Contents

1 Configuring Private VLAN

1.1 Introduction

1.1.1 Overview

Carriers hope to isolate users to authenticate and charge each user, avoid virus attacks and broadcast storms, and strengthen user security. VLANs are isolated at L2. If each user is assigned with a VLAN, the authentication, billing, and security requirements can be met. However, a device supports 4094 VLANs at most. Assigning a VLAN to each user limits the number of users supported by a device. What's more, it is infeasible for an L3 device to assign one IP address to each VLAN in consideration of scarce IP addresses. To solve the problem, the private VLAN (PVLAN) technology is developed.

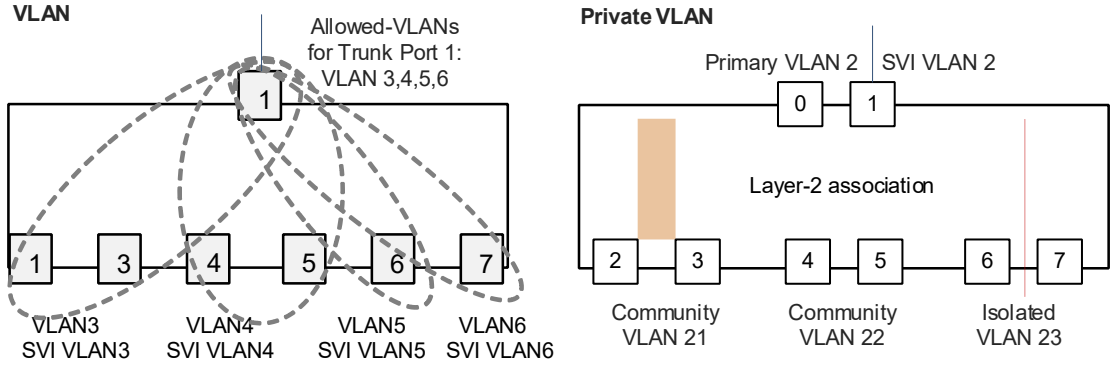
1.1.2 Basic Concepts

The PVLAN technology divides an L2 broadcast domain of a VLAN into multiple sub-domains to form a dual-layer VLAN structure. The outer layer is referred to as primary VLAN, and the inner layer is referred to as secondary VLAN. Secondary VLANs can be further divided to community VLANs and isolated VLANs.

1. Features

- You can configure multiple PVLANs on a device. A PVLAN is a PVLAN domain.
- Each PVLAN can contain only one primary VLAN and multiple secondary VLANs. The primary VLAN corresponds to multiple secondary VLANs. The primary VLAN and one secondary VLAN form a PVLAN pair, which represents a PVLAN sub-domain. For example, VLAN 2/21 represents a PVLAN sub-domain. A PVLAN domain can have multiple PVLAN sub-domains. The secondary VLANs of different sub-domains are different, but they share the same primary VLAN.
- Both the primary VLAN and secondary VLANs can contain physical ports. As shown in Figure 1-1, ports 0 and 1 belong to primary VLAN 2; and ports 2 and 3 belong to community VLAN 21. After an L2 association is configured between primary VLAN 2 and community VLAN 21, ports 0, 1, 2, and 3 belong to the same PVLAN sub-domain VLAN 2/21. They can make L2 communication with each other.
- In a PVLAN, L3 switch virtual interfaces (SVIs) can be created only in the primary VLAN, and L3 SVIs cannot be created in secondary VLANs. Hosts in a secondary VLAN can make L3 communication only after an L3 association is configured between the secondary VLAN and the primary VLAN. Otherwise, the hosts can make only L2 communication.

Figure 1-1 Logic Diagram of PVLAN



2. Primary VLAN and Promiscuous Port

Physical ports belonging to the primary VLAN are referred to as promiscuous ports. A PVLAN can have one or more promiscuous ports.

- In a PVLAN domain, a promiscuous port can communicate with any port, including another promiscuous port, a community VLAN port, and an isolated VLAN port. A promiscuous port is used as an uplink port for connecting to an external network or a port for connecting to a shared server so that hosts in all secondary VLANs can access the network and shared server.
- Outside a PVLAN domain, a promiscuous port belongs to the primary VLAN, allows common packets with the primary VLAN ID to pass through, and discards the other common VLAN packets.

3. Community VLAN and Community Port

A PVLAN domain can have multiple community VLANs. The ports in a community VLAN are referred to as community ports.

- Community ports in a community VLAN can communicate with each other but community ports of different community VLANs cannot communicate with each other.
- Community ports can communicate with promiscuous ports.
- Community ports cannot communicate with isolated ports.

4. Isolated VLAN and Isolated Port

A PVLAN domain can have only one isolated VLAN. Ports in an isolated VLAN are referred to as isolated ports.

- Isolated ports cannot communicate with each other. You can assign required hosts to an isolated VLAN for isolation.
- Isolated ports can communicate with only promiscuous ports. Packets can be forwarded from isolated ports to the promiscuous ports and vice versa.
- Packets can be forwarded from an isolated port to a trunk port. When receiving a packet (packet from the promiscuous port) with the VLAN ID of the primary VLAN ID, the trunk port can forward the packet to the isolated port. This enables the isolated port to communicate with an external network through a promiscuous port. Hosts in an isolated VLAN cannot communicate with each other. Therefore, when receiving a packet with the VLAN ID of the isolated VLAN, the trunk port cannot forward the packet to the isolated port.

Caution

Ports in a PVLAN can be used as mirroring source ports but cannot be used as mirroring destination ports.

1.1.3 L2 Forwarding and Isolation of PVLAN

Table 1-1 lists packet forwarding rules between different types of ports and VLAN tag changes.

Table 1-1 Packet Forwarding Rules between Different Types of Ports and VLAN Tag Changes

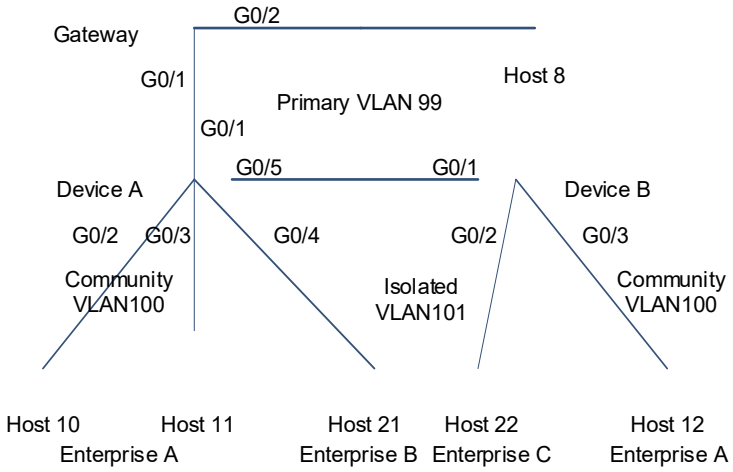
Output Port / Input Port	Promiscuous Port	Community Port	Isolated Port	Trunk Port (in the Same VLAN)
Promiscuous Port	Reachable, VLAN tag unchanged	Reachable, VLAN tag unchanged	Reachable, VLAN tag unchanged	Reachable, a primary VLAN tag added
Community Port	Reachable, VLAN tag unchanged	Reachable in the same community VLAN, VLAN tag unchanged Unreachable in different community VLANs	Unreachable	Reachable, a community VLAN tag added
Isolated Port	Reachable, VLAN tag unchanged	Unreachable	Unreachable	Reachable, an isolated VLAN tag added
Trunk Port	Reachable, VLAN tag removed	Reachable in the primary VLAN, VLAN tag removed Reachable in the same community VLAN, VLAN tag removed Unreachable in different community VLANs Unreachable in an isolated VLAN	Reachable in the primary VLAN, VLAN tag removed Unreachable in a community VLAN Unreachable in an isolated VLAN	Reachable, VLAN tag unchanged
Switch CPU	Reachable, no VLAN tag	Reachable, no VLAN tag	Reachable, no VLAN tag	Reachable, a primary VLAN tag added

1.1.4 Cross-Device L2 Application of PVLAN

As shown in the following figure, in the hosting service operation network, enterprise hosts are connected to the network through Device A or Device B. Hosts of an enterprise can communicate with each other but the host communication between enterprises is isolated. All the enterprise hosts share the same gateway address and can communicate with the external network through this gateway address. The deployment mode is as follows:

- Configure the PVLAN function on Device A and Device B, and add all enterprise hosts to the same PVLAN, for example, primary VLAN 99. All the enterprise hosts communicate with an external network through a shared L3 interface of the primary VLAN 99. The external network perceives the primary VLAN 99 only and does not perceive secondary VLANs. Configure GigabitEthernet 0/5 of Device A and GigabitEthernet 0/1 of Device B as trunk ports.
- If an enterprise has multiple hosts, allocate the hosts to different community VLANs and configure the ports connected to the hosts as host ports of the community VLANs so that the hosts in the enterprise can communicate with each other but host communication between enterprises is isolated.
- If an enterprise has only one host, allocate the host to an isolated VLAN and configure the port connected to the host as the host port of the isolated VLAN, to implement isolation of communication between hosts of different enterprises.
- Connect GigabitEthernet 0/1 of Device A to the gateway and configure this interface as a promiscuous port. The promiscuous port allows only packets with the primary VLAN ID to pass through and outputs untagged packets.
- Configure GigabitEthernet 0/1 of the gateway as a trunk or hybrid port. Because packets forwarded by a promiscuous port do not carry tags, set the native VLAN of GigabitEthernet 0/1 of the gateway to the primary VLAN of the PVLAN.

Figure 1-1 Typical Network Topology of PVLAN Applied Across L2 Devices



1.1.5 L3 Application of PVLAN on a Single Device

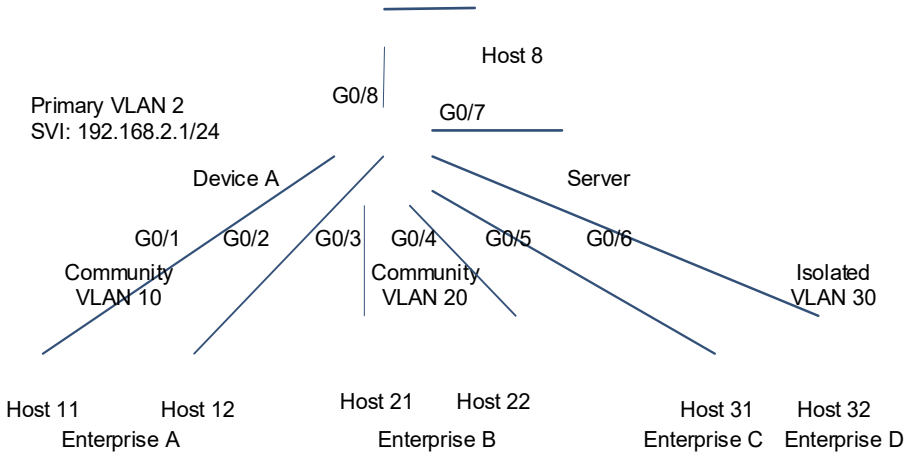
As shown in the following figure, in the hosting service operation network, enterprise hosts are connected to the network through the L3 Device A. Hosts of an enterprise can communicate with each other but the host communication between enterprises is isolated. All enterprise hosts can access the server. All enterprise hosts

share the same gateway address and can communicate with the external network through this gateway address.

The deployment mode is as follows:

- Add all enterprise hosts to the same PVLAN, for example, primary VLAN 2. Assign hosts of enterprise A to community VLAN 10, hosts of enterprise B to community VLAN 20, and hosts of enterprises C and D to isolated VLAN 30.
- Configure GigabitEthernet 0/7 that is directly connected to the server as a promiscuous port. Then, all enterprise hosts can communicate with the server through the promiscuous port.
- Configure the gateway address of the PVLAN on the L3 Device A (in this example, set the SVI address of VLAN 2 to 192.168.2.1/24) and configure the mappings between the primary VLAN and the secondary VLANs on the L3 interface. Then, all enterprise hosts can communicate with the external network through this gateway address.

Figure 1-1 Typical Network Topology of PVLAN Applied on a Single L3 Device



1.2 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

System resources are occupied when debugging information is output. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
show vlan private-vlan	Displays PVLAN configuration.
debug bridge pvlan	Debugs the PVLAN function.