8-PORT GIGABIT ETHERNET POE+ WEB-MANAGED SWITCH WITH 2 SFP PORTS USER MANUAL

MODEL 561051

INT-561051-UM-1015-0

Table of Contents

1 Product Introduction

Thank you for purchasing the Intellinet 8-Port Gigabit Ethernet PoE+ Web-Managed Switch (561051). This user guide covers all aspects of the installation of this product. Note that some of the configuration options require the user to have advanced knowledge of TCP/IP networks.

1.1 Product Overview

The Intellinet 8-Port Gigabit Ethernet PoE+ Web-Managed Switch (561051) is designed to pass both data and electrical power to a number of PoE-compatible devices via standard Cat5e or Cat6 network cables. Equipped with eight Gigabit Ethernet ports (all of which support 802.3at/af PoE/PoE+), this switch can power wireless LAN access points and bridges, VoIP phones, IP video cameras and more while delivering network speeds of up to 1000 Mbps.

1.1.1 Features

- Provides power and data connection for up to eight PoE network devices
- For use on desktop or mounted in standard 19" rack Supports All power up to 140W
- IEEE 802.3at/af-compliant RJ45 PoE/PoE+ output ports Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode
- PoE power budget of 140 watts Supports WEB management interface
- Supports IEEE 802.3at and IEEE 802.3af-compliant PoE devices (wireless access points, VoIP phones, IP cameras) Internal power adapter supply
- Green Ethernet power-saving technology deactivates unused ports and adjusts power levels based on the cable length

1.2 External Component Description

1.2.1 Front Panel

The front panel of the Switch consists of 8 x 10/100/1000Mbps RJ-45 ports, 1 x Console port, 2 x SFP ports, 1 x Reset button and a series of LED indicators.

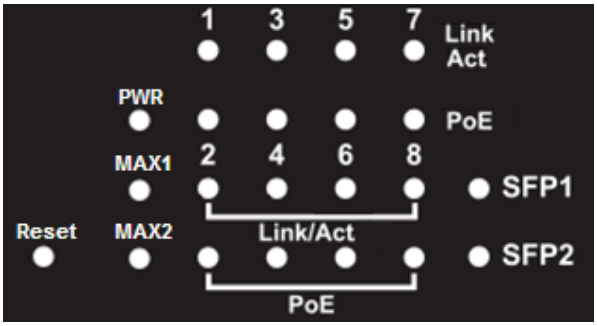
10/100/1000Mbps RJ-45 ports (1~8):
Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.

Console port (Console):
Connect to the Intellinet switch with a serial port of a computer or terminal for monitoring and configuration purposes.

SFP ports (SFP1, SFP2):
Designed to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Reset button (Reset):
While the device is powered on, press the button for 2 seconds to reboot the switch, and press the button for 5 seconds to restore the switch to its original factory default settings.

LED indicators:
The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the switch.



The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
PWR	Green	On	Power On
		Off	Power Off
Link/Act (1-8)	10/100M: Orange	On	A device is connected to the port.
	1000M: Green	Off	No device connected to the port.
		Flashing	Sending or receiving data.
PoE	Green	On	A Powered Device (PD) is connected to the port, and power is being provided.
		Off	No PD is connected to the corresponding port, or no power is supplied to the port.
		Flashing	PoE overload or short circuit. Disconnect the PD right away.
Max 1 (1-4Ports)	Green	On	When the power which output to PDs has reached the maximum power budget(The power of all the connected PoE ports is ≥55W). No power may be supplied if additional PDs are connected.
		Off	The power of all the connected PoE ports is <55W, or No PD connected to the corresponding port.
		Flashing	When the power which output to PDs has exceeded the maximum power budget(The power of all the connected PoE port is ≥70W).
Max 2 (5-8Ports)	Green	On	When the power which output to PDs has reached the maximum power budget(The power of all the connected PoE ports is ≥55W). No power may be supplied if additional PDs are connected.
		Off	The power of all the connected PoE ports is <55W, or No PD connected to the corresponding port.
		Flashing	When the power which output to PDs has exceeded the maximum power budget (The power of all the connected PoE port is ≥70W).
SFP1 SFP2	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

1.2.2 Rear Panel

AC Power Connector:
Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.

1.3 Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- 8-Port Gigabit Ethernet PoE+ Web-Managed Switch with 2 SFP Ports
- Four rubber feet, two mounting ears and eights screws
- One AC power cord
- One Quick Installation Guide
- Installation CD with User Manual

2 Installing and Connecting the Switch

This part describes how to install your PoE Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1 Installation

The following steps will help prevent damage to the device while also helping to maintain proper security.

- Place the switch on a stable surface or desktop to minimize the chances of falling.
- Make sure the switch works in the proper AC input range and matches the voltage labeled on the switch.
- To keep the switch free from lightning damage, do not open the switch's chassis even if it fails to receive power.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch.

2.1.1 Desktop Installation

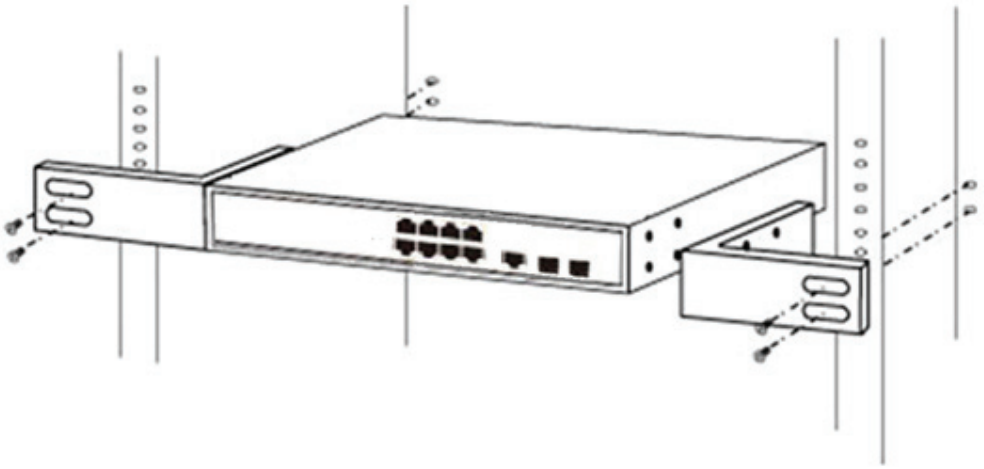
When installing the switch on a desktop (if not in a rack), attach the enclosed rubber feet to the bottom corners of the switch to minimize vibration. Allow adequate space for ventilation between the device and the objects around it.

2.1.2 Rack-mountable Installation in 11-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 11-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

a. Attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

b. Use the screws provided with the 10"rack or cabinet to mount the switch on the rack and tighten it.



2.1.3 Power on the Switch

The switch is powered on by connecting it to an outlet using the AC 100-240V 50/60Hz internal high-performance power supply.

AC Electrical Outlet:
It is recommended to use a single-phase, three-wire receptacle with a neutral outlet or multifunctional computer professional receptacle. Be sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:
Connect the AC power connector on the back panel of the switch to an external receptacle with the included power cord, then check that the power indicator is ON. When it is ON, it indicates the power connection is okay.
PD port by network cable.

3 How to Login the Switch

3.1 Connecting Computer

Use standard Cat5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which they are connected.

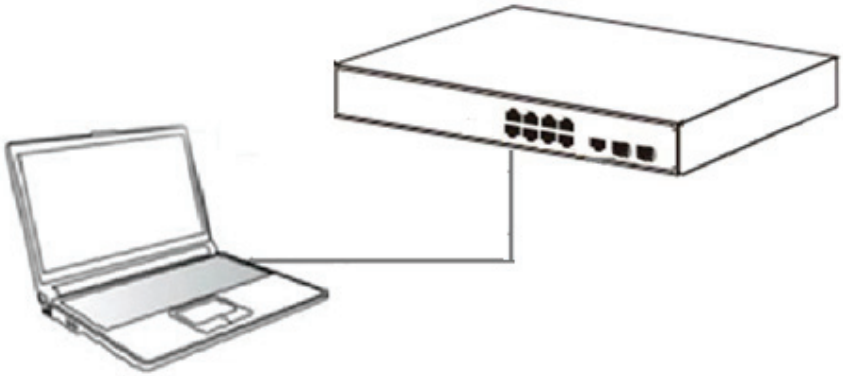


Figure 6 - PC Connect

The LNK/ACT/Speed LEDs for each port light when the link is available.

3.2 How to Login to the Switch

Connection is done by means of any standard web browser. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.2.1
Default user name	admin
Default password	admin

You can log on to the configuration window of the Switch through following steps:

1. Connect the Switch with the computer NIC interface.
2. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx (“xxx” ranges 2~254), for example, 192.168.2.100.
3. Power on the Switch and verify that you have an active link on the port you are connected to.
4. Open the browser, and enter *http://192.168.2.1* and then press “Enter”. The Switch login window appears, as shown below.

5. Enter the Username and Password (The factory default Username is **admin** and Password is **admin**), and then click “LOGIN” to log in to the web configuration.

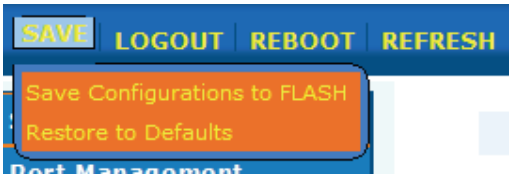
4 Switch Configuration

The PoE+ Web-Managed Gigabit Ethernet Switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the Web-based management interface (Web UI) for this switch.

In the Web UI, the left column shows the configuration menu. The top row shows the switch's current link status. Green squares indicate the port link is up (port 5 in the example below), while black squares indicate the port link is down. Below the switch panel, you can find toolbar (see section 4.1) that provides access to some basic, yet important features. The rest of the screen area displays the configuration settings.

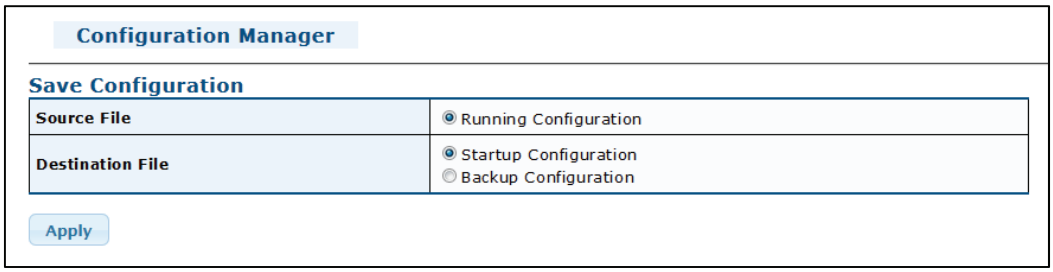
4.1 Toolbar

4.1.1 SAVE



4.1.1.1 Save Configurations to FLASH

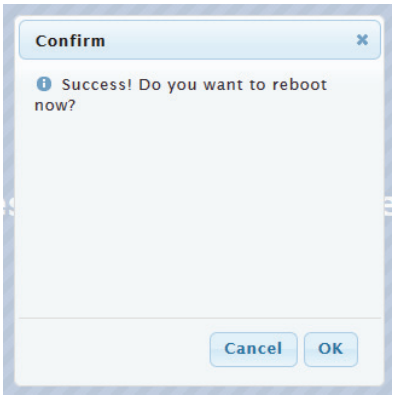
Whenever you make any changes to the configuration of the switch, and you want those changes to be available after the next reboot of the switch, you need to save the configuration. To do that, click on **Save Configurations to Flash**, then click **Apply.**



4.1.1.2 Restore to Defaults

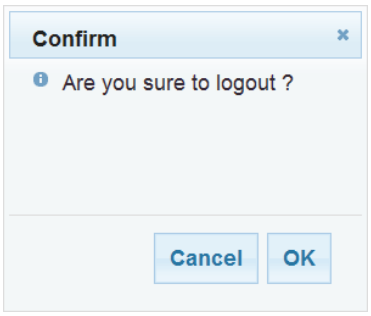
In order to delete all custom configuration data and restore the switch to its factory default state, click on **Restore to Defaults**.

Click on **Restore**, and confirm the next message by clicking **OK**.



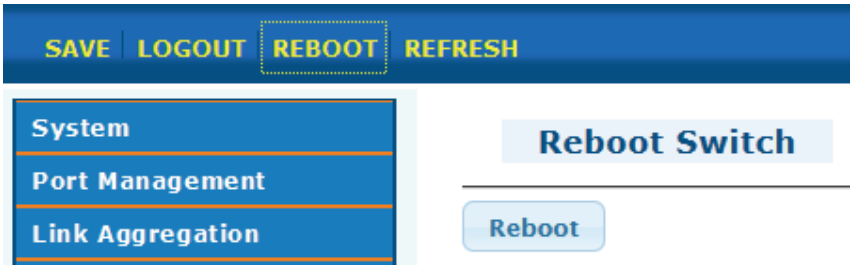
4.1.2 LOGOUT

In order to log out from the web administrator interface, click on **LOGOUT** and then confirm the next message by clicking **OK**.



4.1.3 REBOOT

Click **Reboot** in order to restart the Intellinet switch. After the restart has been completed, you have to re-authenticate at the login page in order to re-gain access.



4.1.4 REFRESH

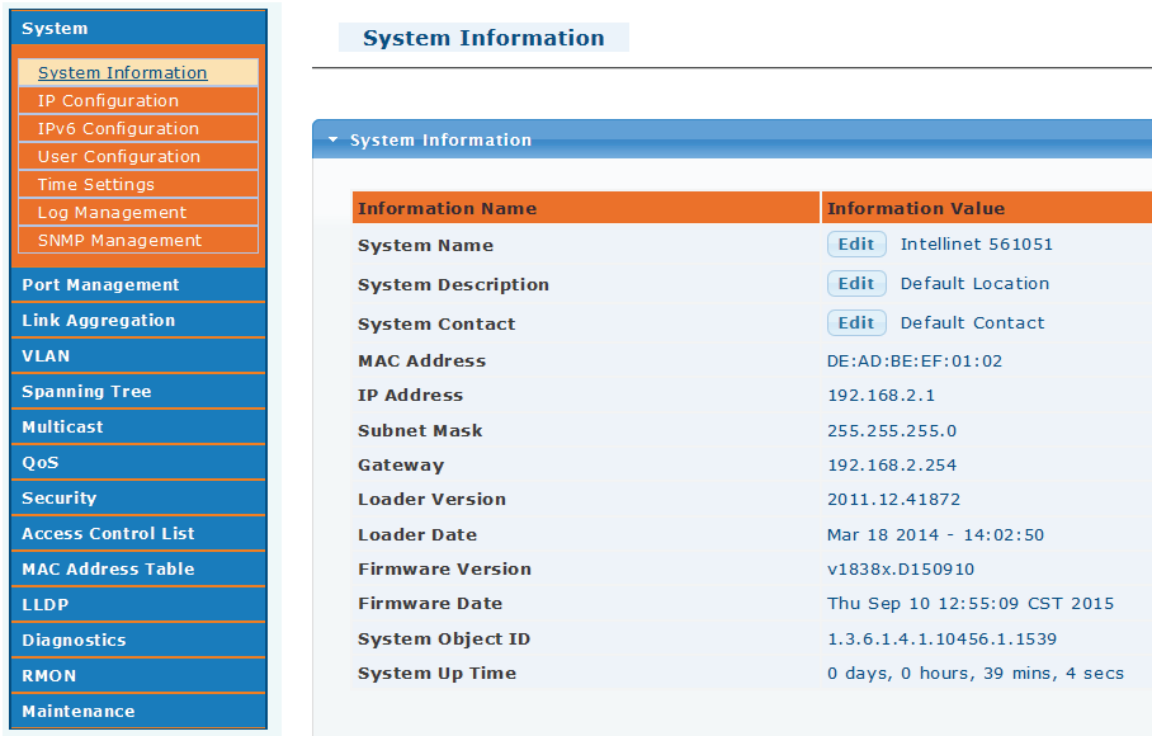
Reloads the contents of the current screen to show the most current information.

4.2 System

Use the Status pages to view system information and status.

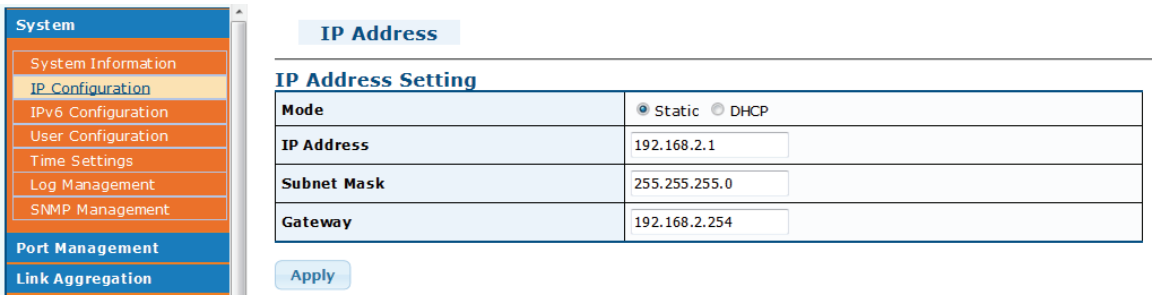
4.2.1 System Information

This page allows you to configure System-related information and browse information such as MAC address, IP address, firmware version, loader version, among others. In addition, you can modify the values **System Name, System Location and System Contact:**



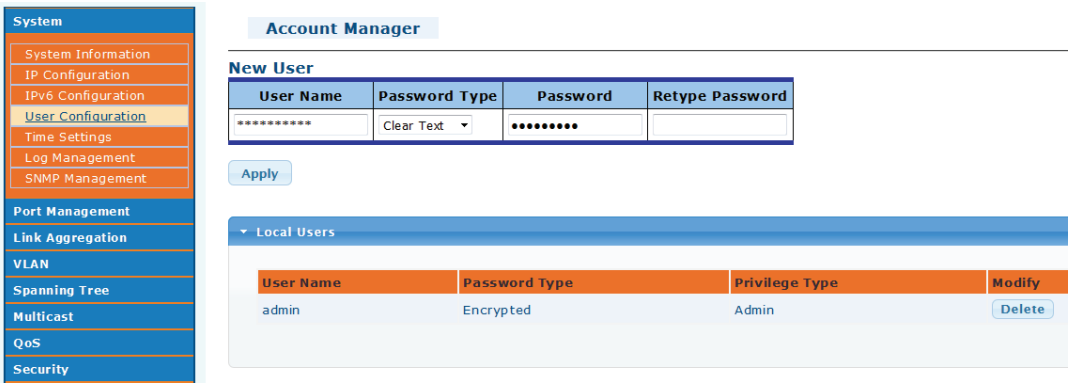
4.2.2 IP Configuration

On this page you set up the management IP address of the Intellinet PoE switch. Set the mode to either **DHCP** or **Static**, and in the latter case provide the **IP Address, Subnet Mask and Gateway.** This page allows to define the IPv4 address. Also refer to the **IPv6 configuration**.



4.2.3 User Configuration

On this screen you can change the password of the administrator account, and you can also create new user accounts. The Intellinet PoE switch only provides administrator level user accounts, which simplifies the setup.

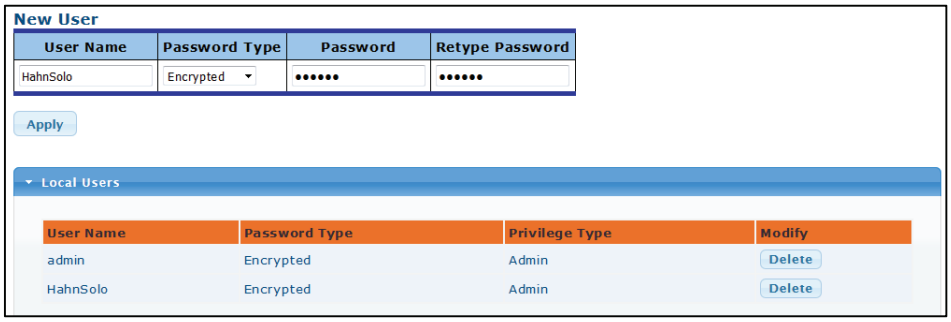


4.2.3.1 Add User Account

Type in a user name, a password and re-type the password. You also can select the password encryption type. Set to **encrypted** for maximum security, or **No Password** if you want to create an administrator account that requires no password in order to log in.

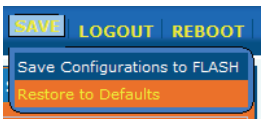
4.2.3.2 Edit Password for existing User Account

If you want to change a password of an existing account, you have to add the existing user account as a new user account. By adding a user account with a user name that already exists, you can overwrite the password of that account. The example below shows how you would change the password of existing user 'HahnSolo'.



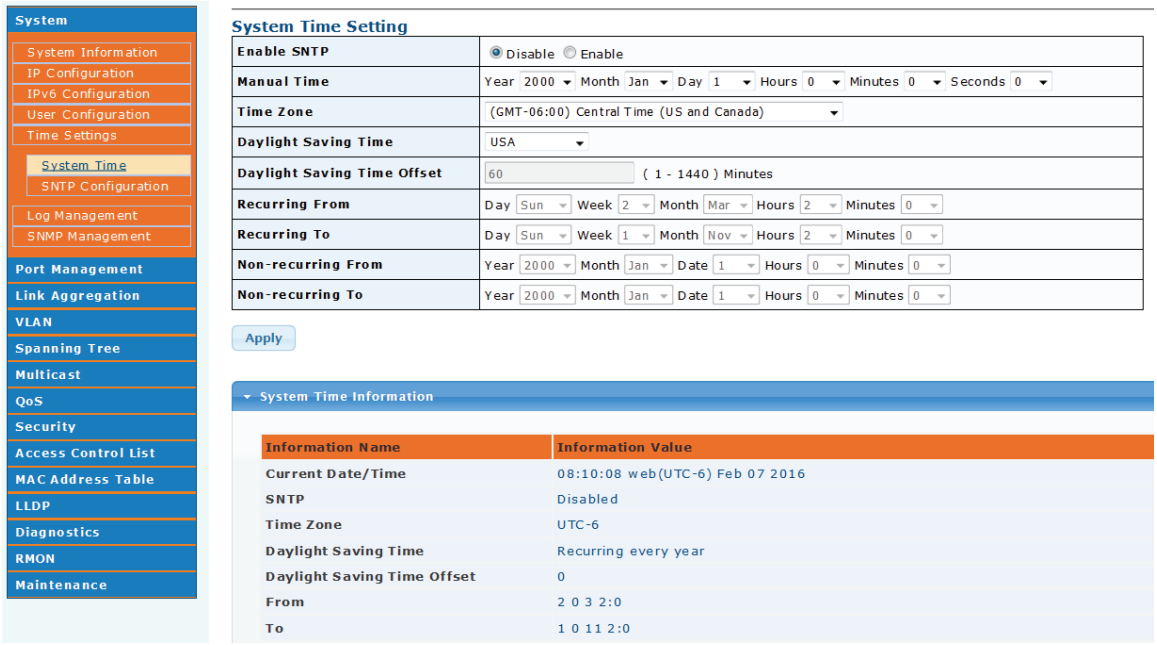
4.2.3.3 Delete User Account

Click on Delete of the user account which you want to delete. The account will be removed from the configuration once you have saved the configuration to the flash memory of the switch.



4.2.4 *Time Settings*

The Intellinet PoE switch is equipped with an internal clock, which is used to give log entries a proper time stamp. There are two ways to configure the clock. You can either configure the switch to obtain the time automatically from an SNTP server on the Internet or on your local network by setting the value **Enable SNTP** to **Enable**, or you can specify the time manually by setting the value **Enable SNTP** to **Disable**.



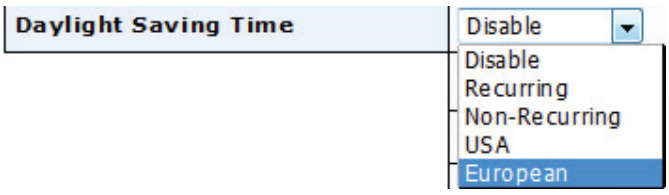
4.2.4.1 *Setting up System Time Manually*

When you disable SNTP, the screen allows you to manually enter the time.

Manual Time: Specify the correct year, month, day, hour, minute and second

Time Zone: Select the time zone that corresponds to the location of the Intellinet PoE switch.

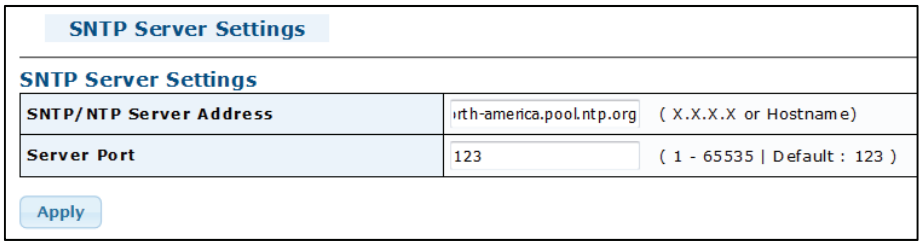
Daylight Saving Time: If the switch is located in an area with daylight saving time, you can define the specifics of it here. If you can, ideally you will want to select either European or USA, because in that case the switch will automatically adjust the time for you.



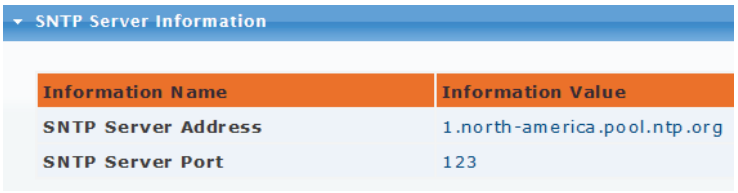
Select Recurring or Non-Recurring in order to enter the specific details about the daylight saving time manually.

4.2.4.2 SNTP Settings

If you set the Intellinet PoE to obtain its time from an SNTP server, then you must specific which SNTP server you want to use. You can use both internal and external SNTP servers. In both cases you have to ensure that the IP configuration of the switch allows it to access the SNTP server. If you wish to use an external SNTP server such as pool.ntp.org, then you must make sure that the switch has access to the Internet by providing a valid Gateway IP address – see section 4.2.2 IP Configuration.



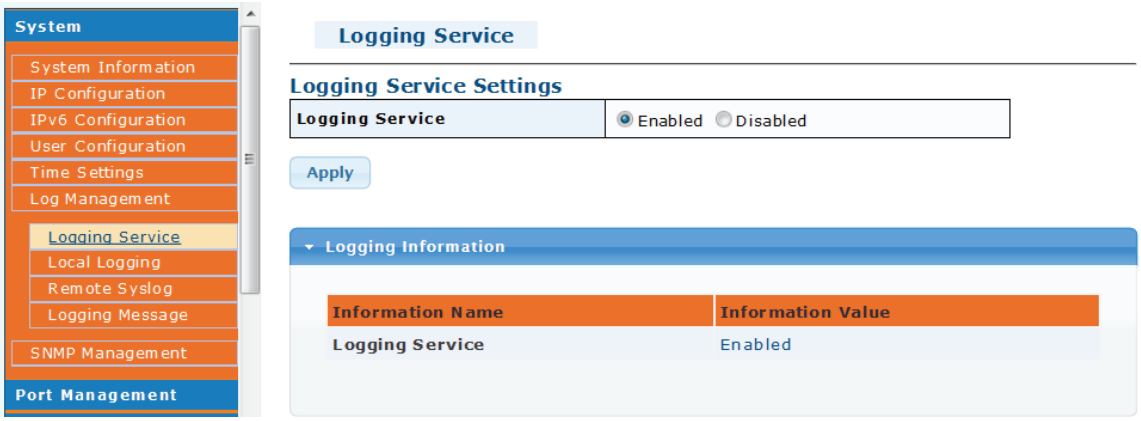
SNTP Server Address: The network address of the SNTP/NTP server.
Server Port: The Port Number of SNTP/NTP server (default = 123).



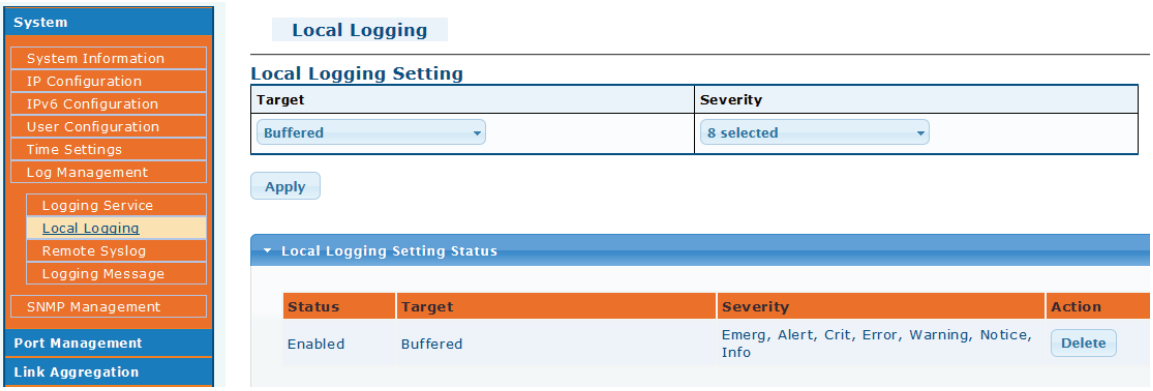
4.2.5 Log Management

4.2.5.1 Logging Service

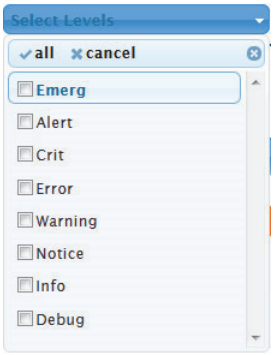
The Intellinet PoE switch has the ability to create a history log of important events. These logs can be stored either in the switches own memory, or on a remote Syslog server. In order to utilize the logging service, you must first enable it.



4.2.5.2 Local Logging



Target: Select the target to store log message
Buffered: Store log messages in the RAM. All log messages will disappear after a system reboot.
FLASH: Store log messages in the FLASH memory. Log messages will not disappear after system reboot.



Severity: Define which levels of messages will be logged. **Debug** will log every single message, regardless how irrelevant it may be. **Emerg** on the other hand will only log mission critical information.

4.2.5.3 Remote Logging

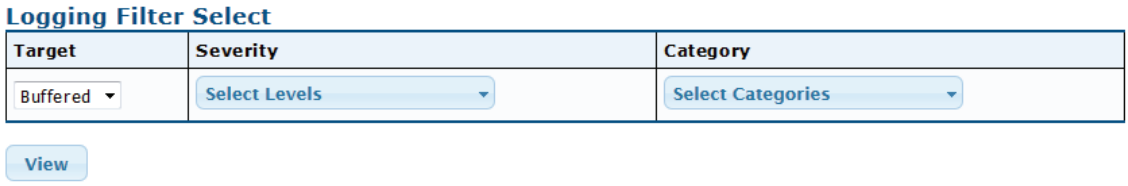
To display Remote Logging web page, click **Diagnostics > Logging Setting > Remote Logging**

Server Address: The IP address of remote log server.
Server Port: The port number of the remote log server (default = 514)..
Severity: Select the severity of log messages which will be recorded.
Facility: A facility code is used to specify the type of program that is logging the message. Messages with different facilities may be handled differently. The list of facilities available is defined by RFC 3164, see chart on the right.

Facility code	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem

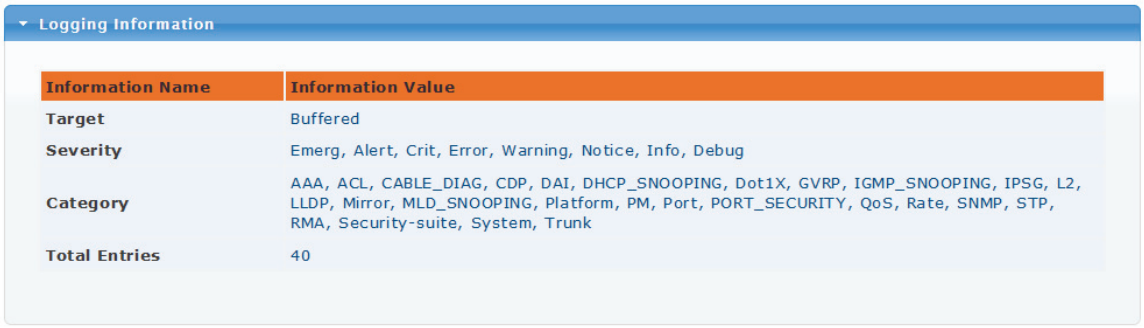
4.2.5.4 Logging Message

This interface screen is designed to let you view log messages that have been recorded earlier. The section Logging Filter Select allows you to define exactly what type of logging messages you wish to see.

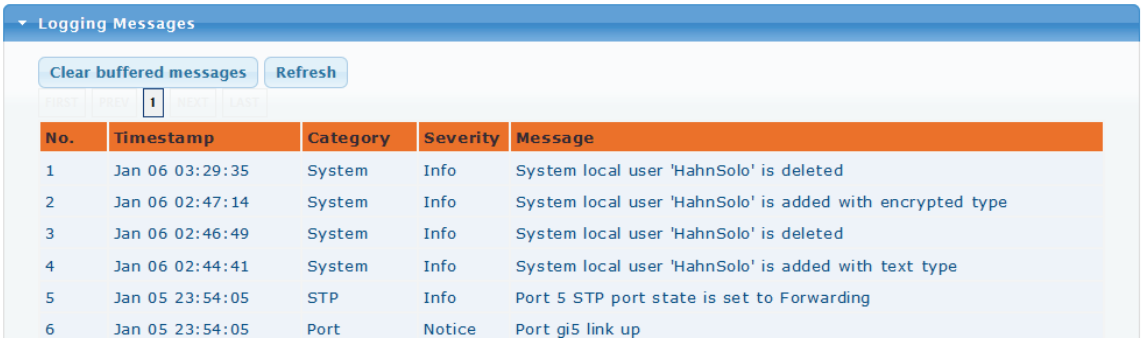


Target: This defines the source of the log messages (either buffered or FLASH).
Severity: Select the severity of log messages which will be recorded.
Category: Log messages are categorized, and the category filter allows you to filter out, which messages you wish to see.

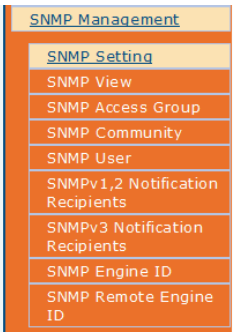
The section shown below displays the current filter settings.



The section below shows messages that have been recorded.

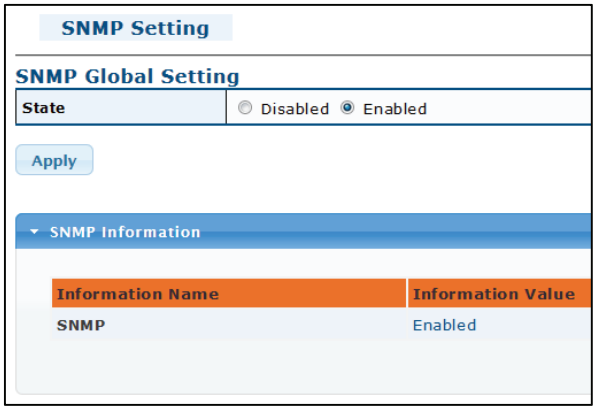


4.2.6 SNMP Management



Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

4.2.6.1 SNMP Setting

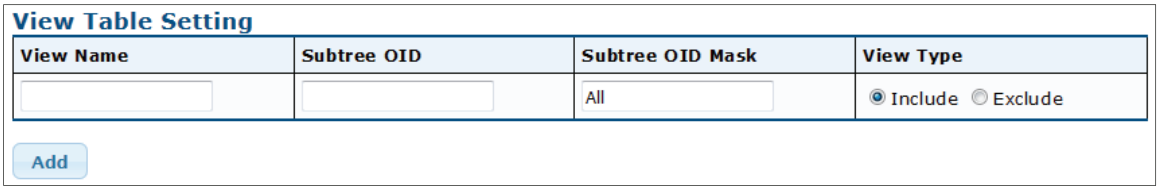


State: SNMP daemon state

- Enabled: Enable SNMP daemon
- Disabled: Disable SNMP daemon

4.2.6.2 SNMP View

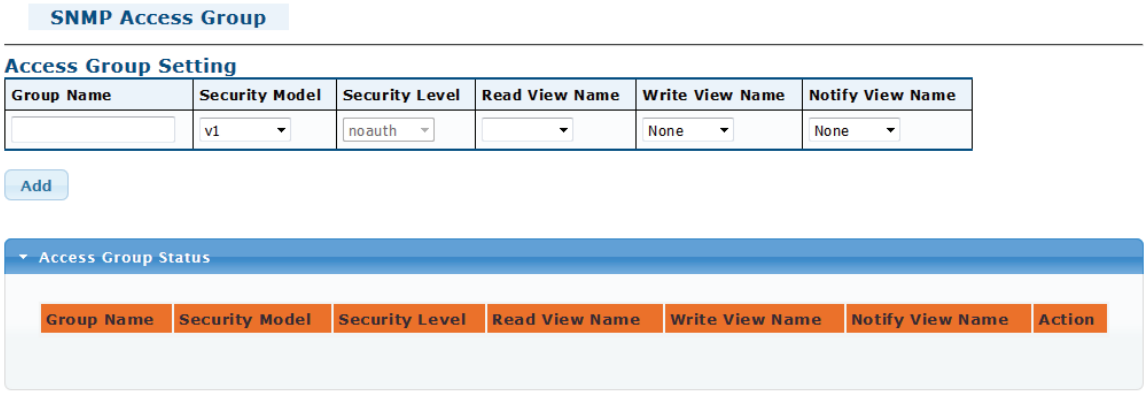
An SNMP view can be used to limit the type of information that is accessible, it is a combination of a set or a family of view subtrees where each view subtree is a subtree within the managed object naming tree. A view named “All” is created automatically by the switch. It contains all supported objects.



Item	Description
View Name	Enter a name to identify the SNM view. The name can contain up to 16 alphanumeric characters.
Subtree OID	An object identifiers (OID) identifies a variable that can be read or set via SNMP. Enter an OID string for the subtree you wish to either include in or exclude from the SNMP view.
Subtree OID Mask	The subtree OID mask couples with a subtree OID to make MIB view subtrees.
View Type	Select whether to include or exclude the information.

4.2.6.3 SNMP Access Group

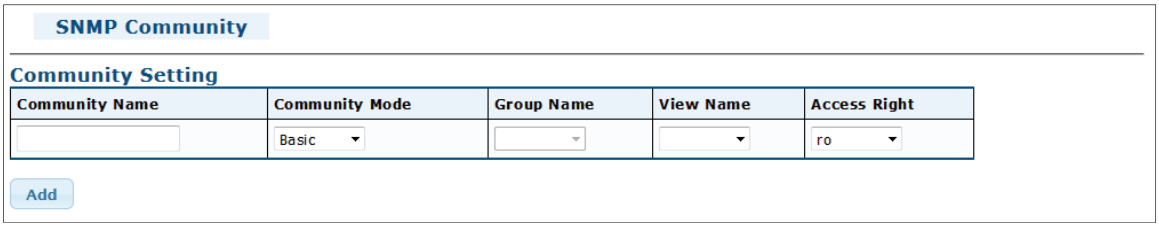
This page allows configuring SNMPv3 access groups. The index keys are Group Name, Security Model and Security Level.

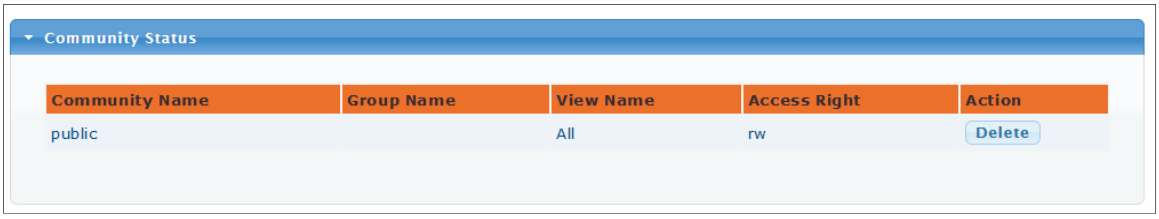


Item	Description
Group Name	This string identifies the group name , length is 1 to 16 characters.
Security Model	Indicates the security model for this entry. v1: SNMPv1. v2c: SNMPv2c. V3: SNMPv3 or User-based Security Model (USM)
Security Level	Note that the security level applies to SNNPv3. It indicates the security model that this entry should belong to. Possible security models are: Noauth: None authentication and none privacy security levels are assigned to the group. auth: Authentication and none privacy. priv: Authentication and privacy. Note:
Read View Name	Read view name is the name of the view in which you can only view the contents of the agent. Maximum length is 16 characters.
Write View Name	Write view name is the name of the view in which you enter data and configure the contents of the agent. Maximum length is 16 characters.
Notify View Name	Notify view name is the name of the view in which you specify a notify, inform, or trap.

4.2.6.4 SNMP Community

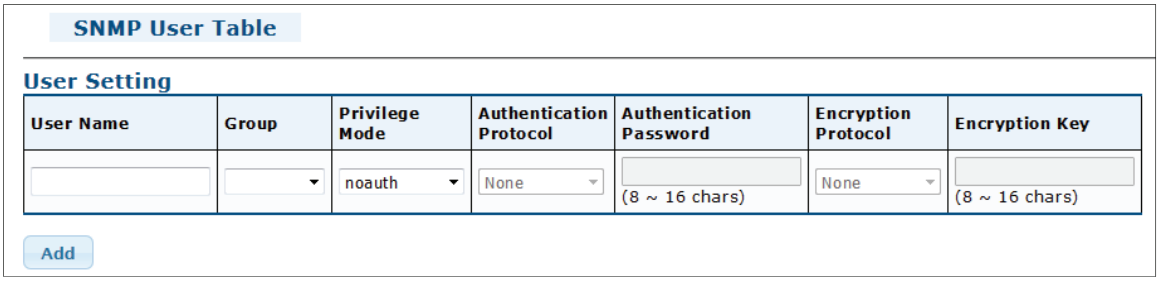
Configure the SNMP community on this page.





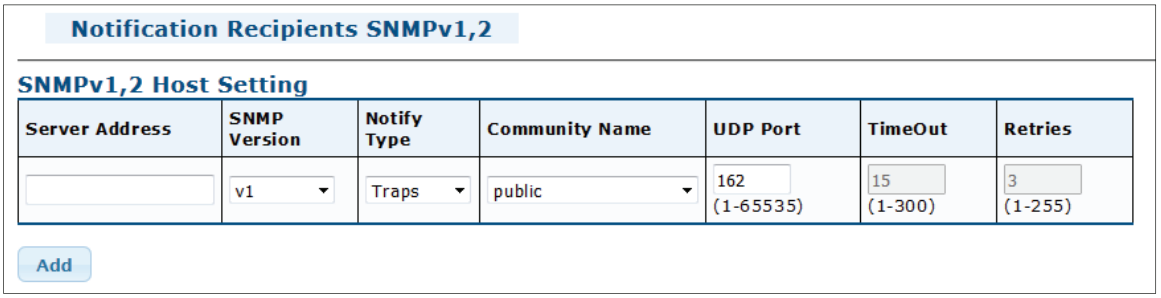
4.2.6.5 SNMP User

This page is used to create SNMP user under the group, And the group with the same level of security and access control permissions.



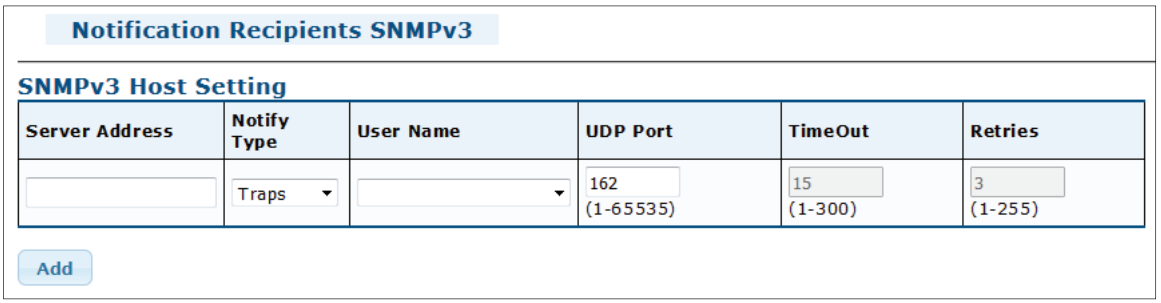
4.2.6.6 SNMPv1,2 Notification Recipients

SNMPv1,2 version notification event receiving host related configuration, you can configure to inform the host in the form of the trap message or log information about the current equipment, can be set up group name, UDP port number and message of the timeout.

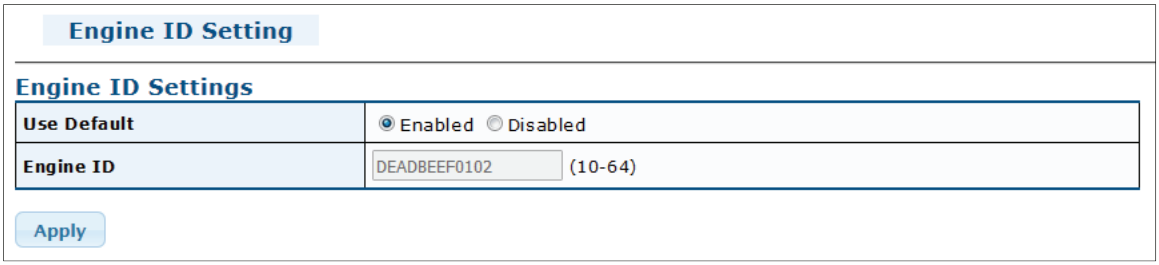


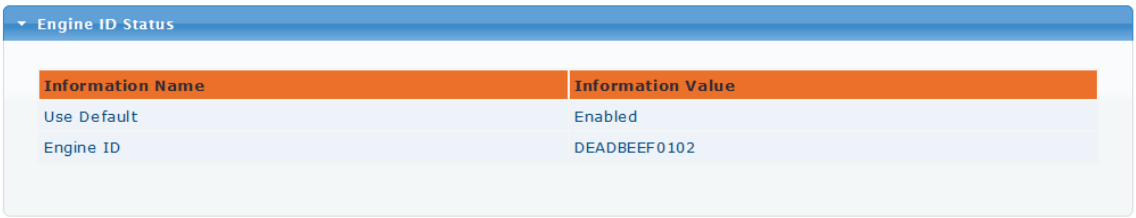
4.2.6.7 SNMPv3 Notification Recipients

SNMPv3 version notification event receiving host related configuration, you can configure to inform the host in the form of the trap message or log information about the current equipment, can be set up group name, UDP port number and message of the timeout.



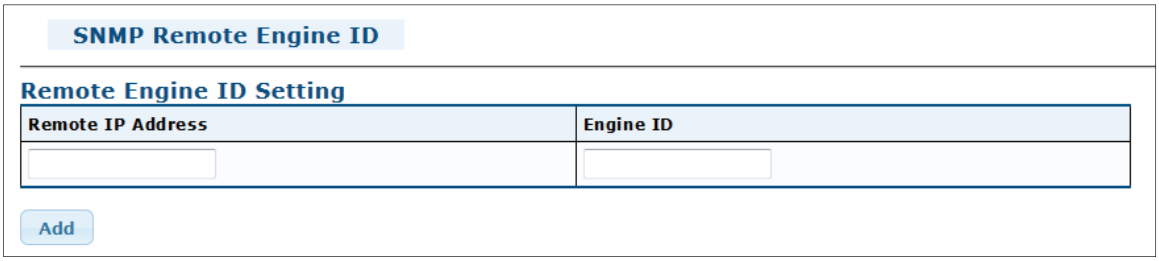
4.2.6.8 SNMP Engine ID





4.2.6.9 SNMP Remote Engine ID

Configure SNMPv3 remote Engine ID on this page.



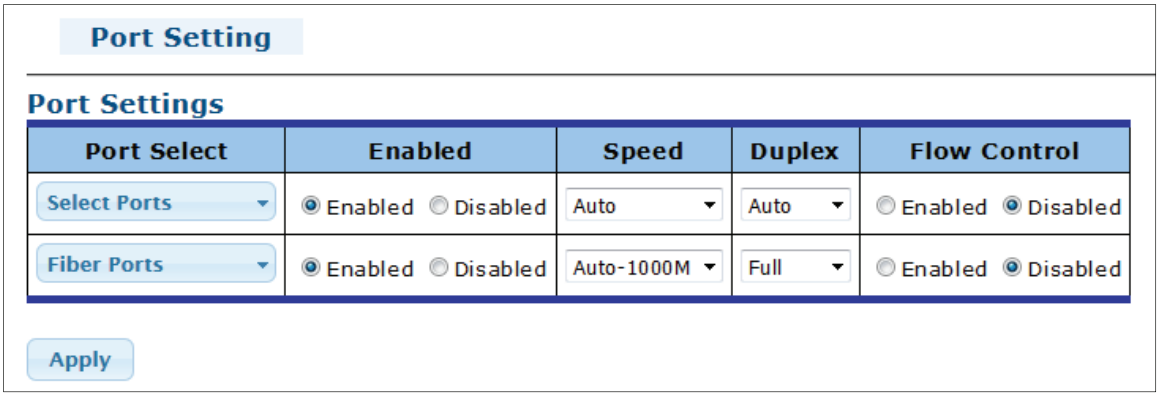
Item	Description
Remote IP Address	Indicates the SNMP remote engine ID address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
Engine ID	An octet string identifying the engine ID that this entry should belong to.

4.3 Port Management

The Intellinet 8-Port Gigabit PoE+ Switch is equipped wth both RJ45 ports and SFP modules. The port management function allows to configure these ports.

4.3.1 Port Configuration

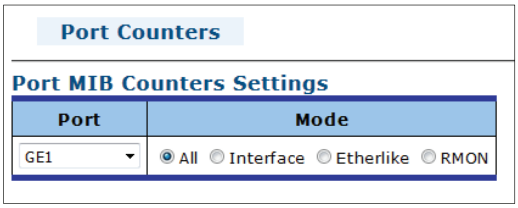
This page displays current port configurations and status. Ports can also be configured here.



Item	Description
Port Select	Select port number for this drop down list.
Enabled	Indicates the port state operation. Enabled – Activate the port. Disabled – Shut down the port.
Speed	Setup the link speed for the given switch port. Select Auto (recommended) to always connect at the best possible speed, and select one of the individual values from 10M to 1000M to set the port speed manually.
Duplex	Define the duplex mode of the port. - Auto - Setup Auto negotiation (recommended). - Full - Force Full-Duplex mode. - Half - Force Half-Duplex mode.
Flow Control	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. Current Rx column indicates whether pause frames on the port are obeyed. Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

4.3.2 Port Counters

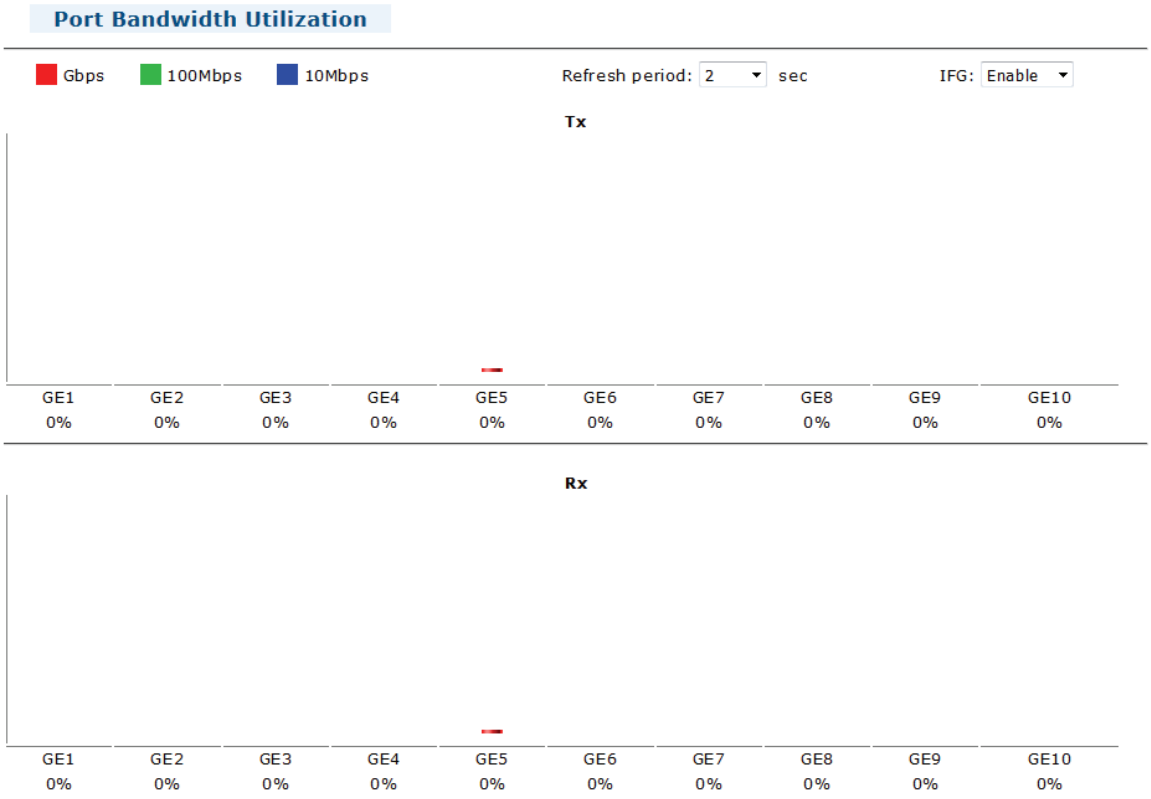
This page provides an overview of traffic and trunk statistics for all switch ports.



Object	Description
• **Port**	Select port number for this drop down list.
• **Mode**	Select port counters mode. Option: ● All ● Interface ● Ether-link ● RMON

4.3.3 *Bandwidth Utilization*

The Bandwidth Utilization page displays the percentage of the total available bandwidth being used on the ports. Bandwidth utilization statistics is represented by graphs.

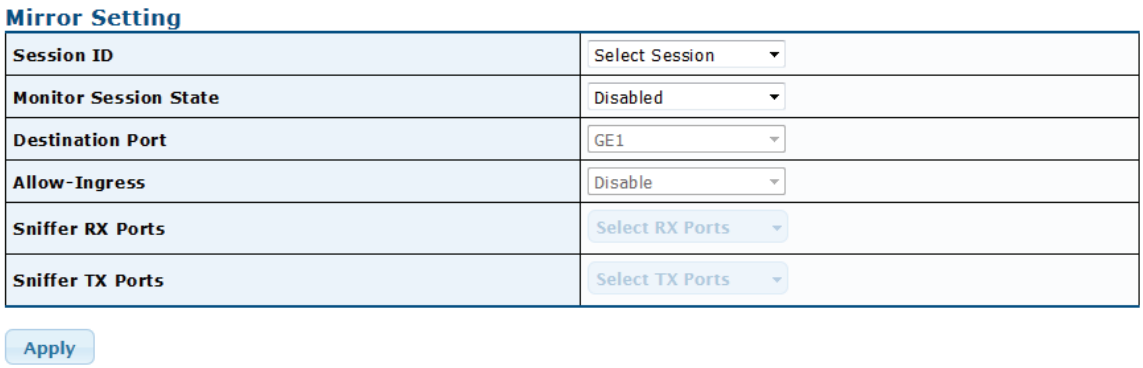


Object	Description
• **Refresh Period**	This shows the period interval between last and next refresh. Options: ■ 2 sec ■ 5 sec ■ 10 sec
• **IFG**	Allow user to **enable** or **disable** this function

4.3.4 Port Mirroring

Network engineers or administrators use port mirroring to analyze and debug data or diagnose errors on a network. It helps administrators keep a close eye on network performance and alerts them when problems occur. It can be used to mirror either inbound or outbound traffic (or both) on single or multiple interfaces. Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. The traffic to be copied to the mirror port is selected as follows:

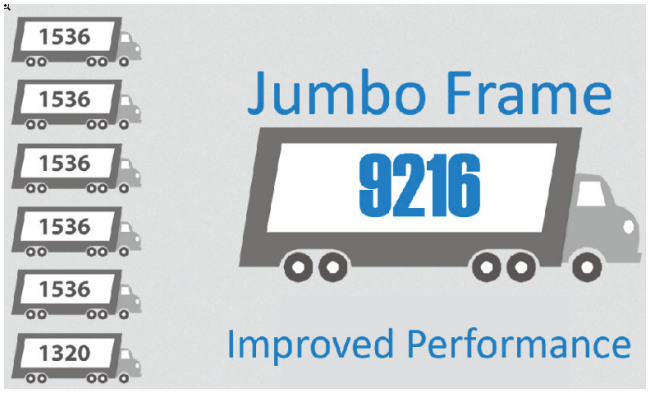
- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

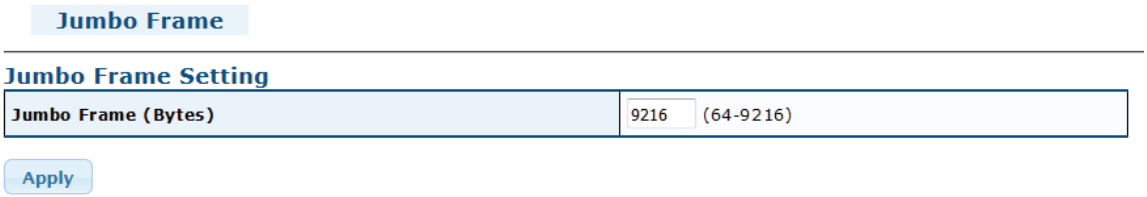


Object	Description
• **Session ID**	Set the port mirror session ID. Possible ID are: **1** to **4**.
• **Monitor Session State**	Enable or disable the port mirroring function.
• **Destination Port**	Select the port to mirror destination port.
• **Allow-ingress**	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.
• **Sniffer TX Ports**	Frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.
• **Sniffer RX Ports**	Frames received at these ports are mirrored to the mirroring port. Frames transmitted are not mirrored.

4.3.5 Jumbo Frame

In computer networking, jumbo frames are Ethernet frames with more than 1500 bytes of payload. Conventionally, jumbo frames can carry up to 9000 bytes of payload, but variations exist. For instance, the Intellinet 8-Port Gigabit PoE+ switch supports Jumbo frames of up to 9216 bytes.



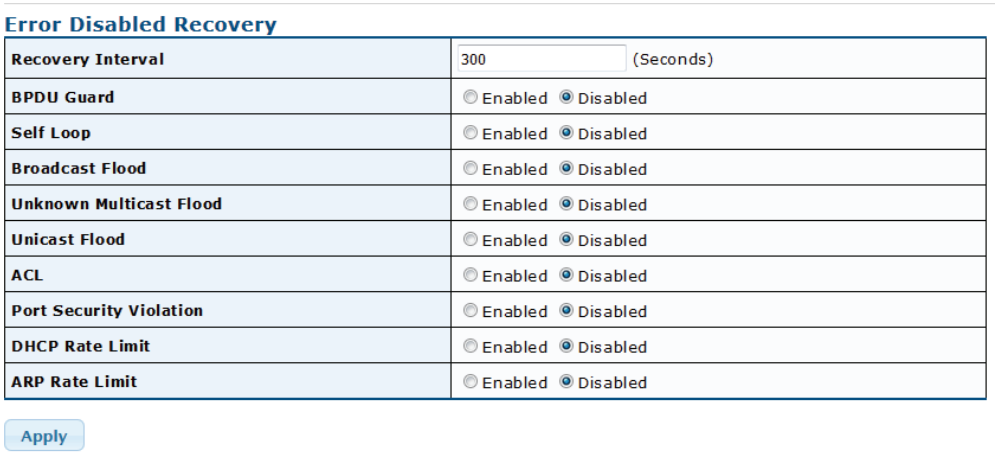


Set the jumbo frame size (64 – 9216) and hit **Apply** to save the settings.

The table above shows the current jumbo frame configuration.

4.3.6 Port Error Disabled Configuration

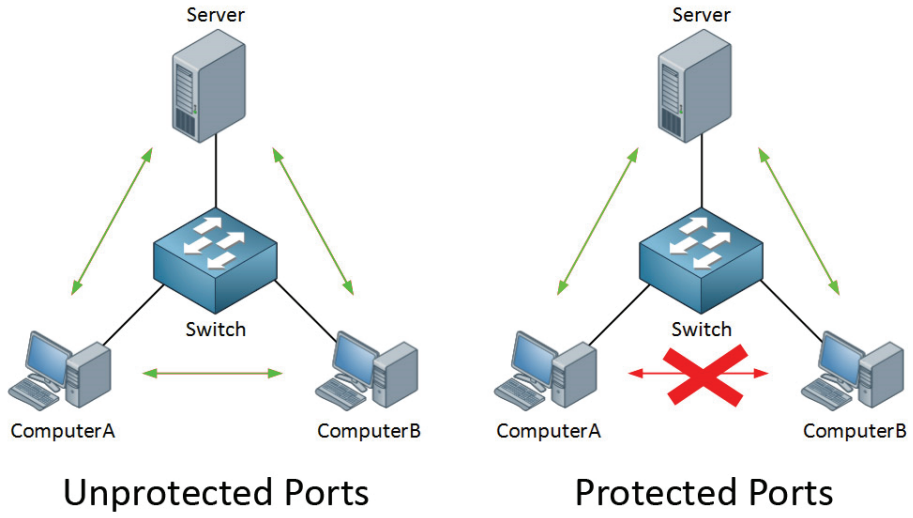
The Intellinet 8-Port Gigabit PoE+ Switch has the ability to disable ports, if an error occurs. By doing so, it can protect the rest of the network, if a network client on one port generates a lot of unwanted traffic, i.e. broadcast flooding. Below you can activate / deactivate the events you wish to monitor, and you can define the recovery interval, which is the time interval in which the port remains disabled (default = 300 seconds (5 minutes).



Object	Description
• **Recovery Interval**	The period (in seconds) for which a port will be kept disabled in the event of a port error is detected (and the port action shuts down the port).
• **BPDU Guard**	Enable or disable the port error disabled function to check status by BPDU guard.
• **Self Loop**	Enable or disable the port error disabled function to check status by self loop.
• **Broadcast Flood**	Enable or disable the port error disabled function to check status by broadcast flood.
• **Unknown Multicast Flood**	Enable or disable the port error disabled function to check status by unknown multicast flood.
• **Unicast Flood**	Enable or disable the port error disabled function to check status by unicast flood.
• **ACL**	Enable or disable the port error disabled function to check status by ACL.
• **Port Security Violation**	Enable or disable the port error disabled function to check status by port security violation.
• **DHCP Rate Limit**	Enable or disable the port error disabled function to check status by DHCP rate limit
• **ARP Rate Limit**	Enable or disable the port error disabled function to check status by ARP rate limit

4.3.7 *Protected Ports*

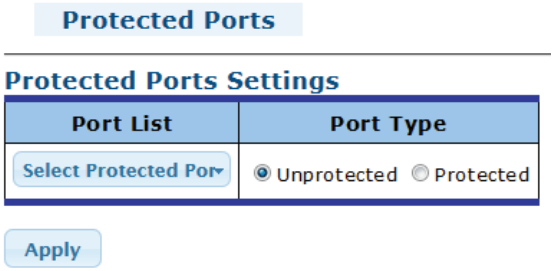
Protected ports can be used to prevent interfaces (i.e., network clients) from communicating with each other. Protected ports can be viewed as 'isolated ports.'



For protected port group to be applied, the network switch must first be configured for standard VLAN operation. Ports in a protected port group fall into one of these two groups:

1. Promiscuous (Unprotected) ports
    a. Ports from which traffic can be forwarded to all ports in the private VLAN
    b. Ports which can receive traffic from all ports in the private VLAN
2. Isolated (Protected) ports
    a. Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN
    b. Ports which can receive traffic from only promiscuous ports in the private VLAN

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.



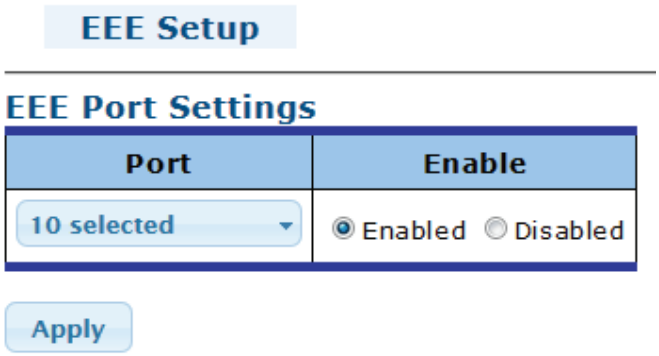
Object	Description
• **Port List**	Select port number for this drop down list.
• **Port Type**	Displays protected port types. - **Protected**: A single stand-alone VLAN that contains one promiscuous port and one or more isolated (or host) ports. This VLAN conveys traffic between the isolated ports and a lone promiscuous port. - **Unprotected**: A promiscuous port can communicate with all the interfaces within a private VLAN. This is the default setting.

The screen also shows the current status of protected v. unprotected ports. In the example above, ports 1 and 2 are protected (as in isolated), RJ45 ports 3 – 8 as well as SFP ports 9 1nd 10 are unprotected.

4.3.8 EEE – Energy Efficient Ethernet

Energy-Efficient Ethernet (EEE) is a set of enhancements to the twisted-pair and backplane Ethernet family of computer networking standards that allow for less power consumption during periods of low data activity. The intention was to reduce power consumption by 50% or more, while retaining full compatibility with existing equipment. The Institute of Electrical and Electronics Engineers (IEEE), through the IEEE 802.3az task force developed the standard. EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic.

When a port is powered down for saving power, the outgoing traffic is stored in a buffer until the port is powered up again. Using this technique, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Keep in mind, that buffering traffic will give some latency in the traffic.



Object	Description
• **Port**	Select port number for this drop down list.
• **Enable**	Enable or disable the EEE function.

4.4 Link Aggregation

In computer networking, the term link aggregation applies to various methods of combining (aggregating) multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail.
Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Group (LAG). Port Aggregation multiplies the bandwidth between the two Ethernet switches and provides link redundancy. Each LAG is composed of ports of the same speed, set to full-duplex operations.

Aggregated Links can be assigned manually (Port Trunk) or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links. Aggregated Links are treated by the system as a single logical port.

The Intellinet 8-Port Gigabit PoE+ switch supports the following Aggregation links :

1. Static LAGs (Port Trunk) – Selected ports are forced to be in a trunk group.
2. Link Aggregation Control Protocol (LACP) LAGs - LACP LAG negotiate aggregated port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

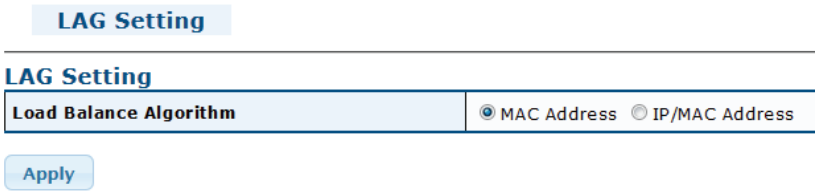
When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ-45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 8 ports to be aggregated at the same time. The Intellint switch support Gigabit Ethernet ports (up to 8 groups). If the group is defined as a LACP static link aggregation group, then any extra port selected is placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, then the number of ports must be the same as the group member ports.

4.4.1 LAG Setting

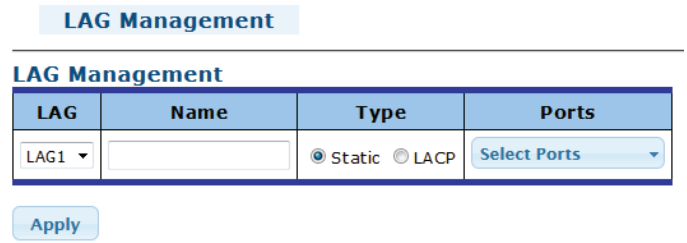
This page allows configuring load balance algorithm configuration settings.



Object	Description
• **Load Balance Algorithm**	Select load balance algorithm mode: ■ **MAC Address**: The MAC address can be used to calculate the port for the frame. ■ **IP/MAC Address**: The IP and MAC address can be used to calculate the port for the frame.

4.4.2 LAG Management

This page is used to configure the basic settings of the Link Aggregation Group.

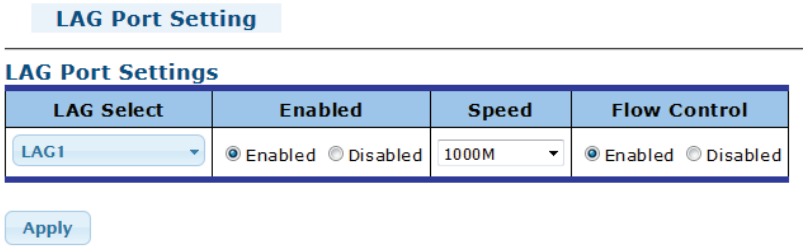


Object	Description
• **LAG**	Select LAG number for this drop down list.
• **Name**	Indicates the per LAG name.
• **Type**	Indicates the trunk type. **Static**: Force aggregared selected ports to be a trunk group. **LACP**: LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
• **Ports**	Select port number for this drop down list to establish Link Aggregation.

Object	Description
• **LAG**	The LAG for the settings contained in the same row.
• **Name**	Display the current name
• **Type**	Display the current type
• **Link State**	Display the link state
• **Active Member**	Display the active member
• **Standby Member**	Display the standby member
• **Modify**	Click Edit to modify LAG configuration.

4.4.3 LAG Port Settings

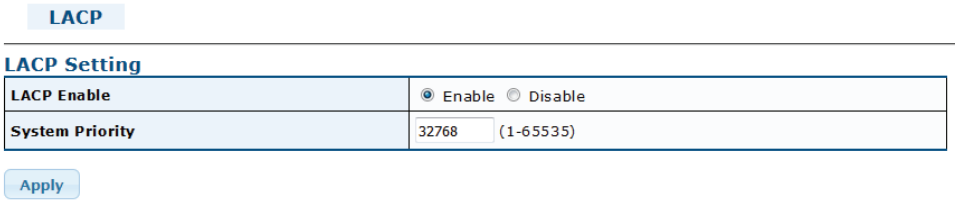
On this screen you define the properties of the ports belonging to a Link Aggregation Group.



Object	Description
• **LAG Select**	Select LAG number for this drop down list.
• **Enable**	Indicates the LAGt state operation. Possible state are: **Enabled** - Start up the LAG manually. **Disabled** - Shutdown the LAG manually.
• **Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. ■ **Auto** - Setup Auto negotiation. ■ **Auto-10M** - Setup 10M Auto negotiation. ■ **Auto-100M** - Setup 100M Auto negotiation. ■ **Auto-1000M** - Setup 1000M Auto negotiation. ■ **Auto-10/100M** - Setup 10/100M Auto negotiation. ■ **10M** - Setup 10M Force mode. ■ **100M** - Setup 100M Force mode. ■ **1000M** - Setup 1000M Force mode.
• **Flow Control**	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used.
	Current Rx column indicates whether pause frames on the port are obeyed. Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

4.4.4 LACP Settings

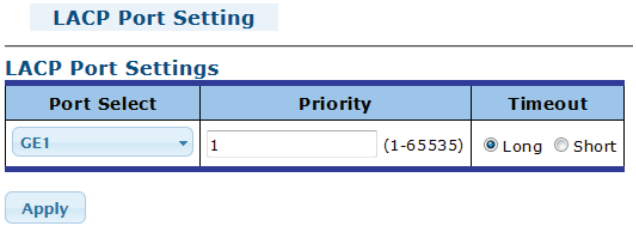
In a trunk group, each switch has to have a priority. That is the system priority. The smaller the number, the higher the priority. The switch with the smallest number (and thus the highest priority) is the active LACP peer of the trunk group.



Object	Description
• **System Priority**	A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.

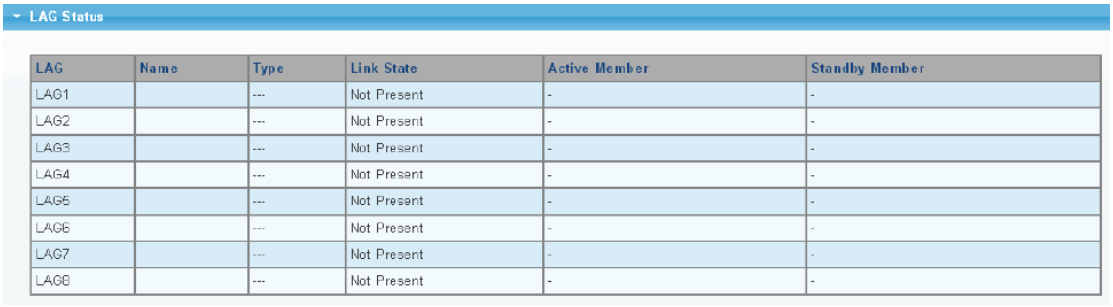
4.4.5 LACP Port Settings

This page is used to configure the LACP port priority settings.



Object	Description
• **Port Select**	Select port number for this drop down list to set LACP port setting.
• **Priority**	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. **Lower number means greater priority.**
• **Timeout**	The Timeout controls the period between BPDU transmissions. Short will transmit LACP packets each second, while Long will wait for 30 seconds before sending a LACP packet.

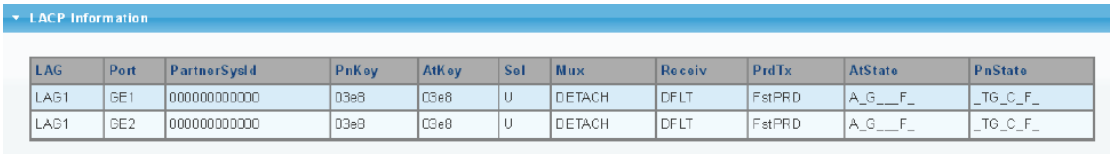
4.4.6 LAG Status



LAG Status

LAG	Name	Type	Link State	Active Member	Standby Member
LAG1		---	Not Present	-	-
LAG2		---	Not Present	-	-
LAG3		---	Not Present	-	-
LAG4		---	Not Present	-	-
LAG5		---	Not Present	-	-
LAG6		---	Not Present	-	-
LAG7		---	Not Present	-	-
LAG8		---	Not Present	-	-

Object	Description
• **LAG**	Display the current trunk entry.
• **Name**	Display the current LAG name.
• **Type**	Display the current trunk type.
• **Link State**	Display the current link state.
• **Active Member**	Display the current active member.
• **Standby Member**	Display the current standby member.



LACP Information

LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState
LAG1	GE1	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G___F_	_TG_C_F_
LAG1	GE2	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G___F_	_TG_C_F_

Object	Description
• **Trunk**	Display the current trunk ID.
• **Port**	Display the current port number.
• **PartnerSysId**	The system ID of link partner. This field would be updated when the port receives LACP PDU from link partner.
• **PnKey**	Port key of partner. This field would be updated when the port receives LACP PDU from link partner.
• **AtKey**	Port key of actor. The key is designed to be the same as trunk ID.
• **Sel**	LACP selection logic status of the port. ■ "**S**" means selected ■ "**U**" means unselected ■ "**D**" means standby
• **Mux**	LACP mux state machine status of the port. ■ "DETACH" means the port is in detached state ■ "WAIT" means waiting state ■ "ATTACH" means attach state ■ "CLLCT" means collecting state

	■ "DSTRBT" means distributing state
• **Receive**	LACP receive state machine status of the port. ■ "INIT" means the port is in initialize state ■ "PORTds" means port disabled state ■ "EXPR" means expired state ■ "LACPds" means LACP disabled state ■ "DFLT" means defaulted state ■ "CRRNT" means current state.
• **PrdTx**	LACP periodic transmission state machine status of the port. ■ "no PRD" means the port is in no periodic state ■ "FstPRD" means fast periodic state ■ "SlwPRD" means slow periodic state ■ "PrdTX" means periodic TX state
• **AtState**	The actor state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.
• **PnState**	The partner state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.

4.5 VLAN

4.5.1 What is VLAN?

4.5.1.1 Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.
VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Things to note:

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.
- The Switch supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
- The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
- The "default" VLAN has a VID = 1.
- The member ports of Port-based VLANs may overlap, if desired.

4.5.1.2 Port-based VLANs

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department. On port-based VLAN.NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

4.5.1.3 IEEE 802.1Q VLANs

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant). VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources. VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as

either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in 30 packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally. Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allow VLAN to work with legacy switches that don ’t recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

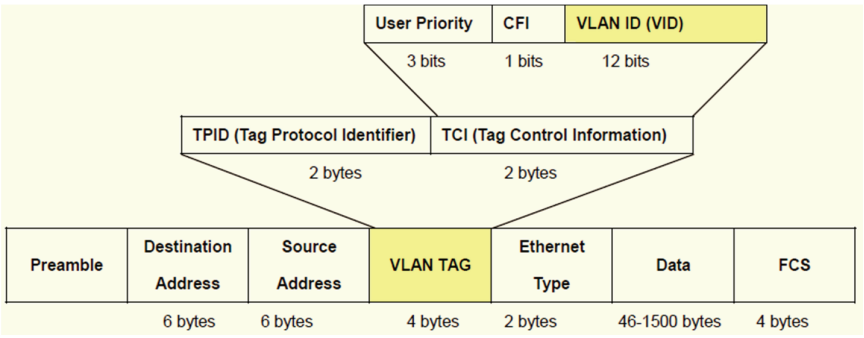
Some relevant terms:

Tagging - The act of putting 802.1Q VLAN information into the header of a packet.

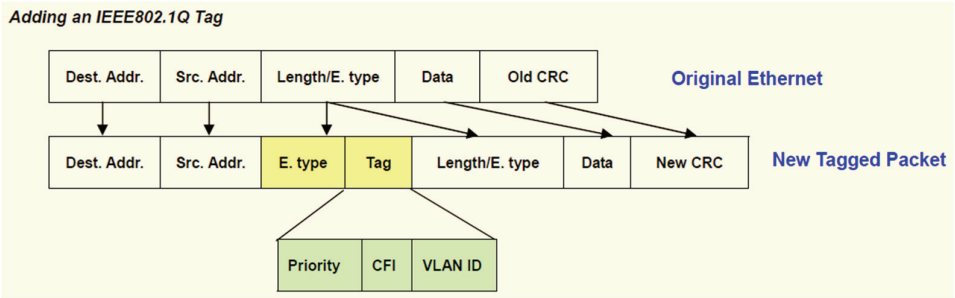
Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

4.5.1.4 802.1Q VLAN Tags

The figure to the right shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to 112 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified. The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.



4.5.1.5 Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant). Original Ethernet New Tagged Packet Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network. A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them. Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

4.5.1.6 Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default". As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

4.5.1.7 Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note:

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

4.5.1.8 VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

4.5.1.9 Port Overlapping

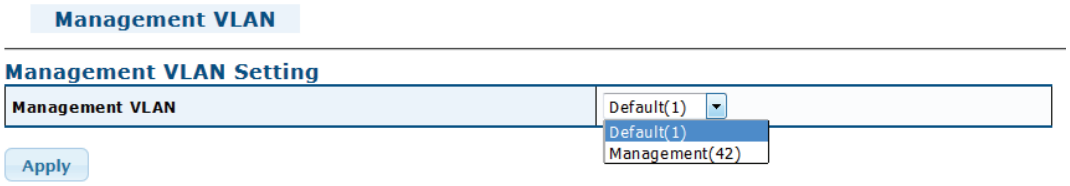
Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

4.5.1.10 Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

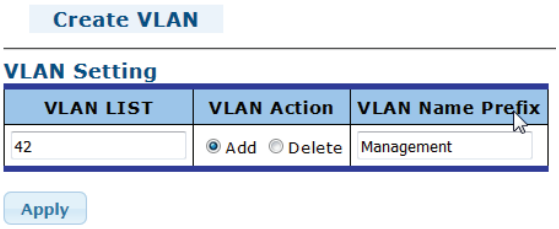
4.5.2 *Management VLAN*

When it comes to switch management, its common to use a dedicated VLAN for management purposes. That VLAN you will have created already (see section 4.5.3), and perhaps named 'Management'. On this screen you simply select the VLAN as the management VLAN.

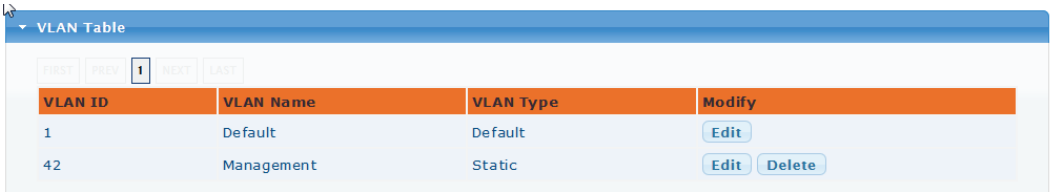


4.5.3 *Create VLAN*

This page allows you to setup, edit and delete VLANs.



Object	Description
• **VLAN List**	Indicates the ID of this particular VLAN.
• **VLAN Action**	This column allowed users to add or delete VLAN s.
• **VLAN Name Prefix**	Indicates the name of this particular VLAN.



Object	Description
• **VLAN ID**	Display the current VLAN ID entry.
• **VLAN Name**	Display the current VLAN ID name.
• **VLAN Type**	Display the current VLAN ID type.
• **Modify**	Click Edit to modify VLAN configuraiton.

4.5.4 Interface Settings

This Page is used for configuring the Managed Switch port VLAN. The VLAN per Port Configuration Page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration Page. All untagged packets arriving to the device are tagged by the ports PVID. Understand nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged
Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

Tagged:
Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Untagged:
Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

IEEE 802.1Q Tunneling (Q-in-Q)
IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

The Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the MAN (Metro Access Network) space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

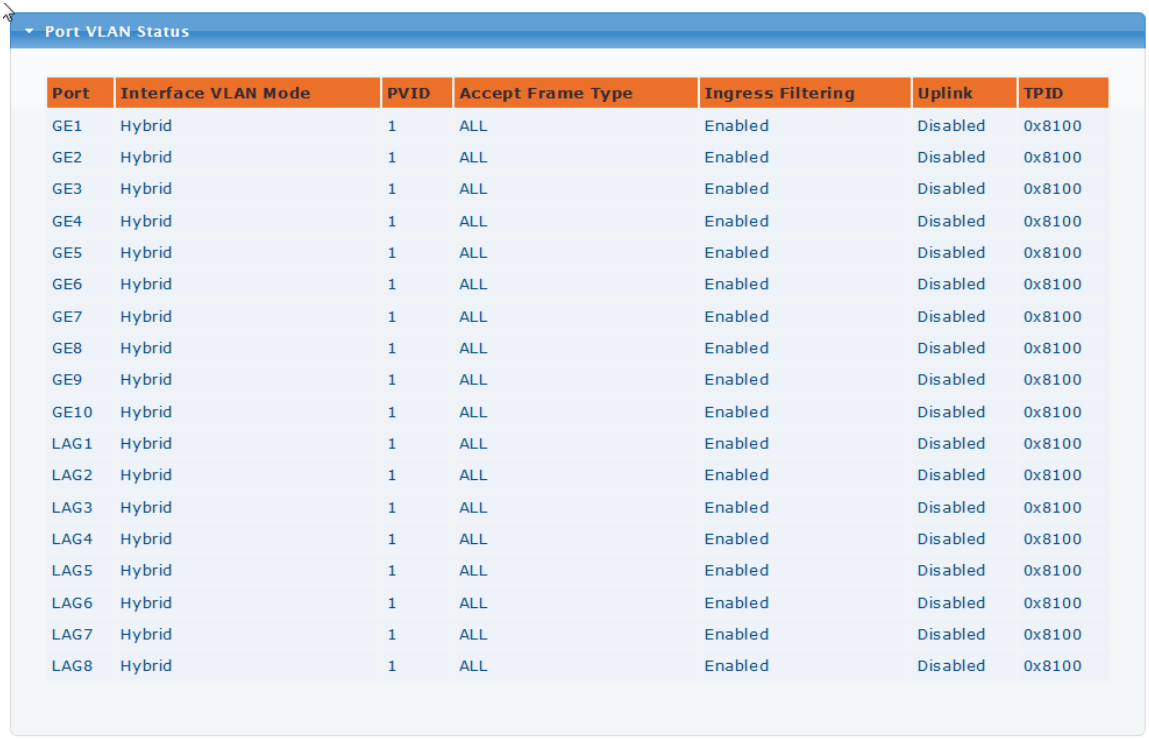
This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType 0x8100 or 0x88A8, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags. In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

Edit Interface Setting

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
Select Ports	Hybrid Access Trunk Tunnel	1 (1 - 4094)	All Tag Only Untag Only	Enabled Disabled	Enabled Disabled	0x8100

Apply

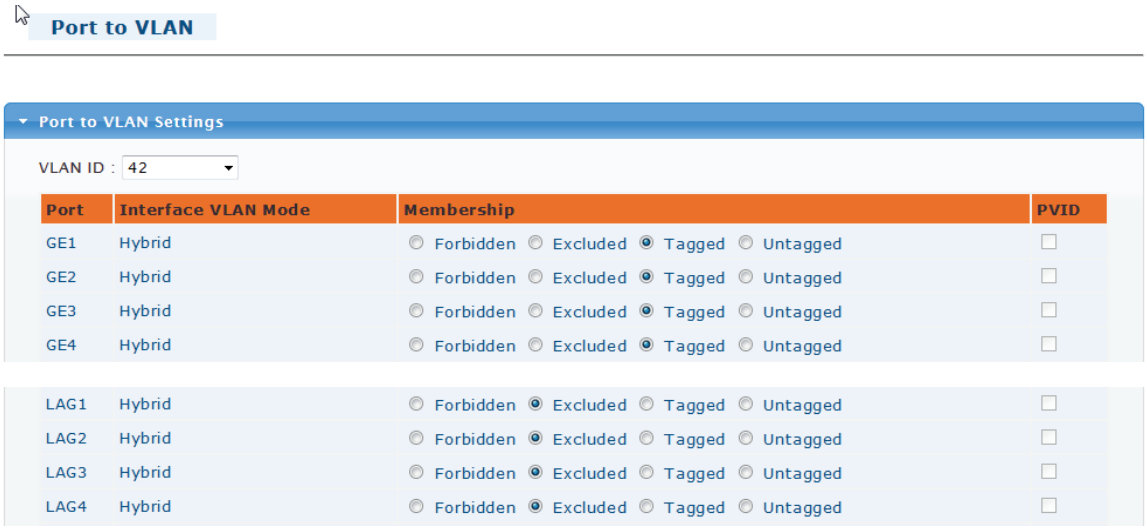
Object	Description
• **Port Select**	Select port number for this drop down list to set VLAN port setting.
• **Interface VLAN Mode**	Set the port in access, trunk, hybrid, tunnel mode. ■ **Trunk** means the port allows traffic of multiple VLAN. ■ **Access** indicates the port belongs to one VLAN only. ■ **Hybrid** means the port allows the traffic of multi-VLANs to pass with tag or untag mode. ■ **Tunnel** configures IEEE 802.1Q tunneling for a downlink port to another device within the customer network.
• **PVID**	Allow assign PVID for selected port. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped. The range for the PVID is **1-4094.**
• **Accepted Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. Options: ■ **All** ■ **Tag Only** ■ **Untag Only** By default, the field is set to **All**.
• **Ingress Filtering**	• If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. • If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
• **Uplink**	Enable/disable uplink function in trunk port.
• **TPID**	Configure the type (TPID) of the protocol of switch trunk port.



Object	Description
• **Port**	The switch port number of the logical port.
• **Interface VLAN Mode**	Display the current interface VLAN mode.
• **PVID**	Display the current PVID.
• **Accepted Frame Type**	Display the current access frame type.
• **Ingress Filtering**	Display the current ingress filtering.
• **Uplink**	Display the current uplink mode.
• **TPID**	Display the current TPID.

4.5.5 *Port to VLAN*

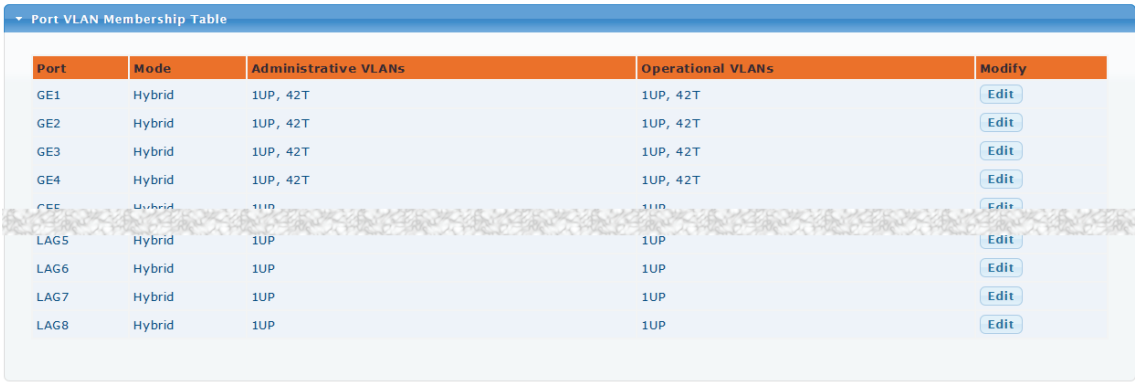
With this function you can assign ports to or delete them from existing VLANs. GE1 designated Gigabit Ethernet port 1, while LAG1 stands fir Link Aggregation Group 1.



Object	Description	
• **VLAN ID**	Select VLAN ID for this drop down list to assign VLAN membership.	
• **Port**	The switch port number of the logical port.	
• **Interface VLAN Mode**	Display the current interface VLAN mode.	
• **Membership**	Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:	
	Forbidden:	Interface is forbidden from automatically joining the VLAN via GVRP.
	Excluded:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Tagged:	Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
	Untagged:	Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
• **PVID**	Display the current PVID	

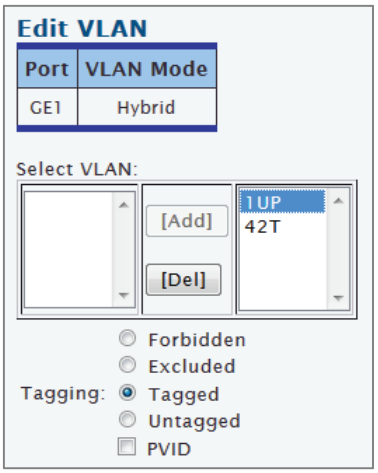
4.5.6 *Port VLAN Membership*

This screen shows an overview of all ports and LAGs, along with their corresponding VLAN status.



Object	Description
• **Port**	The switch port number of the logical port.
• **Mode**	Display the current VLAN mode.
• **Administrative VLANs**	Display the current administrative VLANs.
• **Operational VLANs**	Display the current operational VLANs.
• **Modify**	Click Edit to modify VLAN membership.

When you edit a port or LAG, you can remove the port from existing VLANs by selecting the VLAN in the right box and clicking [Del]. In order to add a port to a VLAN, select the LAN on the left side, and then click [Add].
Additionally, you can define the tagging for this port. See the previous section for details.

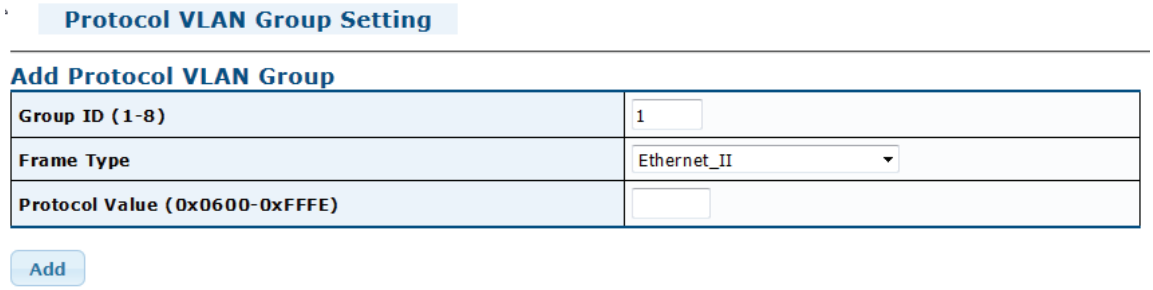


4.5.7 Protocol VLAN Group Settings

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility. To avoid these problems, you can configure this Managed Switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

To configure protocol-based VLANs, follow these steps:
1. First configure VLAN groups for the protocols you want to use. Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.
3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

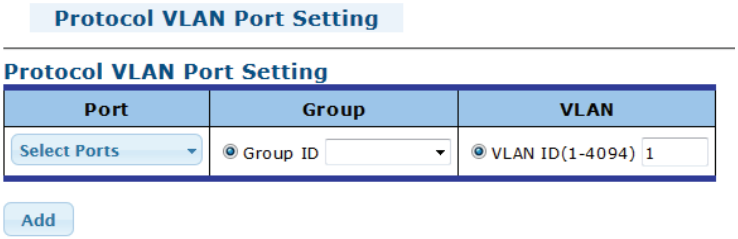
This Page allows for configures protocol-based VLAN Group Setting



Object	Description
• **Group ID**	Protocol Group ID assigned to the Special Protocol VLAN Group.
• **Frame Type**	Frame Type can have one of the following values: ■ **Ethernet II** ■ **IEEE802.3_LLC_Other** ■ **RFC_1042** **Note:** On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.
• **Protocol Value (0x0600-0xFFFE)**	Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu. Valid values for frame type ranges from 0x0600-0xffffe

4.5.8 Protocol VLAN Port Settings

Once the group has been configured, you can map it to a VLAN/port.

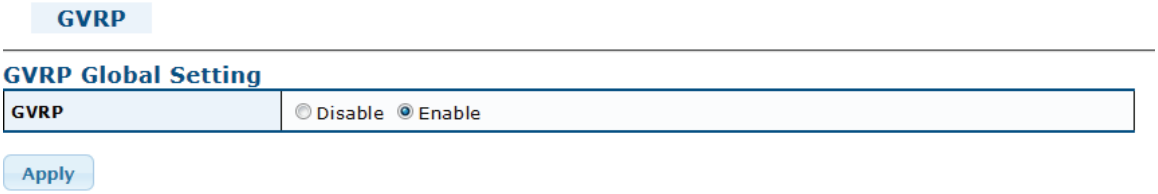


Object	Description
• **Port**	Select port for this drop down list to assign protocol VLAN port.
• **Group**	Select group ID for this drop down list to protocol VLAN group.
• **VLAN**	VLAN ID assigned to the Special Protocol VLAN Group.

4.5.9 GVRP Setting

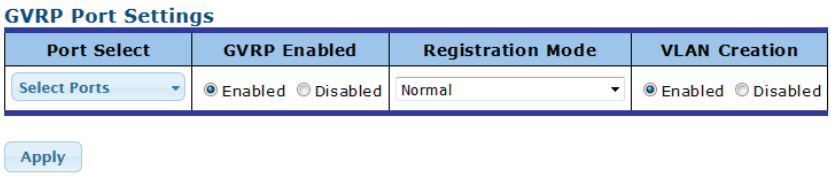
GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

On this configuration page you can activate or deactivate this feature.



4.5.10 GVRP Port Setting

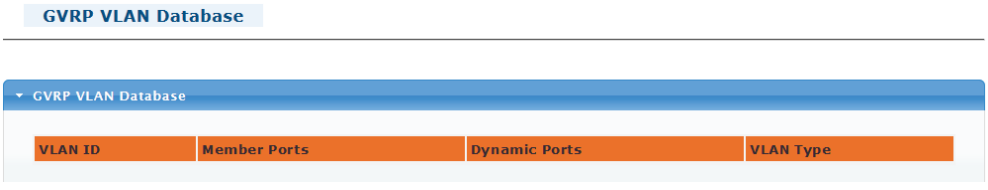
This configuration screen allows you to activate or deactivate GVRP for each port. Additionally, you can define the registration mode and allow or disallow the dynamic creation of VLANs.



Object	Description
• **Port Select**	Select port for this drop down list to assign protocol VLAN port.
• **GVRP Enabled**	Controls whether GVRP is enabled or disabled on port.
• **Registration Mode**	By default GVRP ports are in **normal** registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the **fixed** mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in **forbidden** mode forward only for VLAN 1.
• **VLAN Creation**	GVRP can dynamically create VLANs on switches for trunking purposes. By enabling GVRP dynamic VLAN creation, a switch will add VLANs to its database when it receives GVRP join messages about VLANs it does not have.

4.5.11 GVRP VLAN

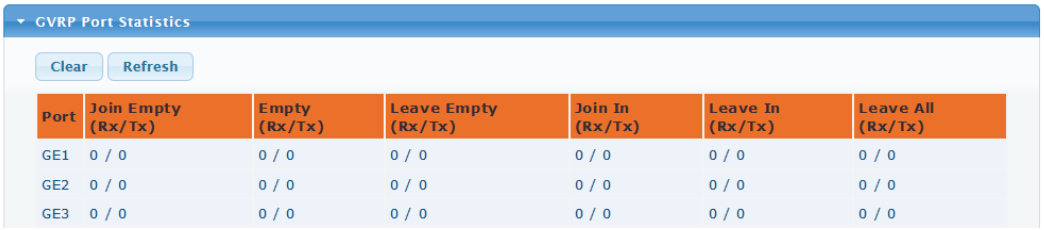
This screen provides an overview of the current GVRP VLAN setup.



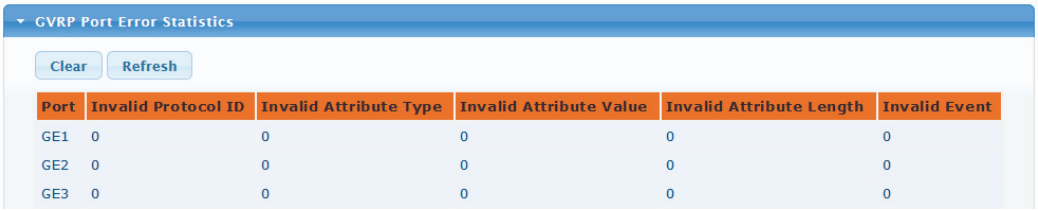
Object	Description
• **VLAN ID**	Display the current VLAN ID.
• **Member Ports**	Display the current member ports.
• **Dynamic Ports**	Display the current dynamic ports.
• **VLAN Type**	Display the current VLAN type.

4.5.12 GVRP Statistics

GVRP Port and Error Statistics are shown on this page.



Object	Description
• **Port**	The switch port number of the logical port.
• **Join Empty (Rx/Tx)**	Display the current join empty (TX/RX) packets.
• **Empty (Rx/Tx)**	Display the current empty (TX/RX) packets.
• **Leave Empty (Rx/Tx)**	Display the current leave empty (TX/RX) packets.
• **Join In (Rx/Tx)**	Display the current join in (TX/RX) packets.
• **Leave In (Rx/Tx)**	Display the current leave in (TX/RX) packets.
• **LeaveAll (Rx/Tx)**	Display the current leaveall (TX/RX) packets.



Object	Description
• **Port**	The switch port number of the logical port.
• **Invaild Protocol ID**	Display the current invalid protocol ID.
• **Invalid Attribute Type**	Display the current invalid attribute type.
• **Invalid Attribute Value**	Display the current invalid attribute value.
• **Invalid Attribute Length**	Display the current invalid attribute length.
• **Invalid Event**	Display the current invalid event.

4.6 Spanning Tree Protocol (STP)

4.6.1 What is STP?

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention. This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch. When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

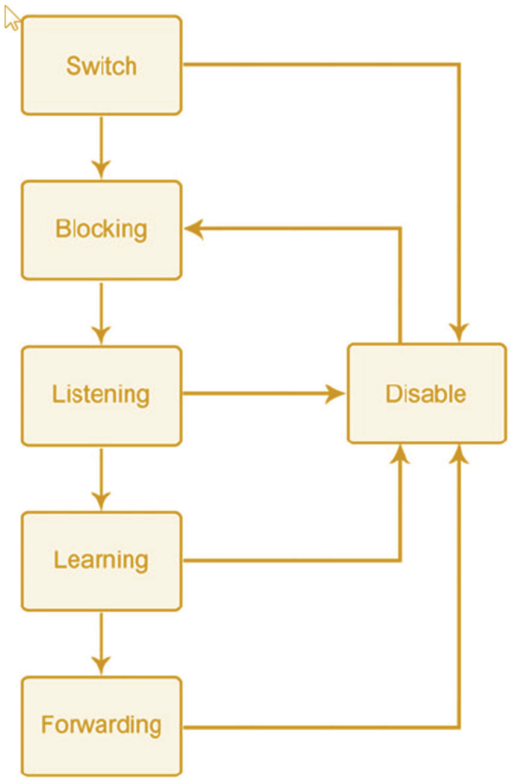
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- Blocking – the port is blocked from forwarding or receiving packets
- Listening – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- Learning – the port is adding addresses to its forwarding database, but not yet forwarding packets
- Forwarding – the port is forwarding packets
- Disabled – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking



You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note:
On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges. On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC.	32768 + MAC
Priority	A relative priority for each switch. Lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge.	32768
Hello Time	The length of time between broadcasts of the hello message by the switch.	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 – Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

Note:
The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

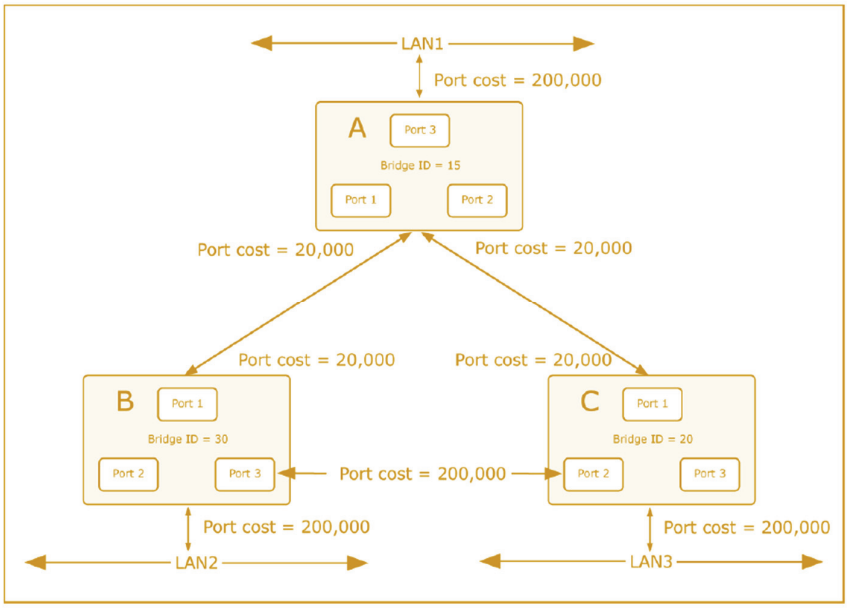
Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Note:
Observe the following formulas when setting the above parameters:
Max. Age _ 2 x (Forward Delay - 1 second)
Max. Age _ 2 x (Hello Time + 1 second)

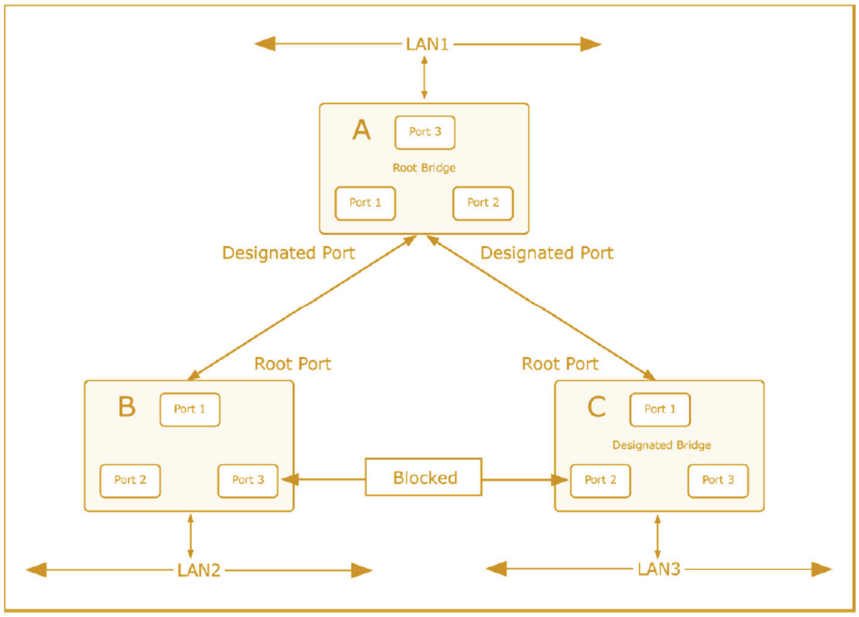
Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.
Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP
A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.
If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure.
In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings. Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.



Before Applying the STA Rules

In this example, only the default STP values are used.



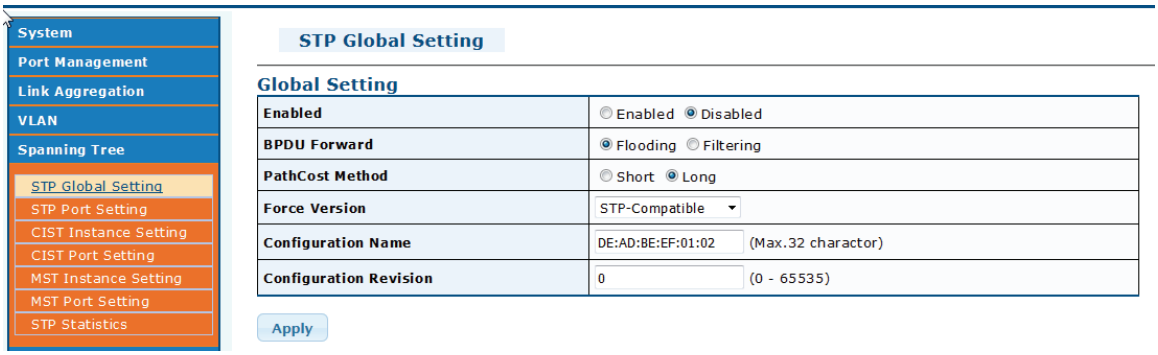
After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

4.6.2 STP Global Settings

This page allows you to configure the STP system settings. The settings are used by all STP Bridge instances in the Intellinet 8-Port Gigabit PoE+ switch. The managed switch supports the following Spanning Tree protocols:

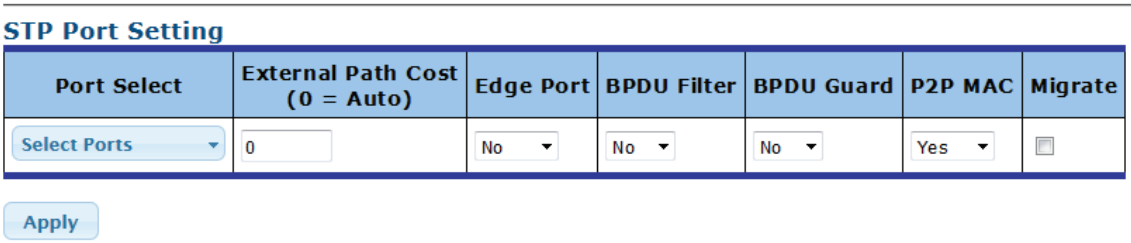
- Compatible -- Spanning Tree Protocol (STP):Provides a single path between end stations, avoiding and eliminating loops.
- Normal -- Rapid Spanning Tree Protocol (RSTP): Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- Extension – Multiple Spanning Tree Protocol (MSTP): Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.



Object	Description
• Enable	Enable or disable the STP function. The default value is "Disabled".
• BPDU Forward	Set the BPDU forward method.
• PathCost Method	The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
• Force Version	The STP protocol version setting. Valid values are **STP-Compatible**, **RSTP-Operation** and **MSTP-Operation**.
• Configuration Name	Identifier used to identify the configuration currently being used.
• Configuration Revision	Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is **0**.

4.6.3 STP Port Settings

All port related settings are configured on this screen.



Object	Description
• **Port Select**	Select port number for this drop down list.
• **External Cost (0 = Auto)**	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Edge Port**	Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized).
• **BPDU Filter**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• **P2P MAC**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always *forced Point2Point*).
• **Migrate**	If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: **Disabled**)

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

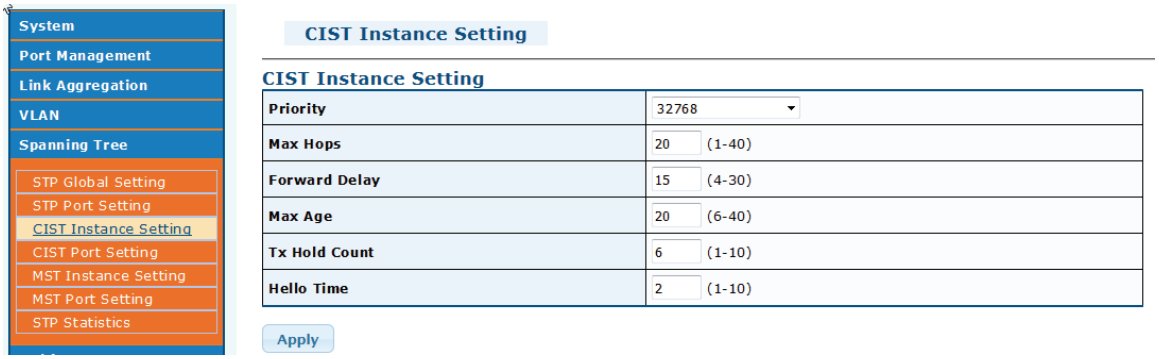
Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Default STP Path Costs

4.6.4 CIST Instance Setting

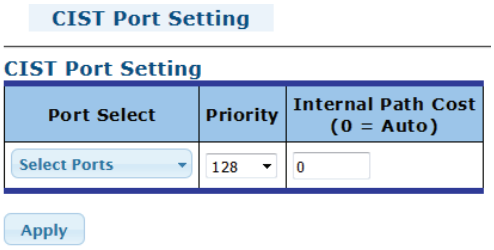
This Page allows you to configure CIST instance settings.



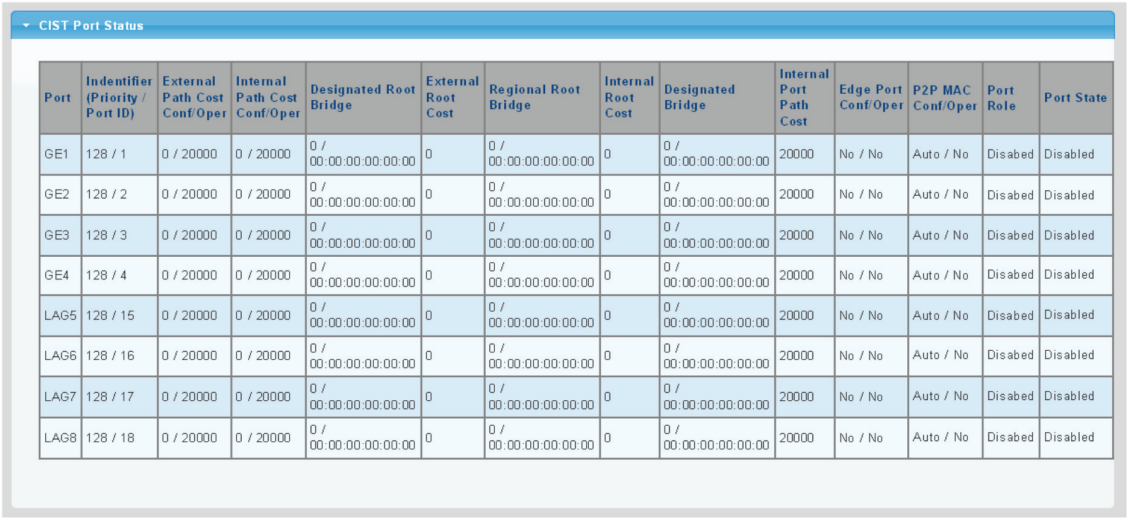
Object	Description
• riority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• Max Hops	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
• Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• Tx Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
• Hello Time	The time that controls the switch to send out the BPDU packet to check STP current status.

4.6.5 CIST Port Settings

ON this page you can configure the CIST priority and internal path cost of the Intellinet 8-Port Gigabit PoE Switch.



Object	Description
• **Port Select**	Select port number for this drop down list.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

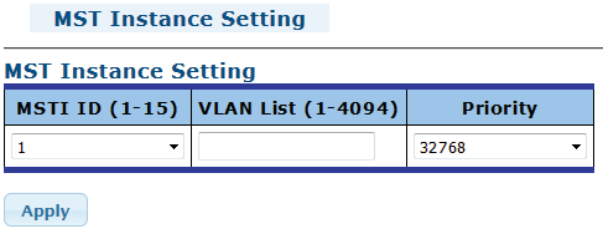


CIST Port Status Page Screenshot

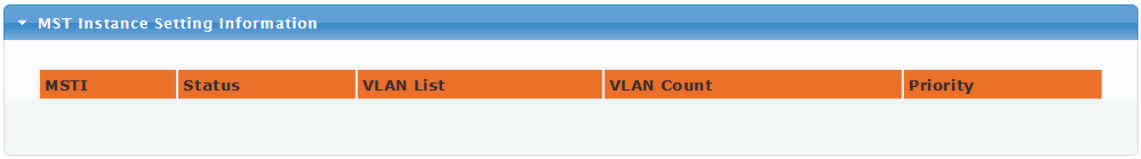
Object	Description
• **Port**	The switch port number of the logical STP port.
• **Indentifier (Priority / Port ID)**	Display the current indentifier (Priority / Port ID).
• **External Path Cost Conf/Oper**	Display the current external path cost conf/oper.
• **Internal Path Cost Conf/Oper**	Display the current internal path cost/oper.
• **Designated Root Bridge**	Display the current designated root bridge.
• **External Root Cost**	Display the current external root cost
• **Regional Root Bridge**	Display the current regional root bridge
• **Internal Root Cost**	Display the current internal root cost
• **Designated Bridge**	Display the current designated bridge
• **Internal Port Path Cost**	Display the current internal port path cost
• **Edge Port Conf/Oper**	Display the current edge port conf/oper
• **P2P MAC Conf/Oper**	Display the current P2P MAC conf/oper
• **Port Role**	Display the current prot role
• **Port State**	Display the current port state

4.6.6 *MST Instance Configuration*

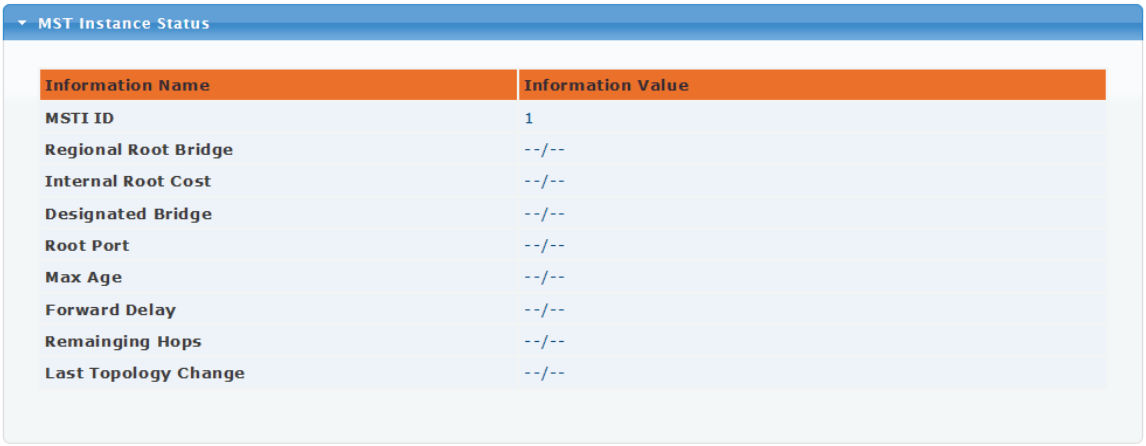
This page allows the user to configure MST Instance Configuration.



Object	Description
• **MSTI ID**	Allow assign MSTI ID. The range for the MSTI ID is 1-15.
• **VLAN List (1-4096)**	Allow assign VLAN list for special MSTI ID. The range for the VLAN list is 1-4094.
• **Priority**	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.



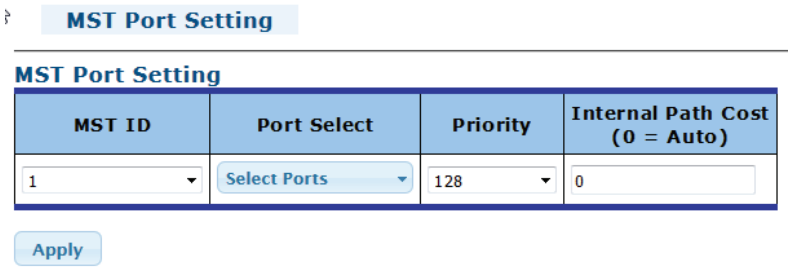
Object	Description
• **MSTI**	Display the current MSTI entry.
• **Status**	Display the current MSTI status
• **VLAN List**	Display the current VLAN list.
• **VLAN Count**	Display the current VLAN count.
• **Priority**	Display the current MSTI priority



Object	Description
• **MSTI ID**	Display the MSTI ID.
• **Regional Root Bridge**	Display the current designated root bridge.
• **Internal Root Cost**	Display the current internal root cost.
• **Designated Bridge**	Display the current designated bridge.
• **Root Port**	Display the current root port.
• **Max Age**	Display the current max. age.
• **Forward Delay**	Display the current forward delay.
• **Remaining Hops**	Display the current remaininging hops.
• **Last Topology Change**	Display the current last topology change.

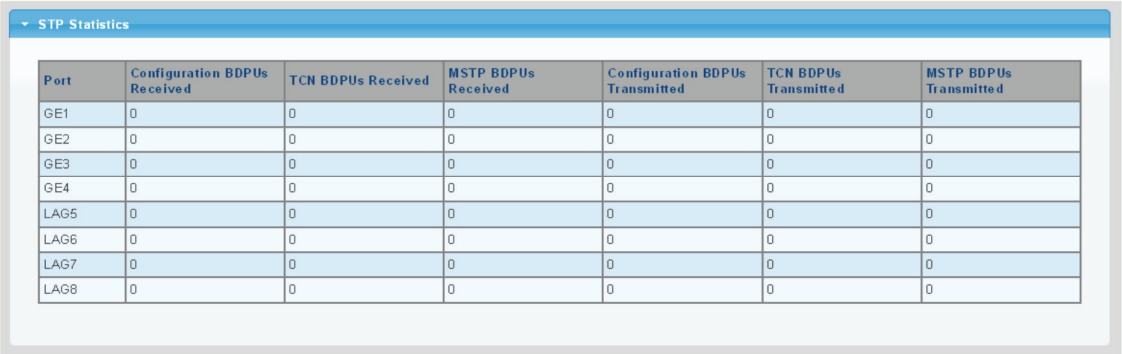
4.6.7 MST Port Settings

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global.



Object	Description
• **MST ID**	Enter the special MST ID to configure path cost & priority.
• **Port Select**	Select port number for this drop down list.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost.
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

4.6.8 STP Statistics

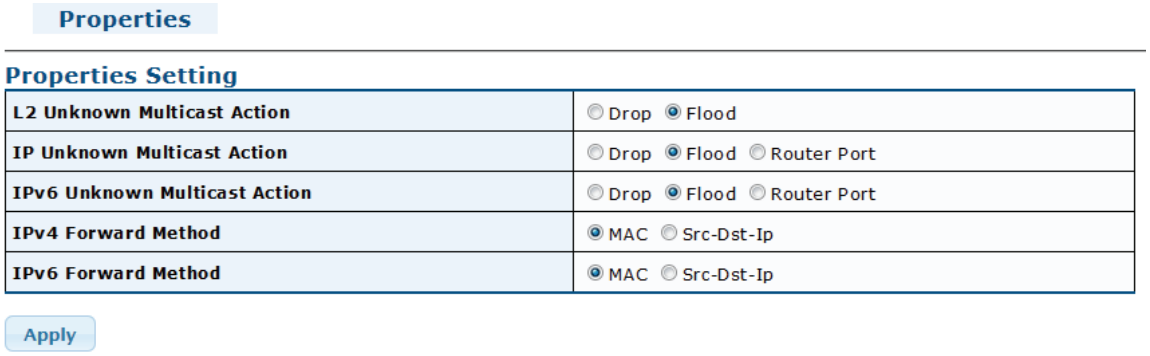


Object	Description
• **Port**	The switch port number of the logical STP port.
• **Configuration BPDUs Received**	Display the current configuration BPDUs received.
• **TCN BPDUs Received**	Display the current TCN BPDUs received
• **MSTP BPDUs Received**	Display the current MSTP BPDUs received
• **Configuration BPDUs Transmitted**	Display the configuration BPDUs transmitted
• **TCN BPDUs Transmitted**	Display the current TCN BPDUs transmitted
• **MSTP BPDUs Transmitted**	Display the current BPDUs transmitted

4.7 Multicast

4.7.1 Properties

This page provides multicast properties related configuration.

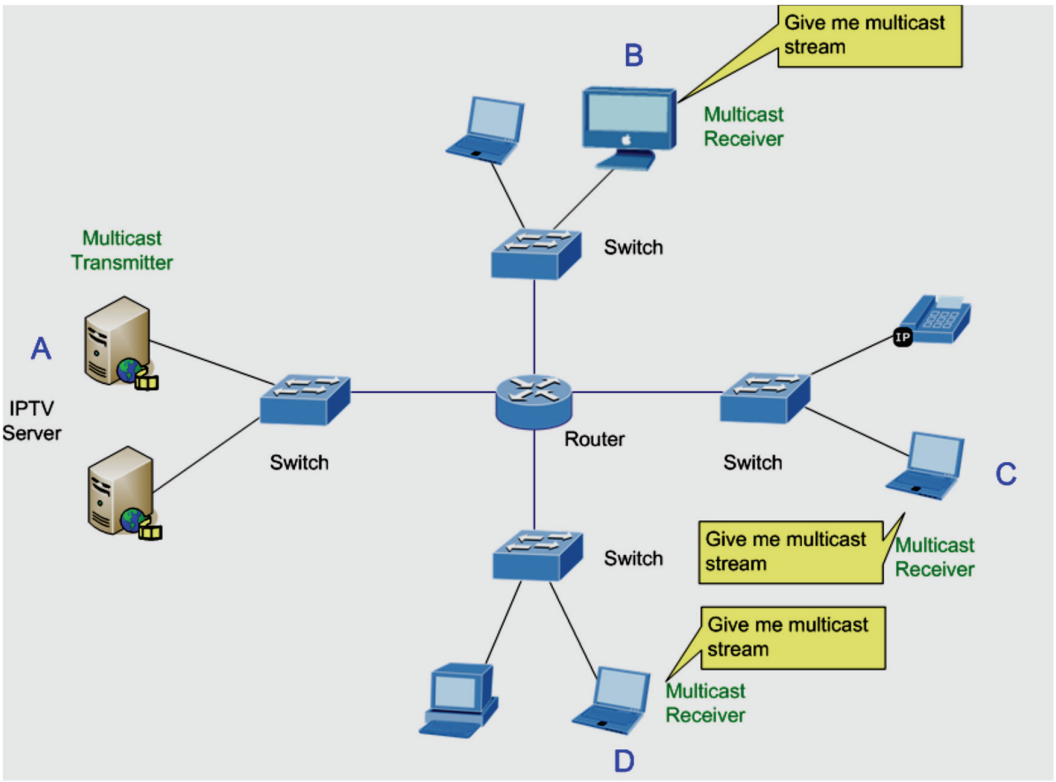


Parameter	Description
L2 Unknown Multicast Action	Unknown Layer 2 multicast traffic can be either dropped, or send out to all ports (flood).
IP Unknown Multicast Action	Unknown IPv4 multicast traffic method: Drop, flood or send to router port.
IPv6 Unknown Multicast Action	Unknown IPv6 multicast traffic method: Drop, flood or send to router port.
IPv4 Forward Method	Forwarding based on MAC or IP address.
IPv6 Forward Method	Forwarding based on MAC or IP address.

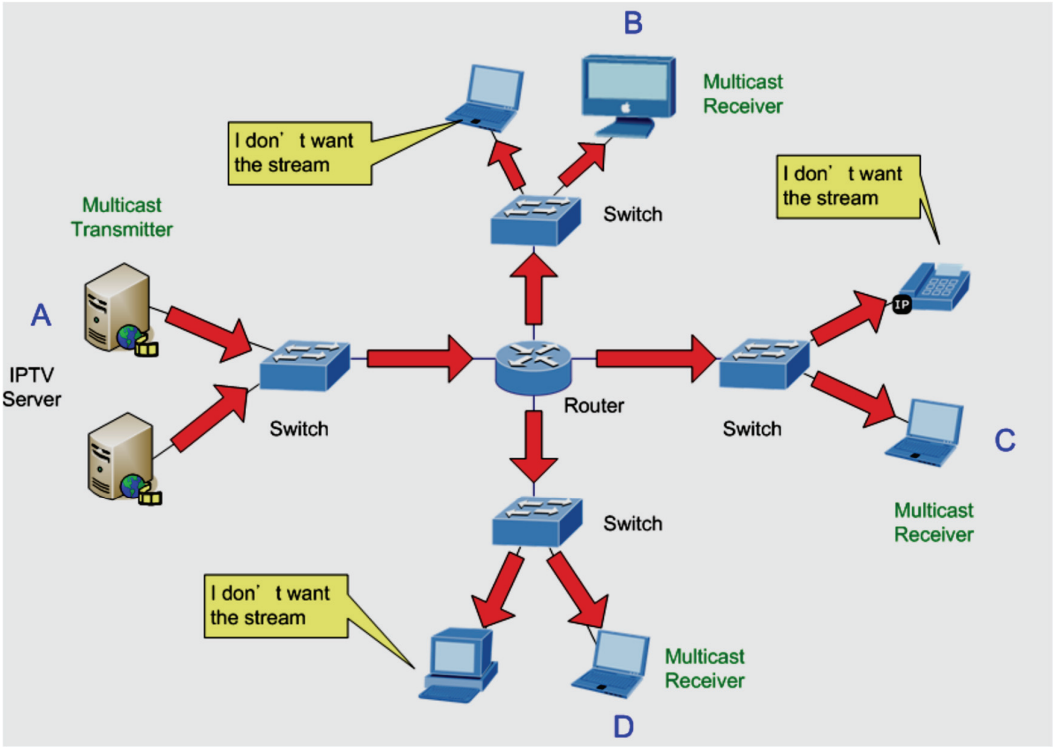
4.7.2 IGMP Snooping

The Internet Group Management Protocol (IGMP) lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

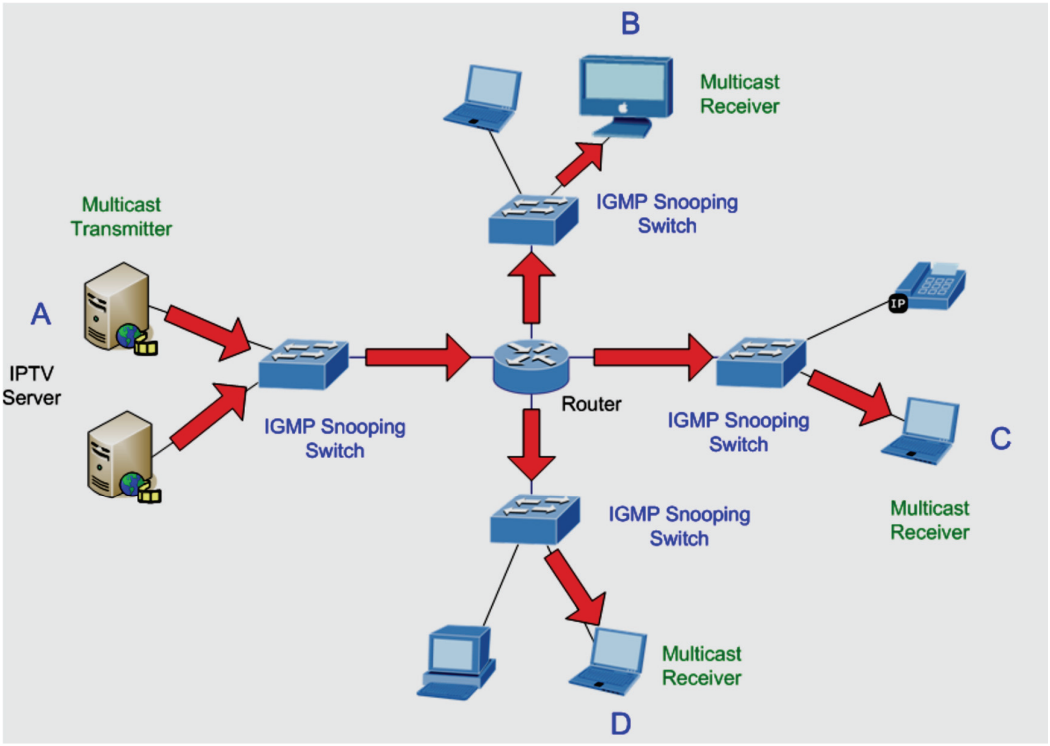
About the Internet Group Management Protocol (IGMP) Snooping
Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The Internet Group Management Protocol (IGMP) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on agiven subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.



Multicast Service



Multicast Flooding



IGMP Snooping Multicast Stream Control

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group. IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

TYPE <- 8 bits ->	**MaxResp Time** <-8 bits->	**CHECKSUM** <- 16 bits ->
GROUP ADDRESS <- 32 bits ->		
< IGMP Payload or future expansion >		

Type

- Type of IGMP message. There are three types: Membership Query, Membership Report and Leave Group.

Maximum Response Time

- This field is used only in Membership Query messages. This field is the maximum time a host is allowed to produce and send a Membership Report message after receiving a Membership Query message.

Checksum

- This is the one's compliment of the one's complement sum of the entire IGMP message, which basically works out to be the entire payload of the IP datagram the IGMP datagram is encapsulated within.

Group Address

- Behavior of this field varies by the type of message sent:
- Membership Query: (set to)
- General Query: All zeroes
- Group Specific Query: multicast group address
- Membership Report: multicast group address
- Leave Group: multicast group address

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP “report” to join a group

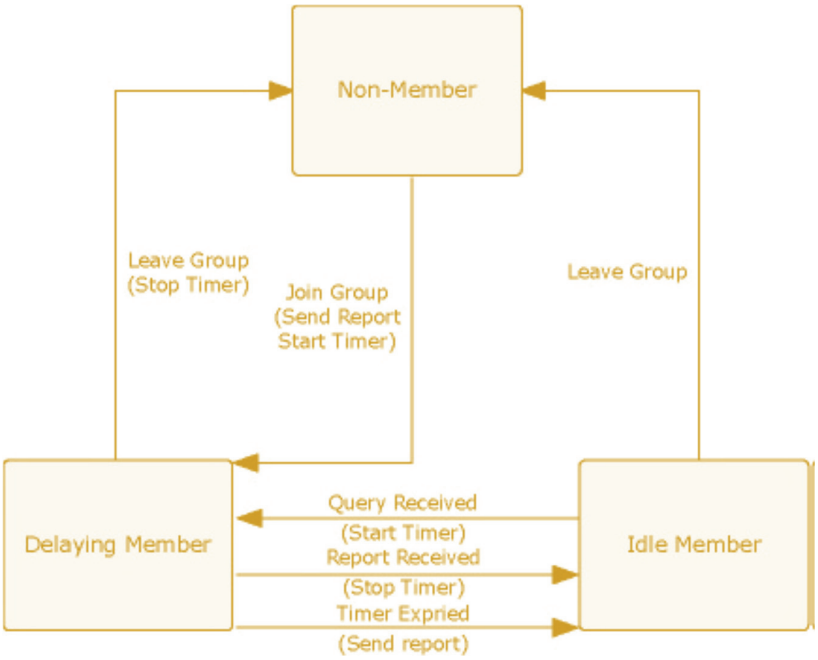
A host will never send a report when it wants to leave a group (for version 1).

A host will send a “leave” report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group. The states a computer will go through to join or to leave a multicast group are shown below:



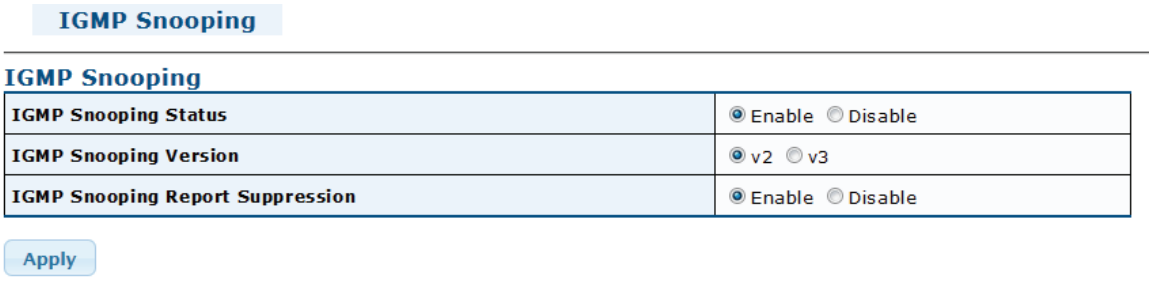
IGMP State Transitions

IGMP Querier –
A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

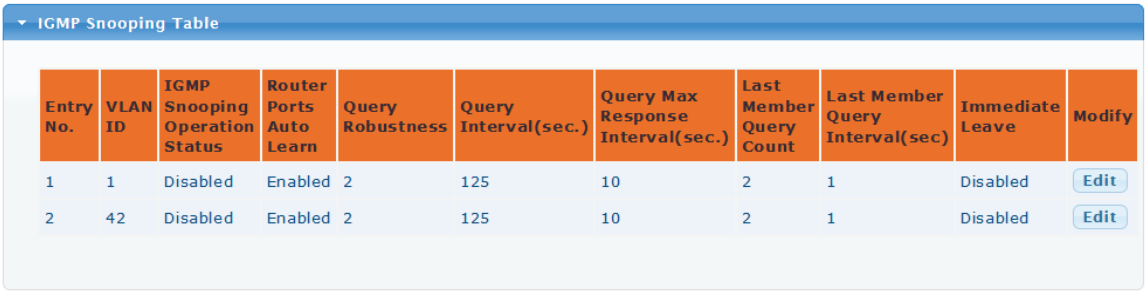
Note:
Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.7.2.1 IGMP Settings

This page provides IGMP Snooping related configuration. Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header.

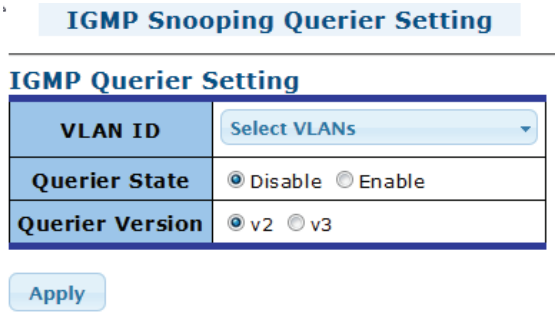


Object	Description
• **IGMP Snooping Status**	Enable or disable the IGMP snooping. The default value is "Disabled".
• **IGMP Snooping Version**	Sets the IGMP Snooping operation version. Possible versions are: ■ **v2**: Set IGMP Snooping supported IGMP version 2. ■ **v3**: Set IGMP Snooping supported IGMP version 3.
• **IGMP Snooping Report Suppression**	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.



Object	Description
• **Entry No.**	Display the current entry number.
• **VLAN ID**	Display the current VLAN ID.
• **IGMP Snooping Operation Status**	Display the current IGMP snooping operation status.
• **Router Ports Auto Learn**	Display the current router ports auto learning.
• **Query Robustness**	Display the current query robustness.
• **Query Interval (sec.)**	Display the current query interval.
• **Query Max Response Interval (sec.)**	Display the current query max response interval.
• **Last Member Query conut**	Display the current last member query count.
• **Last Member Query Interval (sec)**	Display the current last member query interval.
• **Immediate Leave**	Display the current immediate leave.
• **Modify**	Click Edit to edit parameter.

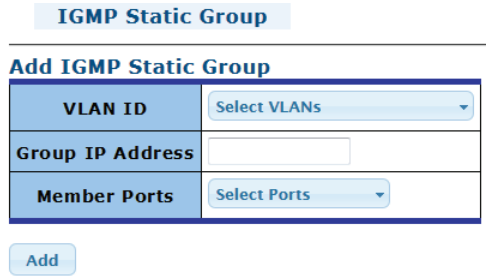
4.7.2.2 *IGMP Snooping Querier Settings*



Object	Description
• VLAN ID	Select VLAN ID for this drop down list.
• Querier State	Enable or disable the querier state. The default value is "Disabled".
• Querier Version	Sets the querier version for compatibility with other devices on the network. Version: 2 or 3; Default: **2**

4.7.2.3 *IGMP Static Group*

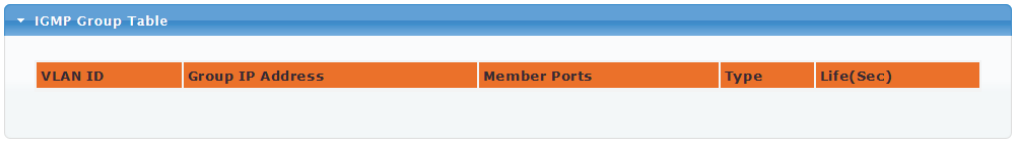
Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in above sections. For certain applications that require tighter control, you may need to statically configure a multicast service on the Managed Switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.
- Static multicast addresses are never aged out.- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.



Object	Description
• VLAN ID	Select VLAN ID for this drop down list.
• Group IP Address	The IP address for a specific multicast service
• Member Ports	Select port number for this drop down list.

4.7.2.4 *IGMP Group Table*

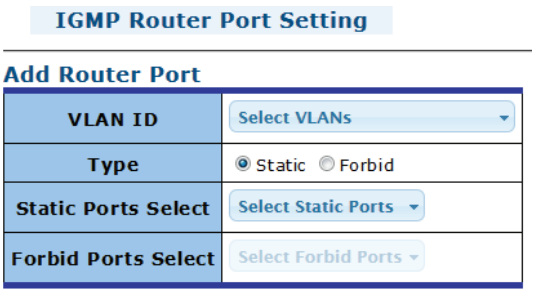
This page provides an overview over the current IGMP group table (multicast database).



Object	Description
• **VLAN ID**	Display the current VID.
• **Group IP Address**	Display multicast IP address for a specific multicast service.
• **Member Port**	Display the current member port.
• **Type**	Member types displayed include Static or Dynamic, depending on selected options.
• **Life(Sec)**	Display the current life.

4.7.2.5 *IGMP Router Port Settings*

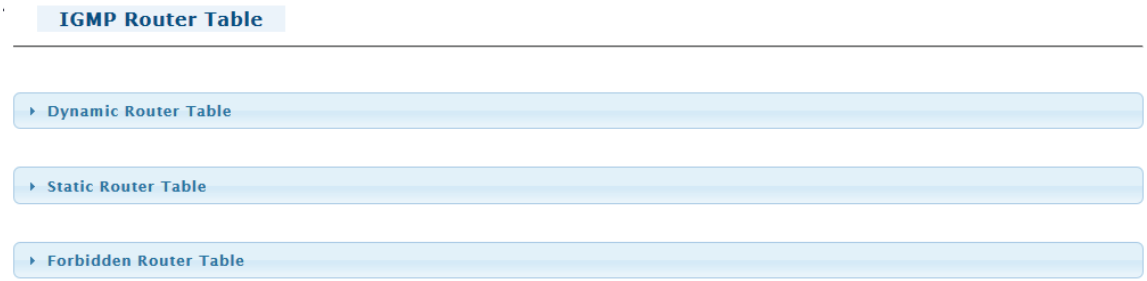
Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch.



Object	Description
• **VLAN ID**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
• **Type**	Sets the Router port type. The types of Router port as below: ■ **Static** ■ **Forbid**
• **Static Ports Select**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
• **Forbid Port Select**	Specify which ports un-act as router ports.

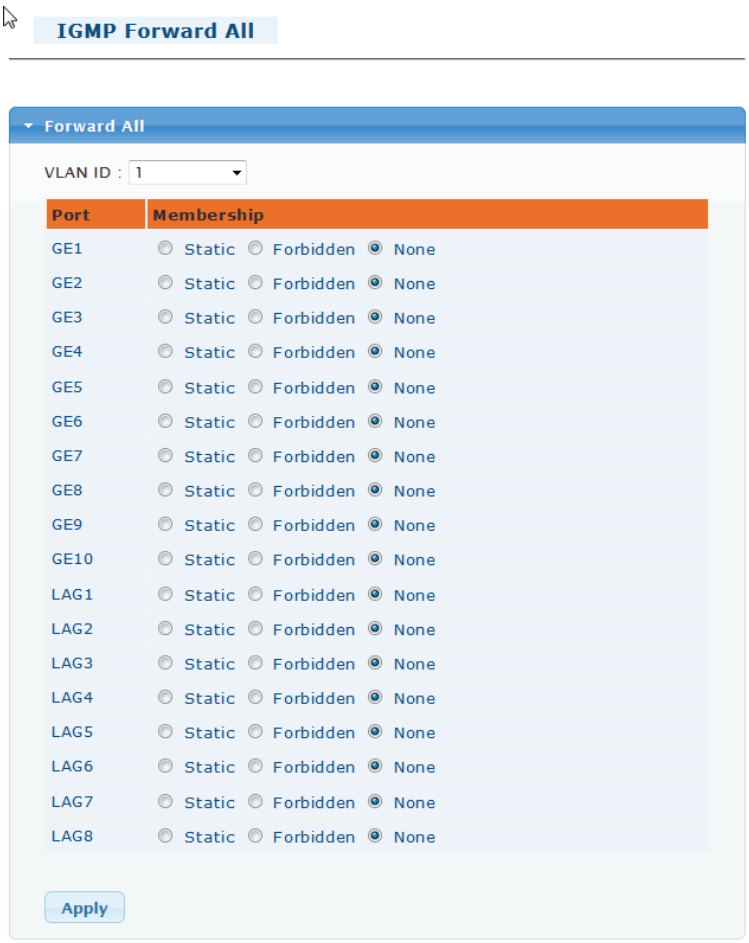
4.7.2.6 *IGMP Router Table*

This section provides statistical information about the current IGMP routing tables. There are no configuration options here.



4.7.2.7 *IGMP Forward All*

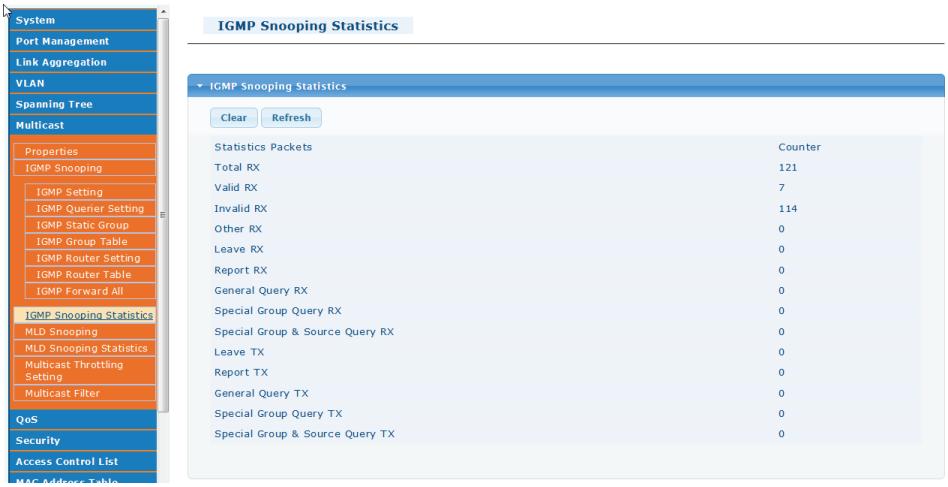
This page provides IGMP Forward All.



Object	Description	
• **VLAN ID**	Select VLAN ID for this drop down list to assign IGMP membership.	
• **Port**	The switch port number of the logical port.	
• **Membership**	Select IGMP membership for each interface:	
	Forbidden:	Interface is forbidden from automatically joining the IGMP via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Static:	Interface is a member of the IGMP.

4.7.3 IGMP Snooping Statics

This page provides IGMP Snooping Statics.

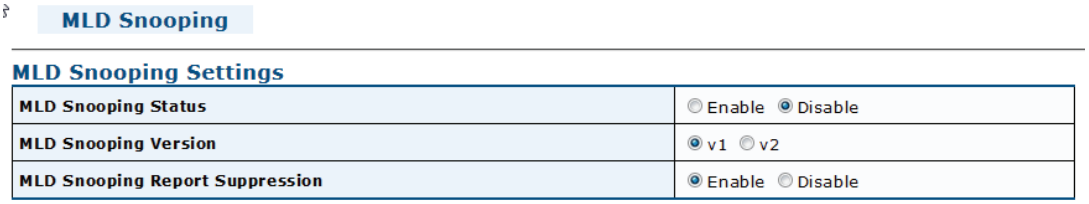


Object	Description
• **Total RX**	Display current total RX
• **Valid RX**	Display current valid RX
• **Invalid RX**	Display current invalid RX
• **Other RX**	Display current other RX
• **Leave RX**	Display current leave RX
• **Report RX**	Display current report RX
• **General Query RX**	Display current general query RX
• **Special Group Query RX**	Display current special group query RX
• **Special Group & Source Query RX**	Display current special group & source query RX
• **Leave TX**	Display current leave TX
• **Report TX**	Display current report TX
• **General Query TX**	Display current general query TX
• **Special Group Query TX**	Display current special group query TX
• **Special Group & Source Query TX**	Display current special group & source query TX

4.7.4 MLD Snooping

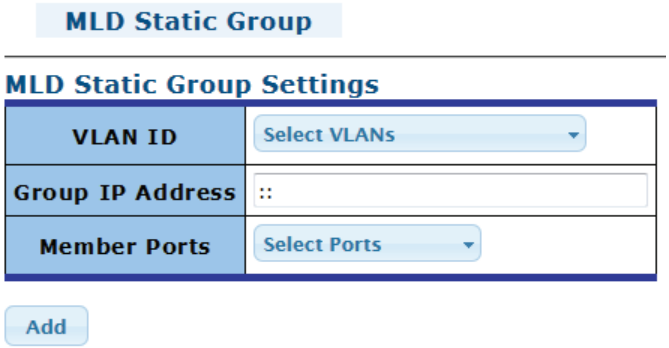
4.7.4.1 MLD Setting

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.
MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58. This page provides MLD (Multicast Listener Discovery) Snooping related configuration. Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header.



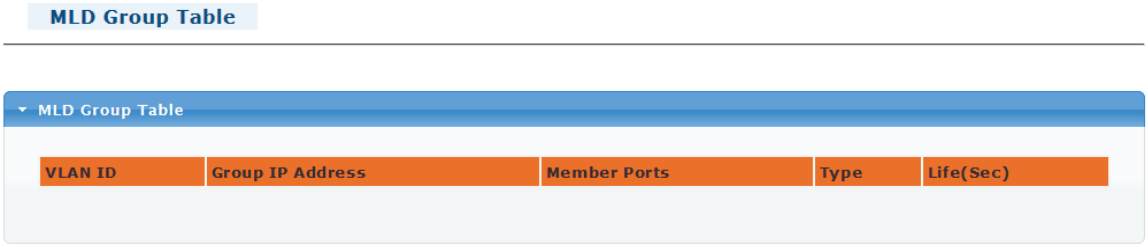
Object	Description
• Entry No.	Display the current entry number.
• VLAN ID	Display the current VLAN ID.
• MLD Snooping Operation Status	Display the current MLD snooping operation status.
• Router Ports Auto Learn	Display the current router ports auto learning.
• Query Robustness	Display the current query robustness.
• Query Interval (sec.)	Display the current query interval.
• Query Max Response Interval (sec.)	Display the current query max response interval.
• Last Member Query conut	Display the current last member query count.
• Last Member Query Interval (sec)	Display the current last member query interval.
• Immediate Leave	Display the current immediate leave.
• Modify	Click Edit to edit parameter.

4.7.4.2 MLD Static Group



Object	Description
• VLAN ID	Select VLAN ID for this drop down list.
• Group IP Address	The IP address for a specific multicast service
• Member Ports	Select port number for this drop down list.

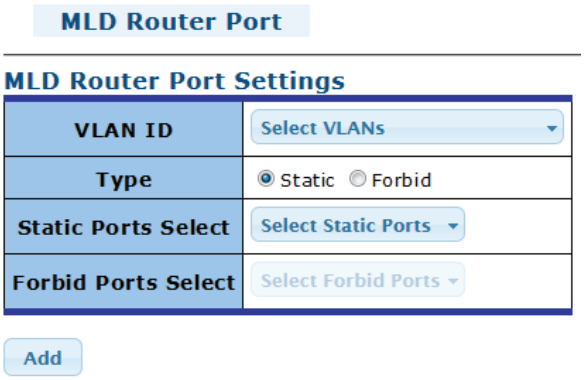
4.7.4.3 MLD Group Table



Object	Description
• VLAN ID	Display the current VID.
• Group IP Address	Display multicast IP address for a specific multicast service.
• Member Port	Display the current member port.
• Type	Member types displayed include Static or Dynamic, depending on selected options.
• Life(Sec)	Display the current life.

4.7.4.4 MLD Router Settings

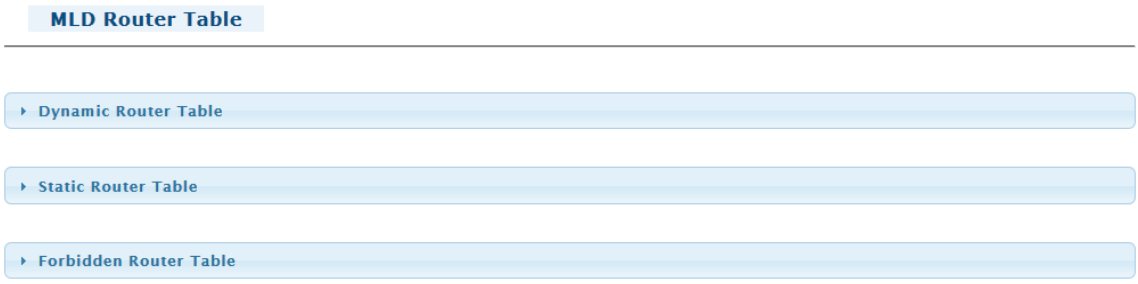
Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch.



Object	Description
• **VLAN ID**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
• **Type**	Sets the Router port type. The types of Router port as below: **Static** **Forbid**
• **Static Ports Select**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
• **Forbid Port Select**	Specify which ports un-act as router ports.

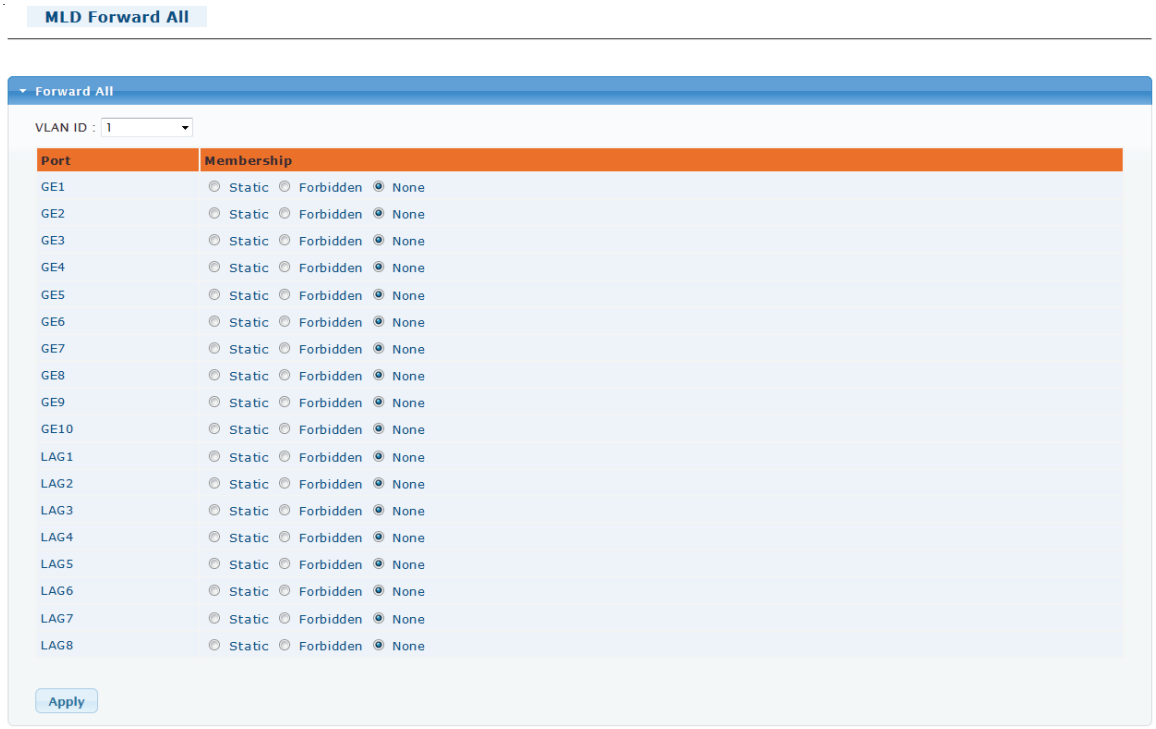
4.7.4.5 MLD Router Table

This page contains the MLD router tables of the Intellinet 8-Port Gigabit PoE+ Switch.



4.7.4.6 MLD Forward All

Define the MLD Forward All settings on this page.



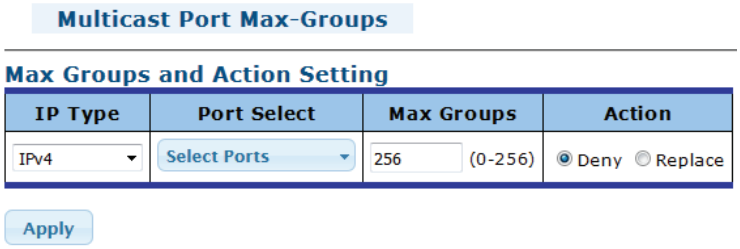
Object	Description	
• **VLAN ID**	Select VLAN ID for this drop down list to assign MLD membership.	
• **Port**	The switch port number of the logical port.	
• **Membership**	Select MLD membership for each interface:	
	Forbidden:	Interface is forbidden from automatically joining the MLD via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Static:	Interface is a member of the MLD.

4.7.5 MLD Snooping Statics

Object	Description
• **Total RX**	Display current total RX
• **Valid RX**	Display current valid RX
• **Invalid RX**	Display current invalid RX
• **Other RX**	Display current other RX
• **Leave RX**	Display current leave RX
• **Report RX**	Display current report RX
• **General Query RX**	Display current general query RX

4.7.6 Multicast Throttling Setting

Multicast throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new multicast join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. Once you have configured multicast profiles, you can assign them to interfaces on the Managed Switch. Also you can set the multicast throttling number to limit the number of multicast groups an interface can join at the same time.



Object	Description
• **IP Type**	Select IPv4 or IPv6 for this drop down list.
• **Port Select**	Select port number for this drop down list.
• **Max Groups**	Sets the maximum number of multicast groups an interface can join at the same time. Range: 0-256; Default: **256**
• **Action**	Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny) **-Deny** - The new multicast group join report is dropped. **-Replace** - The new multicast group replaces an existing group.

4.7.7 Multicast Filter

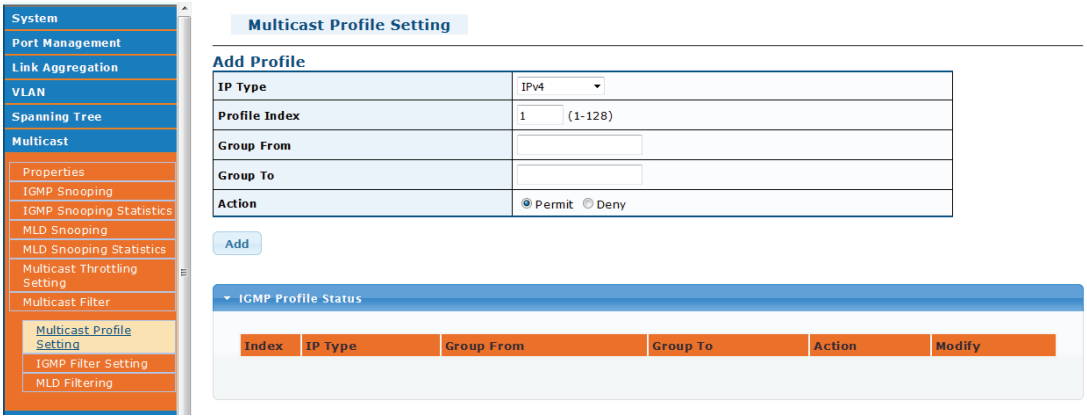
In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service is based on a specific subscription plan. The multicast filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port. Multicast filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A multicast filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port.

When enabled, multicast join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the multicast join report is forwarded as normal. If a requested multicast group is denied, the multicast join report is dropped.
When you have created a Multicast profile number, you can then configure the multicast groups to filter and set the access mode.

Command Usage

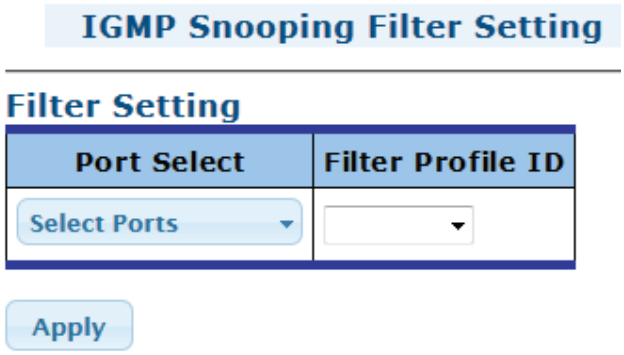
- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, multicast join reports are processed when a multicast group falls within the controlled range.
- When the access mode is set to deny, multicast join reports are only processed when the multicast group is not in the controlled range.

4.7.7.1 Multicast Profile Setting



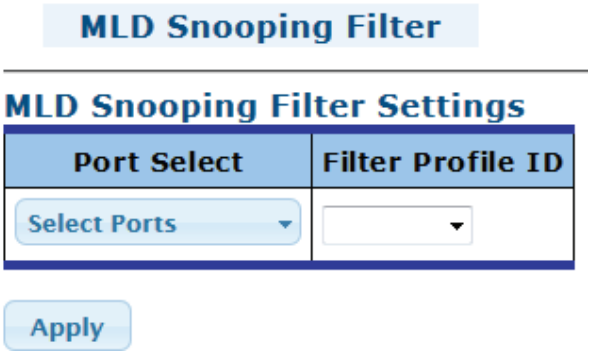
Object	Description	
• **IP Type**	Select IPv4 or IPv6 for this drop down list.	
• **Profile Index**	Indicates the ID of this particular profile.	
• **Group from**	Specifies multicast groups to include in the profile. Specify a multicast group range by entering a start IP address.	
• **Group to**	Specifies multicast groups to include in the profile. Specify a multicast group range by entering an end IP address.	
• **Action**	Sets the access mode of the profile; either **permit** or **deny**.	
	- Permit	Multicast join reports are processed when a multicast group falls within the controlled range.

4.7.7.2 IGMP Filter Setting



Object	Description
• **Port Select**	Select port number for this drop down list.
• **Filter Profile ID**	Select filter profile ID for this drop down list.

4.7.7.3 MLD Filter Setting



Object	Description
• **Port Select**	Select port number for this drop down list.
• **Filter Profile ID**	Select filter profile ID for this drop down list.

4.8 QoS - Quality of Service

4.8.1 General / What is QoS?

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.
QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to control a wide variety of network traffic by:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter. Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

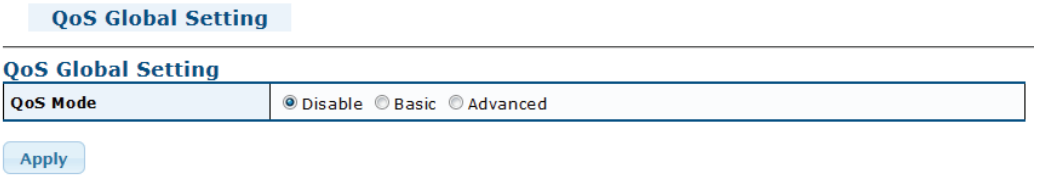
The QoS page of the Managed Switch contains three types of QoS mode - the 802.1p mode, DSCP mode or Port-base mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- 802.1p Tag Priority Mode –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- IP DSCP Mode - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- Port-Base Priority Mode – Any packet received from the specify high priority port will treated as a high priority packet.

The Managed Switch supports eight priority level queue, the queue service rate is based on the WRR (Weight Round Robin) and WFQ (Weighted Fair Queuing) algorithm. The WRR ratio of high-priority and low-priority can be set to “4:1 and 8:1. 4.8.2 General

4.8.1.1 QoS Properties

On this screen you can activate or deactivate QoS.



Parameter	Description
QoS Mode	Disable: QoS is deactivated. Basic: QoS is enabled in basic mode. Basic: QoS is enabled in advanced mode.

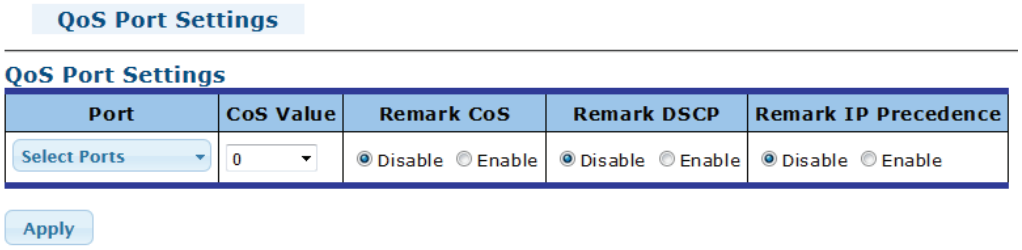
Note:

In QoS advanced mode, the Intellinet 8-Port Gigabit PoE+ switch uses policies to support per-flow QoS. The policy and its components have the following characteristics:

- A policy may contains one or more class maps.
- A policy contains one or more flows, each with a user defined QoS.
- A single policer applies the QoS to a single class map, and thus to a single flow, based on the policer QoS specification.
- An aggregate policer applies the QoS to one or more class maps, and thus one or more flows.
- Per flow QoS are applied to flows by binding the policies to the desired ports.

4.8.1.2 QoS Port Settings

The QoS Port Settings and Status screen.



Object	Description
• **Port Select**	Select port number for this drop down list.
• **CoS Value**	Select CoS value for this drop down list.
• **Remark CoS**	Disable or enable remark CoS
• **Remark DSCP**	Disable or enable remark DSCP
• **Remark IP Precedence**	Disable or enable remark IP Precedence

4.8.1.3 Queue Settings

Define the scheduling method of the 8 QoS queues on this configuration screen.

Queue Settings

Queue Table

Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	◉	○	1	
2	◉	○	2	
3	◉	○	3	
4	◉	○	4	
5	◉	○	5	
6	◉	○	9	
7	◉	○	13	
8	◉	○	15	

Apply

Object	Description
• **Queue**	Display the current queue ID.
• **Strict Priority**	Controls whether the scheduler mode is "Strict Priority" on this switch port.
• **WRR**	Controls whether the scheduler mode is "Weighted" on this switch port.
• **Weight**	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **% of WRR Bandwidth**	Display the current bandwith for each queue.

4.8.1.4 CoS Mapping

This screen controls to mapping of Class of Service (CoS) to the queues.

CoS Mapping

CoS to Queue Mapping

Class of Service	0	1	2	3	4	5	6	7
Queue	2	1	3	4	5	6	7	8

Queue to CoS Mapping

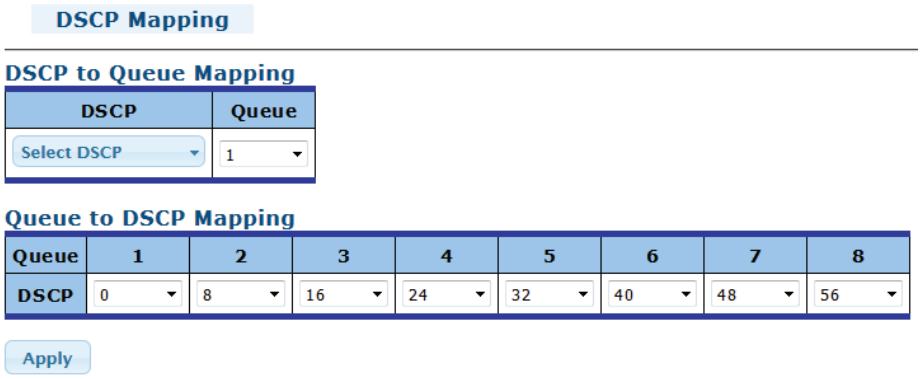
Queue	1	2	3	4	5	6	7	8
Class of Service	1	0	2	3	4	5	6	7

Apply

Object	Description
• Queue	Select Queue value for this drop down list.
• Class of Service	Select CoS value for this drop down list.

4.8.1.5 DSCP Mapping

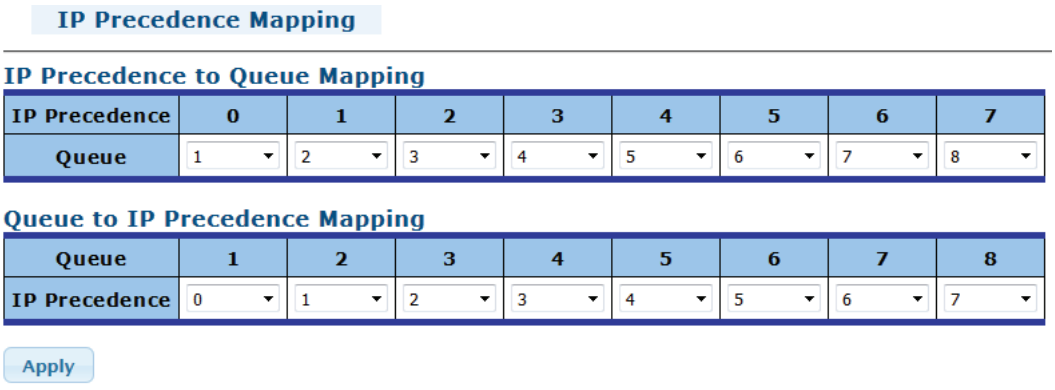
The DSCP to Queue and Queue to DSCP Mapping screen



Object	Description
• Queue	Select Queue value for this drop down list.
• DSCP	Select DSCP value for this drop down list.

4.8.1.6 IP Precedence Mapping

The IP Precedence to Queue and Queue to IP Precedence Mapping screen.

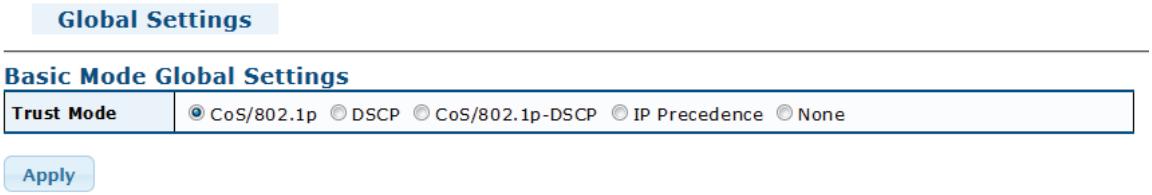


Object	Description
• Queue	Select Queue value for this drop down list.
• IP Precedence	Select IP Precedence value for this drop down list.

4.8.2 QoS Basic Mode

4.8.2.1 Global Settings

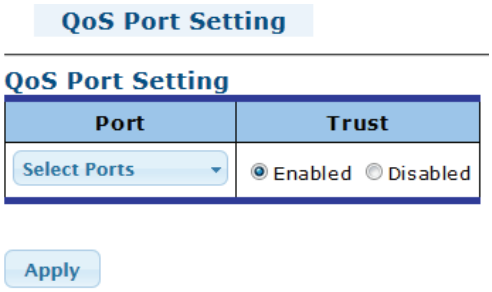
On this interface screen you can define the QoS trust mode.



Parameter	Description
Trust Mode	CoS/802.1p — This is a Layer 2 QoS where traffic is mapped to queues based on the VLAN Priority Tag (VPT) field in the VLAN tag. If there is no VLAN tag on the incoming packet, the traffic is mapped to queues based on the per-port default CoS/802.1p value. DSCP — This is a Layer 3 QoS. Where all IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic, it is mapped to the best effort queue. CoS/802.1p-DSCP — All non-IP traffic is mapped through the use of CoS/802.1p. All IP traffic is mapped through DSCP. IP Precedence — The IP header has a field called the Type of Service (TOS) that sits between the Header Length field and the Total Length field. IP Precedence uses the first three bits of the TOS field to give 8 possible precedence values. ▪ 000 (0) - Routine ▪ 001 (1) - Priority ▪ 010 (2) - Immediate ▪ 011 (3) - Flash ▪ 100 (4) - Flash Override ▪ 101 (5) - Critical ▪ 110 (6) - Internetwork Control ▪ 111 (7) - Network Control

4.8.2.2 QoS Port Setting

Once the trust mode has been properly configured, the next step is to choose the interfaces (switch port) to which QoS is applied.

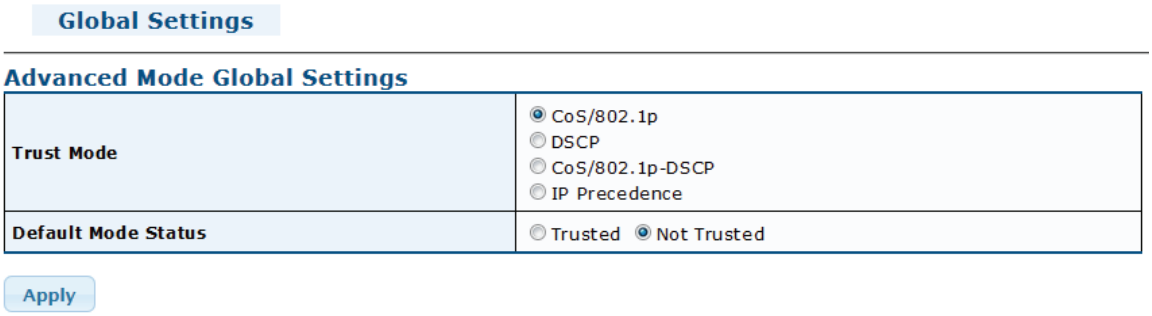


Object	Description
• **Port**	Select port number for this drop down list.
• **Trust Mode**	Enable or disable the trust mode.

4.8.3 QoS Advanced Mode

4.8.3.1 Global Settings

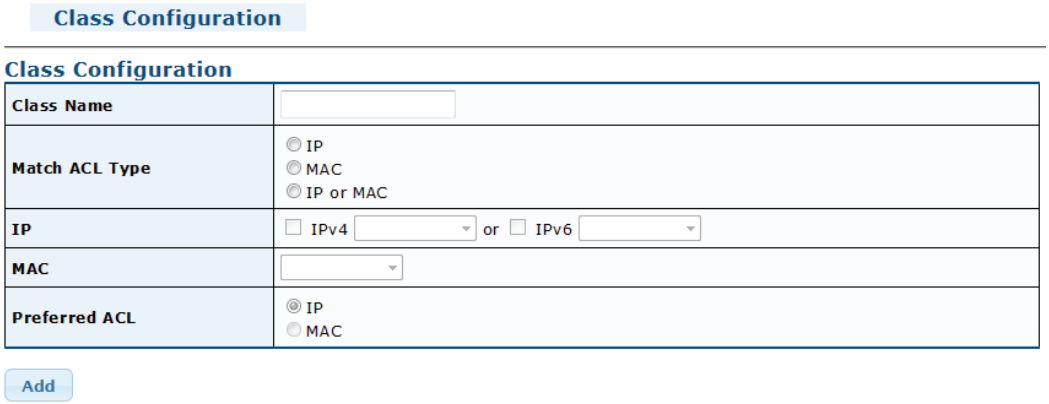
On this interface screen you can define the QoS trust mode.



Parameter	Description
Trust Mode	CoS/802.1p — This is a Layer 2 QoS where traffic is mapped to queues based on the VLAN Priority Tag (VPT) field in the VLAN tag. If there is no VLAN tag on the incoming packet, the traffic is mapped to queues based on the per-port default CoS/802.1p value. DSCP — This is a Layer 3 QoS. Where all IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic, it is mapped to the best effort queue. CoS/802.1p-DSCP — All non-IP traffic is mapped through the use of CoS/802.1p. All IP traffic is mapped through DSCP. IP Precedence — The IP header has a field called the Type of Service (TOS) that sits between the Header Length field and the Total Length field. IP Precedence uses the first three bits of the TOS field to give 8 possible precedence values. ▪ 000 (0) - Routine ▪ 001 (1) - Priority ▪ 010 (2) - Immediate ▪ 011 (3) - Flash ▪ 100 (4) - Flash Override ▪ 101 (5) - Critical ▪ 110 (6) - Internetwork Control ▪ 111 (7) - Network Control
Default Mode Status	Click the radio button that corresponds to the desired mode status. This provides a way to trust CoS/DSCP without the need to create a policy. • Trusted — Trust CoS/DSCP. • Not Trusted — Do not trust CoS/DSCP. The default CoS values configured on the interface are used to prioritize the traffic that arrives on the interface.

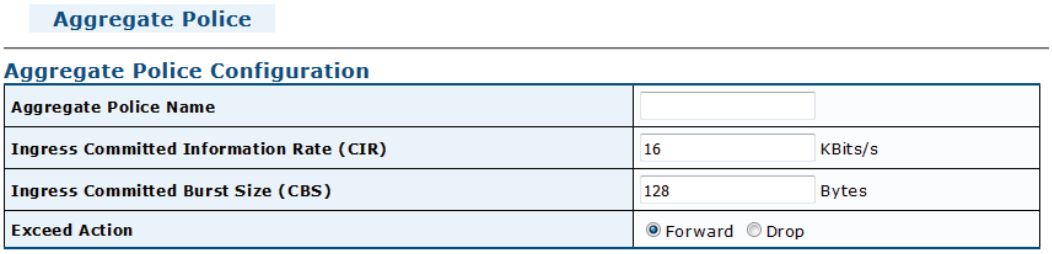
4.8.3.2 Class Configuration

QoS class mapping is configured on this page.



Object	Description
• Class Name	Input the class name and 32 characters allowed.
• Match ACL Type	Choose "IP", "MAC" or "IP or MAC" as match ACL type.
• IP	Choose "IPv4" or "IPv6".
• MAC	Choose specific MAC adrress.
• Preferred ACL	Choose "IP" or "MAC" for preferred ACL.

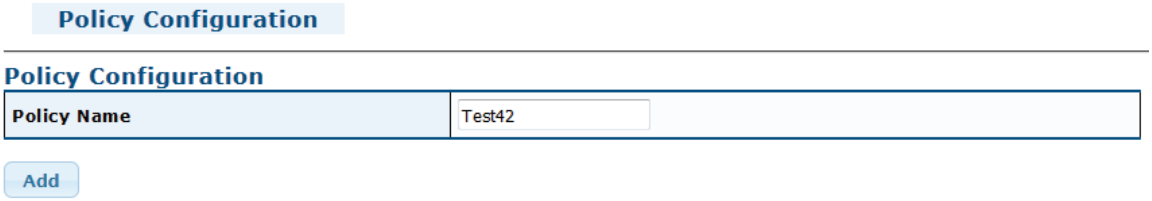
4.8.3.3 Aggregate Police



Object	Description
• Aggregate Police Name	Input the aggregate police name and 32 characters allowed.
• Ingress Committed Information Rate (CIR)	Allow input a number as ingress committed information rate.
• Ingress Committed Burst Size (CBS)	Allow input a number as ingress committed burst size.
• Exceed Action	Choose "Forward" or "Drop" when the exceed action situation appears.

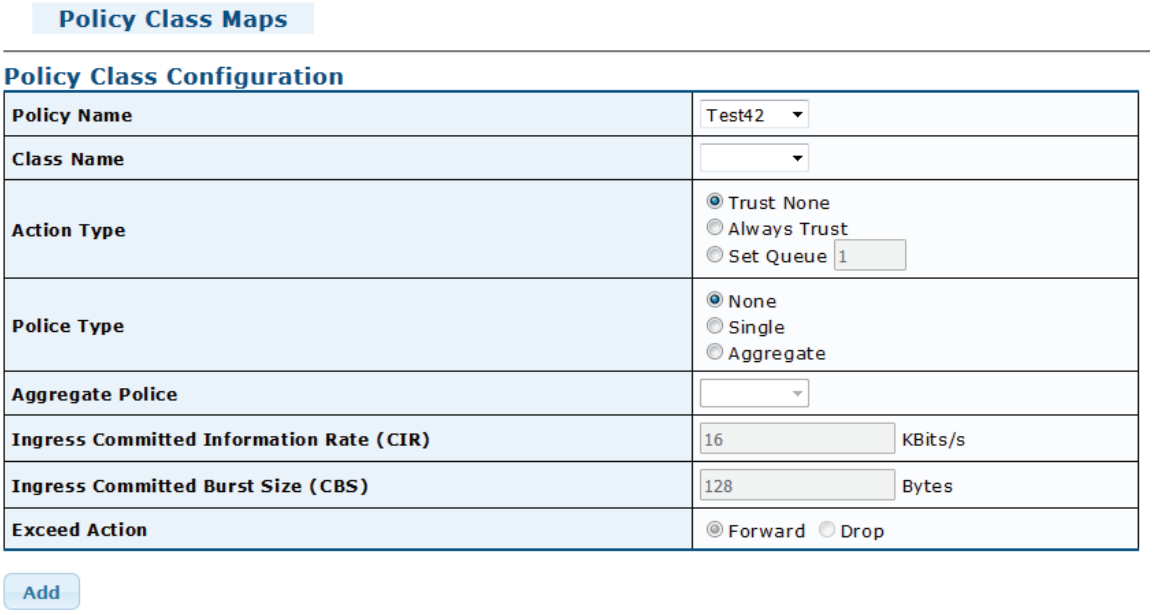
4.8.3.4 *Policy Configuration*

Provide a name for a policy on this page.



Object	Description
• Policy Name	Input the policy name and 31 characters allowed.

4.8.3.5 *Policy Class Maps*

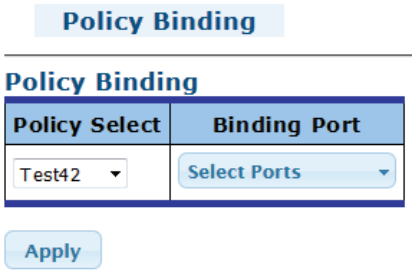


Object	Description
• Policy Name	Allow choose one specific policy name.
• Class Name	Allow choose one specific class name.
• Action Type	Provide “Trust None”, Always Trust” and “Set Queue” oprtions.
• Police Type	Provide “None”, “Single” and “Aggregate” options.
• Aggregate Police	Allow choose one specific aggregate police profile.
• Ingress Committed	Allow input a number as ingress committed information rate.

Information Rate (CIR)	
• Ingress Committed Burst Size (CBS)	Allow input a number as ingress committed burst size.
• Exceed Action	Choose “Forward” or “Drop” when the exceed action situation appears.

4.8.3.6 Policy Binding

On this page you can link the policies to an interface (Network port, or LAG).



Object	Description
• Policy Select	Select policy from this drop down list.
• Binding Port	Select one specific port from this drop down list.

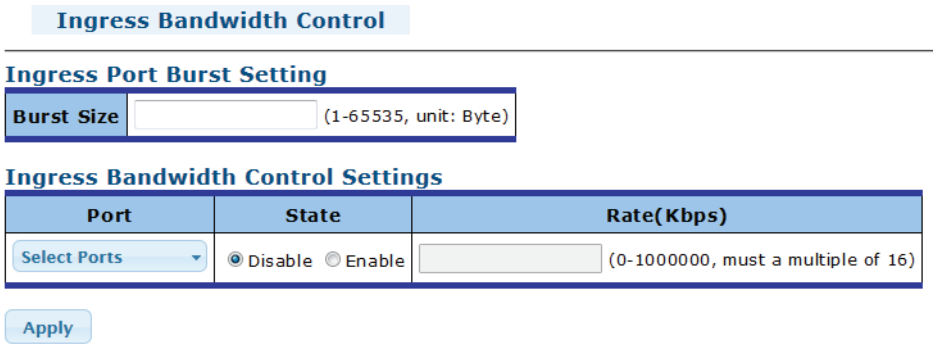
4.8.4 Rate Limit

Policing, or rate limiting, allows you to monitor the data rates for a particular class of traffic. When the data rate exceeds user-configured values, the Intellinet switch drops packets immediately. Because policing does not buffer the traffic; transmission delays are not affected. When traffic exceeds the data rate on a specific class, the switch drops the packets.

Rate limiting is configured for two types of transmissions, which are ingress and egress. Ingress traffic is received on any given port (incoming, or inbound), whereas egress traffic is traffic sent out (outgoing, outbound) to another network client.

4.8.4.1 Ingress Bandwidth Control

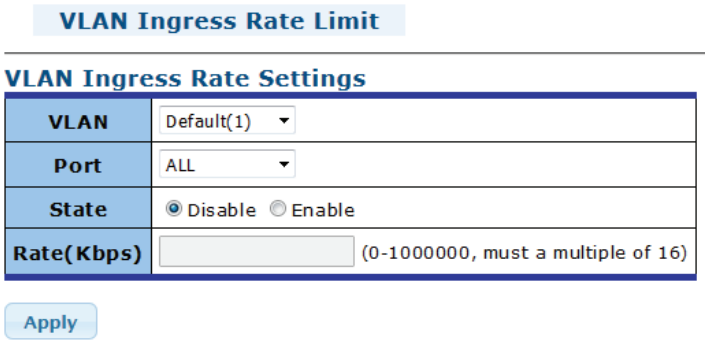
Control inbound bandwidth usage with this configuration screen.



Parameter	Description
Burst Size	The maximum size permitted for bursts of data. Burst sizes are measured in bytes. We recommend this formula for calculating the correct burst size: Burst size = bandwidth x allowable time for burst traffic / 8.
Port	Ports 1 to 10.
State	Disable or enable the ingress bandwidth control.
Rate (kbps)	The average number of kilobits per second permitted for packets received at the interface. You can specify the bandwidth limit as an absolute number of kilobits per second.

4.8.4.2 *VLAN Ingress Rate Limit*

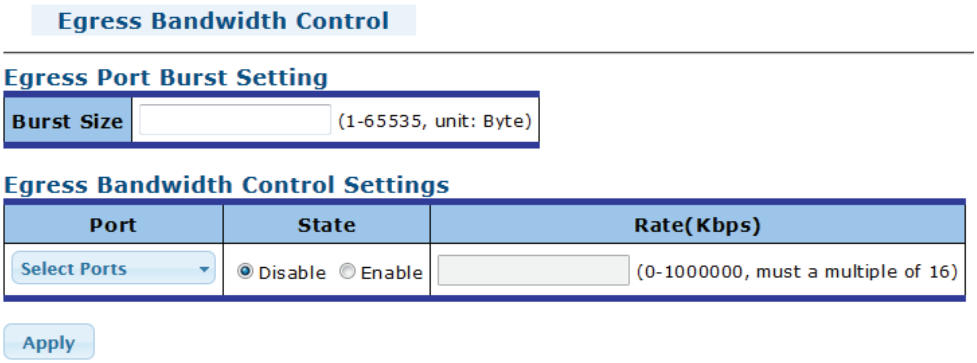
Traffic limiting on VLANs can be achieved by rate limiting per VLAN. Ingress traffic is the traffic which comes into the ports of the switch. When VLAN ingress rate limiting is configured, it constrains the traffic from all the ports on the switch.



Parameter	Description
VLAN	VLAN ID.
Port	Ports 1 to 10, LAG1 to LAG8.
State	Disable or enable the ingress bandwidth control.
Rate (kbps)	The average number of kilobits per second permitted for packets received at the interface. You can specify the bandwidth limit as an absolute number of kilobits per second.

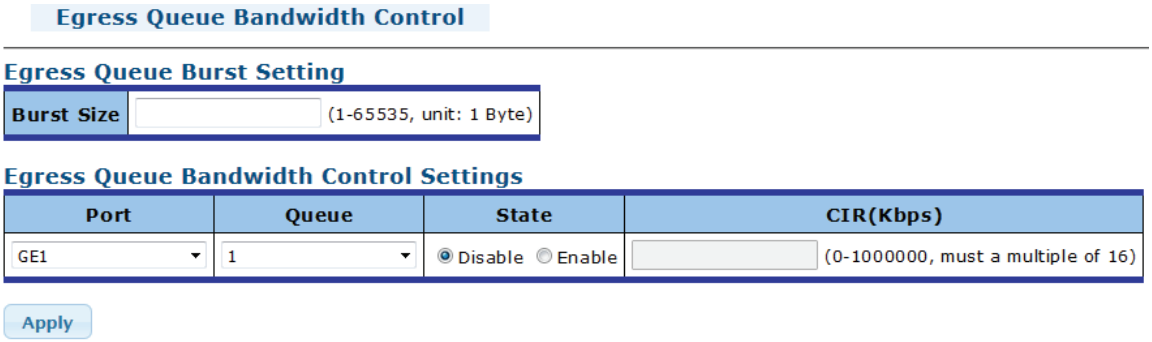
4.8.4.3 *Egress Bandwidth Control*

The configuration of the egress bandwidth is the same as the ingress bandwidth. See section Ingress Bandwidth Control above for details.



4.8.4.4 Egress Queue Bandwidth Control

Egress shaping per queue limits the transmission rate of selected outgoing frames on a per queue, per port basis. To do this, the switch shapes, or limits the output load. This does not include management frames, so they do not count towards the rate limit. Egress queue bandwidth control is used to help prevent congestion for your ISP (Internet Service Provider).



Parameter	Description
Burst Size	The maximum size permitted for bursts of data. Burst sizes are measured in bytes. We recommend this formula for calculating the correct burst size: Burst size = bandwidth x allowable time for burst traffic / 8.
Port	Ports 1 to 10.
Queue	Select the queue from 1 to 8.
State	Disable or enable the ingress bandwidth control.
CIR (kbps)	The committed information rate in kilobits per second.

4.8.5 Voice VLAN

4.8.5.1 What is Voice VLAN?

Voice VLAN is specially configured for user voice data traffic. By setting a Voice VLAN and adding the ports of the connected voice device to Voice VLAN, the user will be able to configure QoS (Quality of service) service for voice data, and improve voice data traffic transmission priority to ensure the calling quality. The Intellinet switch can judge if the data traffic is the voice data traffic from specified equipment according to the source MAC address field of the data packet entering the port. The packet with the source MAC address complying with the system defined voice equipment OUI (Organizationally Unique Identifier) will be considered the voice data traffic and transmitted to the Voice VLAN.

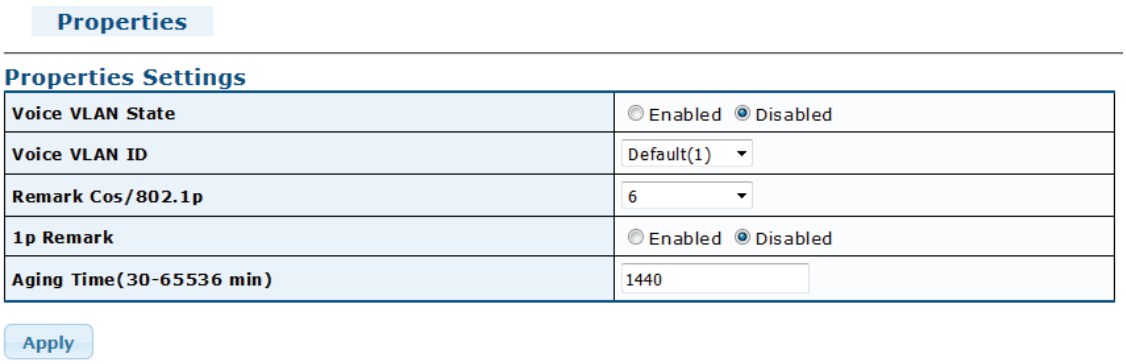
The configuration is based on MAC address, acquiring a mechanism in which every voice equipment transmitting information through the network has got its unique MAC address. VLAN will trace the address belongs to specified MAC. By This means, VLAN allows the voice equipment always belong to Voice VLAN when relocated physically. The greatest advantage of the VLAN is the equipment can be automatically placed into Voice VLAN according to its voice traffic which will be transmitted at specified priority. Meanwhile, when voice equipment is physically relocated, it still belongs to the Voice VLAN without any further configuration modification, which is because it is based on voice equipment other than switch port.

Note:

The Voice VLAN feature enables the voice traffic to forward on the Voice VLAN, and then the switch can be classified and scheduled to network traffic. It is recommended there are two VLANs on a port -- one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

4.8.5.2 Properties

The Voice VLAN feature enables voice traffic to forward on the Voice VLAN, and then the Intellinet switch can be classified and scheduled to network traffic. It is recommended that there are two VLANs on a port -- one for voice and one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly through its own GUI.



Object	Description
• **Voice VLAN State**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are: ■ **Enabled**: Enable Voice VLAN mode operation. ■ **Disabled**: Disable Voice VLAN mode operation
• **Voice VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID, etc. The allowed range is 1 to 4095.
• **Remark CoS/802.1p**	Select 802.1p value for this drop down list.
• **1p remark**	Enable or disable 802.1p remark.
• **Aging Time (30-65536 min)**	The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (\Default: **1440** minutes).

4.8.5.3 Telephony OUI MAC

Configure VOICE VLAN OUI table on this page.

Each IP phone manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is imbedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of an IP phone in the first three complete bytes of its MAC address. Typically, you will find that all of the IP phones you are installing have the same OUI in common.
The 8-Port Intellinet switch identifies a voice data packet by comparing the OUI information in the packet's source MAC address with an OUI table that you configure when you initially set up the voice VLAN. This is important when the Auto-Detection feature for a port and is a dynamic voice VLAN port.

When you are configuring the voice VLAN parameters, you must enter the complete MAC address of at least one of your IP phones. An "OUI Mask" is automatically generated and applied by the AT-S107 management software to yield the manufacturer's OUI. If the OUI of the remaining phones from that manufacturer is the same, then no other IP phone MAC addresses need to be entered into the configuration.
However, it is possible that you can find more than one OUI from the same manufacturer among the IP phones you are installing. It is also possible that your IP phones are from two or more different manufacturers in which case you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP phones being installed, then one MAC address representing each individual OUI must be configured in the voice VLAN. You can enter a total of 10 OUIs.

Telephony OUI MAC

Voice VLAN OUI MAC Setting

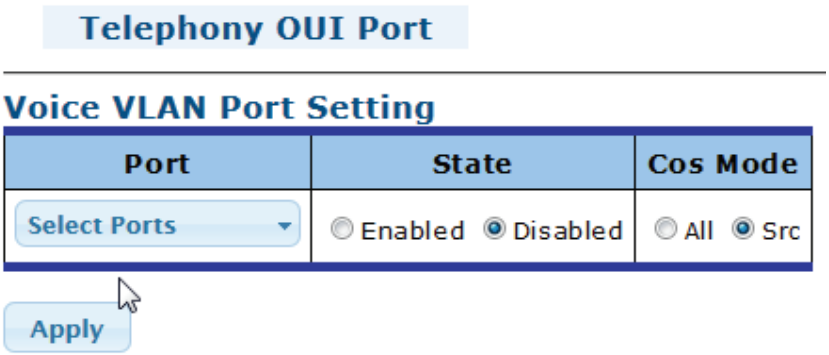
OUI Address	00:00:00
Description	

Add

Object	Description
• **OUI Address**	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx:xx:xx" (x is a hexadecimal digit).
• **Description**	User-defined text that identifies the VoIP devices.

Object	Description
• **OUI Address**	Display the current OUI address
• **Description**	Display the current description
• **Modify**	Click Edit to edit voice VLAN OUI group parameter. Click Delete to delete voice VLAN OUI group parameter.

4.8.5.4 *Telephony OUI Port*

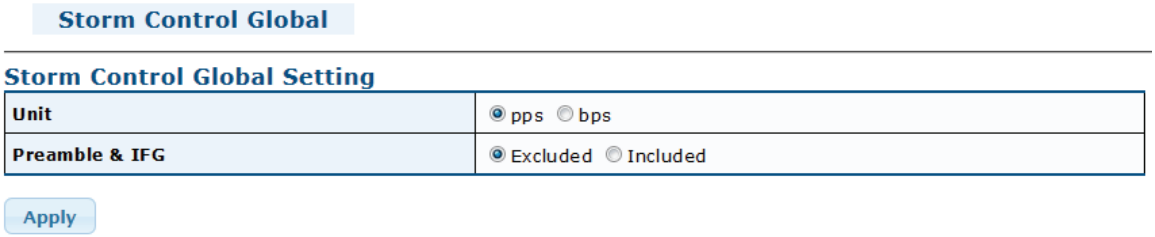


Object	Description
• **Port**	Select port number for this drop down list.
• **State**	Enable or disable the voice VLAN port setting. The default value is "Disabled".
• **CoS Mode**	Select the CoS mode that depend on all or sorce.

4.9 Security

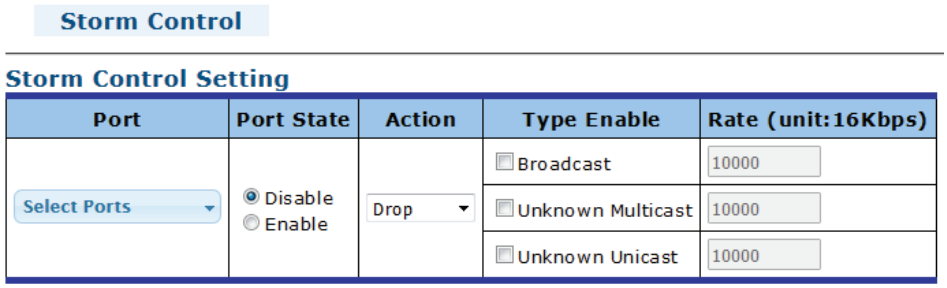
4.9.1 Storm Control

4.9.1.1 Global Settings



Object	Description
• **Unit**	Controls the unit of measure for the storm control rate as "pps" or "bps". The default value is "bps".
• **Preamble & IFG**	Set the excluded or included interframe gap

4.9.1.2 Port Settings



Object	Description
• **Port**	Select port for this drop down list.
• **Port State**	Enable or disable the storm control status for the given storm type.
• **Action**	Configures the action performed when storm control is over rate on a port. Valid values are **Shutdown** or **Drop**.
• **Type Enable**	The settings in a particular row apply to the frame type listed here: ■ **broadcast** ■ **unknown unicast** ■ **unknown multicast**
• **Rate (kbps/pps)**	Configure the rate for the storm control. The default value is "10,000".

4.9.2 802.1x

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- Remote Authentication Dial-in User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Local user name and Privilege Level control

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

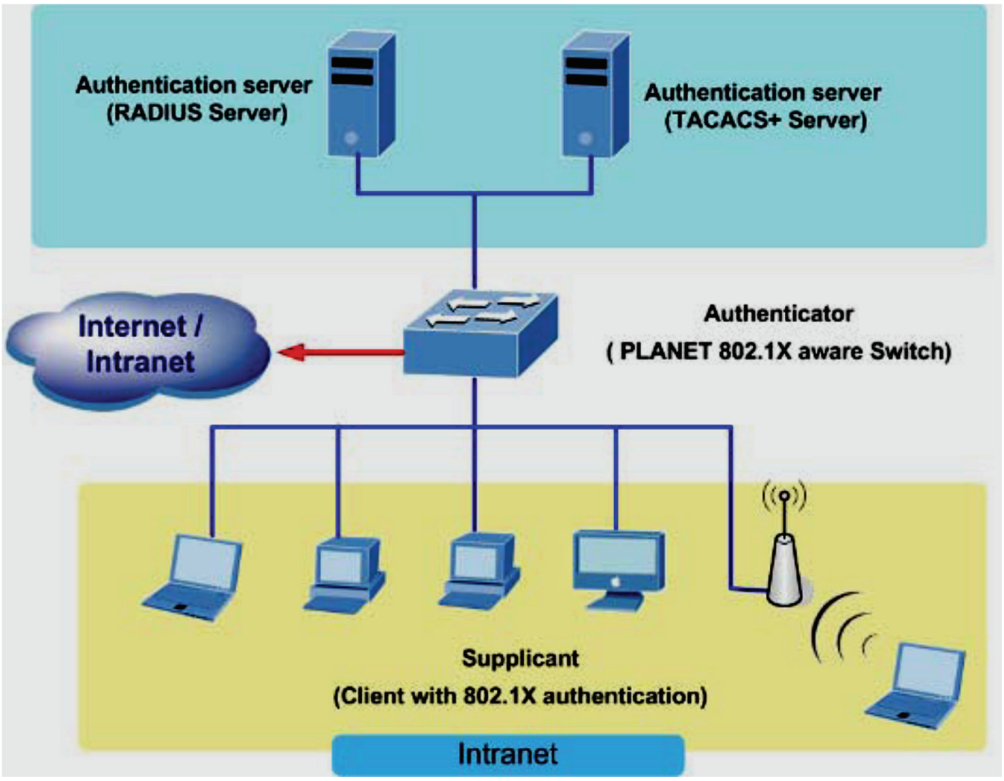
Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

- Device Roles:

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.



Client - the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the supplicant in the IEEE 802.1X specification.)

Authentication server—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

Switch (802.1X device)—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame

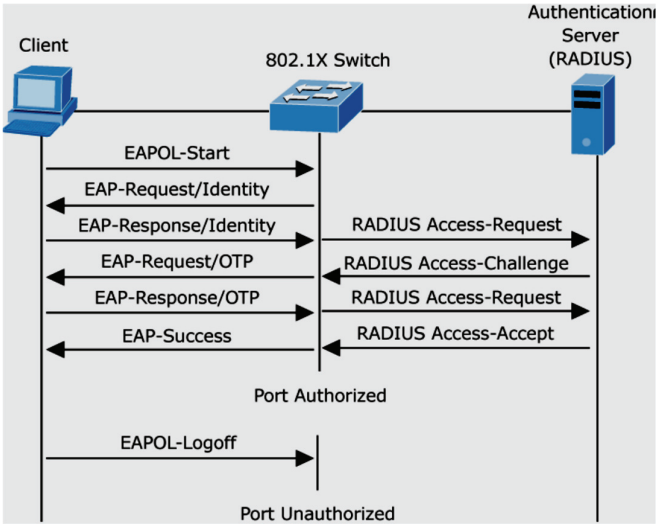
is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

- Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the dot1x port-control auto interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame. However, if during boot-up, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

Note:
If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. The specific exchange of EAP frames depends on the authentication method being used. The picture below shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.



- Ports in Authorized and Unauthorized States

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

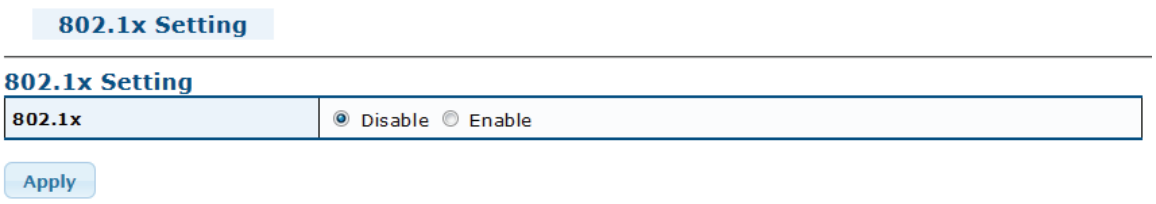
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted. When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.9.2.1 802.1x Setting

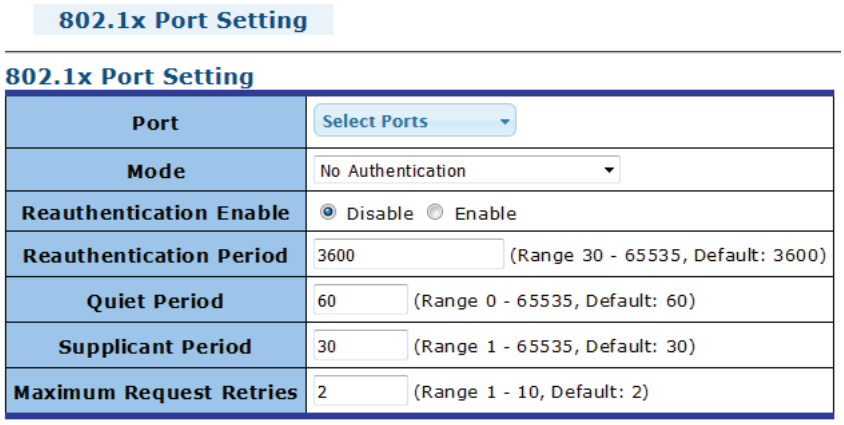
This page allows you to configure the IEEE 802.1X authentication system. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Security→802.1X Access Control→802.1X Setting" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

Enable or disable 802.1x on the Intellinet switch.



4.9.2.2 802.1x Port Setting

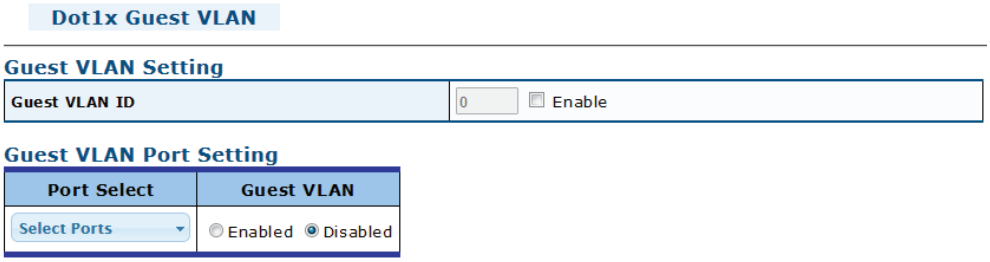
On this interface screen you can define the QoS trust mode.



Object	Description
• **Port**	Select port for this drop down list.
• **Mode**	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: ■ **No Authentication** ■ **Authentication** ■ **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. ■ **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
• **Reauthentication Enable**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 30 to 65535 seconds.
• **Quiet Period**	Sets time to keep silent on supplicant authentication failure.
• **Supplicant Period**	Sets the interval for the supplicant to re-transmit EAP request/identify frame.
• **Maximun Request Retries**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

4.9.2.3 Guest VLAN Settings

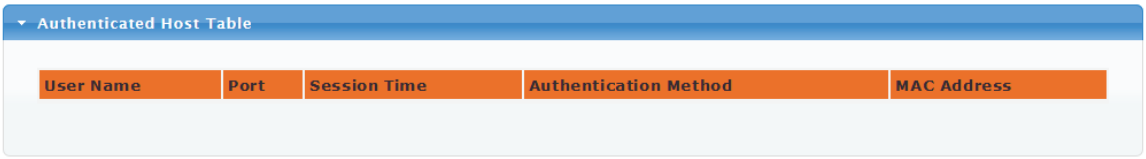
When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.



Object	Description
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1~4094].
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. ■ When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. ■ When unchecked, the ability to move to the Guest VLAN is disabled for all ports.

4.9.2.4 Authenticated Hosts

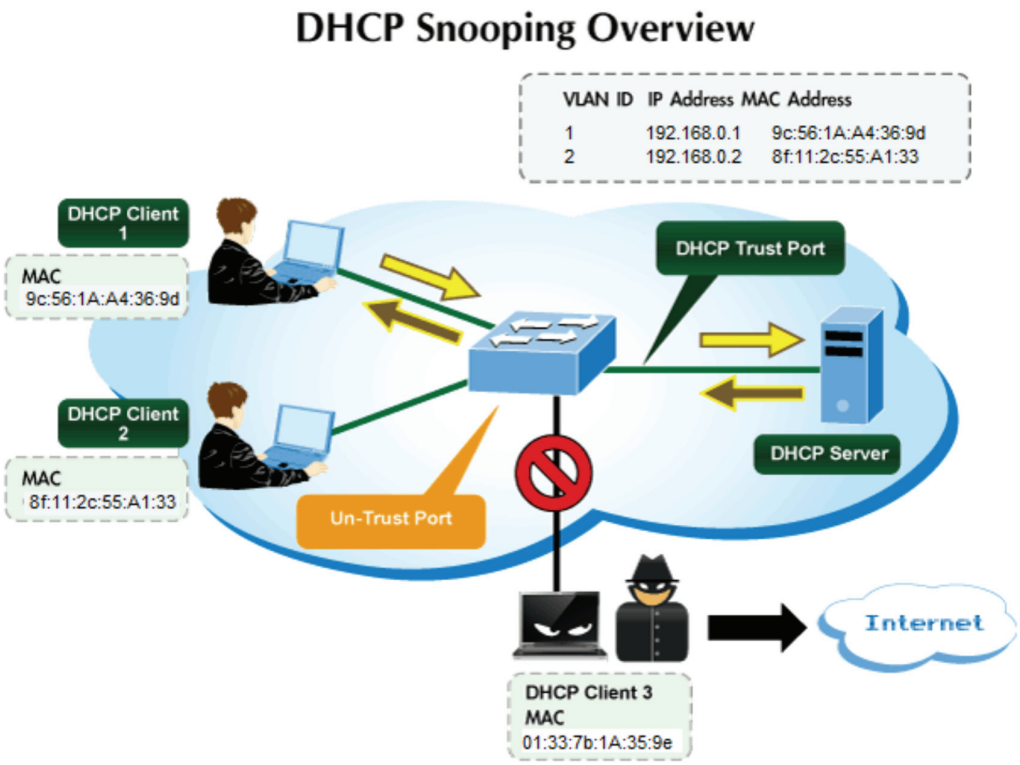
See all currently authenticated hosts on this information screen.



Object	Description
• **User Name**	Display the current user name.
• **Port**	Display the current port number.
• **Session Time**	Display the current session time.
• **Authentication Method**	Display the current authentication method.
• **MAC Address**	Display the current MAC address.

4.9.3 DHCP Snooping

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.



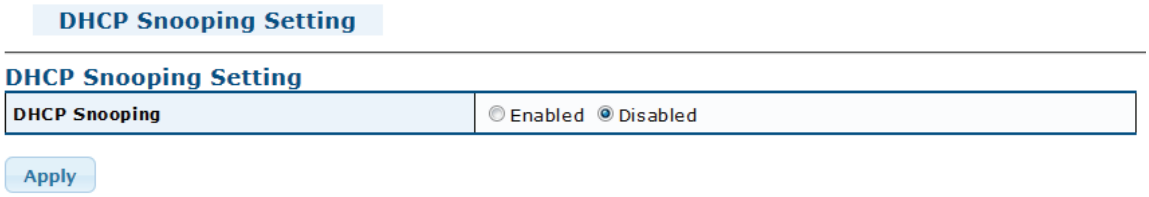
Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Filtering rules are implemented as follows:
  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
    - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
    - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
    - If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
  - Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives

4.9.3.1 DHCP Snooping Settings

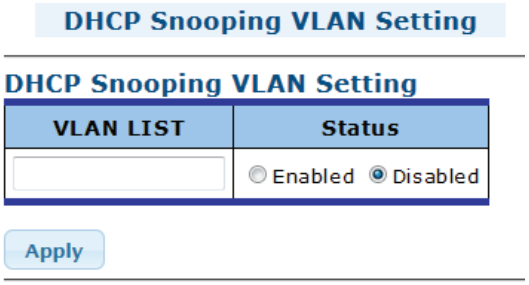
Activate or deactivate DHCP snooping on this configuration screen.



4.9.3.2 LAN Settings

Command Usage

- When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.



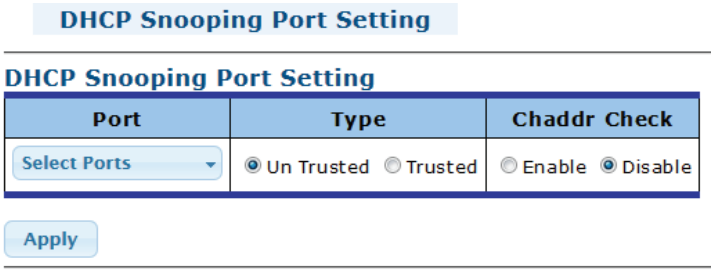
Object	Description
• **VLAN List**	Indicates the ID of this particular VLAN.
• **Status**	Indicates the DHCP snooping mode operation. Possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.

4.9.3.3 DHCP Snooping Port Settings

Configures switch ports as trusted or untrusted.

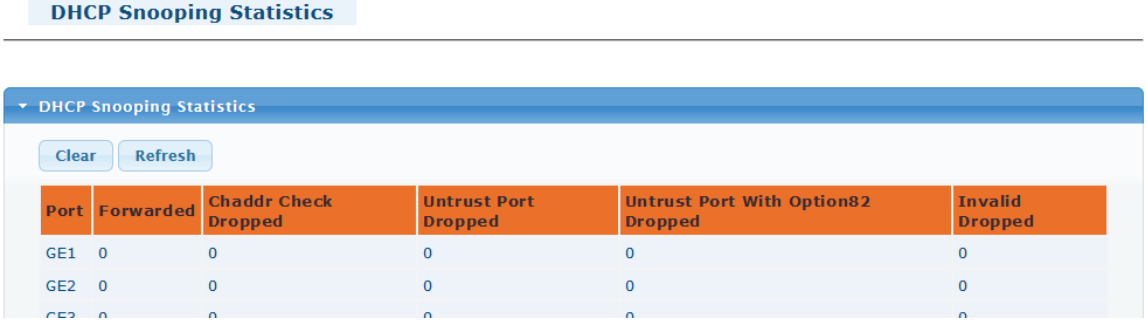
Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
- When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or firewall to trusted state. Set all other ports outside the local network or firewall to untrusted state.



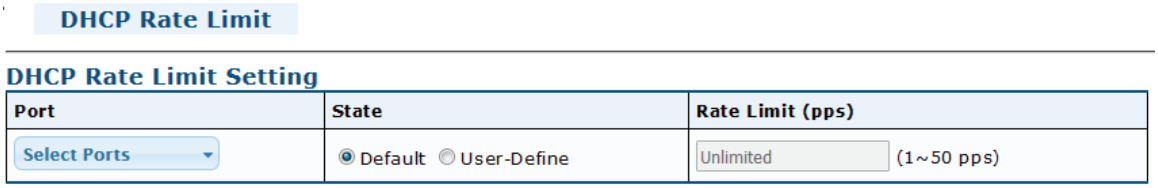
Object	Description
• **Port**	Select port for this drop down list.
• **Type**	Indicates the DHCP snooping port mode. Possible port modes are: ■ **Trusted**: Configures the port as trusted sources of the DHCP message. ■ **Untrusted**: Configures the port as untrusted sources of the DHCP message.
• **Chaddr Check**	Indicates that the Chaddr check function is enabled on selected port. Chaddr: Client hardware address.

4.9.3.4 DHCP Snooping Statistics



4.9.3.5 Rate Limit

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission.



Object	Description
• **Port**	Select port for this drop down list.
• **State**	Set default or user-define.
• **Rate Limit (pps)**	Configure the rate limit for the port policer. The default value is "unlimited". Valid values are in the range 1 to 300.

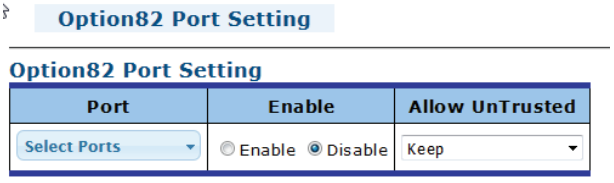
4.9.3.6 Option82 Global Settings

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to DHCP servers. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

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)
- 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 switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.



Object	Description
• **State**	Set the option2 (remote ID option) content of option 82 added by DHCP request packets. ■ **Default** means the default VLAN MAC format. ■ **User-Define** means the remote-id content of option 82 specified by users

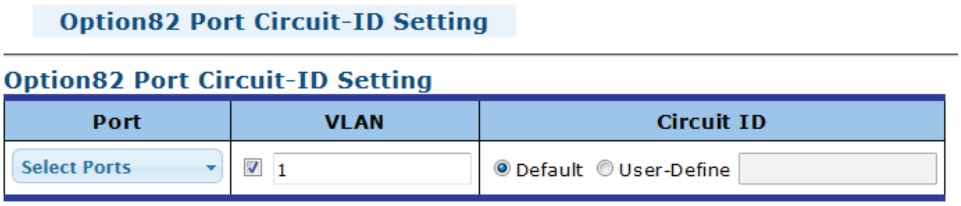
4.9.3.7 Option82 Port Settings

This function is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process.

Object	Description
• **Port**	Select port for this drop down list.
• **Enable**	Enable or disable option82 function on port.
• **Allow Untrusted**	Select modes for this drop down list. The following modes are available: ■ **Drop** ■ **Keep** ■ **Replace**

4.9.3.8 Option82 Circuit-ID Settings

Set creation method for option82, users can define the parameters of circute-id suboption by themselves.



Object	Description
• **Port**	Select port for this drop down list.
• **VLAN**	Indicates the ID of this particular VLAN.
• **Circuit ID**	Set the option1 (Circuit ID) content of option 82 added by DHCP request packets.

4.9.4 Dynamic ARP Inspection

4.9.4.1 Dynamic ARP Inspection Setting

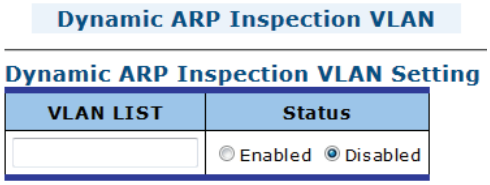
Dynamic ARP Inspection (DAI) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration.

On this configuration screen you activate and deactivate DAI.

Object	Description
• **DAI**	Enable the Global Dynamic ARP Inspection or disable the Global ARP Inspection.

4.9.4.2 VLAN Settings

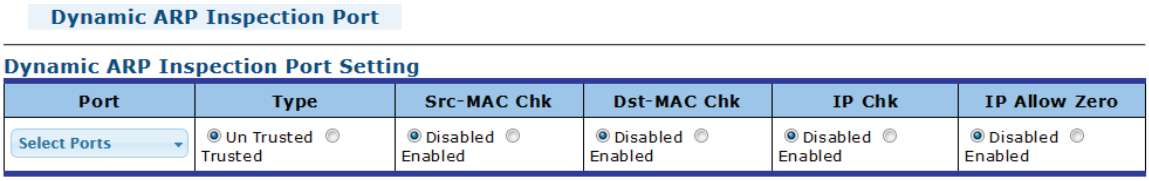
Enable or disable DAI for different VLAN IDs.



Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN.
Status	Enables Dynamic ARP Inspection on the specified VLAN Options: ■ **Enable** ■ **Disable**

4.9.5 Port Settings

DAI-related port settings.



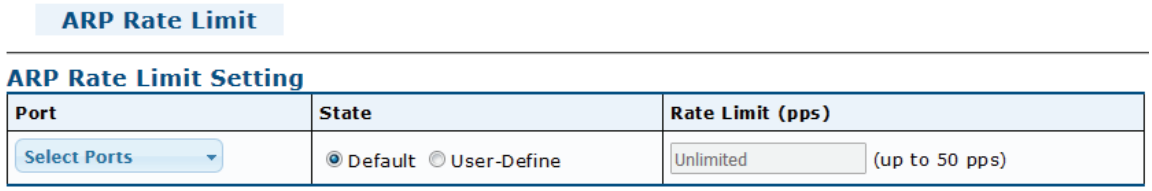
Object	Description
• **Port**	Select port for this drop down list.
• **Type**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Default: All interfaces are untrusted.
• **Src-Mac Chk**	Enable or disable to checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
• **Dst-Mac Chk**	Enable or disable to checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
• **IP Chk**	Enable or disable to checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.
• **IP Allow Zero**	Enable or disable to checks all-zero IP addresses.

4.9.6 Dynamic ARP Inspection Statistics

Provides statistical information about the DAI function.

4.9.6.1 *Rate Limit*

You can specify optional rate limits for each of the ports and LAGs here.



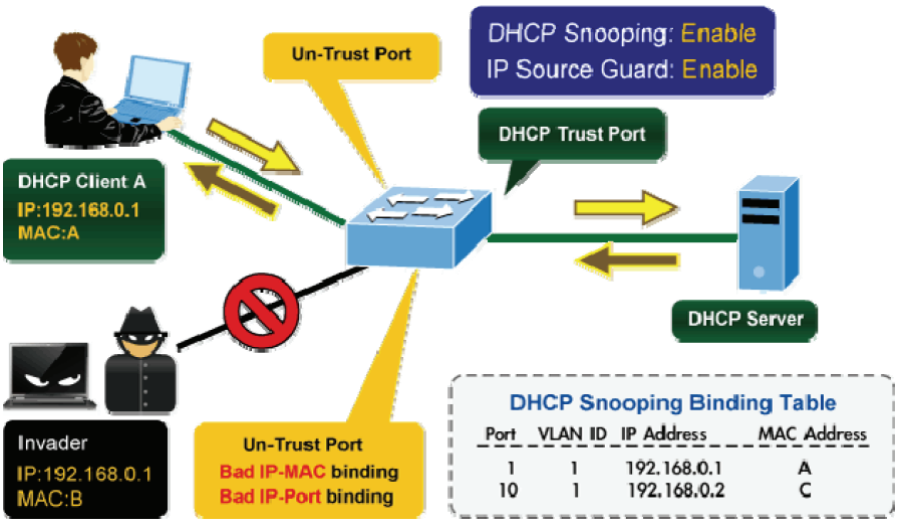
Object	Description
• **Port**	Select port for this drop down list.
• **State**	Set default or user-define.
• **Rate Limit (pps)**	Configure the rate limit for the port policer. The default value is "unlimited".

4.9.7 *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. After receiving a packet, the port looks up the key attributes (including IP address, MAC address and VLAN tag) of the packet in the binding entries of the IP source guard. If there is a matching entry, the port will forward the packet. Otherwise, the port will abandon the packet.

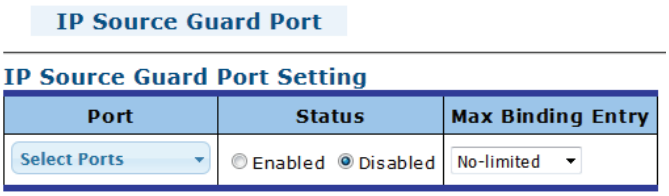
IP source guard filters packets based on the following types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry



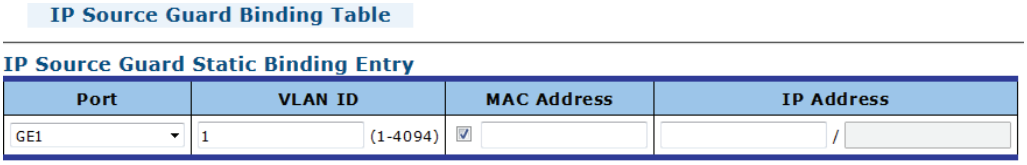
4.9.7.1 Port Settings

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.



Object	Description
• **Port**	Select port for this drop down list.
• **Status**	Enable or disable the IP source guard.
• **Verify Source**	Configures the switch to filter inbound traffic based IP address, or IP address and MAC address. ■ **None** Disables IP source guard filtering on the Managed Switch. ■ **IP** Enables traffic filtering based on IP addresses stored in the binding table. ■ **IP and MAC** Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.
• **Max Binding Entry**	The maximum number of IP source guard that can be secured on this port.

4.9.7.2 IP Source Guard Binding Table

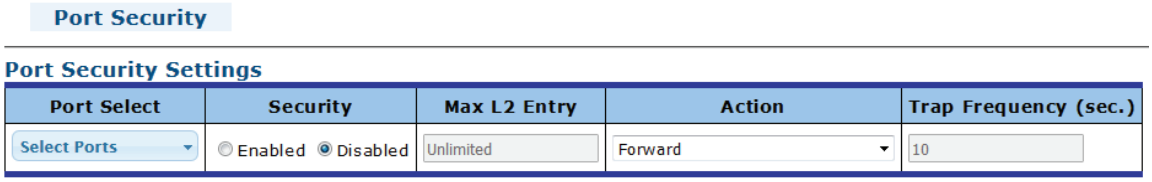


Object	Description
• **Port**	Select port for this drop down list.
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **MAC Address**	Source MAC address is allowed.
• **IP Address**	Source IP address is allowed.

4.9.7.3 Port Security

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of four different as described below.

The Limit Control module is one of a range of modules that utilizes a lower-layer module, the Port Security module, which manages MAC addresses learned on the port. The Limit Control configuration consists of two sections, a system- and a port-wide.

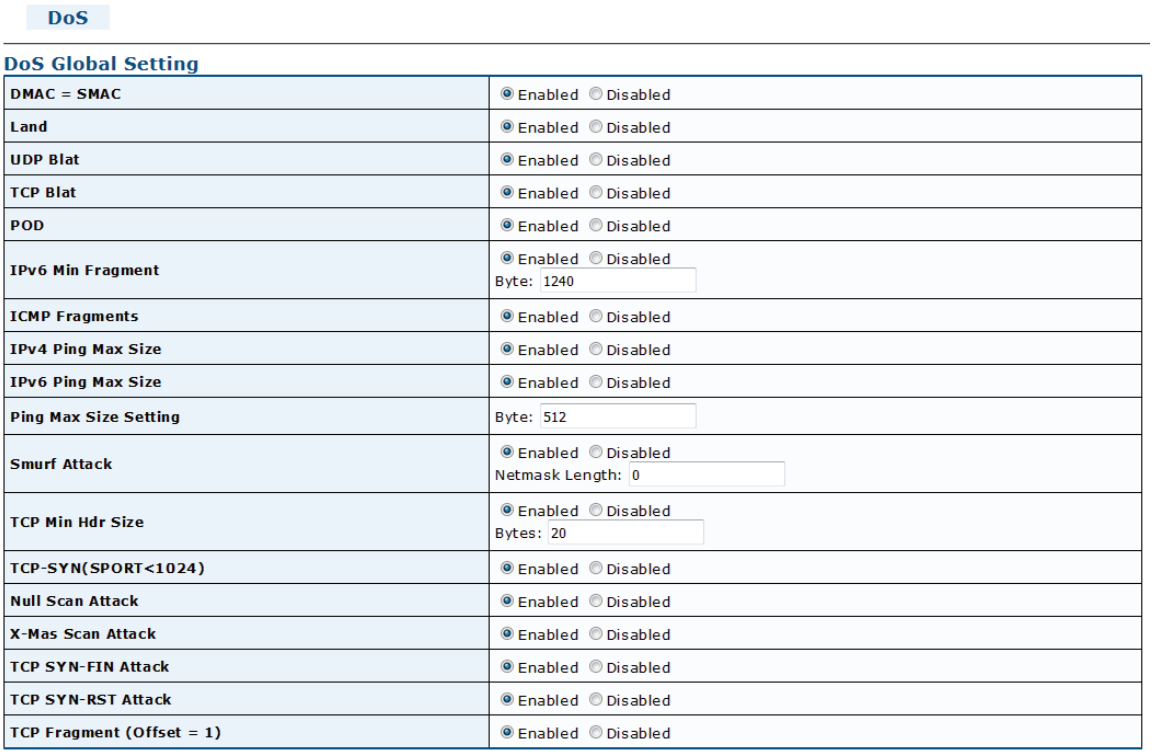


Object	Description
• **Port**	Select port for this drop down list.
• **Security**	Enable or disable the port security.
• **Mac L2 Entry**	The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **Action**	If Limit is reached, the switch can take one of the following actions: ■ **Forward**: Do not allow more than Limit MAC addresses on the port, but take no further action. ■ **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Disable and re-enable Limit Control on the port or the switch, 2) Click the Reopen button. ■ **Discard**: If Limit + 1 MAC addresses is seen on the port, it will trigger the action that do not learn the new MAC and drop the package.

4.9.8 DOS

The DoS is short for Denial of Service, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop processing the attacker's data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server. Security feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against Dos attacks while acting no influence on the linear forwarding performance of the switch.

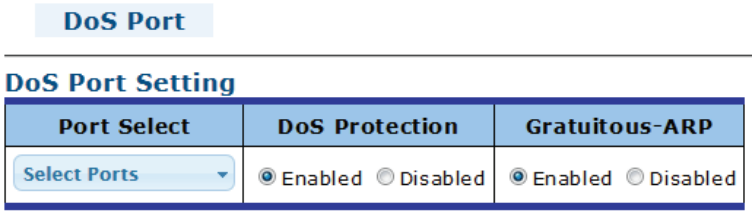
4.9.8.1 Global DoS Setting



Object	Description
• **DMAC = SMAC**	Enable or disable DoS check mode by DMAC = SMAC
• **Land**	Enable or disable DoS check mode by land
• **UDP Blat**	Enable or disable DoS check mode by UDP blat
• **TCP Blat**	Enable or disable DoS check mode by TCP blat
• **POD**	Enable or disable DoS check mode by POD

• **IPv6 Min Fragment**	Enable or disable DoS check mode by IPv6 min fragment
• **ICMP Fragments**	Enable or disable DoS check mode by ICMP fragment
• **IPv4 Ping Max Size**	Enable or disable DoS check mode by IPv4 ping max size
• **IPv6 Ping Max Size**	Enable or disable DoS check mode by IPv6 ping max size
• **Ping Max Size Setting**	Set the max size for ping
• **Smurf Attack**	Enable or disable DoS check mode by smurf attack
• **TCP Min Hdr Size**	Enable or disable DoS check mode by TCP min hdr size
• **TCP-SYN (SPORT < 1024)**	Enable or disable DoS check mode by TCP-syn (sport < 1024)
• **Null Scan Attack**	Enable or disable DoS check mode by null scan attack
• **X-Mas Scan Attack**	Enable or disable DoS check mode by x-mas scan attack
• **TCP SYN-FIN Attack**	Enable or disable DoS check mode by TCP syn-fin attack
• **TCP SYN-RST Attack**	Enable or disable DoS check mode by TCP syn-rst attack
• **TCP Fragment (Offset = 1)**	Enable or disable DoS check mode by TCP fragment (offset = 1)

4.9.8.2 DoS Port Setting



Object	Description
• **Port Select**	Select port for this drop down list.
• **DoS Protection**	Enable or disable per port DoS protection.

4.9.9 Authentication, authorization, and accounting (AAA)

Authentication, authorization, and accounting (AAA) provides a framework for configuring access control on the Managed Switch. The three security functions can be summarized as follows:

- Authentication — Identifies users that request access to the network.
- Authorization — Determines if users can access specific services.
- Accounting — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are then applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The Managed Switch supports the following AAA features:

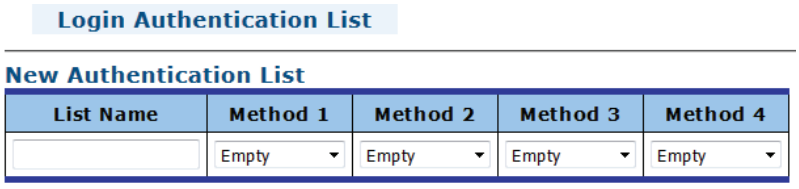
- Accounting for IEEE 802.1X authenticated users that access the network through the Managed Switch.
- Accounting for users that access management interfaces on the Managed Switch through the console and Telnet.
- Accounting for commands that users enter at specific CLI privilege levels. Authorization of users that access management interfaces on the Managed Switch through the console and Telnet.

To configure AAA on the Managed Switch, you need to follow this general process:

- Configure RADIUS and TACACS+ server access parameters. See “Configuring Local/Remote Logon Authentication”.
- Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
- Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use. Apply the method names to port or line interfaces.

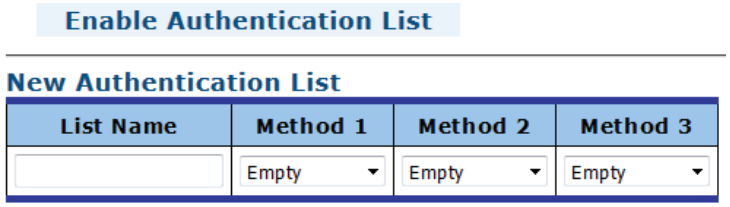
Note: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS or TACACS+ server software.

4.9.9.1.1 Login List



Object	Description
• List Name	Defines a name for the authentication list.
• Method 1-4	Set the login authentication method: Empty / None / Local / TACACS+ / RADIUS / Enable

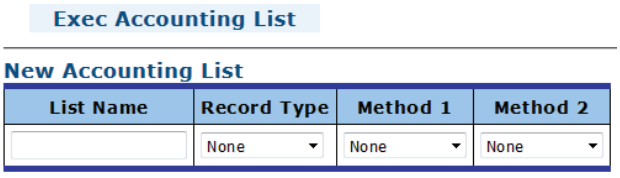
4.9.9.2 Enable List



Object	Description
• List Name	Defines a name for the authentication list.
• Method 1-3	Set the login authentication method: Empty / None / Enable / TACACS+ / RADIUS

4.9.9.3 Accounting List

This page allows the user to add, editor delete accounting list settings. The “default” list cannot be deleted.



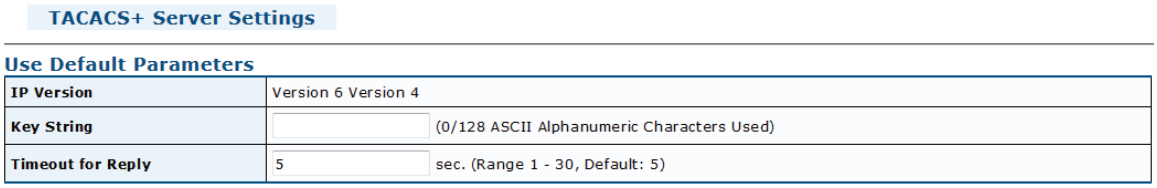
Parameter	Description
List Name	The account list name must be different from other list names, i.e., it must not be called “default”.
Record Type	▪ none: No accounting. ▪ start-stop: Record start and stop without waiting. ▪ stop-only: Record stop when service terminates.
Method 1	Select first priority: ▪ Tacacs+: Use remote TACACS+ server to accounting.

	▪ Radius: Use remote Radius server to accounting.
Method 2	Select second priority: ▪ Tacacs+: Use remote TACACS+ server to accounting. Radius: Use remote Radius server to accounting.

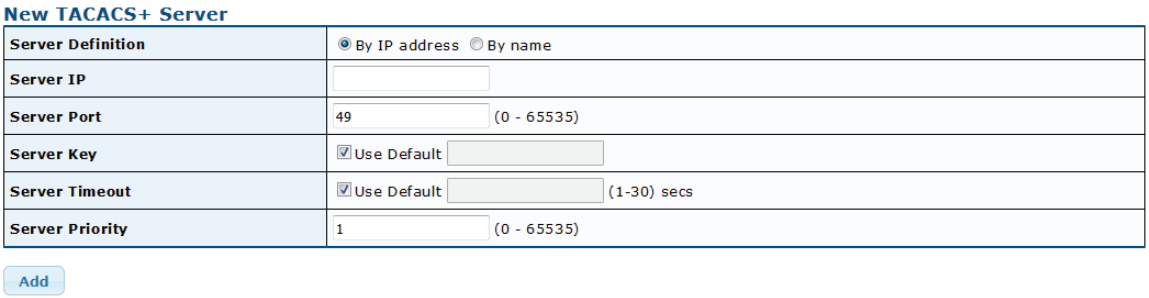
4.9.9.4 Accounting Update

4.9.10 TACACS+ server

TACACS (Terminal Access Controller Access Control System) is an older authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.



Object	Description
• **Key String**	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.
• **Timeout for Reply**	Retransmit is the number of times, in the range 1 to 30, a TACACS+ request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.



Object	Description
• **Server Definition**	Set the server definition.
• **Server IP**	Address of the TACACS+ server IP/name.
• **Server Port**	Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: **49**)
• **Server Key**	The key- shared between the TACACS+ Authentication Server and the switch.
• **Server Timeout**	The number of seconds the switch waits for a reply from the server before it resends the request.
• **Server Priority**	Set the server priority.

4.9.11 Radius server

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

Radius Server Settings

Use Default Parameters

IP Version	Version 6 Version 4
Retries	3 (Range 1 - 10, Default: 3)
Timeout for Reply	3 sec. (Range 1 - 30, Default: 3)
Dead Time	0 min. (Range 0 - 2000, Default: 0)
Key String	(0/128 ASCII Alphanumeric Characters Used)

Object	Description
• **Retries**	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from
	a RADIUS server before retransmitting the request.
• **Timeout for Reply**	Retransmit is the number of times, in the range 1 to 30, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Key String**	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

New Radius Server

Server Definition	◉ By IP address ○ By name
Server IP	
Authentication Port	1812 (0 - 65535)
Acct Port	1813 (0 - 65535)
Key String	☑ Use Default
Timeout for Reply	☑ Use Default (1-30) secs
Retries	☑ Use Default (1 - 10)
Server Priority	1 (0 - 65535)
Dead Time	0 (0 - 2000)
Usage Type	○ Login ○ 802.1x ◉ All

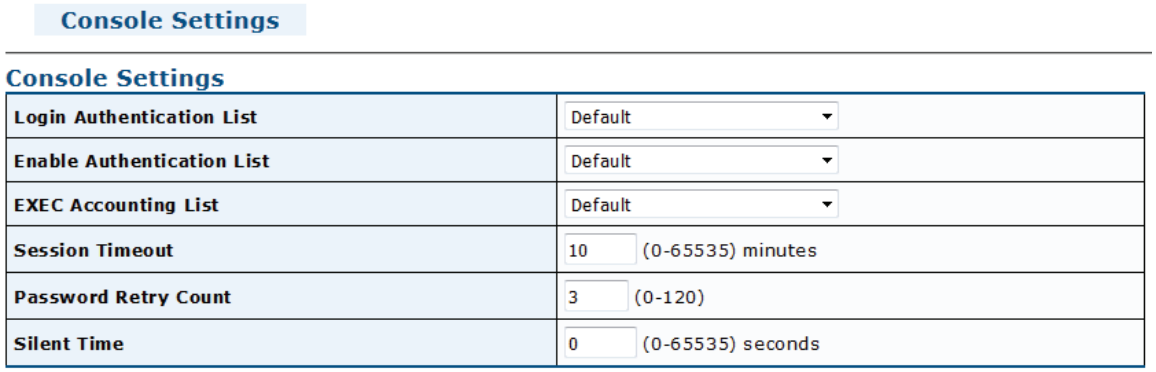
Add

Object	Description
• **Server Definition**	Set the server definition.
• **Server IP**	Address of the Radius server IP/name.
• **Authetication Port**	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
• **Acct Port**	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
• **Key String**	The shared key - shared between the RADIUS Authentication Server and the switch.
• **Timeout for Reply**	The Timeout, which can be set to a number between 1 and 30 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
• **Retries**	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request.
• **Server Priority**	Set the server priority.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Usage Type**	Set the usage type. The following modes are available: ■ **Login** ■ **802.1X** ■ **All**

4.9.12 Access

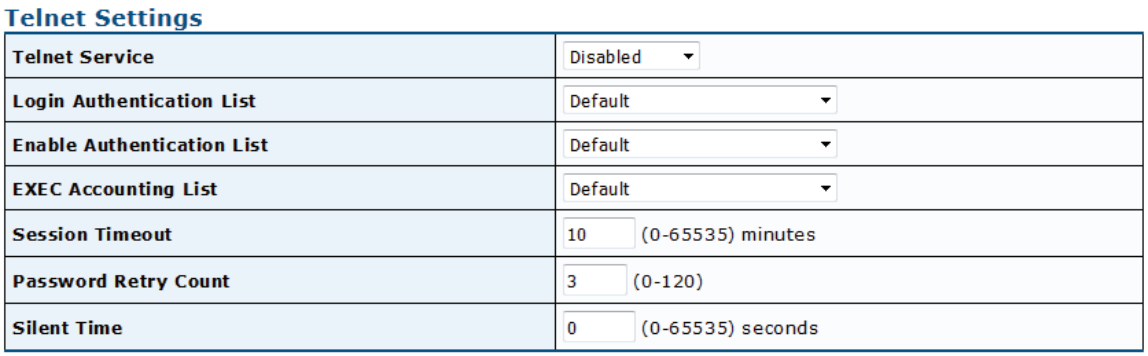
The Intellinet switch allows access via HTTP(S), Telnet and console port. In this section you define the authentication and accounting related settings.

4.9.12.1 Console Settings



Parameter	Description
Login/Enable/Exec List	Select the appropriate list value for each of these entries.
Session Timeout	Specify the length of inactivity in minutes after which the session is automatically terminated.
Password Retry Count	Enter the number of failed login attempts before the silent time is invoked.
Silent Time	Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-retry count.

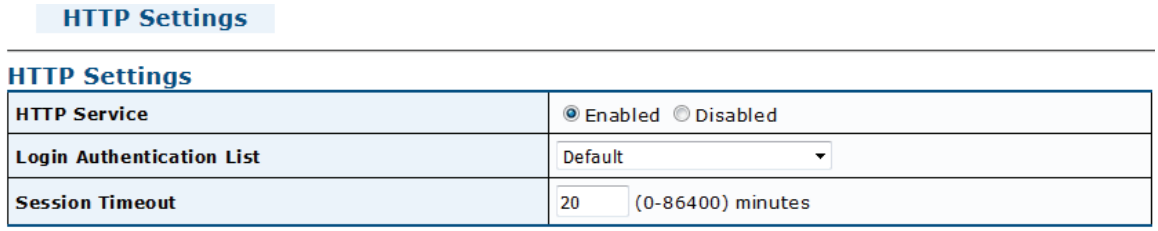
4.9.12.2 Telnet Settings



Very much the same as the console settings, however you can disable or enable the service. All other parameters are identical.

4.9.12.3 HTTP Settings

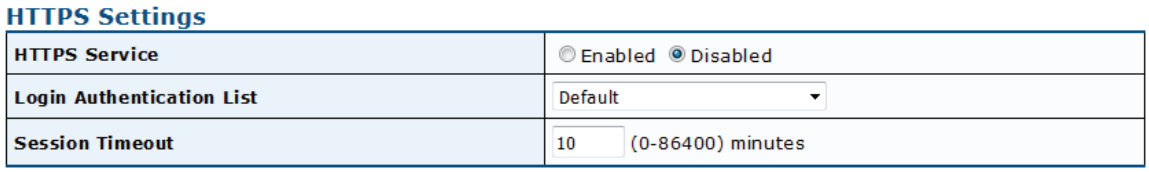
In addition to Telnet and console-based access, the most common method of connecting to the Intellinet 8-Port Gigabit PoE+ Switch is via HTTP (web browser).



Parameter	Description
HTTP Service	Enable or disable access via HTTP..
Login Authentication List	Specify the appropriate value from the drop-down list.
Session Timeout	Specify the length of inactivity in minutes after which the session is automatically terminated.

4.9.12.4 HTTPS Settings

As a variation of HTTP, this access method is more secure by encryption.



The parameters are identical to those of HTTP.

4.10 Access Control List

4.10.1 What is ACL?

ACL is an acronym for Access Control List. 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.

ACE is an acronym for Access Control Entry. 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.

4.10.2 MAC-Based ACL

Create a MAC address based Access Control List on this screen. Type in the name for the ACL and click "Add."

MAC-Based ACL

ACL Name	

Add

4.10.3 MAC-Based ACE

On this page you can define the access control entries.

MAC-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	Permit Deny
DA MAC	Any User Defined
DA MAC Value	
DA MAC Mask	(0s for matching, 1s for no matching)

SA MAC	◉ Any ○ User Defined
SA MAC Value	
SA MAC Mask	(0s for matching, 1s for no matching)
VLAN ID	(Range:1 - 4094)
802.1p	☐ Include
802.1p Value	(Range:0-7)
802.1p Mask	
Ethertype(Range:0x05DD-0xFFFF)	(Range:0x05DD-0xFFFF)

Object	Description
• **ACL Name**	Select ACL name for this drop down list.
• **Sepuence**	Set the ACL sequence.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped. ■ **Shutdown**: Port shutdown is disabled for the ACE..
• **DA MAC**	Specify the destination MAC filter for this ACE. ■ **Any**: No DA MAC filter is specified. ■ **User Defined**: If you want to filter a specific destination MAC address with
	this ACE, choose this value. A field for entering a DA MAC value appears.
• **DA MAC Value**	When "User Defined" is selected for the DA MAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DA MAC value.
• **DA MAC Mask**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ 0: ARP frames where SHA is not equal to the DA MAC address. ■ 1: ARP frames where SHA is equal to the DA MAC address.
• **SA MAC**	Specify the source MAC filter for this ACE. ■ **Any**: No SA MAC filter is specified. ■ **User Defined**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a SA MAC value appears.
• **SA MAC Value**	When "User Defined" is selected for the SA MAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SA MAC value.

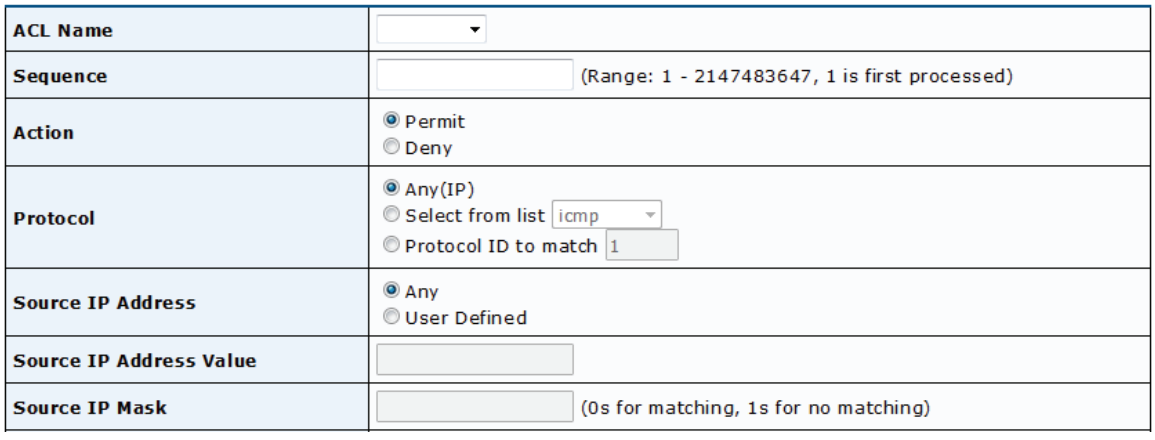
• **SA MAC Mask**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ **0**: ARP frames where SHA is not equal to the SA MAC address. ■ **1**: ARP frames where SHA is equal to the SA MAC address.
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **802.1p**	Include or exclude the 802.1p value
• **802.1p Value**	Set the 802.1p value.
• **802.1p Mask**	■ **0**: where frame is not equal to the 802.1p value. ■ **1**: where frame is equal to the 802.1p value.
• **Ethertype (Range:0x05DD – 0xFFFF)**	You can enter a specific EtherType value. The allowed range is **0x05DD** to **0xFFFF**. A frame that hits this ACE matches this EtherType value.

4.10.4 IPv4-Based ACL

Create a IPv4 address based Access Control List on this screen. Type in the name for the ACL and click "Add."

4.10.5 IPv4-Based ACE

On this page you can define the access control entries for IPv4.



Destination IP Address	◉ Any ○ User Defined
Destination IP Address Value	
Destination IP Mask	(0s for matching, 1s for no matching)
Source Port	◉ Any ○ Single 0 (Range: 0 - 65535) ○ Range 0 - 65535 (Range: 0 - 65535)
Destination Port	◉ Any ○ Single(Range: 0 - 65535) 0 (Range: 0 - 65535) ○ Range(Range: 0 - 65535) 0 - 65535 (Range: 0 - 65535)
TCP Flags	Urg ◉ Set ○ Unset ○ Don't Care Ack ◉ Set ○ Unset ○ Don't Care Psh ◉ Set ○ Unset ○ Don't Care Rst ◉ Set ○ Unset ○ Don't Care Syn ◉ Set ○ Unset ○ Don't Care Fin ◉ Set ○ Unset ○ Don't Care
Type of Service	◉ Any ○ DSCP to match 0 (Range: 0 - 63) ○ IP Precedence to match 0 (Range: 0 - 7)
ICMP	◉ Any ○ Select from list Echo Rep ○ Protocol ID to match 0 (Range: 0 - 255)
ICMP Code	◉ Any ○ User Defined 0 (Range: 0 - 255)

Object	Description
• **ACL Name**	Select ACL name for this drop down list.
• **Sepuence**	Set the ACL sequence.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped. ■ **Shutdown**: Port shutdown is disabled for the ACE..
• **Protocol**	Specify the protocol filter for this ACE. ■ **Any(IP)**: No protocol filter is specified. ■ **Select from list**: If you want to filter a specific protocol with this ACE, choose this value and select protocol for this drop down list. ■ **Protocol ID to match**: I If you want to filter a specific protocol with this ACE, choose this value and set currect protocol ID.

• **Source IP Address**	Specify the Source IP address filter for this ACE. ■ **Any**: No source IP address filter is specified. ■ **User Defined**: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Source IP Address Value**	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this source IP address value.
• **Source IP Wildcard Mask**	When "User Defined" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• **Destination IP Address**	Specify the Destination IP address filter for this ACE. ■ **Any**: No destination IP address filter is specified. ■ **User Defined**: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Destination IP Address Value**	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this destination IP address value.
• **Destination IP Wildcard Mask**	When "User Defined" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
• **Source Port**	Specify the source port for this ACE. ■ **Any**: No specifc source port is specified (source port status is "don't-care"). ■ **Single**: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is `0` to `65535`. A frame that hits this ACE matches this source port value. ■ **Range**: If you want to filter a specific source port range filter with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is `0` to `65535`. A frame that hits this ACE matches this source port value.
• **Destination Port**	Specify the destination port for this ACE. ■ **Any**: No specifc destination port is specified (destination port status is "don't-care"). ■ **Single**: If you want to filter a specific destination port with this ACE, you can enter a specific destiantino port value. A field for entering a destiantino port value appears. The allowed range is `0` to `65535`. A frame that hits this ACE matches this destination port value. ■ **Range**: If you want to filter a specific destiantion port range filter with this ACE, you can enter a specific destiantion port range value. A field for entering a destination port value appears.

• **TCP Flags**	UGR	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. ■ **Set**: TCP frames where the URG field is set must be able to match this entry. ■ **Unset**: TCP frames where the URG field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. ■ **Set**: TCP frames where the ACK field is set must be able to match this entry. ■ **Unset**: TCP frames where the ACK field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	PSH	Specify the TCP "Push Function" (PSH) value for this ACE. ■ **Set**: TCP frames where the PSH field is set must be able to match this entry. ■ **Unset**: TCP frames where the PSH field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	RST	■ Specify the TCP "Reset the connection" (RST) value for this ACE. **Set**: TCP frames where the RST field is set must be able to match this entry. ■ **Unset**: TCP frames where the RST field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. ■ **Set**: TCP frames where the SYN field is set must be able to match this entry. ■ **Unset**: TCP frames where the SYN field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. ■ **Set**: TCP frames where the FIN field is set must be able to match this entry. ■ **Unset**: TCP frames where the FIN field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").

• **Type of Service**	Specify the type pf service for this ACE. ■ **Any**: No specifc type of service is specified (destination port status is "don't-care"). ■ **DSCP**: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is 0 to 63. A frame that hits this ACE matches this DSCP value.
	■ **IP Recedence**: If you want to filter a specific IP recedence with this ACE, you can enter a specific IP recedence value. A field for entering an IP recedence value appears. The allowed range is 0 to 7. A frame that hits this ACE matches this IP recedence value.
• **ICMP**	Specify the ICMP for this ACE. ■ **Any**: No specifc ICMP is specified (destination port status is "don't-care"). ■ **List**: If you want to filter a specific list with this ACE, you can select a specific list value. ■ **Protocol ID**: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this protocol ID value.
• **ICMP Code**	Specify the ICMP code filter for this ACE. ■ **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ **User Defined**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

4.10.6 IPv6-Based ACL

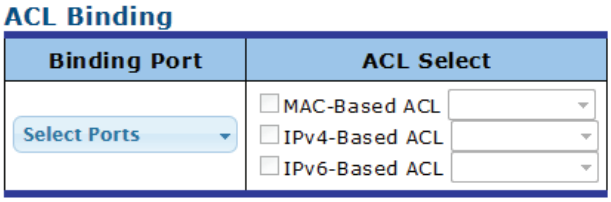
Create an IPv6 address based ACL.

4.10.7 IPv6-Based ACE

Very similar to IPv4-Based ACE (see above) with much of the same parameters.

4.10.8 ACL Binding

Use this configuration page in order to link (or bind) the physical ports or LAGs to an ACL.



Object	Description
• **Bibding Port**	Select port for this drop down list.
• **ACL Select**	Select ACL list for this drop down list.

4.11 MAC Address Table

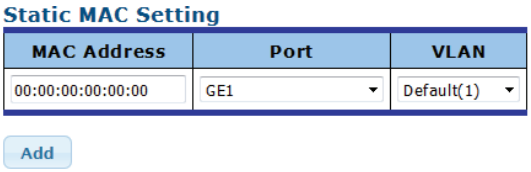
4.11.1 What is a MAC Address Table?

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Layer 2 Ethernet switches, such as the Intellinet 8-Port PoE+ Gigabit switch use these MAC addresses to route the packets from source to destination. The switch builds up a table over time, in which it stores pairings of MAC addresses and physical ports. Whenever a packet has to be delivered and the destination MAC address isn't in the MAC address table, the switch is forced to send out the data packet to all ports, just like an old Ethernet hub would do, and that floods the network with unnecessary traffic. However, once the switch has learnt the port at which the destination client is connected to, it will add this information to its MAC address table, and future deliveries for that MAC address will proceed much more efficiently.

MAC addresses can be stored permanently (static) or temporarily (dynamic).

4.11.2 Static MAC Settings

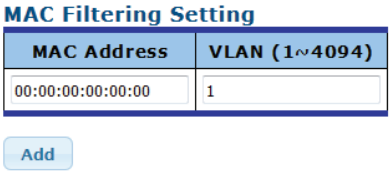
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add/ modify/delete a static MAC address. Additionally, binding a MAC address to a specific port can help protect against spoofing attacks.



Parameter	Description
MAC Address	Physical address of a network client.
Port	Specify the port at which the network client is connected to.
VLAN	If the client is part of a VLAN, define it here accordingly.

4.11.3 MAC Filtering

The switch can filter out (reject) traffic from pre-configured MAC address to increase security.



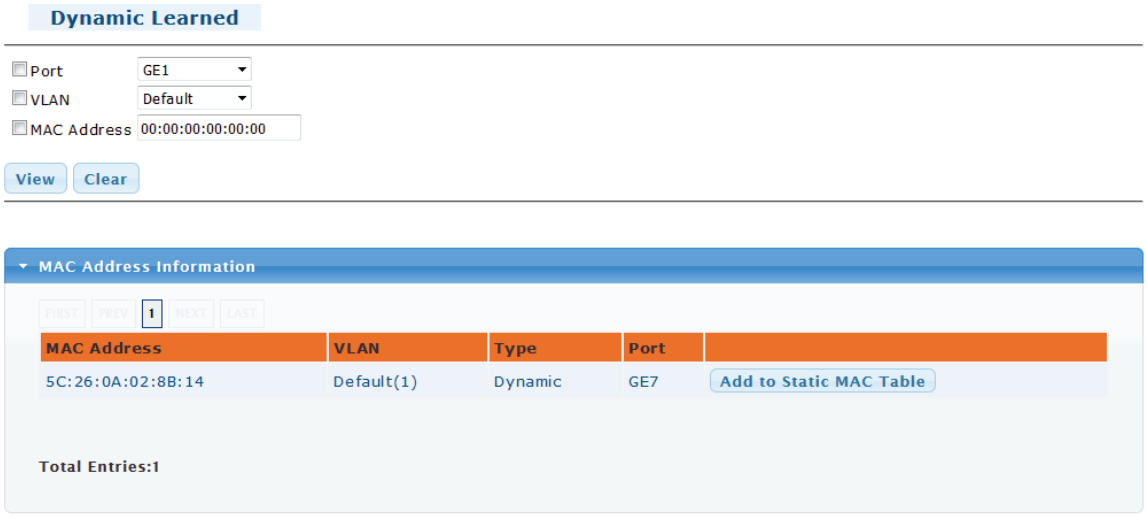
Object	Description
• **MAC Address**	Physical address associated with this interface.
• **VLAN (1~4096)**	Indicates the ID of this particular VLAN.

4.11.4 Dynamic Address Setting

On this screen you define how long MAC address – port pairings are kept in the MAC address table. This is called aging time. The default value is 300 seconds, but may increase this value up to 630 seconds.

4.11.5 Dynamically Learned

This screen shows all MAC addresses that are currently stored in the MAC address table.



In the upper section of the interface you can find tools that help you narrow down the traffic. You can filter by port, VLAN or part of a MAC address.

The table below shows AC addresses currently in the MAC address table. By default the screen shows all MAC addresses, but if you have specified some filters in the upper section, the results will be narrowed down accordingly.

To add a MAC address to the MAC address table permanently, simply click the “Add to Static MAC Table” button.

4.12 Link Layer Discovery Protocol (LLDP)

4.12.1 What is LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.12.2 LLDP Global Setting

This Page allows the user to inspect and configure the current LLDP port settings.

LLDP Global Settings

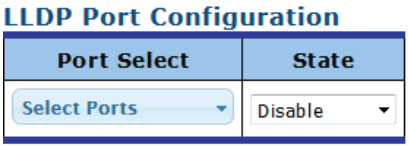
Enabled	○ Enabled ◉ Disabled
LLDP PDU Disable Action	○ Filtering ○ Bridging ◉ Flooding
Transmission Interval	30 (5-32768)
Check-Change Interval	4 (2-10)
Reinitialization Delay	2 (1-10)
Transmit Delay	2 (1-8192)
LLDP-MED Fast Start Repeat Count	3 (1-10)

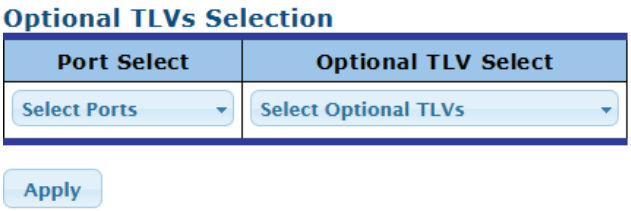
Object	Description
• **Enable**	Globally enable or disable LLDP function
• **LLDP PDU Disable Action**	Set LLDP PDU disable action: include “Filtering”, “Bridging” and “Flooding”. ■ **Filtering**: discrad all LLDP PDU. ■ **Bridging**: transmit LLDP PDU in the same VLAN. ■ **Flooding**: transmit LLDP PDU for all port.
• **Transmission Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Transmission Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)

• **Holdtime Multiplier**	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 **Holdtime** multiplied by **Transmission Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Reinitialization Delay**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
• **Transmit 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 **Transmit Delay** seconds. **Transmit Delay** cannot be larger than 1/4 of the **Transmission Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **LLDP-MED Fast Start Repeat Count**	Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanisim. Range: 1-10 packets; Default: **3** packets The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

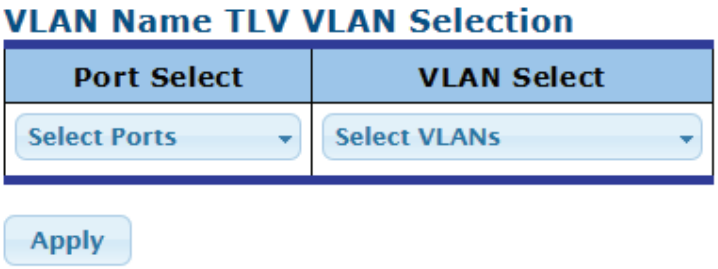
4.12.3 LLDP Port Settings

Use the LLDP Port Setting to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received.





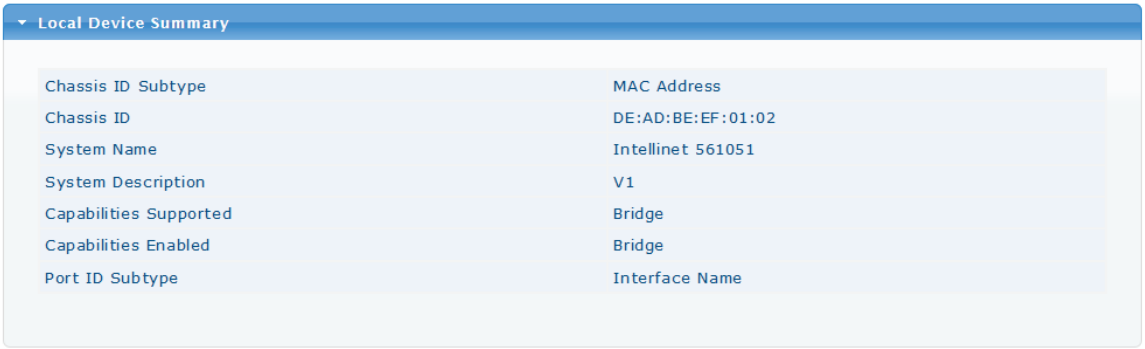
Object	Description
• **Port Select**	Select port for this drop down list.
• **State**	Enables LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options: ■ **Tx only**
	■ **Rx only** ■ **TxRx** ■ **Disabled**
• **Port Select**	Select port for this drop down list.
• **Optional TLV Select**	Configures the information included in the TLV field of advertised messages. ■ **System Name**: When checked the "System Name" is included in LLDP information transmitted. ■ **Port Description**: When checked the "Port Description" is included in LLDP information transmitted. ■ **System Description**: When checked the "System Description" is included in LLDP information transmitted. ■ **System Capability**: When checked the "System Capability" is included in LLDP information transmitted. ■ **802.3 MAC-PHY**: When checked the "802.3 MAC-PHY" is included in LLDP information transmitted. ■ **802.3 Link Aggregation**: When checked the "802.3 Link Aggregation" is included in LLDP information transmitted. ■ **802.3 Maximun Frame Size**: When checked the "802.3 Maximun Frame Size" is included in LLDP information transmitted. ■ **Management Address**: When checked the "Management Address" is included in LLDP information transmitted. ■ **802.1 PVID**: When checked the "802.1 PVID" is included in LLDP information transmitted.



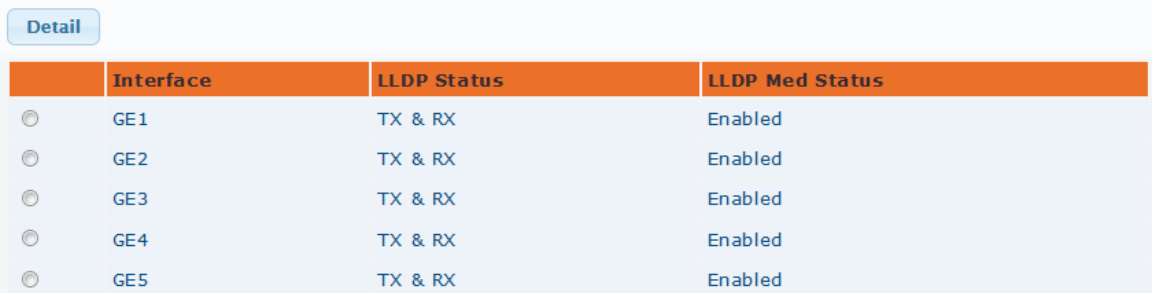
Object	Description
• **Port Select**	Select port for this drop down list.
• **VLAN Select**	Select VLAN for this drop down list.

4.12.4 LLDP Local Device

Use the LLDP Local Device Information screen to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

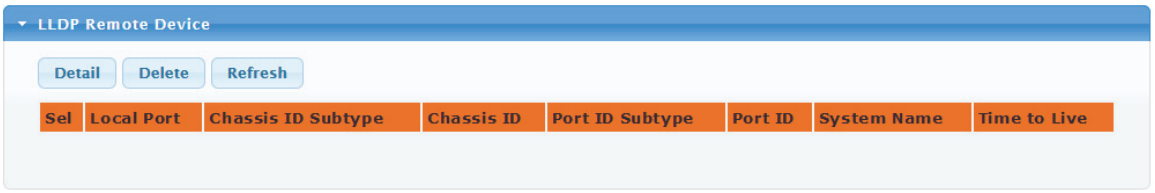


The screen also display LLDP status information of each port. Clicking the “Detail” button opens up a page that presents the information in much greater detail.



4.12.5 LLDP Remove Device

This page provides a status overview for all LLDP remote devices. The displayed table contains a row for each port on which an LLDP neighbor is detected.



4.12.6 LLDP MED Network Policy Settings

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service. Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services. The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port.

The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Voice Auto Mode Configuration

LLDP MED Policy for Voice Application	(•) Auto ( ) Manual

Apply

Network Policy Configuration

Network Policy Number	1
Application	Voice
VLAN ID	1 (1-4095)
VLAN Tag	(•) Tagged ( ) Untagged
L2 Priority	0 (0-7)
DSCP Value	0 (0-63)

Object	Description
• **LLDP MED Policy for Voice Application**	Set the LLDP MED policy for voice application mode.
• **Network Policy Number**	Select network policy number for this drop down list.
• **Application Type**	Intended use of the application types: **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **Guest Voice Signaling** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

	Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. **App Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
	Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
• **Tag**	**Tag** indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

4.12.7 MED Port Settings

Port LLDP MED Configuration

Port Select	MED Enable	MED Optional TLVs	MED Network Policy
Select Ports	Enable	Select Optional TLVs	Select Optional TLVs

Object	Description
• **Port Select**	Select port for this drop down list.
• **MED Enable**	Enable or disable MED configuration.
• **MED Optional TVLs**	Configures the information included in the MED TLV field of advertised
	messages. **-Network Policy –** This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption. **-Location –** This option advertises location identification details. **-Inventory –** This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
• **MED Network Policy**	Select MED network policy for this drop down list.

MED Location Configuration

Ports	Select Ports
Location Coordinate	(16 pairs of hexadecimal characters)
Location Civic Address	(6-160 pairs of hexadecimal characters)
Location ECS ELIN	(10-25 pairs of hexadecimal characters)

Object	Description
• **Port**	Select port for this drop down list.
• **Location Coordinate**	A string identifying the Location Coordinate that this entry should belong to.
• **Location Civic Address**	A string identifying the Location Civic Address that this entry should belong to.
• **Location ESC ELIN**	A string identifying the Location ESC ELIN that this entry should belong to.

4.12.8 LLDP Overloading

Link Layer Discovery Protocol (LLDP) is used to advertise information about a device to other connected devices. Optional information can be sent through an LLDP packet in the form of a Type Length Value (TLV). The more information you want to include, the more TLVs you add. LLDP information is sent in a protocol data unit (PDU). Each interface that information is sent across has a maximum size of PDU that it can handle. If too much information is included in an LLDP packet, it can exceed the maximum PDU size. This is known as an LLDP overload.

Object	Description
• **Interface**	The switch port number of the logical port.
• **Toltal (Bytes)**	Total number of bytes of LLDP information that is normally sent in a packet.
• **Left to Send (Bytes)**	Total number of available bytes that can also send LLDP information in a packet.
• **Status**	Gives the status of the TLVs.
• **Mandatory TLVs**	Displays if the mandatory group of TLVs were transmitted or overloaded.
• **MED Capabilites**	Displays if the capabilities packets were transmitted or overloaded.
• **MED Location**	Displays if the location packets were transmitted or overloaded.

• **MED Network Policy**	Displays if the network policies packets were transmitted or overloaded.
• **MED Extended Power via MDI**	Displays if the extended power via MDI packets were transmitted or overloaded.
• **802.3 TLVs**	Displays if the 802.3 TLVs were transmitted or overloaded.
• **Optional TLVs**	If the LLDP MED extended power via MDI packets were sent, or if they were overloaded.
• **MED Inventory**	Displays if the mandatory group of TLVs was transmitted or overloaded.
• **802.1 TLVs**	Displays if the 802.1 TLVs were transmitted or overloaded.

4.12.9 LLDP Statistics

Use the LLDP Device Statistics screen to general statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

Object	Description
• **Insertions**	Shows the number of new entries added since switch reboot.
• **Deletions**	Shows the number of new entries deleted since switch reboot.
• **Drops**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Age Outs**	Shows the number of entries deleted due to Time-To-Live expiring.

4.13 Diagnostics

This section provide the Physical layer and IP layer network diagnostics tools for troubleshooting purposes. The diagnostic tools are designed for network administrators to help them quickly diagnose problems.

4.13.1 Cable Diagnostics

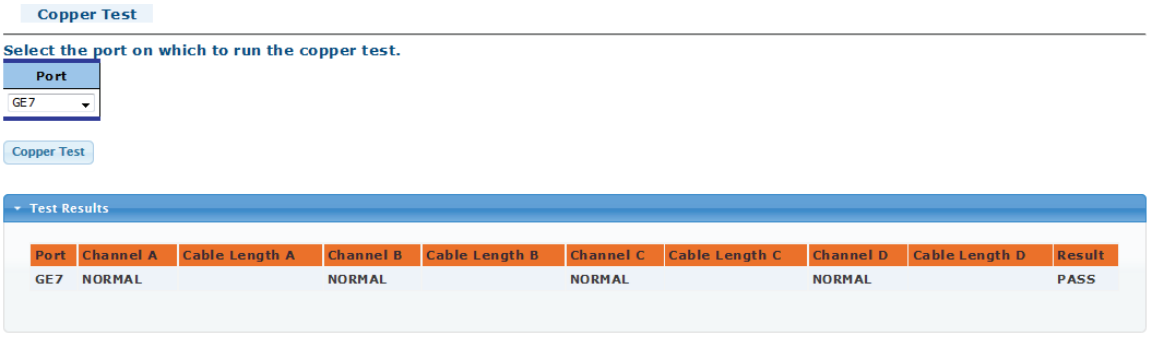
The Cable Diagnostics performs tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

- If the link is established on the twisted-pair interface in 1000Base-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

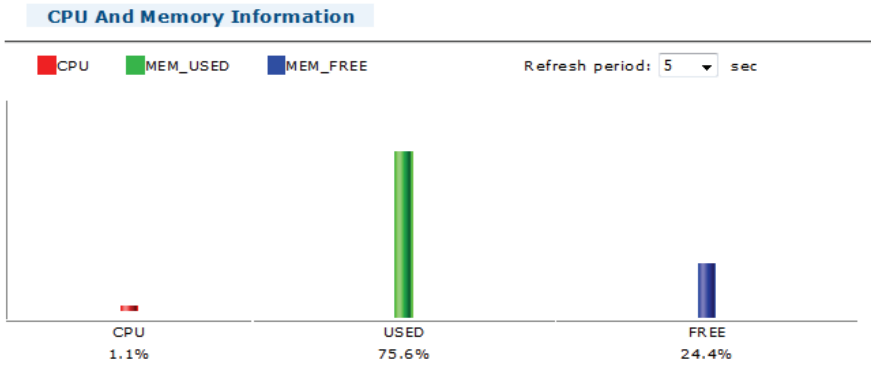
Note:
Cable Diagnostics is only accurate for cables of length from 15 to 100 meters.
Cable pairs are referred to as channels, where channel A represents pins 3 & 4, channel B pins 1 & 2, channel 7 pins 5 & 6 and channel D represents pins 7 & 8.



The picture above shows the test results of port 7, which is connected to a PC with a 3 ft network cable. Due to the short cable, the length test isn't working.

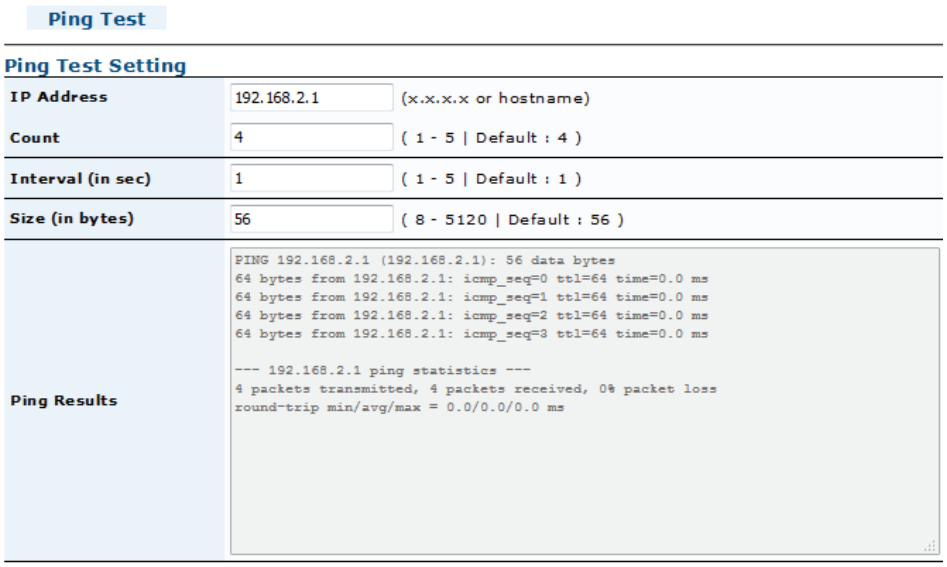
4.13.2 System Status

This page provides information about the switch itself and some of its vital resources.



4.13.3 IPv4 Ping Test

In order to troubleshoot connectivity issues, the Intellinet switch can aide you with an integrated ping tool. This can be very useful if you are remotely connecting to the Intellinet switch and need to perform a PING in the local network.
Provide the IP address, count (how many pings to send), the time interval between each ping, and the size of the payload, click Apply (not shown) and wait for the ping results to be displayed on the screen.



4.13.4 IPv6 Ping Test

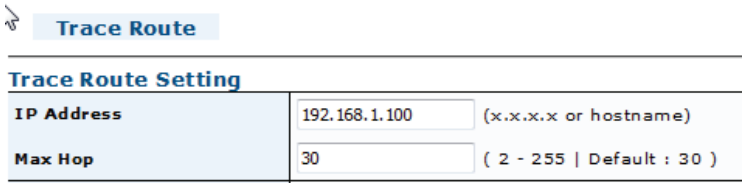
Very much the same as the IPv4 test, except this one is designed for, you guessed it, IPv6 addresses.

4.13.5 Trace Route

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point.

```
$traceroute wikipedia.org
traceroute to wikipedia.org (66.230.200.100), 64 hops max, 44 byte packets
 1  124.ae0.xr1.3d12.xs4all.net (194.109.21.1)  0.305 ms  0.360 ms  0.405 ms
 2  0.so-6-0-0.xr1.tc2.xs4all.net (194.109.5.10)  0.634 ms  0.716 ms  0.673 ms
 3  ams-ix-c00.wvfiber.net (195.69.145.58)  0.638 ms  0.601 ms  0.551 ms
 4  lon-c00-pos-4-0.0C48-ams-pos11-0.wvfiber.net (63.223.28.201)  7.512 ms  7.427 ms  7.494 ms
 5  nyc60-pos-1-0.0C48-lon-c00-pos-3-0.wvfiber.net (63.223.28.145)  84.108 ms  83.804 ms  83.995 ms
 6  66.216.1.181 (66.216.1.181)  83.435 ms  83.278 ms  83.348 ms
 7  ash-c01-tge-3-3.TG-nyc-c01-1-1.wvfiber.net (66.216.1.161)  89.563 ms  89.554 ms  89.551 ms
 8  atl-c01-tge-3-1.TG-ash-c01-3-1.wvfiber.net (66.216.1.157)  103.701 ms  103.606 ms  103.596 ms
 9  cpp-hostway.wvfiber.net (63.223.8.26)  103.678 ms  103.609 ms  103.630 ms
10  e1-12.co2.as30217.net (64.156.25.105)  113.014 ms  113.044 ms  113.084 ms
11  10ge5-1.csw5-pmtpa.wikimedia.org (84.40.25.102)  113.153 ms  113.251 ms  113.180 ms
12  rr.pmtpa.wikimedia.org (66.230.200.100)  113.069 ms  113.172 ms  113.003 ms
```

Above: Example Trace



Type in the IP address of the destination you with to trace, and provide the maximum number of hops.

Note: You can only type in an IP address. Hostnames are not allowed, despite the interface screen claiming otherwise.

4.14 RMON

4.14.1 What is RMON?

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- Statistics: Maintain basic usage and error statistics for each subnet monitored by the Agent.
- History: Record periodical statistic samples available from Statistics.
- Alarm: Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- Event: A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.14.2 RMON Statistics

This page provides RMON statistics for the selected port. Use the drop-down list to select the port you wish to see the statistics for, and a few seconds later the information will appear on the screen. Click “Clear” in order to reset the statistics for the selected port.

4.14.3 RMON Event and Event Log

You can define a RMON event on this page.

RMON Event Settings

Select Index	Create New
Index	0 (1-65535)
Type	None
Community	public
Owner	(0~31 Charactors)
Description	(0~127 Charactors)

Object	Description
• **Select Index**	Select index for this drop down list to create new index or modify index.
• **Index**	Indicates the index of the entry. The range is from 1 to 65535.
• **Type**	Indicates the notification of the event, the possible types are: ■ **none**: The total number of octets received on the interface, including framing characters. ■ **log**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **SNMP-Trap**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ **Log and Trap**: The number of inbound packets that are discarded even the packets are normal.
• **Community**	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
• **Owner**	Indicates the owner of this event, the string length is from 0 to 127, default is a null string.
• **Description**	Indicates description of this event, the string length is from 0 to 127, default is a null string.

The RMON Event Log screen allows you monitor RMON events.

4.14.4 RMON Alarm

An RMON alarm monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified threshold value (threshold), and resets the alarm at another threshold value. You can use alarms with RMON events to generate a log entry or an SNMP notification when the RMON alarm triggers.

RMON Alarm Settings

Select Index	Create New
Index	0 (1-65535)
Sample Port	GE1
Sample Variable	DropEvents
Sample Interval	0 (1-2147483647)
Sample Type	Absolute Delta
Rising Threshold	0 (0-2147483647)
Falling Threshold	0 (0-2147483647)
Rising Event	0: None (Unassigned)
Falling Event	0: None (Unassigned)
Owner	(0~31 Charactors)

Object	Description
• **Select Index**	Select index for this drop down list to create the new index or modify the index
• **Index**	Indicates the index of the alarm entry.
• **Sample Port**	Select port for this drop down list
• **Sample Variable**	Indicates the particular variable to be sampled, the possible variables are: ■ **DropEvents**: The total number of events in which packets were dropped due to lack of resources. ■ **Octets**: The number of received and transmitted (good and bad) bytes.

	Includes FCS, but excludes framing bits. ■ **Pkts**: The total number of frames (bad, broadcast and multicast) received and transmitted. ■ **BroadcastPkts**: The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets. ■ **MulticastPkts**: The total number of good frames received that were directed to this multicast address. ■ **CRCAlignErrors**: The number of CRC/alignment errors (FCS or alignment errors). ■ **UnderSizePkts**: The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **OverSizePkts**: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Fragments**: The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error. ■ **Jabbers**: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets), and had either an FCS or alignment error. ■ **Collisions**: The best estimate of the total number of collisions on this Ethernet segment. ■ **Pkts64Octets**: The total number of frames (including bad packets) received andtransmitted that were 64 octets in length (excluding framing bits but including FCS octets). ■ **Pkts64to172Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). ■ **Pkts158to255Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). ■ **Pkts256to511Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the

	specified range (excluding framing bits but including FCS octets). ■ **Pkts512to1023Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). ■ **Pkts1024to1518Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
• **Sample Interval**	Sample interval (1–2147483647)
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Absolute**: Get the sample directly (default). ■ **Delta**: Calculate the difference between samples.
• **Rising Threshold**	Rising threshold value (0–2147483647)
• **Falling Threshold**	Falling threshold value (0–2147483647)
• **Rising Event**	Event to fire when the rising threshold is crossed
• **Falling Event**	Event to fire when the falling threshold is crossed
• **Owner**	Specify an owner for the alarm

4.14.5 RMON History and History Log

RMON History (also known as RMON group 2) collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.

RMON History Settings

Select Index	Create New
Index	0 (1-65535)
Sample Port	GE1
Bucket Requested	50 (1-65535, Default 50)
Interval	1800 (1-3600 Default 1800)
Owner	(0~31 Charactors)

Object	Description
• **Select Index**	Select index for this drop down list to create the new index or modify the index
• **Index**	Indicates the index of the history entry.
• **Sample Port**	Select port for this drop down list
• **Bucket Requested**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 50, default value is 50.
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Owner**	Specify an owner for the history

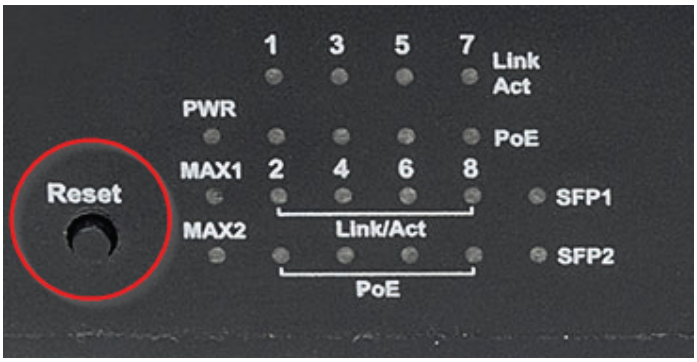
4.15 Maintenance

4.15.1 Factory Default

There are two ways to reset the Intellinet switch back to its factory default settings.

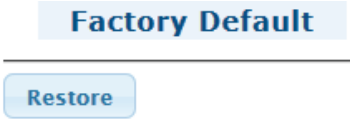
4.15.1.1 Via Reset Button

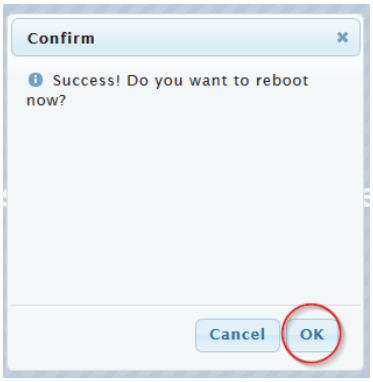
Press the reset button for at least 10 seconds while the switch is operation in order to trigger the factory default reset.



4.15.1.2 Via Web Administrator Menu

Click on Restore and confirm your decision.





4.15.2 Reboot Switch

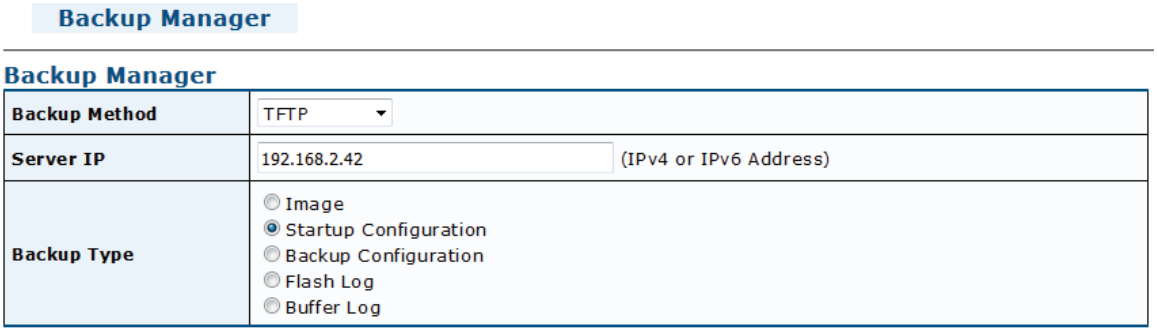
If you need to reboot the Intellinet switch from a remote location, this is the way to do it. When the reboot is triggered, the switch won't be accessible and operational for about 60 seconds.

4.15.3 Backup Manager

This function allows backup of the current image or configuration of the Intellinet 8-Port Gigabit PoE+ switch to the local management station, i.e., a desktop computer.

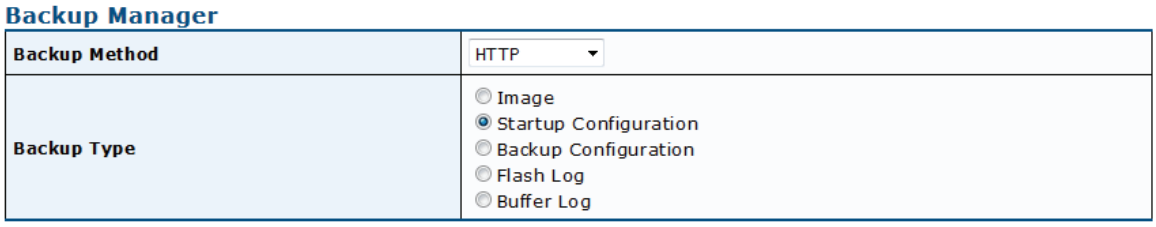
4.15.3.1 Via TFTP

Is you choose TFTP, then a TFTP server has to be available for the switch to connect to. You need to provide the IP address of a valid TFTP server, and you will have to specify what type of backup you wish to make.



4.15.3.2 Via HTTP

Select HTTP for an easier and quicker way to store the configuration and log data.



Click the

button to save the file on your local HDD.

4.15.4 Upgrade Manager

If a new firmware needs to be installed, you can use this screen to do it. You can install a new firmware image using TFTP, or HTTP. You can also use this feature to reload a previously saved configuration.

4.15.4.1 Via TFTP

To install the upgrade via TFTP, a TFTP server must be configured to accept connections from the Intellinet switch. Provide the IP address of the TFTP server along with the correct file name that you wish to install.

Press Upgrade to begin.

Upgrade Manager

Upgrade Method	TFTP
Server IP	0.0.0.0 (IPv4 or IPv6 Address)
File Name	type in file name manually
Upgrade Type	Image Startup Configuration Backup Configuration

4.15.4.2 Via HTTP

In order to install the upgrade, select the appropriate upgrade type, then click on Browse..., select the file from your local HDD. Then press Upgrade to begin.

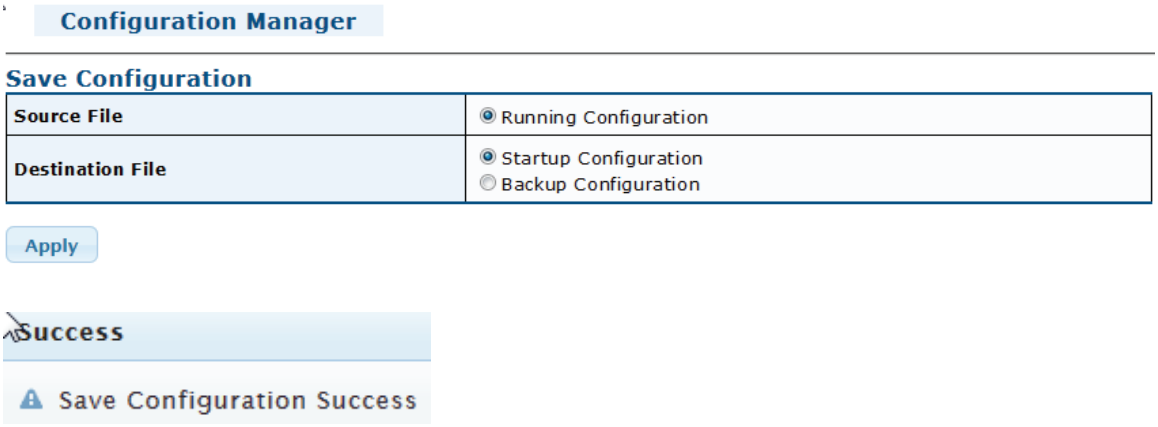
Upgrade Manager

Upgrade Method	HTTP
Upgrade Type	Image Startup Configuration Backup Configuration
Browse file	Browse... No file selected.

4.15.5 Configuration Manager

The Intellinet 8-Port PoE+ Gigabit Switch has two configurations. The startup and the backup configuration. With the backup manager you can save these configurations to a TFTP server, or to the HDD of a computer.

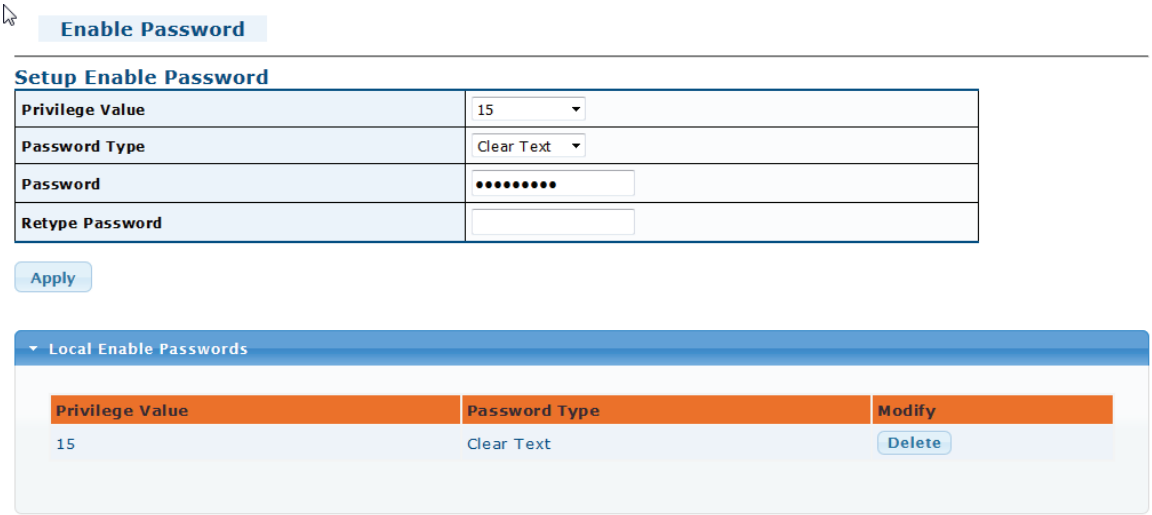
With the configuration manager you can create the startup and backup configuration, by copying the current configuration of the switch (running configuration) to either the startup or backup configuration.



Once the current configuration has been saved this way, it can be backed up with the backup manager.

4.15.6 Enable Password

This page allows you to modify the enable password. In the command line interface, you can use “enable” to change the privilege level to “Admin.” After the “enable” command is issued, you need to enter the enable password to change the privilege level.



5 Warranty

Deutsch Garantieinformationen finden Sie hier unter intellinetnetwork.com/warranty.
English For warranty information, go to intellinetnetwork.com/warranty.
Español Si desea obtener información sobre la garantía, visite intellinetnetwork.com/warranty.
Français Pour consulter les informations sur la garantie, rendezvous à l'adresse intellinetnetwork.com/warranty.
Italiano Per informazioni sulla garanzia, accedere a intellinetnetwork.com/warranty.
Polski Informacje dotyczące gwarancji znajdują się na stronie intellinetnetwork.com/warranty.
México Póliza de Garantía Intellinet — Datos del importador y responsable ante el consumidor IC Intracom México, S.A.P.I. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlan Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500

La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra.
A. Garantizamos cámaras IP y productos con partes móviles por 3 años.
B. Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones:
1. Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor.
2. El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico.
3. La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instaladas de fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor.
Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde ue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos n su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, numero de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese tilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; o si el producto ha sido alterado o tratado de ser reparado por el consumidor o terceras personas.

6 Copyright

7 Federal Communication Commission Interference Statement

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

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

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement:

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

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

intellinetnetworkcom