**Industrial Managed Ethernet Switch User Manual – Layer 2**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



|  |  |
| --- | --- |
|  |  |

|  |
| --- |
| **Firmware Version 1.1.99**  User Manual  Compliant: For Military contracts that require the continuous monitoring and protection of industrial control systems (ICS) Networks Operating / monitoring the operating utilities such as Water, Sewer, Electrical, Security, Video, Building Controls, Street, and Intelligent Transportation Systems (ITS).  Uses: Cyber-Lock, IP Device Binding, Cyber-Secure Video, Clean Code Technology, & Secure Console / Chassis (Patent Pending)  **Meets NSA Guidelines for Secure Network Endpoints** |

**Copyright DYMEC 2020 – All Rights Reserved**

.

**DYMEC Series Layer 2 Switches**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| **DYMEC Models Covered by This Manual** | |
| **Specifications Subject to Change at the Direction of DYMEC** | |
|  | |
| **0402 Series:** | KY-MPG0404, KY-MTG0402, KY-MSG0402 |
| **0802 Series:** | KY-MPG0802, KY-MTG0802, KY-MSG0802, KY-MPX0802, KY-MSX0802  KY-MSGA0802, KY-3100EM |
| **0804 Series:** | KY-MPG0804, KY-MTG0804, KY-MSG0804, KY-MPX0804, KY-MTX0804,  KY-MSX0804, KY-MH0804G4, KY-MH0804X4, KY-MH0804G2,  KY-MQ0804G2, KY-MQ0804X2 |
| **0812 Series:** | KY-MSG0812, KY-MSX0812 |
| **1002 Series:** | KY-MPG1002, KY-MTG1002, KY-MSG1002, KY-MTX1002 |
| **1600 Series**: | KY-MS1600GR-1AC |
| **1604 Series:** | KY-MPG1604, KY-MSG1604, KY-MPX1604, KY-MSX1604  KY-MP1604GB, KY-MP1604XB |
| **2404 Series:** | KY-MSG2404-8C, KY-MS2404GS-8C  KY-MPG2404, KY-MPX2404 |
| **ITS Series:** | KY-3170EM4, KY-3170EM4-P, KY-3170XM |
| **M12 Series:** | KY-MT0802C-M12, KY-MT1000G-M12  KY-MS0802C-M12 |

**Contents**

[Overview](#_bookmark0) [4](#_bookmark0)

[Basic Settings](#_TOC_250000)

[System](#_bookmark1) [9](#_bookmark1)

[IPv4](#_bookmark2) [10](#_bookmark2)

[IPv6](#_bookmark3) [12](#_bookmark3)

[System Time](#_bookmark4) [14](#_bookmark4)

[Precision Time Protocol (PTP)](#_bookmark5) [16](#_bookmark5)

Redundancy

[Spanning Tree](#_bookmark6) [22](#_bookmark6)

[ERPS](#_bookmark7) [31](#_bookmark7)

[MRP](#_bookmark8) [37](#_bookmark8)

Management

[SNMP](#_bookmark9) [42](#_bookmark9)

[DHCP](#_bookmark10) [47](#_bookmark10)

[PoE](#_bookmark11) [54](#_bookmark11)

[Industrial Protocols](#_bookmark12) [60](#_bookmark12)

[UPnP](#_bookmark14) [73](#_bookmark14)

L2 Switching

[Port Management](#_bookmark15) [74](#_bookmark15)

[IGMP Snooping](#_bookmark16) [82](#_bookmark16)

[802.1Q VLAN](#_bookmark17) [86](#_bookmark17)

[Quality of Service](#_bookmark18) [93](#_bookmark18)

[Port Trunk](#_bookmark19) [97](#_bookmark19)

Security

[Storm Control](#_bookmark20) [99](#_bookmark20)

[802.1X](#_bookmark21) [100](#_bookmark21)

[Service Control](#_bookmark22) [104](#_bookmark22)

[Access Control List](#_bookmark23) [106](#_bookmark23)

[SSH](#_bookmark24) [107](#_bookmark24)

Diagnostics

[Port Mirroring](#_bookmark25) [109](#_bookmark25)

[Remote SPAN (RSPAN)](#_bookmark26) [110](#_bookmark26)

[Ping](#_bookmark27) [115](#_bookmark27)

[Cable Diagnostic](#_bookmark28) [117](#_bookmark28)

Monitoring

[LLDP](#_bookmark29) [118](#_bookmark29)

[System Warning](#_bookmark30) [120](#_bookmark30)

[Data Collection](#_bookmark31) [126](#_bookmark31)

[MAC Table](#_bookmark32) [131](#_bookmark32)

Maintenance

[Authorization](#_bookmark33) [133](#_bookmark33)

[Firmware Upgrade](#_bookmark34) [137](#_bookmark34)

[Config Backup](#_bookmark35) [141](#_bookmark35)

[Config Restore](#_bookmark36) [142](#_bookmark36)

[USB Auto-Load & Auto-Backup](#_bookmark37) [143](#_bookmark37)

[Command & Control Node](#_bookmark38) [144](#_bookmark38)

[SFTP File Access](#_bookmark39) [149](#_bookmark39)

[Command Line Interface](#_bookmark40)

[Connect to CLI via Console Port](#_bookmark41) [150](#_bookmark41)

[Connect to CLI via Telnet](#_bookmark42) [151](#_bookmark42)

[Command Groups](#_bookmark44) [158](#_bookmark44)

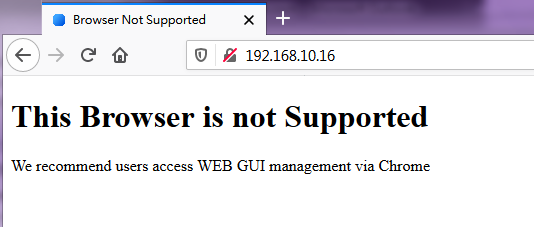
Fun Facts about DYMEC Switches

[Fact Quiz & Information About DYMEC Switches & Software.](#_bookmark41).. [183](#_bookmark41)

# Overview

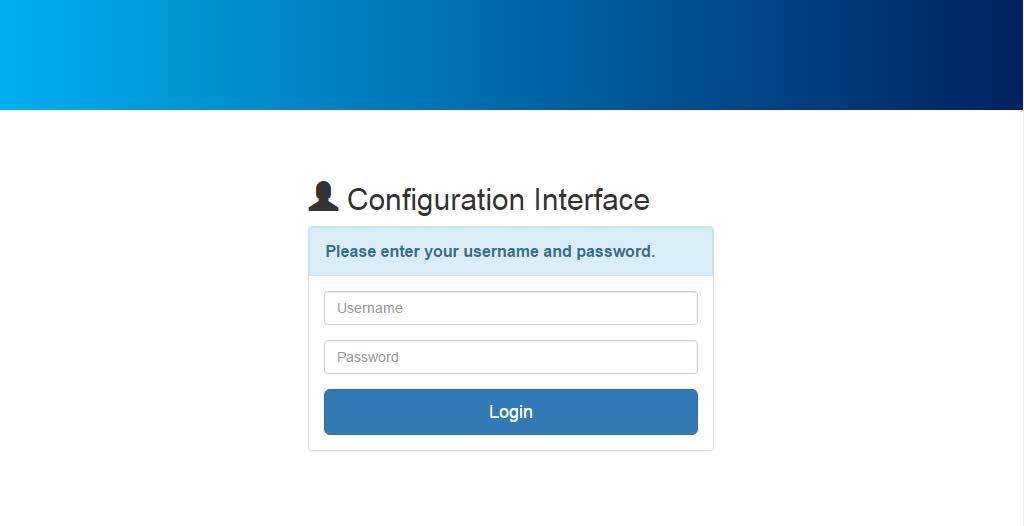
### CONFIGURATION VIA WEB CONSOLE

1. Open the web browser. We recommend using "**Google CHROME**".

**Note:** If the web browser is not supported, the warning message will be shown.

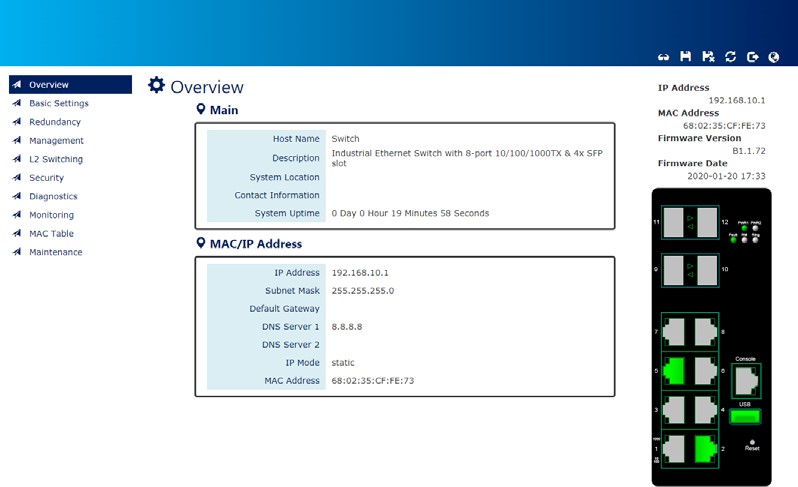
1. Enter the **IP Address** in the **URL** field to connect to the switch and click "Enter" key.

**Note:** The default IP Address is "**192.168.10.1**".

e Th **Login Page** is displayed.

1. Enter the **Username** and **Password** and click "**Login**" Button to login to the system. Note: The default Username and Password is **admin** / **admin**.

After logging into the system, the "**Overview**" page is displayed.



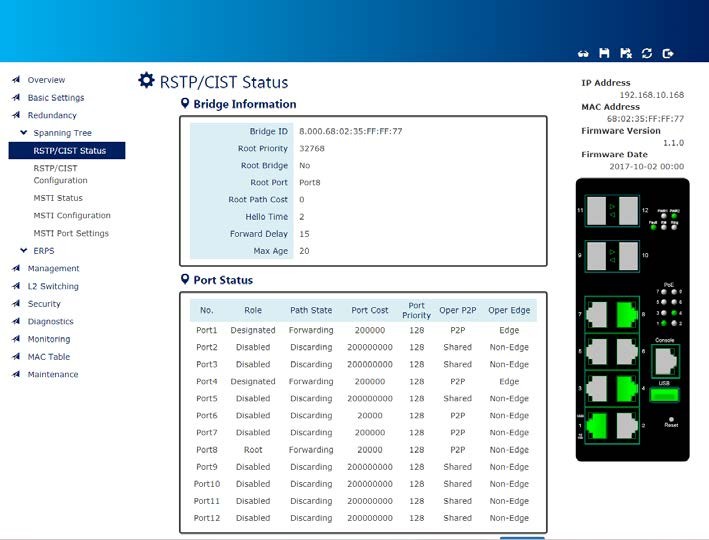
### GLOBAL FUNCTIONS

Five global functions are provided in the header field.

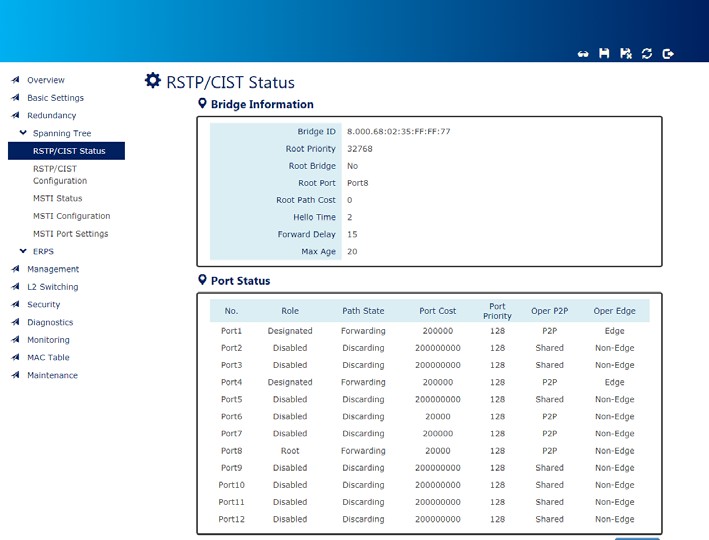
1.  **Hide/Show Model Information**

When a low-resolution environment is used to configure the system via the web console, the "Model Information" field can be hidden to have a better view.

**Show Model Information**:



**Hide Model Information**:



2.  **Save Configuration**

After configuring, click the icon to save the configurations to the "**startup-config**" file. The configurations are retained in the system until a factory reset default is done.

3.  **Restore Factory Default**

Removes the configurations saved in the system. After restoring factory default, all the settings will be set to default values.

4.  **Reboot System**

Reboots the device and restarts the system.

5.  **System Logout**

This option enables you to sign out from the system. Users have to login again if they want to configure the settings.

The system will **auto-logout** after the "timeout" timer expires. The "timeout" timer is configured in the CLI mode by using the "exec-timeout" command.

The maximum value of the timer in the web console is **30 mins**.

6.  **Change Language**

We support multi-languages from firmware version **1.1.72**. The default language is **English** and

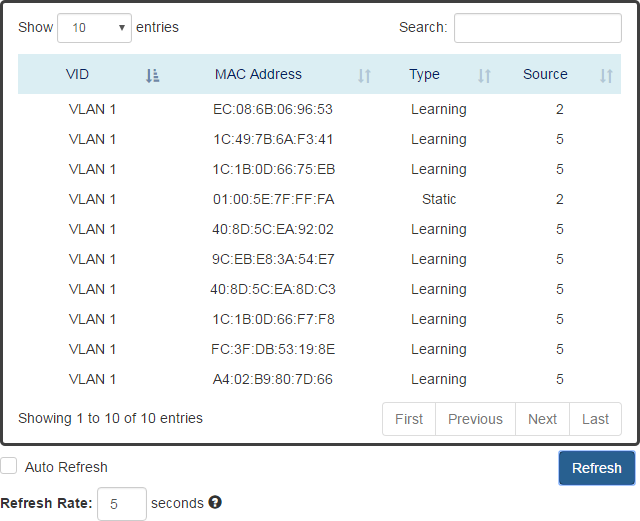
**Traditional Chinese** is also supported by default. If you need other languages, please contact **DYMEC.**



**A USER-FRIENDLY DATA TABLE**

A user-friendly data table is provided on the “**IPv6 Neighbor Table**”, “**IGMP Snooping Table**”, “**VLAN Table**”, “**LLDP Neighbor Table**”, and “**MAC Address Table**”. The following section details how to use the data table functions to help the users to observe the information easily.

The following example is “**MAC Address Table**”.



 

Users will be able to select a value to display the number of entries in one page. The following values can be selected - “**10**”, “**25**”, “**50**”, and “**100**” selections. By default, “**10**” is selected.

 

The search option enables you to search a key word in the data. It will search all the columns and identify the data rows that match the search criteria.

 C:\Users\Kris\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\IPv6NeighborTable.png

It displays the total number of entries and the current entry number.

* + and

This option orders the field from **smaller to larger** or from **larger to smaller**.

 

Changes to “First”, “Previous”, “Next”, or “Last” page.

In addition to the above functions, “**Refresh**” and “**Auto Refresh**” function are available for all status pages including “**IPv6 Neighbor Table**”, “**RSTP Port Status**”, “**DHCP Leased Table**”, “**Port Status**”, “**IGMP Snooping Table**”, “**VLAN Table**”, “**Trunking Status**”, “**LLDP Neighbor Table**”, and “**MAC Address Table**”.

 

Selecting this checkbox enables the “Auto Refresh” function and deselecting the checkbox disables the “Auto Refresh” function.

 

The Refresh Rate option is a **global** configurable variable. When the Auto Refresh option is enabled, the status will refresh automatically based on the Refresh Rate interval.

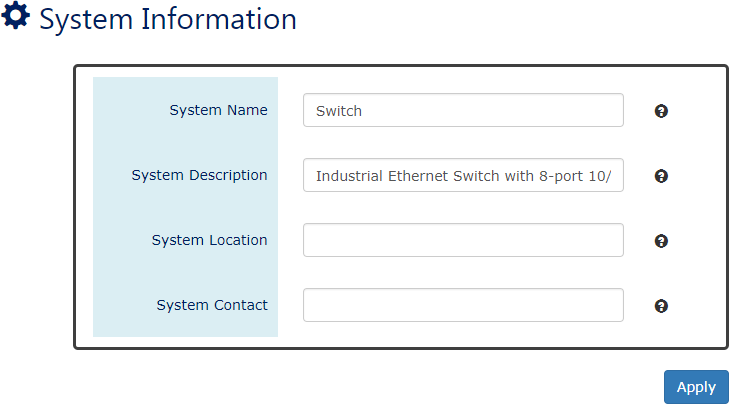
The range of the Refresh Rate is **from 5 to 300** second(s). The default Refresh Rate is **5** seconds.

* + (Refresh Button)

You can click the **“Refresh”** button to manually refresh the status.

# System Information

### CONFIGURE SYSTEM INFORMATION



***For more information, hover the mouse over the icon in the system.***

#### Host Name

It is useful to identify the difference between the switches, for example: CoreSwitch01. The **max. length** for the Host Name is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

#### System Description

The System Description is default defined by the system.

It contains the copper port number, fiber port number, and PoE information (if supported). The **max. length** for the System Description is **68 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

#### Switch Location

It is useful to find the location of the switches, for example: Area01. The **max. length** for the Switch Location is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

#### Contact Information

Records the information of the person responsible for this device and the contact details.

**Note: #, \, ', ", ?** are **invalid** characters.

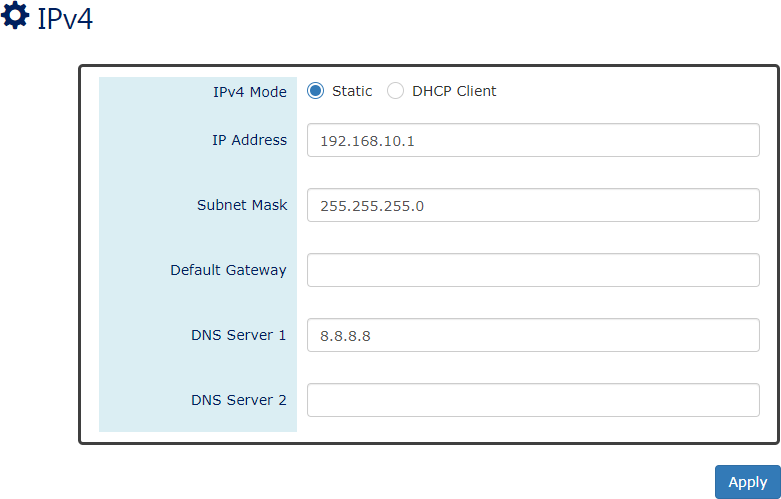
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# IPv4

**Internet Protocol Version 4** (**IPv4**) is the fourth version of the Internet Protocol. It is used on the packet-switched networks and with connectionless communication. IPv4 has four bytes (32 bits) address and the address space is limited to 4,294,967,296 (232) unique addresses. On the local area network (LAN), the “Private Network” is used. It starts from **192.168.0.0** and the address space contains 65,025 (216) IP addresses. The frames can only be sent to the host in the same subnet. For example, the default IP Address of the switch is “192.168.10.1”. When the users want to connect to the web console of the switch, an IP address from “192.168.10.2” to “192.168.10.254” must be assigned to the host.

**CONFIGURE IPV4 INFORMATION**



#### IPv4 Mode

There are 2 ways to configure IPv4 address - one is to configure a **static** IP address manually and another one is to get an IP address by **DHCP**.

If the IPv4 mode is "**DHCP Client**", IPv4 information fields will be set to "**Disabled**".

#### IP Address

Assigns a unique static IP Address in the subnet to access the system. The default IP Address is **"192.168.10.1"**.

#### Subnet Mask

Defines the type of network, to which this device is connected to. The default Subnet Mask is **"255.255.255.0"**.

#### Default Gateway

The IP address of the router used to connect a LAN to a WAN.

#### DNS Server 1 & 2

Specifies the IP address of the DNS Server so that the users can connect to another device based on the **URL** instead of the IP address.

The default DNS Server is **"8.8.8.8"**. It is provided by Google.

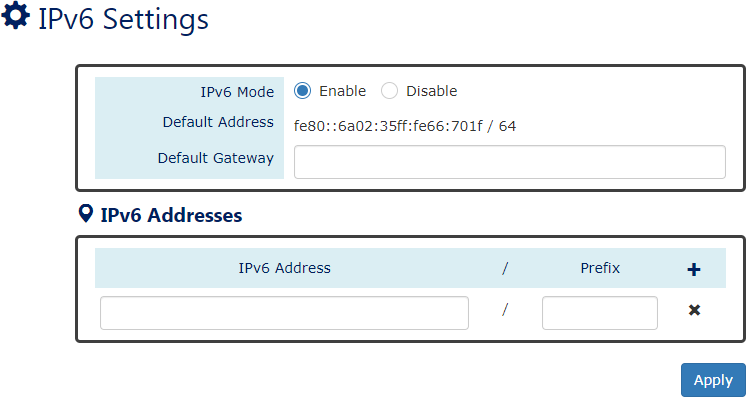
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# IPv6

**Internet Protocol Version 6** (**IPv6**) is a solution to deal with the address space limitation of IPv4 and it is the most recent version of Internet Protocol. It is intended to replace IPv4. IPv6 is a **Layer 3** (Internet Layer) protocol, which is used on the packet-switched networks and with connectionless communication. There are 16 bytes (128 bits) for an IPv6 address and the address space is up to 2128 unique addresses. The IPv6 address is usually represented in hexadecimal digits, 8 groups of 4 digits, and each group is separated by a “**:**” (**colon**). For example, the DNS server address in IPv6 is “2001:4860:4860:0000:0000:0000:0000:8888”.

**CONFIGURE IPV6 INFORMATION**



#### IPv6 Mode

"Enable" or "Disable" IPv6. When the IPv6 Mode is enabled, other devices can connect to this unit.

The default IPv6 Mode is "**Enable**".

#### Default Address

This is the Default IPv6 Address for this device. It is a **Link-Local** address and is automatically generated from the **MAC Address** of the device.

#### Default Gateway

This is the **Default IPv6 Gateway** for this device. The IPv6 address of the router used to connect a LAN to a WAN when the devices are using IPv6 for communication.

#### IPv6 Addresses

Enables the users to define other IPv6 addresses for this device.

The IPv6 address contains 2 section - **IPv6 address** and **prefix**. The default Prefix is **64-bit**.

: Click the **plus icon** to add a IPv6 Address row.

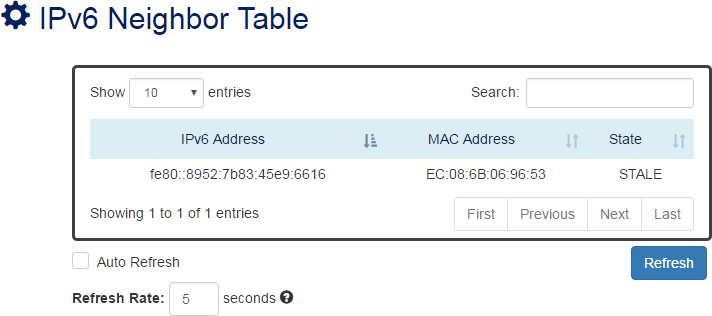


: Click the **remove icon** to delete the IPv6 Address row.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**IPV6 NEIGHBOR TABLE**



#### IPv6 Address

This filed displays the IPv6 address of the neighbor.

#### MAC Address

This filed displays the MAC address of the neighbor.

#### State

The connection state can be “DELAY”, “REACHABLE”, “STALE”, “FAILED”, or “PROBE”.

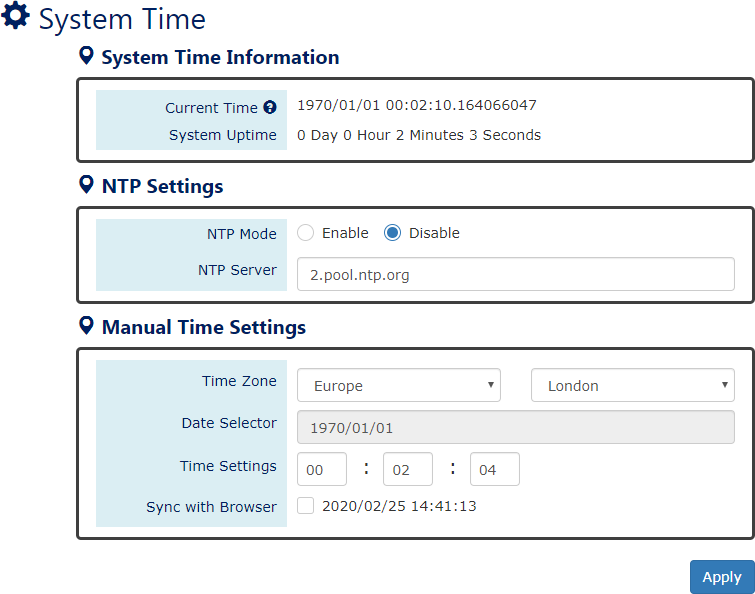
# System Time

The **System Time** represents the date and time. The system uptime defines the passing time after the system boots up. There is no battery on the switch and hence the system time cannot be saved in the system. Users can configure the time zone and system time manually by synchronizing the time with the browser or by enabling the “**NTP**” service to get the time from a **NTP Server**.

## NTP

**Network Time Protocol** (**NTP**) is a clock synchronization protocol, which is used to synchronize the system time with the NTP server. NTP is one of the oldest Internet Protocols in use from 1985 until now. It works based on a client-server model, but it can also be used in peer-to-peer relationships. The NTP application on the switch is follows the client-server model and the switch plays a role in the NTP Client.

### CONFIGURE SYSTEM TIME INFORMATION



#### System Time Information

* + - Current Time: The current date time of the system.

**Note:** Time format: Year/Month/Day 24HR:Min:Sec.NanoSec

* + - System Uptime: The system boot up duration.

#### NTP Settings

* + - NTP Mode

"Enable" or "Disable" NTP Service. If NTP Mode is enabled, the system will sync time with NTP Server on an hourly basis.

* + - NTP Server

This field displays the URL or the IP address of the host that provides the NTP Service.

#### Manual Time Settings

* + - Time Zone

Select the Time Zone to define the local time offset from GMT.

* + - Date Selector

Select the system date manually. The format is "**year/month/day**".

* + - Time Setting

Define the system time manually. The format is "**hour:minute:second**".

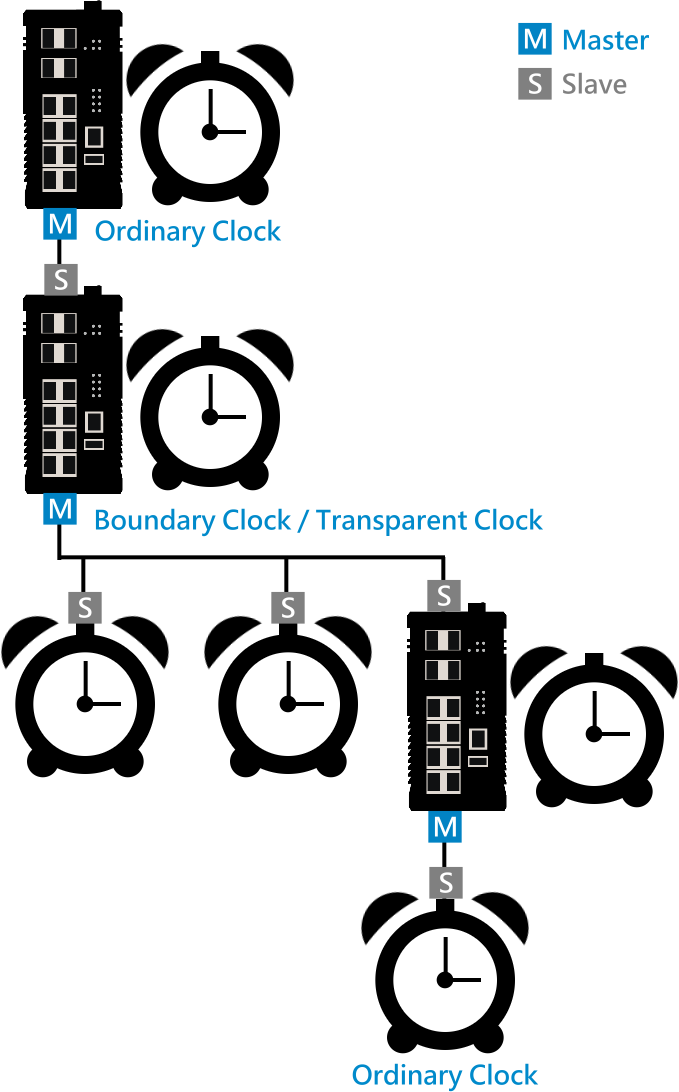
* + - Sync with Browser

Select the checkbox to synchronize the system time with the **browser time**.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

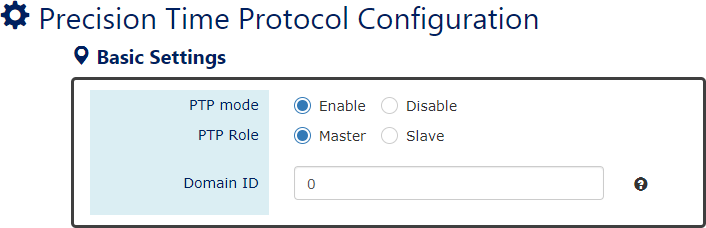
# Precision Time Protocol (PTP)

The **Precision Time Protocol** (**PTP**) is used to synchronize clocks and it is more accurate than NTP. PTP is majorly employed to synchronize the network devices that require precise timing like financial transactions. Synchronization and management of a PTP network is implemented by the exchange of messages across the communications devices.

**PTP** utilizes a **Master** and **Slave** structure. There are three types of PTP clocks – **Ordinary Clock**, **Boundary Clock**, and **Transparent Clock** and currently we support **Ordinary Clock** and **Transparent Clock** on the switches. If the switch is an Ordinary Clock, it can be configured as role Master or Slave. For the Boundary Clock and Transparent Clock, they can be both Master and Salve at the same time to synchronize with the Master and forward to Salves.

Note: Currently the **Transparent Clock** is only supported on MP-1604X.

**CONFIGURE PTP BASIC INFORMATION – ORDINARY CLOCK**



***For more information, hover the mouse over the icon in the system.***

#### PTP Mode

"Enable" or "Disable" the PTP protocol.

**Note**: The **PTP Slave** and **NTP Client** are mutually incompatible, if users want to enable PTP mode with role Slave, please make sure the NTP Client is disabled.

#### PTP Role

There are 2 roles of PTP that supported on the switch – **Master** and **Slave**. The advanced settings of the role Master and Slave are different, and the configurations are presented on the Configure PTP Master and Configure PTP Slave sections.

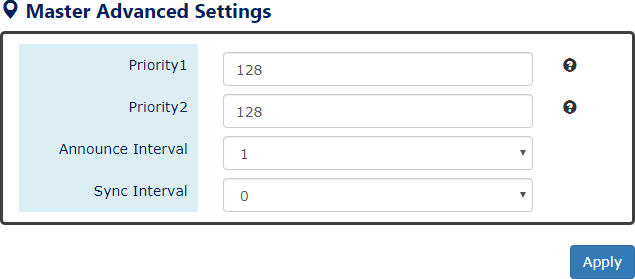
#### Domain ID

The ID is the identifier of the PTP network. Only the nodes with the same Domain ID synchronize the time in the network.

The default value of Domain ID is **0**

The range of Domain ID is **from 0 to 127**

**CONFIGURE PTP OC MASTER**



***For more information, hover the mouse over the icon in the system.***

#### Priority 1

The Priority is used to decide the Best Master when there are several Master nodes in the PTP network. If there are 2 or more Masters with the same **Priority 1**, the system will refer to the **Priority 2**.

The default value of Priority 1 is **128**

The range of Priority 1 is **from 0 to 248**

**Note:** the lower the value the higher the priority

#### Priority 2

The Priority is used to decide the Best Master when there are several Master nodes with the same **Priority 1** in the PTP network. If there are 2 or more Masters with the same **Priority 2**, the system will refer to the **Clock Identity (MAC Address)**.

The default value of Priority 1 is **128**

The range of Priority 1 is **from 0 to 248**

**Note:** the lower the value the higher the priority

#### Announce Interval

The Announce Interval is the period to send Announce Message. The range of Announce Interval is **from -1 to 7**

* + **Sync Interval**

The Sync Interval is the period to send Sync Message. The range of Sync Interval is **from -7 to 7**

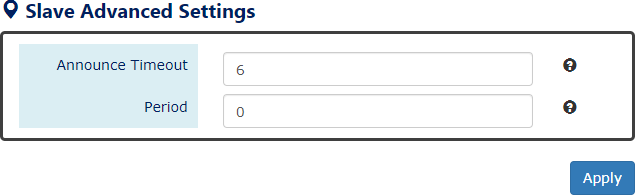
The mapping for Announce Interval and Sync Interval to **second(s)** is as following table:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Interval** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Seconds** | 1s | 2s | 4s | 8s | 16s | 32s | 64s | 128s |
| **Interval** |  | -1 | -2 | -3 | -4 | -5 | -6 | -7 |
| **Seconds** |  | 512ms | 256ms | 128ms | 64ms | 32ms | 16ms | 8ms |

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE PTP OC SLAVE**



***For more information, hover the mouse over the icon in the system.***

#### Announce Timeout

The **Announce Timeout** is the timer for announcing timeout message. The default value of Announce Timeout is **6**

The range of Announce Timeout is **from 2 to 255**

#### Period

The Period is a timeout period. The Slave node will wait n (Period Value) times that announce receipt timeout before resetting.

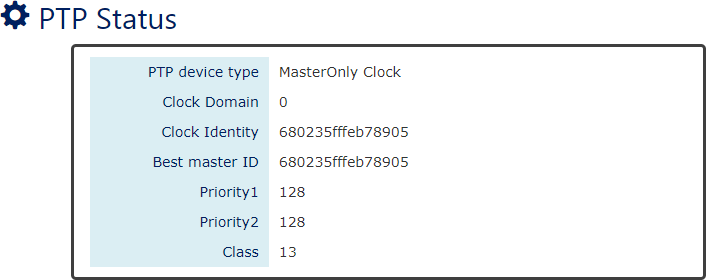
The default value of Period is **0**

The range of Period is **from 0 to 20**

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**PTP STATUS – MASTER**



#### PTP Device Type

This field is the type/role of switch that in a PTP network. The switch can be “**Master Only**” or “**Slave Only**” currently because we only support **Ordinary Clock** now.

#### Clock Domain

This field shows the Domain ID that the system is in now.

#### Clock Identity

This field is the identity of the switch in the PTP network. The Clock Identity is configured to the MAC Address of the switch by default.

#### Best Master ID

The Best Master ID is the Clock Identity of the Best Master in a PTP network. If there are several Master in the PTP network, users can understand which one is the Best Master through this field.

#### Priority 1

This field is the value of **Priority 1** that is configured.

#### Priority 2

This field is the value of **Priority 2** that is configured.

#### Class

The Class field is usually named **colckClass**. The values of PTP clock classes are based on the traditional quality levels from SSM/ESMC.

**PTP STATUS – SLAVE**



#### PTP Device Type

This field is the type/role of switch that in a PTP network. The switch can be “**Master Only**” or “**Slave Only**” currently because we only support **Ordinary Clock** now.

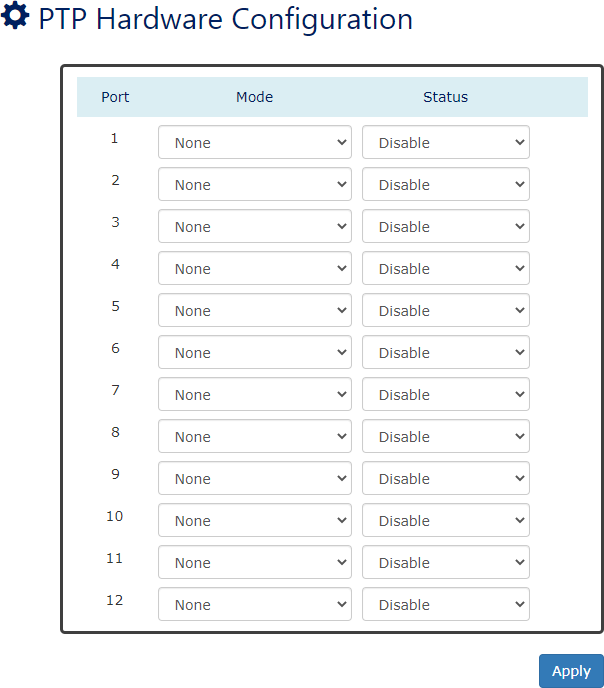
#### Clock Domain

This field shows the Domain ID that the system is in now.

#### Clock Identity

This field is the identity of the switch in the PTP network. The Clock Identity is configured to the MAC Address of the switch by default.

**CONFIGURE PTP BASIC INFORMATION – TRANSPARENT CLOCK**



**Known Limitations:**

The Transparent Clock is only supported on the following conditions:

* **VLAN untagged mode**
* **L2 management switches**
* **Copper ports and 1G SFP Slots**
* **One-step Mode**
* **End-to-End delay mechanism**
  + **Port**

Port 1 to Port N, where N is based on the total port number.

#### Mode

Select Transparent Mode or Normal Mode (None) on the designated port.

#### Status

“Enable” or “Disable” selected mode on the designated port.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

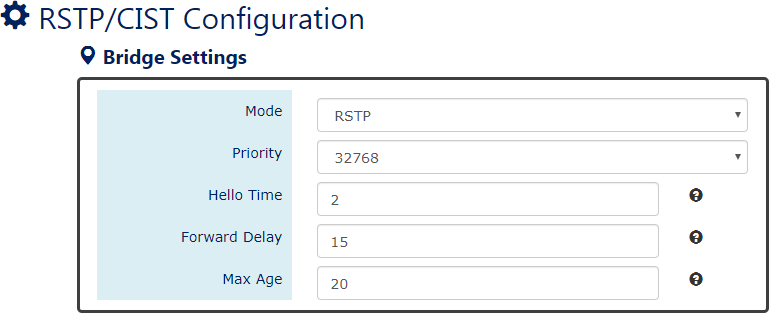
# Spanning Tree

The **Spanning-Tree Protocol** is a standard protocol that is defined in **IEEE 802.1D**. It is used to build a **logical loop-free** topology for layer-2 Networks. The basic function of the protocol is to prevent loops and broadcast flooding around the switches. STP allows spare links in the network design to provide **backup paths** when the active link fails and requires a **convergence time** of **30-50 seconds** to recover the topology when the topology is changed. This prompted the use of **Rapid Spanning-Tree Protocol** as it provides a faster convergence when the topology is changed.

RSTP was introduced by IEEE as **802.1w**. It can respond within **3 x "Hello Time"** when a topology is changed. The "Hello Time" is a configurable value and it is particularly important for RSTP. The default RSTP value is **2 seconds** and typically, the convergence time for RSTP is **under 6 seconds**. RSTP is much faster than STP. RSTP should be used instead of STP.

The **Multiple Spanning-Tree Protocol** defined in the **IEEE 802.1s** is an extension to RSTP for Virtual LANs. MSTP provides a better alternate path than STP/RSTP for different VLANs. It can make a group of VLANs more systemized in the topology.

**CONFIGURE RSTP/CIST BASIC INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### System Time Information

RSTP: Enable STP and run "RSTP" for redundancy. MSTP: Enable STP and run "MSTP" for redundancy.

Disable: Disable STP. Users must enable another protocol to prevent from loop.

#### Root Priority

It is used to define the "**Root Bridge**". The bridge with the **lowest Root Priority** is the "Root Bridge". If all the bridges are set to the same Root Priority value, the system will select the Root Bridge based on the **MAC Addresses**.

The range of Root Priority is **from 0 to 61440** (**multiple of 4096)**. The default Root Priority is **32768**.

#### Hello Time

It is especially important and used to determine the interval to send BPDU (management frame) to check the RSTP topology and status.

The range of Hello Time is **from 1 to 10** second(s). The default Hello Time is **2** seconds.

#### Forward Delay

A delay/timer is used to determine when to change the **Path State** from Learning/Listening to Forwarding.

The range of Forward Delay is **from 4 to 30** seconds. The default Forward Delay is **15** seconds.

#### Maximum Age

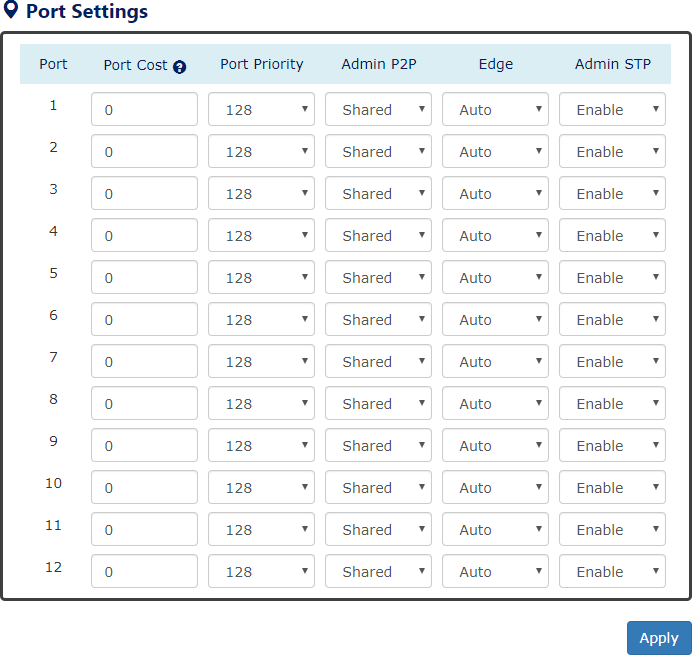
A timer that is used to wait for the Hello BPDU from the Root Bridge. If this device receives the BPDU before the timer expires, the timer will be reset. Else, the device will send the topology changed BPDU to notify other devices.

The range of Maximum Age is **from 6 to 40** seconds. The default Maximum Age is **20** seconds

***The relationship between "Hello Time", "Forward Delay", and "Maximum Age" is:***

***2 x (Forward Delay - 1 sec) >= Max Age >= 2 x (Hello Time + 1 sec)***

**CONFIGURE RSTP PORT INFORMATION**



#### Port

***For more information, hover the mouse over the icon in the system.***

Port 1 to Port N, where N is based on the total port number.

#### Path Cost

The cost from the current node to another device. The range of Path Cost is **from 0 to 200000000**.

The default Path Cost is **0**. This implies that the Path Cost is decided by the system.

#### Port Priority

Used to decide the port to be blocked in the Ring topology.

The range of Root Priority is **from 0 to 240** and are in **multiple of 16**. The default Root Priority is **128**.

#### Admin P2P

The Admin P2P is the link-type for each port. P2P: It is a full-duplex link.

Shared: It is a half-duplex link.

#### Edge

A port that can connect to a **non-STP device** is called an Edge port. Users can manually fix a port to non-Edge or Edge.

Auto: The system **automatically** identifies an Edge or Non-Edge.

Edge: The port is forced to be an Edge port. An edge port will directly be transitioned to the "**Forwarding**" state and is not required to wait for the "Forward Delay". If a port is directly connected to a non-STP device, users can manually set it to "Edge" and enable it to transmit faster.

Non-Edge: The port is forced to be a Non-Edge port. This implies that the port will go through Learning/Listening to Forwarding state even though it is connected to an end device or not.

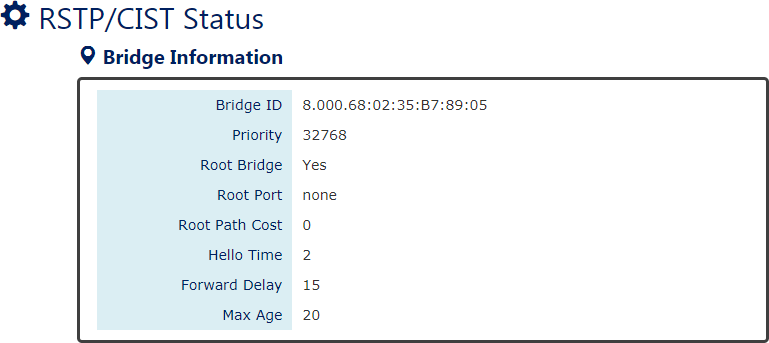
#### Admin STP

"Enable" or "Disable" the Spanning-tree protocol that is running on the specific port.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**RSTP/CIST STATUS**



#### Bridge ID

This field shows the **unique** identity of this node when it is part of a network. It contains **8 bytes** - the first 2 bytes are for **Bridge Priority** (configurable) and the remaining 6 bytes are for the **MAC Address** (unique).

#### Root Bridge

It is elected from the switches in the STP topology via several **STP messages (BPDU)**. The Root Bridge is the node with the **lowest Root Priority**. If all the nodes are with the same Root Priority, the Root Bridge will be selected based on their **MAC Addresses**.

#### Root Priority

It is used to define the "**Root Bridge**". The bridge with the **lowest Root Priority** is the "Root Bridge". If all bridges are set to the same Root Priority value, the system will select the Root Bridge based on the **MAC Addresses**.

#### Root Port

It is the port that is **connected to the Root Bridge** and with the **lowest cost**. If the Root Port shows "**none**", it implies this node is the Root Bridge.

#### Root Path Cost

It is the cost from the current node to the Root Bridge.

#### Hello Time

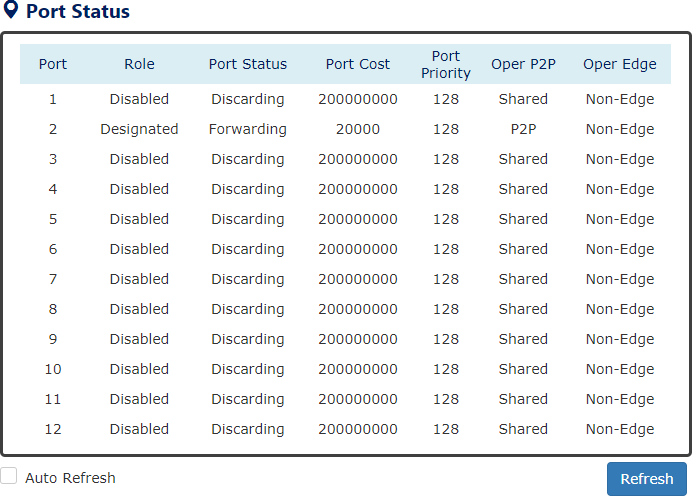
It is used to determine the interval to send BPDU (management frame) to check the RSTP topology and status.

#### Forward Delay

It is used to determine when to change the **Path State** from Learning/Listening to Forwarding.

#### Max Age

It is used during waiting for Hello BPDU from the Root Bridge.



#### Port

Port 1 to Port N, N is based on the total port number.

#### Role

This field shows the role of the STP port.

Root: This is the root port, which is connected to the Root Bridge with the lowest cost. Designated: This is the designated port, which can send the best BPDU on the segment to other connected nodes.

Alternate: This is the alternate port, which is blocked. This port can still receive useful BPDU **from another bridge**. When it receives a useful BPDU, it will help to forward it on the segment.

Backup: This is the backup port, which is blocked. It corresponds with “Alternate Port” to the blocking state. This port also receives useful BPDU, but the BPDU is **from the same bridge**. When it receives a useful BPDU, it will help to forward it on the segment.

Disabled: The port is not linked up.

#### Path State

This field shows the path state of this STP port.

Discarding: The port state can be “Disabled”, “Blocking”, or “Listening”. The incoming frames are dropped and learning MAC addresses are stopped.

Learning: The port is learning MAC addresses, but the incoming frames are dropped. Forwarding: The port in the forwarding state forwards the incoming frames based on the learned MAC address table.

#### Port Cost

This is the cost from the port to the Root Bridge. Spanning-tree Protocol assumes the path cost is determined by the **access speeds of the links**. The **default RSTP path cost** is shown in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Speed** | **RSTP Path Cost** | **Speed** | **RSTP Path Cost** |
| 4 Mbps | 5,000,000 | 1000 Mbps (1Gbps) | 20,000 |
| 10 Mbps | 2,000,000 | 2000 Mbps (2 Gbps) | 10,000 |
| 16 Mbps | 1,250,000 | 10000 Mbps (10 Gbps) | 2,000 |
| 100 Mbps | 200,000 |  | |

#### Port Priority

The Port Priority is used to determine the Root Port on a non-root bridge. The port with the lowest Port Priority value gets the higher priority.

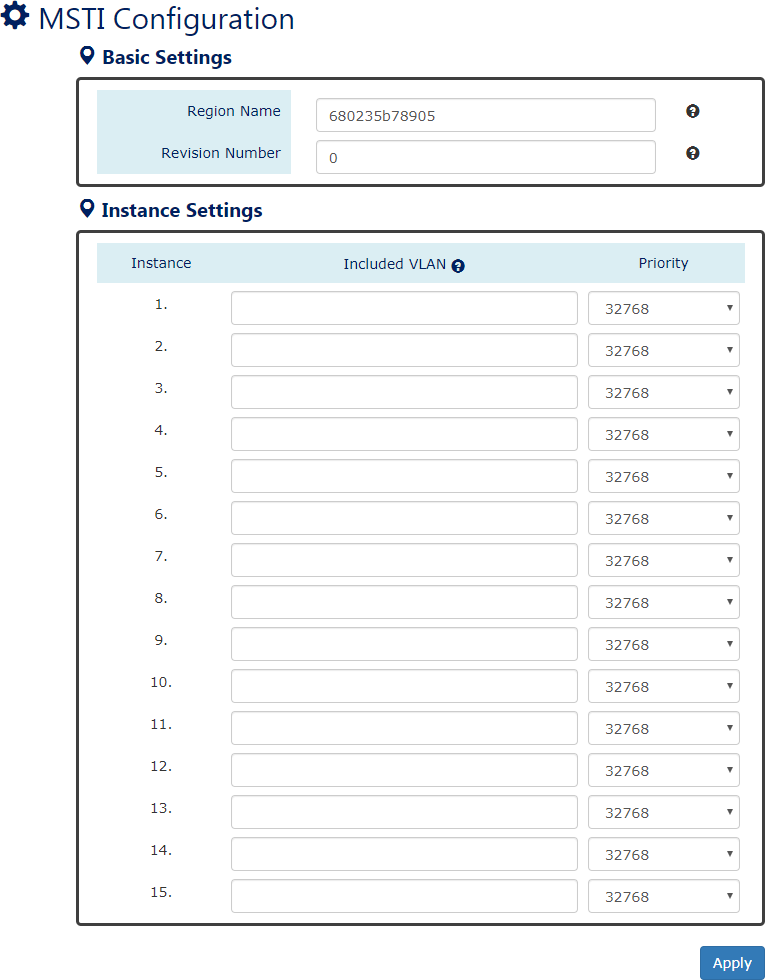
#### Oper. P2P

This field shows the link-type of the STP port. P2P means “**point-to-point**” and Shared means “**point-to-multiple**”.

#### Oper. Edge

This field shows the edge state of this STP port.

**CONFIGURE MSTI INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Basic Settings

* + - Region Name

The Region Name is the name of the MST Region. The switches in the same MST Region must be set to the same Region Name.

The **max. length** for the Region Name is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

* + - Revision Number

The Revision Number is the level of the MST Revision. The switches in the same MST Region must be set to the same Revision Number.

The range of the Revision Number is **from 0 to 65535**.

The default Revision Number is **0**.

#### Instance Settings

* + - Instance

The Instance is from 1 to 15.

* + - Included VLAN

The configured VLANs are involved in the specific Instance.

The format is: 10, 20, 30…. “Comma” is used to separate VLAN IDs.

* + - Priority

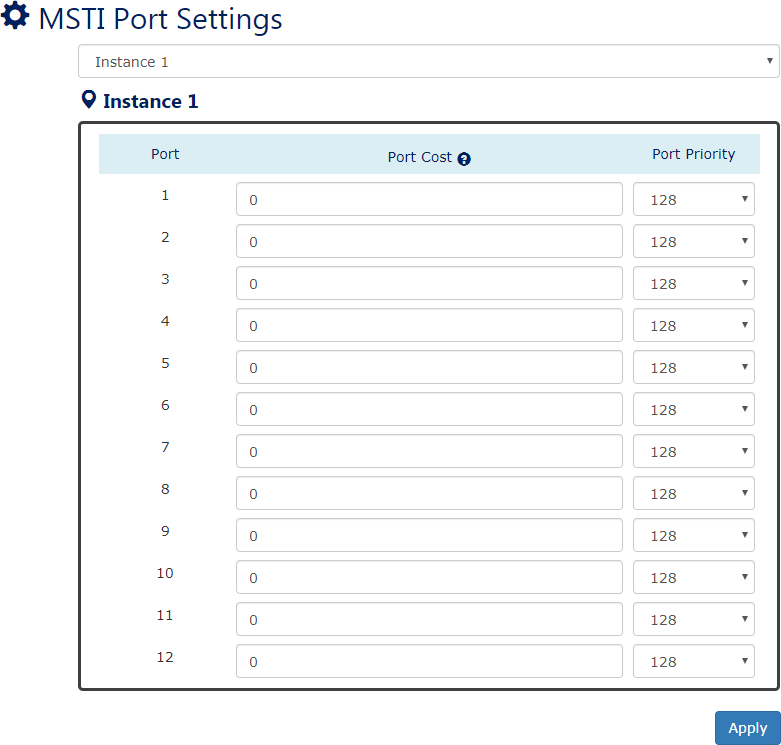
The priority is used to define the “Root Bridge” that is used to communicate with other MSTI Region.

The range of the Root Priority is **from 0 to 61440** (**multiple of 4096)**. The default Root Priority is **32768**.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE MSTI PORT INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Instance Selector

Select the instance to configure the ports. The Instance No. is from 1 to 15.

#### Port

Port1 to PortN, where N is based on the total port number.

#### Path Cost

The Path Cost is the cost from the current node to another device. The range of the Path Cost is **from 0 to 200000000**.

The default Path Cost is **0**. This implies that the Path Cost is decided by the system.

#### Port Priority

This is used to identify the port to be blocked in the Ring topology.

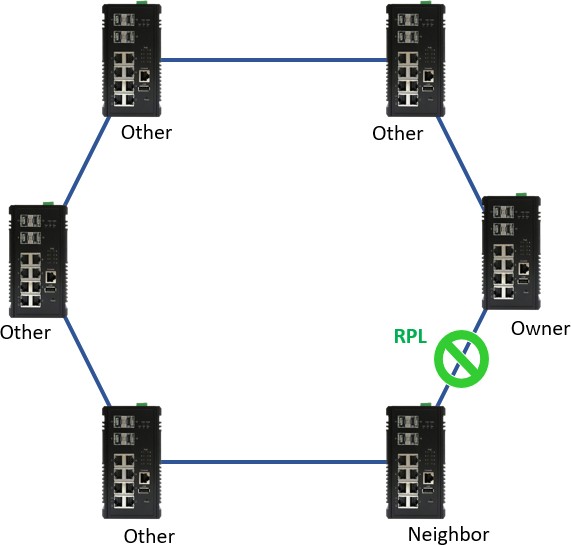
The range of the Root Priority is **from 0 to 240** and is in **multiples of 16**. The default Root Priority is **128**.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# ERPS

**Ethernet Ring Protection Switching** (**ERPS**) applies the protection switching mechanism for Ethernet traffic in a ring topology. This mechanism is defined in **ITU-T G8032**. You can have a protection switching and avoid the possible loops in a network by implementing the ERPS function. This is done by blocking the flow of traffic to the **Ring Protection Link** (**RPL**) there by protecting the entire Ethernet ring.

When an ERPS is implemented in a ring topology, only one switch is allocated as the **owner**. This switch oversees blocking the traffic in the RPL to avoid loops. The switch adjacent to the RPL owner is called the **RPL neighbor** node and it is responsible for blocking the end of the RPL during normal condition. The participating switches that are adjacent to the RPL owner or neighbor in a ring are called the members or RPL next-neighbor nodes. The primary function of these switches is to forward the received traffic.

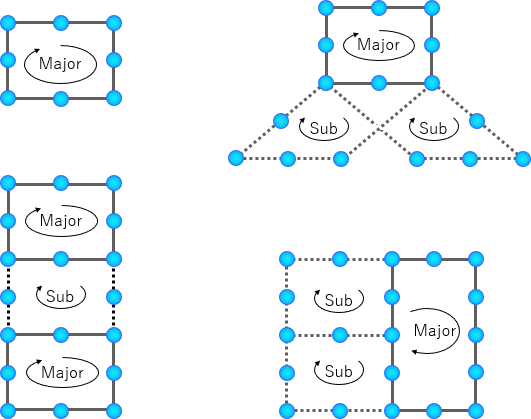
The benefit of the ERPS ring protection switching architecture are:

* Protection switching on Ethernet layer
* Preventing loop by blocking mechanism
* VLAN based protection
* **Sub-50msec** protection switching
* Support administration command
* Hop Count Limitation Reduced (RSTP/ STP)
* **250 switches** and links in singled ring tested

To make sure that a ring is up and loop-free, **Ring Automatic Protection Switching** message is sent regularly as control messages by nodes on the ring. The RPL owner identifies a signal failure (SF) in a ring when the RPL owner misses the poll packets or reads from the fault detection packets. When the fault is identified, the RPL owner unblocks the ring protection link (RPL) and permits the protected VLAN traffic through.

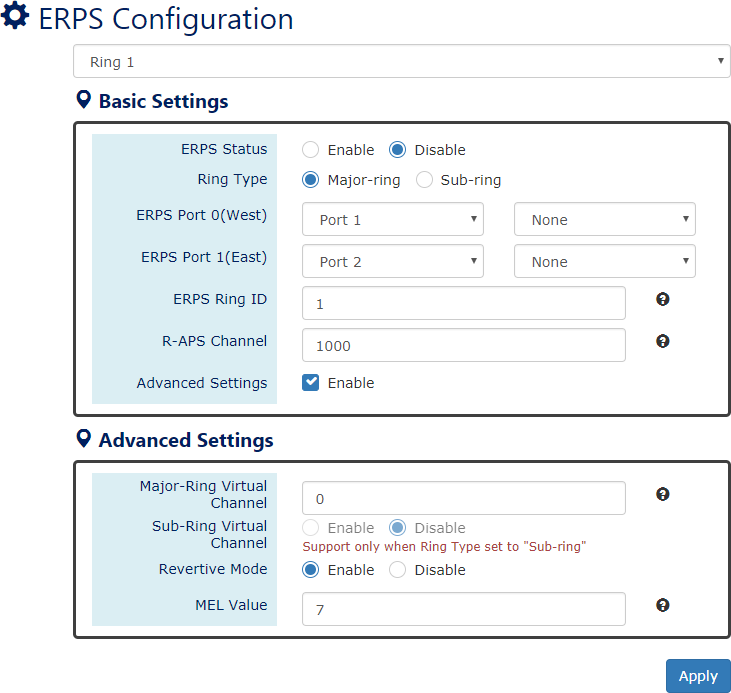
ERPS, is like STP, providing a **loop-free** network by using polling packets to detect faults. If a fault occurs, ERPS restores itself by sending traffic over a protected reverse path rather than making a calculation to identify the forwarding path. The fault detection mechanism in the ERPS enables the ERPS to join in **less than 50 milliseconds** and recovers quickly to forward traffic. In a real test case, the protection switching time is 15ms in 250 devices single ring topology.

In the new ERPS version, G.8032 v2, it supports multiple ring or ladder topology. Rings can conjoin by one or more interconnection nodes. The major ring controls a full physical ring. Sub ring does not constitute a closed ring. It is connected to a major ring at the interconnection nodes.



Using major ring and sub ring can design multiple ring or ladder topology. With these topologies, ERPS can append to variance application with different level of ring network. For example, core ring and branch ring architecture has application in campus and the area with central control node. Ladder topology has lots of case for tunnel and train application. The benefit of small ring is less effect nodes if ring caused of recovery.

**CONFIGURE ERPS INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### ERPS Ring

There are three rings supported on a device. Using the dropdown select to change the ERPS Rings.

#### Basic Settings

* + - ERPS Status

“Enable” or “Disable” ERPS protocol running on the switch. By default, the ERPS protocol is **disabled**.

* + - Ring Type

**Major-ring**: controls a full physical ring.

**Sub-ring**: connected to another ring. It does not constitute a closed ring.

* + - ERPS Port 0

The ERPS Port 0 is also called “**West** Port”. Select one of the switch ports to be the Port 0 of ERPS and decide the role of the port.

* + - ERPS Port 1

The ERPS Port 1 is also called “**East** Port”. Select one of the switch ports to be the Port 1 of ERPS and decide the role of the port.

**Note: Only** One of the switch ports can be configured as ERPS Port 0 or ERPS Port 1.

|  |  |
| --- | --- |
| **Role** | **Description** |
| Owner | There is only one “Owner” in the ERPS ring topology. The Owner is responsible for blocking the traffic in RPL and protects one side of  the RPL. |
| Neighbor | There is only one “Neighbor” in the ERPS ring topology. The Neighbor is the port connected with the Owner port and protects  another side of the RPL. |
| Interconnection | The Interconnection port connects a major-ring and a sub-ring. If one of the ports on the switch is set to “Interconnection” role, the  other port will be set to “Disabled” automatically. |
| None | The “None” implies that the port is other than an Owner or a  Neighbor. |

* + - ERPS Ring ID

The ID is the identifier of the ring. The members in the same ring must be set to the same ERPS Ring ID.

The range of the ERPS Ring ID is **from 1 to 239**.

The default ERPS Ring ID is **1**.

。 R-APS Channel

The R-APS Channel is used to forward ERPS information and is mapped to the VLAN IDs. These VLAN IDs cannot be set as traffic VLAN ID. The members in the same ring must be set to the same R-APS Channel.

The range of the R-APS Channel is **from 1 to 4094**.

The default R-APS Channel is **1000**.

#### Advanced Settings

The Advanced Settings field is only displayed when the “Advanced Settings” checkbox is selected in the Basic Settings.

* + - Major-Ring Virtual Channel

This field is used to configure the specific virtual channel for transmitting the management packets of the sub-ring through the major-ring.

* + - Sub-Ring Virtual Channel

“Enable” or “Disable” using virtual channel in the sub-ring. When the Sub-Ring Virtual Channel is enabled, ERPS protocol will transmit management packets by the configured virtual channel.

* + - Revertive Mode

“Enable” or “Disable” the ERPS Revertive Mode. If the Revertive Mode is enabled, the blocked link will revert to the RPL link after the failed link is recovered.

By default, the ERPS Revertive Mode is **enabled**.

* + - MEL Value

MEL field is for the compliance with other devices which are running ITU-T G.8031 from third-party. The MEL implies the MEG Level. It is a field in the R-APS PDU. A large MEL value involves more devices. For example, level 7 contains levels 0 to 6.

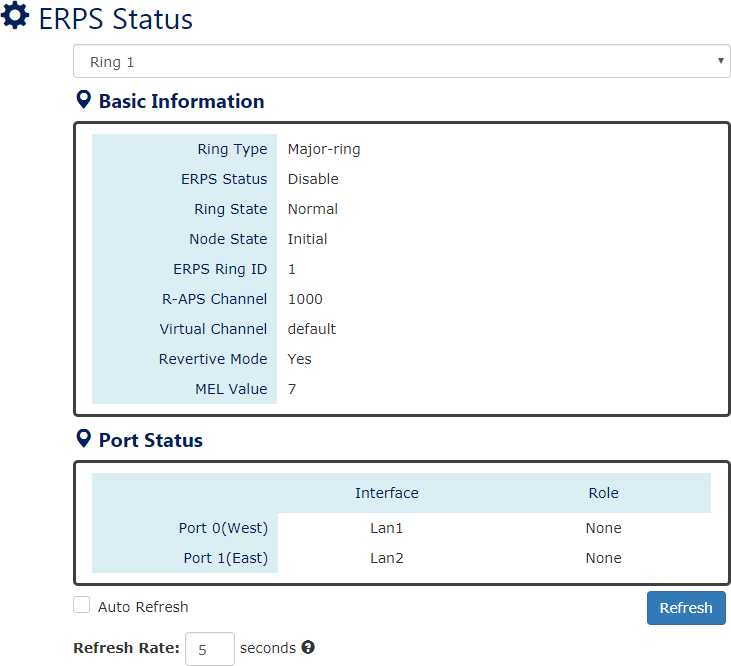
The range of the MEL Value is **from 0 to 7**.

The default MEL Value is **7**.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**ERPS STATUS**



#### ERPS Ring

There are three rings supported on a device. Using the dropdown select to change the ERPS Rings.

#### Basic Information

* + - Ring Type

The type of the selected ERPS Ring shows “**Major-ring**”, “**Sub-ring with virtual channel**”, or “**Sub-ring without virtual channel**”.

* + - ERPS Status

The status of ERPS is “Enable” or “Disable” in the selected ERPS Ring.

* + - Ring State

There are two states for ERPS Rings: **Normal** and **Abnormal**.

* + - Node State

There are three states for ERPS Nodes: **Initial**, **Idle**, **Pending**, and **Protection**.

|  |  |
| --- | --- |
| **State** | **Description** |
| Initial | The ERPS protocol is disabled in the selected ring. |
| Idle | The ERPS protocol is enabled in the selected ring and the ERPS ring  is under control by the RPL Owner. |
| Pending | The ERPS protocol is enabled in the selected ring. The ERPS ring is recovery from Protection state and is waiting for the wtr timer  expired. |
| Protection | The ERPS protocol is enabled in the selected ring but one of the links in the ring is broken. The RPL changes to forward to keep the  ring working. |

* + - ERPS Ring ID

The ID is the identity for the selected ERPS Ring.

* R-APS Channel

This field shows the configured R-APS Channel.

* Virtual Channel

This field shows the virtual channel of sub-ring. If the field shows “default” implies the virtual channel follows the R-APS Channel.

* Revertive Mode

Show the Revertive Mode is enabled (Yes) or disabled (No).

* MEL Value

The field is the configured MEL value.

#### Port Status

* + - Interface

The configured port presents the ERPS port 0/1 in the ERPS protocol.

* + - Role

Display the configured role for the configured port.

# MRP

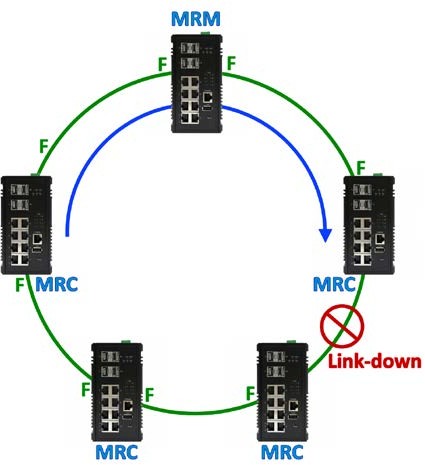
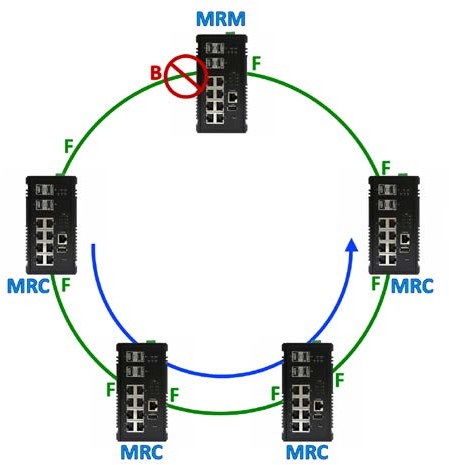
**MRP** function is only supported on the following models:

0804 Series including MT-0804G, MP-0804G, MS-0804G, MT-0804X, MP-0804X, MS-0804X

0802 Series including MT-0802G, MP-0802G, MS-0802G, MT-0802X, MP-0802X, MS-0802X

**Media Redundancy Protocol (MRP)** is an IEC standard protocol to prevent the ring topology from loop, and it is defined as **IEC 62439-2**. The recovery time of MRP is much faster than STP and even than RSTP, so it is suitable in most Industrial Ethernet applications.

In the ring topology with MRP, the manager is called **Media Redundancy Manager (MRM)**, and the clients are called **Media Redundancy Clients (MRC)**. The **MRM** send test packets from both of its ring ports periodically to confirm the health of ring topology.

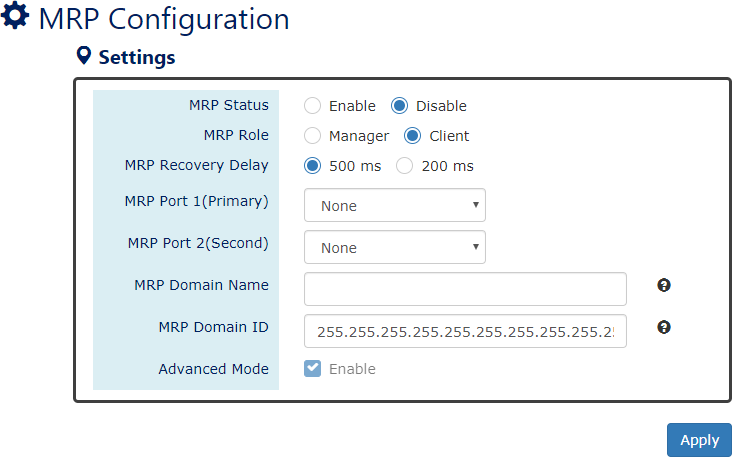
There are three states for MRP Ring Ports – **Disabled**, **Blocked**, and **Forwarding**. When the **MRP** ring is under normal operation, the network works in the **Ring-Closed** state. In the closed state, one of the **MRM** Ring Ports is blocked and the other one is forwarding, while both ring ports of the **MRC**s are forwarding. Due to the blocked port, the topology is a logical stub and the loops are avoided. If one of the forwarding links is failed, the ring topology goes to open state, and the blocked port of **MRM** will be forwarding state to insure the transmission in the ring.

|  |  |
| --- | --- |
| ***Ring Topology Closed*** | ***Ring Topology Open*** |

If the **MRC** detects a link down at one of the ring ports, it can notify this event to the **MRM** initiatively. In **Advanced Mode**, the MRM can activate the blocked ring port to speed-up recovery rather than wait till sufficient loss of test packets.

**MRP** standard guarantees the recovery time in the specifications. The recovery time are 500ms, 200ms, 30ms with maximum 50 switches, and 10ms with up to 14 switches in a ring. Currently, we support the recovery delay of 500ms and 200ms.

**CONFIGURE MRP INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### MRP Status

“Enable” or “Disable” MRP protocol running on the switch. By default, the MRP protocol is

**disabled**.

* + **MRP Role**

Configure the role of the switch when running MRP protocol. The “Manager” item implies MRM and the “Client” item implies MRC.

#### MRP Recovery Delay

The MRP Recovery Delay implies to the number of lost packets. The IEC 62439-2 standard defines 4 recovery delays – **500ms**, **200ms**, **30ms**, and **10ms**. Currently, we only support 500ms and 200ms.

#### MRP Port 1 (Primary)

The MRP Port 1 is the **primary port** of MRP. Select one of the switch ports to be the primary port of MRP. The Primary port is default configured to be **forwarding** when the Ring is closed.

#### MRP Port 2 (Second)

The MRP Port 2 is the **secondary port** of MRP. Select one of the switch ports to be the secondary port of MRP. The secondary port is default configured to be **blocking** when the Ring is closed.

#### MRP Domain Name

The MRP Domain Name is a unique string for the MRP domain to identify MRP domains

#### MRP Domain ID

The MRP Domain ID is the key attribute to define the members in the same MRP ring. The default MRP Domain ID is **255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255**.

#### Advanced Mode

The Advanced Mode is supported only when the MRP Role is configured to “**Manager**”. If the Advanced Mode is checked, it implies the Advanced Mode is enabled. Under the advanced mode, when the MRM received a link-down signal, the MRM actives the backup port immediately rather than waiting for the sufficient loss of test packets.

**MRP STATUS – BASIC & CONFIGURE INFORMATION**



#### Basic Information

* + - Instance ID

The Instance ID is the Ring ID. We only support one ring currently, so the Instance ID displays always **1**.

* + - Domain ID

The Domain ID is the identity of current MRP ring. Only the members with the same Domain ID will be regarded as working in the same ring.

#### Configured Information

* + - Advanced Mode

The field shows the status of Advanced Mode. Advanced Mode is only supported when the switch is configured as an **MRM (Manager)**.

* + - Role of Switch

There are 2 roles of switches in the MRP – **Manager** and **Client** Administrative Setting: the role that users configured for the switch. Real Operating State: the role that the switch is working as.

* + - Domain Name

This field shows the configured name of this MRP Domain.

* + - Recovery Delay

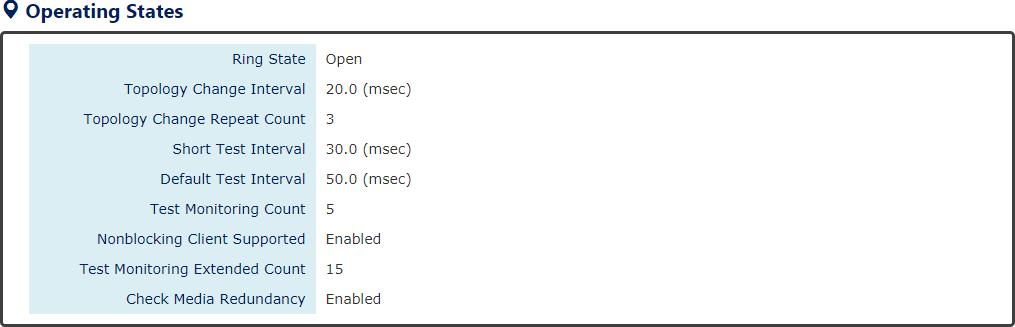
This field shows current operating Recovery Delay. It may be **500** or **200 (msec)**.

* + - Port Number, Secondary
    - Port Number, Primary

These two fields shows two parts of information. The first one is the switch port number configured as Primary / Secondary Port, and the other one is the state of this port. There are 3 states for MRP ports when the MRP is enabled: **Forwarding**, **Blocked**, and **Disabled**. If the MRP is disabled, the state shows “**N/A**”.

* + - Operation

This field shows current Operation State – **Enabled** or **Disabled**.



#### Operating States (Master)

* + - Ring State

The Ring State displays the actual ring sate of MRP, and the state may be

**Open**: some of the links in the MRP ring are down or MRC failure.

**Closed**: the MRP ring is closed and under normal operation without error.

* Topology Change Interval

The interval is the period to send **MRP\_TopologyChange** frames.

* Topology Change Repeat Count

The count is the repeat times to transmit **MRP\_TopologyChange** frames.

* Short Test Interval

This interval is a timer used after **link changes** to send **MRP\_Test** frames on the MRP ring ports.

* Default Test Interval

The interval is the **default** period to send **MRP\_Test** frames on the MRP ring ports.

* Test Monitoring Count

This field is the interval count for monitoring the reception of **MRP\_Test** frames.

* Non-blocking Client Supported

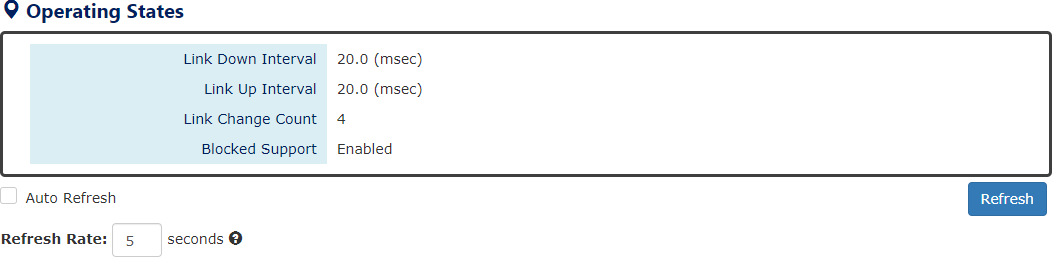
This field displays the ability of the MRM to support MRCs without **BLOCKED** port state support in the ring.

* Test Monitoring Extended Count

This field is an **optional** parameter. It is an extended interval count for monitoring the reception of **MRP\_Test** frames.

* Check Media Redundancy

Check the current state of MRM. The state may be “**Enabled**” or “**Disabled**”.



#### Operating States (Client)

* + - Link Down Interval

The Link-down Interval shows the period that MRP Link-down frames sent on the ring port. The default value of Link-down Interval is **20ms**.

* + - Link Up Interval

The Link-up Interval shows the period that MRP Link-up frames sent on the ring port. The default value of Link-up Interval is **20ms**.

* + - Link Change Count

The Link-change Count controls the repeated times to transmit MRP Link-Change frames. The default Link-change Count is **4** times.

* + - Blocked Support

The Blocked Support is default **enabled**. The MRM with Blocked Support will block the secondary port when there is no Blocked Port in the MRM ring topology to avoid loops.

# SNMP

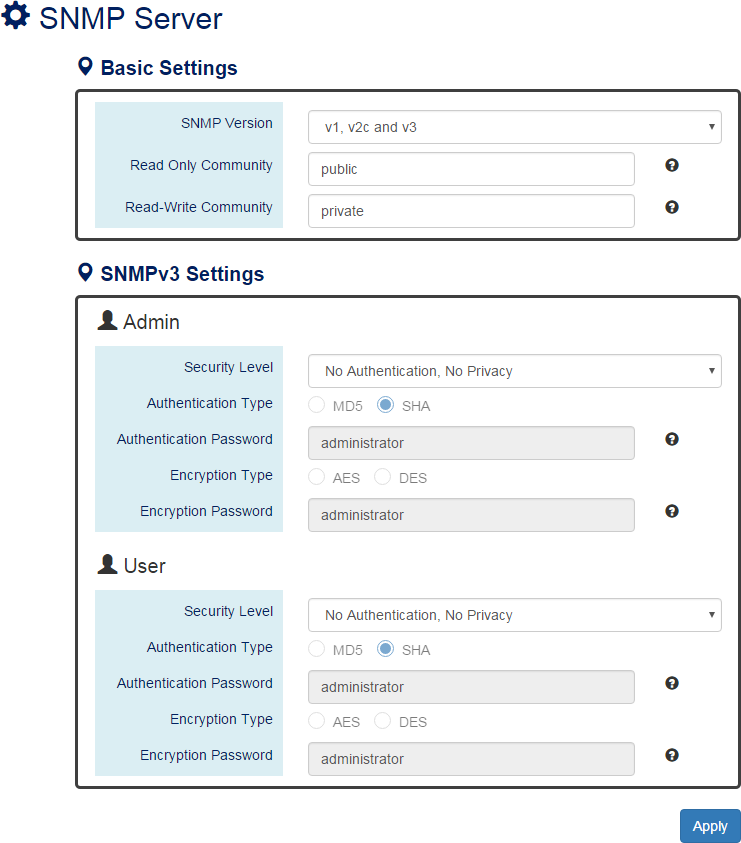
**Simple Network Management Protocol (SNMP)** is a standard for collecting and structuring information on the managed devices of the IP network. It can also modify some of the information to change the behavior of the devices. SNMP is usually used in monitoring the network. The users can remotely query the information provided by the devices running SNMP.

The switches support SNMP v1, v2c, and v3. SNMP v1 and v2c authenticates with a community string for “**read-only**” or “**read-write**” permission. The SNMP v3 authentication requires to select an authentication level (**MD5** or **SHA**) and supports data encryption to make the data safer.

For the SNMP version and authentication method relationship, refer to the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Web Setting** | **Authentication** | **Encryption** | **Method** |
| v1 &  v2c | Read Only Community | Community String | No | String match for authentication |
| Read-Write Community | Community String | No | String match for authentication |
| v3 | Security Level –  No Authentication, No Privacy | No | No | Access by an account (admin or user) |
| Security Level – Authentication, No Privacy | MD5 / SHA | No | Access by an account (admin or user) and password with more than 8 characters, which is based  on MD5 or SHA |
| Security Level – Authentication, Privacy | MD5 / SHA | Yes  AES / DES | Access by an account (admin or user) and password more than 8 characters, which is based on MD5 or SHA. The data encryption is based on AES or DES and the  key requires 8 to 32 characters. |

**CONFIGURE SNMP SERVER INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Basic Settings

* + - SNMP Version

The system enables the SNMP “**v1, v2c and v3**” authentication by default. The users can enable the SNMP server on only “**v1 and v2c**” or “**v3**”. “**None**” refers to disabling the SNMP server.

* + - Read Only Community

The community used to access the SNMP server with the “**read-only**” privilege. The **max. length** for the Read Only Community is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

* + - Read-Write Community

The community used to access the SNMP server with the “**read-write**” privilege. The **max. length** for the Read-Write Community is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

#### SNMPv3 Settings

This section is displayed only when the **SNMP Version** is set to “v3” or “v1, v2c and v3”. Two accounts are provided – Admin and User to access the SNMP agent. The users can set different levels for the 2 accounts.

* + - Security Level

***No Authentication, No Privacy***: Access by an account “admin” or “user”. ***Authentication, No Privacy***: Access by an account “admin” or “user” with password. ***Authentication, Privacy***: Access by an account “admin” or “user” with password and the data will be encrypted.

* + - Authentication Type

Two algorithms are provided - **MD5** and **SHA** for authentication password.

* + - Authentication Password

A string/key is used to authenticate the SNMP Server and obtain the access permission. It will be hashed by MD5 or SHA before authentication.

**The min. length** for the Read-Write Community is **8 characters. The max. length** for the Read-Write Community is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

* + - Encryption Type

Two algorithms are provided - **AES** and **DES** for data encryption.

* + - Encryption Password

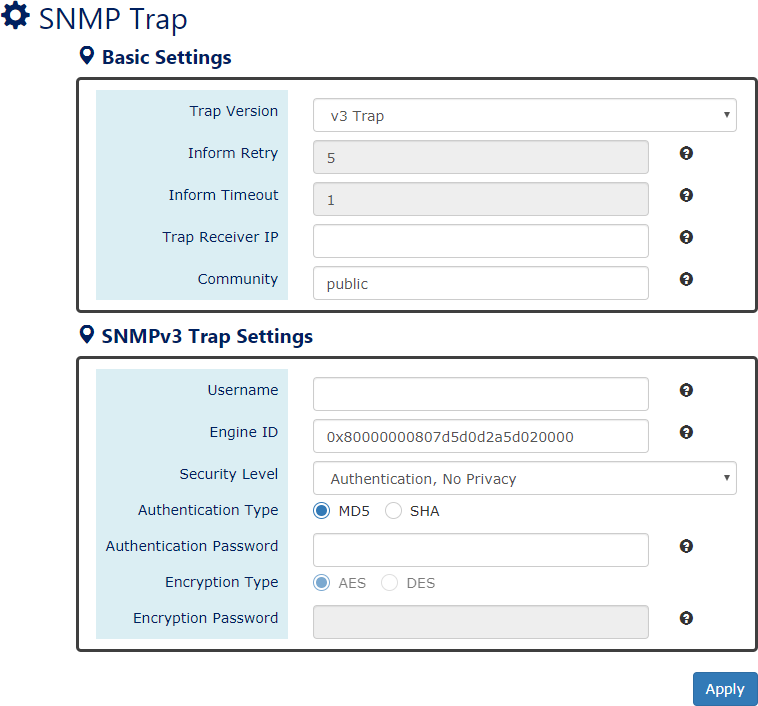
A string/key is used to encrypt the data that is sent to the SNMP server.

**The min. length** for the Read-Write Community is **8 characters. The max. length** for the Read-Write Community is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE SNMP TRAP INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Basic Settings

* + - Trap Mode

The system enables the SNMP “**v1, v2c and v3**” authentication by default. Users can enable the SNMP server only on “**v1 and v2c**” or “**v3**”. “**None**” indicates disabling the SNMP server.

* + - Inform Retry

The SNMP trap will send “Retry” times when the trap set to “v2 Inform” or “v3 Inform” mode.

The range of the Inform Retry is **from 1 to 100**. The default Inform Retry is **5**.

* + - Inform Timeout

The interval is used to send trap when the trap set to “v2 Inform” or “v3 Inform” mode.

The range of the Inform Retry is **from 1 to 300** second(s). The default Inform Retry is **1** second.

* + - Trap Receiver IP

The IP address is the IP address of the trap server to receive the trap information. The system supports both **IPv4** and **IPv6** addresses for the receiver.

* + - Community

The string in the SNMP trap is the identity of the device.

**The max. length** for the Community is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

#### SNMPv3 Trap/Inform Settings

This section is displayed only when **Trap Mode** are set to “v3 Trap” or “v3 Inform”.

* + - Username

Specify the username for authentication with the SNMP trap server.

* + - Engine ID

The Engine ID is the identifier for the given SNMP application.

* + - Security Level

***No Authentication, No Privacy***: Access using the username assigned to the users. ***Authentication, No Privacy***: Access using the username assigned to the users with password.

***Authentication, Privacy***: Access using the username assigned to the users with password and the data will be encrypted.

* + - Authentication Type

Two algorithms are provided - **MD5** and **SHA** for authentication password.

* + - Authentication Password

A string/key is used to authenticate the SNMP trap server and obtain the permission. It will be hashed by MD5 or SHA before authentication.

**The min. length** for the Read-Write Community is **8 characters. The max. length** for the Read-Write Community is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

* + - Encryption Type

Two algorithms are provided - **AES** and **DES** for data encryption.

* + - Encryption Password

A string/key is used to encrypt the data sent to the SNMP trap server.

**The min. length** for the Read-Write Community is **8 characters. The max. length** for the Read-Write Community is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# DHCP

**DHCP SERVER/CLIENT**

DHCP, **Dynamic Host Configuration Protocol**, is a standardized protocol used in the IP networks. The DHCP Server holds an **IP address pool** and when a DHCP Client request for an IP address, the DHCP Server picks an IP address from the pool and assigns it to the client. DHCP Server also manages other IP information such as **Default Gateway** and **DNS Server**. DHCP is especially useful to configure the IP information for several devices. Only the administrator can enable the DHCP Client for each device and setup the DHCP Server. The clients will then obtain a unique IP address and other IP settings to connect to the network.

**DHCP SERVER BINDING**

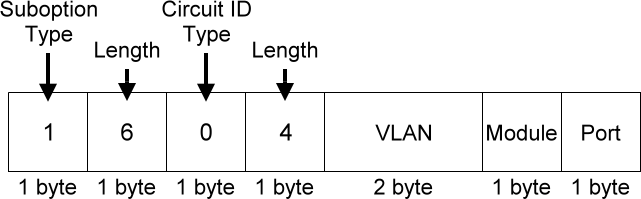
Apart from dynamically allocating an IP address to a DHCP Client, the DHCP Server also provides a function to manually assign a **static IP address** to the device with a specific MAC Address. This is called as DHCP Server Binding.

**DHCP RELAY/OPTION82**

In a large network, there might be several subnets existed and the DHCP Client is not able to serve by DHCP Servers directly. In this case, we need a relay agent to help to transmit the request frames to the DHCP Servers. When a relay agent receives the broadcast request frame from a DHCP Client, the relay agent will transmit the frame to the DHCP Servers, which are in the same subnet by unicast.

Option 82 is an information option to identify the clients by **Circuit ID** and **Remote ID**. The **Circuit ID** is an identity containing the **interface** name and/or **VLAN** information, and the **Remote ID** is to identify the **remote host** (the relay agent). The DHCP Server can distribute an IP address to the DHCP Client according to Option 82 information and make the IP addresses more controllable.

The frame format for the **Circuit ID** is as below:



#### VLAN

The VLAN field is for the **management VLAN ID**, which is natively set to **1**.

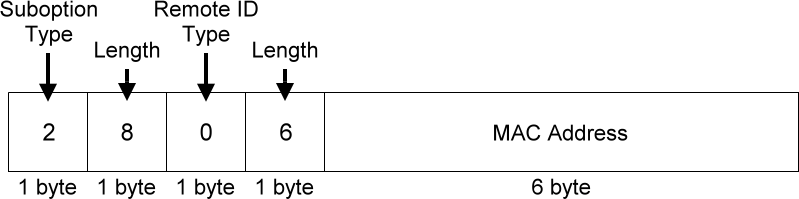
#### Module

The stack number for the device sending the DHCP request is on. For industrial switches, this byte is always filled as **0**.

#### Port

The port number identifies the incoming DHCP request frame/DHCP Client.

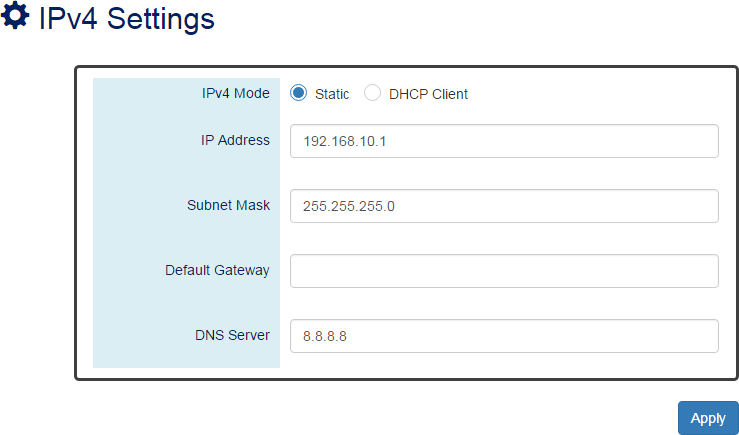
The frame format for the **Remote ID** is as below:



#### MAC Address

By default, the MAC address is set to the MAC address of DHCP relay agent.

**CONFIGURE DHCP CLIENT**



#### IPv4 Mode

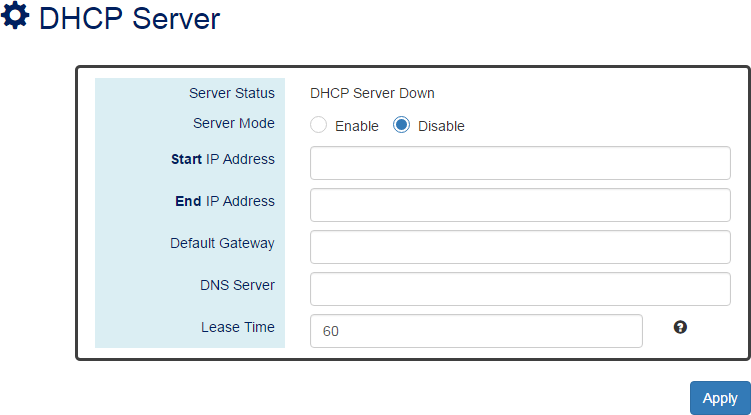
Set the **IPv4 Mode** to “**DHCP Client**” to enable the DHCP Client. The system sends a

**discovery frame** to the network and tires to obtain an IP address from the DHCP Server. After enabling the DHCP Client, users need to connect to the **Console Port** to get the IP address by using “***show ip address***” on the CLI.

* + (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE DHCP SERVER INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Server Status

Shows the status of the DHCP server: **Down** or **Up.**

#### Server Mode

“Enable” or “Disable” the DHCP Server function.

#### Start IP Address

Set the range of the IP pool. The “Start IP Address” is the starting.

“Start IP Address” must be in the **same subnet** as that of the switch itself.

#### End IP Address

Set the range of IP pool. The “End IP Address” is the end.

“End IP Address” must be in the **same subnet** as that of the switch itself.

#### Default Gateway

Set the Default Gateway for the DHCP Clients to make them connect to the WAN. “Default Gateway” must be in the **same subnet** as that of the switch itself.

#### DNS Server

Set the DNS Server for the DHCP Clients to make them connect to another device based on the **URL** instead of IP address.

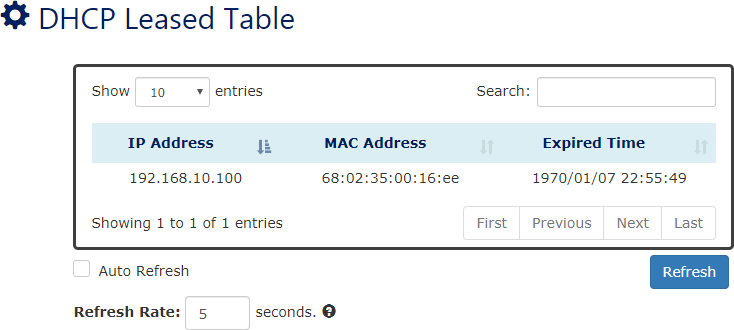
#### Lease Time

DHCP Server leases an IP address to a device for **a specified period**. When the lease time expires, the DHCP server may assign a different IP address in the pool to the device.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**DHCP LEASED TABLE**



#### IP Address

This field implies the IP Address that this device acquired from DHCP Server.

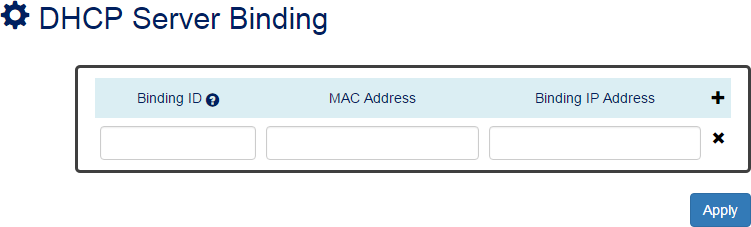
#### MAC Address

The MAC Address of the device that acquired mapped IP Address. Administrators can use MAC Address to map to the device’s IP Address.

#### Expired Time

The Expired Time implies the deadline of designated IP Address that leased from DHCP Server. After Expired Time, the DHCP Client must communicate with DHCP Server and ask for the IP Address again.

**CONFIGURE DHCP SERVER BINDING INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Binding ID

An ID used to identify the binding.

The range of the Binding ID is **from 1 to 32**.

#### MAC Address

The device with the specified MAC Address will be assigned to the static Binding IP Address.

#### Binding IP Address

A static IP Address will be assigned to the specified MAC Address.

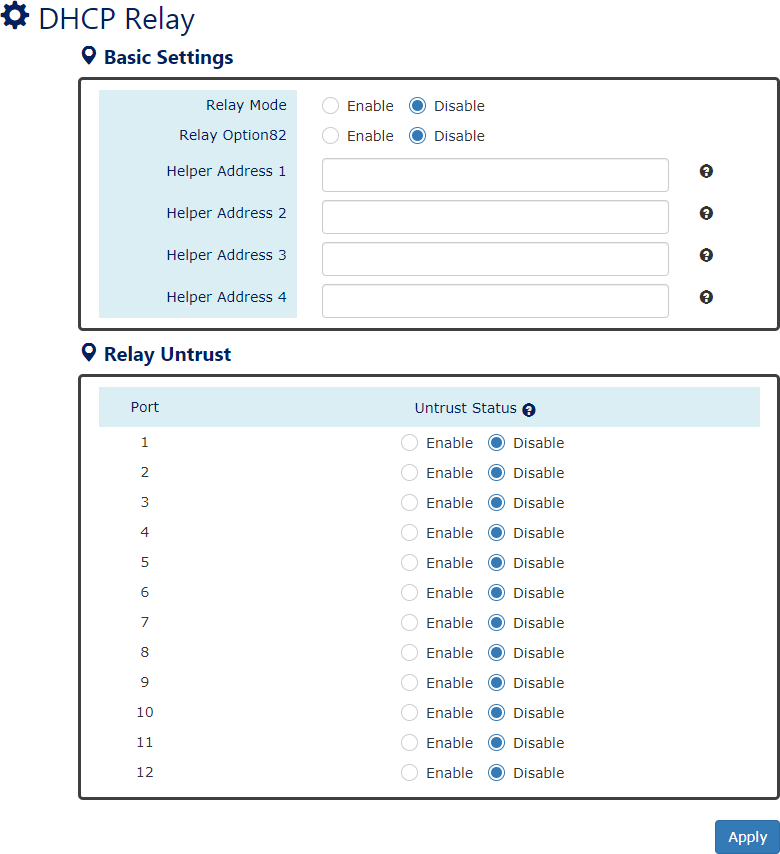
 : Click the **plus icon** to add a DHCP Binding row.

 : Click the **remove icon** to delete the DHCP Binding row.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE DHCP RELAY INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Relay Basic Settings

* + - Relay Mode

“Enable” or “Disable” the DHCP Relay function.

* + - Relay Option82

“Enable” or “Disable” the DHCP Relay with Option82 tag.

* + - Helper Address 1 - 4

The **IP Addresses** of the **DHCP Servers** provide IP addresses to the DHCP Clients. A backup of Four Helper Addresses are available during breakdown.

#### Relay Untrust

* + - Port

Port1 to Port N, where N is based on the total port number.

* + - Untrust Status

“Enable” or “Disable” to untrust the specific port. If the untrusted status is enabled on a port, the system will **drop** the DHCP management frames on the port.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

PoE (PoE Model Only)

The **PoE**, or **Power over Ethernet**, allows switches to provide electric power along with data on the twisted pair Ethernet cables. The Power over Ethernet defined in **IEEE 802.3af** provides up to

15.4 W and **IEEE 802.3at** provides up to 25.5 W. It requires category 5 cables or better to support high power levels. **PoE** is helpful when the AC power is not available or is available with high cost. It is usually used in surveillance IP cameras, I/O sensors, wireless access points, and IP telephones.

**POWER DE-RATING PROTECTION**

Due to the power supply design inside the devices for some models, the power budget will decrease according to the operating temperature. To ensure the functionality of PoE, we do the protection by software in the background. We adjust the budget as the temperature rises. Please refer to the **Hardware User Manual** for the detail in the relationship of power budget and temperature.

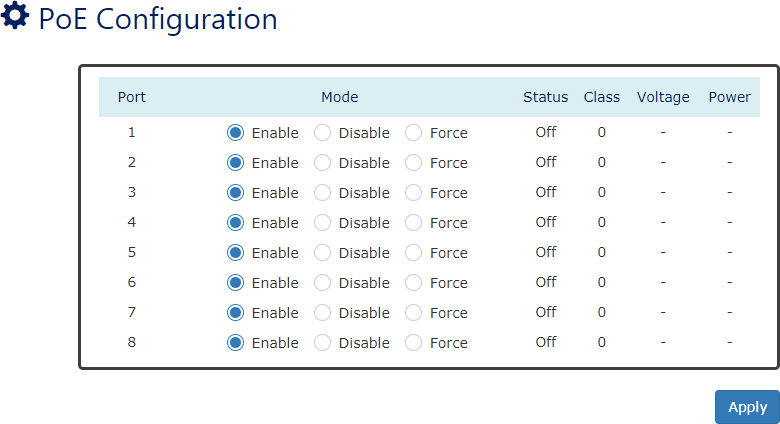
**POE DEBUG CODE**

We provide **PoE Debug Command** on the “[**CLI**](#_bookmark40)**”** for troubleshooting. When users find that the PoE functions work abnormal, users can use the command to acquire the error code. The error codes are mapping to different situations, users can understand the error codes from the following table:

|  |  |
| --- | --- |
| **Code** | **Description** |
| 0x00 | PoE port is on. |
| 0x01 |
| 0x02 |
| 0x03 |
| 0x04 |
| 0x06 | PoE port is off. Mains voltage is higher than maximum voltage limitation. |
| 0x07 | PoE port is off. Mains voltage is lower than minimum voltage limitation. |
| 0x11 | PoE port is not defined yet, please check the PoE power input. |
| 0x20 | PoE port is off because of power budget exceeded. |
| 0x1F | PoE port is off because of over-load state according to 802.3AF/AT. |
| 0x43 | PoE port is off because of class error. |
| 0x81 | 802.3BT - compliant PD was detected using BT Port (30w) |
| 0x85 | 802.3BT - SSPD was detected using BT Port (60w/95w) and operates as BT Port  (30w) if requested class =< 4. |
| 0x86 | 802.3BT - SSPD was detected using BT Port (60w|95w) and operates as BT Port  (60w/95w) if requested class > 4. |
| 0x90 | BT Port (30w) and delivers power due to force power command. |

|  |  |
| --- | --- |
| 0x91 | BT Port (60w/95w) and delivers power due to force power command. |
| 0x1B | PoE port is off because detection is in process. |
| 0xA8 | PoE port is not connected. |
| Others | Please contact your system administrator!! |

### CONFIGURE POWER OVER ETHERNET (POE)



#### Port

Port1 to PortN, where N is based on the total PoE port number.

#### Mode

“**Enable**”, “**Disable**”, or “**Force**” PoE function on the specific port. If the mode is configured to “Force”, the system will provide power forcedly on the specific port even there is no device connected to this port.

#### Status

The field shows the PoE status of the specific port.

On: PoE is enabled or configured to force on the port and power is delivered on the port. Off: PoE is enabled on the port but no Powered Device (PD) is connected.

Disabled: PoE is disabled on the port.

#### Class

The field shows the class followed by the PD. The acceptable power of the class is defined in the IEEE 802.3af/at.

#### Voltage

This field shows the output voltage that PSE provided. The power output of the boost switch will be boosted to 53V.

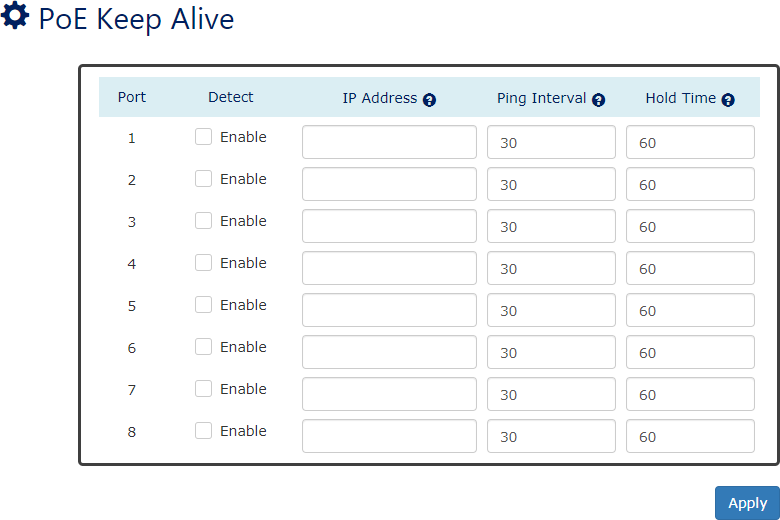
#### Power

The Consumption field contains provided power in watts. The PSE can provide up to 30Watts and the PDs can receive up to 25.5Watts.

* (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE POE KEEP ALIVE**



#### Port

***For more information, hover the mouse over the icon in the system.***

Port1 to PortN, where N is based on the total PoE port number.

#### Detect

“Enable” or “Disable” to detect the Powered Device (PD) on the specific port. When the detection is enabled, the system pings the configured IP Address on every Ping Interval.

#### IP Address

The field is the IP Address of the Powered Device (PD).

#### Ping Interval

The Ping Interval is the duration to ping the Powered Device (PD). The range of the Ping Interval is **from 1 to 65535** seconds.

The default Ping Interval is **30** seconds.

#### Hold Time

The Hold Time is used when the ping fails. The system will wait for the Hold Time to expire and then try to ping the PD again.

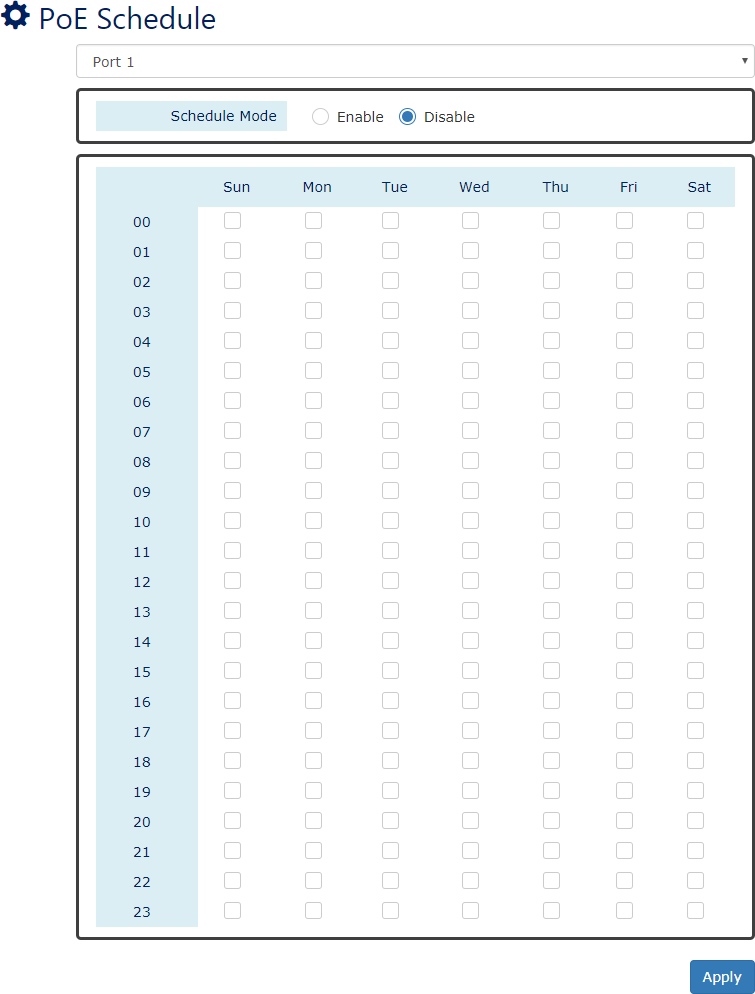
The range of the Hold Time is **from 1 to 65535** seconds.

The default Hold Time is **60** seconds.

* (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE POE SCHEDULE**



#### Port Selector

Select the port number to configure the PoE Schedule.

Port1 to PortN, where N is based on the total PoE port number.

#### Schedule Mode

“Enable” or “Disable” to provide power by the schedule on the specific port.

* **Enable** (for each day)

The week is from Sunday to Saturday.

* **Week** (The x-ray of the table)

The week is from Sunday to Saturday.

* **Hour** (The y-ray of the table)

The hour is from 00 (00:00) to 23 (23:00).

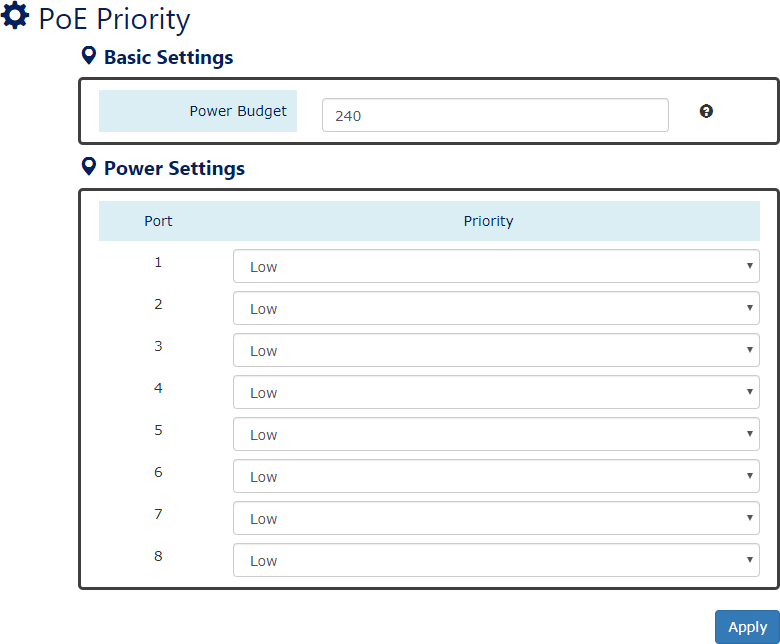
Users can select the checkbox with the Week and Hour in the table to enable the PoE Schedule on the specific time. For example, if the user wants the PoE to be enabled only on Monday from 6:00 to 7:00 and on Wednesday from 13:00 to 15:00, the following checkboxes must be selected – “Mon-06”, “Mon-07”, “Wed-13”, “Wed-14”, and “Wed-15”.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE POE PRIORITY**

From **v1.1.48**, we removed “**Priority Mode**” and “**Power Limit**” for each port configuration in the PoE Priority Page because of the support of the PoE chipsets.

From **v1.1.77**, all PoE Models (including MP/MT/MH/MQ/CP/CT/CH/CQ) support PoE Priority function including 60W/95W 802.3bt switches.

***For more information, hover the mouse over the icon in the system.***

#### Basic Setting

* + Power Budget

This field defines the **maximum power** that can provide to all the connected PDs. The range of Power Budget is **from 1 to 240** Watt.

The default Power Budget is **240** Watt.

#### Power Settings

* + Port

Port1 to PortN, where N is based on the total PoE port number.

* + Priority

Assign the PoE priority to **high**, **middle**, or **low** for the specific port.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# Industrial Protocols

**Industrial Protocols** are supported on all models **except the** KY**-**0802GA series.

There are two industrial protocols provided in the switch – **EtherNet/IP** and **Modbus/TCP**.

**EtherNet/IP** is an **industrial network protocol** that linked up the Common Industrial Protocol (CIP) with standard Ethernet. EtherNet/IP takes advantage of both Internet **Protocol suite** and **IEEE 802 standard**, which are the most widely deployed collections of Ethernet standards, to define the features and functions for its transportation, networking, data link and physical layers. CIP makes use of **object-oriented design** to provide EtherNet/IP with the services and device profiles needed for real-time control applications. The object-oriented design of the CIP is also used to promote consistent implementation of automation functions into a diverse ecosystem of products. EtherNet/IP defines how to organize the data in a TCP/UDP packet and transfers the packet in the application layer.

**Modbus** is a popular communication protocol used for the **industrial serial devices**. It is usually working as “**master-slave**” architecture and working with **programmable logic controllers** which are also called **PLC**s. The Modbus/TCP implies to provide Modbus Messaging service on the TCP/IP, so that the devices which are running Modbus can communicate with each other with Modbus messages. The Modbus messages are encapsulated with an Ethernet TCP/IP wrapper based on the standard. During the transmission, the switches can only acquire the encapsulated information when the Modbus/TCP is enabled. If users would like to understand the real content of Modbus message, users must install other utilities such as “ModScan”. Our switches implements the Modbus/TCP registers including system information, firmware information, port information, and packet information. The details refer to [the “Modbus Data Mapping Information](#_bookmark13)” section.

### MODBUS DATA FORMAT AND FUNCTION CODE

The primary four types of Modbus/TCP data format are as following:

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Access Type** | | **Function Code** | **Function Name** |
| Bit Access | Physical Discrete Inputs | 2 | Read Discrete Inputs |
| Internal Bits or Physical Coils | 1 | Read Coils |
| Word Access  (16-bit Access) | Physical Input Registers | 4 | Read Input Registers |
| Physical Output Registers | 3 | Read Holding Registers |

### MODBUS DATA MAPPING INFORMATION

In the following tables, we assume the total port number is **28**.

The following table is for **Function Code 3** (**Holding Registers**) / **Function Code 6**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Address Offset** | **Data Type** | **Interpretation** | **Description** | |
| **System Information** | | | | |
| 0x0000 to 0x0008 | 1 word | HEX | **Port 1 to Port 8 Status Configuration** | |
| 0x0000: | Disable |
| 0x0001: | Enable |

The following table is for **Function Code 4** (**Input Registers**). The data map addresses in the following table starts from **Modbus address 30001**. For example, the address offset 0x0000H equals Modbus address 30001, and the address offset 0x0030H equals Modbus address 30049. All the information read from our switches is in the **HEX mode** and users can refer to the ASCII table for the translation (e.g. 0x4B=’K’, 0x74=’t’).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Address Offset** | **Data Type** | **Interpretation** | **Description** | | |
| **System Information** | | | | | |
| 0x0030 | 20 words | ASCII | **Product Name = “MT-0804G”** | | |
| Word 0 Hi byte = | | ‘M’ |
| Word 0 Lo byte = | | ‘T’ |
| Word 1 Hi byte = | | ‘-‘ |
| Word 1 Lo byte = | | ‘0’ |
| Word 2 Hi byte = | | ‘8’ |
| Word 2 Lo byte = | | ‘0’ |
| Word 3 Hi byte = | | ‘4’ |
| Word 3 Lo byte = | | ‘G’ |
| 0x0050 | 1 word |  | Product Serial Number | | |
| 0x0051 | 2 words | HEX | **Firmware Version**  For example: | |  |
| Word 0 = | 0x0103 | |
| Word 1 = | 0x0200 | |
| Firmware version is 1.3.2 | | |
| 0x0053 | 2 words | HEX | **Firmware Release Date**  For example: | | |
| Word 0 = | 0x1719 | |
| Word 1 = | 0x1506 | |
| Firmware was released on 2015-06-17 at  19 o’clock | | |
| 0x0056 | 3 words | HEX | **Ethernet MAC Address** | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | Ex: MAC = 01:02:03:0A:0B:0C | | |
| Word 0 Hi byte = | | 0x01 |
| Word 0 Lo byte = | | 0x02 |
| Word 1 Hi byte = | | 0x03 |
| Word 1 Lo byte = | | 0x0A |
| Word 2 Hi byte = | | 0x0B |
| Word 2 Lo byte = | | 0x0C |
| 0x0059 | 1 word | HEX | **Power 1** |  |  |
| 0x0000: | Off |  |
| 0x0001: | On |  |
| 0x005A | 1 word | HEX | **Power 2** |  |  |
| 0x0000: | Off |  |
| 0x0001: | On |  |
| 0x005B | 1 word | HEX | **Fault LED Status** | |  |
| 0x0000: | Boot error | |
| 0x0001: | Normal |  |
| 0x0002: | Fault |  |
| 0x0082 | 1 word | HEX | **DO1** |  |  |
| 0x0000: | Off |  |
| 0x0001: | On |  |
| **Port Information** | | | | | |
| 0x1000 to 0x1008 | 1 word | HEX | **Port 1 to Port 8 Status** | | |
| 0x0000: | Link down | |
| 0x0001: | Link up |  |
| 0x0002: | Disable |  |
| 0xFFFF: | No port |  |
| 0x1100 to 0x1108 | 1 word | HEX | **Port 1 to Port 8 Speed** | | |
| 0x0000: | 10M-Half | |
| 0x0001: | 10M-Full |  |
| 0x0002: | 100M-Half | |
| 0x0003: | 100M-Full | |
| 0xFFFF: | No port |  |
| 0x1200 to 0x1208 | 1 word | HEX | **Port 1 to Port 8 Flow Ctrl** | | |
| 0x0000: | Off |  |
| 0x0001: | On |  |
| 0xFFFF: | No port |  |
| 0x1300 to 0x1313 (Port 1) | 20 words | ASCII | **Port 1 to Port 8 Description**  Port Description = “100Tx,RJ45.” | | |
| Word 0 Hi byte = | | ‘1’ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0x1314 to 0x1327 (Port 2)  …  0x138C to 0x139F (Port 8) |  |  | 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’ |
| 0x1500 to 0x1508 | 1 Word | HEX | **Port 1 to Port 8 PoE Status**  0x0000: PoE Off 0x0001: PoE On | | |
| 0x1600 to  0x1608 | 1 Word | HEX | **Port 1 to Port 8 PoE Power in Watt** | | |
| **Packet Information** | | | | | |
| 0x2000 to 0x200F | 2 words | HEX | Port 1 to Port 8 Tx Packets  Ex: port 1 Tx Packet Amount = 13248635 Received Modbus response: 0x13248635 | | |
| Word 0 = | 1324 |  |
| Word 1 = | 8635 |  |
| 0x2080 to 0x208F | 2 words | HEX | Port 1 to Port 8 Tx Bytes  Ex: port 1 Tx Bytes Amount = 13248635 Received Modbus response: 0x13248635 | | |
| Word 0 = | 1324 |  |
| Word 1 = | 8635 |  |
| 0x2100 to 0x21(YY\*2-1) | 2 words | HEX | Port 1 to YY Rx Packets  Ex: port 1 Rx Packet Amount = 13248635 Received Modbus response: 0x13248635 | | |
| Word 0 = | 1324 |  |
| Word 1 = | 8635 |  |
| 0x2180 to 0x218F | 2 words | HEX | Port 1 to Port 8 Rx Bytes  Ex: port 1 Rx Bytes Amount = 13248635 Received Modbus response: 0x13248635 | | |
| Word 0 = | 1324 |  |
| Word 1 = | 8635 |  |

**ETHERNET/IP CIP OBJECT MAPPING INFORMATION**

The following communication objects that defined in Common Industrial Protocol (CIP) are supported in switches for PLCs and SCADA systems to monitor:

* Identity Object
* TCP/IP Interface Object
* Ethernet Link Object
* Proprietary Object

The following tables introduce the supported attributes, including access rules for each attribute, and services for the above objects. Users can also refer to the official documents of CIP introduction (Vol. 1) and the Ethernet/IP Adaption of CIP (Vol. 2) to understand the details of each attribute of the standard objects.

**Identity Object**

The Class code of Identity object is defined in **CIP Vol 1, 5-2** and the value is **0x01**. **Class Attribute List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **Data Type** | **Description** |
| 1 | Get | Revision | UINT (16) | Revision of this object |
| 2 | Get | Max Instance | UINT (16) | Maximum instance number of an object currently created in this class  level of the device |
| 3 | Get | Number of Instances | UINT (16) | Number of object instances currently  created in this class level of the device. |
| 6 | Get | Maximum ID Number Class Attributes | UINT (16) | The attribute ID number of the last class attribute of the class definition  implemented in the device |
| 7 | Get | Maximum ID Number Instance Attributes | UINT (16) | The attribute ID number of the last instance attribute of the class  definition implemented in the device |

**Instance Attribute List**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **(Struct.)** | **Data Type** | **Description** |
| 1 | Get | Vendor ID |  | UINT (16) | The vendor ID of company |
| 2 | Get | Device Type |  | UINT (16) | 0 x 307, “Managed Ethernet  Switch” |
| 3 | Get | Product Code |  | UINT (16) | Please refer to the Product Code  Table |
| 4 | Get | Revision |  | (Struct.) | The version of the Identity object |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | Major | USINT (8) | The structure member, major |
| Minor | USINT (8) | The structure member, minor |
| 5 | Get | Status |  | WORD (16) | Not used |
| 6 | Get | Serial Number |  | UDINT (32) | The serial number of each device |
| 7 | Get | Product Name |  | SHORT\_  STRING | The product name in  human-readable format |

**Common Service List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service**  **Code** | **Implementation** | | **Service Name** | **Description** |
| **Class** | **Instance** |
| 0x01 | ✓ | ✓ | Get\_Atributes\_All | Return the contents of all attributes of  the class |
| 0x0E | ✓ | ✓ | Get\_Atributes\_Single | Used to read an object instance attribute |
| 0x10 |  | ✓ | Set\_Atributes\_Single | Used to write an object instance attribute |
| 0x05 |  | ✓ | Reset | Invokes the reset service for the device |

**TCP/IP Interface Object**

The Class code of TCP/IP Interface object is defined in **CIP Vol 2, 5-3** and the value is **0xf5**. **Class Attribute List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **Data Type** | **Description** |
| 1 | Get | Revision | UINT (16) | Revision of this object |
| 2 | Get | Max Instance | UINT (16) | Maximum instance number of an object currently created in this class  level of the device |
| 3 | Get | Number of Instances | UINT (16) | Number of object instances currently  created in this class level of the device. |
| 6 | Get | Maximum ID Number Class Attributes | UINT (16) | The attribute ID number of the last class attribute of the class definition  implemented in the device |
| 7 | Get | Maximum ID Number Instance Attributes | UINT (16) | The attribute ID number of the last instance attribute of the class  definition implemented in the device |

**Instance Attribute List**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **(Struct.)** | **Data Type** | **Description** |
| 1 | Get | Status |  | DWORD (32) | Interface status  0 = The Interface Configuration attribute has |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | not been configured. 1 = The Interface Configuration  attribute contains valid configuration obtained from BOOTP, DHCP or non-volatile  storage |
| 2 | Get | Configuration Capability |  | DWORD (32) | Interface capability flags Bit map of capability flags:  Bit 0: BOOTP Client Bit 1: DNS Client Bit 2: DHCP Client  Bit 3: DHCP-DNS Update  Bit 4: Configuration Settable |
| 3 | Get/Set | Configuration Control |  | DWORD (32) | Interface control flags Bit map of control flags:  Bit 0 to 3: Startup Configuration **0** = The device shall use the interface configuration values previously stored (for example,  in non-volatile memory or via hardware witches).  **1** = The device shall obtain its interface configuration values via BOOTP.  **2** = The device shall obtain its interface configuration values via DHCP upon start-up.  **3 to15** = Reserved. |
| 4 | Get | Physical Link Object |  | (Struct.) | Path to physical link object |
| Path Size | UINT (16) | Size of Path |
| Path | Padded  EPATH | Logical segments identifying the  physical link object |
| 5 | Get/Set | Interface Configuration |  | (Struct.) | TCP/IP network interface  configuration |
| IP Address | UDINT (32) | The device’s IP address |
| Network  Mask | UDINT (32) | The device’s network mask |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | Gateway  Address | UDINT (32) | Default gateway address |
| Name  Server | UDINT (32) | Primary name server |
| Name  Server 2 | UDINT (32) | Secondary name server |
| Domain  Name | STRING | Default domain name |
| 6 | Get/Set | Host Name |  | UDINT (32) | Host name |

**Common Service List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service**  **Code** | **Implementation** | | **Service Name** | **Description** |
| **Class** | **Instance** |
| 0x01 | ✓ | ✓ | Get\_Atributes\_All | Return the contents of all attributes of  the class |
| 0x0E | ✓ | ✓ | Get\_Atributes\_Single | Used to read an object instance attribute |
| 0x10 |  | ✓ | Set\_Atributes\_Single | Used to write an object instance attribute |

**Ethernet Link Object**

The Class code of TCP/IP Interface object is defined in **CIP Vol 2, 5-4** and the value is **0xf6**. There is an instance for each switch port, and mapping as the following table:

|  |  |
| --- | --- |
| **Instance Number** | **Mapping to** |
| 0 | Ethernet Link class |
| 1 | 1st switch port |
| 2 | 2nd switch port |
| 3 | 3rd switch port |
| … | Nth switch port |

**Class Attribute List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **Data Type** | **Description** |
| 1 | Get | Revision | UINT (16) | Revision of this object |
| 2 | Get | Max Instance | UINT (16) | Maximum instance number of an object currently created in this class  level of the device |
| 3 | Get | Number of Instances | UINT (16) | Number of object instances currently  created in this class level of the device. |
| 6 | Get | Maximum ID Number Class Attributes | UINT (16) | The attribute ID number of the last class attribute of the class definition  implemented in the device |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7 | Get | Maximum ID Number Instance Attributes | UINT (16) | The attribute ID number of the last instance attribute of the class  definition implemented in the device |

**Instance Attribute List**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **(Struct.)** | **Data Type** | **Description** |
| 1 | Get | Interface Speed |  | UDINT (32) | Interface speed currently in use (Speed in Mbps, e.g., 0, 10, 100,  1000, etc.) |
| 2 | Get | Interface  Flags |  | DWORD  (32) | Refer to the Interface Flags table |
| 3 | Get | Physical  Address |  | ARRAY of 6  USINT (8) | MAC layer address (The System  MAC address) |
| 4 | Get | Interface Counters |  | (Struct.) | Counters relevant to the receipt of  packets |
| In Octets | UDINT (32) | Octets received on the interface. |
| In Ucast  Packets | UDINT (32) | Unicast packets received on  the interface |
| In NUcast  Packets | UDINT (32) | Non-unicast packets received on the  interface |
| In Discards | UDINT (32) | Inbound packets received on  the interface but are discarded |
| In Errors | UDINT (32) | Inbound packets that contain Errors (does not include In  Discards) |
| In Unknown  Protos | UDINT (32) | Inbound packets with unknown  protocol |
| Out Octets | UDINT (32) | Octets sent on the interface |
| Out Ucast  Packets | UDINT (32) | Unicast packets sent on the  interface |
| Out NUcast  Packets | UDINT (32) | Non-unicast packets sent on  the interface |
| Out  Discards | UDINT (32) | Discarded outbound packets |
| Out Errors | UDINT (32) | Outbound packets that contain  errors |
| 6 | Get/Set | Interface Control |  | (Struct.) | Configuration for physical interface |
| Control Bits | WORD (16) | Bit **0**: Auto-Negotiate  Value 0: Force |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | Value 1: Auto-Nego Bit **1**: Half/Full Duplex Value 0: half duplex Value 1: full duplex  Bit **2 to 15**: Reserved, all zero |
| Forced Interface  Speed | UINT (16) | Speed at which the interface shall be forced to operate |
| 7 | Get | Interface Type |  | USINT | Value **0**: Unknown interface type. Value **1**: The interface is internal to the device, for example, in the case of an embedded switch.  Value **2**: Twisted pair (e.g.,  10Base-T, 100Base-TX, 1000Base-T,  etc.)  Value **3**: Optical fiber (e.g., 100Base-FX)  Value **4 to 256**: Reserved |
| 8 | Get | Interface State |  | USINT | Value **0**: Unknown interface state Value **1**: The interface is enabled and is ready to send and receive data  Value **2**: The interface is disabled Value **3**: The interface is testing  Value **4 to 256**: Reserved |
| 9 | Get | Admin State |  | USINT | Value **0**: Reserved  Value **1**: Enable the interface  Value **2**: Disable the interface. If this is the only CIP communications interface, a request to disable the interface shall result in an error (status code 0x09).  Value **3 to 256**: Reserved |
| 10 | Get | Interface  Label |  | SHORT\_  STRING | Human readable identification |
| 101 | Get | PoE  Status |  | USINT (8) | Value **1**: PoE On  Value **2**: PoE Off |
| 102 | Get | PoE  Power |  | UDINT (32) | PoE Power in Watt |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 103 | Get/Set | PoE Mode |  | UDINT (32) | Value **0**: Unknown  Value **1**: Enable  Value **2**: Disable  Value **3**: Force |

**Interface Flags**

|  |  |  |
| --- | --- | --- |
| **Bit(s)** | **Called** | **Definition** |
| 0 | Link Status | 1. indicates an inactive link. 2. indicates an active link. |
| 1 | Half/Full Duplex | 1. indicates half duplex. 2. indicates full duplex. |
| 2-4 | Negotiation Status | Indicates the status of link auto-negotiation 0 = Auto-negotiation in progress.  1 = Auto-negotiation and speed detection failed. Using default values for speed and duplex. Default values are product-dependent; recommended defaults are 10Mbps and half duplex.  2 = Auto negotiation failed but detected speed. Duplex was defaulted. Default value is product-dependent; recommended default is half duplex.  3 = Successfully negotiated speed and duplex.  4 = Auto-negotiation not attempted. Forced speed and duplex. |
| 5 | Manual Setting Requires Reset | 0 indicates the interface can activate changes to link parameters (auto-negotiate, duplex mode, interface speed) automatically. 1 indicates the device requires a Reset service be issued to its Identity Object for the changes to  take effect. |
| 6 | Local Hardware Fault | 0 indicates the interface detects no local hardware fault; 1 indicates a local hardware fault is detected. The meaning of this is product specific. For example, an AUI/MII interface might detect no transceiver attached, or a radio modem might detect no antenna attached. In contrast to the soft, possibly self-correcting nature of the Link Status being inactive, this is assumed a hard fault requiring user  intervention. |
| 7-31 | Reserved | Shall be set to zero |

**Common Service List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service**  **Code** | **Implementation** | | **Service Name** | **Description** |
| **Class** | **Instance** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0x0E | ✓ | ✓ | Get\_Atributes\_Single | Used to read an object instance attribute |
| 0x10 |  | ✓ | Set\_Atributes\_Single | Used to write an object instance attribute |

**Proprietary Object**

The Class code of Proprietary object is defined by vendor, and the value is **0x1C1**. **Class Attribute List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Addr**  **ID** | **Access**  **Rule** | **Name** | **Data Type** | **Description** |
| 1 | Get | Power 1 | USINT (8) | Power 1 status.  Value **1**: On  Value **0**: Off |
| 2 | Get | Power 2 | USINT (8) | Power 2 status.  Value **1**: On  Value **0**: Off |
| 3 | Get | Alarm Relay | USINT (8) | Alarm Relay status. Value **1**: On  Value **0**: Off |
| 4 | Get | Digital Input | USINT (8) | Digital Input status. Value **1**: High  Value **0**: Low |
| 5 | Get | System Time | UDINT (32) | System Time encodes as Unix time. |
| 6 | Get | All Interface Speed | ARRAY of 28  UDINT(32) | Array list of all interface speed  currently in use |
| 7 | Get | All Interface Flags | ARRAY of 28  DWORD(32) | Array list of all interface flags. Refer  to the **Interface Flags** table |
| 8 | Get | All Interface States | UDINT (32) | Bitwise of all current interface states. Bit **0**: Port 1  Value **0**: Link down Value **1**: Link up  Bit **1**: Port 2, and so on |

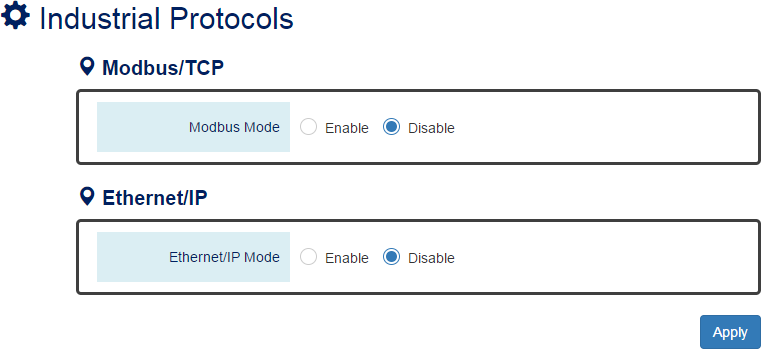
**ETHERNET/IP ELECTRONIC DATA SHEET (EDS) FILE**

The EDS (Electronic Data Sheet) file includes electronic descriptions of all relevant communication parameters and objects of an EtherNet/IP device. It is required for I/O controllers to recognize switch and its CIP capability.

The list includes the sections which are described in our EDS file.

* [File]
* [Device]
* [Device Classification]
* [Port]
* Icon should be **32 \* 32** in pixel.

**CONFIGURE INDUSTRIAL PROTOCOLS INFORMATION**



#### Modbus Mode

“Enable” or “Disable” the Modbus/TCP function.

#### Ethernet/IP Mode

“Enable” or “Disable” the Ethernet/IP function.

  (Apply Button)

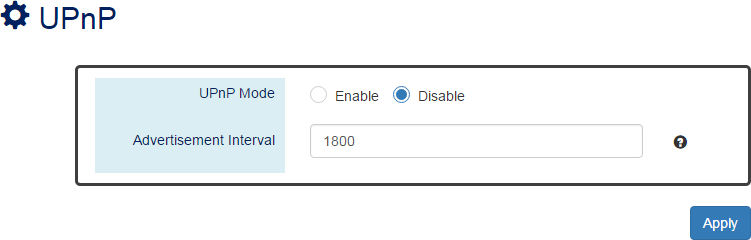
After configuring above fields, click "**Apply**" button to make the changes effective.

# UPnP

UPnP is **Universal Plug and Play**, a set of networking protocols that permit the network devices to seamlessly discover each other in the networks. It is promoted by the UPnP Forum, but since 2016, all UPnP efforts are managed by the Open Connectivity Foundation.

UPnP extends “**plug and play**” to connect to a network device without configuration. When an UPnP device such as printer, Wi-Fi AP, or mobile device connects to a network, it will automatically establish the working configurations with another devices.

**CONFIGURE UPNP INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### UPnP Mode

“Enable” or “Disable” the UPnP function.

#### Advertisement Interval

A period used to send the UPnP advertisement frame.

The range of the Advertisement Interval is **from 300 to 86400** seconds.

The default Advertisement Interval is **1800** seconds.

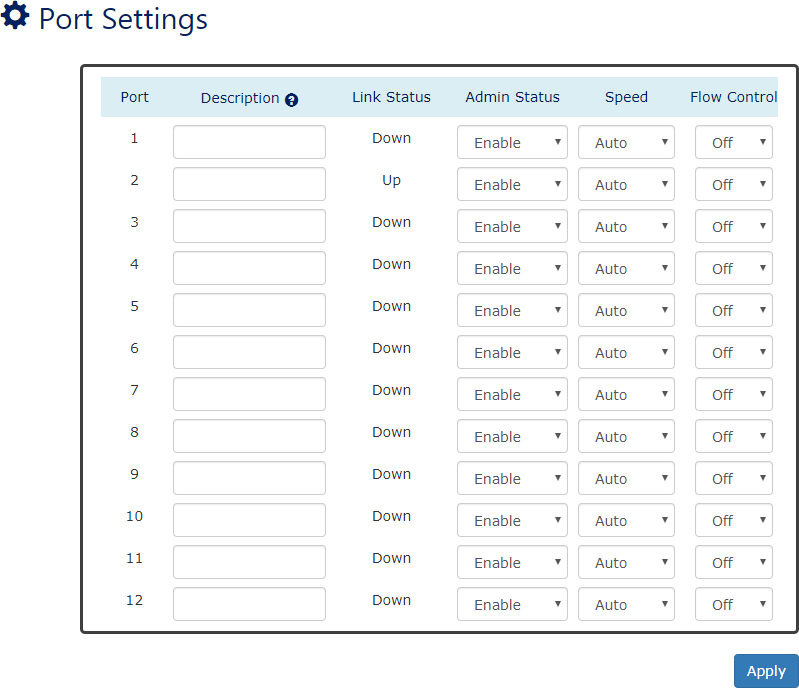
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# Port Management

**Port Management** contains a “Description” field that is used to describe the port, “Enable” or “Disable” option to turn on or turn off a specific port, configure the speed-duplex for the port, and Flow Control on the port. In the Port Status page, the users can obtain information such as Link Status, Speed, Duplex, Flow Control, Tx and Rx in Bytes, and PoE status. These are extremely helpful for the administrator to manage the interfaces on the switch.

### CONFIGURE PORT INFORMATION



#### Port

***For more information, hover the mouse over the icon in the system.***

Port1 to PortN, where N is based on the total port number.

#### Description

The description for the port is helpful for the administrator to identify the difference between the ports.

The **max. length** for the Description is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

#### Link Status

Link Status shows “Up”, “Down”, or “Disable” to reflect the link status of the port.

#### Admin Status

“Enable” or “Disable” the Admin Status of the port to restrict the transmission on the port. **Note:** Administrator can **turn off the un-used port** to **secure** the network with unexpected device.

#### Speed

The users can manually fix the speed and duplex or automatically run auto-negotiation to determine the speed and duplex for copper ports.

* + Auto: The port follows IEEE 802.3u protocol to auto-negotiate with connected device.
  + 100M-Full: The port transmits frames with **100Mbits** per second speed and **full duplex**.
  + 100M-Half: The port transmits frames with **100Mbits** per second speed and **half duplex**.
  + 10M-Full: The port transmits frames with **10Mbits** per second speed and **full duplex**.
  + 10M-Half: The port transmits frames with **10Mbits** per second speed and **half duplex**.

The users must manually configure SFP ports to fix the speed and duplex. The default setting is the highest speed for the SFP slot.

* + 10G-Full (Only supported on **10G models**)

The port transmits frames with **10Gbits** per second speed and **full duplex**.

* + 1G-Full: The port transmits frames with **1Gbits** per second speed and **full duplex**.
  + 100M-Full (Only supported on **dual speed SFP ports**)

The port transmits frames with **100Mbits** per second speed and **full duplex**.

* + Copper-Full: Select Copper-Full when using **copper SFP** module.

**Note:** Configure the port speed to "**1G-Full**" if users need the **VDSL2 SFP** supported.

For **Copper SFP Module**, please refer to the following instructions to configure the correct speed:

|  |  |  |
| --- | --- | --- |
| **Copper SFP Module Type** | **Speed Config** | **Note** |
| SGMII (10/100/1000M) | Copper-Full | Only support transmitting on 1000M |
| Multi-Speed (1G/10G) | 10G-Full | Depends on the connected speed |
| 10G | 10G-Full |  |
| 1G / VDSL2 | 1G-Full |  |

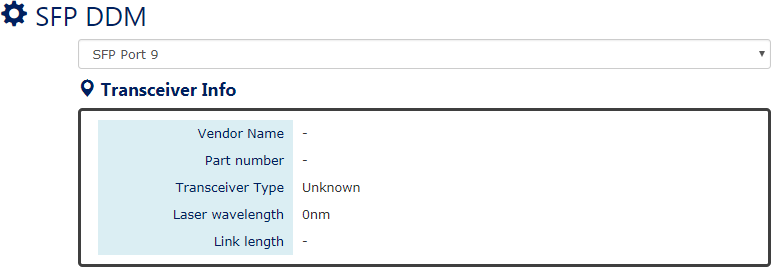
#### Flow Control

“Enable” or “Disable” the Flow Control when the speed is set to “Auto”. Enabling the Flow Control helps to prevent the traffic from losing when the network is in congestion.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**SFP DDM STATUS**



#### SFP Port Selector

Select the SFP port number to display SFP DDM information.

#### Transceiver Info

If there is no SFP module inserted or the information cannot be read, the field will show “-“.

* + Vendor Name

This field shows the **brand or vendor name** of the SFP module.

* + Part Number

This field shows the **model name** (**part number**) of the SFP module.

* + Transceiver Type

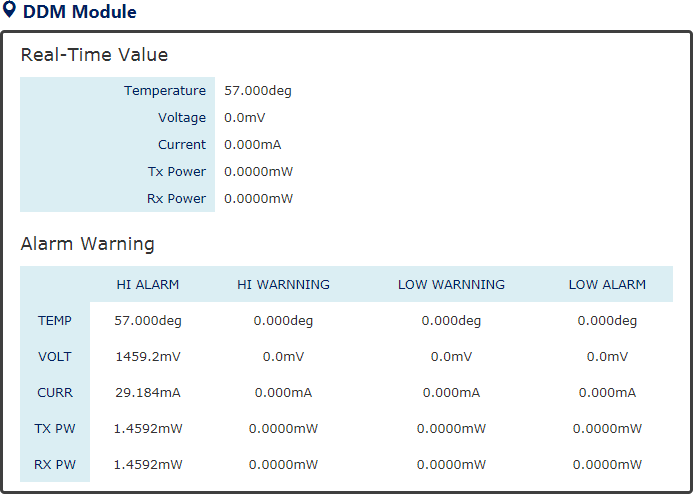
This field shows the **transceiver type** of the SFP module including transmitting **speed** and the **type of fiber**. If there is no SFP module inserted or the transceiver type cannot be read, the field will show “**Unknown**“.

* + Laser Wavelength

This field shows the **laser operating wavelength** of the SFP module.

* + Link Length

This field shows the **maximum link length** of the SFP module.



#### DDM Module

This section only shows when the **SFP DDM** is supported on the inserted SFP module.

* + Real Time Value

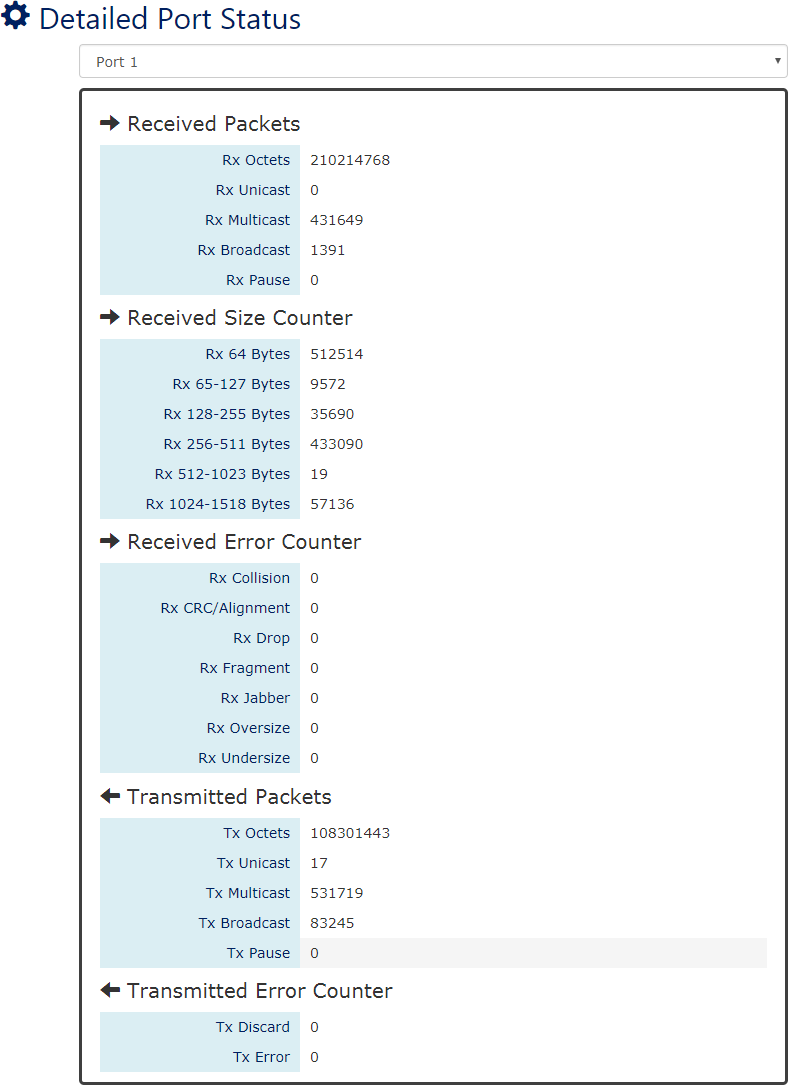
The current operating information including **temperature**, **voltage**, **current**, **Tx power**, and **Rx power**.

* + Alarm Warning

The default configured threshold for triggering the alarm and system warning. There are 5 types of information (**temperature**, **voltage**, **current**, **Tx power**, and **Rx power**) and 4 levels of alarm and warning (**high alarm/warning**, **low alarm/warning**).

### DETAILED PORT STATUS

There are two methods to link to **detailed port status** (**RMON**). One is from **menu** and the other is from the **front panel** picture. Uses can directly click the port on the front panel and then the page will redirect to the detailed port status page of the specific port. The RMON is a set of standard Simple Network Management Protocol (SNMP) and it is useful to monitor and manage the incoming and outgoing traffic.



#### Port Selector

Select the port number to monitor the RMON information. Port 1 to N, where N is based on the total port number.

#### Received Packets

* + Rx Octets: the total received traffic in bytes
  + Rx Unicast: the number of received unicast packets
  + Rx Multicast: the number of received multicast packets
  + Rx Broadcast: the number of received broadcast packets
  + Rx Pause: the number of MAC Control packets received on the specific interface with an opcode indicating the PAUSE operation.

#### Received Size Counter

* + Rx 64 Bytes: the number of received packets that were 64 octets
  + Rx 65-127 Bytes: the number of received packets that were from 65 to 127 octets
  + Rx 128-255 Bytes: the number of received packets that were from 128 to 255 octets
  + Rx 256-511 Bytes: the number of received packets that were from 256 to 511 octets
  + Rx 512-1023 Bytes: the number of received packets that were from 512 to 1023 octets
  + Rx 1024-1518 Bytes: the number of received packets that were from 1024 to 1518 octets

#### Received Error Counter

* + Rx Collision: the total number of collisions on the Ethernet segment.
  + Rx CRC/Alignment: the total number of received packets that have either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
  + Rx Drop: the total number of dropped packets due to lack of resources.
  + Rx Fragment: the total number of received packets that are less than 64 octets and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
  + Rx Jabber: the total number of received packets that are longer than 1518 octets and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
  + Rx Oversize: the total number of received packets that are longer than 1518 octets.
  + Rx Undersize: the total number of received packets that are less than 64 octets.

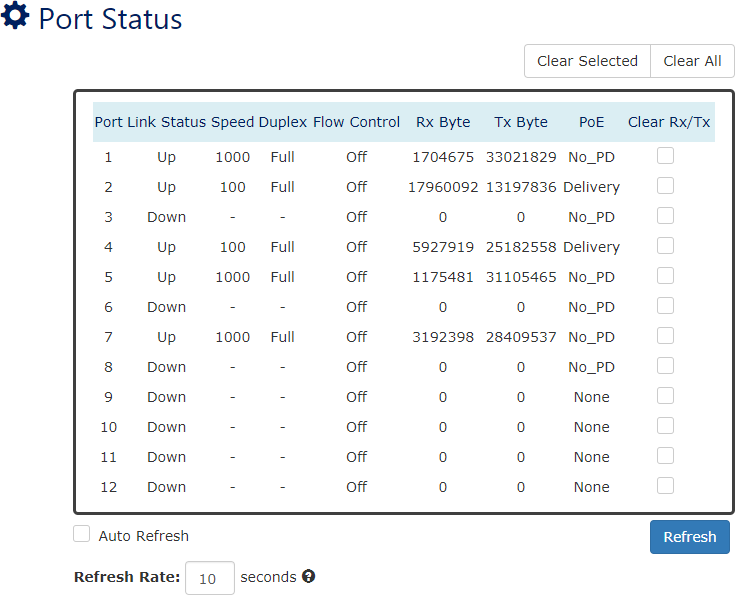
#### Transmitted Packets

* + Tx Octets: the total transmitted traffic in bytes.
  + Tx Unicast: the number of transmitted unicast packets
  + Tx Multicast: the number of transmitted multicast packets
  + Tx Broadcast: the number of transmitted broadcast packets
  + Tx Pause: the number of MAC Control packets transmitted on the specific interface with an opcode indicating the PAUSE operation.

#### Transmitted Error Counter

* + Tx Discard: the number of outbound packets which are chosen to be discarded even though no errors had been detected. One possible reason for discarding such a packet could be to free up buffer space.
  + Tx Error: the number of outbound packets that could not be transmitted because of errors.

### PORT STATUS



#### Port

Port 1 to N, where N is based on the total port number.

#### Link Status

Link Status displays the link state (“Up” or “Down”) of the port. If the port is disabled, it displays “Disabled”.

#### Speed

Speed displays the access speed in bit per second of the port. If the port is linked down, it displays “-“.

#### Duplex

Duplex displays the link-type (Full or Half) of the port. If the port is linked down, it displays “-“.

#### Flow Control

It is the state (On or Off) of the Flow Control.

#### Rx Byte

This is the total **received** frames formatted in byte.

#### Tx Byte

This is the total **transmitted** frames formatted in byte.

* **PoE** (PoE Model Only)

PoE displays the PoE state (Delivery, No PD, Disabled, None) of the port. If the port does not support PoE function, it displays “None”.

**Note:** This information is displayed on the system that supports the PoE function.

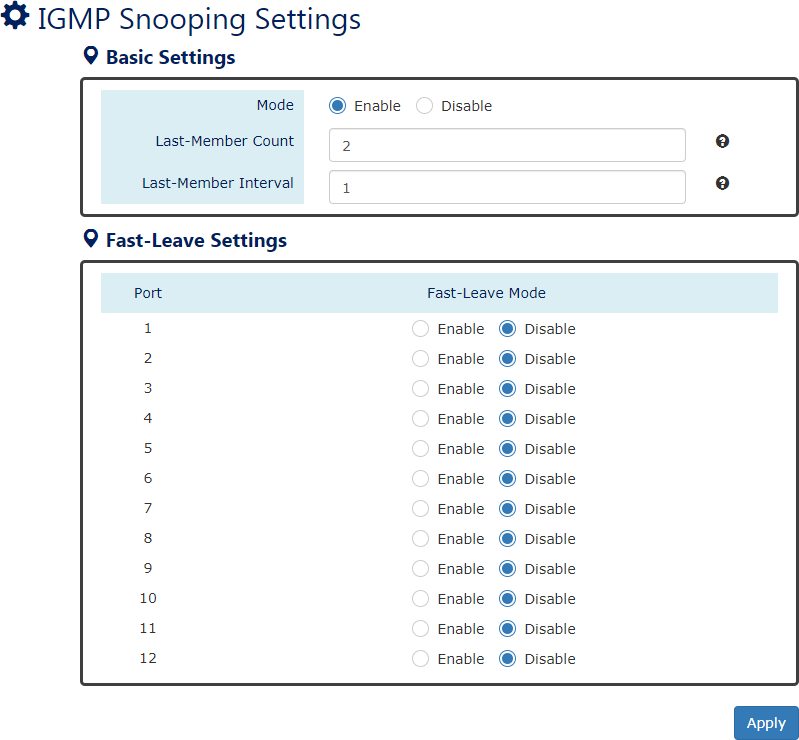
#### Clear Rx/Tx

Select the specific ports and click the “**Click Selected**” button to clear the Tx/Rx Byte information or click “**Click All**” button to clear all ports’ Tx/Rx Byte information.

# IGMP Snooping

**Internet Group Management Protocol (IGMP)** is used in communicating among hosts and establishing a multicast group membership on the IPv4 networks (Layer 3). IGMP provides the ability to prune **multicast traffic** to those who need this kind of traffic and reduce the amount of traffic on the network. However, switches work on the MAC Layer (Layer 2) and are unable to obtain IGMP information. **IGMP Snooping** allows the switch to listen to the IGMP communication between hosts and routers and maintains a table of multicast IPs and group members. **IGMP Snooping** can prevent the hosts on the LAN from receiving traffic from a non-joined multicast group and save bandwidth of the network.

**CONFIGURE IGMP SNOOPING INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Basic Setting

* + Mode

“Enable” or “Disable” the IGMP Snooping function.

* + Last-Member Count

The count is the number of times that the router sends IGMP query messages to receive the leave message.

The range of the Last-Member Count is **from 2 to 10**.

The default Last-Member Count Interval is **2**.

。 Last-Member Interval

The interval is the period to send IGMP query messages.

The range of the Last-Member Interval is **from 1 to 25** seconds.

The default Last-Member Interval is **1** second.

#### Fast-Leave Setting

* + Port

Port 1 to N, where N is based on the total port number.

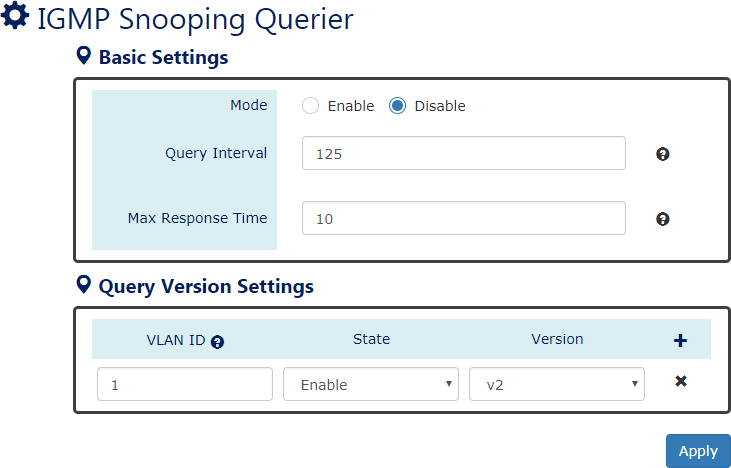
* + Fast-Leave Mode

“Enable” or “Disable” the fast-leave function on the specific port. If the fast-leave mode is enabled on the port, the switch will close the multicast stream when receiving a leave message on this port without further action.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE IGMP SNOOPING QUERIER INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Basic Settings

* + Mode

“Enable” or “Disable” the IGMP Snooping Querier function. If it is enabled, the system sends IGMP snooping **version 1 and 2** queries.

* + Querier Interval

This period is the interval to send the IGMP snooping queries. The range of the Querier Interval is **from 1 to 3600** seconds. The default Querier Interval is **125** seconds.

* + Query Max Response Time

This is a timer to wait for the member response of the IGMP groups. It is used in

**removing** the information of the IGMP groups if no member responds to the query.

#### Query Version Settings

The Query Version Settings is configured for per-VLAN query.

* + VLAN ID

The field is to fill in the VLAN ID to configure the IGMP Snooping query version.

* + State

“Enable” or “Disable” the IGMP Snooping query on the configured VLAN ID.

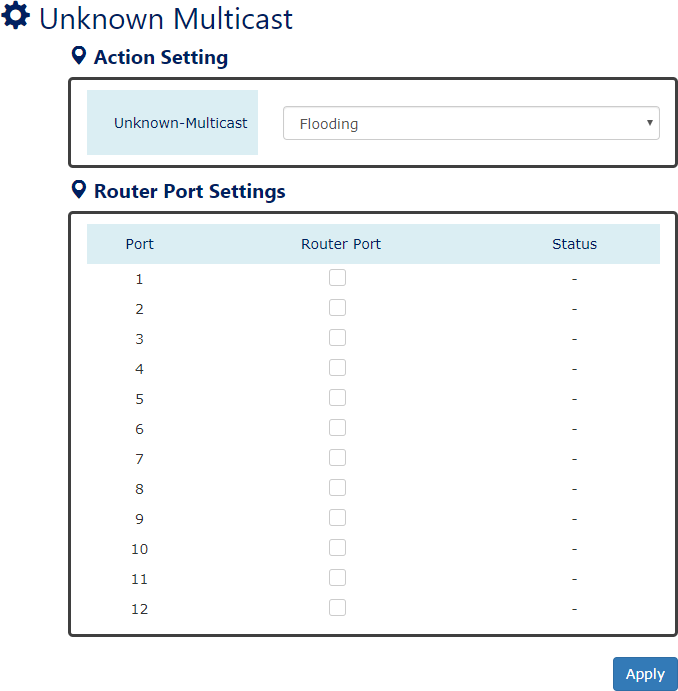
* + Version

Set the IGMP Snooping version (v1, v2c, v3) on the specific VLAN.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE UNKNOWN MULTICAST INFORMATION**



#### Action Settings

* + Unknown-Multicast

Configure the action when the system receives an unknown-multicast packet. Flooding: flood the unknown-multicast packet to all other ports.

Discarding: discard the unknown-multicast packet.

Router: forward the unknown-multicast packet to the router port.

#### Router Port Settings

* + No.

Port 1 to N, where N is based on the total port number.

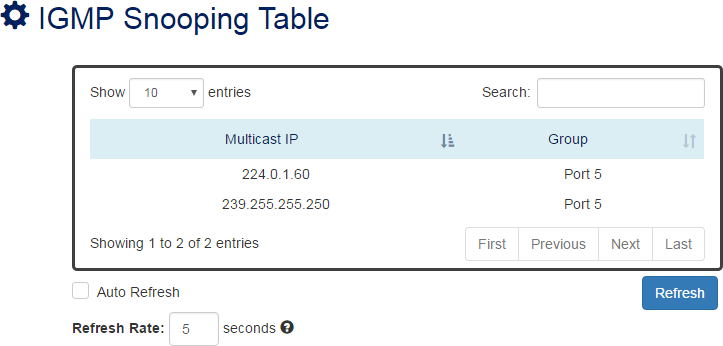
* + Router Port

Set the specific port to router port or not.

* + Status

The status field shows the port’s status which “-“ implies not a router port and “static” implies set to router port.

**IGMP SNOOPING TABLE**



#### Multicast IP

The Multicast IP is the IP address of the multicast group.

#### Group

The group shows the port number, which joined the group.

# 802.1Q VLAN

## Q VLAN

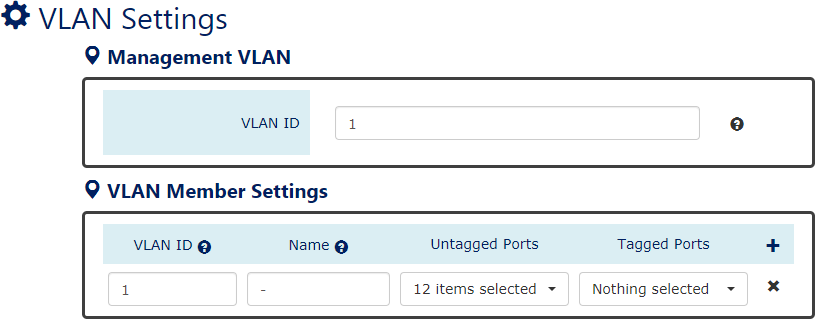
**Virtual Local Area Network (VLAN)** is a structure that can ease Network planning. The devices in a VLAN can be located anywhere without the restriction of physical connections, but work like they are on the same physical segment.

IEEE 802.1Q defines **VLAN tagging** conception for the Ethernet frames. VLAN tagging supports frames in the different VLAN groups transmitting on a link (called **VLAN trunk**). The maximum number of VLANs on the Ethernet network is 4096. The VLAN 0 and VLAN 4095 are for specific use and hence the usable VLAN number is **4094**.

## VLAN Q-IN-Q

**VLAN Q-in-Q**, also called **Stacked VLAN**, is an extension for 802.1Q VLAN. It supports a maximum of 4096\*4096 VLAN groups. VLAN Q-in-Q can apply a port to a provider, customer, or tunnel for different applications. The header of the stacked VLAN frame contains two 802.1Q Headers with different Ethertype (TPID). The TPID “0x88A8” is the outer tag by default and the TPID “0x8100” is the inner tag for 802.1Q VLAN. Customized ethertype called **Specific Provider Ethertype** are supported if one or more ports are set to “**Specific Provider**”.

**CONFIGURE 802.1Q VLAN INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Management VLAN

* + - * VLAN ID

The VLAN ID is for the native VLAN. Only the ports in the same VLAN as Management VLAN can **access the switch** configuration console via **Ethernet**.

The range of the VLAN ID is **from 1 to 4094**. The default Management VLAN ID is **1**.

#### VLAN Member Settings

* + - * VLAN ID

Assigns a unique VLAN ID to this VLAN group. The range of the VLAN ID is **from 1 to 4094**.

* + - * Name

Assigns a name to this VLAN group to identify the different VLANs. The **max. length** for the Name is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

* + - * Untagged Ports

Sets the untagged ports for this VLAN group. The system **removes the VLAN tag** before transmitting from the port that is set to “**untagged**”. Usually, this port is connected to the end device that belongs to this VLAN.

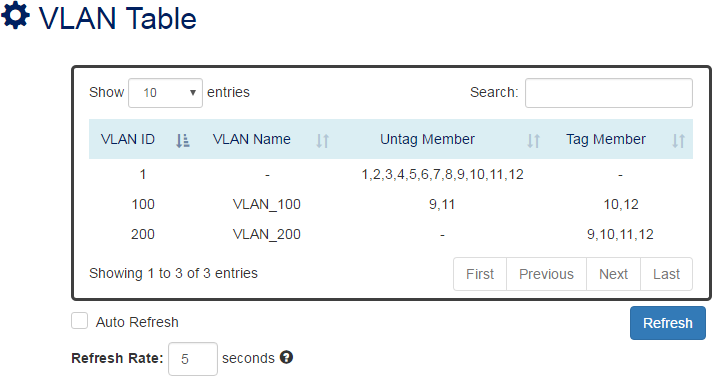
* + - * Tagged Ports

Sets the tagged ports for this VLAN group. The system **keeps the VLAN tag** when transmitting from the port that is set to “**tagged**”. Usually this port is connected to another switch and uses the VLAN tag to transfer the VLAN information.

。 : Click the **plus icon** to add a VLAN Member row.

。 : Click the **remove icon** to delete the VLAN Member row.

* 1. **Q VLAN TABLE**



#### VLAN ID

This is the assigned unique **VLAN ID** for this VLAN group.

#### VLAN Name

This is the assigned **VLAN Name** for this VLAN group.

#### Untag Member

These ports are assigned as VLAN untagged ports.

#### Tag Member

These ports are assigned as VLAN tagged ports.

**CONFIGURE 802.1Q VLAN PVID & ACCEPT TYPE**



***For more information, hover the mouse over the icon in the system.***

#### VLAN PVID

* + - * Port

Port1 to PortN, where N is based on the total port number.

* + - * PVID

Assign a VLAN ID to the frames without a VLAN tag that come into the specific port.

#### Accept Type

* + - * No.

Port1 to PortN, where N is based on the total port number.

* + - * Filter

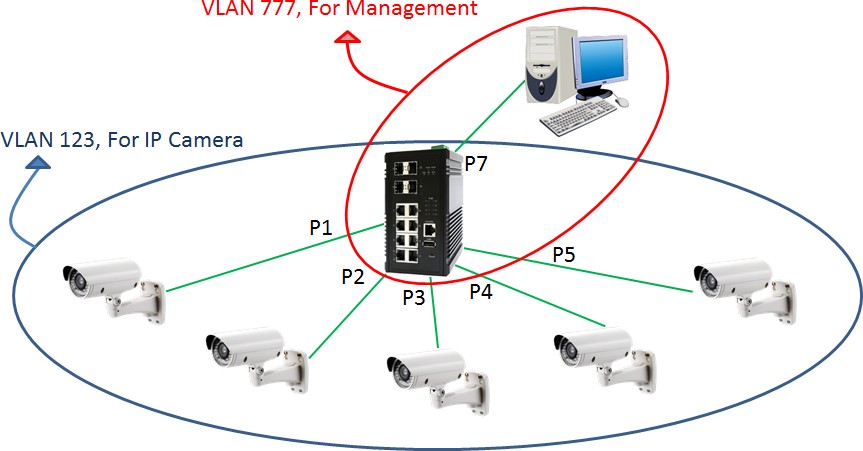
Three types of filters are provided: All, Tagged Only, Untagged Only. All: Accept both tagged and untagged frames that come into the port. Tagged Only: Accept only tagged frames that come into the port.

Untagged Only: Accept only untagged frames that come into the port.

  (Apply Button)

After configuring the above fields, click "**Apply**" button to make it effective.

**CONFIGURATION EXAMPLE FOR MANAGEMENT VLAN**

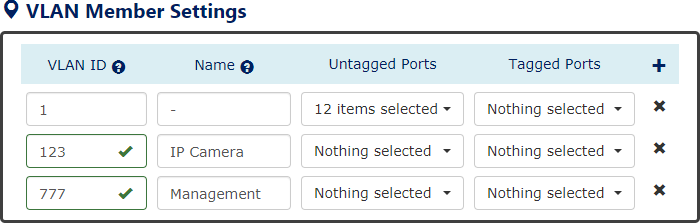


**Key Points**

1. Implement VLAN 777 and apply only Lan7 to VLAN 777
2. Implement VLAN 123 and apply the ports which are connected to IP cameras
3. Assign Management VLAN to VLAN 777

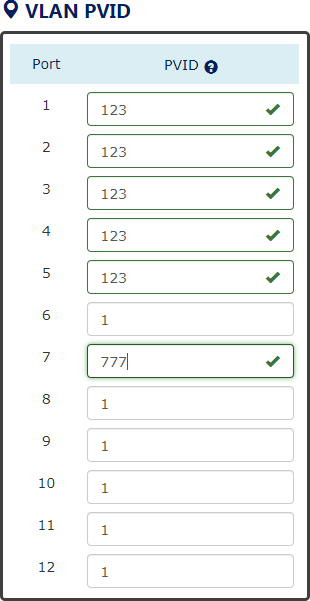
**Step-by-step Configuration**

1. Login Web Console and click menu “*L2 Switching*” -> “*802.1Q VLAN*” -> “*VLAN Settings*”
2. Add rows for VLAN 123 and 777. Apply assigned ports (untagged) to the VLAN.

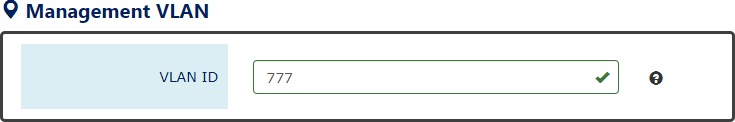
Why untagged? The connected devices are all hosts which are unable to deal with the VLAN tag, so we must remove the VLAN tag when the frame is sending out through the port.

1. Configured the PVID for the applied ports.

The PVID of Port 1 to 5 is 123 and the PVID of Port 7 is 777.



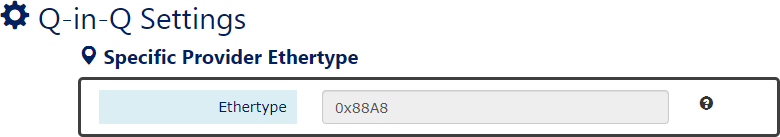
1. Configure Management VLAN to VLAN 777



1. Click the “Apply” button to apply the above configurations.

**Note:** After applying the configurations, the user can only access the management interface via specific interface (in this case: Lan7).

**CONFIGURE VLAN Q-IN-Q**



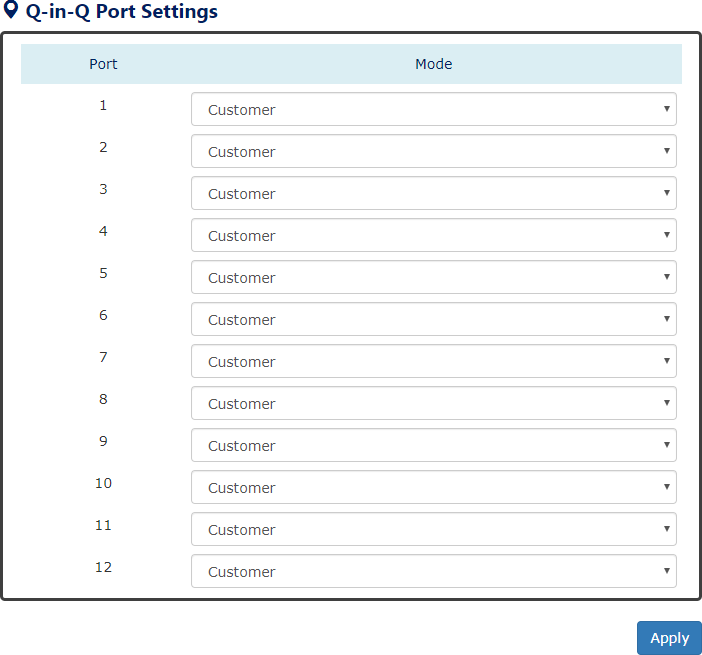
***For more information, hover the mouse over the icon in the system.***

#### Specific Provider Ethertype

This is a global configuration and an Ethertype is assigned for all ports, which are configured as “**Specific Provider**”. This field is locked (disabled) until at least one port is configured to the “**Specific Provider**” in the “**Q-in-Q Port Settings**” section.

The range of the Provider Ethertype is **from 0x0000 to 0xFFFF**, but **0x8100** is **invalid**.

The default Provider Ethertype is **0x88A8**.



#### Q-in-Q Port Settings

* + - * Port

Port1 to PortN, where N is based on the total port number.

* + - * Mode

Set the port to one of the Q-in-Q modes.

The Egress is dependent on the connected device and hence the egress action is skipped.

|  |  |
| --- | --- |
| **Mode** | **Ingress** |
| Q-in-Q Tunnel | **Untagged** Frames: Add TPID:0x88A8 tag and forward.  **Tagged** Frames:   1. TPID:0x8100: Add TPID:0x88A8 tag and forward. 2. TPID:0x88A8: Forward the frames. |
| **Mode** | **Ingress** |
| Customer | A port set to “Customer” runs typically 802.1Q VLAN. **Untagged** Frames: Add TPID:0x8100 tag and forward. **Tagged** Frames:  1. TPID:0x8100:  a. Same VLAN ID: Forward the frames. |

|  |  |
| --- | --- |
|  | b. Different VLAN ID: Discard the frames.  2. TPID:0x88A8: Discard the frames. |
| Provider | **Untagged** Frames: Add TPID:0x88A8 tag and forward.  **Tagged** Frames:   1. TPID:0x8100: Discard the frames. 2. TPID:0x88A8:    1. Same VLAN ID: Forward the frames.    2. Different VLAN ID: Discard the frames. |
| Specific Provider | Users define the Ethertype for the Provider service. **Untagged** Frames: Add the user defined TPID tag and forward.  **Tagged** Frames:   1. TPID:0x8100: Discard the frames. 2. TPID:0x88A8: Discard the frames. 3. TPID: [user-defined]:    1. Same VLAN ID: Forward the frames.    2. Different VLAN ID: Discard the frames. |

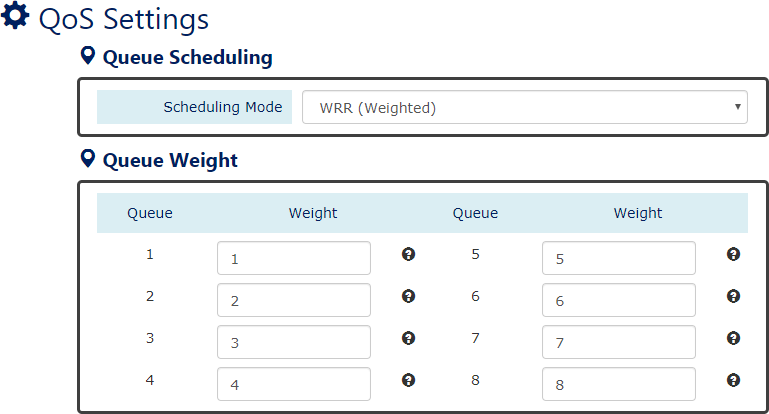
* + - (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# Quality of Service

**Quality of Service** which known as **QoS** provides a stable and predictable transmitting service. It is useful to manage the bandwidth more efficiently based on the requirement of applications. Users can set **different priorities** for different traffics to satisfy the services which need a fixed bandwidth and have more sensitive of delay. **Quality of Service** can also optimize the restrict bandwidth resource and control the network traffic of the switches.

### CONFIGURE QOS INFORMATION



***For more information, hover the mouse over the icon in the system.***

#### Queue Scheduling

* + - * Scheduling Mode

Select the scheduling mode for the Quality of Service.

WRR: **Weighted Round Robin**. WRR ensures that every queue takes turns to transmit the traffic by its weight.

Strict: **Strict Priority Queue**. The traffic is transmitted based on the priority, which is from highest to lowest.

#### Queue Weight

* + - * Queue

Eight queues from queue 0 to queue 7 are supported.

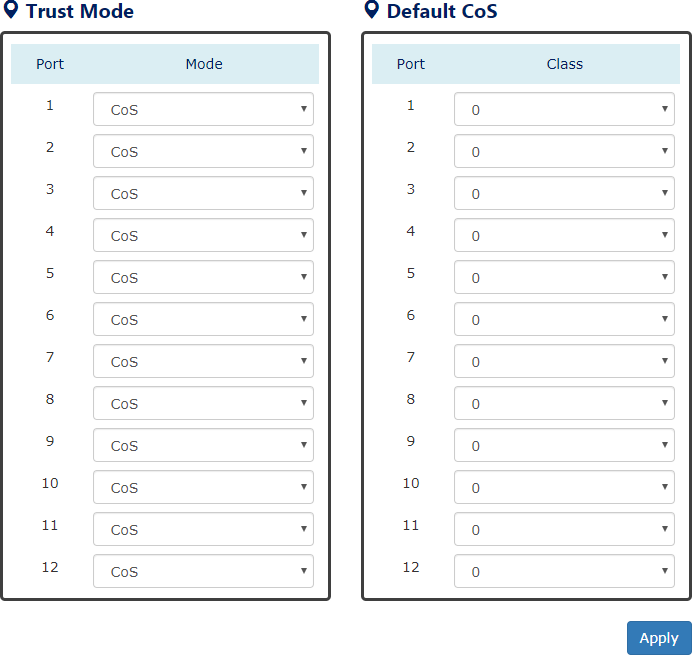
* + - * Weight

Enables you to configure a specific weight for the port.

The range of the Weight is **from 1 to 100**. There is no need to sum all queues to 100. The default Weight for each queue is displayed in the table:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Queue** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Weight** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

**CONFIGURE QOS TRUST MODE AND DEFAULT COS**



#### Trust Mode

* + - * Port

Port1 to PortN, where N is based on the total port number.

* + - * Mode

CoS: Class of Service. Use the 3-bit “PRI” field in the VLAN tag. It enables you to assign traffic to 8 different classes **from 0 to 7**.

DSCP: Use 6-bit field “DSCP” in the Type of Service (ToS) tag. It enables you to assign traffic to 64 different types **from 0 to 63**.

#### Default CoS

* + - * Port

Port1 to PortN, where N is based on the total port number.

* + - * Class

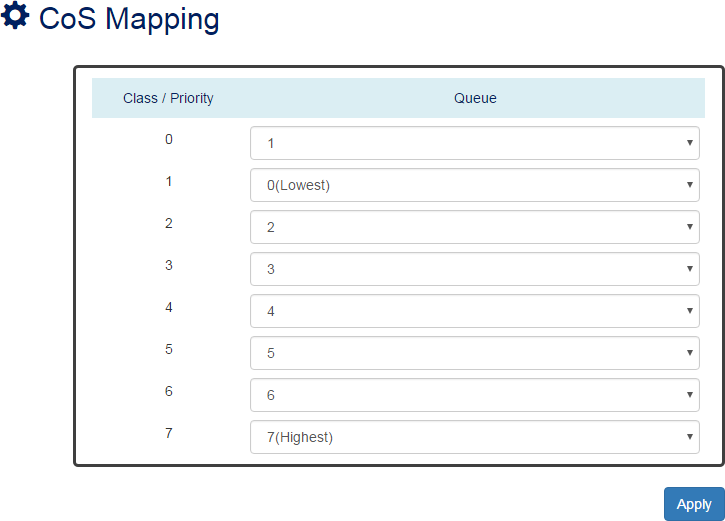
You can assign a default class to the port. The system follows the assigned CoS classes to transmit frames if there is **no VLAN tag** in the frame header.

The default Class for each port is **0**.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE COS MAPPING**



#### Class / Priority

There are **3 bits** for the “Class of Service” field called “**PRI**” in the VLAN tag and there are 8 classes **from 0 to 7**.

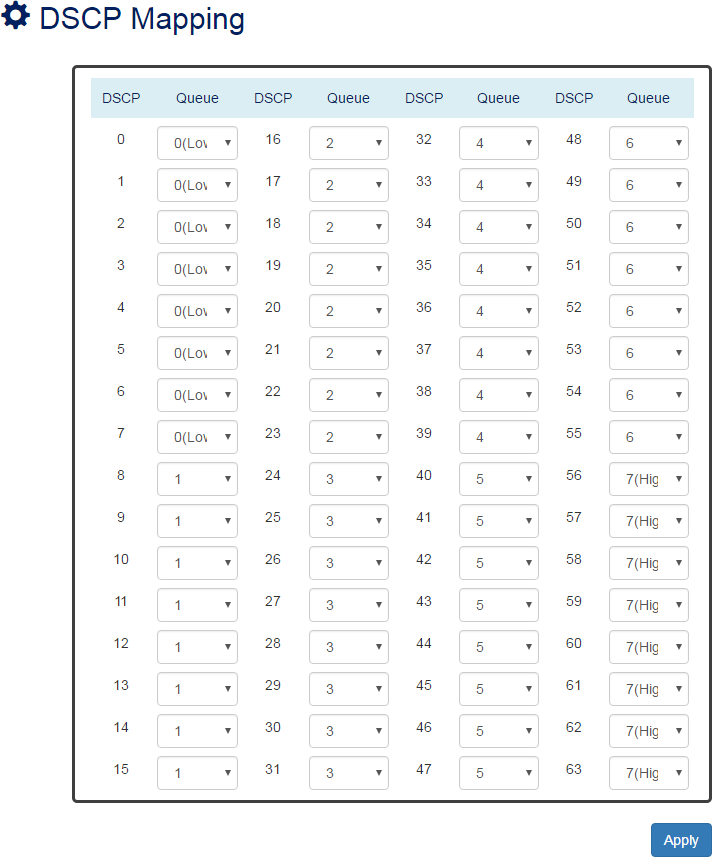
#### Queue

The chipset supports **8 queues from queue 0 to queue 7**. The queue 0 is the lowest priority queue and the queue 7 is the highest priority queue.

The default Queue for each class is displayed in the table:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Class** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Queue** | 1 | 0 | 2 | 3 | 4 | 5 | 6 | 7 |

**CONFIGURE TOS MAPPING**



#### DSCP

There are **6 bits** for the “**DSCP**” in ToS tag and hence there are 64 classes **from 0 to 63**.

#### Queue

The chipset supports **8 queues from queue 0 to queue 7**. The queue 0 is the least priority queue and the queue 7 is the highest priority queue.

The default Queue for each type is displayed in the table:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Type** | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
| **Queue** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

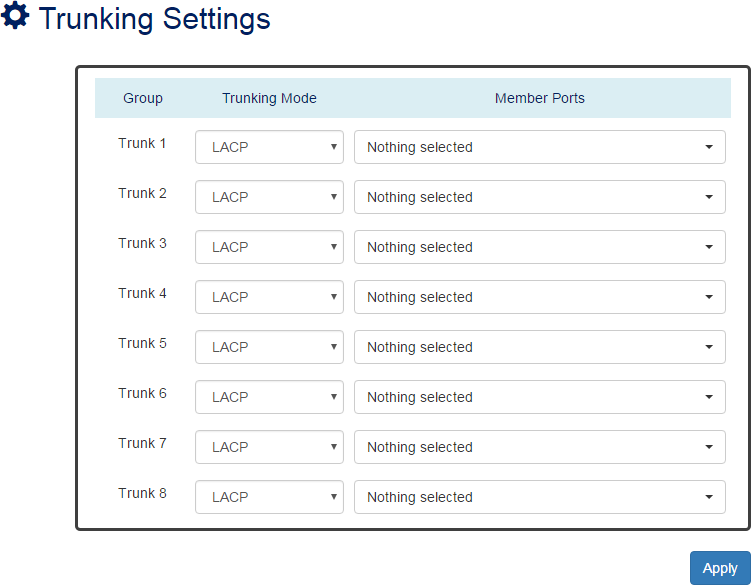
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# Port Trunk

**Port Trunk** is also known as **Link Aggregation**, and it is a protocol to group links to a trunk. A total of **8** trunk groups are provided. It is a good method to reach load balance and link backup. For example, when port 1 to port 4 are combined to trunk 1 and all ports support 100Tx and set to full duplex, the bandwidth of the trunk will be 800Mbps. The traffic transmitting on the trunk is distributed to one of the links by the source **MAC address** to reach the load balance. When the trunk mode is set to LACP and when one of the links is broken, the traffic will transmit on another link on the group.

### CONFIGURE PORT TRUNK INFORMATION



#### Group

Eight trunk groups from **Trunk 1** to **Trunk 8** are supported.

#### Trunking Mode

Two trunking modes are available: “LACP” and “Static”.

Static: The traffic is transmitted on one of the links in the group. The link is determined by the MAC Address in the frame header. If the link is broken, the traffic cannot transmit on the other links in the group.

LACP: It is also known as “Dynamic” trunking. If the current transmitting link is broken, the traffic can be transmitted on another link in the group.

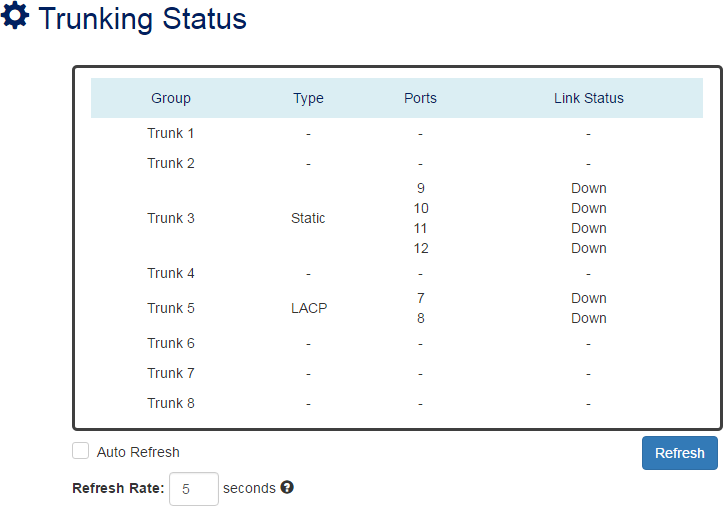
#### Member Ports

Select member ports to be joined in the specified Trunk group. A port can only be in one of the Trunk group. Each Trunk group supports maximum 8 member per ports.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

### PORT TRUNK STATUS



#### Group

The supported trunk groups are from **Trunk 1** to **Trunk 8**.

#### Type

The trunk mode set for this group may be “**LACP**” or “**Static**”. This field displays “-“ if no members are in the group.

#### Ports

The selected member ports in the group will be displayed in this column.

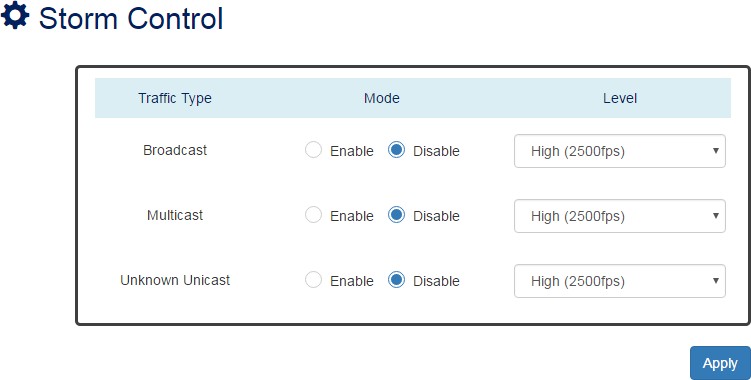
#### Link Status

This field displays the link state (Up or Down) for the specific port.

# Storm Control

A traffic storm happens when there is excessive packets **flood** to the LAN and decreases the performance. The **Storm Control** function is used to prevent the system from breaking down by the broadcast, multicast, or unknown unicast traffic storm. When the **Storm Control** is enabled on the specific traffic type, the system will monitor the incoming traffic. If the traffic is more than the configured level, the traffic will be dropped to avoid the storm.

### CONFIGURE STORM CONTROL INFORMATION



#### Traffic Type

Three types of traffics are supported in the Storm Control: **Broadcast**, **Multicast**, and

**Unknown Unicast**.

* + - **Mode**

“Enable” or “Disable” Storm Control function in the specific traffic type.

#### Level

Three frame levels are available: **High**, **Middle**, and **Low**. If the frames of specific traffic type are more than the set level, the system will drop the type of frames to prevent the system from breaking down.

High: More than 2500 frame per second. Mid: More than 1000 frame per second. Low: More than 500 frame per second.

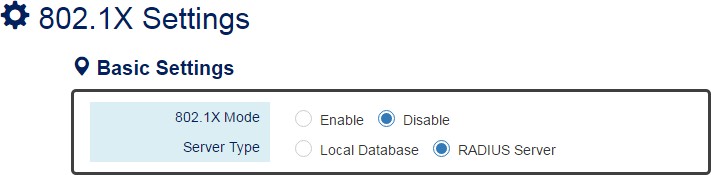
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# 802.1X Settings

802.1X is an **IEEE** standard defined **Port-based Network Access Control**. It provides a more secured authentication mechanism for the devices, which would like to connect to a LAN or a WAN. The **Port-based** Network Access Control protocol is a convenient method for the users because the authentication is per-port and once the port passes the authentication, it is not required to authenticate again when changing to another device, i.e., without security. Therefore, **MAC-based** access control is provided. It is a more secure, but less convenient method for authentication. Only the device with the MAC Address that has passed the authentication can be added to the networks. These two methods are optional on each port and the users can select one of them on different ports.

**CONFIGURE 802.1X BASIC INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Basic Settings

* + - * 802.1X Mode

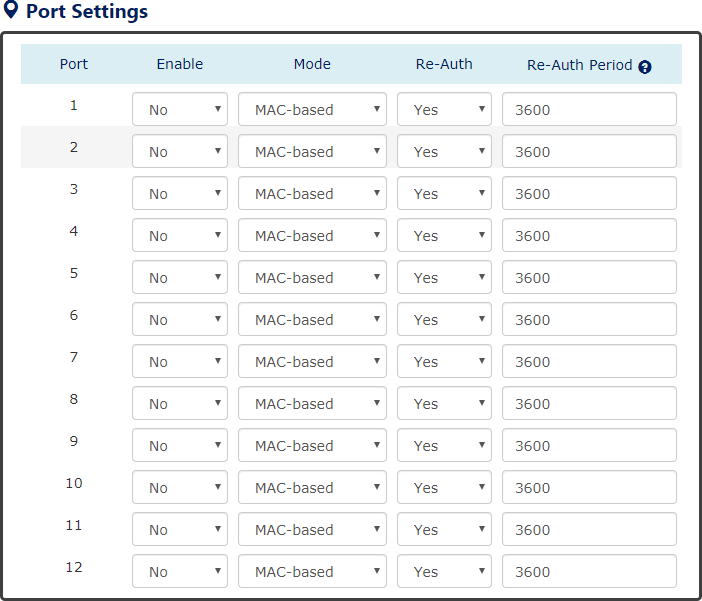
“Enable” or “Disable” 802.1X function on the switch.

* + - * Server Type

Select the 802.1X server type to “Local Database” or “RADIUS Server”.

Local Database: The database is maintained in a table stored in the switch. The client must send the username and password to authenticate with the switch’s database. RADIUS Server: The database is maintained in other devices running RADIUS service. The authentication follows the RADIUS protocol including communication and encryption.

**CONFIGURE 802.1X PORT INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Port Settings

* + - * Port

Port1 to PortN, where N is based on the total port number.

* + - * Enable

“Enable” or “Disable” 802.1X function on the port. “Yes” means 802.1X is enabled on the port and the port is locked until it passes the authentication.

* + - * Mode

Select the 802.1X mode to “Mac-based” or “Port-based”.

Mac-based: Only the MAC Address, which passed the authentication can connect to the networks.

Port-based: If the port had passed the authentication, every device connected to the port can connect to the networks.

* Re-Auth

“Enable” or “Disable” re-authentication on the port. “Yes” means re-authentication is enabled on the port and the port must re-authenticate with the server every re-auth period.

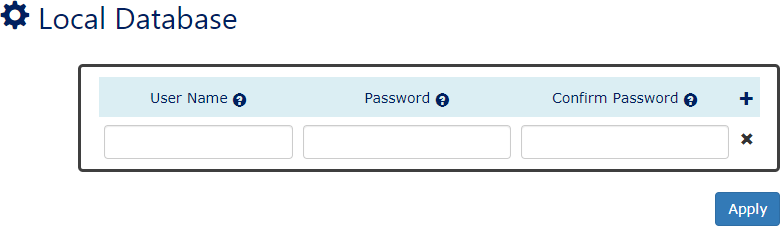
* Re-Auth Period

This is a time interval, which is used in re-authenticating the server.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE LOCAL DATABASE INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Username

The Username is used in authentication.

The **max. length** for the Username is **32 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

#### Password

The Password is used in authentication.

The **max. length** for the Password is **20 characters**. **Note: #, \, ', ", ?** are **invalid** characters.

#### Confirm Password

The Confirm Password field must be the same as Password field.

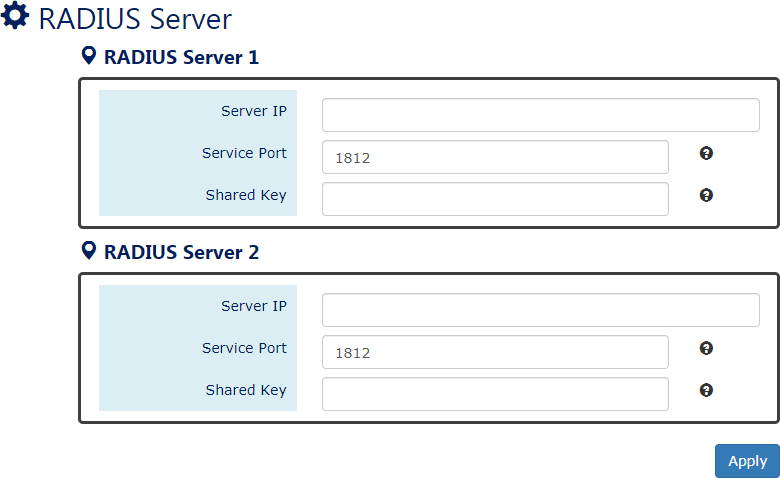
 : Click the **plus icon** to add a Username/Password row.

 : Click the **remove icon** to delete the Username/Password row.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE RADIUS SERVER INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Server IP

The Server IP is the IP address of the server.

#### Service Port

The Service Port is the listening port on the RADIUS server.

#### Shared Key

The key is used in establishing the connection between the server and the authenticator before authentication.

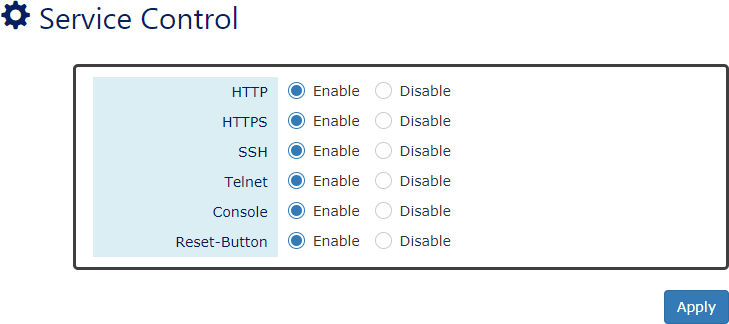
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# Service Control

We provide 5 types of interface which are **HTTP**, **HTTPS**, **SSH**, **Telnet**, and **Console Port** to access the management interface of the switch. Users can configure the authority for each type of service to be enabled or disabled. **Reset Button** is another method to reboot or reset factory default. We also provide the configuration for the Reset Button to enable or disable its function. All the services are enabled by default and users can disable unused service to make the system more secure.

### CONFIGURE SERVICE CONTROL INFORMATION



#### HTTP

Enable or Disable to access management interface by **HTTP** which is the foundation of data communication for the **World Wide Web** (**WWW**).

#### HTTPS

Enable or Disable to access management interface by **HTTPS** which is an adaptation of HTTP for security. The communication will be **encrypted** in HTTPS.

#### SSH

Enable or Disable to access management interface by **SSH,** which is a **cryptographic network** protocol. SSH provides a **secure channel** over an unsecured network in the client-server architecture. The switch plays the role of SSH server and hosts plays the role of SSH client.

#### Telnet

Enable or Disable to access management interface by **Telnet** which is a **text-oriented** virtual terminal connection. It is less secure than SSH because it does not encrypt any data even password when the data is transmitting.

#### Console

Enable or Disable to access management interface by **Serial Console Port**. Disable the Console Port can avoid the misconfiguration by someone who can access the device on-site.

#### Reset Button

Enable or Disable to react when users press the **Reset Button**. The Reset Button provides different functions including reboot and reset factory default. Disable Reset Button is a protection from mistaking the button to reboot the system or restore the system to default state.

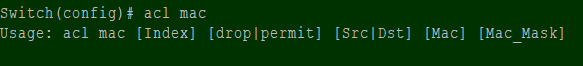
  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

# Access Control List

An access control list provides rules to apply all network ports. The inbound traffic checked the entries in the ACL table. Each entry can be the MAC entry for layer 2 address and IP entry for the layer 3 address. And it can check the source address or destination address. User can adjust the address mask to provide the group setting in one entry. Entry have two actions that can permit or deny network packet transmitting to another port.

### CONFIGURE ACCESS CONTROL LIST



#### Index

Entry number in the ACL table. Traffic packet will be checked with the index sequence.

#### Action

**Drop:** Packet will be discarded if it hit the address rule.

**Permit:** Packet will be forwarded if it hit the address rule.

#### Address Type

**Src:** Address rule bases on the source address

**Dst:** Address rule bases on the destination address

#### Address

MAC address with byte colon format. For example: 00:80:C2:01:23:45

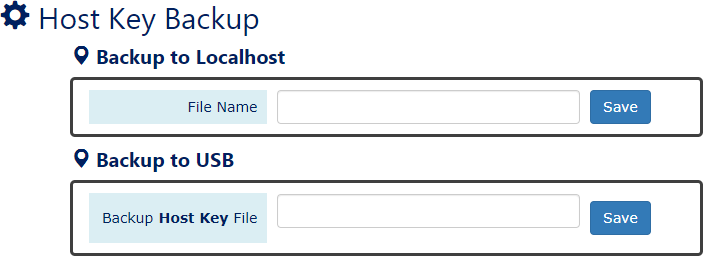
#### Address Mask

Bit mask for address with byte colon. Bit 1 is checking in rule. Otherwise bit 0 is excluded in the checking rule.

# SSH

To reduce the steps for login the system via **SSH** connection, the **public/private key** pair is a good choice for users. The pair of keys is created on the local device and users must provide the public key to the target device, for example, the Ethernet switch. When users connect to the target device, the system creates a safe connection by SSH. The localhost and target device **authenticates** each other with the public and private keys to make sure the security.

### BACKUP HOST KEY FILE



#### Backup to Localhost

* + - * File Name

Specify the File Name for the **SSH Host Key** file, which will be saved to the localhost.

#### Backup to USB

Ensure there is a **USB stick** inserted into the USB port.

* + - * Backup **Host Key** File

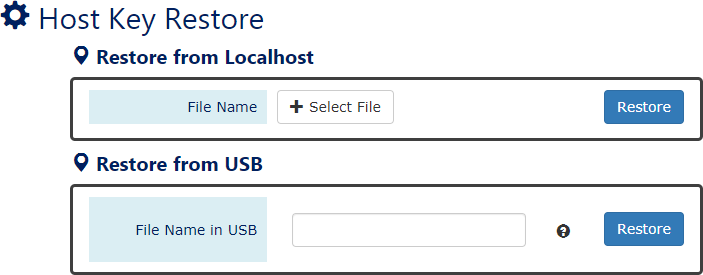
Specify the File Name for the saved **SSH Host Key** file, which will be saved to the USB.

**Note**: The file system of USB must be FAT32.

  (Save Button)

Click the "Save" button to save the configuration file to the **Localhost** or **USB**.

### RESTORE HOST KEY FILE



#### Restore from Localhost

* + - * File Name

Select the **SSH Host Key** file, which is saved in the Localhost.

#### Restore from USB

Please ensure there is a **USB stick** inserted into the USB port.

* + - * File Name in USB

The File Name of the saved **SSH Host Key** file, which is saved to the USB. If the configuration file is saved in the directory, please specify the **full path**.

**Note**: The file system of USB must be FAT32.

  (Restore Button)

Click the "Restore" button to restore the **SSH Host Key** from the **Localhost** or **USB**.

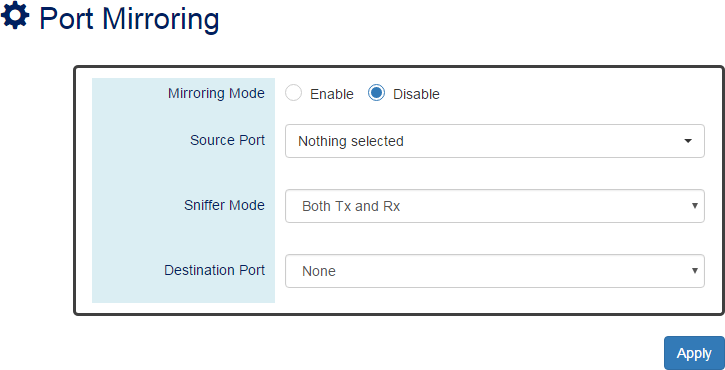
### HOST KEY INFORMATION

The current **SSH Host Key** is displayed in the “**SSH Host Key**” page. The system only accept one SSH Host Key, once users restore another Host Key, the current Host Key will be replaced.

# Port Mirroring

**Port Mirroring** is a feature that copies the incoming or outgoing packets on one or more ports to another destination port. It is especially useful to monitor the network traffic and analyze the copied traffic. **Port Mirroring** helps network management to keep a close eye on the network and debug when some issues arise.

### CONFIGURE PORT MIRRORING INFORMATION



#### Mirroring Mode

“Enable” or “Disable” the Port Mirroring function. If the user enables Port Mirroring function, the system will transmit the traffic of the specific “Sniffer Mode” from “Source Port” to “Destination Port”.

#### Source Port

The traffic on the Source Ports will be sniffed to the Destination Port.

#### Sniffer Mode

Both Tx and Rx: Sniffs both transmitting and receiving traffics. Tx Only: Sniffs only the transmitting traffic.

Rx Only: Sniffs only the receiving traffic.

#### Destination Port

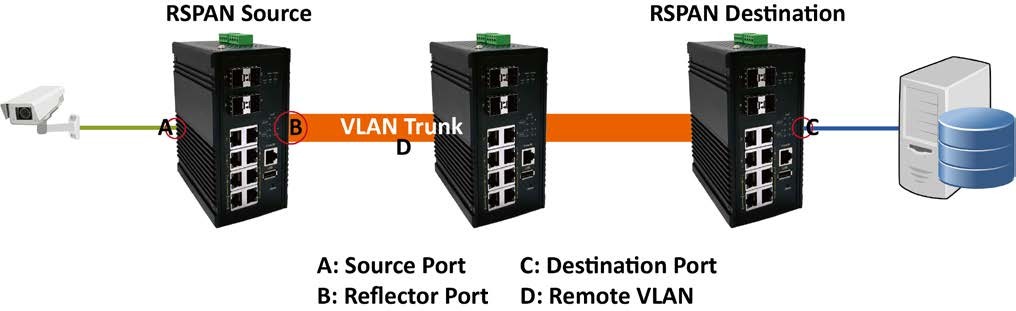
The traffic will sniff to the Destination Port. This port is usually connected to a host running the software to observe the packets.

  (Apply Button)

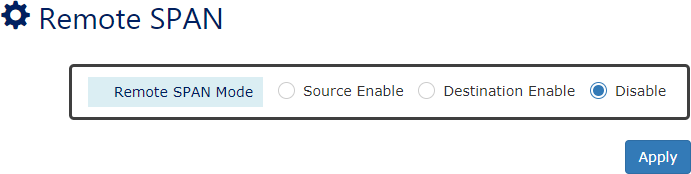
After configuring above fields, click "**Apply**" button to make the changes effective.

# Remote SPAN (RSPAN)

**Switch Port ANalyzer** (**SPAN**) provides efficient, high performance traffic monitoring. It duplicates network traffic from a configured interface to another designated interface on the switch. **SPAN** is used for connectivity troubleshooting and for network performance utilization.

An extension of SPAN called **Remote SPAN** or **RSPAN** allows users to monitor traffic from source ports distributed over multiple switches. In other words, users can centralize the network capture devices. **RSPAN** operates by mirroring the traffic from a source port of an RSPAN session on a VLAN. The VLAN is connected to other switches via trunked mode, allowing the traffic on the RSPAN session to be transported across multiple switches. On the switch that contains the destination port for the RSPAN session, the traffic from the VLAN of RSPAN session is simply mirrored out the destination port.

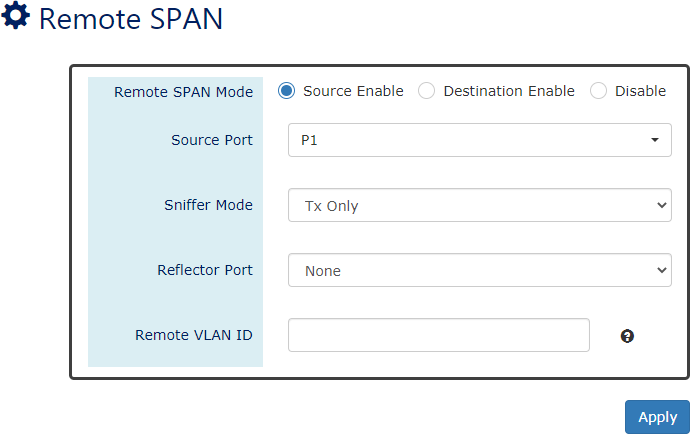
**CONFIGURE REMOTE SPAN INFORMATION**

The RSPN is default disabled. The switch provides Source Mode and Destination Mode. Users can select the mode according to their application.

#### Remote SPAN Mode

“Enable” RSPAN on the Source Mode or Destination Mode or “Disable” RSPAN function.

**CONFIGURE REMOTE SPAN SOURCE MODE**



***For more information, hover the mouse over the icon in the system.***

#### Source Port

The traffic through the Source Port will be mirrored to remote devices.

#### Sniffer Mode

Select the traffic type, **Tx** or **Rx**, to mirror.

#### Reflector Port

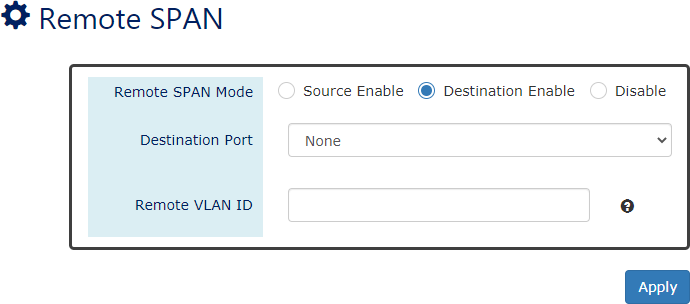
To optimize the utilization of switch interfaces, the Reflector Port on our switches is designed to copy packets from the RSPAN Source Port and forward the copied packets out like an uplink port.

#### Remote VLAN ID

The configured Remote VLAN ID will be the RSPAN session and used to transmit RSPAN traffic. The Remote VLAN ID configured on the RSPAN Source and Destination must be the same one.

The range of the Remote VLAN ID is from VLAN **2 to 1001** and VLAN **1006 to 4094**. VLAN 1 and VLAN 1002 to 1005 are reserved VLANs.

**CONFIGURE REMOTE SPAN DESTINATION MODE**



***For more information, hover the mouse over the icon in the system.***

#### Destination Port

The copied traffic will be forwarded to this Destination Port.

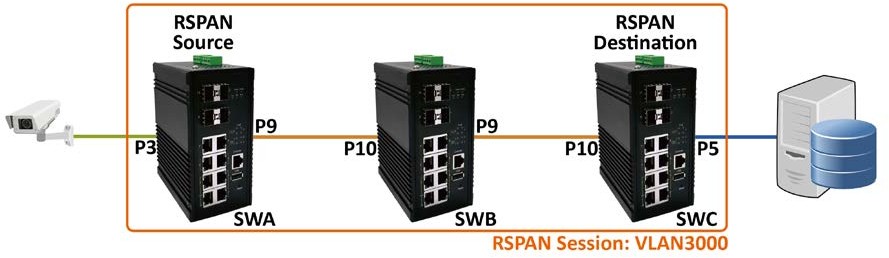
#### Remote VLAN ID

The configured Remote VLAN ID will be the RSPAN session and used to transmit RSPAN traffic. The Remote VLAN ID configured on the RSPAN Source and Destination must be the same one.

The range of the Remote VLAN ID is from VLAN **2 to 1001** and VLAN **1006 to 4094**. VLAN 1 and VLAN 1002 to 1005 are reserved VLANs.

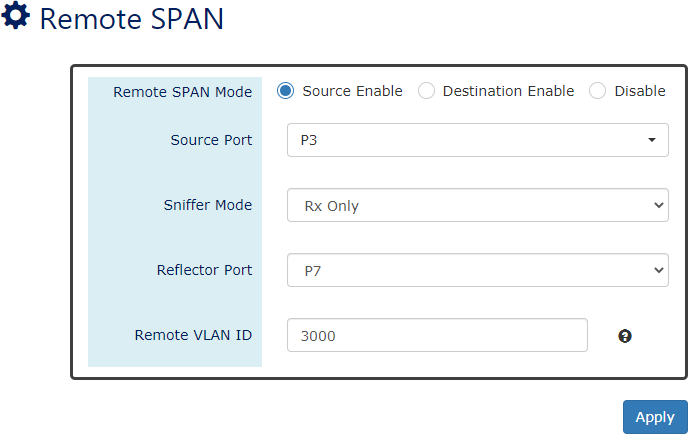
**CONFIGURATION EXAMPLE FOR RSPAN**

In the following diagram, the **SWA** is the **RSPAN Source**, and the **SWC** is the **RSPAN Destination.** Between SWA and SWC, there is a SWB which is a normal switch. We are going to monitor the traffic from the IP Camera on the left side to the Server on the right side.

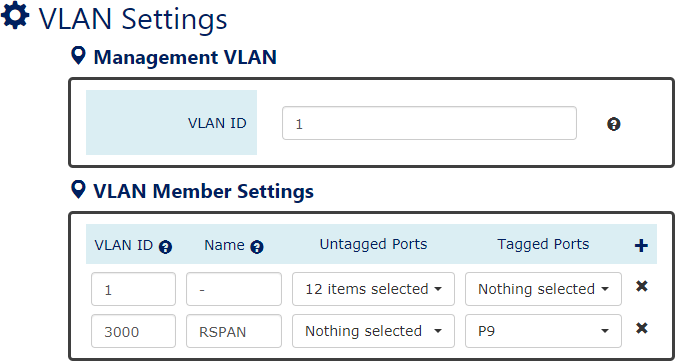


**Step-by-step Configuration**

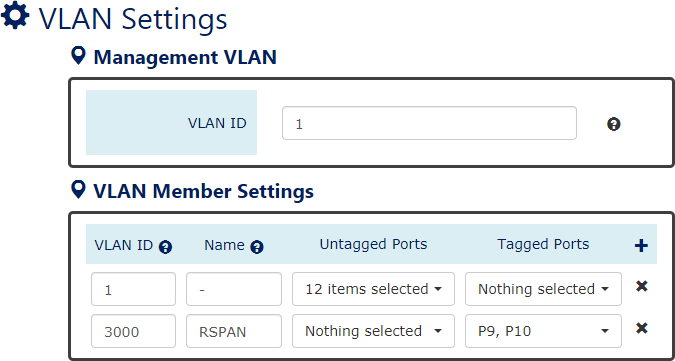
1. Login Web Console and click menu “*Diagnostics*” -> “Remote SPAN”
2. Configure for **SWA**
   1. Click “**Source Enable**” and there will show other related configuration items.
   2. Select the Source Port (**Port 3**) that will be monitored.
   3. Select the **Sniffer Mode**, normally called traffic type. For this example, we want to monitor the traffic from the IP Camera, so we must select “**Rx**”.
   4. Select the **Reflector Port** which will forward the copied traffic to the destination. On the SWA, **Port 9** is the Uplink and Reflector Port.
   5. Decide the **Remote VLAN ID** for **RSPAN Session**; the copied traffic will be transmitted through this VLAN trunk. We use **VLAN 3000** on this example.
   6. Click “**Apply**” button to effect RSPAN configurations.



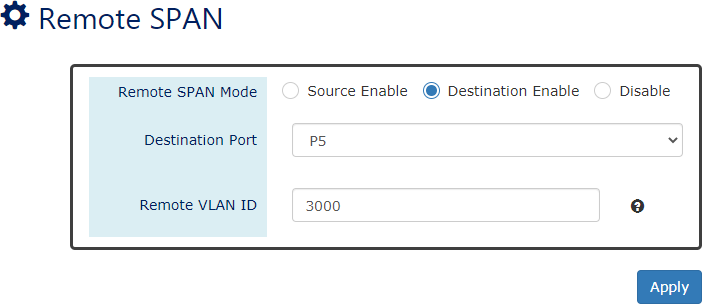
* 1. Configure uplink port (**Port 9**) to **tagged** member on **VLAN 3000**.
  2. Click “**Apply**” button on the bottom of the page to make the VLAN effective.



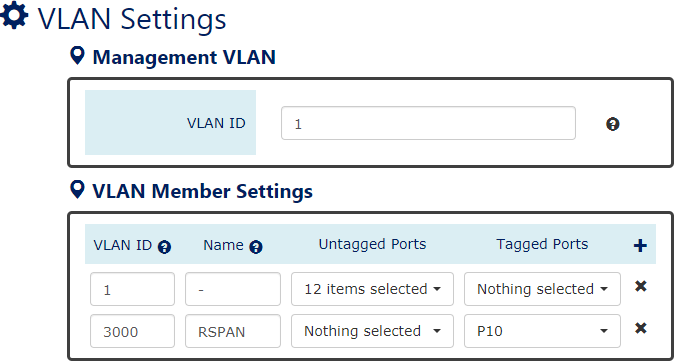
1. Configure for **SWB**
   1. Configure the ports (**Port 9** and **Port 10**) connected with SWA and SWC to tagged members on **VLAN 3000**.
   2. Click “**Apply**” button on the bottom of the page to make the VLAN effective.



1. Configure for **SWC**
   1. Click “**Destination Enable**” and there will show other related configuration items.
   2. Select the Destination Port (**Port 5**) that the copied traffic will be transmitted to.
   3. Configure the **Remote VLAN ID** to **VLAN 3000** for **RSPAN Session**.
   4. Click “**Apply**” button to effect RSPAN configurations.



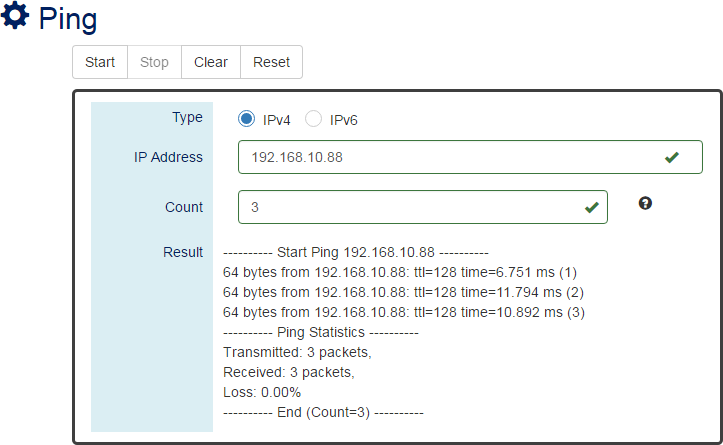
* 1. Configure uplink port (**Port 10**) to **tagged** member on **VLAN 3000**.
  2. Click “**Apply**” button on the bottom of the page to make the VLAN effective.



# Ping

**Ping** is a tool used to test the reachability of a device on the IP network. Ping is enabled by sending **Internet Control Message Protocol** (**ICMP**) request to the target device and waits for the response packet from the target device to check the connection.

**PING ANOTHER DEVICE WITH IPV4/IPV6**



#### Type

***For more information, hover the mouse over the icon in the system.***

Ping a connected device with “**IPv4**” or “**IPv6**” protocol.

#### IP Address

The IP address of the connected device is verified based on the type.

#### Count

Sets the count times. The system will send “Count” number ICMP packets to the specific IP address and wait for the response.

The range of the Count is **from 3 to 50**. The default Count is **3**.

#### Result

The result of the ping shows the response from the specific IP address. If the specific IP address does not respond, it displays No Response.

#### “Start” Button

Click the “Start” Button to start the ping to the IP address.

#### “Stop” Button

Click the “Stop” Button to stop the ping to the IP address before the count is completed.

#### “Clear” Button

Click the “Clear” Button to clear the “Result”.

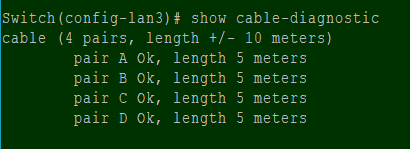
#### “Reset” Button

Click the “Reset” Button to clear the “Result” and reset the “IP Address” and “Count” number.

# Cable Diagnostics

This command can check the status of copper cables with the time domain reflectometer (TDR) technology. It can detect a cable fault by sending a detect signal and read the reflecting back. With this test, it can help to identify and narrow down the physical level issue.

### DISPLAY CABLE DIAGNOSTIC



#### Port Selector

Select the port number to test.

Port 1 to N, where N is based on the total port number.

#### Cable status

The status of cable. It contains the number of pairs in the cable and the error amount.

Usually there are 4 pair in the CAT-5E cable for Gigabit Ethernet link.

#### Pair status

The status of each pair of port. ‘Ok’ status means cable is connected to another node. ‘Open’ status means cable does not connect to any device.

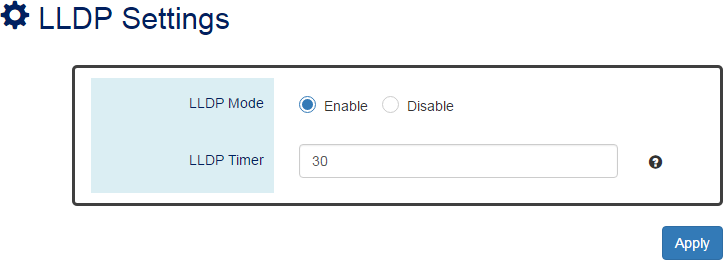
#### Length

The length of each pair of port in meters. Please note the error amount is around 10 meters due to the TDR technology. The short cable less than the error amount might be untastable.

# LLDP

**LLDP** is **Link Layer Discovery Protocol** and it is a vendor-neutral layer 2 protocol that is defined by **IEEE 802.1AB**. **LLDP** is used in advertising identity of the devices, capabilities, and neighbors on the LAN. The information from the neighbors enables the switch to quickly identify the devices and interoperate with each other more smoothly and efficiently. The neighbor table shows the information about the device that is next to the port. The LLDP can only get information from the device that is close to it. If the users want to know the topology of the LAN, they can collect all information from the device and analysis the neighbor table.

**CONFIGURE LLDP INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### LLDP Mode

“Enable” or “Disable” the LLDP function.

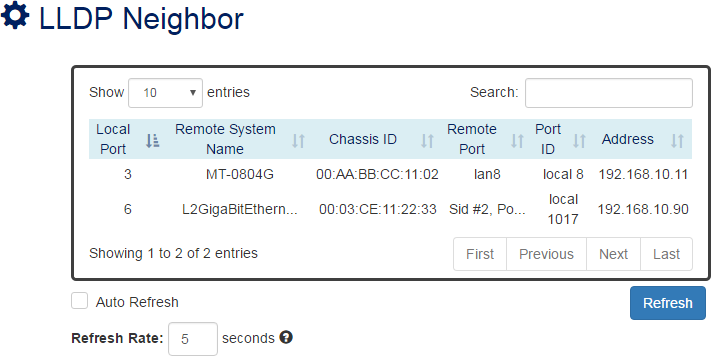
#### LLDP Timer

The LLDP Timer is a time interval to send LLDP messages. The range of the LLDP Timer is **from 5 to 32767** seconds. The default LLDP Timer is **30** seconds.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**LLDP NEIGHBOR TABLE**



#### Local Port

The port connected to the LLDP neighbor on the local switch.

#### Remote System Name

This is the system name of the LLDP neighbor. This value is set and provided by the remote device.

#### Chassis ID

The Chassis ID defines the **MAC Address** of the LLDP neighbor.

#### Remote Port

This field displays the **port information** received from the LLDP neighbor.

#### Port ID

The Port ID displays the **port identity** of the connected port on the LLDP neighbor.

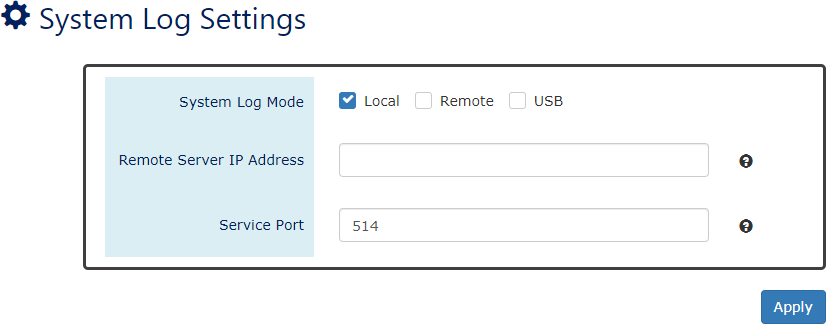
#### Address

The Address displays the **IP address** of the LLDP neighbor.

# System Warning

**System Warning** contains “System Event Log”, “SMTP Settings”, and “Event Selection” for different types of services such as “Fault Alarm”, “System Log”, “SMTP”, and “SNMP Trap”. These logs are especially useful for the administrator to manage and debug the system. When the system is powered off or when someone tries to login the system or the system reboots abnormally, or when some of the interfaces are linked down, the system sends log messages to notify specific users and record the events on the server or assigned platform. Users can also connect an alarm buzzer to the relay alarm pins. When the configured “Fault Alarm” events are triggered, the alarm buzzer will ring to notify the users.

### CONFIGURE SYSTEM WARNING INFORMATION



***For more information, hover the mouse over the icon in the system.***

#### System Log Mode

* + - Select the checkbox to send system log to Local (Switch), Remote, or USB when events happened.

#### Remote Server IP Address

The field contains the IP Address of the remote server. If the “**Remote**” mode is enabled, users must assign this IP Address to receive the system logs. The system supports both **IPv4** and **IPv6** addresses for the remote server.

#### Service Port

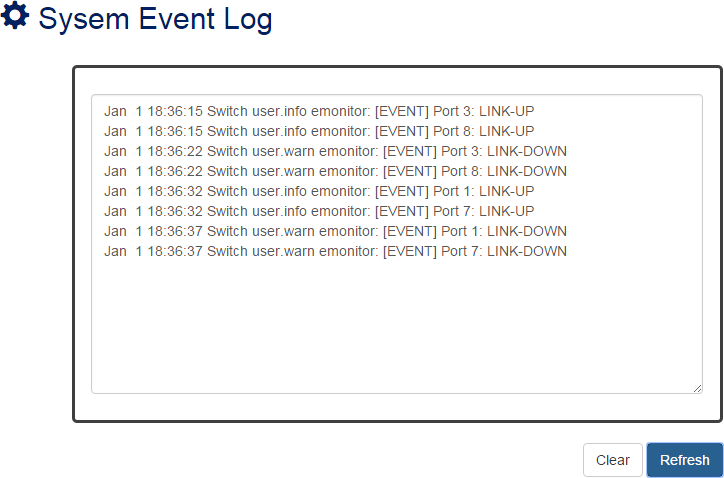
The port is used to listen to the system log packets on the remote server. The range of the Service Port is **from 1 to 65535**.

The default Service Port is **514**.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

### SYSTEM EVENT LOG



#### Log Text Area

The system event information displays if the “**Local**” system log mode is enabled and the configured events are triggered.

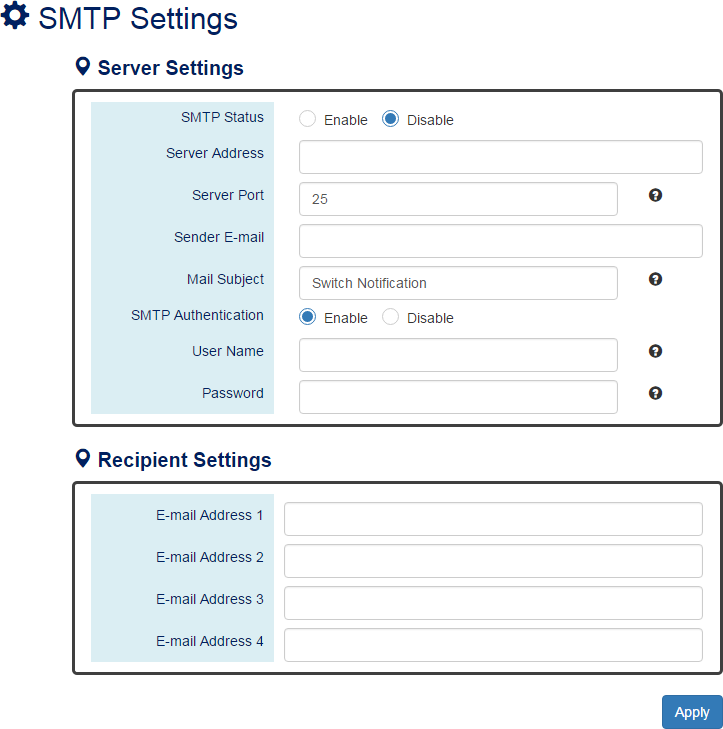
  (Clear Button)

Click the “Clear” button to clear the system event log in the text area.

  (Refresh Button)

Click the “Refresh” button to refresh the system event log in the text area.

**CONFIGURE SMTP INFORMATION**



***For more information, hover the mouse over the icon in the system.***

#### Server Settings

* + - * SMTP Status

“Enable” or “Disable” the SMTP function.

* + - * Server Address

This is the **IP address** or **URL** of the SMTP Server. For example, the SMTP server address provided by Google is “smtp.gmail.com”.

* + - * Server Port

This field is the port listening on the server for the SMTP request. For security, we suggest users configure the server port to **465** for **SSL** or **587** for **TLS**.

The range of the Service Port is **from 1 to 65535**.

The default Service Port is **25**. Port 25 is the default port for e-mail server.

* Sender E-mail

The Sender E-mail is the e-mail address used to send the notifications to Recipients.

* Mail Subject

The Mail Subject is a string that is displayed in the E-mail title.

**Note: #, \, ', ", ?** are **invalid** characters.

* SMTP Authentication

“Enable” or “Disable” to authenticate the SMTP server with the configured username and password.

* Username

The username is used in authentication with the SMTP server. The **max. length** for the Username is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

* Password

The password is used in authentication with the SMTP server. The **max. length** for the Password is **32 characters**.

**Note: #, \, ', ", ?** are **invalid** characters.

#### Recipient Settings

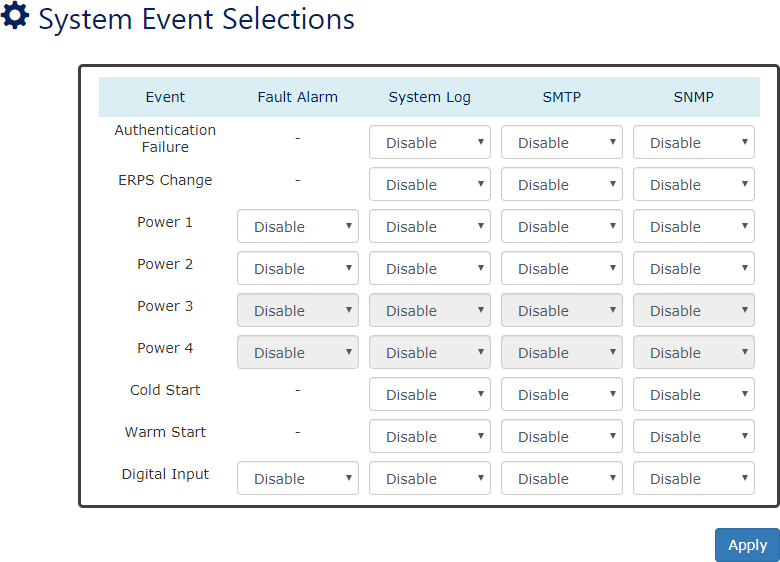
* + - * E-mail Address 1-4

The configured e-mail address will receive the notifications if the SMTP is enabled and the events set on “Event Selection” are triggered.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

### CONFIGURE SYSTEM EVENT SELECTIONS



#### Event

There are 5 events on the System Events.

Authentication Failure: Login failed on the web console or CLI. It may be caused due to incorrect username or password.

ERPS Change: The ERPS function is working and the topology is changed. Power 1 - 4: The power 1 to 4 is powered off.

Cold Start: The system reboots due to interruption of power supply.

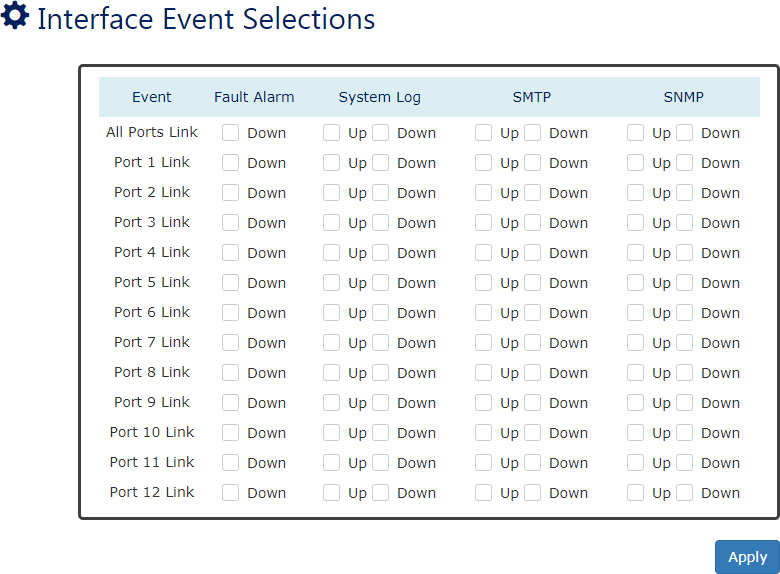
Warm Start: The system reboots by issuing “reboot” command on CLI or clicking the “reboot icon” on the web console.

Digital Input: The signal from the digital input is changed from high to low or low to high.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

### CONFIGURE INTERFACE EVENT SELECTIONS



#### Event

The events on the “Interface Events” display the **link status** for each port. Fault Alarm is triggered only during link down and other system log types support both link up and link down.

#### Fault Alarm

The **Fault LED** will turn on **red** and relay will turn ON, if the configured events are triggered. By default, the Fault LED is **green,** and relay is turned OFF in the normal situation.

#### System Log

When the configured events are triggered, the logs will be displayed in the “System Event Log” page, remote server, or saved to a USB file named “**message**”. This is based on the settings of the “**System Log Mode**” in the “**System Log Settings**” page.

**Note**: The file system of USB must be FAT32.

#### SMTP

If the SMTP is enabled and the configured events are triggered, the system will send an e-mail notification to the e-mail addresses of the assigned recipient set in the “**SNMP Settings**” page.

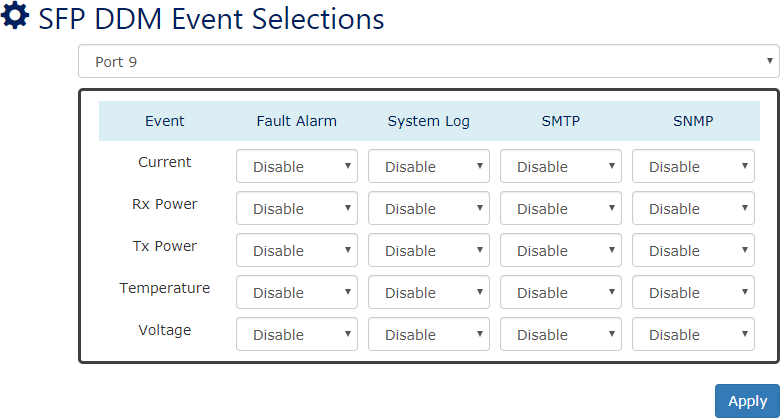
#### SNMP

If the SNMP Trap is enabled and the configured events are triggered, the system will send event information to the assigned “**Trap Receiver IP**”, which is set in the “**SNMP Trap**” page.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE SFP DDM EVENT SELECTIONS**



#### Event

There are 5 events on the “SFP DDM Events”: **Current**, **Rx Power**, **Tx Power**, **Temperature**, and **Voltage**. Enable or Disable the event fault alarm or system warning when the value is higher than the high alarm/warning threshold or the value is lower than the low alarm/warning threshold.

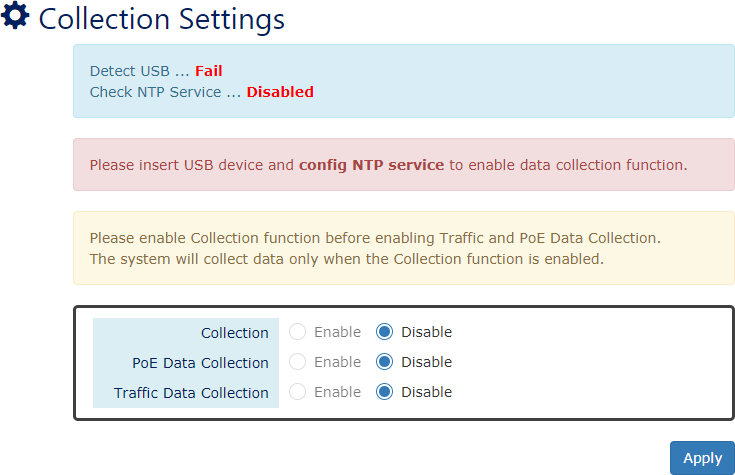
# Data Collection

The health of switch system is especially important in the real application. For most switches, they provide basic real-time traffic and PoE status, but users need the long-time records to analyze and statistic for the system. For this purpose, we implement the Data Collection function to collect traffic and PoE status periodically and save the collected data to the USB device. In addition to this, we also provide charts to display the collected data. Users can easily recognize the situation of the switch system and find the unusual points from the charts.

To ensure the accuracy of the data, the NTP service must be turned on before enable Data Collect function, so that when users find an abnormal record, they can trace it by the recording time. And there is no worry for the size of system storage because the data is saved in the USB. The data even can be move to other devices to display or users can use the collected raw data to do other application.

### CONFIGURE DATA COLLECTION SETTINGS

**USB** and **NTP** are essential before users enable the Data Collection functions. Please check if there is an USB inserted and the NTP service is also enabled. The file system of USB must be FAT32.



#### Collection

“Enable” or “Disable” Data Collection Function on the switch. The Traffic and PoE Data Collection can be enabled only when the Collection is enabled.

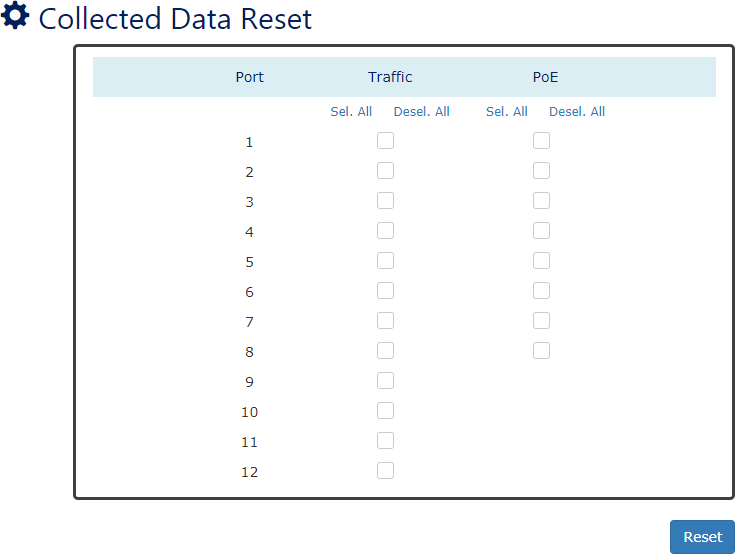
* + - **PoE Data Collection** (PoE Models Only)

“Enable” or “Disable” PoE Data Collection function on the switch.

#### Traffic Data Collection

“Enable” or “Disable” Traffic Data Collection function on the switch.

### RESET COLLECTED DATA



#### Port

Port 1 to Port N, N is based on the total port number.

#### Traffic

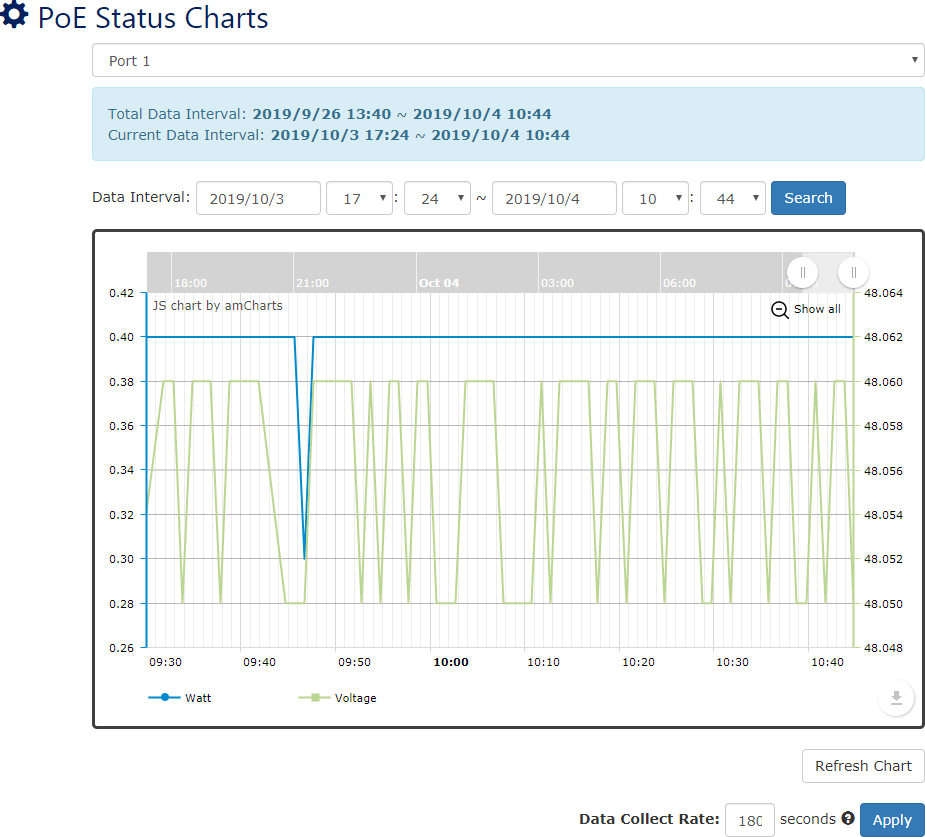
Check the checkbox to reset the data for the designated port. After reset, the collected data will be removed from the USB.

**Note**: It cannot undo after reset, please make sure you want to reset the file.

* + - **PoE** (PoE Models Only)

Port 1 to Port N, N is based on the total port number.

**POE STATUS CHARTS** (PoE Models Only)



***For more information, hover the mouse over the icon in the system.***

#### Port (Drop-down Selector)

Port1 to PortN, where N is based on the total PoE port number. The PoE Status Chart is displayed by port.

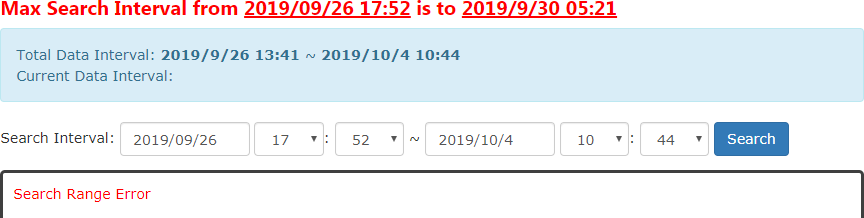
#### Total Data Interval

The interval is the date time from first data to last data that collected in the USB.

#### Current Data Interval

The interval is the date time from first data to last data that displayed on the current chart.

#### Data Interval (Drop-down Selector)

Select an interval to search data. The returned data will be displayed on the chart. The number of data is limited by the system, if the selected interval is larger than the limitation, the system will return an acceptable interval (Shown as the following screenshot).

**Note:** After configuring “Data Interval”, click "**Search**" button to get data in the interval.

#### Chart

The chart displays both watts (blue line) and voltage (green line) data.

#### Refresh Chart (Button)

Press the Refresh Chart button to refresh the chart and get the updated data.

#### Data Collect Rate

The field is the period to collect data. The system will get the real-time data periodically according to the configured Data Collect Rate.

**Note:** PoE Status Charts and Interface Traffic Charts are shared the same Data Collect Rate. The range of the Data Collect Rate is **from 60 to 600** seconds.

The default Data Collect Rate is **180** seconds.

**Note:** After configuring “Data Collect Rate”, click "**Apply**" button to make the changes effective.

### INTERFACE TRAFFIC CHARTS



***For more information, hover the mouse over the icon in the system.***

#### Port (Drop-down Selector)

Port1 to PortN, where N is based on the total switch port number. The Interface Traffic Chart is displayed by port.

#### Total Data Interval

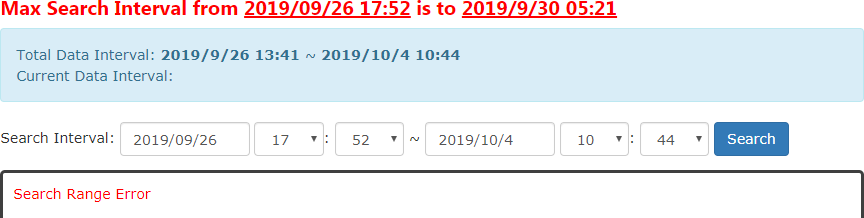
The interval is the date time from first data to last data that collected in the USB.

#### Current Data Interval

The interval is the date time from first data to last data that displayed on the current chart.

#### Data Interval (Drop-down Selector)

Select an interval to search data. The returned data will be displayed on the chart. The number of data is limited by the system, if the selected interval is larger than the limitation, the system will return an acceptable interval (Shown as the following screenshot).



**Note:** After configuring “Data Interval”, click "**Search**" button to get data in the interval.

#### Chart

The chart displays transmitted bytes (blue line) and received bytes (green line) data.

#### Refresh Chart (Button)

Press the Refresh Chart button to refresh the chart and get the updated data.

#### Data Collect Rate

The field is the period to collect data. The system will get the real-time data periodically according to the configured Data Collect Rate.

**Note:** Interface Traffic Charts and PoE Status Charts are shared the same Data Collect Rate. The range of the Data Collect Rate is **from 60 to 600** seconds.

The default Data Collect Rate is **180** seconds.

**Note:** After configuring “Data Collect Rate”, click "**Apply**" button to make the changes effective.

# MAC Table

MAC address is **Media Access Control** address, which is used in layer 2 switching. A **MAC Address table** is maintained by the switch to transmit frames more efficiently. When the switch receives a frame, the system will check the MAC table and forward the frame to the corresponding port. The MAC Address table is built dynamically by the received frames and when the system receives a frame with an unknown MAC address, it **floods** the frame to all LAN ports in the same VLAN. When the destination device replies the system identifies the MAC Address and the target port.

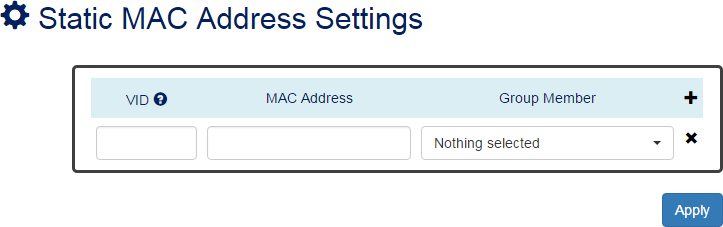
The MAC Address for the switch is designed as per-port-per-MAC, which implies each port has its own MAC Address. This is for MAC sensitive protocols such as Spanning-tree protocol. The MAC Address display on the right side of WEB GUI is the MAC Address for whole system and the MAC Addresses for the ports are increasing by 1 from port 1 to last port.

For example, the MAC Address of the system is 68:02:35:FF:FF:05, and there are 8-port on the switch. The MAC Address for each port will be:

|  |  |  |  |
| --- | --- | --- | --- |
| Port | MAC Address | Port | MAC Address |
| Port 1 | 68:02:35:FF:FF:06 | Port 5 | 68:02:35:FF:FF:0A |
| Port 2 | 68:02:35:FF:FF:07 | Port 6 | 68:02:35:FF:FF:0B |
| Port 3 | 68:02:35:FF:FF:08 | Port 7 | 68:02:35:FF:FF:0C |
| Port 4 | 68:02:35:FF:FF:09 | Port 8 | 68:02:35:FF:FF:0D |

**Note:** The MAC Address is hex format, so the number after “09” is “0A”.

### CONFIGURE STATIC MAC ADDRESS INFORMATION



#### VID

***For more information, hover the mouse over the icon in the system.***

The VID is the VLAN group ID, which contains the configured MAC Address . The range of the VID is **from 1 to 4094**.

#### MAC Address

This field is the static MAC Address of the configured member ports in the VLAN group.

#### Group Member

The Group Member is the port(s) in the VLAN group, to which the configured MAC Address belongs.

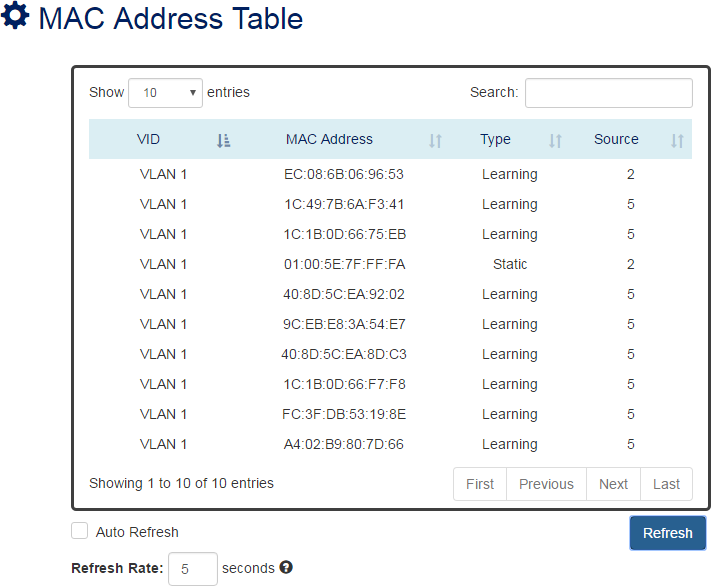
 : Click the **plus icon** to add a static MAC Address row.

 : Click the **remove icon** to delete the static MAC Address row.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**MAC ADDRESS TABLE**



#### VID

The VID is the VLAN group ID, which contains the configured MAC Address.

#### MAC Address

The MAC Address column displays the learnt or configured MAC Addresses.

#### Type

The Type column displays the type (Learning or Static) of the MAC Address. Learning: The MAC address is learnt from the transmitting frames.

Static: The MAC Address is configured by the users or the system.

#### Source

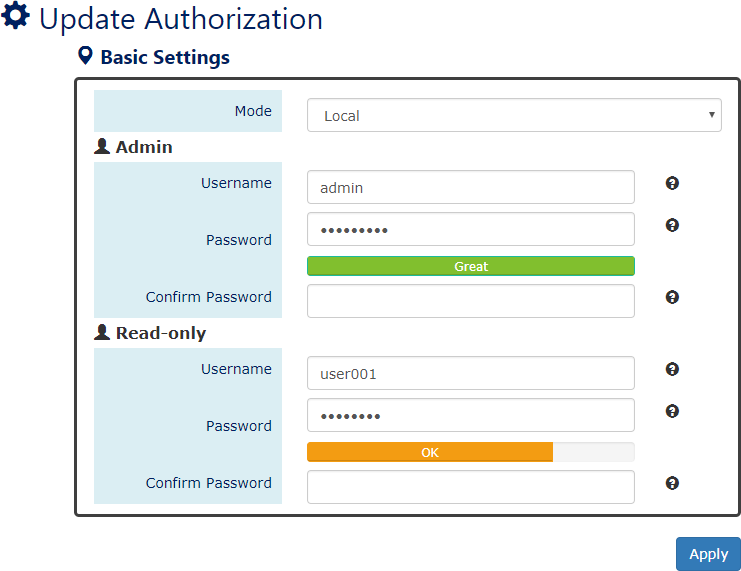
The Source column displays the port(s) to which the MAC Address belong.

# Authorization

The "**Username**" and "**Password**" are particularly important information both in the "**Command Line Interface**" or "**Web Console**". Users have to login into the system before doing any configuration. We strongly suggest the users to change at least the password **for security** when they are going to use this device.

We also provide authentication with **RADIUS**/**TACACS+** server from software **version 1.0.3**. Users can maintain the login information in their own RADIUS/TACACS+ database and allow several usernames/passwords to login the system.

### CONFIGURE LOGIN INFORMATION



#### Mode

***For more information, hover the mouse over the icon in the system.***

There are three modes for login authentication.

Local: The username and password are defined in the system. Currently we support two-level users – **Admin** and **Read-only** user. The Admin can access any page and configure the system but the read-only user can only access status pages.

Radius: The username and password are defined in the **RADIUS server** and when user’s login the system, the system will authenticate with the RADIUS server to get the login permission. The password will be encrypted during the transmitting.

Tacacs+: The username and password are defined in the **TACACS+ server** and when users login the system, the system will authenticate with the TACACS+ server to get the login permission. The whole payload and password will be encrypted during the transmitting.

#### Username

The account used to login to the system.

The maximum length of the Username is **32** characters Only **alphabet** (A-Z, a-z) and **numbers** (0-9) are allowed. The default Username is **admin**.

#### Password

The password used to login to the system. We provide **password strength** bar for reference. There are 3 levels - **Weak**, **OK**, and **Great**. We strongly recommend users configuring the password to “**Great**” level for security.

The maximum length of the Password is **32** characters.

Only **alphabet** (A-Z, a-z), **numbers** (0-9), and **chars** (**!**,**@**,**%**,**^**,**\***,**(**,**)**) are allowed. The default Password is **admin**.

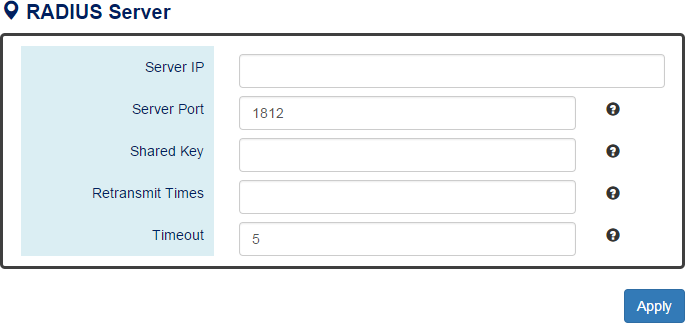
#### Confirm Password

It is used to confirm the value specified by the users in the "Password" field. The value of the field must be the same as "Password".

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE RADIUS SERVER INFORMATION**

This section only display when the mode in the Basic Settings is set to “Radius”.

***For more information, hover the mouse over the icon in the system.***

#### Server IP

The IP address of the RADIUS server must in the same subnet as the IP address of the switch.

#### Server Port

The port is listening to the RADIUS service on the RADIUS server. The range of the Server Port is **from 1 to 65535**.

The default Server Port is **1812**.

#### Shared Key

The Shared Key is a string that used to build the connection with the RADIUS server. It must be the same as the string/secret set in the RADIUS server.

The maximum length of the Shared Key is **32** characters.

#### Retransmit Times

The password used to login to the system.

The range of the Retransmit Times is **from 1 to 1000**.

#### Timeout

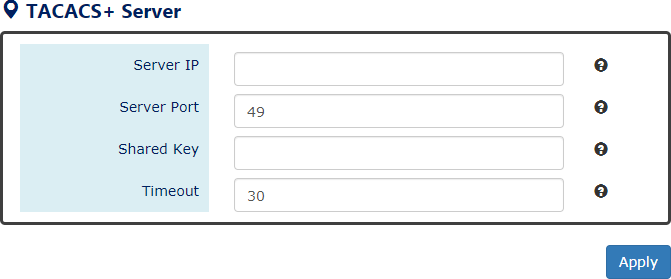
The time interval is used to waiting for the response from the RADIUS server. The range of the Timeout is **from 1 to 1000** seconds.

The default Timeout is **5** seconds.

  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

**CONFIGURE TACACS+ SERVER INFORMATION**

This section only display when the mode in the Basic Settings is set to “Tacacs+”.

***For more information, hover the mouse over the icon in the system.***

#### Server IP

The IP address of the TACSCS+ server must in the same subnet as the IP address of the switch. The system supports both **IPv4** and **IPv6** addresses for the TACACS+ server.

#### Server Port

The port is listening to the TACSCS+ service on the TACSCS+ server. The range of the Server Port is **from 1 to 65535**.

The default Server Port is **49**.

#### Shared Key

The Shared Key is a string that used to build the connection with the TACSCS+ server. It must be the same as the string/secret set in the TACSCS+ server.

The maximum length of the Shared Key is **32** characters.

#### Timeout

The time interval is used to waiting for the response from the TACSCS+ server. The range of the Timeout is **from 1 to 1000** seconds.

The default Timeout is **30** seconds.

  (Apply Button)

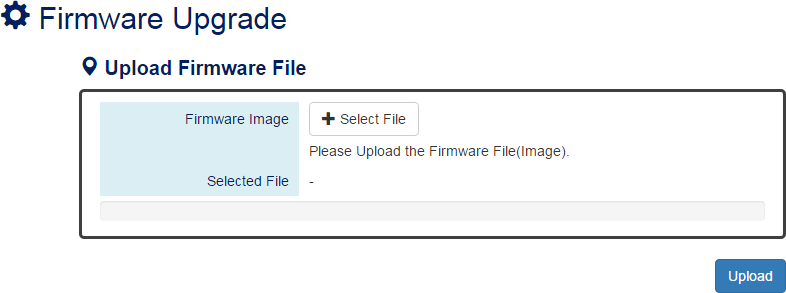
After configuring above fields, click "**Apply**" button to make the changes effective.

# Firmware Upgrade

For a better performance and wider industrial applications, we constantly develop new features and revise the issues from the users. We suggest the users to upgrade the system to the newest firmware version to have a better user experience.

We provide 2 ways to upgrade the firmware from the Web Console, - one is saving the firmware file in the USB stick and another one is to save the firmware file on the PC. If the firmware file is on the PC, the users will have to only **select the file** and click **Apply** button, for the system to upgrade it automatically.

### UPGRADE FIRMWARE VERSION - UPLOAD FIRMWARE FILE



#### Firmware Image

Click the "**Select File**" button to select the firmware image provided by the sales or support. The **Firmware Version** displayed on the system can be customized by the **file name**. For example, if you want the version to be called as 1.2.3, you only need to modify the file name to XXX**-v1.2.3** (XXX is the original file name).

#### Selected File

After selecting a firmware image to be uploaded, the **selected file name** will be displayed in this field.

  (Upload Button)

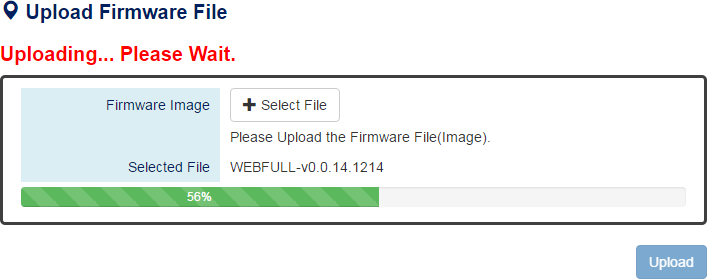
After selecting the firmware image, click "Upload" button to upload it.

### UPGRADE FIRMWARE PROCESS - UPLOADING FIRMWARE FILE

The following steps are performed when the system starts to upgrade after the "Apply" button is clicked:

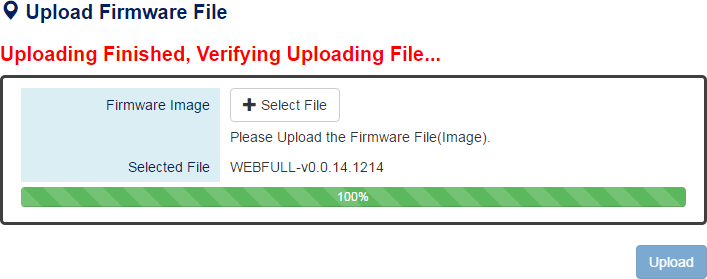
1. **Uploading** the firmware image

The progress bar displays the uploading percentage.



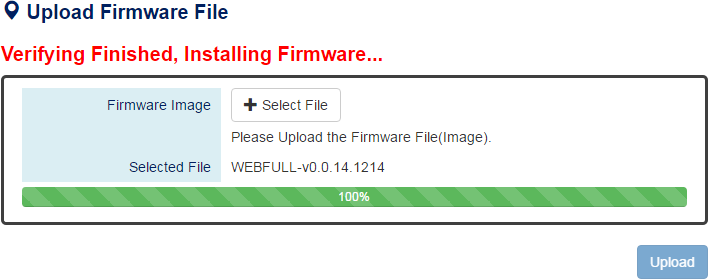
1. **Verifying** the uploaded file

When the file is **100%** uploaded, the system starts to **verify** the uploaded file to make sure it is **valid**. By default, the firmware image is encrypted to prevent the attack on man-in-the-middle. Optionally, higher encryption methodology is also provided.



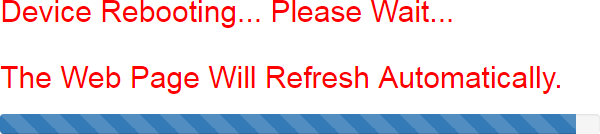
1. **Installing** the uploaded firmware image

The new firmware will install after the system validates it.

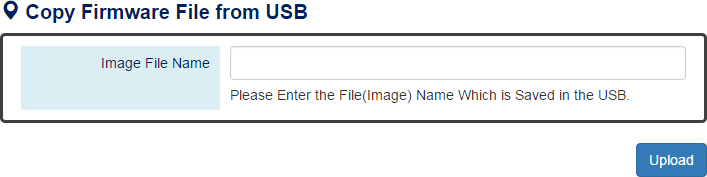


1. **Rebooting** the system

The system will reboot automatically if the firmware is upgraded without any issue. The progress bar displays the rebooting progress.



**UPGRADE FIRMWARE VERSION - COPY FIRMWARE FILE FROM USB**



#### Image File Name

Enter the name of the firmware image in the USB. The system will try to identify the file with specified file name to upload it to the system.

**Note**: The file system of USB must be FAT32.

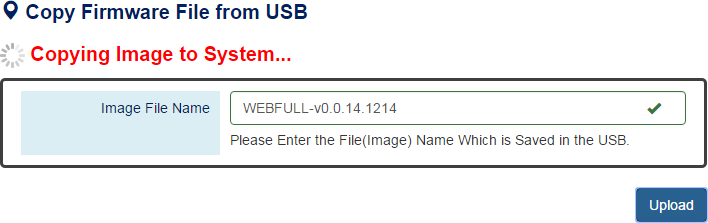
  (Upload Button)

After entering the firmware image name, click "Upload" button to copy it from the USB to the system.

**UPGRADE FIRMWARE PROCESS - COPY FIRMWARE FILE FROM USB**

1. **Copying** the firmware image from USB to switch

The system will also check if the USB is inserted and file exists.

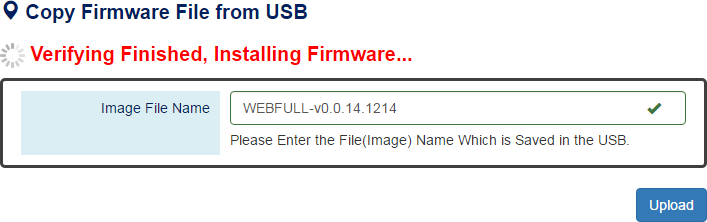


1. **Verifying** the uploaded file

After copying the firmware file to switch, the system starts to **verify** the uploaded file to make sure it is **valid**. By default, the firmware image is encrypted to prevent the attack on man-in-the-middle. Optionally, higher encryption methodology is also provided.

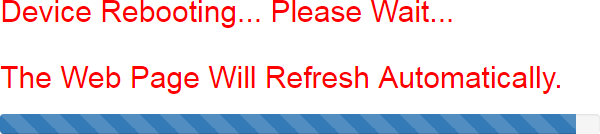
1. **Installing** the uploaded firmware image

The new firmware will install after the system makes sure it is valid.



1. **Rebooting** the system

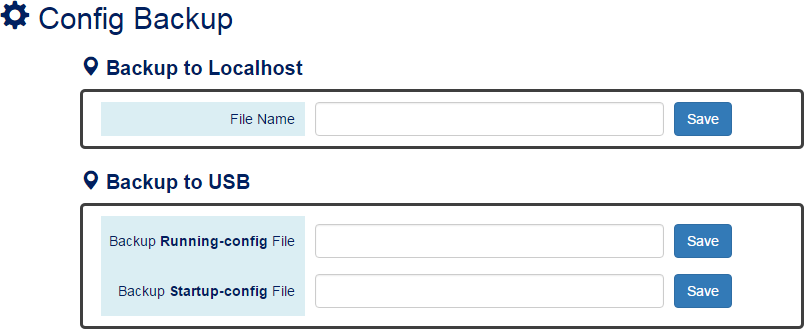
The system will reboot automatically if the firmware is upgraded without any issue. The progress bar displays the rebooting progress.



# Config Backup

Under normal application circumstances, there are several switches in the Network, and they may be configured with the same features. To facilitate this, the users can configure one of the switches and save the configuration file to localhost (for example: users' PC) or USB sticks and then restore the configurations on another switch via "**Config Restore**" function. Configuration files on the USB thumb drive can also provide a way for fast replacement of the device when it is damaged.

### BACKUP CONFIGURATION FILE



#### Backup to Localhost

* + File Name

Specify the File Name for the **Startup-config** file, which will be saved to the localhost.

#### Backup to USB

Ensure there is a **USB stick** inserted into the USB port.

* + Backup **Running-config** File

Specify the File Name for the saved **Running-config** file, which will be saved to the USB.

* + Backup **Startup-config** File

Specify the File Name for the saved **Startup-config** file, which will be saved to the USB.

**Note**: The file system of USB must be FAT32.

The “space” is not allowed in the File Name.

  (Save Button)

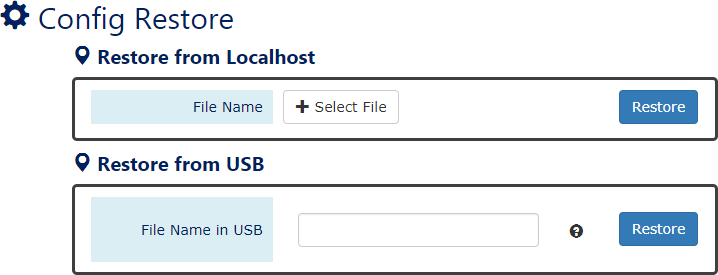
Click the "Save" button to save the configuration file to the **Localhost** or **USB**.

**NOTE:** If the **File Name** filed is empty, the system assigns the default name: ***config-[datetime].cfg***

# Config Restore

We suggest users to save/backup the configurations after a series of settings. If another device needs the same configurations, users can use the **Config Restore** function to restore it.

### RESTORE CONFIGURATION FILE



#### Restore from Localhost

* + File Name

Select the configuration file, which is saved in the Localhost.

#### Restore from USB

Please ensure there is a **USB stick** inserted into the USB port.

* + File Name in USB

The File Name of the saved configuration file, which is saved to the USB. If the configuration file is saved in the directory, please specify the **full path**.

**Note**: The file system of USB must be FAT32.

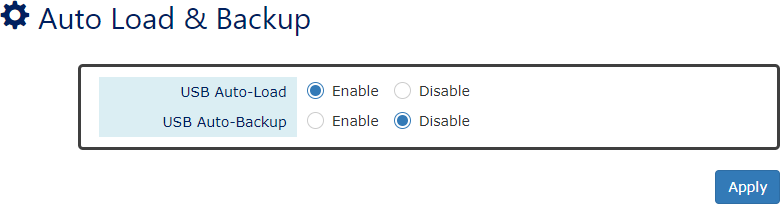
The “space” is not allowed in the File Name.

  (Restore Button)

Click the "Restore" button to restore the configurations from the **Localhost** or **USB**.

# USB Auto-Load & Auto-Backup

**CONFIGURE USB AUTO-LOAD AND AUTO-BACKUP**



#### USB Auto-Load

“Enable” or “Disable” the USB Auto-Load function. If “USB Auto-Load” is **enabled**, the system will search the configuration file named “**startup-config**” in the USB and load it when rebooting.

**Note**: The file system of USB must be FAT32.

#### USB Auto-Backup

“Enable” or “Disable” USB Auto-Backup function. If “USB-Auto-Backup” is **enabled**, the system will save the configurations to a file named “**running-config**” in the USB when users modify the configurations.

**Note**: The file system of USB must be FAT32.

  (Apply Button)

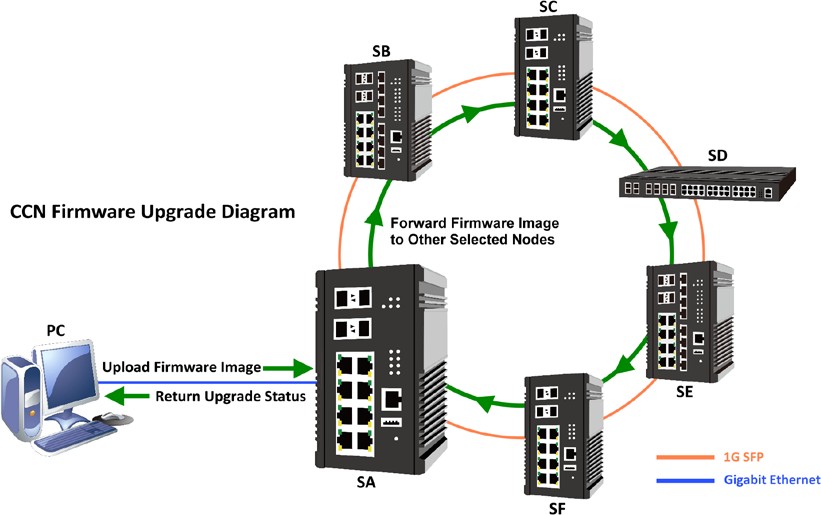
After configuring above fields, click "**Apply**" button to make the changes effective.

# Command & Control Node

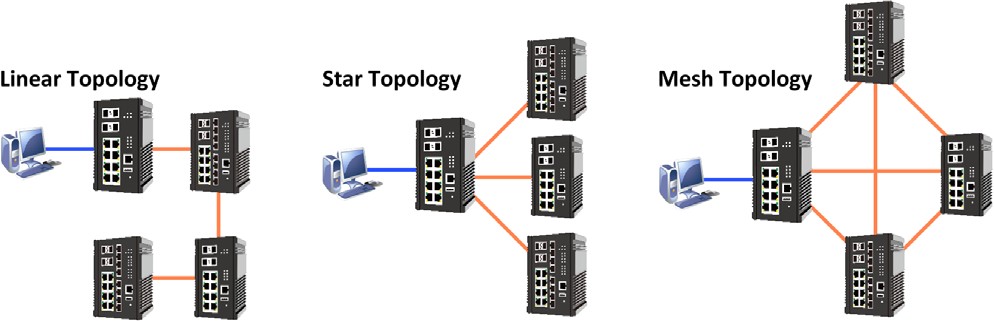
**Command & Control Node** (**CCN**) provides firmware upgrading for batch of switches at once. Currently, the CCN function can upgrade maximum 10 nodes at the same time. With CCN function, administrators can work more efficient and save a lot of time.

The **CCN** function is supported on any kind of topologies, such as ring, linear, mesh, star… etc.

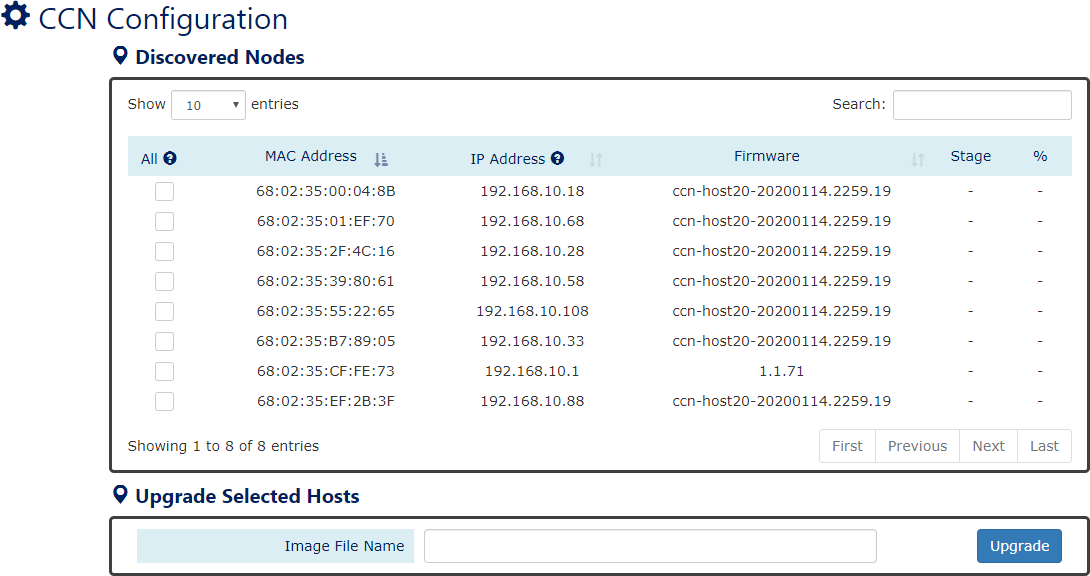
The following diagram is an example with ring topology.



The **SA** Switch is the CCN master connected to PC, and from PC end, users can control the CCN function, such as selection of joined switches and firmware path configuration. The firmware image must be saved in the **USB** device. After clicking Upgrade button on CCN master, the **SA** starts upgrading its firmware if **SA** is selected and forwards the firmware image to other switches (**SB**, **SC**, **SD**, **SE**, or **SF**) that selected to join CCN. Once the switches receive the firmware image, they will also start upgrading their firmware automatically. That is why we say CCN can help administrators save time and work more efficiently.



**CONFIGURE COMMAND & CONTROL NODE (CCN)**



#### Discovered Nodes

* + All / Select Box

Click “**All**” to select or de-select all the discovered nodes. Click **Select Boxes** to select some of the discovered nodes to upgrade their firmware.

**Note-1:** Please select **at least one node** to do CCN upgrade

**Note-2:** Please select **at most 10 nodes** to do CCN upgrade.

* MAC Address

The **MAC Address** of the designated discovered node

* IP Address

The **IP Address** of the designated discovered node

* Firmware

The current **Firmware Version** of the designated discovered node

* Stage

After clicking Upgrade button, the upgrading stage will display on this field. The following table displays all stages.

|  |  |
| --- | --- |
| **Stage** | **Description** |
| IDLE | The initial stage of CCN operation |
| DATA\_RECV | The host is receiving the firmware image |
| UPDATING | The firmware image is received and start upgrading |
| FINISHED | Firmware upgrading is finished |
| ERROR | Firmware upgrading is failed |
| DISCONN | The host disconnects with CCN master |

* %

The operating percentage of current stage

#### Upgrade Selected Hosts

Please ensure there is a **USB stick** inserted into the USB port.

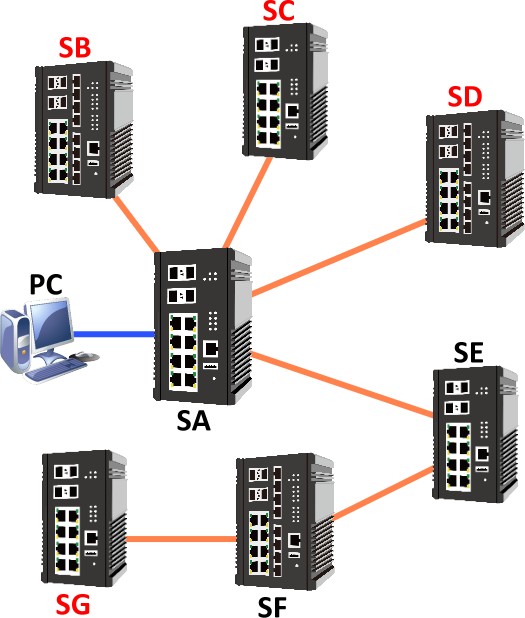
* + Image File Name

The File Name of the firmware image, which is saved to the USB. The firmware image MUST be saved in the **root path** of USB.

**Note**: The file system of USB must be FAT32.

  (Upgrade Button)

After entering the firmware image path, click "Upgrade" button to start upgrading.

**CONFIGURATION EXAMPLE FOR CCN**

In the left diagram, the **SA** is the **CCN master**, and the **SB**, **SC**, **SD**, and **SG** are the nodes that want to upgrade.

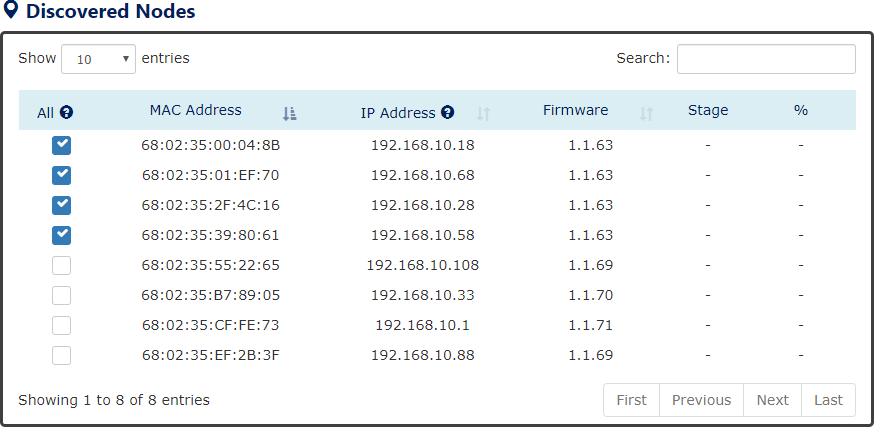
First, we must ensure the firmware image is saved in a USB stick and the USB stick is inserted into the USB port of SA.

And then, open the configuration WEB GUI of **SA** and enter **Command & Control Node** page. The connected nodes will show on the **Discovered Nodes** list.

**Step-by-step Configuration**

1. Login Web Console and click menu “*Maintenance*” -> “*Command & Control Node*”
2. The Discovered Nodes section displays all devices that **SA** (master) can connect to.
3. Click the checkboxes of **SB**, **SC**, **SD**, and **SG** (or the devices that want to upgrade).

**Note:** There is a limitation that users must select the devices that want to upgrade **at once** and **on the same page** and then click upgrade button to start.



1. Check the **USB stick** is inserted, and the firmware image is saved on it.
2. Enter the path of the firmware image.



1. Click **Upgrade** Button to start upgrading
   1. Configure Firmware File Name

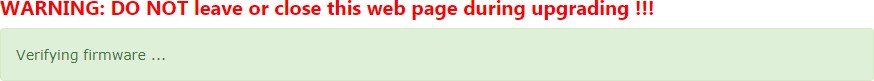


* 1. Copying Firmware - there will be a warning message to notify users to stay

on the CCN page.



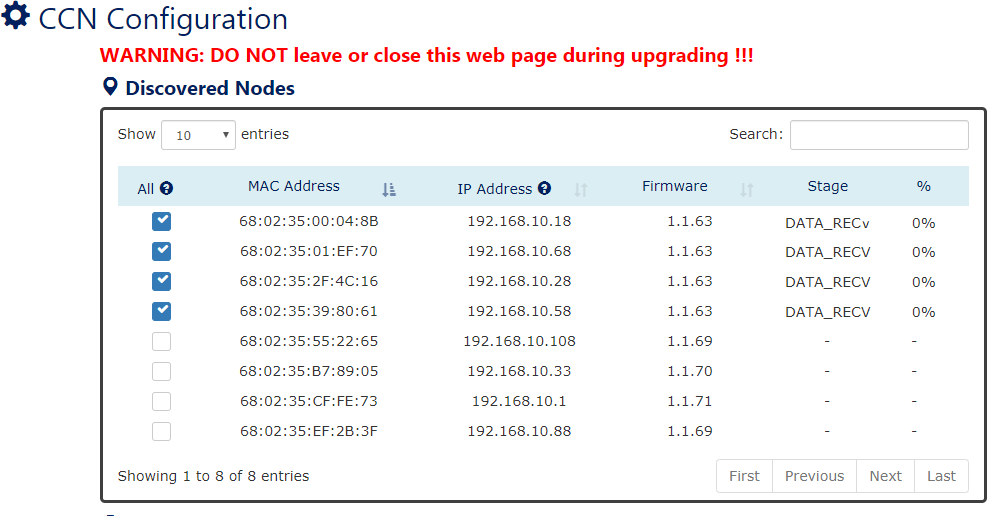
* 1. Verifying Firmware

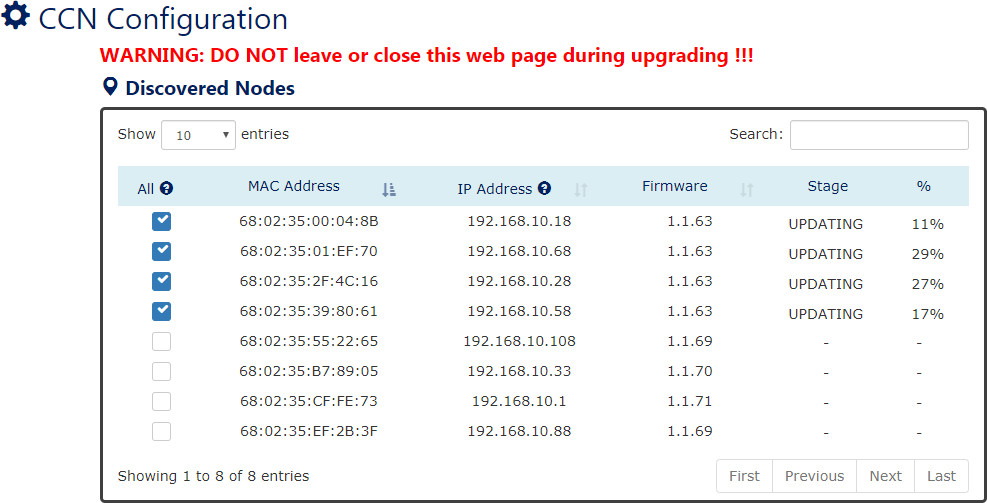


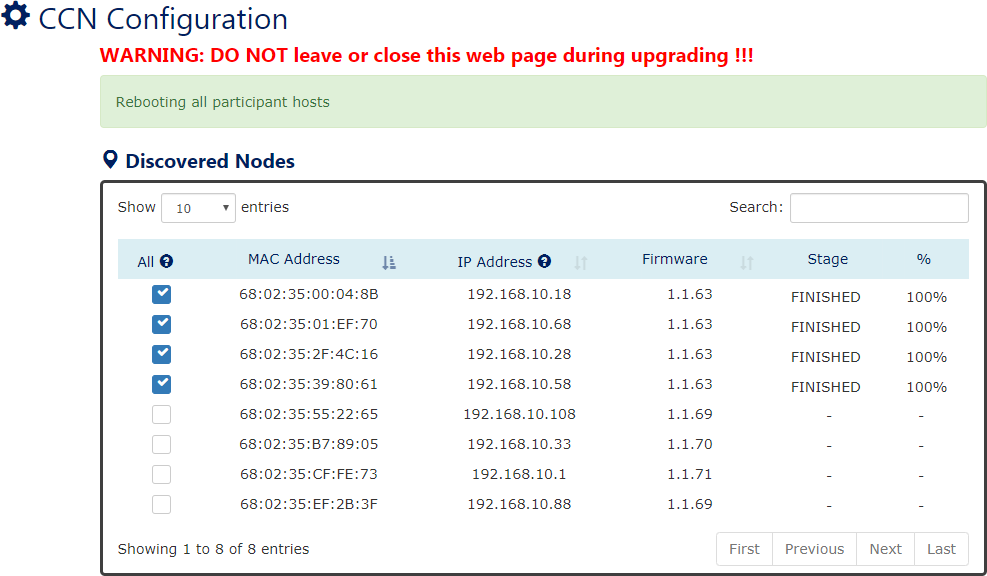
* 1. Decompressing and Extracting Firmware



* 1. Start CCN Upgrading, the Stage and Percentage (%) will change with the upgrading process
  2. Stage *DATA\_RECV*, hosts are receiving the firmware image

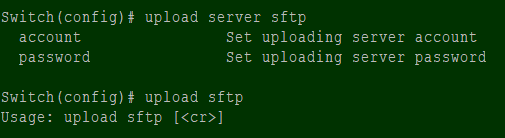


* 1. Stage *UPDATING*, the firmware is upgrading
  2. Stage *FINISHED*, the firmware upgrading is finished, and the selected nodes are rebooting



# SFTP File Access

**CONFIGURE SFTP CONFIGURATION UPLOAD**



1. Config IP address of SFTP server

Switch(config)# **upload server ip [SERVER\_IP]**

1. Config login account name of SFTP server

Switch(config)# **upload sftp server account [SERVER\_ACCOUNT]**

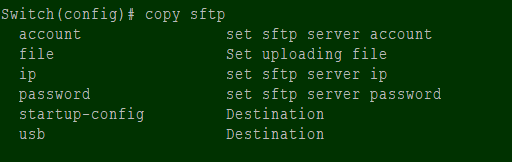
1. Config login account password of SFTP server

Switch(config)# **upload sftp server password [SERVER\_PASSWORD]**

1. Action to do the SFTP upload

Switch(config)# **upload sftp**

**CONFIGURE SFTP CONFIGURATION DOWNLOAD**



1. Config IP address of SFTP server

Switch(config)# **copy sftp ip [SERVER\_IP]**

1. Config login account name for SFTP server

Switch(config)# **copy sftp account [SERVER\_ACCOUNT]**

1. Config login account password for SFTP server

Switch(config)# **copy sftp password [SERVER\_PASSWORD]**

1. Config login account password for SFTP server

Switch(config)# **copy sftp file name [FILE\_NAME]**

1. Action to do the SFTP download to the startup configuration Switch(config)# **copy sftp startup-config**

**Note:** After copy to the startup configuration, system will reboot automatically.

1. Action to do the SFTP download to the USB storage

Switch(config)# **copy sftp USB Note**: The file system of USB must be FAT32.

# Command Line Interface

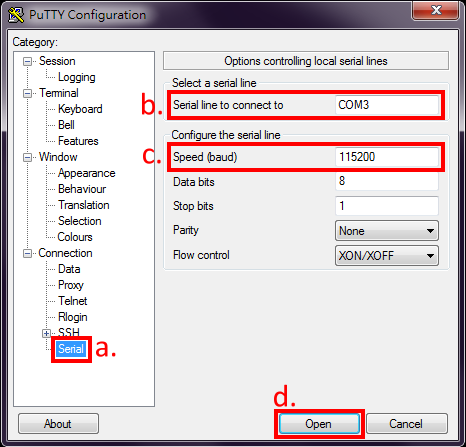
**Command Line Interface** is usually called **CLI**. It allows the users to configure, monitor, and maintain the switch by executing commands directly.

**CONNECT TO CLI VIA CONSOLE PORT**

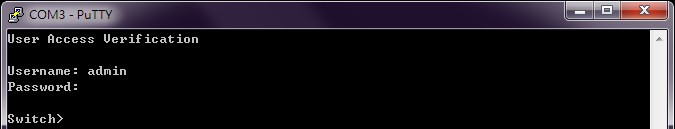
Before starting the connection to the Console Port, ensure that you have a utility (such as “Putty”, “Tera Term”, “HyperTerminal”, “SecureCRT”, etc.) to do that. The following example is operating on **Windows 7** and connected by “**Putty**”.

1. Connect the Console Port to your PC or Laptop and check the port number in the “Device Manager” on the PC.
2. Configure the Serial Information with the COM port number and Speed (Baud Rate: **115200**). By default, the Data bits and Parity are **8** and **1**. Then click “Open” to connect to the CLI.

**Note**: The complete parameters are **COMX/115200/8/1**.



1. Enter the username and password to login to the system. The default username and password is **admin**/**admin**.

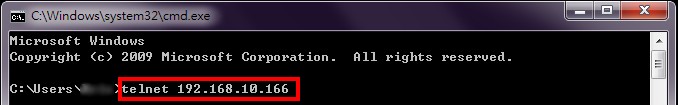


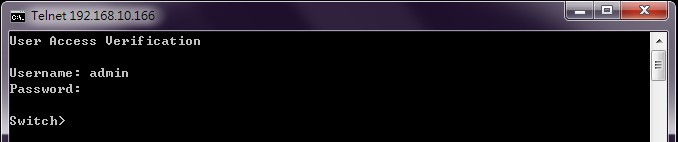
1. When you see “**Switch>**”, it refers that you have logged in to the system. You can then start to configure the system on the CLI mode.

**CONNECT TO CLI VIA TELNET**

The following example is operating on **Windows 7**. If the system shows the information as the picture below, please [enable the “Telnet Client”](#_bookmark43) before using telnet function.



1. Click Windows “Start” button and enter “cmd” on the search box to open the “Command Prompt”.
2. Enter “**telnet [IP\_ADDRESS]**” on the CMD window. For example, the IP address of the switch is “192.168.10.166”, so enter “telnet 192.168.10.166” and then press the “Enter” key.
3. Enter the username and password to login the system. The default username and password is

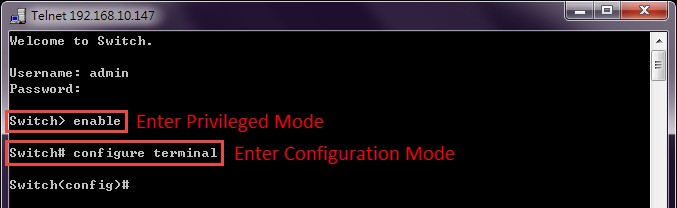
**admin**/**admin**.

1. When “**Switch>**” is displayed, it refers that you have logged in to the system. You can then start to configure the system on the CLI mode.

**CONFIGURE SYSTEM UNDER DIFFERENT MODES**

After login to CLI, users must enter the Privileged Mode for “show” commands. If users want to configure the system via CLI, they must enter Configuration Mode.

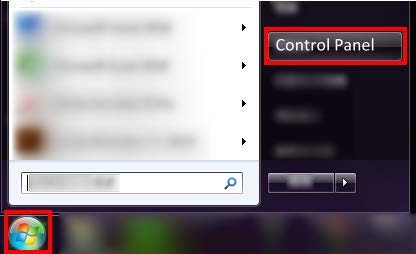
The command to enter Privileged Mode is “**enable**”. After entering Privileged Mode, issue “**configure terminal**” to enter Configuration Mode. When “**Switch(config)#**” is displayed, users can start configuring the system with all commands under Configuration Mode. In the Command Group section, the mode of each command will be marked in the last column of the commands table.

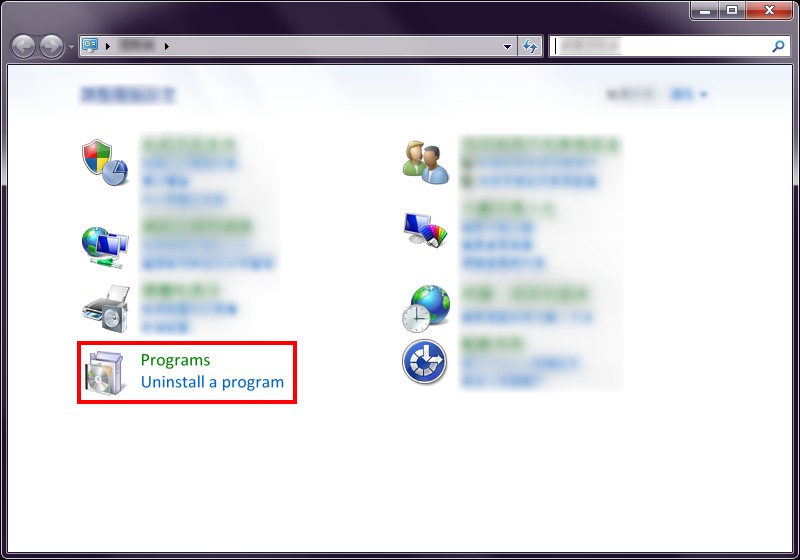


There are different modes under Configuration Mode, such as **Interface** Mode, **VLAN** Mode, **ERPS** Mode, and **MRP** Mode. If the command that users are preparing to issue is under these modes, they must enter the designated mode first. Users can issue “**exit**” to leave current mode. In the following table, we list the commands to enter different modes.

|  |  |  |
| --- | --- | --- |
| **Mode** | **Command** | **Description** |
| Interface | interface lanX | X implies the port number |
| VLAN | vlan X | X implies the VLAN ID |
| ERPS | ethernet redundancy erps-ring X | X implies the Ring number, from 1 to 3 |
| MRP | ethernet redundancy mrp instance-mode 1 | Only support single ring currently |

### ENABLE TELNET CLIENT ON WIDOWS 7

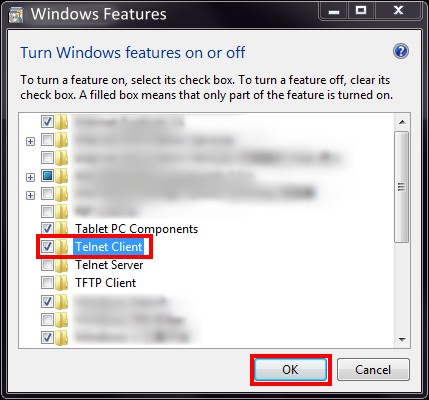
1. Click the Windows “Start” button and click “Control Panel” item.
2. Click the “Programs” item.

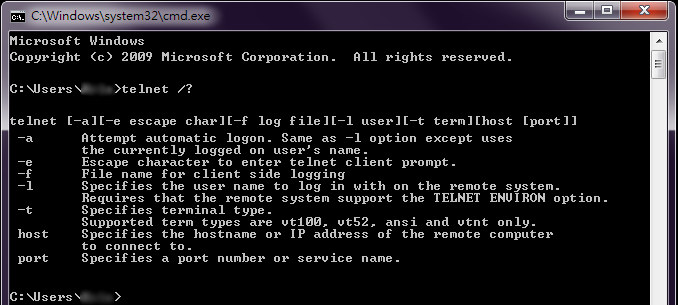


1. Click the “Turn Windows features on or off” item.



1. Select the checkbox of “Telnet Client” and then click “OK” to enable telnet function.



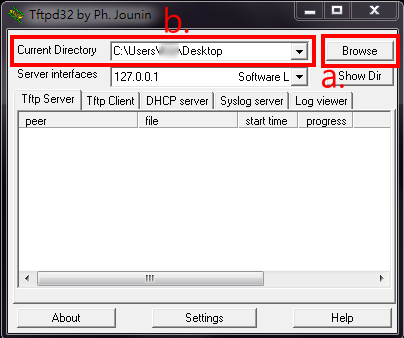
1. Click Windows “Start” button and enter “cmd” on the search box to open the “Command Prompt” to test the telnet function.

**FIRMWARE UPGRADE VIA CLI**

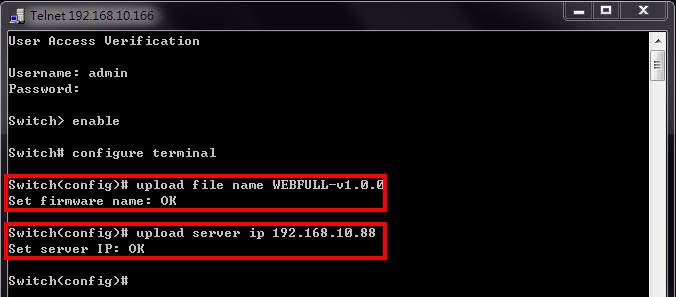
Users can upgrade the system with a new firmware on both the web console and CLI mode. To upgrade on the web console, a high interactivity web GUI is provided for the users. Please refer to [Firmware Upgrade](#_bookmark34) section. To upgrade on the CLI mode, there are 3 methods: TFTP, wget (HTTP), and USB. The following sections explain how to upgrade the firmware using the 3 methods.

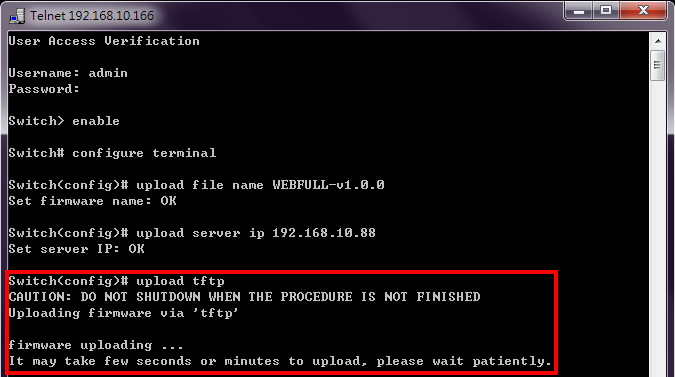
**FIRMWARE UPGRADE VIA CLI – TFTP**

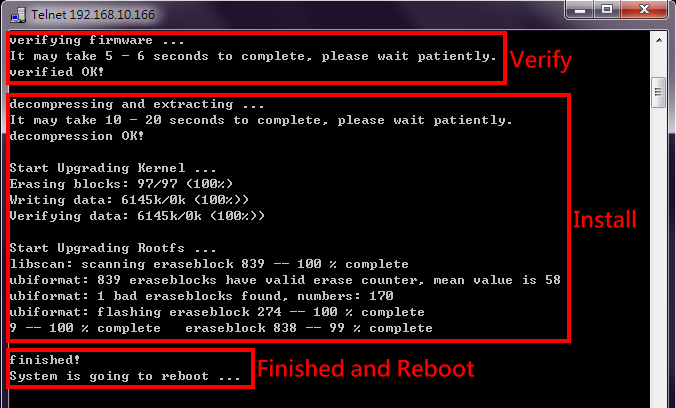
If the users are planning to upgrade the firmware via CLI mode with TFTP, a **TFTP server** is needed before upgrading. You can download the free TFTP server from the [tftpd official website](http://tftpd32.jounin.net/).

1. Open the TFTP Server and browser the file directory path. For example, if the firmware file is saved on the desktop, the path to the desktop should be specified in the “**Current Directory**” field.
2. Make sure the link between the switch and the host (PC or laptop) is connected. To verify it, ping the IP address of the switch IP address from the host to check it.
3. Assign the **firmware file name** by issuing the “**upload file name [FILE\_NAME]**“. The default file name is “WEBFULL”.
4. Assign the TFTP Server IP address by issuing “**upload server ip [SERVER\_IP]**”. The server IP address is the IP address of the host, which is running the TFTP server.

The commands for assigning the filename and server IP are in the **Configure mode**, so before configuring, specify “configure terminal” to enter the **Configure mode**.

If the command is completely configured, the system will display “**OK**”.

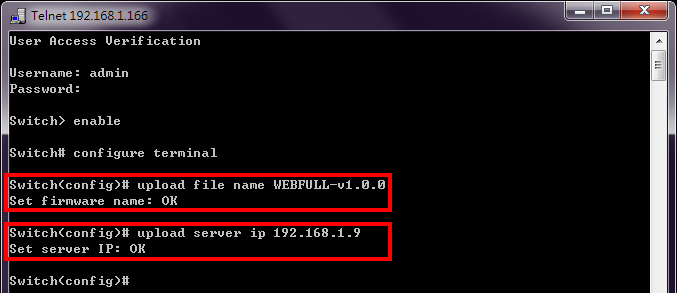
1. Start to upgrade the firmware file by specifying “upload tftp”. The system starts to upload the assigned file by the TFTP. This takes a few minutes.
2. After uploading, the system will **verify** the uploaded file. If the verification passes, the new firmware file will be installed. Ensure the system is **powered on** and the sy**ste**m will **reboot** automatically after the firmware is completely installed.

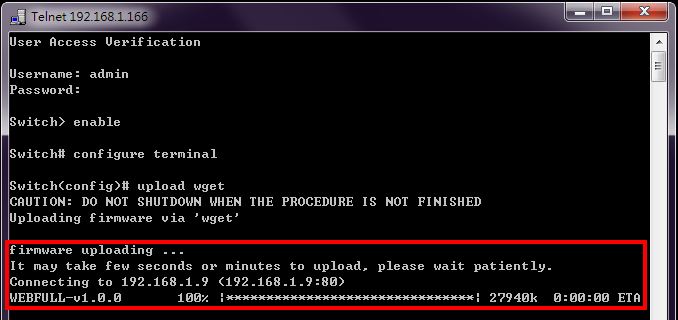


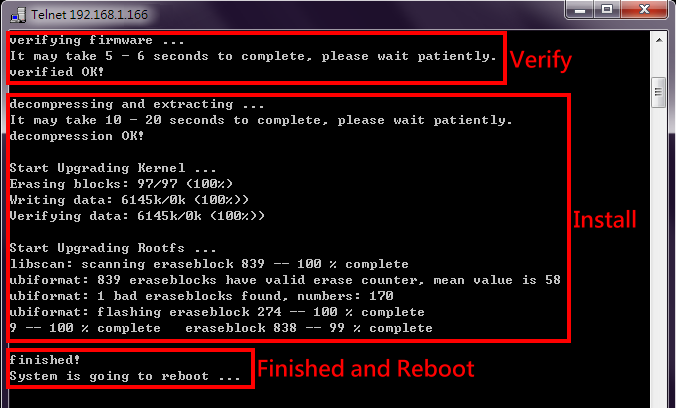
**FIRMWARE UPGRADE VIA CLI – WGET**

“**Wget**” uses the **HTTP** to transmit the file to the switch. Users must establish a **HTTP Server**

such as “[**Apache**](https://httpd.apache.org/)” and upload the firmware file to the HTTP Server.

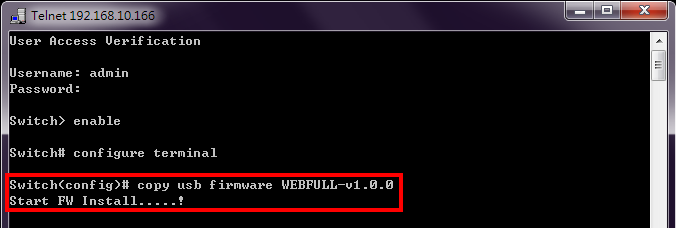
1. Assume there is a HTTP Server existed whose IP address is “**192.168.1.9**” and the firmware file named **WEBFULL-v1.0.0** is uploaded.
2. Make sure the link between the switch and the server is connected. We can ping the IP address of the server from the switch by using the command “**ip ping [IP\_ADDRESS]**”.
3. Assign the **firmware file name** by using “**upload file name WEBFULL-v1.0.0**“.
4. Assign the **Wget Server IP address** by using “**upload server ip 192.168.1.9**”. If the command is completely configured, the system will display “**OK**”.
5. Start to upgrade the firmware file by using “upload wget”. The system starts to upload the assigned file by HTTP. This takes a few seconds or minutes.



1. Once the uploading is complete, the system will **verify** the uploaded file. If the verification passes, the new firmware file will be installed. Ensure to keep the system **powered on** and the sy**ste**m will **reboot** automatically after the firmware is completely installed.

**FIRMWARE UPGRADE VIA CLI – USB**

Check if the firmware file is saved in the USB and the USB stick is inserted in the USB part of the switch before upgrading the firmware file.

1. Save the firmware file to the USB device and insert the USB stick to the USB port.
2. Use “copy usb firmware [FILE\_NAME]” to upgrade the system via USB.
3. After the installation is complete, the system will reboot automatically.

**Note**: The file system of USB must be FAT32.

### COMMAND GROUPS

The following are the commands that the users can use in the CLI mode. Please check if the

**mode** is correct before issuing the command.

### AUTHENTICATION GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| login authentication [tacacs+ | radius] | Set login authentication method | Configure |
| logout | Disconnect | Configure |
| radius-server host [IP\_ADDR] | Set IP address of RADIUS server | Configure |
| radius-server key [SHARED\_KEY] | Set specific characters for authentication  verification | Configure |
| radius-server port [1-65535] | Set communication port of RADIUS server | Configure |
| radius-server retransmit [1-1000] | Set the number of times a request re-sending to  RADIUS server | Configure |
| radius-server timeout [1-1000] | Set the timeout period to wait for RADIUS server  response | Configure |
| tacacs-server host [IP\_ADDR] | Set IP address of TACASC+ server | Configure |
| tacacs-server key [SHARED\_KEY] | Set specific characters for authentication  verification | Configure |
| tacacs-server port [1-65535] | Set communication port of TACASC+ server | Configure |
| tacacs-server timeout [1-1000] | Set the timeout period to wait for TACASC+ server response | Configure |
| username [USER\_ID] [PASSWORD] | Configure username and password | Configure |
| username-ro [USER\_ID] [PASSWORD] | Configure read only username and password | Configure |
| show login authentication | Display login authentication method | Configure |
| show radius-server host | Display IP address of RADIUS server | Configure |
| show radius-server key | Display specific characters for authentication verification | Configure |
| show radius-server port | Display communication port of RADIUS server | Configure |
| show radius-server retransmit | Display the number of times a request is resent | Configure |
| show radius-server timeout | Display the timeout period to wait for RADIUS  server response | Configure |
| show tacacs-server host | Display IP address of the server | Configure |
| show tacacs-server key | Display specific characters for authentication  verification | Configure |
| show tacacs-server port | Display communication port of the server | Configure |
| show tacacs-server timeout | Display the timeout period to wait for the server  response | Configure |
| show username | Display admin ID | Configure |
| show username-ro | Display read only user ID | Configure |
| no login authentication | Default Login authentication method | Configure |
| no radius-server host | Default IP address of the server | Configure |

|  |  |  |
| --- | --- | --- |
| no radius-server key | Default specific characters for authentication  verification | Configure |
| no radius-server port | Default communication port of the server | Configure |
| no radius-server retransmit | Default the number of times a request is resent | Configure |
| no radius-server timeout | Default the timeout period to wait for the server response | Configure |
| no tacacs-server host | Default IP address of TACACS+ server | Configure |
| no tacacs-server key | Default specific characters for authentication verification | Configure |
| no tacacs-server port | Default communication port of TACACS+ server | Configure |
| no tacacs-server timeout | Default the timeout period to wait for TACACS+ server response | Configure |
| no username | Default username and password | Configure |
| no username-ro | Default read only username and password | Configure |

**SSH GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| copy host-key-config usb [FILE\_NAME] | Backup SSH host key to USB | Configure |
| copy usb host-key-config [file] | Upload SSH host key config from USB | Configure |
| download file name [FILE\_NAME] | Set downloading file name, default name is host\_key.cfg | Configure |
| download host-key-config | Download current SSH host key config | Configure |
| download server account  [SERVER\_ACCOUNT] | Set downloading server account | Configure |
| download server ip [SERVER\_IP] | Set downloading server IP Address | Configure |
| download server password [SERVER\_PASSWORD] | Set downloading server password | Configure |
| upload host-key-config wget [file] | Upload SSH host key config from Localhost | Configure |
| show ssh host-key | Display SSH host key | Configure |

### SYSTEM GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| erase startup-config | Reset to factory default and reboot | Configure |
| erase startup-config keep-ip | Reset to factory default except IP | Configure |
| erase startup-config keep-ip-user | Reset to factory default except IP and USER | Configure |
| erase startup-config keep-user | Reset to factory default except USER ID/PASS | Configure |
| exec-timeout [MINUTE] [SECOND] | Set idle timeout [MINUTE] [SECOND] | Configure |
| hostname [HOSTNAME] | Set Switch Host Name | Configure |
| reboot | Reboot the switch | Configure |
| system contact [CONTACT] | Set system contact | Configure |
| system description [SYS\_DESCRIPTION] | Set device description | Configure |
| system location [LOCATION] | Set device location | Configure |

|  |  |  |
| --- | --- | --- |
| show exec-timeout | Display idle timeout | Configure |
| show hostname | Display Switch Host Name | Configure |
| show environment power [1|2] | Display power 1/2 status | Configure |
| show event status relay | Display relay status | Configure |
| show system contact | Display system contact | Configure |
| show system description | Display system description | Configure |
| show system firmware-date | Display system release time | Configure |
| show system location | Display system location | Configure |
| show system mac | Display system MAC address | Configure |
| show system uptime | Display system uptime | Configure |
| show system version firmware | Display system version | Configure |
| show transceiver ddm | Display transceiver DDM information | Interface |
| show transceiver info | Display transceiver information | Interface |
| show transceiver raw | Display transceiver raw data | Interface |
| show username | Display admin ID | Configure |
| no exec-timeout | Default idle timeout | Configure |
| no hostname | Default Switch Host Name | Configure |
| no system contact | Clear system contact | Configure |
| no system description | Clear device description | Configure |
| no system location | Clear device location | Configure |
| no username | Default username and password | Configure |

**SERVICE CONTROL GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| service [http | https | ssh | telnet | console |  reset button] enable | Enable service http, https, ssh, telnet,  console port, or reset button | Configure |
| show service [http | https | ssh | telnet |  console | reset-button] | Display service http, https, ssh, telnet,  console port, or reset button state | Configure |
| no service [http | https | ssh | telnet | console | reset-button] | Disable service http, https, ssh, telnet, console port, or reset button | Configure |

**IPV4 GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ip address [IP\_ADDR] [MASK] | Set IPv4 address and netmask | Configure |
| ip default-gateway  [DEFAULT\_GATEWAY\_ADDR] | Set default gateway address | Configure |
| ip name-server [NAME\_SERVER\_IP] | Set Domain Name-Server | Configure |
| ip ping [IPV4\_ADDR] [<size PKG\_SIZ> |  <repeat PKG\_CNT>] | Issue an IPv4 ping command | Configure |
| show ip address | Display Host address of IPv4 | Configure |
| show ip default-gateway | Display default gateway address | Configure |

|  |  |  |
| --- | --- | --- |
| show ip mode | Display IP mode (Static or Dynamic) | Configure |
| show ip name-server | Display Domain Name-Server | Configure |
| no ip address | Delete IPv4 address | Configure |
| no ip default-gateway | Clear the default gateway address | Configure |
| no ip name-server | Clear the domain name-server | Configure |

**IPV6 GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ipv6 address add [IPV6\_ADDR</PREFIX\_LEN>] | Add an address and netmask of IPv6 | Configure |
| ipv6 enable | Enable IPv6 protocol | Configure |
| ipv6 neighbor flush | Issue a neighbor flush command of IPv6 | Configure |
| ipv6 ping [IPV6\_ADDR] [<size PKG\_SIZ> |  <repeat PKG\_CNT>] | Issue an IPv6 ping command | Configure |
| show ipv6 | Display IPv6 protocol state | Configure |
| show ipv6 address | Display IPv6 addresses | Configure |
| show ipv6 default address | Display default IPv6 address | Configure |
| show ipv6 neighbor | Display neighbor cache of IPv6 | Configure |
| no ipv6 | Disable IPv6 protocol | Configure |
| no ipv6 address add  [IPV6\_ADDR/PREFIX\_LEN] | Delete IPv6 address | Configure |

### TIME GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| clock time [hh:mm:ss] [day] [month] [year] | Configure time | Configure |
| clock timezone [AREA] [CITY] | Configure time zone | Configure |
| ntp client sync [minute | hour | day | month  | year] [NUMBER] | Configure NTP client sync | Configure |
| ntp client timeserver [SERVER\_IP/URL] | Configure NTP client time server | Configure |
| ntp time update | Configure NTP time update | Configure |
| show clock time | Show time | Configure |
| show clock timezone | Show timezone | Configure |
| show ntp client sync | Show sync time | Configure |
| show ntp client timeserver | Show NTP server configuration | Configure |
| no clock timezone | Remove timezone | Configure |
| no ntp client sync | Remove NTP sync time | Configure |
| no ntp client timeserver | Remove NTP time server configuration | Configure |

**PTP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ptp announce interval [-1 to 7] | Set PTP announce interval, the interval is  expressed as **log 2**. i.e. -1 is 0.5s, 0 is 1s. | Configure |

|  |  |  |
| --- | --- | --- |
| ptp announce timeout [2-255] | Set PTP announce timeout | Configure |
| ptp disable | Disable PTP | Configure |
| ptp disable | Disable Hardware PTP | Interface |
| ptp domain [0-127] | Set PTP domain number | Configure |
| ptp enable | Enable PTP | Configure |
| ptp enable | Enable Hardware PTP | Interface |
| ptp mode [t(transparent clock)] | Set Hardware PTP mode | Interface |
| ptp period [0-20] | Set PTP timeout periods | Configure |
| ptp priority1 [0-248] | Set PTP priority1 | Configure |
| ptp priority2 [0-248] | Set PTP priority2 | Configure |
| ptp role [ m(master) | s(slave) ] | Set PTP role | Configure |
| ptp sync interval [-7 to 7] | Set PTP sync interval, the interval is  expressed as **log 2**. i.e. -1 is 0.5s, 0 is 1s. | Configure |
| show ptp announce interval | Display PTP announce interval | Configure |
| show ptp announce timeout | Display PTP announce timeout | Configure |
| show ptp clock | Display PTP sync information | Configure |
| show ptp domain | Display PTP domain number | Configure |
| show ptp enable | Display PTP status | Configure |
| show ptp enable | Display Hardware PTP Enable | Interface |
| show ptp mode | Display Hardware PTP mode | Interface |
| show ptp period | Display PTP timeout periods | Configure |
| show ptp priority1 | Display PTP priority1 | Configure |
| show ptp priority2 | Display PTP priority2 | Configure |
| show ptp role | Display PTP role | Configure |
| show ptp sync interval | Display PTP sync interval | Configure |
| no ptp announce interval | Default PTP announce interval | Configure |
| no ptp announce timeout | Default PTP announce timeout | Configure |
| no ptp domain | Default PTP domain number | Configure |
| no ptp mode | Default Hardware PTP mode | Interface |
| no ptp period | Default PTP timeout periods | Configure |
| no ptp priority1 | Default PTP priority1 | Configure |
| no ptp priority2 | Default PTP priority2 | Configure |
| no ptp role | Default PTP role | Configure |
| no ptp sync interval | Default PTP sync interval | Configure |

**STP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| spanning-tree forward-time [4-30] | Set STP forward time | Configure |
| spanning-tree hello-time [1-10] | Set STP hello time | Configure |
| spanning-tree max-age [6-40] | Set max age | Configure |

|  |  |  |
| --- | --- | --- |
| spanning-tree mode [rstp] | Set STP mode as [RSTP] | Configure |
| spanning-tree mst instance [1-15] vlan [VLAN\_LIST] | Set vlan group for specific MSTP instance | Configure |
| spanning tree mst name [NAME] | Set MSTP name | Configure |
| spanning-tree mst revision [0-65535] | Set MSTP revision | Configure |
| spanning-tree mst [1-15] priority [0-61440] | Set priority for specific MSTP instance | Configure |
| spanning-tree priority [0-61440] | Set STP priority | Configure |
| spanning-tree cost [0-200000000] | Configure STP cost | Interface |
| spanning-tree edge  [admin-edge|admin-non-edge] | Configure STP edge | Interface |
| spanning-tree link-type  [point-to-multiple|point-to-point] | Configure STP link type on port | Interface |
| spanning-tree mst [1-15] cost [0-  200000000] | Configure port cost for specific MSTP instance | Interface |
| spanning-tree mst [1-15] port-priority [0-  200000000] | Configure port priority for specific MSTP instance | Interface |
| spanning-tree port-priority [0-240] | Configure STP port priority | Interface |
| spanning tree stp disable | Disable Spanning Tree Protocol (STP) on port | Interface |
| show spanning-tree forward-time | Show STP forward time | Configure |
| show spanning-tree hello-time | Show STP hello time | Configure |
| show spanning-tree max-age | Show STP max age | Configure |
| show spanning-tree mode | Show Spanning Tree mode (RSTP or disable) | Configure |
| show spanning-tree mst instance [1-15]  vlan | Show vlan group for specific MSTP instance | Configure |
| show spanning-tree mst name | Show MSTP name | Configure |
| show spanning-tree mst revision | Show MSTP revision | Configure |
| show spanning-tree mst [1-15] priority | Show priority for specific MSTP instance | Configure |
| show spanning-tree mst [1-15] status | Show bridge status for specific MSTP instance | Configure |
| show spanning-tree priority | Show STP priority | Configure |
| show spanning-tree rstp-status | Show Spanning Tree rstp status | Configure |
| show spanning-tree cost | Show STP cost | Interface |
| show spanning-tree edge | Show STP auto edge | Interface |
| show spanning-tree link-type | Show STP link type | Interface |
| show spanning-tree mst [1-15] cost | Show port cost for specific MSTP instance | Interface |
| show spanning-tree mst [1-15]  port-priority | Show port priority for specific MSTP instance | Interface |
| show spanning-tree port-priority | Show STP port priority | Interface |
| show spanning-tree stp | Show STP activated status on port | Interface |
| no spanning-tree forward-time | Remove STP forward time configuration | Configure |
| no spanning-tree hello-time | Remove STP hello time configuration | Configure |
| no spanning-tree max-age | Remove STP max age configuration | Configure |
| no spanning-tree mode | Disable STP configuration | Configure |
| no spanning-tree priority | Remove STP priority configuration | Configure |

|  |  |  |
| --- | --- | --- |
| no spanning-tree cost | Remove STP cost configuration | Interface |
| no spanning-tree edge | Remove auto edge configuration | Interface |
| no spanning-tree link-type | Remove link type configuration | Interface |
| no spanning-tree mst [1-15] cost | Remove port cost for specific MSTP instance | Interface |
| no spanning-tree mst [1-15] port-priority | Remove port priority for specific MSTP instance | Interface |
| no spanning-tree port-priority | Remove STP port priority configuration | Interface |
| no spanning-tree stp | Enable STP on port | Interface |

**ERPS GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ethernet redundancy erps-ring [ 1 | 2 | 3 ] | Ethernet Ring Protection Switching (ERPS) mode | Configure |
| aps-channel [1 - 4094] | Set APS channel | ERPS |
| disable | Disable ERPS function | ERPS |
| enable | Enable ERPS function | ERPS |
| erps-ring [ 1 | 2 | 3 ] | Change to Other ERPS Ring | ERPS |
| ext-command clear | Extended ERPS command - Clear | ERPS |
| ext-command fs | Extended ERPS command – Forced Switch | ERPS |
| ext-command ms | Extended ERPS command – Manual Switch | ERPS |
| id [1 - 239] | Set Ring ID | ERPS |
| mel [0 - 7] | ERPS mel | ERPS |
| revertive | Set as revertive mode | ERPS |
| ring-port 0 [1(lan1) - N(lanN)] | Mapping ERPS ring port0 to switch port | ERPS |
| ring-port 1 [1(lan1) - N(lanN)] | Mapping ERPS ring port1 to switch port | ERPS |
| role port0 [o(owner) | n(neigh) | i(interconn)] | Set role on ring port0 | ERPS |
| role port1 [o(owner) | n(neigh) | i(interconn)] | Set role on ring port1 | ERPS |
| timer guard [10 - 2000] | Set guard timer interval | ERPS |
| timer hold-off [0 - 10000] | Set hold-off timer interval | ERPS |
| timer wtr [1 - 12] | Set WTR timer interval | ERPS |
| type [m(major ring) | s(sub-ring)] | Set type as Major-Ring or Sub-Ring | ERPS |
| virtual-channel major-ring channel-id [1-4094] | Set virtual channel for ERPS Ring | ERPS |
| virtual-channel sub-ring set | Set virtual channel for ERPS Sub-ring | ERPS |
| show config | Displays ERPS configuration | ERPS |
| show port status | Displays ERPS ring port status | ERPS |
| show status | Displays ERPS status | ERPS |
| no aps-channel | Default ERPS aps-channel | ERPS |
| no id | Default Ring ID as default | ERPS |
| no revertive | Default mode non-revertive | ERPS |
| no ring-port 0 | Default ring port0 as lan1 | ERPS |
| no ring-port 1 | Default ring port1 as lan2 | ERPS |

|  |  |  |
| --- | --- | --- |
| no role port0 | Default role of ring port0 as none | ERPS |
| no role port1 | Default role of ring port1 as none | ERPS |
| no timer guard | Default guard timer | ERPS |
| no timer hold-off | Default hold-off timer | ERPS |
| no timer wtr | Default wtr timer | ERPS |
| no type | Default ring type as Major-Ring | ERPS |
| no virtual-channel major-ring channel-id | Default virtual channel as ERPS Major Ring's aps-channel | ERPS |
| no virtual-channel sub-ring set | Default virtual channel for ERPS Sub-ring  as None | ERPS |

**MRP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ethernet redundancy mrp instance-mode [1] | Media Redundancy Protocol (MRP) mode | Configure |
| advanced mode [enable | disable] | Enable/Disable MRP Advanced Mode | MRP |
| domain-id [DOMAIN\_ID] | Set MRP Domain-id, the format is 16 bytes  in decimal notation | MRP |
| name [DOMAIN\_NAME] | Set MRP Domain Name | MRP |
| operation [enable | disable] | Enable/Disable MRP Protocol | MRP |
| port 1 [1(lan1) - N(lanN)] | Set MRP ring-port 1 ID | MRP |
| port 2 [1(lan1) - N(lanN)] | Set MRP ring-port 2 ID | MRP |
| recovery-delay [500 | 200] | Set MRP Recovery Delay (unit: ms) | MRP |
| role [m(manager) | c(client)] | Set MRP Role to MRM(manager) or  MRC(client) | MRP |
| show advanced mode | Display MRP Advanced mode | MRP |
| show config | Display MRP Domain Config | MRP |
| show domain-id | Display MRP Domain ID | MRP |
| show name | Display MRP Domain Name | MRP |
| show operation | Display MRP Operation Status | MRP |
| show port [1 | 2] | Display MRP ring-port [1 | 2] ID | MRP |
| show recovery-delay | Display MRP Recovery Delay | MRP |
| show role | Display MRP Domain Expected Role | MRP |
| show summary | Display MRP Domain Summary | MRP |
| no domain-id | Default MRP Domain ID | MRP |
| no name | Clear MRP Domain Name | MRP |
| no port [1 | 2] | Default MRP ring-port [1 | 2] ID | MRP |
| no recovery-delay | Default MRP Recovery Delay | MRP |
| no role | Default MRP Domain role | MRP |

**SNMP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |

|  |  |  |
| --- | --- | --- |
| snmp server community ro [COMMUNITY] | Set v1, v2c snmp server read-only community | Configure |
| snmp server community rw [COMMUNITY] | Set v1, v2c snmp server read-write  community | Configure |
| snmp server enable | Enable snmp server | Configure |
| snmp server enable v1-v2c-only | Enable snmp v1 and v2c | Configure |
| snmp server enable v3-only | Enable snmp v3 command only | Configure |
| snmp server v3 auth admin [md5| sha]  [PASSWORD] | Set SNMPv3 admin authentication type | Configure |
| snmp server v3 auth user [md5| sha] [PASSWORD] | Set SNMPv3 user authentication type | Configure |
| snmp server v3 encryption admin [des| aes]  [PASSWORD] | Set SNMPv3 admin encryption type | Configure |
| snmp server v3 encryption user [des| aes] [PASSWORD] | Set SNMPv3 user encryption type | Configure |
| snmp server v3 level admin [auth| noauth|  priv] | Set SNMPv3 admin security level | Configure |
| snmp server v3 level user [auth| noauth|  priv] | Set SNMPv3 user security level | Configure |
| snmp trap community [COMMUNITY] | Set v1, v2c snmp trap community | Configure |
| snmp trap host [TRAP\_HOST\_IP] | Set snmp trap host IP address | Configure |
| snmp trap inform retry [1-100] | Set snmp inform retry times | Configure |
| snmp trap inform timeout [1-300] | Set snmp inform timeout | Configure |
| snmp trap v3 auth [sha| md5] [PASSWORD] | Set SNMPv3 authentication type: md5 or  sha | Configure |
| snmp trap v3 encryption [des| aes] [PASSWORD] | Set SNMPv3 encryption type: des or aes | Configure |
| snmp trap v3 engine-ID [ENGINE\_ID] | Set snmp trap engine ID | Configure |
| snmp trap v3 level [auth| noauth| priv] | Set SNMPv3 trap security level | Configure |
| snmp trap v3 user [USER\_ID] | Set SNMPv3 trap user | Configure |
| snmp trap version [1| 2c trap| 2c inform| 3  trap| 3 inform] | Set snmp trap version and type | Configure |
| show snmp server | Display snmp server status | Configure |
| show snmp server community ro | Display snmp server read only community | Configure |
| show snmp server community rw | Display snmp server writable community | Configure |
| show snmp server v3 auth admin | Display SNMPv3 admin authentication type and passphrase | Configure |
| show snmp server v3 auth user | Display SNMPv3 user authentication type  and passphrase | Configure |
| show snmp server v3 encryption admin | Display SNMPv3 admin encryption type  and passphrase | Configure |
| show snmp server v3 encryption user | Display SNMPv3 user encryption type and passphrase | Configure |
| show snmp server v3 level admin | Display SNMPv3 admin security level | Configure |
| show snmp server v3 level user | Display SNMPv3 user security level | Configure |

|  |  |  |
| --- | --- | --- |
| show snmp trap community | Display snmp trap community | Configure |
| show snmp trap host | Display snmp trap host | Configure |
| show snmp trap inform retry | Display snmp inform retry times | Configure |
| show snmp trap inform timeout | Display snmp inform timeout | Configure |
| show snmp trap v3 auth | Display SNMPv3 authentication type and passphrase | Configure |
| show snmp trap v3 encryption | Display SNMPv3 encryption type and passphrase | Configure |
| show snmp trap v3 engine-ID | Display snmp trap engine ID | Configure |
| show snmp trap v3 level | Display SNMPv3 trap security level | Configure |
| show snmp trap v3 user | Display SNMPv3 trap user | Configure |
| show snmp trap version | Display snmp trap version and type | Configure |
| no snmp server | Disable snmp server | Configure |
| no snmp server community ro | Default ro-community name | Configure |
| no snmp server community rw | Default rw-community name | Configure |
| no snmp server v3 auth admin | Default SNMPv3 admin authentication type | Configure |
| no snmp server v3 auth user | Default SNMPv3 user authentication type | Configure |
| no snmp server v3 encryption admin | Default SNMPv3 admin encryption type | Configure |
| no snmp server v3 encryption user | Default SNMPv3 user encryption type | Configure |
| no snmp server v3 level admin | Default SNMPv3 admin security level | Configure |
| no snmp server v3 level user | Default SNMPv3 user security level | Configure |
| no snmp trap community | Default snmp trap community | Configure |
| no snmp trap host | Default snmp trap host | Configure |
| no snmp trap inform retry | Default snmp inform retry times | Configure |
| no snmp trap inform timeout | Default snmp inform timeout | Configure |
| no snmp trap v3 auth | Default SNMPv3 authentication type and passphrase | Configure |
| no snmp trap v3 encryption | Default SNMPv3 encryption type and passphrase | Configure |
| no snmp trap v3 engine-ID | Default snmp trap engine ID | Configure |
| no snmp trap v3 level | Default SNMPv3 trap security level | Configure |
| no snmp trap v3 user | Default SNMPv3 trap user | Configure |
| no snmp trap version | Default snmp trap version | Configure |

**DHCP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| boot host dhcp | Directs the system to get an IP address | Configure |
| dhcp relay information option | Set DHCP-relay option | Configure |
| dhcp relay server [server\_number: 1-4]  [server\_IP] | Set DHCP-relay server [1-4] IP | Configure |

|  |  |  |
| --- | --- | --- |
| dhcp relay untrust | Set DHCP-relay untrusted port | Interface |
| dhcp server binding [bind\_ID: 1 - 32] [MAC]  [IP\_TO\_BIND] | Set binding IP and MAC of DHCP | Configure |
| dhcp server default-gateway [IP\_ADDR] | Set default-gateway IP for DHCP client | Configure |
| dhcp server included address [START\_OF\_IP]  [END\_OF\_IP] | Set IP range for its client | Configure |
| dhcp server lease-time [60-2592000] | Set DHCP server lease time | Configure |
| dhcp server name-server [IP\_ADDR] | Set name-server address for DHCP client | Configure |
| dhcp service relay enable | Enable DHCP relay | Configure |
| dhcp service server enable | Enable DHCP server | Configure |
| show boot host dhcp | Display DHCP client state | Configure |
| show dhcp relay information option | Display DHCP relay option | Configure |
| show dhcp relay server [server\_number: 1-4] | Display DHCP relay address | Configure |
| show dhcp relay untrust | Display DHCP untrusted port status | Interface |
| show dhcp server binding | Display all DHCP bounding entries | Configure |
| show dhcp server default-gateway | Display DHCP default-gateway IP | Configure |
| show dhcp server included address | Display DHCP included IP range | Configure |
| show dhcp server lease | Display DHCP lease entries | Configure |
| show dhcp server lease-time | Display DHCP server lease time | Configure |
| show dhcp server name-server | Display DHCP name-server | Configure |
| show dhcp server status | Display DHCP server status | Configure |
| show dhcp service relay | Display DHCP relay agent status | Configure |
| show dhcp service server | Display DHCP server status | Configure |
| no boot host dhcp | Disable DHCP client | Configure |
| no dhcp relay information option | Disable DHCP relay option | Configure |
| no dhcp relay server [server\_number: 1-4] | Remove DHCP relay server [1-4] IP | Configure |
| no dhcp relay untrust | Default port as trusted | Interface |
| no dhcp server binding [bind\_ID: 1-32] | Remove DHCP bounding IP and MAC | Configure |
| no dhcp server default-gateway | Remove DHCP default-gateway IP | Configure |
| no dhcp server included address | Remove DHCP included IP range | Configure |
| no dhcp server lease-time | Remove DHCP lease time | Configure |
| no dhcp server name-server | Remove DHCP name-server | Configure |
| no dhcp service relay | Disable DHCP relay | Configure |
| no dhcp service server | Disable DHCP server | Configure |

### INDUSTRIAL PROTOCOLS GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ethernet-ip enable | Enable EtherNet/IP Protocol | Configure |

|  |  |  |
| --- | --- | --- |
| modbus tcp enable | Enable Modbus/TCP Protocol | Configure |
| show ethernet-ip | Show EtherNet/IP status | Configure |
| show modbus tcp | Show Modbus/TCP status | Configure |
| no ethernet-ip | Disable EtherNet/IP Protocol | Configure |
| no modbus tcp | Disable Modbus/TCP Protocol | Configure |

**UPNP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| upnp advertisement interval [300-86400] | Set UPnP advertisement interval | Configure |
| upnp enable | Enable Universal Plug and Play (UPnP) | Configure |
| show upnp | Display Universal Plug and Play (UPnP) state | Configure |
| show upnp advertisement interval | Display UPnP advertisement interval | Configure |
| no upnp | Disable Universal Plug and Play (UPnP) | Configure |
| no upnp advertisement interval | Default UPnP advertisement interval | Configure |

### PORT GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| flowcontrol [on | off] | Configure port's flow-control to response a pause  frame | Interface |
| name [PORT\_NAME] | Set interface name | Interface |
| shutdown | Disable port | Interface |
| speed\_duplex [10 | 100] [full | half] | Configure port's speed and duplex | Interface |
| show interface all link summary | To display interface link status globally | Configure |
| show administrate | To display port's admin state | Interface |
| show flowcontrol | Display port's flow-control state | Interface |
| show link duplex | To display port's duplex | Interface |
| show link rx | To display port's Rx\_Bytes | Interface |
| show link speed | To display port's speed | Interface |
| show link state | To display port's link state | Interface |
| show link summary | To display port's link summary | Interface |
| show link tx | To display port's Tx\_Bytes | Interface |
| show name | To display port's name | Interface |
| show speed\_duplex | To display port's speed and duplex | Interface |
| show transceiver | Transceiver information | Interface |
| no flowcontrol | Default flow-control as Auto mode | Interface |
| no name | Remove port's name | Interface |
| no shutdown | Enable port | Interface |
| no speed\_duplex | Default port speed-duplex as Auto mode | Interface |

**POE GROUP** (PoE Model Only)

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| power inline budget [1-240] | Power PoE budget | Configure |
| power inline mode-config disable | Disable PoE on port | Interface |
| power inline mode-config enable | Enable PoE on port | Interface |
| power inline mode-config force | Force PoE powered on port | Interface |
| power inline priority [1-3] | Set PoE port priority on port.  1:high, 2:middle, 3:low | Interface |
| keepalive enable | Enable PoE keepalive | Interface |
| keepalive hold-time | Configure PoE keepalive power cycle  hold-time | Interface |
| keepalive ip | Configure IP for PoE keepalive | Interface |
| keepalive time | Configure PoE keepalive cycle time | Interface |
| schedule enable | Enable one port PoE schedule | Interface |
| schedule [Sunday-Saturday] open-time  [time] | Configure PoE schedule open time on one  day | Interface |
| show power inline budget | Display PoE power budget | Configure |
| show power inline detail-code | Display PoE status code, refer to [“PoE Debug](#_bookmark11)  [Code](#_bookmark11)” for more explanation | Interface |
| show power inline operation | Display All PoE ports operation status | Configure |
| show power inline status | Display All PoE ports detail status | Configure |
| show power inline status | Display PoE status for specific port | Interface |
| show power inline temperature | Display temperature of PoE controller | Configure |
| show keepalive table | Display All PoE keepalive info | Configure |
| show power inline status | Display PoE status | Interface |
| show keepalive | Show PoE keepalive status | Interface |
| show keepalive hold-time | Show PoE keepalive hold-time | Interface |
| show keepalive ip | Show IP for PoE keepalive | Interface |
| show keepalive time | Show PoE keepalive cycle time | Interface |
| show schedule | Disable Universal Plug and Play (UPnP) | Interface |
| show schedule [Sunday-Saturday]  open time | Show open time of POE schedule on one day | Interface |
| show schedule table | Show one port PoE schedule table | Interface |
| no power inline budget | Default PoE power budget | Configure |
| no power inline mode-config | Default PoE powered config on port | Interface |
| no power inline priority | Disable PoE port priority on port | Interface |
| no keepalive | Disable PoE keepalive | Interface |

|  |  |  |
| --- | --- | --- |
| no keepalive hold-time | Default PoE keepalive power cycle hold-time | Interface |
| no keepalive ip | Remove IP for PoE keepalive | Interface |
| no keepalive time | Remove PoE keepalive cycle time | Interface |
| no schedule | Remove one port PoE schedule | Interface |
| no schedule [Sunday-Saturday] open-time | Remove PoE schedule on one day | Interface |

**IGMP SNOOPING GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| igmp snooping enable | Enable IGMP snooping | Configure |
| igmp snooping last-member count [2-10] | Set IGMP last-member-count | Configure |
| igmp snooping last-member interval [1-25] | Set IGMP last-member-interval | Configure |
| igmp snooping querier enable | Enable IGMP snooping querier | Configure |
| igmp snooping query interval [1-3600] | Set IGMP query interval | Configure |
| igmp snooping query max-respond-time [1-12] | Set IGMP max-query-respond time | Configure |
| igmp snooping query version [VLAN\_ID]  [STATE:0|1] [VERSION:1|2|3] | Add IGMP query version entry by VLAN  ID. STATE 0: disable; STATE 1: enable | Configure |
| igmp snooping router-port [PORT\_LIST] | Set router port list for multicast | Configure |
| igmp snooping unknown multicast [f|d|r] | Set unknown-multicast action | Configure |
| show igmp snooping all | Display IGMP settings (summary) | Configure |
| show igmp snooping mdb | Display IGMP multicast database | Configure |
| show igmp snooping query-version | Display IGMP Query version by VLAN ID | Configure |
| show igmp snooping router-port | Display IGMP router port list | Configure |
| show igmp snooping unknown multicast | Display unknown-multicast action | Configure |
| no igmp snooping | Disable IGMP snooping | Configure |
| no igmp snooping last-member count | Default IGMP Last-Member-Count | Configure |
| no igmp snooping last-member interval | Default IGMP Last-Member-Interval | Configure |
| no igmp snooping querier | Disable IGMP querier | Configure |
| no igmp snooping query interval | Default IGMP query interval | Configure |
| no igmp snooping query max-respond-time | Default IGMP max-respond-time | Configure |
| no igmp snooping router-port | Default IGMP router port | Configure |
| no igmp snooping unknown multicast | Default unknown-multicast action | Configure |

**VLAN GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| management-vlan [VLAN\_ID: 1-4094] | Configure management vlan ID | Configure |
| provider ethertype [VALUE\_IN\_HEX (i.e.,  0x88A8)] | Setup EtherType in S-TAG for provider  port | Configure |
| member [untag PORT\_LIST] [tag PORT\_LIST] | Set VLAN member | VLAN |

|  |  |  |
| --- | --- | --- |
| name [VLAN\_NAME] | Set VLAN Name | VLAN |
| switchport accept [tagged | untagged] | Set VLAN acceptance of frame | Interface |
| switchport mode [d(dot1q-tunnel)| c(customer)| p(provider)| s(specific-provider)] | Configure port type as dot1q-tunnel, Customer, or Service Provider | Interface |
| switchport pvid [PVID: 1-4094] | Set port VLAN-Id | Interface |
| show management-vlan | Display management vlan ID | Configure |
| show provider ethertype | Display Service Provider EtherType | Configure |
| show vlan global | Display VLAN Global information | Configure |
| show member | Display port VLAN member | VLAN |
| show name | Display VLAN name | VLAN |
| show switchport accept | Display acceptance of VLAN frame | Interface |
| show switchport mode | Display VLAN interface port type | Interface |
| show switchport pvid | Display port VLAN-Id | Interface |
| no management-vlan | Set management vlan to default | Configure |
| no provider ethertype | Default EtherType as 0x88A8 in S-TAG for  provider port | Configure |
| no member | Default VLAN member | VLAN |
| no name | Default VLAN name | VLAN |
| no switchport accept | Default acceptance of VLAN frame | Interface |
| no switchport mode | Default port type as Customer | Interface |
| no switchport pvid | Default port VLAN-Id | Interface |

**QOS GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| qos fair-queue weight [W0] [W1] [W2]  [W3] [W4] [W5] [W6] [W7] | Set WRR Queue Weight | Configure |
| qos map cos [priority:0-7] to tx-queue  [0-7] | Set Cos queue mapping of priority [0-7] | Configure |
| qos map dscp [0-63] to tx-queue [0-7] | Set DSCP mapping queue | Configure |
| qos queue-schedule [strict | wrr] | Set QoS scheduling type | Configure |
| qos default cos [0-7] | Set Default Class of Service (COS) value | Interface |
| qos trust [cos | dscp] | Set trust of cos or dscp | Interface |
| show qos fair-queue weight | Display WRR Queue Weight | Configure |
| show qos map cos | Display global QoS queue mapping status | Configure |
| show qos map cos [0-7] | Display QoS queue mapping status of Priority  [0-7] | Configure |
| show qos map dscp | Display global DSCP queue mapping status | Configure |

|  |  |  |
| --- | --- | --- |
| show qos map dscp [0-63] | Display DSCP queue mapping status of class [0-63] | Configure |
| show qos queue-schedule | Display queue scheduling type | Configure |
| show qos default cos | Display CoS default value | Interface |
| show qos trust | Display QoS trust | Interface |
| no qos fair-queue weight | Default WRR Queue Weight | Configure |
| no qos map cos [0-7] | Reset Cos queue mapping of priority [0-7] | Configure |
| no qos map dscp [0-63] | Reset DSCP mapping queue to default | Configure |
| no qos queue-schedule | Default scheduling type as WRR | Configure |
| no qos default cos | Reset default CoS to initial value | Interface |
| no qos trust | Default trust as CoS | Interface |

### PORT TRUNK GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| trunk group [1-8] [static | lacp] INTERFACES\_LIST | Configure port aggregation group | Configure |
| show trunk group | Show all trunk groups | Configure |
| show trunk group [1-8] | Show trunk group [1-8] | Configure |
| no trunk group [1-8] | Remove trunk group [1-8] | Configure |

**STORM CONTROL GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| storm-control broadcast enable | Enable the broadcast storm control | Configure |
| storm-control broadcast level [low | mid |  high] | Set the broadcast storm control level | Configure |
| storm-control multicast enable | Enable the multicast storm control | Configure |
| storm-control multicast level [low | mid |  high] | Set the multicast storm control level | Configure |
| storm-control unknown-unicast enable | Enable the unknown-unicast storm control | Configure |
| storm-control unknown-unicast level [low |  mid | high] | Set the unknown-unicast storm control  level | Configure |
| show storm-control broadcast | Display the broadcast storm control status | Configure |
| show storm-control broadcast level | Display the broadcast storm control level | Configure |
| show storm-control multicast | Display the multicast storm control status | Configure |
| show storm-control multicast level | Display the multicast storm control level | Configure |
| show storm-control unknown-unicast | Display the unknown-unicast storm  control status | Configure |
| show storm-control unknown-unicast level | Display the unknown-unicast storm  control level | Configure |
| no storm-control broadcast | Disable the broadcast storm control | Configure |

|  |  |  |
| --- | --- | --- |
| no storm-control broadcast level | Default the broadcast storm control to  level high | Configure |
| no storm-control multicast | Disable the multicast storm control | Configure |
| no storm-control multicast level | Default the multicast storm control to  level high | Configure |
| no storm-control unknown-unicast | Disable the unknown-unicast storm  control | Configure |
| no storm-control unknown-unicast level | Default the unknown-unicast storm  control to level high | Configure |

**802.1X GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| dot1x authentication server [1|2] ip [IP] | Set 802.1X authentication server 1 or 2  address | Configure |
| dot1x authentication server [1|2] port [PORT] | Set 802.1X authentication server 1 or 2  port | Configure |
| dot1x authentication server [1|2] share-key  [KEY] | Set 802.1X authentication server 1 or 2  share-key | Configure |
| dot1x authentication server type  [local|radius] | Set 802.1X authentication server type | Configure |
| dot1x enable | Enable 802.1X protocol | Configure |
| dot1x local-db [USER] [PASSWORD] | Set 802.1X local user database | Configure |
| dot1x authenticator enable | Set 802.1X authenticator | Interface |
| dot1x mode [mac-based | port-based] | Set 802.1X mode as 1. MAC-based,  2.Port-based | Interface |
| dot1x reauthentication enable | Set 802.1X reauthentication | Interface |
| dot1x reauthentication period [60-65535] | Set 802.1X reauthentication period | Interface |
| show dot1x | Display 802.1X protocol state | Configure |
| show dot1x authentication server [1|2] ip | Display 802.1X authentication server 1 or 2  address | Configure |
| show dot1x authentication server [1|2] port | Display 802.1X authentication server 1 or 2  port | Configure |
| show dot1x authentication server [1|2]  share-key | Display 802.1X authentication server 1 or 2  key | Configure |
| show dot1x authentication server type | Display 802.1X authentication server type | Configure |
| show dot1x brief | Display 802.1X information | Configure |
| show dot1x local-db | Display 802.1X users and password in  database | Configure |

|  |  |  |
| --- | --- | --- |
| show dot1x server brief | Display 802.1X RADIUS server | Configure |
| show dot1x authenticator | Display 802.1X authenticator state | Interface |
| show dot1x mode | Display 802.1X mode config | Interface |
| show dot1x reauthentication | Display 802.1X reauthentication state | Interface |
| show dot1x reauthentication period | Display 802.1X reauthentication period (in  sec.) | Interface |
| no dot1x | Disable 802.1X protocol | Configure |
| no dot1x authentication server [1|2] ip | Default 802.1X authentication server 1 or  2 address | Configure |
| no dot1x authentication server [1|2] port | Default 802.1X authentication server 1 or  2 port | Configure |
| no dot1x authentication server [1|2]  share-key | Default 802.1X authentication server 1 or  2 share-key | Configure |
| no dot1x authentication server type | Default 802.1X authentication server type | Configure |
| no dot1x local-db [USER] | Remove an entry in 802.1X local database | Configure |
| no dot1x authenticator | Disable 802.1X authenticator | Interface |
| no dot1x mode | Default 802.1X mode as MAC-based | Interface |
| no dot1x reauthentication | Disable 802.1X reauthentication | Interface |
| no dot1x reauthentication period | Default 802.1X reauthentication period | Interface |

### PORT MIRROR GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| mirror destination [DEST\_PORT] | Set mirror interface of destination | Configure |
| mirror enable | Enable port mirror | Configure |
| mirror source [rx | tx | both] [PORT\_LIST] | Set mirror interface of source | Configure |
| show mirror | Show port mirror enable/disable state | Configure |
| show mirror destination | Show port mirror destination configuration | Configure |
| show mirror source | Show port mirror source configuration | Configure |
| no mirror | Disable port mirror | Configure |
| no mirror destination | Delete port mirror Destination configuration | Configure |
| no mirror source | Delete port mirror Source configuration | Configure |

**REMOTE SPAN GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| rspan destination [DEST\_PORT] | Set remote SPAN interface of destination | Configure |
| rspan mode source enable | Enable remote SPAN of source | Configure |
| rspan mode destination enable | Enable remote SPAN of destination | Configure |
| rspan reflector [REFLECTOR\_PORT] | Set remote SPAN interface of reflector | Configure |

|  |  |  |
| --- | --- | --- |
| rspan source [rx | tx] [PORT] | Set remote SPAN monitor traffic and interface of  source | Configure |
| rspan vlan-id [2 - 1001, 1006 - 4094] | Set remote SPAN VLAN-Id | Configure |
| show rspan | Show remote SPAN enable/disable state | Configure |
| show rspan destination | Show remote SPAN destination configuration | Configure |
| show rspan reflector | Show remote SPAN reflector configuration | Configure |
| show rspan source | Show remote SPAN source configuration | Configure |
| show rspan vlan-id | Show remote SPAN VLAN-Id configuration | Configure |
| no rspan | Disable remote SPAN | Configure |
| no rspan destination | Delete remote SPAN destination configuration | Configure |
| no rspan reflector | Delete remote SPAN reflector configuration | Configure |
| no rspan source | Delete remote SPAN source configuration | Configure |
| no rspan vlan-id | Delete remote SPAN VLAN-Id configuration | Configure |

**LLDP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| lldp enable | Enable LLDP protocol | Configure |
| lldp timer [5-32767] | Set LLDP timer | Configure |
| show lldp neighbor | Display LLDP neighbor | Configure |
| show lldp neighbor detail | Display LLDP neighbors in detail | Configure |
| show lldp state | Display LLDP status | Configure |
| show lldp timer | Display LLDP timer | Configure |
| no lldp | Disable LLDP protocol | Configure |
| no lldp timer | Default LLDP timer | Configure |

### SYSLOG GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| syslog local enable | Enable logging to local | Configure |
| syslog log clear | Clear syslog log | Configure |
| syslog remote enable | Enable logging to remote | Configure |
| syslog remote port [PORT] | Set syslog remote server port | Configure |
| syslog remote server [ADDRESS] | Set syslog remote server address | Configure |
| syslog usb enable | Enable log to USB device | Configure |
| show syslog local | Display local logging state | Configure |
| show syslog log | Display syslog messages | Configure |
| show syslog remote | Display remote logging state | Configure |
| show syslog remote port | Display remote server port | Configure |
| show syslog remote server | Display remote server IP | Configure |

|  |  |  |
| --- | --- | --- |
| show syslog usb | Display USB logging state | Configure |
| no syslog local | Disable logging to local | Configure |
| no syslog remote | Disable logging to remote | Configure |
| no syslog remote port | Default syslog remote server port | Configure |
| no syslog remote server | Clear syslog remote server address | Configure |
| no syslog usb | Disable logging to USB | Configure |

**SMTP GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| smtp authentication enable | Enable SMTP authentication | Configure |
| smtp authentication password [PASSWORD] | Set SMTP password | Configure |
| smtp authentication username [USER\_NAME] | Set SMTP username | Configure |
| smtp enable | Enable SMTP | Configure |
| smtp receive [1-4] [RECEIVER\_ADDRESS] | Set SMTP receiver [1-4] address | Configure |
| smtp sender [SMTP\_SENDER\_ADDRESS] | Set SMTP sender | Configure |
| smtp server address [SMTP\_SERVER\_ADDRESS] | Set SMTP server address | Configure |
| smtp server port [SMTP\_SERVER\_PORT] | Set SMTP server port | Configure |
| smtp subject [SUBJECT] | Set SMTP subject | Configure |
| show smtp authentication state | Display SMTP authentication status | Configure |
| show smtp authentication username | Display SMTP username | Configure |
| show smtp receive [1-4] | Display SMTP receiver [1-4] | Configure |
| show smtp sender | Display SMTP sender | Configure |
| show smtp server address | Display SMTP server address | Configure |
| show smtp server port | Display SMTP server port | Configure |
| show smtp state | Display SMTP service | Configure |
| show smtp subject | Display SMTP subject | Configure |
| no smtp authentication | Disable SMTP authentication | Configure |
| no smtp authentication password | Clear SMTP password | Configure |
| no smtp authentication username | Clear SMTP username | Configure |
| no smtp | Disable SMTP | Configure |
| no smtp receive [1-4] | Clear SMTP receiver [1-4] | Configure |
| no smtp sender | Clear SMTP sender | Configure |
| no smtp server address | Clear SMTP server | Configure |
| no smtp server port | Clear SMTP server port | Configure |
| no smtp subject | Clear SMTP subject | Configure |

### EVENT GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |

|  |  |  |
| --- | --- | --- |
| event alarm ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power |  voltage] | Register a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| event alarm digital input [high | low] | Register an event of digital input | Configure |
| event alarm interface [lan1-lanN] down | Register an event of Interface DOWN | Configure |
| event alarm [power1|power2] | Register an event of power 1 or 2 failure | Configure |
| event smtp auth-failure | Register an event of authentication failure | Configure |
| event smtp cold start | Register an event of cold start | Configure |
| event smtp ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power | voltage] | Register a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| event smtp digital input [high | low] | Register an event of digital input | Configure |
| event smtp interface [lan1-lanN] down | Register an event of Interface DOWN | Configure |
| event smtp interface [lan1-lanN] up | Register an event of Interface UP | Configure |
| event smtp [power1|power2] | Register an event of power 1 or 2 failure | Configure |
| event smtp warm start | Register an event of warm start | Configure |
| event snmptrap auth-failure | Register an event of authentication failure | Configure |
| event snmptrap cold start | Register an event of cold start | Configure |
| event snmptrap ddm [lanX-lanY] [current |  rx\_power | temperature | tx\_power | voltage] | Register a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| event snmptrap digital input [high | low] | Register an event of digital input | Configure |
| event snmptrap interface [lan1-lanN] down | Register an event of Interface DOWN | Configure |
| event snmptrap interface [lan1-lanN] up | Register an event of Interface UP | Configure |
| event snmptrap [power1|power2] | Register an event of power 1 or 2 failure | Configure |
| event snmptrap warm start | Register an event of warm start | Configure |
| event syslog auth-failure | Register an event of authentication failure | Configure |
| event syslog cold start | Register an event of cold start | Configure |
| event syslog ddm [lanX-lanY] [current |  rx\_power | temperature | tx\_power | voltage] | Register a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| event syslog digital input [high | low] | Register an event of digital input | Configure |
| event syslog interface [lan1-lanN] down | Register an event of Interface DOWN | Configure |
| event syslog interface [lan1-lanN] up | Register an event of Interface UP | Configure |
| event syslog [power1|power2] | Register an event of power 1 or 2 failure | Configure |
| event syslog warm start | Register an event of warm start | Configure |
| show event alarm ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power |  voltage] | Display current, Rx power, temperature, Tx power, or voltage event registration | Configure |
| show event alarm digital input | Display digital-input event registration | Configure |
| show event alarm interface [lan1-lanN] down | Display interface DOWN event registration | Configure |

|  |  |  |
| --- | --- | --- |
| show event alarm [power1|power2] | Display power 1 or 2 event registration | Configure |
| show event smtp auth-failure | Display authentication failure event  registration | Configure |
| show event smtp cold start | Display cold-start event registration | Configure |
| show event smtp ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power |  voltage] | Display current, Rx power, temperature, Tx power, or voltage event registration | Configure |
| show event smtp digital input | Display digital-input event registration | Configure |
| show event smtp interface [lan1-lanN] down | Display interface DOWN event registration | Configure |
| show event smtp interface [lan1-lanN] up | Display interface UP event registration | Configure |
| show event smtp [power1|power2] | Display power 1 or 2 event registration | Configure |
| show event smtp warm start | Display warm-start event registration | Configure |
| show event snmptrap auth-failure | Display authentication failure event  registration | Configure |
| show event snmptrap cold start | Display cold-start event registration | Configure |
| show event snmptrap ddm [lanX-lanY]  [current | rx\_power | temperature | tx\_power | voltage] | Display current, Rx power, temperature, Tx power, or voltage event registration | Configure |
| show event snmptrap digital input | Display digital-input event registration | Configure |
| show event snmptrap interface [lan1-lanN]  down | Display interface DOWN event registration | Configure |
| show event snmptrap interface [lan1-lanN] up | Display interface UP event registration | Configure |
| show event snmptrap [power1|power2] | Display power 1 or 2 event registration | Configure |
| show event snmptrap warm start | Display warm-start event registration | Configure |
| show event syslog auth-failure | Display authentication failure event  registration | Configure |
| show event syslog cold start | Display cold-start event registration | Configure |
| show event syslog ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power | voltage] | Display current, Rx power, temperature, Tx power, or voltage event registration | Configure |
| show event syslog digital input | Display digital-input event registration | Configure |
| show event syslog interface [lan1-lanN] down | Display interface DOWN event registration | Configure |
| show event syslog interface [lan1-lanN] up | Display interface UP event registration | Configure |
| show event syslog [power1|power2] | Display power 1 or 2 event registration | Configure |
| show event syslog warm start | Display warm-start event registration | Configure |
| no event alarm ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power |  voltage] | Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| no event alarm digital input | Unregister an event of digital input | Configure |
| no event alarm interface [lan1-lanN] down | Unregister an event of Interface DOWN | Configure |
| no event alarm [power1|power2] | Unregister an event of power 1 or 2 failure | Configure |

|  |  |  |
| --- | --- | --- |
| no event smtp auth-failure | Unregister an event of authentication  failure | Configure |
| no event smtp cold start | Unregister an event of cold start | Configure |
| no event smtp ddm [lanX-lanY] [current | rx\_power | temperature | tx\_power |  voltage] | Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| no event smtp digital input | Unregister an event of digital input | Configure |
| no event smtp interface [lan1-lanN] down | Unregister an event of Interface DOWN | Configure |
| no event smtp interface [lan1-lanN] up | Unregister an event of Interface UP | Configure |
| no event smtp [power1|power2] | Unregister an event of power 1 or 2 failure | Configure |
| no event smtp warm start | Unregister an event of warm start | Configure |
| no event snmptrap auth-failure | Unregister an event of authentication  failure | Configure |
| no event snmptrap cold start | Unregister an event of cold start | Configure |
| no event snmptrap ddm [lanX-lanY] [current |  rx\_power | temperature | tx\_power | voltage] | Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| no event snmptrap digital input | Unregister an event of digital input | Configure |
| no event snmptrap interface [lan1-lanN]  down | Unregister an event of Interface DOWN | Configure |
| no event snmptrap interface [lan1-lanN] up | Unregister an event of Interface UP | Configure |
| no event snmptrap [power1|power2] | Unregister an event of power 1 or 2 failure | Configure |
| no event snmptrap warm start | Unregister an event of warm start | Configure |
| no event syslog auth-failure | Unregister an event of authentication  failure | Configure |
| no event syslog cold start | Unregister an event of cold start | Configure |
| no event syslog ddm [lanX-lanY] [current |  rx\_power | temperature | tx\_power | voltage] | Unregister a DDM event of current, Rx power, temperature, Tx power, or voltage | Configure |
| no event syslog digital input | Unregister an event of digital input | Configure |
| no event syslog interface [lan1-lanN] down | Unregister an event of Interface DOWN | Configure |
| no event syslog interface [lan1-lanN] up | Unregister an event of Interface UP | Configure |
| no event syslog [power1|power2] | Unregister an event of power 1 or 2 failure | Configure |
| no event syslog warm start | Unregister an event of warm start | Configure |

**MAC ADDRESS TABLE GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| clear mac address-table dynamic | Flush dynamic MAC addresses in MAC  table | Configure |
| mac address add [VID: 1-4094] [MAC\_ADDR] | Set a MAC address to MAC table | Configure |

|  |  |  |
| --- | --- | --- |
| [PORT] |  |  |
| show mac address | Display MAC table | Configure |
| no mac address [VID: 1-4094] [MAC\_ADDR] | Remove a MAC address from FDB | Configure |

**USB GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| usb auto-backup | Auto save to USB if running config is changed | Configure |
| usb auto-load | Auto load config from USB to switch | Configure |
| show usb auto-backup | Display USB auto backup activated status | Configure |
| show usb auto-load | Display USB auto load activated status | Configure |
| no usb auto-backup | Disable auto save | Configure |
| no usb auto-load | Disable auto load | Configure |

### FILE GROUP

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| copy running-config startup-config | Save running-config to startup-config | Configure |
| copy running-config usb [file] | Save running-config to USB | Configure |
| copy startup-config running-config | Restore from startup-config | Configure |
| copy usb firmware [file] | Upgrade firmware from USB | Configure |
| copy startup-config usb [file] | Save startup-config to USB | Configure |
| copy usb startup-config [file] | Restore startup-config from USB | Configure |
| upload file name [FILE\_NAME] | Set uploading file name | Configure |
| upload server ip [SERVER\_IP] | Set uploading server IP | Configure |
| upload tftp | Upload and update firmware via TFTP (slower) | Configure |
| upload wget | Upload and update firmware via HTTP (faster) | Configure |
| show upload file name | Display uploading file name | Configure |
| show upload server ip | Display uploading server IP | Configure |
| no upload file name | Default uploading file name | Configure |
| no upload server ip | Clear uploading server IP | Configure |

**COMMAND & CONTROL NODE (CCN) GROUP**

|  |  |  |
| --- | --- | --- |
| **Command** | **Explanation** | **Mode** |
| ccn firmware-name [IMAGE\_NAME] | Set firmware image name | Configure |
| ccn probe | Probe CCN-capable hosts in LAN | Configure |
| ccn upgrade | Upgrade CCN-capable hosts in LAN | Configure |
| ccn upgrade exclude [INDEX\_LIST] | Upgrade CCN-capable hosts except the specified | Configure |
| ccn upgrade include [INDEX\_LIST] | Specify specific CCN-capable hosts to upgrade | Configure |

|  |  |  |
| --- | --- | --- |
| show ccn firmware-name | Display firmware image name | Configure |
| show ccn hosts | Display CCN-capable hosts | Configure |
| show ccn probe | Display probing status | Configure |
| no ccn firmware-name | Delete firmware image name | Configure |
| no ccn probe | Stop probing CCN-capable hosts in LAN | Configure |

**Fun Facts about DYMEC Switches**

1. Do you know that **DYMEC** firmware is encrypted?

All **DYMEC** switch and router firmware is encrypted so that it is secure – no matter what form of transmission you use.

1. Do you know that **DYMEC** invented the 3170-traffic switch?

**DYMEC** successfully produced the input file traffic switch in 2008.

1. Do you know that **DYMEC** switches are based on **Broadcom** chipsets?

As a United States Manufacturer of switches, we use USA based chips manufactured and approved for US DOD use.

1. Do you know that **DYMEC** “Power over Ethernet” is ALL standards based?

Many manufacturers fudge their distance or wattage capabilities with fine print. **DYMEC** Power over Ethernet is ALL IEEE 802.3 af / at or bt certified at 100 meters.

* 1. **DYMEC** Power over Ethernet (**IEEE 802.3 af**, TYPE 1) is 15.4 Watts launched at the Power Source Equipment (PSE) or Switch. Delivers a maximum 12.95 Watts at the Powered Device (PD) at 100 Meters
  2. **DYMEC** Power over Ethernet (**IEEE 802.3 at**, TYPE 2) is 30.0 Watts launched at the Power Source Equipment (PSE) or Switch. Delivers a maximum 25.50 Watts at the Powered Device (PD) at 100 Meters
  3. **DYMEC** Power over Ethernet **(IEEE 802.3 bt**, TYPE 3) is 60.0 Watts launched at the Power Source Equipment (PSE) or Switch. Delivers a maximum 51.0 Watts at the Powered Device (PD) at 100 Meters
  4. **DYMEC** Power over Ethernet (**IEEE 802.3 bt**, TYPE 4) is 100.0 Watts launched at the Power Source Equipment (PSE) or Switch. Delivers a maximum 71.0 Watts at the Powered Device (PD) at 100 Meters

1. Do you know that **DYMEC** recommends the use of 48~ 57 Volts DC Power supplies for all Power over Ethernet Applications?

This provides protection against derating of the power delivered to the Power over Ethernet end device because of temperature.

1. Do you know that **DYMEC** Power over Ethernet switches regulate any power fluctuations from the PSE (switch) to the Powered Device (PD)?

**DYMEC** switch software carefully monitors and regulates the delivered Voltage and Wattage through a complex software algorithm designed to provide accurate voltage and wattage to the end device.

1. Do you know that **DYMEC** PoE switches utilize IEEE 802.az Energy Efficient Ethernet(EEE) to save energy?

**DYMEC** switches are the leaders of the small carbon footprint. This saves money in operational costs (OPEX) – a must have for tight budgets.

1. Do you know that **DYMEC** PoE switches have built-in monitoring and statistical data gathering for all PoE functions?

It is true. All **DYMEC** PoE switches record data hour by hour – day by day – allowing for complete statistical analysis of Power usage and problem solving

1. Do you know that all **DYMEC** switches have built-in monitoring and statistical data gathering for all port functions?

It is true. All **DYMEC** switches fully record data hour by hour – day by day – allowing for complete statistical analysis of ports and trunk - complete traffic analysis that is useful for problem solving, charting traffic and traffic growth over time. Built-in switch analysis prevents degradation of the network by having to use a centralized monitor that requires polling (useless overhead traffic)

1. Do you know that **DYMEC** is the only switch manufacturer to offer a complete line of managed traffic switches – used in the input file racks of traffic cabinets?
   1. **DYMEC KY-3170EM4**: 6 x 10/100/1000 Tx & 4 x 1000 SFP Slots – Layer 2
   2. **DYMEC KY-3170EM4/2**: 8 x 10/100/1000 Tx & 2 x 1000 SFP Slots – Layer 2
   3. **DYMEC KY-3170XM**: 6 x 10/100/1000 Tx & 4 x 1 / 10 GbE SFP Slots – Layer 2
   4. **DYMEC KY-3170XM/2**: 8 x 10/100/1000 Tx & 2 x 1 / 10 GbE SFP Slots – Layer 2
   5. **DYMEC KY-3170EM4-P**: 6 x 10/100/1000 PSE Tx / 60 Watt IEEE 802.3bt & 4 x 1000 SFP Slots – Layer 2 Power over Ethernet
   6. **DYMEC KY-3170XR**: 6 x 10/100/1000 Tx & 4 x 1 / 10 GbE SFP Slots – Layer 3 and Supports OSPF, GRE, IPv4 Routing
2. Do you know that **DYMEC** switches have the built-in ability for multiple languages?

**DYMEC** originally introduced our KY-3000EM switch with Spanish and English. Now this is a standard feature – which allows us to support markets where English is not the primary language. It also allows for support by personnel without advanced language training – a savings in operational expenses (OPEX ). We support English, Spanish, Chinese, French, Japanese & Arabic. Please contact DYMEC for any language support.

1. Do you know that all Managed **DYMEC** switches have a built-in user-friendly data table ?

It is true. All **DYMEC** switches have easy to use GUI based tables that allow for easy reading, sorting, and printing of information

Example: MAC Table – Shows VLAN ID , MAC Address, MAC Type and the Source Port for all devices connected to the switch.

**DYMEC** also provides: **IPv6 Neighbor Table**, **IGMP Snooping Table**, **VLAN Table**, **LLDP Neighbor Table**, along with the **MAC Address Table.**

Great for troubleshooting and understanding your network.

In addition to the above functions, “**Refresh**” and “**Auto Refresh**” function are available for all status pages including “**IPv6 Neighbor Table**”, “**RSTP Port Status**”, “**DHCP Leased Table**”, “**Port Status**”, “**IGMP Snooping Table**”, “**VLAN Table**”, “**Trunking Status**”, “**LLDP Neighbor Table**”, and “**MAC Address Table**”.

1. Do you know that **DYMEC** switches support both NTP and PTP timing protocols?

**DYMEC** switches support standard Network Timing Protocol (NTP) and the optional Precision Timing Protocol (PTP).

1. Do you know that **DYMEC** recommends the reduction of Spanning Tree and Rapid Spanning Tree?

**DYMEC** recommends network operations use Ethernet Ring Protection System (ERPSv2) also known as ITU-T G.8032. This allows for larger – more scalable networks – reduces dependence on hop-count and simplifies daily network maintenance with the problem of the root switch issue.

1. Do you know that **DYMEC** ERPSv2 / ITU-T G.8032 is not limited to fiber networks?

ERPSv2 works well on both fiber and copper connection links.

1. Do you know that **DYMEC** switches support Industrial Protocols?

**DYMEC** supports both Ethernet/IP and Modbus/TCP. We support many leading-edge customers in their manufacturing efforts.

1. Do you know that **DYMEC** switches support non-coded SFP’s?

While some manufacturers use SFP coding to lock-in their customers to their brand of SFP, **DYMEC does not.** Coding is anti-competitive behavior – not allowed by US law. The only thing coding provides customers is higher prices – which translates into higher operational costs and confusion during maintenance.

1. Do you know that **DYMEC** switches support Copper Tx SFP’s?

Need an extra copper port? Use an SFP slot with the copper SFP support.

1. Do you know that **DYMEC** switches support VDSL2 SFP’s?

Need to support old TELCO wiring or twisted pair? Use any **DYMEC** SFP slot with our VDSL2 SFP.

1. Do you know that **DYMEC** switches support Q-in-Q VLANs?

Yes -we do. Easy to set up provider Ethertype.

1. Do you know that **DYMEC** switches support IEEE 802.1X Port based Access Control?

**DYMEC** supports easy to use GUI setup

1. Do you know that **DYMEC** switches support easy to change Management VLAN’s?

Easy to change – GUI based. Just type in a VLAN number.

1. Do you know that **DYMEC** switches support Storm Control?

Easy to change – GUI based. Operator sets the level for Broadcast / Multicast or Unknown Unicast (set threshold for frames per second).

1. Do you know that **DYMEC** switches support “SERVICE CONTROL”?

Easy to change – GUI based. Super Security at a glance. Use radio buttons to Enable or disable the following:

* 1. HTTP
  2. HTTPS
  3. SSH
  4. TELNET
  5. Console Port – Used to secure remote – unattended devices.
  6. Reset Button – Used to secure remote – unattended devices.

Used in conjunction with NSA & CSS Guidelines

1. Do you know that **DYMEC** switches support Access Control List?

**DYMEC** supports easy to use ACL’s

1. Do you know that **DYMEC** switches support Port Mirroring?

**DYMEC** supports easy to use GUI setup. Including Sniffer Mode

1. Do you know that **DYMEC** switches support Remote Span (RSPAN)?

**DYMEC Switch Port ANalyzer** (**SPAN**) provides efficient, high performance traffic monitoring. It duplicates network traffic from a configured interface to another designated interface on the switch. **SPAN** is used for connectivity troubleshooting and for network performance utilization. Easy to configure GUI

1. Do you know that **DYMEC** switches support PING?

**DYMEC** supports easy to use PING directly from the switch. This is a better measurement of performance and insures correct path. (both IPv4 & IPv6)

1. Do you know that **DYMEC** switches support Cable Diagnostics?

**DYMEC** supports easy to use cable diagnostics. With a built-in Time Domain Reflectometer (TDR). Allows the operator to check the following:

* 1. Port Selector
  2. Cable Status
  3. Pair Status
  4. Length

1. Do you know that **DYMEC** switches support Event Notifications?

**DYMEC** supports easy to use GUI’s. Any alarm can be event notified

1. Do you know that **DYMEC** switches support built-in DATA COLLECTION?

**DYMEC** supports easy to use GUI’s. Collect Statistics, Traffic Data and Power over Ethernet Data. Produces easy to read charts automatically.

1. Do you know that **DYMEC** switches support encrypted firmware and configuration files?

**DYMEC** supports easy to use GUI’s. Upgrade over the network or use the switch USB

port. Auto-loading and scheduling.

1. Do you know that **DYMEC** switches support “Command & Control Node (CCN)”?

**DYMEC – “Command & Control Node** (**CCN**)” provides built-in firmware upgrading for batch of switches at once. Currently, the CCN function can upgrade maximum 10 nodes at the same time. With CCN function, administrators can work more efficient and save a lot of time.

The **CCN** function is supported on any kind of topology: ring, linear, mesh, and star.

1. Do you know that **DYMEC** switches supports SFTP?

**DYMEC** supports easy to use Secure Transfer File Protocol

1. Do you know that **DYMEC** switches support a Digital Interface?

All **DYMEC** switches have a Digital Interface input

1. Do you know that **DYMEC** switches support a Relay Interface?

All **DYMEC** switches have a Relay Interface input for alarms and sensors.

1. Do you know that **DYMEC** supports Super-Booster Voltage Technology ?

**DYMEC** has a line of Power over Ethernet switches that support 12~48 Volts DC voltage and produces 48 Volts Power over Ethernet. This means you can use 12, 24 or any Voltage less than 48 Volts DC power and have it boosted to 48 Volts DC Power over Ethernet. (See MT Series)

A picture containing drawing

Description automatically generated

A picture containing drawing

Description automatically generated