实验一 网络攻击实验

1. 集线器和嗅探攻击实验

1.1 实验内容

正常网络结构如图 1(a)所示，终端 A 和终端 B 连接在交换机上，交换机和路由器相连，终端 A 和终端 B 可以通过交换机向路由器发送 MAC 帧。如果黑客需要嗅探终端 A 和终端 B 发送给路由器的 MAC 帧，可以在路由器和交换机之间插入一个集线器，并在集线器上连接一个黑客终端，如图 1(b)所示。这种情况下，黑客终端可以嗅探所有终端 A 和终端 B 与路由器之间传输的 MAC 帧。

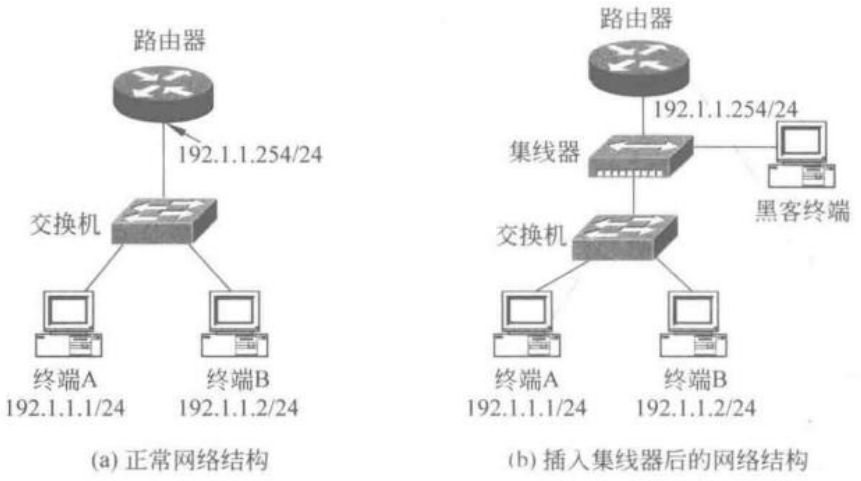


图 1

1.2 实验目的

（1）验证利用集线器实施嗅探攻击的过程。

（2）验证嗅探攻击不会影响正常的 MAC 帧传输过程。

（3）验证嗅探攻击对于源和目的终端是透明的。

1.3 实验原理

集线器是广播设备，从某个端口接收到 MAC 帧后除了接收该 MAC 帧的端口以外的所有其他端口输出该 MAC 帧。因此，当集线器从连接交换机的端口接收到 MAC 帧后，将从连接路由器和黑客终端的端口输出该 MAC 帧，该 MAC 帧同时到达路由器和黑客终端，如图 2(a)所示的嗅探终端 A 发送给路由器的 MAC 帧的过程。同样，当集线器从连接路由器的端口接收到 MAC 帧后，将从连接交换机和黑客终端的端口输出该 MAC 帧，该 MAC 帧同时到达交换机和黑客终端，如图 2(b)所示的嗅探路由器发送给终端 B 的 MAC 帧的过程。

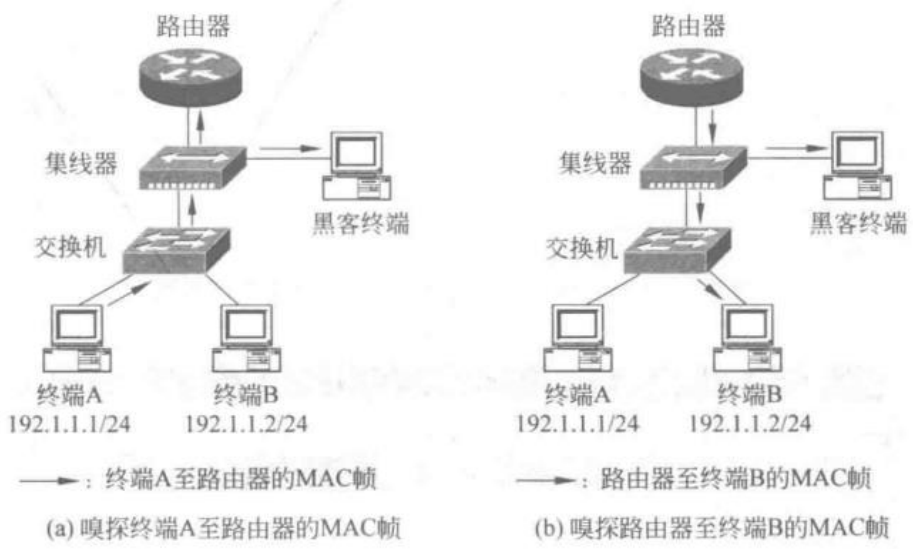


图 2

1.4 实验步骤

（1）画出正常接口的网络拓扑图如图 3，并完成 PC0 的相关配置，如图 4 所示，默认网关是路由器与交换机连接接口的 IP 地址（这是我是 F0/0）。由于本实验只需要实现同一以太网内两个结点之间的通信过程，因此，可以不配置 PC0 和 PC1 的默认网关地址。依此完成 PC1 网络信息配置过程。

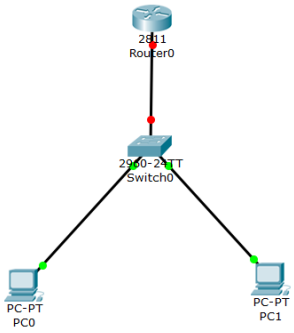


图 3

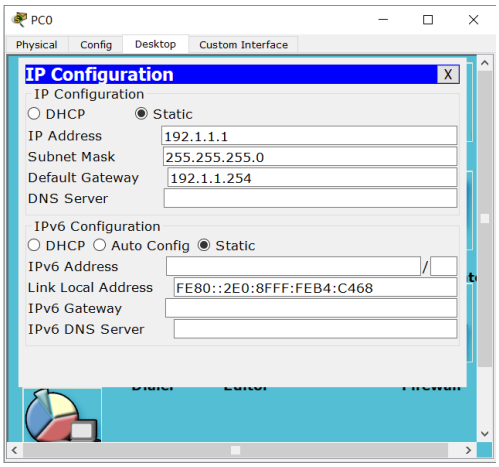


图 4

（2）完成路由器 Router“配置(Config)”→“FastEtherneto/0 接口(F0/0)"操作过程，弹出如图 5 所示的路由器 Router FastEtherneto/0 接口配置界面，MAC Address(MAC 地址栏)中给出的是该接口的 MAC 地址，在 IP Address(IP 地址栏)中输入该接口的 IP 地址 192.1.1.254，该 IP 地址也是该接口所连接的网络中的终端 PCO 和 PC1 的默认网关地址。在 Subnet Mask(子网掩码栏)中输人该接口的子网掩码 255.255.255.0。

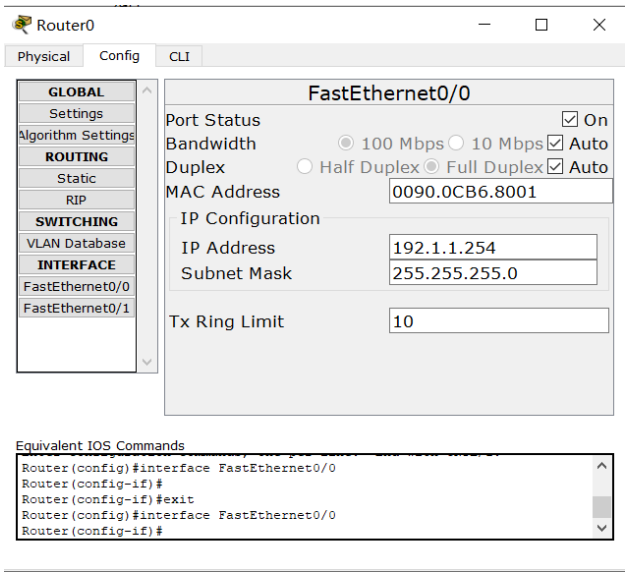


图 5

（3）完成这些配置后，通过简单报文工具确定 PCO 和 PC1 与路由 Router0 之间的连通性，如图 6 所示。

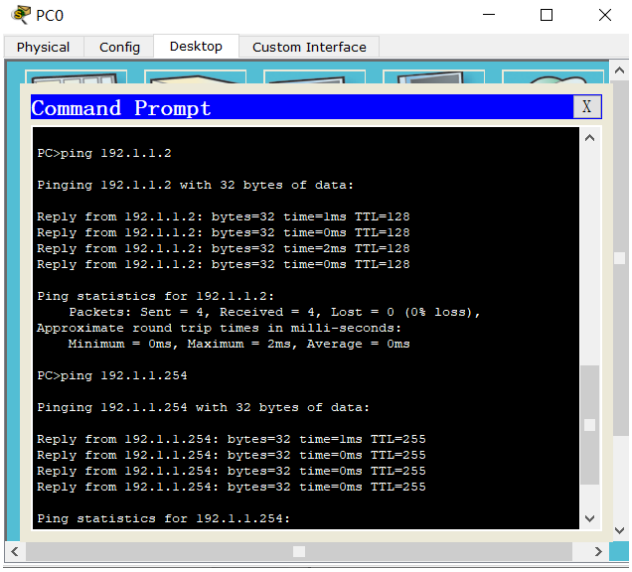


图 6

（4）在交换机和路由器之间接入一个集线器，并将黑客中终端 hack 接入 hub 中，如图 7 所示。

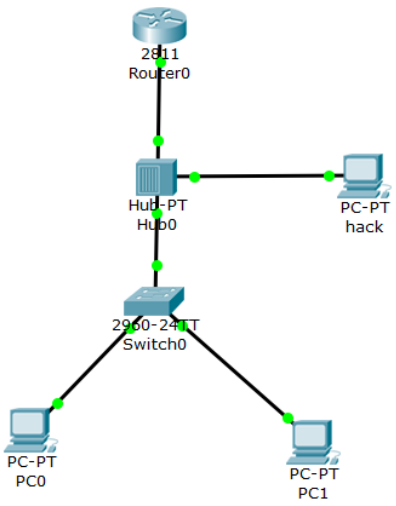


图 7

（5）通过简单报文工具确定 PC0 和 PC1 与路由器 Router 之间的连通性，以此证明插入的集线器 Hub 和黑客终端 hack 对于 PC00、 PC1 和路由器 Router 是透明的。切换到模拟操作模式，进入“Edit Filters”配置界面，勾选 ICMP(Internet 控制报文协议)，如图 8 所示。一旦勾选 ICMP，可以查看终端与路由器之间 ICMP 报文的传输过程。通过简单报文工具启动 PC0 至路由器 Router 的 ICMP 报文传输过程。如图 9 所示，集线器 Hub 不仅把 ICMP 报文转发给路由器 Router，同时，将 ICMP 报文转发给黑客终端 hack ，黑客终端 hack 成功嗅探 PC0 发送给路由器 Router 的 ICMP 报文。

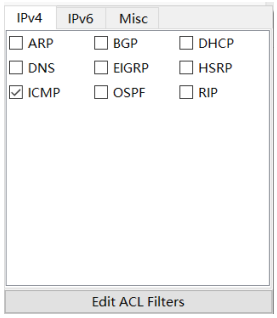


图 8

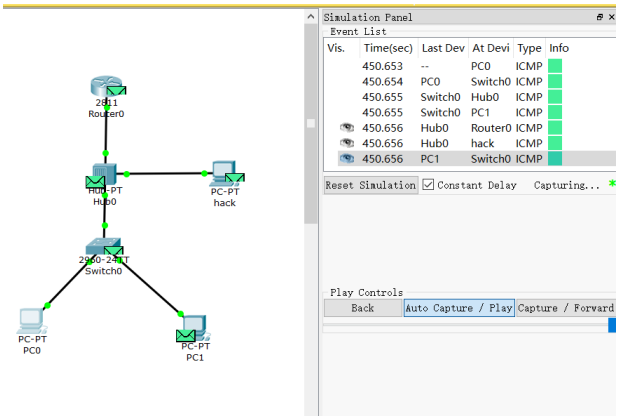


图 9

2. MAC 地址欺骗攻击实验

2.1 实验内容

以太网结构如图 10 所示，交换机建立完整转发表后，终端 B 发送给终端 A 的 MAC 帧只到达终端 A。如果终端 C 将自己的 MAC 地址改为终端 A 的 MAC 地址 MAC A，且向终端 B 发送一帧 MAC 帧，则终端 B 再向终端 A 发送 MAC 帧时，终端 B 发送给终端 A 的 MAC 帧不是到达终端 A，而是到达终端 C。

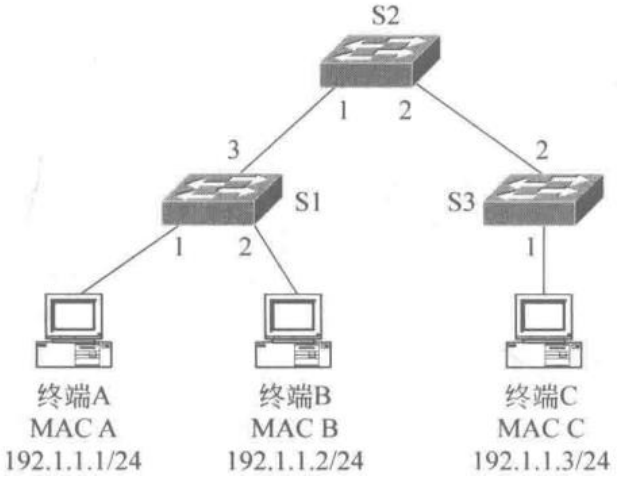


图 10

2.2 实验目的

（1）验证交换机建立 MAC 表(转发表)过程。

（2）验证交换机转发 MAC 帧机制。

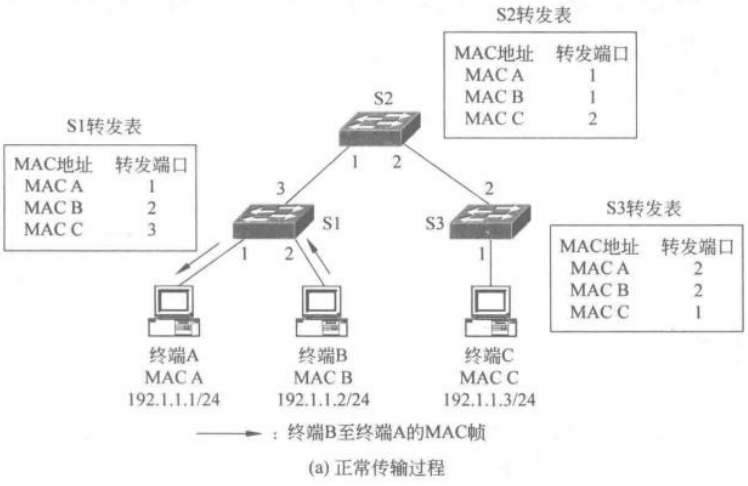
（3）验证 MAC 地址欺骗攻击原理。

（4）掌握 MAC 地址欺骗攻击过程。

2.3 实验原理

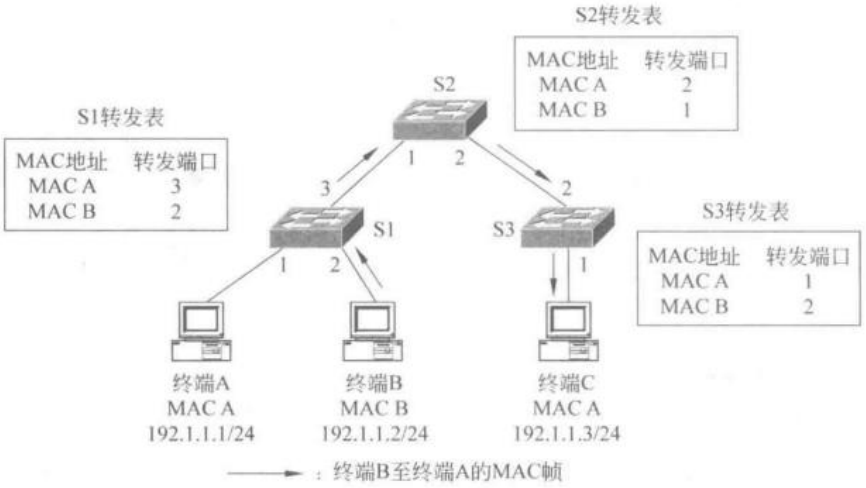
正常传输过程如图 11 所示，当交换机 S1、S2 和 S3 建立完整转发表后，转发项将通往终端 A 的交换路径作为通往 MAC 地址为 MACA 的终端的交换路径，因此，终端 B 发送的目的 MAC 地址为 MAC A 的 MAC 帧沿着通往终端 A 的交换路径到达终端 A。

如果终端 C 将自己的 MAC 地址改为 MAC A，且向终端 B 发送源 MAC 地址为 MAC A 的 MAC 帧，交换机 S1、 S2 和 S3 的转发表改为如图 12 所示，转发项将通往终端 C 的交换路径作为通往 MAC 地址为 MAC A 的终端的交换路径，因此，终端 B 发送的目的 MAC 地址为 MAC A 的 MAC 帧沿着通往终端 C 的交换路径到达终端 C。



(a) 正常传输过程

图 11



(b) 错误传输过程

图 12

2.4 实验步骤

（1）完成网络拓扑图，注意同等设备之间使用交叉线（交换机之间使用交叉线：Copper Cross-Over）。如图 13 所示。

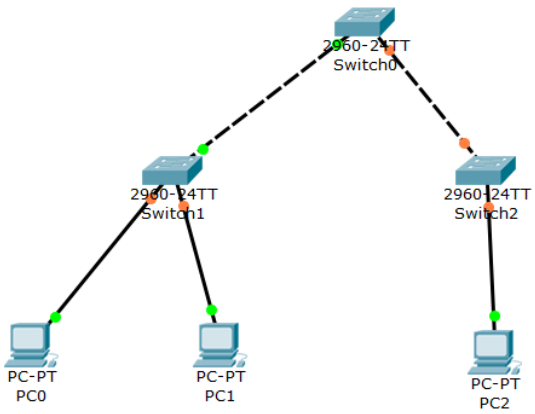


图 13

（2）按照如图 10 所示，完成 PC0、PC1 和 PC2 的 IP 地址和子网掩码配置过程。完成 PC0

“Config(配置)” → “FastEthernet0(FastEthernet0 接口)”操作过程，弹出如图 14 所示的 PC0 FastEthernet0 接口配置界面，其中 MAC Address(MAC 地址栏)中显示的是 PC0 的 MAC 地址 0060.3EA2.148B。

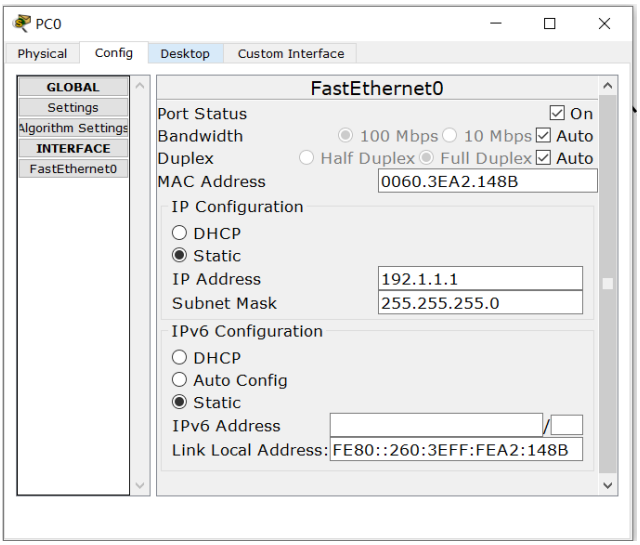


图 14

（3）完成 PC0、PC 和 PC2 两两之间的 ICMP 报文传输过程(相互 ping)，交换机 Switch0，Switch1 和 Switch2 中建立的完整转发表分别如图 15、图 16 和图 17 所示。Switch0 转发表中 MAC 地址 0060.3EA2.148B 对应的转发端口是该交换机连接 switch1 的端口 FastEthernet0/1 ，Switch1 转发表中 MAC 地址 0060.3EA2.148B 对应的转发端口是该交换机连接交换机 PC0 的端口 FastEthernet0/2。Switch2 转发表中 MAC 地址 0060.3EA2.148B 对应的转发端口是该交换机连接交换机 Switch0 的端口 FastEthernet0/1。显然，所有交换机中的转发项将通往 PC0 的交换路径作为通往 MAC 地址为 0060.3EA2.148B 的终端的交换路径。

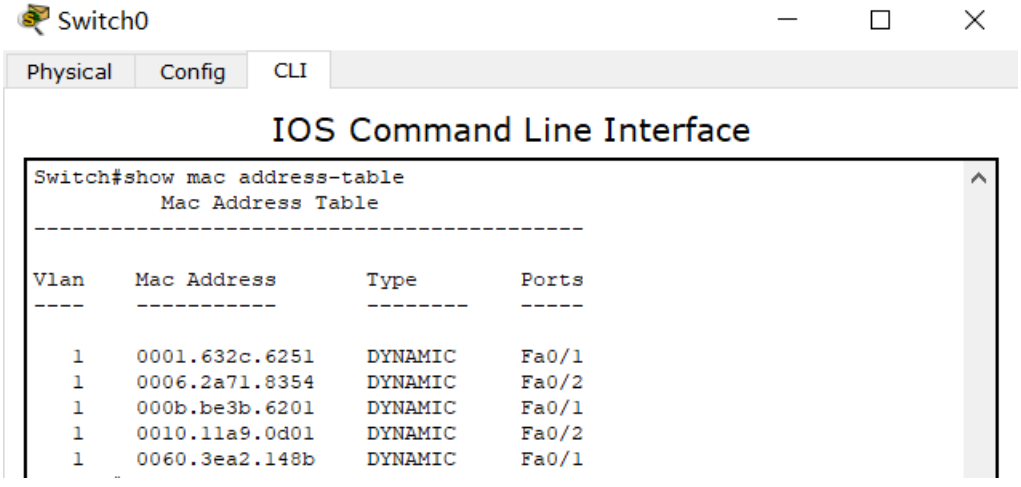


图 15

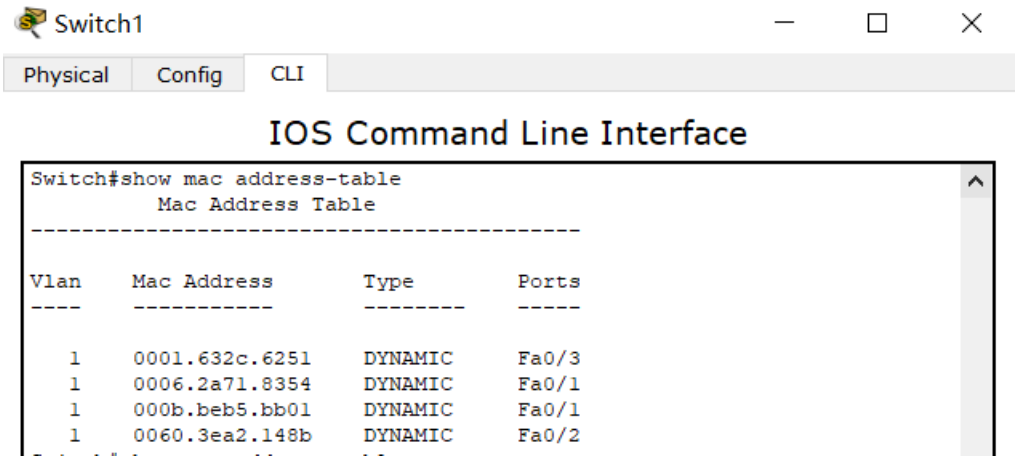


图 16

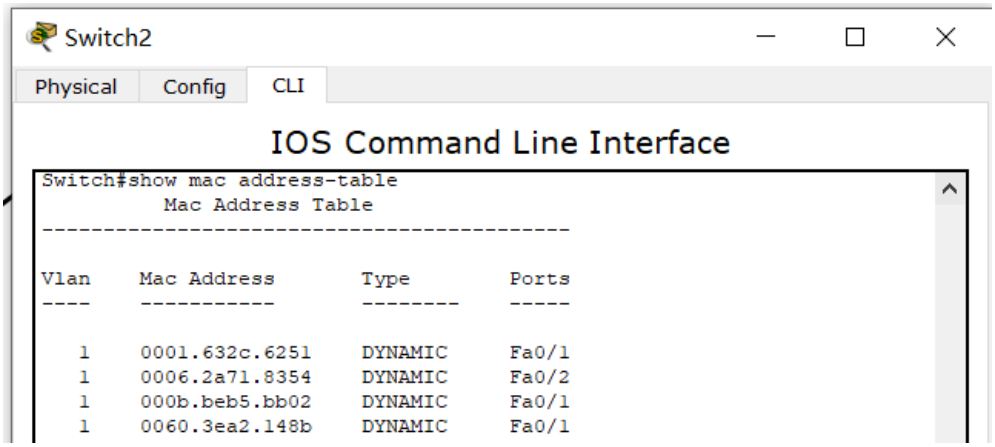


图 17

（4）切换到模拟操作模式，进入“Edit Filters”配置界面，勾选协议 ICMP。通过简单报文工具启动 PC1 至 PC0 的 ICMP 报文传输过程。如图 18 所示，该 ICMP 报文只到达 PC0。

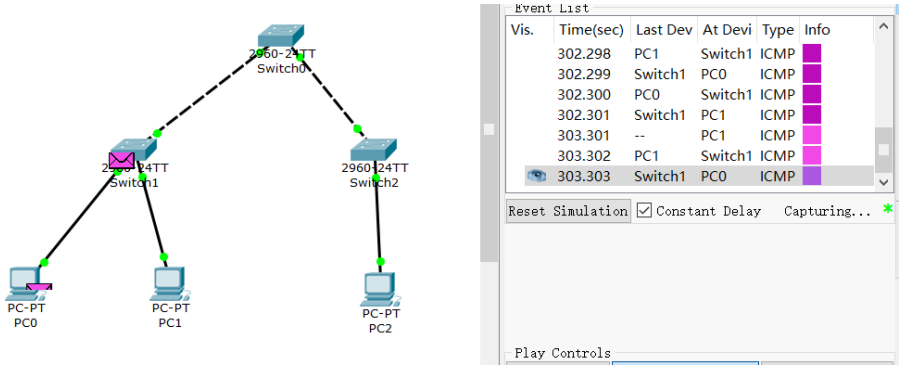


图 18

（5）切换到实时操作模式。完成 PC2"Config(配置)”→“FastEthernet0(FastEthernet0 接口)"操作过程，弹出如图 19 所示的 PC2 FastEthernet0 接口配置界面，将 MAC Address(MAC 地址栏)中的 MAC 地址改为 PC0 的 MAC 地址 0060.3EA2.148B。

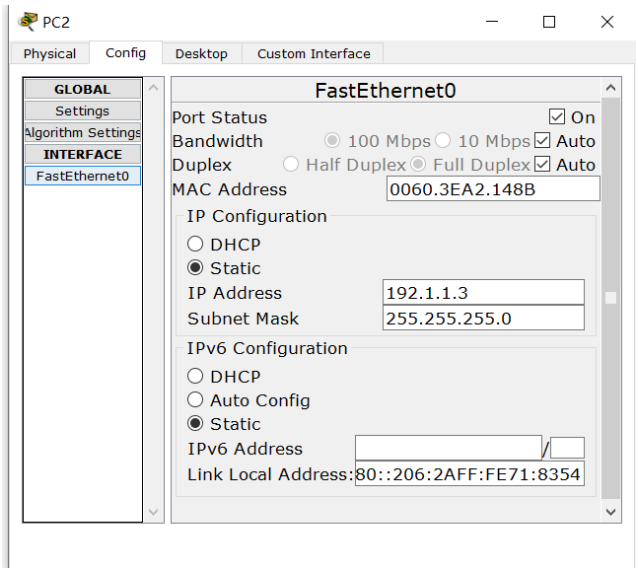


图 19

（6）通过简单报文工具启动 PC2 至 PC1 的 ICMP 报文传输过程，让交换机学习到新的转发表。新的转发表如下图 20.21.22 所示。

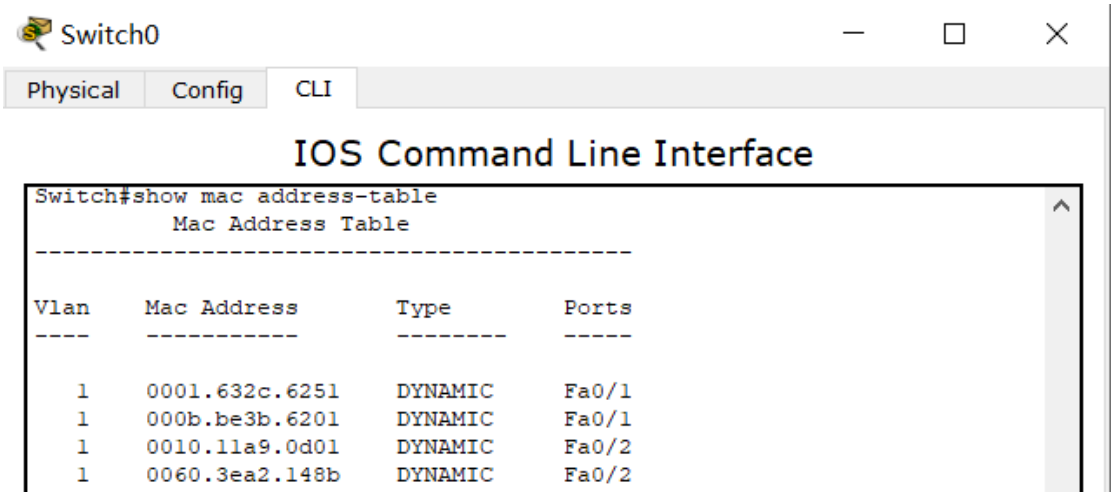


图 20

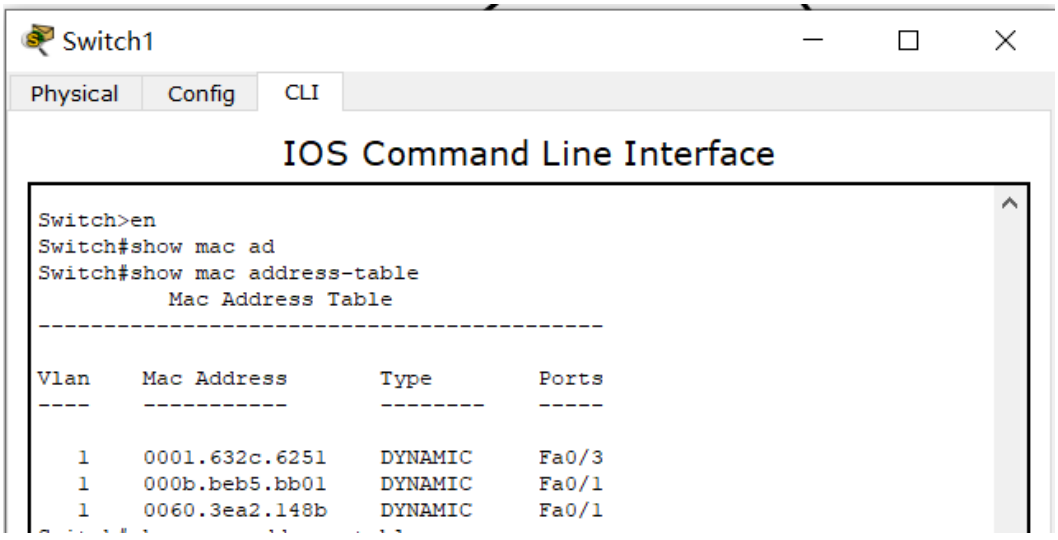


图 21

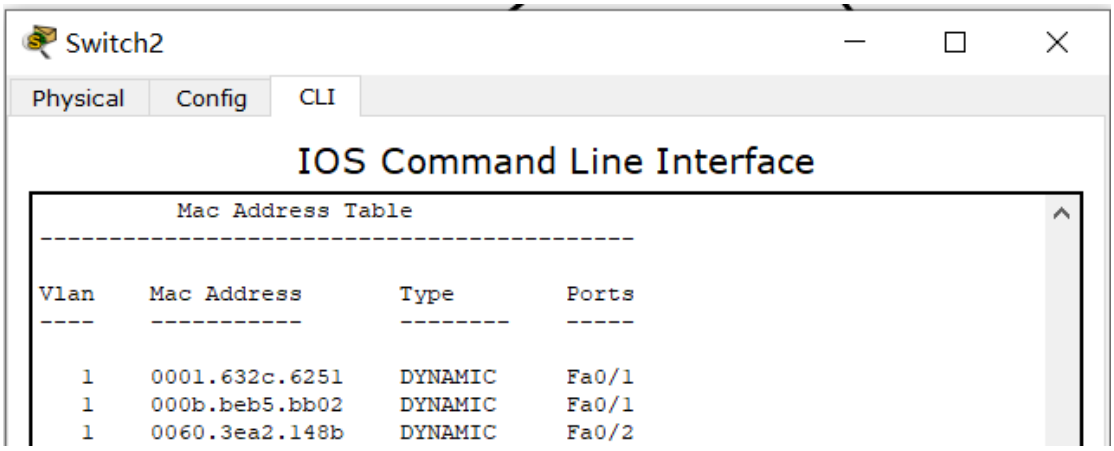


图 22

（7）切换到模拟操作模式，通过简单报文工具启动 PC1 至 PC0 的 ICMP 报文传输过程。如图 23 所示，该 ICMP 报文到达 PC2。

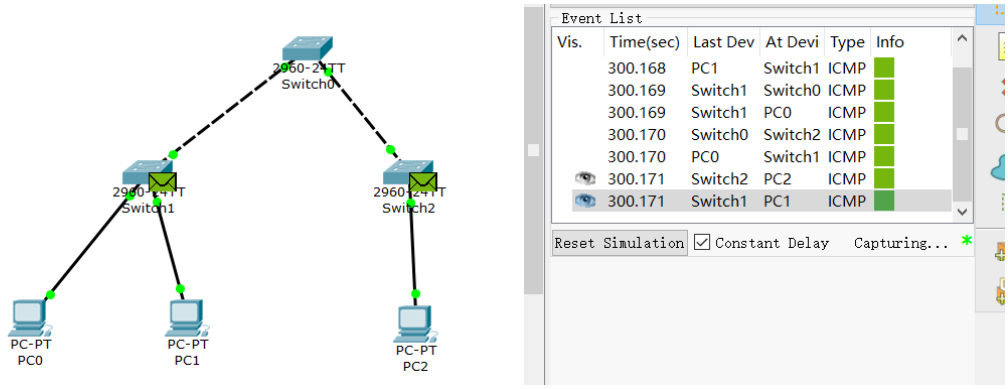


图 23

3. 钓鱼网站实验

3.1 实验内容

钓鱼网站实施过程如图 24 所示，正确情况下，终端应该从 DHCP 服务器获取正确的域名系统(Domain Name System， DNS)服务器地址 192.1.2.7，通过正确的 DNS 服务器解析完全合格的域名 www.bank.com，得到的结果是正确的 Web 服务器地址 192.1.3.7。

当黑客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 服务器后，终端可能从伪造的 DHCP 服务器获取伪造的 DNS 服务器地址 192.1，3.1，通过伪造的 DNS 服务器解析完全合格的域名 www.bank.com，得到的结果是伪造的 Web 服务器地址 192.1.2.5。导致用户通过域名 www.bank.com 访问到伪造的 Web 服务器。

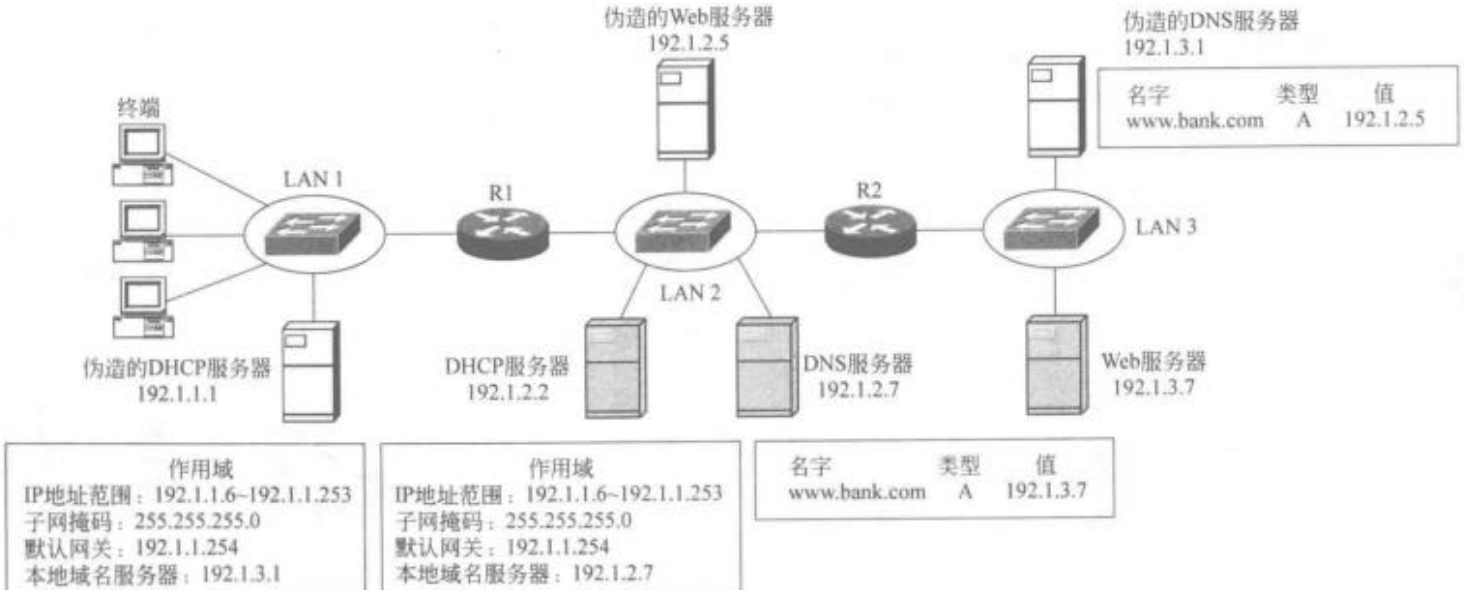


图 24

3.2 实验目的

（1）验证伪造的 DHCP 服务器为终端提供网络信息配置服务的过程。

（2）验证错误的本地域名服务器地址造成的后果。

（3）验证利用网络实施钓鱼网站的过程。

3.3 实验原理

终端通过广播 DHCP 发现消息发现 DHCP 服务器，当 DHCP 服务器与终端不在同一个网络(同一个广播域)时，由路由器完成中继过程。DHCP 服务器通过向终端发送 DHCP 提供消息表明可以为终端提供网络信息配置服务，终端选择发送第一个到达终端的 DHCP 提供消息的 DHCP 服务器为其提供网络信息配置服务。

如图 24 所示，在终端连接的网络中接人伪造的 DHCP 服务器后，终端广播的 DHCP 发现消息到达伪造的 DHCP 服务器，伪造的 DHCP 服务器在网络中广播 DHCP 提供消息，由于伪造的 DHCP 服务器与终端位于同一网络，伪造的 DHCP 服务器发送的 DHCP 提供消息

可能先于 DHCP 服务器发送的 DHCP 提供消息到达终端，导致终端选择伪造的 DHCP 服务器为其提供网络信息配置服务，并将伪造的 DNS 服务器的 IP 地址 192.1.3.1 作为本地域名服务器地址。

3.4 实验步骤

（1）去掉伪造的服务器，画出正常的网络拓扑图，如图 25 所示。

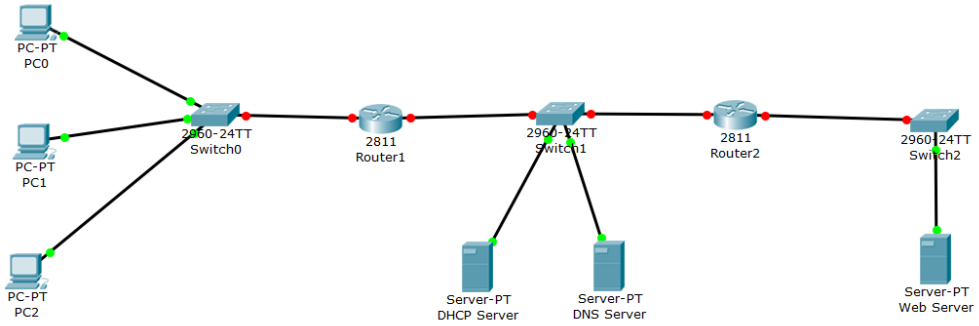


图 25

（2）完成路由器接口 IP 地址和子网掩码配置过程，完成路由器 RIP 配置过程。路由器 Router1 和 Router2 建立完整路由表。

（3）完成路由器 Router1 接口 FastEthernet0/0 的中继地址配置过程。

（4）第二步和第三步的具体配置过程如图 26、27 所示。

（5）按照如图 24 所示的服务器 IP 地址，完成 3 台服务器 IP 地址、子网掩码和默认网关地址配置过程，服务器的默认网关地址是路由器连接服务器所在网络的接口的 IP 地址。由于 Router1 和 Router2 各有一个接口连接 DHCP 服务器和 DNS 服务器所在的网络，DHCP 服务器和 DNS 服务器可以选择其中一个接口的 IP 地址作为默认网关地址。

（6）完成 DHCP 服务器“Services(服务)” →“DHCP”操作过程，弹出如图 28 所示的 DHCP 服务器作用域配置界面，Service(服务)一栏选择 On。serverPool 是 Pool Name(作用域名)，每一个作用域需要取不同的作用域名。192.1.1.254 是该作用域的 Default Gateway(默认网关地址)，192.1.2.7 是该作用域的 DNS Server(DNS 服务器)地址，Start IP Address(起始 IP 地址)192.1.1.10 和 Maximum number of User(最大用户数)50 确定可分配的 IP 地址范围是 192.1.1.10～192.1.1.59。

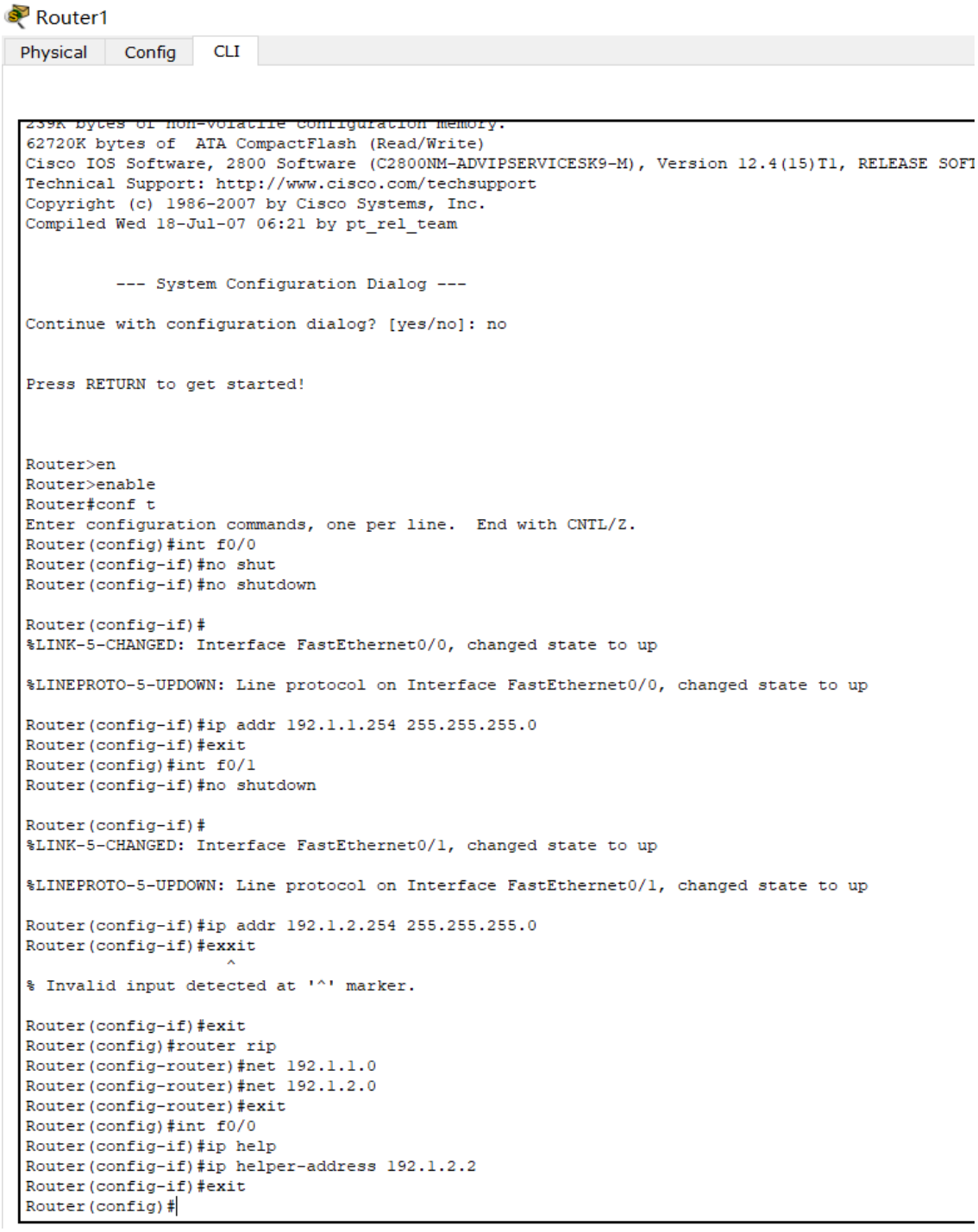

Router1
Physical
Config
CLI
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFT
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#ip addr 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#ip addr 192.1.2.254 255.255.255.0
Router(config-if)#exxit
^
% Invalid input detected at '^' marker.
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#net 192.1.1.0
Router(config-router)#net 192.1.2.0
Router(config-router)#exit
Router(config)#int f0/0
Router(config-if)#ip help
Router(config-if)#ip helper-address 192.1.2.2
Router(config-if)#exit
Router(config)#

图 26

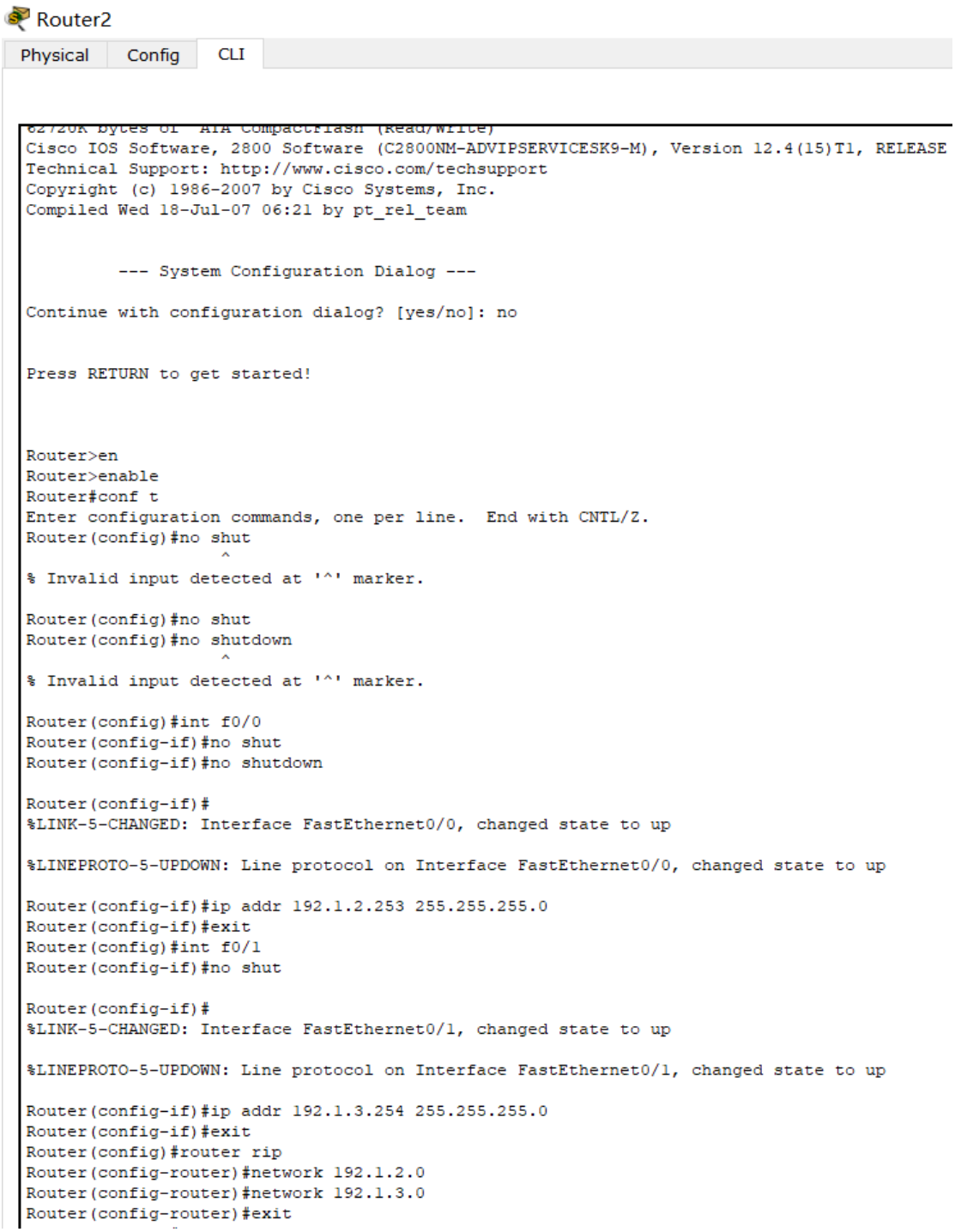

Router2
Physical
Config
CLI
62720K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no shut
^
% Invalid input detected at '^' marker.
Router(config)#no shut
Router(config)#no shutdown
^
% Invalid input detected at '^' marker.
Router(config)#int f0/0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#ip addr 192.1.2.253 255.255.255.0
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#ip addr 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit

图 27

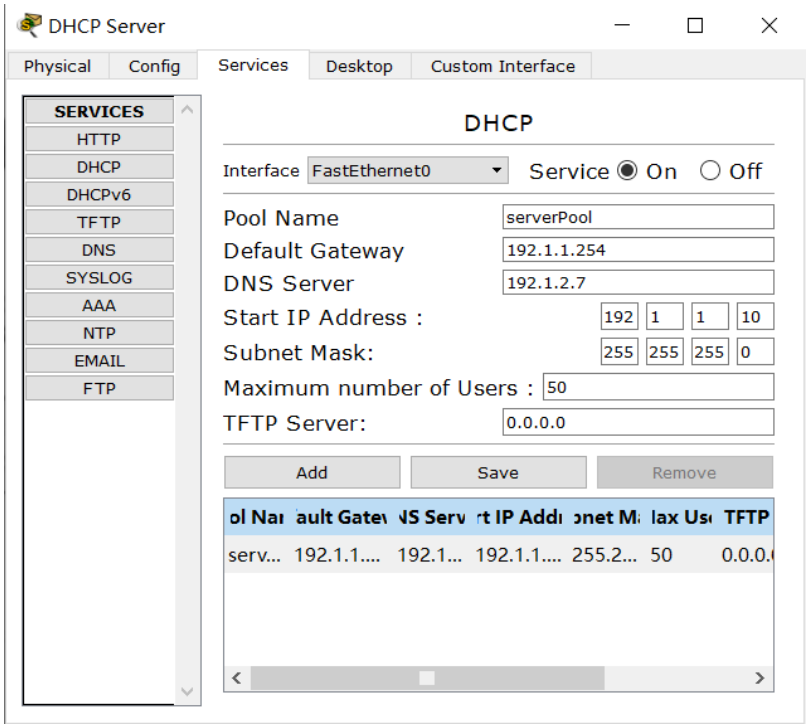


图 28

（7）完成 DNS 服务器“Services(服务)”→“DNS"操作过程，弹出如图 29 所示的，DNS 服务器资源记录配置界面，DNS Service(DNS 服务)一栏选择 On。在 Name(名字)框中输入完全合格的域名 www.bank. com， Type(类型)选择 A Record(A 记录类型)，在 Address(地址)框中输入完全合格的域名为 www.bank.com 的 Web 服务器的 IP 地址 192.1.3.7。

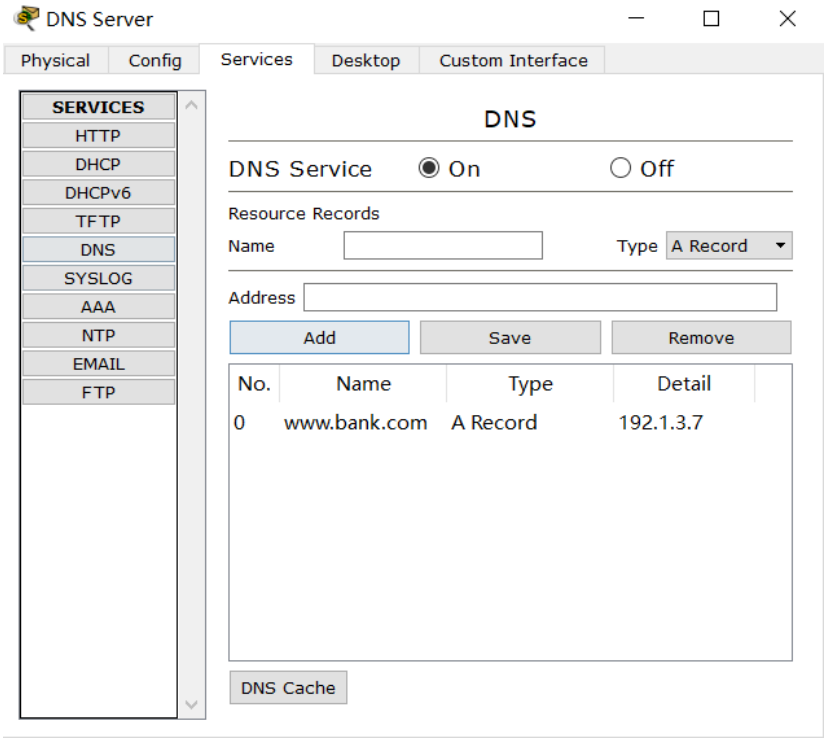


图 29

（8）完成 PC0“Desktop(桌面)”→“IP Configuration(IP 配置)”操作过程，弹出如图 30 所示的 PCO 网络信息配置界面，选择 DHCP 选项， PCO 自动获取如图 2.42 所示的网络信息。其

中 IP 地址是 DHCP 服务器中名为 serverPool 的作用域定义的 IP 地址范围 192.1.1.10~192.1.1.59 中按照大小顺序选取的 IP 地址 192.1.1.10。子网掩码、默认网关地址和 DNS 服务器地址与名为 serverPool 的作用域定义的子网掩码、默认网关地址和 DNS 服务器地址相同。

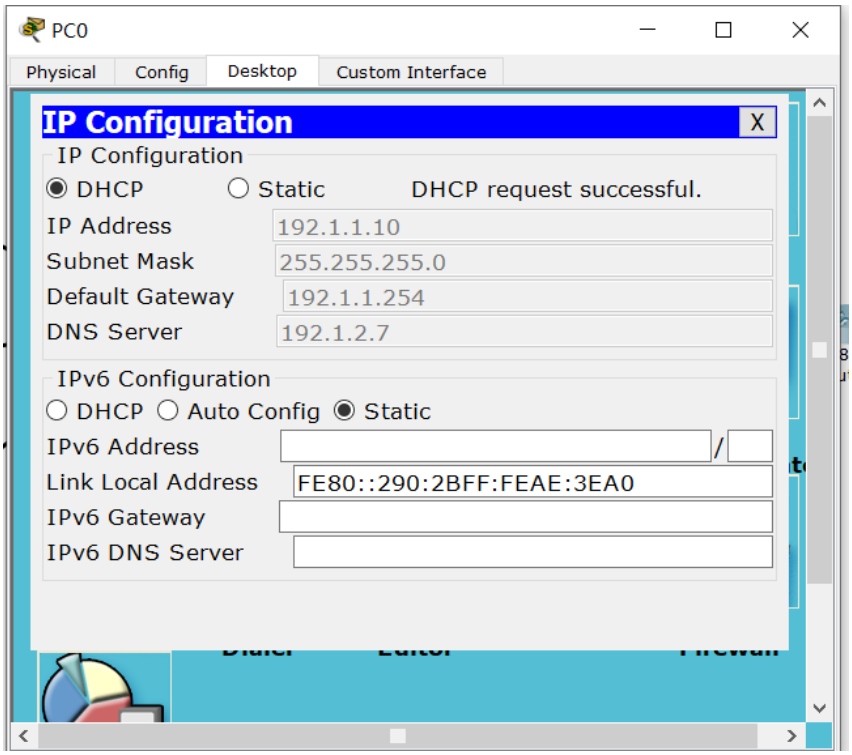


图 30

（9）完成 PC0“Desktop(桌面)”→“Web Browser(浏览器)"操作过程，弹出如图 31 所示的浏览器使用界面，在 URL 栏中输人完全合格的域名 www.bank.com，单击 Go，成功访问到完全合格的域名为 www.bank.com 的 Web 服务器。

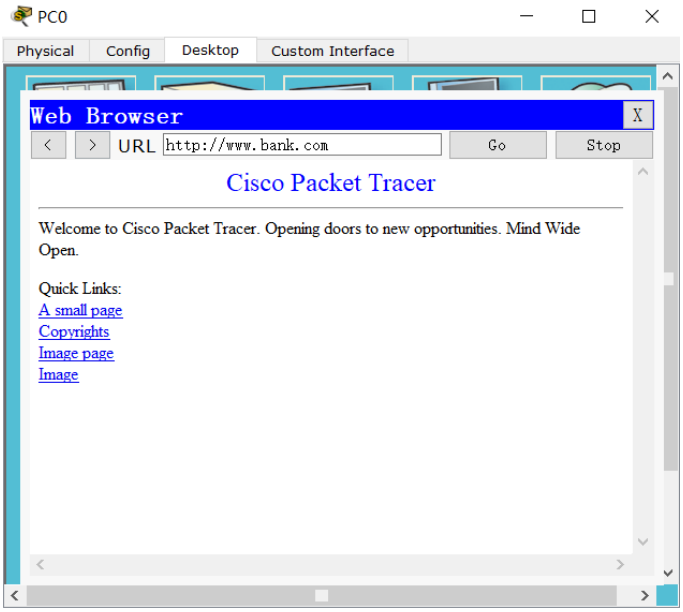


图 31

（10）接入 3 台伪造的服务器，网络拓扑图如图 32 所示。完成 3 台伪造的服务器的 IP 地

址、子网掩码和默认网关地址配置过程。完成伪造的 DHCP 服务器的作用域配置过程，配置的作用域信息如图 33 所示;完成伪造的 DNS 服务器的资源记录配置过程，配置的资源记录如图 34 所示。让 PC0 再次自动获取网络信息，获取的网络信息如图 35 所示，DNS 服务器地址是伪造的 DNS 服务器的 IP 地址 192.1，3.1，表明 PC0 从伪造的 DHCP 服务器获取网络信息。

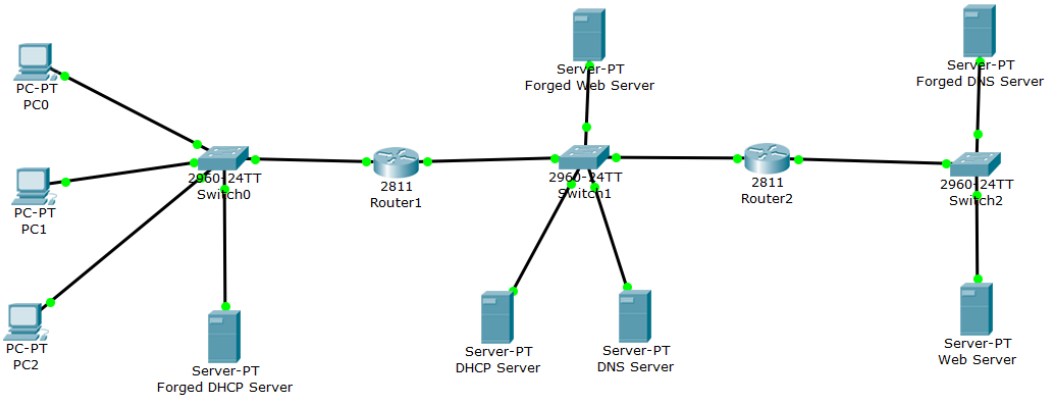


图 32

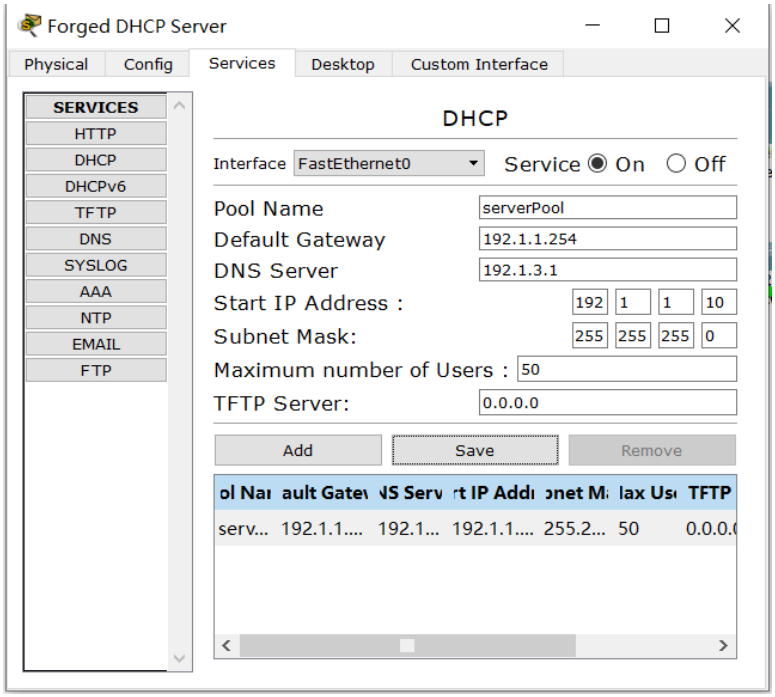


图 33

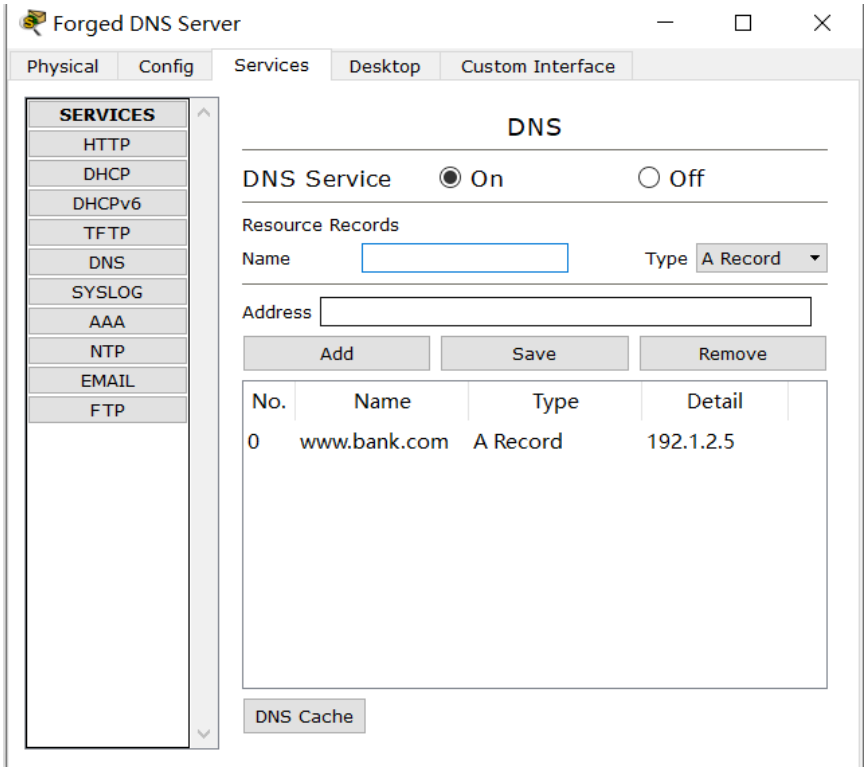


图 34

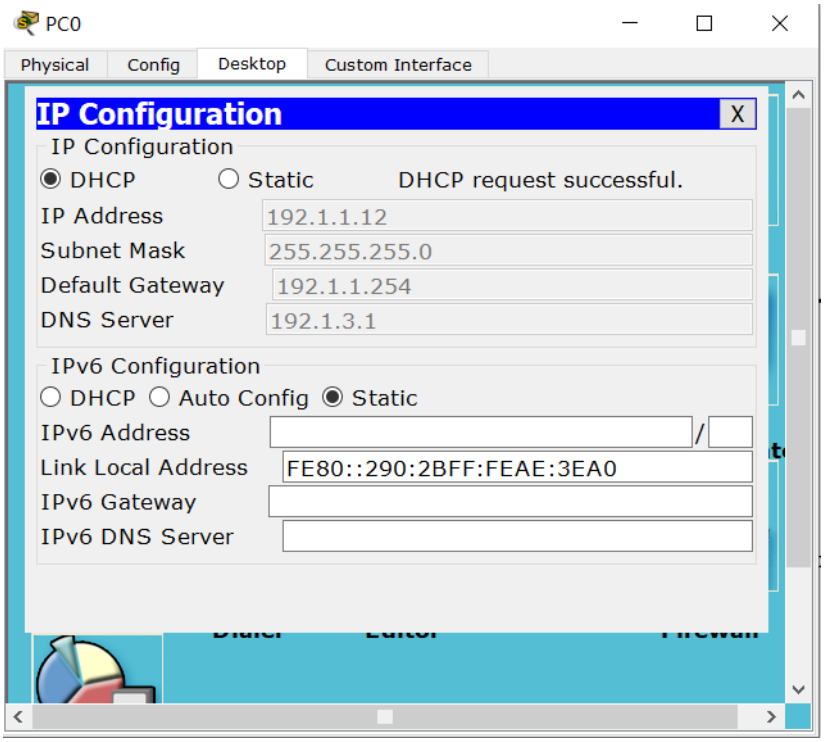


图 35

（11）PC0 再次用浏览器访问完全合格的域名为 www.bank.com 的 Web 服务器，访问结果如图 36 所示，访问结果表明 PC0 访问的是伪造的 Web 服务器。（注：修改 Forged webServer 界面如图 37 所示。 ”Service” →”HTTP”，然后进行修改（可以自己写个 HTML5 网页）。）

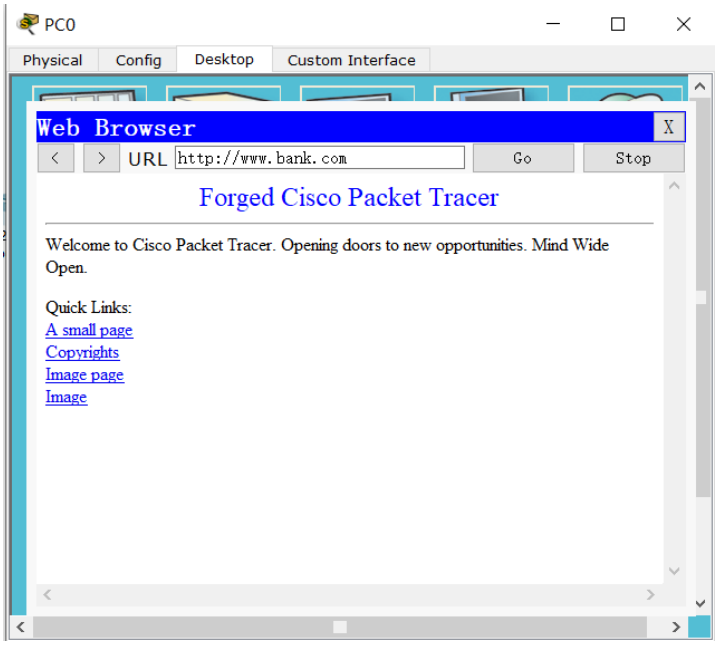

PC0
Physical
Config
Desktop
Custom Interface
Web Browser
X
URL
http://www.bank.com
Go
Stop
Forged Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

图 36

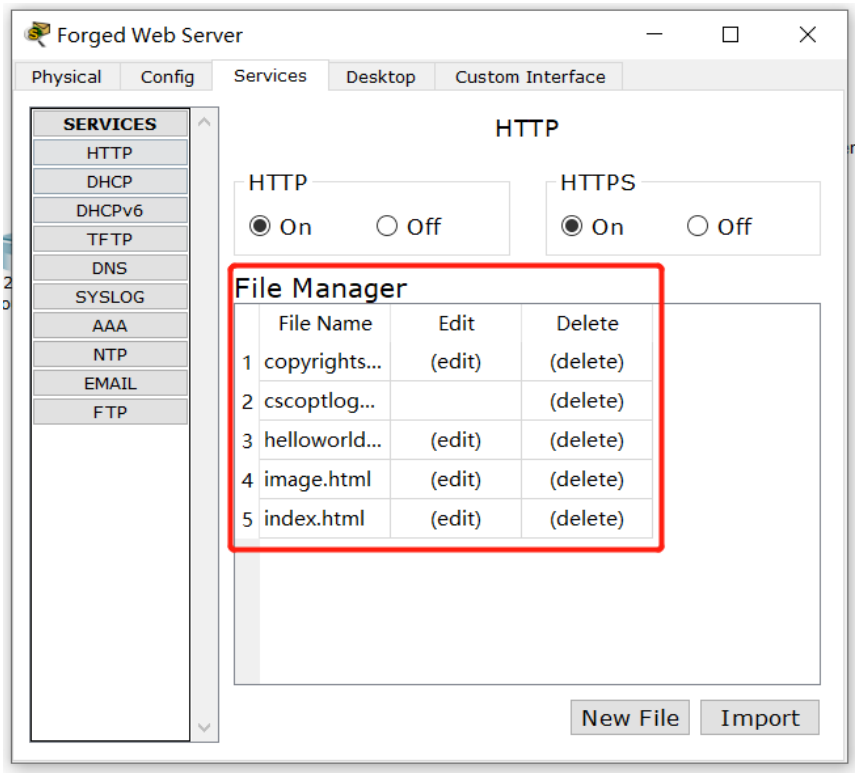

Forged Web Server
Physical
Config
Services
Desktop
Custom Interface
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 copyrights... (edit) (delete)
2 cscoptlog... (delete)
3 helloworld... (edit) (delete)
4 image.html (edit) (delete)
5 index.html (edit) (delete)
New File
Import

图 37