

交换机端口安全总结(配置实例) PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/142/2021_2022__E4_BA_A4_E6_8D_A2_E6_9C_BA_E7_c101_142419.htm

最常用的对端口安全的理解就是可根据MAC地址来做对网络流量的控制和管理，比如MAC地址与具体的端口绑定，限制具体端口通过的MAC地址的数量，或者在具体的端口不允许某些MAC地址的帧流量通过。稍微引申下端口安全，就是可以根据802.1X来控制网络的访问流量。首先谈一下MAC地址与端口绑定，以及根据MAC地址允许流量的配置。

1.MAC地址与端口绑定，当发现主机的MAC地址与交换机上指定的MAC地址不同时，交换机相应的端口将down掉。当给端口指定MAC地址时，端口模式必须为access或者Trunk状态。

```
3550-1#conf t
```

```
3550-1(config)#int f0/1 3550-1(config-if)#switchport mode access /指定端口模式。 3550-1(config-if)#switchport port-security mac-address 00-90-F5-10-79-C1 /配置MAC地址。
```

```
3550-1(config-if)#switchport port-security maximum 1 /限制此端口允许通过的MAC地址数为1。 3550-1(config-if)#switchport port-security violation shutdown /当发现与上述配置不符时，端口down掉。
```

2.通过MAC地址来限制端口流量，此配置允许一TRUNK口最多通过100个MAC地址，超过100时，但来自新的主机的数据帧将丢失。

```
3550-1#conf t 3550-1(config)#int f0/1
```

```
3550-1(config-if)#switchport trunk encapsulation dot1q
```

```
3550-1(config-if)#switchport mode trunk /配置端口模式
```

```
为TRUNK。 3550-1(config-if)#switchport port-security maximum 100 /允许此端口通过的最大MAC地址数目为100。
```

3550-1(config-if)#switchport port-security violation protect /当主机MAC地址数目超过100时，交换机继续工作，但来自新的主机的数据帧将丢失。上面的配置根据MAC地址来允许流量，下面的配置则是根据MAC地址来拒绝流量。1.此配置在Catalyst交换机中只能对单播流量进行过滤，对于多播流量则无效。

```
3550-1#conf t 3550-1(config)#mac-address-table static 00-90-F5-10-79-C1 vlan 2 0drop /在相应的Vlan丢弃流量。
```

```
3550-1#conf t 3550-1(config)#mac-address-table static 00-90-F5-10-79-C1 vlan 2 int f0/1 /在相应的接口丢弃流量。
```

100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com