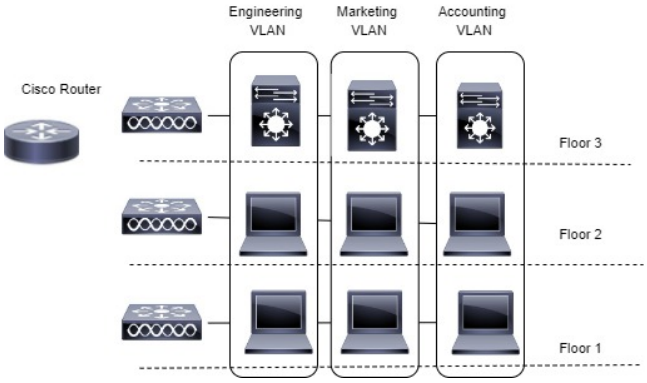
VLAN Management

This chapter contains the following sections:

An Overview of VLANs



A LAN is a group of computers or other devices in the same place – e.g. the same floor or building – that share the same physical network.

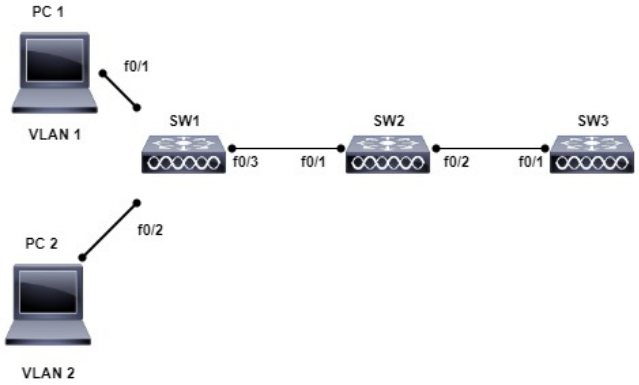
A Virtual Local Area Network (VLAN) is a logical group of ports that allows devices connected to it to communicate with one another over the Ethernet MAC layer, regardless of which physical LAN segment of the bridged network they are connected to.

By default, all switchports on the switch are in the same broadcast domain. This means when one host connected to the switch broadcasts traffic, every device connected to the switch receives that broadcast. All ports also forward multicast and unknown unicast traffic to the connected host. Large broadcast domains can result in

network congestion, and end users might complain that the network is slow. In addition to latency, there is also a greater security risk since all hosts receive all broadcasts.

There are other reasons for creating logical division. Because VLANs enable logical groupings, members do not need to be physically connected to the same switch or network segment. Some network administrators use VLANs to segregate traffic by type so that the time-sensitive traffic, like voice traffic, has priority over other traffic, such as data. Administrators also use VLANs to protect network resources. Traffic sent by authenticated clients might be assigned to one VLAN, while traffic sent from unauthenticated clients might be assigned to a different VLAN that allows limited network access. By linking devices logically instead of physically moving them, it also makes network configuration easier.

VLAN Tagging



Following IEEE 802.1Q VLAN tagging industry standard ports belong to VLAN based on the assigned VLAN tag or combination of the ingress port and packet content.

Each VLAN has a unique VLAN ID (VID) ranging from 1 to 4094. When a VLAN is created, it has no effect until it is manually or dynamically attached to at least one port. A VLAN member is a port on a switch that can send and receive data from the VLAN. When a port is added to a VLAN as an untagged member, untagged packets entering the switch are tagged with the PVID (also called the *native VLAN*) of the port but the port removes a tag to a packet in that VLAN when packets exit the port. This is commonly used when connecting single end devices such as desktop, printer etc.

Tagging may be required when a single port supports multiple devices that are members of different VLANs. For example, a single port might be connected to an IP phone and a PC (the PC is connected via port on the IP phone). IP phones are typically configured to use a tagged VLAN for voice traffic, while the PC typically uses the untagged VLAN. To order to distribute a VLAN over various physical devices and link geographically separated hosts, ports used to connect numerous infrastructure devices, such as a switch or wireless AP, must also support VLAN tagging.

A port belongs to a VLAN as a tagged member if a VLAN tag is present in every packet that is headed for that port. A port can belong to as many tagged VLANs as it wants, but only one untagged VLAN. Only one VLAN may be connected to a port that is in VLAN Access mode. The port can be a part of one or more VLANs if it is in General or Trunk mode.

VLAN Settings

The creation of a VLAN allows you to create separate broadcast domains on a switch. The broadcast domains can communicate with one another via a Layer 3 device such as a router. A VLAN is primarily used to form

groups among hosts regardless of their physical location. As a result of group formation among hosts, a VLAN improves security. When a VLAN is created, it has no effect until it is manually or dynamically attached to at least one port. One of the most common reasons for establishing a VLAN is to create a separate VLAN for voice and another for data. This directs both types of packets.

Create or Configure a VLAN

To create a VLAN or configure a VLAN on a switch, follow these steps:

Step 1 Click **VLAN Management** > **VLAN Settings**.

Step 2 Click **Add** to add one or more new VLANs.

Step 3 To create a single VLAN, select the VLAN radio button, enter the VLAN ID, and optionally the VLAN Name.

Step 4 Add the following fields for the new VLANs.

- **VLAN Interface State**- Check to enable the VLAN.
- **Link Status SNMP Traps**- Check to enable link-status generation of SNMP traps.

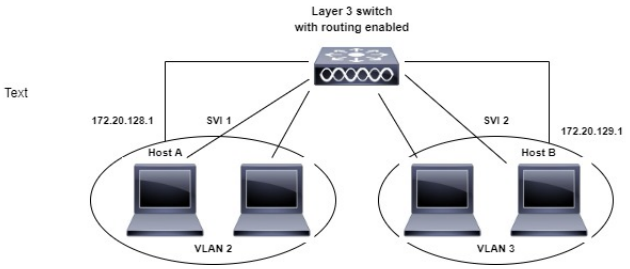
Note In the VLAN Table, the term **Originators** will be displayed which indicates how the VLAN was created.

Step 5 To add a range of VLANs, check **Range** and enter a VLAN Range (Range 2 - 4094) in the VLAN range field.

Step 6 Click **Apply** to create the VLAN(s).

Layer 3 Switching

A layer 3 switch combines a switch's and a router's capabilities. It has IP routing intelligence built into it to double as a router and acts as a switch to quickly link devices that are on the same subnet or virtual LAN. Incoming packets can be inspected, routing decisions can be made depending on source and destination addresses, and it can handle routing protocols. A layer 3 switch functions as both a switch and a router in this manner:



To setup your device as a layer 3 switch, follow these steps:

Step 1 Click **VLAN Management** > **VLAN Settings.**

Step 2 Click **Add**.

Step 3 Enter the VLAN ID and VLAN Name.

Step 4 Click **Apply** to create the VLAN.

Step 5 Next, navigate to **IPv4 Configuration >IPv4 Interface**.

Step 6 Check **Enable** to enable IPv4 Routing. This will allow routing among all Layer 3 Interfaces and will allow traffic from one VLAN to be forwarded to another VLAN.

Step 7 Click **Apply** to enable routing among all Layer 3 interfaces. This will allow traffic from one VLAN to be forwarded to another VLAN.

Interface Settings

A virtual interface that is connected to the physical network port or bond where your VLAN is configured is known as a VLAN interface. The VLAN Interface is used to automatically assign the correct VLAN ID to traffic that is routed over it.

VLAN-related parameters are displayed and configurable on the VLAN Interface Settings page. Use these steps to configure the VLAN settings:

Step 1 Click **VLAN Management** > **Interface Settings.**

Step 2 Select an interface type (Port or LAG), and click **Go**. Ports or LAGs and their VLAN parameters are displayed.

Step 3 To configure a Port or LAG, select it and click **Edit.**

Step 4 Enter the values for the following fields:

Interface	Select a Port/LAG and select or enter the port.
Switchport Mode	Select either Layer 2 or Layer 3.
Interface VLAN Mode	Select the interface mode for the VLAN. The options are: • Access—The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port. • Trunk—The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port. • General—The interface can support all functions as defined in the IEEE 802.1q specification. The interface can be a tagged or untagged member of one or more VLANs. • Customer—Selecting this option places the interface in QinQ mode. This enables you to use your own VLAN arrangements (PVID) across the provider network. The device is in Q-in-Q mode when it has one or more customer ports.
Frame Type	(Available only in General mode) Select the type of frame that the interface can receive. Frames that aren't of the configured frame type are discarded at ingress. Possible values are: • Admit All—The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames. • Admit Tagged Only—The interface accepts only tagged frames. • Admit Untagged Only—The interface accepts only untagged and priority frames.

Ingress Filtering	Select to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface isn't a member. Ingress filtering can be disabled or enabled on general ports. It's always enabled on access ports and trunk ports.

Step 5 Click **Apply**.

Port to VLAN

The Port to VLAN section displays the ports' VLAN memberships in several ways. They can be used to include or exclude members from the VLANs. Any other VLAN membership is not permitted for a port when default VLAN membership is prohibited. The port has a 4095 internal VID assigned to it.

The VLAN-aware devices must be manually setup or must dynamically learn the VLANs and their port memberships from the Generic VLAN Registration Protocol (GVRP) in order to forward packets along the path between end nodes.

When there are no intervening VLAN-aware devices between two VLAN-aware devices, their untagged port membership must belong to the same VLAN. If the ports between the two devices are to send and receive untagged packets to and from the VLAN, the PVID on those ports must match. In the absence of that, traffic may leak from one VLAN to another.

Other network devices that are VLAN-aware or VLAN-unaware can pass through frames that have been VLAN-tagged. The final VLAN-aware device must transfer untagged frames of the destination VLAN to the end node in this scenario: a destination end node that is VLAN-unaware but needs to accept traffic from a VLAN.

To view and configure the ports within a given VLAN, use the Port to VLAN page and follow the steps below.

Step 1 Click **VLAN Management** > **Port to VLAN**.

Step 2 Select a VLAN and the interface type (Port or LAG), and click **Go** to display or to change the port characteristic with respect to the VLAN.

The port mode for each port or LAG appears with its current port mode configured from the Interface Settings, on page 4.

Each port or LAG appears with its current registration to the VLAN.

The following fields are displayed:

- VLAN Mode—Displays port type of ports in the VLAN.
- Membership Type: Select one of the following options:
  - Forbidden—The interface isn't allowed to join the VLAN even from GVRP registration. When a port isn't a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
  - Excluded—The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs when the VLAN is newly created.
  - Tagged—The interface is a tagged member of the VLAN.

- Untagged—The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- Multicast TV VLAN—The interface used for Digital TV using Multicast IP The port joins the VLAN with a VLAN tag of Multicast TV VLAN.

- PVID—Select to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.

Step 3 Click **Apply**. The interfaces are assigned to the VLAN, and written to the Running Configuration file.

You can continue to display and/or configure port membership of another VLAN by selecting another VLAN ID.

Port VLAN Membership

When a VLAN is made available at an access layer switch, an end user must be able to join it. As a result, the Port VLAN Membership page displays all of the device's ports as well as the VLANs to which each port belongs.

On the VLAN to Port page, the port is denoted by an upper case P. To assign a port to one or more VLANs, follow these steps:

Step 1 Click **VLAN Management** > **Port VLAN Membership**.

Step 2 Select interface type (Port or LAG), and click **Go**. The following fields are displayed for all interfaces of the selected type:

- Interface—Port/LAG ID.
- Mode—Interface VLAN mode that was selected in the Interface Settings, on page 4.
- Administrative VLANs—Drop-down list that displays all VLANs of which the interface might be a member.
- Operational VLANs—Drop-down list that displays all VLANs of which the interface is currently a member.
- LAG—If interface selected is Port, displays the LAG in which it’s a member.

Step 3 Select a port, and click **Join VLAN** button.

Step 4 Enter the values for the following fields:

- Interface—Select a Port or LAG.
- Current VLAN Mode—Displays the port VLAN mode that was selected in the Interface Settings, on page 4.
- **Access Mode Membership (Active)**
  - Access VLAN ID—Select the VLAN from the drop-down list.
- **Trunk Mode Membership**
  - Native VLAN ID—When the port is in Trunk mode, it’s a member of this VLAN.
  - Tagged VLANs—When the port is in Trunk mode, it’s a member of these VLANs. The following options are possible:

All VLANs—When the port is in Trunk mode, it's a member of all VLANs.

User Defined—When the port is in Trunk mode, it's a member of the VLANs that are entered here.

- **General Mode Membership**
  - Untagged VLANs—When the port is in General mode, it's an untagged member of this VLAN.
  - Tagged VLANs—When the port is in General mode, it's a tagged member of these VLANs.
  - Forbidden VLANs—When the port is in General mode, the interface isn't allowed to join the VLAN even from GVRP registration. When a port isn't a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
  - General PVID—When the port is in General mode, it's a member of these VLANs.
- **Customer Mode Membership**
  - Customer VLAN ID—When the port is in Customer mode, it's a member of this VLAN.

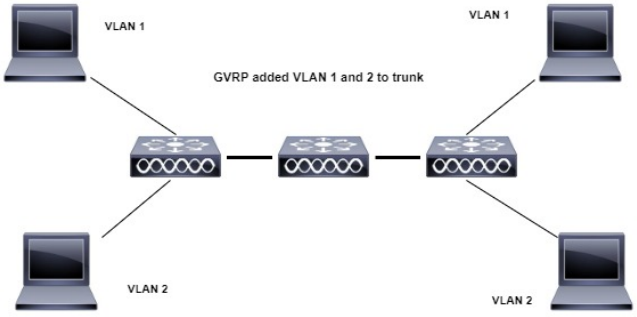
Step 5 Click **Apply**.

Step 6 Select a port and click **Details** to view the following fields:

- Interface—Select a Port or LAG.
- Administrative VLANs—Port is configured for these VLANs.
- Operational VLANs—Port is currently a member of these VLANs.

GVRP Settings

Generic VLAN Registration Protocol (GVRP) is a standards-based protocol that allows VLANs to be controlled within a larger network. GVRP adheres to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data over network trunk interconnects. This allows network devices to exchange VLAN configuration information with other devices on the fly.



GVRP must be enabled globally as well as on each port. When turned on, it sends and receives GARP Packet Data Units (GPDUs). VLANs that have been defined but are not yet active are not propagated. The VLAN must be active on at least one port in order to propagate. GVRP is disabled globally and on ports by default.

To define GVRP settings for an interface, follow these steps:

Step 1 Click **VLAN Management** > **GVRP Settings**.

Step 2 Select **GVRP Global Status** to enable GVRP globally.

Step 3 Click **Apply** to set the global GVRP status.

Step 4 Select an interface type (Port or LAG), and click **Go** to display all interfaces of that type.

Step 5 To define GVRP settings for a port, select it, and click **Edit.**

Step 6 Enter the values for the following fields:

- Interface—Select the interface (Port or LAG) to be edited.
- GVRP State—Select to enable GVRP on this interface.
- Dynamic VLAN Creation—Select to enable Dynamic VLAN Creation on this interface.
- GVRP Registration—Select to enable VLAN Registration using GVRP on this interface.

Step 7 Click **Apply**. GVRP settings are modified, and written to the Running Configuration file.

Voice VLAN

The voice VLAN feature allows IP voice traffic from an IP phone to be carried by access ports. When an IP Phone is connected to the switch, it sends voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values of 5, which are both set by default. Because uneven data transmission can degrade the sound quality of an IP phone call, the switch supports quality of service (QoS) based on IEEE 802.1p CoS. To send network traffic from the switch in a predictable manner, QoS employs classification and scheduling.

Using LLDP-MED Network rules, voice VLAN can propagate the CoS/802.1p and DSCP settings. If an appliance sends LLDP-MED packets, the LLDP-MED is set by default to respond with the Voice QoS option. The voice traffic sent by MED-supported devices must have the same CoS/802.1p and DSCP parameters as those received with the LLDP-MED response. You can use your own network settings and turn off automatic updating between Voice VLAN and LLDP-MED. The device can further set the mapping and remarking (CoS/802.1p) of the voice traffic based on the OUI when used in OUI mode.

By default, all interfaces are CoS/802.1p trusted. The device applies the quality of service based on the CoS/802.1p value found in the voice stream. For Telephony OUI voice streams, you can override the quality of service and optionally remark the 802.1p of the voice streams by specifying the desired CoS/802.1p values and using the remarking option under Telephony OUI.

Properties

Use the Voice VLAN Properties page for the following:

- View how voice VLAN is currently configured.
- Configure the VLAN ID of the Voice VLAN.
- Configure voice VLAN QoS settings.
- Configure the voice VLAN mode (Telephony OUI or Auto Voice VLAN).
- Configure how Auto Voice VLAN is triggered.

To view and configure Voice VLAN properties:

Step 1 Click **VLAN Management** > **Voice VLAN** > **Properties**.

- The voice VLAN settings configured on the device are displayed in the Voice VLAN Settings (Administrative Status) block.
- The voice VLAN settings that are actually being applied to the voice VLAN deployment are displayed in the Voice VLAN Settings (Operational Status) block.

Note Auto Smartport and Telephony OUI are mutually exclusive. CoS/802/1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.

Step 2 Enter values for the following Administrative Status fields:

- Voice VLAN ID—Enter the VLAN that is to be the Voice VLAN.

Note Changes in the voice VLAN ID, CoS/802.1p, and/or DSCP cause the device to advertise the administrative voice VLAN as a static voice VLAN. If the option Auto Voice VLAN Activation triggered by external Voice VLAN is selected, then the default values need to be maintained.

- CoS/802.1p —Select a CoS/802.1p value for the LLDP-MED as a voice network policy. Refer to Administration > Discovery > LLDP > LLDP MED Network Policy for more details.
- DSCP—Selection of DSCP values for the LLDP-MED as a voice network policy. Refer to Administration > Discovery > LLDP > LLDP MED Network Policy for more details.

The following Operational Status fields are displayed:

- Voice VLAN ID—Voice VLAN.
- CoS/802.1p —Value being used by LLDP-MED as a voice network policy. Refer to Administration > Discovery > LLDP > LLDP MED Network Policy for more details.
- DSCP—Value used by the LLDP-MED as a voice network policy.

The following Dynamic Voice VLAN Settings fields are displayed:

- Dynamic Voice VLAN—Select this field to disable or enable voice VLAN feature in one of the following ways:
  - Enable Auto Voice VLAN—Enable Dynamic Voice VLAN in Auto Voice VLAN mode.
  - Enable Telephony OUI—Enable Dynamic Voice VLAN in Telephony OUI mode.
  - Disable-Disable Auto Voice VLAN or Telephony OUI

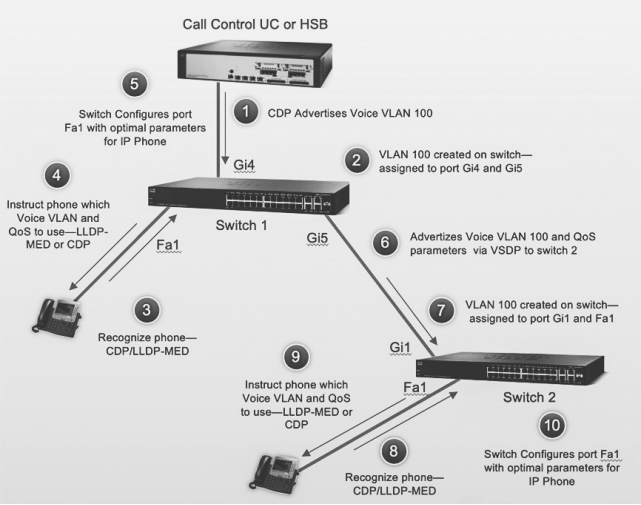
- Auto Voice VLAN Activation—If Auto Voice VLAN was enabled, select one of the following options to activate Auto Voice VLAN:
  - Immediate—Auto Voice VLAN on the device is to be activated and put into operation immediately if enabled.
  - By external Voice VLAN trigger—Auto Voice VLAN on the device is activated and put into operation only if the device detects a device advertising the voice VLAN.

  Note Manually reconfiguring the voice VLAN ID, CoS/802.1p, and/or DSCP from their default values results in a static voice VLAN, which has higher priority than auto voice VLAN.

Step 3 Click **Apply**. The VLAN properties are written to the Running Configuration file.

Auto Voice VLAN

Auto Voice VLAN is responsible to maintain the voice VLAN, but depends on Auto Smartport to maintain the voice VLAN port memberships. Auto Voice VLAN performs the following functions when it is in operation:



When activated, Auto Voice VLAN performs the following tasks:

- It finds information about voice VLANs in CDP advertisements from directly connected neighbor devices.
- If multiple neighbor switches and/or routers advertise their voice VLAN, such as Cisco Unified Communication (UC) devices, the voice VLAN from the device with the lowest MAC address is used.

If Auto Voice VLAN mode is enabled, use the Auto Voice VLAN page to view the relevant global and interface parameters.

You can also use this page to manually restart Auto Voice VLAN, by clicking **Restart Auto Voice VLAN**. After a short delay, this resets the voice VLAN to the default voice VLAN and restarts the Auto Voice VLAN discovery and synchronization process on all the switches in the LAN that are Auto Voice VLAN enabled.

Note This only resets the voice VLAN to the default voice VLAN if the Source Type is in the Inactive state.

To view Auto Voice VLAN parameters:

Step 1 Click **VLAN Management** > **Voice VLAN** > **Auto Voice VLAN**.

The Operational Status block on this page shows the information about the current voice VLAN and its source:

- Auto Voice VLAN Status—Displays whether Auto Voice VLAN is enabled.
- Voice VLAN ID—The identifier of the current voice VLAN
- Source Type—Displays the type of source where the voice VLAN is discovered by the root device.
- CoS/802.1p—Displays CoS/802.1p values to be used by the LLDP-MED as a voice network policy.
- DSCP—Displays DSCP values to be used by the LLDP-MED as a voice network policy.
- Root Switch MAC Address—The MAC address of the Auto Voice VLAN root device that discovers or is configured with the voice VLAN from which the voice VLAN is learned.
- Switch MAC Address—Base MAC address of the device. If the device's Switch MAC address is the Root Switch MAC Address, the device is the Auto Voice VLAN root device.
- Voice VLAN ID Change Time—Last time that voice VLAN was updated.

Step 2 Click **Restart Auto Voice VLAN** to reset the voice VLAN to the default voice VLAN and restart Auto Voice VLAN discovery on all the Auto-Voice-VLAN-enabled switches in the LAN.

The Voice VLAN Local Source Table displays voice VLAN configured on the device, and any voice VLAN configuration advertised by directly connected neighbor devices. It contains the following fields:

- Interface—Displays the interface on which voice VLAN configuration was received or configured. If N/A appears, the configuration was done on the device itself. If an interface appears, a voice configuration was received from a neighbor.
- Source MAC Address—MAC address of a UC from which the voice configuration was received.
- Source Type—Type of UC from which voice configuration was received. The following options are available:
  - Default—Default voice VLAN configuration on the device
  - Static—User-defined voice VLAN configuration defined on the device
  - CDP—UC that advertised voice VLAN configuration is running CDP.
  - LLDP—UC that advertised voice VLAN configuration is running LLDP.
  - Voice VLAN ID—The identifier of the advertised or configured voice VLAN
- Voice VLAN ID—The identifier of the current voice VLAN.
- CoS/802.1p—The advertised or configured CoS/802.1p values that are used by the LLDP-MED as a voice network policy.
- DSCP—The advertised or configured DSCP values that are used by the LLDP-MED as a voice network policy.

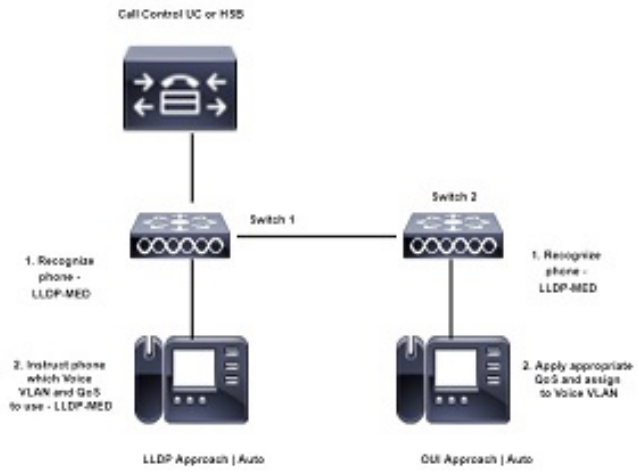
- Best Local Source—Displays whether this voice VLAN was used by the device. The following options are available:
  - Yes—The device uses this voice VLAN to synchronize with other Auto Voice VLAN-enabled switches. This voice VLAN is the voice VLAN for the network unless a voice VLAN from a higher priority source is discovered. Only one local source is the best local source.
  - No—This isn't the best local source.

Step 3 Click **Refresh** to refresh the information on the page

Telephony OUI

When traffic from Voice over Internet Protocol (VoIP) equipment is assigned to a specific VLAN made up of voice devices such as IP phones, VoIP endpoints, and voice systems, the Voice Virtual Local Area Network (VLAN) is used.The switch can detect and add port members to the Voice VLAN automatically, as well as assign the configured Quality of Service (QoS) to packets from the Voice VLAN. IP routers are required to provide communication between voice devices that are in different Voice VLANs.

Organizationally Unique Identifiers (OUI) can be used to add a specific manufacturer's Media Access Control (MAC) address to the OUI table. The first three bytes of the MAC address contain a manufacturer identifier, while the last three bytes contain a unique station ID. Once the OUIs are added to the table, any voice received from a specific IP phone on the ports of the voice VLAN ports is forwarded on the voice VLAN, provided that IP phone is listed in the OUI table



The source MAC address of a received packet is checked by the switch to determine whether it is a voice packet. The source MAC address of VoIP traffic contains a preconfigured OUI prefix. You can manually enter MAC addresses and descriptions for specific manufacturers into the OUI table. All traffic received on the Voice VLAN ports from a specific IP phone with a listed OUI is routed to the Voice VLAN.

To configure Telephony OUI and/or add a new Voice VLAN OUI follow these steps:

Step 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI**.

The Telephony OUI page contains the following fields:

- Telephony OUI Operational Status—Displays whether OUIs are used to identify voice traffic.
- CoS/802.1p—Select the CoS queue to be assigned to voice traffic.
- Remark CoS/802.1p—Select whether to remark egress traffic.
- Auto Membership Aging Time—Enter the time delay to remove a port from the voice VLAN after all of the MAC addresses of the phones detected on the ports have aged out.

Step 2 Click **Apply** to update the Running Configuration of the device with these values.

Step 3 Click **Restore Default OUIs** to delete all of the user-created OUIs, and leave only the default OUIs in the table. A pop-up will appear with the following message " All User-defined OUIs will be erased. Do you want to continue?" Click **OK**.

To delete all the OUIs, select the top checkbox. All the OUIs are selected and can be deleted by clicking **Delete**. If you then click **Restore Default OUIs**, the system recovers the known OUIs.

Step 4 To add a new OUI, click **Add.**

Step 5 Enter the values for the following fields:

- Telephony OUI—Enter a new OUI.
- Description—Enter an OUI name.

Step 6 Click **Apply**. The OUI is added to the Telephony OUI Table.

Telephone OUI Interface

The QoS attributes can be assigned per port to the voice packets in one of the following modes:

- All—Quality of Service (QoS) values configured to the Voice VLAN are applied to all of the incoming frames that are received on the interface and are classified to the Voice VLAN.
- Telephony Source MAC Address (SRC)—The QoS values configured for the Voice VLAN are applied to any incoming frame that is classified to the Voice VLAN and contains an OUI in the source MAC address that matches a configured telephony OUI.

Use the Telephony OUI Interface page to add an interface to the voice VLAN on the basis of the OUI identifier and to configure the OUI QoS mode of voice VLAN.

To configure Telephony OUI on an interface follow these steps:

Step 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI Interface**.

The Telephony OUI Interface page contains voice VLAN OUI parameters for all interfaces.

Step 2 To configure an interface to be a candidate port of the telephony OUI-based voice VLAN, click **Edit.**

Step 3 Enter the values for the following fields:

- Interface—Select a Port or LAG interface.
- Telephony OUI VLAN Membership—If enabled, the interface is a candidate port of the telephony OUI based voice VLAN. When packets that match one of the configured telephony OUI are received, the port is added to the voice VLAN.

- Voice VLAN QoS Mode (Telephone OUI QoS Mode in main page)—Select one of the following options:
  - All—QoS attributes are applied on all packets that are classified to the Voice VLAN.
  - Telephony Source MAC Address—QoS attributes are applied only on packets from IP phones.

Step 4 Click **Apply**. The OUI is added.

Auto-Surveillance VLAN

Network communication between surveillance devices such as cameras and monitoring equipment should often be given higher priority and it is important that the various devices that comprise the surveillance infrastructure in the organization are reachable for each-other. Normally, it falls to the network administrator to ensure that all surveillance devices are connected to the same VLAN and to setup this VLAN and the interfaces on it to allow for this high priority traffic.

The Auto Surveillance VLAN (ASV) feature automates aspects of this setup by detecting surveillance devices on the network, assigning them to a VLAN and setting their traffic priority.

ASV General Settings

The user defines surveillance traffic on their network by creating a list of OUIs and MAC addresses. Any traffic on interfaces with the feature enabled whose source matches one of the OUIs or MAC addresses is considered surveillance traffic. Up to 32 sources for surveillance traffic can be defined in any combination of MAC and OUIs.

Configuring ASV

When activating the feature, the users must select an existing Static VLAN to be designated as the ASV VLAN. The user then sets the CoS for traffic in this VLAN and the aging time for the VLAN membership. Finally, the ASV feature should be activated on the interfaces expected to receive surveillance traffic.

To configure the ASV general settings, follow these steps.

Step 1 Click **VLAN Management** > **Auto-Surveillance VLAN** > **ASV General Settings**.

Step 2 From the drop-down menu, select the Auto Surveillance-VLAN ID. This setting is used to select the ASV VLAN ID. If None is selected, the feature is disabled.

Step 3 Enter the CoS. This setting is used to select the Class of Service (CoS) applied to surveillance traffic on the ASV. The range is 0 - 7 and default is 5.

Step 4 For the Membership Aging Time, enter the Day(s), Hour(s) and Min(s), (Range: 1 min - 30 days: Default 1 day). This setting is used to configure the ASV membership aging time. If no surveillance traffic is received on an interface for this aging time, the interface is removed from the ASV.

Step 5 Click **Add** to add a surveillance traffic source and configure the following:

- Source Type—Select from one of the following:
  - OUI Prefix
  - MAC Address

- Source—Enter the source. The validation and hint for this field changes based on the selected Source Type. If the type is OUI Prefix, the value should be a 3 octets prefix of a unicast MAC address.

  If the type is MAC Address, the value should be a unicast MAC address and no hint should be displayed.

- Description—Provide a description for the source

Step 6 Click **Apply** to save the settings.

ASV Interface Settings

The user activates the auto surveillance feature on selected interfaces. The feature can be activated on ports or LAGs, that are in the general or access VLAN mode.

When surveillance traffic is detected on an interface with ASV enabled, this traffic is routed to the ASV. On interfaces in the general VLAN mode each surveillance traffic consumes an entry in the Resource table that is shared with the ACL and QoS rules. To view the number of consumed entries of this table go to the Hardware Resource Utilization page.

To configure the ASV interface settings, follow these steps:

Step 1 Click **VLAN Management** >**Auto-Surveillance VLAN** > **ASV Interface Settings**.

Step 2 Select the interface type Port or LAG and click **Go**.

Step 3 To edit an ASV interface setting click **Edit.**

Step 4 Next, select the interface (Port or LAG).

Step 5 Check **Enable** to enable auto surveillance VLAN membership.

Step 6 Click **Apply** to save the settings.