VLAN Configuration

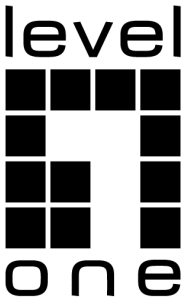

Table of Contents

Chapter 1 VLAN Configuration 1
1.1 VLAN Introduction 1
1.2 Dot1Q Tunnel Overview 1
1.2.1 Preface 1
1.2.2 Dot1Q Tunnel Realization Mode 2
1.2.3 Modifying Attributes through TPID Value 3
1.3 VLAN Configuration Task List 3
1.4 VLAN Configuration Task 4
1.4.1 Adding/Deleting VLAN 4
1.4.2 Configuring Switch Port 4
1.4.3 Creating/Deleting VLAN Interface 5
1.4.4 Monitoring Configuration and State of VLAN 5
1.4.5 Enabling/disabling global Dot1Q Tunnel and Configuring gobal TPID 5
1.4.6 Configuring VLAN translation mode and items on a port 6
1.4.7 Setting MAC-Based VLAN 6
1.4.8 Setting IP Subnet-Based VLAN 7
1.4.9 Setting Protocol-Based VLAN 7
1.5 Dot1Q Tunnel Configuration Examples 8
1.5.1 Dot1Q Tunnel configuration examples 8
Appendix Abbreviations 13

Chapter 1 VLAN Configuration

1.1 VLAN Introduction

VLAN(Virtual Local Area Network) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. In 1999 IEEE established IEEE 802.1Q Protocol Standard Draft used to standardize VLAN realization project. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

There are the following types of Virtual LANs:

- Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs.
- 802.1Q trunk mode is supported on the interface.
- Access mode interface is supported.

  Port-Based Vlan is to ascribe port to one subset of vlan that the switch supports. If this vlan subset has only one vlan, then this port is access port. If this vlan subset has multiple vlan, then this port is trunk port. There is one default vlan among the multiple vlan, and the vlan id is the port vlan id (PVID).
- Vlan-allowed range is supported on the interface.

Vlan-allowed parameter is used to control vlan range that the port belongs. Vlan-untagged parameter is used to configure port to send packets without vlan tag to the corresponding vlan.

VLAN can be classified based on MAC address, IP subnetwork, the protocol and the port. For these VLAN classification methods, VLAN matching is performed in the order of MAC VLAN, IP subnet VLAN, protocol VLAN, and port VLAN by default

1.2 Dot1Q Tunnel Overview

1.2.1 Preface

Dot1Q Tunnel is a lively name of the tunnel protocol based on 802.1Q encapsulation, which is defined in IEEE 802.1ad. Its core idea is to encapsulate the VLAN tag of the private network to that of the public network, and the packets with two layers of tags traverse the backbone network of ISP and finally a relatively simple L2 VPN tunnel is provided to users. The Dot1Q Tunnel protocol is a simple and manageable protocol, which is realized through static configuration without signaling support and widely applied to enterprise networks, which mainly consist of OLTs, or small-scale MAN.

The Dot1Q Tunnel attribute of LEVELONE switches just meets this requirement. As a cheap and compact L2 VPN solution, it is increasingly popular among more and more

small-scale users when VPN network is required. At the inside of carrier's network, P device need not support the Dot1Q Tunnel function. That is, traditional L3 switches can meet the requirements fully and protect the investment of the carrier greatly.

- Enables Dot1Q Tunnel globally.
- Supports the inter-translation between customer VLAN and SPVLAN on the downlink port, including translation in Flat mode and in QinQ mode.
- Supports the configuration of the uplink port.
- Supports variable TPID.

1.2.2 Dot1Q Tunnel Realization Mode

There are two modes to realize Dot1Q Tunnel: port-based Dot1Q Tunnel and Dot1Q Tunnel based on inner CVLAN tag classification.

1) Port-based Dot1Q Tunnel:

When a port of this device receives packets, no matter whether packets have the VLAN tag, the switch will add the VLAN tag of the default VLAN on this port to these packets. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port.

The packet with a single VLAN tag has the following structure, as shown in table 1:

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

Table 1 The packet with a single VLAN tag

The packet with double VLAN tags has the following structure, as shown in table 2:

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

Table 2 Packet with double VLAN tags

2) Dot1Q Tunnel based on the inner CVLAN Tag:

The service is distributed according to the CVLAN ID zone of the inner CVLAN tag of Dot1Q Tunnel. The CVLAN zone can be translated into SPVLAN ID and there are two translation modes: Flat VLAN translation and QinQ VLAN translation. In QinQ VLAN translation mode, when a same user uses different services by using different CVLAN IDs, the services can be distributed according to CVLAN ID. For example, the CVLAN ID of bandwidth service ranges between 101 and 200. The CVLAN ID of VOIP service ranges between 201 and 300. The CVLAN ID of IPTV service ranges between 301 and 400. According to the CVLAN ID range, when the PE device receives the user data, add SPVLAN Tag whose SPVLAN ID is 1000 to the bandwidth service and whose SPVLAN ID is 3000 to the IPTV service. The difference between Flat VLAN translation mode and QinQ VLAN translation mode

is SPVLAN Tag in the Flat VLAN translation mode is not add to the outside layer of CVLAN Tag, but replace CVLAN Tag directly.

1.2.3 Modifying Attributes through TPID Value

The structure of the Tag packet of Ethernet frame that is defined by the IEEE 802.1Q protocol is shown below:

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

Figure 3 Structure of the VLAN Tag of Ethernet frame

TPID is a field in VLAN Tag and the value of this field regulated by IEEE 802.1Q is 0x8100.switches adopt the default TPID value, that is, 0x8100. Some manufacturers do not set the TPID of the outside tag of the Dot1Q Tunnel packets in their devices to 0x8100. In order to be compatible with these devices, most switches provide the function to modify the TPID value of the Dot1Q Tunnel packets. The TPID value of the PE device can be configured by users. After the ports of these devices receive packets, the TPID value of the outside VLAN tag of these packets will be replaced with user-defined value and then these packets will be forwarded. In this way, the Dot1Q Tunnel packets can be identified by the devices of other manufacturer after they are forwarded into the public network.

1.3 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring switch port
- Creating/Deleting VLAN interface
- Monitoring configuration and state of VLAN
- Configuring the VLAN-based access control model
- Enabling/disabling global Dot1Q Tunnel
- Configuring VLAN translation mode and items on a port
- Setting MAC-Based VLAN
- Setting IP Subnet-Based VLAN
- Setting 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 stations 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 message 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

Command	Purpose
vlan-view *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-id* | *vlan-range*	Establish one or multiple VLANs at the same time.
no vlan *vlan-id* | *vlan-range*	Delete one or multiple VLANs.

Vlan can perform dynamic addtion and deletion via vlan management protocol GVRP.

1.4.2 Configuring Switch Port

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

- The access mode indicates that this port is only subordinate to one vlan and only sends and receives untagged ethernet frame.
- The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.
- The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.
- The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. The SPVLAN should be set when packets are forwarded out of the port. If the packets are in the untagged range, all these packets are forwarded out without any change. When the packets are received by the port, their TPIDs will be

checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

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 *vlan-id*	Configure pvid of switch port.
switchport mode {access | trunk | dot1q-translating-tunnel | dot1q-tunnel-uplink [*tpid* **]}**	Configure port mode of the switch.
switchport trunk vlan-allowed *vlan-range*	Configure vlan-allowed range of switch port.
switchport trunk vlan-untagged *vlan-range*	Configure vlan-untagged range of switch 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*vlan-id*	Create/Delete a VLAN interface.

1.4.4 Monitoring Configuration and State of VLAN

Run the following commands in EXEC mode to monitor configuration and state of VLAN:

Run…	To…
show vlan [id *x* **| interface** *intf* **| dot1q-tunnel [interface** *intf***] | mac-vlan | subnet | protocol-vlan| private-vlan | run-config [interface** *intf***] | debug]**	Display configuration and state of VLAN or Dot1Q Tunnel.
show interface vlan*x*	Display the states of vlan ports.

1.4.5 Enabling/disabling global Dot1Q Tunnel and Configuring gobal TPID

After Dot1Q Tunnel is enabled globally, their ports can be defaulted as the downlink ports of Dot1Q Tunnel, and the SPVLAN tag will be added to incoming packets.

The command to enable dot1q-tunnel is shown in the following table:

Run…	To…
dot1q-tunnel	Configures the global dot1q-tunnel on a

	switch.

1.4.6 Configuring VLAN translation mode and items on a port

Both the VLAN translating mode and the VLAN translating items validate in dot1q-translating-tunnel mode after they are configured. The translation modes fall into two kinds: the Flat mode and the QinQ mode. In Flat mode, the CLAN tag of packets which are received by the dot1q-translating-tunnel downlink port will be used as an index to look up the VLAN translating list. The CVLAN will be replaced by detected SPVLANs; when the packets are forwarded out of the port, the SPVLAN will then be replaced by CVLAN. In QinQ mode, the CLAN tag of packets which are received by the dot1q-translating-tunnel downlink port will be used as an index to look up the VLAN translating list and then the detected SPVLANs will form into SPVLAN tag to be added to the outside of CVLAN tag; when the packets are forwarded out of the port, the SPVLAN tag will then be removed.

The command to configure the VLAN translation mode and translation items is shown in the following table:

Run…	To…
switchport dot1q-translating-tunnel mode qinq translate {*oldvlanid* **|** *oldvlanlist***}** *newvlan* **[***priority***]**	Configures the VLAN QinQ translation mode and translation item.
switchport dot1q-translating-tunnel mode flat translate {1to1|nto1} {*oldvlanid* **|** *oldvlanlist***}** *newvlan* **[***priority***]**	Configures the VLAN flat translation mode and translation item.

1.4.7 Setting MAC-Based VLAN

The MAC-based VLAN is a VLAN planning mode based on the source MAC address of the packet. When a port of a device receives an untagged packet, the device will take the source MAC address of the packet as the matchup keyword and know the home VLAN by looking for the MAC VLAN entry.

The settings of the MAC-based VLAN include adding/deleting MAC VLAN entry globally and enabling/disabling the MAC VLAN function on the port.

In global configuration mode run the following commands to add or delete the MAC VLAN entry.

Run…	To…
mac-vlan mac-address ***mac-addr*** vlan ***vlan-id [priority]***	Adds a MAC VLAN entry.
no mac-vlan mac-address ***mac-addr***	Deletes a MAC VLAN entry.

The MAC-based VLAN function takes effect only on a port on which this function is enabled. In port configuration mode, run the following commands respectively to enable or disable the MAC VLAN function on a port.

Run…	To…
[no] switchport mac-vlan	To enable or disable the MAC-based VLAN function.

Note: In port access mode, an incoming packet will be dropped if its VLAN, which is obtained through the matchup of MAC VLAN entry, is not the PVID of the port. Hence, if not necessary, do not set the port mode, which is to enable MAC VLAN, to access.

1.4.8 Setting IP Subnet-Based VLAN

IP subnet-based VLAN is a VLAN planning mode based on the source IP address and configured subnet mask of a packet. When a device receives an untagged packet on one of its ports, the device will locate the VLAN of this packet according to the source IP address of the packet and the configured subnet mask.

The settings of the IP-subnet VLAN includes adding/deleting the subnet VLAN entry and enabling/disabling the subnet VLAN function on the port.

In global configuration mode run the following commands to add or delete the subnet VLAN entry.

Run…	To…
[no] subnet { any | ***ip-addr mask*** }	**Addes/Deletes a subnet VLAN entry.**

The IP-subnet VLAN function takes effect only on a port on which this function is enabled. In port configuration mode, run the following commands respectively to enable or disable the MAC VLAN function on a port.

Run…	To…
[no] switchport vlan-subnet enable	To enable or disable the IP-subnet VLAN function on the ports.

Note: In port access mode, an incoming packet will be dropped if its VLAN, which is obtained through the matchup of MAC VLAN entry, is not the PVID of the port. Hence, if not necessary, do not set the port mode, which is to enable subnet VLAN, to access.

1.4.9 Setting Protocol-Based VLAN

The protocol-based VLAN is a VLAN planning mode which is based on the protocol to which the received packet belongs. When a switch receives an untagged packet on one of its ports, the switch will determine the VLAN of the packet according to the protocol of this packet.

The way the switch determines the type of the protocol that the packet belongs to is based on the encapsulation type and the value of the special field.

Adding/deleting a protocol template globally and adding/deleting the association of a protocol template on a port

In global configuration mode, run the following commands to add or delete a protocol template.

Run…	To…
protocol-vlan ether-type *etype-id* vlan *vlan-id*	Adds a protocol template.
no protocol-vlan *etype-id*	Deletes a protocol template.

In port configuration mode, run the following commands to add or delete the association of a protocol template.

Run…	To…
switchport protocol-vlan	Enables protocol-based vlan function on the port.

no switchport protocol-vlan	Disables the protocol-based vlan function on the port.

Note: When the port mode is **access**, if the VLAN that the incoming packet matches through the protocol VLAN table entry is not the PVID of the port, the packet will be discarded. Therefore, if it is not necessary, please do not configure the port mode that uses the protocol VLAN function to access.

1.5 Dot1Q Tunnel Configuration Examples

1.5.1 Dot1Q Tunnel configuration examples

The following typical solutions show how to apply Dot1Q tunnel.

1. Example 1

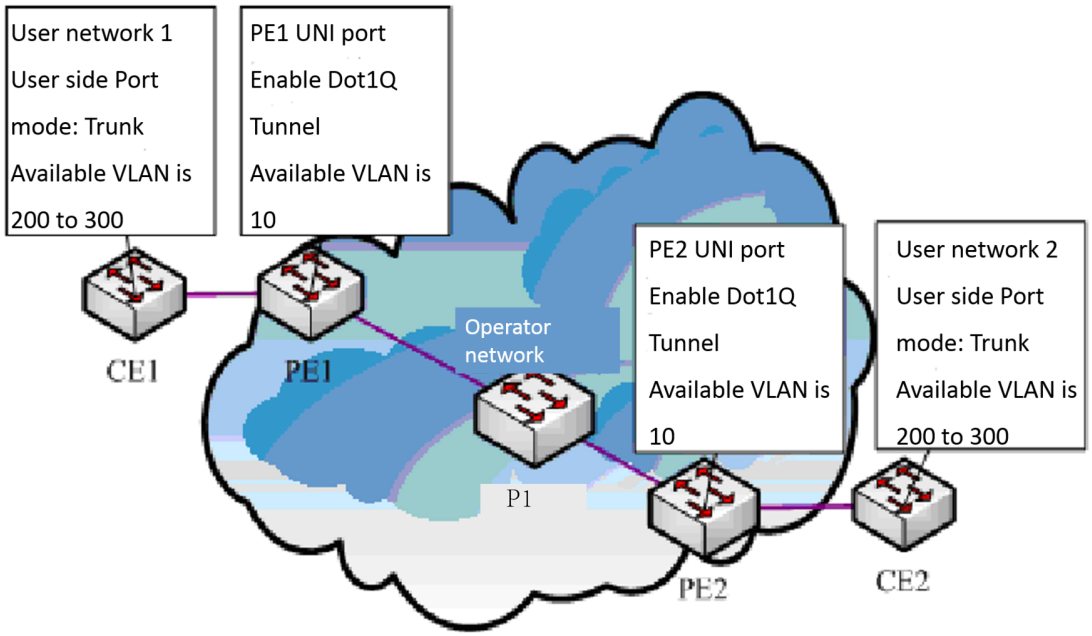

Figure 3 Configuration of Dot1Q Tunnel

As shown in the figure above, port g0/0/1 of CE1 connects port g0/0/1 of PE1; PE1 connects P1 on port g0/0/2; PE2 connects P1 on port g0/0/2; and port g0/0/1of PE2 connects port g0/0/1 of CE1.

The ports of PE are set to be the access port of VLAN 10 and on them Dot1Q Tunnel is enabled. However, the ports of CE still need Trunk VLAN 200-300, enabling the link between CE and PE to be an asymmetrical link. In this case, the public network only needs to distribute users a VLAN ID, 10. No matter how many VLAN IDs of private network are planned in the user's network, the newly distributed VLAN ID of the public network will be mandatorily inserted into the tagged packets when these packets enter the backbone network of ISP. These packets then pass through the backbone network through the VLAN ID of the public network, reach the other side of the backbone network, that is, the PE devices, get rid of the VLAN tag of the public network, resume the user's packets and at last are transmitted to the CE devices of the users. Therefore, the packets that are forwarded in the backbone network have two layers of 802.1Q tag

headers, one being the tag of the public network and the other being the tag of the private network. The detailed flow of packet forwarding is shown as follows:

1) Because the egress port of CE1 is a Trunk port, all the packets that are transmitted by users to PE1 have carried the VLAN tag of the private network (ranging from 200 to 300). One of these packets is shown in figure 4.

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

Figure 4 Structure of a packet from CE1

2) After the packets enter PE1, PE1, for the ingress port is the access port of Dot1Q tunnel, ignores the VLAN tag of the private network but inserts the default VLAN 10's tag into these packets, as shown in figure 5.

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

Figure 5 Structure of a packet going into PE1

3) In the backbone network, packets are transmitted along the port of trunk VLAN 10. The tag of the private network is kept in transparent state until these packets reach PE2.

4) PE2 discovers that the port where it connects CE2 is the access port of VLAN 10, removes the tag header of VLAN 10 according to 802.1Q, resumes the initial packets of users, and transmit the initial packets to CE2, as shown in figure 6.

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

Figure 6 Structure of a packet from PE2

Seen from the forwarding flow, Dot1Q Tunnel is very concise for the signaling is not required to maintain the establishment of the tunnel, which can be realized through static configuration.

As to the typical configuration figure of Dot1Q Tunnel, LEVELONE's products of different models are configured as follows when they run as PE (PE1 has the same configuration as PE2).

1) Dot1Q Tunnel Configuration of the switch:

Switch(config)#dot1q-tunnel

Switch(config)#vlan 1-4094

Switch(config)#interface g0/0/1

Switch(config-g0/0/1)#switchport pvid 10

Switch(config)#interface g0/0/2

Switch(config-g0/0/2)#switchport mode trunk

Switch(config-g0/0/2)#switchport trunk vlan-untagged 1-9,11-4094

2. Example 2

If different services of a same user are dealt with and the access terminal of a user connects the UNI port of PE, the Dot1Q tunnel VLAN translation must be used to differentiate different services and carry different QoS standards.

As shown in figure 8, the carrier distributes three VLANs for each user and each VLAN corresponds to a kind of service. For example, user 1 is distributed with 3 VLANs, that is, VLAN 1001, VLAN 2001 and VLAN 3001, among which VLAN 1001 is for broadband services, VLAN 2001 is for VoIP services and VLAN 3001 is for IPTV services. When a service reaches the UNI port of the PE switch, an out-layer label will be added to the service according to its VLAN ID (different services are added with different outer-layer labels). If the out-layer label of the user data is 1001, the user data will be added with label 1001 directly on its outer layer. As to user 2, different services can be distributed with different VLAN tags. The outer-layer tag of user 2 is different from that of user 1 mainly for differentiating the location of CE and also locating users.

Device	Service	Inner-layer CVLAN tag	Outer-layer SPVLAN tag	Flow classification principle
CE1	broadband	101-200	1001	CVLAN domain
	VOIP	201-300	2001	
	IPTV	301-400	3001	
CE2	broadband	101-200	1002	
	VOIP	201-300	2002	
	IPTV	301-400	3002	

In this networking solution, the two layers of tags differentiate services very well and locate users. The outer-layer tag identifies the location of CE and a service, while the inner-layer tag identifies the location of a user.

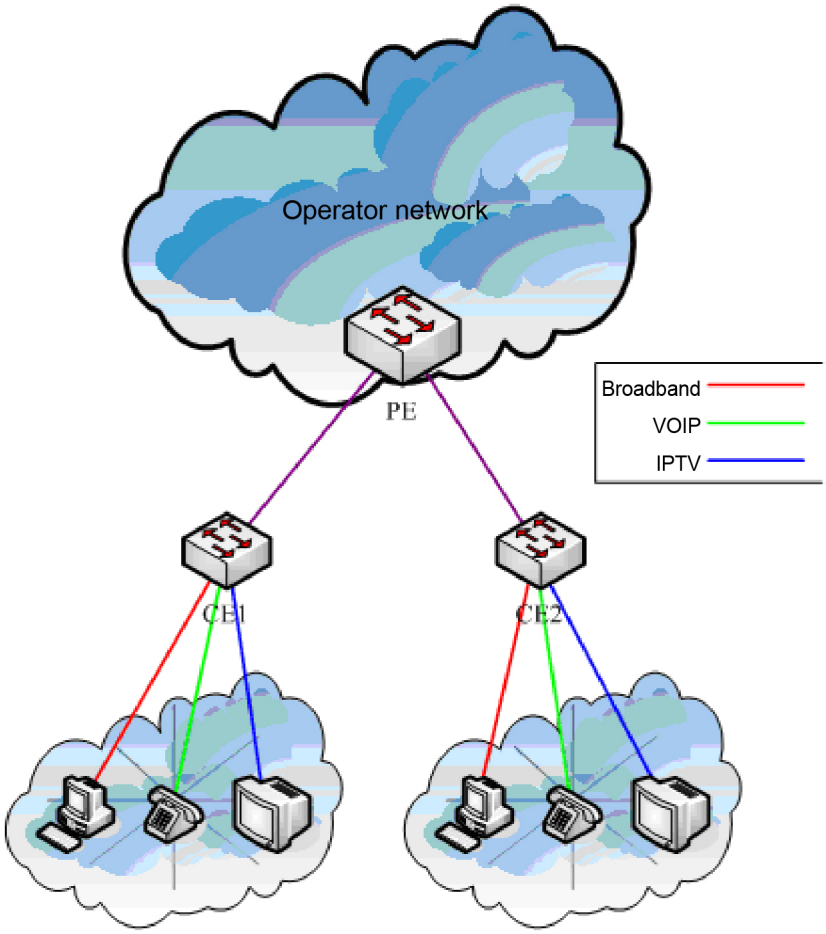

Figure 9 Typical configuration of Dot1Q tunnel

In figure 9, CE1 connects port g0/0/1 of PE1, CE2 connects port g0/0/2 of PE1 and the Dot1Q Tunnel NNI port of PE is port g0/0/3. Configuring the command as follows:

1) Dot1Q Tunnel configuration on this switch

Switch(config)#dot1q-tunnel

Switch(config)#vlan 1-4094

Switch(config)#interface g0/0/1

Switch(config-g0/0/1)#switchport mode dot1q-translating-tunnel

Switch(config-g0/0/1)#switchport dot1q-translating-tunnel mode QinQ translate 101-200 1001

Switch(config-g0/0/1)#switchport dot1q-translating-tunnel mode QinQ translate 201-300 2001

Switch(config-g0/0/1)#switchport dot1q-translating-tunnel mode QinQ translate 301-400 3001

Switch(config)#interface g0/0/2

Switch(config-g0/0/2)#switchport mode dot1q-translating-tunnel

Switch(config-g0/0/2)#switchport dot1q-translating-tunnel mode QinQ translate 101-200 1002

Switch(config-g0/0/2)#switchport dot1q-translating-tunnel mode QinQ translate 201-300 2002

Switch(config-g0/0/2)#switchport dot1q-translating-tunnel mode QinQ translate 301-400 3002

Switch(config)#interface g0/0/3

Switch(config-g0/0/3)#switchport mode dot1q-tunnel-uplink

Appendix Abbreviations

English abbreviation	English 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