HCIP-Datacom 分解实验 - 以太网交换安全

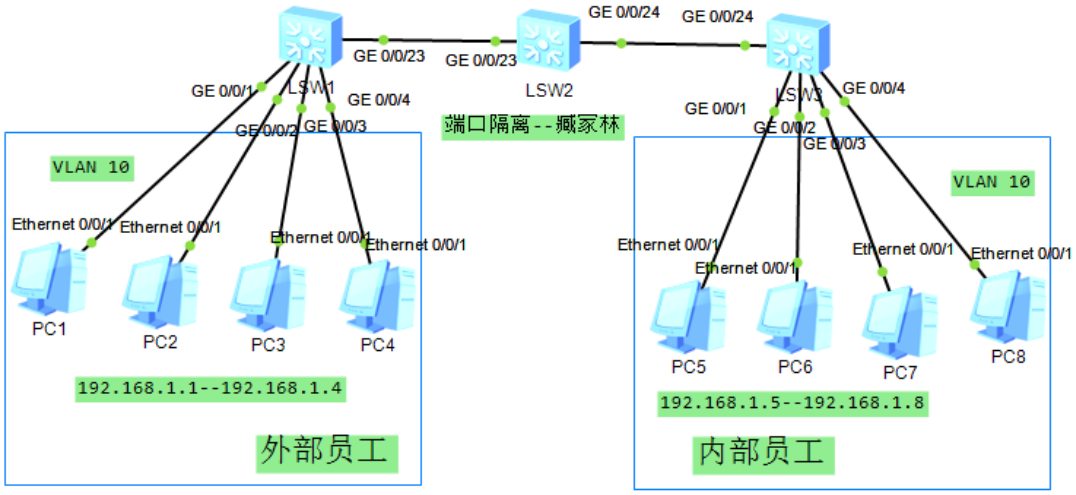
臧家林制作

以太网交换安全 实验 1： 端口隔离
以太网交换安全 实验 2： 端口安全

= = = = = = = = =

以太网交换安全 实验 1： 端口隔离

为了实现用户之间的二层隔离，可以将不同的用户加入不同的 VLAN，但这样会浪费有限的 VLAN 资源。采用端口隔离功能，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到同一隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。



企业内部的员工允许相互通信，属于企业外部的员工不允许相互通信，外部员工与内部员工之间允许通信。

基本配置

SW1：

```
undo ter mo
sy
sys SW1
vlan 10
int g0/0/1
port link-type acc
port default vlan 10
int g0/0/2
port link-type acc
port default vlan 10
int g0/0/3
port link-type acc
port default vlan 10
int g0/0/4
port link-type acc
port default vlan 10
```

```
int g0/0/23
port link-type trunk
port trunk allow-pass vlan 10
q
```

SW2 :

```
undo ter mo
sy
sys SW2
vlan 10
int g0/0/23
port link-type trunk
port trunk allow-pass vlan 10
int g0/0/24
port link-type trunk
port trunk allow-pass vlan 10
q
```

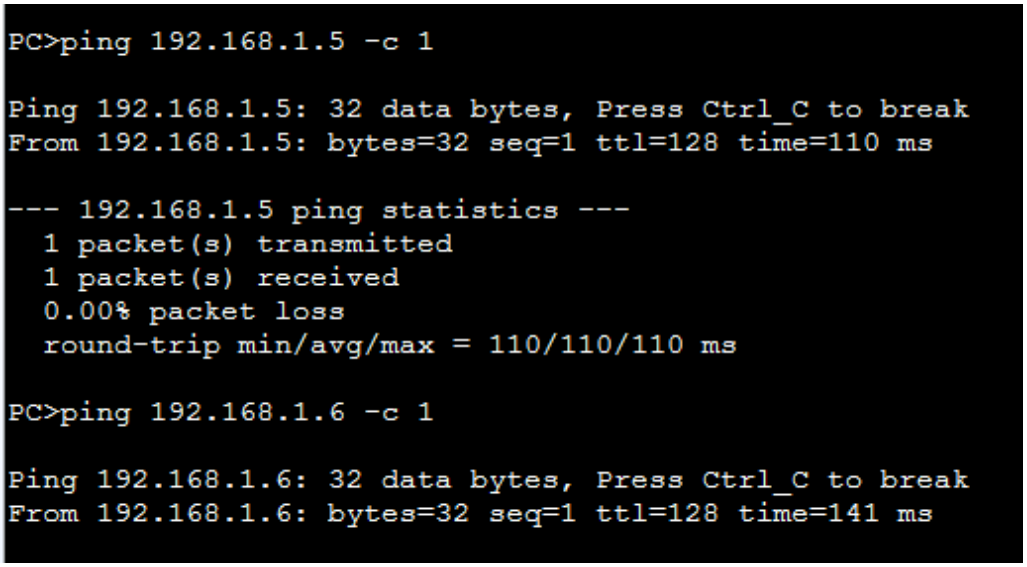
SW3:

```
undo ter mo
sy
sys SW3
vlan 10
int g0/0/1
port link-type acc
port default vlan 10
int g0/0/2
port link-type acc
port default vlan 10
int g0/0/3
port link-type acc
port default vlan 10
int g0/0/4
port link-type acc
```

port default vlan 10
int g0/0/24
port link-type trunk
port trunk allow-pass vlan 10
q

测试，几台 PC 在同一个 VLAN ，同一个网段是可以相互通信的

PC>ping 192.168.1.5 -c 1



配置端口隔离

将 SW1 的 4 个接口配置为端口隔离，为外部员工提供服务

SW1：
int g0/0/1
port-isolate enable group 1
int g0/0/2
port-isolate enable group 1

int g0/0/3
port-isolate enable group 1
int g0/0/4
port-isolate enable group 1

查看一下
display port-isolate group 1 查看所有创建的隔离组情况

```
[SW1]dis port-isolate group 1
  The ports in isolate group 1:
GigabitEthernet0/0/1     GigabitEthernet0/0/2     GigabitEthernet0/0/3
GigabitEthernet0/0/4
```

ping 测试一下 。外部员工之间，不能通信，但可以与内部员工通信
192.168.1.1　不可以 ping 通 1.2 ，1.3 ，1.4
可以与 1.5 ， 1.6 ， 1.7 ， 1.8 通信

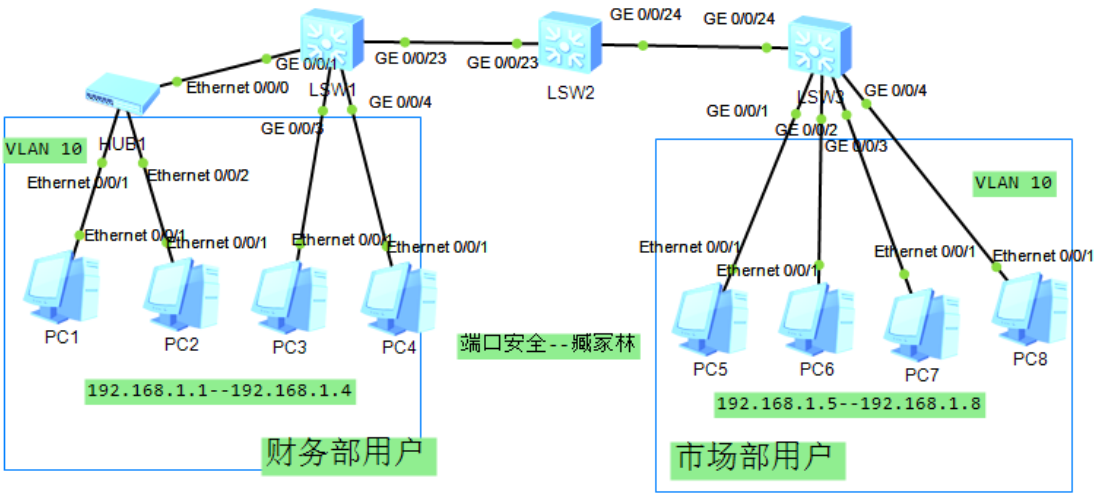
也可以创建两个组 ，group 1 , group 2 ,两个组内的 PC 是可以相互通信的

= = = = = = = =

以太网交换安全 实验 2： 端口安全

配置端口安全功能，将接口学习到的 MAC 地址转换为安全 MAC 地址，接口学习的最大 MAC 数量达到上限后不再学习新的 MAC 地址，只允许学习到 MAC 地址的设备通信。这样可以阻止其他非信任用户通过本接口和交换机通信，提高设备与网络的安全性。

端口安全（Port Security）通过将接口学习到的动态 MAC 地址转换为安全 MAC 地址（包括安全动态 MAC、安全静态 MAC 和 Sticky MAC）阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。



int g0/0/1
port-security enable，使能端口安全功能。
port-security mac-address sticky，使能接口 Sticky MAC 功能。
port-security max-mac-num max-number，配置接口 Sticky MAC 学习限制数量。

缺省情况下，接口学习的 MAC 地址限制数量为 1。
port-security protect-action { protect | restrict | shutdown }，配置端口安全保护动作。

缺省情况下，端口安全保护动作为 restrict。

restrict :丢弃源 MAC 地址不存在的报文并上报告警。推荐使用 restrict 动作。

protect：只丢弃源 MAC 地址不存在的报文，不上报告警。
shutdown：接口状态被置为 error-down，并上报告警。

port-security mac-address sticky mac-address vlan vlan-id ,

手动配置一条 sticky-mac 表项。

基本配置

SW1：
```
undo ter mo
sy
sys SW1
vlan 10
int g0/0/1
port link-type acc
port default vlan 10
int g0/0/3
port link-type acc
port default vlan 10
int g0/0/4
port link-type acc
port default vlan 10
int g0/0/23
port link-type trunk
port trunk allow-pass vlan 10
q
```

SW2：
```
undo ter mo
sy
sys SW2
```

```
vlan 10
int g0/0/23
port link-type trunk
port trunk allow-pass vlan 10
int g0/0/24
port link-type trunk
port trunk allow-pass vlan 10
q
```

SW3:

```
undo ter mo
sy
sys SW3
vlan 10
int g0/0/1
port link-type acc
port default vlan 10
int g0/0/2
port link-type acc
port default vlan 10
int g0/0/3
port link-type acc
port default vlan 10
int g0/0/4
port link-type acc
port default vlan 10
int g0/0/24
port link-type trunk
port trunk allow-pass vlan 10
q
```

配置端口安全

SW1 :

int g0/0/1
port-security enable

默认接口学习的 MAC 地址限制数量为 1
PC1 ping 192.168.1.3 可以通，但 PC2 ping 192.168.1.3 就不可以通了

不通之后，查看 Trap 缓冲区记录的所有信息。
<SW1>display trapbuffer

```
<SW1>display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 6

#Nov 29 2017 13:17:37-08:00 SW1 L2IFPPI/4/PORTSEC_ACTION_ALARM:OID 1.3.6.1.4.1.2
011.5.25.42.2.1.7.6 The number of MAC address on interface (6/6) GigabitEthernet
0/0/1 reaches the limit, and the port status is : 1. (1:restrict;2:protect;3:shu
tdown)
#Nov 29 2017 13:16:30-08:00 SW1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.2
```

如果两个都要通，需要修改限制数量
int g0/0/1
port-security max-mac-num 5

使能接口 Sticky MAC 功能，修改端口安全保护动作为

int g0/0/1
port-security mac-address sticky
port-security protect-action protect

dis mac-address sticky

```
[SW1]display mac-address sticky
MAC address table of slot 0:
-------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type
               VSI/SI
-------------------------------------------------------------------------
5489-9814-1949 10          -      -      GE0/0/1         sticky
5489-98bf-740c 10          -      -      GE0/0/1         sticky
-------------------------------------------------------------------------
Total matching items on slot 0 displayed = 2
```

也可以手工添加
int g0/0/1
port-security mac-addres sticky 5489-9800-0001 vlan 10

SW3：
要 ping 一下，有数据通过交换机，再去查看
int g0/0/1
port-security enable

dis mac-address security

```
[SW3]display mac-address security
MAC address table of slot 0:
-------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type
               VSI/SI
-------------------------------------------------------------------------
5489-98ee-3e25 10          -      -      GE0/0/1         security
-------------------------------------------------------------------------
Total matching items on slot 0 displayed = 1
```