Table of Contents

Chapter 1 VLAN Configuration

When configuring VLAN, go to these sections for information you are interested in:

1.1 Introduction to VLAN

1.1.1 VLAN Overview

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared in an Ethernet, network performance may degrade as the number of hosts on the network is increasing. If the number of the hosts in the network reaches a certain level, problems caused by collisions, broadcasts, and so on emerge, which may cause the network operating improperly. In addition to the function that suppresses collisions (which can also be achieved by interconnecting LANs), virtual LAN (VLAN) can also isolate broadcast packets. VLAN divides a LAN into multiple logical LANs with each being a broadcast domain. Hosts in the same VLAN can communicate with each other like in a LAN. However, hosts from different VLANs cannot communicate directly. In this way, broadcast packets are confined to a single VLAN, as illustrated in the following figure.

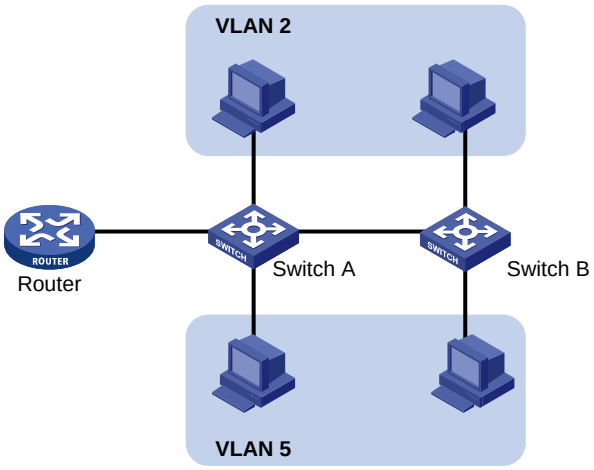

Figure 1-1 A VLAN diagram

A VLAN is not restricted by physical factors, that is to say, hosts that reside in different network segments may belong to the same VLAN, users in a VLAN can be connected to the same switch, or span across multiple switches or routers.

VLAN technology has the following advantages:

1) Broadcast traffic is confined to each VLAN, reducing bandwidth utilization and improving network performance.
2) LAN security is improved. Packets in different VLANs are isolated at Layer 2. That is, users in a VLAN cannot communicate with users in other VLANs directly, unless routers or Layer 3 switches are used.
3) A more flexible way to establish virtual workgroups. With VLAN technology, a virtual workgroup can be created spanning physical network segments. That is, users from the same workgroup do not have to be within the same physical area, making network construction and maintenance much easier and more flexible.

1.1.2 VLAN Fundamental

To enable packets being distinguished by the VLANs they belong to, The VLAN tag fields used to identify VLANs are added to packets. As common switches operate on the data link layer of the OSI model, they only process data link layer encapsulation information and the VLAN tag thus needs to be inserted to the data link layer encapsulation.

The format of the packets carrying the VLAN tag fields is defined in IEEE 802.1Q, which is issued by IEEE in 1999.

In the header of a traditional Ethernet data frame, the field following the destination MAC address and the source MAC address is the Type field, which indicates the upper layer protocol type. Figure 1-2 illustrates the format of a traditional Ethernet frame, where DA stands for destination MAC address, SA stands for source MAC address, and Type stands for the upper layer protocol type of the frame.

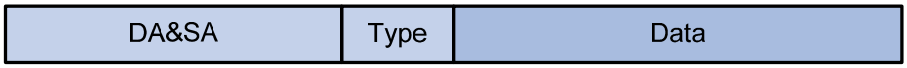

Figure 1-2 The format of a traditional Ethernet frame

IEEE802.1Q defines a four-byte VLAN Tag between the DA&SA field and the Type field to carry VLAN-related information, as shown in Figure 1-3.

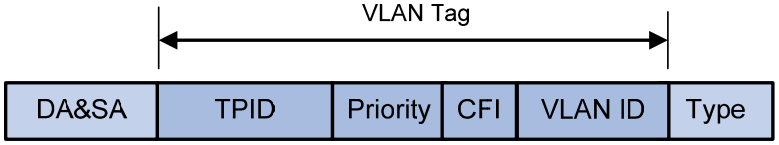

Figure 1-3 The position and the format of the VLAN Tag

The VLAN Tag comprises four fields: the tag protocol identifier (TPID) field, the Priority field, the canonical format indicator (CFI) field, and the VLAN ID field.

- The TPID field, 16 bits in length and with a value of 0x8100, indicates that a packet carries a VLAN tag with it.
- The Priority field, three bits in length, indicates the 802.1p priority of a packet. For information about packet priority, refer to the *QoS* part of the manual.
- The CFI field, one bit in length, specifies whether or not the MAC addresses are encapsulated in standard format when packets are transmitted across different medium. With the field set to 0, MAC addresses are encapsulated in standard format; with the field set to 1, MAC addresses are encapsulated in non-standard format. The filed is 0 by default.
- The VLAN ID field, 12 bits in length and with its value ranging from 0 to 4095, identifies the ID of the VLAN a packet belongs to. As VLAN IDs of 0 and 4095 are reserved by the protocol, the value of this field actually ranges from 1 to 4094.

A network device determines the VLAN to which a packet belongs to by the VLAN ID field the packet carries. The VLAN Tag determines the way a packet is processed. For more information, refer to section Introduction to Port-Based VLAN.

Note:

The frame format mentioned here is that of Ethernet II. Besides Ethernet II encapsulation, other types of encapsulation, including 802.2 LLC, 802.2 SNAP, and 802.3 raw are also supported by Ethernet. The VLAN tag fields are also added to packets adopting these encapsulation formats for VLAN identification.

1.1.3 VLAN Classification

Based on how VLANs are established, VLANs fall into different categories. The following types are the most commonly used:

- Port-based
- MAC address-based
- Protocol-based
- IP-subnet-based
- Policy-based
- Other types

The S5500-EI series Ethernet switches support port-based VLAN, MAC address-based VLAN, protocol-based VLAN, and IP-subnet-based VLAN.

1.2 Configuring Basic VLAN Attributes

Follow these steps to configure basic VLAN attributes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create VLANs	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	Optional Using this command can create multiple VLANs in a bulk.
Enter VLAN view	**vlan** *vlan-id*	Required If the specified VLAN does not exist, the command creates the VLAN and then enters its view. By default, only the default VLAN (that is, VLAN 1) exists in the system.
Specify a descriptive string for the VLAN	**description** *text*	Optional VLAN ID used by default, for example, “VLAN 0001”

Note:

- As the default VLAN, VLAN 1 cannot be created or removed.
- You cannot manually create or remove reserved VLANs, which are reserved for specific functions.
- Dynamic VLANs cannot be removed using the **undo vlan** command.
- If a VLAN has a QoS policy configured, the VLAN cannot be removed.
- If a VLAN is configured as a remote-probe VLAN for remote port mirroring, it cannot be removed using the **undo vlan** command unless its remote-probe VLAN configuration is removed.

1.3 Basic VLAN Interface Configuration

Hosts of different VLANs cannot communicate directly. That is, routers or Layer 3 switches are needed for packets to travel across different VLANs. VLAN interfaces are used to forward VLAN packets on Layer 3.

VLAN interfaces are Layer 3 virtual interfaces (which do not exist physically on devices) used for Layer 3 interoperability between different VLANs. Each VLAN can have one VLAN interface. Packets of a VLAN can be forwarded on network layer through the corresponding VLAN interface. As each VLAN forms a broadcast domain, a VLAN can be an IP network segment and the VLAN interface can be the gateway to enable IP address-based Layer 3 forwarding.

Follow these steps to configure VLAN interface basic attributes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN interface or enter VLAN interface view	**interface Vlan-interface** *vlan-interface-id*	Required This command leads you to VLAN interface view if the VLAN interface already exists.
Configure an IP address for the VLAN interface	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	Optional Not configured by default
Specify the descriptive string for the VLAN interface	**description** *text*	Optional VLAN interface name is used by default, for example, “Vlan-interface1 Interface”.

To do…	Use the command…	Remarks
Bring up the VLAN interface	**undo shutdown**	Optional By default, a VLAN interface is up. The state of a VLAN interface also depends on the states of the ports in the VLAN. If all the ports in the VLAN are down, the VLAN interface is down; if one or more ports in the VLAN are up, the VLAN interface is up. If a VLAN interface is manually shut down, the VLAN interface is always down regardless of the states of ports in the VLAN.

Note:

Before creating a VLAN interface, ensure that the corresponding VLAN already exists. Otherwise, the specified VLAN interface will not be created.

1.4 Port-Based VLAN Configuration

1.4.1 Introduction to Port-Based VLAN

This is the simplest and yet the most effective way of classifying VLANs. It groups VLAN members by port. After added to a VLAN, a port can forward the packets of the VLAN.

I. Port link type

Based on the tag handling mode, a port's link type can be one of the following three:

- Access port: the port only belongs to one VLAN, normally used to connect user device;
- Trunk port: the port can belong to multiple VLANs, can receive/send packets for multiple VLANs, normally used to connect network devices;
- Hybrid port: the port can belong to multiple VLANs, can receive or send packets for multiple VLANs, used to connect either user or network devices;

The differences between Hybrid and Trunk port:

- A Hybrid port allows packets of multiple VLANs to be sent without the Tag label;

- A Trunk port only allows packets from the default VLAN to be sent without the Tag label.

II. Default VLAN

You can configure the default VLAN for a port. By default, VLAN 1 is the default VLAN for all ports. However, this can be changed as needed.

- An Access port only belongs to one VLAN. Therefore, its default VLAN is the VLAN it resides in and cannot be configured.
- You can configure the default VLAN for the Trunk port or the Hybrid port as they can both belong to multiple VLANs.
- After deletion of the default VLAN using the **undo vlan** command, the default VLAN for an Access port will revert to VLAN 1, whereas that for the Trunk or Hybrid port remains, meaning the port can use a nonexistent VLAN as the default VLAN.

Note:

For a port in automatic voice VLAN mode, do not set the voice VLAN as the default VLAN of the port. Otherwise, the system prompts error information. For information about voice VLAN, refer to Voice VLAN Configuration.

Configured with the default VLAN, a port handles packets in the following ways:

Port type	Inbound packets handling		Outbound packets handling
	If no tag is carried in the packet	If a tag is carried in the packet	
Access Port	Tag the packet with the default VLAN ID	• Receive the packet if its VLAN ID is the same as the default VLAN ID • Discard the packet if its VLAN ID is different from the default VLAN ID	Strip the Tag and send the packet as the VLAN ID is the same with the default VLAN ID

<table>
<tr><th rowspan="2">Port type</th><th colspan="2">Inbound packets handling</th><th rowspan="2">Outbound packets handling</th></tr>
<tr><th>If no tag is carried in the packet</th><th>If a tag is carried in the packet</th></tr>
<tr><td>Trunk port</td><td rowspan="2">Check whether the default VLAN ID of the port is in the list of VLANs allowed to pass through the port, if yes, tag the packet with the default VLAN ID; if no, discard the packet</td><td rowspan="2">• Receive the packet if the VLAN ID is in the list of VLANs allowed to pass through the port
• Discard the packet if the VLAN ID is not in the list of VLANs allowed to pass through the port</td><td>• Strip the tag and send the packet if the VLAN ID is the same as the default VLAN ID
• Keep the tag and send the packet if the VLAN ID is not the same as the default VLAN ID but allowed to pass through the port</td></tr>
<tr><td>Hybrid port</td><td>Send the packet if the VLAN ID is allowed to pass through the port. Use the port hybrid vlan command to configure whether the port keeps or strips the tags when sending packets of a VLAN (including the default VLAN).</td></tr>
</table>

1.4.2 Configuring an Access-Port-Based VLAN

There are two ways to configure Access-port-based VLAN: one way is to configure in VLAN view, the other way is to configure in Ethernet port view/port group view.

Follow these steps to configure the Access-port-based VLAN in VLAN view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	Required If the specified VLAN does not exist, this command be created first creates the VLAN before entering its view.
Add an Access port to the current VLAN	**port** *interface-list*	Required By default, system will add all ports to VLAN 1.

Follow these steps to configure the Access-port-based VLAN in Ethernet port view/port group view:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Use either command In Ethernet port view, the subsequent configurations only apply to the current port; In port group view, the subsequent configurations apply to all ports in the port group.
	Enter port group view	**port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	
Configure the port link type as Access		**port link-type access**	Optional The link type of a port is Access by default.
Add the current Access port to a specified VLAN		**port access vlan** *vlan-id*	Optional By default, all Access ports belong to VLAN 1.

Note:

To add an Access port to a VLAN, make sure the VLAN already exists.

1.4.3 Configuring a Trunk-Port-Based VLAN

A Trunk port may belong to multiple VLANs, and you can only perform this configuration in Ethernet port view or port group view.

Follow these steps to configure the Trunk-port-based VLAN:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Use either command In Ethernet port view, the subsequent configurations only apply to the current port; in port group view, the subsequent configurations apply to all ports in the port group.
	Enter port group view	**port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	
Configure the port link type as Trunk		**port link-type trunk**	Required

To do…	Use the command…	Remarks
Allow the specified VLANs to pass through the current Trunk port	**port trunk permit vlan** { *vlan-id-list* | **all** }	Required By default, all Trunk ports only allow packets of VLAN 1 to pass.
Configure the default VLAN for the Trunk port	**port trunk pvid vlan** *vlan-id*	Optional VLAN 1 is the default by default.

Note:

- To convert a Trunk port into a Hybrid port (or vice versa), you need to use the Access port as a medium. For example, the Trunk port has to be configured as an Access port first and then a Hybrid port.
- The default VLAN IDs of the Trunk ports on the local and peer devices must be the same. Otherwise, packets cannot be transmitted properly.

1.4.4 Configuring a Hybrid-Port-Based VLAN

A Hybrid port may belong to multiple VLANs, and this configuration can only be performed in Ethernet port view or port group view.

Follow these steps to configure the Hybrid-port-based VLAN:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Use either command; In Ethernet port view, the subsequent configurations only apply to the current port; in port group view, the subsequent configurations apply to all ports in the port group
	Enter port group view	**port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	
Configure the port link type as Hybrid		**port link-type hybrid**	Required
Allow the specified VLANs to pass through the current Hybrid port		**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required By default, all Hybrid ports only allow packets of VLAN 1 to pass.

To do…	Use the command…	Remarks
Configure the default VLAN of the Hybrid port	**port hybrid pvid vlan** *vlan-id*	Optional VLAN 1 is the default by default

Note:

- To configure a Trunk port into a Hybrid port (or vice versa), you need to use the Access port as a medium. For example, the Trunk port has to be configured as an Access port first and then a Hybrid port.
- Ensure that the VLANs already exist before configuring them to pass through a Hybrid port.
- The default VLAN IDs of the Hybrid ports on the local and the peer devices must be the same. Otherwise, packets cannot be transmitted properly.

1.5 MAC Address-Based VLAN Configuration

1.5.1 Introduction to MAC Address-Based VLAN

With MAC address-based VLANs created, the VLAN to which a packet belongs is determined by its source MAC address, and packets in a MAC address-based VLAN are forwarded after being tagged with the tag of the VLAN. This function is usually coupled with the security technologies (such as 802.1X) to provide secure and flexible network accesses for terminal devices.

I. MAC address-based VLAN implementation

With MAC address-based VLANs created on a port, the port operates as follows:

- If an untagged packet is received, the port checks its MAC address VLAN entries for the one that matches the source MAC address of the packet. If the entry exists, the packet is forwarded based on the matched VLAN ID and the precedence value; otherwise, the packet is forwarded based on other match rules.
- If a tagged packet is received, the port processes the packet in the same way as it processes port-based VLAN packets, that is, forwards the packet if the VLAN corresponding to the VLAN tag is permitted by the port or drops the packet if the VLAN corresponding to the VLAN tag is not permitted by the port.

II. The ways to create MAC address-based VLANs

A MAC address-based VLAN can be created in one of the following two ways.

- Static configuration (through CLI)

You can associate MAC addresses and VLANs by using corresponding commands.

- Auto configuration though the authentication server (that is, VLAN issuing)

The device associates MAC addresses and VLANs dynamically based on the information provided by the authentication server. If a user goes offline, the corresponding MAC address-to-VLAN association is removed automatically. Auto configuration requires MAC address-to–VLAN mapping relationship be configured on the authentication server. For detailed information, refer to *802.1x Configuration*.

The two configuration methods can be used at the same time, that is, you can configure a MAC address-to-VLAN entry on both the local device and the authentication serer at the same time. Note that the MAC address-to-VLAN entry configuration takes effect only when the configuration on the local device is consistent with that on the authentication server.

1.5.2 Configuring a MAC Address-Based VLAN

Note:

MAC address-based VLANs are available only on Hybrid ports.

Follow these steps to configure a MAC address-based VLAN:

To do...		Use the command...	Remarks
Enter system view		**system-view**	—
Associate MAC addresses with a VLAN		**mac-vlan mac-address** *mac-addr* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *priority*]	Required
Enter Ethernet interface view or port group view	Enter Ethernet interface view	**interface** *interface-type interface-number*	Use either command. The configuration performed in Ethernet interface view applies to the current port only; the configuration performed in port group view applies to all the ports in the port group.
	Enter port group view	**port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	
Configure the link type of the port(s) as hybrid		**port link-type hybrid**	Required
Configure the current hybrid port(s) to permit packets of specific MAC address-based VLANs		**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required By default, a hybrid port only permits the packets of VLAN 1.
Enable MAC address-based VLAN		**mac-vlan enable**	Required Disabled by default

To do...	Use the command...	Remarks
Configure VLAN matching precedence	**vlan precedence** { **mac-vlan** | **ip-subnet-vlan** }	Optional By default, VLANs are preferentially matched based on MAC addresses.

1.6 Protocol-Based VLAN Configuration

1.6.1 Introduction to Protocol-Based VLAN

Note:

Protocol-based VLANs are only applicable to Hybrid ports.

In this approach, inbound packets are assigned with different VLAN IDs based on their protocol type and encapsulation format. The protocols that can be used to categorize VLANs include: IP, IPX, and AppleTalk (AT). The encapsulation formats include: Ethernet II, 802.3 raw, 802.2 LLC, and 802.2 SNAP.

A protocol-based VLAN can be defined by a protocol template, which is determined by encapsulation format and protocol type. A port can be associated to multiple protocol templates. An untagged packet (that is, packet carrying no VLAN tag) reaching a port associated with a protocol-based VLAN will be processed as follows.

- If the packet matches a protocol template, the packet will be tagged with the VLAN ID of the protocol-based VLAN defined by the protocol template.
- If the packet matches no protocol template, the packet will be tagged with the default VLAN ID of the port.

The port processes a tagged packet (that is, a packet carrying a VLAN tag) in the same way as it processes packets of a port-based VLAN.

- If the port is configured to permit the VLAN identified by this VLAN tag, the port forwards the packet.
- If the port is configured to deny the VLAN identified by this VLAN tag, the port discards the packet.

This feature is mainly used to bind the service type with VLAN for ease of management and maintenance.

1.6.2 Configuring a Protocol-Based VLAN

Follow these steps to configure a protocol-based VLAN:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter VLAN view		**vlan** *vlan-id*	Required If the specified VLAN does not exist, this command creates the VLAN and then enters its view.
Configure the protocol-based VLAN and specify the protocol template		**protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }	Required
Exit the VLAN view		**quit**	Required
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Use either command In Ethernet port view, the subsequent configurations only apply to the current port; in port group view, the subsequent configurations apply to all ports in the port group
	Enter port group view	**port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	
Configure the port link type as Hybrid		**port link-type hybrid**	Required
Allow the packets of protocol-based VLANs to pass through the current Hybrid port in untagged way (with the tags of the packets stripped)		**port hybrid vlan** *vlan-id-list* **untagged**	Required
Configure the association between the Hybrid port and the protocol-based VLAN		**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	Required

Caution:

- At present, the AppleTalk-based protocol template cannot be associated with a port on an S5500-EI series Ethernet switch.
- Do not configure both the *dsap-id* and *ssap-id* arguments in the **protocol-vlan** command as 0xe0 or 0xff when configuring the user-defined template for **llc** encapsulation. Otherwise, the encapsulation format of the matching packets will be the same as that of the **ipx llc** or **ipx raw** packets respectively.
- When you use the **mode** keyword to configure a user-defined protocol template, do not set *etype-id* in **ethernetii etype** *etype-id* to 0x0800, 0x8137, 0x809b, or 0x86dd. Otherwise, the encapsulation format of the matching packets will be the same as that of the IPv4, IPX, AppleTalk, and IPv6 packets respectively.
- Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN. Because a protocol-based VLAN requires that the inbound packets on the Hybrid port are untagged packets, whereas the Hybrid port working in auto voice VLAN mode only supports to process tagged voice traffic. For more information, refer to Voice VLAN Configuration.

1.7 Configuring IP-Subnet-Based VLAN

1.7.1 Introduction

In this approach, VLANs are categorized based on the source IP addresses and the subnet masks of packets. After receiving an untagged packet from a port, the device identifies the VLAN the packet belongs to based on the source address contained in the packet, and then forwards the packet in the VLAN. This allows packets from a certain network segment or with certain IP addresses to be forwarded in a specified VLAN.

1.7.2 Configuring an IP-Subnet-Based VLAN

Note:

This feature is only applicable to Hybrid ports.

Follow these steps to configure an IP-subnet-based VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—

To do…		Use the command…	Remarks
Configure the association between an IP subnet with the current VLAN		**ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* [*mask*]	Required The configured IP network segment or IP address cannot be a multicast network segment or a multicast address
Return to system view		**quit**	—
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Use either command; In Ethernet port view, the subsequent configurations only apply to the current port; in port group view, the subsequent configurations apply to all ports in the port group
	Enter port group view	**port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	
Configure port link type as Hybrid		**port link-type hybrid**	Required
Allow an IP-subnet-based VLAN to pass through the current Hybrid port		**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required
Configure the association between the Hybrid port and the IP-subnet-based VLAN		**port hybrid ip-subnet-vlan vlan** *vlan-id*	Required

1.8 Displaying and Maintaining VLAN

To do...	Use the command…	Remarks
Display the information about specific VLANs	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]	Available in any view
Display the information about a VLAN interface	**display interface Vlan-interface** [*vlan-interface-id*]	Available in any view
Display all the ports with MAC address-based VLAN enabled.	**display mac-vlan interface**	Available in any view
Display the information about specific MAC address-to-VLAN entries	**display mac-vlan** { **all** | **dynamic** | **mac-address** *mac-addr* [**mask** *mac-mask*] | **static** | **vlan vlan-id** }	Available in any view

To do...	Use the command…	Remarks
Display the protocol information and protocol indexes of specified VLANs	**display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }	Available in any view
Display protocol-based VLAN information on specified interfaces	**display protocol-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Available in any view
Display the IP-subnet-based VLAN information and IP subnet indexes of specified VLANs	**display ip-subnet-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }	Available in any view
Display the IP-subnet-based VLAN information and IP subnet index of specified ports	**display ip-subnet-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number* | **all** }	Available in any view
Clear the statistics on a VLAN interface	**reset counters interface Vlan-interface** [*vlan-interface-id*]	Available in user view

1.9 VLAN Configuration Example

I. Network requirements

- Device A connects to Device B through Trunk port GigabitEthernet 1/0/1;
- The default VLAN ID of the port is 100;
- This port allows packets from VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

II. Network diagram

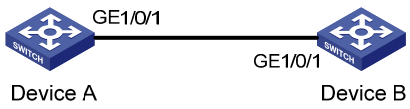

Figure 1-4 Network diagram for port-based VLAN configuration

III. Configuration procedure

1) Configure Device A

Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100.

```
<DeviceA> system-view
[DeviceA] vlan 2
```

```
[DeviceA-vlan2] quit
[DeviceA] vlan 100
[DeviceA-vlan100] vlan 6 to 50
Please wait... Done.
```

Enter GigabitEthernet 1/0/1 port view.

```
[DeviceA] interface GigabitEthernet 1/0/1
```

Configure GigabitEthernet 1/0/1 as a Trunk port and configure its default VLAN ID as 100.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

Configure GigabitEthernet 1/0/1 to deny the packets of VLAN 1 (by default, the packets of VLAN 1 are permitted on all the ports).

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure packets from VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 6 to 50 100
Please wait... Done.
```

2) Configure Device B following similar steps as that of Device A.

IV. Verification

Verifying the configuration of Device A is similar to that of Device B. So only Device A is taken for example here.

Display the information about GigabitEthernet 1/0/1 of Device A to verify the above configurations.

```
<DeviceA> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0011-2233-5577
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 1000Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9212
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 100
```

```
Mdi type: auto
Link delay is 0(sec)
Port link-type: trunk
 Tagged   VLAN ID : 2, 6-50, 100
 Untagged VLAN ID : 2, 6-50, 100
Port priority: 0
Last 300 seconds input:  8 packets/sec 1513 bytes/sec   0%
Last 300 seconds output:  1 packets/sec 179 bytes/sec   0%
Input (total):  25504971 packets, 13911485028 bytes
         14288575 broadcasts, 11111535 multicasts
Input (normal):  25504971 packets, - bytes
         14288575 broadcasts, 11111535 multicasts
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
Output (total): 175995 packets, 31290143 bytes
         47 broadcasts, 68494 multicasts, 0 pauses
Output (normal): 175995 packets, - bytes
         47 broadcasts, 68494 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

The output above shows that:

- The port is a Trunk port (Port link-type: trunk).
- The default VLAN is VLAN 100 (PVID: 100).
- The port permits packets of VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 (VLAN permitted: 2, 6-50, 100).

So the configuration is successful.

Chapter 2 Voice VLAN Configuration

When configuring Voice VLAN, go to these sections for information you are interested in:

2.1 Introduction to Voice VLAN

A voice VLAN is configured specially for voice traffic. By adding the ports that connect voice devices to the voice VLAN, you can configure quality of service (QOS for short) attributes for the voice traffic, improving transmission priority and ensuring voice quality. A device determines whether a received packet is a voice packet by checking its source MAC address. Packets containing source MAC addresses that comply with the voice device Organizationally Unique Identifier (OUI for short) addresses are regarded as voice traffic, and are forwarded to the voice VLAN.

You can configure the OUI addresses in advance or use the default OUI addresses, which are listed as follows.

Table 2-1 The default OUI addresses of different vendors

Number	OUI address	Vendors
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	0060-b900-0000	Philips/NEC phone
5	00d0-1e00-0000	Pingtel phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3Com phone

Note:

- As the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by IEEE (Institute of Electrical and Electronics Engineers).
- You can add or remove default OUI address manually.

2.1.1 Voice VLAN Modes on a Port

There are two voice VLAN modes on a port: automatic and manual (the mode here refers to the way of adding a port to a voice VLAN).

- In automatic mode, the system identifies the source MAC address contained in the protocol packets (untagged packets) sent when the IP phone is powered on and matches it against the OUI addresses. If a match is found, the system will automatically add the port into the Voice VLAN and apply ACL rules and configure the packet precedence. An aging time can be configured for the voice VLAN. The system will remove a port from the voice VLAN if no voice packet is received from it after the aging time. The adding and removing of ports are automatically realized by the system.
- In manual mode, administrators add the IP phone access port to the voice VLAN manually. It then identifies the source MAC address contained in the packet, matches it against the OUI addresses. If a match is found, the system issues ACL rules and configures the precedence for the packets. In this mode, the operation of adding ports to and removing ports from the voice VLAN are carried out by the administrators.
- Both modes forward tagged packets according to their tags.

The following table lists the co-relation between the port voice VLAN mode, the voice traffic type of an IP phone, and the port link type.

Table 2-2 Voice VLAN operating mode and the corresponding voice traffic types

Port voice VLAN mode	Voice traffic type	Port link type
Automatic mode	Tagged voice traffic	Access: not supported
		Trunk: supported provided that the default VLAN of the access port exists and is not the voice VLAN and that the access port belongs to the voice VLAN
		Hybrid: supported provided that the default VLAN of the access port exists and is not the voice VLAN, and is in the list of tagged VLANs whose packets can pass through the access port
	Untagged voice traffic	Access, Trunk, Hybrid: not supported
Manual mode	Tagged voice traffic	Access: not supported
		Trunk: supported provided that the default VLAN of the access port exists and is not the voice VLAN and that the access port belongs to the default VLAN
		Hybrid: supported provided that the default VLAN of the access port exists and is not the voice VLAN, and is in the list of tagged VLANs whose packets can pass through the access port
	Untagged voice traffic	Access: supported provided that the default VLAN of the access port is the voice VLAN
		Trunk: supported provided that the default VLAN of the access port is the voice VLAN and that the access port allows packets from the voice VLAN to pass through
		Hybrid port: supported provided that the default VLAN of the access port is the voice VLAN and is in the list of untagged VLANs whose packets are allowed to pass through the access port

Caution:

- If the voice traffic sent by an IP phone is tagged and that the access port has 802.1x authentication and Guest VLAN enabled, assign different VLAN IDs for the voice VLAN, the default VLAN of the access port, and the 802.1x guest VLAN.
- If the voice traffic sent by an IP phone is untagged, to realize the voice VLAN feature, the default VLAN of the access port can only be configured as the voice VLAN. Note that at this time 802.1 x authentication function cannot be realized.

Note:

- The default VLAN for all ports is VLAN 1. Using commands, users can either configure the default VLAN of a port, or configure to allow a certain VLAN to pass through the port. For more information, refer to section Port-Based VLAN Configuration.
- Use the **display interface** command to display the default VLAN and the VLANs that are allowed to go through a certain port.

2.1.2 Security Mode and Normal Mode for the Voice VLAN

Voice VLAN modes fall into security mode and normal mode based on the filtering mechanisms of the voice VLAN-enabled ports on the inbound packets. In the two modes, the voice VLAN-enabled ports process untagged packets and packets with the voice VLAN tags in different ways, as shown in the following table:

Voice VLAN mode	Inbound packet type	Processing way
Security mode	Untagged packets	If the source MAC addresses of the packets are OUI addresses that can be identified by the system, send the packets to the voice VLAN; otherwise, discard the packets.
	Packets with the voice VLAN tag	
Normal mode	Untagged packets	The packet source MAC address will not be checked, and all packets can be transmitted in the voice VLAN.
	Packets with the voice VLAN tag	

In the two modes, the port processes a packet with other VLAN tag in the same way, that is, forwards the packet if the VLAN is allowed on the port, or discards the packet if the VLAN is not allowed on the port.

It is recommended that you do not mix voice packets with other types of data in a voice VLAN. If necessary, please ensure that the security mode is disabled.

2.2 Configuring Voice VLAN

2.2.1 Configuration Prerequisites

- Create the corresponding VLAN before configuring the voice VLAN;
- As a default VLAN, VLAN 1 does not need to be created. However, it cannot be enabled with the voice VLAN feature.

2.2.2 Configuring Voice VLAN Mode on a Port to Automatic Mode

Follow these steps to set the port voice VLAN mode to automatic:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the aging time of the voice VLAN	**voice vlan aging** *minutes*	Optional Only applicable to ports in automatic mode and defaults to 1,440 minutes
Enable the security mode for the voice VLAN	**voice vlan security enable**	Optional Enabled by default
Configure the OUI address for the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, each voice VLAN has default OUI addresses configured. Refer to Table 2-1 for the default OUI addresses of different vendors.
Enable the voice VLAN feature globally	**voice vlan** *vlan-id* **enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port voice VLAN mode as automatic	**voice vlan mode auto**	Optional Automatic mode by default Different voice VLAN modes can be configured on different ports, independent of one another.

To do...	Use the command...	Remarks
Enable the voice VLAN feature on the port	**voice vlan enable**	Required Not enabled by default

Note:

- Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN. Because a protocol-based VLAN requires that the inbound packets on the Hybrid port are untagged packets (refer to section Protocol-Based VLAN Configuration), whereas the Hybrid port working in auto voice VLAN mode only supports to process tagged voice traffic.
- The default VLAN of a port in automatic mode cannot be configured as the voice VLAN. Otherwise, the system will prompt error information.

2.2.3 Configuring Voice VLAN Mode on a Port to Manual Mode

Follow these steps to set the port voice VLAN mode to manual:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the security mode of a voice VLAN	**voice vlan security enable**	Optional Enabled by default
Configure the OUI address of a voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, each voice VLAN has default OUI addresses configured. Refer to Table 2-1 for the default OUI addresses of different vendors.
Enable the voice VLAN feature globally	**voice vlan** *vlan-id* **enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the working mode as manual	**undo voice vlan mode auto**	Required Disabled by default

To do...		Use the command...	Remarks
Add the ports in manual mode to the voice VLAN	Access port	Refer to Configuring an Access-Port-Based VLAN.	Use one of the three approaches. After you add an Access port to the voice VLAN, the voice VLAN becomes the default VLAN of the port automatically.
	Trunk port	Refer to Configuring a Trunk-Port-Based VLAN.	
	Hybrid port	Refer to Configuring a Hybrid-Port-Based VLAN.	
Configure the voice VLAN as the default VLAN of the port	Trunk port	Refer to section Configuring a Trunk-Port-Based VLAN	Optional This operation is required if the inbound voice traffic is untagged. If the inbound voice traffic is tagged, do not configure the voice VLAN as the default VLAN of the port.
	Hybrid port	Refer to Configuring a Hybrid-Port-Based VLAN.	
Enable the voice VLAN feature on the port		**voice vlan enable**	Required

Note:

- Only one VLAN of a device can have the voice VLAN function enabled at a time, and the VLAN must be an exsiting static VLAN.
- A port that is in a link aggregation port group cannot have the voice VLAN feature enabled.
- If a port is enabled with voice VLAN and works in the manual voice VLAN mode, you need to add the port to the voice VLAN manually to make the voice VLAN takes effect on the port.

2.3 Displaying and Maintaining Voice VLAN

To do...	Use the command...	Remarks
Display the voice VLAN state	**display voice vlan state**	Available in any view
Display the OUI addresses currently supported by system	**display voice vlan oui**	Available in any view

2.4 Voice VLAN Configuration Examples

2.4.1 Automatic Voice VLAN Mode Configuration Example

I. Network requirement

- Create VLAN 2 and configure it as a voice VLAN with an aging time of 100 minutes.
- The voice traffic sent by the IP phones is tagged. Configure GigabitEthernet 1/0/1 as a Hybrid port and as the access port, with VLAN 6 as the default VLAN.
- The device allows voice packets from GigabitEthernet 1/0/1 with an OUI address of 0011-2200-0000 and a mask of ffff-ff00-0000 to be forwarded through the voice VLAN.

II. Network diagram

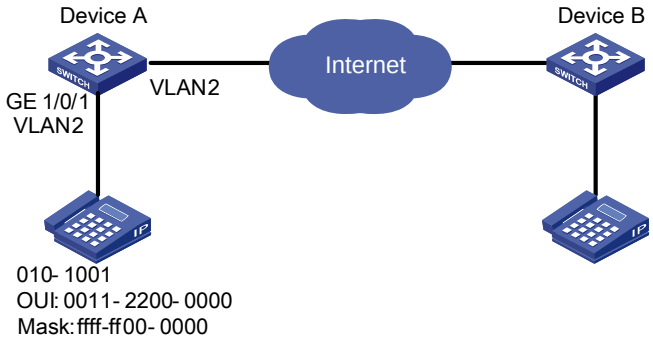

Figure 2-1 Network diagram for automatic voice VLAN mode configuration

III. Configuration procedure

Create VLAN 2 and VLAN 6.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 6
[DeviceA-vlan6] quit
```

Configure the voice VLAN aging time.

```
[DeviceA] voice vlan aging 100
```

Configure the OUI address 0011-2200-0000 as the legal address of the voice VLAN.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

Enable the voice VLAN feature globally.

```
[DeviceA] voice vlan 2 enable
```

Configure the voice VLAN mode on GigabitEthernet 1/0/1 as automatic. (Optional, by default, the voice VLAN mode on a port is automatic mode)

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] voice vlan mode auto
```

Configure GigabitEthernet 1/0/1 as a Hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type access
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

Configure the default VLAN of the port as VLAN 6 and allow packets from VLAN 6 to pass through the port.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 6
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 6 tagged
```

Enable the voice VLAN feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
[DeviceA-GigabitEthernet1/0/1] return
```

IV. Verification

Display information about the OUI addresses, OUI address masks, and descriptive strings.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0011-2200-0000  ffff-ff00-0000
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

Display the current Voice VLAN state.

```
<DeviceA> display voice vlan state
Voice VLAN status: ENABLE
 Voice VLAN ID: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 100 minutes
 Voice VLAN enabled port and its mode:
 PORT                    MODE
 --------------------------------
 GigabitEthernet1/0/1              AUTO
```

```
<DeviceA>
```

2.4.2 Manual Voice VLAN Mode Configuration Example

I. Network requirement

- Create VLAN 2 and configure it as a voice VLAN.
- The voice traffic sent by the IP phones is untagged. Configure GigabitEthernet 1/0/1 as a Hybrid port and as the access port.
- GigabitEthernet 1/0/1 works in manual mode. It only allows voice packets with an OUI address of 0011-2200-0000, a mask of ffff-ff00-0000, and a descriptive string of **test** to be forwarded through the voice VLAN.

II. Network diagram

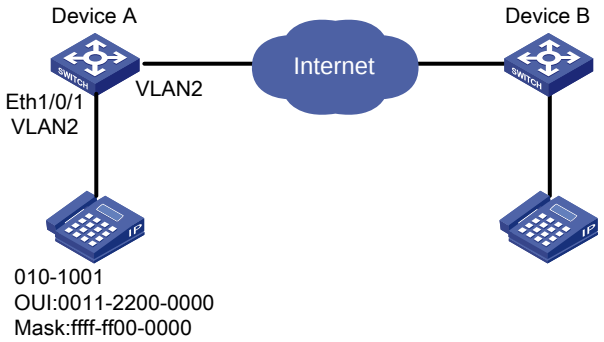

Figure 2-2 Network diagram for manual voice VLAN mode configuration

III. Configuration procedure

Configure the voice VLAN to work in security mode and only allows legal voice packets to pass through the voice VLAN enabled port. (Optional, enabled by default)

```
<DeviceA> system-view
[DeviceA] voice vlan security enable
```

Configure the OUI address 0011-2200-0000 as the legal voice VLAN address.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
description test
```

Create VLAN 2. Enable voice VLAN feature for it.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] voice vlan 2 enable
```

Configure GigabitEthernet 1/0/1 to work in manual mode.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice vlan mode auto
```

Configure GigabitEthernet 1/0/1 as a Hybrid port.

```
[DeviceA-GigabitEthernet1/0/1]port link-type access
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1]port link-type hybrid
```

Configure the default VLAN of GigabitEthernet 1/0/1 as voice VLAN and add the voice VLAN to the list of tagged VLANs whose packets can pass through the port.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

Enable the voice VLAN feature of GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
```

IV. Verification

Display information about the OUI addresses, OUI address masks, and descriptive strings.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0011-2200-0000  ffff-ff00-0000  test
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

Display the current voice VLAN state.

```
<DeviceA> display voice vlan state
Voice VLAN status: ENABLE
Voice VLAN ID: 2
Voice VLAN security mode: Security
Voice VLAN aging time: 100 minutes
Voice VLAN enabled port and its mode:
PORT               MODE
--------------------------------
GigabitEthernet1/0/1        MANUAL
```

Chapter 3 GVRP Configuration

GARP VLAN Registration Protocol (GVRP) is a GARP application. It functions based on the operating mechanism of GARP to maintain and propagate dynamic VLAN registration information for the GVRP devices on the network.

When configuring GVRP, go to these sections for information you are interested in:

3.1 Introduction to GVRP

3.1.1 GARP

Generic Attribute Registration Protocol (GARP) provides a mechanism that allows participants in a GARP application to distribute, propagate, and register with other participants in a bridged LAN the attributes specific to the GARP application, such as the VLAN or multicast address attribute.

GARP itself does not exist on a device as an entity. GARP-compliant participants are known as GARP applications. One example is GVRP. When a GARP participant is present on a port on your device, the port is regarded as a GARP participant.

I. GARP messages and timers

1) GARP messages

GARP participants exchange information through the following three types of messages: Join message, Leave message, and LeaveAll message.

- A GARP participant uses Join messages to have its attributes registered on other devices. A GARP participant also sends Join messages to register attributes on other GARP participants when it receives Join messages from other GARP participants or static attributes are configured on it.
- A GARP participant uses Leave messages to have its attributes deregistered on other devices. A GARP participant also sends Leave messages when it receives Leave messages from other GARP participants or static attributes are deregistered on it.
- LeaveAll messages are used to deregister all the attributes, through which all the other GARP participants begin to have all their attributes registered. A GARP

participant sends LeaveAll messages upon the expiration of the LeaveAll timer, which is triggered when the GARP participant is created.

Join messages, Leave messages, and LeaveAll message make sure the reregistration and deregistration of GARP attributes are performed in an orderly way.

Through message exchange, all attribute information that needs registration propagates to all GARP participants throughout a LAN.

2) GARP timers

The interval of sending of GARP messages is controlled by the following four timers:

- Hold timer — A GARP participant usually does not forwards a received registration request immediately after it receives a registration request, instead, it waits for the expiration of the hold timer. That is, a GARP participant sends Join messages when the hold timer expires. The Join message contains all the registration information received during the latest Hold timer cycle. Such a mechanism saves the bandwidth.
- Join timer — Each GARP participant sends a Join message twice for reliability sake and uses a join timer to set the sending interval. If the first Join message is not acknowledged after the interval defined by the Join timer, the GARP participant sends the second Join message.
- Leave timer — Starts upon receipt of a Leave message sent for deregistering some attribute information. If no Join message is received before this timer expires, the GARP participant removes the attribute information as requested.
- LeaveAll timer — Starts when a GARP participant starts. When this timer expires, the entity sends a LeaveAll message so that other participants can re-register its attribute information. Then, a LeaveAll timer starts again.

Note:

- The settings of GARP timers apply to all GARP applications, such as GVRP, on a LAN.
- Unlike other three timers, which are set on a port basis, the LeaveAll timer is set in system view and takes effect globally.
- A GARP participant may send LeaveAll messages at the interval set by its LeaveAll timer or the LeaveAll timer on another device on the network, whichever is smaller. This is because each time a device on the network receives a LeaveAll message it resets its LeaveAll timer.

II. Operating mechanism of GARP

The GARP mechanism allows the configuration of a GARP participant to propagate throughout a LAN quickly. In GARP, a GARP participant registers or deregisters its

attributes with other participants by making or withdrawing declarations of attributes and at the same time, based on received declarations or withdrawals, handles attributes of other participants. When a port receives an attribute declaration, it registers the attribute; when a port receives an attribute withdrawal, it deregisters the attribute.

GARP participants send protocol data units (PDU) with a particular multicast MAC address as destination. Based on this address, a device can identify to which GVRP application, GVRP for example, should a GARP PDU be delivered.

III. GARP message format

The following figure illustrates the GARP message format.

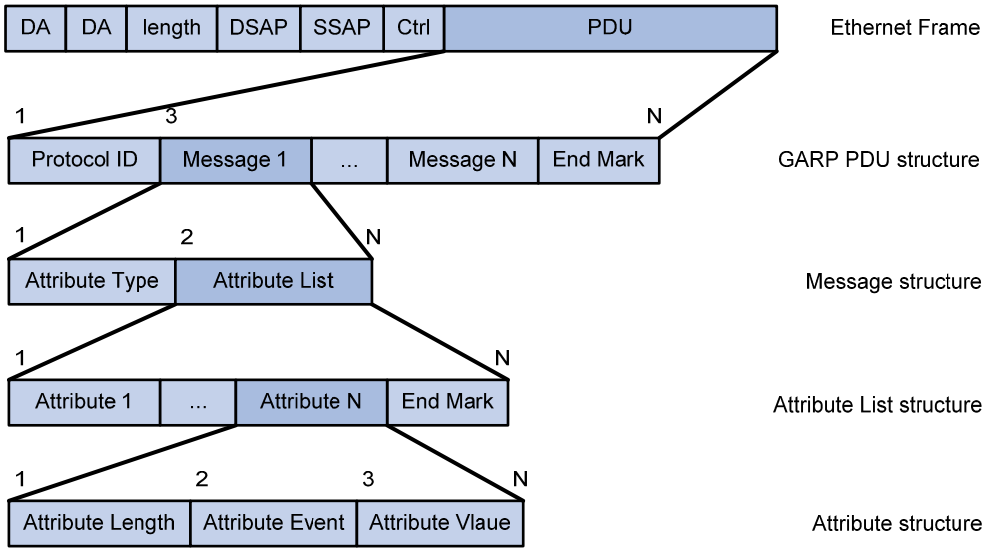

Figure 3-1 GARP message format

Table 3-1 describes the GARP message fields.

Table 3-1 Description on the GARP message fields

Field	Description	Value
Protocol ID	Protocol identifier for GARP	1
Message	One or multiple messages, each containing an attribute type and an attribute list	—
Attribute Type	Defined by the concerned GARP application	0x01 for GVRP, indicating the VLAN ID attribute
Attribute List	Contains one or multiple attributes	—

Field	Description	Value
Attribute	Consists of an Attribute Length, an Attribute Event, and an Attribute Value	—
Attribute Length	Number of octets occupied by an attribute, inclusive of the attribute length field	2 to 255 (in bytes)
Attribute Event	Event described by the attribute	0: LeaveAll event 1: JoinEmpty event 2: JoinIn event 3: LeaveEmpty event 4: LeaveIn event 5: Empty event
Attribute Value	Attribute value	VLAN ID for GVRP If the Attribute Event is LeaveAll, Attribute Value is omitted.
End Mark	Indicates the end of a GARP PDU	0x00

3.1.2 GVRP

GVRP enables a device to propagate local VLAN registration information to other participant devices and dynamically update the VLAN registration information from other devices to its local database about active VLAN members and through which port they can be reached. It thus ensures that all GVRP participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

GVRP provides the following three registration types on a port:

- Normal — Enables the port to dynamically register and deregister VLANs, and to propagate both dynamic and static VLAN information.
- Fixed — Disables the port to dynamically register and deregister VLANs or propagate information about dynamic VLANs, but allows the port to propagate information about static VLANs. A trunk port with fixed registration type thus allows only manually configured VLANs to pass through even though it is configured to carry all VLANs.
- Forbidden — Disables the port to dynamically register and deregister VLANs, and to propagate VLAN information except information about VLAN 1. A trunk port with

forbidden registration type thus allows only VLAN 1 to pass through even though it is configured to carry all VLANs.

3.1.3 Protocols and Standards

GVRP is described in IEEE 802.1Q.

3.2 GVRP Configuration Task List

Note:

GVRP can only be configured on Trunk ports.

Complete the following tasks to configure GVRP:

Task	Remarks
Enabling GVRP	Required
Configuring GARP Timers	Optional

3.3 Configuring GVRP

3.3.1 Enabling GVRP

Follow these steps to enable GVRP on a trunk port:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enable GVRP globally		**gvrp**	Required Globally disabled by default
Enter Ethernet port view or port-group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Use either command. In Ethernet port view, the subsequent configurations only apply to the current port; in port group view, the subsequent configurations apply to all ports in the port group.
	Enter port group view	**port-group** { **aggregation** *agg-id* | **manual** *port-group-name* }	
Enable GVRP on the port		**gvrp**	Required Disabled by default

To do…	Use the command…	Remarks
Configure the GVRP registration mode on the port	**gvrp registration** { **fixed** | **forbidden** | **normal** }	Optional The default is **normal**.

Note:

Because GVRP is not compatible with the BPDU tunneling feature, you must disable BPDU tunneling before enabling GVRP on a BPDU tunneling–enabled Ethernet port.

3.3.2 Configuring GARP Timers

Follow these steps to configure GARP timers:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Configure the GARP LeaveAll timer</td><td>garp timer leaveall timer-value</td><td>Optional
The default is 1000 centiseconds.</td></tr>
<tr><td rowspan="2">Enter Ethernet port view or port-group view</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td><td rowspan="2">Use either command.
In Ethernet port view, the subsequent configurations only apply to the current port; in port group view, the subsequent configurations apply to all ports in the port group.</td></tr>
<tr><td>Enter port-group view</td><td>port-group { manual port-group-name | aggregation agg-id }</td></tr>
<tr><td colspan="2">Configure the hold timer, join timer, and leave timer</td><td>garp timer { hold | join | leave } timer-value</td><td>Optional
The default is 10 centiseconds for the hold timer, 20 centiseconds for the join timer, and 60 centiseconds for the leave timer.</td></tr>
</table>

As for the GARP timers, note that:

- The setting of each timer must be a multiple of five (in centiseconds).
- The settings of the timers are correlated. If you fail to set a timer to a certain value, you can try to adjust the settings of the rest timers. Table 3-2 shows the relationship of the timers.

Table 3-2 Dependencies of GARP timers

Timer	Lower limit	Upper limit
Hold	10 centiseconds	Not greater than half of the join timer setting
Join	Not less than two times the hold timer setting	Less than half of the leave timer setting
Leave	Greater than two times the join timer setting	Less than the LeaveAll timer setting
LeaveAll	Greater than the leave timer setting	32765 centiseconds

3.4 Displaying and Maintaining GVRP

To do…	Use the command…	Remarks
Display statistics about GARP	**display garp statistics** [**interface** *interface-list*]	Available in any view
Display GARP timers for specified or all ports	**display garp timer** [**interface** *interface-list*]	Available in any view
Display the local VLAN information maintained by GVRP	**display gvrp local-vlan interface** *interface-type interface-number*	Available in any view
Display the current GVRP state	**display gvrp state interface** *interface-type interface-number* **vlan** *vlan-id*	Available in any view
Display statistics about GVRP	**display gvrp statistics** [**interface** *interface-list*]	Available in any view
Display the global GVRP state	**display gvrp status**	Available in any view
Display the information about dynamic VLAN operations performed on a port	**display gvrp vlan-operation interface** *interface-type interface-number*	Available in any view
Clear the GARP statistics	**reset garp statistics** [**interface** *interface-list*]	Available in user view

3.5 GVRP Configuration Examples

3.5.1 GVRP Configuration Example I

I. Network requirements

Configure GVRP for dynamic VLAN information registration and update among devices, adopting the normal registration mode on ports.

II. Network diagram

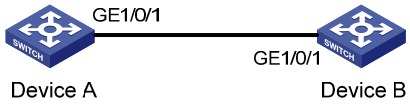

Figure 3-2 Network diagram for GVRP configuration

III. Configuration procedure

1) Configure Device A

Enable GVRP globally.

```
<DeviceA> system-view
[DeviceA] gvrp
```

Configure port GigabitEthernet 1/0/1 as a Trunk port, allowing all VLANs to pass.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1, the Trunk port.

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] quit
```

Create VLAN 2 (a static VLAN).

```
[DeviceA] vlan 2
```

2) Configure Device B

Enable GVRP globally.

```
<DeviceB> system-view
[DeviceB] gvrp
```

Configure port GigabitEthernet 1/0/1 as a Trunk port, allowing all VLANs to pass.

```
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1, the Trunk port.

```
[DeviceB-GigabitEthernet1/0/1] gvrp
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

Create VLAN 3 (a static VLAN).

```
[DeviceB] vlan 3
```

3) Verify the configuration

Display dynamic VLAN information on Device A.

```
[DeviceA] display vlan dynamic
 Now, the following dynamic VLAN exist(s):
  3
```

Display dynamic VLAN information on Device B.

```
[DeviceB] display vlan dynamic
 Now, the following dynamic VLAN exist(s):
  2
```

3.5.2 GVRP Configuration Example II

I. Network requirements

Configure GVRP for dynamic VLAN information registration and update among devices. Specify fixed GVRP registration on Device A and normal GVRP registration on Device B.

II. Network diagram

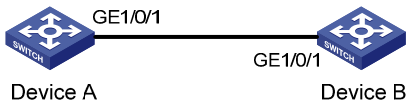

Figure 3-3 Network diagram for GVRP configuration

III. Configuration procedure

1) Configure Device A

Enable GVRP globally.

```
<DeviceA> system-view
[DeviceA] gvrp
```

Configure port GigabitEthernet 1/0/1 as a Trunk port, allowing all VLANs to pass.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] gvrp
```

Set the GVRP registration type to fixed on the port.

```
[DeviceA-GigabitEthernet1/0/1] gvrp registration fixed
[DeviceA-GigabitEthernet1/0/1] quit
```

Create VLAN 2 (a static VLAN).

```
[DeviceA] vlan 2
```

2) Configure Device B

Enable GVRP globally.

```
<DeviceB> system-view
[DeviceB] gvrp
```

Configure port GigabitEthernet 1/0/1 as a Trunk port, allowing all VLANs to pass.

```
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] quit
```

Create VLAN 3 (a static VLAN).

```
[Sysname] vlan 3
```

3) Verify the configuration

Display dynamic VLAN information on Device A.

```
[DeviceA] display vlan dynamic
 No dynamic vlans exist!
```

Display dynamic VLAN information on Device B.

```
[DeviceB] display vlan dynamic
 Now, the following dynamic VLAN exist(s):
  2
```

3.5.3 GVRP Configuration Example III

I. Network requirements

To prevent dynamic VLAN information registration and update among devices, set the GVRP registration mode to **forbidden** on Device A and **normal** on Device B.

II. Network diagram

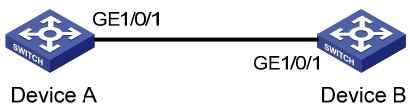

Figure 3-4 Network diagram for GVRP configuration

III. Configuration procedure

1) Configure Device A

Enable GVRP globally.

```
<DeviceA> system-view
[DeviceA] gvrp
```

Configure port GigabitEthernet 1/0/1 as a Trunk port, allowing all VLANs to pass.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] gvrp
```

Set the GVRP registration type to forbidden on the port.

```
[DeviceA-GigabitEthernet1/0/1] gvrp registration forbidden
[DeviceA-GigabitEthernet1/0/1] quit
```

Create VLAN 2 (a static VLAN).

```
[DeviceA] vlan 2
```

2) Configure Device B

Enable GVRP globally.

```
<DeviceB> system-view
[DeviceB] gvrp
```

Configure port GigabitEthernet 1/0/1 as a Trunk port, allowing all VLANs to pass.

```
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable GVRP on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] quit
```

Create VLAN 3 (a static VLAN).

```
[DeviceB] vlan 3
```

3) Verify the configuration

Display dynamic VLAN information on Device A.

```
[DeviceA] display vlan dynamic
 No dynamic vlans exist!
```

Display the VLANs allowed on GigabitEthernet 1/0/1.

```
[DeviceA] display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN
```

```
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 00e0-fc55-0010
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9212
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: trunk
  VLAN passing  : 1(default vlan)
  VLAN permitted: 1(default vlan)
(Omitted)
```

The above output indicates that port GigabitEthernet 1/0/1 only allows packets of VLAN 1 to pass.

Display dynamic VLAN information on Device B.

```
[DeviceB] display vlan dynamic
 No dynamic vlans exist!
```