H3C S5510使用用户自定义acl实现防ARP仿冒网关的典型配置

赵国卫 2008-03-27 发表

H3C S3610/S5510使用用户自定义acl实现防ARP仿冒网关的典型配置

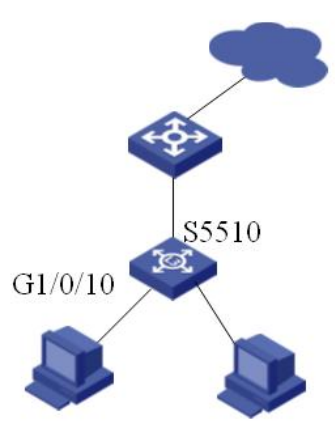
一、 组网需求：

H3C S5510设备作为接入设备

要求实现防止下挂PC发送仿冒网关的ARP攻击报文

网关IP: 10.1.1.1/24

二、 组网图：



三、 配置步骤：

(1) 全局视图去使能ndp,ntdp,habp,cluster,dot1x功能

```
undo ndp enable
undo ntdp enable
undo habp enable
undo cluster enable
undo dot1x
```

(2) 全局视图定义流模板

```
flow-template anti_arp extend start 28 4 l2 12 2
```

(3) 定义ACL

```
acl number 5000
rule 5 deny start 0A010101 ffffffff 28 l2 0806 ffff 12
```

(4) 定义类

```
traffic classifier anti_arp operator and
if-match acl 5000
```

(5) 定义行为

```
traffic behavior anti_arp
filter deny
```

(6) 定义策略

```
qos policy anti_arp
classifier anti_arp behavior anti_arp
```

(7) 下发流模板以及策略

```
interface GigabitEthernet 1/0/10
[H3C-GigabitEthernet1/0/10]flow-template anti_arp
[H3C-GigabitEthernet1/0/10]qos apply policy anti_arp inbound
```

四、 配置关键点：

(1) 用户自定义acl需要和扩展流模板一起使用

(2) 在端口上应用流模板时，请关闭如下功能：802.1x功能、集群功能（NDP、NTDP、HABP、Cluster）、DHCP Snooping、端口隔离、MAC+IP+端口绑定、灵活QinQ、Voice VLAN，否则流模板将不能成功应用。

(3) 类型偏移量，不带tag时为12，带tag时为16

(4) 先在端口下发流模板，再下发流策略

(5) 最多支持配置两个用户自定义流模板

(6) 同样配置适用于交换机H3C S3610。