实验一 ARP协议抓包

（一）ARP协议简介

ARP（地址解析协议，Address Resolution Protocol）是 TCP/IP 协议栈中的关键底层协议，主要用于将IP 地址解析为对应的 MAC 地址（数据链路层物理地址），从而实现不同设备在局域网内的通信。以下是其核心工作原理的详细解析：

一、核心功能

- **地址映射**：将目标设备的 IP 地址转换为对应的 MAC 地址，以便数据帧能在局域网中正确传输。
- **通信基础**：在以太网等链路层协议中，数据传输依赖 MAC 地址，ARP 为 IP 层提供了跨层转换的桥梁。

二、ARP协议工作原理

1、ARP 协议的核心目标

在 TCP/IP 模型中：

- **网络层**使用 IP 地址标识设备（如`192.168.1.100`）。
- **数据链路层**使用 MAC 地址标识设备（如`00-0C-29-12-34-AB`）。**ARP 的作用**：建立 IP 地址与 MAC 地址的映射关系，使网络层数据能封装成数据链路层帧进行传输。

2、ARP 协议的工作流程

1）. 场景假设

主机 A（IP:`192.168.1.100`，MAC:`A1-A2-A3-A4-A5-A6`）需要向主机 B（IP:`192.168.1.200`）发送数据，但不知道主机 B 的 MAC 地址。

2）. 步骤解析

步骤 1：发送 ARP 请求（广播）

- **主机 A 的操作**：
  - 检查本地**ARP 缓存表**（存储 IP-MAC 映射的临时表），若找不到主机 B 的 IP 对应的 MAC 地址，则触发 ARP 解析流程。
  - 构造一个**ARP 请求数据包**，内容包括：
    - **发送方 IP**：`192.168.1.100`，**发送方 MAC**：`A1-A2-A3-A4-A5-A6`。

        - **目标 IP**：`192.168.1.200`，**目标 MAC**：全 0（`00-00-00-00-00-00`，表示未知）。
    - 将 ARP 请求封装在**以太网广播帧**中（目标 MAC 为`FF-FF-FF-FF-FF-FF`），通过网卡发送到局域网。
- **网络中的行为**：局域网内所有设备（如主机 B、交换机、路由器等）都会收到该广播包，但**只有目标 IP 匹配的主机 B 会处理**，其他设备直接丢弃。

步骤 2：主机 B 响应 ARP 请求（单播）

- **主机 B 的操作**：
    - 解析 ARP 请求包，提取发送方 IP（`192.168.1.100`）和 MAC 地址（`A1-A2-A3-A4-A5-A6`），并将此映射关系存入自己的**ARP 缓存表**（用于后续通信）。
    - 构造**ARP 响应数据包**，内容包括：
        - **发送方 IP**：`192.168.1.200`，**发送方 MAC**：`B1-B2-B3-B4-B5-B6`（主机 B 的真实 MAC）。
        - **目标 IP**：`192.168.1.100`，**目标 MAC**：`A1-A2-A3-A4-A5-A6`（主机 A 的 MAC）。
    - 将 ARP 响应封装在**以太网单播帧**中（目标 MAC 为`A1-A2-A3-A4-A5-A6`），直接发送回主机 A。

步骤 3：主机 A 更新 ARP 缓存表

- 主机 A 收到响应后，从包中提取主机 B 的 IP（`192.168.1.200`）和 MAC 地址（`B1-B2-B3-B4-B5-B6`），存入本地 ARP 缓存表。
- **后续通信**：主机 A 向主机 B 发送数据时，直接从缓存表中获取 MAC 地址，无需再次广播请求。

3、ARP 缓存表（ARP Table）

作用

- 存储 IP 地址与 MAC 地址的映射关系，避免重复发送 ARP 请求，提高通信效率。
- **缓存时效**：表中的条目有生存周期（通常为几分钟，可通过`arp -v`命令查看），超时后自动删除，确保映射关系及时更新。

三、ARP包

ARP 包（地址解析协议数据包） 是 ARP 协议在网络中传输的具体数据单元，用于实现 IP 地址与 MAC 地址的解析和交互。以下是关于 ARP 包的详细解析：

1、核心功能

- **地址映射**：将目标设备的 IP 地址转换为对应的 MAC 地址，以便数据帧能在局域网中正确传输。
- **通信基础**：在以太网等链路层协议中，数据传输依赖 MAC 地址，ARP 为 IP 层提供了跨层转换的桥梁。

2、工作原理

1）. ARP 请求（广播）

- 当主机 A 需要与主机 B 通信时，先检查自身的**ARP 缓存表**（存储 IP-MAC 映射关系）。
- 若缓存中无主机 B 的记录，主机 A 会发送一个**广播包**（目标 MAC 为全 F：FF-FF-FF-FF-FF-FF），内容包含：
  - 自身 IP 地址和 MAC 地址；
  - 目标 IP 地址（主机 B 的 IP），请求对应的 MAC 地址。

2）. ARP 响应（单播）

- 局域网内所有设备都会收到广播包，但只有目标主机 B 会解析并响应：
  - 主机 B 将主机 A 的 IP-MAC 信息存入自己的 ARP 缓存表；
  - 主机 B 向主机 A 发送**单播响应包**，包含自身的 MAC 地址。

3. 缓存更新

- 主机 A 收到响应后，更新 ARP 缓存表，后续通信直接使用缓存中的 MAC 地址。
- 缓存条目有**生存时间（TTL）**（通常几分钟），超时后自动删除，确保映射关系实时有效。

4、关键术语与概念

1）ARP 缓存表

- 存储 IP 地址与 MAC 地址的映射关系，可通过命令查看：
  - Windows：`arp -a`
  - Linux/macOS：`arp -n` 或 `ip neighbor show`

2）ARP 欺骗（ARP 攻击）

- 恶意设备伪造 ARP 响应，将错误的 MAC 地址注入其他主机的缓存表，导致通信流量被劫持或中断（如中间人攻击）。

3）免费 ARP（Gratuitous ARP）

- 主机主动发送 ARP 响应包（即使无请求），用于更新他人缓存或检测 IP 冲突（如服务器上线时）。

（二）实验环境

抓取ARP包可以通过Cisco Packet Tracer 或是Wireshark软件进行，两者的区别在于前者是仿真模式，后者是真实的抓取本机发送或获取的ARP包。具体步骤如下：

一、使用Packet Tracer6.2软件抓取ARP包

1、实验目的

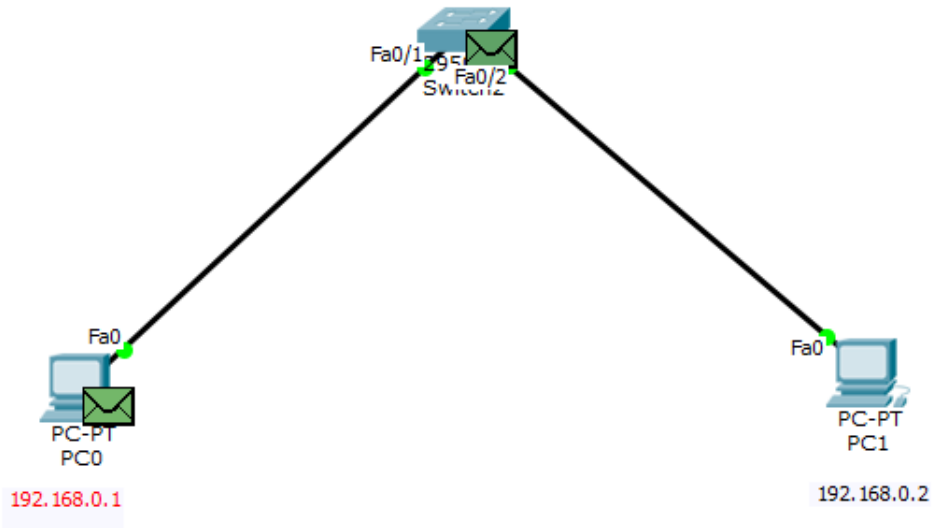
通过模拟局域网环境，观察 ARP 协议工作流程，解析 ARP 报文核心字段。

2、实验拓扑

实验网络拓扑采用以下网络拓扑图，

3、实验步骤

3.1 网络拓扑配置



添加2台PC和一台二层交换机，如上图所示，两台PC。

ARP Table for PC0

IP Address	Hardware Address	Interface
192.168.0.2	0001.6362.3987	FastEthernet0

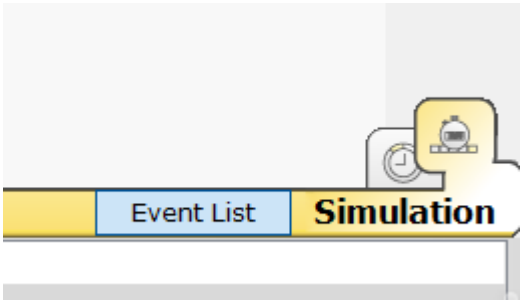
ARP Table for PC1

IP Address	Hardware Address	Interface
192.168.0.1	0003.E420.B519	FastEthernet0

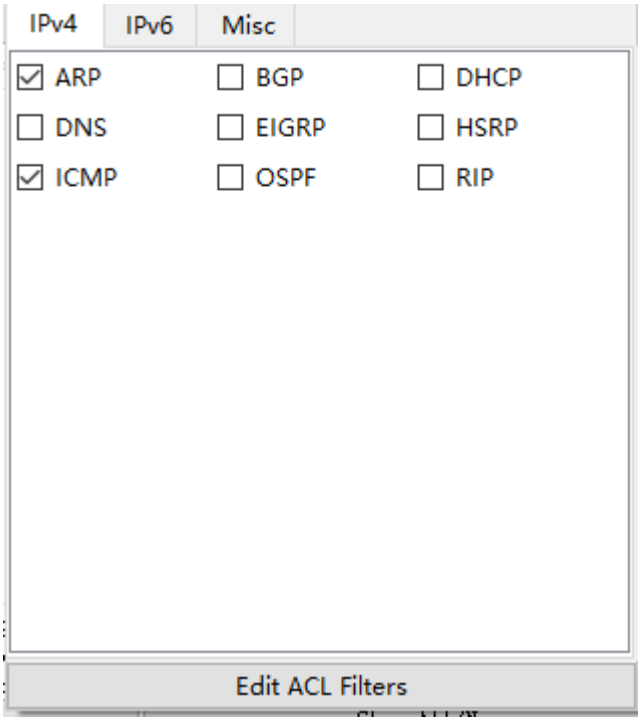
3.2 IP配置与交换机配置

IP地址如上图进行设置，主机IP地址不能相同，子网掩码为255.255.255.0，二层交换机不用设置。

3.3 切换至模拟模式并设置过滤



- 点击软件右下角 **Simulation**按钮（沙漏图标），进入模拟模式。
- 点击工具栏 **Edit Filters**按钮，在弹出窗口勾选 **ARP** 和 **ICMP** 协议，点击 **OK**。



3.4 触发 ARP 交互并捕获报文

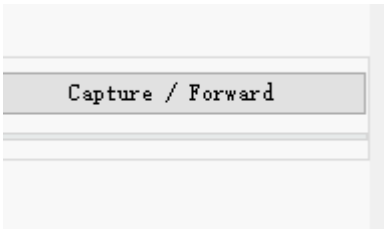
- **清除 PC0的 ARP 缓存**：双击 PC0 → **Command Prompt**，输入：

```
arp -d  # 清除现有ARP缓存
```

- **发送 ping 命令触发 ARP 请求**：继续输入：

```
ping 192.168.0.2  # 向PC1发送ICMP请求，强制触发ARP解析
```

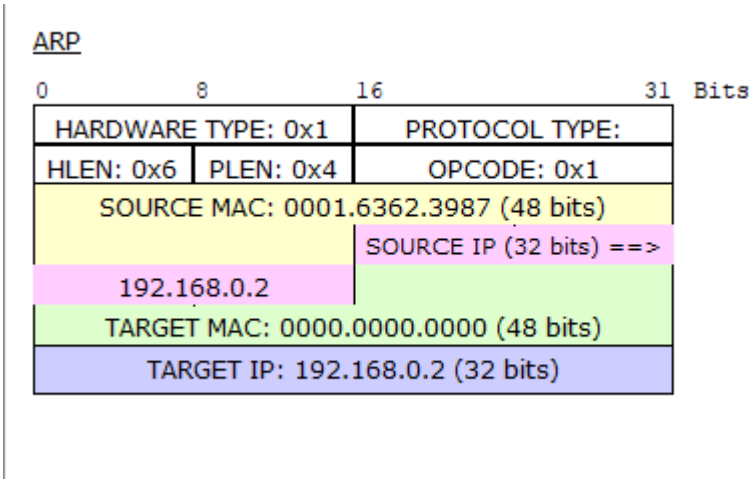
- **开始抓包**：点击模拟模式工具栏 **Auto Capture/Play**按钮（自动捕获），或手动点击 **Capture/Forward** 逐帧捕获。



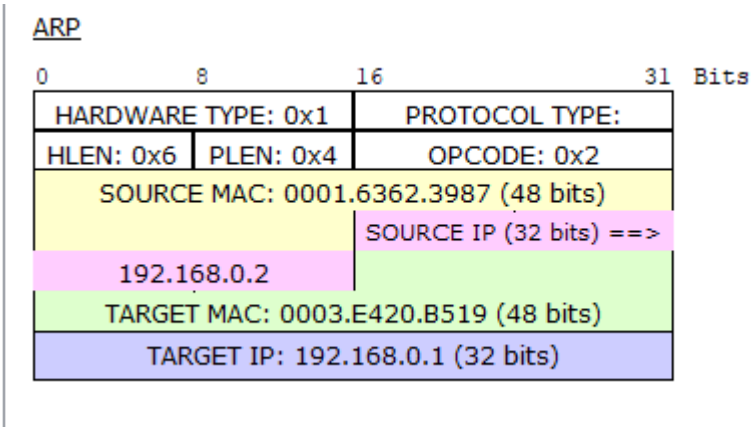
3.5 分析 ARP 报文细节

- **查看事件列表**：在模拟模式下方 **Event List**中，找到类型为 **ARP Request**（广播请求）和 **ARP Reply**（单播应答）的事件。

- **解析PDU内容**：点击事件右侧的彩色正方形图标，在弹出窗口查看：
  - **ARP 请求报文**（Outbound PDU Details）：
    - **Hardware Type**：1（以太网）
    - **Operation Code**：1（请求）



    - **Target MAC Address**：FF:FF:FF:FF:FF:FF（广播地址）
  - **ARP 应答报文**（Inbound PDU Details）：
    - **Operation Code**：2（应答）
    - **Sender MAC Address**：PC1的物理地址（可通过 PC1的**Command Prompt**输入 ipconfig /all查看）



3.6 验证 ARP 缓存

- 在 PC0 的命令提示符中输入：

```
arp -a  # 查看ARP缓存表，确认PC1的IP与MAC地址已绑定
```

二、Wireshark 4.2.2 本地 ARP 报文分析

通过在真实网络环境下运行Wireshark ，深入分析 ARP 报文底层结构。

1、实验目的

通过在真实网络环境下运行Wireshark ，深入分析 ARP 报文底层结构。

2、实验准备

1. 关闭本地防火墙（避免拦截网络流量）。
2. 记录本地网卡名称（如 "以太网" 或 "WLAN"，可通过控制面板→网络和共享中心查看）。

3、实验步骤

3.1 启动 Wireshark 并设置过滤

- 打开 Wireshark 4.0.8，在**接口列表**中选择本地连接的网卡（如 "以太网"），点击右侧 **开始捕获**。
- 在顶部过滤栏输入 arp并回车，仅显示 ARP 协议报文。

3.2 清除并观察 ARP 缓存

- 以管理员身份打开命令提示符，输入：

```
arp -d  # 清除本地ARP缓存
arp -a  # 此时ARP缓存应为空，无目标IP记录
```

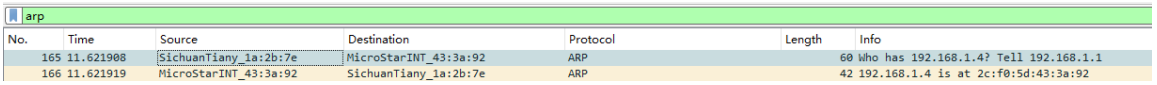
3.3 触发 ARP 请求

- 在命令提示符中输入：

```
ping 192.168.1.4  # ping同网段未通信过的IP（比如，同桌的IP），强制触发ARP请求
```

3.4 解析报文结构

- 在 Wireshark 捕获列表中找到 **ARP Request**（广播）和 **ARP Reply**（单播）报文（一般成对出现），展开字段分析：



- ARP请求报文

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: SichuanTiany_1a:2b:7e (04:6b:25:1a:2b:7e)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.4
```

ARP应答报文

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: MicroStarINT_43:3a:92 (2c:f0:5d:43:3a:92)
    Sender IP address: 192.168.1.4
    Target MAC address: SichuanTiany_1a:2b:7e (04:6b:25:1a:2b:7e)
    Target IP address: 192.168.1.1
```

  - **以太网头部**：
    - 源 MAC 地址：本地网卡物理地址（与ipconfig /all一致）
    - 目标 MAC 地址：请求报文为FF:FF:FF:FF:FF:FF（广播），应答报文为目标主机 MAC 地址
  - **ARP 头部**：
    - **Hardware address length**：6（以太网 MAC 地址长度）

- **Protocol address length**：4（IPv4 地址长度）
- **Sender IP address**：本地 IP 地址
- **Target IP address**：目标 IP 地址（即步骤 3 中 ping 的 IP）

验证一致性

- 再次输入 arp -a，确认目标 IP 对应的 MAC 地址与 Wireshark 捕获的应答报文完全一致。

实验现象对比与工具差异

（一）核心现象总结

阶段	Packet Tracer 6.2模拟环境	Wireshark 真实环境
请求发送	广播包（目标 MAC 为全 F）	广播包（目标 MAC 为全 F）
应答返回	单播包（携带目标主机 MAC）	单播包（携带目标主机 MAC）
缓存更新	PC0 的 ARP 缓存表新增 PC1 的 IP-MAC 映射	本地 ARP 缓存新增目标 IP-MAC 映射

（二）工具特性对比

特性	Packet Tracer 6.2	Wireshark 4.2.2
环境类型	网络模拟（虚拟设备）	真实网络（本地网卡实时流量）
抓包方式	模拟模式下事件驱动（需手动控制）	网卡实时监听（自动捕获）
报文展示	分层显示 PDU 结构（简化版）	完整协议栈解析（含底层数据）
适用场景	教学演示、协议流程可视化	真实网络故障排查、协议深度分析

注意事项

（一）Packet Tracer 6.2软件特别说明

1. **仅支持模拟模式抓包**：实时模式（Realtime Mode）下无法捕获 ARP 报文，必须通过右下角**Simulation**按钮切换至模拟模式。
2. **过滤条件设置**：若未勾选 ARP 协议，事件列表可能包含 DHCP、DNS 等无关报文，建议仅保留 ARP 和 ICMP 过滤。
3. **PDU 查看技巧**：点击事件右侧图标后，通过**Outbound/Inbound PDU Details**选项卡区分请求与应答报文。

（二）通用注意事项

1. **管理员权限**：Windows 系统下执行arp -d和 Wireshark 抓包时，建议以管理员身份运行程序，避免权限不足问题。
2. **版本兼容性**：严格使用指定版本（Packet Tracer 5.3/Wireshark 4.0.8），高版本工具的操作界面和抓包逻辑可能存在差异。

实验报告要求

1. **报文对比**：列表记录两种工具捕获的 ARP 请求 / 应答报文的关键字段（如硬件类型、操作码、目标 MAC），分析差异原因。
2. **协议原理**：简述 ARP 协议的工作流程，说明 "为何需要 ARP 协议实现 IP 到 MAC 的映射"。
3. **工具总结**：结合实验体验，总结 Packet Tracer 6.2 与 Wireshark 在网络协议分析中的适用场景与优缺点。

PDU