

S5130 ARP Detection典型配置

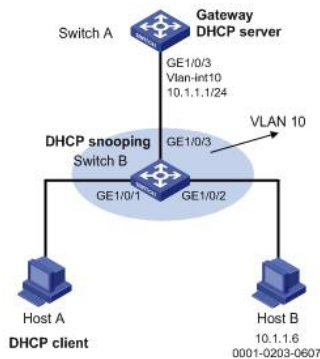
一、组网需求：

Switch A是DHCP服务器；

Host A是DHCP客户端；用户Host B的IP地址是10.1.1.6，MAC地址是0001-0203-0607。

Switch B是DHCP Snooping设备，在VLAN 10内启用ARP Detection功能，对DHCP客户端和用户进行用户合法性检查和报文有效性检查。

二、组网图



三、配置步骤

(1) 配置组网图中所有接口属于VLAN及Switch A对应VLAN接口的IP地址（略）

(2) 配置DHCP服务器Switch A

配置DHCP地址池0。

```
system-view
```

```
[SwitchA] dhcp enable
```

```
[SwitchA] dhcp server ip-pool 0
```

```
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

(3) 配置DHCP客户端Host A和用户Host B（略）

(4) 配置设备Switch B

启用DHCP Snooping功能。

```
system-view
```

```
[SwitchB] dhcp snooping enable
```

```
[SwitchB] interface gigabitethernet 1/0/3
```

```
[SwitchB-GigabitEthernet1/0/3] dhcp snooping trust
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

在接口GigabitEthernet1/0/1上启用DHCP Snooping表项记录功能。

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] dhcp snooping binding record
```

```
[SwitchB-GigabitEthernet1/0/1] quit
```

使能ARP Detection功能，对用户合法性进行检查。

```
[SwitchB] vlan 10
```

```
[SwitchB-vlan10] arp detection enable
```

接口状态缺省为非信任状态，上行接口配置为信任状态，下行接口按缺省配置。

```
[SwitchB-vlan10] interface gigabitethernet 1/0/3
```

```
[SwitchB-GigabitEthernet1/0/3] arp detection trust
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

在接口GigabitEthernet1/0/2上配置IP Source Guard静态绑定表项。

```
[SwitchB] interface gigabitethernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 00
```

```
01-0203-0607 vlan 10
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```

配置进行报文有效性检查。

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

完成上述配置后，查看dhcp snooping表项

```
[S5310]display dhcp snooping binding
```

```
1 DHCP snooping entries found.
```

```
IP address MAC address Lease VLAN SVLAN Interface
```

=====
10.1.1.5 8434-9820-7018 86080 10 N/A GE1/0/1

对于接口GigabitEthernet1/0/1和GigabitEthernet1/0/2收到的ARP报文，先进行报文有效性检查，然后基于IP Source Guard静态绑定表项、DHCP Snooping安全表项进行用户合法性检查。

四、配置要点

(1)S5130 dhcp snooping表项记录需要在对应接口下使能`dhcp snooping binding record`，否则不记录dhcp snooping表项，导致开启arp Detection后端口收到的ARP报文，对进行报文有效性检查，找不到DHCP Snooping安全表项，从而导致访问失败。此为V7平台与V5平台实现的不同，V5平台设备不需要配置该命令，使能dhcp snooping后就会记录表项。

(2) S5130 查看dhcp snooping表项的命令也与V5平台不同，S5130上查看命令为`display dhcp snooping binding`，V5平台设备查看命令直接为`display dhcp snooping`。