8-Port 10M/100/1000M PoE+ and 2 Gigabit Uplink Ports (1 TP + 1 SFP) Web Managed PoE Switch

User Manual

Version 2.0

FCC/CE Mark Warning

FCC Warning

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

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

CE Mark Warning

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

Table of Contents

Before Starting

In Before Starting:

This section contains introductory information, which includes:

- **Intended Readers**
- **Icons for Note, Caution, and Warning**
- **Product Package Contents**

Before Starting

Intended Readers

This manual provides information regarding to all the aspects and functions needed to install, configure, use, and maintain the product you’ve purchased.

This manual is intended for technicians who are familiar with in-depth concepts of networking management and terminologies.

Icons for Note, Caution, and Warning

To install, configure, use, and maintain this product properly, please pay attention when you see these icons in this manual:

A **Note** icon indicates important information which will guide you to use this product properly.

A **Caution** icon indicates either a potential for hardware damage or data loss, including information that will guide you to avoid these situations.

A **Warning** icon indicates potentials for property damage and personal injury.

Before Starting

Product Package Contents

Before starting install this product, please check and verify the contents of the product package, which should include the following items:

	One Network Switch
	One Power Cord
	One User Manual CD
	One pair Rack-mount kit + 8 Screws (Optional)

Note: If any item listed in this table above is missing or damaged, please contact your distributor or retailer as soon as possible.

Chapter 1:

Product Overview

In Product Overview:

This section will give you an overview of this product, including its feature functions and hardware/software specifications.

- **Product Brief Description**
- **Product Specification**
- **Hardware Description**
- **Hardware Installation**

1.1. Product Brief Description

Introduction

This switch is 8-port 10M/100M/1000M PSE Ports + 2-port Giga uplink (1 × TP + 1 × SFP)

Desktop Web Managed PoE Switch, the switch supports IEEE 802.3at Power over Ethernet standard, maximum 130W/250W power consumption per system and no special network cable required for your PD devices. The switch also provides exceptionally smart Web management features, such as VLAN, QoS, LLDP…etc. The switch is designed for small or medium network environment to strengthen its network connection. This product is compact 11” size, making it ideal for Desktop users with limited space. It also gives you the option of installing it in a 19” cabinet by rack-mount kits or underneath a desk.

IEEE 802.3at Power over Ethernet (PoE) Ports

This switch features 8 IEEE 802.3at Power over Ethernet (PoE) ports supplying up to 30 watts per port. This product can convert standard 100~240V/AC power into low-voltage DC that runs over existing LAN cable to power up IEEE 802.3at compliant network accessories. It also features PoE awareness to verify whether the network device receive power is IEEE 802.3at compliant, or only the data will be sent through LAN cable. By adding this switch to existing networking, installing networking products such as Access Points and IP cameras can be easily managed and set up. Wireless device deployments are easily located with available power outlets and network administrators don’t need to use heavy AC power adapters anymore.

Exceptionally Smart

This switch features management interface that can be managed through web browser and provides smart features that are ideal for simple network applications and basic monitoring tools to improve network efficiency. Through a web-based interface, an administrator can set up VLANs to segregate traffic, QoS to prioritize mission-critical data, link aggregation to create fat traffic pipelines, bandwidth control to limit traffic load and Port Security to secure your network. All of these features offer extra protection on the network edge. Best of all, the password-protected configuration interface can be accessed remotely.

1.2. Product Specification

Interface		
10/100/1000 Base-T(X) RJ45 Ports		8
1G Uplink SFP Open Slot		1
1000 Base-T Uplink Port		1
System Performance		
Packet Buffer		4Mb
MAC Address Table Size		8K
Switching Capacity		20Gbps
Forwarding Rate		14.88Mpps
PoE Features		
IEEE 802.3 af/at		IEEE 802.3 af/at
Number of PSE Ports		8
Max. Power Consumption		130W/250W
External/Internal Power		Internal Power
Power Feeding Detecting Capability on PD		•
PD Classification		•
RJ45 Pin Assignment		Power over Pairs: 1/2(+); 3/6(-)
Power Management (per-port)	Enable/Disable PoE Per Port	•
	Overloading Protection	•
Power Budget		110W/230W
L2 Features		
Auto-negotiation		•
Auto MDI/MDIX		•
Flow Control (duplex)	802.3x (Full)	•
	Back-Pressure (Half)	•
VLAN	VLAN Group	16
	Tagged Based	•
	Port-based	•
Link Aggregation	IEEE 802.3ad with LACP	•
	Max. LACP Link Aggregation Group	8
IGMP Snooping v1/v2		•
Jumbo Frame Support		9.6K
QoS Features		
CoS	IEEE 802.1p	•
	IP ToS precedence, IP DSCP	•
Security		
Management System User Name/Password Protection		•
Management VLAN		•
Management		
Web Based Management		•
Firmware Upgrade via HTTP		•
Configuration Download/Upload		•
DHCP Client		•
Cable Diagnostics		•
Port Mirroring		One to One or Many to One

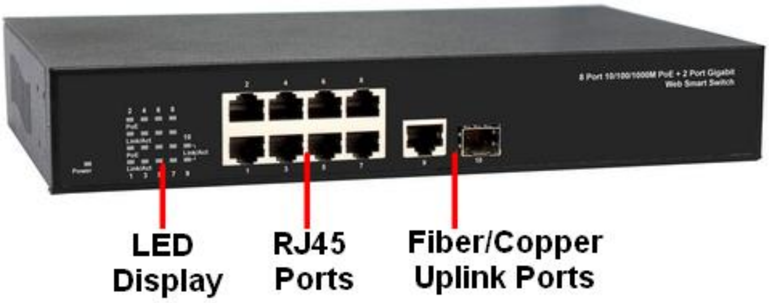
Mechanical	
Power Input	100~240VAC
Dimension (H*W*D)	44*266*161 mm
LED	Power, Link/Act, PoE
Operating Temperature	0 ~ 50°C
Storage Temperature	-20 ~ 85°C
Operating Humidity	10~90% (non-condensing)
Weight	1.8 KG
Certification	CE Mark. Commercial FCC Part 15 Class A; VCCI Class A UL 60950-1
Standard	
IEEE 802.3 – 10BaseT	•
IEEE 802.3u - 100BaseTX	•
IEEE 802.3ab - 1000BaseT	•
IEEE 802.3z 1000BaseSX/LX	•
IEEE 802.3af Power over Ethernet (PoE)	•
IEEE 802.3at Power over Ethernet (PoE+)	•
IEEE 802.3x - Flow Control	•
IEEE 802.1Q - VLAN	•
IEEE 802.1p - Class of Service	•
IEEE 802.3ad - Link Aggregation Control Protocol (LACP)	•

1.3. Hardware Description

This section mainly describes the hardware of this PoE switch and gives a physical and functional overview on the certain switch.

Front Panel

The front panel of this switch consists of 8 10/100/1000 Base-TX RJ-45 ports, 1 Gigabit SFP Uplink port, and 1 1000 Base-T RJ-45 Uplink port. The LED Indicators are also located on the front panel.



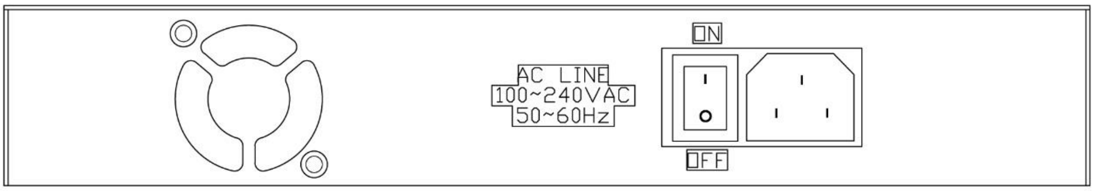
LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

LED	Color/Status	Description
Power	Amber On	Power on
Link/ ACT	Green On	Link Up
	Green Blinking	Data activating
PoE	Amber On	Port is linked to Power Device
	Off	No Power Device is connected

Rear Panel

The 3-pronged power plug is placed at the rear panel of the switch right side shown as below.



1.4. Hardware Installation

To install this switch, please place it on a large flat surface with a power socket close by. This surface should be clean, smooth, and level. Also, please make sure that there is enough space around this switch for RJ45 cable, power cord and ventilation.

If you’re installing this switch on a 19-inch rack, please make sure to use the rack-mount kit (L brackets) and screws come with the product package. All screws must be fastened so the rack-mount kit and your product are tightly conjoined before installing it on your 19-inch rack.

Ethernet cable Request

The wiring cable types are as below:

- 10 Base-T: 2-pair UTP/STP CAT. 3, 4, 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- 100 Base-TX: 2-pair UTP/STP CAT. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- 1000 Base-T: 4-pair UTP/STP CAT. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- PoE: To delivery power properly, it is recommended to use CAT 5e and CAT 6 cable. Ethernet cables of higher qualities can reduce the power lost during transmission.

SFP Installation

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issue.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

For more information regarding to the product safety and maintenance guide, please refer to **Appendix A: Product Safety**.

Chapter 2:

Preparing for Management

In Preparing for Management:

This section will guide your how to manage this product via management web page.

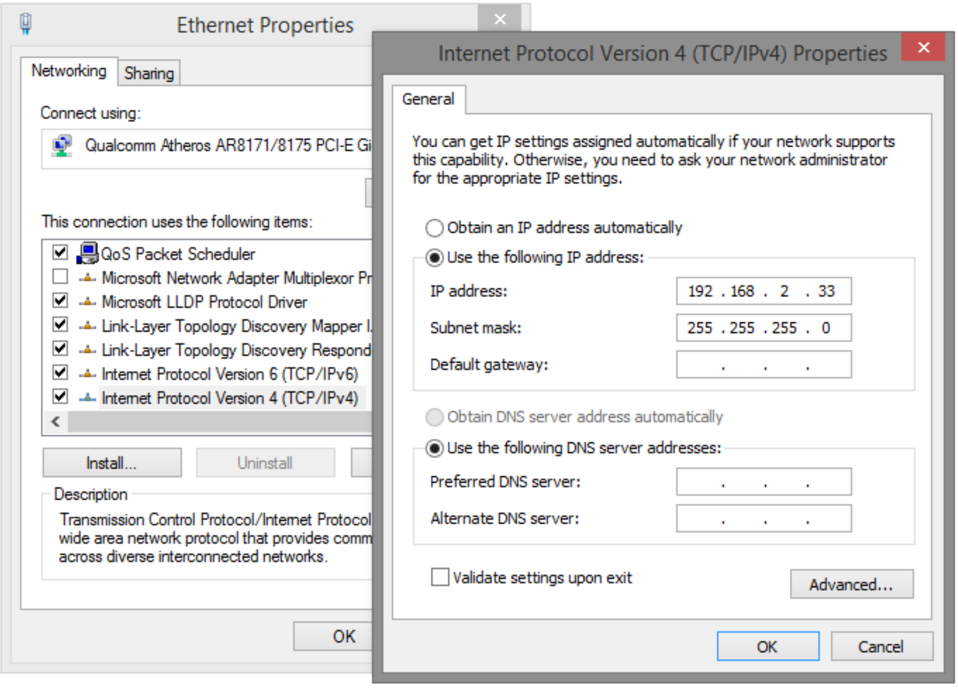
- **Preparation for Web Interface**

2.1. Preparation for Web Interface

The management web page allows you to use a web browser (such as Microsoft IE, Google Chrome, or Mozilla Firefox) to configure and monitor the switch from anywhere on the network.

Before using the web interface to manage your switch, please verify that your switch and your PC are on the same network. Please follow the steps down below to configure your PC properly:

1. Verify that the network interface card (NIC) of your PC is operational and properly installed, and that your operating system supports TCP/IP protocol.
2. Connect your PC with the switch via an RJ45 cable.
3. The default IP address of the switch is **192.168.2.1**. The switch and your PC should locate within the same IP Subnet. Change your PC's IP address to 192.168.2.X, where X can be any number from 2 to 254. Please make sure that the IP address you've assigned to your PC cannot be the same with the switch.



Ethernet Properties

Networking | Sharing

Connect using:
Qualcomm Atheros AR8171/8175 PCI-E Gi

This connection uses the following items:
☑ QoS Packet Scheduler
☐ Microsoft Network Adapter Multiplexor Pr
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I
☑ Link-Layer Topology Discovery Respond
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Install... | Uninstall

Description
Transmission Control Protocol/Internet Protocol wide area network protocol that provides comm across diverse interconnected networks.

OK

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 33
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

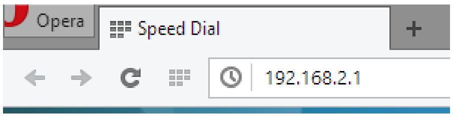
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

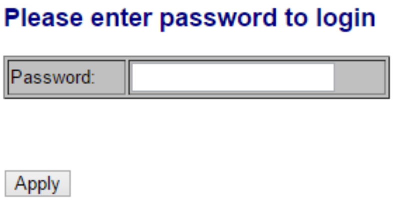
OK | Cancel

4. Launch the web browser (IE, Firefox, or Chrome) on your PC.
5. Type **192.168.2.1** (or the IP address of the switch) in the web browser's URL field, and press Enter.



192.168.2.1

6. The web browser will prompt you to log in. The default password for the configuration web page is **admin**.



For more information, please refer to **Appendix B: IP Configuration for Your PC**.

Chapter 3:

Web Management

In Web Management:

As mentioned in *Chapter 2.1. Preparation for Web Interface*, This switch provides a web-based management interface. You can make all settings and monitor system status with this management web page.

Configuration/Monitor options included in the management web page can be divided into the following 3 categories, which will be discussed in detail in this chapter:

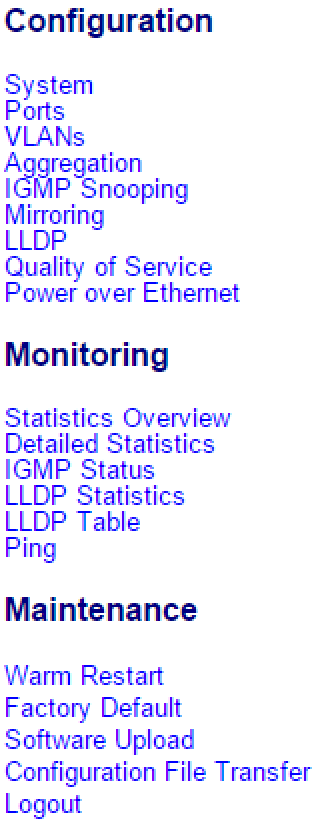
- **Web Management - Configuration**
- **Web Management - Monitoring**
- **Web Management - Maintenance**

3.1. Web Management - Overview

As shown in the figure on the right side, this switch's setting options can be divided into three main categories:

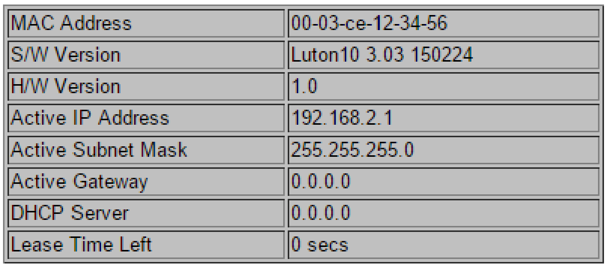
- **Configuration:** Here you can make system configurations. The settings you can configure here include changing the IP address of the switch, setting rate limit of each port, VLAN, IGMP Snooping, Quality of Service (QoS), and Power over Ethernet (turning PoE ON or OFF).
- **Monitoring:** Here you can monitor system status, or performing system diagnostic with VeriPHY and Ping.
- **Maintenance:** This section allows you to make system maintenance such as reboot your switch, reset settings (except switch's IP address) to default value, upload switch firmware, and download/upload system setting values.

The following section will discuss all the functions in detail.



3.2. Web Management - Configuration

3.2.1. Configuration - System



MAC Address	00-03-ce-12-34-56
S/W Version	Luton10 3.03 150224
H/W Version	1.0
Active IP Address	192.168.2.1
Active Subnet Mask	255.255.255.0
Active Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Time Left	0 secs

MAC Address

Displays the unique hardware address assigned by manufacturer (default).

S/W Version

Display the switch’s firmware version.

H/W Version

Display the switch’s Hardware version.

Active IP Address

The current active IP address of the switch.

Active Subnet mask

The current active subnet mask of the IP Address.

Active Gateway

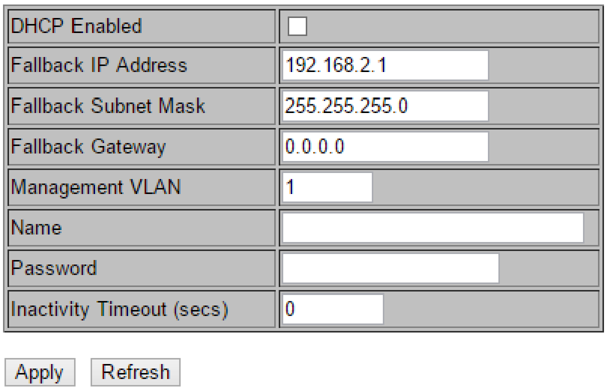
The current active Gateway of the switch.

DHCP Server

The IP of the DHCP Server. Display after DHCP Client enabled.

Lease Time Left

The least received from the DHCP server. Display after the DHCP Client enabled.



DHCP Enabled	□
Fallback IP Address	192.168.2.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	0.0.0.0
Management VLAN	1
Name	
Password	
Inactivity Timeout (secs)	0

DHCP Enabled

Click the box to enable DHCP Client mode.

Fallback IP address

Manually assign the IP address that the network is using. The default IP is 192.168.2.1

Fallback Subnet Mask

Assign the subnet mask to the IP address

Fallback Gateway

Assign the network gateway for industrial switch. The default gateway is 192.168.2.254.

Management VLAN

ID of a configured VLAN (1-4094) through which you can manage the switch. By default, all ports on the switch are members of VLAN 1. However, if the management VLAN is changed, the management station must be attached to a port belonging to this VLAN.

Name

Type in the new user name information.

Password

Type in the new password (The default value of the switch is **admin**).

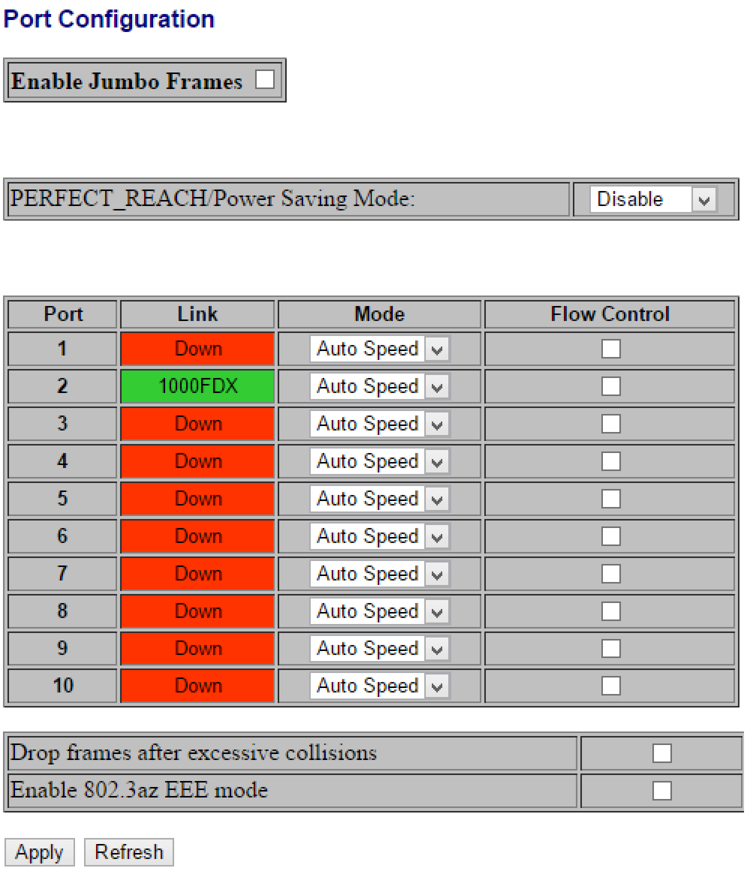
Inactive Timeout

Here you can set the inactive timeout in seconds.

Buttons

- **Apply:** Apply and save all the settings you've made on this page.
- **Refresh:** Refresh the page.

3.2.2. Configuration - Ports



Port Configuration

Enable Jumbo Frames □

PERFECT_REACH/Power Saving Mode: Disable

Port	Link	Mode	Flow Control
1	Down	Auto Speed	□
2	1000FDX	Auto Speed	□
3	Down	Auto Speed	□
4	Down	Auto Speed	□
5	Down	Auto Speed	□
6	Down	Auto Speed	□
7	Down	Auto Speed	□
8	Down	Auto Speed	□
9	Down	Auto Speed	□
10	Down	Auto Speed	□

Drop frames after excessive collisions	□
Enable 802.3az EEE mode	□

Enable Jumbo Frames

This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

Power Saving Mode

Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

Mode

Allows user to manually set the port speed such as Auto, 10 half, 10 Full, 100 Half, 100 Full, 1000 Full or Disabled. User may press Apply button to complete the configuration procedure.

Flow Control

Allows user to manually enable or disable the Flow Control feature. Click the checkbox of the specific ports you and press Apply button to complete the configuration procedure.

Drop frames after excessive collisions

If enabled, the switch will drop frames if excessive collisions happen.

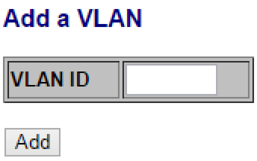
Enable 802.3az EEE mode

EEE (Energy-Efficient Ethernet) is a power saving option that reduces the power usage when there is low or no traffic utilization by powering down circuits when there is no traffic. You can enable this function to save power.

Buttons

- **Apply:** Apply and save all the settings you've made on this page.
- **Refresh:** Refresh the page.

3.2.3. Configuration - VLANs



Add a VLAN

VLAN ID	

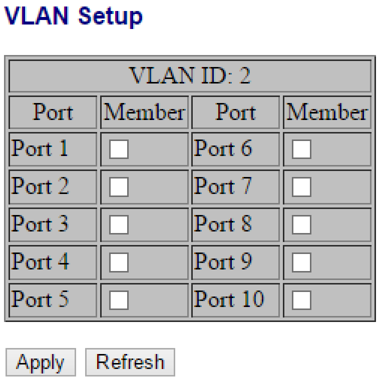
VLAN stands for Virtual LAN, which is a logical network grouping that limits the broadcast domain and allows you to isolate network traffic so that only the members of the same VLAN group can communicate with each other.

VLAN ID

ID of configured VLAN (1-4094, no leading zeroes). Type the new ID and click Add. The web UI is directed to the VLAN Setup screen.

Add

After inputting the VLAN ID, press this button to add a new VLAN with the VLAN ID you inputted.

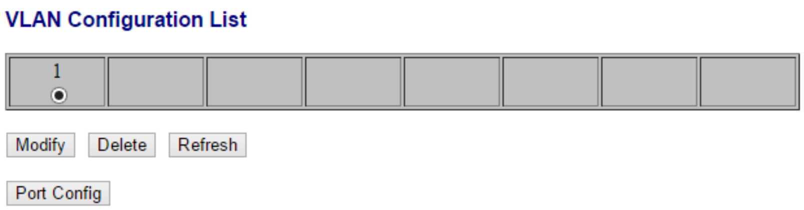


VLAN Setup

VLAN ID: 2			
Port	Member	Port	Member
Port 1	□	Port 6	□
Port 2	□	Port 7	□
Port 3	□	Port 8	□
Port 4	□	Port 9	□
Port 5	□	Port 10	□

Member

Check the check box of the port that you would like to add to the VLAN. Press the **Apply** button to save the settings you've made.



VLAN Configuration List

1 ●							

VLAN Configuration List

Lists all the current VLAN groups created for this system. Up to 16 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

Modify

Press this button to modify the VLAN member port of the selected VLAN.

Delete

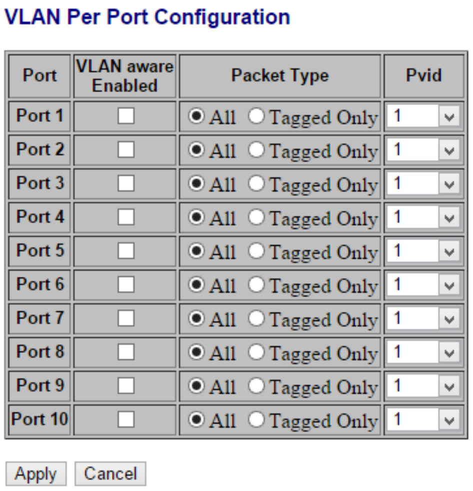
Press this button to delete the selected VLAN.

Refresh

Press this button to refresh web page.

Port Config

Press this button to enter the VLAN Per Port Configuration, as shown in the figure down below.



VLAN Per Port Configuration

Port	VLAN aware Enabled	Packet Type	Pvid
Port 1	□	● All ○ Tagged Only	1
Port 2	□	● All ○ Tagged Only	1
Port 3	□	● All ○ Tagged Only	1
Port 4	□	● All ○ Tagged Only	1
Port 5	□	● All ○ Tagged Only	1
Port 6	□	● All ○ Tagged Only	1
Port 7	□	● All ○ Tagged Only	1
Port 8	□	● All ○ Tagged Only	1
Port 9	□	● All ○ Tagged Only	1
Port 10	□	● All ○ Tagged Only	1

VLAN Aware Enabled

Click the check box to enable the VLAN Aware function.

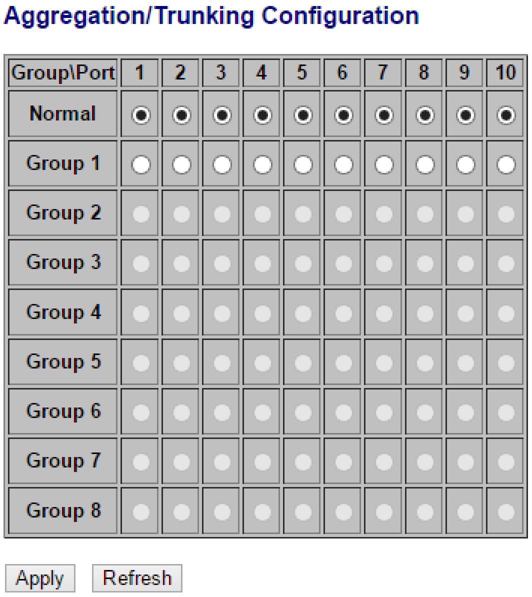
Packet Type

Here you can set if the port will accept all packets, or only packets that are tagged with the set PVID.

PVID

Click the scroll-down menu to select an existing VLAN as the PVID.

3.2.4. Configuration - Aggregation



Aggregation/Trunking Configuration

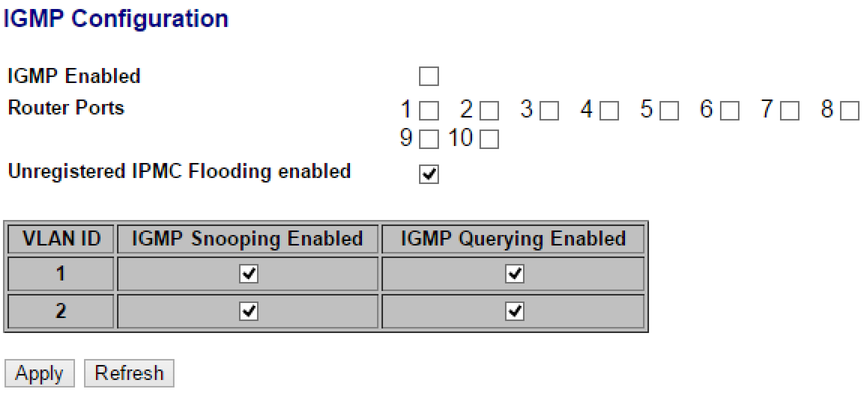
Group\Port	1	2	3	4	5	6	7	8	9	10
Normal	●	●	●	●	●	●	●	●	●	●
Group 1	○	○	○	○	○	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○	○	○
Group 3	○	○	○	○	○	○	○	○	○	○
Group 4	○	○	○	○	○	○	○	○	○	○
Group 5	○	○	○	○	○	○	○	○	○	○
Group 6	○	○	○	○	○	○	○	○	○	○
Group 7	○	○	○	○	○	○	○	○	○	○
Group 8	○	○	○	○	○	○	○	○	○	○

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service.

Aggregation / Trunking Configuration

To assign the ports to a trunk, click on the ports that you would like to set as the same aggregation/trunking group, and click the **Apply** button to save the settings you've made.

3.2.5. Configuration - IGMP Snooping



IGMP Configuration

IGMP Enabled □

Router Ports 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □

Unregistered IPMC Flooding enabled ☑

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	☑
2	☑	☑

IGMP Snooping is the process of listening to IGMP network traffic. IGMP Snooping, as implied by the name, is a feature that allows a Layer 2 switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer3 IGMP packets sent in a multicast network.

When IGMP Snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host’s port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host’s port from the table entry.

Prevents flooding of IP multicast traffic, and limits bandwidth intensive video traffic to only the subscribers.

IGMP Enabled

When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

Router Ports

Set if ports are connecting to the IGMP administrative routers.

Unregistered IPMC Flooding enabled

Set the forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled, and forward to router-ports only when disabled.

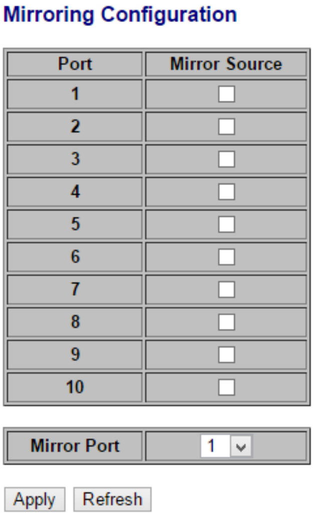
IGMP Snooping Enabled

When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.

IGMP Querying Enabled

When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.

3.2.6. Configuration - Mirroring



Mirroring Configuration

Port	Mirror Source
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□

Mirror Port	1

Port Mirroring is used on a network switch to send a copy of network packets seen on one port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

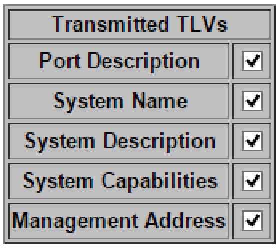
Port to Mirror to

The port that will “duplicate” or “mirror” the traffic on the source port. Only incoming packets can be mirrored. Packets will be dropped when the available egress bandwidth is less than ingress bandwidth.

Ports to Mirror

Select the ports that you want to mirror from this section of the page. A port will be mirrored when the “Mirroring Enabled” check-box is checked.

3.2.7. Configuration - LLDP



Transmitted TLVs	
Port Description	☑
System Name	☑
System Description	☑
System Capabilities	☑
Management Address	☑

Port Description

When checked the "port description" is included in LLDP information transmitted.

System Name

When checked the "system name" is included in LLDP information transmitted.

System Description

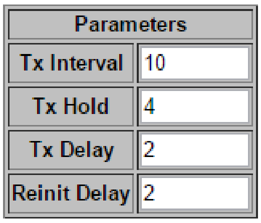
When checked the "system description" is included in LLDP information transmitted.

System Capabilities

When checked the "system capability" is included in LLDP information transmitted.

Management Address

When checked the "management address" is included in LLDP information transmitted.



Parameters	
Tx Interval	10
Tx Hold	4
Tx Delay	2
Reinit Delay	2

Tx Interval

The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value.

Tx Hold

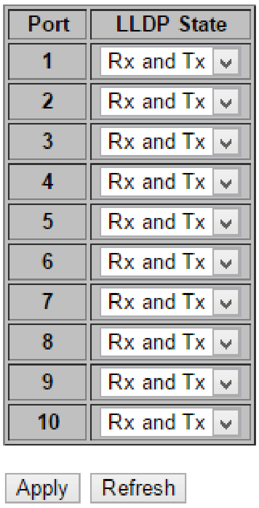
Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value.

Reinit Delay

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization.



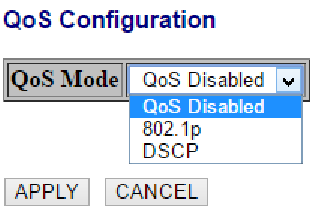
Port	LLDP State
1	Rx and Tx
2	Rx and Tx
3	Rx and Tx
4	Rx and Tx
5	Rx and Tx
6	Rx and Tx
7	Rx and Tx
8	Rx and Tx
9	Rx and Tx
10	Rx and Tx

LLDP State

Select LLDP mode here. The modes here available here include:

- **Rx and Tx:** The switch will send out LLDP information, and will analyze LLDP information received from neighbours.
- **Rx only:** The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed.
- **Tx only:** The switch will drop LLDP information received from neighbours, but will send out LLDP information.
- **Disabled:** The switch will not send out LLDP information, and will drop LLDP information received from neighbours.

3.2.8. Configuration - Quality of Service

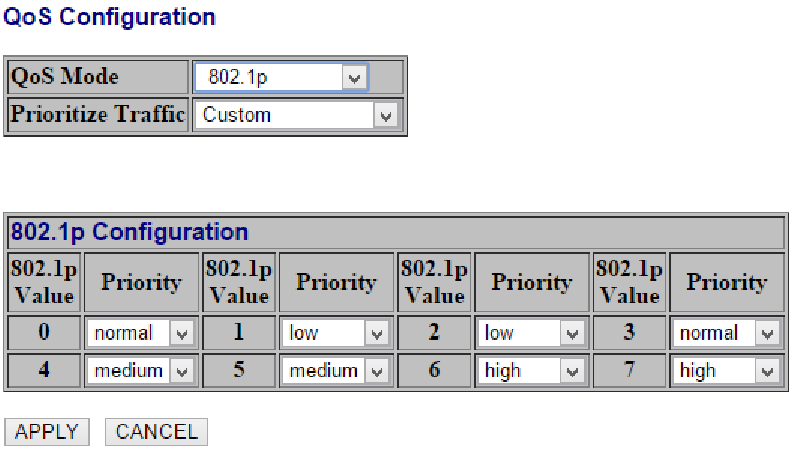


QoS Configuration

QoS Mode	QoS Disabled

This switch supports IEEE 802.1p and DSCP for QoS. Click the QoS Mode scroll-down menu to choose the QoS mode you would like to apply, and the QoS Configuration will change according.

QoS IEEE 802.1p



QoS Configuration

QoS Mode	802.1p
Prioritize Traffic	Custom

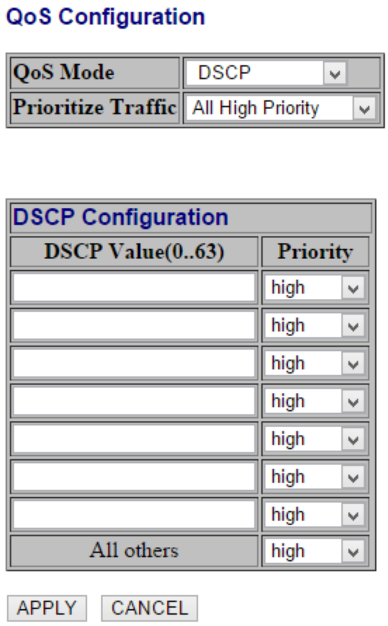
802.1p Configuration

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal	1	low	2	low	3	normal
4	medium	5	medium	6	high	7	high

Packets are prioritized using the 802.1p field in the VLAN tag. This field is three bits long, representing the values 0 - 7. When the QoS Mode is set to 802.1p, the 802.1p Configuration table appears, allowing you to map each of the eight 802.1p values to a local priority queue (low, normal, medium or high). The default settings are shown below.

When the QoS Mode is set to 802.1p, the 802.1p Configuration table is displayed as shown below. The Custom Prioritize Traffic is the default and suggested value.

QoS DSCP



QoS Configuration

QoS Mode	DSCP
Prioritize Traffic	All High Priority

DSCP Configuration

DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

In DSCP mode, packets are prioritized using the DSCP (Differentiated Services Code Point) value. The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0 - 63. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, allowing you to map each of the DSCP values to a hardware output queue (low, normal, medium or high). The default settings map all DSCP values to the high priority egress queue.

User can use the Prioritize Traffic drop-down list to quickly set the values in the DSCP Configuration table to a common priority queue. Use Custom if you want to set each value individually.

When the QoS Mode is set to DSCP, the DSCP Configuration table is displayed as shown below.

Strict

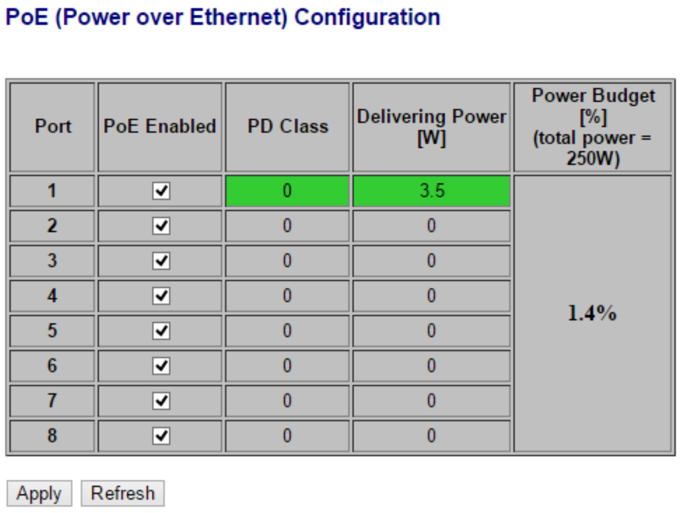
Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

WRR

Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights with default values of 1, 2, 4, 8 for queues 0 through 7, respectively. (This is the default selection.)

Note: WRR can only be selected if Jumbo Frame mode is disabled on the Port Configuration page

3.2.9. Configuration - Power over Ethernet



PoE (Power over Ethernet) Configuration

Port	PoE Enabled	PD Class	Delivering Power [W]	Power Budget [%] (total power = 250W)
1	☑	0	3.5	1.4%
2	☑	0	0	
3	☑	0	0	
4	☑	0	0	
5	☑	0	0	
6	☑	0	0	
7	☑	0	0	
8	☑	0	0	

PoE (Power over Ethernet) technology is a system to pass electrical power safely, along with data, on Ethernet cabling. Power is supplied in common mode over two or more of the differential pairs of sires found in the Ethernet cables and comes from a power supply within a PoE enabled networking device such as Switch or can be injected into a cable run with a mid-span power supply.

This screen shows all the PoE status when connect or disconnect to the PD devise.

PoE Enabled

POE of the port is able to supply power to the attached PD (Powered Device)

PD Class

Detect the class of PD

Delivering Power (W)

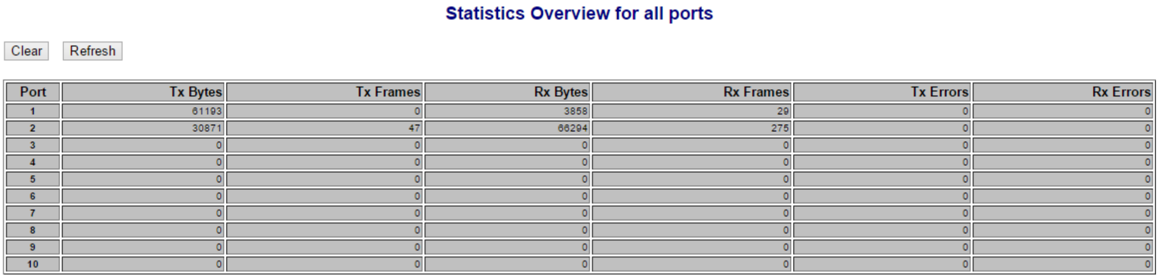
The power (in Watt) that is delivered to the PD device connected to the port.

Power Budget Percentage

This field displays the total PoE power used.

3.3. Web Management - Monitoring

3.3.1. Monitoring - Statistics Overview



Statistics Overview for all ports

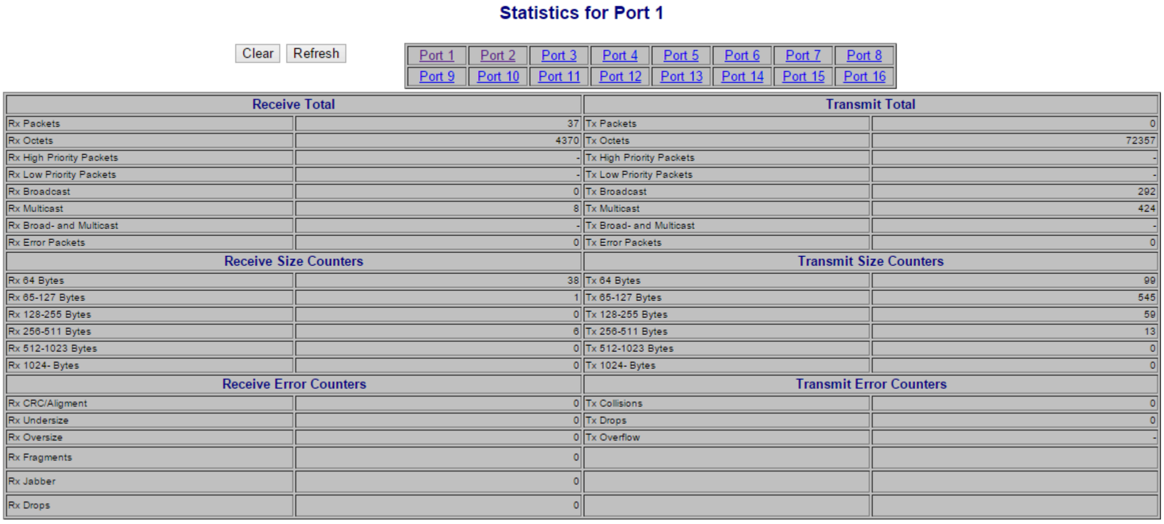
Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	61193	0	3858	29	0	0
2	30871	47	66294	275	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

This page displays the TX/RX Bytes/Frames/Errors of the switch.

Buttons

- **Clear:** Clear all the counters listed here.
- **Refresh:** Refresh the page.

3.3.2. Monitoring - Detailed Statistics



Statistics for Port 1

Receive Total		Transmit Total	
Rx Packets	37	Tx Packets	0
Rx Octets	4370	Tx Octets	72357
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	0	Tx Broadcast	292
Rx Multicast	8	Tx Multicast	424
Rx Broad- and Multicast	-	Tx Broad- and Multicast	-
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	38	Tx 64 Bytes	99
Rx 65-127 Bytes	1	Tx 65-127 Bytes	545
Rx 128-255 Bytes	0	Tx 128-255 Bytes	59
Rx 256-511 Bytes	6	Tx 256-511 Bytes	13
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024- Bytes	0	Tx 1024- Bytes	0
Receive Error Counters		Transmit Error Counters	
Rx CRC/Aligment	0	Tx Collisions	0
Rx Undersize	0	Tx Drops	0
Rx Oversize	0	Tx Overflow	-
Rx Fragments	0		
Rx Jabber	0		
Rx Drops	0		

This page displays the detailed information regarding to each port of the switch.

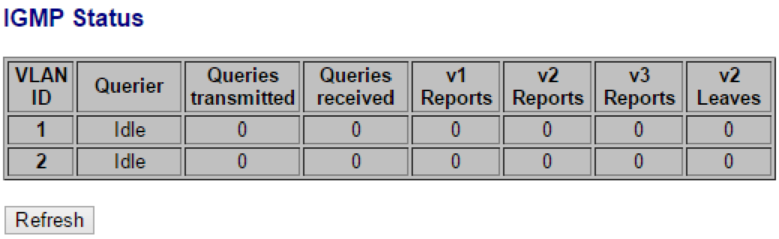
Ports

Press the hyper-link listed to display detailed information regarding to each port.

Buttons

- **Clear:** Clear all the counters listed here.
- **Refresh:** Refresh the page.

3.3.3. Monitoring - IGMP Status



IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	0	0	0	0	0
2	Idle	0	0	0	0	0	0

VLAN ID

VLAN ID number.

Querier

Show whether Querying is enabled.

Queries transmitted

Show the number of transmitted Query packets.

Queries received

Show the number of received Query packets.

v1 Reports

Show the number of received v1 Report packets.

v2 Reports

Show the number of received v2 Report packets.

v3 Reports

Show the number of received v2 Report packets.

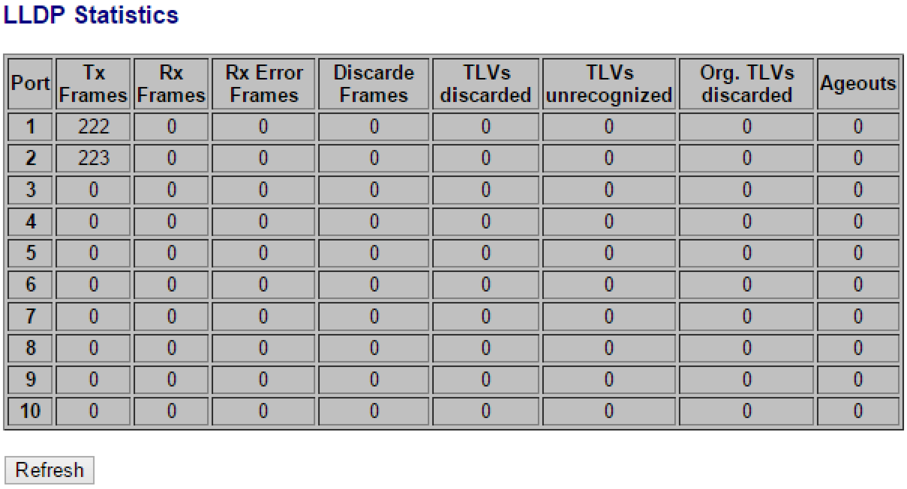
v3 Leave

Show the number of v3 leave packets received.

Buttons

- **Refresh:** Refresh the page.

3.3.4. Monitoring - LLDP Statistics



LLDP Statistics

Port	Tx Frames	Rx Frames	Rx Error Frames	Discarde Frames	TLVs discarded	TLVs unrecognized	Org. TLVs discarded	Ageouts
1	222	0	0	0	0	0	0	0
2	223	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Tx Frames

The number of LLDP frames transmitted on the port.

Rx Frames

The number of LLDP frames received on the port.

Rx Error

The number of received LLDP frames containing some kind of error.

Discarded Frames

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

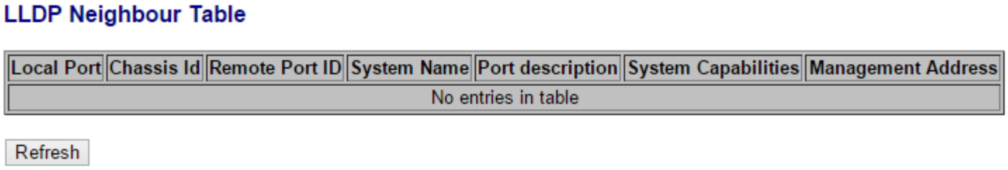
Org. TLVs Discarded

The number of organizationally received TLVs.

Ageouts

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

3.3.5. Monitoring - LLDP Table



LLDP Neighbour Table

Local Port	Chassis Id	Remote Port ID	System Name	Port description	System Capabilities	Management Address
No entries in table						

Local Port

The port on which the LLDP frame was received.

Chassis ID

The Chassis ID is the identification of the neighbor's LLDP frames.

Remote Port ID

The Remote Port ID is the identification of the neighbour port.

System Name

System Name is the name advertised by the neighbour unit.

Port Description

Port Description is the port description advertised by the neighbour unit.

System Capabilities

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

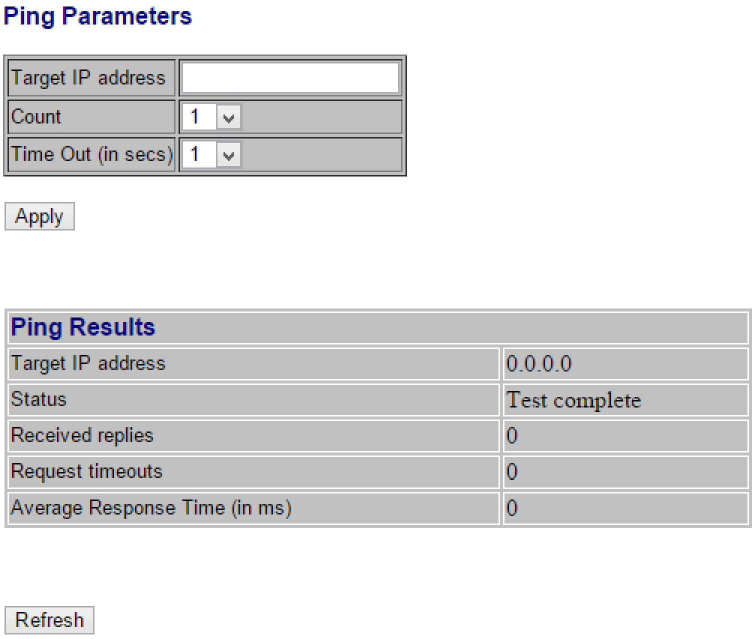
1. Other
2. Repeater
3. Bridge
4. WAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

3.3.6. Monitoring - Ping



Ping Parameters

Target IP address	
Count	1 ▾
Time Out (in secs)	1 ▾

Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Target IP Address

IP address of the host

Count

Number of packets to send. (Range: 1-20)

Time Out

setting the time period of host will be Ping

Normal response

The normal response occurs in one to ten seconds, depending on network traffic.

Destination does not respond

If the host does not respond, a “timeout” appears in ten seconds.

Destination unreachable

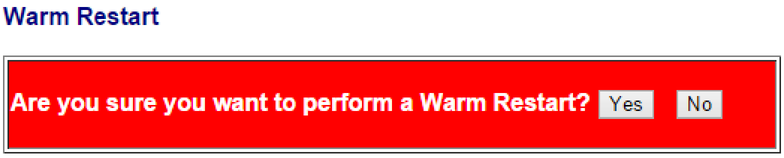
The gateway for this destination indicates that the destination is unreachable.

Network or host unreachable

The gateway found no corresponding entry in the route table.

3.4. Web Management - Maintenance

3.4.1. Maintenance - Warm Restart



Warm Restart

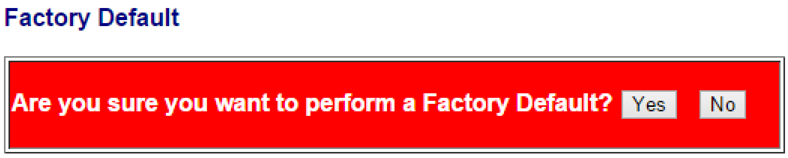
Are you sure you want to perform a Warm Restart?

Here you can reboot the switch.

Buttons

- **Yes:** Reboot the switch.
- **No:** Cancel switch rebooting.

3.4.2. Maintenance - Factory Default



Factory Default

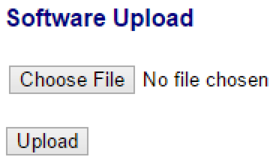
Are you sure you want to perform a Factory Default?

You can reset all current settings back to the switch's factory default settings. Please note that the switch must be ON while the resetting process.

Buttons

- **Yes:** Reset all settings of the switch back to the factory default settings, including switch's IP address and system administrator password.
- **No:** Cancel resetting all settings back to the factory default settings.

3.4.3. Maintenance - Software Upload



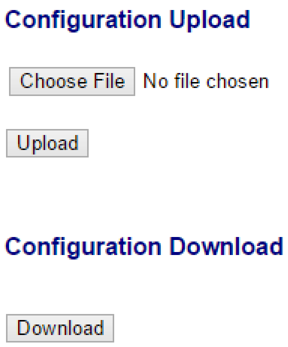
Software Upload

Here you can upload firmware from your PC to the switch.

Buttons

- **Choose File:** Press this button to choose the firmware file you would like to update to the switch.
- **Upload:** After choosing the firmware file, press this button to upload the firmware. Please note that the switch MUST BE ON during the uploading process. Turning the switch's power off during the uploading process might cause system malfunction. Also, it is highly recommended to reset your switch's setting back to factory default after uploading the firmware.

3.4.4. Maintenance - Configuration File Transfer



Here you can upload pre-saved configuration file, or save all the current settings as a "*.cfg" file.

Configuration Upload

Buttons

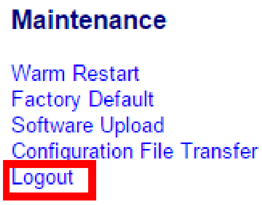
- **Choose File:** Press this button to choose the pre-saved configuration file.
- **Upload:** After choosing the configuration file, press this button to upload the file. Please note that the switch MUST BE ON during the uploading process. Turning the switch's power off during the uploading process might cause system malfunction.

Configuration Download

Buttons

- **Download:** Press this button to save all the current settings as a "*.cfg" file.

3.4.5. Maintenance - Logout



Maintenance

Warm Restart
Factory Default
Software Upload
Configuration File Transfer
Logout

Press the “Logout” option on the management web page to logout. It is highly recommended to logout after using the switch’s management web page. Also, the system will automatically logout if the management web page is not active after a set of time.

Appendix A: Product Safety

This appendix describes safety issues regarding to this product. To use this product safely, it is highly recommended to read this appendix before installing and using this product.

Failure to follow these precautions and warnings might cause product malfunction, electrical shock, or even fire. If this product is working abnormally (e.g. generating smoke), please stop using this product and contact your distributor or retailer immediately.

DO NOT install this product under conditions listed below:

- DO NOT install this product in an environment with conditions exceeding its specified operating environment.
- DO NOT install this product in an environment that is subjected to direct sunlight or near any heating equipment.
- DO NOT install this product in an environment with extreme temperature changes. Extreme temperature changes, even within the product's operating temperature range, may cause malfunctions.
- DO NOT install this product in a location near any sources of water or liquid.
- DO NOT stack this product with other network devices directly on top of one another. Stacking network devices directly without applying a mounting rack will cause this product to overheat.
- DO NOT install this product on an unstable surface. Doing so might cause this product to fall, resulting malfunction.

Product Maintenance Guide:

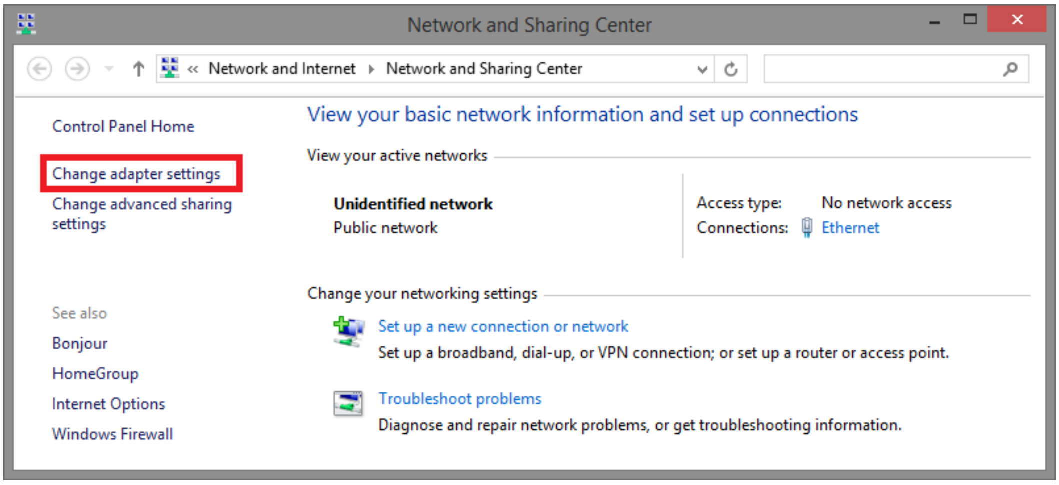
- DO NOT disassemble this product. Doing so might cause malfunction and void your product's warranty.
- It is recommended to keep your product clear of dust. To remove dust from your product, please use a dry brush and brush it off gently.
- When not using this product, please store it in an environment with low humidity, cool temperature, and free of dust. Failure to do so might cause malfunction.
- Before powering up this product, please make sure that the electric power source meets this product's requirement. DO NOT use other power adapters if this product comes with its own power adapter in the package.

Appendix B: IP Configuration for Your PC

This appendix describes how to set the IP address of your PC so you can connect to product configuration webpage. The configuration webpage allows you to set system variables or monitor system status.

The following section will guide you to set the IP address properly in a Microsoft Windows 8 environment. Setting IP address in other Microsoft operating system (such as Windows Vista or Windows 7) is quite the same and can be related.

1. Open **Network and Sharing Center** in **Control Panel**, and click on **Change adapter settings** as shown in the figure down below.


Network and Sharing Center
« Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Bonjour
HomeGroup
Internet Options
Windows Firewall

View your basic network information and set up connections

View your active networks

Unidentified network
Public network

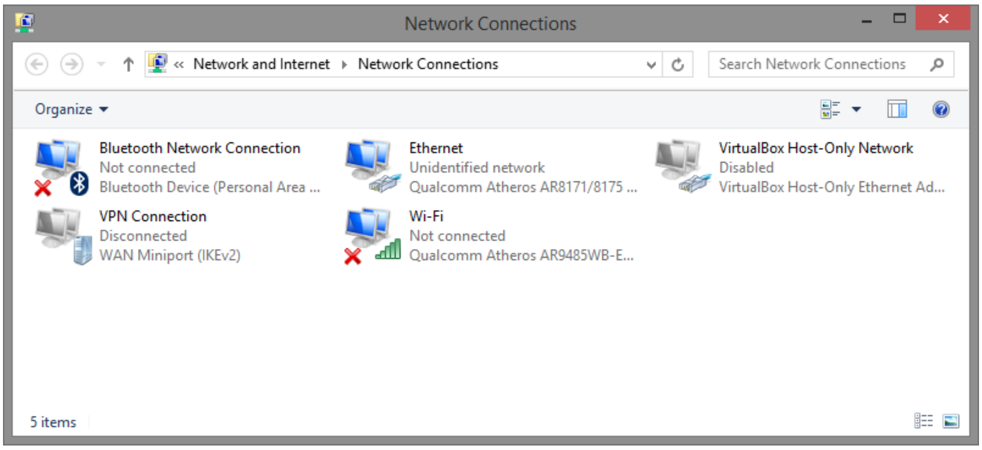
Access type: No network access
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2. A **Network Connections** window will pop up, **showing** all the network connections available on your PC. Please double-click on the network connection you are using to connect the


Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize ▾

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Ethernet
Unidentified network
Qualcomm Atheros AR8171/8175 ...

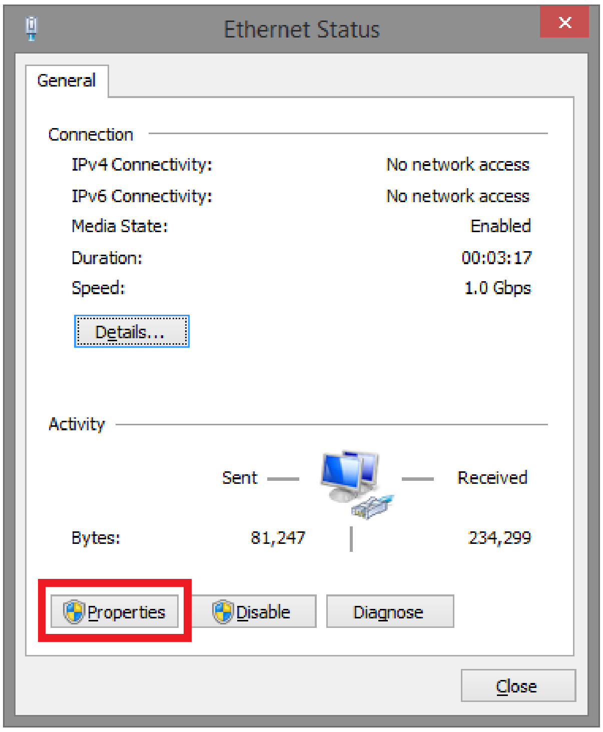
VirtualBox Host-Only Network
Disabled
VirtualBox Host-Only Ethernet Ad...

VPN Connection
Disconnected
WAN Miniport (IKEv2)

Wi-Fi
Not connected
Qualcomm Atheros AR9485WB-E...

5 items

3. An **Ethernet Status** window will pop up. Please click on the **Properties** button as shown in the figure down below.



Ethernet Status

General

Connection

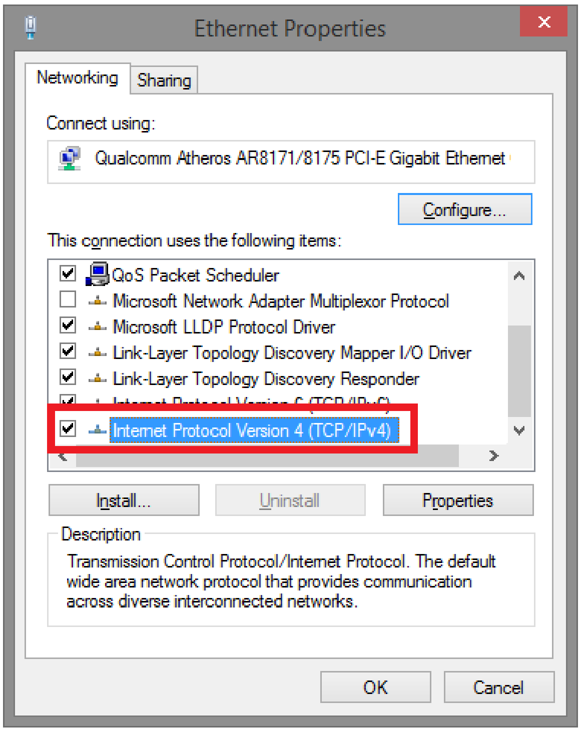
IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:03:17
Speed: 1.0 Gbps

Activity

Sent — Received

Bytes: 81,247 | 234,299

4. An **Ethernet Properties** window will pop up. Please double click on the **Internet Protocol Version 4 (TCP/IPv4)**.



Ethernet Properties

Networking | Sharing

Connect using:

Qualcomm Atheros AR8171/8175 PCI-E Gigabit Ethernet

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

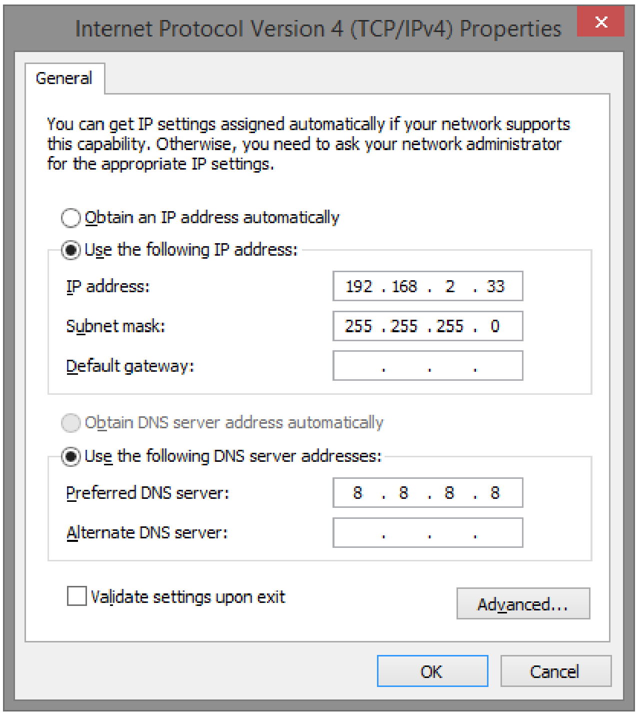
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. An **Internet Protocol Version 4 (TCP/IPv4) Properties** window will pop up. Please set your PC's IP address and subnet mask as shown in the figure down below.

   By default, your product's IP address should be **192.168.2.1**.You can set any IP address as long as it's not the same with your product's IP address and is in the same network segment with your product's IP address.

   Press **OK** to apply the TCP/IPv4 settings you just made. Now you can connect to your product using a web browser (i.e. Internet Explorer, Chrome, or Firefox).



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 33
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .

□ Validate settings upon exit

Appendix C: Glossary

This appendix contains the terms and glossaries that are used in this user manual.

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 **L**ogical **L**ink **C**ontrol (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the **M**ultiple **S**panning **T**ree **P**rotocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for **P**riority **C**ode **P**oint. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for **P**ower **O**ver **E**thernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for **P**recision **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The **S**ub **N**etwork **A**ccess **P**rotocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**cess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.