实验(二十)：IP数据包分析实验

一.实验目的

本实验的核心目的是深入理解和掌握IP协议的数据报文格式和传输过程。通过具体的分析和实践操作理解网络层的工作机制，实验目的如下：

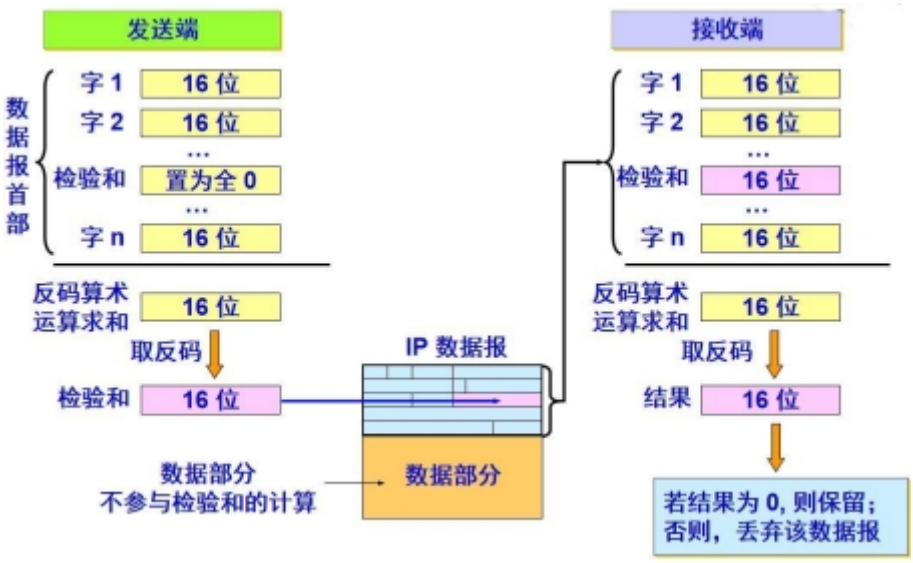
- **理解和分析IP数据报文的结构**：通过研究IP协议的各个部分，包括首部和数据区，以及首部中的固定部分和可选字段，学习如何IP数据报是如何封装和拆封的。
- **掌握IP数据报的传输过程**：通过分析数据报的各字段如版本、首部长度、服务类型等，了解它们在数据传输中的具体作用和意义。
- **应用实际工具进行IP数据包分析**：使用工具Wireshark和Packet Tracer来抓取和分析IP数据包，以实际查看IP数据报文的字段内容，并解读这些内容的具体意义。
- **了解IP数据报的选项字段**：学习选项字段中的各种设置，如源路由选择、记录路由、时间戳等，这些选项是如何影响数据报的传输路径和性能的。

二.实验原理

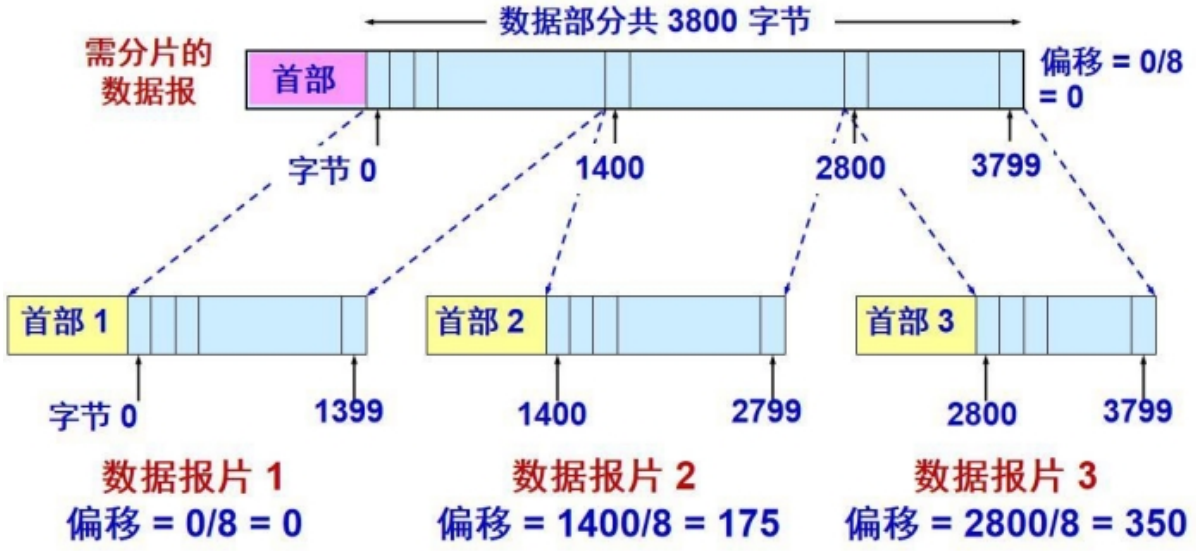
- IP协议是一种无连接的、不可靠的传输协议，用于在网络层进行数据传输。本实验的目的是深入探索和理解IP数据报文的结构及其传输过程，通过分析首部格式、不同字段的功能以及数据的封装与拆封来实现这一目标。
- IP数据报文格式总览
    - IP协议提供不可靠无连接的数据报传输服务，IP层提供的服务是通过IP层对数据报的封装与拆封来实现的。IP数据报的格式分为报头区和数据区两大部分，其中报头区是为了正确传输高层数据而加的各种控制信息，数据区包括高层协议需要传输的数据。
    - 一个 IP 数据报由首部和数据两部分组成。

- 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。

- 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。
- 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

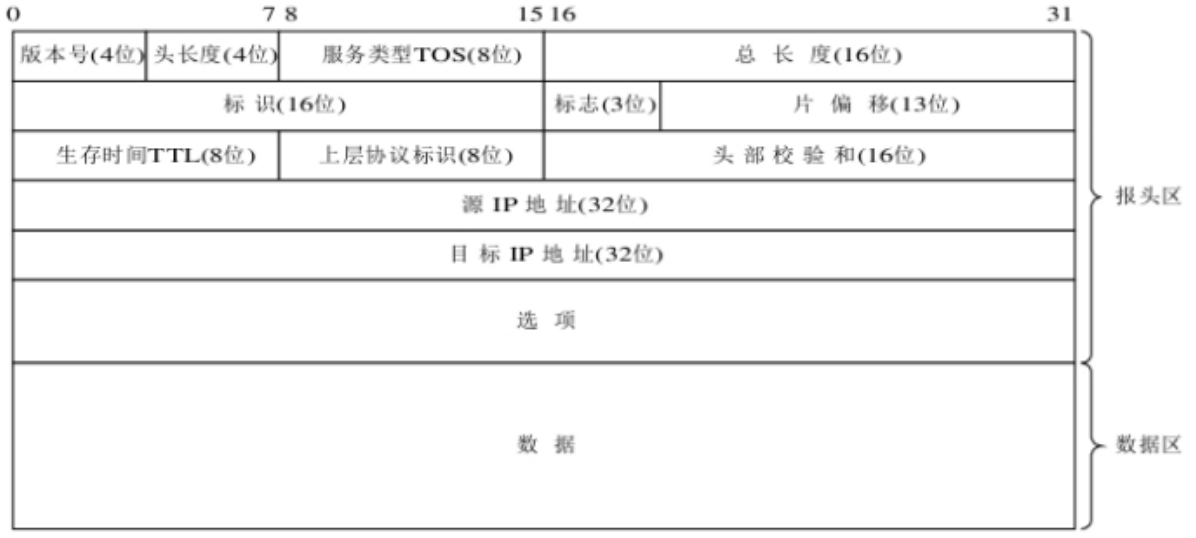


- IP数据报分段
  - 给出一数据报的总长度为 3820 字节，其数据部分的长度为 3800 字节（使用固定首部），需要分片为长度不超过 1420 字节的数据报片。因固定首部长度为 20 字节，因此每个数据报片的数据部分长度不能超过 1400 字节。于是分为 3 个数据报片，其数据部分的长度分别为 1400、1400 和 1000 字节。原始数据报首部被复制为各数据报片的首部，但必须修改有关字段的值（如标志字段）。



	总长度	标识	MF	DF	片偏移
原始数据报	3820	12345	0	0	0
数据报片1	1420	12345	1	0	0
数据报片2	1420	12345	1	0	175
数据报片3	1020	12345	0	0	350

- IP数据报文格式传输

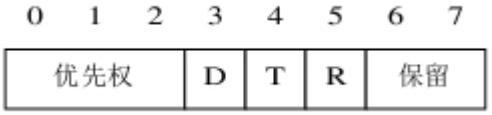


上图表示的数据，最高位在左边，记为0位；最低位在右边，记为31位。在网络中传输数据时，先传输0~7位，其次是8~15位，然后传输16~23位，最后传输24~31位。

- IP数据报文上层协议

十进制编号	协　议	说　　明
0	无	保留
1	ICMP	网际控制报文协议
2	IGMP	网际组管理协议
3	GGP	网关—网关协议
4	无	未分配
5	ST	流
6	TCP	传输控制协议
8	EGP	外部网关协议
9	IGP	内部网关协议
11	NVP	网络声音协议
17	UDP	用户数据报协议

- 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。



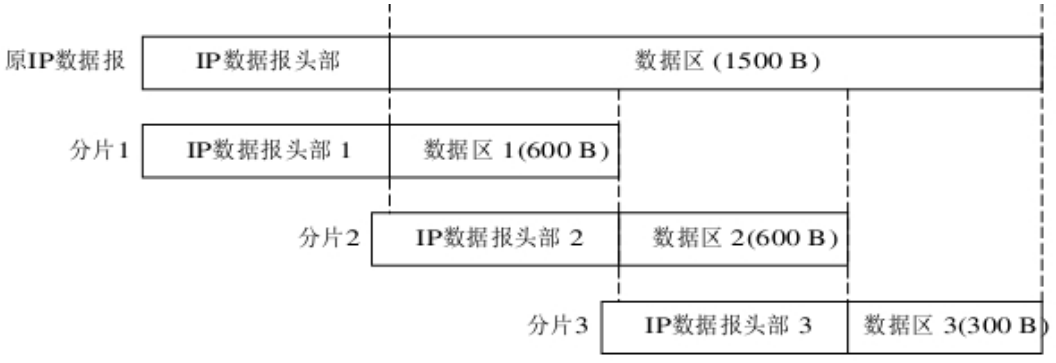
  - 服务类型字段的8位分成了5个子域：
    - 优先权（0-7）数越大，表示该数据报优先权越高。网络中路由器可以使用优先权进行拥塞控制，如当网络发生拥塞时可以根据数据报的优先权来决定数据报的取舍。
    - 短延迟位D(Delay)：该位置1时，数据报请求以短延迟信道传输，0表示正常延时。
    - 高吞吐量位T(Throughput)：该位置1时，数据报请求以高吞吐量信道传输，0表示普通。
    - 高可靠位R(Reliability)：该位置1时，数据报请求以高可靠性信道传输，0表示普通。
    - 保留位。
- 目前在Internet中使用的TCP/IP协议大多数情况下网络并未对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：

应用程序	短延迟位D	高吞吐量位T	高可靠性位	低成本位	十六进制值	特性
Telnet	1	0	0	0	0x10	短延迟
FTP控制	1	0	0	0	0x10	短延迟
FTP数据	0	1	0	0	0x08	高吞吐量
TFTP	1	0	0	0	0x10	短延迟
SMTP命令	1	0	0	0	0x10	短延迟
SMTP数据	0	1	0	0	0x08	高吞吐量
DNS UDP查询	1	0	0	0	0x10	短延迟
DNS TCP查询	0	0	0	0	0x00	普通
DNS 区域传输	0	1	0	0	0x08	高吞吐量
ICMP差错	0	0	0	0	0x00	普通
ICMP查询	0	0	0	0	0x00	普通
SNMP	0	0	1	0	0x04	高可靠性
IGP	0	0	1	0	0x04	高可靠性
NNTP	0	0	0	1	0x02	低成本

- 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：

网 络 名 称	MTU(单位：字节)
以太网	1500
IEEE802.3/802.2	1492
FDDI	4352
ATM(信元)	48
X.25	576
点到点(低延时)	296
令牌环网(IBM 16 MB/s)	17 914
令牌环网(IEEE802.5 IBM 16 MB/s)	4464

- 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

- 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：
  - 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；
  - 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；
  - 根据“偏移量”字段可以确定分片在原数据报中的位置。

- IP数据报选项
  - IP数据报“选项”主要有两大功能：
    - 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；
    - 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。
- 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。
  - 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。
  - 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：

1字节	1字节	1字节	4位	4位	4字节	4字节	4字节	4字节	
选项码	选项长度	指针	溢出	标志	第1站IP地址	第1时间戳	第2站IP地址	第2时间戳	…

- 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：

标志字段值	含　义
0	只记录时间戳，不记录 IP 地址，即在图 2-15 所示的格式中去掉 IP 地址项，只记录每台路由器的时间戳。由于没有 IP 地址做参考，所以用途有限
1	记录数据报通过路径时每台路由器的 IP 地址和时间戳。在选项列表中只有存放 4 对 IP 地址和时间戳的空间。其格式与图 2-15 所示的格式一致
3	发送端对选项列表进行初始化，存放了 4 个 IP 地址和 4 个取值为 0 的时间戳值。只有当列表中的下一个 IP 地址与当前路由器地址相匹配时，才记录它的时间戳。这种方式用途较广

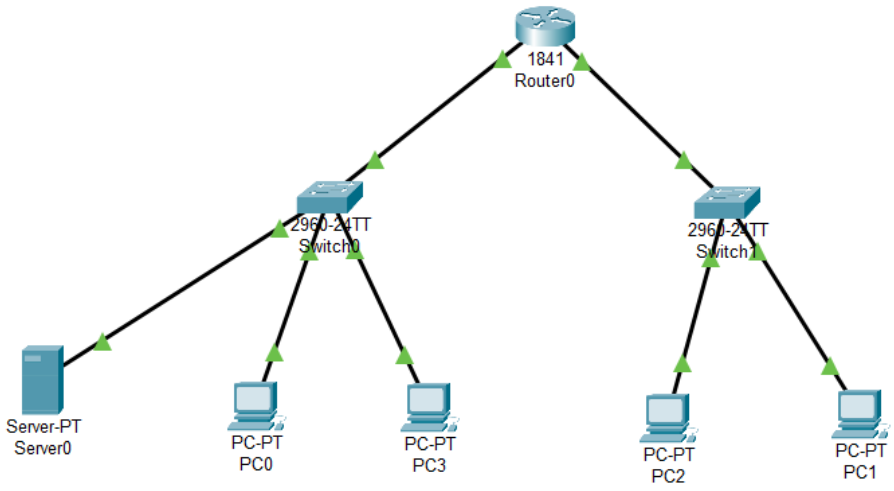
三.实验环境

- 操作系统：Windows 11
- 网络环境：局域网
- 软件：`Cisco Packet Tracer`虚拟实验环境

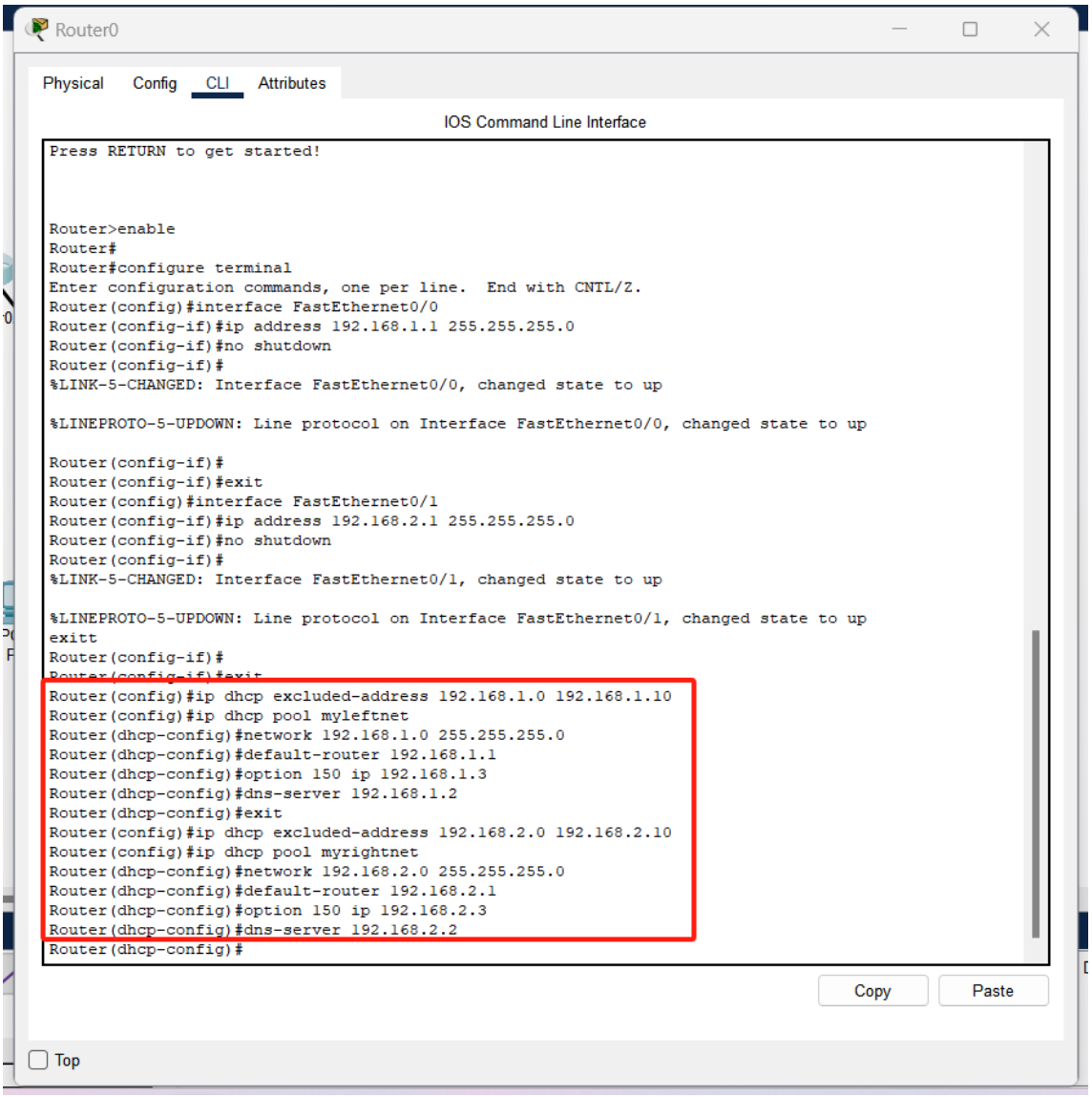
四.实验步骤

- 规划网络地址及拓扑图；

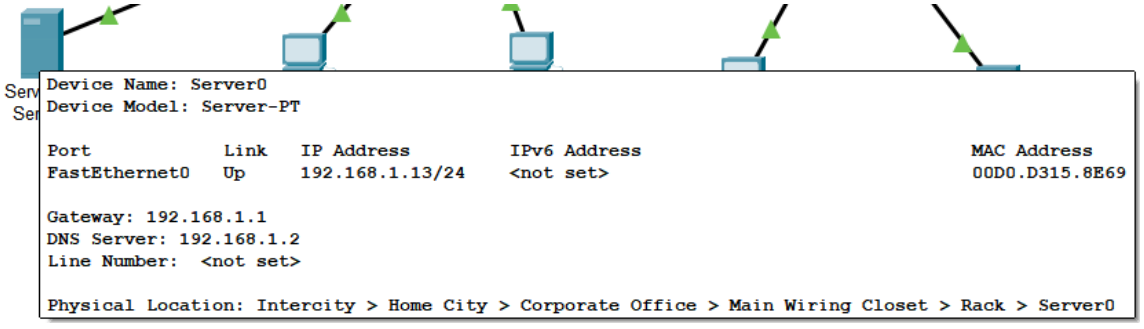
本实验中使用四台PC和一台WEB服务器，按下图拓扑结构进行连接。



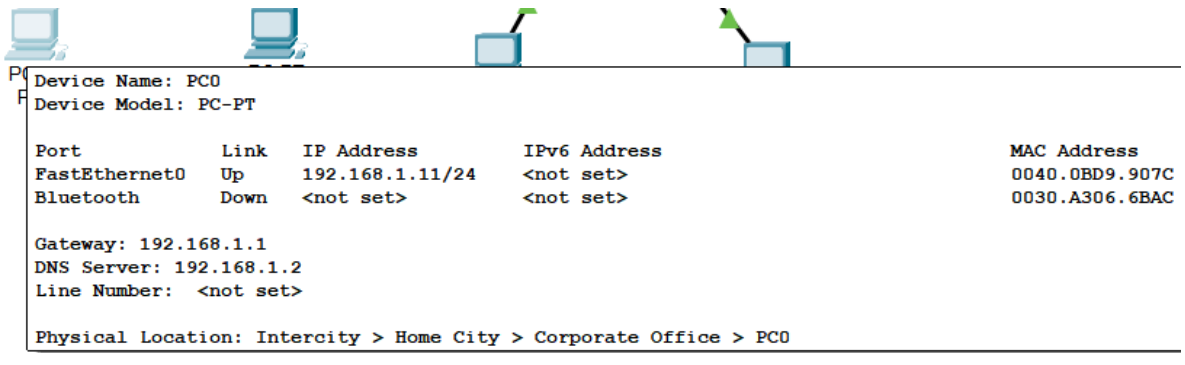
- 路由器接口IP地址配置；
  - F0/0：IP：`192.168.1.1`
  - F0/1：IP：`192.168.2.1`
- 配置DHCP
  - 为简化实验流程，这里采用前几次实验使用过的DHCP，让PC动态获取IP。



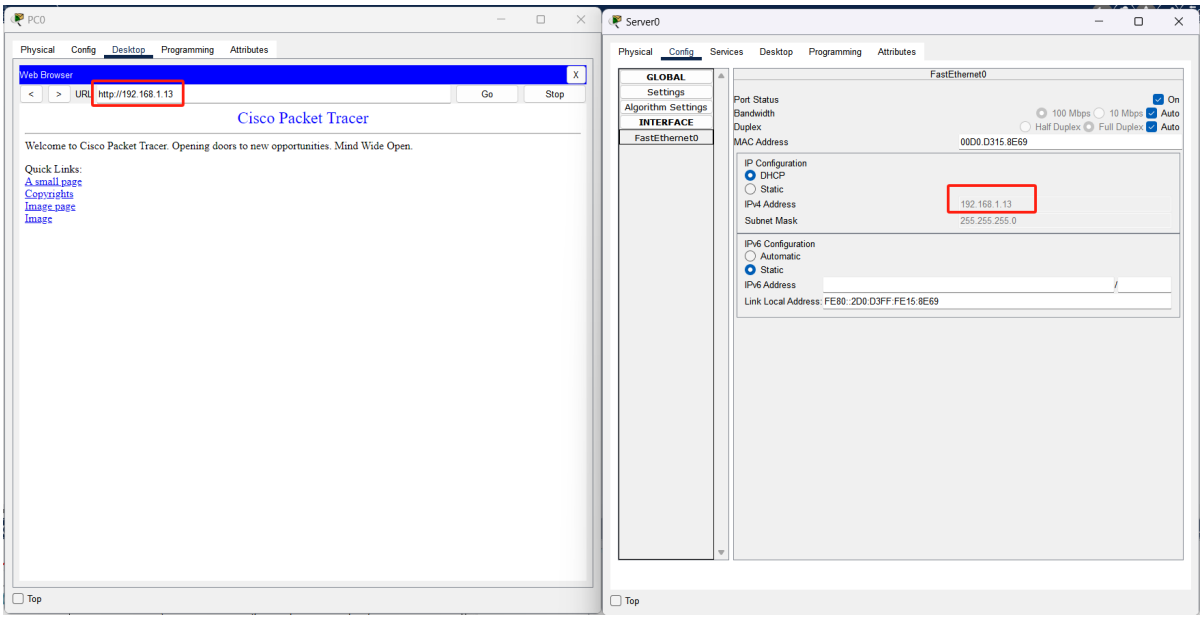
- 验证各个PC（以PC0为例）及server的IP地址。
  - Server：IP：`192.168.1.13`



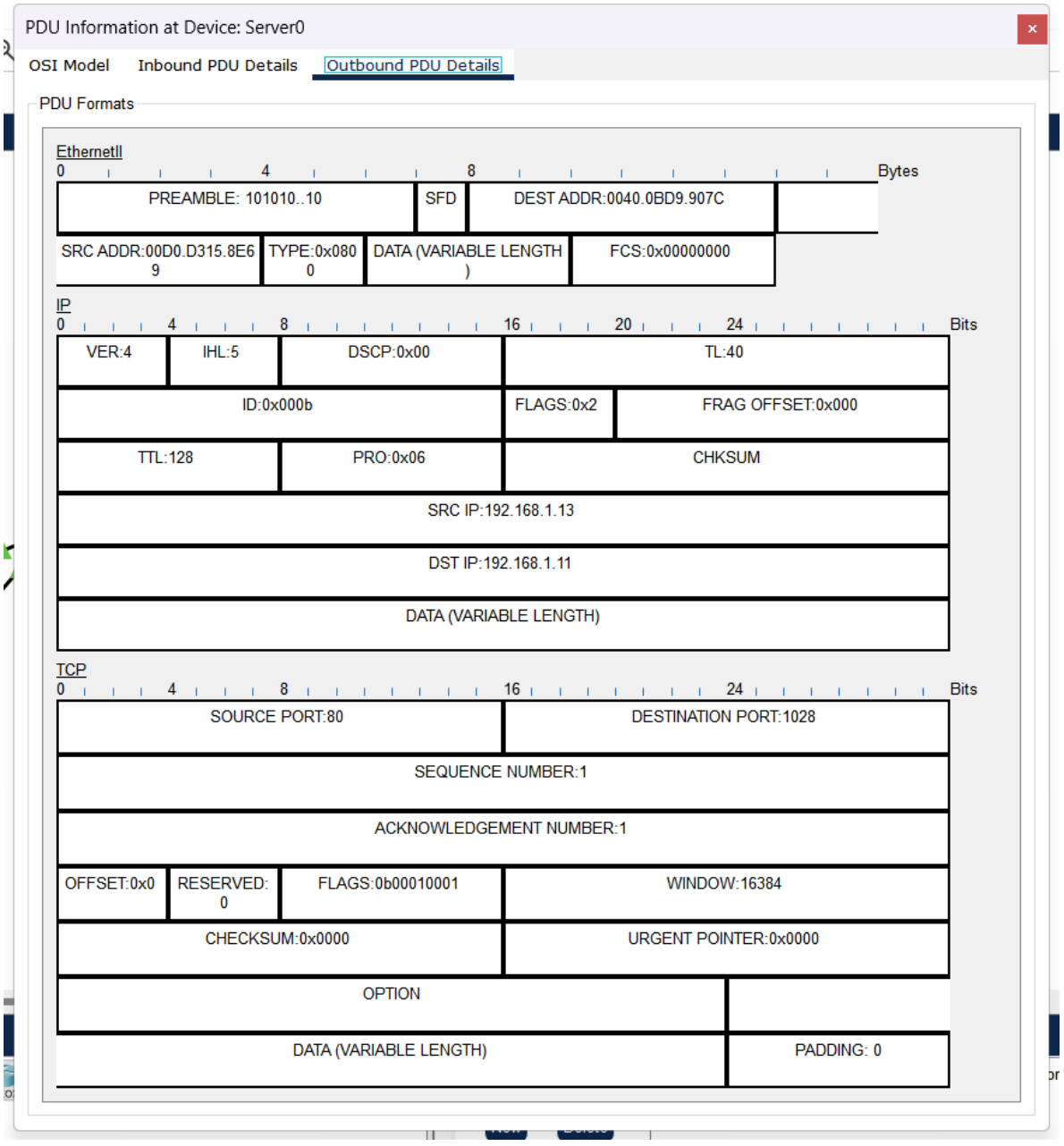
  - PC0：IP：`192.168.1.11`



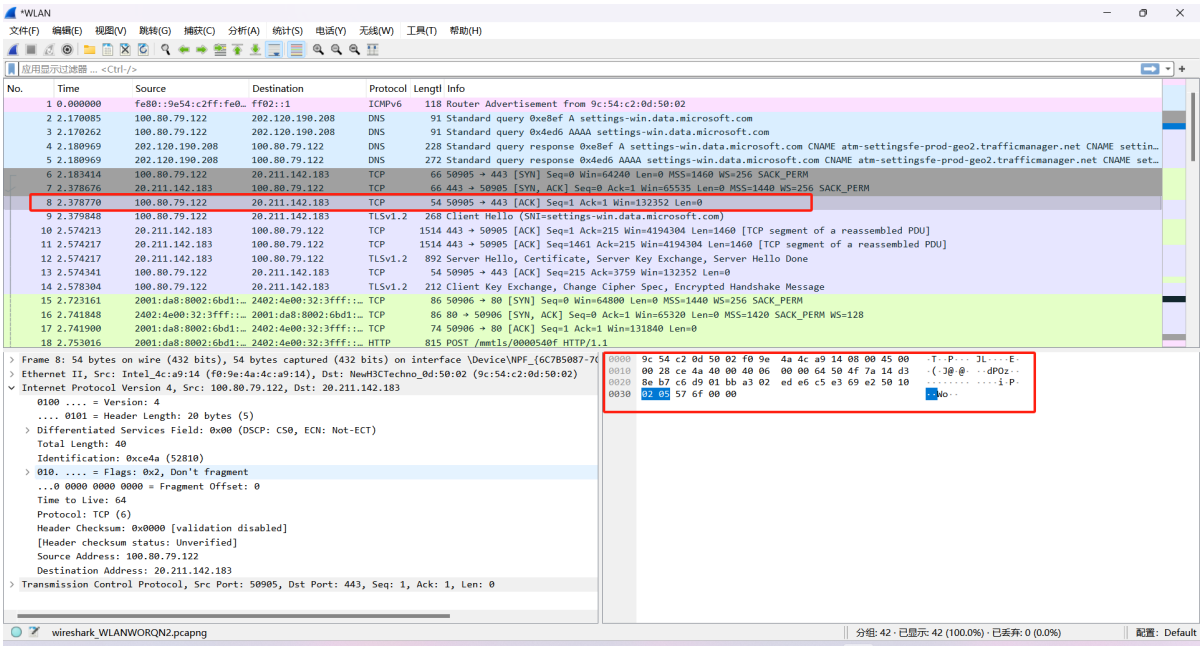
- 打开PC0浏览器，输入WEB服务器的IP地址，产生IP数据报文



- 查看报文

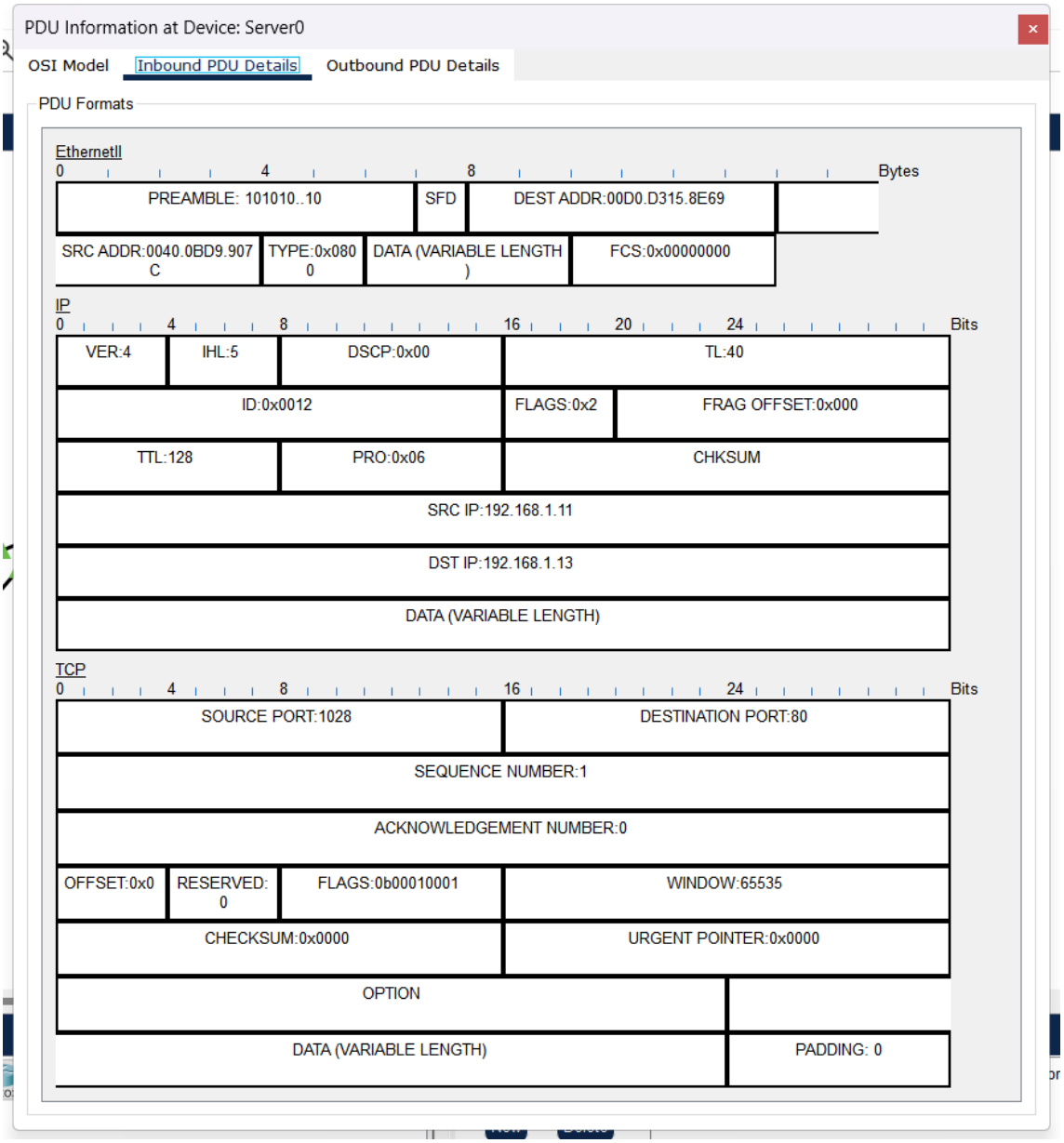


- 用WireShark抓取IP数据包并查看抓取的IP报文字段内容

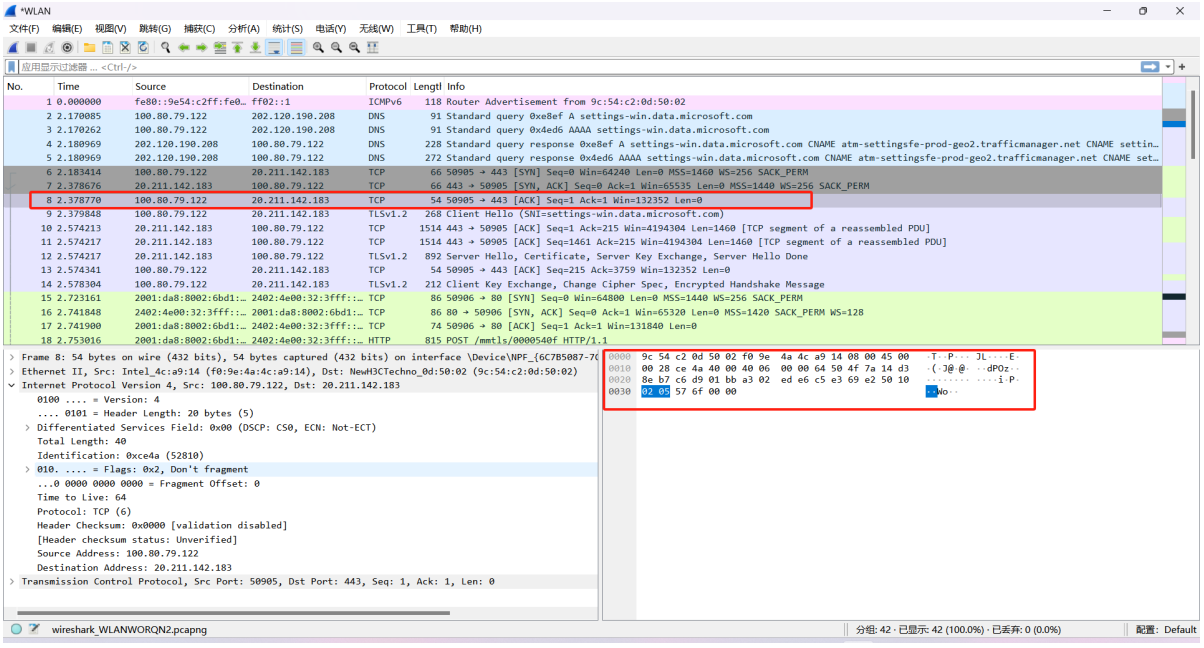


五、实验现象

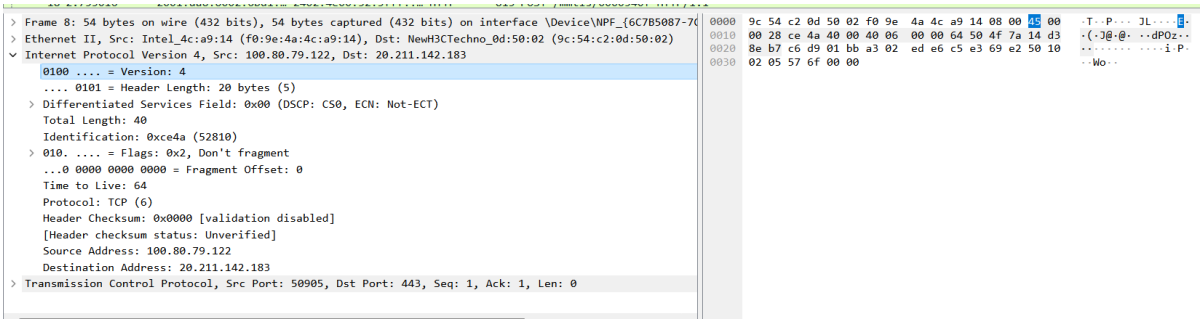
- 查看Packet Tracer中的IP报文可以获得以下信息（以下图中的报文为例）：



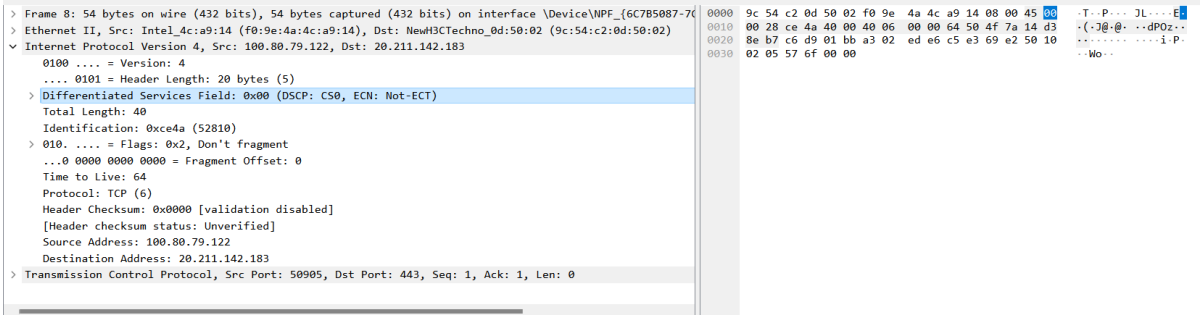
    - 版本：占4位，值为4，表示IPv4；
    - 首部长度：占4位，值为5，表示首部长度为4*5=20个字节；
    - 区分服务（服务类型）：占8位，未使用
    - 总长度：占16位，值为40，表示总长度40字节
    - 标识：占16位，值为12
    - 标志，占3位，值为2，即0x010，表示不允许分片
    - 片偏移：占13位，值为0
    - 生存时间：占8位，值为128，表示最多可经过128个路由器
    - 协议：占8位，值位0x06，表示TCP协议
    - 校验和：占16位，这里没有具体显示
    - 源地址：占4字节，为192.168.1.11
    - 目的地址：占4字节，为192.168.1.13
- 用WireShark抓取IP数据包，选择WLAN抓包



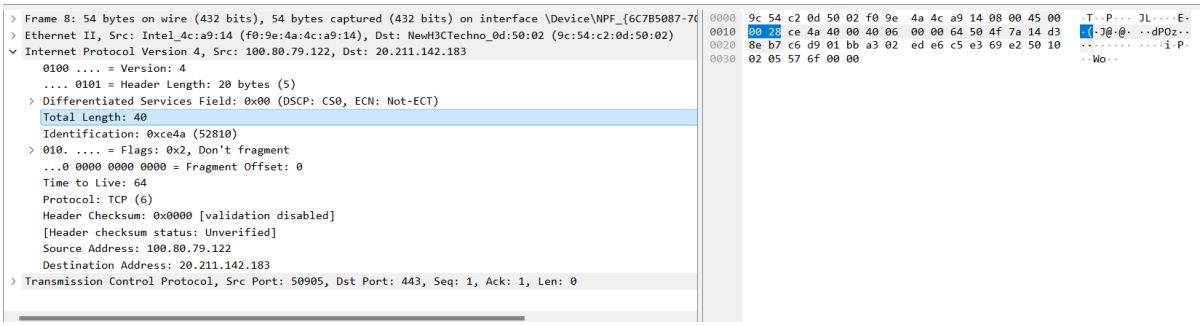
- 版本号为4，头长度为20字节（头长度为5个单位，一个单位表示四字节，共20字节）



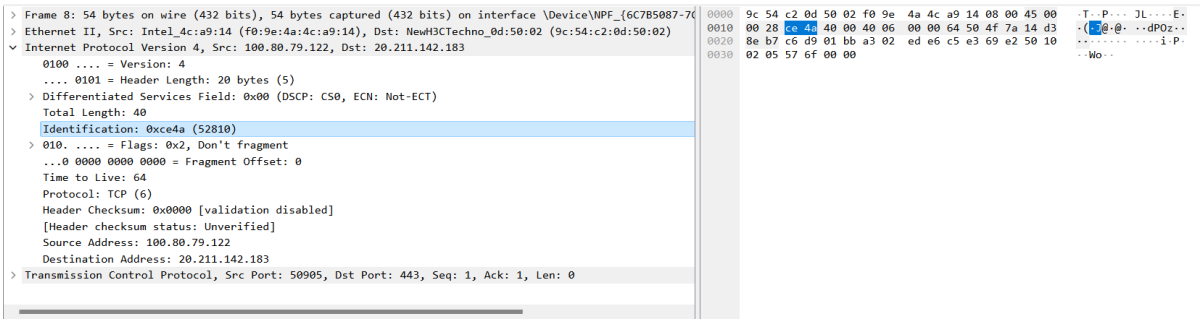
- 服务类型，该字段未被使用。



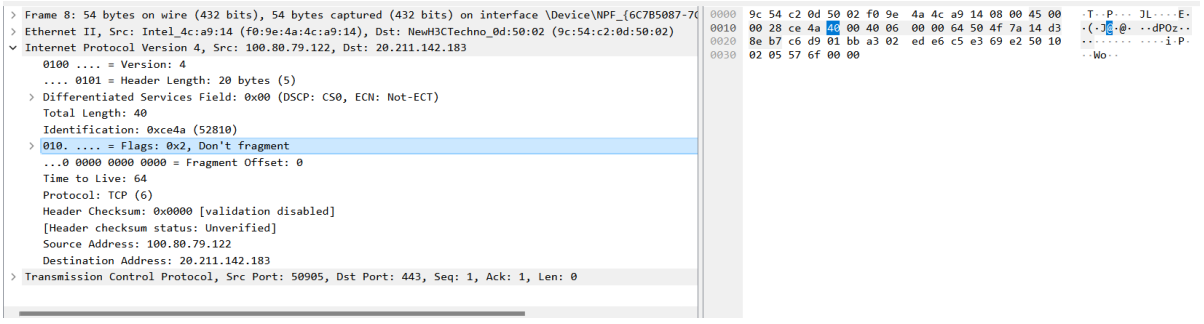
- 总长度：这里为0x28，即40个字节（首部和数据长度之和）



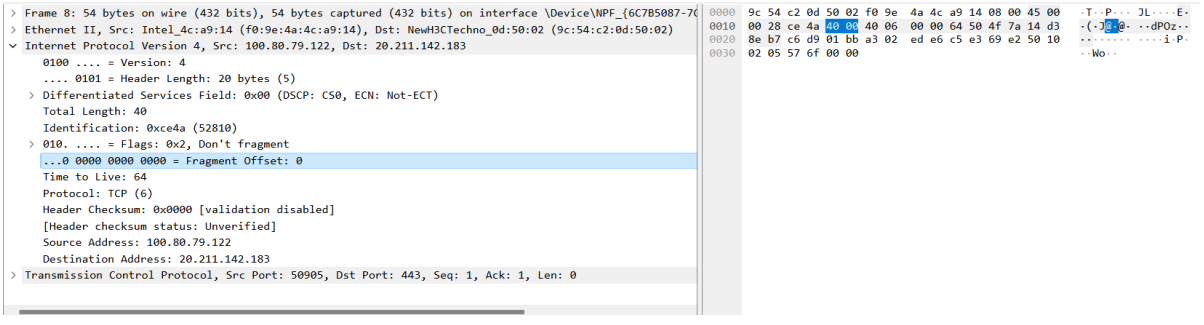
- 标识，这里为0xce4a，即52810



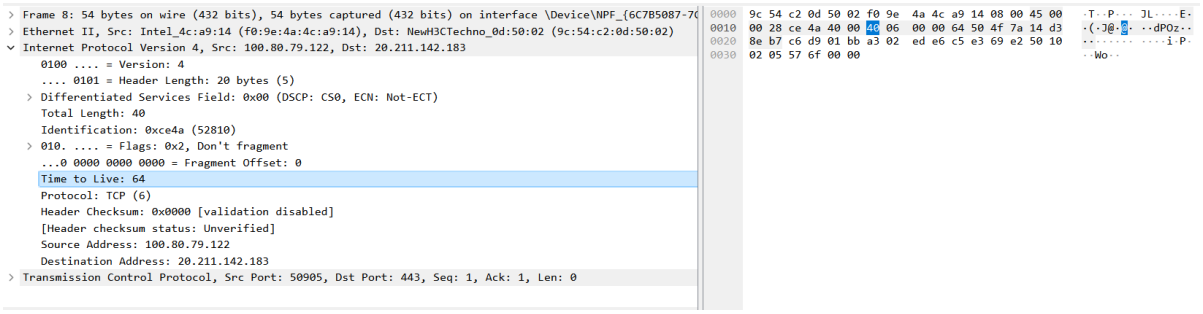
- 标志，3位，为0x010，表示不允许分片



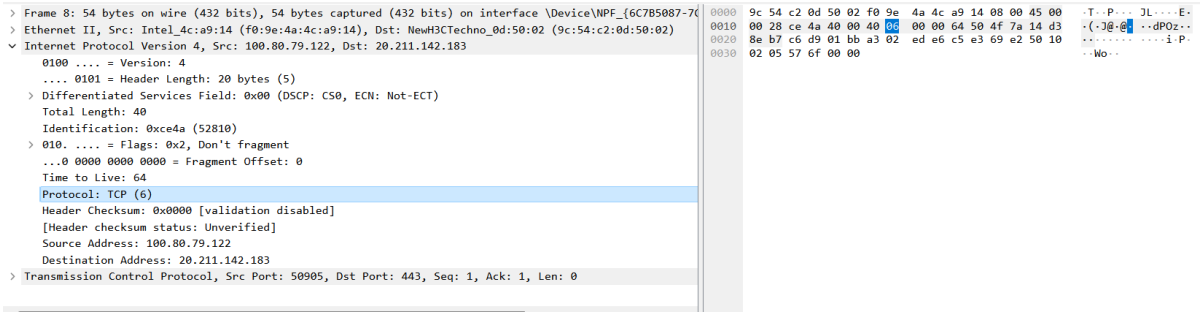
- 片偏移，13位，因为这里未分片，因此片偏移为0



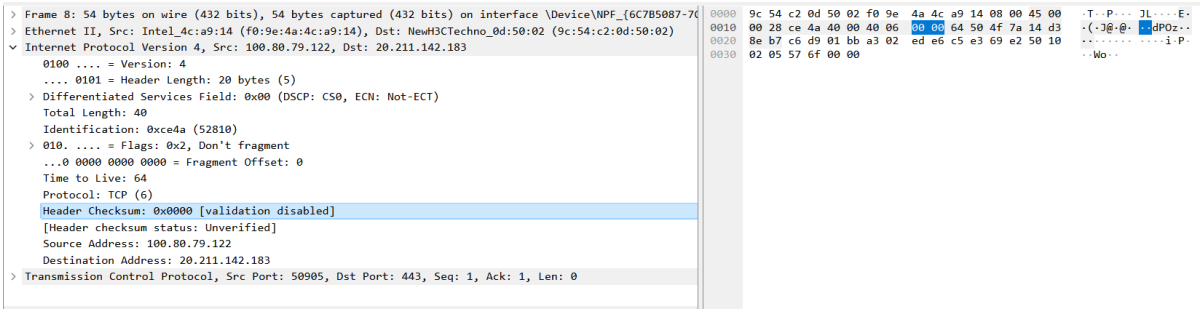
- 生存时间，表示数据报在网络中可通过的路由器数量，这里为0x40，即64.



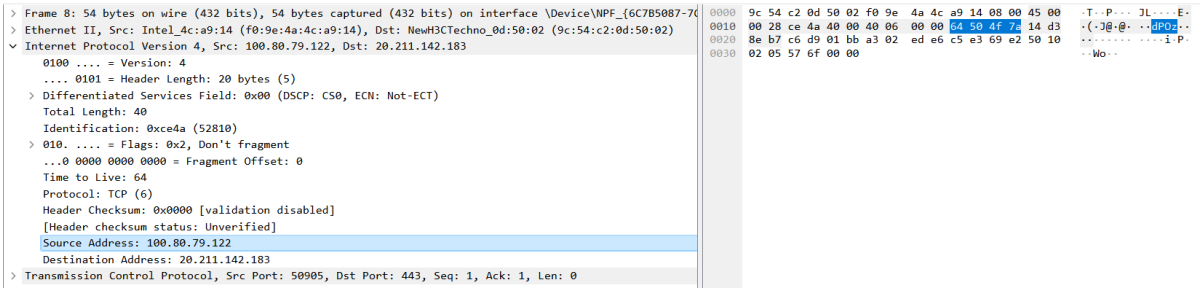
- 协议字段，根据不同值表示不同协议：ICMP（1）、IGMP（2）、IP（4）、TCP（6）、EGP（8）、IGP（9）、UDP（17）、IPv6（41）、ESP（50）、OSPF（89）。这里为0x06，表示TCP协议。



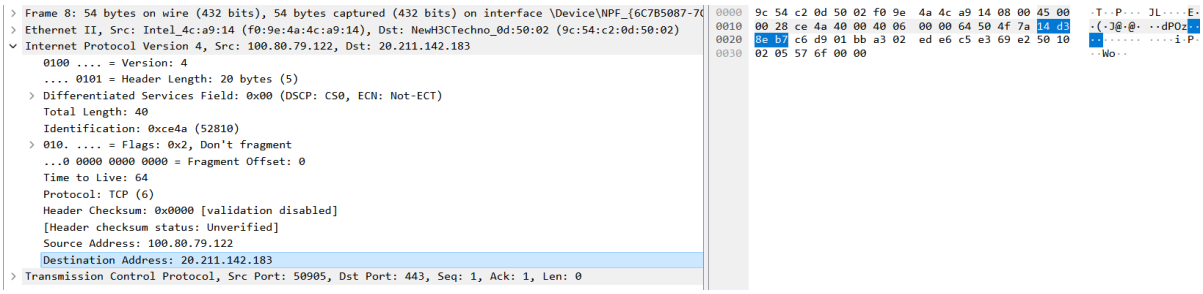
- 首部校验和，占16位，这里为0x0000，采用二进制反码求和算法



- 源地址IP，占16位，源地址为100.80.79.122



- 目的地址IP，占16位，目的地址为20.211.142.183



六、实验结论

- **结构理解**：通过详细学习和分析IP数据报的结构，包括首部和数据区的细节，我能够准确地描述IP数据报的组成。这有助于我更好地理解网络层是如何处理和转发数据的。
- **封装与拆封过程的重要性**：实验中，我学习到了封装和拆封过程对于数据在网络中传输的重要性。封装确保数据能够被正确地发送到网络上，而拆封则确保数据能够被正确地传递给接收端的应用程序。
- **分片和重组的实际应用**：通过操作和观察在不同MTU设置的网络环境中的数据传输，我理解了IP分片和重组的必要性及其在大型数据传输中的作用。这增强了我的实际问题解决能力。
- **首部字段的作用**：我学习了各个首部字段，如TTL、协议类型和首部检验和的功能，并通过实验观察了这些字段在实际网络操作中的重要性。这种知识对于网络监控和管理非常重要。
- **网络工具的应用**：使用Wireshark等网络分析工具，我能够实时捕捉和分析IP数据包。这不仅帮助我理解数据包的行为，也让我体会到了网络条件对数据传输的影响。
- **选项字段的高级功能**：我还探索了IP首部的选项字段，如源路由和时间戳等，这些选项对于网络测试、安全和性能优化具有重要意义。

通过这个实验，我不仅巩固了对IP协议的理解，还提升了我的实际操作能力和问题解决技巧，这将对我的未来学习和职业生涯产生积极影响。