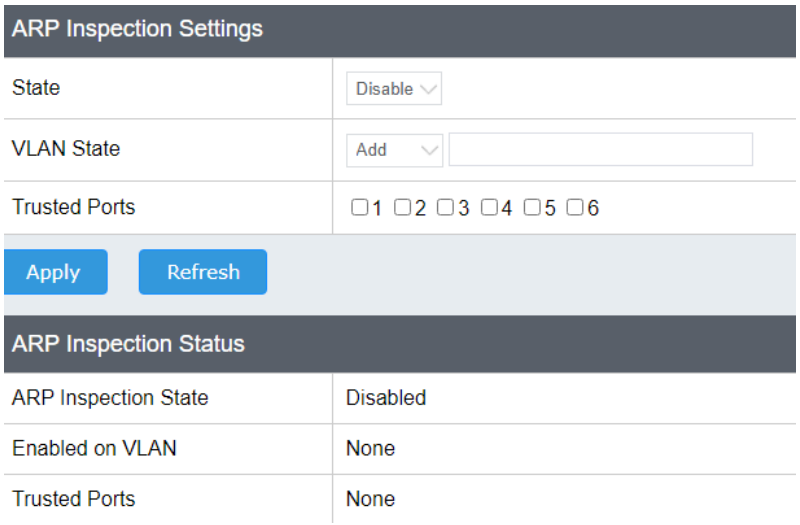
Example:

[DEVICE_NAME]#*configure terminal*

[DEVICE_NAME](config)*#arp-inspection enable*
[DEVICE_NAME](config)*#arp-inspection vlan 1*
[DEVICE_NAME](config)*#interface 1/0/1*
[DEVICE_NAME](config-if)*#arp-inspection trust*

Web Configuration

Security > Dynamic ARP Inspection > Port Settings



Parameter	Description
State	Use this to **Enable** or **Disable** ARP inspection on the Switch.
VLAN State	Enter the VLAN IDs you want the Switch to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).
Trusted Ports	Select the ports which are trusted and deselect the ports which are untrusted.
	The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Apply	Click **Apply** to add/modify the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
ARP Inspection Status	
ARP Inspection State	This field displays the current status of the ARP Inspection feature, **Enabled** or **Disabled**.
Enabled on VLAN	This field displays the VLAN IDs that have ARP Inspection enabled on them. This will display None if no VLANs have been set.
Trusted Ports	This field displays the ports which are trusted. This will display **None** if no ports are trusted.

Filter Table

Dynamic ARP inspections validates the packet by performing IP to MAC address binding inspection stored in a trusted database (the DHCP snooping database) before forwarding the packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. The switch also periodically deletes entries if the age-time for the entry is expired.

- If the ARP Inspection is enabled and the system detects invalid hosts, the system will create a filtered entry in the MAC address table.

- When Port link down and ARP Inspection was disabled, Switch will remove the MAC-filter entries learned by this port.
- When Port link down and ARP Inspection was enabled, Switch will remove the MAC-filter entries learned by this port.
- The maximum entry of the MAC address filter table is 256.
- When MAC address filter table of ARP Inspection is full, the Switch receives unauthorized ARP packet, and it automatically creates a SYSLOG and drop this ARP packet. The SYSLOG event happens on the first time.

Default Settings:

The mac-filter age time: 5 minutes. (0 – No age)

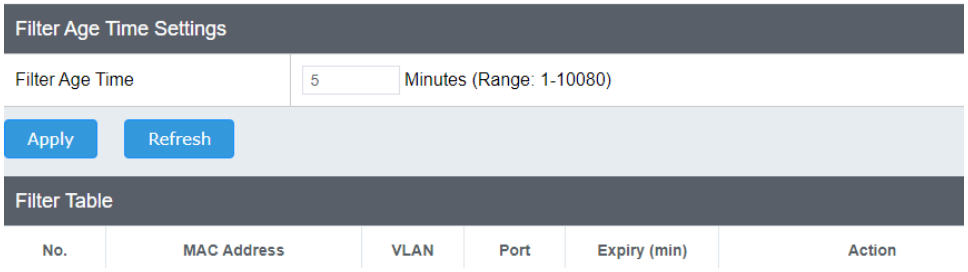
The maximum mac-filter entries: 256.

CLI Configuration

Node	Command	Description
enable	show arp-inspection mac-filter	This command displays the current ARP Inspection filtered MAC.
configure	arp-inspection macfilter age VALUE	This command configures the age time for the ARP inspection MAC filter entry.
configure	clear arp-inspection mac-filter	This command clears all of entries in the filter table.
configure	no arp-inspection mac-filter mac MACADDR vlan VLANID	This command removes an entry from the ARP inspection MAC filter table.

Web Configuration

Security > Dynamic ARP Inspection > Filter Table



Parameter	Description
Filter Age Time	This setting has no effect on existing MAC address filters. Enter how long (1-10080 minutes) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.
Apply	Click **Apply** to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Filter Table	
No.	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VLAN	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (min)	This field displays how long (in minutes) the MAC address filter remains in the Switch.
Action	Click **Delete** to remove the record manually.

Access Control List (ACL)

L2 Access control list (**ACL**) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny". "deny" means rejecting these packets.

The Action Resolution engine collects the information (action and metering results) from the hit entries: if more than one rule matches, the actions and meter/counters are taken from the policy associated with the matched rule with highest priority.

L2 ACL Support:

1. Filter a specific source MAC address.
   Command: *source mac host MACADDR*
2. Filter a specific destination MAC address.
   Command: *destination mac host MACADDR*
3. Filter a range of source MAC address.
   Command: *source mac MACADDR MACADDR*
   The second MACADDR is a mask, for example: ffff.ffff.0000
4. Filter a range of destination MAC address.
   Command: *destination mac MACADDR MACADDR*
   The second MACADDR is a mask, for example: ffff.ffff.0000

L3 ACL Support:

1. Filter a specific source IP address.
   Command: *source ip host IPADDR*
2. Filter a specific destination IP address.
   Command: *destination ip host IPADDR*
3. Filter a range of source IP address.
   Command: *source ip IPADDR IPADDR*
   The second IPADDR is a mask, for example: 255.255.0.0
4. Filter a range of destination IP address.
   Command: *destination ip IPADDR IPADDR*

L4 ACL Support:

1. Filter a UDP/TCP source port.
2. Filter a UDP/TCP destination port.

Default Settings:

Maximum profile: 64.

Maximum profile name length: 16.

Notices

The ACL name should be a combination of alphanumeric characters.

CLI Configuration

Node	Command	Description
enable	show access-list	This command displays all of the access control profiles.
configure	access-list STRING iptype (ipv4|ipv6)	This command creates a new access control profile. Where the STRING is the profile name. And you can specify the type, ipv4 or ipv6.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.

acl	action (disable|drop|permit)	This command actives this profile. disable – disable the profile. drop – If packets match the profile, the packets will be dropped. permit – If packets match the profile, the packets will be forwarded.
acl	action dscp remarking <0-63>	This command actives this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile.
acl	action 802.1p remarking <0-7>	This command actives this profile and specify that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile.
acl	802.1p VALUE	This command configures the 802.1p value for the profile.
acl	dscp VALUE	This command configures the DSCP value for the profile.
acl	destination mac host MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hexdecimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source AMC and mask for the profile.
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and mask for the profile.
acl	no source ip	This command removes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and mask for the profile.

acl	no destination ip	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Where the MAC mask allows users to filter a range of MAC in the packets' source MAC or destination MAC.

For example:

source mac 00:01:02:03:04:05 ff:ff:ff:ff:00

➔ The command will filter source MAC range from 00:01:02:03:00:00 to 00:01:02:03:ff:ff

Where the IPMASK mask allows users to filter a range of IP in the packets' source IP or destination IP.

For example:

source ip 172.20.1.1 255.255.0.0

➔ The command will filter source IP range from 172.20.0.0 to 172.20.255.255

Example:

[DEVICE_NAME]#*configure terminal*

[DEVICE_NAME](config)#*access-list 111*

[DEVICE_NAME](config-acl)#*vlan 2*

[DEVICE_NAME](config-acl)#source interface 1

[DEVICE_NAME](config-acl)#show

Profile Name: 111

Activate: disabled

VLAN: 2

Source Interface: 1

Destination MAC Address: any

Source MAC Address: any

Ethernet Type: any

Source IP Address: any

Destination IP Address: any

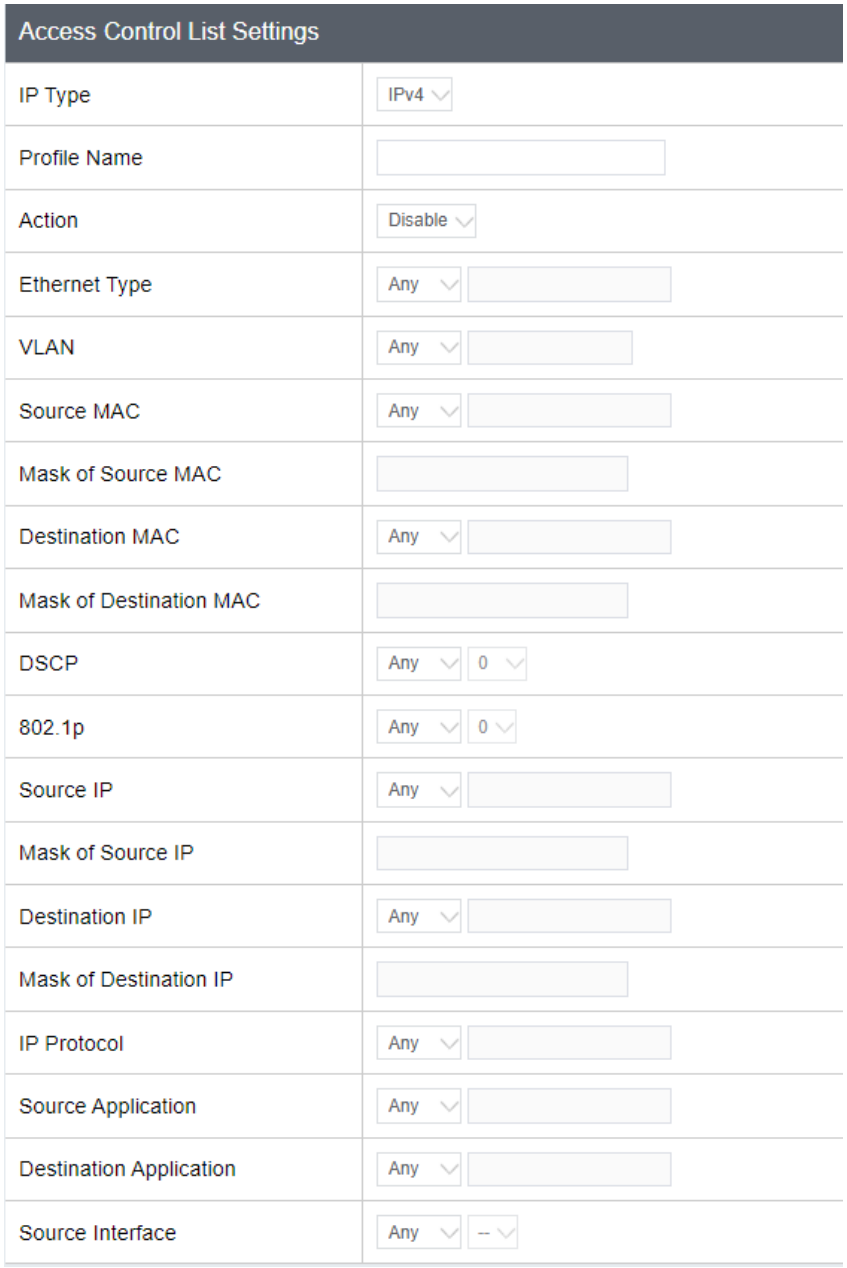
Source Application: any

Destination Application: any

Note: Any: Doesn't matter.

Web Configuration

Security > Access Control List



Parameter	Description
IP Type	Selects IPv4 / IPv6 type for the profile.
Profile Name	The access control profile name.
Action	Selects Disables / Drop / Permits / DSCP action for the profile.
Ethernet Type	Configures the Ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures the source MAC of the packets that you want to filter.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets that you want to filter. If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Destination MAC field.
DSCP	Configure the DSCP for the profile.
802.1p	Configures the 802.1p for the profile.
Source IP	Configures the source IP of the packets that you want to filter.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets that you want to filter.

	If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets that you want to filter.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets that you want to filter. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
IP Protocol	Configures the IP protocol type. The setting will be used for Source Application and Destination Application. TCP:0x06. UDP:0x11.
Source Application	Configures the source UDP/TCP ports of the packets that you want to filter.
Destination Application	Configures the destination UDP/TCP ports of the packets that you want to filter.
Source Interface(s)	Configures one or a rage of the source interfaces of the packets that you want to filter.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

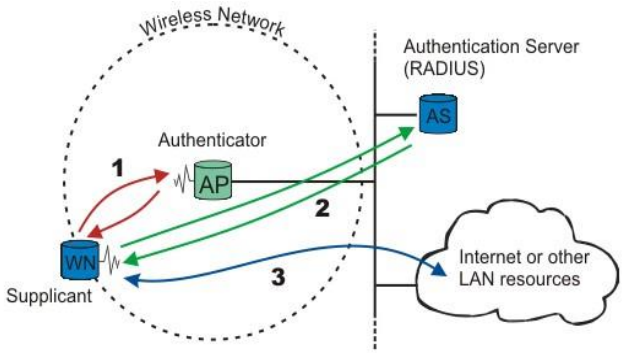
802.1x

IEEE 802.1X is an IEEE Standard for port-based Network Access Control ("port" meaning a single point of attachment to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP).

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity is authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

Upon detection of the new client (supplicant), the port on the switch (authenticator) is enabled and set to the "**unauthorized**" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant logs off, it sends an EAP-logoff message to the authenticator. The authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

The following figure illustrates how a client connecting to an IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password.



When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

Guest VLAN:

The Guest VLAN in IEEE 802.1x port authentication on the switch to provide limited services to clients, such as downloading the IEEE 802.1x client. These clients might be upgrading their system for IEEE 802.1x authentication.

When you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

Port Parameters:

- **Admin Control Direction:**

  both- drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.

  in- drop only incoming packets on the port when a user has not passed 802.1x port authentication.

- **Re-authentication:**

  Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.

- **Reauth-period:**

  Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.

- **Port Control Mode:**

  auto: Users can access network after authenticating.

  force-authorized: Users can access network without authentication.

  force-unauthorized: Users cannot access network.

- **Quiet Period:**

  Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.

- **Server Timeout:**

  The server-timeout value is used for timing out the Authentication Server.

- **Supp-Timeout:**

  The supp-timeout value is the initialization value used for timing out a Supplicant.

- **Max-req Time:**

  Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.

Default Settings

The default global 802.1x state is disabled.

The default 802.1x Authentication Method is local.

The default port 802.1x state is disabled for all ports.

The default port Admin Control Direction is both for all ports.

The default port Re-authentication is disabled for all ports.

The default port Control Mode is auto for all ports.

The default port Guest VLAN is 0 for all ports. (Guest VLAN is disabled).

The default port Max-req Time is 2 times for all ports.

The default port Reauth period is 3600 seconds for all ports.

The default port Quiet period is 60 seconds for all ports.

The default port Supp timeout is 30 seconds for all ports.

The default port Server timeout is 30 seconds for all ports.

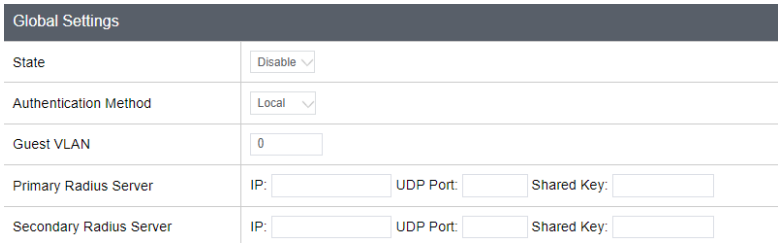
CLI Configuration

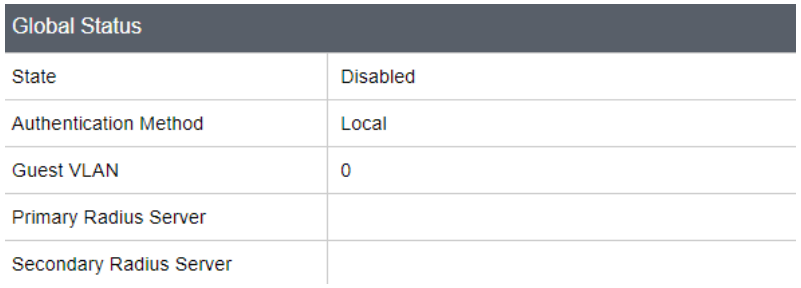
Node	Command	Description
enable	show dot1x	This command displays the current 802.1x configurations.
enable	show dot1x username	This command displays the current user accounts for the local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable|enable)	This command enables/disables the 802.1x authentication on the switch.
configure	dot1x authenticmethod (local|radius)	This command configures the authentic method of 802.1x.
configure	no dot1x authenticmethod	This command configures the authentic method of 802.1x to default.
configure	dot1x radius primaryserver-ip <IP> port PORTID	This command configures the primary radius server.
configure	dot1x radius primaryserver-ip <IP> port PORTID key KEY	This command configures the primary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary radius server.
configure	no dot1x radius secondary-server-ip	This command removes the secondary radius server.
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable|enable)	This command enables/disables the dot1x local accounting records.
configure	dot1x guest-vlan VLANID	This command configures the guest vlan.
configure	no dot1x guest-vlan	This command removes the guest vlan.
interface	dot1x admin-controldirection (both|in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command sets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the max-req times of a port. (1~10).
interface	dot1x port-control (auto | forceauthorized | forceunauthorized)	This command configures the port control mode on the port.
interface	dot1x authentication (disable|enable)	This command enables/disables the 802.1x on the port.
interface	dot1x reauthentication (disable|enable)	This command enables/disables reauthentication on the port.

interface	dot1x timeout quietperiod	This command configures the quiet-period value on the port.
interface	dot1x timeout servertimeout	This command configures the server-timeout value on the port.
interface	dot1x timeout reauthperiod	This command configures the re-auth-period value on the port.
interface	dot1x timeout supptimeout	This command configures the supp-timeout value on the port.
interface	dot1x guest-vlan (disable|enable)	This command configures the 802.1x state on the port.

Web Configuration

Security > 802.1X > Global Settings



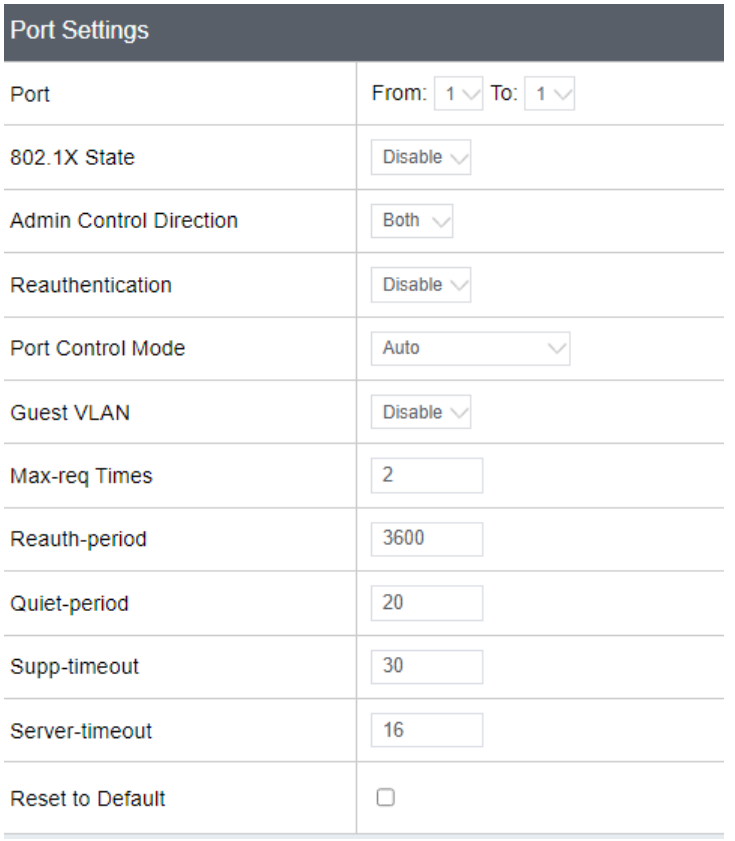


Parameter	Description
State	Select **Enable** to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Authentication Method	Select whether to use **Local** or **RADIUS** as the authentication method. The **Local** method of authentication uses the "guest" and "user" user groups of the user account database on the Switch itself to authenticate. However, only a certain number of accounts can exist at one time. **RADIUS** is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.
Guest VLAN	Configure the guest vlan.
Primary Radius Server	When **RADIUS** is selected as the 802.1x authentication method, the **Primary Radius Server** will be used for all authentication attempts.
Second Radius Server	This is the backup server used only when the **Primary Radius Server** is down.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**.
Share Key	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Global Status	

State	This field displays if 802.1x authentication is **Enabled** or **Disabled**.
Authentication Method	This field displays if the authentication method is **Local** or **RADIUS**.
Guest VLAN	The field displays the guest vlan.
Primary Radius Server	This field displays the IP address, UDP port and shared key for the **Primary Radius Server**. This will be blank if nothing has been set.
Secondary Radius Server	This is the backup server used only when the **Primary Radius Server** is down.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

802.1X Port Settings

Security > 802.1X > Port Settings



Port Status

Port	802.1X State	Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
2	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
3	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
4	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
5	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
6	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16

Parameter	Description
Port	Select a port number to configure.
802.1x State	Select **Enable** to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the Switch before configuring it on each port.
Admin Control Direction	Select **Both** to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select **In** to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	Select **Auto** to require authentication on the port. Select **Force Authorized** to always force this port to be authorized. Select **Force Unauthorized** to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select **Disable** to disable Guest VLAN on the port. Select **Enable** to enable Guest VLAN on the port.
Max-req Time	Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
Supp timeout	Specify how long the Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the Switch to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click **Apply** to reset the custom 802.1x port authentication settings back to default.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
802.1x State	This field displays if 802.1x authentication is **Enabled** or **Disabled** on the port.
Admin Control Direction	This field displays the Admin Control Direction. **Both** will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. **In** will drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	This field displays if the subscriber must periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	This field displays the port control mode. **Auto** requires authentication on the port. **Force Authorized** forces the port to be authorized. **Force Unauthorized** forces the port to be unauthorized. No packets can Pass through the port.
Guest VLAN	This field displays the Guest VLAN setting for hosts that have not passed authentication.

Max-req Time	This field displays the amount of times the Switch will try to connect to the authentication server before determining the server is down.
Reauth period	This field displays how often a client has to re-enter his or her username and password to stay connected to the port.
Quiet period	This field displays the period of the time the client has to wait before the next re-authentication attempt.
Supp timeout	This field displays how long the Switch will wait before communicating with the server.
Server timeout	This field displays how long the Switch will wait before communicating with the client.

TACACS+

Web Configuration

Security > TACACS+

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 5 TACACS+ servers. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server. The user-assigned TACACS+ parameters are applied to newly defined TACACS+ servers. If values are not defined, the system defaults are applied to the new TACACS+ servers.

Parameter	Description
State	Select **Enable/Disable** to enable or disable this TACACS+
Authentication Console Mode	Select **Enable/Disable** to enable or disable management through the console
Authentication Login Mode	Select **Enable/Disable** to enable or disable login locally on the network
Authentication Enable Mode	Select **Enable/Disable** to enable or disable to authenticate each login
Authorization	Select **Enable/Disable** to enable or disable to authorize the login through console
Accounting	Select **Enable/Disable** to enable or disable this function
Primary TACACS Server	Select **IPv4/IPv6** and input the IP address of the primary server
Secondary TACACS Server	Select **IPv4/IPv6** and input the IP address of the secondary server

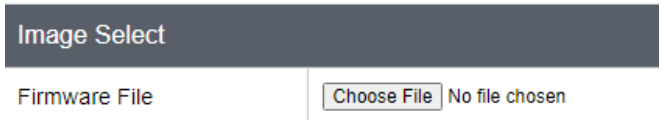
Tools

Firmware Upgrade

Web Configuration

Tools > Firmware Upgrade

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.



Configuration

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:

[DEVICE_NAME]#*configure terminal*

[DEVICE_NAME](config)#*interface eth0*

[DEVICE_NAME](config-if)#*ip address 172.20.1.101/24*

[DEVICE_NAME](config-if)#*ip address default-gateway 172.20.1.1*

[DEVICE_NAME](config-if)#*management vlan 1*

Enable the DHCP client function for the switch.

- **[DEVICE_NAME]#***configure terminal*
- **[DEVICE_NAME](**config)#*interface eth0*
- **[DEVICE_NAME](**config-if)#*ip dhcp client enable*

[DEVICE_NAME]#show config-change-status

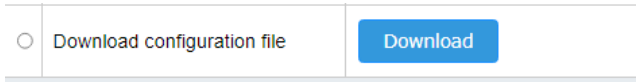
The user configuration file is default.

The configurations have been modified.

Web Configuration

Tools > Config Backup/Restore

Download Configuration



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

Upload / Download Configuration to /from a your server

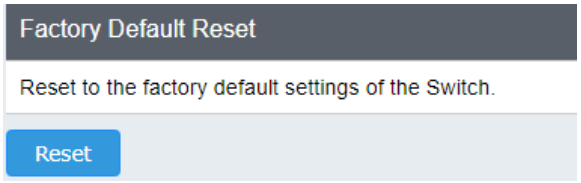
Follow the steps below to save the configuration file to your PC.

- 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.

Factory Reset



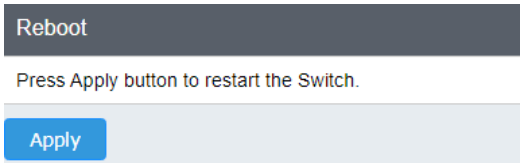
Press the Reset button to set the settings to factory default configuration.

Reboot

Tools > Reboot

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

Follow the steps below to reboot the Switch.

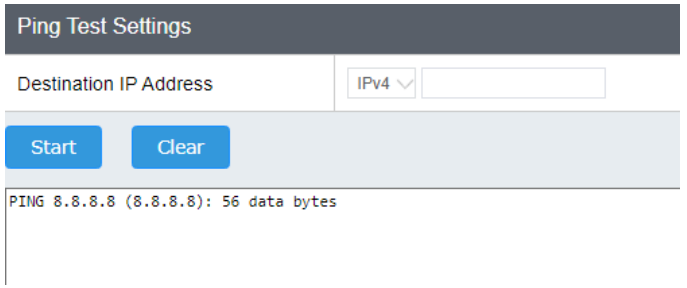


- In the **Reboot** screen, click the **Reboot** button. The following screen displays.

- 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.

Ping

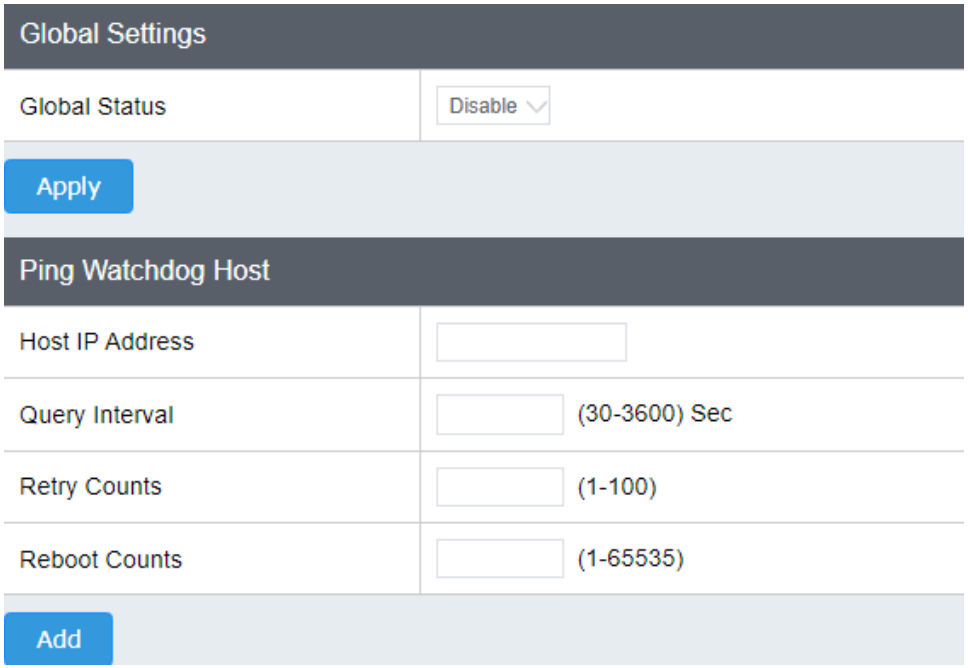
Tools > Ping



- Select either **IPv4** or **IPv6** and input the IP address. Click **Start** to start a ping to the IP address.

Ping Watchdog

Tools > Ping Watchdog



Parameter	Description
Global Status	Select **Enable/Disable** to enable or disable this Ping Watchdog
Apply	Click Apply to save the settings
Ping Watchdog Host	
Host IP Address	Input the IP address for the switch to ping
Query Interval	Input how often a ping will be sent
Retry Counts	Input the number of times the switch will try to ping after a ping failure
Reboot Counts	Input the number of times the switch will reboot before stopping

Technical Specifications

TI-BG262i

Standards

- IEEE 802.1d
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab
- IEEE 802.1ax
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3z
- IEEE 802.3ab
- IEEE 802.3ad
- IEEE 802.3az
- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3bt

Device Interface

- 4 x Gigabit PoE++ ports
- 2 x Gigabit SFP slots
- 1 x Console port (RJ-45)
- Fixed 4-pin power terminal
- Dip Switches
- LED indicators

Data Transfer Rate

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

Performance

- Switch fabric: 12Gbps
- RAM buffer: 512MB
- MAC address table: 16K entries
- Jumbo frames: 10KB
- Forwarding mode: store and forward
- Forwarding rate: 8.9Mpps (64-byte packet size)

Management

- HTTP web-based GUI
- CLI: Telnet / SSHv2
- SNMP v1, v2c, v3
- SNMP trap (up to 5 receivers)
- RMON groups 1/2/3/9
- Device configuration backup & restore, upgrade firmware, reboot, and reset to default
- Multiple administrative or read-only user accounts
- Enable or disable power saving mode per port
- Static MAC entries
- LLDP (Link layer discovery protocol)
- Netlite device map
- ONVIF device discovery
- SNTP
- SMTP alert
- Syslog
- Port statistics/utilization
- Traffic monitor
- Port mirror: one to one, many to one
- Storm control: Broadcast, multicast, destination lookup failure (Min. limit: 1pps)
- Loopback detection
- DHCP relay/option 82
- Xpress Ring

- ERPS (Ethernet Ring Protection Switching) G8032v2
- SFP DDMI (Digital Diagnostic Monitoring Interface)

MIB

- MIB II RFC 1213
- Bridge MIB RFC 1493
- RMON (Group 1,2,3,9) RFC 2819 RFC 1757

Spanning Tree

- IEEE 802.1d STP (spanning tree protocol)
- IEEE 802.1w RSTP (rapid spanning tree protocol)
- IEEE 802.1s MSTP (multiple spanning tree protocol)
- BPDU filter, guard, and root guard

Link Aggregation

- Static link aggregation and 802.3ad dynamic LACP (Up to 3 groups)

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 round robin (WRR), weighted fair queuing (WFQ)

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
- IGMP querier
- IGMP fast leave
- Up to 256 multicast groups
- Static multicast entries

Access Control

- 802.1X authentication (Local user database, RADIUS, guest VLAN assignment)
- DHCP snooping/screening
- Trusted host/IP access list for management access
- Port Security/MAC address learning restriction (Up to 100 entries per port)
- Static/dynamic ARP inspection

ACL

- Source/Destination MAC address
- Source/Destination IP address
- Source Interface
- VLAN ID
- EtherType
- TCP/UDP port 1-65535

Layer 3 Features

- IPv4 / IPv6 static routing
- IPv4 / IPv6 proxy ARP
- IP interfaces: Up to 16
- Routing table entries: Up to 500 (IPv4: 400 / IPv6: 100)
- DHCP Relay / Option 82

Special Features

- Netlite device discovery and map display in GUI
- Port security: MAC address learning restriction per port
- DHCP relay/option 82 & DHCP server snooping/screening support
- Wide operating temperature range
- Dual redundant power inputs
- Alarm relay triggered by power failure
- Surge and ESD protection

- Fast PoE & Perpetual PoE

Power

- PWR (Primary) terminal input: 48 – 57V DC
- RPS (Redundant) terminal input: 48 – 57V DC
- Compatible power supply: TI-S12024 (120W), TI-S24048 (240W), TI-S48048 (480W) sold separately
- Max. Consumption: 20W (no PoE load), 380W (full PoE load)

PoE

- PoE budget: 360W@48V DC input,
- PoE++ (802.3bt): Up to 95W per port
- PoE++: mode A+ (1, 2, 3, 6) and mode B- (4, 5, 7, and 8) for power
- PoE auto classification
- PoE port priority/power scheduling/PD alive check
- Fast PoE/perpetual PoE
- Over current/short circuit protection

Terminal Block

- Redundant power inputs, alarm relay contact, 6 pin
- Wire range: 0.5 mm^2 to 2.5 mm^2
- Solid wire (AWG): 12-26
- Stranded wire (AWG): 12-26
- Wire strip length: 10-11mm

DIP Switch

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

Alarm Relay Output

- Relay output with current carrying capacity of 1A, 24V DC
- Short circuit mode when one power source is connected
- Open circuit mode when two power sources are connected

Enclosure

- IP30 rated metal enclosure
- Fanless passive cooling
- DIN-Rail mount
- Grounding point
- ESD (Ethernet) Protection: 8KV DC
- Surge (Power) Protection: 6KV DC

MTBF

- 379,100 hours @ 25° C
- 48,624 hours @ 75° C

Operating Temperature

- -40° – 705° C (-40° – 167° F)

Operating Humidity

- Max. 95% non-condensing

Dimensions

- 170 x 118 x 50mm (6.69 x 4.65 x 1.97 in.)

Weight

- 956g (2.1lbs.)

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 7/8.1/10/11

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**

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

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

Answer:

You should still configure the switch first. After all the settings are applied, go to the switch configuration page, click on Basic, click General Settings and change the IP address of the switch to be within your network's IP subnet. Click Save in the top right to save the IP settings to the NV-RAM.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7/8.1/10/11

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 7/8.1/10/11

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**

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 7/8.1/10/11

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type ***cmd*** to bring up the command prompt.
3. In the command prompt, type ***ping <ip_address>*** with the *<ip_address>* being the IP address you want ping and check for connectivity.

Example: Usage of ping command and successful replies from device.

C:\Users>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type ***ping –c <#> <ip_address>*** with the *<#> ping being the number of time you want to ping and* the *<ip_address>* being the IP address you want ping and check for connectivity.

Example: *ping –c 4 192.168.10.100*

Federal Communication Commission Interference Statement

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

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

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

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

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

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

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

- **EN 55032: 2015 + A11: 2020 Class A**
- **EN 55024: 2010 + A1: 2015**
- **EN 55035: 2017 + A11: 2020**
- **EN 61000-4-2: 2009**
- **EN 61000-4-3:2006 + AMD1: 2007 + AMD2: 2010**
- **EN 61000-4-4: 2012**
- **EN 61000-4-5: 2014 + A1: 2017**
- **EN 61000-4-6: 2014 + AC: 2015**
- **EN 61000-4-8: 2010**

Directives:

EMC Directive 2014/30/EU
RoHS Directive 2011/65/EU
RoHS 3 Directive 2015/863/EU
REACH Regulation (EC) No. 1907/2006
WEEE Directive 2012/19/EU

CE Mark Warning

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

Limited Warranty

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

Limited Warranty

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

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

Limited Lifetime Warranty

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

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

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

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

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

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

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

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

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

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

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

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

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Visit http://www.trendnet.com/gpl or the support section on http://www.trendnet.com and search for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please visit http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP07172015v3 2018/09/15

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