

VLAN Configuration Commands

Table of Contents

1	VLAN Configuration.....	- 1 -
1.1	VLAN Overview.....	- 1 -
1.2	Dot1Q Tunnel Overview.....	- 2 -
1.2.1	Preface.....	- 2 -
1.2.2	Implementation of Dot1Q tunnel.....	- 2 -
1.2.3	TPID Value can be modified.....	- 3 -
1.3	VLAN Configuration Task List.....	- 4 -
1.4	VLAN Configuration Task.....	- 4 -
1.4.1	Adding/Deleting VLAN.....	- 4 -
1.4.2	Configuring Switch Port.....	- 5 -
1.4.3	Creating/Deleting VLAN Interface.....	- 6 -
1.4.4	Monitoring configuration and state of VLAN.....	- 6 -
1.4.5	Enable/ Disable Global Dot1Q Tunnel.....	- 6 -
1.4.6	Configuring flat N:1 VLAN Reversal Translation Function in Global.....	- 6 -
1.4.7	Configuring VLAN Translation Mode and Entry of Port.....	- 7 -
1.4.8	Configuring MAC-Based VLAN.....	- 7 -
1.4.9	Configuring IP Subnet-Based VLAN.....	- 8 -
1.4.10	Configuring Protocol-Based VLAN.....	- 9 -
1.5	Configuration Example.....	- 9 -
1.5.1	Example for Dot1Q Tunnel.....	- 9 -
Appendix A	Abbreviations.....	- 15 -

1 VLAN Configuration

1.1 VLAN Overview

VLAN (Virtual Local Area Network), that is, a virtual local area network, is a network which divides the equipment of the LAN logically rather than physically. IEEE in 1999 promulgated a draft standard for IEEE 802.1Q protocol for standardized VLAN implementation. VLAN technology can logically divide a physical LAN to different broadcast domains (VLAN). Each VLAN contains a group of devices with the same requirements that have the same attributes as the physically formed LAN. But it is logically Rather than physically partitioning, so the devices in the same VLAN need not to be placed in the same physical space, that is, these devices may not belong to the same physical LAN segment, a VLAN internal broadcast and unicast traffic will not be forwarded to other VLANs, which helps to control traffic, reduce equipment investment, simplify network management, and improve network security.

- Support port-based VLAN
- The port supports 802.1Q relay mode
- Support access port

Port-based VLANs are assigned to a subset of VLANs supported by the switch. If the VLAN subset has only one VLAN, then the port is the access port; if there are multiple VLANs in the VLAN subset, the port is a trunk port. And it has a default VLAN which is native VLAN of the port. The VLAN ID is the Port VLAN ID (PVID).

- Support controlling the range of the port VLAN.

The **vlan-allowed** parameter is used to control the range of VLANs which the port belongs to. The **vlan-untagged** parameter is used to control the port to sent packets without VLAN tag to the corresponding VLAN.

VLANs are divided into a variety of ways, based on the MAC address, based on IP subnet, based on protocol, based on port to divide VLANs. And the VLAN is divided according to the sequence of the MAC VLAN, IP subnet VLAN, protocol VLAN, and port VLAN by default.

1.2 Dot1Q Tunnel Overview

1.2.1 Preface

The Dot1Q tunnel is a visualized call to the 802.1Q-based tunnel protocol and is defined in IEEE 802.1ad. The core concept is to encapsulate the user's private VLAN tag into the public network VLAN tag. The packet carries the two-layer tag through the backbone network of the service provider, so as to provide the user with a relatively simple Layer 2 VPN tunnel. Dot1Q Tunnel protocol is a simple and easy to manage. It does not require the support of the signaling, and it can be achieved only through the static configuration, especially for small, three-tier switch as the backbone of the enterprise network or small-scale MAN.

The Dot1Q tunnel feature meets the requirement of some user, providing a low-cost, simple two-tier VPN solution, and more and more small users tend to use the this function to build their own VPN network. In the operator's network, P devices do not need to support Dot1Q tunnel, that is, the traditional three-layer switch can meet the demand. It greatly protects the operator's investment.

- Support to enable the Dot1Q tunnel in global.
- Support for translation of Customer VLAN and SPVLAN, including translation of flat mode and translation of double-label (QinQ) mode.
- Support the configuration of the connection.
- Support for variable TPID.

1.2.2 Implementation of Dot1Q tunnel

One of the implementation of Dot1Q tunnel is based on port and the other is based on CVLAN Tag classification.

1) Dot1Q tunnel based on port

When the device receives the packet, the switch will tag the port with the VLAN tag of the default VLAN, regardless of whether the packet contains a VLAN tag. In this case, if the packet is received with a VLAN tag, the packet becomes the packet of the Double Tag. If receives untagged packets, the packet will be tagged with the default VLAN tag of the port.

The structure of the packet with single VLAN Tag as the figure 1 shows:

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	------------------	---------------	-------------------	-------------

Figure 1 Packet with single VLAN Tag

The structure of the packet with double VLAN Tag as the figure 2 shows:

DA (6B)	SA (6B)	ETYPE(8100) (2B)	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	-------------------------	-------------------	---------------	---------------	-------------------	-------------

Figure 2 Packets with outer VLAN tags

2) Dot1Q tunnel based on CVLAN Tag classification.

The service shunts are implemented according to the CVLAN ID range of the inner CVLAN tag of the Dot1Q tunnel. You can translate the CVLAN interval into an SPVLAN ID, with flat VLAN translation mode and QinQ VLAN translation mode. In the QinQ VLAN translation mode, when different service of the same users use different CVLAN IDs, traffic can be divided according to the CVLAN ID range. For example, the CVLAN ID range of the broadband service is 101 to 200, the CVLAN ID range of the VOIP service is 201 to 300, the CVLAN ID range of the IPTV service is 301 to 400. After PE device receiving the user data, tag the broadband services with the SPVLAN Tag, SPVLAN ID of which is 1000; tag the VOIP with the SPVLAN Tag, SPVLAN ID of which is 2000; tag the IPTV with the SPVLAN Tag, SPVLAN ID of which is 3000.

The difference between the Flat VLAN translation mode and the QinQ VLAN translation mode is that the SPVLAN Tag in the Flat VLAN translation mode is not superimposed on the outer layer of the CVLAN tag, but instead replaces the CVLAN tag directly.

1.2.3 TPID Value can be modified

Following figure shows the structure of the Tag defined by IEEE802.1Q:

TPID 2 byte	User Priority 3 bit	CFI 1 bit	VLAN ID 12 bit
----------------	------------------------	--------------	-------------------

Figure 3 tag structure of the VLAN Tag

The TPID is a field in the VLAN tag. The value of field is 0x8100 specified by IEEE 802.1Q. The switch use the TPTD value (0x8100) specified by the protocol by default. Some vendors' devices does not set the TPID value of the outer tag on the Dot1Q tunnel packet to 0x8100. In order to be compatible with these devices, most switches can modify the TPID value of the Dot1Q tunnel packets. The TPID value of the PE device can be configured by the user. When the port of these devices receives the packet, the TPID value in the outer VLAN tag of the packet will be replaced with value set by the user and

sent to the public network. Then these Dot1Q tunnel packets can be identified by other vendors' devices.

1.3 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring switch port
- Creating/Deleting VLAN interface
- Monitoring configuration and state of VLAN
- Configuring VLAN-based access control list
- Enable/ disable global Dot1Q Tunnel
- Configuring VLAN transmit mode and entry on the interface mode
- Configuring MAC-based VLAN
- Configuring IP subnet-based VLAN
- Configuring protocol-based VLAN

1.4 VLAN Configuration Task

1.4.1 Adding/Deleting VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end device to be grouped together even if they are not located on the same LAN segment. A VLAN may have multiple ports and all unicast, multicast and broadcast packet can only be forwarded from the same VLAN to the terminal. Each VLAN is a logistical network. If the data wants to reach another VLAN, it must be forwarded by router or bridge.

Run the following command to configure VLAN.

Run	To
vlan vlan-id	Enter the VLAN configuration mode.
name str	Name in the VLAN configuration mode.
Exit	Exit vlan configuration mode, and establish vlan.

vlan vlan-range	Establish multiple VLANs at the same time.
no vlan vlan-id vlan-range	Delete one or multiple VLANs.

It can also dynamically add/delete VLAN via VLAN management protocol GVRP.

1.4.2 Configuring Switch Port

The switch port supports the following modes: access mode, trunk mode, dot1q-tunnel mode and VLAN tunnel linkup port mode.

- The access mode indicates that this port is only subordinate to one VLAN and only sends and receives untagged Ethernet frame.
- The trunk mode indicates that this port is connected to other switches and can send and receive tagged Ethernet frame.
- The dot1q-tunnel mode takes is based on the trunk mode. This port search the SPVLAN on the VLAN translation table according to the received VLAN tag. The switch chip changes the original tag with SPVLAN tag or adds SPVLAN tag to the original tag. When the packet goes out from the port, it will change changes the original tag with SPVLAN tag or forcibly adds SPVLAN tag to the original tag. Therefore allowing switch to ignore the different VLAN partitions that connected to the network. Then the packet will be delivered to the other port in the other sub network of the same customer. The transparent transmission is realized in this way.
- VLAN tunnel linkup port mode is a sub mode based on trunk mode. When the packet goes out of the port, SPVLAN should be configured in the untagged range to ensure that all packets are intact. When a packet arrives from the port, the TPID of the packet will be checked. If the packet is found to be undeserved or untagged, the SPVLAN tag containing its own TPID is added as the outer label of the packet.

Each port has one default VLAN and PVID, and all the data without VLAN tag received on the port belong to the data packets of the VLAN.

Trunk mode can ascribe port to multiple VLAN and also can configure which kind of packet to forward and the number of VLAN that belongs, that is, the packet sent on the port is tagged or untagged, and the VLAN list that the port belongs.

Run the following command to configure the switch port:

Run	To
switchport pvid <i>vlan-id</i>	Configure PVID of switch port.
switchport mode	Configure port mode of the switch.

access [trunk dot1q-translation-tunnel dot1q-tunnel-uplink <i>tpid</i>	
switchport trunk vlan-allowed	Configure vlan-allowed range of switch port.
switchport trunk vlan-untagged	Configure vlan-untagged range of switch port.
switchport flat-translation	Enable flat N:1 VLAN reversal translation function of the port

1.4.3 Creating/Deleting VLAN Interface

Vlan interface can be established to realize network management or layer 3 routing feature. The vlan interface can be used to specify ip address and mask. Run the following command to configure vlan interface:

Run	To
[no] interface vlan <i>vlan-id</i>	Create/Delete a VLAN interface.

1.4.4 Monitoring configuration and state of VLAN

Run the following command to monitor the configuration and state of VLAN and other Dot1Q Tunnel:

Run	To
show vlan [<i>id x</i> interface <i>intf</i> dot1q-tunnel [interface <i>intf</i>] mac-vlan subnet protocol-vlan]	Display the configuration and state of VLAN and other Dot1Q Tunnel
show interface vlan <i>x</i>	Display the state of vlan port/supervlan port.

1.4.5 Enable/ Disable Global Dot1Q Tunnel

Enable the dot1q-tunnel in global mode. All the ports will become Dot1Q Tunnel uplink port and the coming packet will be forced to be tagged with SPVLAN tag.

Run	To
dot1q-tunnel	Configure dot1q-tunnel in global.

1.4.6 Configuring flat N:1 VLAN Reversal Translation Function in Global

Enable flat N:1 VLAN reversal translation function in global.

Run	To
-----	----

[no] flat-translation-global	Enable flat N:1 VLAN reversal translation function in global.
---------------------------------------	---------------------------------------------------------------

1.4.7 Configuring VLAN Translation Mode and Entry of Port

VLAN translation mode and VLAN translation entries are configured in port mode **dot1q-translating-tunnel**. There are two types of translation modes: Flat mode and QinQ mode. Flat mode will use the CVLAN tag which enter into dot1q-translating-tunnel linkup port as the index, search the VLAN translation table, replace the SPVLAN with the CVLAN, and the SPVLAN to CVLAN will be converted when the packet came out from the port. The QinQ mode will use the CVLAN tag which enter into dot1q-translating-tunnel linkup port as the index, search the VLAN translation table. Then the SPVLAN tag will be superimposed on the outer edge of the CVLAN tag. When the packet comes out of this port, the SPVLAN tag will be removed.

When configuring a VLAN translation entry on port configuration, QinQ mode can configure multiple-to-one mapping between CVLAN and SPVLAN. To configure a multi-to-one mapping between CVLAN and SPVLAN in flat mode, you must configure flat-translation, then SPVLAN and CVLAN will be correctly converted when the packet comes out of this port.

Following is the command to configure VLAN translation mode and entry.

Run	To
switchport dot1q-translating-tunnel mode {flat qinq} translate {oldvlanid oldvlanlist} newvlan [priority]	Configure VLAN translation mode and entry.

1.4.8 Configuring MAC-Based VLAN

A MAC-Based VLAN is a way of dividing a VLAN by the source MAC address of a packet. When a port receives an untagged packet, the device obtains the source MAC address of the packet as the matching keyword to find the VLAN which the packet belongs to by searching the MAC VLAN entry.

The MAC-Based VLAN configuration includes adding / deleting MAC VLAN entries and enabling / disabling MAC VLAN on the port.

In the global configuration mode, use the following command to add / remove MAC address entries:

Run	To
mac-vlan mac-address mac-addr vlan vlan-id	Add a MAC VLAN entry.

[priority]	
no mac-vlan mac-address mac-addr	Delete a MAC VLAN entry.

MAC-Based VLAN only works on ports that enable the function. In the port configuration mode, use the following command to enable / disable the MAC VLAN on the port:

Run	To
[no] switchport mac-vlan	Enable/Disable MAC-Based VLAN on the port configuration.

Caution: When the port mode is access, if the incoming VLAN matched through MAC VLAN is not the PVID of the port, the packets will be discarded. Therefore, if not, do not configure the port mode for MAC VLAN enabled as access.

1.4.9 Configuring IP Subnet-Based VLAN

IP Subnet-Based VLAN is a way to divide VLANs based on the source IP address of packets and the subnet mask. When a port receives an untagged packet, the device will determine the VLAN to which the packet belongs based on the source IP address of the packet and the subnet mask.

IP subnet-based VLAN configuration includes adding / removing subnet VLAN entries and enable/disable the Subnet VLAN function on the port.

Use the following command to add / remove a Subnet VLAN entry in VLAN configuration mode:

Run	To
[no] subnet { any ip-addr mask }	add / remove a Subnet VLAN entry

The IP subnet-based VLAN only works on ports that enable the function. In the port configuration mode, use the following command to enable / disable the Subnet VLAN function on the port:

Run	To
[no] switchport vlan-subnet enable	Enable/disable IP Subnet-based VLAN on port configuration mode.

Caution: When the port mode is access, if the incoming VLAN matched through Subnet VLAN is not the PVID of the port, the packets will be discarded. Therefore, if not, do not configure the port mode for Subnet VLAN enabled as access.

1.4.10 Configuring Protocol-Based VLAN

Protocol-Based VLAN divide the VLAN based on the protocol which the receiving message belongs to on the port. When the port receives an untagged packet, the device will divide the VLAN based on the protocol which the receiving message belongs to on the port.

The way to determine the protocol of the packet on the switch is to determine the protocol-based VLAN configuration according to the encapsulation format of the packet and the value of the special field: add / remove protocol templates in global mode and add / remove associations with protocol templates in port configuration mode.

- add / remove protocol templates in global mode and add / remove associations with protocol templates on the port configuration mode.

In the global configuration mode, use the following command to add / remove protocol templates.

Run	To
protocol-vlan <i>protocol_index</i> frame-type { ETHERII SNAP LLC } ether-type <i>etype-id</i>	add a protocol templates
no protocol-vlan <i>protocol_index</i>	remove a protocol templates

Note that when frame-type is LLC, the upper and lower bytes of ether-type correspond to DSAP and SSAP in the packet respectively.

The protocol template only works on the port of the template. The same protocol template can correspond to different VLANs on different ports. In port configuration mode, use the following command to add / remove association with the protocol template:

Run	To
switchport protocol-vlan <i>protocol_index</i> vlan <i>vlan-id</i>	add association with the protocol template
no switchport protocol-vlan <i>protocol_index</i>	remove association with the protocol template

1.5 Configuration Example

1.5.1 Example for Dot1Q Tunnel

Here are a few typical networking schemes to explain the application of the Dot1Q Tunnel.

- Example 1

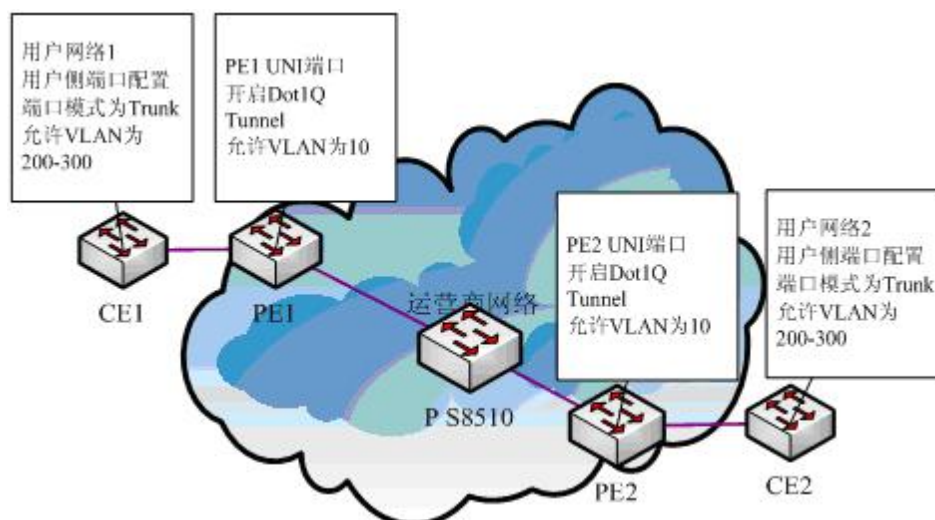


Figure 4 typical networking schemes for Dot1Q Tunnel

Assume that F0/1 of CE1 is connected to F0/1 (or G0/1) of PE1. PE1 and S8510 are connected to F0/2 (or G0/2). PE2 and S8510 are F0/2 (or G0/2). F0/1 (or G0/1) of PE2 is connected to F0/1 of CE1.

The port G0/1 of the PE is configured as the access port of VLAN 10 and enables Dot1Q tunnel. However, the trunk port still needs trunk VLAN 200-300, so that the connection between CE and PE becomes an Asymmetrical Link. So the public network only need to assign a VLAN number 10 to the user, regardless of how many private network VLAN ID within the user network. When the user message with the tag came into the service provider's backbone network, the newly assigned Public network is uniformly forced to be inserted. After the packet arrives at the PE device on the other side of the backbone network according to the VLAN number of the public network passes through the backbone network, the public network VLAN tag is stripped, the user packets are restored, and then transmitted to the user's CE device. Therefore, the packets transmitted in the backbone network have two 802.1Q tag headers. One is the public network tag, another is the private network tag. Following is the specific message forwarding process:

- 1) Because the out port of CE1 is a trunk port, the packets sent to PE1 carry the VLAN tag of the private network (range is 200-300). The message is shown in Figure 5.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	------------------	---------------	-------------------	-------------

Figure 5 The message structure from CE1

- 2) After entering PE1, because the ingress port is the access port of the Dot1Q tunnel, PE1 ignores the VLAN tag of the user's private network, but instead inserts the tag of the default VLAN 10 into the user's message, as shown in Figure 6.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	SPVLAN Tag (2B)	ETYPESA(8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	-----------------------	-----------------------	----------------------	---------------	-------------------	-------------

Figure 6 The message structure from PE1

- 3) In the backbone network, the packets are propagated along the port of trunk port 10, and the tag of the user's private network remains transparent in the backbone network until it reaches the network edge device PE2.
- 4) PE2 discovers the access port VLAN 10 connected to CE2, and strips the tag of VLAN 10 according to the traditional 802.1Q protocol. Then send the original packet of the user to CE2, as shown in Figure 7.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	------------------	---------------	-------------------	-------------

Figure 7 The message structure from PE2

It can be seen that, the Dot1Q tunnel protocol is very simple. And it requires no signaling to maintain the tunnel establishment and can be configured by static configuration.

For the typical configuration of the Dot1Q Tunnel, the switch needs the following configuration (PE1 is the same as PE2):

Dot1Q Tunnel configuration for the switch:

```
Switch_config#dot1q-tunnel
```

```
Switch_config_g0/1#switchport pvid 10
```

```
Switch_config_g0/2#switchport mode trunk
```

```
Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094
```

➤ Example 2

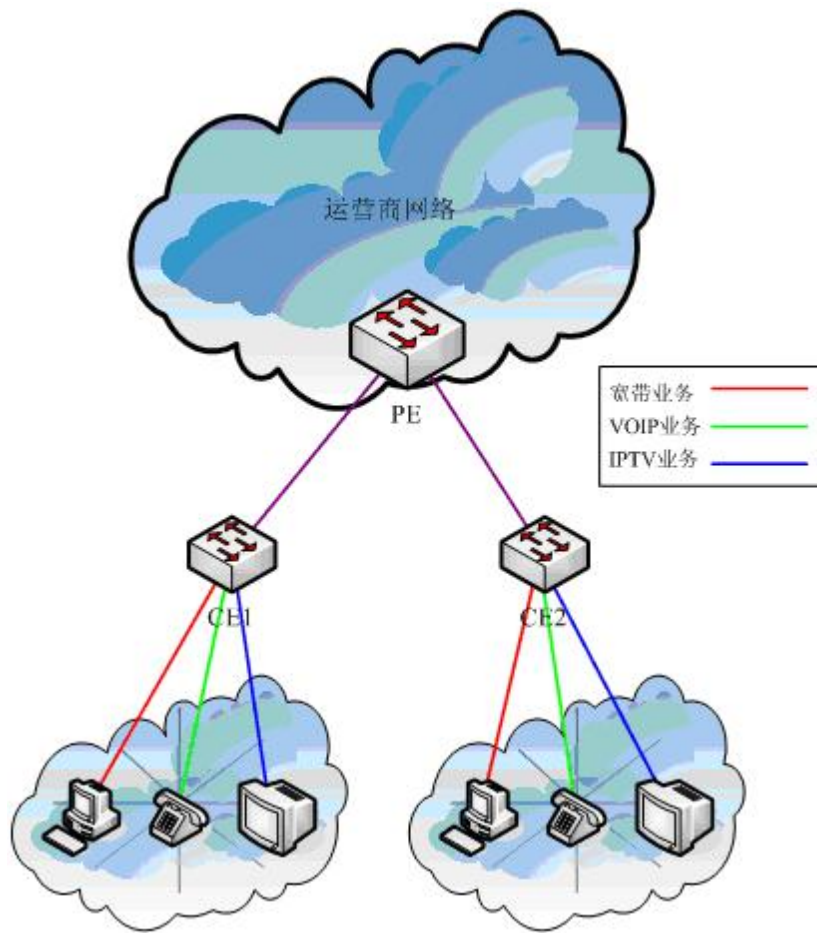
If different services of the same user are involved, the user access point is set on a UNI port of the PE. To distinguish between different services and implement different QOS standards, you must use Do1Q tunnel VLAN translation.

As shown in Figure 8, the operator assigns three VLANs to each user, one VLAN corresponding to one service. For example, for users 1, VLAN tag values are 1001, 2001, and 2001 respectively. VLAN1001 corresponds to broadband. VLAN 2001 corresponds

to the VOIP. VLAN 3001 corresponds to the IPTV. After the service enters into the UNI port of the PE switch, it will be marked with a different outer tag according to the user VLAN ID. If the user data outer label is 1001, the label 1001 is added directly to the outer tag. For user 2, its different business can also be assigned different VLAN tags. The difference between the assignment of outer labels and users is mainly to distinguish the location of the CE, but also to find the final positioning of the user.

Device	Service	Inner CVLAN tag	Outer SPVLAN tag	Stream classification principle
CE1	Broadband	101-200	1001	VLAN Interval
	VOIP	201-300	2001	
	IPTV	301-400	3001	
CE2	Broadband	101-200	1002	
	VOIP	201-300	2002	
	IPTV	301-400	3002	

In this networking scheme, the inner and outer labels well distinguish the business and locate the user. The inner label + outer label can locate a user whose outer label identifies the location of the CE and also identifies the service, the inner label identifies the location of the user on the CE.



Assume that CE1 is connected to G0/1 port of PE1 and CE2 is connected to G0/2 port of PE1. The Dot1Q tunnel NNI port of PE is g0/3, which needs to be configured as follows:

Dot1Q Tunnel configuration for the switch:

```
Switch_config#dot1q-tunnel
```

```
Switch_config_g0/1#switchport mode dot1q-translating-tunnel
```

```
Switch_config_g0/1#switchport dot1q-translating-tunnel mode QinQ translate 101-200 1001
```

```
Switch_config_g0/1#switchport dot1q-translating-tunnel mode QinQ translate 201-300 2001
```

```
Switch_config_g0/1#switchport dot1q-translating-tunnel mode QinQ translate 301-400 3001
```

```
Switch_config_g0/2#switchport mode dot1q-translating-tunnel
```

```
Switch_config_g0/2#switchport dot1q-translating-tunnel mode QinQ translate 101-200 1002
```

```
Switch_config_g0/2#switchport dot1q-translating-tunnel mode QinQ translate 201-300  
2002
```

```
Switch_config_g0/2#switchport dot1q-translating-tunnel mode QinQ translate 301-400  
3002
```

```
Switch_config_g0/3#switchport mode dot1q-tunnel-uplink
```


Appendix A Abbreviations

Abbreviations	Full name
VPN	Virtual Private Network
TPID	Tag Protocol Identifier
QoS	Quality of Service
P	provider bridged network core
PE	provider bridged network edge
CE	customer network edge
UNI	user-network interface
NNI	network-network interface
CVLAN	Customer VLAN
SPVLAN	Service provider VLAN