V5交换机DHCP Snooping配置方法（命令行版)

目录

1 配置需求或说明

1.1适用产品系列

本案例适用于如S3100V2-16TP-EI、S5120-28P-SI、S5130S-28S-SI等的V5交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comvare V5、V7平台交换机分类说明”。

本案例适用于如S3100V2-16TP-EI、S5008PV2-EI、S5120-28P-SI、MS4120-26TP等的V5交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comware V5、V7平台交换机分类说明”。

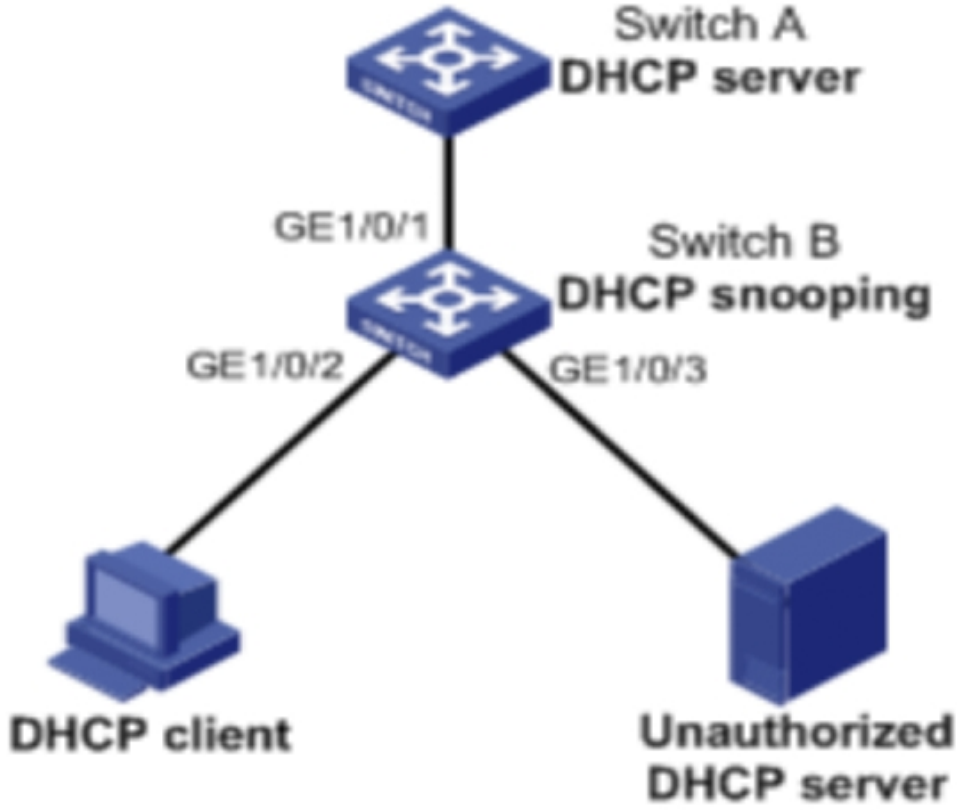
本案例适用于如S5130S-20P-PWR-E、S5130-28TP-PWR-EI等的 V7型号中带有“PWR”的交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comvare V5、V7平台交换机分类说明”。

1.2配置需求

SwitchB通过以太网端口GigabitEthernet1/0/1连接到合法DHCP服务器，通过以太网端口GigabitEthernet1/0/3连接到非法DHCP服务器，通过GigabitEthernet1/0/2连接到DHCP客户端。

要求： 与合法DHCP服务器相连的端口可以转发DHCP服务器的响应报文，而其他端口不转发DHCP服务器的响应报文。记录DHCP-REQUEST报文和信任端口收到的DHCP-ACK报文中DHCP客户端IP地址及MAC地址的绑定信息。

2 组网图



3 配置步骤

3.1设备配置

开启DHCP Snooping功能。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
```

设置GigabitEthernet1/0/1端口为信任端口。

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

[SwitchB-GigabitEthernet1/0/1] dhcp snooping
trust

[SwitchB-GigabitEthernet1/0/1] quit

#保存配置

[SwitchB]save force
```

3.2 验证配置

配置完成后，DHCP客户端只能从合法DHCP服务器获取IP地址和其它配置信息，非法DHCP服务器无法为DHCP客户端分配IP地址和其他配置信息。且使用display dhcp snooping binding可查询到获取到的DHCP Snooping表项。