

交换机 DHCP Snooping 配置案例 (WEB)

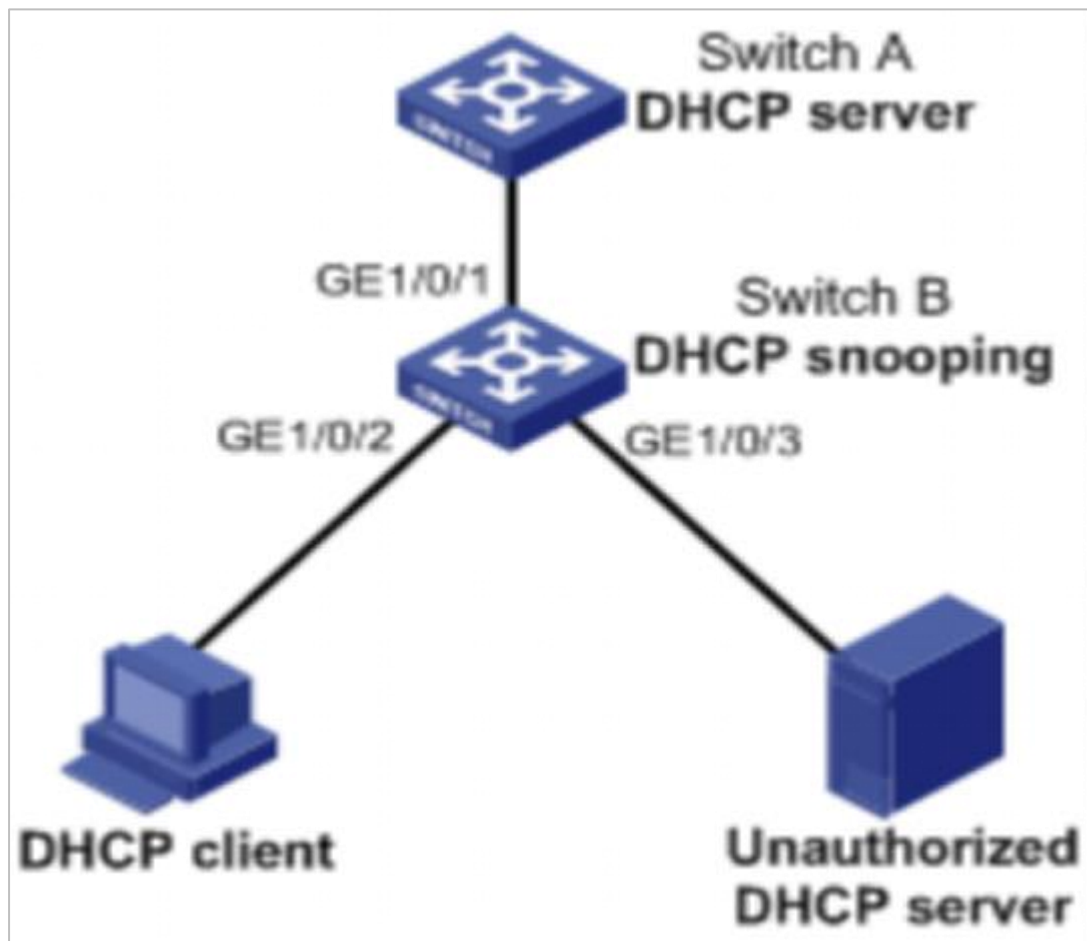
一、配置需求

本案例适用于 US1750、US300S 及以上系列交换机。

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。

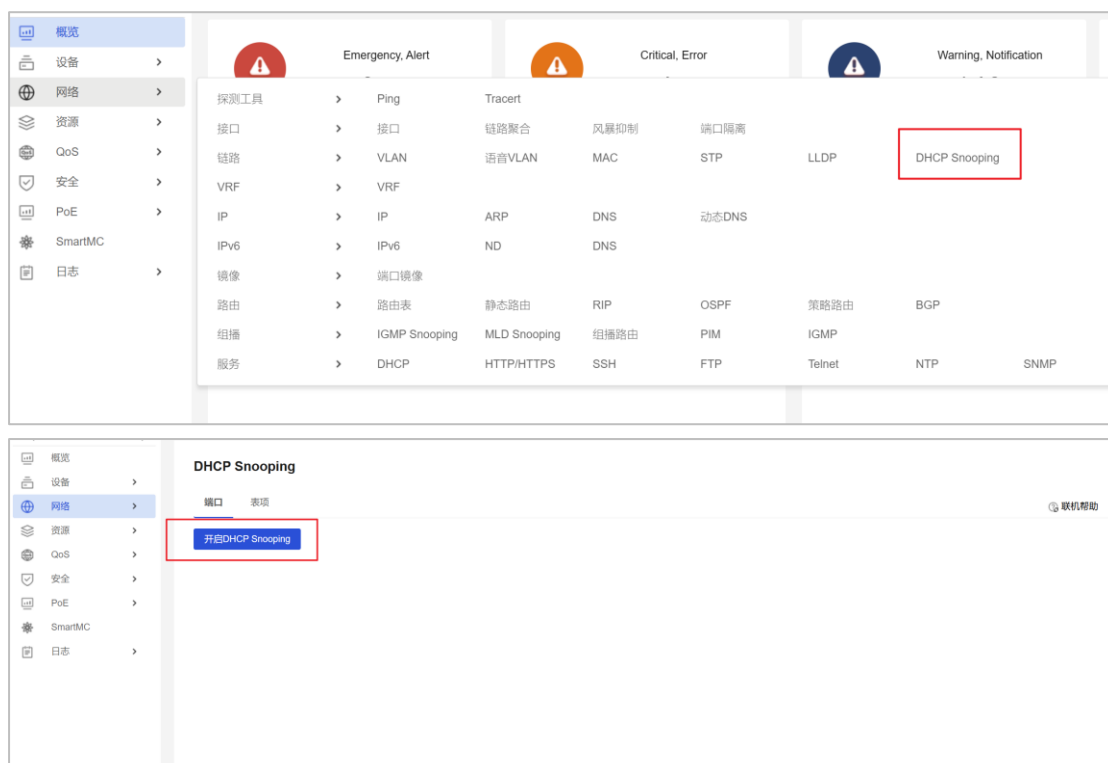
要求: 与合法 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文, 而其他端口不转发 DHCP 服务器的响应报文。记录 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

二、组网图

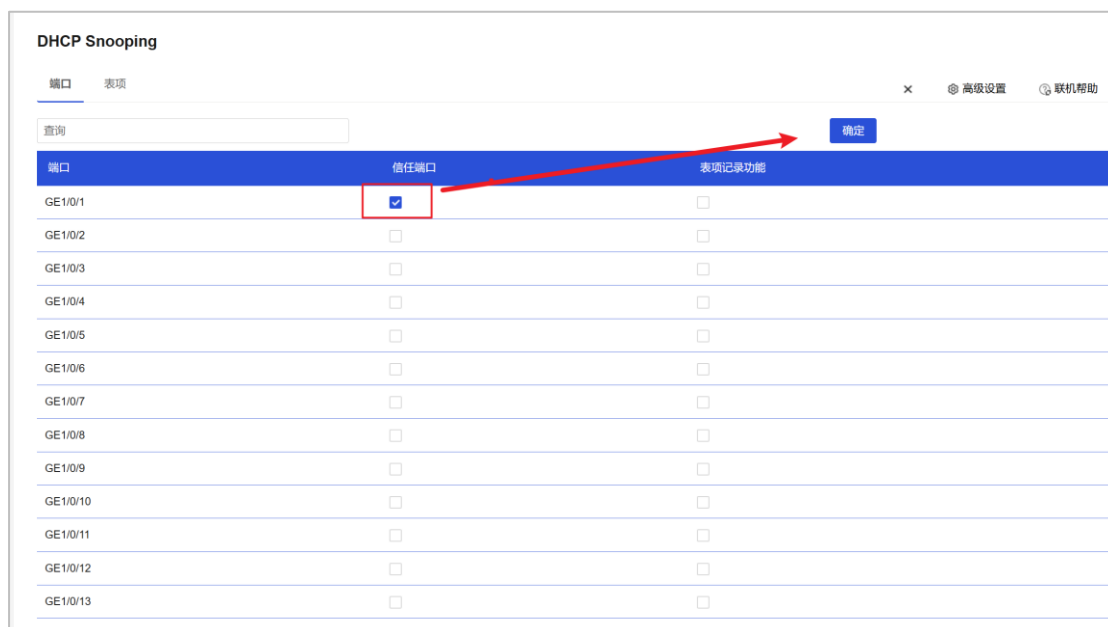


三、配置步骤

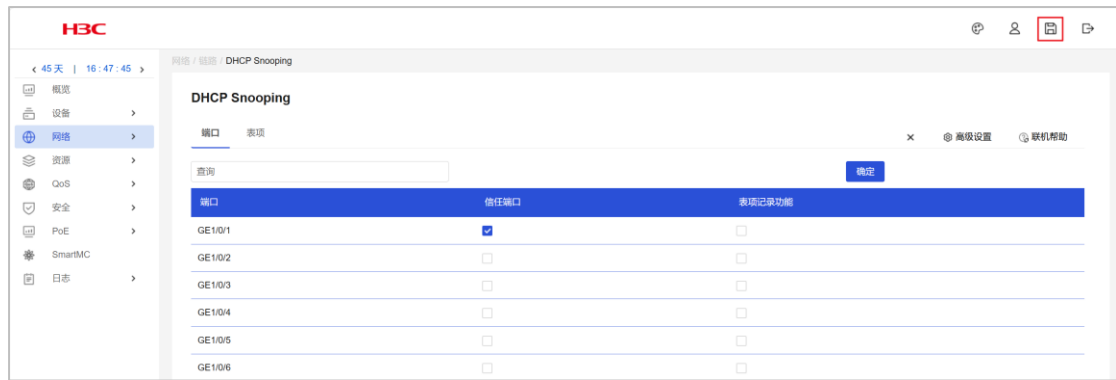
1) 开启 DHCP Snooping 功能。点击导航栏，网络---链路---DHCP Snooping，开启对应功能



2) 选择合法 dhcp 服务器的接口，将该接口设置为信任接口，最后点击确认



3) 保存设备配置



四、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`（需设备支持命令行）可查询到获取到的 DHCP Snooping 表项。