《信息安全及实践》课程实验报告

学院： 信息学院 专业： 计算机科学与技术 年级： 2019

姓名： 赵浩杰 学号： 20191060074
姓名： 李泽昊 学号： 20191060065
姓名： 白文强 学号： 20191060064

实验时间： 2021 年 10 月 29 日

实验名称： 安全端口实验和防 DHCP 欺骗攻击实验

实验成绩：

安全端口实验

一、实验目的

(1)验证交换机端口安全功能配置过程。

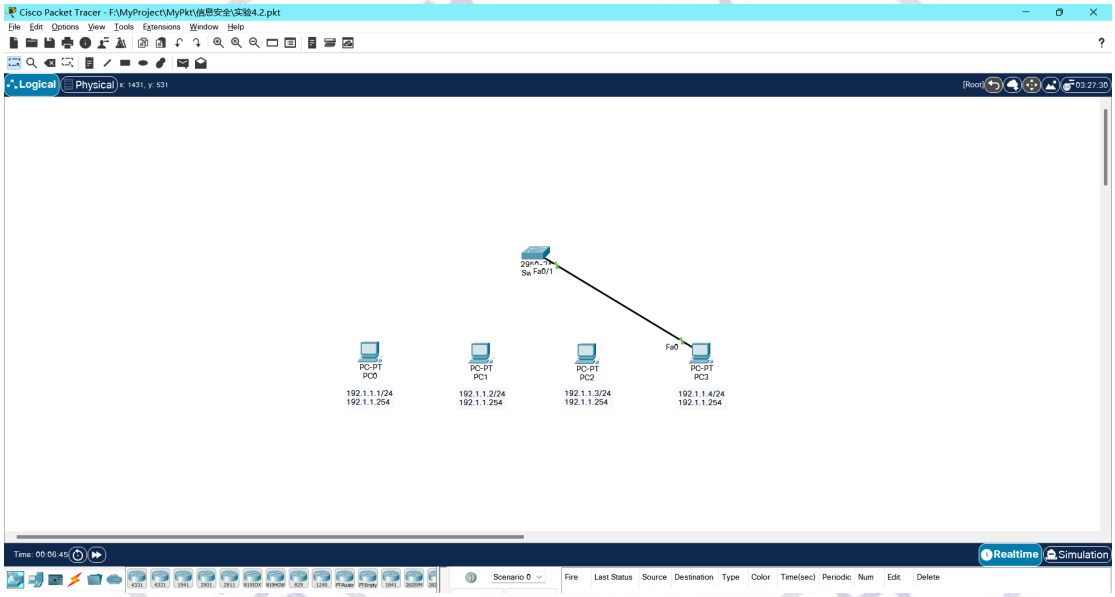
(2)验证访问控制列表自动添加 MAC 地址的过程。

(3)验证对违规接入终端采取的各种动作的含义。

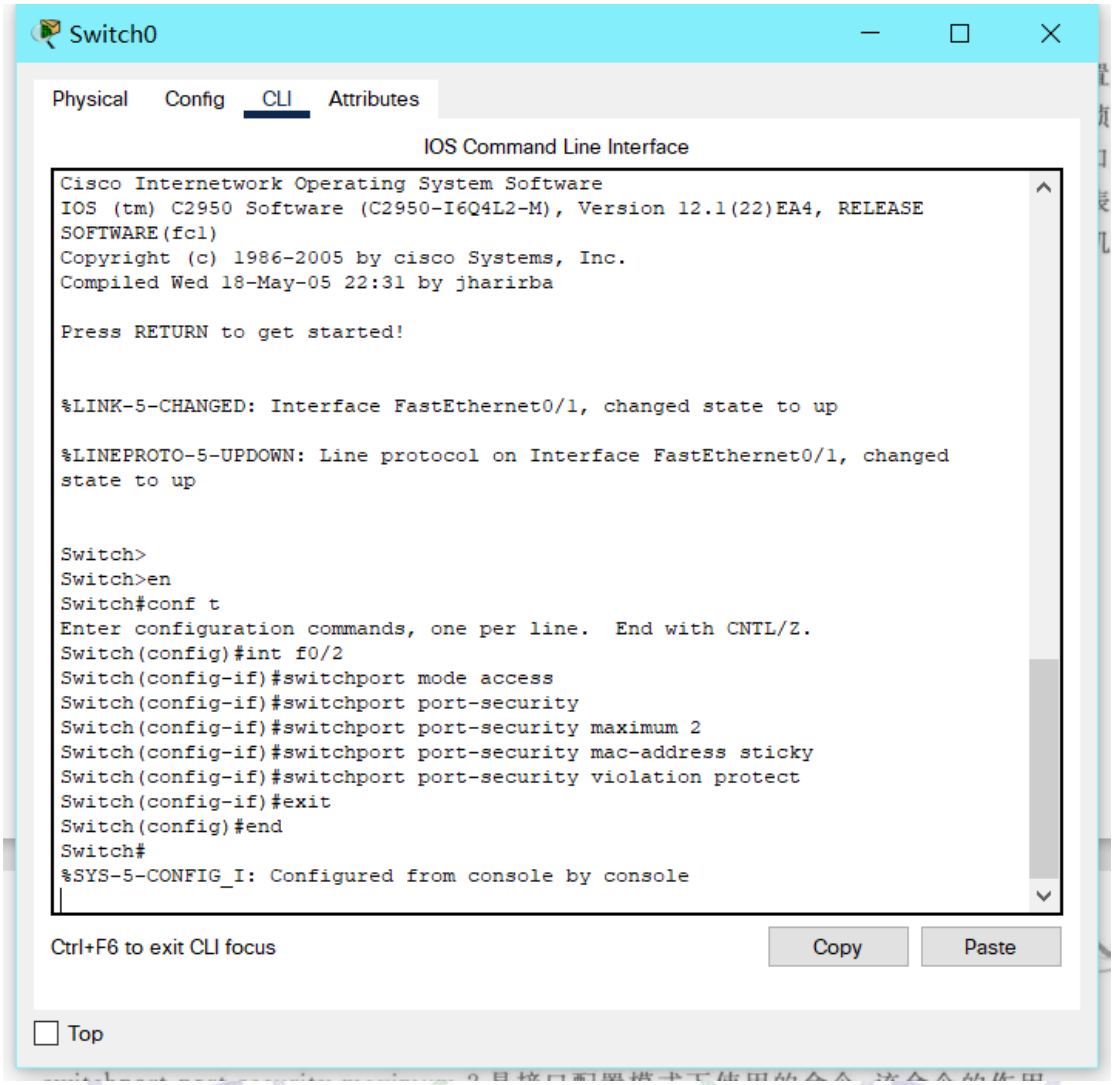
(4)验证安全端口方式下的终端接入控制过程。

二、实验步骤

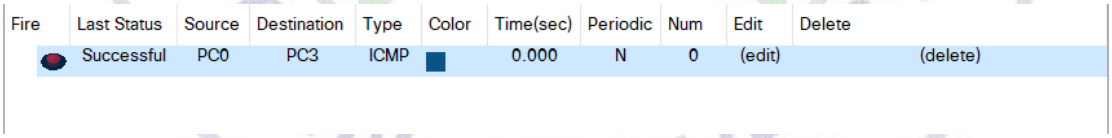
(1) 完成 4 个终端 PC0、PC1、PC2 和 PC3 以及交换机的拓扑图，配置好 4 台终端的网络信息，将 PC3 连接到交换机端口 F0/1；



(2) 完成交换机端口 F0/2 安全功能配置；

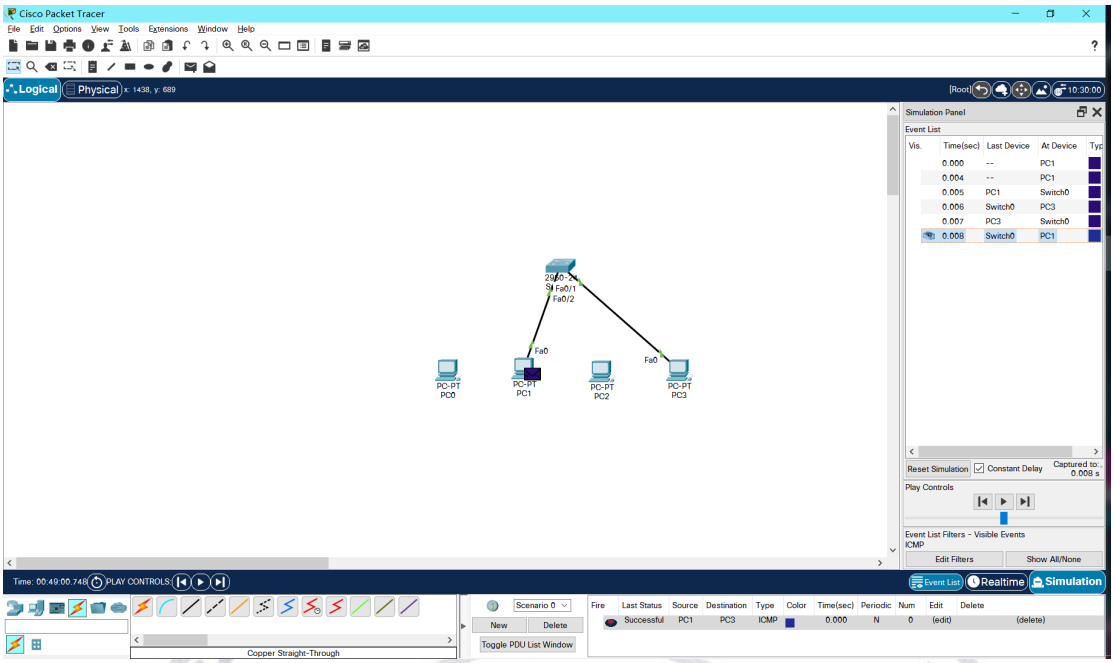


(3) 启动 PC0 与 PC3 之间的 ICMP 报文交换；

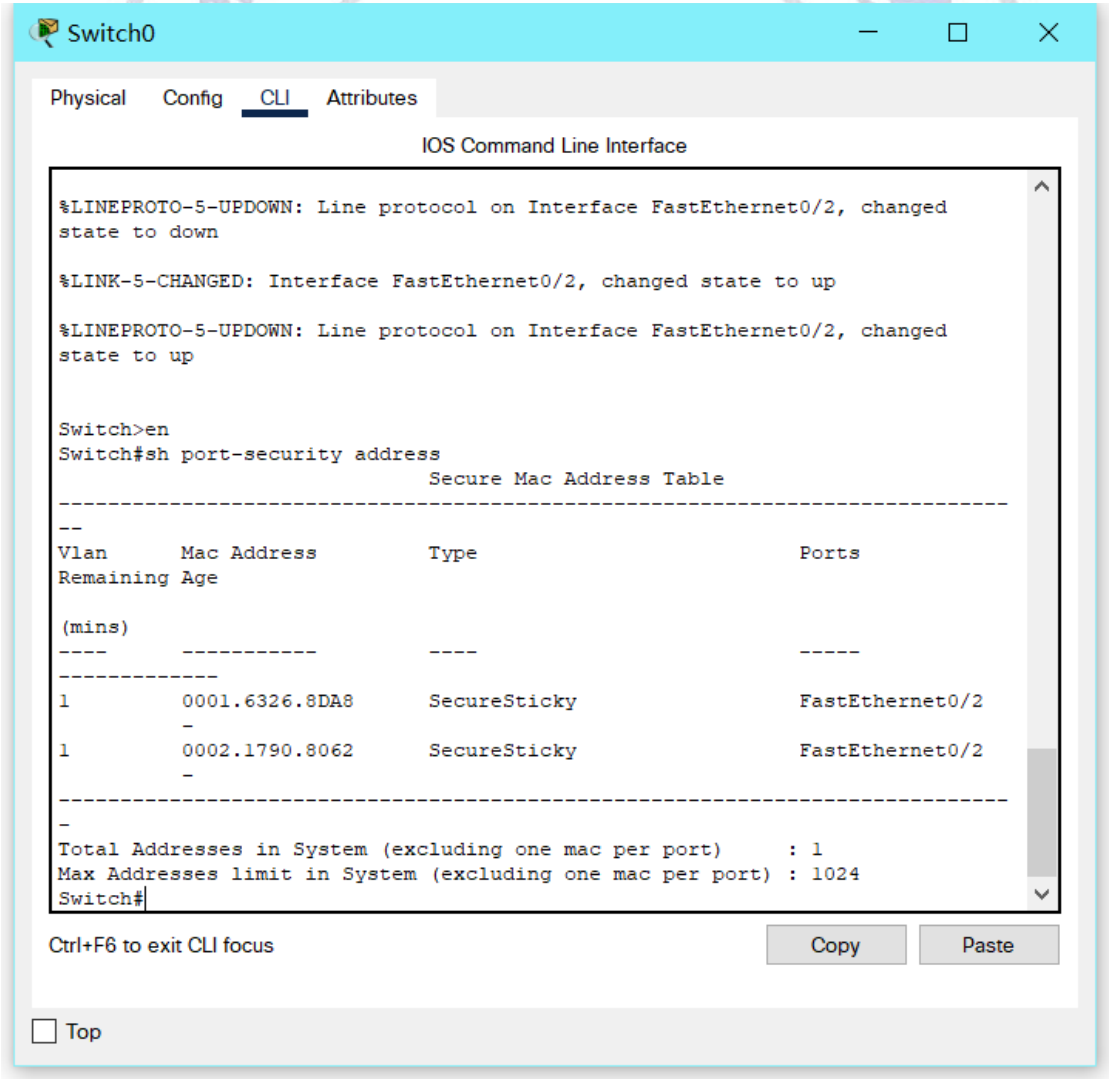


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)	(delete)

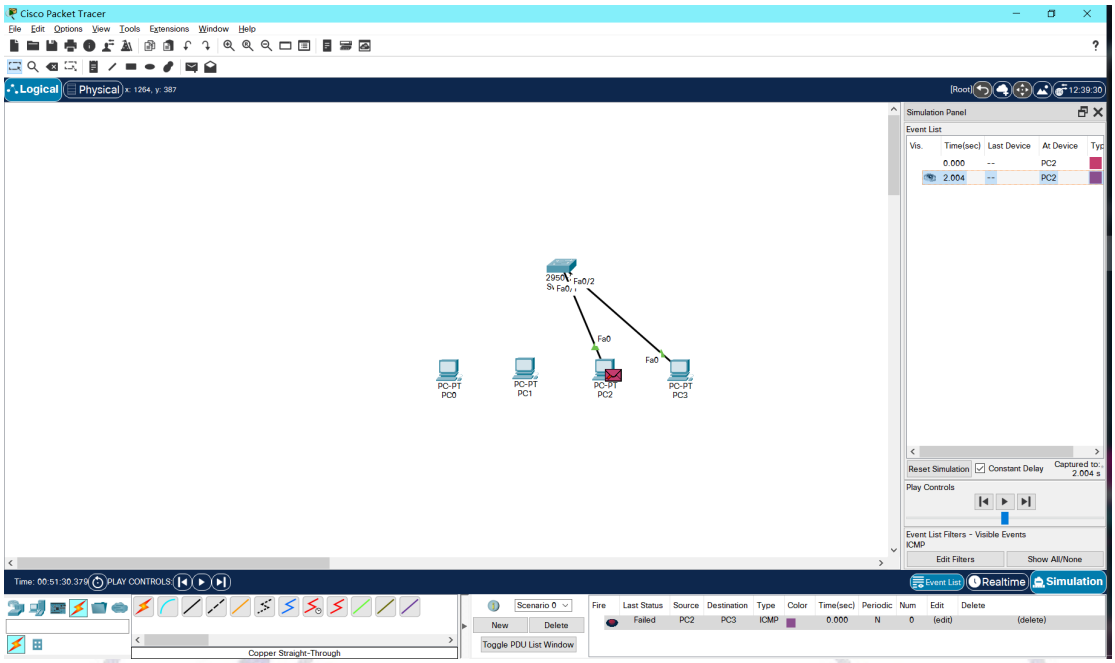
(4) 删除 PC0 与交换机端口 F0/2 的连接，将 PC1 连接到交换机端口 F0/2，启动 PC1 与 PC3 之间的 ICMP 报文交换；



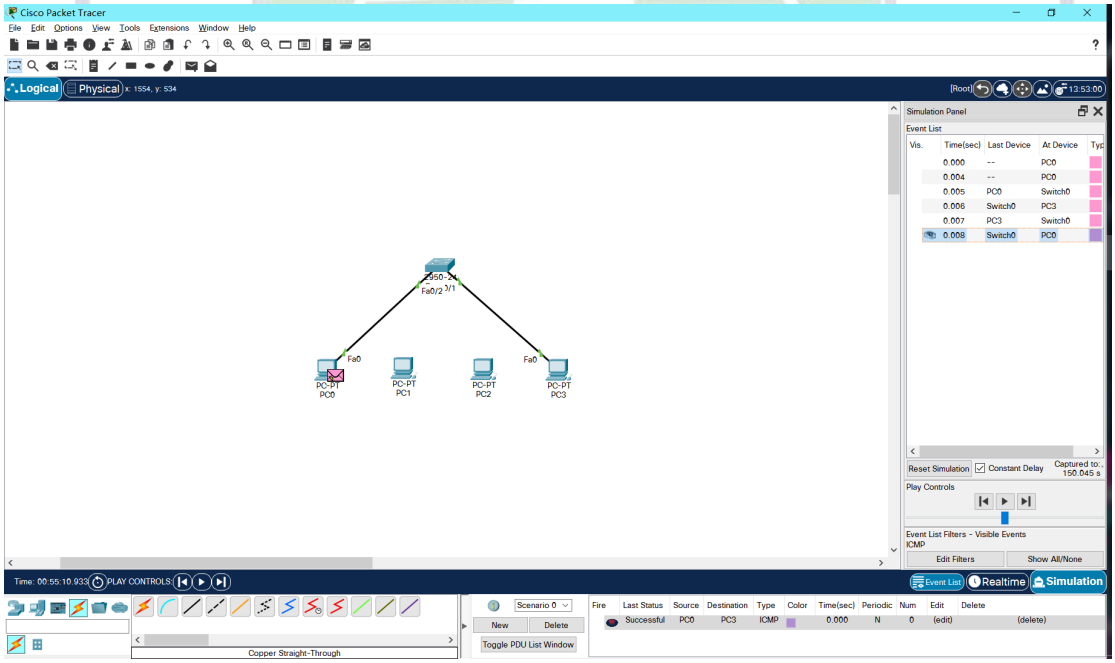
(5) 查看访问控制列表中的 MAC 地址；



(6) 删除 PC1 与交换机端口 F0/2 的连接，将 PC2 连接到交换机端口 F0/2，启动 PC2 与 PC3 之间的 ICMP 报文交换；



(7) 删除 PC2 与交换机端口 F0/2 的连接，重新将 PC0 或 PC1 连接到交换机端口 F0/2，与 PC3 进行 ICMP 报文交换。



三、实验结果及分析

配置过网络信息后，PC0、PC1 与 PC3 交换报文以后，访问控制列表中添加了 PC0、PC1 的 MAC 地址，由于设置的访问控制列表最大 MAC 地址数为 2，所以此时已经达到最大值。所以 PC2 启动与 PC3 交换报文时，MAC 地址不

属于访问控制列表中的 MAC 地址，丢弃该 MAC 帧，PC 2 无法完成与 PC 3 的 ICMP 报文交换。重新连接 PC 0 与 PC1，来自这两个属于访问列表中的 MAC 地址的报文，能成功进行交换。

四、实验总结及体会

如果想控制终端的访问，可以在交换机中进行安全功能配置，限制首先交换 ICMP 报文的终端的 MAC 地址可以加入访问控制列表，并且设置最大 MAC 地址数量，这样只要是计划内的终端先进行报文交换，将 MAC 地址存入访问控制列表并达到最大数量，随后非计划内的终端就无法进行报文交换，MAC 帧会被丢弃，达成控制访问的目的。

防 DHCP 欺骗攻击实验

一、实验目的

(1)验证 DHCP 服务器配置过程。

(2)验证 DNS 服务器配置过程。

(3)验证终端用完全合格的域名访问 Web 服务器的过程。

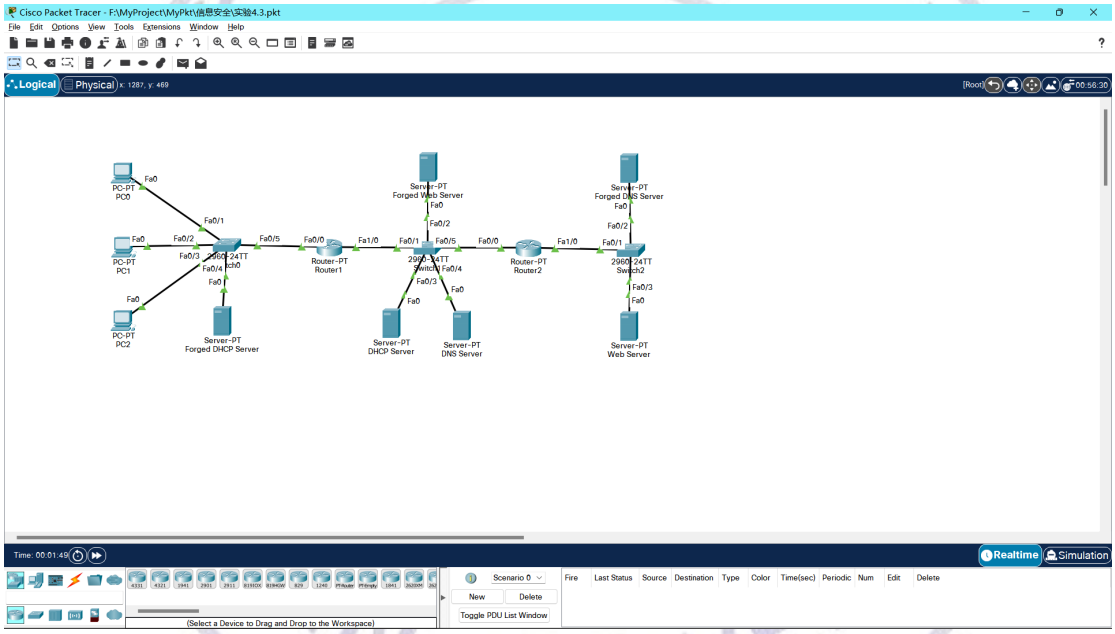
(4)验证 DHCP 欺骗攻击过程。

(5)验证钓鱼网站实施过程。

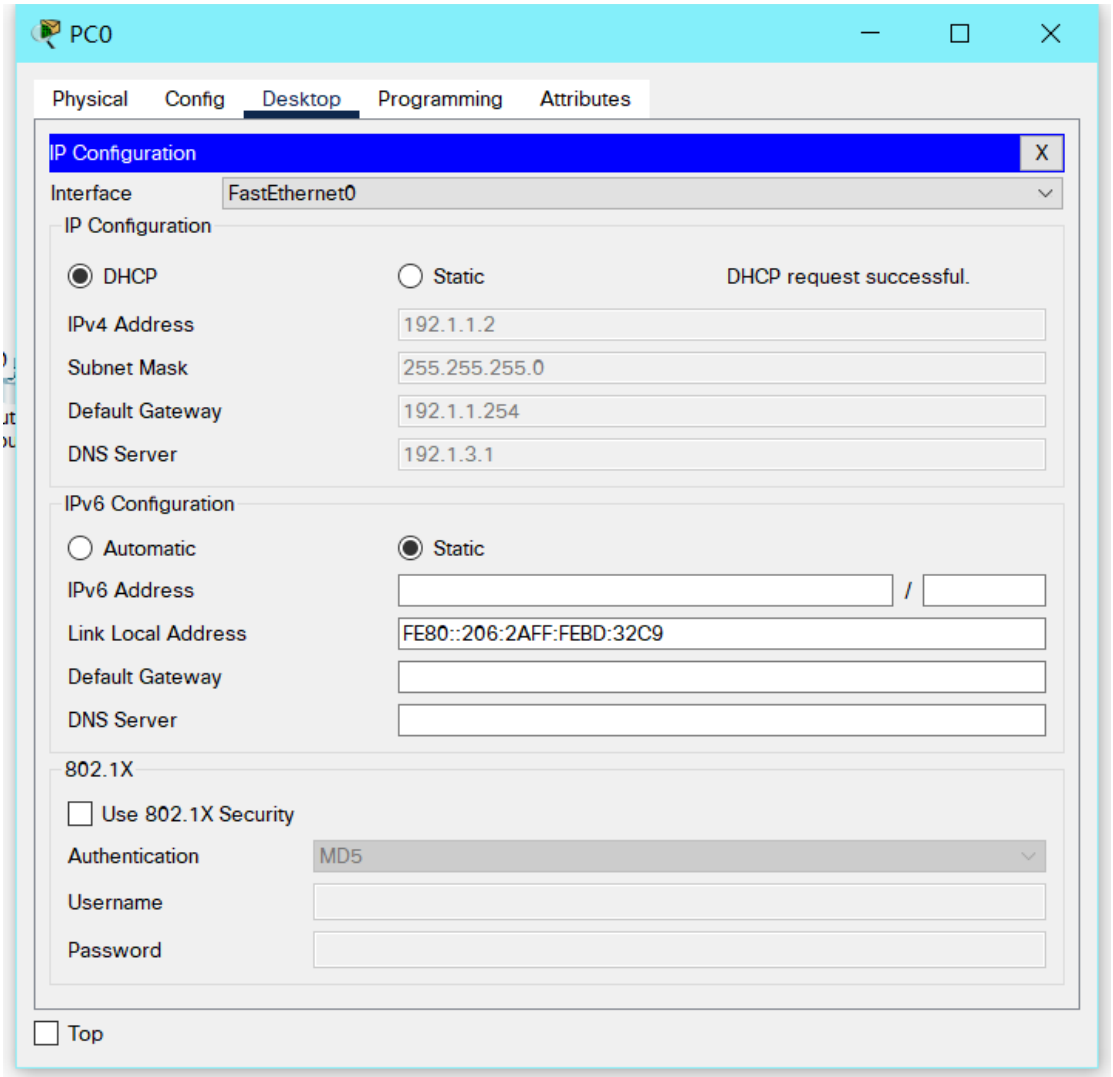
(6)验证交换机防 DHCP 欺骗攻击功能的配置过程。

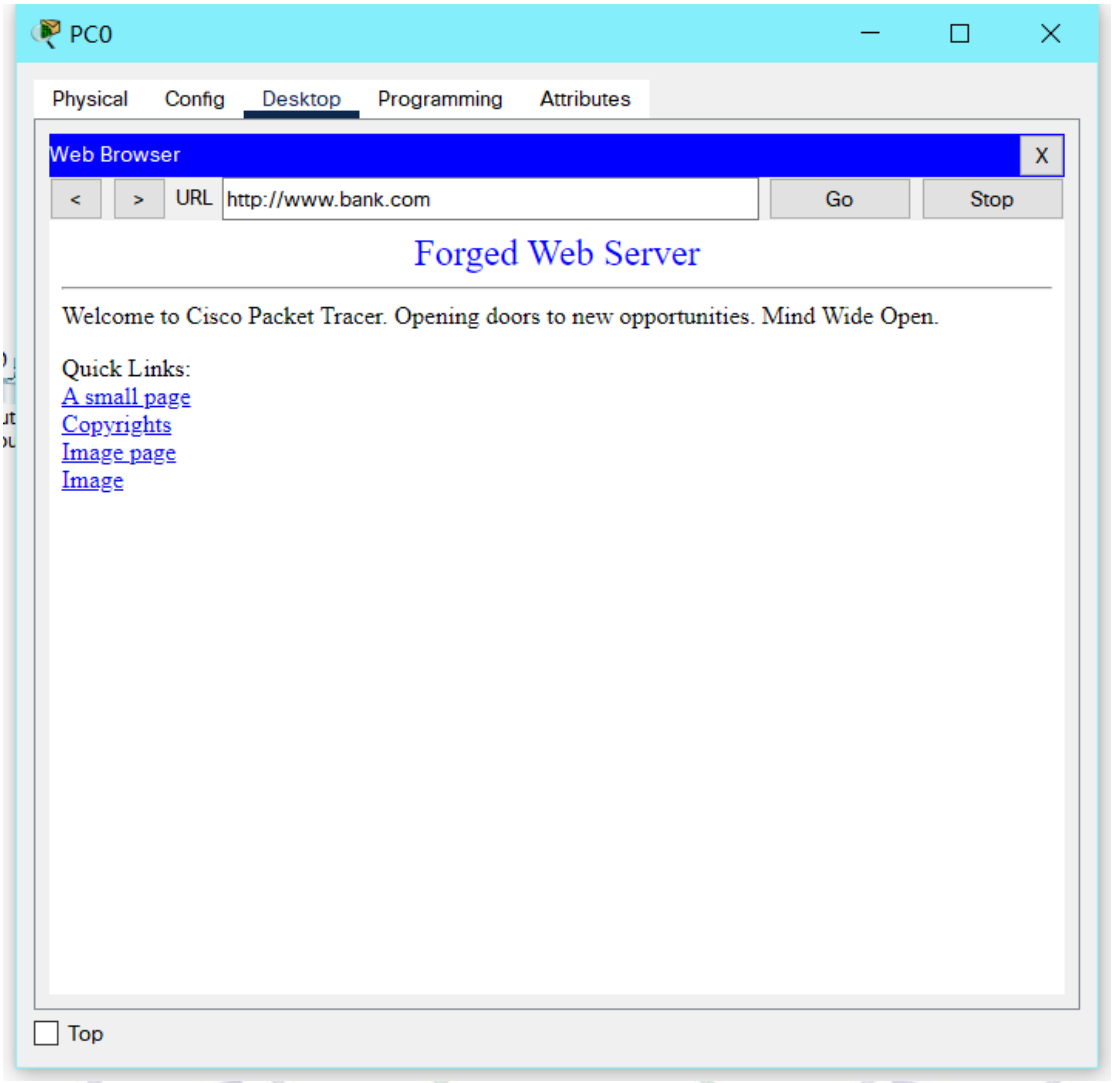
二、实验步骤

(1) 在实验 2.5 的基础上进行，拓扑图为；

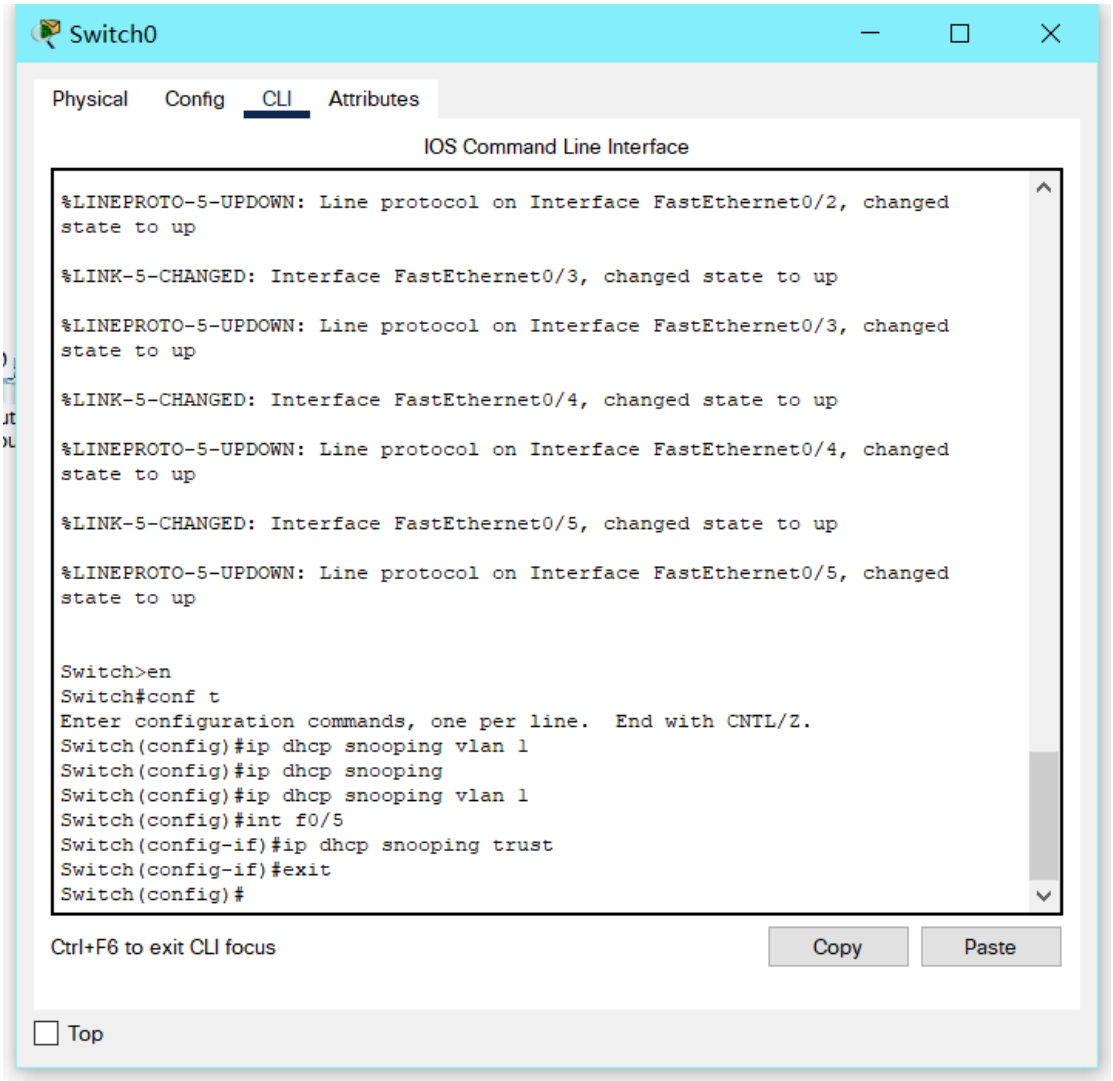


(2) 在启动防 DHCP 欺骗攻击的功能之前，PC0 从伪造的 DHCP 服务器获取网络信息，从而使 PC0 用完全合格的域名 www.bank.com 访问伪造的 Web 服务器；

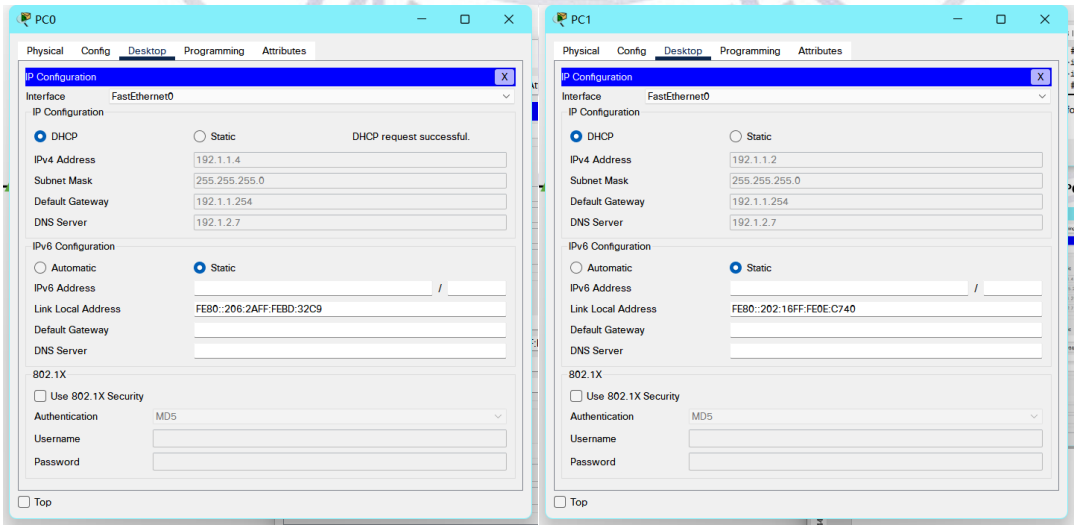

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
192.1.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.1.1.254
DNS Server
192.1.3.1
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::206:2AFF:FEBD:32C9
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

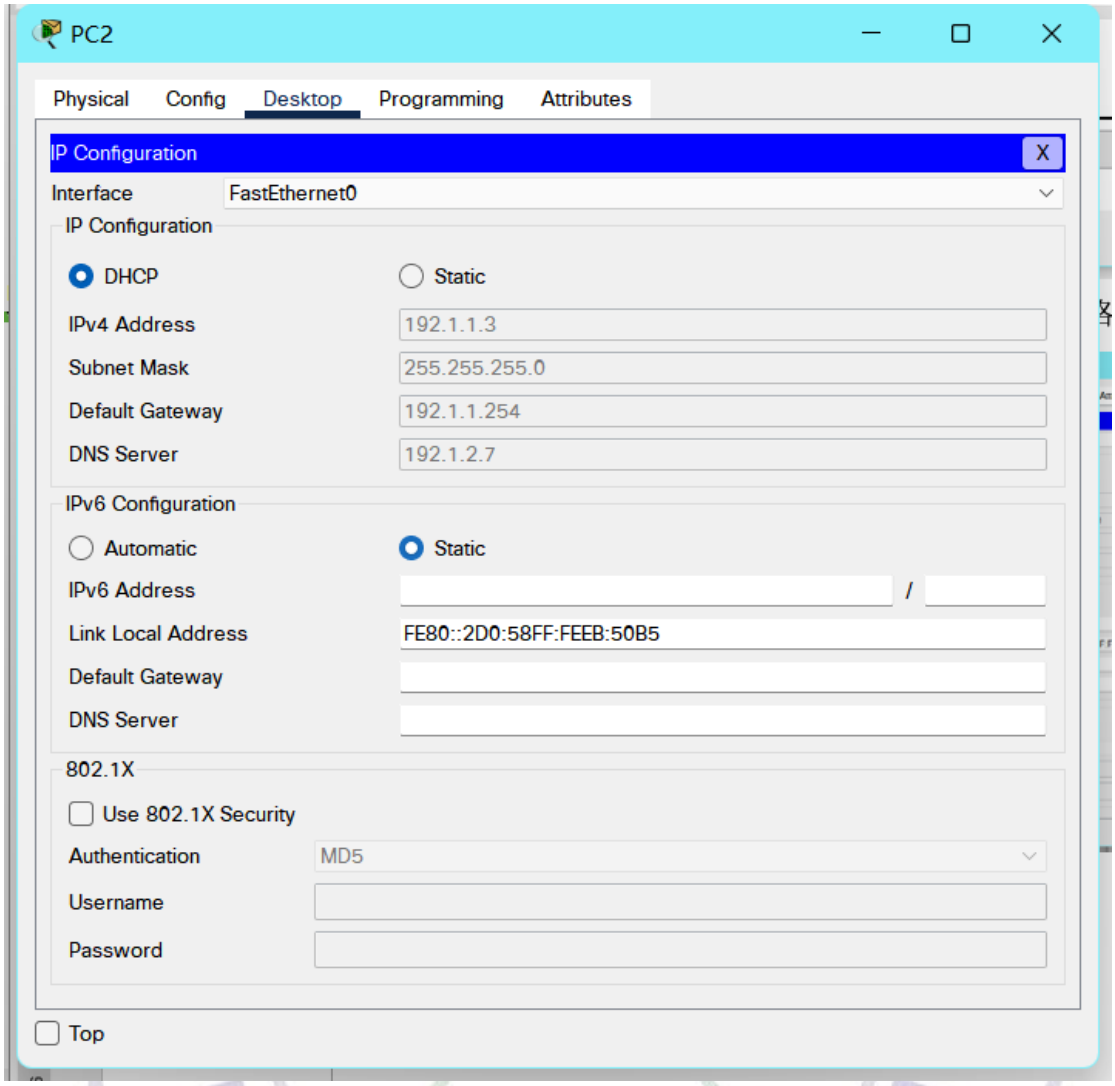


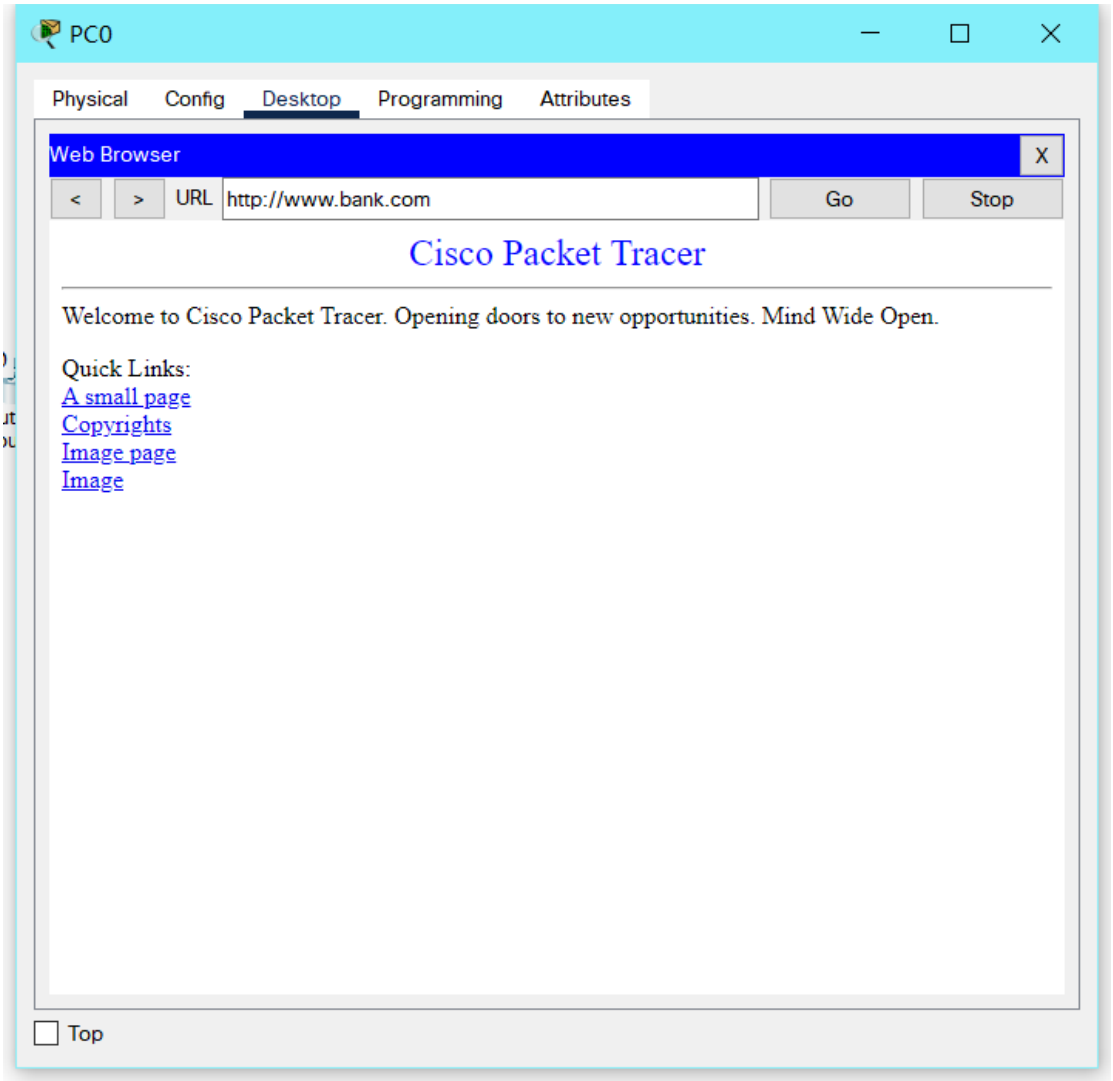
(3) 在交换机中启动防 DHCP 欺骗攻击的功能；



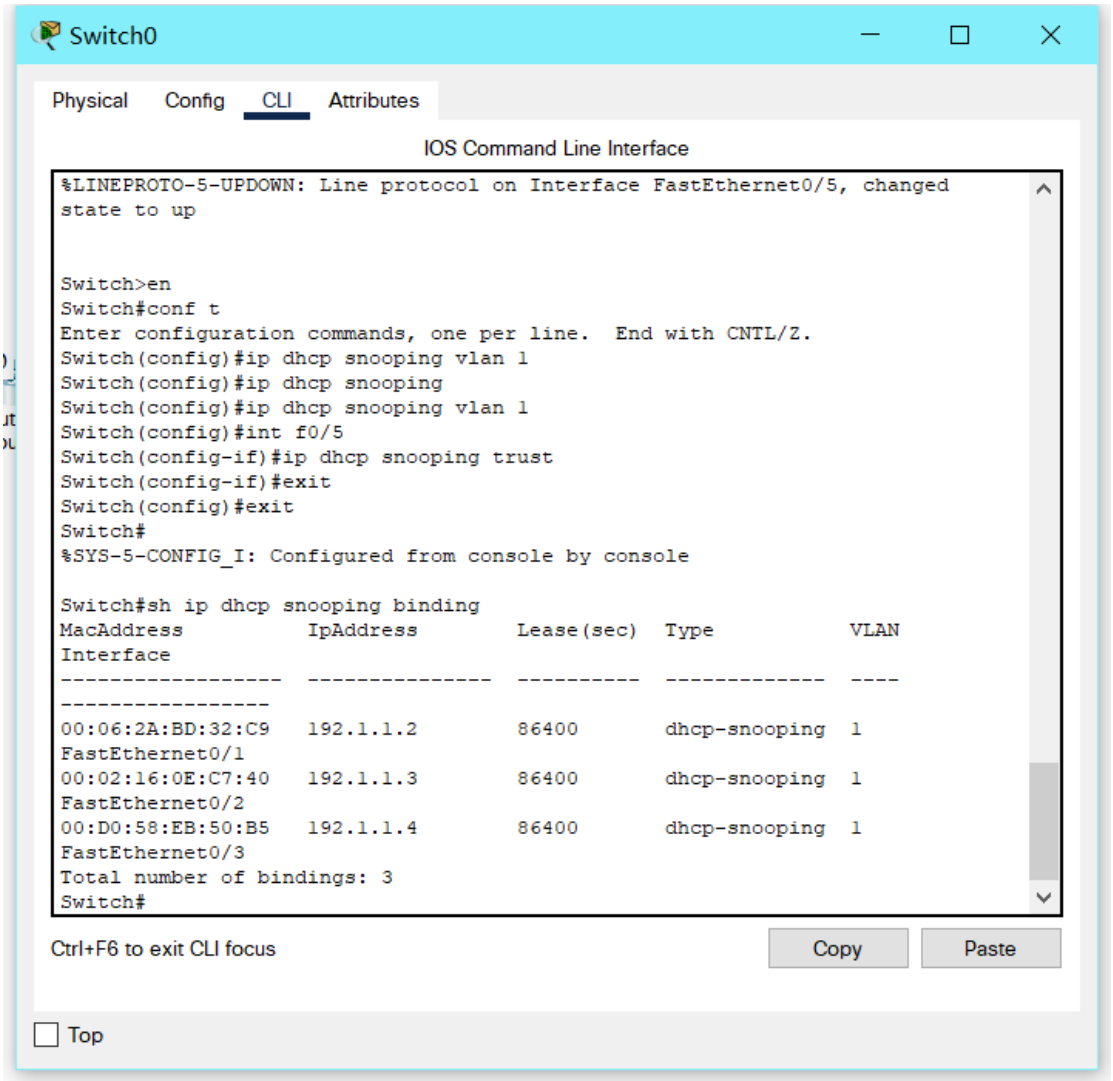
(4) 再次让 PC0、PC1、PC2 通过 DHCP 自动抓取网络信息，得到的 DNS 服务器地址为正确的 192.1.2.7，通过完全合格的域名 www.bank.com 访问正确的 Web 服务器；




PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.1.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.1.1.254
DNS Server
192.1.2.7
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:58FF:FEEB:50B5
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top



(5) 查看交换机 DHCP 帧听信息库的情况；



三、实验结果及分析

实验继用实验 2.5，首先让 PC0 通过 DHCP 自动抓取网络信息，会得到伪造的 DNS 服务器地址，从而访问伪造的 Web 服务器。在交换机中启动防 DHCP 欺骗攻击功能之后，只有连接在信任端口的 DHCP 服务器才能为终端提供自动抓取网络信息的服务，PC 再通过 DHCP 自动抓取网络信息就是得到正确的 DNS 服务器地址，从而访问正确的 Web 服务器。

实验中将连接路由器 R1 的交换机端口设置为信任端口，终端只能接收由路由器 R 1 转发的 DHCP 消息，从而防止了被伪造的 DHCP 服务器进行欺骗攻击。

四、实验总结及体会

这种防御方法通过限制交换机端口的信任与否来控制终端接收的 DHCP 消息来源，攻击者只要无法将伪造的 DHCP 服务器连接在设置信任端口的交换机上，

终端就不会接收来自伪造 DHCP 服务器提供的网络信息，进而保证了用户网络访问的安全性。