

Adding a New VLAN:

Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4094.

The VLAN is enabled on the selected switch unit when you click on "Save". The VLAN is thereafter present on the other switch units, but with no port members. The check box is greyed out when VLAN is displayed on other switches, but user can add member ports to it.

A VLAN without any port members on any unit will be deleted when you click "Save".

The button can be used to undo the addition of new VLANs.

Buttons:

Save:

Click to save changes.

Reset:

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

Refresh:

Refresh the VLAN entries manually.

Clear:

Clean up the VLAN table.

|<<, >>:

Go to the previous/next page of the table.

3.10.2 Ports

In the VLAN Tag Rule Settings, PVID number for each port can be set. The range of PVID numbers is from 1 to 4094. Ingress filtering rules for each port are available. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is "forward only packets with PVID matching this port's configured PVID". The Ingress Filtering Rule 2 is "drop untagged frame". You can also select the Role of each port as Access, Trunk, or Hybrid.

Web Interface

To configure VLAN Port configuration in the web interface:

1. Click VLAN Port Configuration.
2. Specify the VLAN Port Configuration parameters.
3. Click Apply.

Figure 3-10.2: The VLAN Port Configuration (GS-2310P)

3 Configuration

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	<input type="checkbox"/>	<>	<>	
1	C-port	<input type="checkbox"/>	All	Hybrid	1
2	C-port	<input type="checkbox"/>	All	Hybrid	1
3	C-port	<input type="checkbox"/>	All	Hybrid	1
4	C-port	<input type="checkbox"/>	All	Hybrid	1
5	C-port	<input type="checkbox"/>	All	Hybrid	1
6	C-port	<input type="checkbox"/>	All	Hybrid	1
7	C-port	<input type="checkbox"/>	All	Hybrid	1
8	C-port	<input type="checkbox"/>	All	Hybrid	1
9A	C-port	<input type="checkbox"/>	All	Hybrid	1
10A	C-port	<input type="checkbox"/>	All	Hybrid	1
9B	C-port	<input type="checkbox"/>	All	Hybrid	1
10B	C-port	<input type="checkbox"/>	All	Hybrid	1

Apply Reset

Parameter description:

Ethertype for Custom S-ports:

This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports. Custom Ethertype enables the user to change the Ethertype value on a port to any value to support network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

Port:

This is the logical port number of this row.

Port Type:

Port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

Table 1: Explanation of possible port types

	Ingress action	Egress action
Unaware	<p>When the port receives an untagged frame, a tag - based on the defined PVID - is added and the frame is forwarded.</p> <p>When the port receives a tagged frame, an additional outer tag - based on the defined PVID - is added and the frame is forwarded.</p>	The TPID (Tag Protocol Identifier) of a frame transmitted by an unaware port will be set to 0x8100. The final status of the frame after egressing is also effected by the egress rule.
C-port	<p>When the port receives an untagged frame, a tag - based on the defined PVID - is added and the frame is forwarded.</p> <p>When the port receives a tagged frame and the TPID</p> <ol style="list-style-type: none"> is 0x8100, the frame is forwarded (no additional tag added). is not 0x8100, not 0x88a8 and not Ethertype, an additional outer tag - based on the defined PVID - is added and the frame is forwarded. is 0x88A8 or Ethertype, the frame is discarded. 	The TPID of a frame transmitted by a C-port will be set to 0x8100.
S-port	<p>When the port receives an untagged frame, a tag - based on the defined PVID - is added and the frame is forwarded.</p> <p>When the port receives a tagged frame and the TPID</p> <ol style="list-style-type: none"> is 0x8100, the frame is discarded. 	The TPID of a frame transmitted by an S-port will be set to 0x88A8.

	Ingress action	Egress action
S-custom-port	<p>2. is not 0x8100, the frame is forwarded (no additional tag added).</p> <p>When the port receives an untagged frame, a tag - based on the defined PVID - is added and the frame is forwarded.</p> <p>When the port receives a tagged frame and the TPID</p> <ol style="list-style-type: none"> 1. is 0x8100, the frame is discarded. 2. is not 0x8100, the frame is forwarded (no additional tag added). 	<p>The TPID of frame transmitted by an S-custom-port will be set to a self-customized value, which can be set by using the field Ethertype for Custom S-ports.</p>

3 Configuration

Port Type – Ingress samples (each arrow color represents its operate behavior to individual packet)

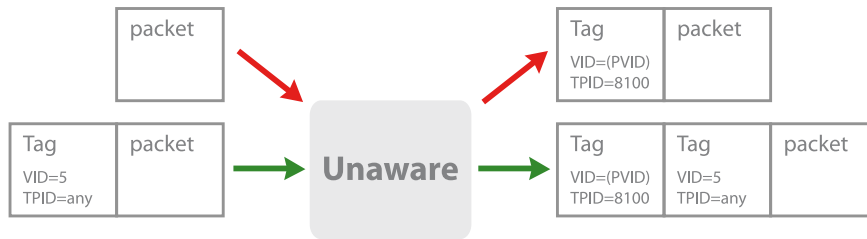


Figure 1: Ingress sample: Unaware

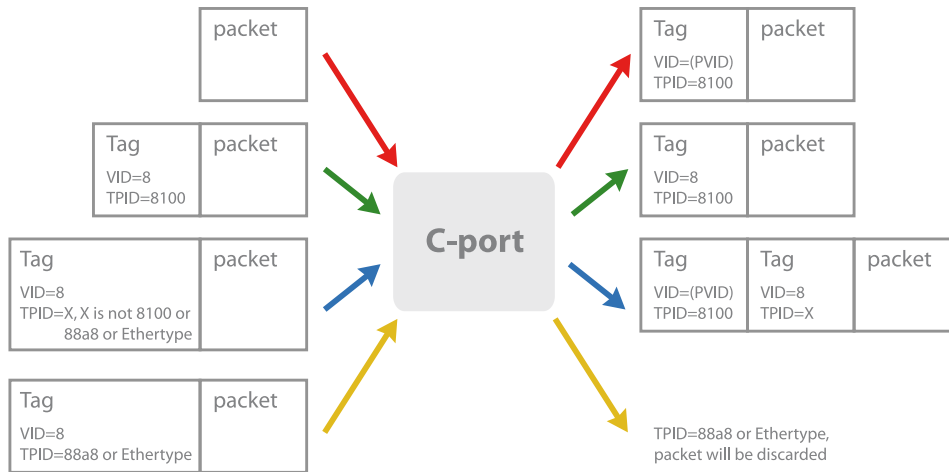


Figure 2: Ingress sample: C-port

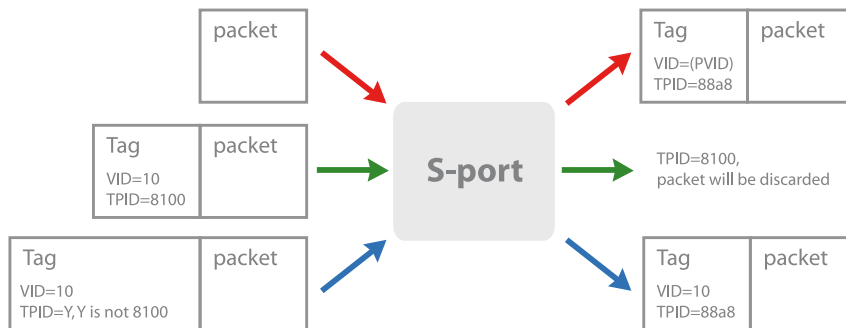


Figure 3: Ingress sample: S-port

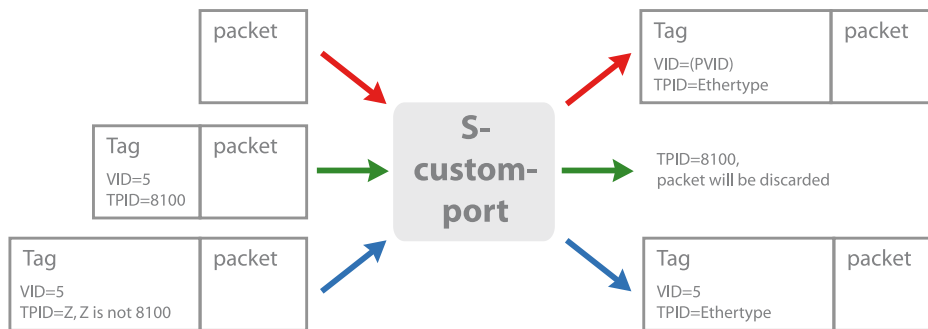


Figure 4: Ingress sample: S-custom-port

Ingress Filtering:

Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

Frame Type:

Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.

Port VLAN Mode:


Configures the Port VLAN Mode. The allowed values are None or Specific. This parameter affects VLAN ingress and egress processing.

If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches.

If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID:

Configures the VLAN identifier for the port. The allowed values are 1 through 4094. The default value is 1.

 The port must be a member of the same VLAN as the Port VLAN ID.

Buttons:

Save – Click to save changes.

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

3.10.3 Switch Status

The Switch Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To display VLAN membership status in the web interface:

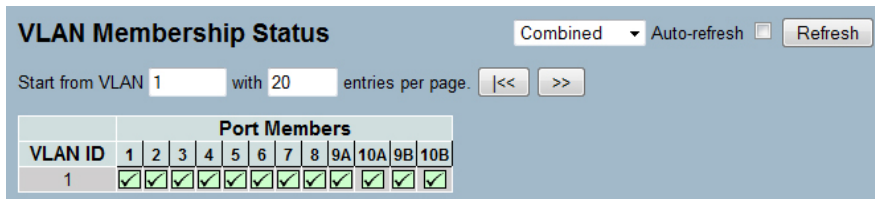
1. Click VLAN membership.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP

Combined.

3. Display membership information.

Figure 3-10.3: The VLAN Membership Status for Combined users (GS-2310P)

The ports belong to the currently selected stack unit, as reflected by the page header.



VLAN Membership Status		Combined	Auto-refresh	Refresh									
Start from VLAN	1	with	20	entries per page. << >>									
VLAN ID		Port Members											
1		1	2	3	4	5	6	7	8	9A	10A	9B	10B
		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter description:

VLAN USER (You can scroll to select one kind VLAN user as below)

3 Configuration

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

Web/SNMP: These are referred to as static.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MVRP: Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

GVRP: GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

VLAN ID:

Indicates the ID of this particular VLAN.

VLAN Membership:

The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the VLAN entries manually.

3.10.4 Port Status

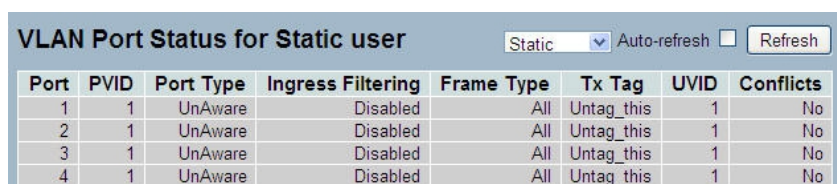
The Port Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To display VLAN Port Status in the web interfaces:

1. Click VLAN Port Status.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display Port Status information.

Figure 3-10.4: The VLAN Port Status for Static user



Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No

Parameter description:

Port:

The logical port for the settings contained in the same row.

PVID:

Shows the VLAN identifier for that port. The allowed values are 1 through 4094. The default value is 1.

Port Type:

Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

Ingress Filtering:

Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type:

Shows 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 that port are discarded.

Tx Tag:

Shows egress filtering frame status whether tagged or untagged.

UVID:

Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

Conflicts:

Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

Functional Conflicts between features.

Conflicts due to hardware limitation.

Direct conflict between user modules.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the VLAN Port Status information manually.

3.10.5 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. Any VLAN can be configured as a private VLAN.

Private VLAN Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

3 Configuration

To configure Private VLAN in the web interface:

1. Click add new Private VLAN configuration.
2. Specify the Private VLAN ID and Port Members.
3. Click Save.

Figure 3-10.5.1: The Port Isolation Configuration

Private VLAN Membership Configuration		Port Members																									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Parameter description:

Delete:

Check to delete a private VLAN entry. The entry will be deleted during the next save.

Private VLAN ID

The ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked.

Adding a New Private VLAN

Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

The Private VLAN is enabled when you click "Save".

Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN, Port Isolation.
2. Activate which port want to enable Port Isolation
3. Click Apply.

Figure 3-10.5.1: The Port Isolation Configuration (GS-2310P)

Port Number											
1	2	3	4	5	6	7	8	9A	10A	9B	10B
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Reset

Parameter description:

Port Members:

A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons:

Save – Click to save changes.

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

3.10.6 MAC-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

The most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the mean time, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Configuration

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click MAC address-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Apply.

Figure 3-10.6.1: The MAC-based VLAN Membership Configuration (GS-2310P)

MAC-based VLAN Membership Configuration			Port Members											
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9A	10A	9B	10B
<input type="checkbox"/>	00-00-00-00-00-00	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Refresh, <<, >>

Buttons: Add new entry, Apply, Reset

Parameter description:

Delete:

To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch.

MAC Address:

Indicates the MAC address.

VLAN ID:

Indicates the VLAN ID.

Port Members:

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

Adding a New MAC-based VLAN

Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4094.

The MAC-based VLAN entry is enabled on the selected switch unit when you click on "Save". A MAC-based VLAN without any port members on any unit will be deleted when you click "Save".

The button can be used to undo the addition of new MAC-based VLANs.

Buttons:

Save – Click to save changes.

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

Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Web Interface

To display MAC-based VLAN configured in the web interface:

1. Click MAC-based VLAN Status.
2. Specify the Static NAS Combined.
3. Display MAC-based information.

Figure 3-10.6.2: The MAC-based VLAN Membership Status for User Static (GS-2310P)

MAC-based VLAN Membership Configuration for User Static		Static	Auto-refresh	Refresh									
MAC Address	VLAN ID	Port Members											
		1	2	3	4	5	6	7	8	9A	10A	9B	10B
No data exists for the user													

Parameter description:

MAC Address:

Indicates the MAC address.

VLAN ID:

Indicates the VLAN ID.

Port Members:

Port members of the MAC-based VLAN entry.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the MAC-based VLAN Membership information manually.

3.10.7 Protocol-based VLAN

This section describe Protocol-based VLAN. The Switch supports protocols including Ethernet, LLC, and SNAP.

LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Sub-network Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected switch.

Web Interface

To configure Protocol -based VLAN configuration in the web interface:

1. Click Protocol -based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Apply.

Figure 3-10.7.1: The Protocol to Group Mapping Table

3 Configuration

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add new entry

Save Reset

Protocol to Group Mapping Table Refresh

Delete	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x0800	

Add new entry

Save Reset

Parameter description:

Delete:

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.


Frame Type:

Frame Type can have one of the following values:

Ethernet

LLC

SNAP

 On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value:

Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria for three different Frame Types:

For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff

For LLC: Valid value in this case is comprised of two different sub-values. a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff)

For SNAP: Valid value in this case also is comprised of two different sub-values. a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name:

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

! Special character and underscore(_) are not allowed.

Adding a New Group to VLAN mapping entry:

Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

The button can be used to undo the addition of new entry.

Save:

Click to save changes.

Reset:

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

Refresh:

Refresh the Protocol Group Mapping information manually.

Group to VLAN

This section allows you to map an already configured Group Name to a VLAN for the selected switch.

Web Interface

To display Group Name to VLAN mapping table configured in the web interface:

1. Click Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Apply.

Figure 3-12.7.2: The Group Name of VLAN Mapping Table

The screenshot shows the 'Group Name to VLAN mapping Table' web interface. At the top right, there are 'Auto-refresh' (unchecked) and 'Refresh' buttons. The table has columns for 'Delete', 'Group Name', 'VLAN ID', and 'Port Members' (ports 1-23). The table is currently empty, and a message 'No Group entry found!' is displayed below it. Below the table are 'Add new entry', 'Apply', and 'Reset' buttons.

The screenshot shows the 'Group Name to VLAN mapping Table' web interface with one row for configuration. The 'Delete' column contains a 'Delete' checkbox. The 'Group Name' and 'VLAN ID' columns are empty text input fields. The 'Port Members' columns (ports 1-23) each contain a small square checkbox. Below the table are 'Add new entry', 'Apply', and 'Reset' buttons.

Parameter description:

Delete:

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

Group Name:

A valid Group Name is a string of at most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be used by any other existing mapping entry on this page.

3 Configuration

VLAN ID:

Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4094.

Port Members:

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

Adding a New Group to VLAN mapping entry:

Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4094. The button can be used to undo the addition of new entry.

Buttons:**Save:**

Click to save changes.

Reset:

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

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the Protocol Group Mapping information manually.

3.11 Voice VLAN

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

3.11.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be 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.

Web Interface

To configure Voice VLAN in the web interface:

1. Select "Enabled" in the Voice VLAN Configuration.
2. Specify VLAN ID, Aging Time, and Traffic Class.
4. Specify (Port Mode, Security, Discovery Protocol) in the Port Configuration
5. Click Apply.

Figure 3-11.1: The Voice VLAN Configuration (GS-2310P)

Voice VLAN Configuration

Mode	Disabled ▾
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High) ▾

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<> ▾	<> ▾	<> ▾
1	Disabled ▾	Disabled ▾	OUI ▾
2	Disabled ▾	Disabled ▾	OUI ▾
3	Disabled ▾	Disabled ▾	OUI ▾
4	Disabled ▾	Disabled ▾	OUI ▾
5	Disabled ▾	Disabled ▾	OUI ▾
6	Disabled ▾	Disabled ▾	OUI ▾
7	Disabled ▾	Disabled ▾	OUI ▾
8	Disabled ▾	Disabled ▾	OUI ▾
9A	Disabled ▾	Disabled ▾	OUI ▾
10A	Disabled ▾	Disabled ▾	OUI ▾
9B	Disabled ▾	Disabled ▾	OUI ▾
10B	Disabled ▾	Disabled ▾	OUI ▾

Parameter description:

Mode:

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

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 a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4094.

Aging Time:

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class:

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode:

Indicates the Voice VLAN port mode.

When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.

Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.