**【实验名称】：**以太网帧分析实验

**学生姓名：2151133**孙韩雅

**实验地点：**济事楼330 **实验时间：**2023-11-20

**【实验目的】**

了解以太网的背景，发展历史，发展现状等基本知识，通过分析以太网帧了解以太网数据包传输原理。学习使用WireShark抓包软件的使用，对其抓包内容做实际分析解读。

**【实验原理】**

1.以太网概念

以太网是一种计算机局域网技术。IEEE组织的IEEE 802.3标准制定了以太网的技术标准，它规定了包括物理层的连线、电子信号和介质访问层协议的内容。以太网是目前应用最普遍的局域网技术。以太网是现实世界中最普遍的一种计算机网络。以太网有两类：第一类是经典以太网，第二类是交换式以太网，使用了一种称为交换机的设备连接不同的计算机。

经典以太网是以太网的原始形式，运行速度从3~10 Mbps不等；而交换式以太网正是广泛应用的以太网，可运行在100、1000和10000Mbps那样的高速率，分别以快速以太网、千兆以太网和万兆以太网的形式呈现。以太网的标准拓扑结构为总线型拓扑，但目前的快速以太网（100BASE-T、1000BASE-T标准）为了减少冲突，将能提高的网络速度和使用效率最大化，使用交换机来进行网络连接和组织。如此一来，以太网的拓扑结构就成了星型；但在逻辑上，以太网仍然使用总线型拓扑和CSMA/CD（Carrier Sense Multiple Access/Collision Detection，即载波多重访问/碰撞侦测）的总线技术。每一个节点有全球唯一的48位地址也就是制造商分配给网卡的MAC地址，以保证以太网上所有节点能互相鉴别。由于以太网十分普遍，许多制造商把以太网卡直接集成进计算机主板。

2.MAC地址

MAC地址也叫物理地址、硬件地址，由网络设备制造商生产时烧录在网卡(Network lnterface Card)的EPROM(一种闪存芯片，通常可以通过程序擦写) 。MAC地址的长度为48位(6个字节)，通常表示为12个16进制数，如：00-16-EA-AE-3C-40就是一个MAC地址，其中前3个字节，16进制数00-16-EA代表网络硬件制造商的编号，它由IEEE(电气与电子工程师协会)分配，而后3个字节，16进制数AE-3C-40代表该制造商所制造的某个网络产品(如网卡)的系列号。MAC地址在世界是唯一的。

MAC地址由网络其前3字节表示OUI（Organizationally Unique Identifier），是IEEE的注册管理机构给不同厂家分配的代码，区分不同的厂家。后3字节由厂家自行分配MAC地址最高字节（MSB）的低第二位（LSb）表示这个MAC地址是全局的还是本地的，即U/L（Universal/Local）位，如果为0，表示是全局地址。所有的OUI这一位都是0。MAC地址最高字节（MSB）的低第一位 (LSb），表示这个MAC地址是单播还是多播。0表示单播。

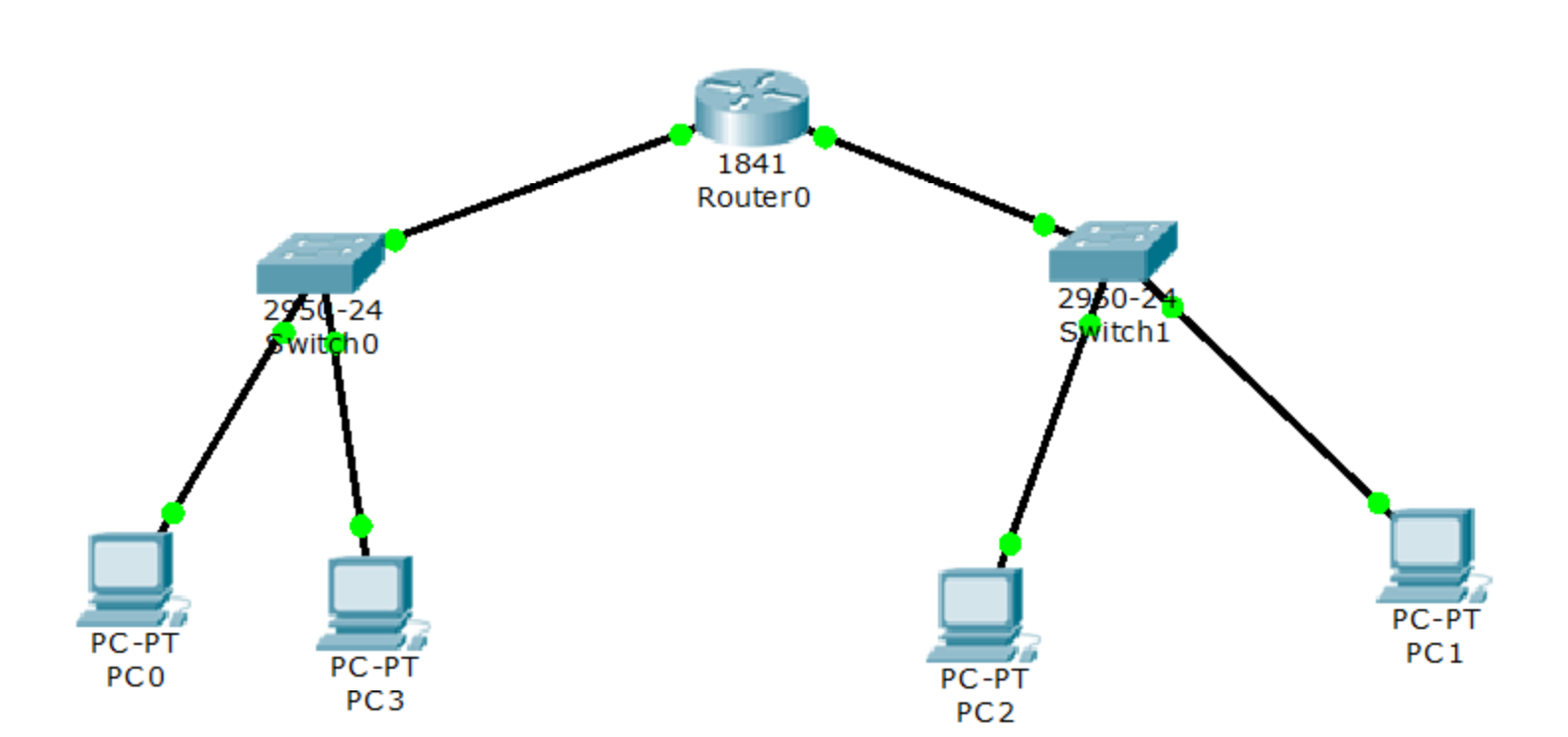
3.MAC数据包格式（概念略）。

**【实验设备】**

HUAWEI MateBook X Pro（安装有Cisco Packet Tracer与Wireshark抓包分析工具）

【**实验步骤**】

1.首先规划网络地址及拓扑图路由器的DHCP配置：



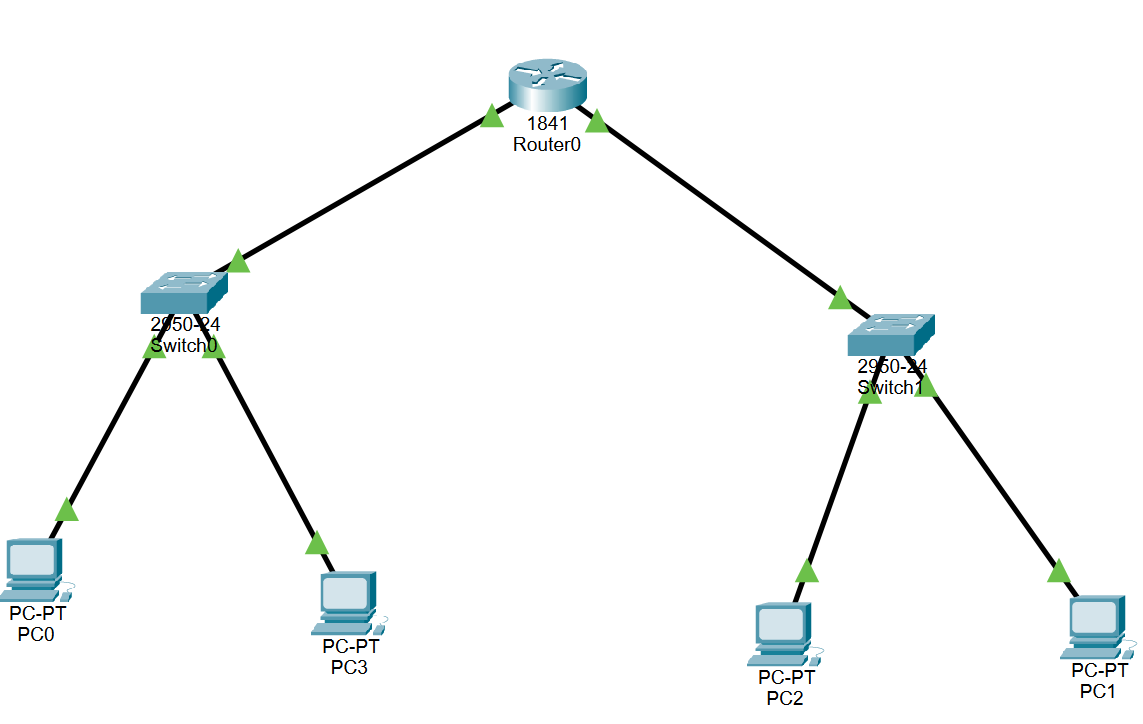
2.配置DHCP。

3.模拟ICMP包的传输过程。

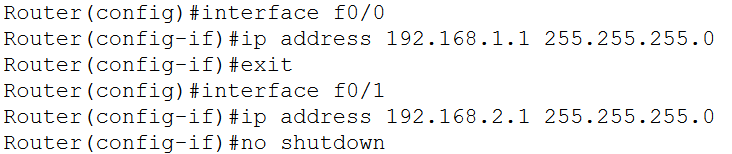
4.下载安装wireshark软件，使用其进行MAC数据包相关的实验。

**【实验现象】**

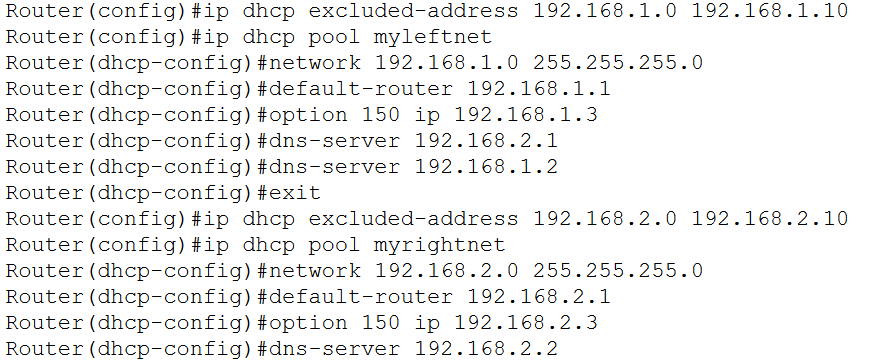
1.按照拓扑图进行连线：



2.进行路由器接口的相关配置。



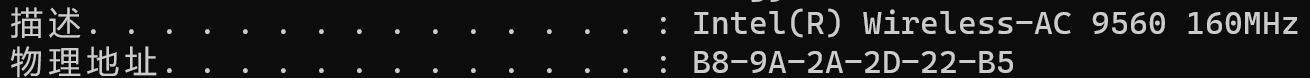
3.配置路由器的DHCP，并给PC设置DCHP。



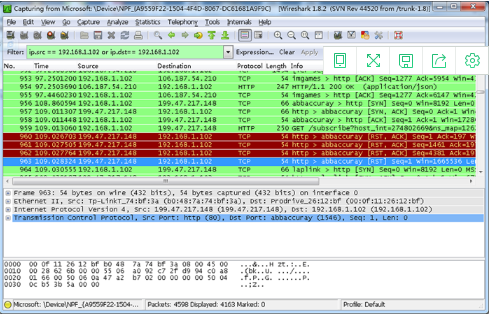


4.模拟ICMP包的传输过程，选择发送ping包和接收ping包的PC。

5.使用ipconfig /all 命令，查看到本机的MAC地址为：



6.打开wireshark软件进行MAC数据包相关的实验：



打开wireshark界面，选择一条数据包记录，点击显示其详细信息，在其中可以看到源MAC地址和目的MAC地址

**【分析讨论】**

要分析 ICMP 数据包在转发过程中的 MAC 地址变化情况，首先要使用网络抓包工具在源设备和目标设备之间进行抓包操作。确保抓取的数据包包含 ICMP 协议的数据包。再使用过滤器在抓包工具中筛选出 ICMP 相关的数据包，以便进行进一步的分析。

然后在抓包工具的数据包列表中查看每个 ICMP 数据包的源 MAC 地址和目标 MAC 地址，注意观察数据包在经过不同网络设备转发过程中 MAC 地址的变化情况。通过比对数据包中的源和目标 MAC 地址，可以判断 ICMP 数据包在转发过程中经过了哪些网络设备。同时还可以观察数据包中的 TTL （Time to Live）字段，它会逐跳减少，直到达到目标设备。

再细致分析每个网络设备的 MAC 地址变化情况。根据抓包工具提供的信息，可以检查每个转发节点的源和目标 MAC 地址，观察是否有变化或替换的情况发生。