Contents

1 Configuring Super VLAN

1.1 Introduction

1.1.1 Overview

Super virtual local area network (VLAN), also referred to as VLAN aggregation, is a VLAN assignment method.

A common VLAN corresponds to a subnet and is used to complete L3 communication with another VLAN based on a gateway IP address.

The super VLAN technology allows you to configure common VLANs as sub VLANs, aggregate them into one super VLAN, assign only one IP address to the super VLAN as the gateway IP address to implement inter-VLAN L3 communication. This technology saves IP address resources and facilitates network management.

1.1.2 Background and Function

1. Background

A common VLAN corresponds to a logical subnet and is isolated from other VLANs at L2. Each subnet must be assigned with a gateway IP address to implement inter-VLAN L3 communication. In addition to the gateway IP address, each subnet also requires a subnet ID and a subnet-directed broadcast IP address as dedicated addresses. These three addresses cannot be assigned to hosts.

Suppose that a local area network (LAN) covers three departments and therefore requires three VLANs. The VLAN IDs and hosts of the three departments are as follows: VLAN 10 (31 hosts), VLAN 20 (44 hosts), and VLAN 30 (128 hosts). There are 203 hosts in total. The network segment 192.168.1.0/24 has 256 IP addresses, which are assigned to the three departments to meet network requirements. A device performs a logical "AND" operation on IP addresses and subnet masks in binary format to identify the subnet, to which the hosts belong. The VLAN assignment result is as follows:

- VLAN 10 requires 31 host addresses and 3 dedicated addresses, totaling 34 addresses. VLAN 10 needs to be assigned with 64 IP addresses (2^6) with the subnet mask of /26.

  IP address range: 192.168.1.0 to 192.168.1.63 = 11000000.10101000.00000001.(00000000 to 00111111)

  Subnet mask (/26): 255.255.255.192 = 11111111.11111111.11111111.11000000

  Network ID obtained via logical "AND" operation in binary format: 192.168.1.0 = 11000000.10101000.00000001.00000000

  Gateway IP address: 192.168.1.1 = 11000000.10101000.00000001.00000001

  Subnet-directed broadcast IP address: 192.168.1.63 = 11000000.10101000.00000001.00111111

  Host IP address: 192.168.1.2 to 192.168.1.62 (31 hosts must be assigned with 61 addresses, and therefore 30 addresses are wasted)

- VLAN 20 requires 44 host addresses and 3 dedicated addresses, totaling 47 addresses. VLAN 20 needs to be assigned with 64 addresses (2^6) with the subnet mask of /26.

IP address range: 192.168.1.64 to 192.168.1.127 = 11000000.10101000.00000001.(01000000 to 01111111)

Subnet mask (/26): 255.255.255.192 = 11111111.11111111.11111111.11000000

Network ID obtained via logical "AND" operation in binary format: 192.168.1.64 = 11000000.10101000.00000001.01000000

Gateway IP address: 192.168.1.65 = 11000000.10101000.00000001.01000001

Subnet-directed broadcast IP address: 192.168.1.127 = 11000000.10101000.00000001.01111111

Host IP address: 192.168.1.66 to 192.168.1.126 (44 hosts must be assigned with 61 addresses, and therefore 17 addresses are wasted)

- Only 125 addresses are available to VLAN 30 that includes 128 hosts.

IP address range: 192.168.1.128 to 192.168.1.255 = 11000000.10101000.00000001.(10000000 to 11111111)

Subnet mask (/25): 255.255.255.128 = 11111111.11111111.11111111.10000000

Network ID obtained via logical "AND" operation in binary format: 192.168.1.128 = 11000000.10101000.00000001.10000000

Gateway IP address: 192.168.1.129 = 11000000.10101000.00000001.10000001

Subnet-directed broadcast IP address: 192.168.1.255 = 11000000.10101000.00000001.11111111

Host IP address: 192.168.1.130 to 192.168.1.254 (128 hosts are assigned with only 125 addresses)

It can be inferred from the assignment method that if each VLAN is assigned with a subnet, 9 dedicated addresses are required and 47 (30 + 17) host addresses are wasted. Though the network segment 192.168.1.0/24 contains 256 addresses, they cannot meet the IP address requirements of the 203 hosts.

This assignment method also lacks flexibility. If you add hosts to VLAN 20, exceeding the limit 64, you have to add the new hosts to another VLAN and assign IP addresses of another network segment to the new hosts unless you change the original IP address assignment policy. As a result, hosts from the same department do not belong to the same network segment.

To avoid the IP address waste and address assignment management problems, the super VLAN technology is developed.

2. Function

The super VLAN technology is used to aggregate multiple sub VLANs into one super VLAN.

L2 isolation is implemented by sub VLANs, and L3 interconnection is implemented by super VLANs.

A super VLAN corresponds to a logical subnet, and all sub VLANs in the super VLAN belong to this subnet and share the same network ID, gateway IP address, and subnet-directed broadcast IP address. This saves IP address resources and improves network management flexibility.

3. Features

- Super VLAN

A super VLAN corresponds to a network segment. Switch virtual interfaces (SVIs) can be created only in super VLANs, but no physical port can be added to the super VLANs. Super VLAN manages inter-VLAN communication of sub VLANs by using the SVIs. A super VLAN cannot be considered as an IEEE 802.1Q VLAN. A super VLAN has only L3 attributes of a common VLAN.
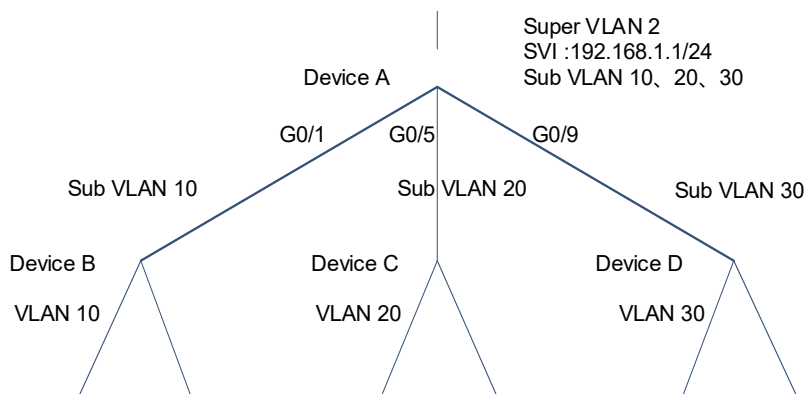
● Sub VLAN

Each sub VLAN is an independent broadcast domain, and is isolated from other sub VLANs at L2. A sub VLAN belongs to only one super VLAN. No SVI can be created in a sub VLAN, which can contain only physical ports. A sub VLAN has only L2 attributes of a common VLAN. To implement L3 communication across broadcast domains, sub VLANs must use the SVIs of the super VLAN.

4. **Application**

After the super VLAN technology is applied to the case described in Background, the network segment 192.168.1.0/24 can meet the requirement for IP addresses. As shown in Figure 1-1, on Device A, VLAN 2 is configured as a super VLAN, SVI address 192.168.1.1/24 as the gateway address, and VLAN 10, VLAN 20 and VLAN 30 as sub VLANs. Hosts are isolated at L2 through sub VLANs and make L3 communication with hosts in other network segments based on the common gateway IP address. The network segment accommodates IP addresses ranging from 192.168.1.2 to 192.168.1.254. A total of 253 IP addresses can be assigned to the 203 hosts in the sub VLANs, and there are some idle addresses left. Devices B, C, and D are used to expand the access ports and configured with VLAN 10, VLAN 20, and VLAN 30, respectively.

Figure 1-1   Application of Super VLAN

1.1.3 Principles

1. **Communication in a Sub VLAN**

A common VLAN corresponds to a subnet, and hosts in the subnet belong to the same broadcast domain. When a host (source host) in a common VLAN sends a packet, the host determines whether the destination host is in the same subnet as the source host. If yes, the host broadcasts an Address Resolution Protocol (ARP) request to request and obtain the MAC address of the destination host, and then completes L2 communication with the destination host. If not, the host broadcasts an ARP request to request and obtain the MAC address of the gateway, and then forwards the packet to the gateway for L3 communication.

In a super VLAN, when a host (source host) in a sub VLAN sends a packet, the host determines whether the destination host is in the same subnet as the source host and whether they belong to the same sub VLAN. If

yes, the communication procedure is similar to the L2 communication procedure of a common VLAN. The communication steps are as follows:

(1) The source host determines that the destination host is in the same subnet as the source host but the destination MAC address is unknown. The source host broadcasts an ARP request to request the destination MAC address.

(2) A switch learns the MAC address and forwards the ARP broadcast request to all ports except the source port in the sub VLAN.

(3) Upon receiving the ARP request, the destination host in the sub VLAN sends a unicast ARP reply to the source host.

(4) The switch learns the MAC address and forwards the ARP reply packet.

(5) Upon receiving the ARP reply packet, the source host obtains the destination MAC address and then can realize L2 communication with the destination host.

2.   Communication Between Different Sub VLANs in a Super VLAN

Though the sub VLANs in a super VLAN belong to the same subnet, they are isolated at L2 and belong to different broadcast domains. When a host (source host) in a sub VLAN tries to communicate with a host (destination host) in another sub VLAN of the super VLAN, the communication initially follows an L2 forwarding procedure because the source host does not know it is isolated from the destination host. In this case, communication between different sub VLANs relies on proxy ARP of a switch. The actual communication procedure is completed at L3. The communication steps are as follows.

(1) The source host determines that the destination host is in the same subnet as the source host but the destination MAC address is unknown. The source host broadcasts an ARP request to request the destination MAC address.

(2) A switch learns the source MAC address and forwards the ARP request to all ports except the source port in the sub VLAN.

(3) Hosts in other sub VLANs cannot receive this ARP request. Therefore, no ARP reply is sent to the switch. After a specified period of time, the switch enables proxy ARP, replaces the source MAC address in the request packet with the gateway MAC address of the super VLAN, and broadcasts the ARP request in all sub VLANs of the super VLAN to request the destination MAC address.

  ⓘ   **Note**

●   The IP addresses in sub VLANs may be discontinuous and dynamic due to the address assignment policy of a Dynamic Host Configuration Protocol (DHCP) server or capacity expansion. This makes the super VLAN unable to identify the sub VLAN, to which the destination IP address belongs. Therefore, the broadcast packet is sent to all sub VLANs in the super VLAN by default.

●   You can configure an IP address range for each sub VLAN so that the broadcast packet can be sent to a specific sub VLAN based on the IP address. In this case, the DHCP function must be disabled, because the IP addresses assigned by this function may fall out of the IP address range of a specific sub VLAN. The configured static IP addresses must be within the IP address range of a specific sub VLAN. Otherwise, communication between sub VLANs cannot be realized.

●   You can configure a sub VLAN as a broadcast VLAN so that broadcast packets sent by the super VLAN are destined to this sub VLAN. However, this configuration may cause the failure of the destination host to receive the ARP broadcast request, resulting in a communication exception.

---

(4) Upon receiving the ARP request, the destination host in another sub VLAN learns the mapping between the gateway MAC address and the source IP address and sends a unicast ARP reply to the gateway.

(5) The switch learns the following mapping of the destination host: "IP address – MAC address – sub VLAN – port". The switch replaces the destination MAC address with the gateway MAC address and sends the unicast ARP reply to the source host.

(6) Upon receiving the ARP reply, the source host regards the gateway MAC address as the destination MAC address, learns the mapping between the gateway MAC address and the destination IP address, and completes L3 communication through the proxy gateway.

The process in which the gateway replaces the source MAC address with the gateway MAC address to send an ARP request and the process in which the gateway replaces the destination MAC address with the gateway MAC address to send an ARP reply are referred to as proxy ARP. Communication across broadcast domains needs to rely on proxy ARP.

3. **Communication Between Super VLANs**

Different super VLANs correspond to different subnets and the destination host and source host in different super VLANs belong to different broadcast domains. The source host can determine that the destination host is in a different broadcast domain based on the IP address network segment. The communication process is similar to the communication between different network segments of common VLANs. In this communication procedure, the gateway also performs proxy ARP. However, the gateway is an SVI of the super VLAN rather than the SVI of a common VLAN.

4. **Inter-Device L2 Communication**

Super VLAN works at L3. The SVI of a super VLAN is used as a gateway only in L3 communication across broadcast domains (across network segments or in the same network segment). The VLAN ID of a super VLAN is not used in L2 communication.

No physical port can be added to a super VLAN. On a device where a super VLAN is configured, packets with containing VLAN ID of the super VLAN cannot pass through any port of the device.

As shown in [Figure 1-1](#), VLAN 2 is configured as a super VLAN on Device A. Assume that VLAN 2 is configured as a common VLAN on Device B. When Device A receives a packet from VLAN 2 on Device B, Device A discards this packet.

The communication between sub VLAN 10 on Device A and VLAN 10 on Device B is inter-device L2 communication. Their connected interfaces must allow packets of sub VLAN 10 to pass so that the packets can be forwarded by the interface. If packets are tagged, the VLAN ID in the tags is the VLAN ID of sub VLAN 10.

1.2 Configuration Task Summary

The configuration includes the following tasks:

(1) Configure a super VLAN and sub VLANs.

    a   [Configuring L2 Association for a Super VLAN](#)

    b   [Configuring L3 Communication for a Super VLAN](#)

    c   (Optional) [Configuring an IP Address Range for a Sub VLAN](#)

    d   (Optional) [Configuring a Broadcast VLAN](#)

(2) Configure ports and add the ports to the sub VLANs. For more information, see *Configuring VLAN*.

1.3 Configuring L2 Association for a Super VLAN

1.3.1 Overview

You can configure a common VLAN as a super VLAN, configure other common VLANs as sub VLANs, and add the sub VLANs to the super VLAN. A sub VLAN is a broadcast domain, hosts in a sub VLAN can make L2 communication with each other but are L2 isolated from hosts outside the sub VLAN.

1.3.2 Restrictions and Guidelines

- Super VLAN

  o VLAN 1 cannot be configured as a super VLAN.

  o No physical port can be added to a super VLAN. After a common VLAN is configured as a super VLAN, the ports that have been added to the VLAN exit the VLAN and are added to VLAN 1.

  o A super VLAN does not belong to any physical port. Therefore, the device configured with the super VLAN cannot process packets that contain the super VLAN tag.

  o A super VLAN cannot be configured as a sub VLAN of another super VLAN. A sub VLAN of a super VLAN cannot be configured as a super VLAN.

  o You can use the **no supervlan** command to restore a super VLAN and all its sub VLANs to common VLANs. You must restore a super VLAN to a common VLAN before deleting this super VLAN by running the **no vlan** command.

- Sub VLAN

  o You must configure sub VLANs for a super VLAN so that the super VLAN is valid.

  o VLAN 1 cannot be configured as a sub VLAN.

  o You can configure multiple super VLANs on a device. A sub VLAN can be added to one super VLAN only and the sub VLANs in different super VLANs must be unique.

  o Avoid configuring too many sub VLANs. A broadcast packet of a super VLAN is sent to all its sub VLANs by default. The configuration of too many sub VLANs will degrade the performance.

  o Physical ports can be added to a sub VLAN. A common VLAN configured with an L3 SVI cannot be configured as a sub VLAN.

  o You must restore a sub VLAN to a common VLAN by running the **no subvlan** command before deleting this sub VLAN by running the **no vlan** command. In super VLAN configuration mode, you can use the **no subvlan** [*vlan-id-list*] command to restore a specific sub VLAN in the super VLAN to a common VLAN.

1.3.3 Procedure

(1) Create a common VLAN to be configured as a sub VLAN.

  a   Enter the privileged EXEC mode.

      enable

  b   Enter the global configuration mode.

configure terminal

c   Create a common VLAN to be configured as a sub VLAN.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d   Return to the global configuration mode.

exit

(2) Create a common VLAN to be configured as a super VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

Only VLAN 1 exists by default.

(3) Configure a common VLAN as a super VLAN.

supervlan

The super VLAN function is disabled by default. Therefore, created VLANs are common VLANs.

(4) Add the common VLAN to the super VLAN to make the common VLAN become a sub VLAN of the super VLAN.

subvlan *vlan-id-list*

No common VLAN is added to a super VLAN to become a sub VLAN by default.

1.4   Configuring L3 Communication for a Super VLAN

1.4.1 Overview

A super VLAN corresponds to a logical subnet. No physical port can be added to a super VLAN and only an L3 SVI can be configured for the super VLAN. IP addresses must be configured for L3 SVIs. Sub VLANs of a super VLAN share the gateway address of the super VLAN and reside in the same network segment.

Proxy ARP must be enabled on the super VLAN and sub VLANs so that hosts in the sub VLANs can implement L3 communication across broadcast domains through proxy ARP of the super VLAN.

1.4.2 Restrictions and Guidelines

● An SVI and an IP address must be configured for a super VLAN. The SVI is a virtual interface used for communication between sub VLANs. You cannot configure an SVI for a sub VLAN.

● When you configure an SVI for a super VLAN, the system assigns an L3 interface invisible to hosts to each sub VLAN in the super VLAN. The system may restore some sub VLANs to common VLANs due to resource deficiency. After an SVI is configured for a super VLAN, the attempt of adding sub VLANs may fail due to resource deficiency.

● Proxy ARP must be configured in VLAN configuration mode. Proxy ARP must be enabled on both the super VLAN and its sub VLANs so that L3 communication can be implemented. Proxy ARP is enabled by default. To isolate communication between sub VLANs, you can use the **no proxy-arp** command to disable proxy ARP.

1.4.3 Procedure

(1) Configure a gateway for a super VLAN.

a   Enter the privileged EXEC mode.

enable

b   Enter the global configuration mode.

configure terminal

c   Create an SVI for the super VLAN and enter the SVI configuration mode.

interface vlan *vlan-id*

No SVI exists in a VLAN by default.

d   Configure an IP address and a subnet mask for the gateway of the super VLAN.

ip address *ip-address mask*

No IP address is configured for an SVI by default.

e   Return to the global configuration mode.

exit

(2) (Optional) Enable proxy ARP.

a   Enter the VLAN configuration mode of the super VLAN and sub VLAN.

vlan { *vlan-id* | **range** *vlan-range* }

b   Enable proxy ARP for the super VLAN and the sub VLAN.

proxy-arp

Proxy ARP is enabled for the super VLAN and the sub VLAN by default.

1.5   Configuring an IP Address Range for a Sub VLAN

1.5.1 Overview

The gateway IP address and subnet mask of a super VLAN jointly determine the subnet range. A super VLAN sends a broadcast packet to all sub VLANs in the super VLAN by default. To limit the broadcast range, you can configure an IP address range for each sub VLAN so that the super VLAN can send a broadcast packet to a specific sub VLAN based on an IP address range. The IP addresses of hosts must be within the IP address range of the local sub VLAN. Otherwise, the hosts cannot make L3 communication. Unless otherwise specified, you do not need to configure an IP address range for a sub VLAN.

1.5.2 Restrictions and Guidelines

●   The IP address range of a sub VLAN must be within the gateway IP address range of the super VLAN that the sub VLAN belongs to.

●   IP address ranges for different sub VLANs of a super VLAN cannot overlap.

●   IP addresses (both static and dynamic IP addresses) of hosts in a sub VLAN must be within the IP address range of the sub VLAN. Otherwise, hosts in the sub VLAN cannot make L3 communication.

●   The IP addresses assigned by the DHCP function may fall out of the IP address range you specify for a sub VLAN. If the IP addresses assigned by the DHCP function fall out of the specified IP address range, hosts in the sub VLAN cannot communicate with an external network. Therefore, you are not advised to configure an IP address range for a sub VLAN if DHCP is used to dynamically assign IP addresses to hosts.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

   enable

(2) Enter the global configuration mode.

   configure terminal

(3) Enter the sub VLAN configuration mode.

   vlan *vlan-id*

(4) Configure an IP address range for the sub VLAN.

   subvlan-address-range *start-ip-address end-ip-address*

   No IP address range is specified for a sub VLAN by default.

1.6 Configuring a Broadcast VLAN

1.6.1 Overview

A super VLAN sends a broadcast packet to all sub VLANs in the super VLAN by default. To limit the broadcast range, you can configure a sub VLAN as a broadcast VLAN so that broadcast packets of the super VLAN are sent in only this sub VLAN.

1.6.2 Restrictions and Guidelines

Only a sub VLAN of a super VLAN can be configured as a broadcast VLAN. Only one broadcast VLAN can be configured for a super VLAN. A later configured broadcast VLAN overwrites a previously configured broadcast VLAN.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

   enable

(2) Enter the global configuration mode.

   configure terminal

(3) Enter the super VLAN configuration mode.

   vlan { *vlan-id* | **range** *vlan-range* }

(4) Configure a broadcast VLAN.

   bcast vlan *sub-vlan-id*

   No broadcast VLAN exists by default. A super VLAN sends broadcast packets to all of its sub VLANs.

1.7 Monitoring

Run the **show** commands to check the running status of a configured function and 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.

You can 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 supervlan	Displays the super VLAN configuration.
debug bridge svlan	Debugs the super VLAN function.

1.8 Configuration Examples

1.8.1 Configuring Super VLAN

1.   Requirements

A super VLAN 2 is configured and the network segment 192.168.1.0/24 is assigned to the super VLAN. Sub VLANs 10, 20 and 30 are added to the super VLAN. Hosts in the sub VLANs are in the same network segment and share a gateway IP address 192.168.1.1/24 to save IP addresses. Hosts are assigned static IP addresses. IP address ranges are configured for the three sub VLANs:

● Sub VLAN 10: 192.168.1.10/24 to 192.168.1.50/24

● Sub VLAN 20: 192.168.1.60/24 to 192.168.1.100/24

● Sub VLAN 30: 192.168.1.110/24 to 192.168.1.150/24

2. Topology

Figure 1-1   Application of Super VLAN
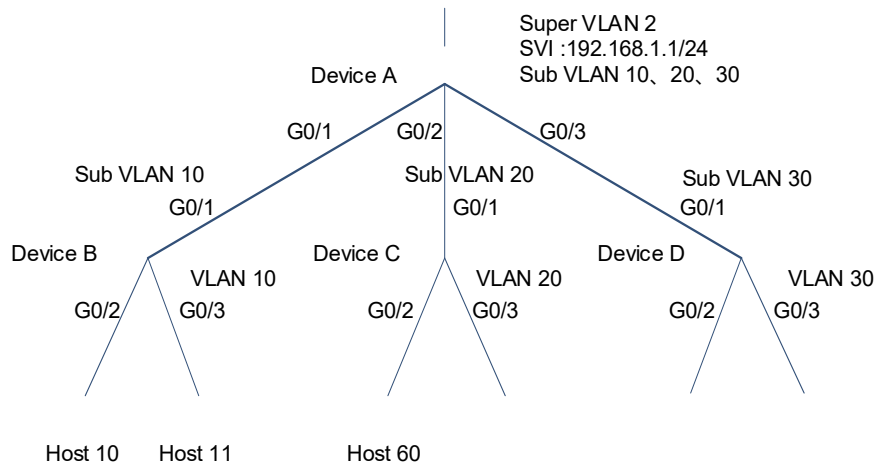
3. Notes

- Configure a super VLAN and sub VLANs on Device A (core device).
- Configure the common VLANs on Devices B, C, and D (access devices) that correspond to the sub VLANs on Device A.

4. Procedure

(1) Create a common VLAN to be configured as a sub VLAN.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20,30
DeviceA(config-vlan-range)# exit
```

(2) Create VLAN 2, configure VLAN 2 as a super VLAN, configure VLANs 10, 20 and 30 as sub VLANs of the super VLAN, and configure VLAN 10 as a broadcast VLAN of the super VLAN.

```
DeviceA(config)# vlan 2
DeviceA(config-vlan)# supervlan
DeviceA(config-vlan)# subvlan 10,20,30
DeviceA(config-vlan)# bcast vlan 10
DeviceA(config-vlan)# exit
```

(3) Configure a gateway for the super VLAN.

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-VLAN 2)# exit
```

(4) Configure IP address ranges for the sub VLANs.

```
DeviceA(config)# vlan 10
DeviceA(config-vlan)# subvlan-address-range 192.168.1.10 192.168.1.50
```

```
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 20
DeviceA(config-vlan)# subvlan-address-range 192.168.1.60 192.168.1.100
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 30
DeviceA(config-vlan)# subvlan-address-range 192.168.1.110 192.168.1.150
DeviceA(config-vlan)# exit
```

(5) Configure GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 as trunk ports, and add them to the sub VLANs.

```
DeviceA(config)# interface range gigabitethernet 0/1,0/2,0/3
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# end
DeviceA# write
```

5. Verification

(1) Check the super VLAN configuration.

```
DeviceA(config)# show supervlan
supervlan id  supervlan arp-proxy  bcast vlan  subvlan id  subvlan arp-proxy
subvlan ip range
-----------  -------------------  ----------  ----------  -----------------
----------------
2            ON                   10          10          ON    192.168.1.10
- 192.168.1.50
                                              20          ON    192.168.1.60
- 192.168.1.100
                                              30          ON    192.168.1.110
- 192.168.1.150
```

(2) Check ports that are added to VLANs.

```
DeviceA(config)# show vlan
VLAN      Name                              Status    Ports
----------  --------------------------------  ---------
----------------------------------
        2 VLAN0002                           SUPER
       10 VLAN0010                           SUB       Gi0/1, Gi0/2, Gi0/3
       20 VLAN0020                           SUB       Gi0/1, Gi0/2, Gi0/3
       30 VLAN0030                           SUB       Gi0/1, Gi0/3, Gi0/3
```

(3) Verify that hosts in a sub VLAN can make L2 communication with each other.

On host 10 in sub VLAN 10, set the default gateway address to the gateway IP address of the super VLAN 192.168.1.1 and the IP address in the IP address range of the sub VLAN (that is, 192.168.1.10 to 192.168.1.50).

```
Host10> enable
Host10# configure terminal
Host10(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.1
```

```
Host10(config)# interface gigabitethernet 0/1
Host10(config-if-GigabitEthernet 0/1)# no switchport
Host10(config-if-GigabitEthernet 0/1)# ip address 192.168.1.10 255.255.255.0
```

On host 11 in sub VLAN 10, set the default gateway address to the gateway IP address of the super VLAN 192.168.1.1 and the IP address in the IP address range of the sub VLAN (that is, 192.168.1.10 to 192.168.1.50).

```
Host11> enable
Host11# configure terminal
Host11(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.1
Host11(config)#interface gigabitethernet 0/1
Host11(config-if-GigabitEthernet 0/1)# no switchport
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.1.11 255.255.255.0
```

Verify that host 10 can ping host 11 no matter whether the gateway IP address of the super VLAN is configured on Device A.

```
Host10# ping 192.168.1.11
Sending 5, 100-byte ICMP Echoes to 192.168.1.11, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms.
```

Set the IP address of host 11 to 192.168.1.51/24, which falls out of the IP address range of the sub VLAN, and verify that the communication of host 11 in the sub VLAN is not affected.

```
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.1.51 255.255.255.0
Host10# ping 192.168.1.51
Sending 5, 100-byte ICMP Echoes to 192.168.1.51, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/21/97 ms.
```

(4) Verify that hosts in different sub VLANs can make L3 communication but are isolated at L2.

On host 60 in sub VLAN 20, set the default gateway address to the gateway IP address of the super VLAN 192.168.1.1 and the IP address in the IP address range of the sub VLAN (that is, 192.168.1.60 to 192.168.1.100).

```
Host60> enable
Host60# configure terminal
Host60(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.1
Host60(config)# interface gigabitethernet 0/1
Host60(config-if-GigabitEthernet 0/1)# no switchport
Host60(config-if-GigabitEthernet 0/1)# ip address 192.168.1.60 255.255.255.0
```

Configure an SVI and a gateway IP address for super VLAN 2, and verify that host 60 (192.168.1.60/24) can ping host 10 (192.168.1.10/24) and that host 60 cannot ping host 11 (192.168.1.51/24) because host 11 falls out of the IP address range of the sub VLAN.

```
Host60# ping 192.168.1.10
Sending 5, 100-byte ICMP Echoes to 192.168.1.10, timeout is 2 seconds:
  < press Ctrl+C to break >
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/19/95 ms.
Host60# ping 192.168.1.51
Sending 5, 100-byte ICMP Echoes to 192.168.1.51, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

Delete the gateway IP address of super VLAN 2, and verify that host 60 (192.168.1.60/24) cannot ping host 10 (192.168.1.10/24).

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# no ip address
%notice: all IPv4 addresses on this interface are removed.
Host60# ping 192.168.1.10
Sending 5, 100-byte ICMP Echoes to 192.168.1.10, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

6.   Configuration Files

- Device A configuration file

```
vlan 2
 supervlan
 subvlan 10,20,30
 bcast vlan 10
!
vlan 10
 subvlan-address-range 192.168.1.10 192.168.1.50
!
vlan 20
 subvlan-address-range 192.168.1.60 192.168.1.100
!
vlan 30
 subvlan-address-range 192.168.1.110 192.168.1.150
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.1.1 255.255.255.0
```

- Device B configuration file

```
vlan range 1,10
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
!
interface GigabitEthernet 0/3
 switchport access vlan 10
```

- Device C configuration file

```
vlan range 1,20
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 20
!
interface GigabitEthernet 0/3
 switchport access vlan 20
```

- Device D configuration file

```
vlan range 1,30
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 30
!
interface GigabitEthernet 0/3
 switchport access vlan 30
```

7. Common Errors

- An SVI is configured for a common VLAN before the VLAN is configured as a sub VLAN. As a result, the common VLAN cannot be configured as a sub VLAN of a super VLAN.
- No SVI and gateway IP address are configured for a super VLAN. Consequently, communication between sub VLANs and between sub VLANs and other VLANs fails.
- Proxy ARP is disabled on the super VLAN or sub VLANs. Consequently, communication between the sub VLANs fails.
- An IP address range is configured for a sub VLAN. However, the static or dynamic IP addresses allocated to hosts in the sub VLAN are not in this range. Consequently, the hosts cannot make L3 communication.