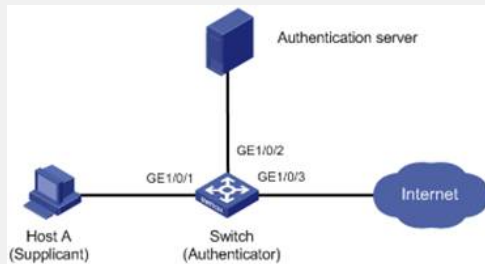


S5600系列交换机ARP/IP攻击防御功能的配置

一、组网需求:

- (1) 接入用户Host A使用手工配置的静态IP地址。且安装了802.1x客户端。
- (2) 服务器采用H3C公司的CAMS认证、授权、计费服务器。
- (3) 在接入交换机Switch上开启802.1x认证通过的信息用于ARP入侵检测与IP过滤功能, 防御接入用户的ARP攻击。

二、组网图:



三、配置步骤:

```
# 进入系统视图。
<Switch> system-view
# 全局开启802.1x认证功能。
[Switch] dot1x
# 在VLAN1内开启ARP入侵检测功能。
[Switch] vlan 1
[Switch-vlan1] arp detection enable
[Switch-vlan1] quit
# 设置端口GigabitEthernet1/0/2, GigabitEthernet1/0/3为ARP入侵检测信任端口。
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] arp detection trust
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] arp detection trust
[Switch-GigabitEthernet1/0/3] quit
# 在Switch 上开启802.1x认证通过的信息用于ARP Detection的安全检查功能。
[Switch] ip source static import dot1x
# 端口GigabitEthernet 1/0/1上开启802.1x功能。
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
# 端口GigabitEthernet 1/0/1上开启802.1x认证通过的信息用于IP过滤功能。
[Switch-GigabitEthernet1/0/1] ip check dot1x enable
```

四、配置关键点:

无