杭州电子科技大学

网络空间安全技术课程设计

实验三 以太网安全防御实验

安全端口实验

一、 实验目的

安全端口实验：

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、 实验原理

1、利用集线器的什么原理可以实施嗅探攻击?

集线器采用的是共享式传输原理，它不会区分目标设备，而是把收到的数据帧广播给所有端口。由于所有主机都能收到同一条数据，只是由网卡决定是否处理，因此攻击者只要把网卡设置为混杂模式，就能够接收其他主机的通信数据，从而实现嗅探攻击。也就是说，集线器的广播式工作方式使得网络中所有数据都可以被监听。

2、通过交换机可以有哪些方式实施窃听攻击?

交换机会根据 MAC 地址表进行定向转发，正常情况下不容易窃听。但如果攻击者破坏或干扰交换机的转发表，就能让交换机误转发数据，从而达到窃听目的。常见方式包括:

（1）MAC 泛洪攻击

攻击者向交换机发送大量伪造的不同源 MAC 地址的数据帧，使交换机的 MAC 地址表被填满。MAC 表无效后，交换机会退回广播式转发，攻击者即可像在集线器环境一样嗅探所有数据。

（2）ARP 欺骗攻击

攻击者伪造 ARP 响应，将自己的 MAC 地址冒充为网关或其他主机的 MAC。交换机更新 MAC 表后，会把原本发给网关或其他主机的数据错误地转发给攻击者，从而实现中间人窃听。

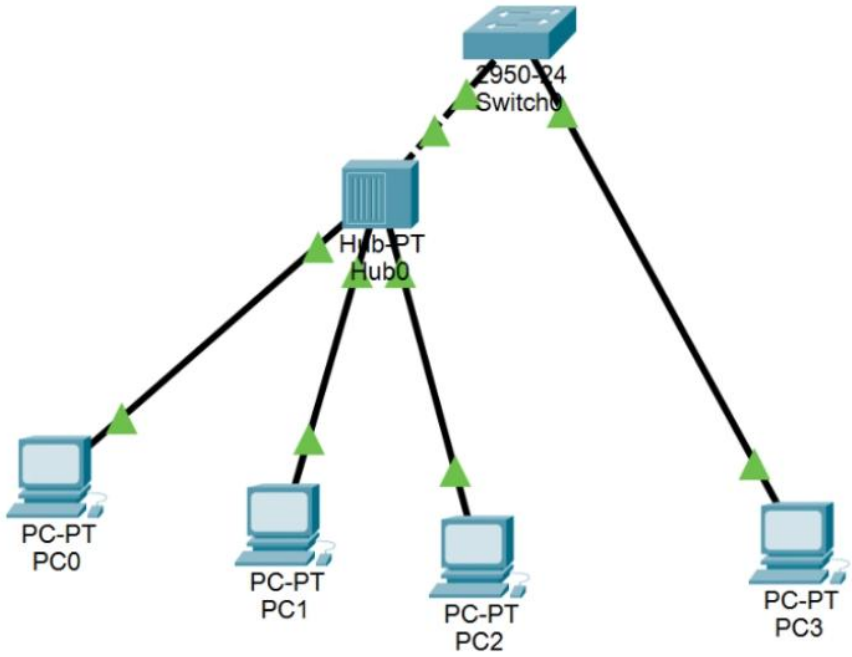
（3）端口镜像滥用

如果攻击者获得交换机管理权限，可以开启端口镜像功能，让某端口复制其他端口的数据流，从而直接监听目标主机的通信。

3、安全端口实验原理

由于交换机端口 1 设置为安全端口, 并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 并向交换机端口 1 发送 MAC 帧后, 访问控制列表中已添加终端 A 和终端 B 的 MAC 地址。当终端 C 接入交换机端口 1 并向交换机端口 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 地址数已达到最大地址数 2，因此交换机丢弃该 MAC 帧。

三、 实验环境/实验拓扑图



四、 主要操作步骤及实验结果记录

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。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 4.5 所示。

```
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#exit
Switch(config)#
```

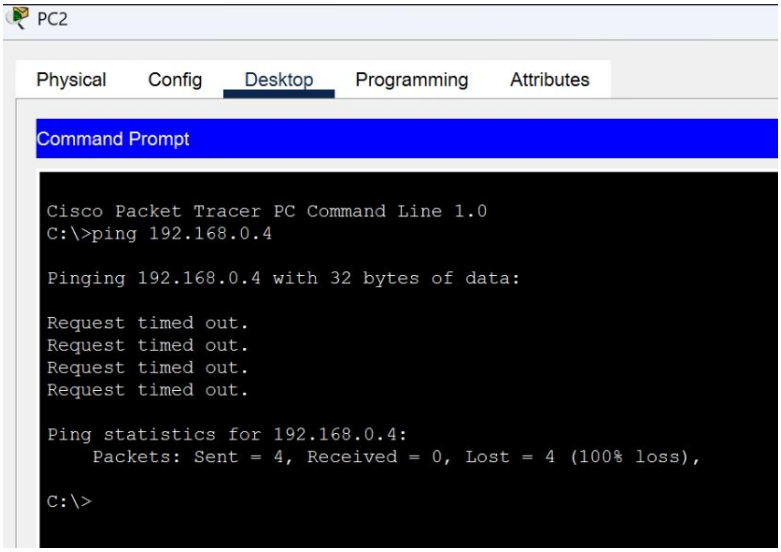
2）启动 PC0 与 PC3 之间的 ICMP 报文交换过程，PC0 和 PC3 之间能够成功交换 ICMP 报文。

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，PC1 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，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)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    00E0.F7B6.C84C    SecureSticky                  Fa0/1         -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    0010.1146.B418    SecureSticky                  Fa0/1         -
   1    00E0.F7B6.C84C    SecureSticky                  Fa0/1         -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
```

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。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。



五、 实验分析总结及心得

本次实验围绕交换机端口安全功能的验证展开，通过多个终端的接入与 ICMP 报文交互过程，全面观察了端口安全配置对设备接入和数据通信的影响。实验内容包括网络信息配置、端口安全模式设置、MAC 地址学习、访问控制列表更新以及异常接入行为的处理逻辑。通过逐步操作与现象观察，进一步理解了交换机端口安全机制在网络安全中的具体作用。

首先，在完成 PC0、PC1、PC2 和 PC3 的网络参数配置后，对交换机 FastEthernet0/1 端口进行了安全模式设置，并限定最大 MAC 地址学习数量为 2。在此基础上，当 PC0 与 PC3、PC1 与 PC3 进行 ICMP 交互测试时，均能够正常通信，说明前两个合法接入的 MAC 地址被交换机成功学习并写入访问控制列表。随后，当 PC2 接入端口并尝试与 PC3 通信时，由于其 MAC 地址不在访问控制列表中，同时端口已达到最大 MAC 数量限制，交换机直接丢弃其发送的帧，使通信无法建立，但端口工作状态保持正常。这一过程体现了端口安全功能能够在不影响端口物理状态的前提下阻断未授权设备的数据传输，提高接入层安全性。

通过本次实验，我对交换机端口安全功能有了更加直观和深入的理解。端口安全机制通过限制 MAC 地址数量和管理访问控制列表，有效防止了非法设备接入、防止 MAC 地址泛洪攻击，并能保证已授权设备的正常通信。实验还让我意识到在实际网络部署中，合理配置端口安全策略对于提升局域网安全性具有重要意义。此外，在操作过程中，我也体会到逐步验证、观察状态变化的重要性，这对于排查网络问题和理解配置效果非常有帮助。

总体而言，本次实验不仅巩固了对交换机端口配置命令与安全特性的理解，也提升了

分析网络行为和设计安全策略的能力，为后续深入学习网络安全防护技术打下了良好基础。

MAC 地址欺骗实验

一. 实验目的

1. 利用思科 Packet tracer 软件模拟实现利用相关协议进行攻击的实验；

2. MAC 地址欺骗攻击实验

1）验证交换机构建 MAC 表（转发表）的过程。

2）验证交换机转发 MAC 帧的机制。

3）验证 MAC 地址欺骗攻击的原理。

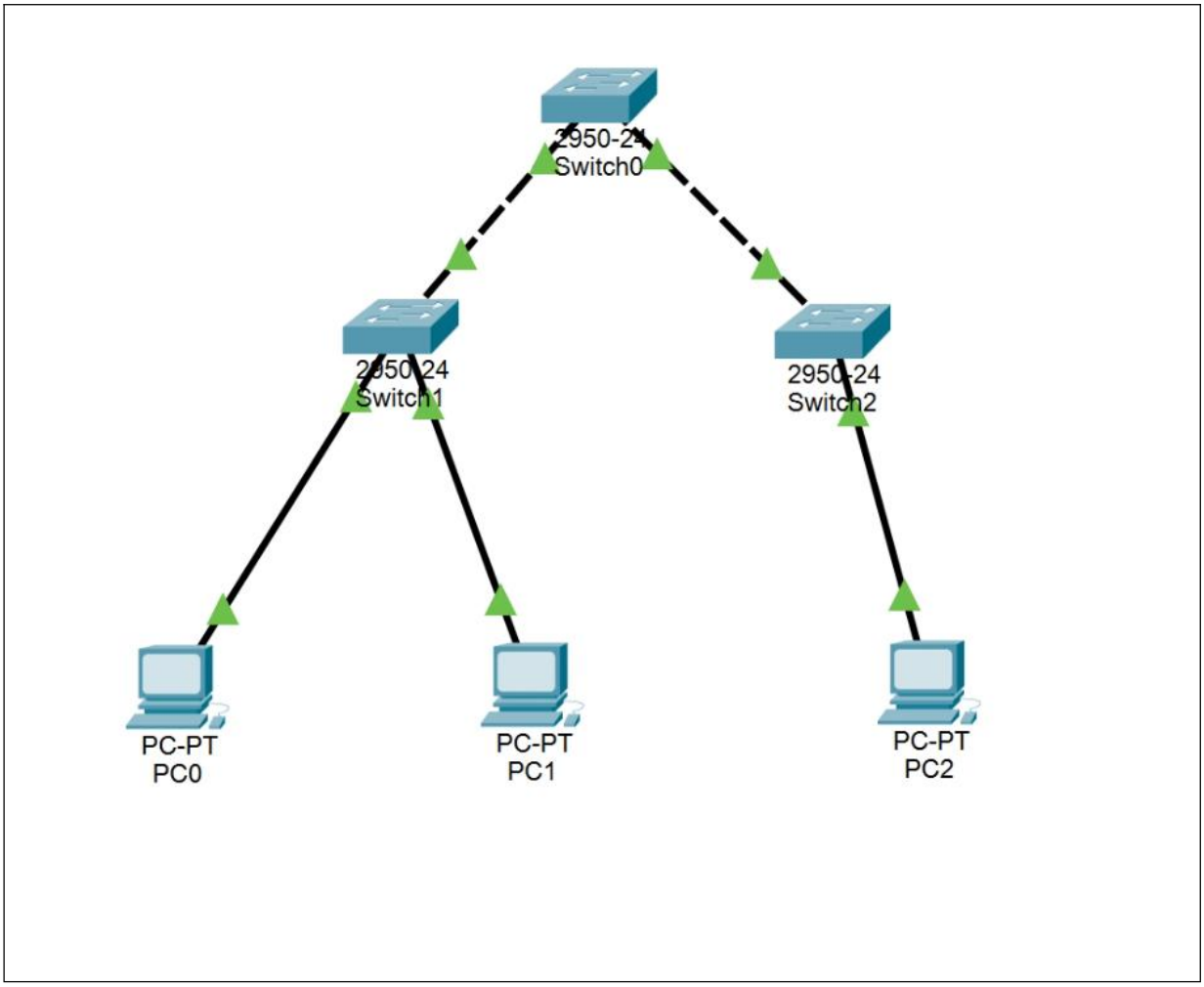
4）掌握 MAC 地址欺骗攻击的具体实施过程。

二. 实验原理

正常的传输过程中，当交换机 S1、S2 和 S3 建立了完整的转发表后，转发项会将通往终端 A 的交换路径作为到达 MAC 地址为 MAC_A 的目标路径。因此，终端 B 发送的、目标 MAC 地址为 MAC_A 的 MAC 帧，会沿着通往终端 A 的路径转发并最终抵达终端 A。

如果终端 C 将自己的 MAC 地址伪装成 MAC_A，并向终端 B 发送源 MAC 地址为 MAC_A 的 MAC 帧，那么交换机 S1、S2 和 S3 的转发表会被更新为图 2.10 (b) 所示状态。此时，转发项会误将通往终端 C 的交换路径视为通往 MAC_A 的路径。因此，终端 B 之后发送的、目标地址为 MAC_A 的所有 MAC 帧都会沿着通往终端 C 的路径转发，并最终到达终端 C，从而导致通信被劫持。

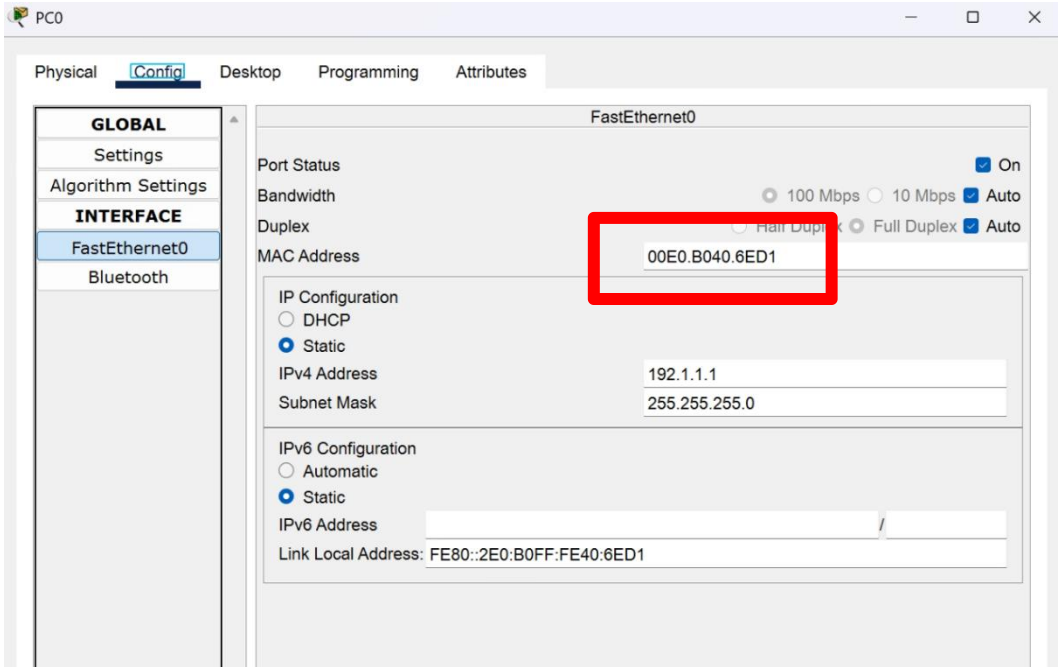
三. 实验环境/实验拓扑图


2950-24
Switch0
2950-24
Switch1
2950-24
Switch2
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2

四. 主要操作步骤及实验结果记录

（1）启动 Packet Tracer，在逻辑工作区根据图示的网络结构放置并连接设备。终端与交换机之间使用直通线连接，交换机之间使用 Copper Cross-Over（交叉线）连接。完成设备连接后，逻辑工作区应呈现完整的网络拓扑。

（2）按照网络结构配置 PC0、PC1 和 PC2 的 IP 地址和子网掩码。以 PC0 为例，在 “Config（配置）” - “FastEthernet0（接口）” 中可看到其 MAC 地址为 00E0.B040.6ED1。

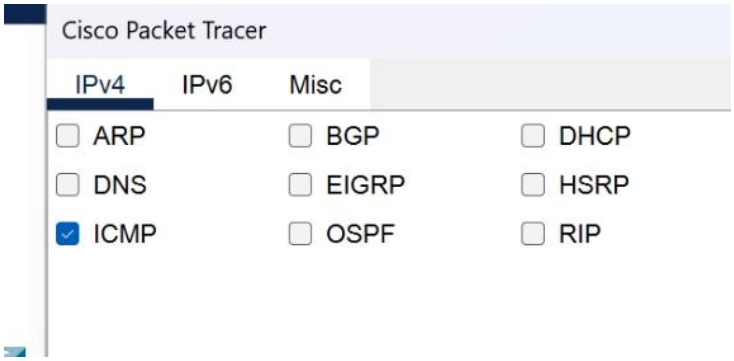


（3）完成 PC0、PC1 和 PC2 之间相互的 ICMP 报文传输后，交换机 Switch0、Switch1 和 Switch2 会分别建立完整的转发表。

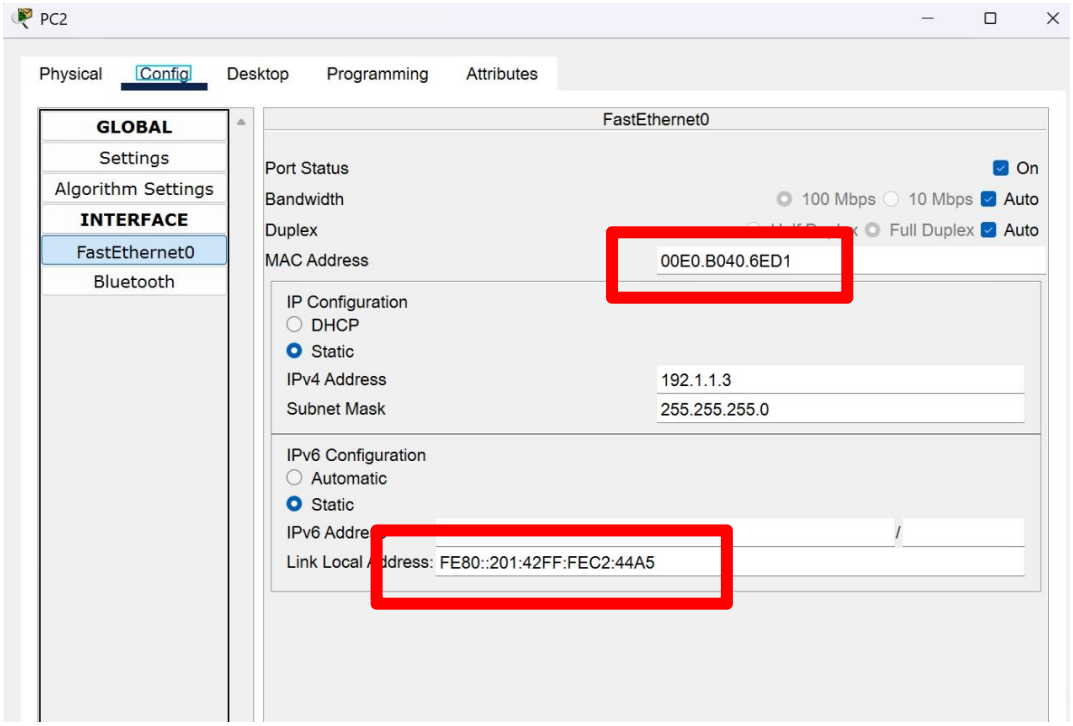
其中，MAC 地址 0006.2A2B.865A 在 Switch0 的转发端口为该交换机连接 PC0 的 FastEthernet0/1；在 Switch1 的转发端口为连接 Switch0 的 FastEthernet0/1；在 Switch2 的转发端口为连接 Switch1 的 FastEthernet0/2。

可见，各交换机均将通往 PC0 的路径记录为通往 MAC 地址 0006.2A2B.865A 的转发路径。

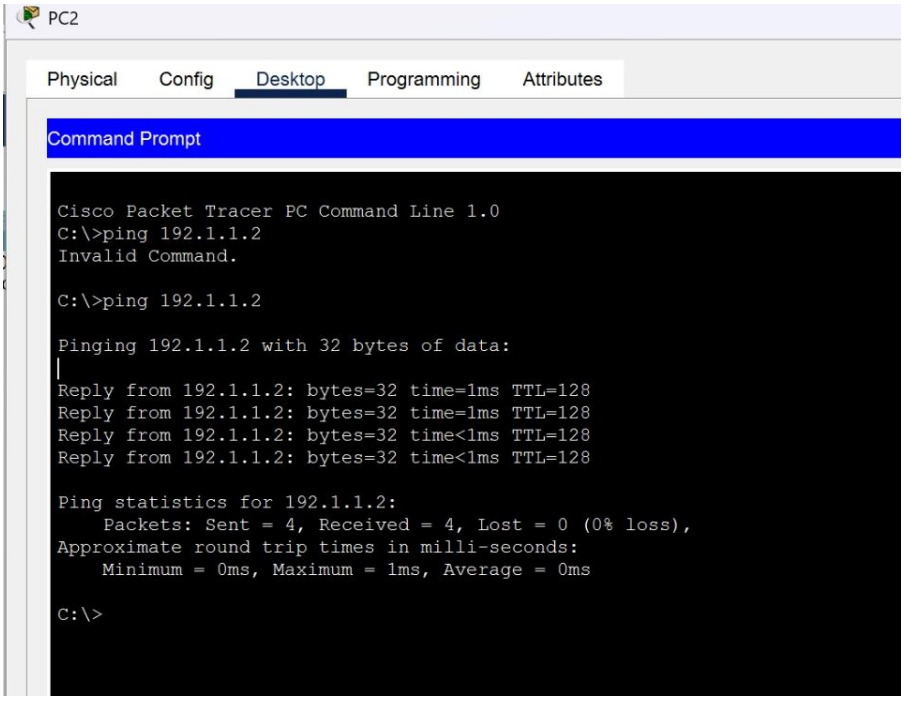
（4）切换到模拟模式，进入 “Edit Filters” 配置界面，勾选 ICMP 协议。通过简单报文工具启动从 PC1 到 PC0 的 ICMP 报文传输，可看到报文最终仅到达 PC0。



（5）切换回实时模式。在 PC2 中进入 “Config” - “FastEthernet0” 修改 MAC 地址，将其改为 PC0 的 MAC 地址 00E0.B040.6ED1，从而伪造 PC0 的 MAC 身份。



（6）通过简单报文工具启动 PC2 至 PC1 的 ICMP 报文传输。传输完成后，交换机的转发表发生变化：



- Switch1 中 MAC 00E0.B040.6ED1 的转发端口变为连接 Switch0 的 FastEthernet0/3；

MAC Table for Switch1

VLAN	Mac Address	Port
1	0006.2A93.7C51	FastEthernet0/2
1	0060.2FBB.D001	FastEthernet0/3
1	00E0.B040.6ED1	FastEthernet0/3

- Switch0 中对应转发端口变为连接 Switch2 的 FastEthernet0/1；

MAC Table for Switch0

VLAN	Mac Address	Port
1	0006.2A93.7C51	FastEthernet0/1
1	0060.2F76.CA02	FastEthernet0/2
1	00E0.B040.6ED1	FastEthernet0/2
1	00E0.F7CC.5A03	FastEthernet0/1

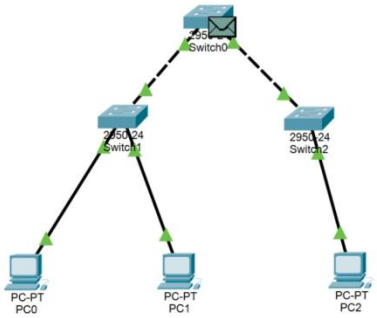
- Switch2 中对应转发端口变为连接 PC2 的 FastEthernet0/1。

MAC Table for Switch2

VLAN	Mac Address	Port
1	0006.2A93.7C51	FastEthernet0/2
1	0060.2FBB.D002	FastEthernet0/2
1	00E0.B040.6ED1	FastEthernet0/1

所有交换机现在将通往 PC2 的路径作为通往 MAC 地址 00E0.B040.6ED1 的路径。

（7）切换至模拟模式，使用简单报文工具启动 PC1 至 PC0 的 ICMP 报文传输。此时 ICMP 报文不再到达 PC0，而是被转发到 PC2，说明 MAC 地址欺骗成功生效。


Switch0
Switch1
Switch2
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2

五. 实验分析总结及心得

本次实验围绕交换机转发机制和 MAC 地址欺骗攻击展开，主要通过 Packet Tracer 模拟网络环境，实现了终端、交换机之间的 ICMP 报文传输和 MAC 表变化观察。实验内容涵盖了交换机转发表的建立、正常通信路径的形成、以及在 MAC 地址被伪造情况下的报文转发异常。

在实验过程中，我首先完成了 PC0、PC1 和 PC2 的 IP 地址和 MAC 地址配置，并验证了正常情况下各终端之间的 ICMP 通信。通过观察交换机 Switch0、Switch1 和 Switch2 的转发表，可以清楚地看到每个 MAC 地址对应的转发端口，理解了交换机根据 MAC 表进行帧转发的工作原理。接着，通过在 PC2 上伪造 PC0 的 MAC 地址并发送报文，我观察到各交换机的转发表发生相应更新，原本发送给 PC0 的 ICMP 报文被错误转发到 PC2，实现了 MAC 地址欺骗攻击。这一现象直观地展示了 MAC 欺骗对局域网通信安全的影响，同时验证了交换机转发机制的动态性与潜在风险。

通过本次实验，我对交换机的工作原理和 MAC 表管理有了更深入的理解。尤其是 MAC 地址欺骗攻击，使我意识到在实际网络中，交换机虽然可以高效转发数据，但也可能成为攻击目标，必须结合安全策略（如端口安全和动态 ARP 检测）来防护网络。实验还锻炼了我在模拟环境中配置网络、观察报文传输和分析转发表变化的能力，加强了对理论知识与实际操作的结合理解。

总体而言，本次实验不仅巩固了交换机基础配置与转发原理，也提升了我对局域网安全威胁的认识，为后续深入学习网络安全防护技术和攻击防御策略提供了实践基础。

实验四 网络攻击原理分析与验证实验

钓鱼攻击与防御实验·防 DHCP 欺骗攻击实验

一. 实验目的

2. 利用思科 Packet tracer 软件模拟实现利用相关协议进行攻击的实验；

2. 钓鱼攻击与防御实验

1）验证伪造的 DHCP 服务器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. 防 DHCP 欺骗攻击实验

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. 实验原理

1. 生成树协议的安全缺陷?

生成树协议依靠交换机之间自动选举根桥和路径。如果网络中出现恶意设备，它可以通过伪造更高优先级的参数来冒充根桥，导致网络拓扑被重新计算。这可能造成网络环路、延迟上升，甚至让部分网络无法正常通信。此外，协议本身缺乏认证机制，交换机无法判断对方参数是否可信。

2. DHCP 协议的安全缺陷?

DHCP 在分配 IP 地址时没有身份验证，任何人都可以伪装成客户端或服务器。如果攻击者假冒 DHCP 服务器，就可能向用户下发错误的网关、DNS 等信息，用户所有流量都会被错误引导。另外，攻击者还能通过大量伪造的请求耗尽地址池，让正常用户无法获得 IP。

3. 实施钓鱼攻击的方式有哪些?

常见的钓鱼方式主要有三类。第一类是伪造网站，攻击者搭建外观与真实网站相似的登录页面，引诱用户输入账号信息。第二类是伪造邮件或消息，内容通常带有紧急提示或诱惑，促使用户点击恶意链接或下载附件。第三类是社交工程，例如冒充同事、客服等，通过对话让受害者主动透露敏感信息。钓鱼的特点是利用人的信任和疏忽，因此不一定依赖复杂技术，但效果往往严重。

4. 钓鱼攻击与防御实验原理

终端通过广播 DHCP 发现消息查找 DHCP 服务器，当 DHCP 服务器与终端不在同一网络（同一广播域）时，由路由器进行中继。DHCP 服务器向终端发送 DHCP 提供消息以表明可以提供网络信息配置服务，终端会选择第一个到达的 DHCP 提供消息对应的服务器作为自己的 DHCP 服务器。

在终端所在网络中接入伪造的 DHCP 服务器后，终端广播的 DHCP 发现消息会到达伪造服务器。伪造的 DHCP 服务器在网络中广播 DHCP 提供消息，由于其与终端处于同一网络，它发送的消息可能早于真正的 DHCP 服务器的消息到达终端，从而使终端选择伪造的 DHCP 服务器提供服务，并将伪造 DNS 服务器的 IP 地址 192.1.3.1 作为本地域名服务器地址。

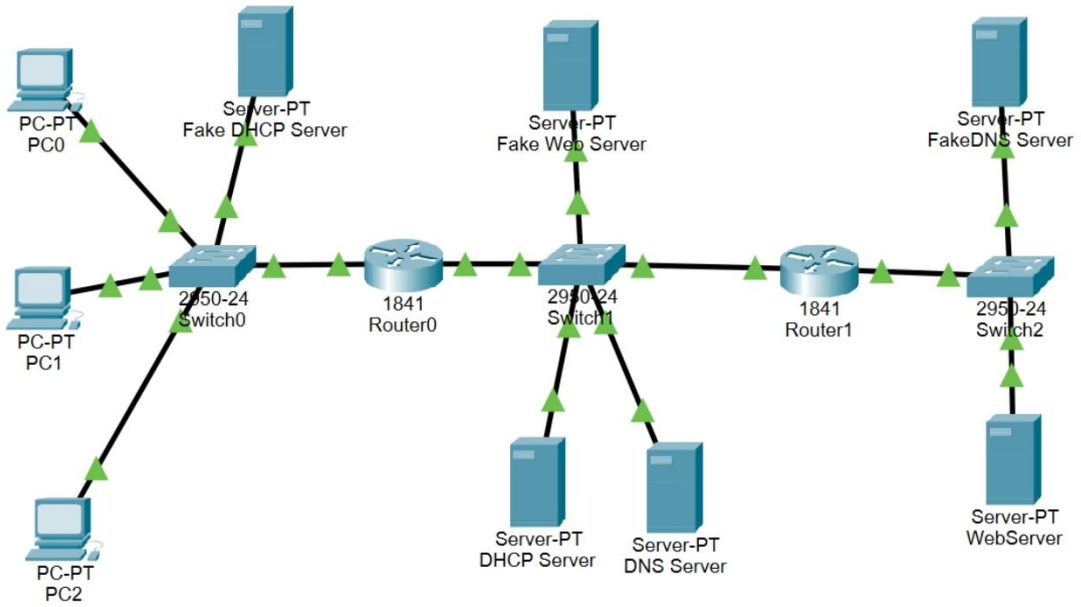
4. 防 DHCP 攻击实验原理

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 4.7 所示的网络应用系统，DHCP 服务器提供的本地域名服务器地址是 192.1.2.7，该地址对应的域名服务器中将完全合格域名 www.bank.com 绑定到 Web 服务器地址 192.1.3.7，因此终端可以使用域名 www.bank.com 访问正确的 Web 服务器。

一旦终端所在网络接入伪造的 DHCP 服务器，终端可能从伪造服务器获取网络信息，得到伪造的域名服务器 IP 地址 192.1.3.1，而伪造的域名服务器将完全合格域名 www.bank.com 与伪造 Web 服务器 IP 地址 192.1.2.5 绑定在一起，导致终端访问域名 www.bank.com 时访问的是伪造的 Web 服务器。

如果交换机启用防 DHCP 欺骗攻击功能，只有连接在信任端口的 DHCP 服务器才能为终端提供自动网络配置服务。对于如图 4.7 所示的网络系统，只需将连接路由器 R1 的交换机端口设置为信任端口，其它端口设置为非信任端口，终端则只能接收由路由器 R1 转发的 DHCP 消息，从而保证终端仅能获取合法 DHCP 服务器提供的网络信息。

三. 实验环境/实验拓扑图



四. 主要操作步骤及实验结果记录

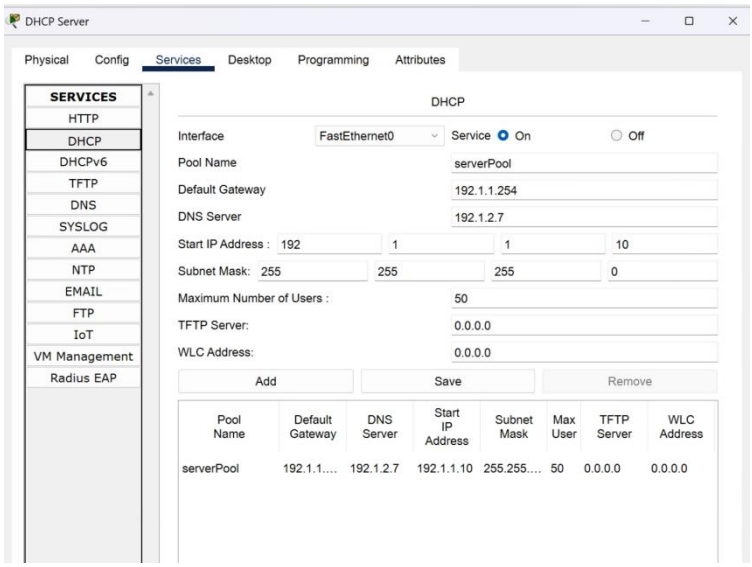
（1）首先搭建正常网络环境。在原有网络拓扑中去掉所有伪造服务器，根据精简后的拓扑放置并连接所有真实设备，使网络仅包含路由器、三台服务器及终端。完成设备放置和连线后，形成正常网络的逻辑结构。

（2）对两台路由器分别进行接口 IP 地址与子网掩码的配置，随后完成 RIP 路由协议的配置，使 Router1 与 Router2 建立完整的路由表，确保三台服务器与终端之间的路由可达。

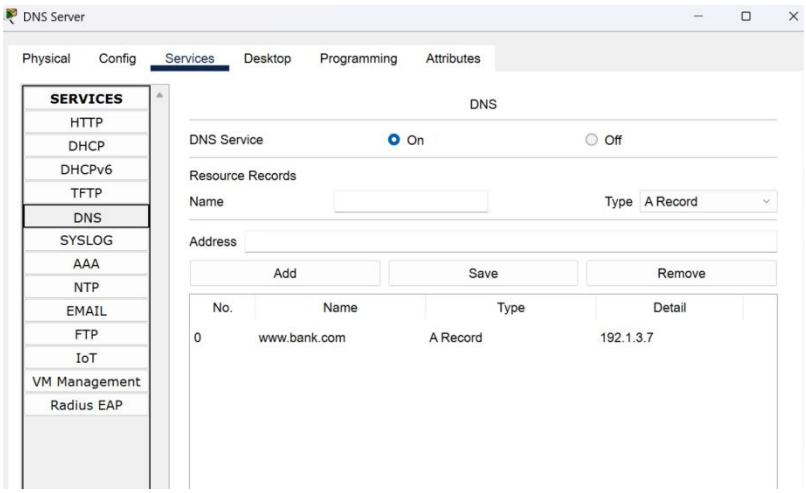
（3）在 Router1 上配置 FastEthernet0/0 接口的 DHCP 中继地址。该操作需要在命令行界面输入相应命令，使该接口能够将来自客户端的 DHCP 请求转发至 DHCP 服务器。

（4）根据网络拓扑中服务器的规划地址，为三台真实服务器分别配置 IP 地址、子网掩码和默认网关。默认网关应设置为其所在网络的路由器接口 IP 地址。由于 Router1 和 Router2 分别连接 DHCP 与 DNS 所在网络，服务器可任选与自身网络相连的路由器接口作为默认网关。

（5）在 DHCP 服务器中进入 Services → DHCP，开启 DHCP 服务。为作用域设置名称、默认网关（如 192.1.1.254）、DNS 服务器地址（如 192.1.2.7）、起始可分配地址（如 192.1.1.10）及最大用户数（如 50），从而定义地址池范围 192.1.1.10 至 192.1.1.59。

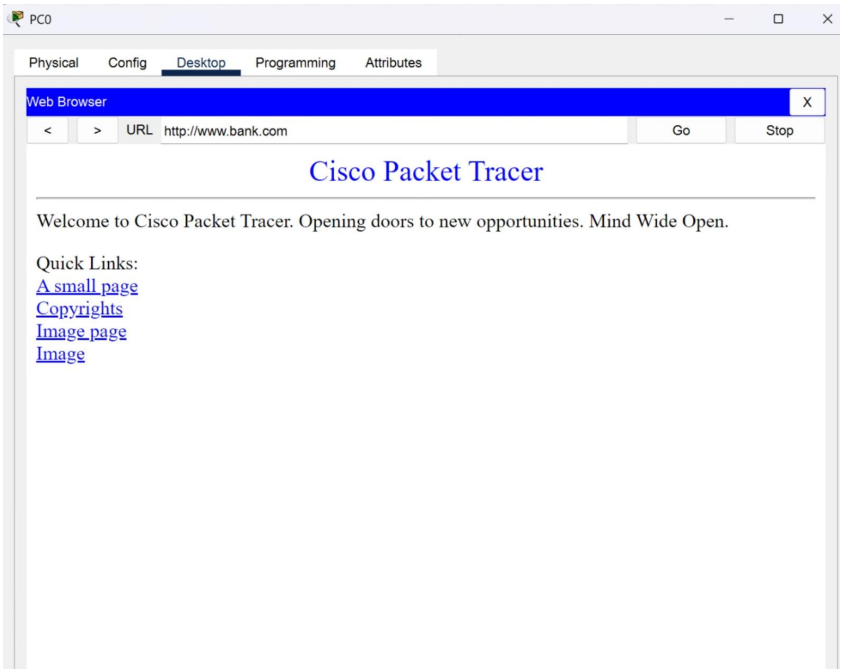


（6）在 DNS 服务器中进入 Services → DNS，开启 DNS 服务。在 Name 字段输入 www.bank.com，记录类型选择 A 记录，在 Address 字段填写该域名对应的真实 Web 服务器的 IP（如 192.1.3.7），完成资源记录的添加。

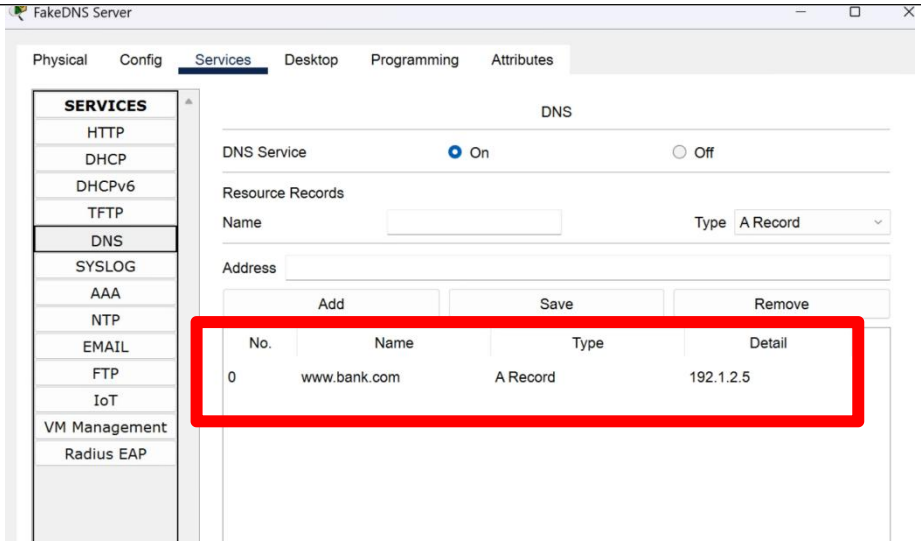


（7）在终端 PC0 的 Desktop → IP Configuration 中选择 DHCP，使其自动获取 IP 地址。终端将获得作用域范围内分配的地址（如 192.1.1.10），并同时获取正确的子网掩码、默认网关与 DNS 服务器地址。

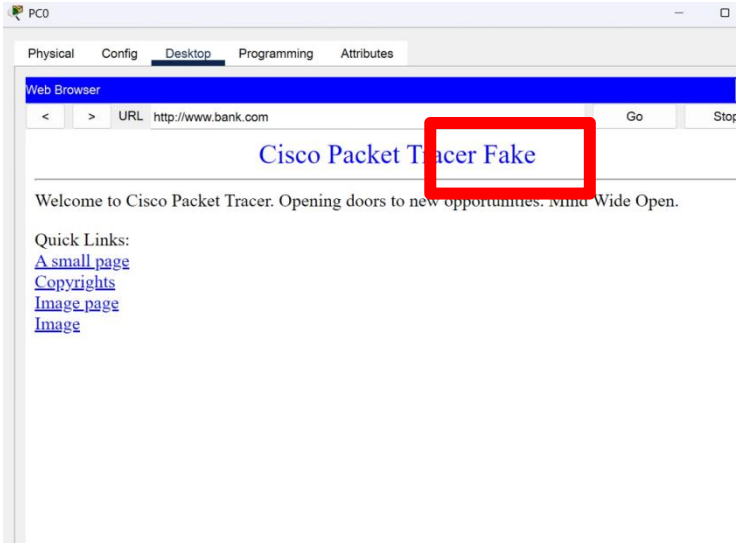
（8）在 PC0 通过 Desktop → Web Browser 输入 www.bank.com 并访问。由于 DNS 记录和路由均已正确配置，终端能成功访问真实的 Web 服务器。



（9）在此基础上加入三台伪造服务器（伪造 DHCP、伪造 DNS、伪造 Web），并为它们配置 IP 地址、子网掩码和默认网关。随后在伪造 DHCP 服务器中配置新的作用域，在伪造 DNS 服务器中添加同样的 www.bank.com 域名，但将其解析到伪造 Web 服务器的 IP。让 PC0 再次通过 DHCP 自动获取网络信息，可看到其 DNS 地址已变为伪造 DNS 的 IP（如 192.1.3.1），说明终端已从伪造 DHCP 获取配置。

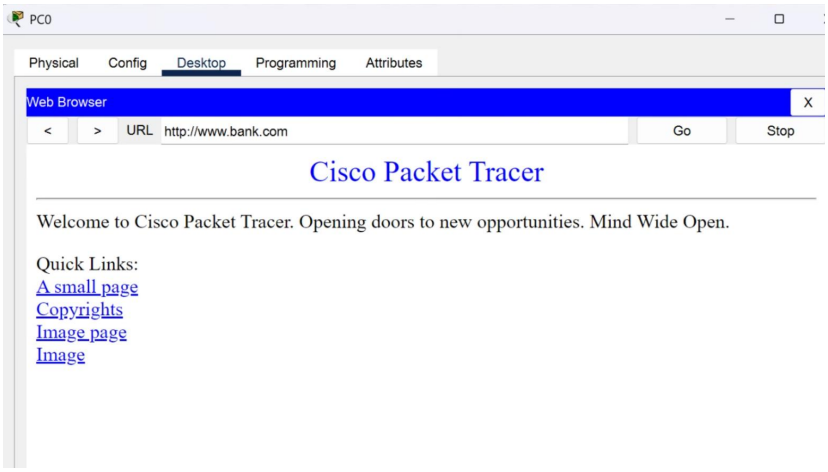


（10）此时 PC0 再次在浏览器中访问 www.bank.com，浏览器将根据伪造 DNS 的记录解析到伪造 Web 服务器，最终访问结果为伪造页面，从而验证了钓鱼攻击的效果。



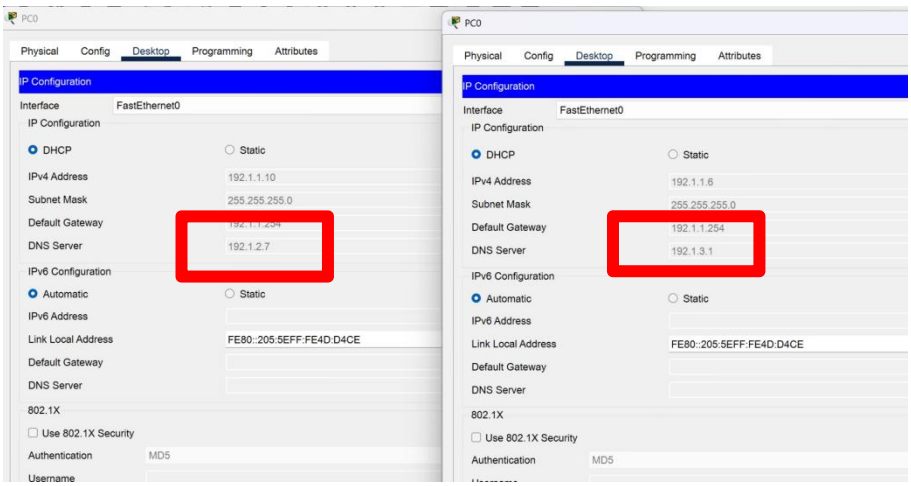
（10）在 Switch0 的 CLI（命令行接口）下输入用于启动交换机防 DHCP 欺骗攻击功能的命令序列。让 PC0、PC1、PC2 再次通过 DHCP 自动获取网络信息，发现 PC0、PC1、PC2 只从 DHCP 服务器获取网络信息。如图 4.11 所示，PC0 得到的 DNS 服务器地址是正确的 DNS 服务器 IP 地址 192.1.2.7，从而使 PC0 用完全合格的域名 www.bank.com 访问正确的 Web 服务器。

```
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#interface FastEthernet0/4
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
```



实验结果分析:

1、攻击与防御实验中 PC0 发出的 dhcp 请求收到了不同的 dhcp 服务器回复，从而被绑定了不同的 DNS 服务器地址。
2、当输入相同 url 时，DNS 解析得到的 ip 地址不同，访问到的实际 web 服务器不同，返回的网页不同，在交换机设置的端口安全策略成功防御了黑客部署的恶意 dhcp 服务器。



五. 实验分析总结及心得

通过本次基于 Cisco Packet Tracer 的实验，我对局域网环境中的 DHCP、DNS、Web 服务访问流程，以及伪造服务器实施网络钓鱼的原理有了更清晰的理解。在实验中，我首先搭建了正常的网络结构，配置路由器、服务器和客户端，使整个网络能够完成从 DHCP 自动获取地址到成功访问 Web 服务的完整流程。这个过程帮助我系统地梳理了地址分配、默认网关选择、DNS 解析和最终 Web 访问之间的关系，也加强了对基本网络配置命令和参数含义的掌握。

随后，通过在网络中加入伪造的 DHCP、DNS 和 Web 服务器，我直观地看到了伪造服务如何影响客户端的网络行为。例如，当伪造的 DHCP 服务器提供错误的 DNS 服务器地址时，PC 会在不知情的情况下将域名解析到伪造的 Web 服务器上，从而导致访问被引导到错误的网站。这个过程让我理解了网络诈骗和钓鱼攻击在现实环境中是如何利用协议缺陷和信任机制来误导用户的。

本次实验也让我意识到 DHCP 与 DNS 协议缺乏认证机制带来的安全风险，网络设备和服务器的配置顺序、参数准确性对整个网络是否正常运作也非常关键。在配置过程中，如果网关地址、地址池范围或 DNS 记录出现偏差，都会导致客户端无法访问网络服务，这对我后续进行网络排错提供了经验。

总体来说，本次实验不仅训练了我搭建网络、配置协议和观察数据包流动的能力，还让我更深刻地理解了网络基础服务的安全隐患和攻击方式。在实际网络环境中，如何防止伪造服务、保障关键协议的安全，将是后续学习和实践中需要持续关注的问题。

防生成树欺骗实验

一、 实验目的

(1) 验证交换机优先级对生成树构建的影响。

(2) 验证生成树生成过程。

(3) 验证生成树欺骗攻击原理。

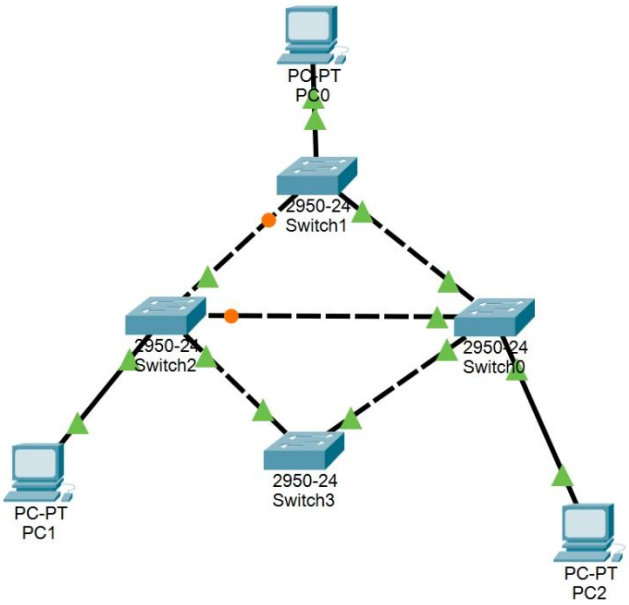
(4) 验证生成树欺骗攻击的实现过程。

二、 实验原理

将仿黑客终端的交换机的优先级设置为最高后，仿黑客终端的交换机成为根交换机，终端 A 与终端 B、终端 C 之间传输的数据都会经过仿黑客终端的交换机。

将交换机 S1 和 S3 上连接仿黑客终端交换机的端口设置为 BPDU 防护端口后，一旦仿黑客终端的交换机发送 BPDU，交换机 S1 和 S3 会立即关闭连接该仿黑客交换机的端口，导致仿黑客终端的交换机无法再与网络相连。这样，仿黑客终端的交换机将不再参与生成树的构建，也就不会成为重新构建后的生成树的一部分。终端之间传输的数据也不再通过仿黑客终端的交换机转发。

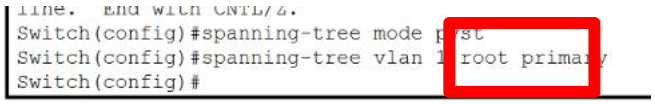
三、 实验环境/实验拓扑图



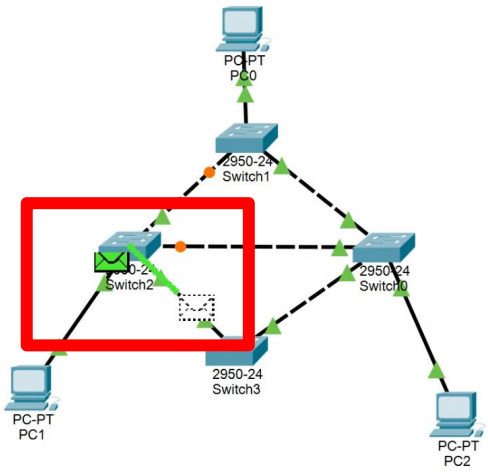
四、 主要操作步骤及实验结果记录

（1）根据图示的以太网结构放置和连接设备。

（2）完成终端网络信息配置过程。通过在交换机 CLI（命令行接口）中输入用于指定交换机生成树工作模式以及交换机优先级的命令序列，将仿黑客终端的交换机配置为根交换机。



（3）完成生成树构建过程后，切换到模拟操作模式，启动从 PC1 到 PC0 的 ICMP 报文传输，观察到这些 ICMP 报文会经过仿黑客终端的交换机。

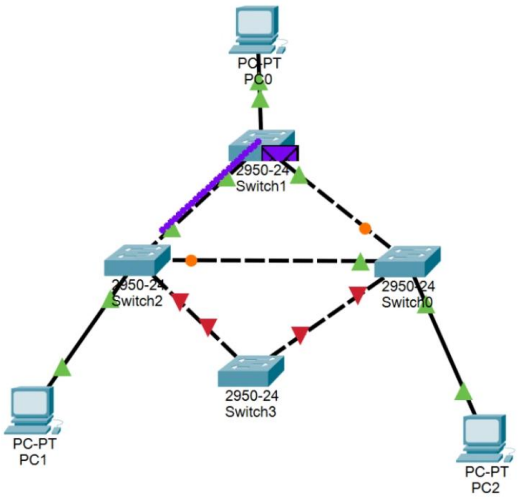


（4）通过在 CLI 中输入用于将交换机端口设置为 BPDU 防护端口的命令序列，将 Switch2 和 Switch0 上连接仿黑客终端交换机的端口（此处为 FastEthernet0/2）设置为 BPDU 防护端口。一旦仿黑客终端的交换机向 Switch2 和 Switch0 发送 BPDU，这两台交换机会立即关闭与仿黑客交换机相连的端口（FastEthernet0/2），使仿黑客终端的交换机与以太网隔离。

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/2 with BPDU
Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/2, putting 0/2 in err-disable state


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

Copy Paste

（5）仿黑客终端的交换机不再成为重新构建的生成树的一部分。切换到模拟操作模式，再次启动 PCO 至 PC1 的 ICMP 报文传输，观察到报文已不再经过仿黑客终端的交换机。



五、实验分析总结及心得

本次实验围绕生成树协议的运行机制及其在网络安全防护中的应用展开，重点验证了交换机优先级对生成树结构的影响，以及利用 BPDU 防护机制抵御生成树欺骗攻击的实际效果。通过对网络拓扑的构建、交换机优先级的配置、仿黑客终端交换机的引入及相应防护机制的启用，我对生成树协议的运行方式和网络安全防护策略有了更加直观和系统的认识。

在实验初始阶段，通过将仿黑客终端的交换机设置为最高优先级，可以观察到生成树在重构后将其选为根交换机。此时，从终端 PCO 到 PC1 的 ICMP 报文都必须经由该交换机转发，充分说明生成树协议是以优先级和 MAC 地址作为依据来选择根交换机的，因此恶意设备若提高自身优先级，就可能控制网络的转发路径。这一现象体现了生成树协议的潜在安全隐患，使我认识到在实际网络环境中不加防护地暴露 STP 会带来被攻击者利用的风险。

随后，当在 Switch1 和 Switch3 上将连接仿黑客交换机的端口设置为 BPDU 防护端口后，只要这些端口接收到来自仿黑客交换机的 BPDU，就会立即关闭端口，使该交换机从拓扑中被隔离。实验结果表明，一旦 BPDU Guard 功能生效，仿黑客终端交换机将无法再参与生成树重计算，也无法再成为网络路径的一部分。此时再次发送 ICMP 报文，可以清晰地看到报文转发路径恢复正常，不再经过仿黑客设备，这验证了 BPDU 防护在实际应用中能有效阻断生成树欺骗攻击。

通过本次实验，我深刻体会到生成树协议在提高二层网络可靠性方面的重要性，同时也认识到其本身存在的安全风险。恶意设备若故意伪造 BPDU 或提升优先级，就可能影响整个网络的稳定性。而 BPDU Guard、Root Guard 等机制则是网络管理员在部署安全策略时必须启用的重要功能，能够有效防止异常设备扰乱拓扑结构。

总的来说，本次实验帮助我系统掌握了生成树协议的构建过程、根交换机选举机制以

及 BPDU 防护的具体实现方法。在实际网络运维中，这些知识不仅有助于判断和解决 STP 相关故障，也能够提升网络架构在面对攻击时的整体防御能力。实验提升了我对二层网络安全威胁的认识，也为后续更复杂的网络安全实验打下了扎实基础。