**【实验名称】：IP数据包分析实验**

**学生姓名：陈嘉瑞 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27日**

**【实验目的】**

1. 了解IP数据包格式以及各个数据域含义。
2. 了解IP数据包传输原理。

**【实验原理】**

1. IP数据报文格式总览

IP协议提供不可靠无连接的数据报传输服务，IP层提供的服务是通过IP层对数据报的封装与拆封来实现的。IP数据报的格式分为报头区和数据区两大部分，其中报头区是为了正确传输高层数据而加的各种控制信息，数据区包括高层协议需要传输的数据。

一个 IP 数据报由首部和数据两部分组成。



1. 头部

在首部的固定部分的后面是一些可选字段，其长度是可变的。



1. IP 数据报首部的各字段

版本——占 4 位，指 IP 协议的版本。目前的IP 协议版本号为 4 (即 IPv4)。

首部长度——占 4 位，可表示的最大数值是15 个单位(一个单位为 4 字节)，因此 IP 的首部长度的最大值是 60。

区分服务——占 8 位，用来获得更好的服务。在旧标准中叫做服务类型，但实际上一直未被使用过。

总长度——占 16 位，指首部和数据之和的长度，单位为字节，因此数据报的最大长度为65535 字节。总长度必须不超过最大传送单元MTU。

标识(identification) ——占 16 位，它是一个计数器，用来产生 IP 数据报的标识。

标志(flag) ——占 3 位，目前只有前两位有意义。标志字段的最低位是 MF (More ragment)。MF= 1 表示后面“还有分片”。MF = 0 表示最后一个分片。 标志字段中间的一位是 DF (Don’t Fragment) 。只有当 DF = 0 时才允许分片。

片偏移—— 占13 位，表示较长的分组在分片后某片在原分组中的相对位置。片偏移以 8 个字节为偏移单位。

生存时间——占8 位，记为 TTL (Time To Live)，指示数据报在网络中可通过的路由器数的最大值。

协议——占8 位，指出此数据报携带的数据使用何种协议，以便目的主机的 IP 层将数据部分上交给那个处理过程。

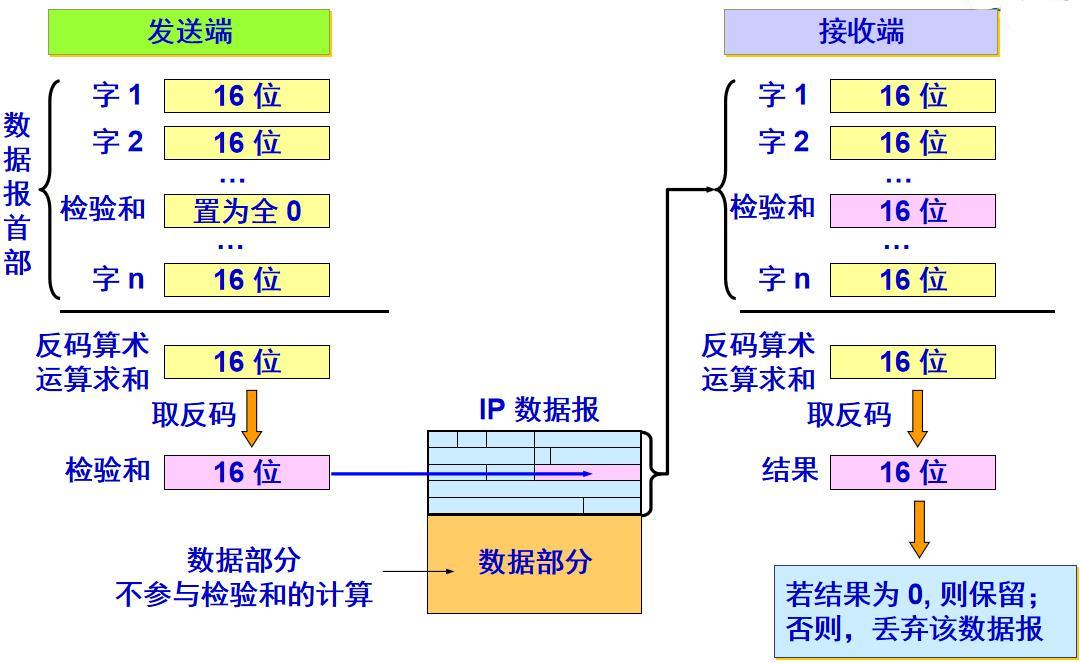
首部检验和——占16 位，只检验数据报的首部，不检验数据部分。这里不采用 CRC 检验码而采用简单的计算方法。IP 数据报首部检验和的计算采用 16 位二进制反码求和算法

源地址和目的地址都各占 4 字节

IP 首部的可变部分就是一个选项字段，用来支持排错、测量以及安全等措施，内容很丰富。选项字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。

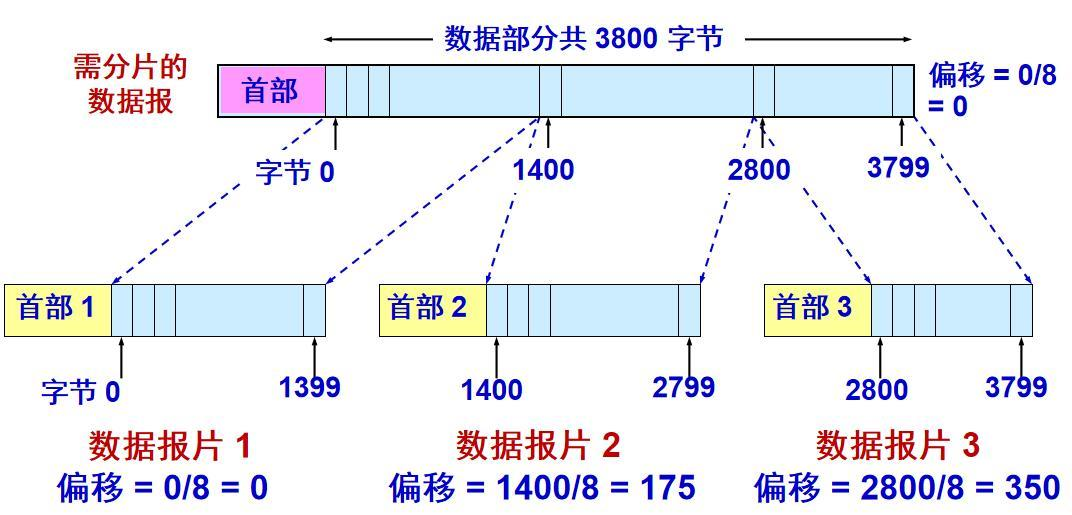
1. IP数据报首部校验

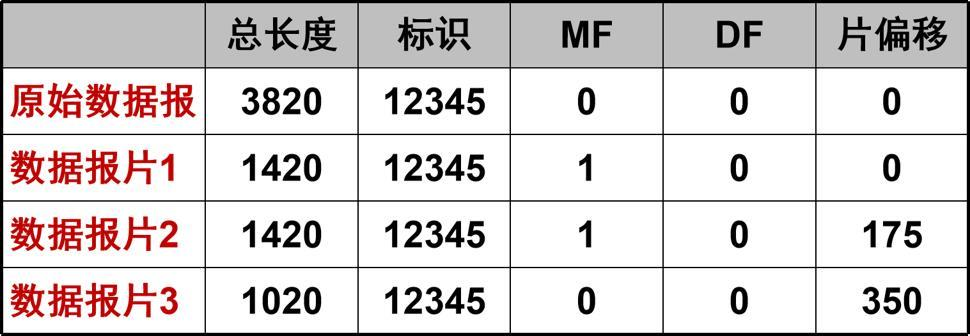
IP 数据报首部检验和的计算采用 16 位二进制反码求和算法



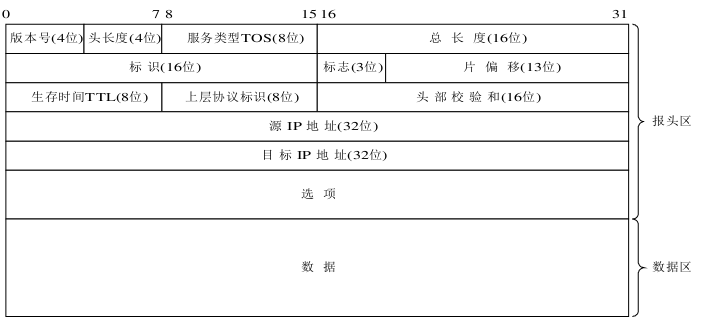
1. IP数据报分段

给出一数据报的总长度为 3820 字节，其数据部分的长度为 3800 字节（使用固定首部），需要分片为长度不超过 1420 字节的数据报片。因固定首部长度为 20 字节，因此每个数据报片的数据部分长度不能超过 1400 字节。于是分为 3 个数据报片，其数据部分的长度分别为 1400、1400 和 1000 字节。原始数据报首部被复制为各数据报片的首部，但必须修改有关字段的值（如标志字段）。





1. IP数据报文格式传输



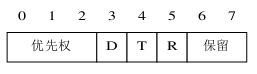
上图表示的数据，最高位在左边，记为0位；最低位在右边，记为31位。在网络中传输数据时，先传输0~7位，其次是8~15位，然后传输16~23位，最后传输24~31位。

1. IP数据报文上层协议



1. IP数据报文的服务类型

服务类型（TOS、type of service）：占用8位二进制位，用于规定本数据报的处理方式。



服务类型字段的8位分成了5个子域：

(1)—优先权（0-7）数越大，表示该数据报优先权越高。网络中路由器可以使用优先权进行拥塞控制，如当网络发生拥塞时可以根据数据报的优先权来决定数据报的取舍。

(2)—短延迟位D(Delay)：该位置1时，数据报请求以短延迟信道传输，0表示正常延时。

(3)—高吞吐量位T(Throughput)：该位置1时，数据报请求以高吞吐量信道传输，0表示普通。

(4)—高可靠位R(Reliability)：该位置1时，数据报请求以高可靠性信道传输，0表示普通。

(5)—保留位。

目前在Internet中使用的TCP/IP协议大多数情况下网络并未对TOS进行处理，但在实际编程时，有专门的函数来设置该字段的各域。一些重要的网际应用协议中都设置了建议使用的TOS值：

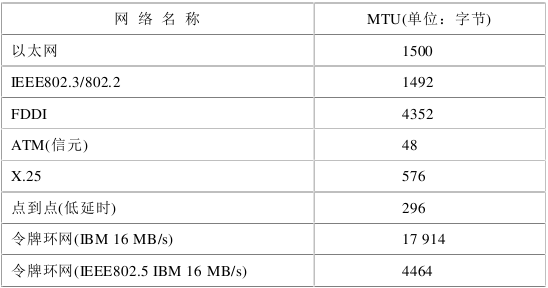


1. 最大传输单元

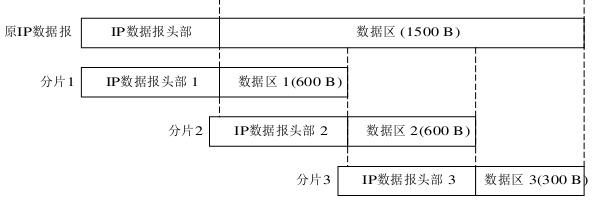
IP数据报在互联网上传输时，可能要经过多个物理网络才能从源端传输到目的端。不同的网络由于链路层和介质的物理特性不同，因此在进行数据传输时，对数据帧的最大长度都有一个限制，这个限制值即最大传输单元MTU（Maximum Transmission Unit）。

同一个网络上的两台主机之间通信时，该网络的MTU值是确定的，不存在分片问题。分片问题一般只存在于具有不同MTU值的互联网中。

由于现在互联网主要使用路由器进行网络连接，因此分片工作通常由路由器负责。当两台主机之间的通信要通过多个具有不同MTU值的网络时，MTU的瓶颈是通信路径上最小的MTU值，它被称为路径MTU。由于路由选择不一定是对称的（从A到B的路由可能与从B到A的路由不同），因此，路径MTU在两个方向上不一定是一致的，下表是几种常用网络的MTU值：



1. 分片

把一个数据报为了适合网络传输而分成多个数据报的过程称为分片，被分片后的各个IP数据报可能经过不同的路径到达目标主机。一个IP数据报在传输过程中可能被分片，也可能不被分片。如果被分片，分片后的IP数据报和原来没有分片的IP数据报结构是相同的，即也是由IP头部和IP数据区两个部分组成：分片后的IP数据报，数据区是原IP数据报数据区的一个连续部分，头部是原IP数据报头部的复制，但与原来未分片的IP数据报头部有两点主要不同：标志和片偏移：

片偏移：IP数据报被分片后，各片数据区在原来IP数据区中的位置用13位片偏移来表示。上图中分片1的偏移为0；分片2的偏移为600；分片3的偏移为1200实际在IP地址中,由于偏移是以8个字节为单位进行计算的,因而在IP数据报中分片1的偏移是0；分片2的偏移是75；分片3的偏移是150

1. 接收组包

当分了片的IP数据报到达最终目标主机时，目标主机对各分片进行组装，恢复成源主机发送时的IP数据报，这个过程叫做IP数据报的重组。在IP数据报头部中，标识用16位二进制数表示，它唯一地标识主机发送的每一份数据报。在一个数据报被分片时，每个分片仅把数据报“标识”字段的值原样复制一份，所以一个数据报的所有分片具有相同的标识。

目标端主机重组数据报的原理是：

(1)—根据“标识”字段可以确定收到的分片属于原来哪个IP数据报；

(2)—根据“标志”字段的“片未完MF”子字段可以确定分片是不是最后一个分片；

(3)—根据“偏移量”字段可以确定分片在原数据报中的位置。

1. IP数据报选项

IP数据报“选项”主要有两大功能：

1）用来实现对数据报传输过程中的控制，如规定数据报要经过的路由；

2）进行网络测试，如一个数据报传输过程中经过了哪些路由器。

IP“选项“域共分为四大类，每类分为若干个选项，每个选项有确定的编号：



IP数据报“选项”由三个部分组成：选项码、选项长度和选项数据。选项码和选项长度各占一个字节，中，选项长度用于确定整个选项部分的长度；选项码又分为复制、选项类和选项号：

复制：占一位，用来控制一个带有选项的IP数据报被分片后对选项的处理方式。该位置1时将选项复制到所有分片中；置0时将选项仅复制到第一个分片中。

选项类和选项号用于确定该选项是哪类选项中的哪个选项，其实就是确定该选项的功能。

1）源路由选择：是指IP数据报在互联网中传输时，所经过的路由是由发出IP数据报的源主机指定的，以区别于数据报在互联网中传输时由路由器的IP层自动寻径所得到的路由。通过设置源路由选择选项，可以测试网络中指定路由的连通性，以使数据报绕开出错的网络，也可用于测试特定网络的吞吐量。源路由选择可分为两类：严格源路由选择和宽松源路由选择。

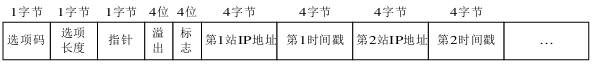
a.—严格源路由选择有发送端规定IP数据报必须经过的路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过的路由器的顺序不可更改。如果一个路由器发送源路由所指定的下一个路由器不在其直接连接的网络上，那么它就返回一个“源路由失败”的ICMP差错报文。严格源路由选择选项格式如下：



b.—宽松源路由选择：由发送方指明一个数据报经过的IP地址清单，但是在数据报传输的路径上，在选项中指定的两个IP地址之间可以有其他IP地址的路由器。格式与严格的相同，只是选项码字段值为0x83。

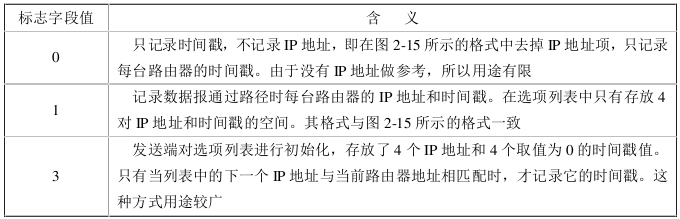
2）记录路由：通过设置记录路由选项，IP数据报就可以记录数据报从源主机传输到目标主机时，所经过路径上的各个路由器的IP地址。记录路由选项的数据格式和严格源路由选择格式相同，但选项码字段值为0x87，指针初值为4，指向存放第一个IP地址的位置。每个路由器的IP地址存入选项的数据区中，指针字段的值也随着增加（从4开始到8，12，16，最大到36），它始终指向下一个存放IP地址的位置。当记录了9个IP地址后，指针字段的值为40，表示数据区已满。

3）记录时间戳：就是IP数据报每经过一个路由器都记下它的IP地址和时间。时间戳中的时间以ms为单位，时间戳取值一般为格林威治时间（UT，Universal Time）自午夜开始计时的毫秒数时间戳选项格式如下：



时间戳选项的选项码是0x44。选项长度表示选项的总长度（一般为36或40），指针指向下一个可用空间的指针（值为5、9、13等）。

“溢出OF”字段表示因时间戳选项数据区空间不够而未能记录下来的时间戳个数；“标志FL”字段用于控制时间戳选项的格式，取值如下：



**【实验设备】**

个人笔记本电脑、Cisco Packet Tracer实验软件。

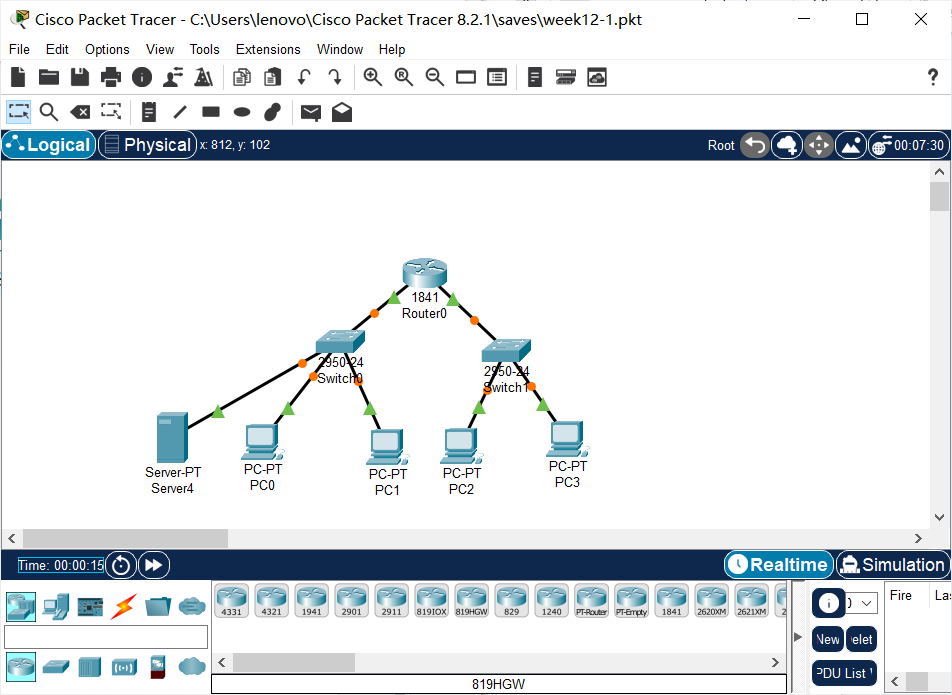
**【实验步骤】**

1. 首先规划网络地址及拓扑图；
2. 设置WEB服务器
3. 路由器接口IP地址配置；
4. 配置DHCP
5. 验证各个PC的IP地址。
6. 打开PC0浏览器，输入WEB服务器的IP地址，产生IP数据报文
7. 分析报文
8. 用WireShark抓取IP数据包
9. 查看抓取的IP报文字段内容并解读

**【实验现象】**

1. 规划网络地址及拓扑图；

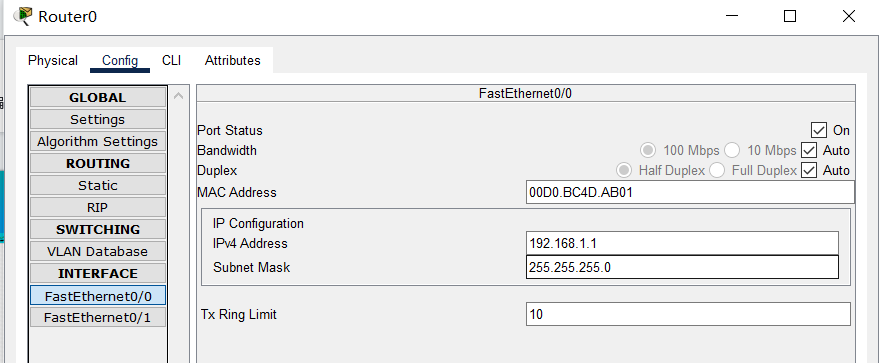
本实验中使用四台PC和一台WEB服务器，按下图拓扑结构进行连接。



1. 路由器接口IP地址配置；

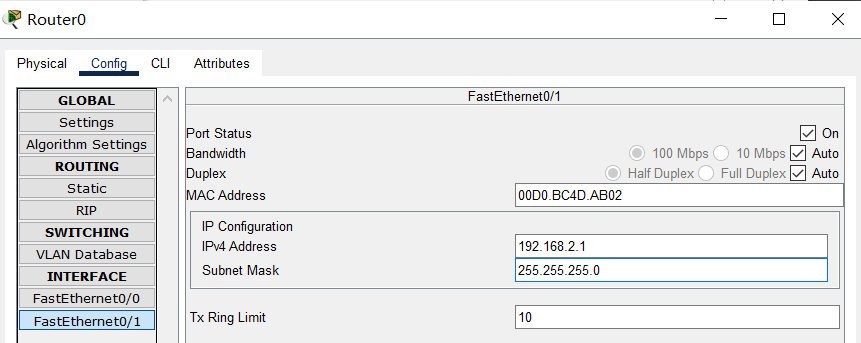
F0/0:

IP:192.168.1.1



F0/1:

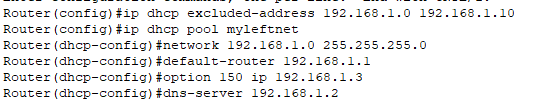
IP:192.168.2.1



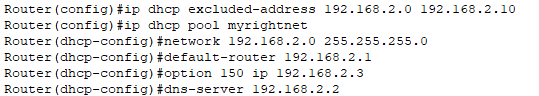
1. 配置DHCP

为简化实验流程，这里采用前几次实验使用过的DHCP，让PC动态获取IP。

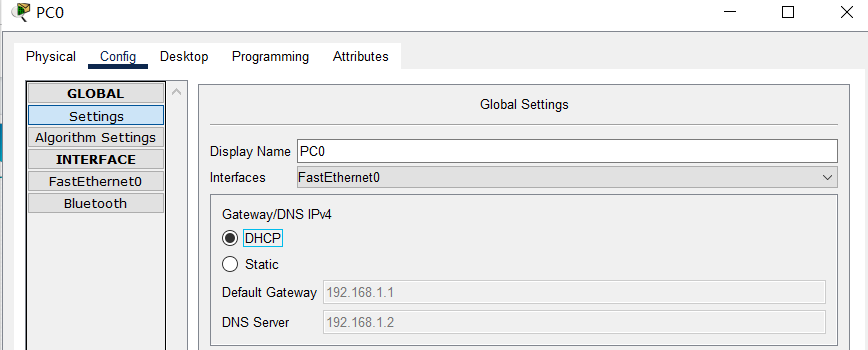
配置左侧子网DHCP：



配置右侧子网DHCP：



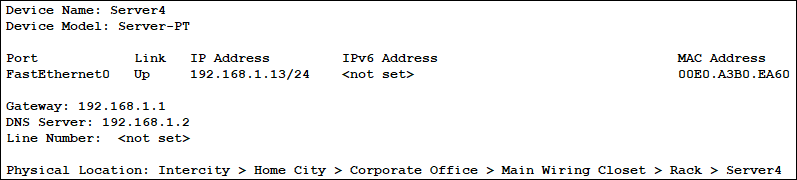
各个PC及server开启使用DHCP（以PC0为例）：



1. 验证各个PC（以PC0为例）及server的IP地址。

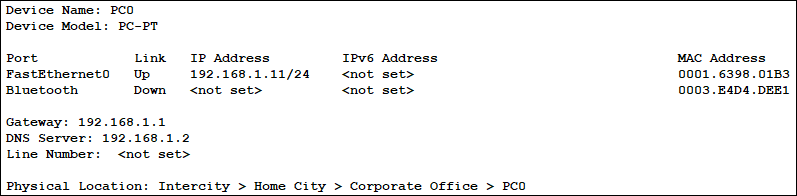
Server：

IP:192.168.1.13

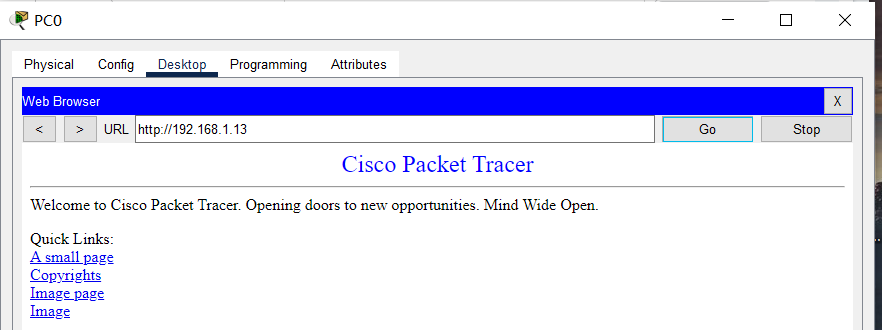


PC0：

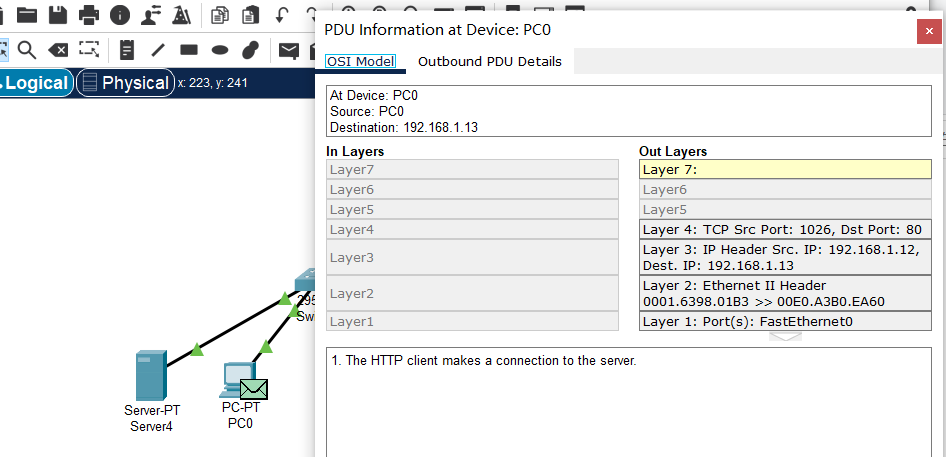
IP：192.168.1.11

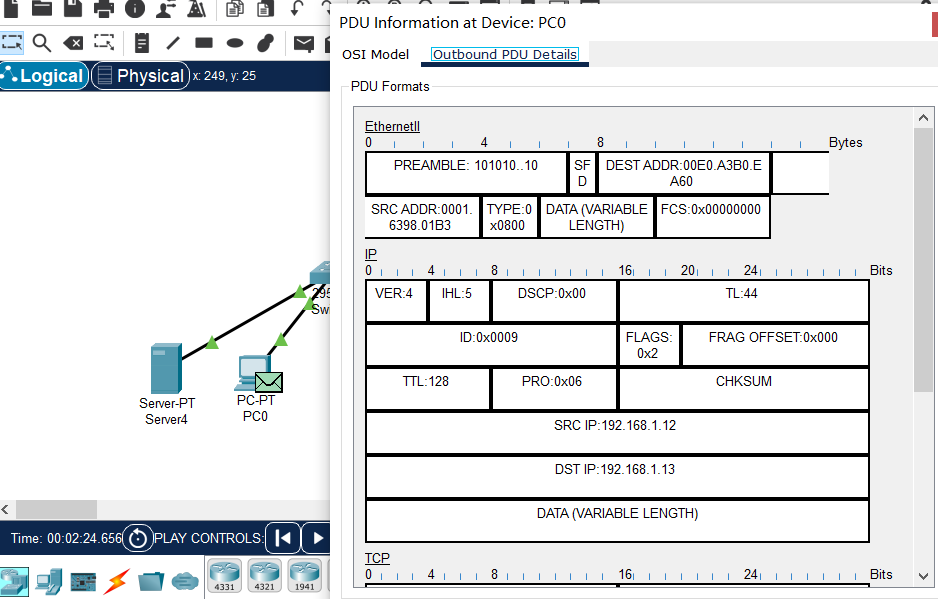


1. 打开PC0浏览器，输入WEB服务器的IP地址，产生IP数据报文

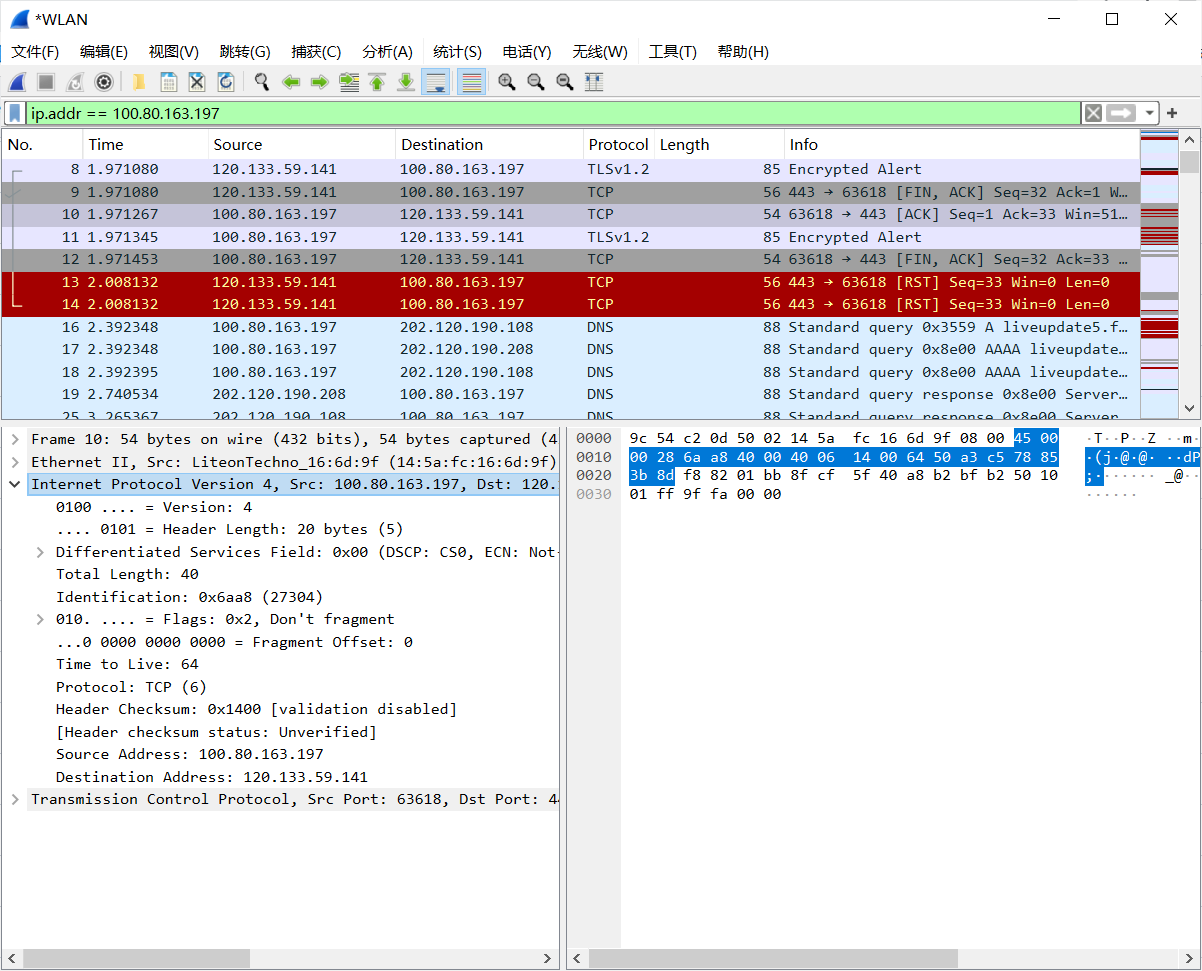


1. 查看报文



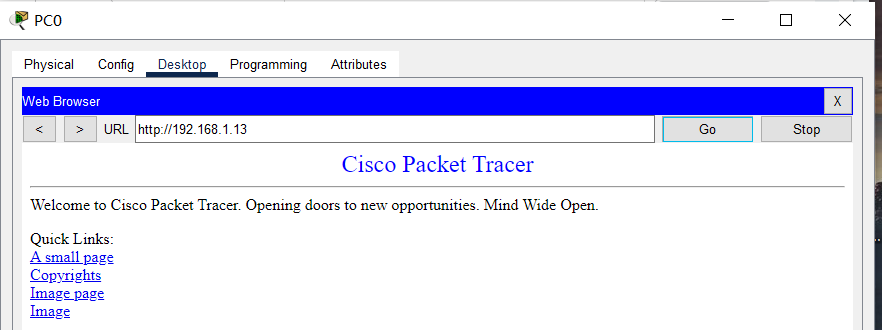


1. 用WireShark抓取IP数据包并查看抓取的IP报文字段内容



**【分析讨论】**

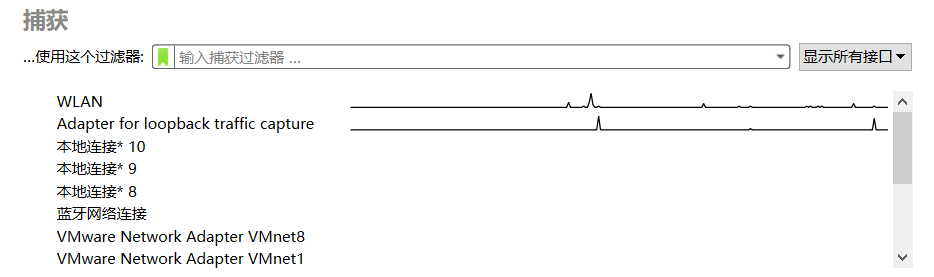
1. 配置Web服务器，并从客户端查看；

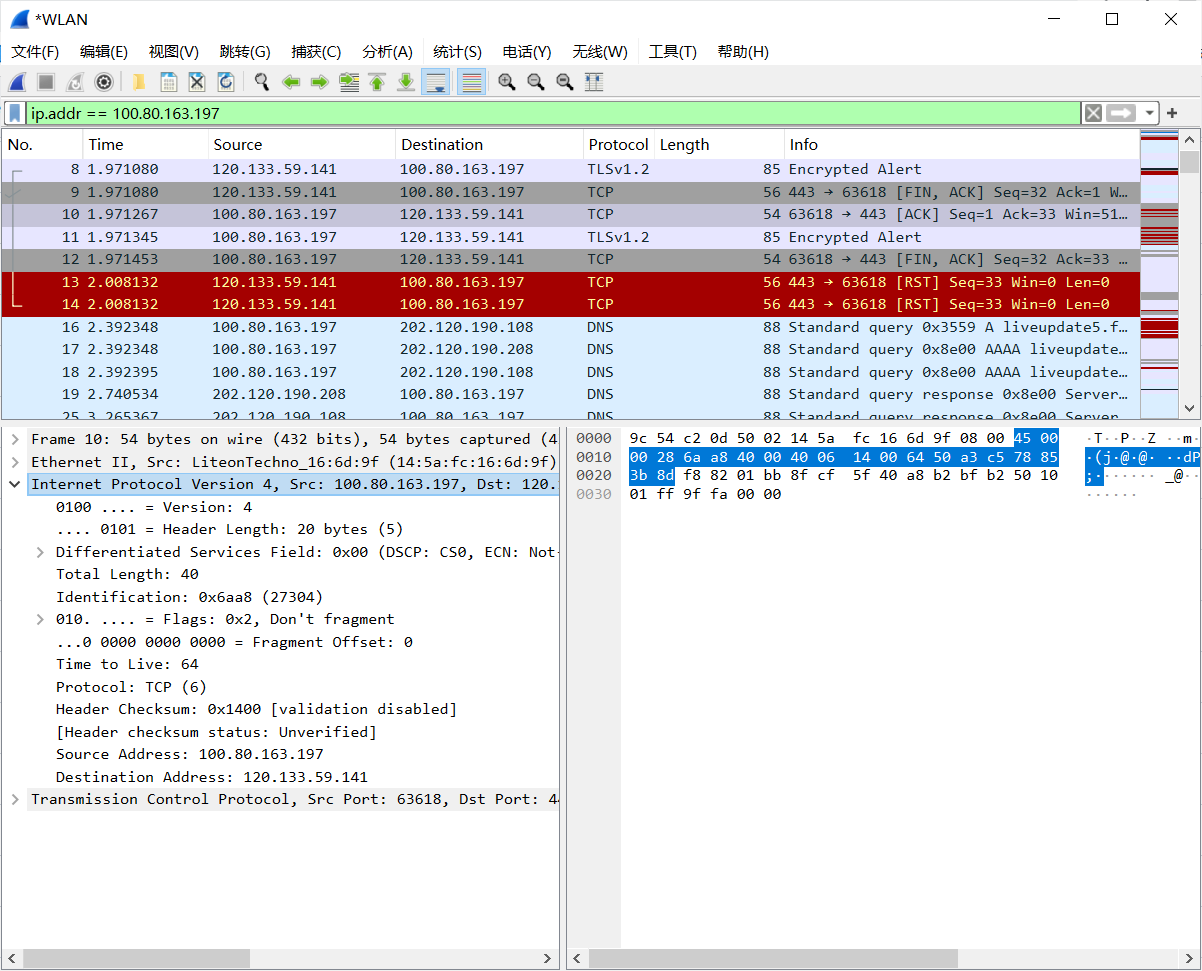


在PC的地址栏输入Web Server的IP地址，可以访问服务器。

1. 用WireShark抓取IP数据包。

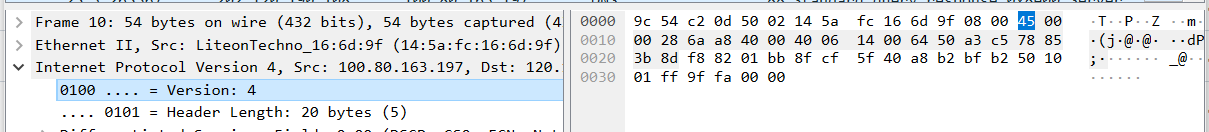
选择WLAN并开始捕获



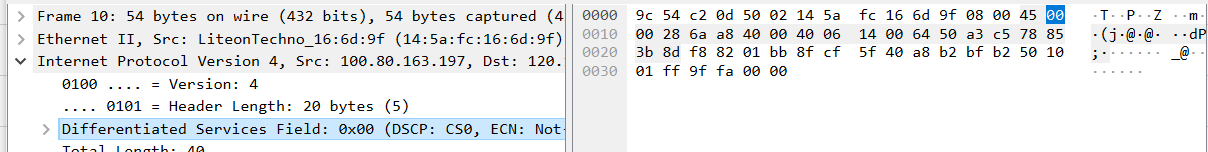


筛选出protocal（协议）字段为TCP的数据包

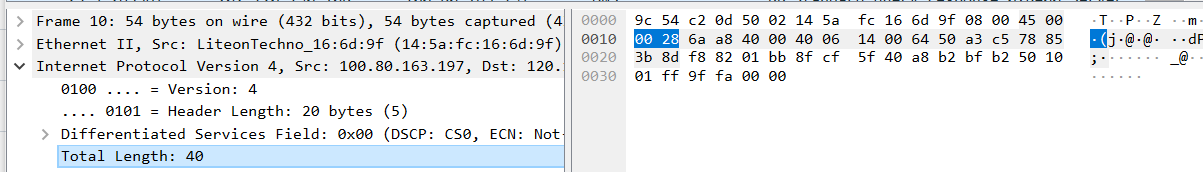
1. 查看IP报文字段内容，并解读；



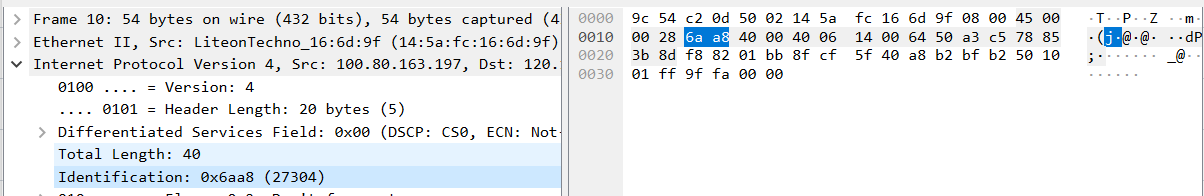
版本号为4，头长度为20字节（头长度为5个单位，一个单位表示四字节，共20字节）



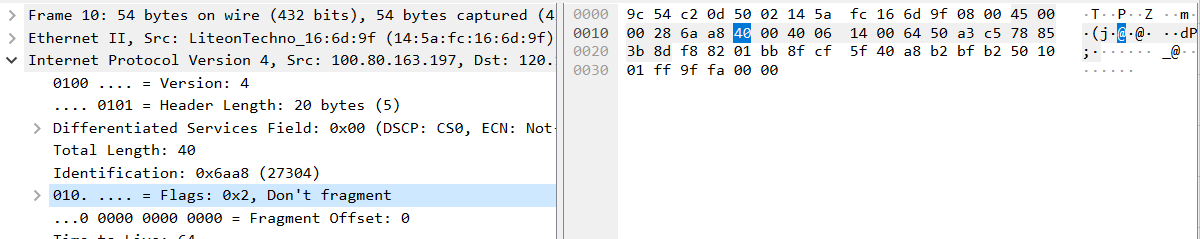
服务类型，该字段未被使用。



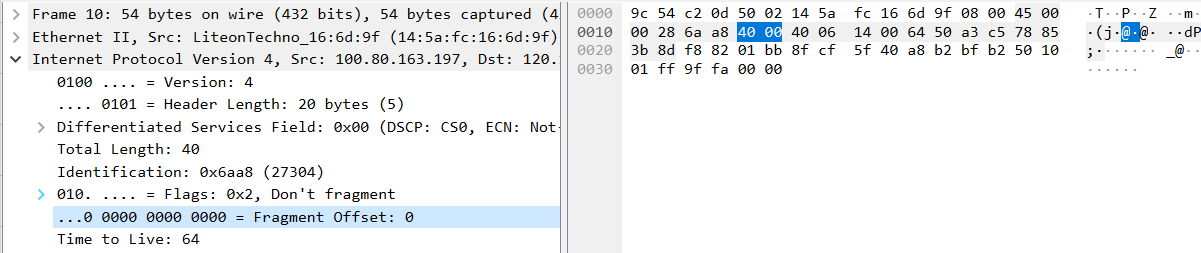
总长度：这里为0x28，即40个字节（首部和数据长度之和）



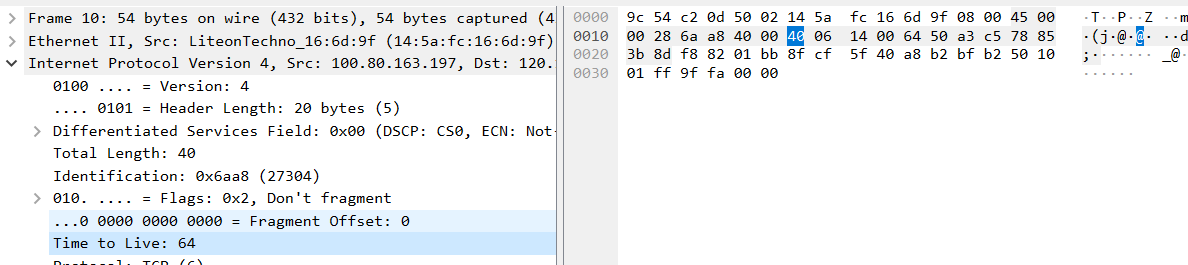
标识，这里为0x6aa8，即27304



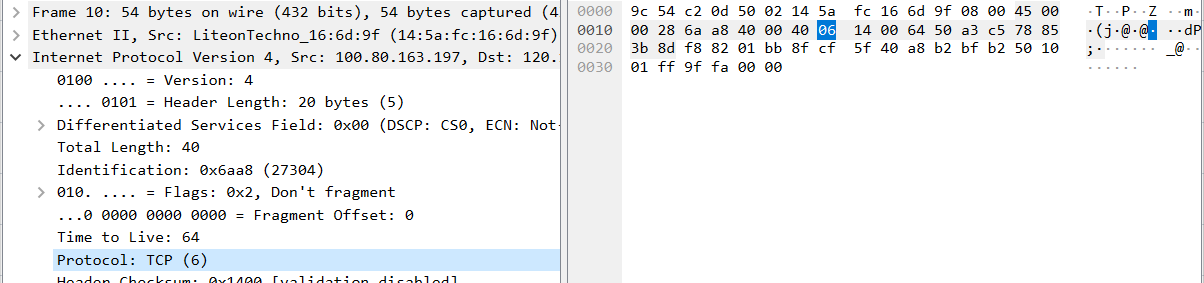
标志，3位，为0x010，表示不允许分片



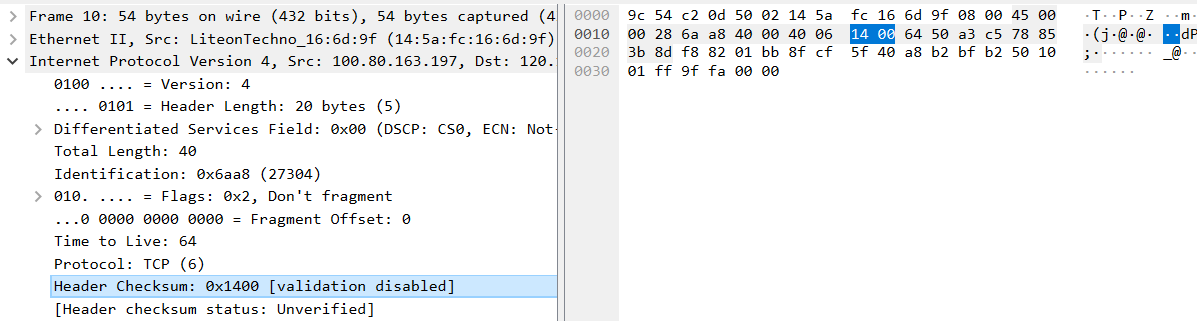
片偏移，13位，因为这里未分片，因此片偏移为0



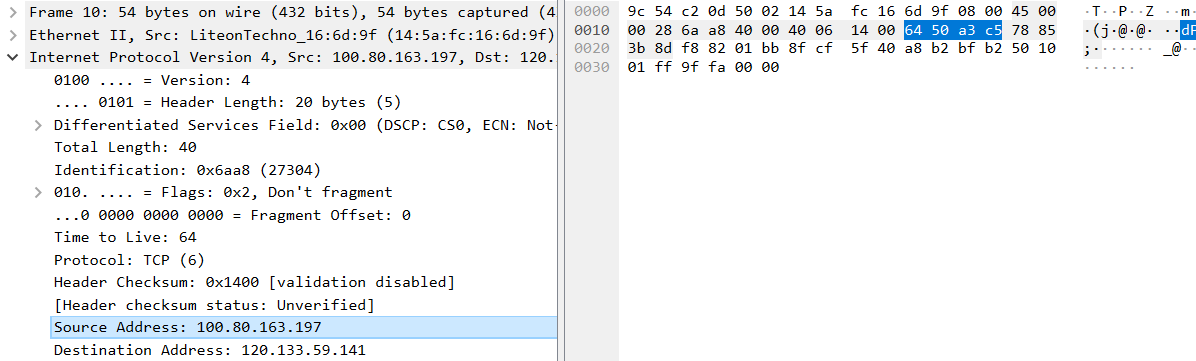
生存时间，表示数据报在网络中可通过的路由器数量，这里为0x40，即64.



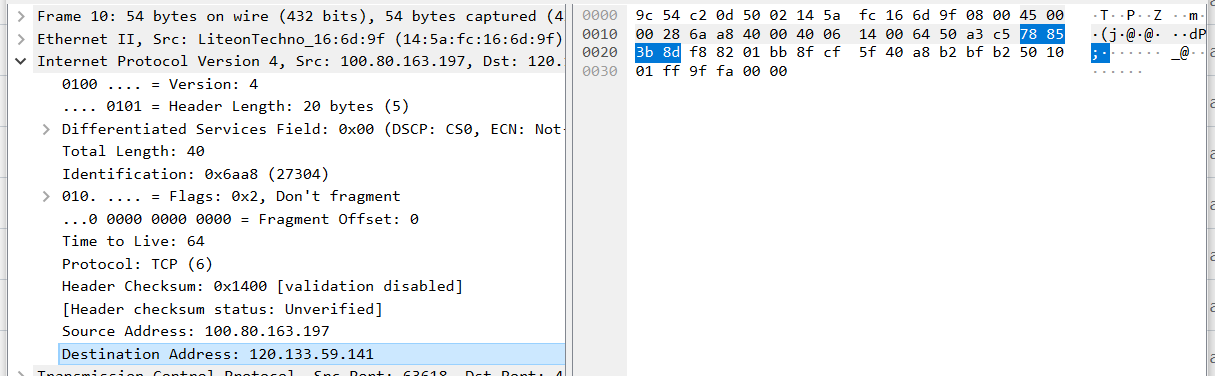
协议字段，根据不同值表示不同协议：ICMP（1）、IGMP（2）、IP（4）、TCP（6）、EGP（8）、IGP（9）、UDP（17）、IPv6（41）、ESP（50）、OSPF（89）。这里为0x06，表示TCP协议。



首部校验和，占16位，这里为0x1400，采用二进制反码求和算法



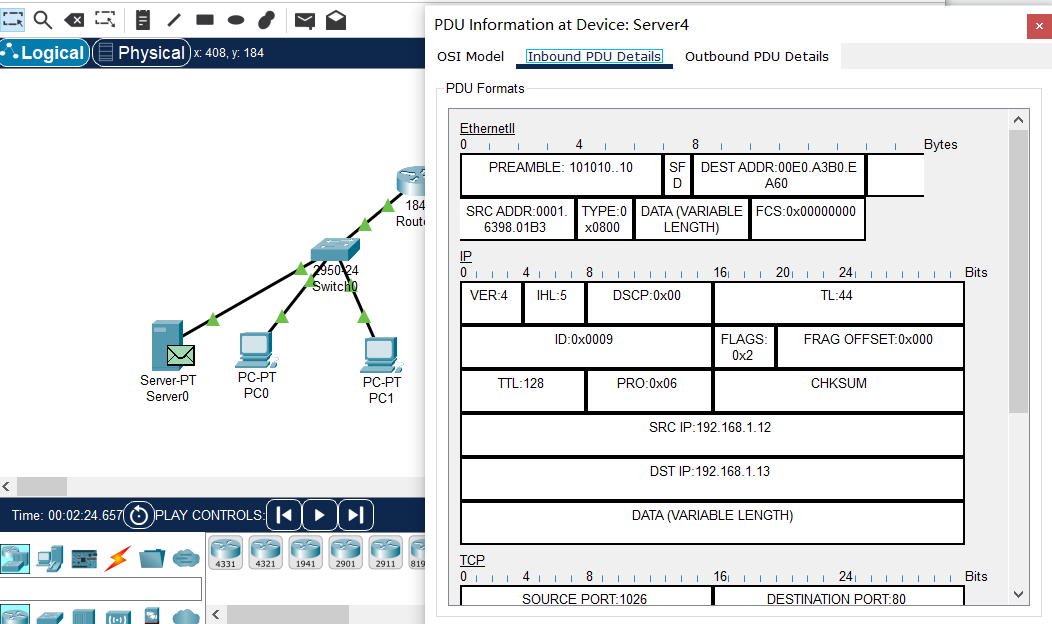
源地址IP，占16位，源地址为100.80.163.197



目的地址IP，占16位，目的地址为120.133.59.141

1. 分析在Packet Tracer中IP报文情况；

以PC0访问WEB 服务器为例



查看Packet Tracer中的IP报文可以获得以下信息（以上图报文为例）：

1. 版本：占4位，值为4，表示IPv4；
2. 首部长度：占4位，值为5，表示首部长度为4\*5=20个字节；
3. 区分服务（服务类型）：占8位，未使用
4. 总长度：占16位，值为44，表示总长度44字节
5. 标识：占16位，值为9
6. 标志，占3位，值为2，即0x010，表示不允许分片
7. 片偏移：占13位，值为0
8. 生存时间：占8位，值为128，表示最多可经过128个路由器
9. 协议：占8位，值位0x06，表示TCP协议
10. 校验和：占16位，这里没有具体显示
11. 源地址：占4字节，为192.168.1.12
12. 目的地址：占4字节，为192.168.1.13

**【实验名称】：APR消息分析实验**

**学生姓名：陈嘉瑞 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27日**

**【实验目的】**

1. 了解ARP协议
2. 掌握使用WireShark抓取ARP数据包的方法
3. 掌握分析ARP数据包的方法

**【实验原理】**

1. ARP出现原因

ARP协议是“Address Resolution Protocol”（地址解析协议）的缩写。其作用是在以太网环境中，数据的传输所依懒的是MAC地址而非IP地址，而将已知IP地址转换为MAC地址的工作是由ARP协议来完成的。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的MAC地址的。在以太网中，一个主机和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？它就是通过地址解析协议获得的。

所谓“地址解析”就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。

1. ARP映射方式
   1. 静态映射

静态映射的意思是要手动创建一张ARP表，把逻辑（IP）地址和物理地址关联起来。这个ARP表储存在网络中的每一台机器上。

例如，知道其机器的IP地址但不知道其物理地址的机器就可以通过查ARP表找出对应的物理地址。这样做有一定的局限性，因为物理地址可能发生变化：

（1）机器可能更换NIC（网络适配器），结果变成一个新的物理地址。

（2）在某些局域网中，每当计算机加电时，他的物理地址都要改变一次。

（3）移动电脑可以从一个物理网络转移到另一个物理网络，这样会时物理地址改变。

要避免这些问题出现，必须定期维护更新ARP表，此类比较麻烦而且会影响网络性能。

* 1. 动态映射

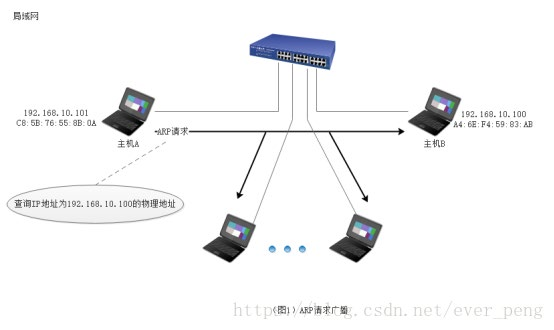
动态映射时，每次只要机器知道另一台机器的逻辑（IP）地址，就可以使用协议找出相对应的物理地址。已经设计出的实现了动态映射协议的有ARP和RARP两种。ARP把逻辑（IP）地址映射为物理地址。RARP把物理地址映射为逻辑（IP）地址。

1. ARP原理及流程

在任何时候，一台主机有IP数据报文发送给另一台主机，它都要知道接收方的逻辑（IP）地址。但是IP地址必须封装成帧才能通过物理网络。这就意味着发送方必须有接收方的物理（MAC）地址，因此需要完成逻辑地址到物理地址的映射。而ARP协议可以接收来自IP协议的逻辑地址，将其映射为相应的物理地址，然后把物理地址递交给数据链路层。

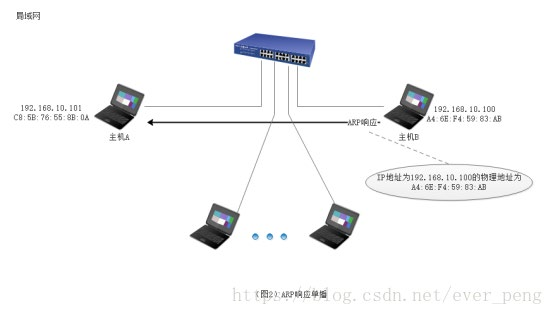
* 1. ARP请求

任何时候，当主机需要找出这个网络中的另一个主机的物理地址时，它就可以发送一个ARP请求报文，这个报文包好了发送方的MAC地址和IP地址以及接收方的IP地址。因为发送方不知道接收方的物理地址，所以这个查询分组会在网络层中进行广播。

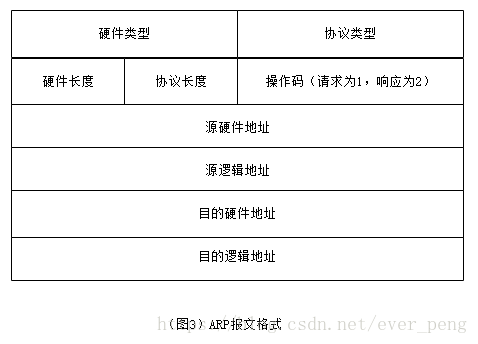


* 1. ARP响应

局域网中的每一台主机都会接受并处理这个ARP请求报文，然后进行验证，查看接收方的IP地址是不是自己的地址，只有验证成功的主机才会返回一个ARP响应报文，这个响应报文包含接收方的IP地址和物理地址。这个报文利用收到的ARP请求报文中的请求方物理地址以单播的方式直接发送给ARP请求报文的请求方。



1. ARP协议报文字段抓包解析
   1. 报文格式



硬件类型：16位字段，用来定义运行ARP的网络类型。每个局域网基于其类型被指派一个整数。例如：以太网的类型为1。ARP可用在任何物理网络上。

协议类型：16位字段，用来定义使用的协议。例如：对IPv4协议这个字段是0800。ARP可用于任何高层协议

硬件长度：8位字段，用来定义物理地址的长度，以字节为单位。例如：对于以太网的值为6，对于IPv4协议的值为4。

操作码：16位字段，用来定义报文的类型。已定义的分组类型有两种：ARP请求（1），ARP响应（2）。

源硬件地址：这是一个可变长度字段，用来定义发送方的物理地址。例如：对于以太网这个字段的长度是6字节。

源逻辑地址：这是一个可变长度字段，用来定义发送方的逻辑（IP）地址。例如：对于IP协议这个字段的长度是4字节。

目的硬件地址：这是一个可变长度字段，用来定义目标的物理地址，例如，对以太网来说这个字段位6字节。对于ARP请求报文，这个字段为全0，因为发送方并不知道目标的硬件地址。

目的逻辑地址：这是一个可变长度字段，用来定义目标的逻辑（IP）地址，对于IPv4协议这个字段的长度为4个字节。

* 1. ARP报文总长度

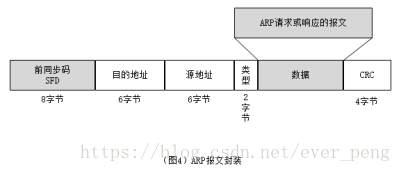
ARP报文的总长度为64字节。首先要知道帧的概念 帧是在数据链路层传输的数据格式，比如以太网v2，以太网IEEE802.3和PPP等。所以Wireshark抓到的帧是包含帧头的，即包含以太网v2的帧头，长14 bytes；而ARP数据包的长度固定为28 bytes；帧总长度 = 帧头 + 网络层包头 + 传输层报文头 + 应用数据；

而ARP请求中ARP包已经是最高层，之上没有传输层和应用层，所以总长度为：帧总长度 = 帧头 + ARP包头 = 14 + 28 = 42bytes；而真正发包的时为了保证以太网帧的最小帧长为64 bytes，会在报文里添加一个padding字段，用来填充数据包大小。使用wireshark抓包时，抓到的包为60 bytes。比以太网帧的最小帧长少了4 bytes，原因是因为wireshark抓包时不能抓到数据包最后的CRC字段。

CRC字段是为了校验以太网帧的正确性。在数据包填充完成后，回去通过算法计算一个值放到数据包的CRC字段中。当接受端收到数据包后，会同样使用算法计算一个值，然后和CRC字段的值进行对比，查看是否相同。如果不同则证明数据包被更改，如果相同则证明数据包并未被更改。

* 1. 报文封装

ARP报文直接封装在数据链路帧中，例如，图4中，ARP分组被封装在以太网的帧中。注意，帧中的类型字段指出此帧所携带的数据是ARP报文。

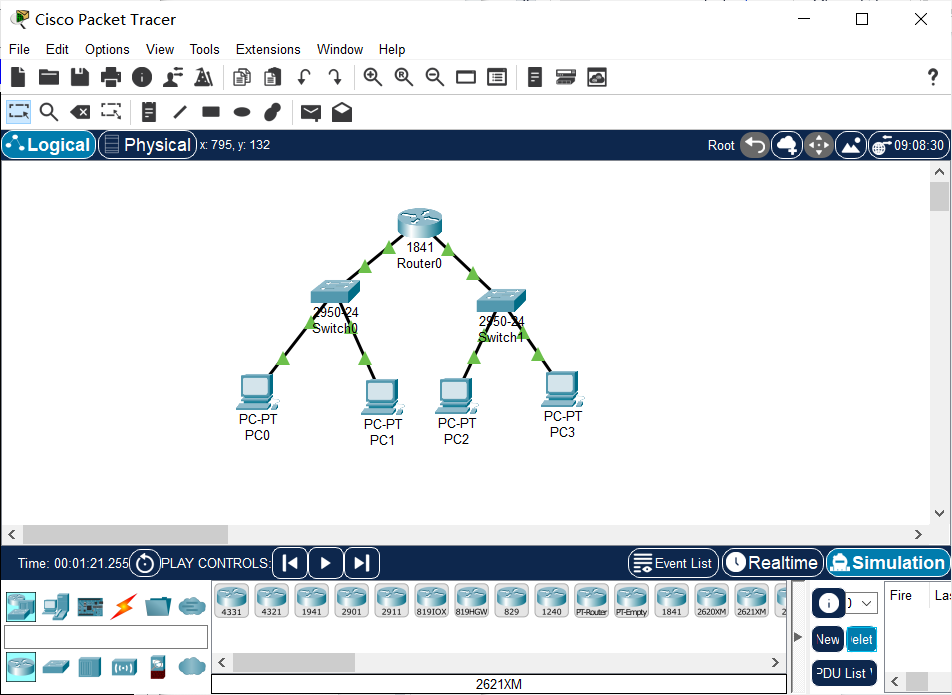


**【实验设备】**

个人笔记本电脑、Cisco Packet Tracer实验软件。

**【实验步骤及现象】**

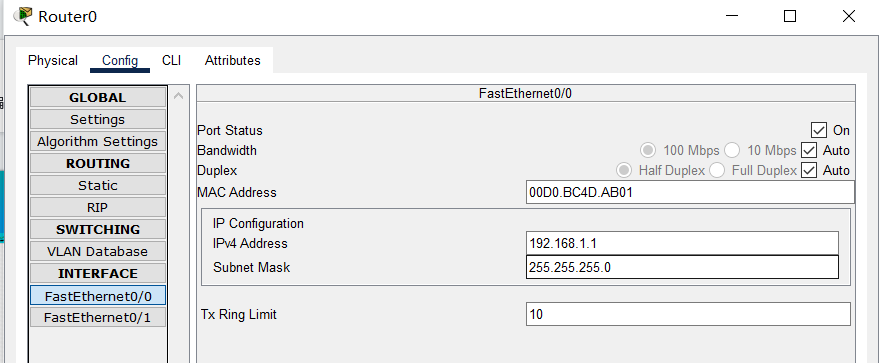
1. 首先规划网络地址及拓扑图；



1. 路由器接口IP地址配置；

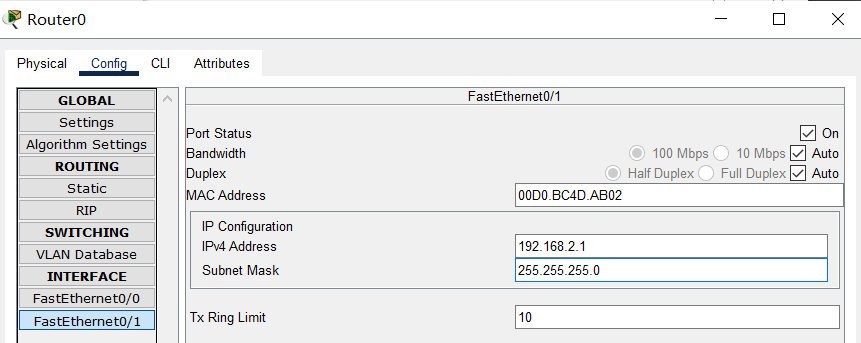
F0/0:

IP:192.168.1.1



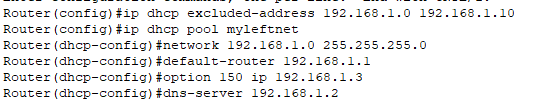
F0/1:

IP:192.168.2.1

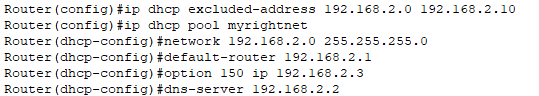


1. 配置DHCP

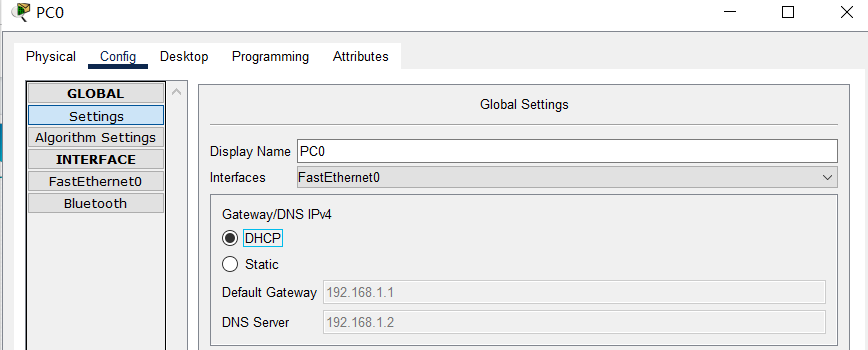
配置左侧子网DHCP：



配置右侧子网DHCP：



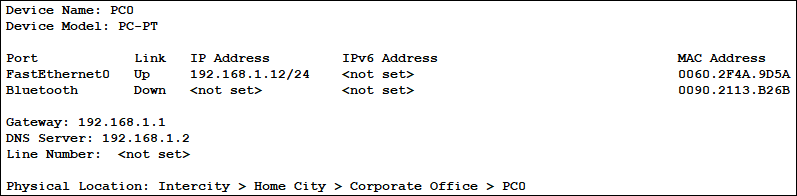
各个PC及server开启使用DHCP（以PC0为例）：



1. 验证各个PC的IP地址。

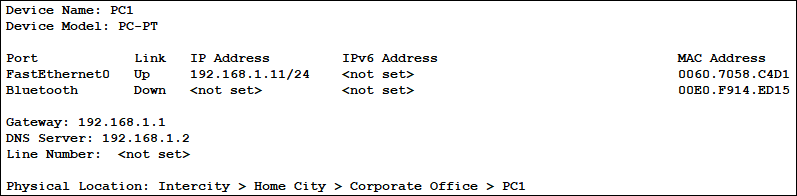
PC0

IP:192.168.1.12



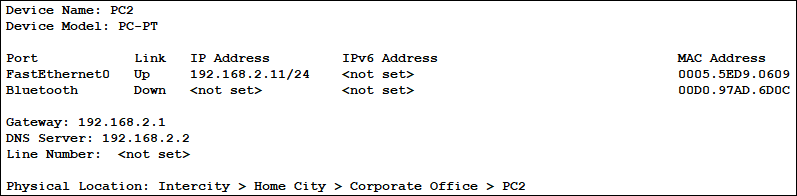
PC1

IP:192.168.1.11



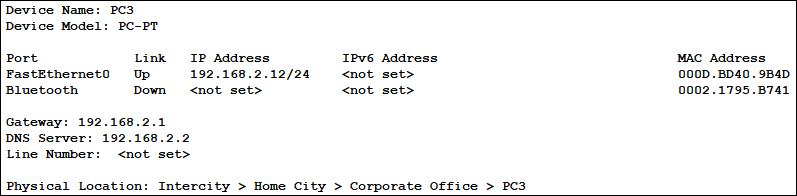
PC2

IP:192.168.2.11

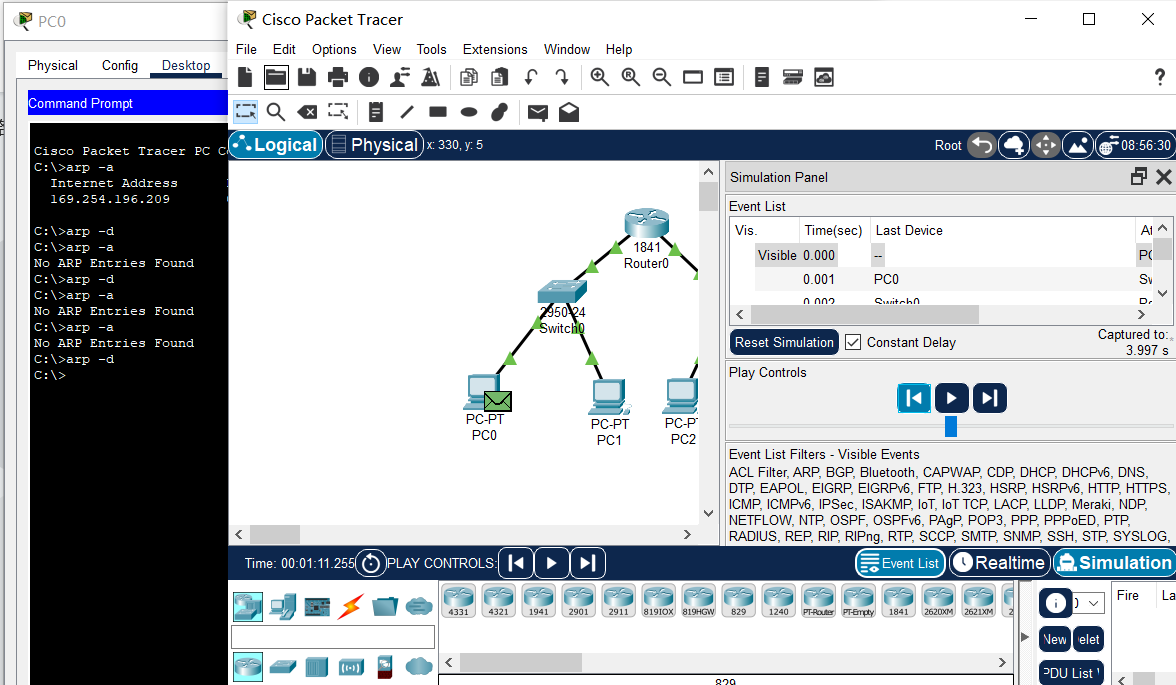


PC3

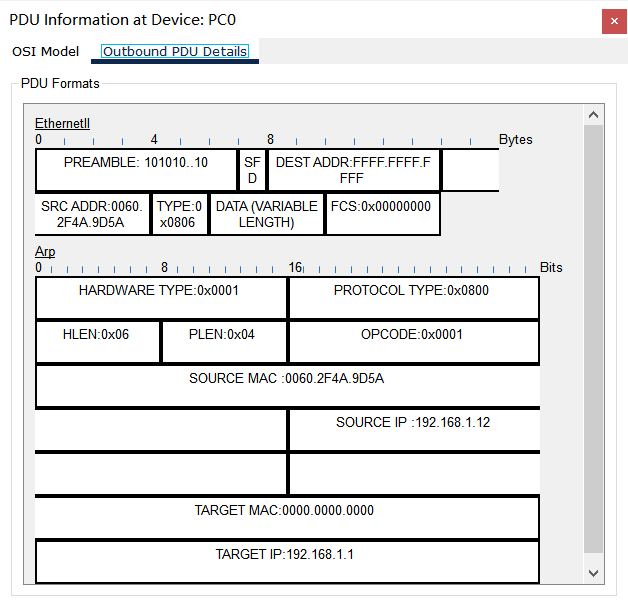
IP:192.168.2.12



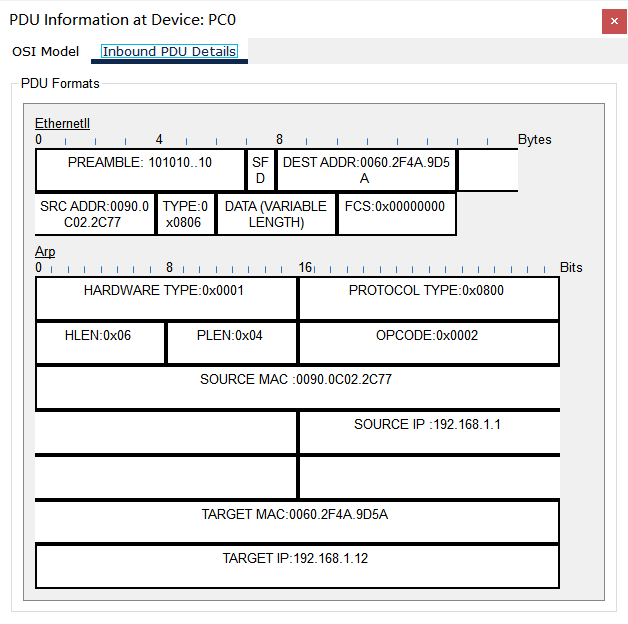
1. PC0发送arp报文并查看报文内容



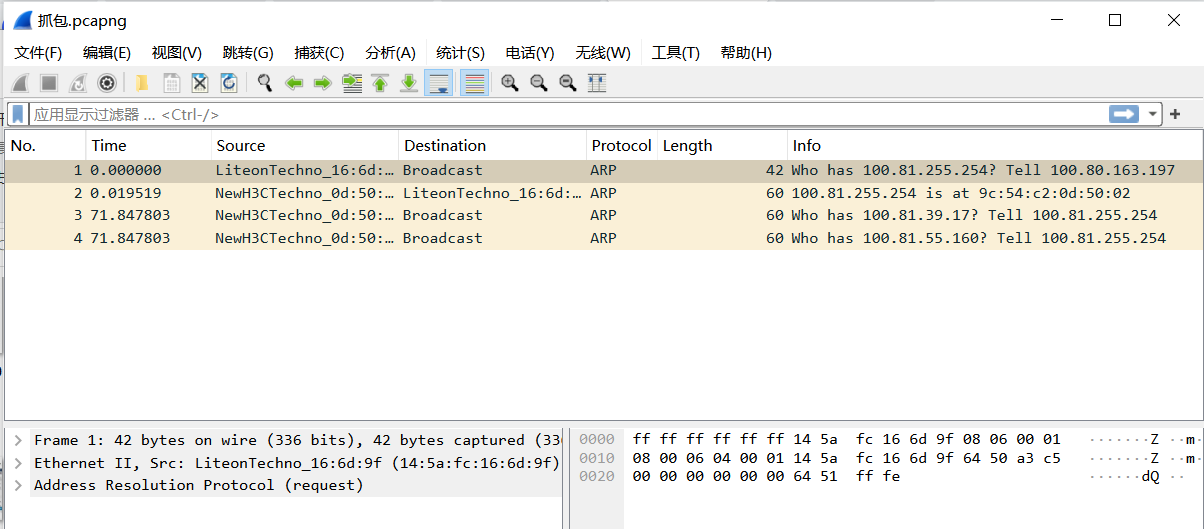
PC0发送时：



PC0接收时：

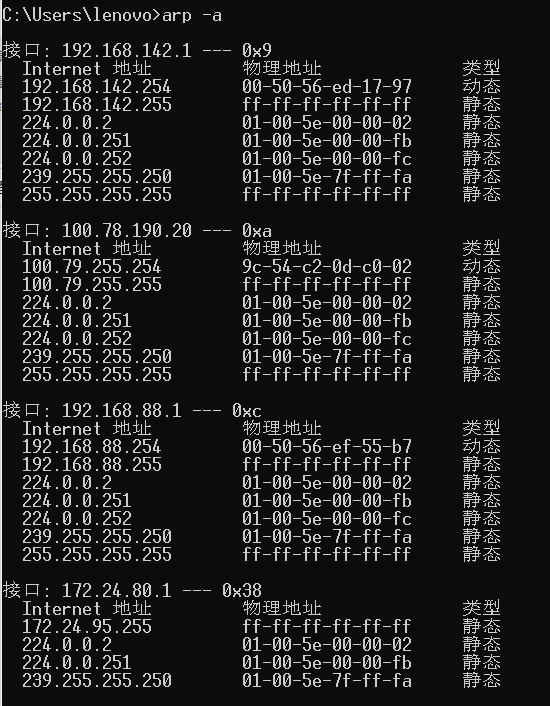


1. 用WireShark抓取ARP数据包并查看ARP报内容



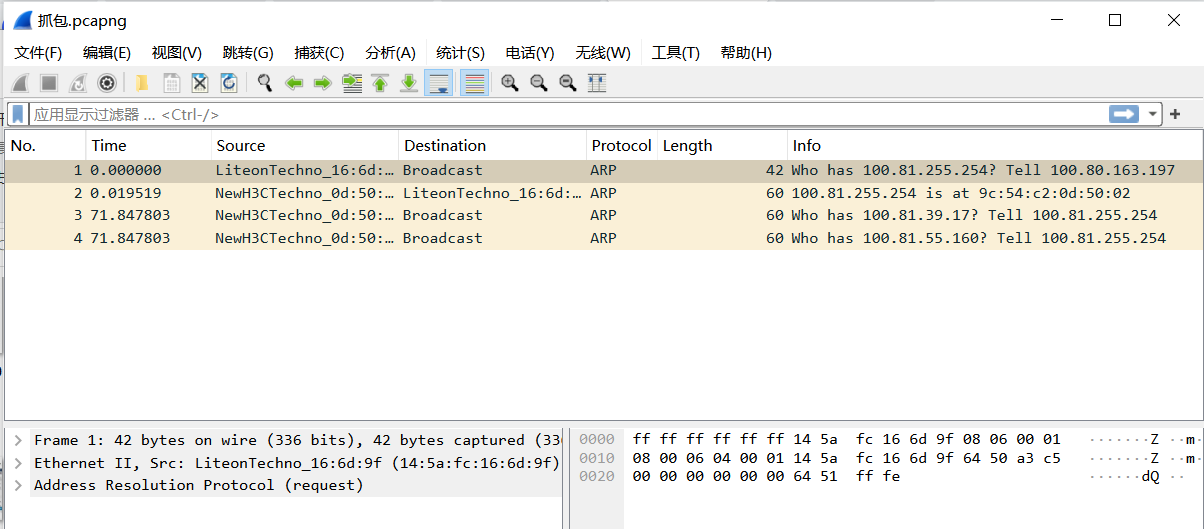
**【分析讨论】**

1. 查看本机ARP内容

****

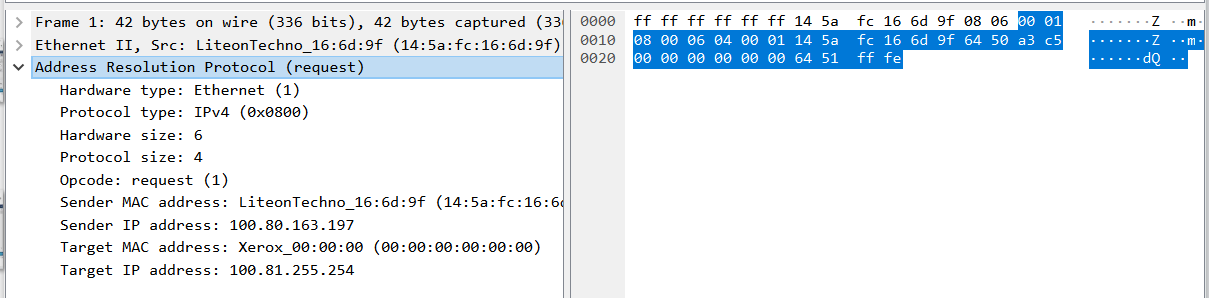
1. 用WireShark抓取ARP数据包

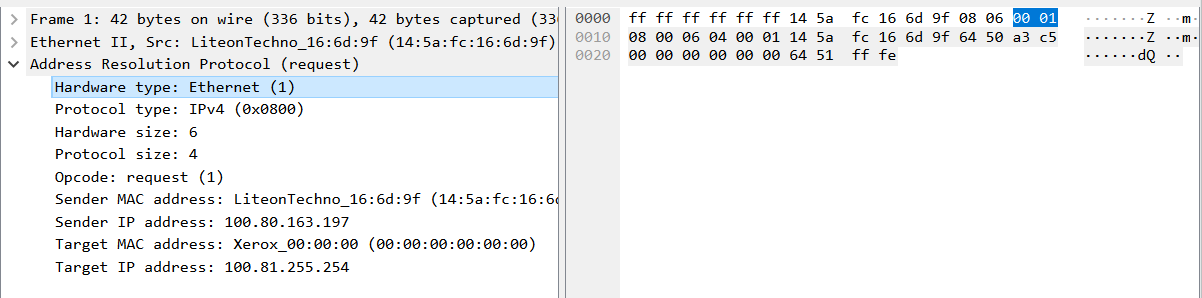
这里先用arp -d删除目前存储的其他IP对应的物理地址，然后捕获ping baidu.com时本机发送以及对方应答的ARP包

****

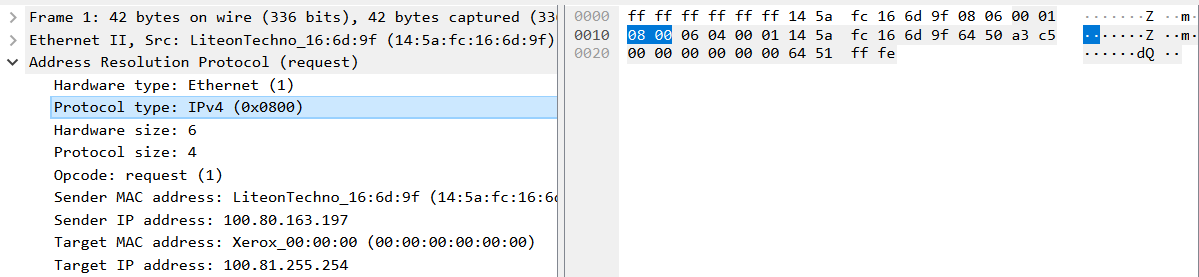
1. 查看ARP报文字段内容并解读

ARP请求：

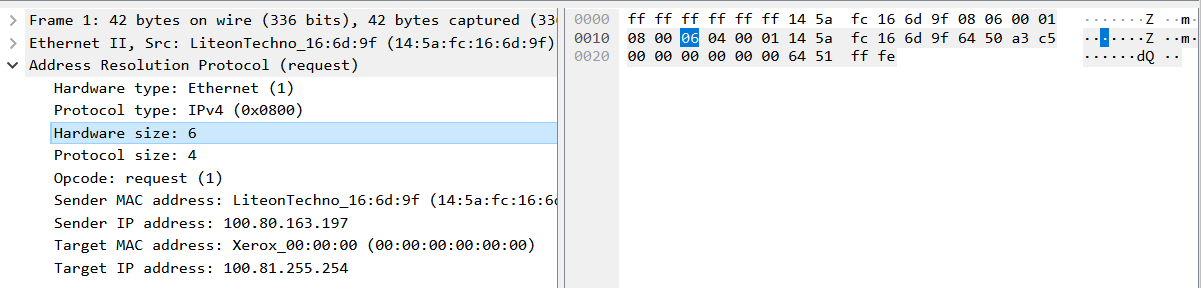




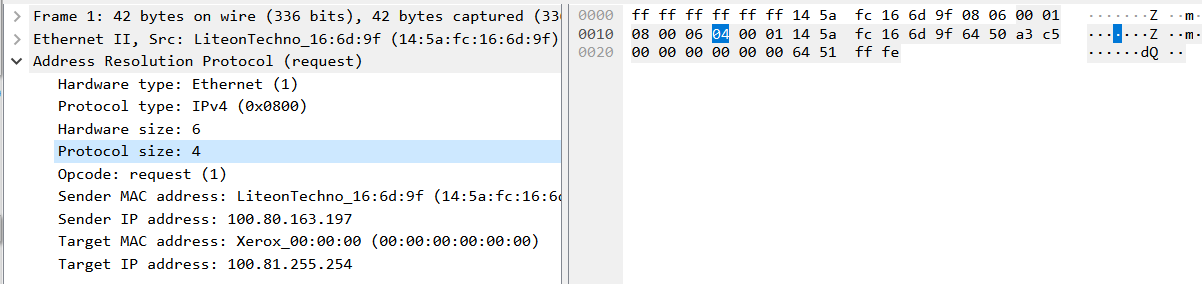
硬件类型，16位，这里为0x0001，表示以太网



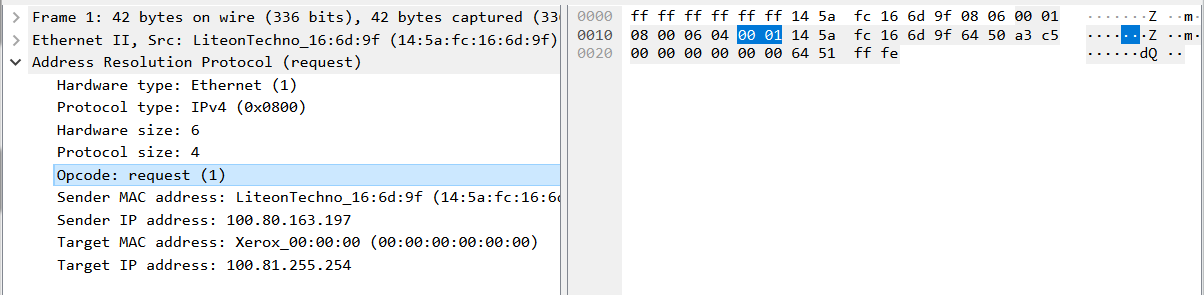
协议类型，16位，这里为0x0800，表示IPv4



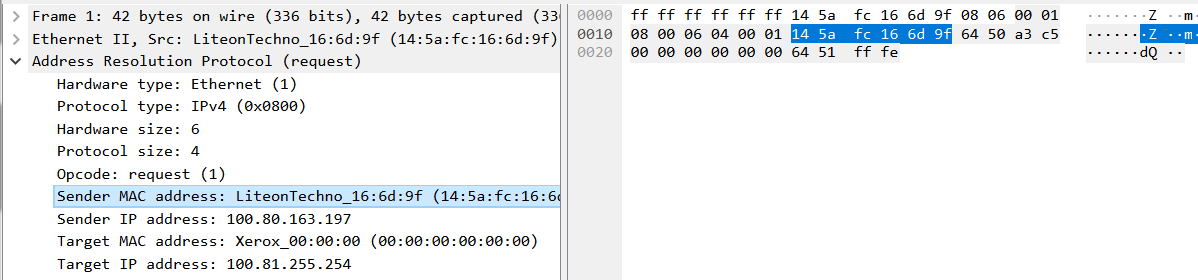
硬件长度，8位，代表物理地址长度，这里为0x06，表示这是一个以太网的物理地址。



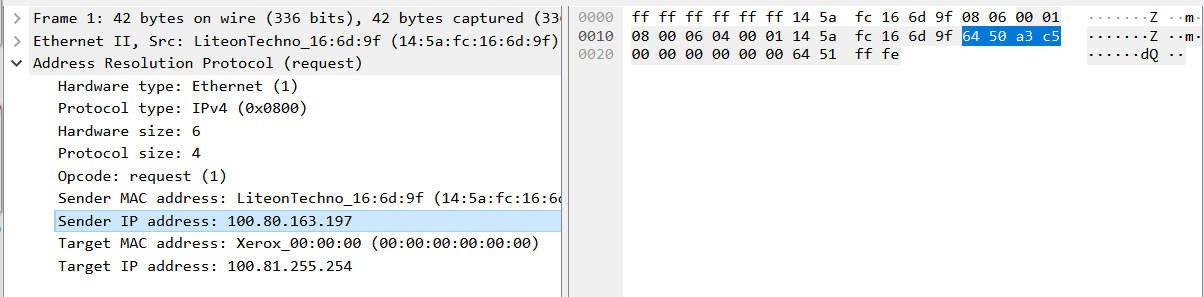
协议长度，8位，这里为0x04，表示IPv4协议



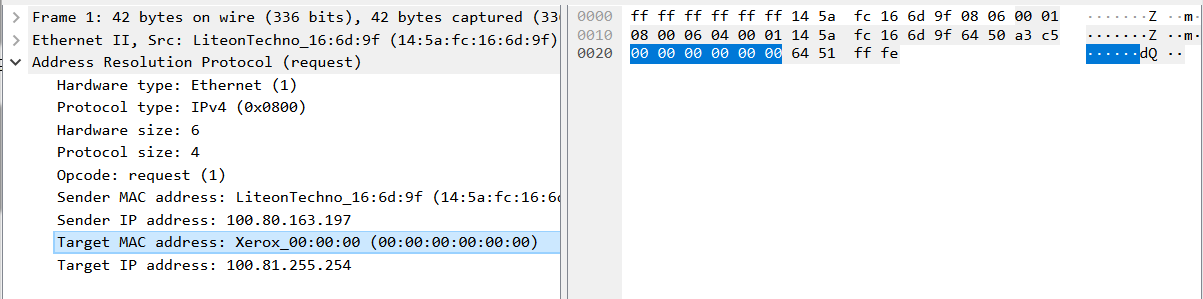
操作码，16位，这里为0x0001，表示ARP请求



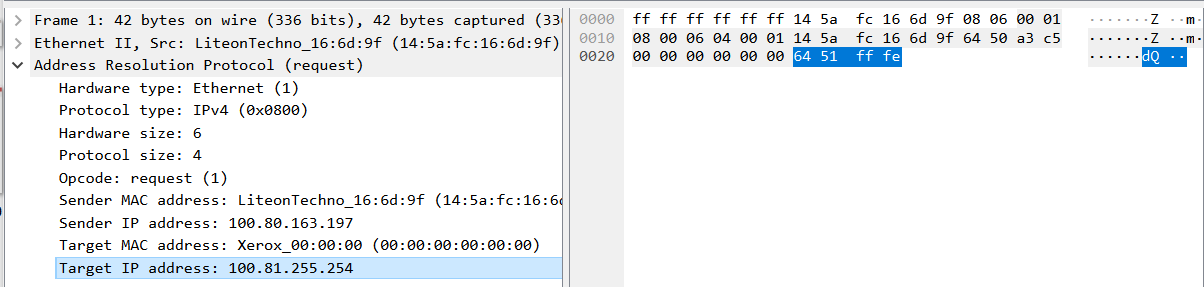
源硬件地址，对于以太网为6字节，这里地址为14:5a:fc:16:6d:9f



源逻辑地址，对于IP协议为4字节，这里为100.80.163.197

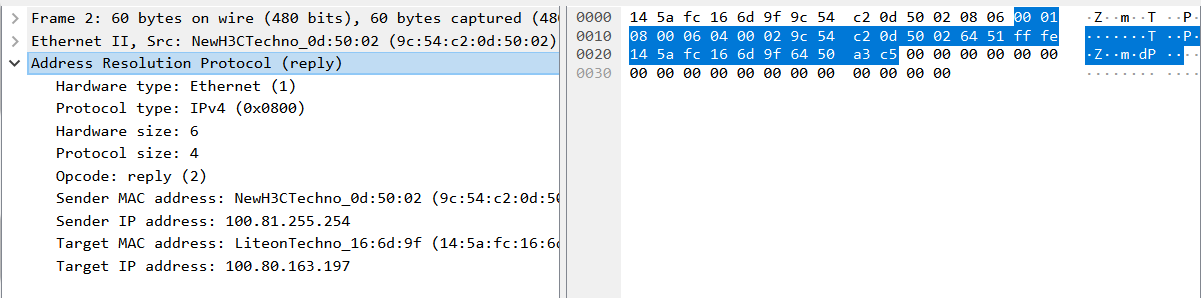


目的硬件地址，因为这是一个ARP请求报文，因此该字段为全0，因为发送方不知道目标的硬件地址。



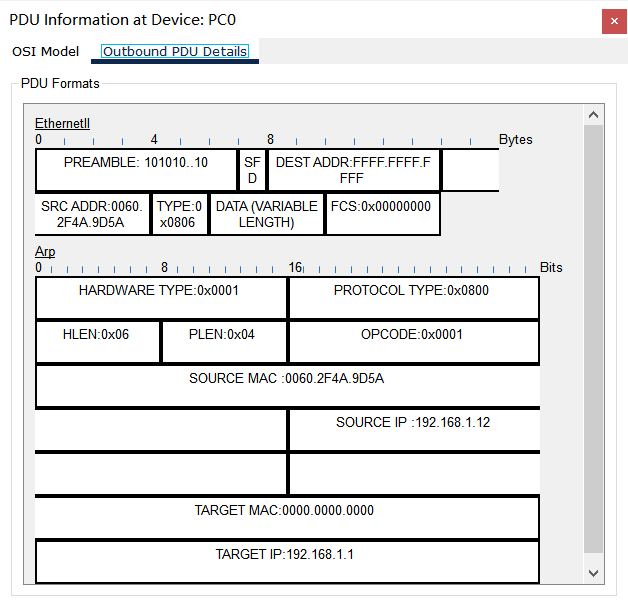
目的逻辑地址，4字节，这里为100.81.255.254

ARP响应：



可以看到，在ARP响应中，操作码变为0x0002，源地址为ARP请求中的目的逻辑地址所对应的物理地址，这里为9c:54:c2:0d:50:02

1. 分析在Packet Tracer中ARP报文情况



在PC0发送的ARP请求中：

硬件类型为1

协议类型为IPv4

硬件物理地址长度为6（以太网）

逻辑地址长度为4（IPv4协议）

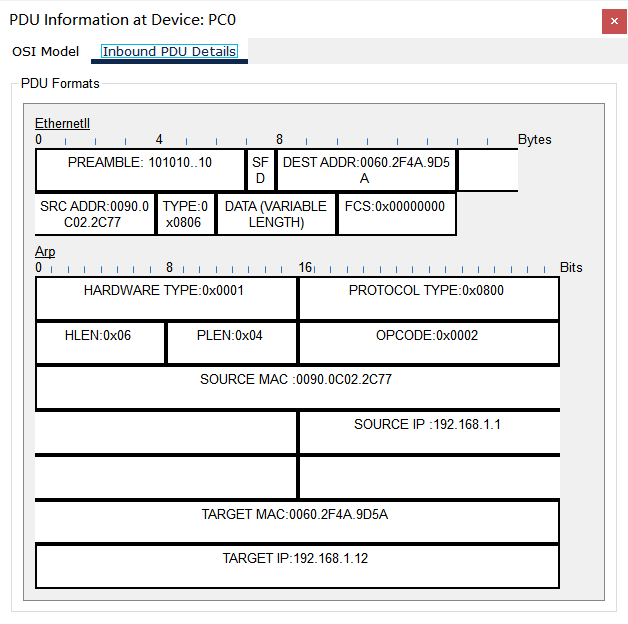
操作码为1（表示ARP请求）

源硬件地址为0060.2F4A.9D5A

源逻辑地址为192.168.1.12

目标硬件地址目前未知，为全0

目的逻辑地址为192.168.1.1



在PC0收到的ARP响应中：

硬件类型为1

协议类型为IPv4

硬件物理地址长度为6（以太网）

逻辑地址长度为4（IPv4协议）

操作码为2（表示ARP响应）

源硬件地址为0090.0C02.2C77

源逻辑地址为192.168.1.1

目标硬件地址为0060.2F4A.9D5A

目的逻辑地址为192.168.1.12