

S3100-EI系列交换机ARP入侵检测与ARP报文限速功能的配置

一、组网需求：

如下图所示，Switch A（S3100-EI）的端口Ethernet1/0/1连接DHCP服务器，端口Ethernet1/0/2和Ethernet1/0/3分别连接Client A和Client B，且三个端口都属于VLAN 1。

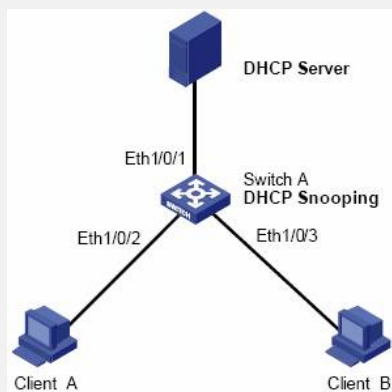
（1）开启交换机的DHCP Snooping功能，并设置端口Ethernet1/0/1为DHCP Snooping信任端口。

（2）为防止ARP中间人攻击，配置VLAN 1的ARP入侵检测功能，设置Switch的端口Ethernet1/0/1为ARP信任端口。

（3）开启端口Ethernet1/0/2和Ethernet1/0/3上的ARP报文限速功能，防止来自Client A和Client B的ARP报文流量攻击。

（4）开启Switch A上的端口状态自动恢复功能，设置恢复时间间隔为200秒。

二、组网图：



三、配置步骤：

开启交换机DHCP Snooping功能。

```
<SwitchA> system-view
```

```
[SwitchA] dhcp-snooping
```

设置端口Ethernet1/0/1为DHCP Snooping信任端口，ARP信任端口。

```
[SwitchA] interface Ethernet1/0/1
```

```
[SwitchA-Ethernet1/0/1] dhcp-snooping trust
```

```
[SwitchA-Ethernet1/0/1] arp detection trust
```

```
[SwitchA-Ethernet1/0/1] quit
```

开启VLAN 1内所有端口的ARP入侵检测功能。

```
[SwitchA] vlan 1
```

```
[SwitchA-vlan1] arp detection enable
```

开启端口Ethernet1/0/2上的ARP报文限速功能，设置ARP报文通过的最大速率为20pps。

```
[SwitchA] interface Ethernet1/0/2
```

```
[SwitchA-Ethernet1/0/2] arp rate-limit enable
```

```
[SwitchA-Ethernet1/0/2] arp rate-limit 20
```

```
[SwitchA-Ethernet1/0/2] quit
```

开启端口Ethernet1/0/3上ARP报文限速功能，设置ARP报文通过的最大速率为50pps。

```
[SwitchA] interface Ethernet1/0/3
```

```
[SwitchA-Ethernet1/0/3] arp rate-limit enable
```

```
[SwitchA-Ethernet1/0/3] arp rate-limit 50
```

```
[SwitchA-Ethernet1/0/3] quit
```

配置端口状态自动恢复功能，恢复时间间隔为200秒。

```
[SwitchA] arp protective-down recover enable
```

```
[SwitchA] arp protective-down recover interval 200
```

四、配置关键点：

无

