Revision Record

Do Not Print this Page

Course Code	Product	Product Version	Course Version
		V5R2	V1R1

Author/ID	Date	Reviewer/ID	New/ Update
Shi Miaomiao/swx791350	2019.10.23		

Inter-VLAN Communication

Foreword

- By default, a Layer 2 switching network is a broadcast domain, which brings many problems. Virtual local area network (VLAN) technology isolates such broadcast domains, preventing users in different VLANs from communicating with each other. However, such users sometimes need to communicate.
- This course describes how to implement inter-VLAN communication.

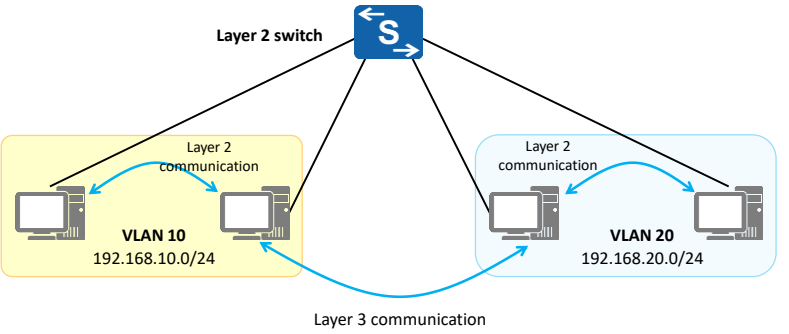
Objectives

- On completion of this course, you will be able to understand:
  - Methods of implementing inter-VLAN communication.
  - How to use routers (physical interfaces or sub-interfaces) to implement inter-VLAN communication.
  - How to use Layer 3 switches to implement inter-VLAN communication.
  - How Layer 3 packets are forwarded.

Contents

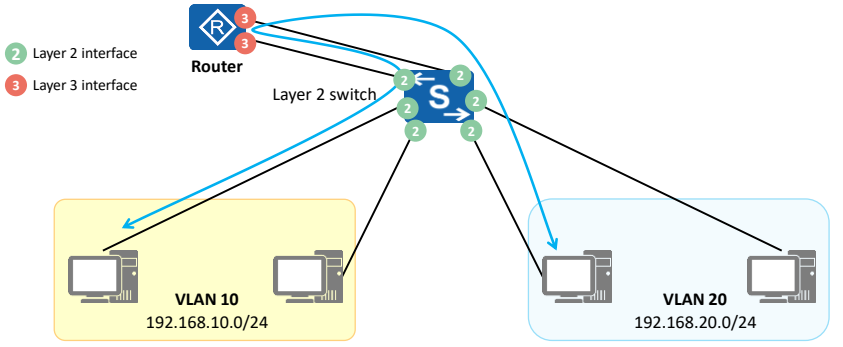
Inter-VLAN Communication (1)

- In real-world network deployments, different IP address segments are assigned to different VLANs.
- PCs on the same network segment in the same VLAN can directly communicate with each other without the need for Layer 3 forwarding devices. This communication mode is called Layer 2 communication.
- Inter-VLAN communication belongs to Layer 3 communication, which requires Layer 3 devices.



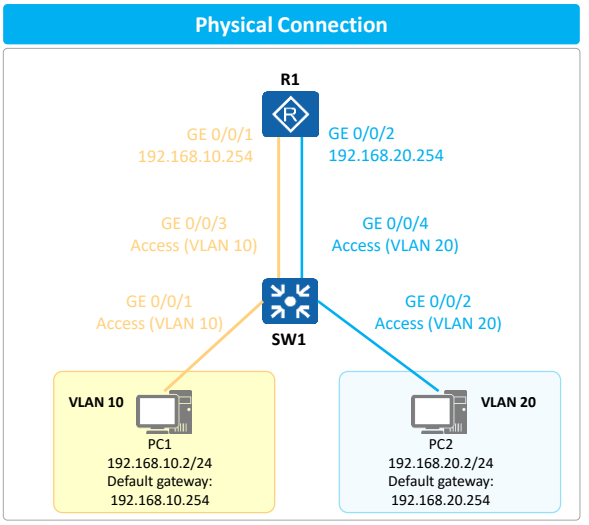
Inter-VLAN Communication (2)

- Common Layer 3 devices: routers, Layer 3 switches, firewalls, etc.
- Inter-VLAN communication is implemented by connecting a Layer 2 switch to a Layer 3 interface of a Layer 3 device. The communication packets are routed by the Layer 3 device.



Contents

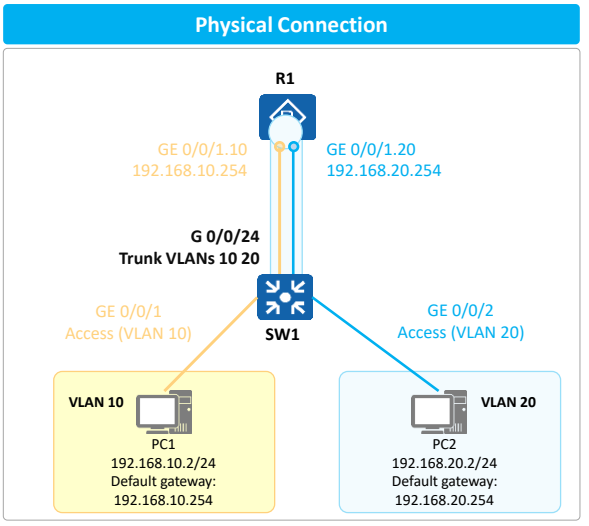
Using a Router's Physical Interfaces



- The Layer 3 interfaces of the router function as gateways to forward traffic from the local network segment to other network segments.
- The Layer 3 interfaces of the router cannot process data frames with VLAN tags. Therefore, the interfaces of the switch connected to the router must be set to the access type.
- One physical interface of the router can function as the gateway of only one VLAN, meaning that the number of required physical interfaces are determined by the quantity of the deployed VLANs.
- A router, mainly forwarding packets at Layer 3, provides only a small number of physical interfaces. Therefore, the scalability of this solution is poor.

- Configure VLANs on the Layer 2 switch. Each VLAN uses an independent switch interface to connect to the router.
- The router provides two physical interfaces as the default gateways of PCs in VLAN 10 and VLAN 20, respectively, for the PCs to communicate with each other.

Using a Router's Sub-interfaces

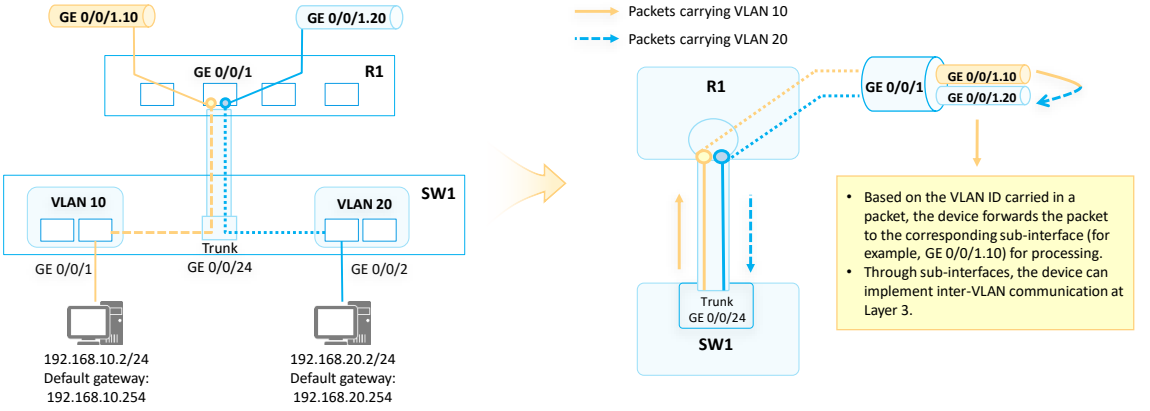


- A sub-interface is a logical interface created on a router's Ethernet interface and is identified by a physical interface number and a sub-interface number. Similar to a physical interface, a sub-interface can perform Layer 3 forwarding.
- Different from a physical interface, a sub-interface can terminate data frames with VLAN tags.
- You can create multiple sub-interfaces on one physical interface. After connecting the physical interface to the trunk interface of the switch, the physical interface can provide Layer 3 forwarding services for multiple VLANs.

- R1 connects to SW1 through a physical interface (GE 0/0/1). Two sub-interfaces (GE 0/0/1.10 and GE 0/0/1.20) are created on the physical interface and used as the default gateways of VLAN 10 and VLAN 20, respectively.
- Layer 3 sub-interfaces do not support VLAN packets and discard them once received. To prevent this issue, the VLAN tags need to be removed from the packets on the sub-interfaces. That is, VLAN tag termination is required.

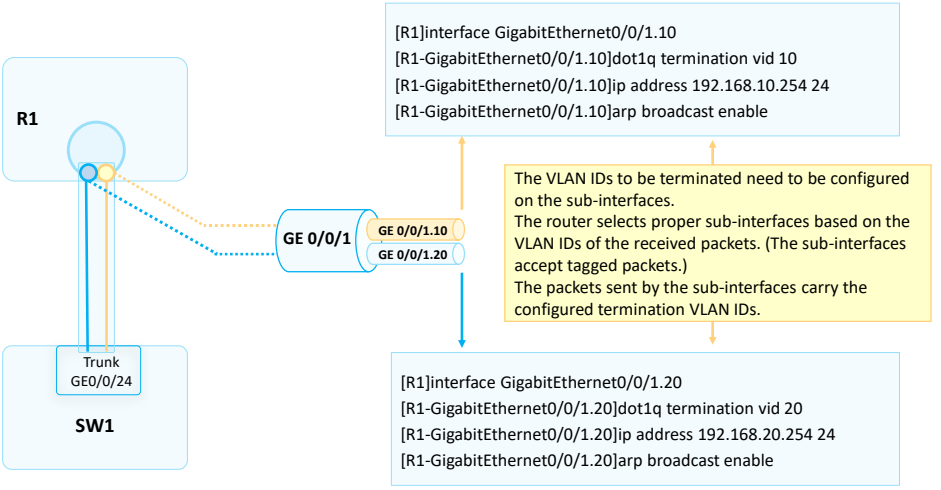
Sub-Interface Processing

- The interface connecting the switch to the router is set to a trunk interface. The router forwards the received packets to the corresponding sub-interfaces according to the VLAN tags in the packets.



- A sub-interface implements VLAN tag termination as follows:
  - Removes VLAN tags from the received packets before forwarding or processing the packets.
  - Adds VLAN tags to the packets before forwarding the packets.

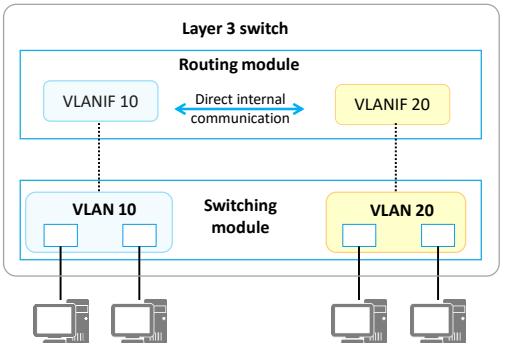
Example for Configuring Sub-interfaces



- The **interface** *interface-type interface-number.sub-interface number* command creates a sub-interface. *sub-interface number* specifies the number of a sub-interface on a physical interface. For easy memorization, a sub-interface number is generally the same as the VLAN ID to be terminated on the sub-interface.
- The **dot1q termination vid** command enables Dot1q VLAN tag termination for single-tagged packets on a sub-interface. By default, Dot1q VLAN tag termination for single-tagged packets is not enabled on sub-interfaces. The **arp broadcast enable** command enables ARP broadcast on a VLAN tag termination sub-interface. By default, ARP broadcast is not enabled on VLAN tag termination sub-interfaces. VLAN tag termination sub-interfaces cannot forward broadcast packets and automatically discard received ones. To allow a VLAN tag termination sub-interface to forward broadcast packets, run the **arp broadcast enable** command.

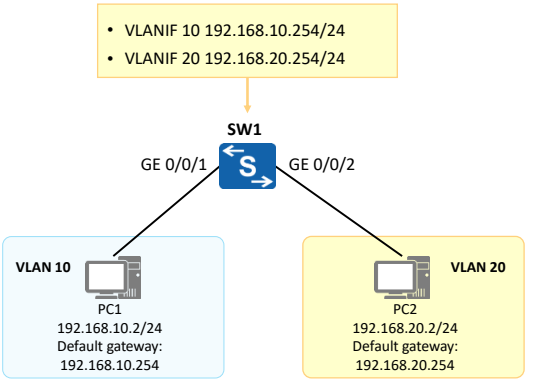
Contents

Layer 3 Switch and VLANIF Interfaces



- A Layer 2 switch provides only Layer 2 switching functions.
- A Layer 3 switch provides routing functions through Layer 3 interfaces (such as VLANIF interfaces) as well as the functions of a Layer 2 switch.
- A VLANIF interface is a Layer 3 logical interface that can remove and add VLAN tags. VLANIF interfaces therefore can be used to implement inter-VLAN communication.
- A VLANIF interface number is the same as the ID of its corresponding VLAN. For example, VLANIF 10 is created based on VLAN 10.

Example for Configuring VLANIF Interfaces



- Configuration Requirements
  Configure VLANs 10 and 20 for the interfaces connecting to PC1 and PC2, respectively. Configure the Layer 3 switch to allow the two PCs to communicate with each other.

Basic configurations:

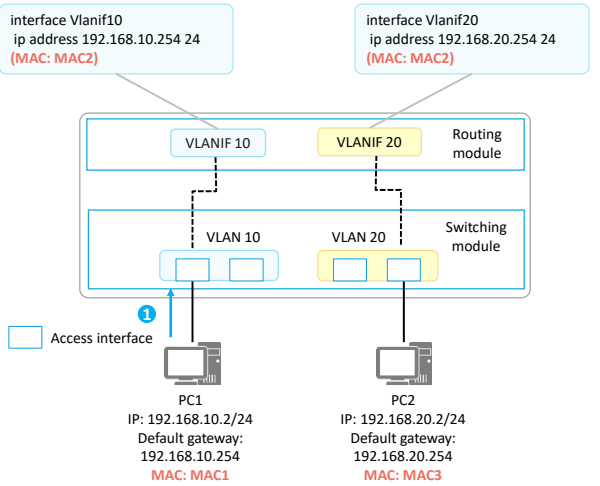
```
[SW1]vlan batch 10 20
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1-GigabitEthernet0/0/2] port default vlan 20
```

Configure VLANIF interfaces:

```
[SW1]interface Vlanif 10
[SW1-Vlanif10]ip address 192.168.10.254 24
[SW1]interface Vlanif 20
[SW1-Vlanif20]ip address 192.168.20.254 24
```


- The **interface vlanif** *vlan-id* command creates a VLANIF interface and displays the VLANIF interface view. *vlan-id* specifies the ID of the VLAN associated with the VLANIF interface. The IP address of a VLANIF interface is used as the gateway IP address of a PC and must be on the same network segment as the IP address of the PC.

VLANIF Forwarding Process (1)

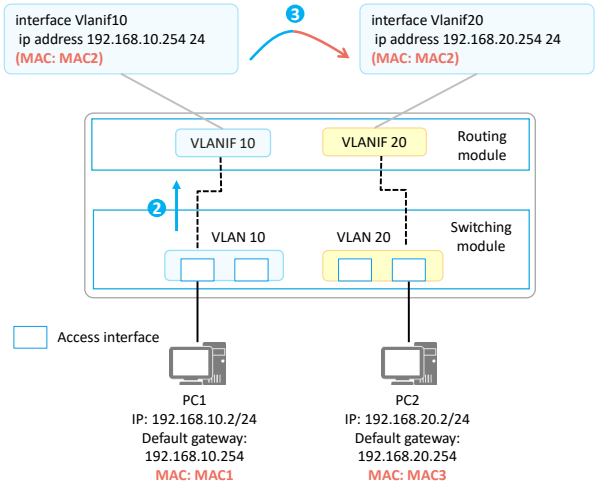


This example assumes that the required ARP or MAC address entries already exist on the PCs and the Layer 3 switch.

The communication process between PC1 and PC2 is as follows:

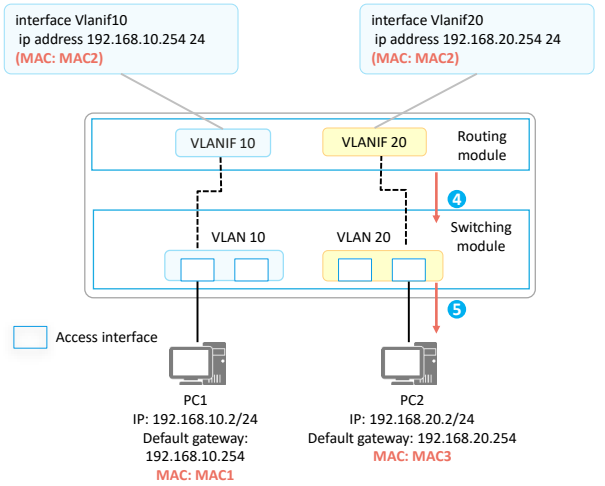
1. PC1 performs calculation based on its local IP address, local subnet mask, and destination IP address, and finds that the destination device PC2 is not on its network segment. PC1 then determines that Layer 3 communication is required and sends the traffic destined for PC2 to its gateway. Data frame sent by PC1: source MAC = MAC1, destination MAC = MAC2

VLANIF Forwarding Process (2)



2. After receiving the packet sent from PC1 to PC2, the switch decapsulates the packet and finds that the destination MAC address is the MAC address of VLANIF 10. The switch then sends the packet to the routing module for further processing.
3. The routing module finds that the destination IP address is 192.168.20.2, which is not the IP address of its local interface, and determines that this packet needs to be forwarded at Layer 3. By searching the routing table, the routing module finds a matching route – the direct route generated by VLANIF 20 – for this packet.

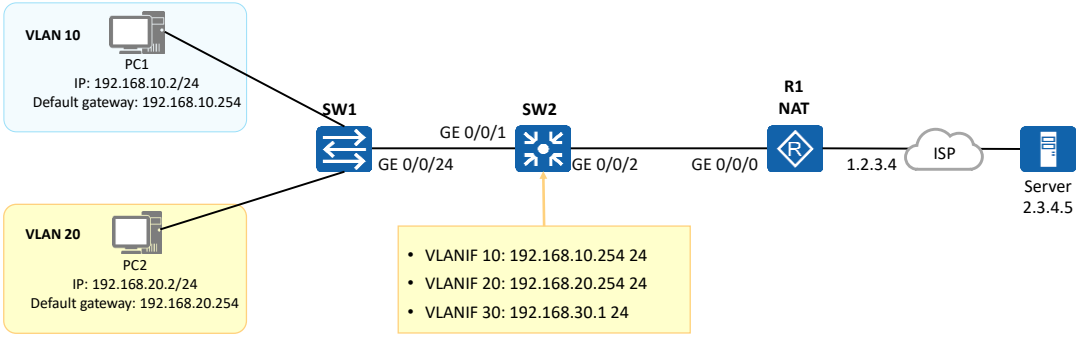
VLANIF Forwarding Process (3)



4. Because the matching route is a direct route, the switch determines that the packet has reached the last hop. It searches its ARP table for 192.168.20.2, obtains the corresponding MAC address, and sends the packet to the switching module for re-encapsulation.
5. The switching module searches its MAC address table to determine the outbound interface of the frame and whether the frame needs to carry a VLAN tag. Data frame sent by the switching module: source MAC = MAC2, destination MAC = MAC3, VLAN tag = None

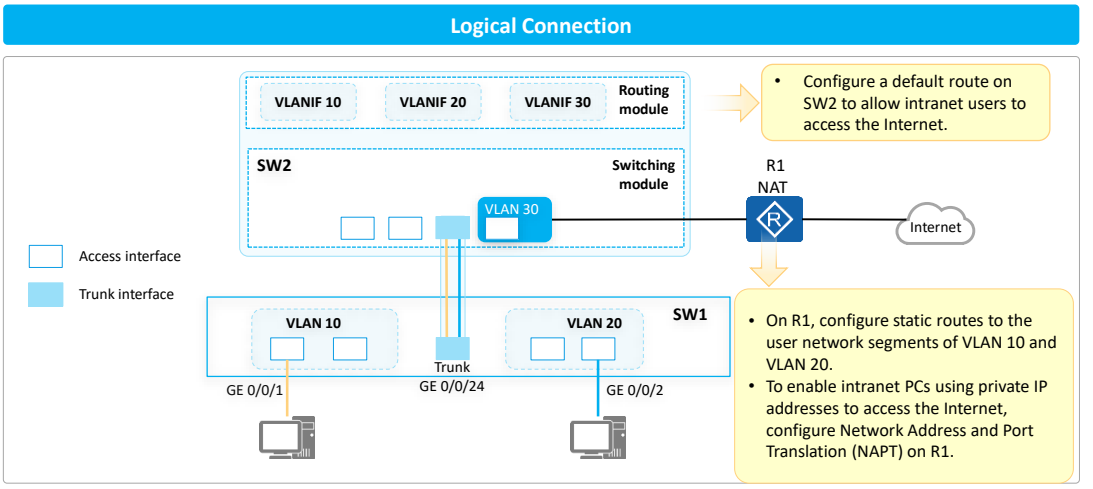
Contents

Network Topology



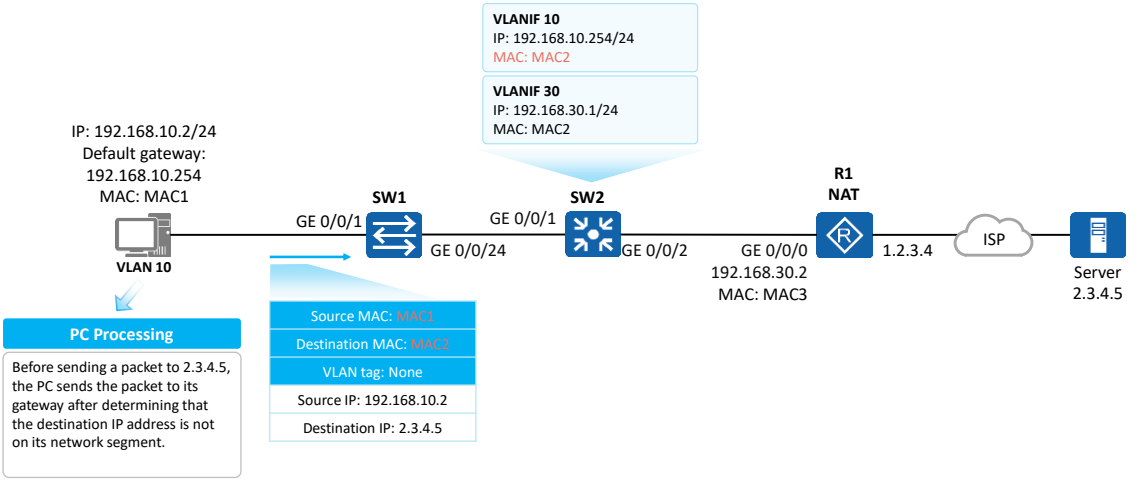
This topology is used as an example to describe the communication process from PC1 in VLAN 10 to the server (2.3.4.5) on the Internet.

Logical Connection



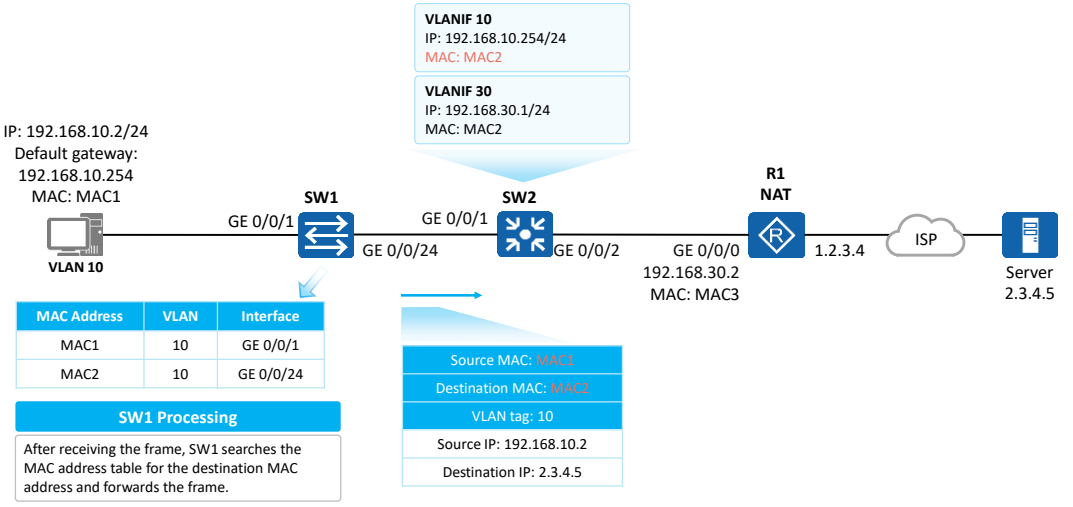
- NAPT: translates the IP address and port number in an IP packet header to another IP address and port number. NAPT is mainly used to enable devices on an internal network (private IP addresses) to access an external network (public IP addresses). NAPT allows multiple private IP addresses to be mapped to the same public IP address. In this way, multiple private IP addresses can access the Internet at the same time using the same public IP address.

Communication Process (1)

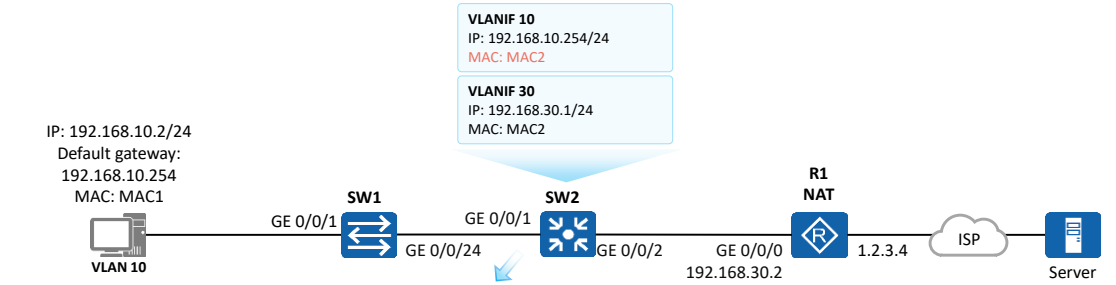


- This example assumes that the required ARP or MAC address entries already exist on all devices.

Communication Process (2)



Communication Process (3)



Operational data of a routing table.

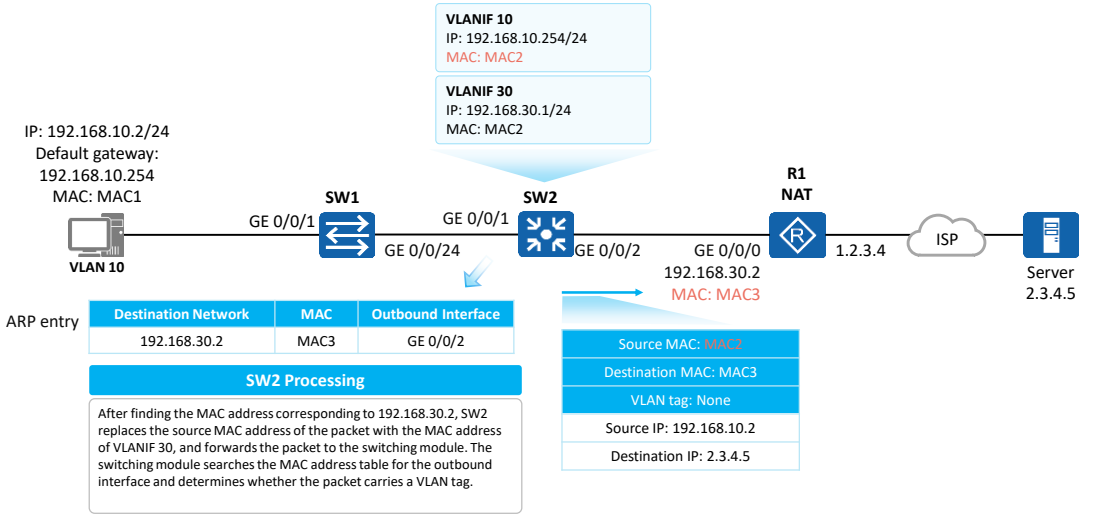
Destination Network	Next Hop	Outbound Interface
0.0.0.0/0	192.168.30.2	Vlanif30

SW2 Processing

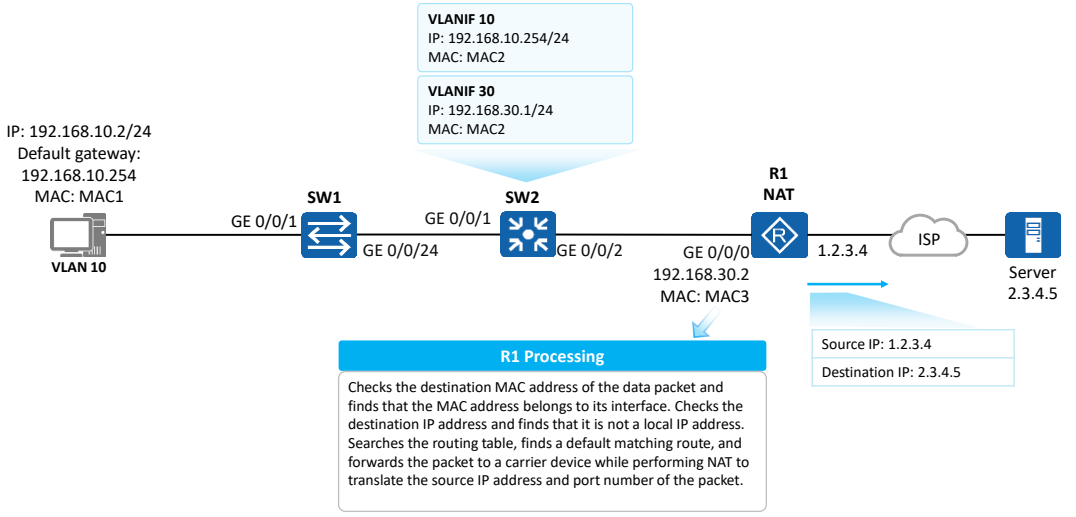
After SW2 receives the frame, it finds that the destination MAC address is the MAC address of its VLANIF 10 and sends the frame to the routing module, which then searches the routing table for a route matching the destination IP address 2.3.4.5.

After finding that the matching route is a default route, the outbound interface is VLANIF 30, and the next hop is 192.168.30.2, SW2 searches its ARP table to obtain the MAC address corresponding to 192.168.30.2.

Communication Process (4)



Communication Process (5)



- Network Address Translation (NAT) translates the IP addresses in IP packet headers to other IP addresses.

Quiz

1. When a sub-interface is used to implement inter-VLAN communication, how does the switch interface connected to the router need to be configured?
2. How are packets changed when being forwarded at Layer 3?

1. Configure the interface as a trunk or hybrid interface to permit packets carrying VLAN tags corresponding to terminals.
2. The source and destination IP addresses remain unchanged during packet forwarding (without NAT), but the source and destination MAC addresses change. Each time a packet passes through a Layer 3 device, its source and destination MAC addresses change.

Summary

- This course describes three methods of implementing inter-VLAN communication: through physical interfaces, sub-interfaces, and VLANIF interfaces.
- It also elaborates the Layer 3 communication process, and device processing mechanism and packet header changes during the communication.

More Information

- Comparison between Layer 2 and Layer 3 interfaces

Layer 2 Interface	Layer 3 Interface
An IP address cannot be configured for a Layer 2 interface.	An IP address can be configured for a Layer 3 interface
A Layer 2 interface does not have a MAC address.	A Layer 3 interface has a MAC address.
After a Layer 2 interface receives a data frame, it searches its MAC address table for the destination MAC address of the frame. If a matching MAC address entry is found, it forwards the frame according to the entry. If no matching MAC address entry is found, it floods the frame.	After a Layer 3 interface receives a data frame, if the destination MAC address of the data frame is the same as the local MAC address, it decapsulates the data frame and looks up the destination IP address of the data packet in the routing table. If a matching route is found, it forwards the data frame according to the instruction of the route. If no matching route is found, it discards the packet.
A physical interface on a Layer 2 switch (has only Layer 2 switching capabilities) is a typical Layer 2 interface. By default, the physical interfaces of most Layer 3 switches (have both Layer 2 and Layer 3 switching capabilities) work at Layer 2.	A Layer 3 interface on a router is a typical Layer 3 interface. Physical interfaces on some Layer 3 switches can be switched to Layer 3 mode. In addition to Layer 3 physical interfaces, there are Layer 3 logical interfaces, such as VLANIF interfaces on switches or logical sub-interfaces on other network devices, such as GE 0/0/1.10.
Layer 2 interfaces do not isolate broadcast domains. They flood received broadcast frames.	Layer 3 interfaces isolate broadcast domains. They directly terminate received broadcast frames instead of flooding them.


Thank You
www.huawei.com