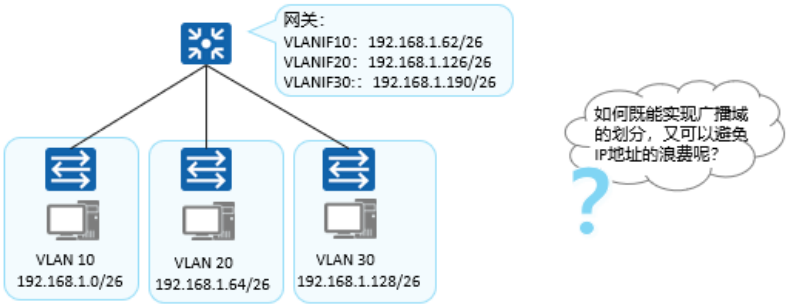
VLAN 高级技术

- VLAN 技术在园区网络中应用非常广泛，通常利用 VLAN 进行广播域的隔离，每个 VLAN 属于一个广播域。网络规划时需要为每个广播域分配一个网关，如果 VLAN 数量过多，会导致 IP 地址规划难度加大，甚至会出现大量 IP 地址的浪费。
- 另外，在大型企业中，不仅仅有企业内部员工，还有很多合作伙伴同时在企业园区办公。对于不同合作伙伴来说，他们之间是不能直接访问的，需要给每个合作伙伴分配一个 VLAN 进行隔离，这样又会给网络带来管理维护上的难度。面临以上这些情况，是否有更好的技术能够解决这个问题呢？
- 本课程主要介绍几种 VLAN 的高级技术，包括 VLAN 聚合、MUX VLAN、QinQ，进一步加深对 VLAN 高级技术的理解与应用。

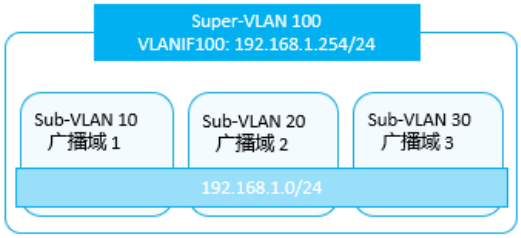
VLAN聚合产生的技术背景

- 在一般的三层交换机中，通常是采用一个VLAN对应一个VLANIF接口的方式实现广播域之间的互通，这在某些情况下导致了IP地址的浪费。
- 因为一个VLAN对应的子网中，子网号、子网广播地址、子网网关地址不能用作VLAN内的主机IP地址，且子网中实际接入的主机可能少于可用IP地址数量，空闲的IP地址也会因不能再被其他VLAN使用而被浪费掉。

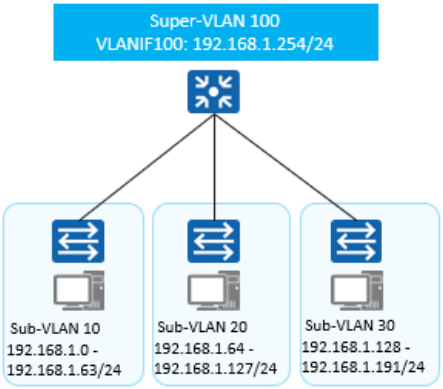


VLAN聚合概述

- **VLAN聚合**（VLAN Aggregation，也称Super-VLAN）：指在一个物理网络内，用多个VLAN（称为Sub-VLAN）隔离广播域，并将这些Sub-VLAN聚合成一个逻辑的VLAN（称为Super-VLAN），这些Sub-VLAN使用同一个IP子网和缺省网关，进而达到节约IP地址资源的目的。
- **Sub-VLAN**：只包含物理接口，不能建立三层VLANIF接口，用于隔离广播域。每个Sub-VLAN内的主机与外部的三层通信是靠Super-VLAN的三层VLANIF接口来实现的。
- **Super-VLAN**：只建立三层VLANIF接口，不包含物理接口，与子网网关对应。与普通VLAN不同，Super-VLAN的VLANIF接口状态取决于所包含Sub-VLAN的物理接口状态。



VLAN聚合的原理



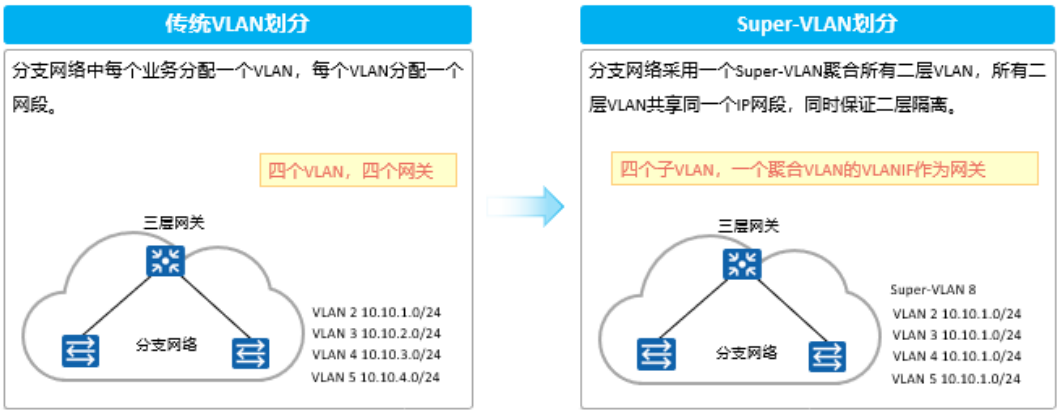
每个Sub-VLAN对应一个广播域，多个Sub-VLAN和一个Super-VLAN关联，只给Super-VLAN分配一个IP子网，所有Sub-VLAN都使用Super-VLAN的IP子网和缺省网关进行三层通信。

所有主机的默认网关都是192.168.1.254/24

- 多个 Sub-VLAN 共享一个网关地址，节约了子网网络地址、子网定向广播地址、子网缺省网关地址，且各 Sub-VLAN 间的界线也不再是从前的子网界线了，可以根据每个 Sub-VLAN 内所需的 IP 地址数量进行灵活的地址规划，从而既保证了各个 Sub-VLAN 作为一个独立广播域实现广播隔离，又节省了 IP 地址资源，提高了编址的灵活性。

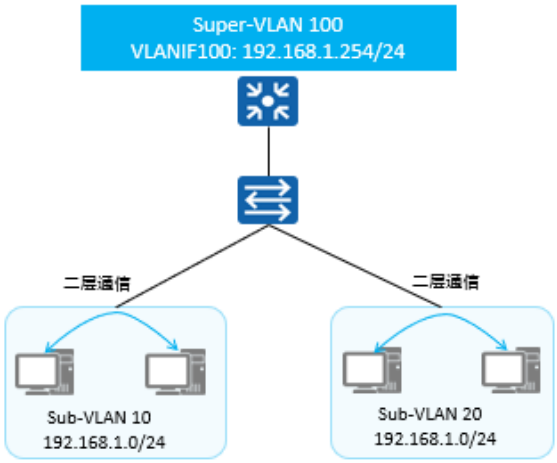
VLAN聚合的应用

传统VLAN方式每一个VLAN需要划分不同的IP地址网段，在本例中需要耗费4个IP网段和产生4条路由条目；Super-VLAN方式只需要分配一个IP地址网段，下属二层VLAN共用同一个IP地址网段，共用同一个三层网关，同时VLAN之间保持二层隔离。

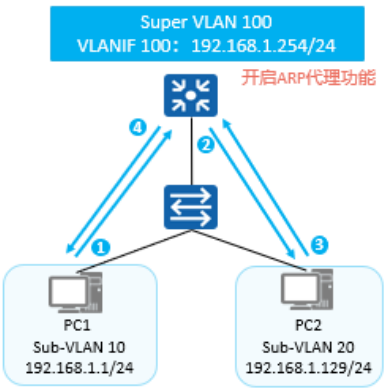


相同Sub-VLAN内部通信

同一个Sub-VLAN之间属于同一个广播域，因此相同Sub-VLAN之间可以通过二层直接通信。



不同Sub-VLAN之间通信举例

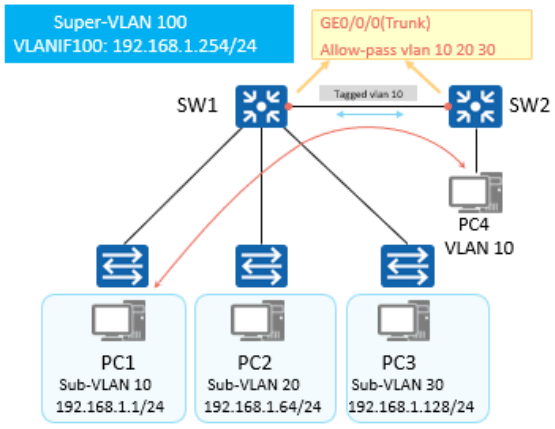


Super-VLAN VLANIF100开启ARP代理之后PC1和PC2之间通信过程如下：

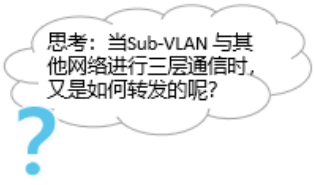
1. PC1发现PC2与自己在同一网段，且自己ARP表无PC2对应表项，则直接发送ARP广播请求PC2的MAC地址。
2. 作为网关的Super-VLAN对应的VLANIF 100收到PC1的ARP请求，由于网关上使能Sub-VLAN间的ARP代理功能，则向Super-VLAN 100的所有Sub-VLAN接口发送一个ARP广播，请求PC2的MAC地址。
3. PC2收到网关发送的ARP广播后，对此请求进行ARP应答。
4. 网关收到PC2的应答后，就把自己的MAC地址回应给PC1，PC1之后要发给PC2的报文都先发送给网关，由网关做三层转发。

- 不同 Sub-VLAN 之间进行通信，IP 地址属于相同网段，因此主机会发送 ARP 请求，但是实际不同 Sub-VLAN 之间属于不同的广播域，因而 ARP 报文无法传递到其他 Sub-VLAN，ARP 请求得不到响应，设备无法学习到对端 MAC 地址，从而无法完成 Sub-VLAN 之间通信。
- 要实现 Sub-VLAN 之间的通信，需要在 Super-VLAN 的 VLANIF 中开启 ARP 代理功能。

Sub-VLAN与其他设备的二层通信



- 当Sub-VLAN与其他设备进行二层通信时，与普通的VLAN内二层通信无区别。
- 由于Super-VLAN不属于任何物理接口，即不会处理任何携带Super-VLAN标签的报文。



- Sub-VLAN 二层通信过程举例：
- 从 PC1 进入 SW1 的报文会被打上 VLAN10 的 Tag。在

SW1 中这个 Tag 不会因为 VLAN10 是 VLAN100 的 Sub-VLAN 而变为 VLAN100 的 Tag。

- 当报文从 SW1 的 GE0/0/0 出去时，依然携带 VLAN10 的 Tag。也就是说，SW1 本身不会发出 VLAN100 的报文。就算其他设备有 VLAN100 的报文发送到该设备上，这些报文也会因为 SW1 上没有 VLAN100 应的物理接口而被丢弃。
- 对于其他设备而言，有效的 VLAN 只有 Sub-VLAN10，20 和 30， 所有的报文都是在这些 VLAN 中交互的。因此，SW1 上虽然配置了 VLAN 聚合，但与其他设备的二层通信，不会涉及到 Super-VLAN，与正常的二层通信流程一样。
- 当 Sub-VLAN 内的 PC 需要与其他网络进行三层通信时，首先将数据发往默认网关，即 Super-VLAN 对应的 VLANIF，再进行路由。

VLAN聚合关键配置命令

1. 创建Super-VLAN

```
[Huawei-vlan100] aggregate-vlan
```

Super-VLAN中不能包含任何物理接口，VLAN1不能配置为Super-VLAN。
Super-VLAN中的VLAN ID与Sub-VLAN中的VLAN ID 必须使用不同的 VLAN ID。

2. 将Sub-VLAN加入Super-VLAN

```
[Huawei-vlan100] access-vlan { vlan-id1 [ to vlan-id2 ] }
```

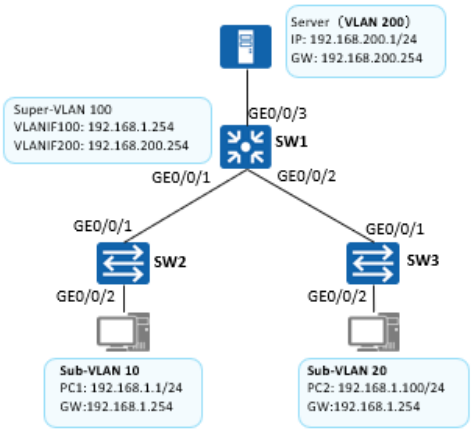
将Sub-VLAN加入到Super-VLAN中时，必须保证Sub-VLAN没有创建对应的VLANIF接口。

3. （可选）使能Super-VLAN对应的VLANIF接口的Proxy ARP

```
[Huawei-vlanif100] arp-proxy inter-sub-vlan-proxy enable
```

使能Sub-VLAN间的Proxy ARP功能。

VLAN聚合配置举例 (1)

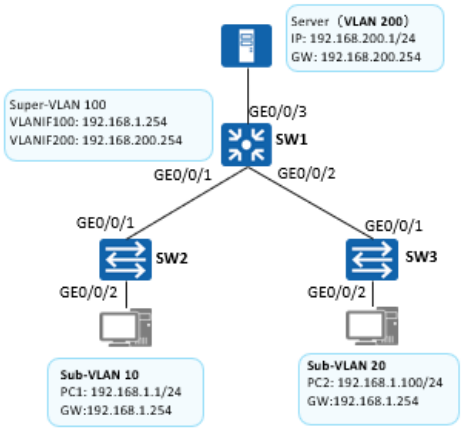


- 要求：如上图所示完成SW1上VLAN聚合的配置

SW1的配置如下：

```
[SW1] vlan batch 10 20          #创建Sub-VLAN
[SW1] interface GigabitEthernet0/0/1
[SW1-GigabitEthernet0/0/1] port link-type trunk
[SW1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SW1] interface GigabitEthernet0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[SW1] vlan 100                  #创建Super-VLAN
[SW1-vlan100] aggregate-vlan
[SW1-vlan100] access-vlan 10 20  #将VLAN10,20作为VLAN100的Sub-VLAN
[SW1] interface vlanif 100
[SW1-vlanif100] ip address 192.168.1.254 24
[SW1-vlanif100] arp-proxy inter-sub-vlan-proxy enable
#使能Sub-VLAN间的Proxy ARP功能
```

VLAN聚合配置举例 (2)



要求：如上图所示完成SW1上VLAN聚合的配置

SW1的配置如下：

```
[SW1] vlan 200
[SW1] interface GigabitEthernet0/0/3
[SW1-GigabitEthernet0/0/3] port link-type access
[SW1-GigabitEthernet0/0/3] port default vlan 200
[SW1] interface vlanif 200
[SW1-VLANIF200] ip address 192.168.200.254 24
```

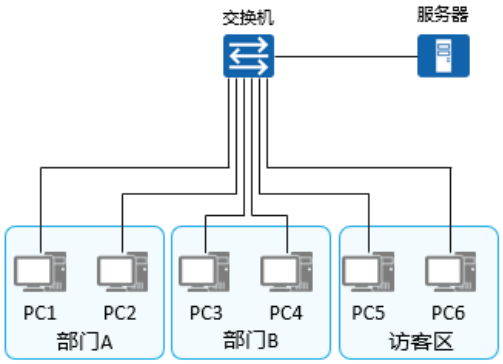
SW2的配置如下：

```
[SW2] vlan 10
[SW2] interface GigabitEthernet0/0/2
[SW2-GigabitEthernet0/0/2] port link-type access
[SW2-GigabitEthernet0/0/2] port default vlan 10
[SW2] interface GigabitEthernet0/0/1
[SW2-GigabitEthernet0/0/1] port link-type trunk
[SW2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
```

SW3的配置与SW2类似，此处省略

MUX VLAN产生背景

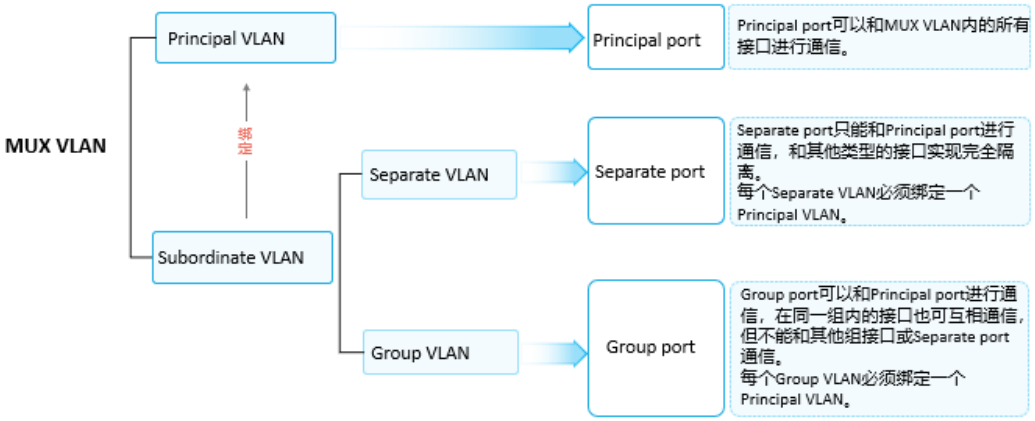
在企业网络中，各个部门之间网络需要相互独立，通常用VLAN技术可以实现这一要求。如果企业规模很大，且拥有大量的合作伙伴，要求各个合作伙伴能够访问公司服务器，但是不能相互访问，这时如果使用传统的VLAN技术，不但需要耗费大量的VLAN ID，还增加了网络管理者的工作量同时也增加了维护量。



MUX VLAN（Multiplex VLAN）提供了一种通过VLAN进行网络资源控制的机制。

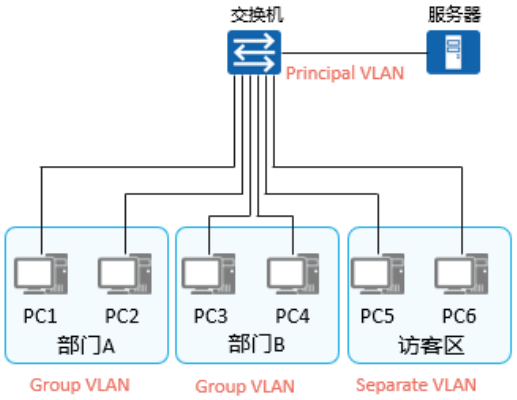
MUX VLAN的基本概念

MUX VLAN分为Principal VLAN（主VLAN）和Subordinate VLAN（从VLAN），Subordinate VLAN又分为Separate VLAN（隔离型从VLAN）和Group VLAN（互通型从VLAN）。



- 在使用 MUX VLAN 的过程中，无论是 Separate VLAN 还是 Group VLAN 都必须与一个 Principle VLAN 绑定。
- 加入 Principal VLAN（主 VLAN）中的接口，可以与 MUX VLAN 内的所有接口进行通信。

MUX VLAN的应用



在交换机上，通过把部门A和部门B所在的VLAN分别设置为互通型从VLAN，把访客区所属的VLAN设置为隔离型从VLAN，把服务器所连接口所属VLAN设置为Principal VLAN，即主VLAN。并且所有从VLAN都与主VLAN绑定。从而实现如下网络设计要求：

- 部门A内的用户之间能够实现二层互通。
- 部门B内的用户之间能够实现二层互通。
- 部门A与部门B的用户之间二层隔离。
- 部门A和部门B的员工都能够通过二层访问服务器。
- 访客区内的任意PC除了能访问服务器之外，不能访问其他任意设备，包括其他访客。

MUX VLAN配置命令

1. 配置MUX VLAN中的Principal VLAN

   [Huawei-vlan100] **mux-vlan**

   配置该VLAN为MUX VLAN，即Principal VLAN。如果指定VLAN已经用于Principal VLAN，那么该VLAN不能在Super-VLAN、Sub-VLAN的配置中使用。

2. 配置Subordinate VLAN中的Group VLAN

   [Huawei-vlan100] **subordinate group** { *vlan-id1* [**to** *vlan-id2*] }

   一个Principal VLAN下最多配置128个Group VLAN。

3. 配置Subordinate VLAN中的Separate VLAN

   [Huawei-vlan100] **subordinate separate** *vlan-id*

   一个Principal VLAN下只能配置一个Separate VLAN，同一MUX VLAN中Group VLAN和Separate VLAN的VLAN ID不能相同。

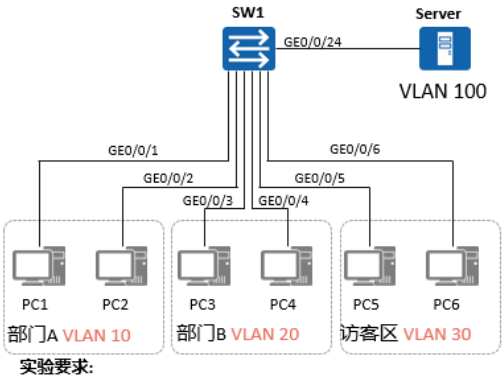
4. 使能接口MUX VLAN功能

   [Huawei-GigabitEthernet0/0/1] **port mux-vlan enable** *vlan-id*

   使能接口的MUX VLAN功能，协商类型negotiation-auto和negotiation-desirable接口不支持配置port mux-vlan enable。

- 只有使能接口 MUX VLAN 功能后，才能实现 Principal VLAN 与 Subordinate VLAN 之间通信、Group VLAN 内的接口可以相互通信及 Separate VLAN 接口间不能相互通信的目的。

MUX VLAN配置举例



- **实验要求:**
  - Server能与所有主机二层互通
  - 部门A、部门B、访客区相互间二层不互通
  - 部门A与部门B内部二层互通
  - 访客区内部二层不互通

SW1配置如下:

```
[SW1] vlan batch 10 20 30 100          #创建所有VLAN
[SW1] vlan 100
[SW1-vlan100] mux-vlan
#指定VLAN100为主VLAN
[SW1-vlan100] subordinate group 10 20
#指定VLAN10， 20为互通型从VLAN
[SW1-vlan100] subordinate separate 30
#指定VLAN30为隔离型从VLAN
[SW1] interface GigabitEthernet0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
[SW1-GigabitEthernet0/0/1] port mux-vlan enable vlan 10
#接口加入相关VLAN，并且激活MUX VLAN功能
#其他接口与GE0/0/1配置类似，此处省略
```

MUX VLAN配置验证

查看VLAN配置结果，通过ping命令检测PC5（192.168.1.5/24）与PC6（192.168.1.6/24）之间的网络连通性。

```
[SW1]display vlan
The total number of vlans is : 5
--------------------------------------------------------------------------------
U: Up;        D: Down;        TG: Tagged;        UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------------------------
10   mux-sub UT:GE0/0/1(U)     GE0/0/2(U)
20   mux-sub UT:GE0/0/3(U)     GE0/0/4(U)
30   mux-sub UT:GE0/0/5(U)     GE0/0/6(U)
100  mux     UT:GE0/0/24(U)
```

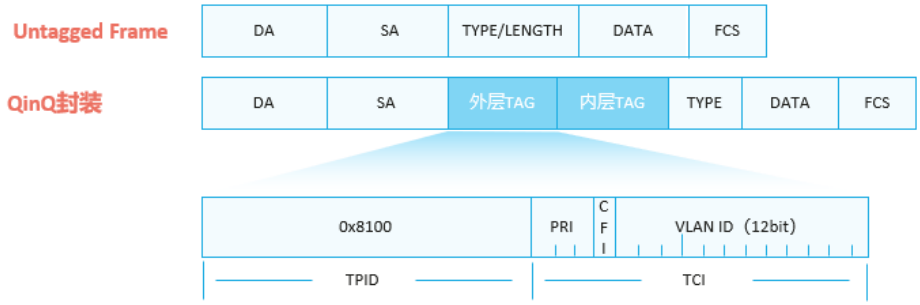
```
PC5>ping 192.168.1.6

Ping 192.168.1.6: 32 data bytes, Press Ctrl_C to break
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable

--- 192.168.1.6 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

QinQ概述

- 随着以太网技术在网络中的大量部署，利用VLAN对用户进行隔离和标识受到很大限制。因为IEEE802.1Q中定义的VLAN Tag域只有12个比特，仅能表示4096个VLAN，无法满足城域以太网中标识大量用户的需求，于是QinQ技术应运而生。
- QinQ（802.1Q in 802.1Q）技术是一项扩展VLAN空间的技术，通过在802.1Q标签报文的基础上再增加一层802.1Q的Tag来达到扩展VLAN空间的功能。
- 如下图所示用户报文在公网上传递时携带了两层Tag，内层是私网Tag，外层是公网Tag。

QinQ封装结构

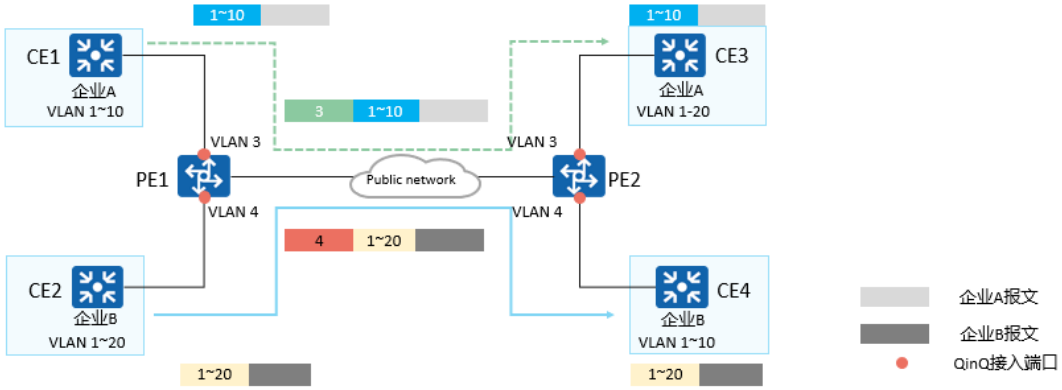
QinQ封装报文是在无标签的以太网数据帧的源MAC地址字段后面加上两个VLAN标签构成。



- TPID（Tag Protocol Identifier，标签协议标识）表示帧类型。取值为 0x8100 时表示 802.1Q Tag 帧。如果不支持 802.1Q 的设备收到这样的帧，会将其丢弃。
- 对于内层的 802.1Q Tag，该值设置为 0x8100；对于外层的 802.1Q Tag，不同厂商所使用的值可能不相同：
- 0x8100：Huawei 路由器使用
- 0x88A8：802.1ad 规定外层 802.1Q Tag 中的 TPID 为 0x88a8
- 在华为设备上，外层 802.1Q Tag 缺省情况下值为 0x8100，可以通过命令行调整该值。

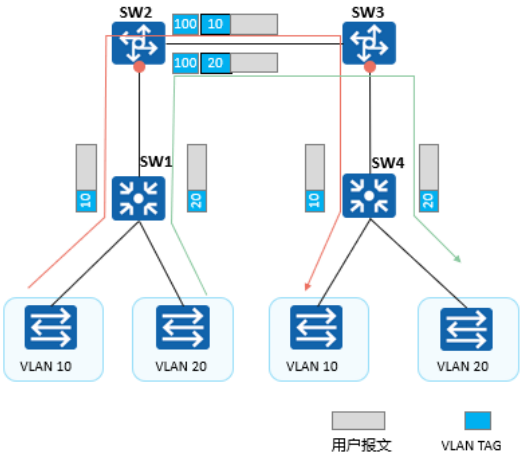
QinQ工作原理

在公网的传输过程中，设备只根据外层VLAN Tag转发报文，并根据报文的外层VLAN Tag进行MAC地址学习，而用户的私网VLAN Tag将被当作报文的数据部分进行传输。即使私网VLAN Tag相同，也能通过公网VLAN Tag区分不同用户。



- 企业 A 和企业 B 的私网 VLAN 分别为 VLAN 1～10 和 VLAN 1～20。公网为企业 A 和企业 B 分配的公网 VLAN 分别为 VLAN 3 和 VLAN 4。当企业 A 和企业 B 中带 VLAN Tag 的报文进入公网时，报文外面就会被分别封装上 VLAN 3 和 VLAN 4 的 VLAN 标签。这样，来自不同企业网络的报文在公网中传输时被完全分开，即使这些企业网络各自的 VLAN 范围存在重叠，在公网中传输时也不会产生冲突。当报文穿过公网，到达公网另一侧 PE 设备后，报文会被剥离公网为其添加的公网 VLAN 标签，然后再传送给用户网络的 CE 设备。

QinQ实现方式 - 基本QinQ

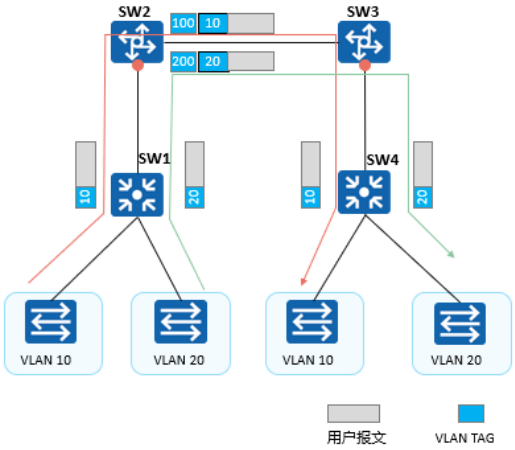


基本QinQ的报文处理过程:

1. SW1收到VLAN ID为10和20的报文，将该报文发给SW2。
2. SW2收到该报文后，在该报文原有Tag的外侧再添加一层VLAN ID 为100的外层Tag。
3. 带着两层Tag的用户数据报文在网络中按照正常的二层转发流程转发。
4. SW3收到VLAN100的报文后，剥离报文的外层Tag（VLAN ID为100）。将报文发送给SW4，此时报文只有一层Tag（VLAN ID 为10或20）。
5. SW4收到该报文，根据VLAN ID和目的MAC地址进行相应的转发。

- 基本 QinQ 是基于端口方式实现的。开启端口的基本 QinQ 功能后，当该端口接收到报文，设备会为该报文打上本端口缺省 VLAN 的 VLAN Tag。如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是不带 VLAN Tag 的报文，该报文就成为带有端口缺省 VLAN Tag 的报文。
- 基于端口的 QinQ 的缺点是外层 VLAN Tag 封装方式固定，不能根据业务种类选择外层 VLAN Tag 封装的方式，从而很难有效支持多业务的灵活运营。

QinQ实现方式 - 灵活QinQ

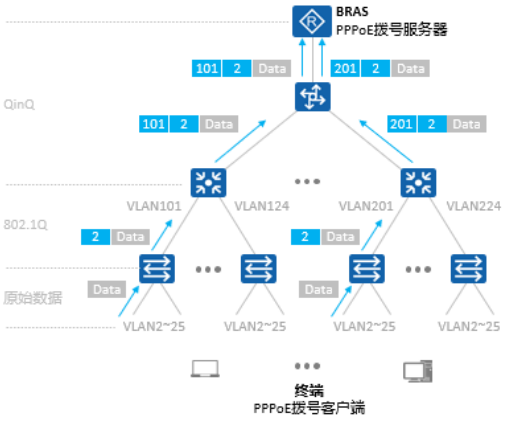


灵活QinQ的报文处理过程：

1. SW1收到VLAN ID为10和20的报文，将该报文转发给SW2。
2. SW2收到VLAN ID为10的报文后，添加一层VLAN ID 为100 的外层Tag；SW2收到VLAN ID为20的报文后，添加一层VLAN ID为200的外层Tag。
3. 带着两层Tag的用户数据报文在网络中按照正常的二层转发流程转发。
4. SW3收到报文后，剥离报文的外层Tag（VLAN ID 为100或200）。将报文发送给SW4，此时报文只有一层Tag（VLAN ID为10或20）。
5. SW4收到报文，根据VLAN ID和目的MAC地址进行相应的转发。

- 灵活 QinQ（Selective QinQ）可根据流分类的结果选择是否打外层 VLAN Tag，打上何种外层 VLAN Tag。灵活 QinQ 可根据用户的 VLAN 标签、优先级、MAC 地址、IP 协议、IP 源地址、IP 目的地址、或应用程序的端口号进行流分类。
- 基于 VLAN ID 的灵活 QinQ：为具有不同内层 VLAN ID 的报文添加不同的外层 VLAN Tag。
- 基于 802.1p 优先级的灵活 QinQ：根据报文的原有内层 VLAN 的 802.1p 优先级添加不同的外层 VLAN Tag。
- 基于流策略的灵活 QinQ：根据 QoS 策略添加不同的外层 VLAN Tag。基于流策略的灵活 QinQ 能够针对业务类型提供差别服务。
- 灵活 QinQ 功能是对基本 QinQ 功能的扩展，它比基本 QinQ 的功能更灵活。二者之间的主要区别是：
- 基本 QinQ：对进入二层 QinQ 接口的所有帧都加上相同的外层 Tag。
- 灵活 QinQ：对进入二层 QinQ 接口的帧，可以根据不同的内层 Tag 而加上不同的外层 Tag，对于用户 VLAN 的划分更加细致

QinQ在园区网络中的应用



场景需求

1. 单个终端用户可溯源。
2. 每个终端一个独立的二层广播域，最大限度地限制BUM流量对网络造成的影响。
3. 终端用户到BRAS设备之间二层互通，匹配PPPoE等认证需求。

解决方案

1. 接入交换机为每个下行端口划分一个独立的VLAN。
2. 接入交换机将用户的原始数据转发给汇聚交换机时打上一层802.1Q标记。
3. 汇聚交换机部署QinQ，为每个下行接口分配一个独立的VLAN（每台接入交换机都对应一个唯一的VLAN），将数据打上第二层标记，然后将流量送往核心交换机。
4. 核心交换机将流量透传给BRAS设备，由其执行QinQ解封装。

- BRAS：Broadband Remote Access Server，宽带远程接入服务器。BRAS 提供宽带接入服务、实现多种业务的汇聚与转发，能满足不同用户对传输容量和带宽利用率的要求，因此 RRAS 是宽带用户接入的核心设备。
- BUM：Broadcast、Unknown unicast、Multicast，广播，未知单播、组播。交换机以泛洪的方式处理以上类型的数据帧。

QinQ配置命令介绍

1. 配置接口类型为dot1q-tunnel

```
[Huawei-GigabitEthernet0/0/1] port link-type dot1q-tunnel
```

配置接口类型为dot1q-tunnel，该接口可以是物理接口，也可以是Eth-Trunk接口。

2. 使能接口VLAN转换功能

```
[Huawei-GigabitEthernet0/0/1] qinq vlan-translation enable
```

3. 配置配置灵活QinQ

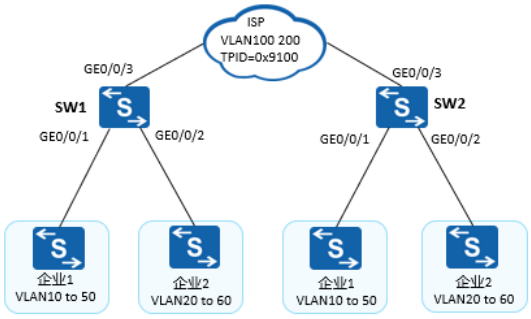
```
[Huawei-GigabitEthernet0/0/1] port vlan-stacking vlan vlan-id1 [ to vlan-id2 ] stack-vlan vlan-id3 [ remark-8021p 8021p-value ]
```

配置不同的内层VLAN叠加不同的外层VLAN，缺省情况下，外层VLAN优先级与内层VLAN优先级保持一致。

- 配置灵活 QinQ 的当前接口类型建议为 Hybrid，并且必须先通过命令 qinq vlan-translation enable 先使能 VLAN 转换功能。灵活 QinQ 功能只在当前接口的入方向生效。
- 接口配置 VLAN Stacking 功能后在发送帧时，若需要剥掉外层 Tag，该接口要以 Untagged 方式加入叠加后的 stack-

vlan；若不需要剥掉外层 Tag，该接口要以 Tagged 方式加入叠加后的 stack-vlan。

QinQ配置举例 - 基本QinQ



实验要求：

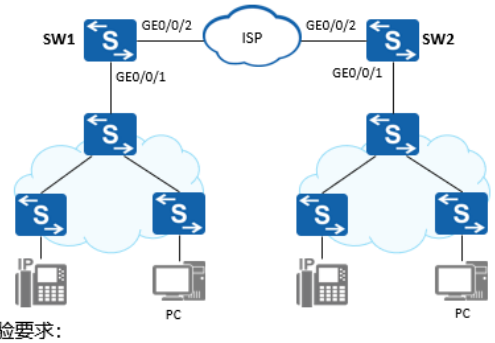
- 企业1与企业2接入同一个ISP网络，并使用了重叠的VLAN空间。
- ISP通过QinQ技术，实现同一个企业的不同站点之间的数据交互。
- 为企业1规划的VLAN ID为100，为企业2规划的VLAN ID为200。

SW1配置如下：

```
[SW1] vlan batch 100 200
[SW1] interface GigabitEthernet 0/0/1
#配置GE0/0/1外层TAG为100
[SW1-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[SW1 -GigabitEthernet0/0/1] port default vlan 100
[SW1] interface GigabitEthernet 0/0/2
#配置GE0/0/2外层TAG为200
[SW1-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[SW1-GigabitEthernet0/0/2] port default vlan 200
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200
#配置外层VLAN tag的TPID值
[SW1-GigabitEthernet0/0/3] qinq protocol 9100
```

SW2配置与SW1类似，此处省略

QinQ配置举例 - 灵活QinQ



实验要求：

- 上网用户和VoIP用户通过SW1和SW2接入ISP网络，通过ISP的网络互相通信；企业为PC分配的内部VLAN为100，为VoIP电话分配的内部VLAN为300。
- 上网用户和VoIP用户分别以VLAN2和VLAN3通过ISP网络。

SW1配置如下：

```
[SW1] vlan batch 2 3
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid untagged vlan 2 3
[SW1-GigabitEthernet0/0/1] qinq vlan-translation enable
[SW1-GigabitEthernet0/0/1] port vlan-stacking vlan 100 stack-vlan 2
[SW1-GigabitEthernet0/0/1] port vlan-stacking vlan 300 stack-vlan 3
[SW1-GigabitEthernet0/0/1] quit
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 3
[SW1-GigabitEthernet0/0/2] quit
```

SW2配置与SW1类似，此处省略

思考题：

- （单选题）当 Sub-VLAN 与外部进行二层通信时，在出接口打上的 VLAN 标记为？
- Sub-VLAN
- Secondary VLAN
- Super-VLAN
- Isolate VLAN

- （单选题）下面关于 QinQ 描述错误的是？
- QinQ 报文在公网中报文根据外层 VLAN Tag 转发。
- QinQ 报文在公网中报文根据内层 VLAN Tag 转发。
- QinQ 为用户提供了一种更为简单的二层 VPN 隧道。
- QinQ 不需要信令协议的支持，可以通过纯静态配置实现。

参考答案：

- A
- B
-