HCIP-Datacom 分解实验 - VLAN

臧家林制作

VLAN 实验 1： VLAN 聚合
VLAN 实验 2： Mux　VLAN
VLAN 实验 3： qinq

= = = = = = = =

VLAN 实验 2： VLAN 聚合

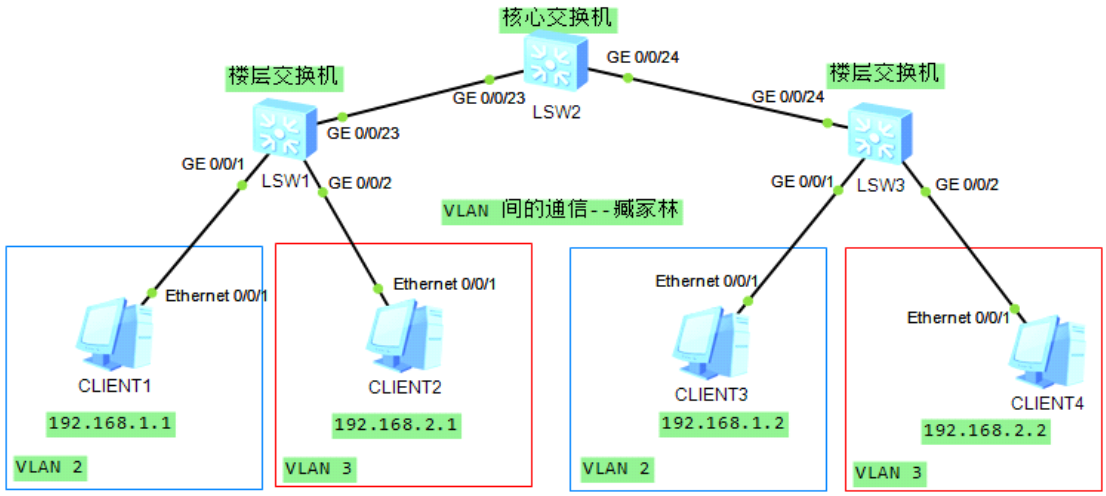
通常情况下，如果不采用一些特殊的方法（如采用 Hybrid 端口的方法），不同的 VLAN 之间是不能够进行二层（数据链路层）通信的，这也是 VLAN 技术的基本出发点；一般地，VLAN 之间的通信是需要在第三层（网络层）才能实现的。

实现 VLAN 间的三层通信的方法有很多，最为传统的方法是使用路由器。除此之外，常用的方法还有很多，例如，在交换机上使用 VLANIF 接口，在交换机上使用 VLAN 聚合方法等。

VLANIF 接口只是一个逻辑意义上的三层接口。采用 VLANIF 接口的方法时，每一个 VLAN 都对应了交换机上的一

个 VLANIF 接口，不同的 VLNA 对应了不同的 VLANIF 接口，并且每个 VLAN 中的终端设备的网关地址就是所对应的 VLANIF 接口的 IP 地址。显然，使用 VLANIF 接口方法的一个主要缺点就是比较耗费 IP 地址资源，这是因为每一个不同的 VLAN 都必须对应一个不同的 VLANIF 接口，而每个不同的 VLANIF 接口都必须配置一个不同的 IP 地址。

VLAN 间的通信也可以通过使用 VLAN 聚合的方法来实现。VLAN 聚合使用了两种类型的 VLAN，分别称为 Sub-VLAN 和 Super-VLAN。VLAN 聚合的方法可以节省大量的 IP 地址资源。这是因为一个 Super-VLAN 需要配置一个 VLANIF 接口，并为该 VLANIF 接口配置一个 IP 地址，但该 Super-VLAN 下的各个 Sub-VLAN 都无需再配置 VLANIF 接口。



在 SW1 SW3 上创建 VLAN 2 VLAN3,并将相应的接口划分到 VLAN 中

SW1:

```
undo ter mo
sy
sys SW1
vlan batch 2 3
int g0/0/1
port link-type access
port default vlan 2
int g0/0/2
port link-type access
port default vlan 3
q
```

SW3:

```
undo ter mo
sy
sys SW3
vlan batch 2 3
int g0/0/1
port link-type access
port default vlan 2
int g0/0/2
port link-type access
port default vlan 3
q
```

在 SW1 ,SW2 ,SW3 上完成 Trunk 端口配置，允许所有 VLAN 帧通过

==========

Port-group

Port-group 是端口组的意思, Port-group 命令就是将要进行同样操纵的端口添加到一个组里，在这个组里进行操作就行了。

将要处理的端口加入到一个组里，对这个组进行操作后，系统会自动对组里的成员进行操作。这样在处理多个端口时就变得很方便了。

把 SW2 的 2 个接口都做成 trunk

port-group 1
group-member g0/0/23
group-member g0/0/24
port link-type trunk
port trunk allow-pass vlan 2 3

==========

SW1:
int g0/0/23
port link-type trunk
port trunk allow-pass vlan 2 3
q

SW2:
undo ter mo
sy
sys SW2
int g0/0/23
port link-type trunk
port trunk allow-pass vlan 2 3
int g0/0/24
port link-type trunk
port trunk allow-pass vlan 2 3
q

SW3:
int g0/0/24
port link-type trunk
port trunk allow-pass vlan 2 3
q

现在用 PC 1 ping PC 3 发现不通

```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
From 192.168.1.1: Destination host unreachable
```

原因是 SW2 上没有创建 VLAN 2,VLAN3
SW2：
vlan batch 2 3

```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time=78 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time=62 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=62 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time=78 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=46 ms
```

现在就可以 ping 通了

========

使用 VLANIF 接口实现 VLAN 间的通信
SW2:
int vlanif 2
ip add 192.168.1.100 24
int vlanif 3
ip add 192.168.2.100 24
q

4 台 PC 的网关设置好

测试一下,PC 1 ping PC2 ,PC4 是可以通的

```
PC>ping 192.168.2.1

Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break
From 192.168.2.1: bytes=32 seq=1 ttl=127 time=156 ms
From 192.168.2.1: bytes=32 seq=2 ttl=127 time=62 ms
From 192.168.2.1: bytes=32 seq=3 ttl=127 time=47 ms
From 192.168.2.1: bytes=32 seq=4 ttl=127 time=47 ms
From 192.168.2.1: bytes=32 seq=5 ttl=127 time=78 ms
```

========

使用 VLAN 聚合实现 VLAN 间通信

为了减少 VLANIF 接口的数目，节省 IP 地址的使用，我们还可以使用 VLAN 聚合的方法来实现不同 VLAN 间的通信。
SW2:
undo interface vlanif 2
undo interface vlanif 3
vlan 4

int g0/0/23
undo port trunk allow-pass vlan 4
int g0/0/24
undo port trunk allow-pass vlan 4

Super-VLAN 是不能包含任何物理接口的，但目前 SW2 的 g0/0/23, g0/0/24 已经做为 Trunk 端口被划分进了所有 VLAN，所以需要将 g0/0/23, g0/0/24 从 VLAN4 中移除。

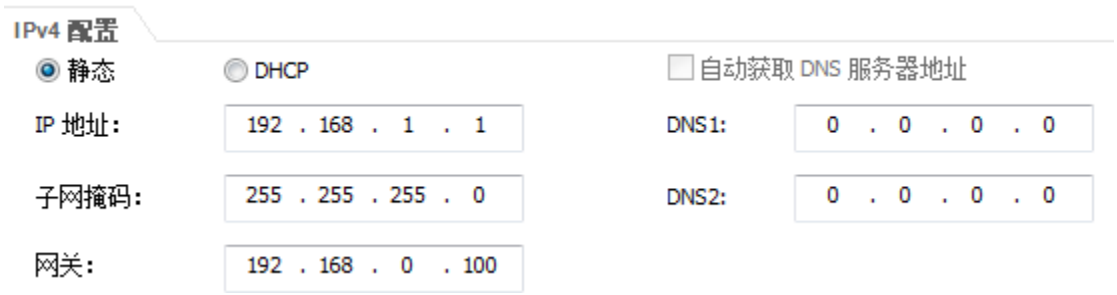
配置 VLAN4 为 Super-VLAN

将 VLAN2 ,VLAN3 作为 Sub-VLAN 划分进 Super-VLAN

SW2:
vlan 4
aggregate-vlan
access-vlan 2 3

VLAN4 创建 VLANIF 接口，配置 IP 地址为，192.168.0.100 16，然后开启 ARP 代理功能
SW2:
int vlanif 4
ip add 192.168.0.100 16
arp-proxy inter-sub-vlan-proxy enable

修改 PC 上的网关为 192.168.0.100



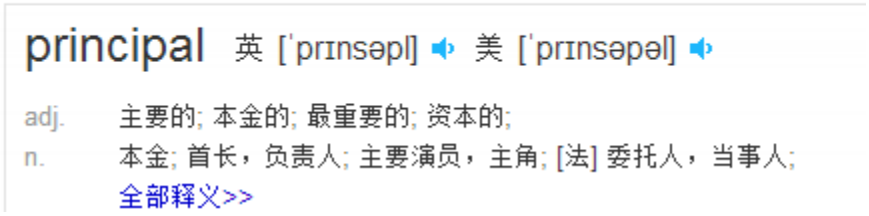
修改之后，4 台 PC 是可以相互 ping 通的

= = = = = = = =

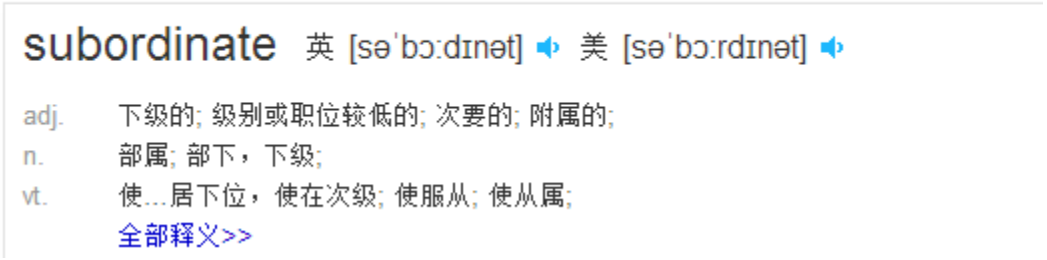
VLAN 实验 2：Mux VLAN

multiplex_百度翻译

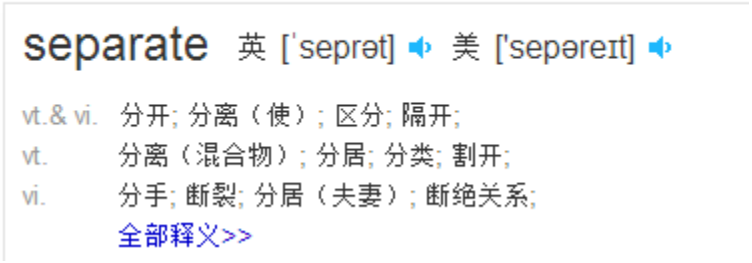
principal_百度翻译



subordinate_百度翻译



separate_百度翻译



MUX VLAN 实现了二层流量的弹性管控。

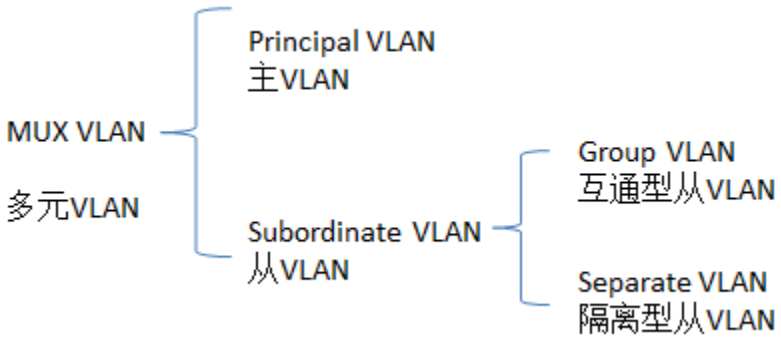
MUX VLAN

作用：MUX VLAN（Multiplex vlan ）猫特扑来克斯 提供了一种在 VLAN 内的端口间进行二层流量隔离的机制。

需求：在企业网络中，企业员工和企业客户可以访问企

业的服务器。对于企业来说，希望企业内部员工之间可以互相交流，而企业客户之间是隔离的，不能够互相访问。通过 MUX VLAN 提供的二层流量隔离的机制可以实现企业内部员工之间可以互相交流，而企业客户之间是隔离的。

原理： MUX VLAN 分为 Principal VLAN 和 Subordinate VLAN，
Subordinate VLAN 又分为 Separate VLAN 和 Group VLAN



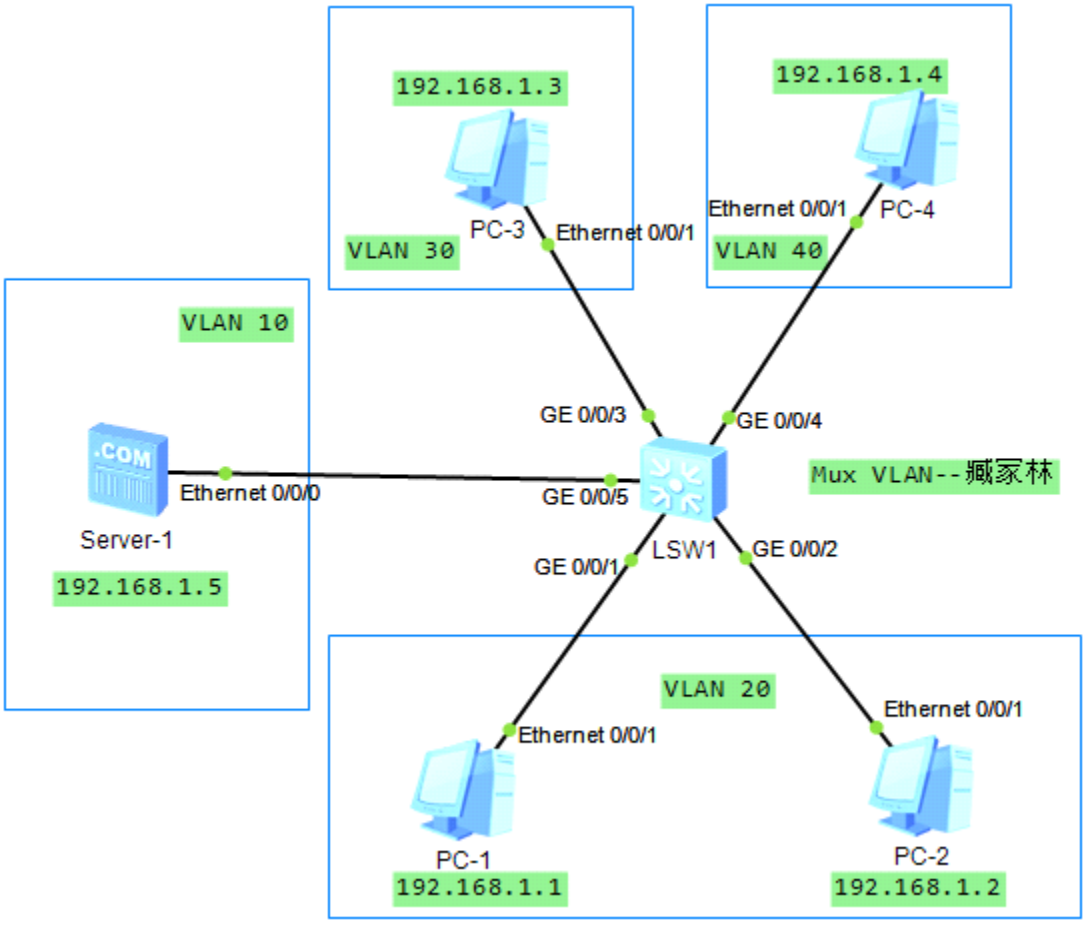
在实际的企业网络环境中，往往需要所有的终端用户都能够访问某些特定的服务器，而用户之间的访问控制规则比较复杂。在这样的场景下，使用普通 VLAN 划分的方法往往是很难满足需求的，通常的解决方法是使用 Mux VLAN

Mux VLAN 拥有一个 Principal VLAN,即主 VLAN，同时拥有多个与主 VLAN 关联的 Subordinate VLAN,即从 VLAN。从 VLAN 又有两种类型，一种是 Separate VLAN,即隔离型从 VLAN，另一种是 Group VLAN,即互通型从 VLAN。任何从 VLAN 中的设备都能够与主 VLAN 中的设备进行通信。除此之外，互通型从 VLAN 中的设备只能与本互通型从 VLAN 中的设备进行通信，不能与其他互通型从 VLAN 中的设备进行通信，也不能与隔离型从 VLAN 中的设备进行通信。隔离型从 VLAN 中的设备不能与互通型从 VLAN 中的设备进行通信，也不能与其他隔离型从 VLAN 中以及本隔离型从 VLAN 中的设备进

行通信。

交换机上加入 Mux VLAN 的端口只能允许一个 VLAN 的帧通过，允许多个 VLAN 的帧通过的端口是不能被加入到 Mux VLAN 中的。

在一个主 VLAN 中，隔离型从 VLAN 有一个，互通型从 VLAN 可以有多个



要求 VLAN 30 ,VLAN 40 只能与 VLAN 10 通信，

VLAN 30 不能访问 VLAN40, 也不能访问 VLAN 20

VLAN 20 中的两台设备相互间可以访问，也可以访问 VLAN 10

没有配置之前，5 台设备都可以相互 ping 通

= = = = = = = =

使用 Hybrid 端口实现

g0/0/1,g0/0/2 配置为 Hybrid，并要求端口对收到的 Untagged 帧添加 VLAN 20 的标签后进行转发，且在发送属于 VLAN 10 和 VLAN 20 的帧之前进行去标签处理。

SW1:

```
vlan batch 10 20 30 40

int g0/0/1
port link-type hybrid
port hybrid untagged vlan 10 20
port hybrid pvid vlan 20
int g0/0/2
port link-type hybrid
port hybrid untagged vlan 10 20
port hybrid pvid vlan 20
```

g0/0/5 配置为 Hybrid，并要求端口对收到的 Untagged 帧添加 VLAN 10 的标签后进行转发，且在发送属于 VLAN 10 ,VLAN20,VLAN30 和 VLAN 40 的帧之前进行去标签处理。

```
int g0/0/5
port link-type hybrid
```

port hybrid untagged vlan 10 20 30 40
port hybrid pvid vlan 10

int g0/0/3
port link-type hybrid
port hybrid untagged vlan 10 30
port hybrid pvid vlan 30

int g0/0/4
port link-type hybrid
port hybrid untagged vlan 10 40
port hybrid pvid vlan 40

PC 间进行 ping 的测试

= = = = = = = =

使用 MUX VLAN 实现

VLAN 10 为主 VLAN，VLAN20 为互通型从 VLAN，VLAN30 隔离型从 VLAN（VLAN 30 和 VLAN40 合并为 VLAN 30）。Mux VLAN 的端口仅能够允许一个 VLAN 的帧通过，所以需要将加入 Mux VLAN 的端口类型修改为 Access,要删掉之前的配置

SW1:
int g0/0/1
undo port hybrid pvid vlan
undo port hybrid untagged vlan 10 20
port link-type access
port default vlan 20
int g0/0/2
undo port hybrid pvid vlan

undo port hybrid untagged vlan 10 20
port link-type access
port default vlan 20
int g0/0/3
undo port hybrid pvid vlan
undo port hybrid untagged vlan 10 30
port link-type access
port default vlan 30
int g0/0/4
undo port hybrid pvid vlan
undo port hybrid untagged vlan 10 40
port link-type access
port default vlan 30
int g0/0/5
undo port hybrid pvid vlan
undo port hybrid untagged vlan 10 20 30 40
port link-type access
port default vlan 10

VLAN 10 为主 VLAN， VLAN 20 互通型从 VLAN
VLAN 30,为隔离型从 VLAN，只能有一个隔离 VLAN
SW1:
vlan 10
mux-vlan
subordinate group 20
subordinate separate 30

交换机端口开启 Mux VLAN 功能
int g0/0/1
port mux-vlan enable
int g0/0/2
port mux-vlan enable
int g0/0/3
port mux-vlan enable

int g0/0/4
port mux-vlan enable
int g0/0/5
port mux-vlan enable

<SW1>display mux-vlan

```
[SW1]dis mux-vlan
Principal Subordinate Type         Interface
------------------------------------------------------------------------------
10        -           principal    GigabitEthernet0/0/5
10        30          separate     GigabitEthernet0/0/3 GigabitEthernet0/0/4
10        20          group        GigabitEthernet0/0/1 GigabitEthernet0/0/2
10        40          group
------------------------------------------------------------------------------
```

PC 间相互 ping 一下，满足要求

= = = = = = = =

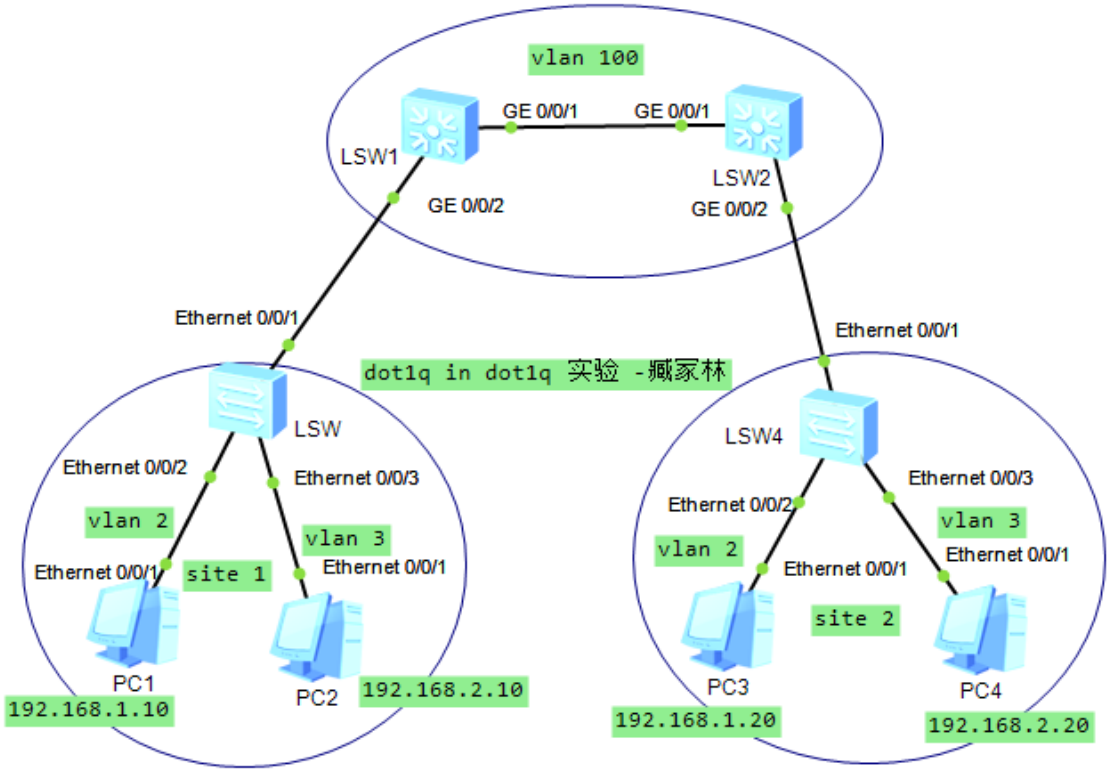
VLAN 实验 3：qinq

qinq（dot1q in dot1q）是一种二层环境中的二层 vpn 技术，用于二层 ISP 网络将相同客户网络中的 vlan 帧，再打一层 vlan-tag 的手段实现同一个客户的不同站点之间的数据通信。

qinq 的配置类型分为端口 qinq 和灵活 qinq
端口 qinq 是在 isp 设备入端口收到多个帧都打上同一个外层 tag 发送到对端
灵活 qinq 是在 isp 设备入端口根据收到的不同客户 vlan 帧打上不同的外层 vlan-tag 发送到对端的模式

site1 和 site2 分别为同一个客户的两个站点,分别规划了 vlan2 和 vlan3,中间 sw1 和 sw2 模拟了 ISP 的网络,整个网络使用二层通信。

现在因为 site1 和 site2 中使用的 vlan2 和 vlan3 在 isp 内部并没有，正常情况下需要 isp 在网络内部也创建 vlan2 和 vlan3，但是由于 isp 的客户数量众多不可能创建那么多与客户网络一样的 vlan，所以使用 qinq 技术在同一个客户的数据帧上再打一层 isp 内部的 vlan-tag（isp 使用 vlan100 来封装客户多个 site 的帧），使用外层的 vlan-tag 在 isp 内部寻址，而到达客户对端站点的时候设备剥离 isp 的外层 vlan-tag，还原成客户站点本来的 vlan-tag 从而使得同一个客户的多个站点之间可以相互通信。



根据拓扑使用端口 qinq 配置，使得 site1 与 site2 的相同 vlan 通信，即 pc1 与 pc3 通信，pc2 与 pc4 通信

port link-type dot1q-tunnel　　启用端口 qinq 模式，qi

nq 通道

port default vlan 100　　isp 设备接口收到的帧全部在外侧打上 vlan100 的 tag

SW1 ：配置

```
undo ter mo
sys
sys SW1
vlan 100
interface g0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface g0/0/2
port link-type dot1q-tunnel
port default vlan 100
q
```

SW2 ：配置

```
undo ter mo
sys
sys SW2
vlan 100
interface g0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface g0/0/2
port link-type dot1q-tunnel
port default vlan 100
q
```

SW3：配置

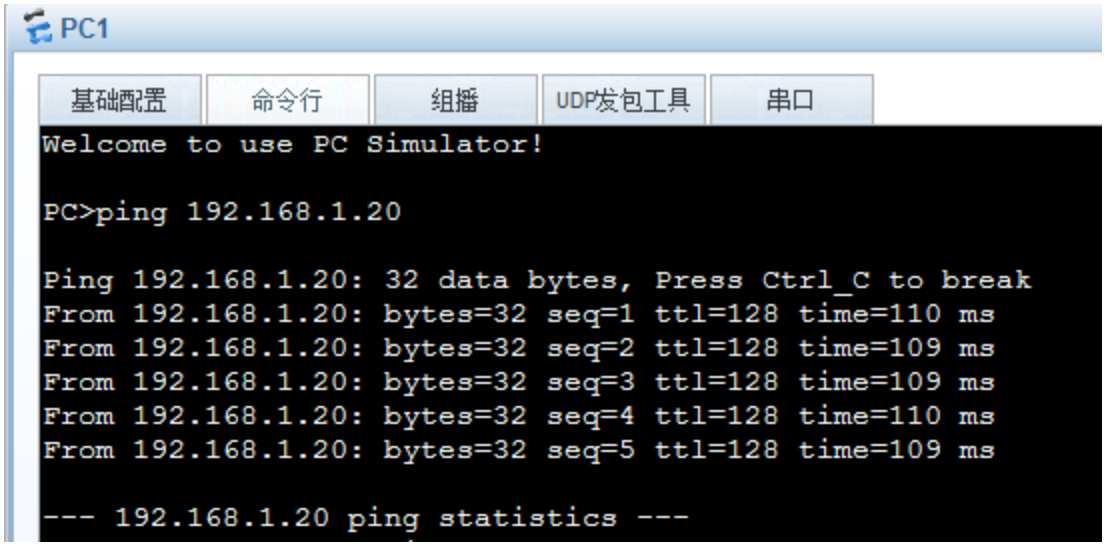
```
undo ter mo
sys
```

sys SW3
vlan batch 2 3
int e0/0/1
port link trunk
port trunk allow-pass vlan 2 3
undo port tr allow-pass vlan 1
int e0/0/2
port link acce
port default vlan 2
int e0/0/3
port link acce
port default vlan 3

SW4：配置
undo ter mo
sys
sys SW4
vlan batch 2 3
int e0/0/1
port link trunk
port trunk allow-pass vlan 2 3
undo port tr allow-pass vlan 1
int e0/0/2
port link acce
port default vlan 2
int e0/0/3
port link acce
port default vlan 3
q

测试，pc1 与 pc3 通信结果

pc1: ping 192.168.1.20



根据拓扑使用灵活 qinq 配置，使得 site1 与 site2 的相同 vlan 通信，即 pc1 与 pc3 通信，pc2 与 pc4 通信

灵活的 qinq 可以根据需求将客户网络的多个 vlan 集合分别对应 isp 内的多个 vlan 集合,如上述拓扑中客户 site 中的 vlan2、vlan3 在进入 isp 网络的时候分别在外层打上 vlan100、vlan200 的外层 tag 传递到对端的 site 中

qinq vlan-translation enable　　在 isp 入接口开启 qinq 的 vlan 映射功能
port hybrid untagged vlan 100 200　　允许 vlan100、200 通过该接口（出时剥离 vlan100、200 的标签）
port vlan-stacking vlan 2 stack-vlan 100　　客户网络中的 vlan2 的外层打上 isp 网络的 vlan100 的 tag
port vlan-stacking vlan 3 stack-vlan 200　　客户网络中的 vlan3 的外层打上 isp 网络的 vlan200 的 tag

VLAN Stacking 端口有以下特点：

具备 VLAN Stacking 功能的端口可以配置多个外层 VLAN，端口可以给不同 VLAN 的帧加上不同的外层 Tag。
具备 VLAN Stacking 功能的端口可以在接收帧时，给帧加上外层 Tag；发送帧时，剥掉帧最外层的 Tag。

SW1 ：配置
vlan 200
int g0/0/2
undo port default vlan
port link-type hybrid
port hybrid untagged vlan 100 200

qinq vlan-translation enable
port vlan-stacking vlan 2 stack-vlan 100
port vlan-stacking vlan 3 stack-vlan 200
q

SW2 ：配置
vlan 200
int g0/0/2
undo port default vlan
port link-type hybrid
port hybrid untagged vlan 100 200

qinq vlan-translation enable
port vlan-stacking vlan 2 stack-vlan 100
port vlan-stacking vlan 3 stack-vlan 200
q

测试，pc1 与 pc3 通信结果, 也是可以通的

pc1:ping 192.168.1.20

同时开启抓包，抓　SW1 的 g0/0/1，两台 ISP 相连的接口可以，看到 VLAN ID，VLAN 2 打 tag 为 100，

```
⊞ Frame 282: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
⊞ Ethernet II, Src: HuaweiTe_90:6c:44 (54:89:98:90:6c:44), Dst: HuaweiT
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 100
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
⊞ Internet Protocol, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.1
⊞ Internet Control Message Protocol
```

pc2:ping 192.168.2.20 ，可以看到 VLAN 3 打 tag 为 200

```
Frame 359: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: HuaweiTe_d5:69:a6 (54:89:98:d5:69:a6), Dst: HuaweiT
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 200
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 3
Internet Protocol, Src: 192.168.2.10 (192.168.2.10), Dst: 192.168.2.2
Internet Control Message Protocol
```

查看 VLAN，ST：Vlan-stacking;
display vlan

```
[SW1]dis vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
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(U)      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)      GE0/0/10(D)     GE0/0/11(D)     GE0/0/12(D)
                GE0/0/13(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)

100  common  UT:GE0/0/2(U)
             TG:GE0/0/1(U)
             ST:GE0/0/2(U)
200  common  UT:GE0/0/2(U)
             TG:GE0/0/1(U)
             ST:GE0/0/2(U)
```