Contents

1 Configuring Voice VLAN

1.1 Introduction

1.1.1 Overview

A voice virtual local area network (VLAN) is a VLAN dedicated to voice traffic of users. The voice VLAN technology constrains data traffic and voice traffic in the data VLAN and the voice VLAN, respectively, to prevent mutual interference between voice calls and data services and improve call quality.

1.1.2 Background and Function

- Background

Voice over IP (VoIP) telephones are widely used thanks to rapid development of technologies. Packet loss and latency greatly affect the quality of voice calls and users are more sensitive to the reduction of the quality of voice calls than the reduction of the quality of data or videos. Therefore, when the bandwidth is limited, it is necessary to guarantee the quality of voice data first so as to ensure the quality of voice calls.

- Functions of voice VLAN

a Identifies voice traffic.

b Supports automatic or manual adding of ports to a voice VLAN.

c Delivers Quality of Service (QoS) policies for voice traffic to improve the transmission priority of the voice traffic.

d Transmits voice data in a voice VLAN to ensure quality of voice calls.

1.1.3 Identifying Voice Traffic

Before assigning voice traffic to a voice VLAN, a switch device should be able to identify the voice traffic. Two methods can be used for the switch to identify voice data:

- Identifying voice data based on the Organizationally Unique Identifier (OUI) in the source MAC address of a packet

The source MAC address of a voice packet contains the OUI of a voice device vendor. After a voice VLAN OUI is configured, the device compares the source MAC address in a received packet with the voice VLAN OUI. If they match, the device can identify the voice packet and assign the packet to the voice VLAN.

Note

The MAC address field of an Ethernet packet is composed of 48 bits. The first 24 bits are referred to as an OUI, which is assigned by the Institute of Electrical and Electronics Engineers (IEEE) to device vendors. Each vendor assigns the last 24 bits based on this address segment to provide 48-bit MAC addresses.

- Identifying VoIP telephones based on the Link Layer Discovery Protocol (LLDP)

If there are a large number of VoIP telephones in a network, it is complex to configure OUIs of the VoIP telephones.

If a VoIP telephone supports LLDP, it automatically sends an LLDP packet when it goes online. This device can capture the LLDP packet and identify the device capability field in the packet. If the capability is "telephone", the device identifies the voice device as a VoIP telephone. Then, the device extracts the source MAC address from the packet and uses the address as the MAC address of the VoIP telephone, implementing automatic identification of the VoIP telephone.

If the policy of delivering a voice VLAN by LLDP is configured, this device can capture the LLDP packet from the VoIP telephone, fill voice VLAN information to related fields of the packet, and send the packet to the VoIP telephone. The VoIP telephone obtains the voice VLAN ID of this device. If the VoIP telephone supports tagged packets, it adds a VLAN tag to a voice packet before sending the packet. Upon receiving the tagged packet from the VoIP telephone, this device compares the VLAN tag in the packet with the voice VLAN ID. If they match, the device identifies the packet as a voice packet.

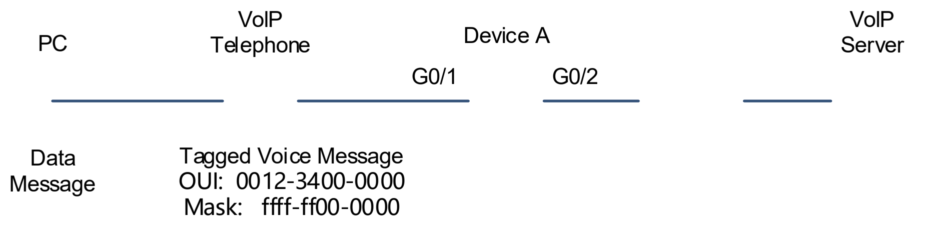
1.1.4 Work Mode of the Voice VLAN

The voice VLAN function supports manual and automatic work modes, which differ in the method of adding ports to a voice VLAN.

1. Automatic Mode

Connecting a PC and a VoIP telephone to a switch port in serial mode is the most common connection mode. The port transmits both voice data and common service data. When transmitting voice data, the port automatically forwards the voice packets to the voice VLAN. In this case, the port works in the automatic mode.

Figure 1-1 Network Topology of Voice VLAN in Automatic Mode



The working procedure of the voice VLAN in automatic mode is as follows:

(1) Adding a port to a voice VLAN: The device identifies the source MAC address in a packet, and compares the source MAC address with the OUI. If they match, the packet is identified as a voice packet. The voice packet can be identified based on a tag as well. The device automatically adds the input port of this voice packet to the voice VLAN and forwards the voice packet to the voice VLAN.

(2) Applying a priority policy: After the device identifies the voice packet based on the OUI, the device delivers a policy and changes the priority of the voice packet to the voice traffic priority.

(3) Removing the port from the voice VLAN after aging: The device maintains the port in the voice VLAN according to the aging mechanism. After the MAC address in the voice packet ages, if the port still fails to receive any voice packet within the aging time, the device removes this port from the voice VLAN.

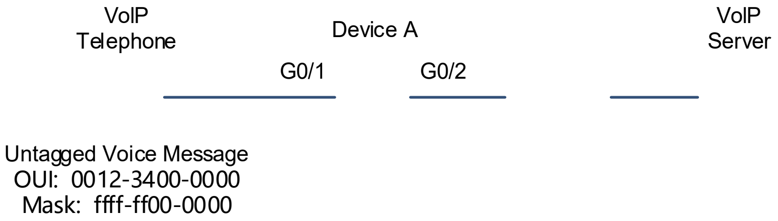
⚠ **Caution**

- In automatic mode, ports are automatically added to and removed from a voice VLAN. You are not allowed to manually add ports to a voice VLAN. Before you enable the voice VLAN function on a port, remove the voice VLAN from the allowed static VLAN list of the port to prevent the port from staying in the voice VLAN.
- Static MAC addresses do not age. Therefore, you are not advised to configure OUIs as static MAC addresses in automatic mode.

2. Manual Mode

If only a VoIP telephone is connected to a device port, the port transmits only voice packets. The administrator can manually add the port to a voice VLAN or remove the port from the voice VLAN. In this networking mode, the port transmits voice data only, which prevents service data from affecting transmission of voice data.

Figure 1-1 Network Topology of Voice VLAN in Manual Mode



The working procedure of the voice VLAN in manual mode is as follows:

(1) Applying a priority policy: The device identifies the source MAC address in a packet, and compares the source MAC address with the configured OUI. If they match, the device delivers a policy and changes the priority of the voice packet to the voice traffic priority.

1.1.5 Selection of the Work Mode

You can find out whether voice traffic contains tags based on the type and configuration of VoIP telephones and then select a proper work mode for the device.

1. Types of VoIP Telephones

Like any other network device, a VoIP telephone needs an IP address before it can implement communication normally in the network. VoIP telephones are categorized into two types, based on whether they automatically obtain IP addresses and voice VLAN information. One type of VoIP telephones can automatically obtain IP addresses and voice VLAN IDs. The other type of VoIP telephone requires you to configure IP addresses and voice VLAN IDs for them. The two types of VoIP telephones may send tagged and untagged voice traffic.

- VoIP telephones that can automatically obtain IP addresses and voice VLAN IDs

  The VoIP telephones can automatically obtain IP addresses via the Dynamic Host Configuration Protocol (DHCP).

  A VoIP telephone requests voice VLAN information from the DHCP server. If the DHCP server returns the required information, the VoIP telephone sends a voice packet carrying the voice VLAN tag. If the DHCP server does not return the required information, the VoIP telephone sends a voice packet that does not carry the voice VLAN tag.

- VoIP telephones in need of manual configuration of IP addresses and voice VLAN IDs

  IP addresses must be manually configured. Otherwise, the VoIP telephones cannot normally work.

  If a voice VLAN ID is configured for a VoIP telephone, the VoIP telephone sends and receives only tagged voice traffic based on the configuration. If no voice VLAN ID is configured for a VoIP telephone, the VoIP telephone sends and receives only untagged voice traffic.

2. Types of Voice Traffic

- Tagged voice traffic

  When a VoIP telephone obtains voice VLAN information automatically or via manual configuration, the VoIP telephone sends tagged voice traffic.

  In this case, a port can be configured as a trunk, hybrid, or uplink port. The port sends data packets to the native VLAN, and sends tagged voice packets to a non-native VLAN that is used as a voice VLAN. A voice VLAN supports both automatic and manual modes.

  - In automatic mode, the allowed static VLAN list of a port must contain the native VLAN and exclude the voice VLAN, and the voice VLAN is automatically added to or removed from the allowed VLAN list of the port. After the voice VLAN function is enabled on the port, when the port receives a tagged voice packet, the port is added to the voice VLAN to transmit tagged voice traffic. If the port does not receive a new voice packet within the aging time after the MAC address in the packet ages, the port removes the voice VLAN from the allowed VLAN list of the port.
  - In manual mode, the native VLAN and voice VLAN must be added to the allowed static VLAN list of a port.

- Untagged voice traffic

  If a VoIP telephone automatically obtains an IP address but does not obtain voice VLAN information, or an IP address is configured for the VoIP telephone but no voice VLAN is configured, the VoIP telephone sends and receives untagged voice traffic.

  In this case, the voice VLAN of the port must work in manual mode. You must configure a native VLAN for the receive port and allow packets with the native VLAN ID to pass. The native VLAN can be configured as a voice VLAN so that untagged voice packets are transmitted over the voice VLAN.

Note

VoIP telephones from different vendors may be different in the work principle, support for voice VLAN, and the process of obtaining IP addresses and voice VLAN information. For more information, see the user manual of the VoIP telephone.

3. Supported Work Modes

Table 1-1 Work Modes for Tagged Voice Traffic

Mode	Port Type	Supported Work Mode and Configuration Requirement
Automatic mode	Trunk Hybrid	Automatic mode is supported. Configuration requirements: The native VLAN is added to the allowed VLAN list of a port to transmit common data. The voice VLAN is removed from the allowed VLAN list of the port and the port can join or exit the

Mode	Port Type	Supported Work Mode and Configuration Requirement
	Uplink	VLAN automatically. A native VLAN cannot be configured as a voice VLAN.
	Access Promiscuous Host	The access ports, promiscuous ports of PVLAN, and host ports do not support tagged voice traffic.
Manual mode	Trunk Hybrid Uplink	Manual mode is supported. Configuration requirements: Both the native VLAN and voice VLAN (tagged) are added to the allowed VLAN list of a port. A native VLAN cannot be configured as a voice VLAN.
	Access Promiscuous Host	The access ports, promiscuous ports of PVLAN, and host ports do not support tagged voice traffic.

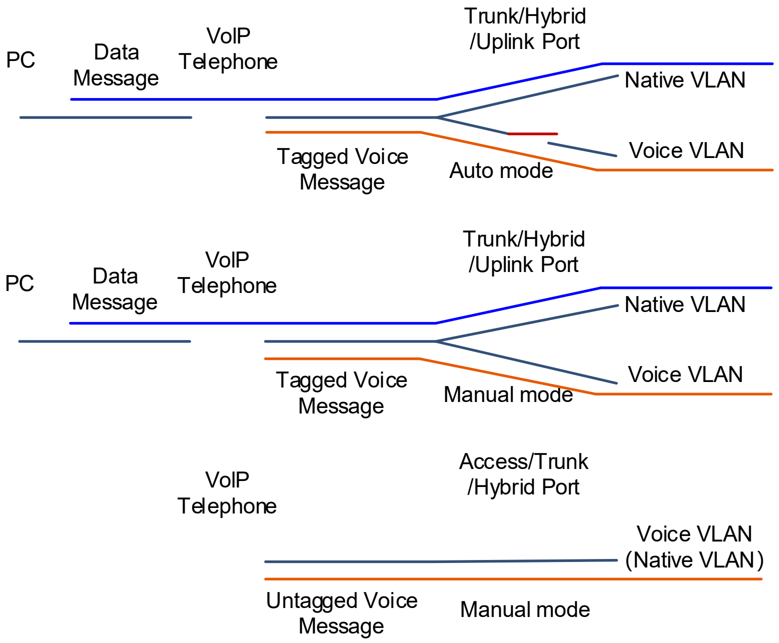
Table 1-2 Work Modes for Untagged Voice Traffic

If the voice traffic is untagged, the device supports only the manual mode.

Mode	Port Type	Supported Work Mode and Configuration Requirement
Manual mode	Access	Manual mode is supported. Configuration requirement: The voice VLAN is the VLAN, to which the access port belongs.
	Host	Manual mode is supported. Configuration requirement: The voice VLAN is the secondary VLAN (isolated or community VLAN) of a host port.
	Promiscuous	Manual mode is supported. Configuration requirement: A voice VLAN is the primary VLAN of a promiscuous port.
	Trunk	Manual mode is supported. Configuration requirement: The voice VLAN is the native VLAN of an access port and the port allows packets with the native VLAN ID to pass.
	Hybrid	Manual mode is supported. Select either of the following configuration methods: ● The voice VLAN is the native VLAN of an access port and the port allows packets with the native VLAN ID to pass through. ● The MAC VLAN function is configured to identify packets with MAC addresses matching the MAC address of a VoIP telephone as voice traffic and assign them to the voice VLAN. In this case, the voice VLAN is not necessarily configured as a native VLAN of a hybrid port.
	Uplink	When the voice traffic is untagged, the port cannot be configured as an

Mode	Port Type	Supported Work Mode and Configuration Requirement
		uplink port (not sending untagged packets).

Figure 1-2 Work Mode Selection



1.1.6 Security Mode of Voice VLAN

When a port is added to a voice VLAN, the device no longer checks the source MAC address in the packets. Theoretically, all voice packets can be transmitted over the voice VLAN. Therefore, the device may suffer malicious packet attacks, which affects normal voice communication in the voice VLAN.

To better isolate voice traffic from data traffic during transmission, the device provides the security mode for a voice VLAN.

When the security mode is enabled, only voice traffic can be transmitted in the voice VLAN. The device checks the source MAC address in each packet. When the source MAC address in the packet matches the voice VLAN OUI, the packet can be transmitted in the voice VLAN. Otherwise, the device discards the packet.

Note

In security mode, the device checks the source MAC addresses of only untagged packets and tagged packets with the voice VLAN ID. For tagged packets with non-voice VLAN IDs, the device forwards or discards the packets according to VLAN rules, irrespective of the security/common mode of the voice VLAN.

Caution

It is not recommended that both voice data and service data be transmitted over the voice VLAN. If you want to transmit both voice data and service data over the voice VLAN, disable the voice VLAN function in security mode.

1.2 Configuration Task Summary

Configuring Voice VLAN The configuration includes the following tasks:

(1) Configuring a Voice VLAN

(2) (Optional) Configuring a Voice VLAN OUI

(3) (Optional) Configuring a Voice Traffic Priority for a Voice VLAN

(4) (Optional) Configuration Aging Time for a Voice VLAN

(5) (Optional) Configuring Security Mode for a Voice VLAN

(6) Add a port to a voice VLAN and enable the voice VLAN function on the port. Select at least one of the following to configure.

- Configuring the Device to Automatically Add a Port to a Voice VLAN to Transmit Tagged Voice Traffic
- Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic
- Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic

(7) (Optional) Configuring LLDP to Deliver a Voice VLAN Policy

1.3 Configuring a Voice VLAN

1.3.1 Overview

You can create a voice VLAN on a device used to transmit voice packets only, and enable the voice VLAN function in global configuration mode. The voice VLAN function must be enabled on the port that is connected to a VoIP telephone so that the voice VLAN function can take effect.

1.3.2 Restrictions and Guidelines

- Only one voice VLAN can be configured. You must disable the voice VLAN function before you modify the voice VLAN ID. You can use the **no voice vlan** command to disable the voice VLAN function in global configuration mode.
- You must create a VLAN before configuring a voice VLAN. VLAN IDs must meet the following requirements:
  - VLAN 1 cannot be configured as a voice VLAN. Therefore, the value range of *vlanid* is from 2 to 4094.
  - A VLAN cannot be configured as a voice VLAN and a super VLAN at the same time.
  - A protocol VLAN is valid to only untagged packets received by a trunk or hybrid port. In a voice VLAN in automatic mode, the trunk and hybrid ports can process only tagged voice traffic. Therefore, do not configure a VLAN as a protocol VLAN and a voice VLAN at the same time.
  - If the 802.1x automatic VLAN hopping function is enabled on an access port, do not configure the VLAN ID delivered by 802.1x as the voice VLAN ID to ensure that the function works properly.
  - If a VoIP telephone sends tagged voice traffic and the 802.1x authentication and guest VLAN functions are enabled on the access port, configure different VLAN IDs for the voice VLAN, native VLAN, and 802.1x guest VLAN to ensure proper running of the functions.

  - Do not configure a VLAN as a remote VLAN of the remote switched port analyzer (RSPAN) and a voice VLAN at the same time. Otherwise, the RSPAN and voice VLAN functions may be affected.

- If a PC and a VoIP telephone are connected to the same port in serial mode, and both the 802.1x authentication and voice VLAN functions are enabled on the port, the PC must pass 802.1X authentication to access the network. If the OUI of the VoIP telephone matches the voice VLAN OUI, the VoIP telephone can make communication via the voice VLAN without passing 802.1x authentication.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a VLAN.

vlan *voice-vlan-id*

Only VLAN 1 exists by default.

(4) Return to the global configuration mode.

exit

(5) Configure the VLAN as a voice VLAN.

voice vlan *voice-vlan-id*

No voice VLAN is configured by default.

1.4 Configuring a Voice VLAN OUI

1.4.1 Overview

After a VoIP telephone is connected to the device, you must configure the OUI of the VoIP telephone on the device so that the VoIP telephone can communicate over the network.

The device allows you to set an OUI to be identified by the voice VLAN function. For more information about the OUI, see the principle of the voice VLAN function. The device that supports the voice VLAN function identifies the source MAC address in a received packet, and compares the source MAC address with the OUI of the voice VLAN configured on the device to check whether the traffic is sent from a specified voice device. The priority of a received packet can be changed to the voice traffic priority only when the source MAC address in the packet matches the OUI of the voice VLAN.

1.4.2 Restrictions and Guidelines

- The OUI of the voice VLAN cannot be a multicast address, and the configured mask should not contain non-consecutive 1's.

- *mac-address* indicates the source MAC address in a voice packet. *oui-mask* indicates the valid length of an OUI, which is expressed by a mask. *text* indicates a descriptor of an OUI.

- You can use the **no voice vlan mac-address oui** command in global configuration mode to delete an OUI configured on a device.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a voice VLAN OUI.

voice vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

No OUI is configured by default.

1.5 Configuring a Voice Traffic Priority for a Voice VLAN

1.5.1 Overview

You can modify the Class of Service (CoS) and differentiated services code point (DSCP) values for voice traffic in a voice VLAN on the device to improve the priority of the voice traffic and the quality of voice calls.

- The CoS value indicates L2 priority and is represented by three bits. The value range is from 0 to 7. A larger value indicates a higher priority. The CoS value is stored in the L2 header of a packet and filled in the PRI field of an 802.1Q VLAN tag. The CoS value of a common VLAN packet is **0**, which indicates the lowest priority. The default CoS value of voice traffic in a voice VLAN is **6**, which indicates a higher priority than common VLAN packets.
- The DSCP value indicates IP priority (IP PRE) and is represented by six bits. The value range is from 0 to 63. A larger value indicates a higher priority. The DSCP value is stored in the L3 header of a packet. For an IPv4 packet, the DSCP value is filled in the first six bits (bit 0 to bit 5) of the type of service (ToS) field in the header of the packet. For an IPv6 packet, the DSCP value is filled in the first six bits in the **Traffic Class** field of the IPv6 packet header. The DSCP value of a common IP packet is **0**, which indicates the lowest priority. The default DSCP value of voice traffic in a voice VLAN is **46**, which indicates a higher priority than common IP packets.
- The packet trust mode of the QoS module is disabled by default. This causes the QoS module to change the priority of all packets to **0**, and overwrites the packet priority modified by the voice VLAN function. You must run the **mls qos trust** { **cos** | **ip-precedence** | **dscp** | **exp** } command in interface configuration mode, and select the **cos** and **dscp** parameters to enable the trust mode of the QoS module to trust the packet priority modified by the voice VLAN function.

For more information about CoS and DSCP, see *Configuring CoS*.

1.5.2 Restrictions and Guidelines

- To restore the QoS and DSCP values to default values, you can run the **no voice vlan cos** or **no voice vlan dscp** command in global configuration mode.
- *cos-value* indicates the CoS value of voice traffic in a voice VLAN. The value range is from 0 to 7, and the default value is **6**.
- *dscp-value* indicates the DSCP value of voice traffic in a voice VLAN. The value range is from 0 to 63, and the default value is **46**.

1.5.3 Prerequisites

A voice VLAN has been configured. A OUI has been configured.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(1) Enter the global configuration mode.

configure terminal

(2) Specify the priority of voice packets in a voice VLAN.

voice vlan { **cos** *cos-value* | **dscp** *dscp-value* }

The default CoS and DSCP values of voice packets are **6** and **46**, respectively.

(3) Enter the interface configuration mode of the port connected to a voice device.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

(4) Enable the trust mode of the QoS module to trust the priority of voice packets.

mls qos trust { **cos** | **dscp** }

The trust mode of the QoS module is disabled by default.

1.6 Configuration Aging Time for a Voice VLAN

1.6.1 Overview

In automatic mode, after the MAC address in a voice packet ages, if the port does not receive any more voice packets within the aging time, the device removes this port from the voice VLAN.

The aging time is only valid in automatic mode. In manual mode, the aging time is invalid and therefore does not need to be configured.

1.6.2 Restrictions and Guidelines

- The aging time of a voice VLAN starts after the MAC address in a voice packet ages. The value range is from 5 to 10000, in minutes.
- To restore the aging time to the default value, you can run the **no voice vlan aging** command in global configuration mode.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure aging time of a voice VLAN.

voice vlan aging *age*

The default aging time of a voice VLAN is 1440 minutes.

1.7 Configuring Security Mode for a Voice VLAN

1.7.1 Overview

To guarantee quality of voice traffic during transmission and prevent malicious attacks, you can enable the security mode of a voice VLAN to allow only voice traffic to be transmitted in the voice VLAN.

1.7.2 Restrictions and Guidelines

To disable the security mode of the voice VLAN, you can run the **no voice vlan security enable** command in global configuration mode.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the security mode of the voice VLAN.

voice vlan security enable

The security mode of a voice VLAN is enabled by default.

1.8 Configuring the Device to Automatically Add a Port to a Voice VLAN to Transmit Tagged Voice Traffic

1.8.1 Overview

To use a port for VoIP telephone communication, you must add the port to a voice VLAN, configure the work mode for the voice VLAN, and enable the voice VLAN function on the port.

1.8.2 Restrictions and Guidelines

- You can enable the voice VLAN function only on an L2 physical port (for example, access, trunk, hybrid, uplink, or private VLAN port). The function cannot be enabled on an aggregation port or a routing port.
- Even if the voice VLAN function is disabled in global configuration mode, you can still enable the voice VLAN function on a port but the configuration does not take effect.
- When a port works in automatic mode, the native VLAN is used to transmit common VLAN packets. Do not configure the native VLAN of the port as a voice VLAN. If a port is automatically added to a voice VLAN after the port identifies voice traffic, you cannot manually add the port to or delete the port from the voice VLAN by using commands.
- If a port does not transmit packet data of a voice VLAN, remove the voice VLAN from the allowed VLAN list of the port.
- When a port works in manual mode, you must manually add the port to the voice VLAN to ensure that the voice VLAN function can take effect. To configure a port to work in manual mode, you can run the **no voice**

vlan mode auto command.

- After the voice VLAN function is enabled on a port, you are not allowed to switch the port between the manual mode and automatic mode and the allowed VLAN list of the port cannot be changed. To change the voice VLAN work mode or the allowed VLAN list of the port, disable the voice VLAN function on the port first. After the voice VLAN function is enabled on a port, to ensure normal operation of the function, you are not advised to change the port type (such as access, trunk, or hybrid port). To change the port type, disable the voice VLAN function on this port first. To disable the voice VLAN function of a port, you can run the **no voice vlan enable** command.
- If the voice traffic is tagged, a user port can be configured as a trunk, hybrid, or uplink port. The access port, host port of PVLAN, and promiscuous port of PVLAN do not support tagged voice traffic.
- If you want to transmit untagged common packets from a PC and tagged voice packets from a VoIP telephone over a user port, configure the user port as a trunk port and configure the device to automatically add the port to a voice VLAN. The configuration steps are as follows: The configuration steps for a hybrid or an uplink port are similar to the following configuration steps.

1.8.3 Prerequisites

Configure a voice VLAN.

1.8.4 Procedure

(1) Create a data VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN to transmit common packets.

vlan *data-vlan-id*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the native VLAN of a user port as a data VLAN, add the data VLAN to the allowed VLAN list of the port, and exclude the voice VLAN from the allowed VLAN list.

a Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

b Configure the user port as a trunk port.

switchport mode trunk

An interface works in access mode by default.

c Configure the VLAN used for transmitting common packets as a native VLAN of the user port to transmit untagged common packets.

switchport trunk native vlan *data-vlan-id*

The default native VLAN of a trunk port is VLAN 1.

d Configure an allowed VLAN list for the user port, add the data VLAN to the list, and exclude the voice VLAN from the list.

switchport trunk allowed vlan remove *voice-vlan-id*

The default allowed VLANs of a trunk port are VLANs 1 to 4094.

(3) Configure the voice VLAN to work in automatic mode so that the voice VLAN is automatically added to the allowed VLAN list of this port when the port receives voice data.

voice vlan mode auto

A voice VLAN works in automatic mode by default.

(4) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.9 Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic

1.9.1 Overview

To use a port for VoIP telephone communication, you must add the port to a voice VLAN, configure the work mode for the voice VLAN, and enable the voice VLAN function on the port.

1.9.2 Restrictions and Guidelines

- If the voice traffic is tagged, a user port can be configured as a trunk, hybrid, or uplink port. The access port, host port of PVLAN, and promiscuous port of PVLAN do not support tagged voice traffic. Therefore, they cannot be added to a voice VLAN.
- If you want to transmit untagged common packets from a PC and tagged voice packets from a VoIP telephone over a user port, configure the user port as a trunk port and manually add the port to a voice VLAN. The configuration steps are as follows: The configuration steps for a hybrid or an uplink port are similar to the following configuration steps.

1.9.3 Prerequisites

Configure a voice VLAN.

1.9.4 Procedure

(1) Create a data VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN to transmit common packets.

vlan *data-vlan-id*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the native VLAN of the user port as a data VLAN, and add the data VLAN and voice VLAN to the allowed VLAN list of the port.

a Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

b Configure the user port as a trunk port.

switchport mode trunk

An interface works in access mode by default.

c Configure the VLAN used for transmitting common packets as a native VLAN of the user port to transmit untagged common packets.

switchport trunk native vlan *data-vlan-id*

The default native VLAN of a trunk port is VLAN 1.

d Configure an allowed VLAN list for the user port, and add only the data VLAN and voice VLAN to the allowed VLAN list.

switchport trunk allowed vlan only *data-vlan-id*,*voice-vlan-id*

The default allowed VLANs of a trunk port are VLANs 1 to 4094.

(3) Configure the voice VLAN to work in manual mode.

no voice vlan mode auto

A voice VLAN works in automatic mode by default.

(4) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.10 Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic

1.10.1 Overview

To use a port for VoIP telephone communication, you must add the port to a voice VLAN, configure the work mode for the voice VLAN, and enable the voice VLAN function on the port.

1.10.2 Restrictions and Guidelines

- When the voice traffic is untagged, you must manually add a port to a voice VLAN. The port type can be access port, trunk port, hybrid port, host port of PVLAN, or promiscuous port of PVLAN. The uplink port does not send untagged packets. Therefore, it cannot be added to a voice VLAN.
- If you want to transmit untagged voice packets from a VoIP telephone over a user port, configure the user port as an access port and manually add the port to a voice VLAN. The configuration steps are as follows:

1.10.3 Prerequisites

Configure a voice VLAN.

1.10.4 Procedure

(1) Add a user port to a voice VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

d Configure the user port as an access port.

switchport mode access

An interface works in access mode by default.

e Add the access port to the voice VLAN to transmit common untagged packets.

switchport access vlan *voice-vlan-id*

An access port belongs to VLAN 1 by default.

(2) Configure the voice VLAN to work in manual mode.

no voice vlan mode auto

A voice VLAN works in automatic mode by default.

(3) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.11 Configuring LLDP to Deliver a Voice VLAN Policy

1.11.1 Overview

A VoIP telephone supporting the LLDP function automatically sends an LLDP packet when it goes online. If the LLDP Network Policy type/length/value (TLV) function is enabled on this device, the device can capture the LLDP packet sent by the VoIP telephone and deliver a voice VLAN policy to the VoIP telephone. If a voice VLAN policy requires the VoIP telephone to send tagged frames and the VoIP telephone supports tagged frames, the VoIP telephone adds a VLAN tag to voice packets before transmission according to the voice VLAN policy. If the voice VLAN policy requires the VoIP telephone to send untagged frames, the VoIP telephone sends untagged packets.

If the VoIP telephone does not support the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED), you must manually add the MAC address of the VoIP telephone to the OUI list of the voice VLAN.

1.11.2 Restrictions and Guidelines

- You can run the **lldp network-policy profile** *profile-num* command in global configuration mode to create a policy or enter the LLDP network policy configuration mode of a policy. *profile-num* indicates the ID of an LLDP network policy. The value range is from 1 to 1024.

- After entering the LLDP network policy configuration mode, you can run the { **voice** | **voice-signaling** } **vlan** command to configure a specific network policy. You can run the **no** { **voice** | **voice-signaling** } **vlan** command to delete a voice VLAN policy.
- You can run the **no lldp network-policy profile** *profile-num* command in interface configuration mode to delete an LLDP network policy.
- For more information about command description, see *Configuring LLDP*.

1.11.3 Prerequisites

- A voice VLAN has been configured.
- The trust mode of the QoS module has been enabled to trust packet priority modification.
- The port connected to a VoIP telephone has been manually added to a voice VLAN and the voice VLAN function has been enabled on the port.
  - To enable the VoIP telephone to send tagged frames, see Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic.
  - To enable the VoIP telephone to send untagged voice traffic, see Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic.

1.11.4 Procedure

(1) Create an LLDP network policy and enter the configuration mode.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create an LLDP network policy and enter the LLDP network policy configuration mode.

lldp network-policy profile *profile-num*

No LLDP network policy is configured by default.

(2) Configure a voice VLAN policy. Select at least one of the following to configure:

- Configure a policy to enable the VoIP telephone to send tagged frames, with the VLAN ID of *voice-vlan-id* or **0** and priority of *cos* and *dscp*.

  { **voice** | **voice-signaling** } **vlan** { *voice-vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]

  The default CoS value and DSCP value of voice packets in a voice VLAN are **6** and **46** respectively.

- Configure a policy to enable the VoIP telephone to send untagged frames. In this case, you need to manually add the port to the voice VLAN.

  { **voice** | **voice-signaling** } **vlan untagged**

  No voice VLAN policy is configured by default.

(3) Configure the user port to allow advertising the Network Policy TLV.

a Return to the global configuration mode.

exit

b Enter the interface configuration mode.

interface *interface-type interface-number*

c Configure the port to allow advertising the Network Policy TLV.

lldp tlv-enable med-tlv network-policy profile *profile-num*

No port is allowed to advertise the Network Policy TLV by default.

1.12 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

⚠ **Caution**

System resources are occupied when debugging information is output. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

⚠ **Caution**

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	**Purpose**
show voice vlan	Displays the voice VLAN configuration.
show voice vlan oui	Displays the OUI configuration of the voice VLAN.
debug bridge vvlan	Debugs the voice VLAN function.

1.13 Configuration Examples

1.13.1 Configuring a Port to Transmit Tagged Voice Traffic in Automatic Mode

1. Requirements

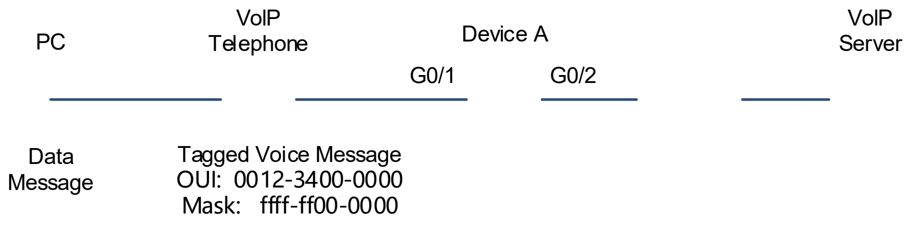
Each office staff member is assigned an Ethernet port. This port is used for service communication of a PC and voice communication of a VoIP telephone.

The VoIP telephone can automatically obtain an IP address and voice VLAN information and send tagged voice traffic. The MAC address of the VoIP telephone is 0012.3456.7890 and the OUI is 0012.3400.0000. To ensure the quality of voice calls, voice traffic is directed to a voice VLAN. The port aging time is set to 1000 minutes, CoS value to **5**, and DSCP value to **40**. The security mode of the voice VLAN needs to be enabled to transmit only voice traffic.

The PC is connected to the network through the VoIP telephone in serial mode and the PC sends untagged data traffic. The data traffic of the PC is isolated from the voice traffic of the VoIP telephone.

2. Topology

Figure 1-1 Network Topology of Voice VLAN in Automatic Mode



3. Notes

- The link needs to carry both tagged voice traffic and untagged data traffic. Therefore, set the port connected to the VoIP telephone to work in automatic mode.
- Configure GigabitEthernet 0/1 as a trunk port so that data traffic is transmitted in native VLAN 5 and voice traffic is transmitted in voice VLAN 2 separately.
- In automatic mode, GigabitEthernet 0/1 is automatically added to the voice VLAN. You are not allowed to manually add the port to the voice VLAN. Remove voice VLAN 2 from the allowed VLAN list of GigabitEthernet 0/1 so that the port determines whether to reside in the voice VLAN based on the aging time. The aging time must be configured for the port.
- GigabitEthernet 0/1 is connected to the VoIP telephone that automatically obtains an IP address. After the VoIP telephone obtains an IP address in the voice VLAN, the VoIP telephone can be normally used.
- (Optional) If 802.1x authentication is needed for the PC, enable the 802.1x authentication function on GigabitEthernet 0/1; to enable the voice packets of the VoIP telephone to be forwarded to the voice VLAN without 802.1x authentication, configure a security channel and an ACL policy. For more information about the support of this function and specific configuration, see the *Configuring 802.1X* and *Configuring ACL*.

4. Procedure

(1) Configure voice VLAN 2 to transmit voice traffic.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 2
DeviceA(config-vlan)# exit
DeviceA(config)# voice vlan 2
```

(2) Set the OUI used for identifying voice packets to 0012.3400.0000, mask to ffff.ff00.0000, and vendor to B. The priority of a received packet can be changed only when the source MAC address in the packet matches the voice VLAN OUI.

```
DeviceA(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description B
```

(3) Set the CoS value to **5** and the DSCP value to **40** for voice traffic of the voice VLAN.

```
DeviceA(config)# voice vlan cos 5
DeviceA(config)# voice vlan dscp 40
```

(4) Set the aging time of the voice VLAN to 1000 minutes. This configuration is required in automatic mode only.

```
DeviceA(config)# voice vlan aging 1000
```

(5) Enable the security mode of the voice VLAN. This mode is enabled by default.

```
DeviceA(config)# voice vlan security enable
```

(6) Create VLAN 5 to transmit common data.

```
DeviceA(config)# vlan 5
DeviceA(config-vlan)# exit
```

(7) Configure GigabitEthernet 0/1 as a trunk port and data VLAN 5 as a native VLAN of the port, and remove voice VLAN 2 from the allowed VLAN list of GigabitEthernet 0/1 so that voice VLAN 2 is automatically added to the allowed VLAN list of the port.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 5
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan remove 2
```

(8) Enable the trust mode of the QoS module to trust the packet priority modification. Configure automatic adding of the port to the voice VLAN and enable the voice VLAN function on the port. The voice VLAN works in automatic mode by default.

```
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan mode auto
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan enable
```

(9) (Optional) Enable 802.1x authentication on GigabitEthernet 0/1. Configure a security channel and an ACL policy.

```
DeviceA(config-if-GigabitEthernet 0/1)# dot1x port-control auto
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# expert access-list extended safe_channel
DeviceA(config-exp-nacl)# permit etype-any 0012.3400.0000 0000.00ff.ffff any
DeviceA(config-exp-nacl)# exit
DeviceA(config)# security global access-group safe_channel
```

(10) Configure the uplink port GigabitEthernet 0/2 as a trunk port.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# end
DeviceA# write
```

5. Verification

Run the **show voice vlan** command to check the current status of the voice VLAN on the device.

```
DeviceA# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID        : 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1000 minutes
Voice Vlan cos       : 5
Voice Vlan dscp      : 40
Current voice vlan enabled port mode:
PORT                 MODE
-------------------- ----------
Gi0/1                AUTO
```

Check the voice VLAN OUI of the device.

```
DeviceA# show voice vlan oui
Oui             Mask              Description
0012.3400.0000  ffff.ff00.0000    B
```

Check port configuration.

```
DeviceA# show interface swithport
Interface             Switchport Mode      Access Native Protected VLAN lists
--------------------- ---------- ---------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled    TRUNK     1      5      Disabled  1,3-4094
GigabitEthernet 0/2   enabled    TRUNK     1      1      Disabled  ALL
```

6. Configuration Files

Device A configuration file

```
voice vlan 2
voice vlan cos 5
voice vlan dscp 40
voice vlan aging 1000
voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description "B"
!
expert access-list extended safe_channel
 10 permit etype-any 0012.3400.0000 0000.00ff.ffff any
!
security global access-group safe_channel
!
vlan range 1-2,5
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport trunk native vlan 5
 switchport trunk allowed vlan only 1,3-4094
 voice vlan enable
 dot1x port-control auto
 mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

7. Common Errors

- When a voice VLAN works in automatic mode, the voice VLAN is not removed from the allowed VLAN list of the port.
- The trust mode of the QoS module is not enabled. Consequently, the packet priority modification cannot take effect, affecting voice traffic transmission.

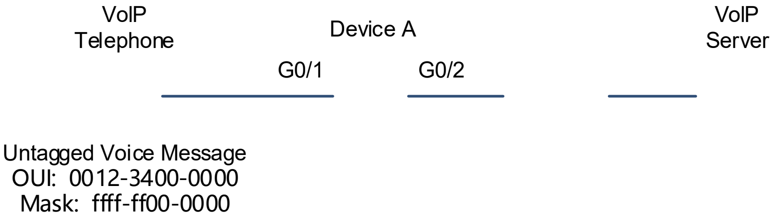
1.13.2 Configuring a Port to Transmit Untagged Voice Traffic in Manual Mode

1. Requirements

A VoIP telephone is connected to voice VLAN 2 through GigabitEthernet 0/1 of device A. This link carries only voice traffic. This type of networking is generally used when VoIP telephones are deployed in conference rooms or when no PC is required to transmit data services. The port connected to the VoIP telephone is set to work in manual mode to send untagged voice traffic to device A. The security mode is enabled to enable the voice VLAN to transmit only voice traffic. The CoS value is changed to **5** and the DSCP value is changed to **40** for the voice VLAN.

2. Topology

Figure 1-1 Network Topology of Voice VLAN in Manual Mode



3. Notes

- GigabitEthernet 0/1 receives only untagged voice traffic from the VoIP telephone. Since the untagged voice traffic cannot be forwarded in automatic mode. Therefore, configure the voice VLAN on the port to work in manual mode.
- You can configure GigabitEthernet 0/1 as a hybrid port and voice VLAN 2 as a native VLAN, and add the voice VLAN to the allowed untagged VLAN list of the port. You can also configure GigabitEthernet 0/1 as an access port, and add the port to the voice VLAN. In the following example, GigabitEthernet 0/1 is configured as an access port.

4. Procedure

(1) Create VLAN 2, and configure this VLAN as a voice VLAN.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 2
DeviceA(config-vlan)# exit
DeviceA(config)# voice vlan 2
```

(2) Set the CoS value to **5** and the DSCP value to **40** for voice traffic of the voice VLAN.

```
DeviceA(config)# voice vlan cos 5
DeviceA(config)# voice vlan dscp 40
```

(3) Set the OUI for identifying voice packets to 0012.3400.0000, mask to ffff.ff00.0000, and vendor to B on the device.

```
DeviceA(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description B
```

(4) Enable the security mode of the voice VLAN. This mode is enabled by default.

```
DeviceA(config)# voice vlan security enable
```

(5) Configure GigabitEthernet 0/1 as an access port and add the port to voice VLAN 2.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode access
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 2
```

(6) Enable the trust mode of the QoS module to trust the priority of voice packets. Manually add the user port to the voice VLAN and enable the voice VLAN function on the port.

```
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# no voice vlan mode auto
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan enable
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(7) Configure the uplink port GigabitEthernet 0/2 as a trunk port.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# end
DeviceA# write
```

5. Verification

Run the **show voice vlan** command to check the current status of the voice VLAN on the device. GigabitEthernet 0/1 is manually added.

```
DeviceA# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID        : 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Voice Vlan cos       : 5
Voice Vlan dscp      : 40
Current voice vlan enabled port mode:
PORT                 MODE
-------------------- ----------
Gi0/1                MANUAL
```

Check the voice VLAN OUI of the device.

```
DeviceA# show voice vlan oui
Oui             Mask              Description
0012.3400.0000  ffff.ff00.0000    B
```

Check port configuration.

```
DeviceA(config)#show interface swithport
Interface             Switchport Mode      Access Native Protected VLAN lists
--------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled    Access    2      1      Disabled  ALL
GigabitEthernet 0/2   enabled    TRUNK     1      1      Disabled  ALL
```

6. Configuration Files

Device A configuration file

```
voice vlan 2
voice vlan cos 5
voice vlan dscp 40
voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description "B"
!
vlan range 1-2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
 no voice vlan mode auto
 voice vlan enable
 mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

7. Common Errors

The trust mode of the QoS module is not enabled. Consequently, the packet priority modification cannot take effect, affecting voice traffic transmission.

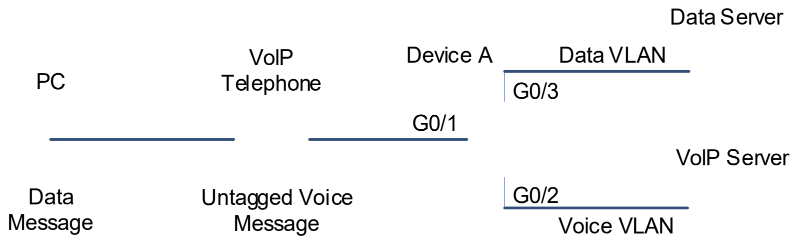
1.13.3 Configuring Isolation of Untagged Voice Traffic from Data Traffic

1. Requirements

A PC is connected to a VoIP telephone and the VoIP telephone is connected to device A. The VoIP telephone automatically obtains an IP address and sends untagged voice traffic. The PC sends untagged data traffic. To ensure quality of voice calls, the voice data must be transmitted in the dedicated voice VLAN 2 and this voice VLAN cannot transmit non-voice data. Common data is transmitted in VLAN 3 separately.

2. Topology

Figure 1-1 Network Topology of Isolation of Voice VLAN from Data VLAN



3. Notes

- Configure GigabitEthernet 0/1 to forward voice traffic and data traffic separately. Packets from the VoIP telephone and PC are untagged. Therefore, configure the port as a hybrid port and enable data traffic to be forwarded in the native VLAN and voice traffic to be forwarded over the voice VLAN.
- The VoIP telephone connected to GigabitEthernet 0/1 sends untagged voice traffic. Therefore, set the voice VLAN to work in manual mode. The PC sends untagged data traffic. To isolate the data traffic from the voice traffic, enable the MAC VLAN function on GigabitEthernet 0/1 so that the port identifies the MAC address of the voice traffic and assigns the voice traffic to the voice VLAN.
- To ensure that the hybrid port receives untagged data traffic and voice traffic, add the data VLAN and voice VLAN to the allowed untagged VLAN list of the port.

4. Procedure

(1) A voice VLAN has been configured.

```
DeviceA>en
DeviceA# configure terminal
DeviceA(config)# vlan 2
DeviceA(config-vlan)# exit
DeviceA(config)# voice vlan 2
```

(2) Configure the device to identify packets with the OUI of 0012.3400.0000 and mask of ffff.ff00.0000 as voice packets and forward the packets to the voice VLAN.

```
DeviceA(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description B
```

(3) Configure MAC VLAN entries in global configuration mode so that voice traffic is forwarded to voice VLAN 2.

```
DeviceA(config)# mac-vlan mac-address 0012.3456.7890 mask ffff.ffff.ffff vlan
2
```

(4) Create data VLAN 3 to transmit common data.

```
DeviceA(config)# vlan 3
DeviceA(config-vlan)# exit
```

(5) Configure GigabitEthernet 0/1 as a hybrid port and data VLAN 3 as a native VLAN. In this way, the device sends untagged packets of data VLAN 3 and untagged packets of voice VLAN 2 to the user port.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode hybrid
DeviceA(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3
DeviceA(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan add
untagged 2-3
```

(6) Enable the trust mode of the QoS module to trust packet priority modification. Set the voice VLAN of GigabitEthernet 0/1 to work in manual mode and enable the voice VLAN and MAC VLAN functions on the port.

```
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# no voice vlan mode auto
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan enable
DeviceA(config-if-GigabitEthernet 0/1)# mac-vlan enable
```

(7) Add GigabitEthernet 0/2 connected to the voice server to voice VLAN 2.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport access vlan 2
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(8) Configure GigabitEthernet 0/3 connected to the data server as a trunk port, and remove voice VLAN 2 from the allowed VLAN list of the port.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan remove 2
DeviceA(config-if-GigabitEthernet 0/3)# end
DeviceA# write
```

5. Verification

Check the current status of the voice VLAN on the device.

```
DeviceA# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440minutes
Voice Vlan cos: 6
Voice Vlan dscp: 46
Current voice vlan enabled port mode:
PORT                   MODE
-------------------- ----------
Gi0/1                  MANUAL
```

Check the OUI of the voice device.

```
DeviceA# show voice vlan oui
OUI             Mask            Description
--------------- --------------- ------------------------------
0012.3400.0000  ffff.ff00.0000  B
```

Check the MAC VLAN entries.

```
DeviceA# show mac-vlan all
The following MAC VLAN address exist:
S: Static   D: Dynamic
MAC ADDR        MASK            VLAN ID  PRIO  STATE
----------------------------------------------------
0012.3456.7890  ffff.ffff.ffff  2        0     S
Total MAC VLAN address count: 1
```

6. Configuration Files

Device A configuration file

```
voice vlan 2
voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description "B"
mac-vlan mac-address 0012.3456.7890 mask ffff.ffff.ffff vlan 2
!
vlan range 1-3
!
interface GigabitEthernet 0/1
 switchport mode hybrid
 switchport hybrid native vlan 3
 switchport hybrid allowed vlan only tagged 1,4-4094
 switchport hybrid allowed vlan add untagged 2,3
 no voice vlan mode auto
 voice vlan enable
 mac-vlan enable
 mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport access vlan 2
!
interface GigabitEthernet 0/3
 switchport mode trunk
 switchport trunk allowed vlan only 1,3-4094
!
```