2 Creating a Switched Ethernet Network

2.1 Lab 1: Ethernet Basics and VLAN Configuration

2.1.1 Introduction

2.1.1.1 About This Lab

Ethernet technology allows data communication over shared media through Carrier Sense Multiple Access/Collision Detection (CSMA/CD). When an Ethernet network has a large number of hosts, collision becomes a serious problem and can lead to broadcast storms. This can degrade network performance or even result a complete breakdown. Using switches to connect LANs can mitigate collisions, but broadcast may still pose an issue.

To alleviate broadcast storms, VLAN technology divides a physical LAN into multiple VLANs so that the broadcast domains are smaller. Hosts within a VLAN can only directly communicate with hosts in the same VLAN. They must use a router to communicate with hosts in other VLANs.

In this lab activity, you will learn how to configure VLAN on Huawei switches.

2.1.1.2 Objectives

Upon completion of this task, you will be able to:

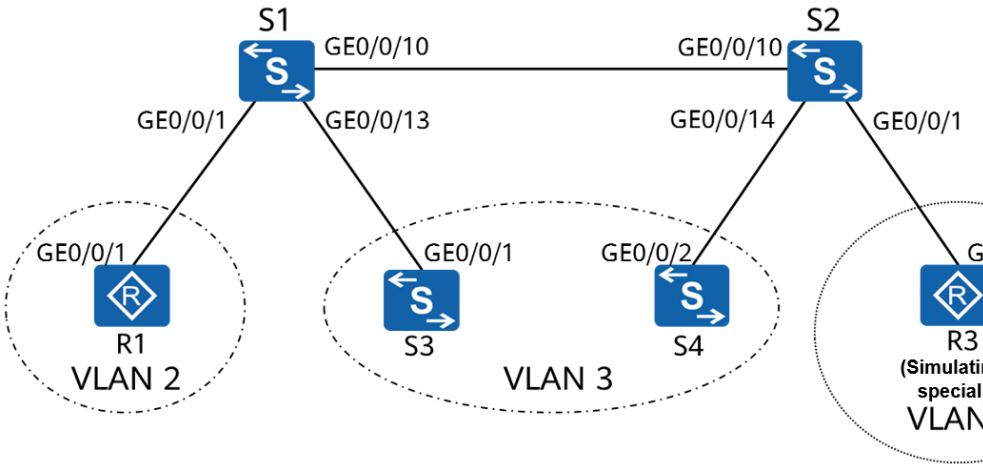
- Learn how to create a VLAN
- Learn how to configure access, trunk, and hybrid ports
- Learn how to configure VLANs based on ports
- Learn how to configure VLANs based on MAC addresses
- Learn how to view the MAC address table and VLAN information

2.1.1.3 Networking Topology

A company needs to divide a Layer 2 network into multiple VLANs based on service requirements. In addition, VLAN 10 requires a higher level of security and only specified PCs can be added to VLAN 10.

To meet this requirement, user ports of identical services on S1 and S2 can be assigned to the same VLAN, and ports with specified MAC addresses on S2 can be assigned to a VLAN.

Figure 2-1 Lab topology for VLAN configuration



2.1.2 Lab Configuration

2.1.2.1 Configuration Roadmap

1. Create a VLAN.
2. Configure a port-based VLAN.
3. Configure a MAC address-based VLAN.

2.1.2.2 Configuration Procedure

Step 1 Configure names for S1 and S2 and disable unnecessary ports.

Name the devices.

The details are not provided here.

Shut down GE0/0/11 and GE0/0/12 on S1. This step applies only to the environment described in *HCIA-Datacom Lab Construction Guide V1.0*.

```
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
[S1-GigabitEthernet0/0/11]quit
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
[S1-GigabitEthernet0/0/12]quit
```

Shut down GE0/0/11 and GE0/0/12 on S2.

```
[S2]interface GigabitEthernet 0/0/11
[S2-GigabitEthernet0/0/11]shutdown
[S2-GigabitEthernet0/0/11]quit
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
[S2-GigabitEthernet0/0/12]quit
```

Step 2 Configure the device IP addresses.

Set the IP addresses for R1 and R3 to 10.1.2.1/24 and 10.1.10.1/24, respectively.

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.1.2.1 24
```

```
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.1.10.1 24
```

Set the IP addresses of S3 and S4 to 10.1.3.1/24 and 10.1.3.2/24, respectively. (For scenario 1: S3 and S4 support switching from Layer 2 interfaces to Layer 3 interfaces.)

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]undo portswitch
The interface changes to Layer 3 mode.
```

The **undo portswitch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode.

```
[S3-GigabitEthernet0/0/1]ip address 10.1.3.1 24
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]undo portswitch
[S4-GigabitEthernet0/0/2]ip address 10.1.3.2 24
```

Set the IP addresses of VLANIF3 on S3 and S4 to 10.1.3.1/24 and 10.1.3.2/24, respectively. (For scenario 2: S3 and S4 do not support switching from Layer 2 interfaces to Layer 3 interfaces.)

1. Create VLAN 3 on S3 and S4.

```
[S3]vlan 3
[S3-vlan3]
```

```
[S4]vlan 3
[S4-vlan3]
```

2. Configure ports on S3 and S4 as access ports and assign them to corresponding VLANs.

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]port link-type access
[S3-GigabitEthernet0/0/1]port default vlan 3
[S3-GigabitEthernet0/0/1]quit
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]port link-type access
[S4-GigabitEthernet0/0/2]port default vlan 3
[S4-GigabitEthernet0/0/2]quit
```

3. # Create VLANIF interfaces and configure IP addresses.

```
[S3] interface Vlanif 3
```

The **interface vlanif** *vlan-id* command creates a VLANIF interface and displays the VLANIF interface view.

```
[S3-Vlanif3]ip address 10.1.3.1 24
```

```
[S4] interface Vlanif 3
[S4-Vlanif3]ip address 10.1.3.2 24
```

Step 3 Create a VLAN.

Create VLANs 2, 3, and 10 on S1 and S2.

```
[S1]vlan batch 2 to 3 10
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
VLANs 2, 3, and 10 are created successfully.
```

The **vlan** *vlan-id* command creates a VLAN and displays the VLAN view. If the VLAN exists, the VLAN view is displayed.

The **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } command creates VLANs in batches.

```
[S2]vlan batch 2 to 3 10
```

Step 4 Configure port-based VLANs.

Configure user ports on S3 and S4 as access ports and assign them to corresponding VLANs.

```
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
```

The **port link-type { access | hybrid | trunk }** command specifies the link type of an interface, which can be Access, Trunk, or Hybrid.

```
[S1-GigabitEthernet0/0/1]port default vlan 2
```

The **port default vlan** *vlan-id* command configures the default VLAN of an interface and assigns the interface to the VLAN.

```
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3
[S1-GigabitEthernet0/0/13]quit
```

```
[S2]interface GigabitEthernet0/0/14
[S2-GigabitEthernet0/0/14]port link-type access
[S2-GigabitEthernet0/0/14]port default vlan 3
[S2-GigabitEthernet0/0/14]quit
```

Configure the ports connecting S1 and S2 as trunk ports and allow only packets from VLAN 2 and VLAN 3 to pass through.

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
```

The **port trunk allow-pass vlan** command assigns a trunk port to the specified VLANs.

```
[S1-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

The **undo port trunk allow-pass vlan** command deletes a trunk port from the specified VLANs.

By default, VLAN 1 is in the allowed list. If VLAN 1 is not used for any service, it needs to be deleted for security purposes.

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port link-type trunk
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
[S2-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

Step 5 Configure MAC address-based VLANs.

As shown in the networking diagram, R3 simulates a special service PC. Assume that the MAC address of the PC is a008-6fe1-0c46. The PC is expected to connect to the network through any of GigabitEthernet0/0/1, GigabitEthernet0/0/2, and GigabitEthernet0/0/3 on S2 and transmit data through VLAN 10.

Configure S2 to associate the MAC address of the PC with VLAN 10.

The VLAN membership depends on the source MAC addresses of packets, and VLAN tags are added accordingly. This VLAN assignment method is independent of the location, providing a higher level of security and flexibility.

```
[S2] vlan 10
[S2-vlan10] mac-vlan mac-address a008-6fe1-0c46
```

The **mac-vlan mac-address** command associates a MAC address with a VLAN.

Set GigabitEthernet0/0/1, GigabitEthernet0/0/2, and GigabitEthernet0/0/3 on S2 to hybrid ports and configure them to allow packets from MAC address-based VLANs to pass through.

On access and trunk ports, MAC address-based VLAN assignment can be used only when the VLAN is the same as the PVID. Therefore, it is recommended that you configure MAC address-based VLAN assignment on a hybrid port to receive untagged packets from multiple VLANs.

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]port link-type hybrid
[S2-GigabitEthernet0/0/1]port hybrid untagged vlan 10
```

The **port hybrid untagged vlan** command assigns a hybrid port to the specified VLANs to allow untagged frames to pass through.

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]port link-type hybrid
[S2-GigabitEthernet0/0/2]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]port link-type hybrid
[S2-GigabitEthernet0/0/3]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/3]quit
```

Configure the ports connecting S1 and S2 to allow packets from VLAN 10 to pass through.

The ports need to allow tagged frames from multiple VLANs to pass through. Therefore, the ports can be configured as trunk ports.

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/10]quit
```

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S2-GigabitEthernet0/0/10]quit
```

Configure S2 and enable MAC address-based VLAN assignment on GE0/0/1, GE0/0/2, and GE0/0/3.

To enable a port to forward packets based on associations between MAC addresses and VLANs, you must run the **mac-vlan enable** command.

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]mac-vlan enable
```

The **mac-vlan enable** command enables MAC address-based VLAN assignment on a port.

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]mac-vlan enable
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]mac-vlan enable
[S2-GigabitEthernet0/0/3]quit
```

Step 6 Display the configuration information.

Display the VLAN information on the switch.

```
[S1]display vlan
```

The **display vlan** command displays information about VLANs.

The **display vlan verbose** command displays detailed information about a specified VLAN, including the ID, type, description, and status of the VLAN, status of the traffic statistics function, ports in the VLAN, and mode in which the ports are assigned to the VLAN.

```
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;        D: Down;        TG: Tagged;        UT: Untagged;
MP: Vlan-mapping;             ST: Vlan-stacking;
#: ProtocolTransparent-vlan;     *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common                UT: GE0/0/2(D)        GE0/0/3(D)     GE0/0/4(D)     GE0/0/5(D)
                           GE0/0/6(D)            GE0/0/7(D)     GE0/0/8(D)     GE0/0/9(D)
                           GE0/0/11(D)           GE0/0/12(D)    GE0/0/14(D)    GE0/0/15(D)
                           GE0/0/16(D)           GE0/0/17(D)    GE0/0/18(D)    GE0/0/19(D)
                           GE0/0/20(D)           GE0/0/21(D)    GE0/0/22(D)    GE0/0/23(D)
                           GE0/0/24(D)
2    common                UT: GE0/0/1(U)
                           TG: GE0/0/10(U)
3    common                UT: GE0/0/13(U)
                           TG: GE0/0/10(U)
10   common                TG: GE0/0/10(U)

VID  Status  Property      MAC-LRN Statistics  Description
--------------------------------------------------------------------------------
1    enable  default       enable   disable    VLAN 0001
2    enable  default       enable   disable    VLAN 0002
3    enable  default       enable   disable    VLAN 0003
10   enable  default       enable   disable    VLAN 0010
```

```
[S2]display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;        D: Down;        TG: Tagged;        UT: Untagged;
MP: Vlan-mapping;             ST: Vlan-stacking;
#: ProtocolTransparent-vlan;     *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common                UT: GE0/0/1(U)        GE0/0/2(D)     GE0/0/3(D)     GE0/0/4(D)
                           GE0/0/5(D)            GE0/0/6(D)     GE0/0/7(D)     GE0/0/8(D)
                           GE0/0/9(D)            GE0/0/11(D)    GE0/0/12(D)    GE0/0/13(D)
                           GE0/0/15(D)           GE0/0/16(D)    GE0/0/17(D)    GE0/0/18(D)
                           GE0/0/19(D)           GE0/0/20(D)    GE0/0/21(D)    GE0/0/22(D)
                           GE0/0/23(D)           GE0/0/24(D)
2    common                TG: GE0/0/10(U)
3    common                UT: GE0/0/14(U)
                           TG: GE0/0/10(U)
10   common                UT: GE0/0/1(U)        GE0/0/2(D)     GE0/0/3(D)
                           TG: GE0/0/10(U)

VID  Status  Property      MAC-LRN Statistics  Description
--------------------------------------------------------------------------------
1    enable  default       enable   disable    VLAN 0001
2    enable  default       enable   disable    VLAN 0002
3    enable  default       enable   disable    VLAN 0003
10   enable  default       enable   disable    VLAN 0010
```

Display the MAC address-based VLAN configuration on the switch.

```
[S2]display mac-vlan vlan 10
--------------------------------------------------------------------------------
MAC Address     MASK                VLAN    Priority
--------------------------------------------------------------------------------
00e0-fc1c-47a7  ffff-ffff-ffff              10      0

Total MAC VLAN address count: 1
```

The **display mac-vlan** command displays the configuration of MAC address-based VLAN assignment.

2.1.3 Verification

Test the device connectivity and verify the VLAN configuration.

1. Ping S4 from S3 and ensure that the ping operation is successful.
2. Ping other devices from R1 and ensure that the ping operation fails.
3. Ping R1 from R3, capture packets on the link between S1 and S2, and ensure that the ping operation fails but data frames with VLAN 10 tag can be captured.
4. Run the **display mac-address verbose** command on S1 and S2 to check the MAC address tables on the switches.

2.1.4 Configuration Reference

Configuration on S1

```
#
sysname S1
#
vlan batch 2 to 3 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
return
```

Configuration on S2

```
#
sysname S2
#
vlan batch 2 to 3 10
#
vlan 10
 mac-vlan mac-address a008-6fe1-0c46 priority 0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
```

```
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 3
#
return
```

2.1.5 Quiz

1. As shown in the following figure, to ensure the information security of a special service, only some special PCs can access the network through VLAN 10. How can this requirement be implemented on S1?