实验三 以太网安全实验

1. 访问控制列表实验

1.1 实验内容

如图 1 所示，交换机端口 1 的访问控制列表中静态配置终端 A 的 MAC 地址，交换机其他端口不启动安全功能，将终端 C 接入交换机端口 2。进行以下操作：先将终端 A 接入交换机端口 1，实现终端 A 与终端 C 之间的数据传输过程；再将终端 B 接入交换机端口 1，进行终端 B 与终端 C 之间的数据传输过程，发现交换机端口 1 自动关闭。重新开启交换机端口 1，再将终端 A 接入交换机端口 1，实现终端 A 与终端 C 之间的数据传输过程。

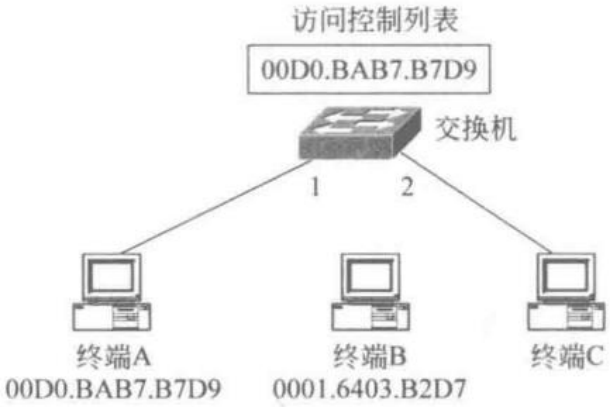


图 1

1.2 实验目的

1) 验证交换机端口静态配置访问控制列表的过程。
2) 验证访问控制列表控制终端接入的过程。
3) 验证关闭端口的重新开启过程。

1.3 实验原理

由于交换机端口 1 的访问控制列表中静态配置了终端 A 的 MAC 地址，因此当终端 A 接入交换机端口 1 且向交换机端口 1 发送 MAC 帧时，MAC 帧的源 MAC 地址与访问控制列表中的 MAC 地址相同，交换机继续转发该 MAC 帧。当终端 B 接入交换机端口 1 且向交换机端口 1 发送 MAC 帧时，由于 MAC 帧的源 MAC 地址与访问控制列表中的 MAC 地址不同，因此交换机丢弃该 MAC 帧，并关闭交换机端口 1。需要通过特殊的命令序列才能重新开启交换机端口 1。

1.4 实验步骤

1. 完成 3 个终端 PC0、PC1 和 PC2 的网络信息配置过程。将 PC2 连接到交换机端口 FastEthernet0/2。在 CLI(命令行接口)配置方式下，完成交换机端口 FastEthernet0/1 安全功能配置过程，在访问控制列表中静态配置 PC0 的 MAC 地址，如图 2 所示。将 PC0 连接到交换机端口 FastEthernet0/1。完成设备放置和连接后的逻辑工作区界面如图 3 所示。

```
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switch
Switch(config-if)#switchport  mode access
Switch(config-if)#swit
Switch(config-if)#switchport  port-sec
Switch(config-if)#switchport  port-security
Switch(config-if)#switch
Switch(config-if)#switchport port
Switch(config-if)#switchport port-security max
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-
Switch(config-if)#switchport port-security mac-address
000A.F3CD.E91A
Switch(config-if)#switchport port-security vio
Switch(config-if)#switchport port-security violation shu
Switch(config-if)#switchport port-security violation
shutdown
Switch(config-if)#exit
```

图 2

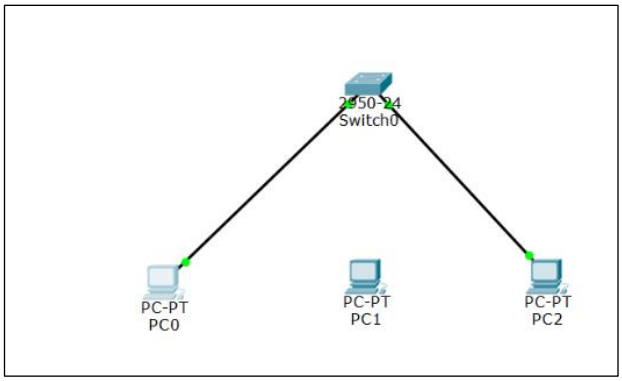


图 3

2. 启动 PC0 与 PC2 之间的 ICMP 报文交换过程。PC0 和 PC2 之间能够成功交换 ICMP 报文，如图 4 所示。

```
Packet Tracer PC Command Line 1.0
PC>ping 192.1.1.3

Pinging 192.1.1.3 with 32 bytes of data:

Reply from 192.1.1.3: bytes=32 time=81ms TTL=128
Reply from 192.1.1.3: bytes=32 time=0ms TTL=128
Reply from 192.1.1.3: bytes=32 time=0ms TTL=128
```

图 4

3. 删除 PC0 与交换机端口 FastEthernet0/1 之间的连接，将 PC1 连接到交换机端 FastEthernet0/1。完成设备连接后的逻辑工作区界面如图 5 所示。

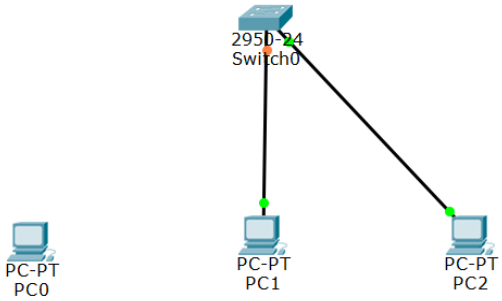


图 5

4. 启动 PC1 与 PC2 之间的 ICMP 报文交换过程，导致交换机端口 FastEthernet0/1 关闭，查看交换机端口状态 port status 为未开启状态。
5. 通过在交换机端口 FastEthernet0/1 对应的接口配置模式下执行命令 shutdown 和 no shutdown 重新开启交换机端口 FastEthernet0/1，开启命令如图 6 所示，只有当 PC0 接入该交换机端口时，才能正常传输 MAC 帧，再次查看交换机端口状态变为开启。

```
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
Switch(config-if)#no
Switch(config-if)#no shut
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to up
```

图 6

2.安全端口实验

2.1 实验内容

如图 7 所示，将交换机端口 1 设置为安全端口，自动将先学习到的两个 MAC 地址添加到访问控制列表中。交换机其他端口不启动安全功能。将终端 D 接入交换机端口 2。进行以下操作：先将终端 A 接入交换机端口 1，实现终端 A 与终端 D 之间的数据传输过程，此时终端 A 的 MAC 地址自动添加到访问控制列表中；然后将终端 B 接入交换机端口 1，实现终端 B 与终端 D 之间的数据传输过程，此时终端 B 的 MAC 地址自动添加到访问控制列表中(添加两个 MAC 地址后的访问控制列表如图 7 所示)；再将终端 C 接入交换机端口 1，进行终端 C 与终端 D 之间的数据传输过程，由于该 MAC 帧的源 MAC 地址不在访问控制列表中，且访问控制列表中的 MAC 地址数已经达到最大 MAC 地址数 2，交换机丢弃该 MAC 帧。如果再将终端 A 接入交换机端口 1，依然可以实现终端 A 与终端 D 之间的数据传输过程。

图 7

2.2 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。

2.3 实验原理

由于交换机端口 1 设置为安全端口，且将访问控制列表中的最大 MAC 地址数设置为 2，因此，当分别将终端 A 和终端 B 接入交换机端口 1，且向交换机端口 1
发送 MAC 帧后，访问控制列表中已经添加终端 A 和终端 B 的 MAC 地址。当终端 C 接入交换机端口 1 且向交换机端口 1 发送 MAC 帧时，由于 MAC 帧的源 MAC 地址不属于访问控制列表中的 MAC 地址，且访问控制列表中的 MAC 地址数已经达到最大地址数 2，因此，交换机丢弃该 MAC 帧。

2.4 实验步骤

1. 完成 4 个终端 PC0、PC1、PC2 和 PC3 的网络信息配置过程。将 PC3 连接到交换机端口 FastEthernet0/2。在 CLI(命令行接口）配置方式下，完成交换机端口 FastEthernet0/1 安全功能配置过程，如图 9 所示。将 PC0 连接到交换机端口 FastEthernet0/1。完成设备放置和连接后的逻辑工作区界面如图 8 所示。

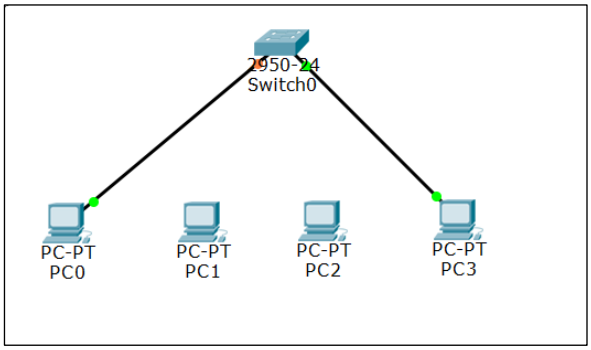


图 8

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switch mode access
Switch(config-if)#switch
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security  max
Switch(config-if)#switchport port-security  maximum 2
Switch(config-if)#switchport port-security  mac
Switch(config-if)#switchport port-security  mac-address
st
Switch(config-if)#switchport port-security  mac-address
sticky
Switch(config-if)#switchport port-security  vio
Switch(config-if)#switchport port-security  violation rop
Switch(config-if)#switchport port-security  violation
protect
Switch(config-if)#exit
```

图 9

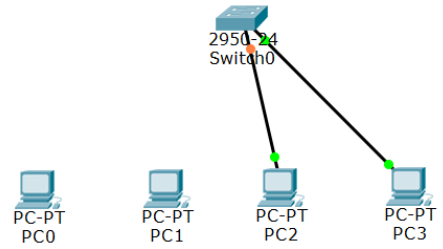
2. 启动 PC0 与 PC3 之间的 ICMP 报文交换过程。PC0 和 PC3 之间能够成功交换 ICMP 报文。
3. 删除 PC0 与交换机端口 FastEthernet0/1 之间的连接，将 PC1 连接到交换机端口 FastEthernet0/1，启动 PC1 与 PC3 之间的 ICMP 报文交换过程。PCl 和 PC3 之间能够成功交换 ICMP 报文。
4. 查看访问控制列表中的 MAC 地址，如图 10 所示，访问控制列表中已经存在 PC0 和 PC1 的 MAC 地址。

```
Switch#show port-security address
                          Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports           Remaining Age
                                                                  (mins)
----    -----------       ----                  -----           -------------
1       000B.BECE.CA7D    SecureSticky          FastEthernet0/1         -
1       00D0.FF03.7590    SecureSticky          FastEthernet0/1         -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
```

图 10

5. 删除 PC1 与交换机端口 FastEthernet0/1 之间的连接，将 PC2 连接到交换机端口 FastEthernet0/1，启动 PC2 与 PC3 之间的 ICMP 报文交换过程，如图 11 所示，PC2 和 PC3 之间无法交换 ICMP 报文，但交换机端口 FastEthernet0/1 的工作状态没有发生变

化。如果再次将 PC0 或 PC1 连接到交换机端口 FastEthernet0/1，则依然能够与 PC3 成功交换 ICMP 报文，如图 12 所示。



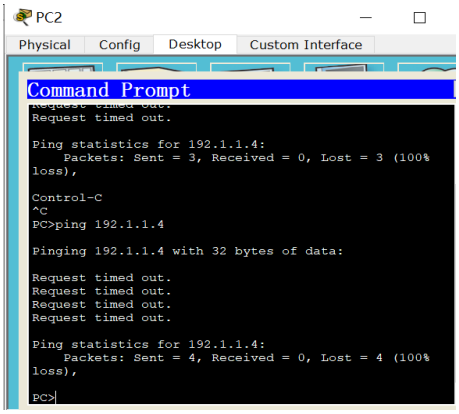
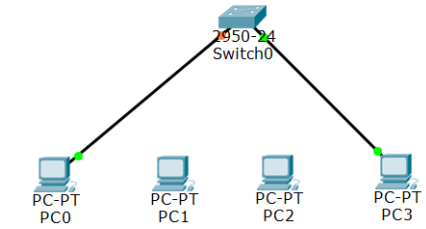


图 11



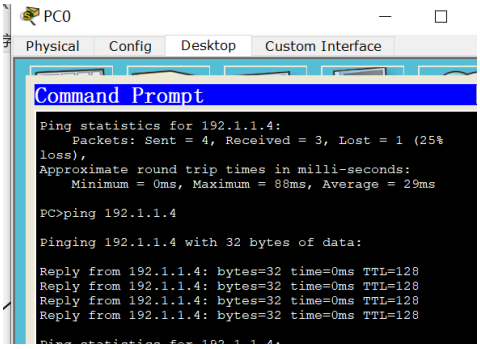


图 12

3. 防 DHCP 欺骗攻击实验

3.1 实验内容

图 13 所示是黑客实施钓鱼网站的常见手段。黑客通过在网络中接入伪造的 DHCP 服务器、伪造的 DNS 服务器和伪造的 Web 服务器，使用户用正确的完全合格的域名 www.bank.com 访问黑客伪造的 Web 服务器。

如图 13 所示的钓鱼网站实施过程中，使用户用正确的完全合格的域名 www.bank.com 访问黑客伪造的 Web 服务器的关键是，终端从伪造的 DHCP 服务器中获取网络信息。通过接入伪造的 DHCP 服务器使终端从伪造的 DHCP 服务器中获取网络信息的过程称为 DHCP 欺骗攻击。因此，成功实施 DHCP 欺骗攻击是成功实施如图 13 所示的钓鱼网站的基础。

在交换机中启动防 DHCP 欺骗攻击功能，在接入伪造的 DHCP 服务器的情况下，保证终端只从 DHCP 服务器获取网络信息。

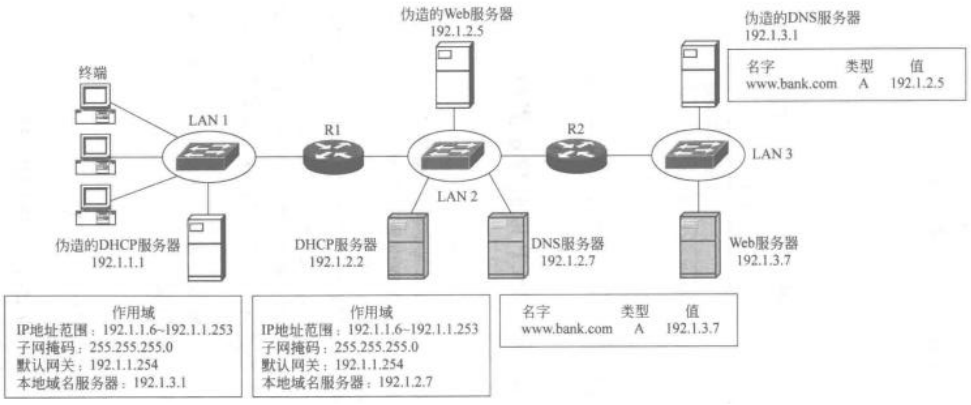


图 13

3.2 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。

3.3 实验原理

终端通过 DHCP 自动获取的网络信息中包含本地域名服务器地址，对于如图 13 所示的网络应用系统，终端通过 DHCP 自动获取的网络信息中包含本地域名服务器地址，对于如图 13 所示的网络应用系统，DHCP 服务器中给出的本地域名服务器地址是 192.1.2.7，地址

为 192.1.2.7 的域名服务器中与完全合格的域名 www.bank.com 绑定的 Web 服务器地址是 192.1.3.7。因此，终端可以用完全合格的域名 www.bank.com 访问 Web 服务器。

一旦终端连接的网络中接入伪造的 DHCP 服务器，终端很可能从伪造的 DHCP 服务器获取网络信息，得到伪造的域名服务器的 IP 地址 192.1.3.1，伪造的域名服务器中将完全合格的域名 www.bank.com 与伪造的 Web 服务器的 IP 地址 192.1.2.5 绑定在一起，导致终端用完全合格的域名 www.bank.com 访问伪造的 Web 服务器。

如果交换机启动防 DHCP 欺骗攻击的功能，只有连接在信任端口的 DHCP 服务器才能为终端提供自动配置网络信息的服务。因此，对于如图 13 所示的实施 DHCP 欺骗攻击的网络应用系统，连接终端的以太网中，如果只将连接路由器 R1 的交换机端口设置为信任端口，将其他交换机端口设置为非信任端口，则终端只能接收由路由器 R1 转发的 DHCP 消息，使终端只能获取 DHCP 服务器提供的网络信息。

3.4 实验步骤

1) 该实验在实验一中的钓鱼网站实验基础上进行。根据如图 13 所示的钓鱼网站实施过程完成设备放置和连接，完成设备放置和连接后的逻辑工作区界面如图 14 所示。

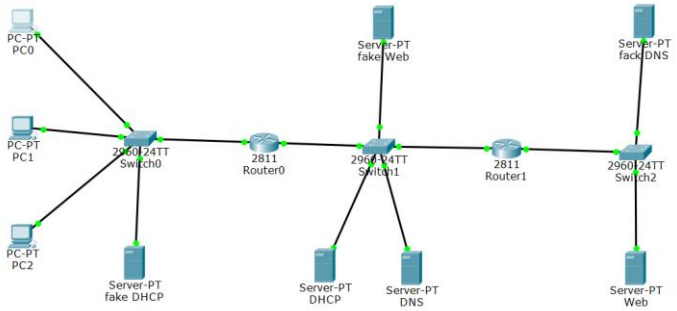


图 14

2) 在启动交换机 Switch0 防 DHCP 欺骗攻击的功能前，PC0 很可能从伪造的 DHCP 服务器获取网络信息，如图 15 所示，得到的 DNS 服务器地址是伪造的 DNS 服务器的 IP 地址 192.1.3.1，从而使 PC0 用完全合格的域名 www.bank.com 访问伪造的 Web 服务器，如图 16 所示。

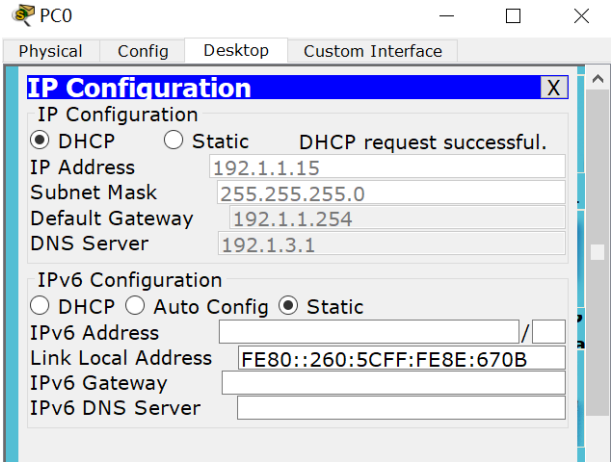


图 15

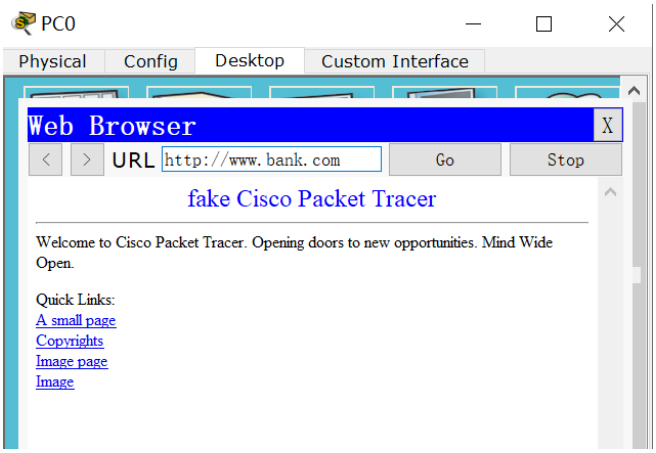


图 16

3) 在 Switch0 CLI(命令行接口)下输入用于启动交换机防 DHCP 欺骗攻击的功能的命令序列，需要说明的是交换机端口 FastEthernet0/4 是图 14 中交换机 Switch0 连接路由器 Router0 的端口，如图 17 所示。让 PC0、PC1、PC2 再次通过 DHCP 自动获取网络信息，发现 PC0、PC1、PC2 只从 DHCP 服务器获取网络信息。如图 18 所示，PC0 得到的 DNS 服务器地址是正确的 DNS 服务器的 IP 地址 192.1.2.7，从而使 PC0 用完全合格的域名 www.bank. com 访问正确的 Web 服务器，如图 19 所示。

```
Switch>enable
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#ip dhcp snoo
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping  vlan1
                                 ^
% Invalid input detected at '^' marker.

Switch(config)#ip dhcp snooping  vlan 1
Switch(config)#interface Fa
Switch(config)#interface FastEthernet 0/4
Switch(config-if)#ip dhcp snooping  trust
Switch(config-if)#exit
Switch(config)#
```

图 17

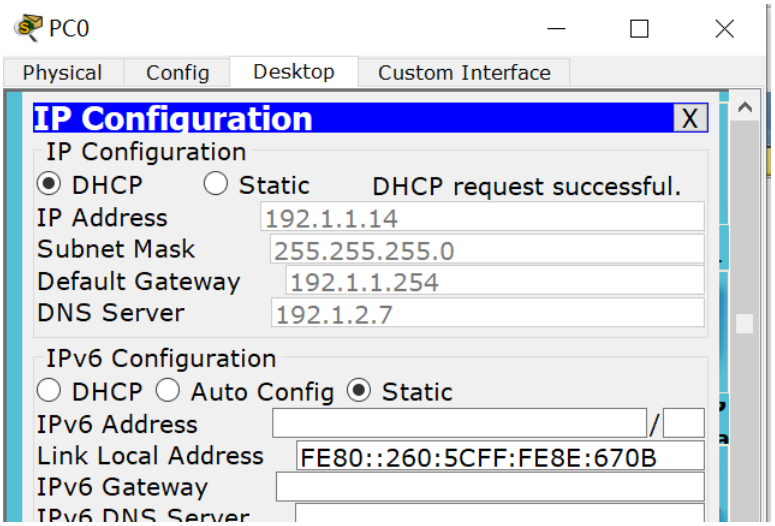


图 18

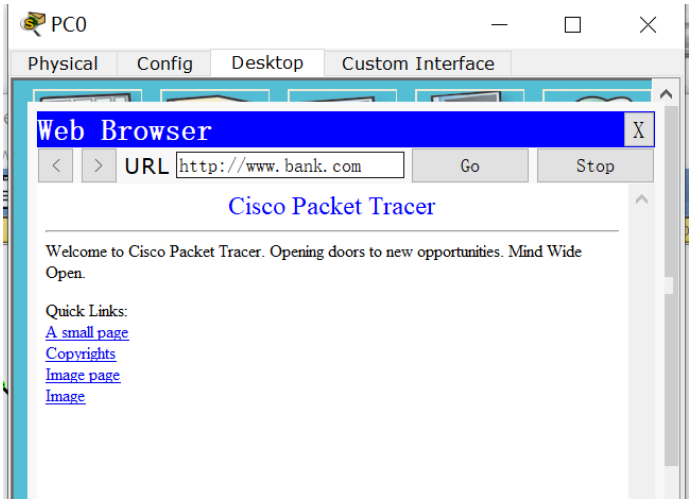


图 19

4) 显示 Switch0 的 DHCP 侦听信息库，得到以下三者之间的绑定关系：一是 Switch0 连接 PC0、PC1、PC2 的交换机端口；二是 PC0、PC1、PC2 的 MAC 地址；三是 DHCP 服务器分配给 PC0、PC1、PC2 的 IP 地址。如图 20 所示，FastEthernet0/1 是 Switch0 连接 PC0 的端口，00：60：5C：8E：67：0B 是 PC0 的 MAC 地址，192.1.1.14 是 DHCP 服务器分配给 PC0 的 IP 地址。

```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:60:5C:8E:67:0B   192.1.1.14       86400       dhcp-snooping  1     FastEthernet0/1
00:0A:F3:B3:B8:10   192.1.1.15       86400       dhcp-snooping  1     FastEthernet0/2
00:0C:85:21:30:88   192.1.1.16       86400       dhcp-snooping  1     FastEthernet0/3
Total number of bindings: 3
Switch#
```

图 20