**【实验名称】：**IP数据包分析实验

**学生姓名：2151133**孙韩雅

**实验地点：**济事楼330 **实验时间：**2023-11-27

**【实验目的】**

了解IP协议的原理，分析IP报文。

**【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。

格式总览 ：一个IP数据报由首部和数据两部分组成。



2.头部

头部的前一部分是固定长度，共20字节，是所有IP数据报必须具有的。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。



3.IP数据报首部的固定部分中的各字段

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)。

IP数据报首部的固定部分中的各字段首部长度——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，指出：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。

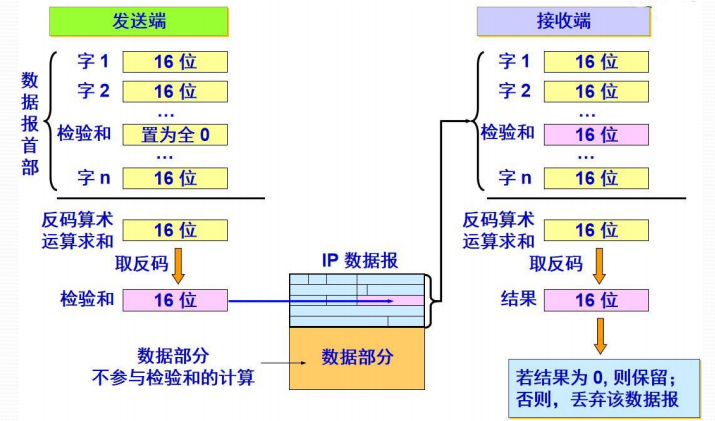
首部检验和——占16位，只检验数据报的首部，不检验数据部分。这里不采用CRC检验码而采用简单的计算方法。IP 数据报首部检验和的计算采用16位二进制反码求和算法。

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。

4.IP数据报首部校验

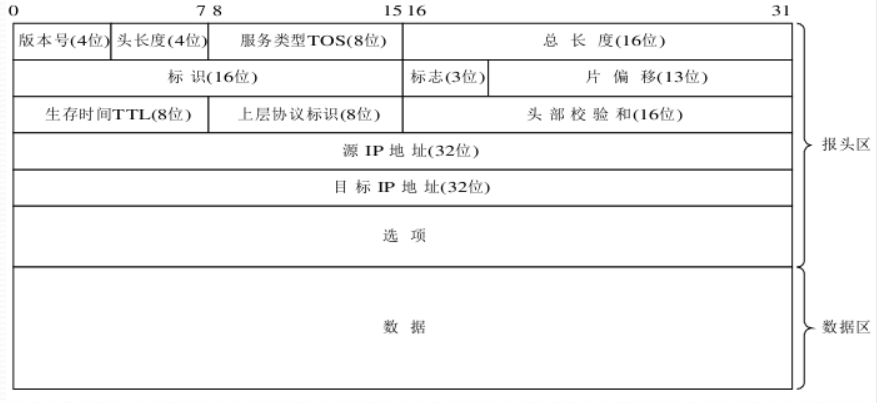
IP数据报首部检验和的计算采用16位二进制反码求和算法。



5.IP数据报分段

给出数据报的总长度为 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。

6.IP数据报文格式传输

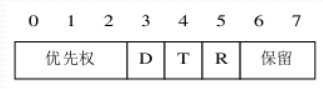
****

7.IP数据报文上层协议

****

8.IP数据报文的TOS

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。

9.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）。

10.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。

11.接收组包

重组：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；

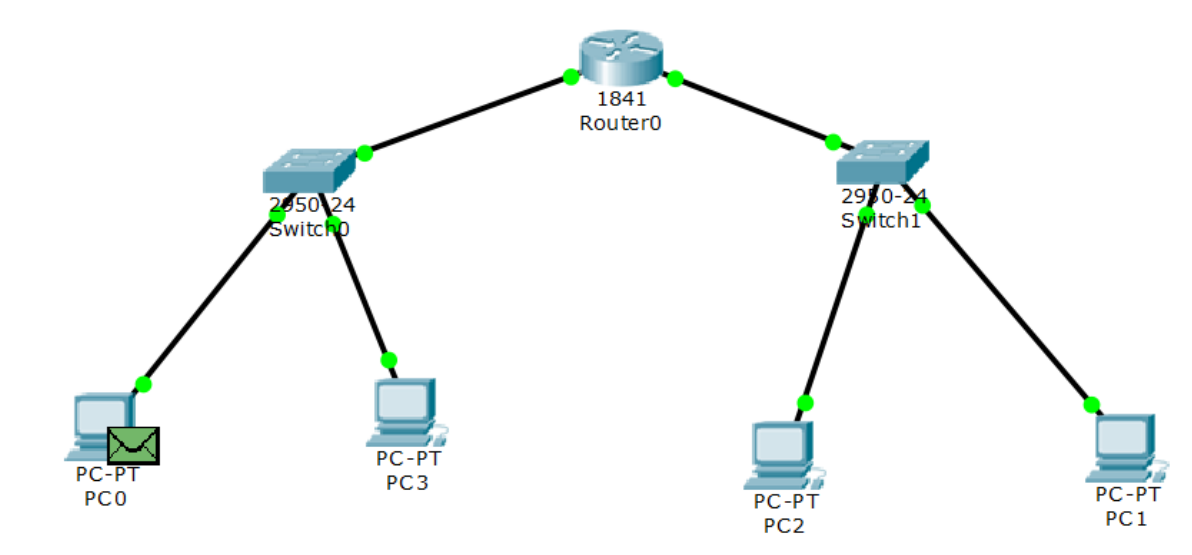
(3)—根据“偏移量”字段可以确定分片在原数据报中的位置。

**【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.规划网络地址连接线路：



2.配置动态DHCP。

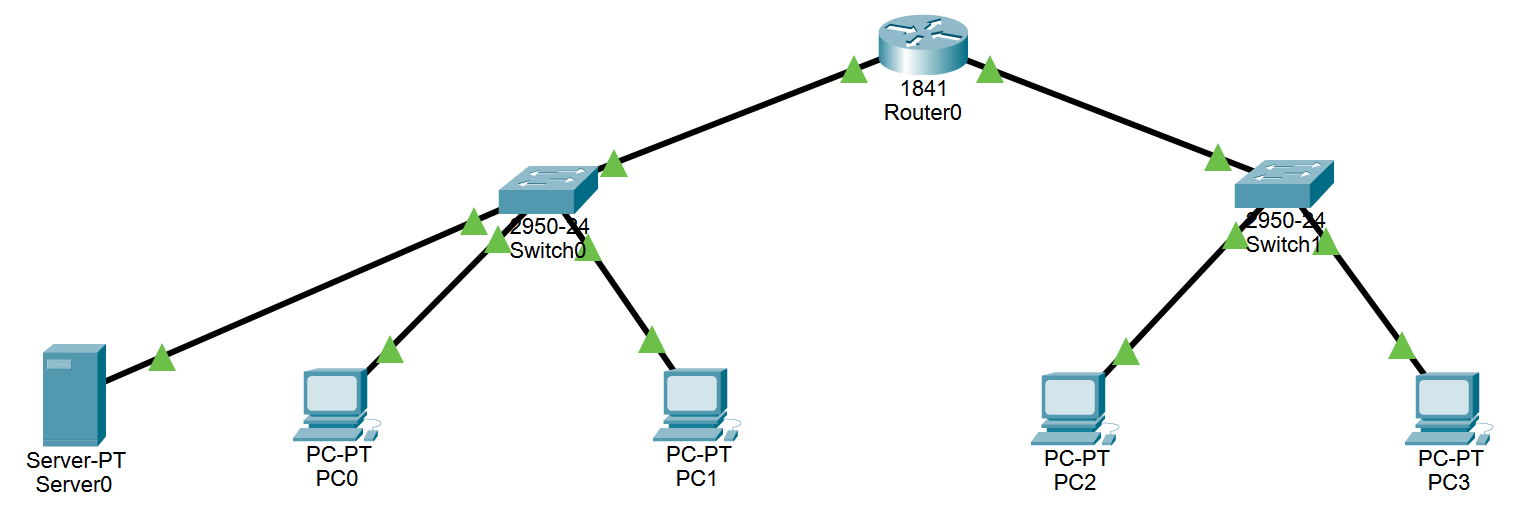
3.打开浏览器输入配置WEB服务器的IP地址，产生IP数据报文。

4.用WireShark抓取IP数据包。

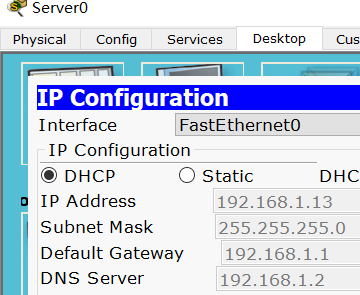
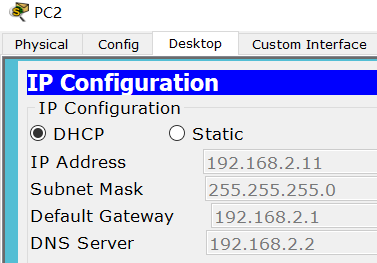
5.分析IP报文情况。

**【实验现象】**

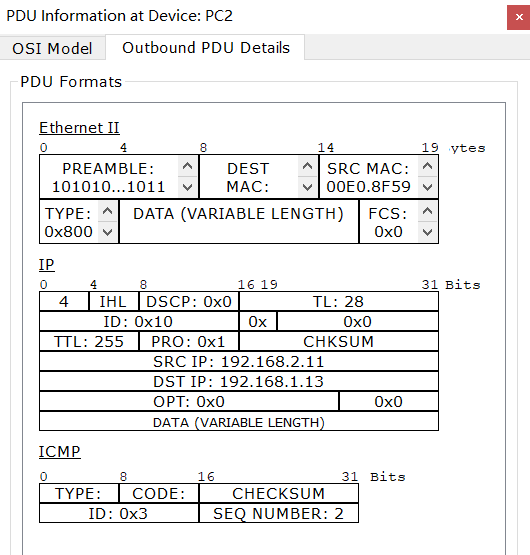
1.按照拓扑图进行连线，加上一个web服务器：



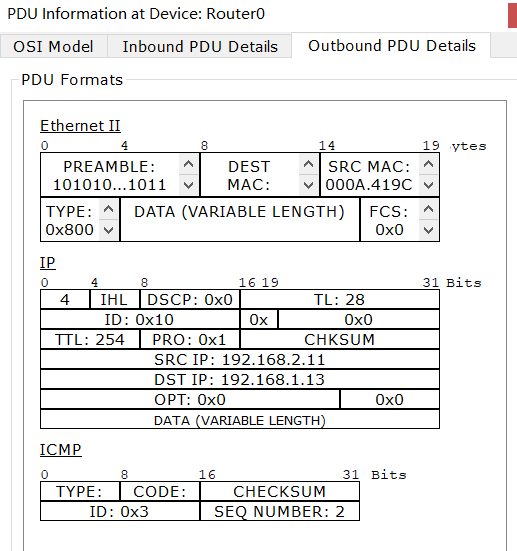
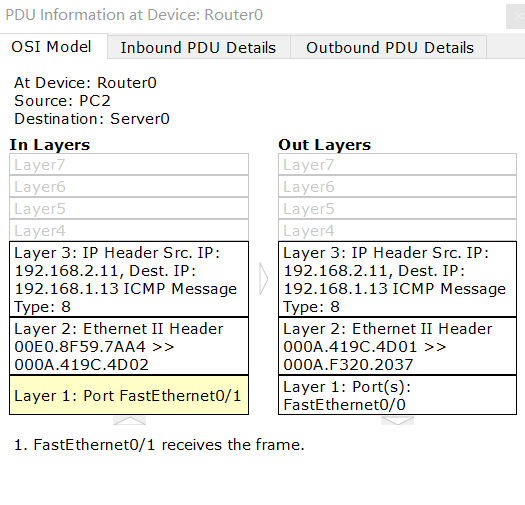
2.配置动态DHCP：

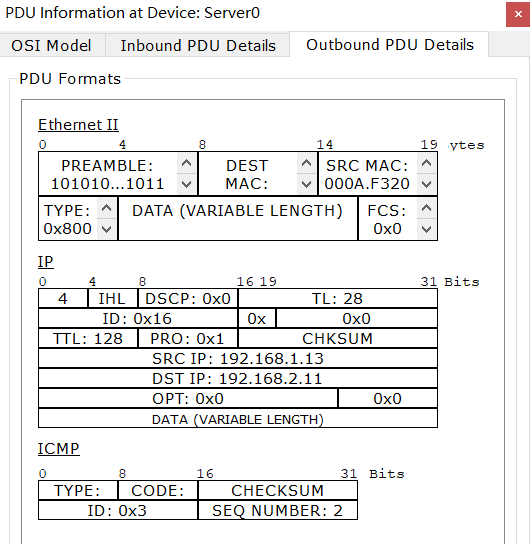
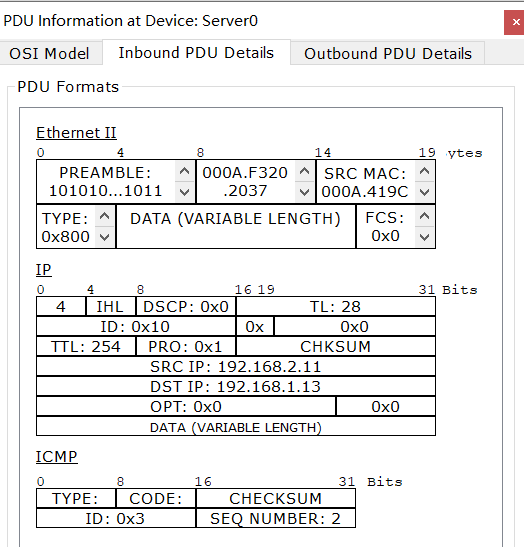
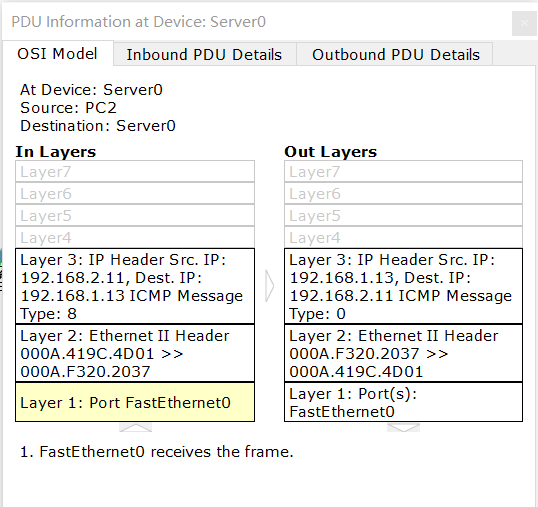
****

3.打开PC2浏览器输入WEB地址，查看IP报文：

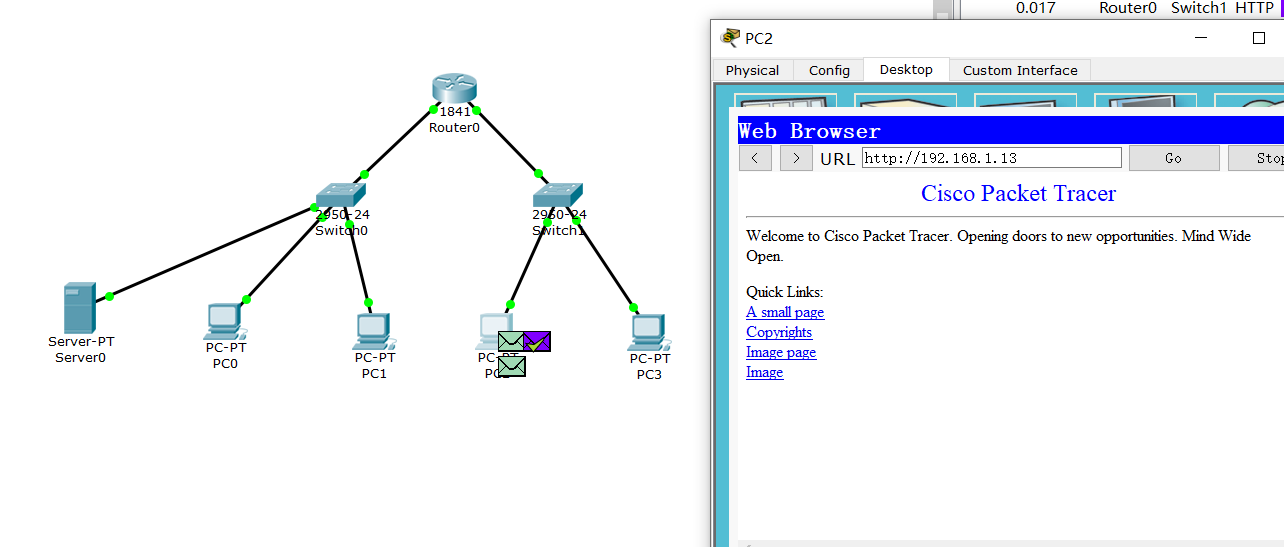


4.查看路由器与服务端报文：

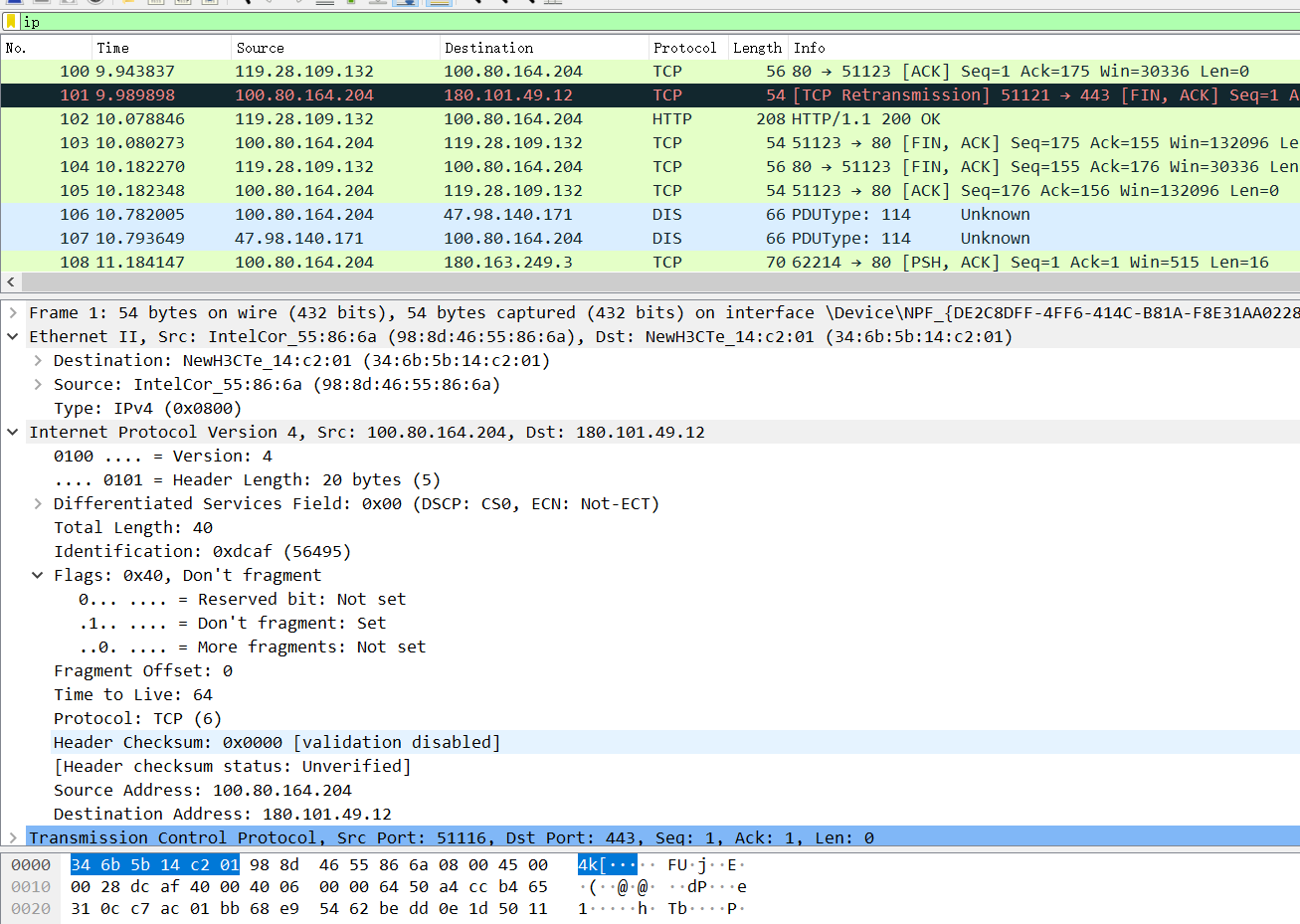




5.PC2收到响应报文，表示连接网页成功：



6.利用WireShark IP进行报文抓取



由内容可知，IP协议版本为4，报文头为20个字节，总长度为40个字节；标识符值为56495，标志字段为010，该报文为不分片，片偏移字段为0，表示是第一个报文；TTL值为64，表示该报文还可以在网络中传输64跳；协议字段为TCP，表示接收端收到该报文后，会上送给传输层TCP协议处理；校验和字段为correct，表示该报文无差错；数据包从源IP地址100.80.164.204发送给目的IP地址180.101.49.12。

**【分析讨论】**

在这次实验中，我学习了如何使用Wireshark抓包并进行IP数据分析。通过这次实验，我深刻理解了网络通信的基本原理，并掌握了如何通过抓包分析网络传输过程中的IP数据包，了解网络通信中的细节和异常。

另外我还学会了如何根据协议类型、源IP和目标IP等关键字过滤IP数据包，以便更方便地查找和分析数据包。