VLAN Management

This chapter contains the following sections:

- VLAN Settings, on page 1
- VLAN Interface Settings, on page 2
- Port to VLAN, on page 4
- Port VLAN Membership, on page 5
- VLAN Translation, on page 6
- Private VLAN Settings, on page 9
- GVRP Settings, on page 9
- VLAN Groups, on page 10
- Voice VLAN, on page 13
- Access Port Multicast TV VLAN, on page 18
- Customer Port Multicast TV VLAN, on page 19

VLAN Settings

Virtual Local Area Network (VLAN) creation allows you to make separate broadcast domains on a switch. The broadcast domains can associate with one another with the help of a Layer 3 device such as a router. A VLAN is mainly used to form groups among the hosts regardless of where the hosts are physically located. Thus, a VLAN improves security with the help of group formation among the hosts. When a VLAN is created, it has no effect until that VLAN is attached to at least one port either manually or dynamically. One of the most common reasons to set up a VLAN is to set up a separate VLAN for voice, and a separate VLAN for data. This directs the packets for both types of data despite using the same network.

To create a VLAN, follow these steps:

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

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

The page enables the creation of either a single VLAN or a range of 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-Select to enable the VLAN.

- Link Status SNMP Traps-Select to enable link-status generation of SNMP traps.

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).

VLAN Interface Settings

The VLAN Interface Settings page displays and enables configuration of VLAN-related parameters.

To configure the VLAN settings, follow these steps:

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

Step 2 Select a Global Ethertype Tagging method for the S-VLAN tag.

- Dot1q-8100
- Dot1ad-88a8
- 9100
- 9200

Step 3 Select an interface type (Port or LAG), and click **Go**. Ports or LAGs and their VLAN parameters are displayed.

Step 4 To configure a Port or LAG, select it and click **Edit.**

Step 5 Enter the values for the following fields:

Interface	Select a Port/LAG.
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. • Private VLAN—Host—Select to set the interface as either isolated or community. Then select either an isolated or community VLAN in the Secondary VLAN - Host field. • Private VLAN—Promiscuous—Select to set the interface as promiscuous. • VLAN Mapping—Tunnel—Select to set the interface as a VLAN tunnel edge port. • VLAN Mapping—One to One—Select to set the interface as to be used as a VLAN mapping one to one edge port.
Ethertype Tagging	Select an Ethertype tagging method for the S-VLAN tag (see the Global Ethertype Tagging field above).
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	Available only in General mode) 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.
Primary VLAN	Select the primary VLAN in the private VLAN. The primary VLAN is used to allow Layer 2 connectivity from promiscuous ports to isolated ports and to community ports. If None is selected if the interface isn't in private VLAN mode.
Secondary VLAN Host	Select an isolated or community VLAN for those hosts that only require a single secondary VLAN

Available Secondary VLANs to Selected Secondary VLANs	For promiscuous ports, move all secondary VLANs that are required for normal packet forwarding from the Available Secondary VLANs. Promiscuous and trunk ports can be members in multiple VLANs

Step 6 Click **Apply**.

Port to VLAN

The Port to VLAN and pages displays the VLAN memberships of the ports in various presentations. You can use them to add or remove memberships to or from the VLANs.

When a port is forbidden default VLAN membership, that port isn't allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port.

To forward packets, the VLAN-aware devices that carry VLAN traffic along the path between end nodes must be manually configured or must dynamically learn the VLANs and their port memberships from the Generic VLAN Registration Protocol (GVRP).

Untagged port membership between two VLAN-aware devices with no intervening VLAN-aware devices, must be to the same VLAN. The PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.

Frames that are VLAN-tagged can pass through other network devices that are VLAN-aware or VLAN-unaware. If a destination end node is VLAN-unaware, but is to receive traffic from a VLAN, then the last VLAN-aware device, must send frames of the destination VLAN to the end node untagged.

Use the Port to VLAN page to display and configure the ports within a specific VLAN.

To map ports or LAGs to a VLAN, follow these steps:

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 VLAN Interface Settings, on page 2.

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 MTV 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

The Port VLAN Membership page displays all ports on the device along with a list of VLANs to which each port belongs. If the port-based authentication method for an interface is 802.1x and the Administrative Port Control is Auto, then:

- Until the port is authenticated, it's excluded from all VLANs, except guest and unauthenticated ones. In the VLAN to Port page, the port is marked with an upper case P.
- When the port is authenticated, it receives membership in the VLAN in which it was configured.

Note VLAN IS mode is supported. This means that port VLAN membership can be configured ahead of time for various VLAN modes. When the port is put into the specific VLAN mode, the configuration becomes active.

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 VLAN Interface Settings, on page 2.
- 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**.

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 VLAN Interface Settings, on page 2.
- Access Mode Membership (Active)
  - Access VLAN ID—Select the VLAN from the drop-down list.
  - Multicast TV VLAN—Select the multicast TV 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.
  - Customer Multicast VLANs—When the port is in Customer mode, it's a member of this Multicast TV VLAN.

Step 5 Select a port and click **Details** to view the following fields:

- Administrative VLANs—Port is configured for these VLANs.
- Operational VLANs—Port is currently a member of these VLANs.

Click **Apply** (for Join VLAN). The settings are modified and written to the Running Configuration file.

VLAN Translation

VLAN Translation is sometimes referred to when the same forwarding domain includes several different VLANS. Therefore, a frame ingressing an interface with a certain VLAN ID can be forwarded to another port with another VLAN ID.

VLAN Mapping

To configure a VLAN mapping, follow these steps:

Step 1 Click **VLAN Management** > **VLAN Translation** > **VLAN Mapping**.

A table of previously defined VLAN mappings setting is displayed.

Step 2 Select one of the following mapping types:

- One to One—Select this option to display and edit settings of the interface set to one-to-one VLAN mapping mode.
- Tunnel Mapping—Select this option to display and edit settings of the interface set to Tunnel VLAN mapping mode.

Step 3 Click **Add** and enter the following fields:

- Interface—Select the port.
- Interface VLAN Mode—Displays the current interface mode.
- Mapping Type—Select one of the following:
  - One to One—Select this option to define one-to-one VLAN mapping settings.
  - Tunnel Mapping—Select this option to define tunnel VLAN mapping settings.
- One to One Translation—This option is available if you selected the one-to-one option in Mapping Type selection. Select one of the following:
  - Source VLAN—Configure the ID of the customer VLAN (C-VLAN) that will be translated to S-VLAN (translated VLAN).
  - Translated VLAN—Configure the S-VLAN that replaces the specified C-VLAN.
- Tunnel Mapping—This option is available if you selected the Tunnel Mapping option in the Mapping Type selection. Select one of the following:
  - Customer VLAN—Select **Default** to define the required action for C-VLANs not specified or VLAN List to specifically define VLAN tunnel behavior for listed VLANs.
  - Tunneling—Select **Drop** or Outer VLAN ID If Outer VLAN ID is selected, enter the VLANs.

Step 4 Click **Apply**. The parameters are written to the Running Configuration file.

Protocol Handling

Note In order to configure per-interface protocol handling behavior, Hardware Resources must be allocated to the VLAN Mapping feature.

To configure the handling of L2CP PDUs received on a VLAN translation tunnel edge port, follow these steps:

Step 1 Click **VLAN Management** > **VLAN Translation** > **Protocol Handling**.

Note In order to configure per-interface protocol handling behavior, hardware resources must be allocated to the VLAN Mapping feature.

Step 2 Optionally, set the Default Tunneling CoS: enter a value between 0-7 (default=5) to define a global CoS value to apply to L2CP PDUs which are forwarded and encapsulated on VLAN tunneling edge ports. This value is used for all interfaces that do not have specific user CoS settings.

Step 3 Select one of the entries listed and click **Copy Settings** to copy the settings in the selected entry to one or more entries. Click **Edit** to edit the selected entry.

Step 4 Enter the following fields.

- Interface—Select the port.
- Interface VLAN Mode—Displays the current interface VLAN mode
- BPDU VLAN ID—Select one of the following:
  - None—there is no VLAN selected for L2CP BPDU tunneling. Use this selection to disable tunneling L2CP PDUs.
  - vlan-id—one of the VLAN IDs configured on device - select one of the available VLAN IDs to use for tunneling L2CP PDUs on this interface.
- CoS—Select one of the following:
  - Use Default—Select this to use the global default value
  - User Defined—Select this option set a value between 0-7.
- Drop Threshold—Select one of the following:
  - None—Select this to disable the drop threshold.
  - User Defined—Select this option to set the drop threshold. Valid values are between 8-256 Kbps (default is 32Kbps).
- Protocol Forwarding—Check the protocols that the device will forward and encapsulate:
  - CDP —Check to enable forwarding and encapsulating this protocol.
  - LLDP —Check to enable forwarding and encapsulating this protocol
  - STP —Check to enable forwarding and encapsulating this protocol.
  - VTP —Check to enable forwarding and encapsulating this protocol.

Step 5 Click **Apply**. The parameters are written to the Running Configuration file.

Private VLAN Settings

The Private VLAN feature provides layer-2 isolation between ports. This means that at the level of bridging traffic, as opposed to IP routing, ports that share the same Broadcast domain cannot communicate with each other. The ports in a private VLAN can be located anywhere in the layer 2 network, meaning that they do not have to be on the same switch. The private VLAN is designed to receive untagged or priority-tagged traffic and transmit untagged traffic.

Note Interface membership in the Private VLANs is configured on the VLAN Interface Settings, on page 2. Use Private VLAN—Host interface mode for Community and Isolated VLANs, or Private VLAN—Promiscuous interface mode for Primary VLAN.

To create a new private VLAN, follow these steps:

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

Step 2 Click **Add**.

Step 3 Enter the values for the following fields:

- Primary VLAN ID—Select a VLAN to be defined as the primary VLAN in the private VLAN. The primary VLAN is used to allow Layer 2 connectivity from promiscuous ports to isolated ports and to community ports.
- Isolated VLAN ID—An isolated VLAN is used to allow isolated ports to send traffic to the primary VLAN.
- Available Community VLANs—Move the VLANs that you want to be community VLANs to the Selected Community VLANs list. Community VLANs allow Layer 2 connectivity from community ports to promiscuous ports and to community ports of the same community. This is called Community VLAN Range on the main page.

Step 4 Click **Apply**. The settings are modified and written to the Running Configuration file.

GVRP Settings

Adjacent VLAN-aware devices can exchange VLAN information with each other by using the Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

GVRP must be activated globally and on each port. When it's activated, it transmits and receives GARP Packet Data Units (GPDUs). VLANs that are defined but not active aren't propagated. To propagate the VLAN, it must be up on at least one port. By default, GVRP is disabled globally and on ports.

To define GVRP settings for an interface:

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.

VLAN Groups

VLAN groups are used for load balancing of traffic on a Layer 2 network. Packets are assigned a VLAN according to various classifications.

If several classifications schemes are defined, packets are assigned to a VLAN in the following order:

- TAG—If the packet is tagged, the VLAN is taken from the tag.
- MAC-Based VLAN—If a MAC-based VLAN has been defined, the VLAN is taken from the source MAC-to-VLAN mapping of the ingress interface.
- Subnet-Based VLAN—If a subnet-based VLAN has been defined, the VLAN is taken from the source IP-to-VLAN mapping of the ingress interface.
- Protocol-Based VLAN—If a protocol-based VLAN has been defined, the VLAN is taken from the (Ethernet type) protocol-to-VLAN mapping of the ingress interface.
- PVID—VLAN is taken from the port default VLAN ID.

MAC-Based Groups

MAC-based VLAN classifications enable packets to be classified by their source MAC address. You can then define MAC-to-VLAN mapping per interface. You can define several MAC-based VLAN groups, which each group containing different MAC addresses. These MAC-based groups can be assigned to specific ports/LAGs. MAC-based VLAN groups can’t contain overlapping ranges of MAC addresses on the same port.

To assign a MAC address to a VLAN Group, complete the following steps:

Step 1 Click **VLAN Management** > **VLAN Groups** > **MAC-Based Groups**.

Step 2 Click **Add.**

Step 3 Enter the values for the following fields:

- MAC Address—Enter a MAC address to be assigned to a VLAN group.

  Note This MAC address can’t be assigned to any other VLAN group.

- Prefix Mask—Enter one of the following:
  - Host(48)—To include all bits of MAC address in the prefix mask (48 bits)
  - Length—Prefix of the MAC address
- Group ID—Enter a user-created VLAN group ID number.

Step 4 Click **Apply**. The MAC address is assigned to a VLAN group.

MAC-Based Groups to VLAN

To assign a MAC-based VLAN group to a VLAN on an interface, complete the following:

Step 1 Click **VLAN Management** > **VLAN Groups** > **MAC-Based Groups to VLAN.**

Step 2 Click **Add.**

Step 3 Enter the values for the following fields:

- Group Type—Displays that the group is MAC-Based.
- Interface—Enter a general interface (port/LAG) through which traffic is received.
- Group ID—Select a VLAN group.
- VLAN ID—Select the VLAN to which traffic from the VLAN group is forwarded.

Step 4 Click **Apply** to set the mapping of the VLAN group to the VLAN. This mapping does not bind the interface dynamically to the VLAN; the interface must be manually added to the VLAN.)

Subnet-Based Groups

The subnet-based group VLAN classification enable packets to be classified according to their subnet. You can then define subnet-to-VLAN mapping per interface. You can define several subnet-based VLAN groups, which each group containing different subnets.

These groups can be assigned to specific ports/LAGs. Subnet-based VLAN groups cannot contain overlapping ranges of subnets on the same port.

To add a subnet-based group, complete the following steps:

Step 1 Click **VLAN Management** > **VLAN Groups** > **Subnet-Based Groups**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- IP Address—Enter the IP address on which the subgroup is based.
- Prefix Mask—Enter the prefix mask that defines the subnet.

- Group ID—Enter a group ID.

Step 4 Click **Apply**. The group is added, and written to the Running Configuration file.

Subnet-Based Groups to VLAN

To map a subnet group to a port, the port must not have DVA configured on it (see VLAN Interface Settings, on page 2). Several groups can be bound to a single port, with each port being associated to its own VLAN. It is possible to map several groups to a single VLAN as well.

To map the subnet group to a VLAN, follow these steps:

Step 1 Click **VLAN Management** > **VLAN Groups** > **Subnet-Based Groups to VLAN.**

Step 2 To associate an interface with a protocol-based group and VLAN, click **Add.**

The Group Type field displays the type of group being mapped.

Step 3 Enter the following fields.

- Interface—Port or LAG number assigned to VLAN according to protocol-based group.
- Group ID—Protocol group ID.
- VLAN ID—Attaches the specified group for this interface to a user-defined VLAN ID.

Step 4 Click **Apply**. The subnet-based group ports are mapped to VLANs, and written to the Running Configuration file.

Protocol-Based Groups

Groups of protocols can be defined and then bound to a port. After the protocol group is bound to a port, every packet originating from a protocol in the group is assigned the VLAN that is configured in the Protocol-Based Groups page. To define a set of protocols, follow these steps.

Step 1 Click **VLAN Management** > **VLAN Groups** > **Protocol-Based Groups**.

Step 2 Click **Add** to add a protocol-based VLAN group.

Step 3 Enter the following fields:.

- Encapsulation—Protocol Packet type. The following options are available:
  - Ethernet V2—If this is selected, select the Ethernet Type.
  - LLC-SNAP (rfc1042)—If this is selected, enter the Protocol Value.
  - LLC—If this is selected, select the DSAP-SSAP Values.
- Ethernet Type—Select the Ethernet type for Ethernet V2 encapsulation. This is the two-octet field in the Ethernet frame used to indicate which protocol is encapsulated in the payload of the Ethernet packet) for the VLAN group.

- Protocol Value—Enter the protocol for LLC-SNAP (rfc 1042) encapsulation.
- Group ID—Enter a protocol group ID.

Step 4 Click **Apply**. The Protocol Group is added, and written to the Running Configuration file.

Protocol-Based Groups to VLAN

Protocol-based VLANs divide the physical network into logical VLAN groups for each protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type. Several groups can be bound to a single port, with each port being associated to its own VLAN. It's possible to map several groups to a single VLAN as well.

To map the protocol port to a VLAN, follow these steps:

Step 1 Click **VLAN Management** > **VLAN Groups** > **Protocol-Based Groups to VLAN.**

Step 2 To associate an interface with a protocol-based group and VLAN, click **Add.**

The Group Type field displays the type of group being mapped.

Step 3 Enter the following fields.

- Interface—Port or LAG number assigned to VLAN according to protocol-based group.
- Group ID—Protocol group ID.
- VLAN ID—Attaches the interface to a user-defined VLAN ID.

Step 4 Click **Apply**. The protocol ports are mapped to VLANs, and written to the Running Configuration file.

Voice VLAN

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to an IP Phone, the phone sends voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values, which are both set to 5 by default. Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS) based on IEEE 802.1p CoS. QoS uses classification and scheduling to send network traffic from the switch in a predictable manner.

Voice VLAN can propagate the CoS/802.1p and DSCP settings by using LLDP-MED Network policies. The LLDP-MED is set by default to response with the Voice QoS setting if an appliance sends LLDP-MED packets. MED-supported devices must send their voice traffic with the same CoS/802.1p and DSCP values, as received with the LLDP-MED response.You can disable the automatic update between Voice VLAN and LLDP-MED and use your own network polic ies. Working with the OUI mode, the device can additionally configure the mapping and remarking (CoS/802.1p) of the voice traffic based on the OUI.

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.

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

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

OUIs are assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. Since the number of IP phone manufacturers is limited and well-known, the known OUI values cause the relevant frames, and the port on which they are seen, to be automatically assigned to a Voice VLAN. Use the Telephony OUI page to configure Telephony OUI QoS properties. In addition, the Auto Membership Aging time can be configured. If the specified time period passes with no telephony activity, the port is removed from the Voice VLAN.

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

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.

The Telephony OUI table appears:

- Telephony OUI—First six digits of the MAC address that are reserved for OUIs.
- Description—User-assigned OUI description.

Step 3 Click **Restore Default OUIs** to delete all of the user-created OUIs, and leave only the default OUIs in the table. The OUI information may not be accurate until the restoration is completed. This may take several seconds. After several seconds have passed, refresh the page by exiting it and reentering it.

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:

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 an 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.

Access Port Multicast TV VLAN

Multicast TV VLANs enable Multicast transmissions to subscribers who are not on the same data VLAN (Layer 2-isolated), without replicating the Multicast transmission frames for each subscriber VLAN.

Subscribers, who are not on the same data VLAN (Layer 2-isolated) and are connected to the device with different VLAN ID membership, can share the same Multicast stream by joining the ports to the same Multicast VLAN ID.

The network port, connected to the Multicast server, is statically configured as a member in the Multicast VLAN ID.

The network ports, which through subscribers communicate with the Multicast server (by sending IGMP messages), receive the Multicast streams from the Multicast server, while including the Multicast TV VLAN in the Multicast packet header. For this reasons, the network ports must be statically configured as the following:

- Trunk or general port type (see VLAN Interface Settings, on page 2)
- Member of the Multicast TV VLAN

The subscriber receiver ports can be associated with the Multicast TV VLAN only if it is defined as an access port.

One or more IP Multicast address groups can be associated with the same Multicast TV VLAN.

Any VLAN can be configured as a Multicast-TV VLAN. A port assigned to a Multicast-TV VLAN:

- Joins the Multicast-TV VLAN.
- Packets passing through egress ports in the Multicast TV VLAN are untagged.
- The port's Frame Type parameter is set to Admit All, allowing untagged packets (see VLAN Interface Settings, on page 2).

The Multicast TV VLAN configuration is defined per port. Customer ports are configured to be member of Multicast TV VLANs using the Port Multicast VLAN Membership page.

Multicast Group to VLAN

You can map up to 256 ranges of IPv4 addresses to a Multicast TV VLAN. In each range, you can configure the full scope of Multicast addresses.

Note An * indicates that the corresponding Multicast Group is inactive because the associated Multicast TV VLAN does not exist. Go to the VLAN Settings, on page 1 to create the VLAN.

To define the Multicast TV VLAN configuration, follow these steps:

Step 1 Click **VLAN Management** > **Access Port Multicast TV VLAN** > **Multicast Group to VLAN**.

Step 2 Click **Add** to associate a Multicast group to a VLAN. Any VLAN can be selected.

Enter the following fields:

- Multicast TV VLAN-VLAN to which the Multicast packets are assigned. When a VLAN is selected here, it becomes a Multicast TV VLAN.
- Multicast Group Start-First IPv4 address of the Multicast group range.
- Group Definition-Select one of the following range options:
  - By group size-Specify the number of Multicast addresses in the group range.
  - By range-Specify an IPv4 Multicast address greater than the address in the Multicast Group Start field. This is the last address of the range.

Step 3 Click **Apply**. Multicast TV VLAN settings are modified, and written to the Running Configuration file.

Port Multicast TV VLAN Membership

To define the Multicast TV VLAN configuration:

Step 1 Click **VLAN Management** > **Access Port Multicast TV VLAN** > **Port Multicast VLAN Membership**.

Step 2 Select a VLAN from Multicast TV VLAN.

Step 3 Select an interface from Interface Type.

Step 4 The Candidate Access Ports list contains all access ports configured on the device. Move the required ports to the Member Access Ports field.

Step 5 Click **Apply**. Multicast TV VLAN settings are modified, and written to the Running Configuration file.

Customer Port Multicast TV VLAN

A triple play service provisions three broadband services, over a single broadband connection:

- High-speed Internet access
- Video
- Voice

The triple play service is provisioned for service provider subscribers, while keeping Layer 2-isolation between them.

Each subscriber has a CPE MUX box. The MUX has multiple access ports that are connected to the subscriber's devices (PC, telephone and so on), and one network port that is connected to the access device.

The box forwards the packets from the network port to the subscriber's devices based on the VLAN tag of the packet. Each VLAN is mapped to one of the MUX access ports.

Packets from subscribers to the service provider network are forwarded as VLAN tagged frames, in order to distinguish between the service types, which mean that for each service type there is a unique VLAN ID in the CPE box.

All packets from the subscriber to the service provider network are encapsulated by the access device with the subscriber’s VLAN configured as customer VLAN (Outer tag or S-VID), except for IGMP snooping messages from the TV receivers, which are associated with the Multicast TV VLAN. VOD information that is also sent from the TV receivers are sent like any other type of traffic.

Packets from the service provider network that received on the network port to the subscriber are sent on the service provider network as double tag packets, while the outer tag (Service Tag or S-Tag) represent one of the two type of VLAN as following:

- Subscriber’s VLAN (Includes Internet and IP Phones)
- Multicast TV VLAN

The inner VLAN (C-Tag) is the tag that determines the destination in the subscriber’s network (by the CPE MUX).

CPE VLAN to VLAN

To support the CPE MUX with subscribers VLANs, subscribers may require multiple video providers, and each provider is assigned a different external VLAN.

CPE (internal) Multicast VLANs must be mapped to the Multicast provider (external) VLANs.

After a CPE VLAN is mapped to a Multicast VLAN, it can participate in IGMP snooping.

To map CPE VLANs, follow these steps:

Step 1 Click **VLAN Management** > **Customer Port Multicast TV VLAN** > **CPE VLAN to VLAN.**

Step 2 Click **Add**.

Step 3 Enter the following fields:

- CPE VLAN-Enter the VLAN defined on the CPE box.
- Multicast TV VLAN-Select the Multicast TV VLAN which is mapped to the CPE VLAN.

Step 4 Click **Apply**. CPE VLAN Mapping is modified, and written to the Running Configuration file.

Port Multicast VLAN Membership

The ports associated with the Multicast VLANs must be configured as customer ports (see VLAN Interface Settings, on page 2).

To map ports to Multicast TV VLANs, follow these steps, follow these steps:

Step 1 Click **VLAN Management** > **Customer Port Multicast TV VLAN** > **Port Multicast VLAN Membership**.

Step 2 Select a VLAN from Multicast TV VLAN.

Step 3 Select an interface from Interface Type.

Step 4 The Candidate Customer Ports list contains all access ports configured on the device. Move the required ports to the Member Customer Ports field.

Step 5 Click **Apply**. The new settings are modified, and written to the Running Configuration file.