

Table of Contents

Chapter 1 VLAN-VPN Configuration	1-1
1.1 VLAN-VPN Overview	1-1
1.1.1 Introduction to VLAN-VPN	1-1
1.1.2 Implementation of VLAN-VPN	1-1
1.1.3 Adjusting the TPID Values of VLAN-VPN Packet	1-2
1.2 VLAN-VPN Configuration	1-2
1.2.1 Configuration Prerequisites	1-2
1.2.2 Configuration procedure	1-3
1.3 Inner VLAN Tag Priority Replication Configuration	1-3
1.3.1 Configuration Prerequisites	1-3
1.3.2 Configuration procedure	1-4
1.4 TPID Adjusting Configuration	1-4
1.4.1 Configuration Prerequisites	1-4
1.4.2 Configuration Procedure	1-4
1.5 VLAN-VPN Configuration Example	1-5
Chapter 2 VLAN-VPN Configuration Commands	2-1
2.1.1 display port vlan-vpn	2-1
2.1.2 vlan-vpn enable	2-2
2.1.3 vlan-vpn inner-cos-trust	2-2
2.1.4 vlan-vpn tpid	2-3
2.1.5 vlan-vpn uplink enable	2-4

Chapter 1 VLAN-VPN Configuration

1.1 VLAN-VPN Overview

1.1.1 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 1-1 describes the structure of the packets with single VLAN tags.

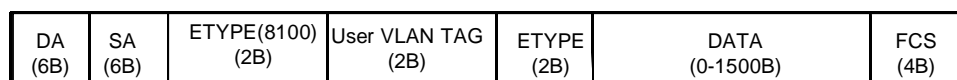


Figure 1-1 Structure of packets with private network VLAN tags only

Figure 1-2 describes the structure of the packets with nested VLAN tags.

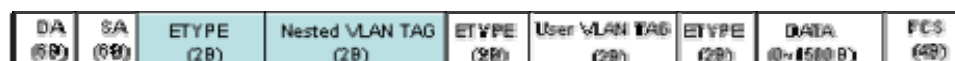


Figure 1-2 Structure of packets with nested VLAN tags

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.

1.1.2 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.

1.1.3 Adjusting the TPID Values of VLAN-VPN Packet

Tag protocol identifier (TPID) is a portion of the VLAN tag field. IEEE 802.1Q specifies the value of TPID to be 0x8100.

Figure 1-3 illustrates the structure of the Tag field of an Ethernet frame defined by IEEE 802.1Q.

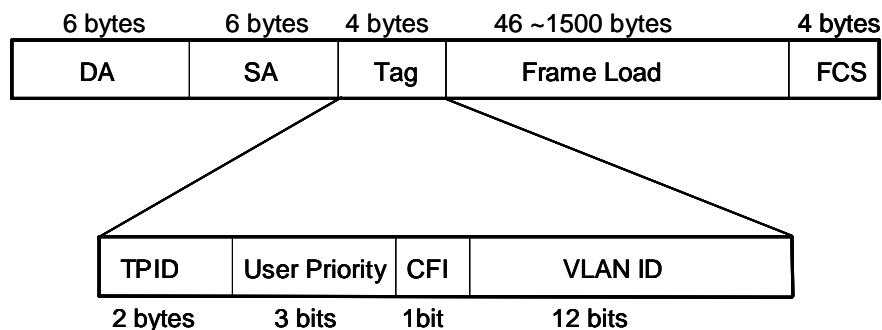


Figure 1-3 The structure of the Tag field of an Ethernet frame

As for S5600 series switches, the value of the TPID field is 0x8100, which is defined by IEEE 802.1Q. Other vendors use other TPID values (such as 0x9100 or 0x9200) in the outer tags of VLAN-VPN packets.

To be compatible with devices coming from other vendors, S5600 series switches can adjust the TPID values of VLAN-VPN packets. You can configure TPID value for ports connecting to the public networks to enable these ports to forward received packets after replacing the TPID values carried in the outer VLAN tags of the received packets with the user-defined TPID value, through which the VLAN-VPN packets sent to public networks can be recognized by devices of other vendors.

1.2 VLAN-VPN Configuration

1.2.1 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.
- The port is not a VLAN-VPN uplink 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.

1.2.2 Configuration procedure

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

Operation	Command	Description
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the VLAN-VPN function	vlan-vpn enable	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	display port vlan-vpn	You can execute the display 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.

1.3 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.

1.3.1 Configuration Prerequisites

The VLAN-VPN function is enabled.

1.3.2 Configuration procedure

Table 1-2 Configure to replicate the tag priority of the inner VLAN tag

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

1.4 TPID Adjusting Configuration

1.4.1 Configuration Prerequisites

Before you configure a VLAN-VPN uplink port, make sure that:

- The VLAN-VPN function is not enabled.

1.4.2 Configuration Procedure

Table 1-3 Adjust TPID values for VLAN-VPN packets

Operation	Command	Description
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set a TPID value for the port	vlan-vpn tpid <i>value</i>	Required Do not set the TPID value to a value that conflicts with known protocol type values.
Set the port to be a VLAN-VPN uplink port	vlan-vpn uplink enable	Optional By default, the VLAN-VPN uplink function is disabled.

Operation	Command	Description
Display VLAN-VPN configuration information about all ports	display port vlan-vpn	You can execute the display command in any view.



Caution:

- You can execute the **vlan-vpn enable** or **vlan-vpn uplink enable** command for a port, but do not execute both of the two commands for a port.
- When the TPID field is set to the default value (that is, 0x8100), a port can serve as an uplink port no matter whether or not you enable the VLAN-VPN uplink function for the port. However, if the TPID field is not set to 0x8100, you need to enable the VLAN-VPN uplink function for the port if you want to make the port an uplink port.

1.5 VLAN-VPN Configuration Example

I. Network requirements

- Switch A and Switch C are S5600 series switches. Switch B is a switch comes from another vendor, which uses a TPID value of 0x9100.
- 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

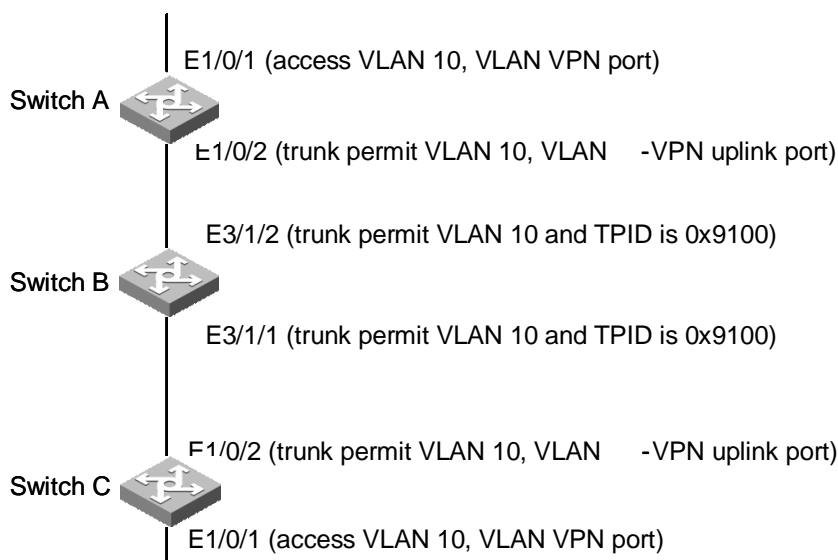


Figure 1-4 Network diagram for adjusting TPID values

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 VLAN-VPN uplink port and add it to VLAN 10. Set the TPID value of the port to 0x9100.

```
<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] vlan-vpn tpid 9100
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-GigabitEthernet1/0/2] vlan-vpn uplink enable
```

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

Because Switch B comes from another vendor, the commands involved may differ from those for S5600 switches. So only the operations are listed, as shown below:

- Configure Ethernet3/1/1 and Ethernet3/1/2 ports of Switch B to be trunk ports.
- Add the two ports to 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 Ethernet1/0/1 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.
- Because GigabitEthernet1/0/2 port is a VLAN-VPN uplink port with a TPID of 0x9100, Switch A changes the TPID value in the outer VLAN Tag of the packet to 0x9100 and forwards the packet to the public network.
- The packet reaches Ethernet3/1/2 port of Switch B. Switch B sends the packet to its Ethernet3/1/1 port to enable the packet being forwarded in VLAN 10.
- The packet is forwarded from Ethernet3/1/1 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.

Chapter 2 VLAN-VPN Configuration Commands

2.1.1 display port vlan-vpn

Syntax

display port vlan-vpn

View

Any view

Parameter

None

Description

Use the **display port vlan-vpn** command to display the information about VLAN VPN configuration of the current system, including current IPID value, VLAN-VPN ports, VLAN-VPN uplink ports and whether the inner tag priority replication function is enabled.

Example

Display the VLAN-VPN configuration of the system.

```
<Quidway> display port vlan-vpn
GigabitEthernet1/0/1
  VLAN-VPN TPID: 8100

GigabitEthernet1/0/2
  VLAN-VPN status: enabled
  VLAN-VPN VLAN: 1
  VLAN-VPN inner-cos-trust status: disable
  VLAN-VPN TPID: 8100

GigabitEthernet1/0/3
  VLAN-VPN TPID: 8100

GigabitEthernet1/0/4
  VLAN-VPN TPID: 8100
.....(Omitted)
```

2.1.2 vlan-vpn enable

Syntax

vlan-vpn enable

undo vlan-vpn

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn enable** command to enable the VLAN-VPN function for a port.

Use the **undo vlan-vpn** command to disable the VLAN-VPN function for a port.

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 transmitted with the default VLAN tag of the port carried.



Caution:

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

By default, the VLAN-VPN function is disabled.

Example

Enable the VLAN-VPN function for GigabitEthernet1/0/1 port.

```
<Quidway> system-view
```

```
System View: return to User View with Ctrl+Z.
```

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

```
[Quidway-GigabitEthernet1/0/1] vlan-vpn enable
```

2.1.3 vlan-vpn inner-cos-trust

Syntax

vlan-vpn inner-cos-trust enable

undo vlan-vpn inner-cos-trust

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn inner-cos-trust enable** command to enable the inner VLAN tag priority replication function.

Use the **undo vlan-vpn inner-cos-trust** command to disable the inner VLAN tag priority replication function.

Example

Enable the inner VLAN tag priority replication function for Ethernet 1/0/2 port.

```
<Quidway> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] interface GigabitEthernet 1/0/2
```

```
[Quidway-GigabitEthernet1/0/2] vlan-vpn inner-cos-trust enable
```

2.1.4 vlan-vpn tpid

Syntax

vlan-vpn tpid *value*

undo vlan-vpn tpid

View

Ethernet port view

Parameter

value: TPID value (in hexadecimal format) to be set, This argument ranges from 1 to 0xFFFF.

Description

Use the **vlan-vpn tpid** command to set a TPID value for a port. The setting takes effect only when the VLAN-VPN or VLAN-VPN uplink function is enabled.

Use the **undo vlan-vpn tpid** command to restore the default TPID value.

The default TPID value is 0x8100.

Do not set the TPID value to a value that conflicts with the known protocol type values (such as 0x0806, which is that of ARP packets). Otherwise, the packet may be discarded.

Table 2-1 Common Ethernet frame protocol type values

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

Example

Set the TPID value to 0x12 for Ethernet1/0/2 port.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface GigabitEthernet 1/0/2
[Quidway-GigabitEthernet1/0/2] vlan-vpn tpid 12
```

2.1.5 vlan-vpn uplink enable

Syntax

vlan-vpn uplink enable
undo vlan-vpn uplink

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn uplink enable** command to configure a port to be a VLAN-VPN uplink port.

Use the **undo vlan-vpn uplink** command to remove the configuration.

When sending a VLAN-VPN packet, a VLAN-VPN uplink port replaces the TPID value in the outer VLAN tag of the packet with the customized TPID value. You can use the **vlan-vpn tpid** command to set the TPID value used by the VLAN-VPN uplink port.



Caution:

The **vlan-vpn uplink enable** command and the **vlan-vpn enable** command are mutually exclusive. That is, if you execute the **vlan-vpn enable** command on a port, you will fail to execute the **vlan-vpn uplink enable** command on the same port. Similarly, if you execute the **vlan-vpn uplink enable** command on a port, you will fail to execute the **vlan-vpn enable** command on the same port.

Example

Configure GigabitEthernet1/0/2 port to be a VLAN-VPN uplink port.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway]interface GigabitEthernet 1/0/2
[Quidway-GigabitEthernet1/0/2] vlan-vpn uplink enable
VLAN-VPN uplink status: enabled
```