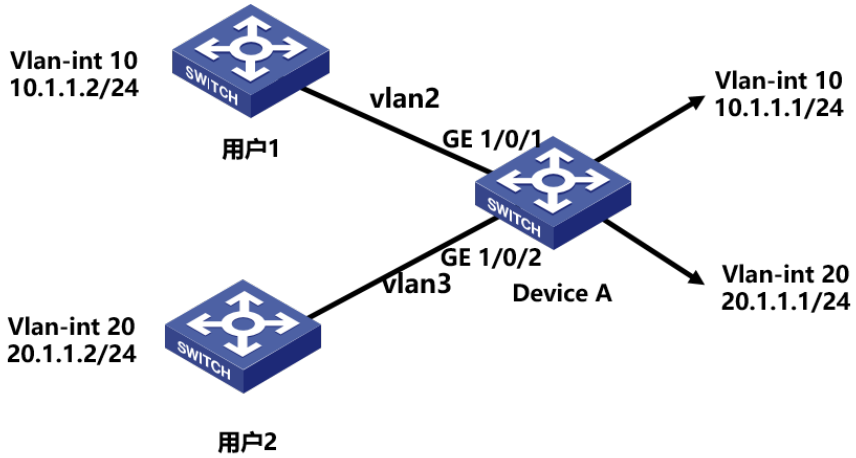
同一设备下多个supervlan用户互访限制典型配置

Super Vlan 曾招维 2022-08-04 发表

组网及说明

Device A连接不同VLAN用户，其中，端口GigabitEthernet1/0/1属于VLAN 2，端口GigabitEthernet1/0/2属于VLAN 3。 为实现Device A连接的各VLAN用户（均在10.1.1.0/24网段）之间能够满足二层隔离和三层互通的同时，节省IP资源，创建Super VLAN，其关联的Sub VLAN公用Super VLAN interface的IP地址10.1.1.1/24和20.1.1.1/24作为三层通信的网关地址。

同时限制vlan 10和vlan 20的supervlan间用户不能互访，及用户1和用户2禁止互访。



配置步骤

1、用户1和用户2配置vlan，vlan-int地址，配置静态路由。
2、supervlan基本配置。
创建VLAN 10，配置VLAN接口的IP地址为10.1.1.1/24。
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
创建VLAN 20，配置VLAN接口的IP地址为20.1.1.1/24。
<DeviceA> system-view
[DeviceA] vlan 20
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface10] ip address 20.1.1.1 255.255.255.0
开启设备的本地代理ARP功能。
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
[DeviceA-Vlan-interface20] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
创建VLAN 2，并向VLAN 2中添加端口GigabitEthernet1/0/1
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
创建VLAN 3，并向VLAN 3中添加端口GigabitEthernet1/0/2
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
配置VLAN 10为Super VLAN，其关联的Sub VLAN为VLAN 2
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] subvlan 2
[DeviceA-vlan10] quit
[DeviceA] quit
配置VLAN 20为Super VLAN，其关联的Sub VLAN为VLAN 3
[DeviceA] vlan 20
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] subvlan 3
[DeviceA-vlan10] quit
[DeviceA] quit
3、用户1和用户2禁止互访配置,比如限制互ping：
#
traffic classifier cl operator and
 if-match acl 3001
#
traffic behavior b1
 filter deny
#
qos policy q1
 classifier cl behavior b1
#
#
acl advanced 3001
 rule 5 permit icmp source 10.1.1.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
 rule 10 permit icmp source 20.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
或者将上述QOS策略在接口下调用
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge

```
 port access vlan 2
 qos apply policy q1 inbound
 qos apply policy q1 outbound
#
```

配置关键点

请注意在流量进入角是带sub VLAN的tag的，在super vlan的三层口上调用包过滤或者QOS策略均不生效。

再次强调，Sub VLAN不支持创建VLAN接口，interface Vlan-interface1.0/1也不能在sub vlan的三层口调用。

```
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 packet-filter 3000 inbound
 packet-filter 3000 outbound
#
#
acl advanced 3000
 rule 5 deny icmp source 10.1.1.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
 rule 10 deny icmp source 20.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
```