**实验五 传输层协议（UDP/TCP）**

**实验目的**

1. 掌握UDP协议的报文格式

2. 掌握UDP协议校验和的计算方法

3. 理解UDP协议的优缺点

4. 理解协议栈对UDP协议的处理方法

5. 理解UDP上层接口应满足的条件

6. 掌握TCP协议的报文格式

7. 掌握TCP连接的建立和释放过程

8. 掌握TCP数据传输中编号与确认的过程

**实验步骤**

**练习1：编辑并发送UDP数据报**

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。本练习将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

1. 主机A打开协议编辑器，编辑发送给主机B的UDP数据报。

MAC层：

目的MAC地址：接收方MAC地址

源MAC地址：发送方MAC地址

协议类型或数据长度：0800，即IP协议

IP层：

总长度：包括IP层、UDP层和数据长度

高层协议类型：17，即UDP协议

首部校验和：其它所有字段填充完毕后填充此字段

源IP地址：发送方IP地址

目的IP地址：接收方IP地址

UDP层：

源端口：1030

目的端口：大于1024的端口号

有效负载长度：UDP层及其上层协议长度

其它字段默认，计算校验和。

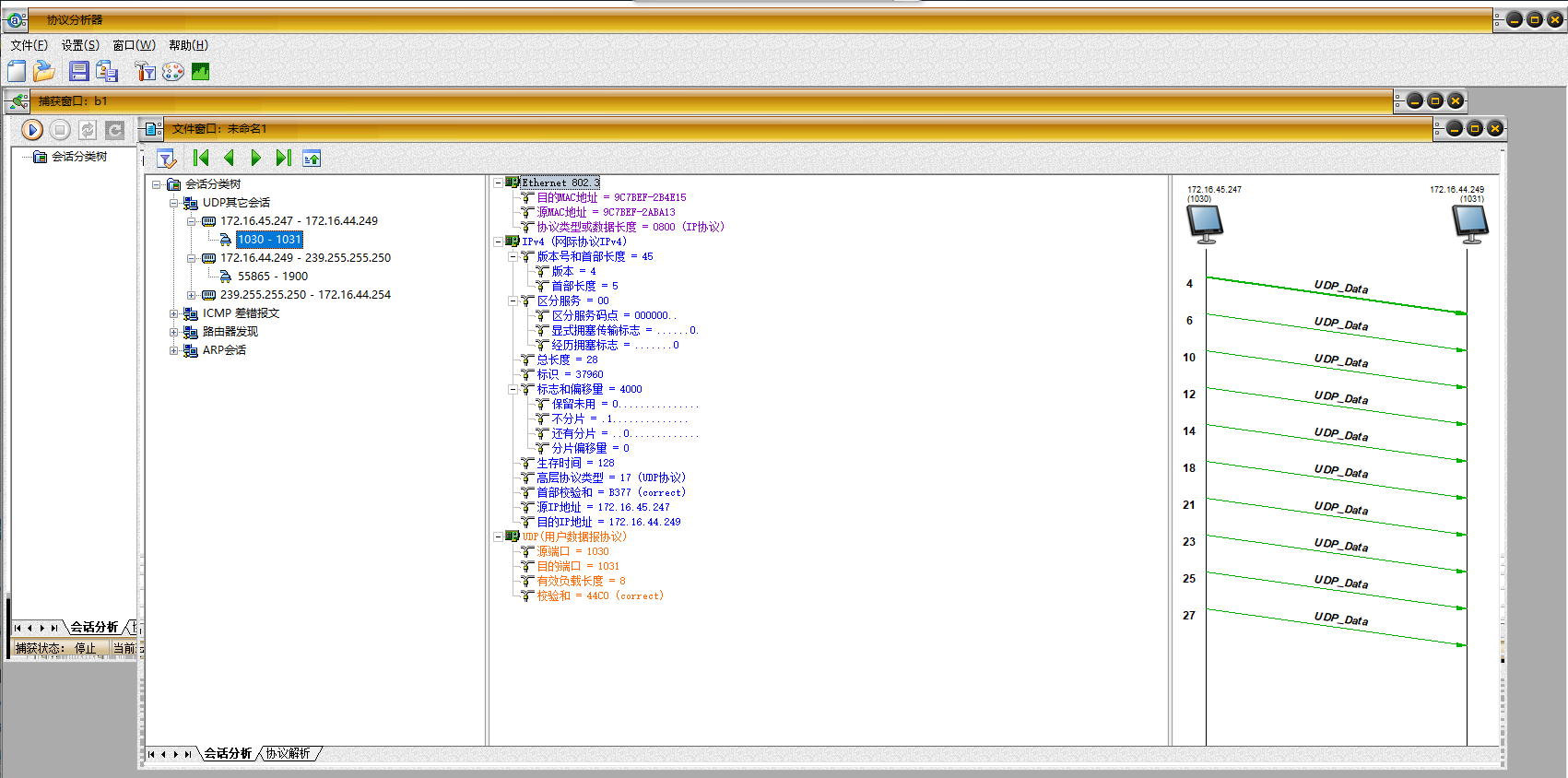
● UDP在计算校验和时包括哪些内容？

伪首部，UDP首部和UDP数据(从应用层来的数据)。

2. 在主机B上启动协议分析器捕获数据，并设置过滤条件（提取UDP协议）。

3. 主机A发送已编辑好的数据报。

4. 主机B停止捕获数据，在捕获到的数据中查找主机A所发送的数据报。



Ethernet 802.3

目的MAC地址 = 9C7BEF-2B4E15

源MAC地址 = 9C7BEF-2ABA13

协议类型或数据长度 = 0800 (IP协议)

IPv4 (网际协议IPv4)

版本号和首部长度 = 45

版本 = 4

首部长度 = 5

区分服务 = 00

区分服务码点 = 000000..

显式拥塞传输标志 = ......0.

经历拥塞标志 = .......0

总长度 = 28

标识 = 37960

标志和偏移量 = 4000

保留未用 = 0...............

不分片 = .1..............

还有分片 = ..0.............

分片偏移量 = 0

生存时间 = 128

高层协议类型 = 17 (UDP协议)

首部校验和 = B377 (correct)

源IP地址 = 172.16.45.247

目的IP地址 = 172.16.44.249

UDP(用户数据报协议)

源端口 = 1030

目的端口 = 1031

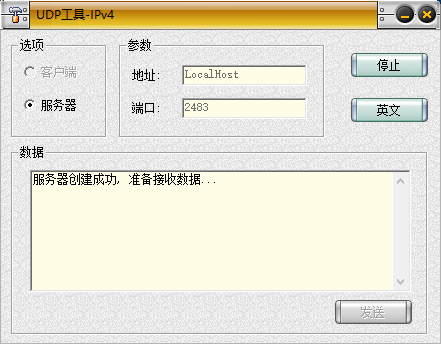
有效负载长度 = 8

校验和 = 44C0 (correct)

**练习2：UDP单播通信**

本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 主机B、C、D、E、F上启动“实验平台工具栏中的UDP工具”，作为服务器端，监听端口设置为2483，“创建”成功。



2. 主机C、E上启动协议分析器开始捕获数据，并设置过滤条件（提取UDP协议）。

3. 主机A上启动“实验平台工具栏中的UDP工具”，作为客户端，以主机C的IP为目的IP地址，以2483为端口，填写数据并发送。

4. 查看主机B、C、D、E、F上的“UDP工具”接收的信息。

● 哪台主机上的“UDP工具”能够接收到主机A发送的UDP报文？

主机C能够收到。

5. 查看主机C协议分析器上的UDP报文，并回答以下问题：

● UDP是基于连接的协议吗？阐述此特性的优缺点。

不是。优点：相对于面向连接的服务，UDP传送数据较快速，系统开销也少。缺点：但它不能防止报文的丢失、重复和乱序。由于它的每个报文必须包括完整的源地址的目的地址因此开销很大；每个请求必须足够小，使其能够装入到用户数据报中。

● UDP报文交互中含有确认报文吗？阐述此特性的优缺点。

无。优点是可以提高传输效率；缺点是在传输过程中可能有丢失、重复、乱序的现象。

6. 主机A上使用协议编辑器向主机E发送UDP报文，其中：

目的MAC地址：E的MAC地址

目的IP地址：主机E的IP地址

目的端口：2483

校验和：0

发送此报文，并回答以下问题：

● 主机E上的UDP通信程序是否接收到此数据包？UDP是否可以使用0作为校验和进行通信？

主机E上的UDP通信程序能接收到此数据包；

UDP可以使用0作为校验和进行通信。

1. 主机B、C、D、E、F关闭服务端，主机A关闭客户端。

**练习3：UDP广播通信**

本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 主机B、C、D、E、F上启动“实验平台工具栏中的UDP工具”，作为服务器端，监听端口设为2483。

2. 主机B、C、D、E、F启动协议分析器捕获数据，并设置过滤条件（提取UDP协议）。

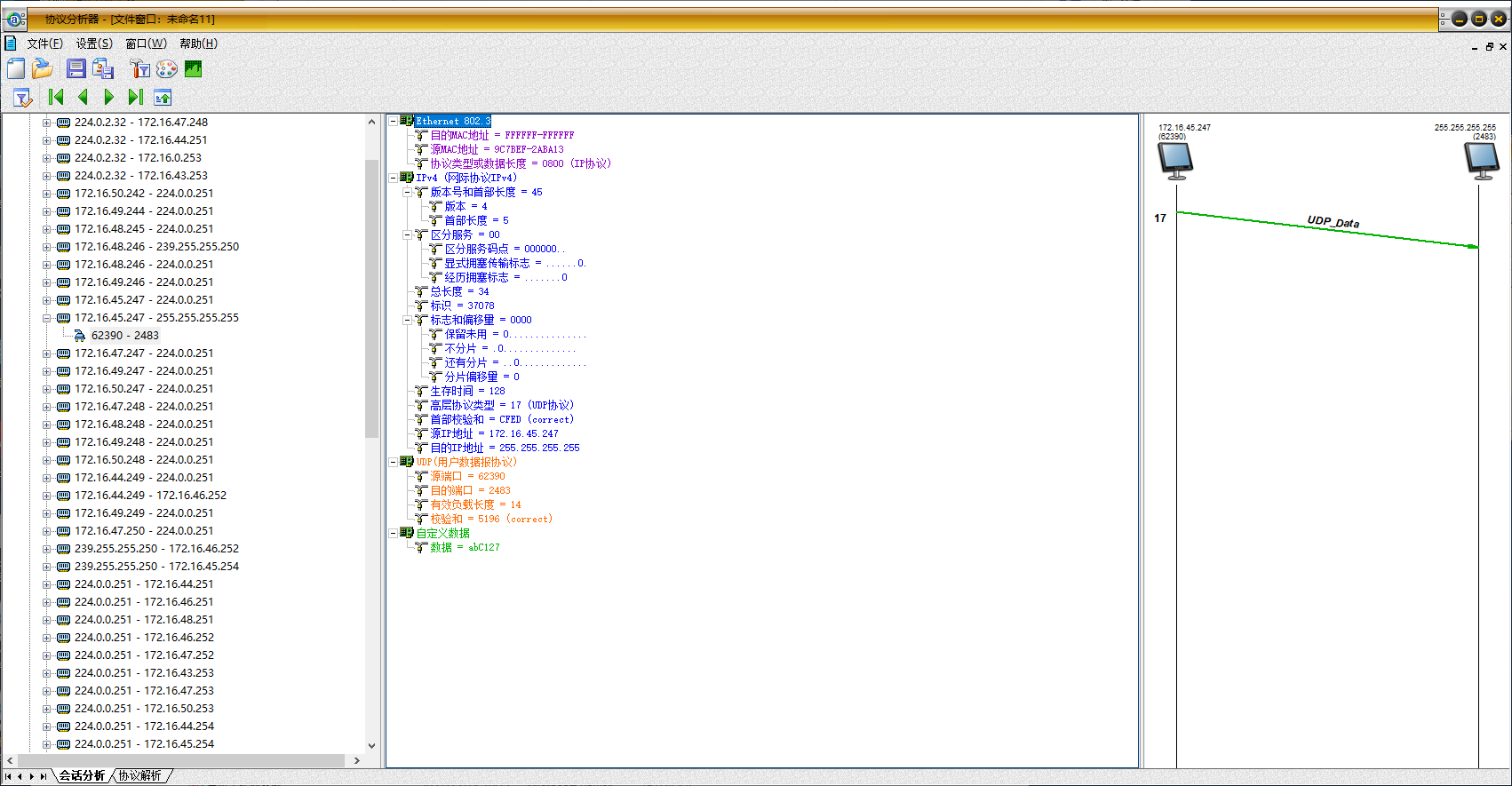
3. 主机A上启动“实验平台工具栏中的UDP工具”，作为客户端，以255.255.255.255为目的地址，以2483为端口，填写数据并发送。

4. 查看主机B、C、D、E、F上的“UDP工具”接收的信息。

● 哪台主机能够接收到主机A发送的UDP报文？

主机B、C、D、E、F都可以收到

5. 查看协议分析器上捕获的UDP报文，并回答以下问题：



Ethernet 802.3

目的MAC地址 = FFFFFF-FFFFFF

源MAC地址 = 9C7BEF-2ABA13

协议类型或数据长度 = 0800 (IP协议)

IPv4 (网际协议IPv4)

版本号和首部长度 = 45

版本 = 4

首部长度 = 5

区分服务 = 00

区分服务码点 = 000000..

显式拥塞传输标志 = ......0.

经历拥塞标志 = .......0

总长度 = 34

标识 = 37078

标志和偏移量 = 0000

保留未用 = 0...............

不分片 = .0..............

还有分片 = ..0.............

分片偏移量 = 0

生存时间 = 128

高层协议类型 = 17 (UDP协议)

首部校验和 = CFED (correct)

源IP地址 = 172.16.45.247

目的IP地址 = 255.255.255.255

UDP(用户数据报协议)

源端口 = 62390

目的端口 = 2483

有效负载长度 = 14

校验和 = 5196 (correct)

自定义数据

数据 = abC127

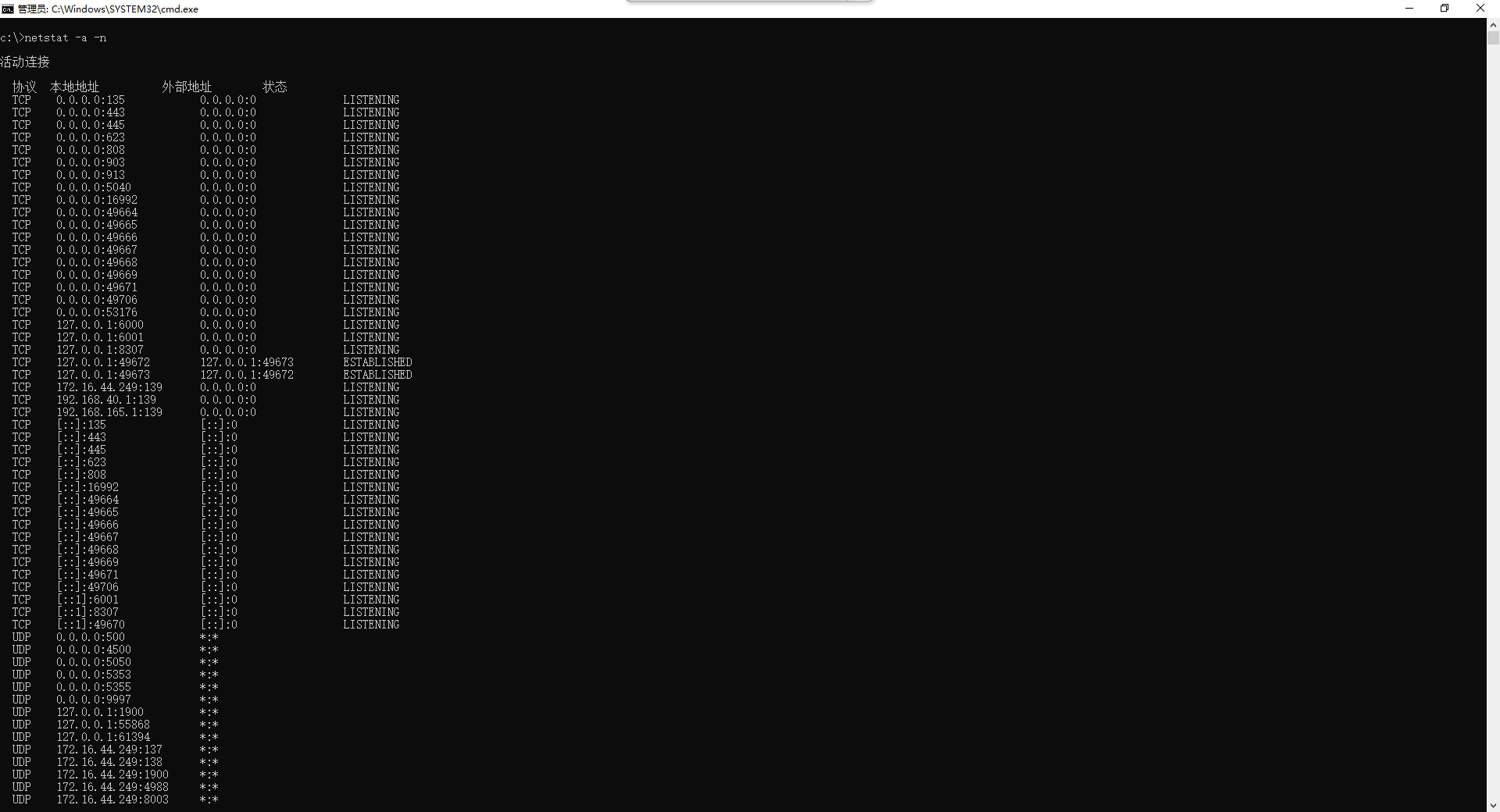
● 主机A发送的报文的目的MAC地址和目的IP地址的含义是什么？

MAC地址是广播的物理地址，IP地址是广播的IP地址，这样广播到网络上的每个主机。

**练习4：查看TCP连接的建立和释放**

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。  
     本练习将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B为例，其它组的操作参考主机A、B的操作。

1. 主机B启动协议分析器捕获数据，并设置过滤条件（提取TCP协议）。  
        主机B在命令行下输入：netstat -a -n命令来查看主机B的TCP端口号。



1. 主机A启动TCP工具连接主机B。  
        主机A启动实验平台工具栏中的“TCP工具”。选中“客户端”单选框，在“地址”文本框中填入主机B的IP地址，在“端口”文本框中填入主机B的一个TCP端口，点击[连接]按钮进行连接。
2. 察看主机B捕获的数据，填写下表。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 报文1 | 报文2 | 报文3 |
| 序列号 | 2804218146 | 3784105999 | 2804218147 |
| 确认号 | 0 | 2804218147 | 3784106000 |
| ACK | …0…. | …1…. | …1…. |
| SYN | ……1. | ……1. | ……0. |

● TCP连接建立时，前两个报文的首部都有一个“最大段长度”字段，它的值是多少？作用是什么？结合IEEE802.3协议规定的以太网最大帧长度分析此数据是怎样得出的。

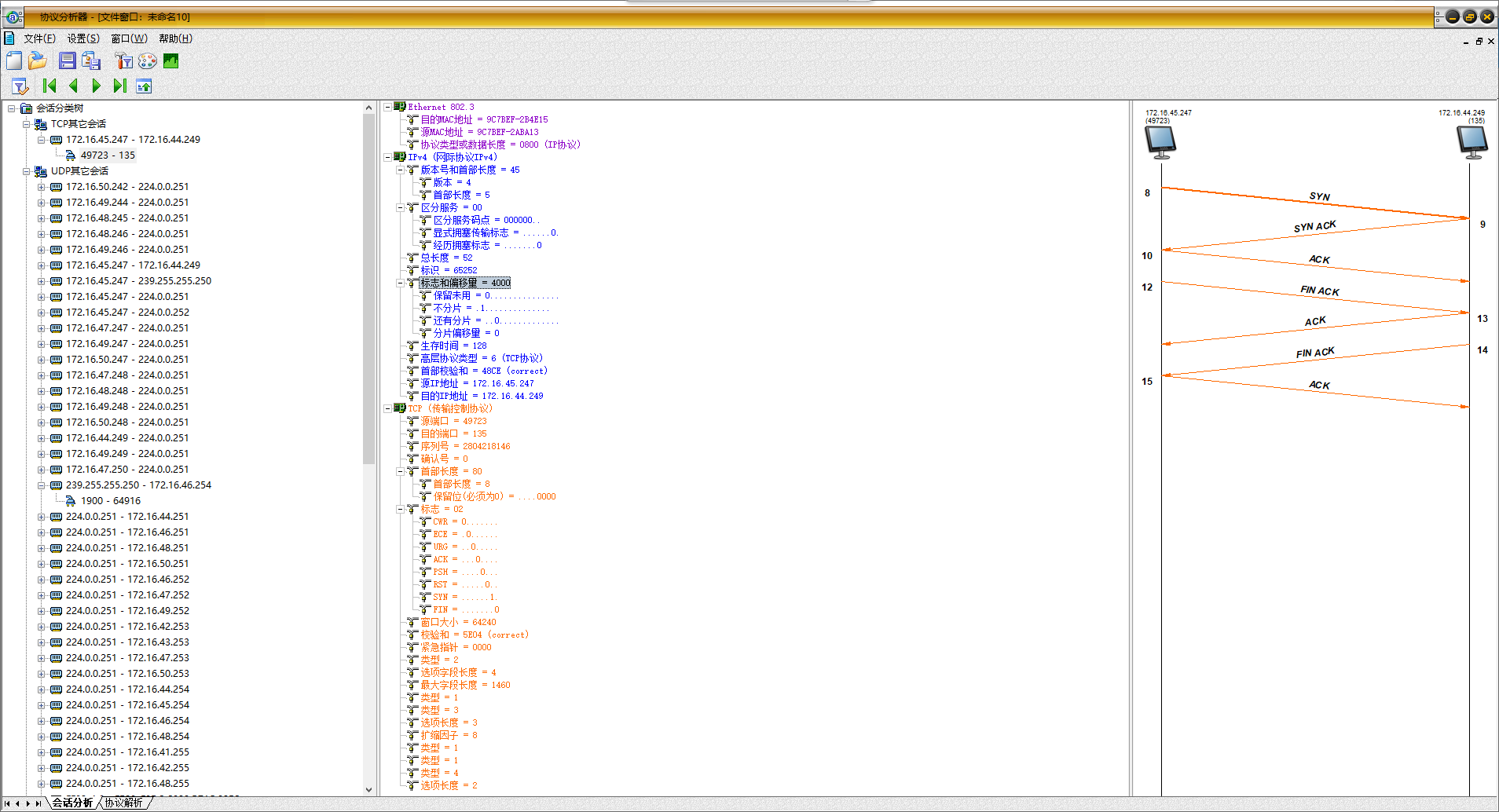
1460；由发送端指定，表明了能在网络上传输的最大的段尺寸

maximum segment size=MTU 20（首部）-20（TCP 首部）

4. 主机A断开与主机B的TCP连接。

5. 查看主机B捕获的数据，填写下表。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 报文4 | 报文5 | 报文6 | 报文7 |
| 序列号 | 2804218147 | 3784106000 | 3784106000 | 2804218148 |
| 确认号 | 3784106000 | 2804218148 | 2804218148 | 3784106001 |
| ACK | …1…. | …1…. | …1…. | …1…. |
| FIN | …….1 | …….0 | …….1 | …….0 |



● 结合步骤3、5所填的表，理解TCP的三次握手建立连接和四次握手的释放连接过程，理解序号、确认号等字段在TCP可靠连接中所起的作用。

**三次握手过程说明：**

TCP服务器进程先创建传输控制块TCB（存储了每一个连接中的一些重要信息，如：TCP连接表，到发送和接收缓存的指针，到重传队列的指针，当前的发送和接收序号等），准备接受客户进程的连接请求。然后服务器进程就处于LISTEN（收听）状态，等待客户的连接请求。如有，即作出相应。

**第一次握手：**客户端Client向服务端Server发起建立连接请求。客户端会发送位码SYN（请求建立连接），以及序列号x（seq=x），TCP规定，SYN报文段（即SYN=1的报文段）不能携带数据，但要消耗掉一个序号。这时，TCP客户进程进入SYN-SENT（同步已发送）状态。

**第二次握手：**服务端Server接受到请求报文段之后。如同意建立连接，则向客户端发送确认消息。在确认报文段中应把SYN位和ACK位都置1，确认号是ack=x+1，同时也为自己选择一个初始序号seq=y。注意。这个报文段也不能携带数据，但同样要消耗掉一个序号。这时服务端进程进入SYN-RCVD（同步收到）状态。

**第三次握手：**客户端Client收到服务端Server的确认后，还要向服务端给出确认。确认报文段的ACK置1，确认号ack=y+1，而自己的序号seq=x+1。这时，TCP连接已经建立，客户端进入ESTABLISHED（已连接状态）。当服务端收到客户端的确认之后，也进入ESTABLISHED状态。

**四次挥手过程说明：**

在客户端和服务端已经建立连接的情况下，需要四次挥手来断开连接。

**第一次挥手：**客户端发送一个FIN=1的报文段和顺序号为u（seq=u）的请求关闭消息（客户端没有消息要发给你了，我准备关闭连接了，但是如果你还有数据没有发送完成，则不必急着关闭Socket，可以继续发送数据。所以你先发送ACK）。客户端进入FIN-WAIT-1状态，等待服务端的FIN报文段。

**第二次挥手：**服务端收到客户端的FIN报文段，会发送一个确认报文段ACK=1，以及确认序列号ack=u+1，还有自己的序列号seq=v（告诉客户端，我已经收到你的请求关闭消息，但是我还没准备好，请继续等待），服务单进入CLOSE-WAIT阶段，此时服务端还未关闭。

**第三次挥手：**服务端向客户端发送FIN=1报文段（告诉Client端，好了，我这边数据发完了，准备好关闭连接了），ACK=1,序列号seq=w，ack=u+1，服务端进入LAST-ACK状态

**第四次挥手：**客户端收到服务端发来的FIN=1报文段，给服务端发送ACK=1报文段，序列号seq=u+1，ack=w+1的消息。这时客户端就可以关闭连接了，但是他还是不相信网络，怕Server端不知道要关闭，所以发送ACK后进入TIME\_WAIT状态，如果Server端没有收到ACK则可以重传 ，客户端等待了2MSL后依然没有收到回复，客户端关闭。服务端也关闭。