**【实验名称】：**以太网帧分析实验

**学生姓名：**马威 **合作学生：**无

**实验地点：**济事楼330网络实验室 **实验时间：**2023年11月20日

**【实验目的】**

在学习以太网协议相关知识的基础上，在仿真网络中探究帧传输时MAC地址的变化情况，同时学习使用WireShark软件进行抓包并分析MAC帧。

**【实验原理】**

**1.以太网**

以太网是一种计算机局域网技术。IEEE 802.3标准就是以太网的技术标准，包括物理层连线、电信号和介质访问层协议内容，是目前应用最普遍的局域网技术。

以太网主要有两类：

* 经典以太网：运行速度为3-10Mbps
* 交换式以太网：运行于100/1000/10000Mbps的高速率，使用交换机连接不同计算机

以太网的标准拓扑结构为总线型拓扑，即多个结点连接到一条延展的总线上。但快速以太网为了减少冲突，并提高网络速度和最大化使用效率，使用了交换机进行网络连接和组织。交换机的出现使得局域网呈星形，但逻辑上以太网还是总线型的拓扑，并使用CSMA/CD的总线技术。

**2.MAC地址**

MAC地址（物理地址、硬件地址）是网卡被制造时由制造商分配的一个属性，全球唯一，使得以太网上所有节点都能互相鉴别。许多制造商现已经将以太网卡集成进计算机主板。

MAC地址长度为48位（6B），通常表示为12个16进制数，两两一组，其中前3个字节是网络硬件制造商的编号，由IEEE分配，后3个字节代表该制造商生产的某个网络产品（如网卡）的系列号，由厂家自行分配。

**3.MAC数据包**

MAC数据包（以太帧）就是在数据链路层传播的以MAC地址作为地址描述方式的帧，主要有两种类型：

* DIX：即EthernetⅡ帧，紧跟在目标和源MAC地址后的是Type字段，告诉接收方帧种类，并应该调用哪些协议处理该帧
* IEEE 802.3：紧跟在目标和源MAC地址后的是Length字段，表示数据的长度

由于IEEE 802.3出现时，DIX已被广泛应用，重新适应新协议势必成本巨大。幸运的是，Type和Length字段在同一位置，而在DIX中该字段必须大于0x600（1536），因此只要在长度上做规定不超过该值，两种协议就可以被广泛使用。事实上，IEEE 802.3数据长度不能超过1500（0x05dc），而两种协议也都被广泛使用了。

一般来说，以太帧的格式如下：

* 前导码+帧开始符（7B+1B，IEEE 802.3）/前导码（8B，DIX）
* MAC目标地址（6B）+MAC源地址（6B）
* 类型字段（2B，大于1536）/数据长度（2B，小于1500）
* 数据（0-1500B）
* 填充位（0-46B）
* 校验和（4B）

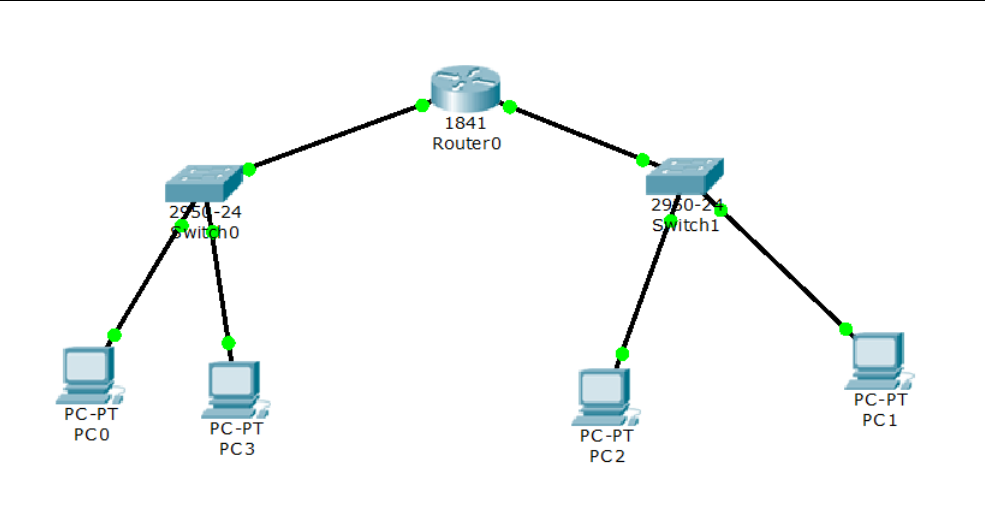
**【实验设备】**

Windows10 x64电脑 1台

**【实验步骤】**

1.启动并进入Windows环境，打开Cisco Packet Tracer

2.按照下图构建仿真网络，连线



4.配置路由器端口地址：

* enable
* configure terminal
* interface FastEthernet0/0
* ip address 192.168.1.1 255.255.255.0
* no shutdown
* exit
* enable
* configure terminal
* interface FastEthernet0/1
* ip address 192.168.2.1 255.255.255.0
* no shutdown

5.配置路由器DHCP：

* ip dhcp excluded-address 192.168.1.0 192.168.1.10
* ip dhcp pool myleftnet
* network 192.168.1.0 255.255.255.0
* default-router 192.168.1.1
* option 150 ip 192.168.1.3
* dns-server 192.168.1.2
* exit
* ip dhcp excluded-address 192.168.2.0 192.168.2.10
* ip dhcp pool myrightnet
* network 192.168.2.0 255.255.255.0
* default-router 192.168.2.1
* option 150 ip 192.168.2.3
* dns-server 192.168.2.2

6.将各PC的网关设置或IP设置调为“自动配置”

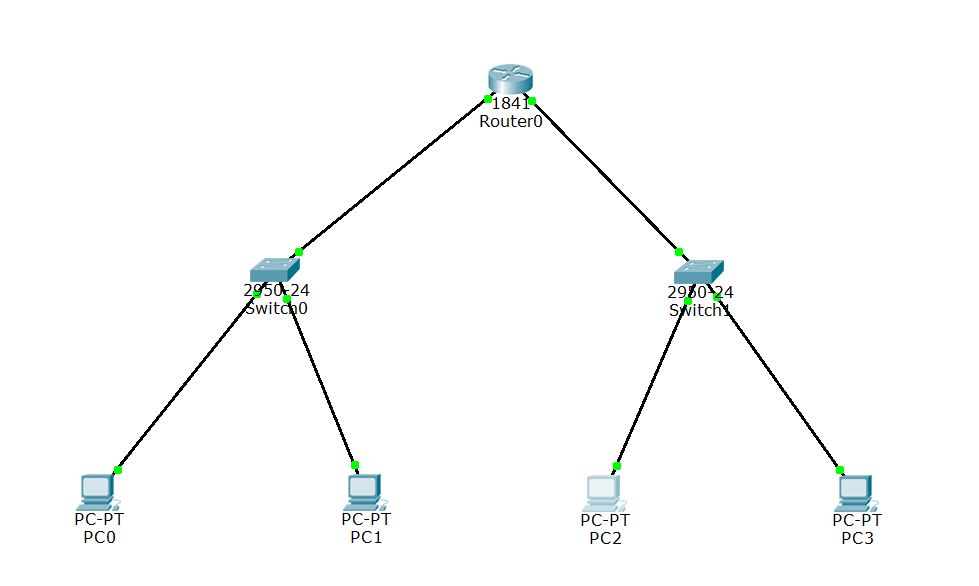
7.调整为“模拟”模式，在PC0上ping到PC2

8.使用捕获/转发按钮进行单步调试，记录每一步帧的方向、种类和MAC地址，并观察现象

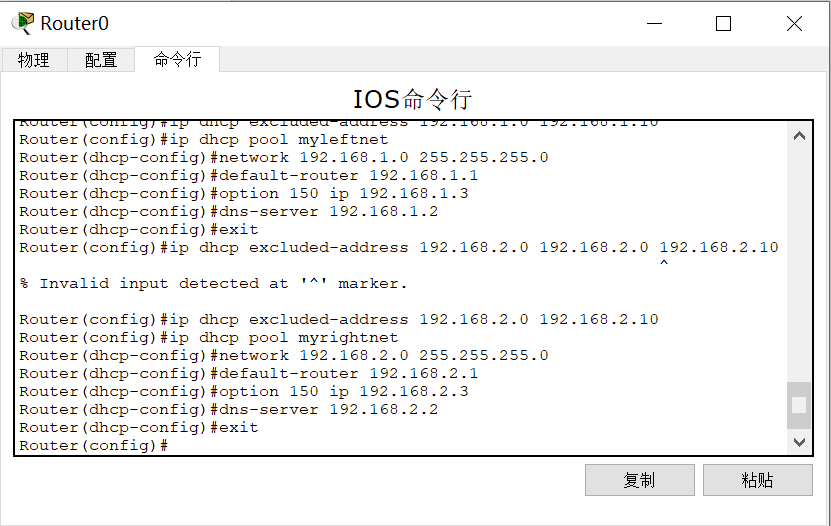
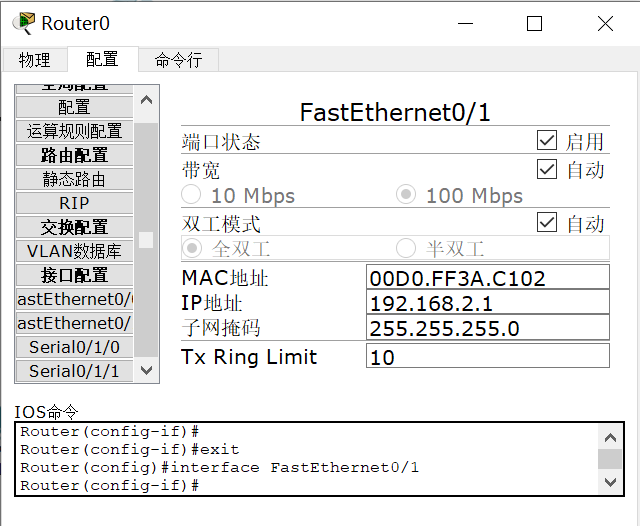
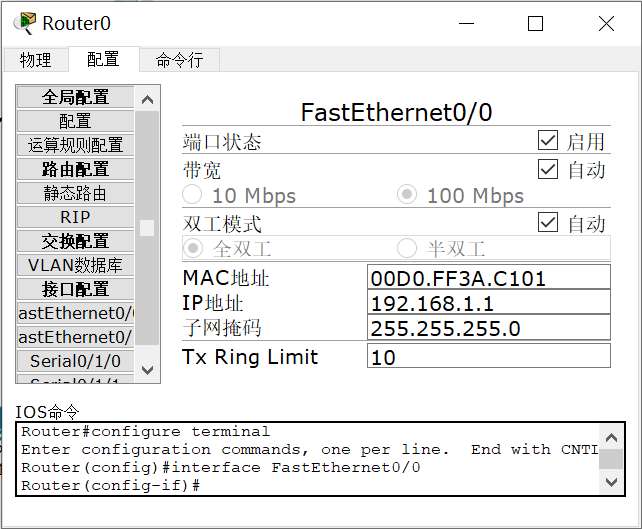
9.下载安装WireShark软件，抓取WLAN端口上的MAC帧进行结构分析

**【实验现象】**

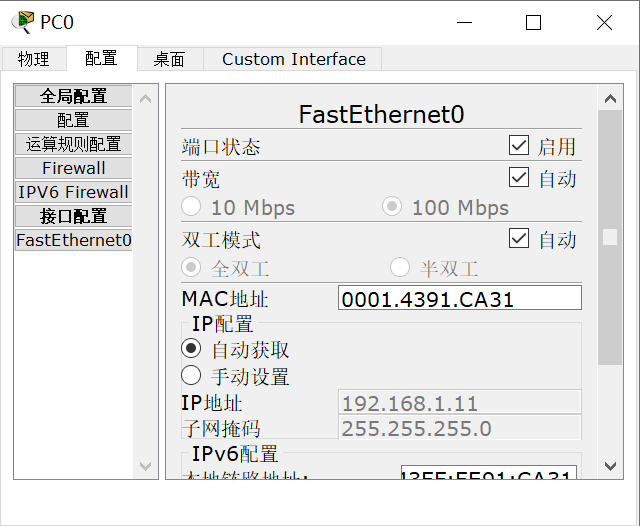
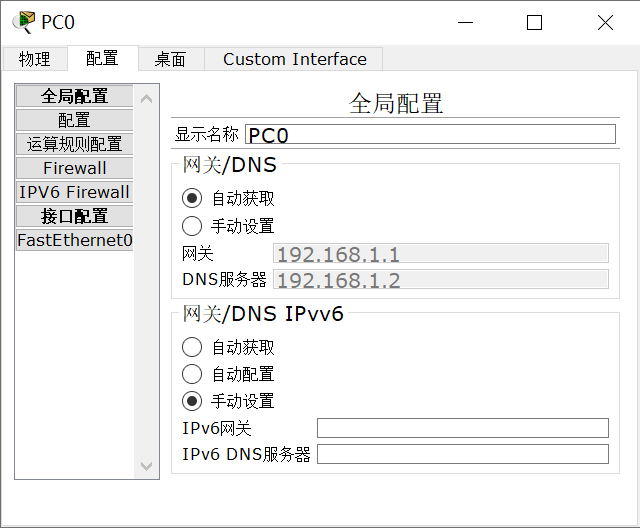
1.构建仿真网络：

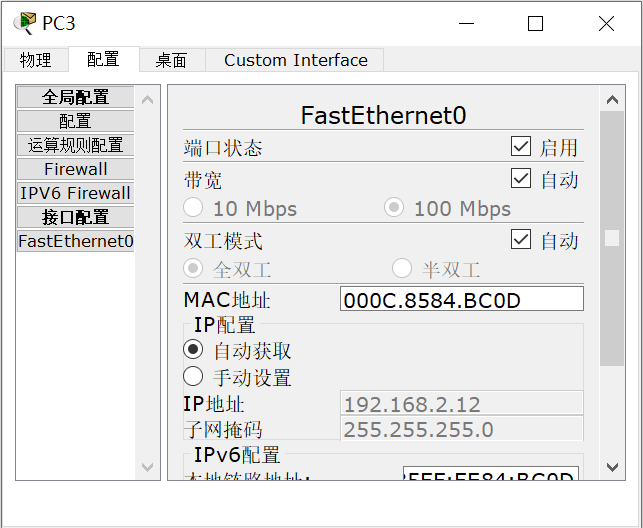
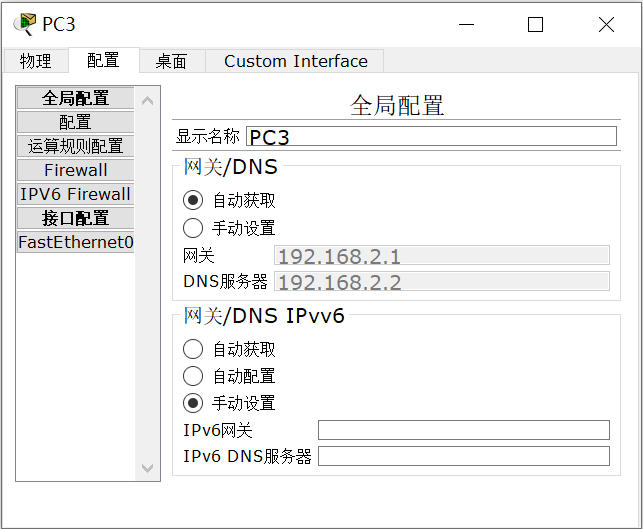
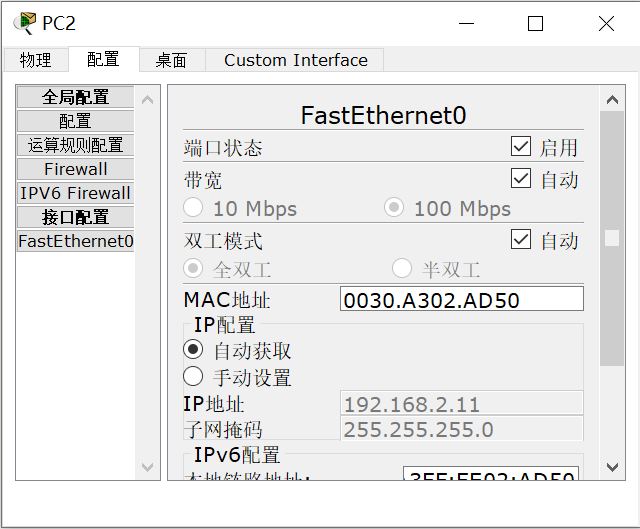
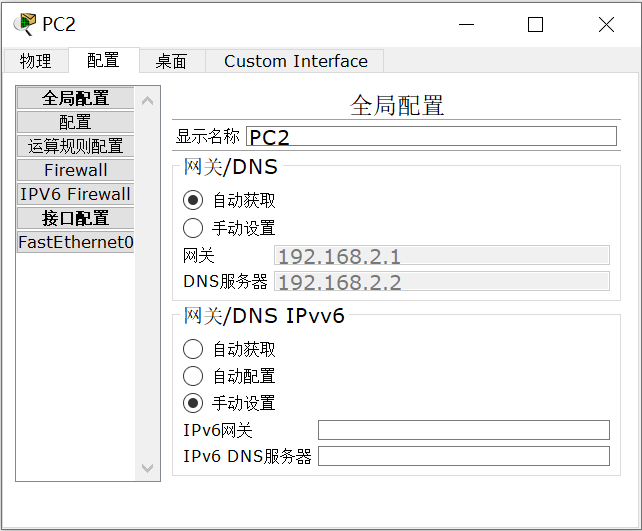
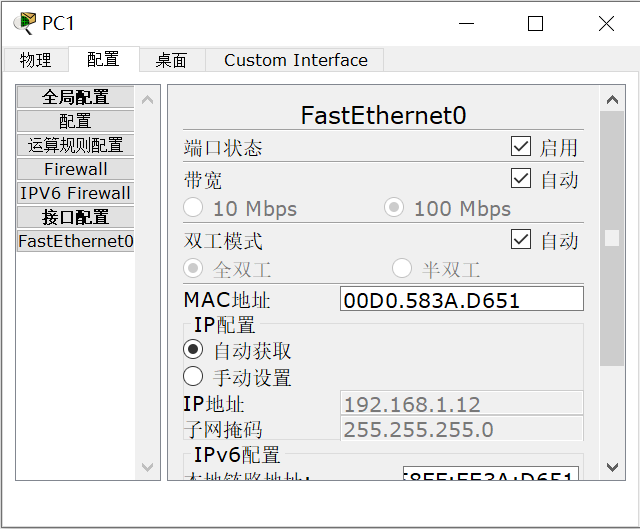


2.配置路由器端口和DHCP：

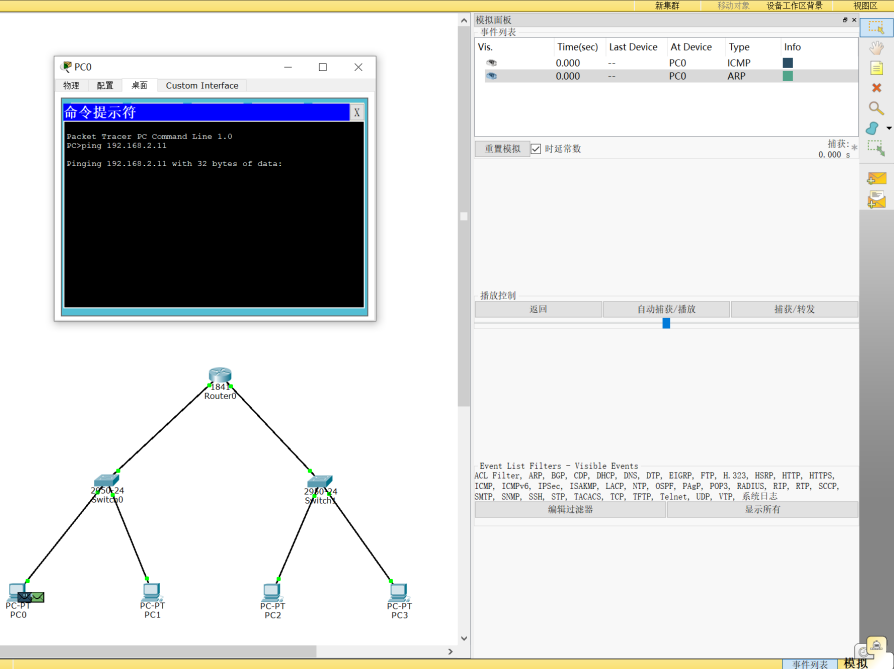


3.自动配置PC的IP等信息：





4.转为“模拟”模式，并在PC0上ping到PC2：



**5.1 PC0生产出一个ICMP帧，然后装载到ARP帧上发送给Switch0**

生成的ICMP：

|  |  |
| --- | --- |
| 目的MAC：/ | 源MAC：/ |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

装载的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.2 目的MAC未知，Switch0需更新映射表，向所有端口（除fa0/2外）发送信息**

接收并发送的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.3 Router0是这一跳的终点将其MAC回传；而PC1为终端，发现IP地址不符后，便不回复信息**

Router0接收的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

Router0回传的ARP：

|  |  |
| --- | --- |
| 目的MAC：0001.4391.CA31（PC0） | 源MAC：00D0.9757.B001（fa0/0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

PC1接收的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.4 目的MAC已知，Switch0转发给PC0**

接收并发送的ARP：

|  |  |
| --- | --- |
| 目的MAC：0001.4391.CA31（PC0） | 源MAC：00D0.9757.B001（fa0/0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.5 PC0收到回传信息，生成ICMP帧并传给Switch0**

接收的ARP：

|  |  |
| --- | --- |
| 目的MAC：0001.4391.CA31（PC0） | 源MAC：00D0.9757.B001（fa0/0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

生成的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B001（fa0/0） | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.6 目的MAC已知，Switch0转发给Router0**

接收并发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B001（fa0/0） | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.7 Router0发现IP地址不符后，生成ARP帧传给Switch1**

接收的的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B001（fa0/0） | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

生成的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.2.1 |

**5.8 目的MAC未知，Switch1需更新映射表，向所有端口（除fa0/2外）发送信息**

接收并发送的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.2.1 |

**5.9 PC2为目的地，将其MAC回传；而PC1为终端，发现IP地址不符后，便不回复信息**

PC2接收的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.2.1 |

PC2回传的ARP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B002（fa0/1） | 源MAC：0030.A302.AD50（PC2） |
| 目的IP：192.168.2.1 | 源IP：192.168.2.11 |

PC3接收的ARP：

|  |  |
| --- | --- |
| 目的MAC：FFFF.FFFF.FFFF | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.2.1 |

**5.9 目的MAC已知，Switch1转发给Router0**

接收并发送的ARP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B002（fa0/1） | 源MAC：0030.A302.AD50（PC2） |
| 目的IP：192.168.2.1 | 源IP：192.168.2.11 |

**5.10 Router0为目的地**

接收的ARP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B002（fa0/1） | 源MAC：0030.A302.AD50（PC2） |
| 目的IP：192.168.2.1 | 源IP：192.168.2.11 |

**5.11 Switch0、Switch1连续向所有端口发送4次STP帧（由于不会解读，故不赘述）**

**5.12 PC0生成ICMP帧发向Router0**

**生成的ICMP：**

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B001（fa0/0） | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.13 目的MAC已知，Switch1转发给Router0**

接收并发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B001（fa0/0） | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.14 目的IP已知，Router0将ICMP送出到fa0/1**

接收的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B001（fa0/0） | 源MAC：0001.4391.CA31（PC0） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：0030.A302.AD50（PC2） | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.14 目的MAC已知，Switch1转发给PC2**

接收并发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：0030.A302.AD50（PC2） | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

**5.15 PC2为目的地，为了ping指令回传给Router0**

接收的ICMP：

|  |  |
| --- | --- |
| 目的MAC：0030.A302.AD50（PC2） | 源MAC：00D0.9757.B002（fa0/1） |
| 目的IP：192.168.2.11 | 源IP：192.168.1.11 |

发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B002（fa0/1） | 源MAC：0030.A302.AD50（PC2） |
| 目的IP：192.168.1.11 | 源IP：192.168.2.11 |

**5.16 目的MAC已知，Switch1转发给Router0**

接收并发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B002（fa0/1） | 源MAC：0030.A302.AD50（PC2） |
| 目的IP：192.168.1.11 | 源IP：192.168.2.11 |

**5.17 目的IP已知，Router0将ICMP送出到fa0/0**

接收的ICMP：

|  |  |
| --- | --- |
| 目的MAC：00D0.9757.B002（fa0/1） | 源MAC：0030.A302.AD50（PC2） |
| 目的IP：192.168.1.11 | 源IP：192.168.2.11 |

发送的ICMP：

|  |  |
| --- | --- |
| 目的MAC：0001.4391.CA31（PC0） | 源MAC：00D0.9757.B001（fa0/0） |
| 目的IP：192.168.1.11 | 源IP：192.168.2.11 |

**5.18 目的MAC已知，Switch1转发给PC0**

接收并发送的ICMP：

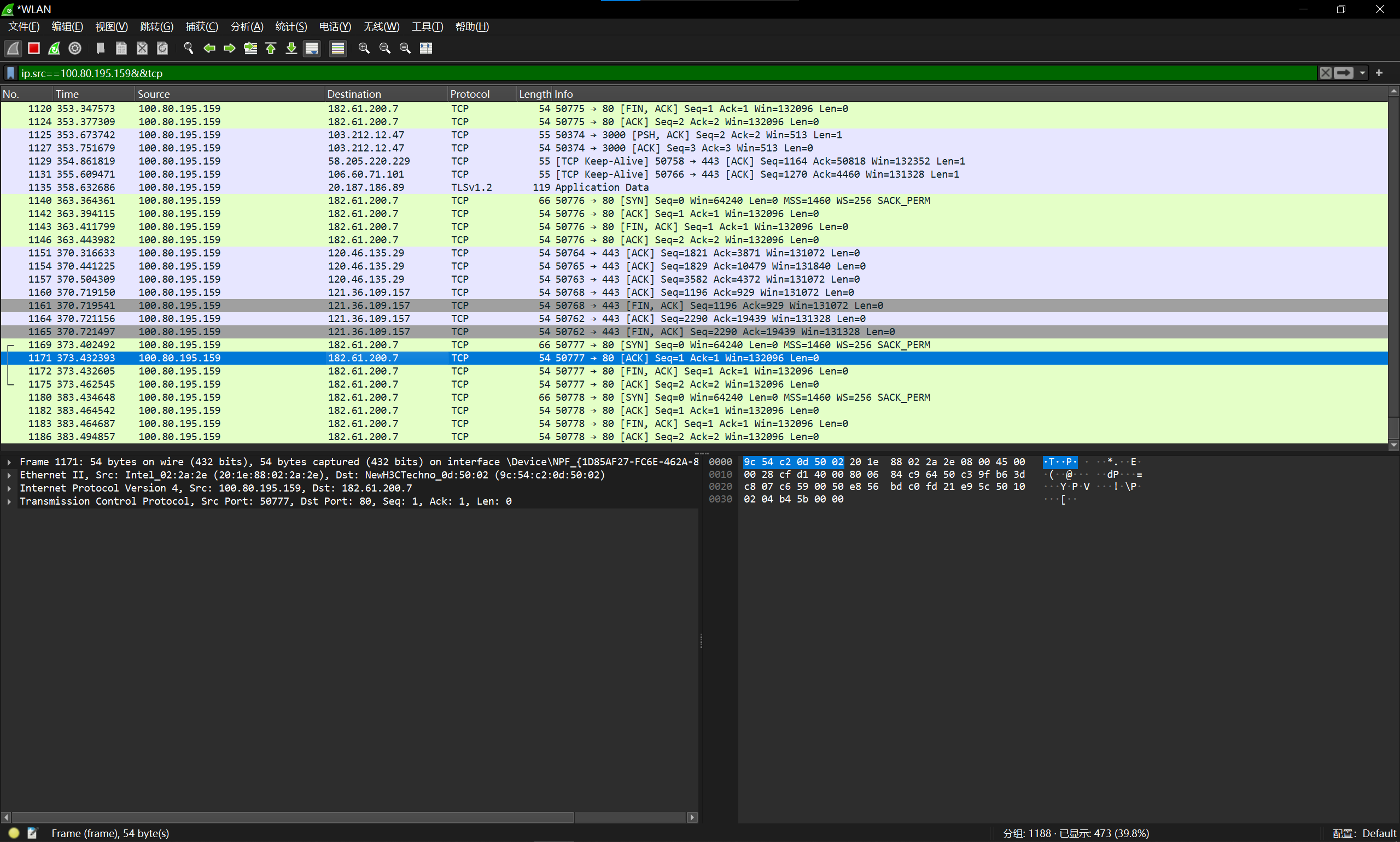
|  |  |
| --- | --- |
| 目的MAC：0001.4391.CA31（PC0） | 源MAC：00D0.9757.B001（fa0/0） |
| 目的IP：192.168.1.11 | 源IP：192.168.2.11 |

**5.19 PC0为目的地，源IP和ping的地址一致，说明ping通，在控制台上显示本次ping结果**

**5.20 重复5.12-5.19三次（ping有4次尝试，均为该过程）**

6.本机MAC地址（设置——网络和Internet——查看硬件和连接属性，由于抓取的是WLAN的包，因此查看的是WLAN的信息）：



7.使用WireShark软件进行抓包（只抓从本机发送的TCP协议帧）：

**【分析讨论】**

本次实验详细介绍了以太网这个局域网技术及其分类，并且对于数据链路层上的协议相关知识，包括帧的格式进行了详尽的展示。仿真网络的单步调试，不仅让我更加了解ping的原理，而且也对帧的转发过程中MAC地址的转换有了一定的了解。WireShark抓包更是直接抓取现实中的MAC帧，以实例生动展示了以太网帧的格式。

**1.ICMP帧在转发过程中MAC地址变化**

* 每一跳中，源MAC是该跳出发端口MAC，目的MAC是该跳目的端口MAC（从终端出发时，目的MAC是网关的MAC）
* 经过交换机时帧内容不变

除此之外，在仿真网络构建初期，路由器、交换机没有任何信息的情况下，会发送大量的ARP帧。一般来说：

* 初始ARP帧的目的MAC未知
* 不断向前发送“摸索”，在遇到路由设备或终端时会带着MAC返回，告诉发送方这一跳已通
* 发送方接着把目的MAC设为返回来的这个MAC，等帧到达了下一跳起始位置后，重复上述过程直到找到目的端
* 交换机接收到ARP帧时，若目的MAC不在映射表中，则交换机会在局域网中“招呼一声”，除了接收ARP帧的端口外，向其余所有端口发送转发ARP帧。接收到ARP帧的设备若为终端，检查IP地址，错误则不回复；若为路由设备，则可能连接到目的网段，带着端口MAC返回。

这个过程中除非没有转发到路由设备或者转发到的终端全部MAC不正确，交换机至少会更新路由表，增加端口到MAC地址的映射，这也是理论课上所讲的学习网桥。虽然学习代价较高，但在不改变局域网结构的情况下，仅需学习一次即可，代价可接受。且从实验现象5.12-5.19可以看出，学习相当于把网路给“走通了”，终端知道网关的MAC、交换机知道该转发到哪个端口、路由器知道发向目的网段，就没有较为繁琐的“摸索”过程了。这也解决了一直以来做实验时我的两个疑问：

* 为什么ping的时候总是第一次尝试time out？
* 交换机如何知道要转发到哪个端口？

经过课上网桥相关知识的介绍以及本次实验可以知道，第一次ping由于网路各个节点中并没有存储映射信息，需要时间进行学习，势必会造成时间消耗。但只需一次学习，网络设备就会知道每一步的MAC地址，就可以正常通信了。

IP地址方面，ARP帧“摸索”到某一跳时，会把源IP和目的IP改成该跳两端的IP，且可能会对调；而ICMP帧总是保持原来发送时的源IP和目的IP不变。

**2.MAC帧的解读**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9c | 54 | c2 | 0d | 50 | 02 | 20 | 1e | 88 | 02 | 2a | 2e | 08 | 00 | 45 | 00 |
| 00 | 28 | 21 | 3e | 40 | 00 | 80 | 06 | 65 | cf | 64 | 50 | c3 | 9f | 28 | 7e |
| 23 | 55 | de | 6c | 01 | bb | 62 | 57 | 58 | f4 | a5 | 46 | d7 | 4d | 50 | 10 |
| 02 | 05 | 22 | 05 | 00 | 00 |  |  |  |  |  |  |  |  |  |  |

9c-54-c2-0d-50-02：目的MAC



20-1e-88-02-2a-2e：源MAC（本机）



08-00：Type字段（DIX的ipv4帧）

45：版本和头部长度

00：Explicit Congestion Notification

00-28：总长度

21-3e：标识符

40-00：片偏移（不偏移）

80：生存时间

06：协议（TCP）

65-cf：头部校验和

64-50-c3-9f：源IP（100.80.195.159，本机）

28-7e-23-55：目的IP（40.126.35.85）

de-6c：源端口（56940）

01-bb：目的端口（443）

62-57-58-f4：序列号

a5-46-d7-4d：确认号

50-10：其他标志位

02-05：窗口大小

22-05：校验和

00-00：Urgent Pointer