VLAN Management

This chapter contains the following sections:

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:

Procedure

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:

Procedure

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:

Procedure

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. **Note** When using GVRP enabled port, make sure that the Interface VLAN mode is set to "General". • 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.
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 isn't 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 set up 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 following steps.

Procedure

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 regarding the VLAN.

The port mode for each port or LAG appears with its current port mode configured from the 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 an 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:

Procedure

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 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** 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 2.
- **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.

VLAN Translation

VLAN translation involves replacing an ingress tag with another and vice-versa pn egress. It is used on an interface to configure a set of VLAN translation rules. When these rules are applied, VLAN-IDs in that interface's incoming and outgoing packets are mapped to the appropriate VLAN-IDs from the translation rules. This configuration is useful when the VLAN identifiers on the frames need to be changed at the interface.

VLAN Tunneling One-to-One

VLAN tunneling is a feature that extends the QinQ/Nested VLAN/Customer mode VLAN functionality. It enables service providers to support customers with multiple VLANs using a single VLAN while preserving customer VLAN IDs and segregating traffic in different customer VLANs. Packets that enter the tunnel port on the service-provider edge switch, which are already 802.1Q-tagged with the appropriate VLAN IDs, are encapsulated with another layer of an 802.1Q tag that contains a VLAN ID that is unique to the customer.

The original 802.1Q tag from the customer is preserved in the encapsulated packet. Therefore, packets that enter the service-provider infrastructure are double-tagged.

This feature is known as "double tagging" or QinQ, because the switch adds a second ID tag known as a Service Tag (S-VLAN) in addition to the regular 802.1Q tag (Customer VLAN/C-VLAN) to forward traffic over the network. C-VLANs are mapped to S-VLANs on an edge interface, which is an interface where a customer network connects to the provider edge switch, and the original C-VLAN tags are kept as part of the payload. Untagged frames are eliminated.

The initial C-VLAN-ID of a frame is mapped to another layer of S-VLAN tag when it is delivered across a non-edge tagged interface. As a result, packets broadcast on frames with non-edge interfaces have two tags: an outside S-VLAN tag and an inside C-VLAN tag. While traffic is forwarded across the network service provider's infrastructure, the Service VLAN Tag is kept intact. When a frame is sent out on an edge interface of an egress device, the S-VLAN tag is removed. Frames without tags are dropped.

The VLAN tunneling feature offers the following capability over and above the basic QinQ/Nested VLAN implementation by using a separate set of commands:

- Provides, per edge interface, multiple mappings of different C-VLANs to separate S-VLANs
- Allows configuring a drop action for certain C-VLANs received on edge interfaces
- Allows configuring the action for C-VLANs not specifically mapped to an S-VLAN (drop or map to certain S-VLANs)
- Allows configuring, globally and per NNI interface (network node interfaces – backbone ports) the Ethertype of the S-VLAN tag. In the previous QinQ implementation, only the Ethertype of 0x8100 was supported for a S-VLAN tag.

The S-VLAN specified by the user must be created on the device before configuring it on an interface as an S-VLAN. If this VLAN does not exist, the command fails.

IPv4/IPv6 forwarding and VLAN tunneling are mutually exclusive. Meaning that if either IPv4 or IPv6 forwarding are enabled, an interface cannot be set to VLAN tunneling mode. And if any interface is set to VLAN tunneling mode, IPv4 and IPv6 forwarding cannot be enabled on that device.

The following features are also mutually exclusive with the VLAN tunneling feature:

- Auto Voice VLAN
- Auto Smartport
- Voice VLAN

IPv4 and IPv6 interfaces cannot be defined on VLANs containing edge interfaces.

VLAN Translation

The following Layer 2 features are not supported on VLANs containing edge interfaces:

- IGMP/MLD snooping
- DHCP Snooping
- IPv6 First Hop Security

The following protocols cannot be enabled on edge interfaces (UNI - user network interfaces):

- STP

- GVRP

The following features are not supported on edge interfaces (UNI - user network interfaces):

- RADIUS VLAN assignment
- 802.1x VLAN
- SPAN/RSPAN – As a destination port with the network keyword or as a reflector port destination port with the network keyword or reflector port.

Applying VLAN tunneling on an interface requires the use of router TCAM rules. If there is not a sufficient number of router TCAM resources, the command will fail. Users can add/remove router TCAM resources allocation for VLAN tunneling (and mapping) purposes via the **Administration**> **Routing Resources** (this requires a system reboot).

The original QinQ implementation (customer mode-related commands) continues to exist alongside the new implementation of VLAN tunneling. The customer port mode is a particular case of VLAN-mapping tunnel port mode, and does not require allocation of TCAM resources.

Layer 2 Control Protocol (L2CP) BPDU Tunneling

By default, input L2 PDUs with the following destination MAC addresses are dropped (and not processed) on VLAN tunnel edge ports:

- 01:80:C2:00:00:00-01:80:C2:00:00:FF (with the exception of LACP frames (destination MAC 01:80:C2:00:00:02) which are processed and not dropped)
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF

As part of the VLAN tunnel settings you can define if to drop, or forward and encapsulate the following Layer 2 Control Protocol PDUs - CDP, LLDP, VTP and STP. This is known as L2CP tunneling. This feature creates a tunnel which enables forwarding specific untagged Layer 2 Protocol frames over a provider network (tagged frames are dropped). The feature is configured on a VLAN mapping interface. The L2CP tunneling feature is useful when connecting 2 customer sites on different sides of the provider network. This feature enables transferring packets of supported protocols across the ISP cloud between the 2 sites.

In order to tunnel such frames you need to define the VLAN which will be used as the VLAN ID (2nd tag) when the PDUs are forwarded across provider network. When PDUs are received on the remote customer site - the outer VLAN is stripped and the PDUs are processed on the remote customer network as if they were originated on that network. In addition to enabling per-interface L2CP tunnel forwarding, this feature also enables you to assign the S-VLAN to use for the encapsulation, the pre-defined CoS value for this traffic, and rate-limit the L2CP PDUs that the interface forwards.

VLAN Mapping One-to-One

The device supports VLAN one-to-one mapping in addition to VLAN tunneling. In VLAN one-to-one mapping, C-VLANs are mapped to S-VLANs on an edge interface (an edge interface is an interface where a customer network connects to the provider edge switch), and the original C-VLAN tags are replaced by the specified S-VLAN. Untagged frames are eliminated. When a frame is sent over a non-edge tagged interface, it contains only one VLAN tag, that of the specified S-VLAN. The Service VLAN Tag is preserved while traffic is routed through the infrastructure network of the service provider. When a frame is sent to an edge interface, the S-VLAN tag on the egress device is replaced with the C-VLAN tag. In the one-to-one VLAN-mapping mode, an interface belongs to all S-VLANs for which mapping is defined as an egress-tagged interface. The PVID of the interface is set to 4095.

VLAN Mapping

A backbone network can connect two Layer 2 user networks in the same VLAN. The two user networks must interoperate seamlessly in order to ensure Layer 2 connectivity between users and to uniformly deploy Layer 2 protocols. However, because the VLAN plans on the backbone and user networks differ, the backbone network cannot directly transmit VLAN packets from the user networks. Configure VLAN mapping to solve this issue. When VLAN packets from a user network enter the backbone network, a backbone network edge device changes the customer VLAN (C-VLAN) ID to the service VLAN (S-VLAN ID).

The device reverses the VLAN ID change after the packets have been transmitted. This ensures that the two user networks communicate seamlessly.

To configure a VLAN mapping, follow these steps:

Procedure

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

Different Layer 2 protocols must be used by customers at various sites connected by a service provider network in order to scale their topologies to encompass both local and remote sites. Every VLAN should establish a good spanning tree that includes the local site and any remote sites over the service-provider network, and STP must function correctly. Cisco equipment nearby must be found by the Cisco Discovery Protocol (CDP) from both local and remote sites. All sites in the customer network that are taking part in VTP must have a consistent VLAN configuration thanks to the VLAN Trunking Protocol (VTP).

When protocol tunneling is enabled, inbound service-provider switches encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. These packets are not processed by network core switches, but are instead forwarded as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP traverse the service-provider network and are delivered to customer switches on the service-provider network's outbound side.

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

Procedure

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

Different Layer 2 protocols must be used by customers at various sites connected by a service provider network in order to scale their topologies to encompass both local and remote sites. Every VLAN should establish a good spanning tree that includes the local site and any remote sites over the service-provider network, and STP must function correctly. Cisco equipment nearby must be found by the Cisco Discovery Protocol (CDP) from both local and remote sites. All sites in the customer network that are taking part in VTP must have a consistent VLAN configuration thanks to the VLAN Trunking Protocol (VTP).

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

Step 2 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—select a VLAN ID 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 0–7.

- Drop threshold—Select one of the following:
  - None—Select to disable the drop threshold.
  - User defined—Select to set threshold 8–256 Kbps (default is 32Kbps).

- Protocol Forwarding—Check the protocols that the device forwards 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

To separate the ports on the switch from one another, a private VLAN divides the Ethernet broadcast domain of a VLAN into sub domains. A principal VLAN and one or more subsidiary VLANs make up a sub domain. The primary VLAN is shared by all VLANs in a private VLAN domain. One sub domain can be distinguished from another using the secondary VLAN ID.

The Private VLAN feature provides layer-2 isolation between ports. This means that, unlike IP routing, ports in the same Broadcast domain cannot communicate with each other at the level of bridging traffic. A private VLAN's ports can be located anywhere in the layer 2 network, which means they don't have to be on the same switch. The private VLAN is intended to receive untagged or priority-tagged traffic and to transmit untagged traffic.

To create a new private VLAN, follow these steps:

Procedure

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

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:

Procedure

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

A VLAN group is a logical grouping of tagged or untagged VLANs. If a VLAN is tagged, each packet sent to and received from that VLAN contains a VLAN ID. Network traffic can include both tagged and untagged packets. If a packet does not have a VLAN tag, it is sent to an untagged VLAN.

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

The MAC-based VLAN classification classifies packets based on their source MAC address. Then, for each interface, you can define MAC-to-VLAN mapping. You can also define multiple MAC-based VLAN groups, each with its own set of MAC addresses. Specific ports or LAGs can be assigned to these MAC-based groups. MAC-based VLAN groups cannot have overlapping MAC address ranges on the same port.

To forward packets based on the MAC addresses of the devices, groups of MAC addresses must be created and then mapped to VLANs. Up to 256 MAC addresses, host or range, can be configured and mapped to one or more MAC-based VLAN groups.

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

Procedure

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:

Procedure

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:

Procedure

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 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:

Procedure

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.

Procedure

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:

Procedure

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 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:

Procedure

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:

Procedure

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 or disabled.
- 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:

Procedure

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:

Procedure

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.

Procedure

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:

Procedure

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.

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 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 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:

Procedure

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

Multicast TV VLANs allow multicast transmissions to subscribers who are not on the same data VLAN (Layer 2-isolated) without having to replicate the Multicast transmission frames for each subscriber VLAN. To define the Multicast TV VLAN configuration:

Procedure

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

Mapping CPE VLANs to Multicast TV VLANs

Subscribers may require multiple video providers to support the CPE MUX with their VLANs, and each provider is assigned a different external VLAN. CPE Multicast VLANs (internal) must be mapped to Multicast provider (external) VLANs. After mapping a CPE VLAN to a Multicast VLAN, it can participate in IGMP snooping.

To map CPE VLANs, follow these steps:

Procedure

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 Interface Settings, on page 2).

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

Procedure

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.