实验(十五)：ARP消息分析实验

一.实验目的

- IP数据包在封装到以太网帧之前，需要获得下一跳IP地址的物理网络地址，TCP/IP协议使用ARP协议帮助进行IP地址解析，ARP协议（Address Resolution Protocol，地址解析协议）是网际层协议，作为联结IP协议和网络接口层的纽带，起着承上启下作用。本实验旨在：
  - 深入理解ARP的工作原理及其在网络通信中的重要作用
  - 通过分析ARP报文的结构和行为，学习如何从理论到实践应用ARP协议进行IP地址到MAC地址的映射
  - 利用工具观测和分析ARP通信过程。

二.实验原理

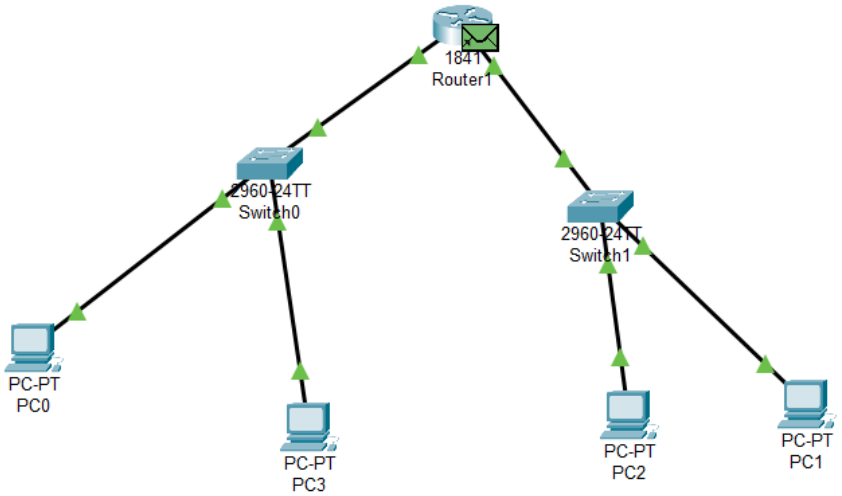
- `ARP（地址解析协议）`的核心功能是将网络层的IP地址转换为数据链路层的MAC地址，这一转换对于在以太网环境中的数据传输至关重要，因为数据链路层的通信依赖于MAC地址。实验中，我们通过两种方式展示地址转换过程：静态映射和动态映射。静态映射涉及手动创建ARP表来固定IP地址与MAC地址的关系，而动态映射则依赖于ARP和反向地址解析协议（RARP）来自动发现并记录这些地址。实验还包括了对ARP请求和响应流程的探讨，以及对ARP报文结构和字段的分析，从而全面理解ARP在网络中的工作机制和重要性。

三.实验环境

- 操作系统：Windows 10
- 网络环境：局域网
- 软件：`Cisco Packet Tracer`虚拟实验环境

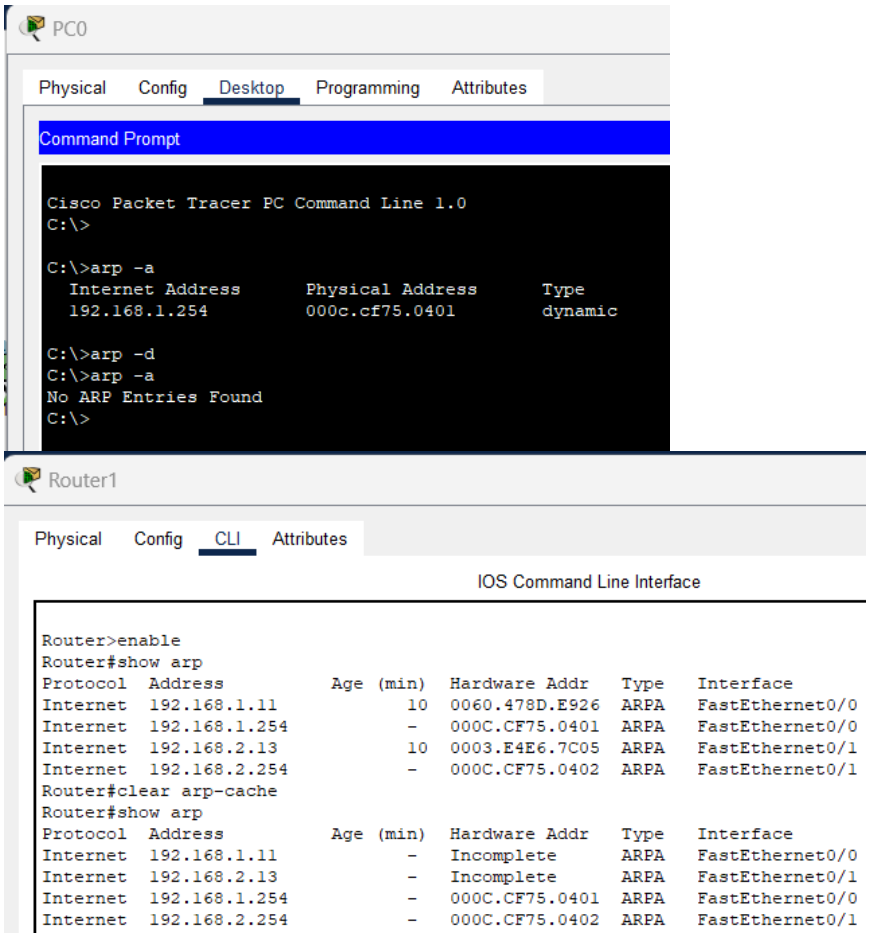
四.实验步骤

- 打开Cisco Packet Tracer虚拟实验环境，按照下面的网络结构图连线



- 使用`arp -d`清除PC端的`arp`缓存，使用`clear arp-cache`清空`Router0`的`arp`缓存

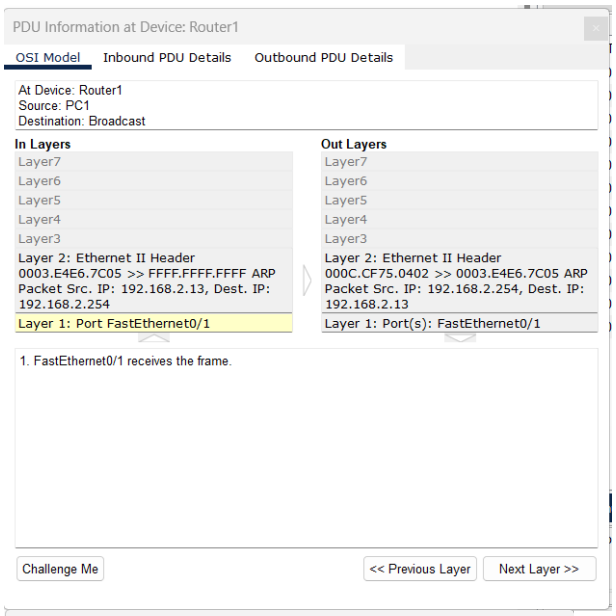
- 清理前后如下图所示：

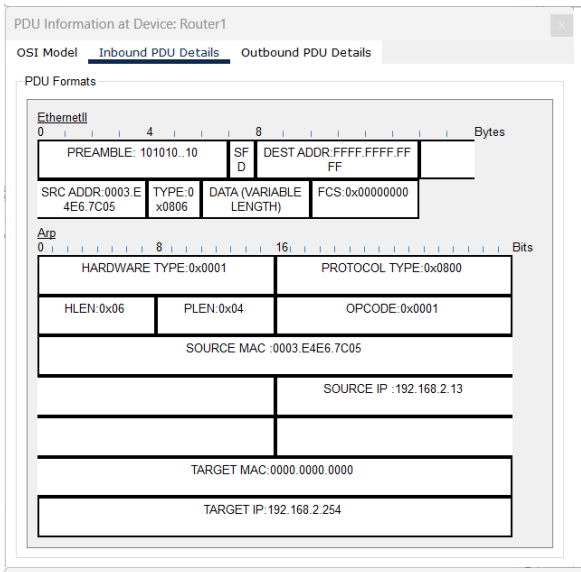


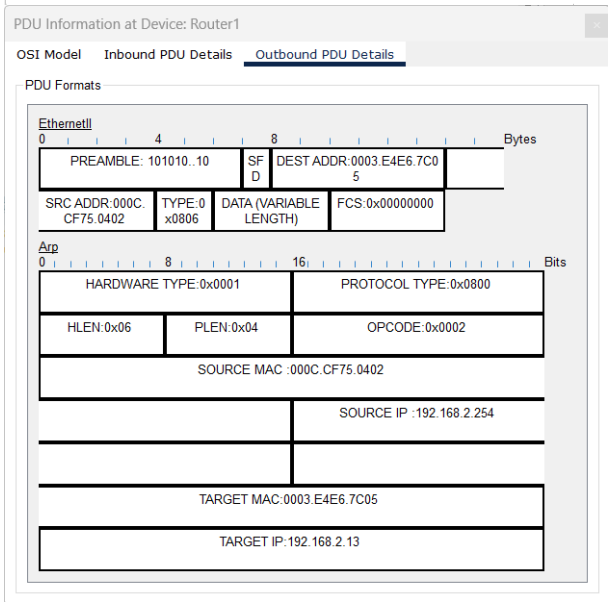
- 打开Simulation模式，使用PC1（`192.168.2.13`）去ping PC0（`192.162.1.11`）使用`simulation`去捕获其中的数据包，分析其中的ARP数据包
- 查看本机ARP内容
- 使用`WireShark`抓取ARP报文，对报文进行分析

五、实验现象

- **Cisco虚拟环境中的报文**
  - 以PC1->Router1为例分析ARP报文：

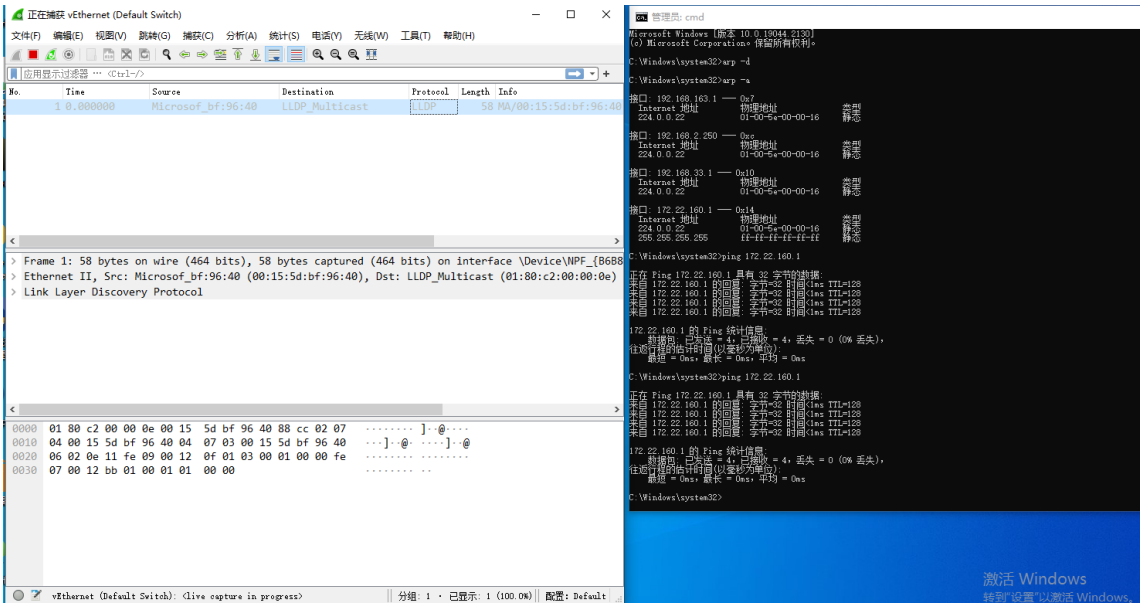






- **OSI Model**：展示了ARP请求报文是如何被Router1接收的。在OSI模型的第二层（数据链路层），`Ethernet II Header` 显示源MAC地址为 `0003.E4E6.7C05`（PC1），目的地MAC地址为广播地址 `FFFF.FFFF.FFFF`，表明这是一个广播帧。ARP包的源IP地址是 `192.168.2.13`（PC1），目的IP地址是 `192.168.2.254`（Router右端口），这说明主机试图解析IP地址 `192.168.2.254` 对应的MAC地址。
- **输入PDU详情**：详细描述了ARP请求的格式。

        - **硬件类型**（Hardware Type）：在这个ARP响应中，硬件类型为`0x0001`，指示这是一个以太网帧。
        - **硬件长度**（HLEN, Hardware Length）：为6，表示物理地址（MAC地址）的长度为6个字节。
        - **协议长度**（PLEN, Protocol Length）：为4，表示协议地址（IP地址）的长度为4个字节。
        - **操作码**（Opcode）：为`0x0001`，代表这是一个ARP请求报文。
        - **发送方MAC地址**（Sender MAC Address）：在ARP响应中，发送方的MAC地址为`0003.E4E6.7C05`，表示PC1的物理地址。
        - **发送方IP地址**（Sender IP Address）：与发送方MAC地址相对应的IP地址为`192.168.2.13`。
        - **目标MAC地址**（Target MAC Address）：由于是响应，这里填充了发起ARP请求的设备的MAC地址，即`0000.0000.0000`，因为这是一个ARP请求，发送方正在查询这个MAC地址。
        - **目标IP地址**（Target IP Address）：请求ARP解析的IP地址为`192.168.2.254`，请求相应的设备。
    - **输出PDU详情**：详细描述了ARP响应的格式。
        - **硬件类型**（Hardware Type）：在这个ARP响应中，硬件类型为`0x0001`，指示这是一个以太网帧。
        - **硬件长度**（HLEN, Hardware Length）：为6，表示物理地址（MAC地址）的长度为6个字节。
        - **协议长度**（PLEN, Protocol Length）：为4，表示协议地址（IP地址）的长度为4个字节。
        - **操作码**（Opcode）：为`0x2`，代表这是一个ARP响应报文。
        - **发送方MAC地址**（Sender MAC Address）：在ARP响应中，发送方的MAC地址为`000C.CF75.0402`，表示Router1右端口的物理地址。
        - **发送方IP地址**（Sender IP Address）：与发送方MAC地址相对应的IP地址为`192.168.2.254`。
        - **目标MAC地址**（Target MAC Address）：由于是响应，这里填充了发起ARP请求的设备的MAC地址，即`0003.E4E6.7C05`。
        - **目标IP地址**（Target IP Address）：请求ARP解析的IP地址为`192.168.2.13`，对应于发起请求的设备。
- **本机ARP内容**



- ARP请求包含以下信息：
  - `Hardware type` 使用的硬件类型：这里的 `1` 代表以太网。
  - `Protocol type` 协议类型： `0x0800` 是IPv4地址。
  - `Hardware size` 硬件地址的长度：这里是6，对应于MAC地址的字节长度。
  - `Protocol size` 协议地址的长度：这里是4，对应于IPv4地址的字节长度。
  - `Opcode` 操作码：1代表这是一个ARP请求。
  - `Sender MAC address` 发送者的MAC地址：与上面的Src字段相同。
  - `Sender IP address` 发送者的IP地址：这里是 `172.22.160.4`。
  - `Target MAC address` 目标MAC地址：在ARP请求中这通常是0，因为这是正在查询的地址。
  - `Target IP address` 目标IP地址：这里是 `172.22.160.1`。发送者想要知道这个IP地址对应的MAC地址。

六、实验结论

- **实验结论分析**：
  在网络中实施RIP之前，通常会观察到个别PC无法成功执行ping命令以通信。这是因为缺乏必要的路由信息，导致数据包无法找到正确的路径到达目的地。然而，一旦在网络中的一个路由器上配置了RIP，该路由器与直连PC之间的通信就变得可行，这是因为路由器开始广播它所知道的路由信息。尽管如此，在另一个路由器未配置RIP的情况下，跨路由器的通信可能仍然受阻。只有当网络中的所有路由器都配置了RIP并开始交换路由信息时，整个网络的设备才能实现全互通。这种观察结果突出了RIP协议在维护网络连通性中的作用和效能。

- **RIP的基本工作原理**：
  RIP是一种基于距离矢量的动态路由选择协议，它采用跳数作为衡量路径成本的度量。跳数是指一个数据包在到达目的地前需要通过的路由器数量。在RIP协议中，路径的最大有效跳数被限定为15跳，超过这个数值的路径会被视为不可达。RIP通过每30秒的定期广播来交换路由信息，或者当网络拓扑发生变化时立即发送更新，这样可以确保路由表保持最新状态，从而支持有效的网络路由决策。

- **RIP配置的重要性**：
  在实验的初期阶段，若没有进行RIP配置，网络设备的路由表将只包含直接连接的网络信息。这意味着设备将不能识别或联系到其他路由器管理下的网络，因为它们没有这些网络的路由信息。一旦通过RIP配置了路由器，路由器就能够广播其路由表，包括学习到的新路由信息，从而实现网络中更广泛的通信能力。

- **动态路由协议的优势**：
  RIP等动态路由协议提供了多方面的优势。它们可以自动地响应网络拓扑的变化，更新路由信息，这为网络管理员减轻了工作负担，并减少了因人为错误导致的网络问题。动态路由使网络可以在设备故障或其他变化发生时自行恢复和适应，确保网络的稳定性和弹性。此外，动态路由协议增强了网络的扩展性，因为新增的路由器或网络可以被自动发现并纳入到现有的路由结构中。