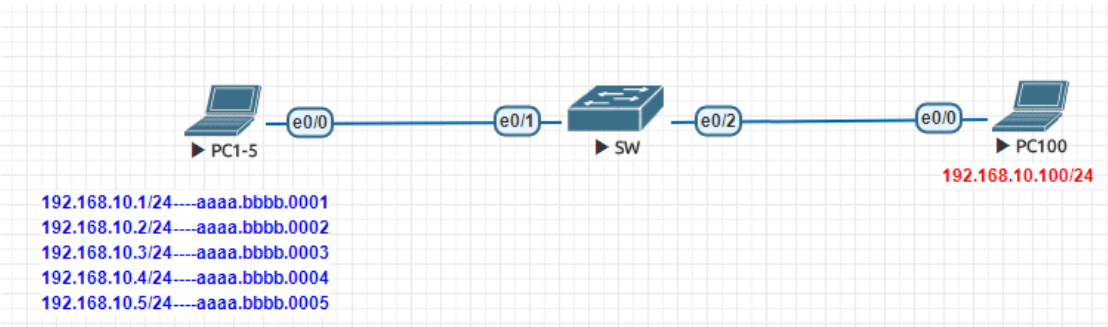
port-security 特性演示

一、拓扑



要求：

1.通过路由器模拟 PC1-5、PC100，其中 PC1-5 通过修改 MAC 地址和 IP 地址，分别扮演 PC1、PC2、PC3、PC4、PC5。

2.通过在 SW 的 e0/1 接口上配置 port-security 特性，检查接口的转发特性。

二、配置过程

1.PC100 配置 IP 地址为 192.168.10.100/24。（过程省略）

2.交换机 SW 上配置 e0/1

```
SW(config)#interface e0/1
SW(config-if)#switchport mode access
SW(config-if)#spanning-tree portfast
SW(config-if)#switchport port-security
SW(config-if)#switchport port-security maximum 4
SW(config-if)#switchport port-security violation shutdown
```

※注意配置以上命令时，先关闭接口，然后再打开。

3.配置 PC1-5，

分别通过配置 PC1-5 的 MAC、IP 地址，再 ping PC100，记录能否成功访问，再查看 SW 的 MAC 表。

①第 1 次改 MAC 和 IP

```
PC1-5(config)#interface e0/0
PC1-5(config-if)#mac-address aaaa.bbbb.0001
PC1-5(config-if)#ip address 192.168.10.1 255.255.255.0
```

```
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 s
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/
PC1-5#
```

```
SW#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aaaa.bbbb.0001    STATIC      Et0/1
   1    aabb.cc00.3000    DYNAMIC     Et0/2
Total Mac Addresses for this criterion: 2
SW#
```

②第 2 次修改

```
PC1-5(config)#interface e0/0
PC1-5(config-if)#mac-address aaaa.bbbb.0002
PC1-5(config-if)#no shutdown
```

```
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1008 ms
PC1-5#
```



```
SW#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aaaa.bbbb.0001    STATIC      Et0/1
   1    aaaa.bbbb.0002    STATIC      Et0/1
   1    aabb.cc00.3000    DYNAMIC     Et0/2
Total Mac Addresses for this criterion: 3
SW#
```

第 3 次修改这里省略，直接看第 4 次、第 5 次修改

③第 4 次修改

```
PC1-5(config)#interface e0/0
PC1-5(config-if)#mac-address aaaa.bbbb.0004
PC1-5(config-if)#no shutdown
```

```
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1002 ms
PC1-5#
```

```
SW#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aaaa.bbbb.0001    STATIC      Et0/1
   1    aaaa.bbbb.0002    STATIC      Et0/1
   1    aaaa.bbbb.0003    STATIC      Et0/1
   1    aaaa.bbbb.0004    STATIC      Et0/1
   1    aabb.cc00.3000    DYNAMIC     Et0/2
Total Mac Addresses for this criterion: 5
SW#
```

④第 5 次修改

```
PC1-5(config)#interface e0/0
PC1-5(config-if)#mac-address aaaa.bbbb.0005
PC1-5(config-if)#no shutdown
```

```
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC1-5#
```

```
SW#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aabb.cc00.3000    DYNAMIC     Et0/2
Total Mac Addresses for this criterion: 1
SW#
```

从上面的图中可以看到，当第 5 次修改 MAC 时，PC1-5 无法访问 PC100，这是为什么呢？我们查看 SW 的接口状态。

```
SW#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  down                  down
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
SW#
```

可以看到此时 SW 的 e0/1 已经关闭。

此时，可能会感到奇怪，没有任何操作去人为关闭 SW 的 e0/1，为什么该接口会关闭呢？

这个原因就要从 port-security 的工作机制说起。

此时，查看 SW 的 port-security 配置

```
SW#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Et0/1              4            0                  1         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW#
```

从上图可以看到，该交换机的 e0/1 上配置了 port-security 特性，并且最大的 MaxSecureAddr 为 4，其含义为，在交换机的 MAC 表中，从 e0/1 上学习到的 MAC 条目，最多只能有 4 条，一旦出现大于 4 条的情况，则接口会执行 Security Action，即 shutdown。

由于前面我们在 PC1-5 上通过修改接口 MAC，在短时内从 e0/1 处学习到的 MAC 条目达到 5 条，则会触发关闭的行为，故 SW 的 e0/1 被关掉，则 PC1-5 没法访问 PC100。

由于从 e0/1 上学习到 5 个 MAC 地址，触发 SW 的 e0/1 被关掉，为了重新通信，需要恢复 SW 的 e0/1，此时人为关掉再打开该接口，

```
SW(config)#interface e0/1
SW(config-if)#shutdown
SW(config-if)#no shutdown
```

```
SW#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
SW#
```

则 PC1-5 和 PC100 可以正常通信。

通过上面的演示，可以看到，合理设置 maximum 数值，限制从交换机 e0/1 接口上学习到时的 MAC 地址的数目，可以有效地防止，一些不安全的 PC 连接到裸露在室外的交换机接口上，对网络发起的攻击，如 ARP 攻击。

但是在室内环境下，如果有一个活动的交换机接口供合法用户连接自己的笔记本，该笔记本可能时连时不连，当连接时，需要接口正常转发数据，同时又要防止其它用户（特别是一些陌生人）通过该接口访问网络，此时如果按照上面的方法，会出现：其它用户一旦尝试连接口后，会永久性的关闭该接口，合法用户正常连接到该接口后，也没法访问网络的现象。（要想正常访问网络，必须找网络管理人员重新关闭、打开该接口，这是很不方便的）

为了解决上面的问题，可以有一种设想，即让交换机预先记下合活用户所有的设备 MAC 地

址，一旦非法用户接入设备时，接口受到限制而无法使用网络，而非法用户因无法使用网络拿掉自己的设备后，接口又能自动打开，则这个特效可以使用 MAC 授权名单来完成。
现假设合法用户拥有 2 台移动 PC，其 MAC 地址分别为 aaaa.bbbb.0001、aaaa.bbbb.0002，则可以在 SW 的 e0/1 上配置如下：
①SW 上定义授权 MAC 表和最大合活 MAC 数

```
SW(config)#interface e0/1
SW(config-if)#spanning-tree portfast
SW(config-if)#switchport port-security
SW(config-if)#switchport port-security maximum 2
SW(config-if)#switchport port-security violation restrict
SW(config-if)#switchport port-security mac-addres aaaa.bbbb.0001
*Jun 29 14:19:42.551: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Eth
half duplex).
SW(config-if)#switchport port-security mac-addres aaaa.bbbb.0001
SW(config-if)#switchport port-security mac-addres aaaa.bbbb.0002
SW(config-if)#exit
```

②开启接口，用 PC1-5 模拟非法用户的设备

```
PC1-5#show interface e0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aaaa.bbbb.0004 (bia aabb.cc00.2000)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

此处可看到 PC1-5 的 MAC 明显是 aaaa.bbbb.0004，则成功模拟一台非法用户设备。

```
SW(config)#interface e0/1
SW(config-if)#no shutdown
```

打开 SW 的接口 e0/1 后，可看到其 MAC 表为

```
SW#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aaaa.bbbb.0001    STATIC      Et0/1
   1    aaaa.bbbb.0002    STATIC      Et0/1
   1    aabb.cc00.3000    DYNAMIC     Et0/2
Total Mac Addresses for this criterion: 3
SW#
```

再测试非法用户 PC1-5 能否访问 PC100

```
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC1-5#
```

可以看到非法用户 PC1-5 的设备虽然接在交换机的 e0/1 上，但没法访问网络，则避免其对网络的非法攻击。
③接着修改 PC1-5 的 MAC 地址，模拟合法用户设备

```
PC1-5(config)#interface e0/0
PC1-5(config-if)#mac-address aaaa.bbbb.0001
PC1-5(config-if)#no shutdown
```

```
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1003 ms
PC1-5#
```

则合法用户设备 PC1-5 能正常访问网络。

```
PC1-5(config)#interface e0/0
PC1-5(config-if)#mac-address aaaa.bbbb.0002
PC1-5(config-if)#end
PC1-5#ping 192.16.10
*Jun 29 14:27:15.436: %SYS-5-CONFIG_I: Configured from console by console
PC1-5#ping 192.168.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1003 ms
PC1-5#
```

当然，这种方法比较安全，但不够灵活，常常用在一些安全场合比较高的地方，如连接服务器的交换机接口上，因为这类接口上的设备一般比较固定，MAC 地址比较固定。而在一些 MAC 地址不固定的交换机接口上，不宜使用。