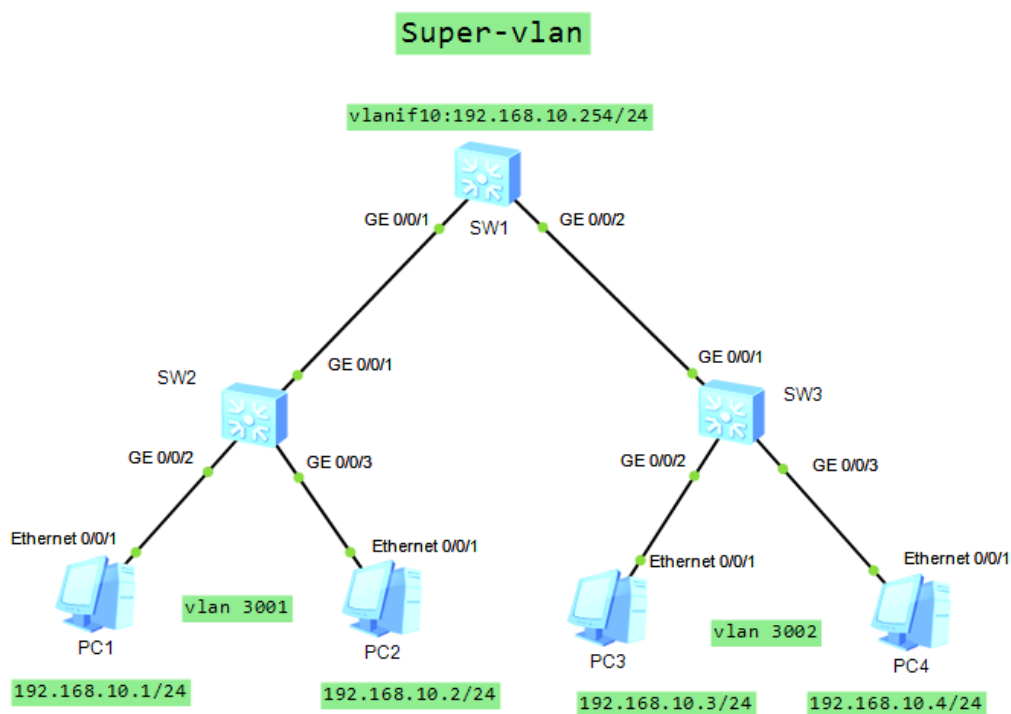


【HCIP 实验 05】 Super-vlan+端口安全

一、 实验拓扑



二、 实验需求及解法

本实验模拟某企业内网，多个部门分隔为不同的 vlan，但是每个部门主机数量都较少。为了简化 IP 地址规划，节省 IP 地址，需配置 Super-vlan。请完成以下需求：

1.SW1 创建 vlan10，vlan3001 和 vlan3002

将 vlan10 设置为 Super-vlan，vlan3001 和 3002 为子 vlan。

SW1:

```
vlan batch 10 3001 3002
```

```
vlan 10
```

```
aggregate-vlan  
access-vlan 3001 to 3002
```

2.SW2/3 创建 vlan3001 和 vlan3002

```
SW2/3:  
vlan batch 3001 3002
```

3.SW1/2/3 之间使用 trunk 链路，并仅允许 vlan3001 和 3002 通过。

```
SW1:  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 3001 to 3002  
interface GigabitEthernet0/0/2  
    port link-type trunk  
    port trunk allow-pass vlan 3001 to 3002  
#  
SW2:  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 3001 to 3002  
#  
SW3:  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 3001 to 3002
```

4.SW2/3 与 PC 之间使用 access 链路，并划入对应 vlan。

```
SW2:  
interface GigabitEthernet0/0/2  
    port link-type access  
    port default vlan 3001  
interface GigabitEthernet0/0/3  
    port link-type access  
    port default vlan 3001  
#  
SW3:  
interface GigabitEthernet0/0/2  
    port link-type access  
    port default vlan 3002  
interface GigabitEthernet0/0/3
```

```
port link-type access
port default vlan 3002
```

5.验证通信：

PC1 可以与 PC2 通信，PC3 可以与 PC4 通信
PC1/2 不能与 PC3/4 通信。

6.在网关 vlanif10 中开启 vlan 间代理 ARP 功能。

SW1:

```
interface Vlanif10
ip address 192.168.10.254 255.255.255.0
arp-proxy inter-sub-vlan-proxy enable
```

7.验证通信：

PC1 可以与 PC3 通信，且使用 tracert 命令验证需先经过网关。

PC1>tracert 192.168.10.3

```
tracert to 192.168.10.3, 8 hops max
(ICMP), press Ctrl+C to stop
 1  192.168.10.254    47 ms  47 ms  31 ms
 2  192.168.10.3     62 ms  109 ms  94 ms
```

8.为保证企业内网安全，需要在 vlan3001 中开启端口安全，完成以下需求：

- 8.1 最大学习 mac 地址数量为 5 个。
- 8.2 学习到的 mac 地址永不超时，且端口关闭或设备重启后不会删除。
- 8.3 当学习的 mac 地址数量超过 5 个时，会自动关闭端口。

SW2:

```
interface GigabitEthernet0/0/2
port-security enable
port-security protect-action shutdown
port-security max-mac-num 5
port-security mac-address sticky
interface GigabitEthernet0/0/3
port-security enable
port-security protect-action shutdown
port-security max-mac-num 5
port-security mac-address sticky
```