TP-LINK®

The Reliable Choice

Configuration Guide

Managing VLAN-VPN

T2500/T2600G/T2700G/T3700G Series Switches

CONTENTS

1 VLAN-VPN

1.1 Overview

VLAN-VPN (Virtual Private Network) is an easy-to-implement layer 2 VLAN technology, and it is usually deployed at the edge of the ISP (Internet Service Provider) network.

With VLAN-VPN, when forwarding packets from the customer network to the ISP network, the switch tags the packets with outer VLAN tags. Thus, packets can be transmitted through ISP networks with double VLAN tags. In the ISP network, packets are forwarded according to the outer VLAN tag (VLAN tag of the ISP network), while the inner VLAN tag is treated as part of the payload. When forwarding packets from the ISP network to the customer network, the switch remove the outer VLAN tag of the packets. Thus, packets are forwarded according to the inner VLAN tag (VLAN tag of the customer network) in the customer network.

Figure 1-1 shows the typical application scenario of VLAN-VPN. To realize the communication between two customer VLANs across the ISP network, you can configure VLAN-VPN at the ISP edge switches to allow packets from customer VLAN 100 and VLAN 200 to be forwarded through the ISP network with the outer tag of VLAN 1050.

Figure 1-1   Application Scenario of VLAN-VPN
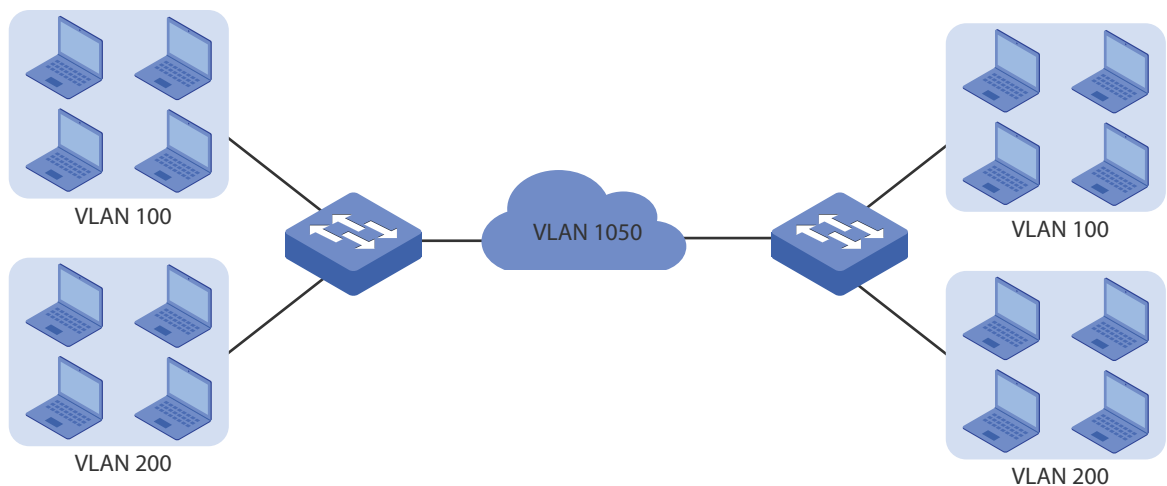
1.2   Supported Features

The VLAN-VPN function includes: basic VLAN-VPN and flexible VLAN-VPN (VPN mapping).

Basic VLAN-VPN

All packets from customer VLANs are encapsulated with the same VLAN tag of the ISP network, and sent to the ISP network. Additionally, you can set the TPID (Tag Protocol Identifier) of to-be-sent packets for compatibility with devices in the ISP network.

Flexible VLAN-VPN

You can configure different VLANs in the customer network to map to different VLANs in the ISP network. When the switch receives a customer VLAN tagged packet, the switch will encapsulate the packet with the corresponding VLAN tag of the ISP network and forward it; when an untagged packet arrives, the switch will tag it with the default VLAN tag of the receiving port.

2 Basic VLAN-VPN Configuration

To complete the basic VLAN-VPN configuration, follow these steps:

1) Configure 802.1Q VLAN.

2) Configure VPN up-link ports and VPN ports.

3) Enable VLAN-VPN globally.

Configuration Guidelines

The TPID preset by the switch is 0x8100. If devices in the ISP network do not support the value, you should change it to ensure VLAN-VPN packets sent to the ISP network can be recognized and forwarded by devices of other manufacturers.

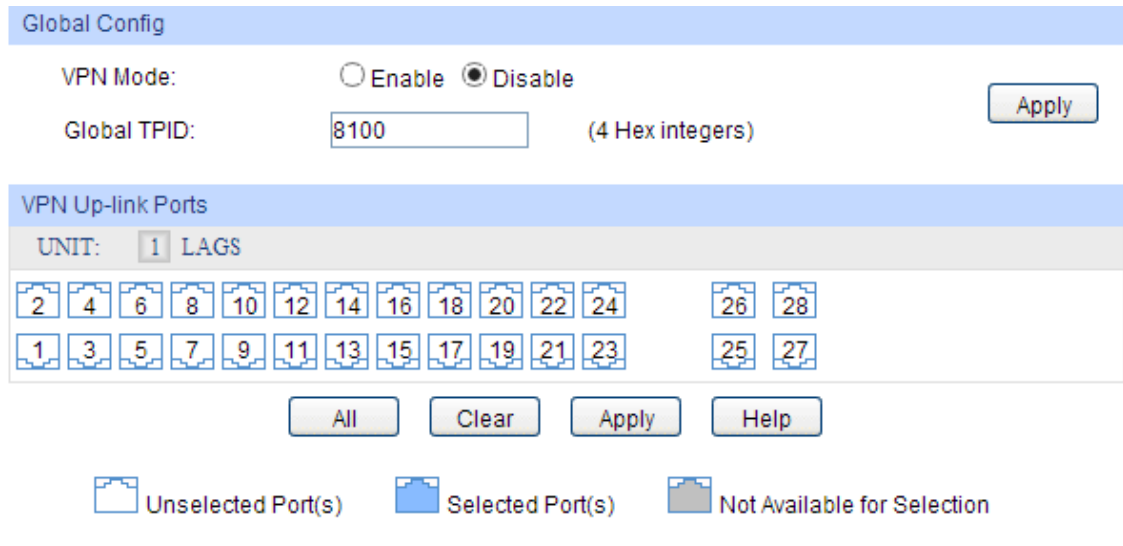## 2.1 Using the GUI

2.1.1 Configuring 802.1Q VLAN

Before configuring VLAN-VPN, set the link type of ports according to network requirements, and create an 802.1Q VLAN as ISP network VLAN and an 802.1Q VLAN as customer network VLAN. Add ports connecting the customer network to the customer network VLAN; add ports connecting the customer network and ports connecting the ISP network to the ISP network VLAN.

For details, refer to *Managing 802.1Q VLAN*.

2.1.2 Configuring Global VLAN-VPN and Up-link Ports

Choose the menu **VLAN > VLAN-VPN > VPN Config** to load the following page.

Figure 2-1   Global VPN Configuration

Follow these steps to configure the global VLAN-VPN parameters and up-link ports:

1) In the **Global Config** section, enable VPN mode in the Global Config section, modify the TPID value for compatibility with devices in the ISP network, and click **Apply**.

VPN Mode	VLAN-VPN works only when the VPN mode is enabled.
Global TPID	Set the global TPID which is used to identify the protocol of the tag. The default value is 0x8100 in hexadecimal format. You can modify it if needed. Before a VPN up-link port forwards a packet, the port will replace its TPID value in the outer VLAN tag with the user-defined value.

2) In the **VPN Up-link Ports** section, set ports that are connected to the ISP network as VPN up-link ports. Click **Apply**.

VPN Up-link Port	VPN up-link ports are usually connected to the ISP network , and packets sent out from these ports will be tagged with the outer VLAN tag of the ISP network.

Note:

For T2600G series switches, the member pot of an LAG (Link Aggregation Group) follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

2.1.3 Configuring VPN Ports

Choose the menu **VLAN > VLAN-VPN > Port Enable** to load the following page.

Figure 2-2   Enabling VPN Ports

Follow these steps to configure VPN ports:

Select ports that are connected to the customer network and click **Apply** to enable the VLAN-VPN feature on the selected ports.

VPN Port	VPN ports are usually connected to the customer network.

Note:

For T2600G series switches, the member pot of an LAG follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

2.2   Using the CLI

2.2.1 Configuring 802.1Q VLAN

Before configuring VLAN-VPN, set the link type of ports according to network requirements, and create an 802.1Q VLAN as ISP network VLAN and an 802.1Q VLAN as customer network VLAN. Add ports connecting the customer network to the customer network VLAN; add ports connecting the customer network and ports connecting the ISP network to the ISP network VLAN.

For details, refer to *Managing 802.1Q VLAN*.

2.2.1 Configuring Basic VLAN-VPN

Follow these steps to configure basic VLAN-VPN:

Step 1	**configure**
	Enter global configuration mode.

Step 2	**dot1q-tunnel**
	Enable the VLAN-VPN feature globally.

Step 3	**dot1q-tunnel tpid** *num*
	(Optional) Set the TPID value globally.
	num: Set the global TPID which is used to identify the protocol of the tag. The default value is 0x8100 in hexadecimal format. You can modify it if needed. Before a VPN up-link port forwards a packet, the port will replace its TPID value in the outer VLAN tag with the user-defined value.

Step 4	**interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***]**
	Enter interface configuration mode for VPN up-link ports and VPN ports respectively.

For T2500 series switches:

switchport dot1q-tunnel mode uplink

Set ports that are connected to the ISP network as VPN up-link ports.

switchport dot1q-tunnel mapping

Set ports that are connected to the customer network as VPN ports.

Note:

One port cannot be set as VPN up-link port and VPN port simultaneously. To switch from the current mode to another mode, disable the current mode first. Use **no switchport dot1q-tunnel mode uplink** to disable the VPN up-link port mode; use **no switchport dot1q-tunnel mapping** to disable the VPN port mode.

For other series switches:

switchport dot1q-tunnel mode { *nni* **|** *uni* **}**

Set ports that are connected to the ISP network as VPN up-link ports, and ports that connected to the customer network as VPN ports.

nni: Set ports that are connected to the ISP network as VPN up-link ports.

uni: Set ports that are connected to the customer network as VPN ports.

Note:

The direct shift between ports modes uni and nni is not supported. To switch from the current mode to another mode, you can use **no switchport dot1q-tunnel mode** to disable the current mode.

Step 5	**end**
	Return to privileged EXEC mode.

Step 6	**copy running-config startup-config**
	Save the settings in the configuration file.

The following example shows how to enable the VLAN-VPN feature globally and set the TPID as 0x9100:

Switch#configure

Switch(config)#dot1q-tunnel

Switch(config)#dot1q-tunnel tpid 9100

Switch(config)#show dot1q-tunnel

 VLAN-VPN Mode: Enabled

 Global TPID: 0X9100

 Mapping Mode: Disabled

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to set port 1/0/1 of switch as the VPN port and 1/0/2 as the VPN up-link port (Exampled with T2600-28TS):

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#switchport dot1q-tunnel mode uni

Switch(config-if)#exit

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#switchport dot1q-tunnel mode nni

Switch(config-if)#show dot1q-tunnel interface

Port Type   Member

-------------   -------------------------

NNI   Gi1/0/2

UNI   Gi1/0/1

Switch(config-if)#end

Switch#copy running-config startup-config

3 Flexible VLAN-VPN Configuration

To complete the flexible VLAN-VPN configuration, follow these steps:

1) Configure 802.1Q VLAN and basic VLAN-VPN.

2) Configure VLAN mapping.

Configuration Guidelines

■ Before you start, configure 802.1Q VLAN and the basic VLAN-VPN.

Configure 802.1Q VLAN based on network requirements. Besides, VLAN mapping entries work only after you have set VPN up-link ports and VPN ports in the basic VLAN-VPN configuration and enabled the VPN feature globally.

■ With the flexible VLAN-VPN feature, the switch processes tagged packets and untagged packets differently.

With the flexible VLAN-VPN feature, when a VPN port receives a packet with the customer network tag, the switch will check the VLAN Mapping List. If a match is found, the switch encapsulates the packet with the corresponding VLAN tag of the ISP network, and forwards it to the corresponding port. If no match is found, the switch tags the packet according to PVID of the port.

For untagged packets, the switch processes them in rules of other VLAN types, such as Protocol VLAN, MAC VLAN, and 802.1Q VLAN.

3.1 Using the GUI

Choose the menu **VLAN > VLAN-VPN > VLAN Mapping** to load the following page.

Figure 3-1 Configuring Flexible VLAN-VPN

Follow these steps to configure flexible VLAN-VPN:

1) In the **Global Config** section, enable VLAN mapping globally and click **Apply**.

Note:

For T2500 series switches, VPN mapping is automatically enabled after the global VPN is enabled.

2) In the **VLAN Mapping Config** section, choose a VPN port to enable VLAN mapping. Enter customer network VLAN ID in the **C VLAN** field, enter ISP network VLAN ID in the **SP VLAN** field, and enter a name to identify the entry. Then click **Create** to add a mapping entry.

Port	Choose a VPN port to enable VLAN mapping. Usually, ports that are connected to the customer network are set as VPN ports. You can also enter the port number in 1/0/1 format. *Note:* For T2500 series switches, you need not choose any VPN port to enable VLAN mapping, VLAN mapping works for all VPN ports.
C_VLAN	Enter the VLAN ID of the customer network. When the specified port receives a packet from the VLAN, the switch will encapsulate the packet with the VLAN tag of the ISP VLAN based on the mapping entry.
SP_VLAN	Enter the VLAN ID of the ISP network.
Name	Enter a name of the mapping entry for identification.

3.2   Using the CLI

Follow these steps to configure flexible VLAN-VPN:

Step 1	**configure**
	Enter global configuration mode.

Step 2	For T2500 series switches:
	dot1q-tunnel mapping *c-vlan sp-vlan [descript]*
	Set global VLAN mapping. VLAN mapping works for all VPN ports, and it is automatically enabled after the global VPN is enabled.
	c vlan: Enter VLAN ID of the customer network.
	sp vlan: Enter VLAN ID of the ISP network.
	descript: Give a description of the mapping entry for identification.
	For other series switches :
	dot1q-tunnel mapping
	Enable VLAN mapping.
	interface [fastEthernet *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***]**
	Enter interface configuration mode.
	switchport dot1q-tunnel mapping *c-vlan sp-vlan [descript]*
	Set VLAN mapping entries for the specified port.
	c vlan: Enter VLAN ID of the customer network.
	sp vlan: Enter VLAN ID of the ISP network.
	descript: Give a description of the mapping entry for identification.

Step 3	**end**
	Return to privileged EXEC mode.

Step 4	**copy running-config startup-config**
	Save the settings in the configuration file.

The following example shows how to enable VLAN mapping and set a VLAN mapping entry named mapping1 on port 1/0/3 to map customer network VLAN 15 to ISP network VLAN 1040 (Exampled with T2600G-28TS):

Switch#configure

Switch(config)#dot1q-tunnel mapping

Switch(config)#show dot1q-tunnel

VLAN-VPN Mode: Enabled

Global TPID: 0X8100

Mapping Mode: Enabled

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#switchport dot1q-tunnel mapping 15 1040 mapping1

Switch(config-if)#show dot1q-tunnel mapping

Port   C-VLAN   SP-VLAN   Name

----------   ---------   -----------   -----------

 Gi1/0/3   15   1040   mapping1

Switch(config-if)#end

Switch#copy running-config startup-config

4 Configuration Example

4.1 Network Requirements

Two divisions of the company are located in different areas and have to communicate across an ISP network. A normal communication is required.

Figure 4-1 shows the network topology. Switches of the two divisions are connected to customer networks VLAN 100 and VLAN 200 respectively. And they communicate across ISP network VLAN 1050. Devices in the ISP network adopt TPID value 0x9100.

Figure 4-1   Network Topology
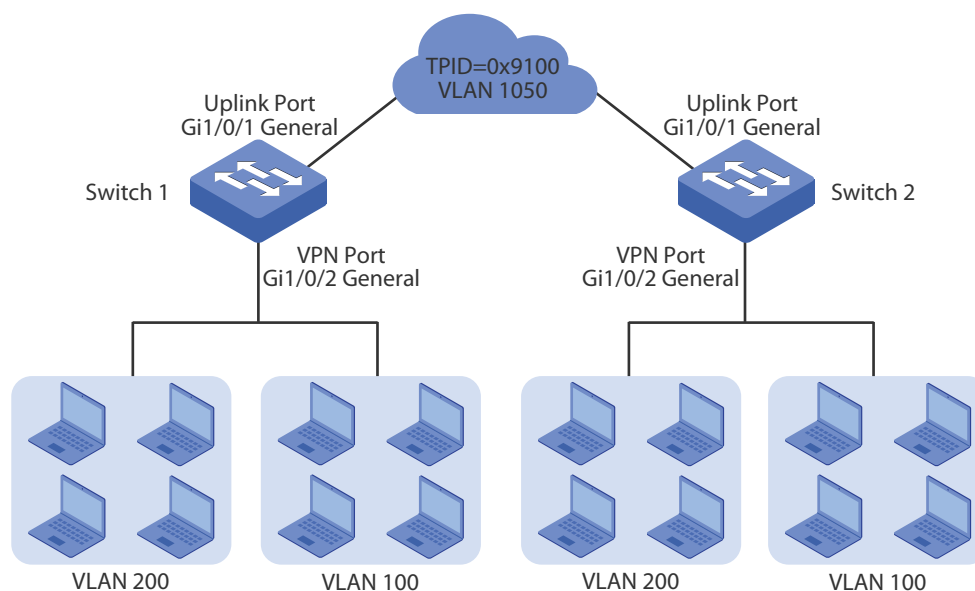
4.2 Configuration Scheme

Users can configure VLAN-VPN on Switch 1 and Switch 2 to allow packets sent with double VLAN tags, and thus ensure the communication between them. The general configuration procedure is as follows:

1) Configure 802.1Q VLAN before VLAN-VPN configuration. Create ISP network VLAN 1050 on the switch, and add port1/0/1 tagged and port 1/0/2 untagged to the VLAN. Create client network VLAN 100 and VLAN 200, and add port 1/0/2 tagged to both the VLANs. Set the PVID of port 1/0/1 and port 1/0/2 as 1050.

2) Set port 1/0/1 as the VPN up-link port and port 1/0/2 as the VPN port.

3) Enable the VPN feature globally, and set global TPID as 0x9100.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

4.3 Using the GUI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of ports 1/0/1-2 as General, and modify PVID of the two ports as 1050. Then click **Apply**.

Figure 4-2   Setting Link Type of Ports

2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 1050, and add port 1/0/1 tagged and port 1/0/2 untagged to the VLAN. Then click **Apply**.

Figure 4-3   Creating VLAN 1050

3) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 100, and add port 1/0/2 tagged to the VLAN. Click **Apply**.

Figure 4-4   Creating VLAN 100

4) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 200, and add port 1/0/2 tagged to the VLAN. Click **Apply**.

Figure 4-5   Creating VLAN 200

5) Choose the menu **VLAN > VLAN-VPN > VPN Config** to load the following page. Enable VPN globally, set TPID as 9100, and select port 1/0/1 as the up-link port. Click **Apply**.

Figure 4-6   Configuring Global VLAN-VPN

6) Choose the menu **VLAN > VLAN-VPN > Port Enable** to load the following page. Select port 1/0/2 and click **Apply**.

Figure 4-7   Enabling the VPN Port

7) Click **Save Config** to save the settings.

4.4   Using the CLI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

1) Create VLAN 1050, VLAN 100 and VLAN 200.

Switch_1#configure

Switch_1(config)#vlan 1050

Switch_1(config-vlan)#name SP_VLAN

Switch_1(config-vlan)#exit

Switch_1(config)#vlan 100

Switch_1(config-vlan)#name Client_VLAN100

Switch_1(config-vlan)#exit

Switch_1(config)#vlan 200

Switch_1(config-vlan)#name Client_VLAN200

Switch_1(config-vlan)#exit

2) Set the link type of port 1/0/1 as General, add it to VLAN 1050 as tagged port, modify PVID as 1050, and set the port as VPN up-link port.

Switch_1(config)#interface gigabitEthernet 1/0/1

Switch_1(config-if)#switchport mode general

Switch_1(config-if)#switchport general allowed vlan 1050 tagged

Switch_1(config-if)#switchport pvid1050

Switch_1(config-if)#switchport dot1q-tunnel mode nni

Switch_1(config-if)#exit

3) Set the link type of port 1/0/2 as general, add it to VLAN 1050 as untagged port, and add it to VLAN 100 and VLAN 200 as tagged port. Modify PVID of the port as 1050. Set the port as the VPN port.

Switch_1(config)#interface gigabitEthernet 1/0/2

Switch_1(config-if)#switchport mode general

Switch_1(config-if)#switchport general allowed vlan 1050 untagged

Switch_1(config-if)#switchport general allowed vlan 100,200 tagged

Switch_1(config-if)#switchport pvid 1050

Switch_1(config-if)#switchport dot1q-tunnel mode uni

Switch_1(config-if)#exit

4) Enable VLAN-VPN globally, and modify TPID as 9100.

Switch_1(config)#dot1q-tunnel

Switch_1(config)#dot1q-tunnel tpid 9100

Switch_1(config)#end

Switch_1#copy running-config startup-config

Verify the Configurations

Verify the configurations of global VLAN-VPN:

Switch_1#show dot1q-tunnel

VLAN-VPN Mode: Enabled

Global TPID: 0X9100

Mapping Mode: Disabled

Verify the configurations of VPN up-link port and VPN port:

Switch_1#show dot1q-tunnel interface

Port Type   Member
--------------   -----------------
NNI   Gi1/0/1
UNI   Gi1/0/2

5 Appendix: Default Parameters

Default settings of VLAN-VPN are listed in the following table.

Parameter	Default Setting
Global VLAN-VPN	Disable
VLAN Mapping	Disable
Global TPID	0x8100