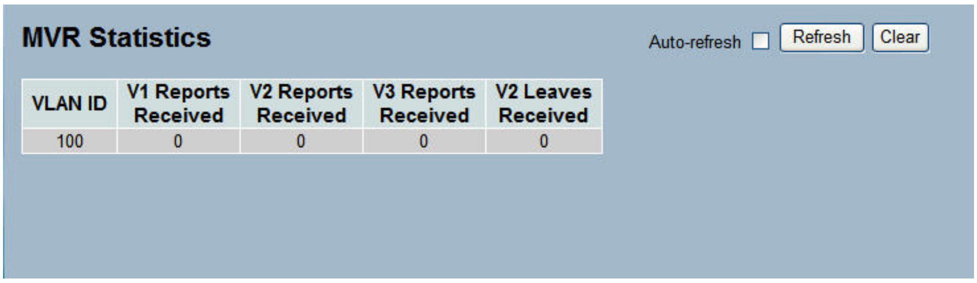
Figure 3-7.3: The MVR Statistics Information



MVR Statistics

VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

Parameter description:

VLAN ID:

The Multicast VLAN ID.

V1 Reports Received:

The number of Received V1 Reports.

V2 Reports Received:

The number of Received V2 Reports.

V3 Reports Received:

The number of Received V3 Reports.

V2 Leaves Received:

The number of Received V2 Leaves.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the MVR Group information manually.

<<, >>

Go to the previous/next page or entry.

3.8 LLDP

The switch supports the LLDP. The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

3.8.1 LLDP Configuration

You can configure LLDP and the detail parameters per port, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click LLDP configuration

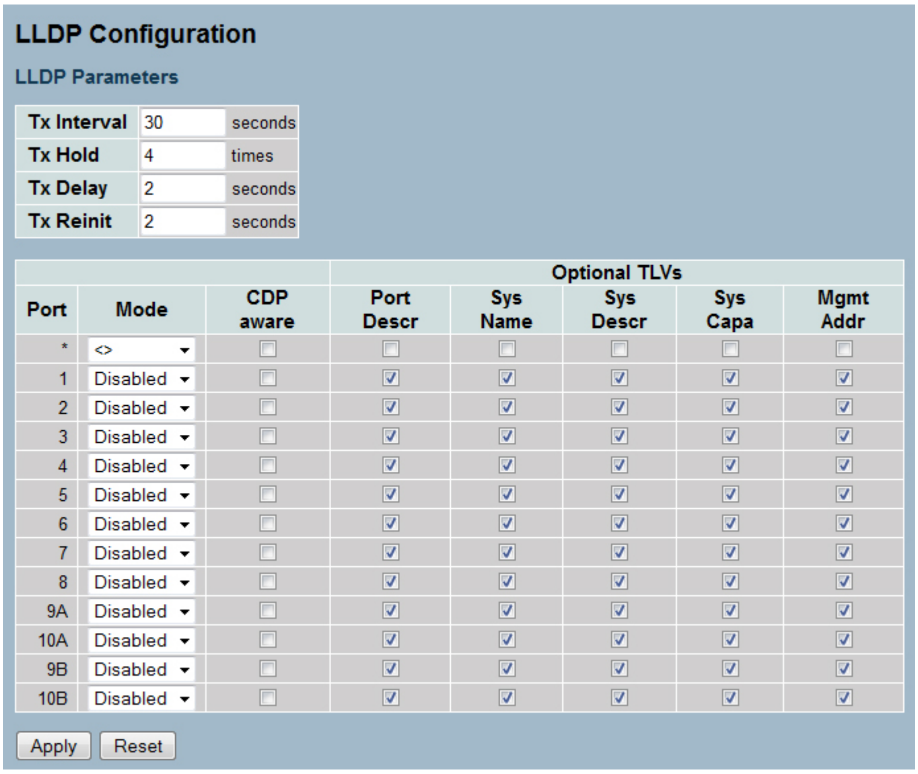
2. Modify LLDP timing parameters

3. Set the required mode for transmitting or receiving LLDP messages

4. Specify the information to include in the TLV field of advertised messages

5. Click Apply

Figure 3-8.1: The LLDP Configuration (GS-2310P)



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	□	□	□	□	□	□
1	Disabled	□	☑	☑	☑	☑	☑
2	Disabled	□	☑	☑	☑	☑	☑
3	Disabled	□	☑	☑	☑	☑	☑
4	Disabled	□	☑	☑	☑	☑	☑
5	Disabled	□	☑	☑	☑	☑	☑
6	Disabled	□	☑	☑	☑	☑	☑
7	Disabled	□	☑	☑	☑	☑	☑
8	Disabled	□	☑	☑	☑	☑	☑
9A	Disabled	□	☑	☑	☑	☑	☑
10A	Disabled	□	☑	☑	☑	☑	☑
9B	Disabled	□	☑	☑	☑	☑	☑
10B	Disabled	□	☑	☑	☑	☑	☑

Parameter description:

LLDP Parameters

Tx Interval:

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold:

Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay:

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit:

When a port is disabled, LLDP is disabled or the switch is rebooted, an 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.

LLDP Port Configuration

The LLDP port settings relate to the currently selected, as reflected by the page header.

Port:

The switch port number of the logical LLDP port.

Mode:

Select LLDP mode.

Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled the switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware:

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors’ table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors’ table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors’ table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors’ table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

When CDP awareness on a port is disabled the CDP information isn't removed immediately, but when the hold time is exceeded.

Port Descr:

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

Sys Name:

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

Sys Descr:

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

Sys Capa:

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

Mgmt Addr:

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

Buttons:

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

3.8.2 LLDP Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

Web Interface

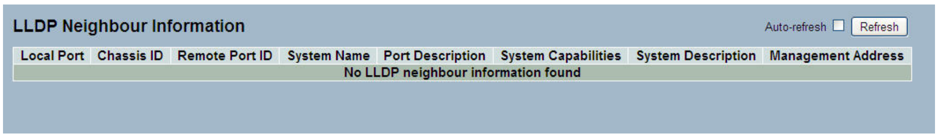
To show LLDP neighbors:

1. Click LLDP Neighbors

2. Click Refresh for manual update web screen

3. Click Auto-refresh for auto-update web screen

Figure 3-8.2: The LLDP Neighbors information



LLDP Neighbour Information

Auto-refresh □ Refresh

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	System Description	Management Address
No LLDP neighbour information found							

If your network without any device supports LLDP then the table will show “No LLDP neighbor information found”.

Parameter description:

Local Port:

The port on which the LLDP frame was received.

Chassis ID:

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

Remote Port ID:

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

System Name:

System Name is the name advertised by the neighbor unit.

Port Description:

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

System Capabilities:

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

1. Other

2. Repeater

3. Bridge

4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

8. Station only

9. Reserved

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

System Description:

System Description is the port description advertised by the neighbor unit.

Management Address:

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

Auto-refresh:

Activate the auto-refresh to the information automatically.

Refresh:

Refresh the LLDP Neighbors information manually.

3.8.3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED, which provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery allows creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click LLDP-MED Configuration

2. Modify Fast start repeat count parameter, default is 4

3. Modify Coordinates Location parameters

4. Fill Civic Address Location parameters

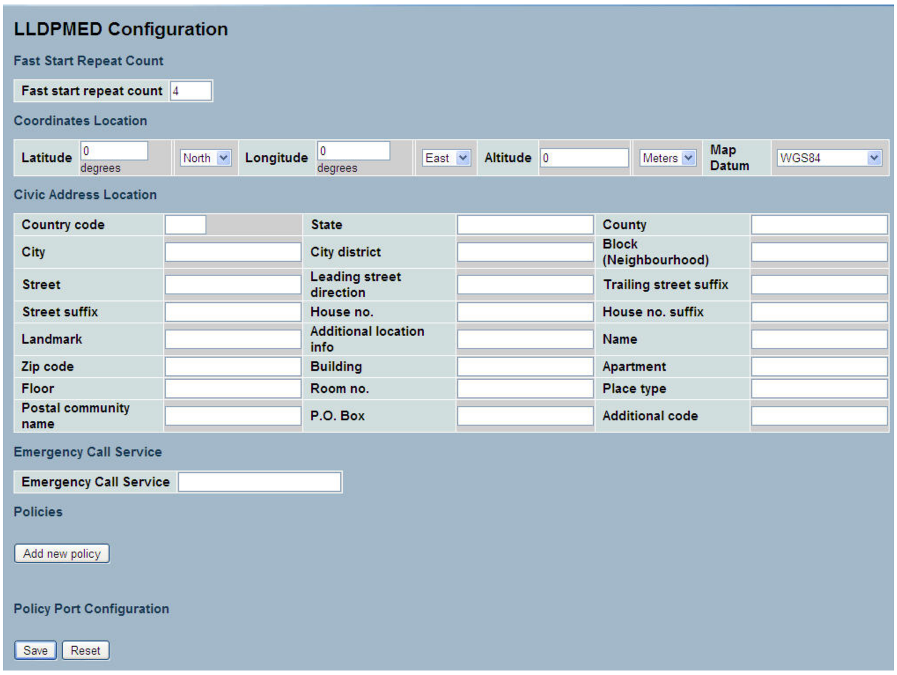
5. Add new policy

6. Click Apply, will show following Policy Port Configuration

7. Select Policy ID for each port

8. Click Apply

Figure 3-8.3: The LLDP-MED Configuration



LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Coordinates Location

Latitude	0 degrees	North	Longitude	0 degrees	East	Altitude	0	Meters	Map Datum	WGS84

Civic Address Location

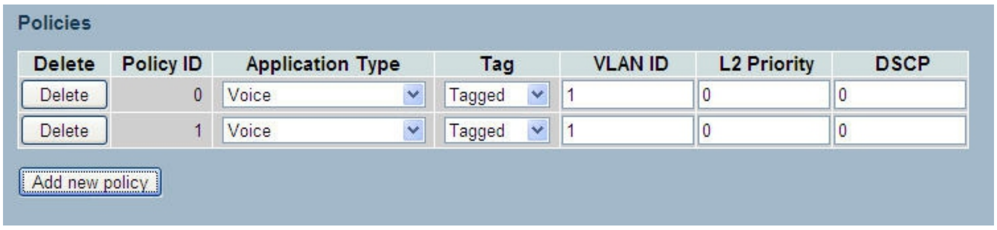
Country code		State		County	
City		City district		Block (Neighbourhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Policy Port Configuration



Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0
Delete	1	Voice	Tagged	1	0	0

Parameter description:

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

Latitude:

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

It is possible to specify the direction to either North of the equator or South of the equator.

Longitude:

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude:

Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.

It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum:

The Map Datum is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code:

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State:

National subdivisions (state, canton, region, province, prefecture).

County:

County, parish, gun (Japan), district.

City:

City, township, shi (Japan) - Example: Copenhagen.

City district:

City division, borough, city district, ward, chou (Japan).

Block (Neighborhood):

Neighborhood, block.

Street:

Street - Example: Poppelvej.

Leading street direction:

Leading street direction - Example: N.

Trailing street suffix:

Trailing street suffix - Example: SW.

Street suffix:

Street suffix - Example: Ave, Platz.

House no.:

House number - Example: 21.

House no. suffix:

House number suffix - Example: A, 1/2.

Landmark:

Landmark or vanity address - Example: Columbia University.

Additional location info:

Additional location info - Example: South Wing.

Name:

Name (residence and office occupant) - Example: Flemming Jahn.

Zip code:

Postal/zip code - Example: 2791.

Building:

Building (structure) - Example: Low Library.

Apartment:

Unit (Apartment, suite) - Example: Apt 42.

Floor:

Floor - Example: 4.

Room no.:

Room number - Example: 450F.

Place type:

Place type - Example: Office.

Postal community name:

Postal community name - Example: Leonia.

P.O. Box:

Post office box (P.O. BOX) - Example: 12345.

Additional code:

Additional code - Example: 1320300003.

Emergency Call Service:

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service:

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

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.

Delete:

Check to delete the policy. It will be deleted during the next save.

Policy ID:

ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

Application Type:

Intended use of the application types:

1. 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.

2. Voice Signaling (conditional) - 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.

3. 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.

4. Guest Voice Signaling (conditional) - 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.

5. 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.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. 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.

8. Video Signaling (conditional) - 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.

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.

VLAN ID:

VLAN identifier (VID) for the port as defined in 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.

Adding a new policy:

Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".

Port Policies Configuration:

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port:

The port number to which the configuration applies.

Policy Id:

The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons:

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

3.8.4 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Web Interface

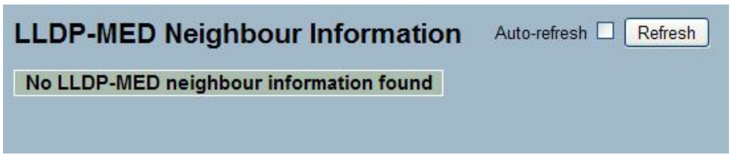
To show LLDP-MED neighbor:

1. Click LLDP-MED Neighbor

2. Click Refresh for manual update web screen

3. Click Auto-refresh for auto-update web screen

Figure 3-9.4: The LLDP-MED Neighbors information



LLDP-MED Neighbour Information

Auto-refresh ☐ Refresh

No LLDP-MED neighbour information found

If your network without any device supports LLDP-MED then the table will show “No LLDP-MED neighbor information found”.

Parameter description:

Port:

The port on which the LLDP frame was received.

Device Type:

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition:

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I):

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II):

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III):

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management.

LLDP-MED Capabilities:

LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities

2. Network Policy

3. Location Identification

4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. Reserved

Application Type:

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. 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.

2. Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media.

3. Guest Voice - to 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.

4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. 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.

8. Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.

Policy:

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

TAG:

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID:

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority:

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP:

DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

3.8.5 EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to the circuits EEE turns off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Web Interface

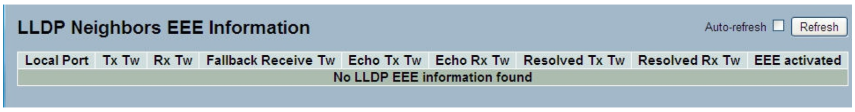
To show LLDP EEE neighbors:

1. Click LLDP, than click EEE to show discover EEE devices

2. Click Refresh for manual update web screen

3. Click Auto-refresh for auto-update web screen

Figure 3-8.5: The LLDP Neighbors EEE information



LLDP Neighbors EEE Information

Auto-refresh □ Refresh

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE activated
No LLDP EEE information found								

If your network without any devices which enables EEE function then the table will show “No LLDP EEE information found”.

Parameter description:

Local Port:

The port on which LLDP frames are received or transmitted.

Tx Tw:

The link partner’s maximum time that transmit path can hold off sending data after reassertion of LPI.

Rx Tw:

The link partner’s time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.

Fallback Receive Tw:

The link partner’s fallback receives Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw:

The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partners’ reflection (echo) of the remote link partners’ respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw:

The link partner's Echo Rx Tw value.

Resolved Tx Tw:

The resolved Tx Tw for this link. Note: NOT the link partner

The resolved value that is the actual "tx wakeup time“used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw:

The resolved Rx Tw for this link. Note: NOT the link partner

The resolved value that is the actual "tx wakeup time“ used for this link (based on EEE information exchanged via LLDP).

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the LLDP Neighbors information manually.

3.8.6 Port Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch

Web Interface

To show LLDP Statistics:

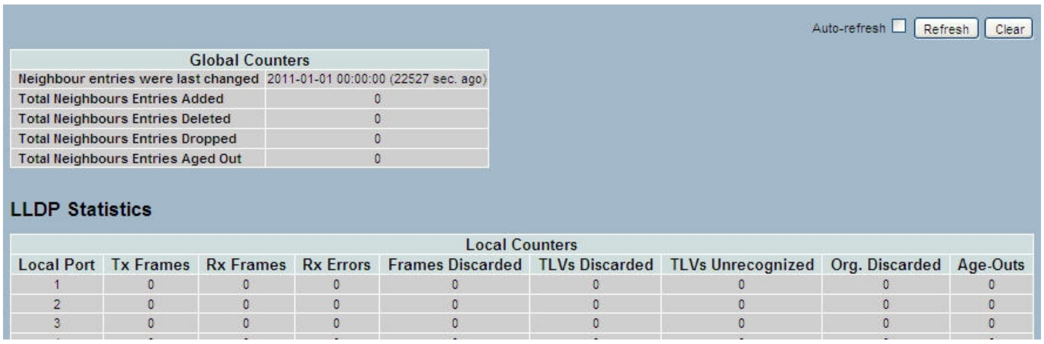
1. Click LLDP, than click Port Statistics to show LLDP counters

2. Click Refresh for manual update of the view

3. Click Auto-refresh for auto-update web screen

4. Click Clear to clear all counters

Figure 3-8.6: The LLDP Port Statistics information



Global Counters	
Neighbour entries were last changed	2011-01-01 00:00:00 (22527 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0

Parameter description:

Global Counters

Neighbor entries were last changed at:

It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added:

Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted:

Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped:

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out:

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port:

The port on which LLDP frames are received or transmitted.

Tx Frames:

The number of LLDP frames transmitted on the port.

Rx Frames:

The number of LLDP frames received on the port.

Rx Errors:

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

Frames Discarded:

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

TLVs Discarded:

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

TLVs Unrecognized:

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

Org. Discarded:

The number of organizationally received TLVs.

Age-Outs:

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

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the LLDP Port Statistics information manually.

Clear:

Press clear to clean up the entries.

3.9 Filtering Data Base

The Filtering Data Base Configuration includes many functions, including MAC Table Information, Static MAC Learning, which cannot be categorized to some function type.

MAC table

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

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

3.9.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Web Interface

To configure MAC Address Table in the web interface:

Aging Configuration

1. Click configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

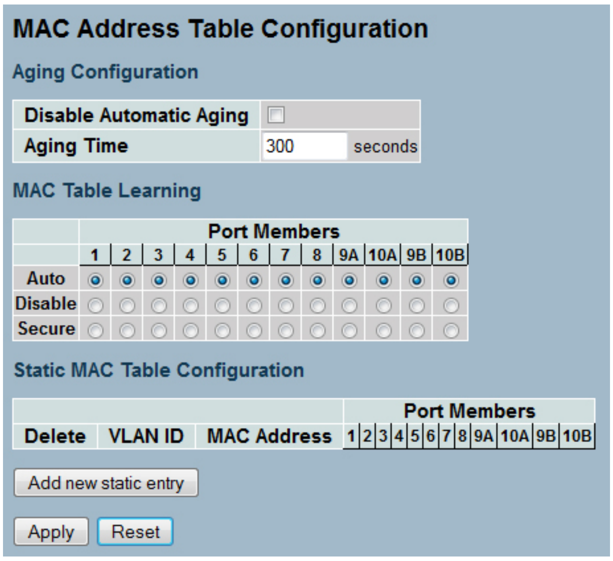
MAC Table Learning

1. Click configuration.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Apply.

Static MAC Table Configuration

1. Click configuration and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click Apply.

Figure 3- 9.1: The MAC Address Table Configuration (GS-2310P)



MAC Address Table Configuration

Aging Configuration

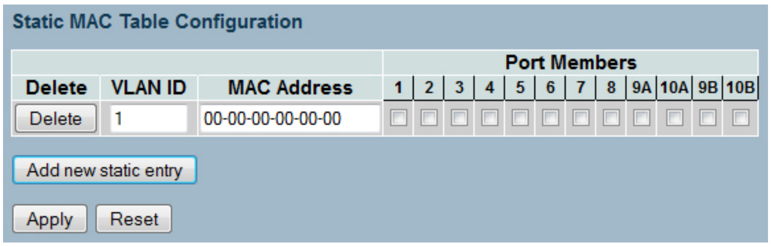
Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Auto	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9A	10A	9B	10B



Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□	□	□

Parameter description:

Aging Configuration:

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking Disable automatic aging.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

Auto:

Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable:

No learning is done.

Secure:

Only static MAC entries are learned, all other frames are dropped.

Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete:

Check to delete the entry. It will be deleted during the next save.

VLAN ID:

The VLAN ID of the entry.

MAC Address:

The MAC address of the entry.

Port Members:

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry:

Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons:

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

3.9.2 Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Web Interface

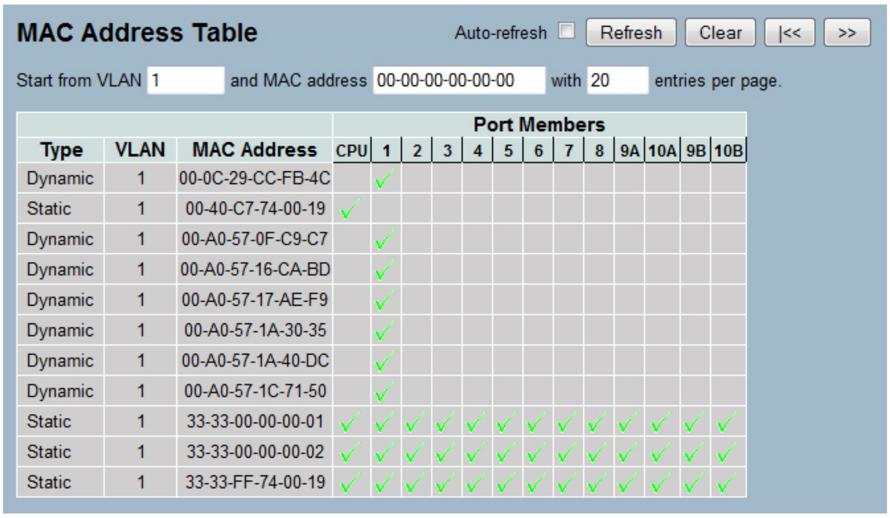
To display MAC Address Table in the web interface:

1. Click Dynamic MAC Table.

2. Specify the VLAN and MAC Address.

3. Display MAC Address Table.

Figure 3- 9.2: The Dynamic MAC Address Table information (GS-2310P)



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Dynamic	1	00-0C-29-CC-FB-4C		✓											
Static	1	00-40-C7-74-00-19	✓												
Dynamic	1	00-A0-57-0F-C9-C7		✓											
Dynamic	1	00-A0-57-16-CA-BD		✓											
Dynamic	1	00-A0-57-17-AE-F9		✓											
Dynamic	1	00-A0-57-1A-30-35		✓											
Dynamic	1	00-A0-57-1A-40-DC		✓											
Dynamic	1	00-A0-57-1C-71-50		✓											
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-74-00-19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter description:

MAC Table Columns

Type:

Indicates whether the entry is a static or a dynamic entry.

VLAN:

The VLAN ID of the entry.

MAC address:

The MAC address of the entry.

Port Members:

The ports that are members of the entry.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh, Clear, <<, >>):

Refresh the MAC address entries manually.

Clear

Press clear to clean up the MAC table.

<<, >>

Go to the previous/next entries of the table.

00-A0-57-73-01-29: your switch MAC address (for IPv4)

33-33-00-00-00-01: Destination MAC (for IPv6 Router Advertisement)

33-33-00-00-00-02: Destination MAC (for IPv6 Router Solicitation)

33-33-FF-73-01-29: Destination MAC (for IPv6 Neighbor Solicitation)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast

3.10 VLAN

How to assign a specific VLAN for management purposes

The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, Telnet, HTTP(S) and SSH session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the management VLAN window. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

3.10.1 VLAN Membership

The VLAN membership configuration for the selected switch unit can be monitored and modified here. Up to 4094 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Web Interface

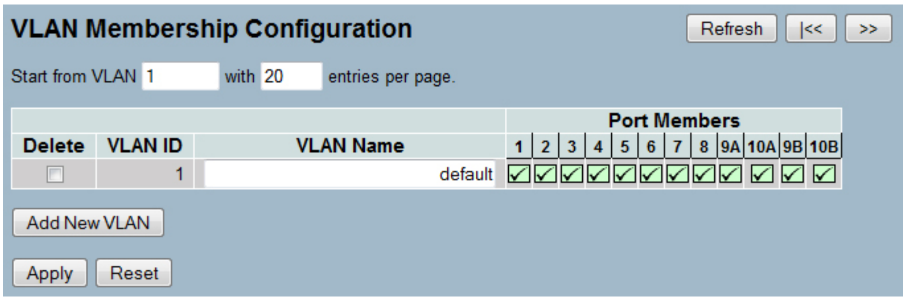
To configure VLAN membership configuration in the web interface:

1. Click VLAN membership Configuration.

2. Specify VLAN ID. 1 4094

3. Click Apply.

Figure 3-10.1: The VLAN Membership Configuration (GS-2310P)



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9A	10A	9B	10B
☐	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Parameter description:

Delete:

To delete a VLAN entry, check this box. The entry will be deleted on the selected switch. If none of the ports of this switch are members of a VLAN then the delete checkbox will be greyed out (you cannot delete that entry. during the next Save.

VLAN ID:

Indicates the ID of this particular VLAN.

VLAN Name:

Indicates the name of VLAN. VLAN name can only contain alphabets or numbers. VLAN name should contain at least one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

Port Members:

A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.