

# Table of Contents

<b>Chapter 1 VLAN Configuration .....</b>	<b>1-1</b>
1.1 VLAN Overview.....	1-1
1.2 VLAN Configuration .....	1-1
1.2.1 Creating/Deleting a VLAN .....	1-1
1.2.2 Adding Ethernet Ports to a VLAN.....	1-2
1.2.3 Setting/Deleting VLAN or VLAN interface Description Character String .....	1-2
1.2.4 Specifying/Removing the VLAN Interface .....	1-2
1.2.5 Shutting down/Enabling the VLAN Interface .....	1-3
1.3 Displaying and Debugging VLAN .....	1-3
1.4 VLAN Configuration Example One .....	1-4
1.5 VLAN Configuration Example Two .....	1-4
<b>Chapter 2 Voice VLAN Configuration.....</b>	<b>2-1</b>
2.1 Voice VLAN Overview .....	2-1
2.2 Voice VLAN Configuration .....	2-2
2.2.1 Enabling/Disabling Voice VLAN Features.....	2-2
2.2.2 Enabling/Disabling Voice VLAN Features on a Port.....	2-2
2.2.3 Setting/Removing the OUI Address Learned by Voice VLAN .....	2-3
2.2.4 Enabling/Disabling Voice VLAN Security Mode.....	2-3
2.2.5 Enabling/Disabling Voice VLAN Auto Mode .....	2-4
2.2.6 Setting the Aging Time of Voice VLAN .....	2-4
2.3 Displaying and Debugging of Voice VLAN .....	2-5
2.4 Voice VLAN Configuration Example .....	2-5
<b>Chapter 3 VLAN-VPN Configuration.....</b>	<b>3-1</b>
3.1 VLAN-VPN Overview .....	3-1
3.1.1 Introduction to VLAN-VPN .....	3-1
3.1.2 Implementation of VLAN-VPN.....	3-1
3.2 VLAN-VPN Configuration .....	3-2
3.2.1 Configuration Prerequisites .....	3-2
3.2.2 Configuration Procedure .....	3-2
3.3 Inner VLAN Tag Priority Replication Configuration .....	3-3
3.3.1 Configuration Prerequisites .....	3-3
3.3.2 Configuration Procedure .....	3-3
3.4 VLAN-VPN Configuration Example .....	3-3

# Chapter 1 VLAN Configuration

## 1.1 VLAN Overview

Virtual Local Area Network (VLAN) groups the devices of a LAN logically but not physically into segments to implement the virtual workgroups. IEEE issued the IEEE 802.1Q in 1999, which was intended to standardize VLAN implementation solutions.

Through VLAN technology, network managers can logically divide the physical LAN into different broadcast domains. Every VLAN contains a group of workstations with the same demands. The workstations of a VLAN do not have to belong to the same physical LAN segment.

With VLAN technology, the broadcast and unicast traffic within a VLAN will not be forwarded to other VLANs, therefore, it is very helpful in controlling network traffic, saving device investment, simplifying network management and improving security.

## 1.2 VLAN Configuration

VLAN configuration includes:

- Creating/deleting a VLAN
- Adding Ethernet ports to a VLAN
- Setting/deleting VLAN or VLAN interface description character string
- Specifying/removing a VLAN interface
- Shutting down/enabling a VLAN Interface

To configure a VLAN, first create a VLAN according to the requirements.

### 1.2.1 Creating/Deleting a VLAN

You can use the following command to create/delete a VLAN. If the VLAN to be created exists, enter the VLAN view directly. Otherwise, create the VLAN first, and then enter the VLAN view.

Perform the following configurations in system view.

**Table 1-1** Creating/deleting a VLAN

Operation	Command
Create a VLAN and enter the VLAN view	<b>vlan</b> <i>vlan_id</i>
Delete the specified VLAN	<b>undo vlan</b> { <i>vlan_id</i> [ <b>to</b> <i>vlan_id</i> ]   <b>all</b> }

Note that the default VLAN, namely VLAN 1, cannot be deleted.

## 1.2.2 Adding Ethernet Ports to a VLAN

You can use the following command to add the Ethernet ports to a VLAN.

Perform the following configuration in VLAN view.

**Table 1-2** Adding Ethernet ports to a VLAN

Operation	Command
Add Ethernet ports to a VLAN	<b>port</b> <i>interface_list</i>
Remove Ethernet ports from a VLAN	<b>undo port</b> <i>interface_list</i>

By default, the system adds all the ports to a default VLAN, whose ID is 1.

Note that you can add/delete trunk port and hybrid port to/from VLAN by **port** and **undo port** commands in Ethernet port view, but not in VLAN view.

## 1.2.3 Setting/Deleting VLAN or VLAN interface Description Character String

You can use the following command to set/delete VLAN or VLAN interface description character string.

Perform the following configuration in VLAN or VLAN interface view.

**Table 1-3** Setting/deleting VLAN or VLAN interface description character string

Operation	Command
Set the description character string for VLAN or VLAN interface	<b>description</b> <i>string</i>
Restore the default description of current VLAN or VLAN interface	<b>undo description</b>

By default, VLAN description character string is "VLAN 0001". VLAN interface description character string of VLAN interface is the interface name, e.g. Vlan-interface1 Interface.

## 1.2.4 Specifying/Removing the VLAN Interface

You can use the following command to specify/remove the VLAN interface. To implement the network layer function on a VLAN interface, VLAN interface should be set the IP address and mask. For corresponding configuration, refer to "Network protocol" in this manual.

Perform the following configurations in system view.

**Table 1-4** Specifying/removing the VLAN interface

Operation	Command
Create a new VLAN interface and enter VLAN interface view	<b>interface Vlan-interface</b> <i>vlan_id</i>
Remove the specified VLAN interface	<b>undo interface Vlan-interface</b> <i>vlan_id</i>

Create a VLAN first before create an interface for it.

For this configuration task, *vlan\_id* takes the VLAN ID.

## 1.2.5 Shutting down/Enabling the VLAN Interface

You can use the following command to shut down/enable VLAN interface.

Perform the following configuration in VLAN interface view.

**Table 1-5** Shutting down/enabling the VLAN interface

Operation	Command
Shut down the VLAN interface	<b>shutdown</b>
Enabling the VLAN interface	<b>undo shutdown</b>

The operation of shutting down or enabling the VLAN interface has no effect on the UP/DOWN status of the Ethernet ports on the local VLAN.

By default, when all the Ethernet ports belonging to a VLAN are in DOWN status, this VLAN interface is also DOWN, i.e. this VLAN interface is shut down. When there is one or more Ethernet ports in UP status, this VLAN interface is also UP, i.e. this VLAN interface is enabled.

## 1.3 Displaying and Debugging VLAN

After the above configuration, execute **display** command in any view to display the running of the VLAN configuration, and to verify the effect of the configuration.

**Table 1-6** Displaying and debugging VLAN

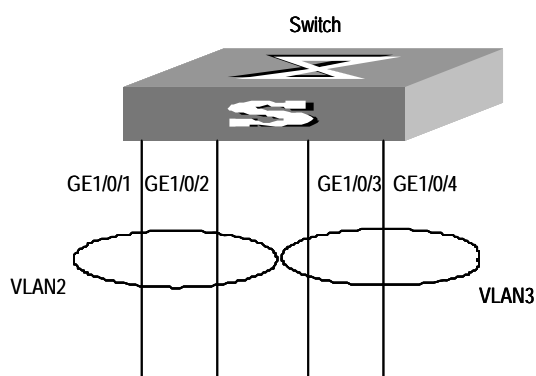
Operation	Command
Display the related information about VLAN interface	<b>display interface Vlan-interface</b> [ <i>vlan_id</i> ]
Display the related information about VLAN	<b>display vlan</b> [ <i>vlan_id</i> [ <i>to vlan_id</i> ]   <b>all</b>   <b>static</b>   <b>dynamic</b> ]

## 1.4 VLAN Configuration Example One

### I. Networking requirements

Create VLAN2 and VLAN3. Add GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to VLAN2 and add GigabitEthernet1/0/3 and GigabitEthernet1/0/4 to VLAN3.

### II. Networking diagram



**Figure 1-1** VLAN configuration example one

### III. Configuration procedure

# Create VLAN 2 and enters its view.

```
[Quidway] vlan 2
```

# Add GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to VLAN2.

```
[Quidway-vlan2] port gigabitethernet1/0/1 to gigabitethernet1/0/2
```

# Create VLAN 3 and enters its view.

```
[Quidway-vlan2] vlan 3
```

# Add GigabitEthernet1/0/3 and GigabitEthernet1/0/4 to VLAN3.

```
[Quidway-vlan3] port gigabitethernet1/0/3 to gigabitethernet1/0/4
```

## 1.5 VLAN Configuration Example Two

### I. Networking requirements

Create VLAN3. Configure an IP address and subnet mask for the VLAN3 interface.

### II. Networking diagram

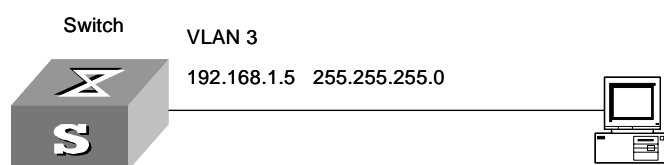


Figure 1-2 VLAN configuration example two

### III. Configuration procedure

# If the VLAN does not currently exist, then create it. This example uses VLAN ID

3.

```
[Quidway] vlan 3
```

```
[Quidway-vlan3] quit
```

# Enter the VLAN interface view.

```
[Quidway-vlan3] interface Vlan-interface 3
```

# Configure the IP address and subnet mask.

```
[Quidway-Vlan-interface3] ip address 192.168.1.5 255.255.255.0
```

```
[Quidway-Vlan-interface3] quit
```

## Chapter 2 Voice VLAN Configuration

### 2.1 Voice VLAN Overview

Voice VLAN is specially designed for user's voice flow, and it distributes different port precedence in different cases.

The system uses the source MAC of the traffic traveling through the port to identify the IP Phone data flow. You can either preset an OUI address or adopt the default OUI address as the standard. Here the OUI address refers to that of a vendor.

Voice VLAN can be configured either manually or automatically. In auto mode, the system learns the source MAC address and automatically adds the ports to a Voice VLAN using the untagged packets sent out when IP Phone is powered on; in manual mode, however, you need to add ports to a Voice VLAN manually. Both of the modes forward the tagged packets sent by IP Phone without learning the address.

Since there are multiple types of IP Phones, you must ensure that the mode on a port matches the IP Phone. Please see the following table:

**Table 2-1** The corresponding between port mode and IP Phone

Voice VLAN Mode	Type of IP Phone	Port Mode
Auto mode	Tagged IP Phone	Access: Do not support
		Trunk: Support, but the default VLAN of the connected port must exist and cannot be the voice VLAN. The default VLAN is allowed to pass the connected port.
		Hybrid: Support, but the default VLAN of the connected port must exist and it is in the tagged VLAN list which is allowed to pass the connected port.
	Untagged IP Phone	Access, Trunk, and Hybrid: Do not support, because the default VLAN of the connected port must be the Voice VLAN, and the connected port belongs to the Voice VLAN, that is, user add the port to the Voice VLAN manually.

Voice VLAN Mode	Type of IP Phone	Port Mode
Manual mode	Tagged IP Phone	Access: Do not support
	Untag IP Phone Untagged IP Phone	Trunk: Support, but the default VLAN of the connected port must exist and cannot be the voice VLAN. The default VLAN is allowed to pass the connected port.
		Hybrid: Support, but the default VLAN of the connected port must exist and it is in the tagged VLAN list which is allowed to pass the connected port.
		Access: Support, but the default VLAN of the connected port must be the Voice VLAN.

## 2.2 Voice VLAN Configuration

The configuration of Voice VLAN includes:

- Enable/disable Voice VLAN features globally
- Enable/disable Voice VLAN features on a port
- Set/remove the OUI address learned by Voice VLAN
- Enable/disable Voice VLAN security mode
- Enable/disable Voice VLAN auto mode
- Set the aging time of Voice VLAN

If you change the status of Voice VLAN security mode, you must first enable Voice VLAN features globally.

### 2.2.1 Enabling/Disabling Voice VLAN Features

Enable/disable the Voice VLAN in system view.

**Table 2-2** Configuring Voice VLAN features

Operation	Command
Enable Voice VLAN features	<b>voice vlan <i>vlan_id</i> enable</b>
Disable Voice VLAN features	<b>undo voice vlan enable</b>

The VLAN must exist for a successful Voice VLAN features enabling. You cannot delete a specified VLAN that has enabled Voice VLAN features and only one VLAN can enable Voice VLAN at one time.



## 2.2.2 Enabling/Disabling Voice VLAN Features on a Port

Perform the following configuration in Ethernet port view.

**Table 2-3** Configuring Voice VLAN features on a port

Operation	Command
Enable the Voice VLAN features on a port	<b>voice vlan enable</b>
Disable the Voice VLAN features on a port	<b>undo voice vlan enable</b>

Only the Voice VLAN features in system view and port view are all enabled can the Voice VLAN function on the port run normally.

## 2.2.3 Setting/Removing the OUI Address Learned by Voice VLAN

Configure OUI addresses which can be learned by Voice VLAN using the following command; otherwise the system uses the default OUI addresses as the standard of IP Phone traffic.

The OUI address system can learn 16 MAC addresses at most.

Perform the following configuration in system view.

**Table 2-4** Configuring the OUI address learned by Voice VLAN

Operation	command
Set the OUI address learned by Voice VLAN	<b>voice vlan mac-address oui mask oui_mask [ description string ]</b>
Remove the OUI address learned by Voice VLAN	<b>undo voice vlan mac-address oui</b>

There are four default OUI addresses after the system starts:

**Table 2-5** Default OUI addresses

No.	OUI	Description
1	00:E0:BB	3com phone
2	00:03:6B	Cisco phone
3	00:E0:75	Polycom phone
4	00:D0:1E	Pingtel phone

## 2.2.4 Enabling/Disabling Voice VLAN Security Mode

In security mode, the system can filter out the traffic whose source MAC is not OUI within the Voice VLAN, while the other VLANs are not influenced. Disabling security mode, the system cannot filter anything.

Perform the following configuration in system view.

**Table 2-6** Configuring the Voice VLAN security mode

Operation	Command
Enable Voice VLAN security mode	<b>voice vlan security enable</b>
Disable Voice VLAN security mode	<b>undo voice vlan security enable</b>

By default, the Voice VLAN security mode is enabled.

## 2.2.5 Enabling/Disabling Voice VLAN Auto Mode

In auto mode, if you enable Voice VLAN features on a port and there is IP Phone traffic through the port, the system automatically adds the port to the Voice VLAN. But in manual mode, you have to perform the above operation manually.

Perform the following configuration in system view.

**Table 2-7** Configuring the Voice VLAN auto mode

Operation	Command
Enable the Voice VLAN auto mode	<b>voice vlan mode auto</b>
Disable the Voice VLAN auto mode (that is, to enable manual mode)	<b>undo voice vlan mode auto</b>

By default, the Voice VLAN auto mode is enabled.

## 2.2.6 Setting the Aging Time of Voice VLAN

In auto mode, using the follow command, you can set the aging time of Voice VLAN. After the OUI address, the MAC address of IP Phone, is aged on the port, this port enters the aging phase of Voice VLAN. If OUI address is not learned by a port within the aging time, the port is automatically deleted from Voice VLAN. This command does not make sense in manual mode.

Perform the following configuration in system view.

**Table 2-8** Configuring the aging time of Voice VLAN

Operation	command
Set the aging time of Voice VLAN	<b>voice vlan aging</b> <i>minutes</i>
Restore the default aging time	<b>undo voice vlan aging</b>

The default aging time is 1440 minutes.

## 2.3 Displaying and Debugging of Voice VLAN

Finishing the above configuration, use the **display** command in any view to view the configuration and running state of Voice VLAN.

**Table 2-9** Displaying Voice VLAN

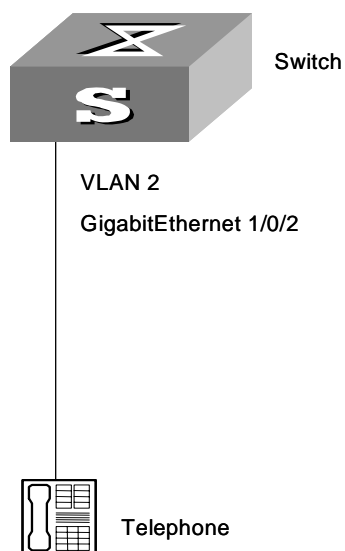
Operation	Command
Display the status of Voice VLAN	<b>display voice vlan status</b>
Display the OUI address supported by the current system	<b>display voice vlan oui</b>

## 2.4 Voice VLAN Configuration Example

### I. Networking Requirements

Create VLAN 2 as the Voice VLAN in manual mode and enable its security mode. It is required to set the aging time to 100 minutes, the OUI address to 0011-2200-0000, and configure the port GigabitEthernet1/0/2 as the IP Phone access port. The type of IP Phone is untagged.

## II. Network Diagram



**Figure 2-1** Voice VLAN Configuration

## III. Configuration Steps

```
[Quidway] vlan2
[Quidway-vlan2] port GigabitEthernet1/0/2
[Quidway-vlan2] interface GigabitEthernet1/0/2
[Quidway-GigabitEthernet1/0/2] voice vlan enable
[Quidway -GigabitEthernet1/0/2] quit
[Quidway] undo voice vlan mode auto
[Quidway] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
description private
[Quidway] voice vlan 2 enable
[Quidway] voice vlan aging 100
```

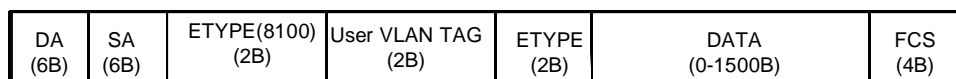
## Chapter 3 VLAN-VPN Configuration

### 3.1 VLAN-VPN Overview

#### 3.1.1 Introduction to VLAN-VPN

The VLAN-VPN function enables packets to be transmitted across the operators' backbone networks with VLAN tags of private networks nested in those of public networks. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks). And those of private networks, which are nested in the VLAN tags of public networks, remain intact.

Figure 3-1 describes the structure of the packets with single VLAN tags.



**Figure 3-1** Structure of packets with private network VLAN tags only

Figure 3-2 describes the structure of the packets with nested VLAN tags.



**Figure 3-2** Structure of packets with nested VLAN tags

Compared with MPLS-based L2VPN, VLAN-VPN has the following features:

- It allows Layer 2 VPN tunnels that are simpler.
- VLAN-VPN can be implemented without the support of signaling protocols. You can enable VLAN-VPN by static configuring.

The VLAN-VPN function provides you with the following benefits:

- Saves public network VLAN ID resource.
- You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
- Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.

### 3.1.2 Implementation of VLAN-VPN

VLAN-VPN can be implemented by enabling the VLAN-VPN function on ports.

With the VLAN-VPN function enabled, a received packet is tagged with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag. If the packet already carries a VLAN tag, the inserted VLAN tag becomes a nested VLAN tag in the packet. Otherwise, the packet is then transmitted with the default VLAN tag of the port carried.

## 3.2 VLAN-VPN Configuration

### 3.2.1 Configuration Prerequisites

GARP VLAN registration protocol (GVRP), GARP multicast registration protocol (GMRP), intelligent resilient framework (IRF), neighbor topology discovery protocol (NTDP), spanning tree protocol (STP) and 802.1x protocol are disabled on the port.



#### Caution:

By default, STP and NTDP are enabled on a device. You can disable these two protocols using the **stp disable** and **undo ntdp enable** commands.

### 3.2.2 Configuration Procedure

**Table 3-1** Configure the VLAN-VPN function for a port

Operation	Command	Description
Enter system view	<b>system-view</b>	—
Enter Ethernet port view	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	—
Enable the VLAN-VPN function	<b>vlan-vpn enable</b>	Required  By default, the VLAN-VPN function is disabled on a port.  The VLAN-VPN function is applicable to access ports only.

Display VLAN VPN configuration information about all ports	<b>display port vlan-vpn</b>	You can execute the <b>display</b> command in any view.
------------------------------------------------------------	------------------------------	---------------------------------------------------------



#### Caution:

The VLAN-VPN function is unavailable if the port has any of the protocols among GVRP, GMRP, IRF, NTDP, STP and 802.1x enabled.

## 3.3 Inner VLAN Tag Priority Replication Configuration

You can configure to replicate the tag priority of the inner VLAN tag of a VLAN-VPN packet to the outer VLAN tag to remain the original tag priority after the packet is inserted an outer VLAN tag.

### 3.3.1 Configuration Prerequisites

The VLAN-VPN function is enabled.

### 3.3.2 Configuration Procedure

**Table 3-2** Configure to replicate the tag priority of the inner VLAN tag

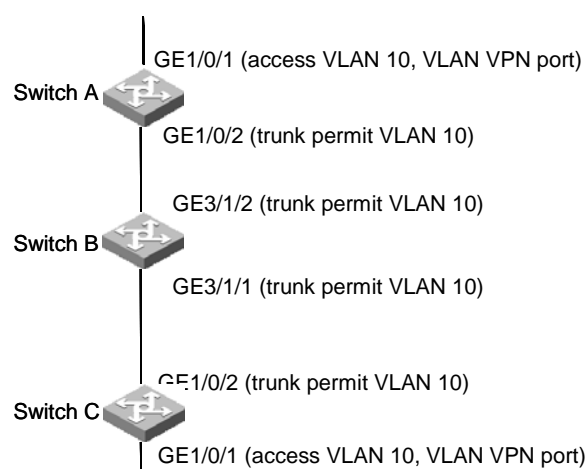
Operation	Command	Description
Enter system view	<b>system-view</b>	—
Enter Ethernet port view	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	—
Enable the inner VLAN Tag priority replication function	<b>vlan-vpn</b> <b>inner-cos-trust enable</b>	Required  By default, the inner VLAN tag priority replicating function is disabled. And the priority of an outer VLAN tag is that of the default priority of the current port.
Display the VLAN-VPN configuration information about all ports	<b>display port vlan-vpn</b>	You can execute the <b>display</b> command in any view.

## 3.4 VLAN-VPN Configuration Example

### I. Network requirements

- Switch A, Switch B and Switch C all are S5600 series switches.
- Two networks are connected to the GigabitEthernet1/0/1 ports of Switch A and Switch C respectively.
- Switch B only permits packets of VLAN 10.
- It is desired that packets of VLANs other than VLAN 10 can be exchanged between the networks connected to Switch A and Switch C.

### II. Network diagram



**Figure 3-3** Network diagram for VLAN-VPN configuration

### III. Configuration procedure

#### 1) Configure Switch A and Switch C

As the configuration performed on Switch A and Switch C is the same, configuration on Switch C is omitted.

# Configure GigabitEthernet1/0/2 port of Switch A to be a trunk port and add it to VLAN 10.

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 10
```



# Configure GigabitEthernet1/0/1 port of Switch A to be a VLAN-VPN port and add it to VLAN 10.

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] port access vlan 10
[SwitchA-GigabitEthernet1/0/1] vlan-vpn enable
[SwitchA-GigabitEthernet1/0/1] quit
```

## 2) Configure Switch B

# Configure GigabitEthernet3/1/1 and GigabitEthernet3/1/2 ports of Switch B to be trunk ports and add these two ports to VLAN 10.

```
<SwitchB> system-view
System View: return to User View with Ctrl+Z.
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface GigabitEthernet3/1/1
[SwitchB-GigabitEthernet3/1/1] port link-type trunk
[SwitchB-GigabitEthernet3/1/1] port trunk permit vlan 10
[SwitchB-GigabitEthernet3/1/1] interface GigabitEthernet3/1/2
[SwitchB-GigabitEthernet3/1/2] port link-type trunk
[SwitchB-GigabitEthernet3/1/2] port trunk permit vlan 10
```

---

### Note:

The following describes how a packet is forwarded from Switch A to Switch C.

- As the GigabitEthernet1/0/1 port of Switch A is a VLAN-VPN port, when a packet reaches GigabitEthernet1/0/1 port of Switch A, it is tagged with the default VLAN tag of the port (VLAN 10, the outer tag) and is then forwarded to GigabitEthernet1/0/2 port.
- GigabitEthernet1/0/2 forwards the packet to the public network.
- The packet reaches GigabitEthernet3/1/2 port of Switch B. Switch B sends the packet to its GigabitEthernet3/1/1 port to enable the packet being forwarded in VLAN 10.
- The packet is forward from GigabitEthernet3/1/1 port of Switch B to the network on the other side and enters GigabitEthernet1/0/2 port of Switch C; Switch C sends the packet to its GigabitEthernet1/0/1 port by forwarding the packet in VLAN 10. As GigabitEthernet1/0/1 port is an access port, Switch C strips off the outer VLAN tag of the packet and restores the original packet.

It is the same case when a packet travel from Switch C to Switch A.

---

After the configuration, the networks connecting Switch A and Switch C can receive data packets from each other.