https://community.fs.com/blog/what-is-private-vlan-and-how-it-works.html

What Is Private VLAN and How It Works?

What Is Private VLAN?

Private VLAN (PVLAN), also known as port isolation, is a network segmentation technology for layer 2 networks, which enables the ports isolation or traffic segmentation under the same IP segment. By applying private VLAN in a shared network environment, it greatly saves IP addresses and improves switch port security within layer 2.

Overview of Private VLAN Terms

Port Types of PVLAN

Typically, there are three VLAN port types:

Promiscuous Port: This port type is able to send and receive frames from any other ports in the VLAN. It usually connects with a layer 3 switch, router, or other gateway devices.

Isolated Port: Existing in a sub-VLAN, the isolated port connects with a host and can only communicate with promiscuous ports.

Community Port: Community port is also resided in a sub-VLAN and connects with a host. However, it can only chat with promiscuous ports and other community ports in the same sub-VLAN.

VLAN Types of PVLAN

Within a private VLAN, VLANs are accessible in three types:

Primary VLAN: This type of VLAN refers to the original VLAN, which can downstream frames to all its sub-VLANs (secondary VLANs) from promiscuous ports to all the host-connected ports.

Isolated VLAN: As a secondary VLAN, the isolated VLAN can only support switch ports (isolated ports) within the isolated VLAN forwarding data to promiscuous ports in the primary VLAN. Even in the same isolated VLAN, the isolated ports can not talk with each other.

Community VLAN: Community VLAN is also a type of secondary VLAN. Switch ports (community ports) within the same community VLAN can communicate with each other as well as ports of primary VLAN. But such a type of VLAN is also unable to communicate with other secondary VLANs, including other community VLANs.

How Private VLAN Works?

Generally, the private VLAN will go through the following stages :

1. The primary VLAN delivers frames downstream from the promiscuous port to all mapped hosts.

2. The isolated VLAN transports frames from the stub hosts upstream to the promiscuous port only.

3. Community VLANs allow bi-directional frame exchange within a single community group. Meanwhile, it will upstream data towards promiscuous ports.

4. Ethernet MAC address learning and forwarding procedure remain the same, as well as broadcast/multicast flooding procedure within boundaries of primary/secondary VLANs.

To know more details about what is VLAN and how it works, please refer to Understanding Virtual LAN (VLAN) Technology.

Confusing Questions About Private VLAN

1. How to Configure Private VLAN?

In FS, the S5800-8TF12S, S5850-32S2Q, S5850-48S6Q, S5850-48S2Q4C, S5850-48T4Q, S8050-20Q4C and N series switches all can support private VLAN. To configure the private VLAN, there are three steps to follow:

Step 1: Create primary and secondary VLANs and associate them.

Step 2: Configure isolated ports and community ports and bind them to the respective secondary VLANs.

Step 3: Configure interfaces as promiscuous ports, and map the promiscuous ports to the primary-secondary VLAN pair.

Step 4: If inter-VLAN routing will be used, configure the primary switch virtual interface, and map secondary VLANs to the primary.

Step 5: Verify private VLAN configuration.

2. How to Configure Isolated Ports (Traffic Segmentation) on FS Switches?

FS S3900 series Ethernet switches enable the traffic segmentation and S5800/5900/8050 series and N series switches can support the port isolation. The configuration roadmap for traffic segmentation or port isolation can be followed as below:

Step 1: Configure VLAN, IP addresses, and Ethernet interface for the specified switches to enable network interconnection.

Step 2: Add the interfaces to a traffic segmentation or port isolation group to implement layer 2 segmentation between these interfaces.

Step 3: Verify the configuration.

More details about how to configure traffic segmentation on FS 3900 series switches, you can refer to Traffic Segmentation Configuration on FS S3900 Series Switches.

3. VLAN Vs. Private VLAN: What's the Difference?

Usually, different VLANs map to different IP subnets. Devices in a VLAN can be configured to share the same broadcast domain. It can be worked in both layer 2 and layer 3.