**实验三 网际协议（IP）**

**实验目的**

1. 掌握IP数据报的报文格式

2. 掌握IP校验和计算方法

3. 掌握子网掩码和路由转发

4. 理解特殊IP地址的含义

5. 理解IP分片过程

6. 理解协议栈对IP协议的处理方法

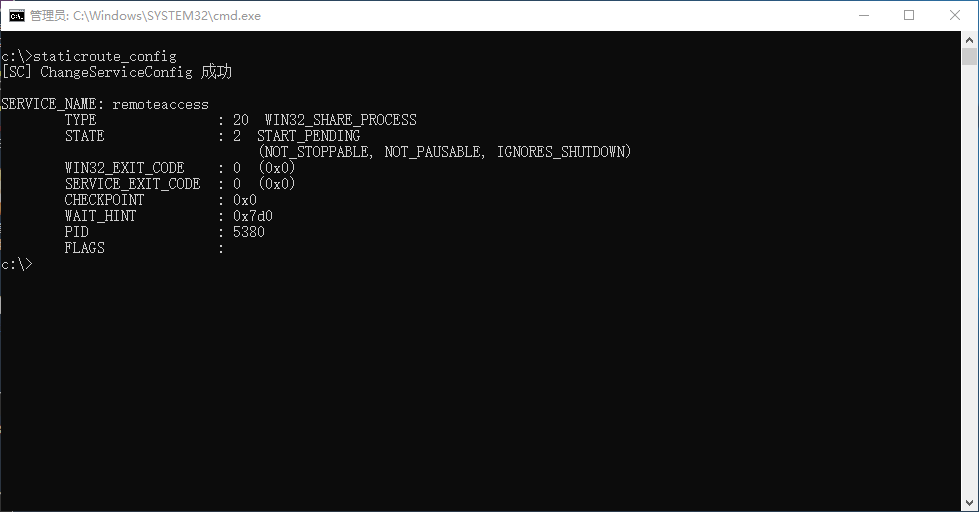
7. 理解IP路由表作用以及IP路由表的管理

**实验步骤：**

**练习1：编辑并发送IP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、B、C、D、E、F作为一组进行实验。

1. 主机B在命令行方式下输入staticroute\_config命令，开启静态路由服务。



2. 主机A启动协议编辑器，编辑一个IP数据报，其中：

MAC层：

目的MAC地址：主机B的MAC地址（对应于172.16.1.1接口的MAC）。

源MAC地址：主机A的MAC地址。

协议类型或数据长度：0800。

IP层：

总长度：IP层长度。

生存时间：128。

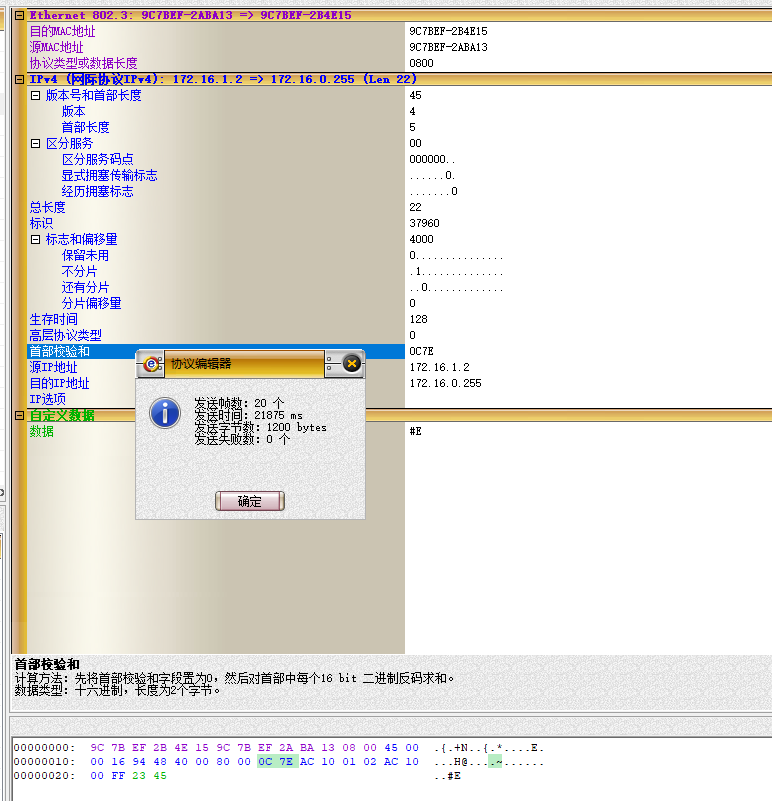
源IP地址：主机A的IP地址（172.16.1.2）。

目的IP地址：主机E的IP地址（172.16.0.2）。

校验和：在其它所有字段填充完毕后计算并填充。

自定义字段：

数据：填入大于1字节的用户数据。



【说明】先使用协议编辑器的“手动计算”校验和，再使用协议编辑器的“自动计算”校验和，将两次计算结果相比较，若结果不一致，则重新计算。

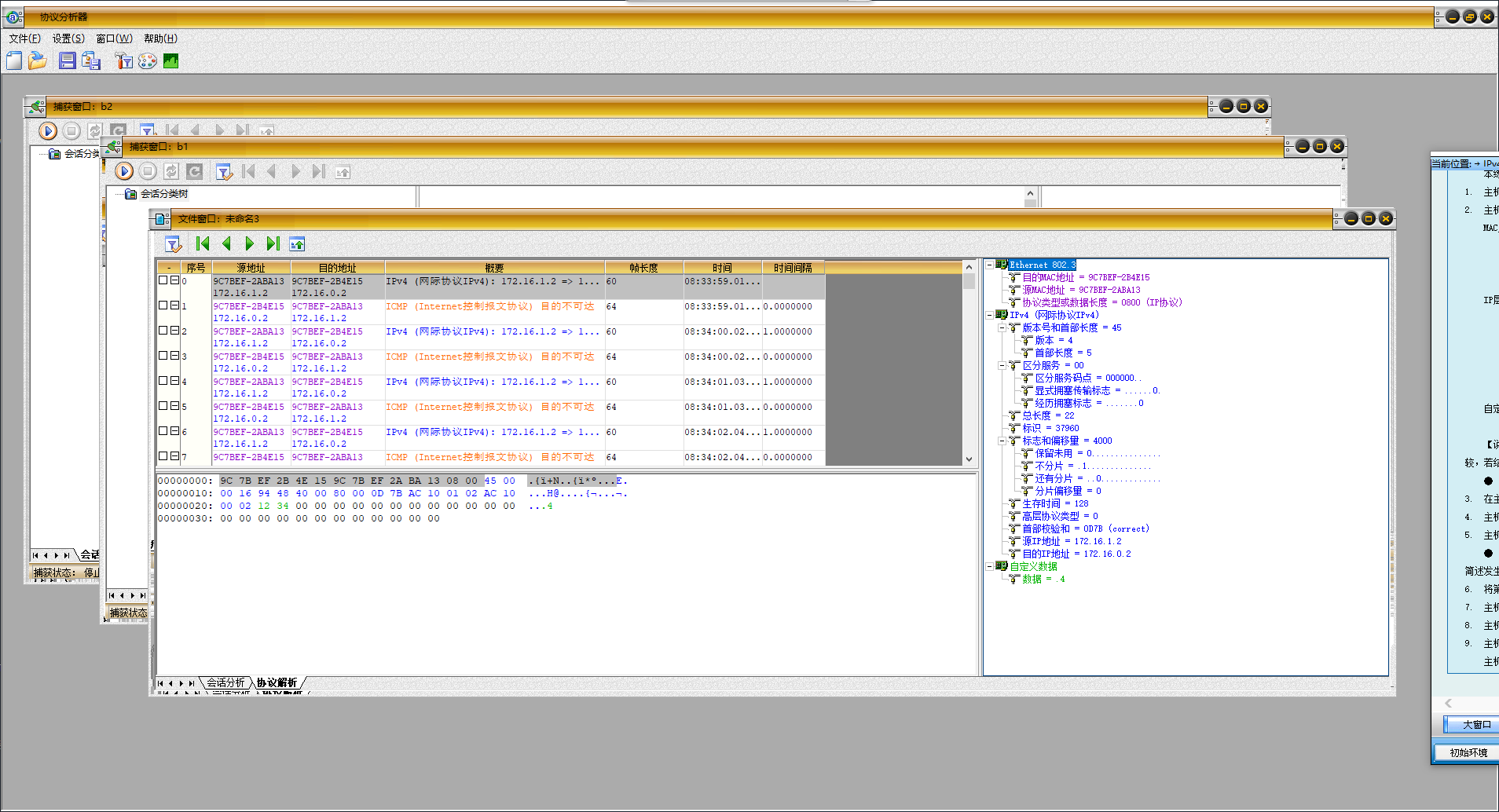
● IP在计算校验和时包括哪些内容？

**IP在计算校验和时包括IP数据报的首部，即版本、首部长度、区分服务、总长度、标识、标志、片偏移、生存时间、协议、首部检验和、源地址、目标地址、可选字段。**

3. 在主机B（两块网卡分别打开两个捕获窗口）、E上启动协议分析器，设置过滤条件（提取IP协议），开始捕获数据。

4. 主机A发送第1步中编辑好的报文。

5. 主机B、E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

并回答以下问题：

● 第1步中主机A所编辑的报文，经过主机B到达主机E后，报文数据是否发生变化？若发生变化，记录变化的字段，并简述发生变化的原因。

**报文数据发生变化，变化的字段为：生存时间、首部校验和，由于A发送给E的报文跨网段，经过路由器B，B在转发数据报前将生存时间（TTL）减1，并重新计算校验和。**

6. 将第1步中主机A所编辑的报文的“生存时间”设置为1，重新计算校验和。

7. 主机B、E重新开始捕获数据。

8. 主机A发送第5步中编辑好的报文。



9. 主机B、E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，并回答以下问题：

● 主机B、E是否能捕获到主机A所发送的报文？简述产生这种现象的原因。

**主机B捕获到了A主机发送的报文，E未捕获A主机发送的报文。B主机对应于172.16.1.1的网卡与A主机在同一局域网内，所以B主机收到了A主机发送的报文，而B主机作为路由器在转发数据报前将报文的生存时间减1得到0，将该数据报丢弃，不转发。所以E主机（172.16.0.2）没有收到数据报。**

**练习2：特殊的IP地址**

本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 直接广播地址

（1）主机A编辑IP数据报1，其中：

目的MAC地址：FFFFFF-FFFFFF。

源MAC地址：A的MAC地址。

源IP地址：A的IP地址。

目的IP地址：172.16.1.255。

自定义字段数据：填入大于1字节的用户数据。

校验和：在其它字段填充完毕后，计算并填充。



（2）主机A再编辑IP数据报2，其中：

目的MAC地址：主机B的MAC地址（对应于172.16.1.1接口的MAC）。

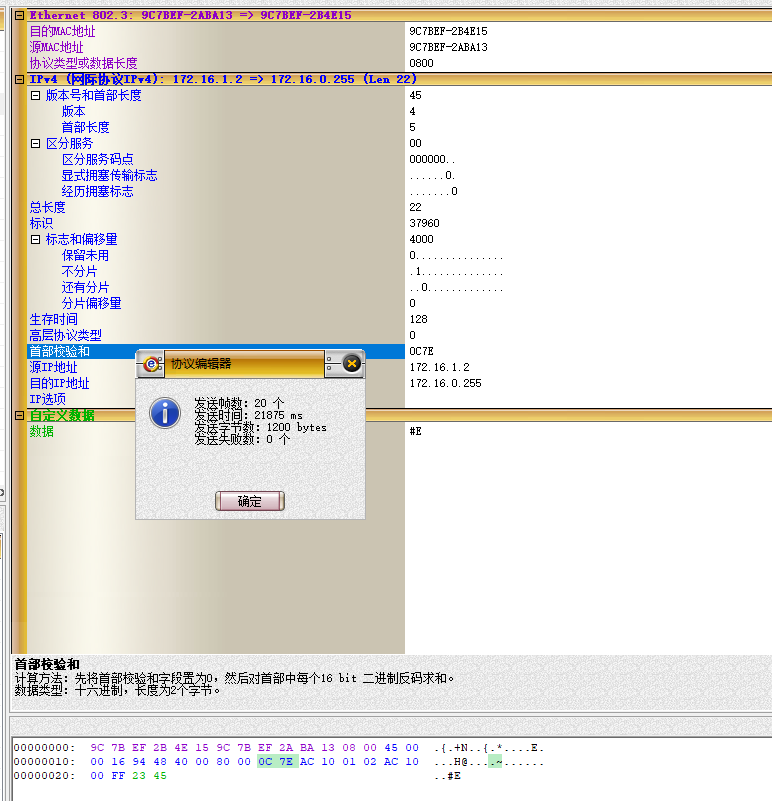
源MAC地址：A的MAC地址。

源IP地址：A的IP地址。

目的IP地址：172.16.0.255。

自定义字段数据：填入大于1字节的用户数据。

校验和：在其它字段填充完毕后，计算并填充。



（3）主机B、C、D、E、F启动协议分析器并设置过滤条件（提取IP协议，捕获172.16.1.2接收和发送的所有IP数据包，设置地址过滤条件如下：172.16.1.2<->Any）。

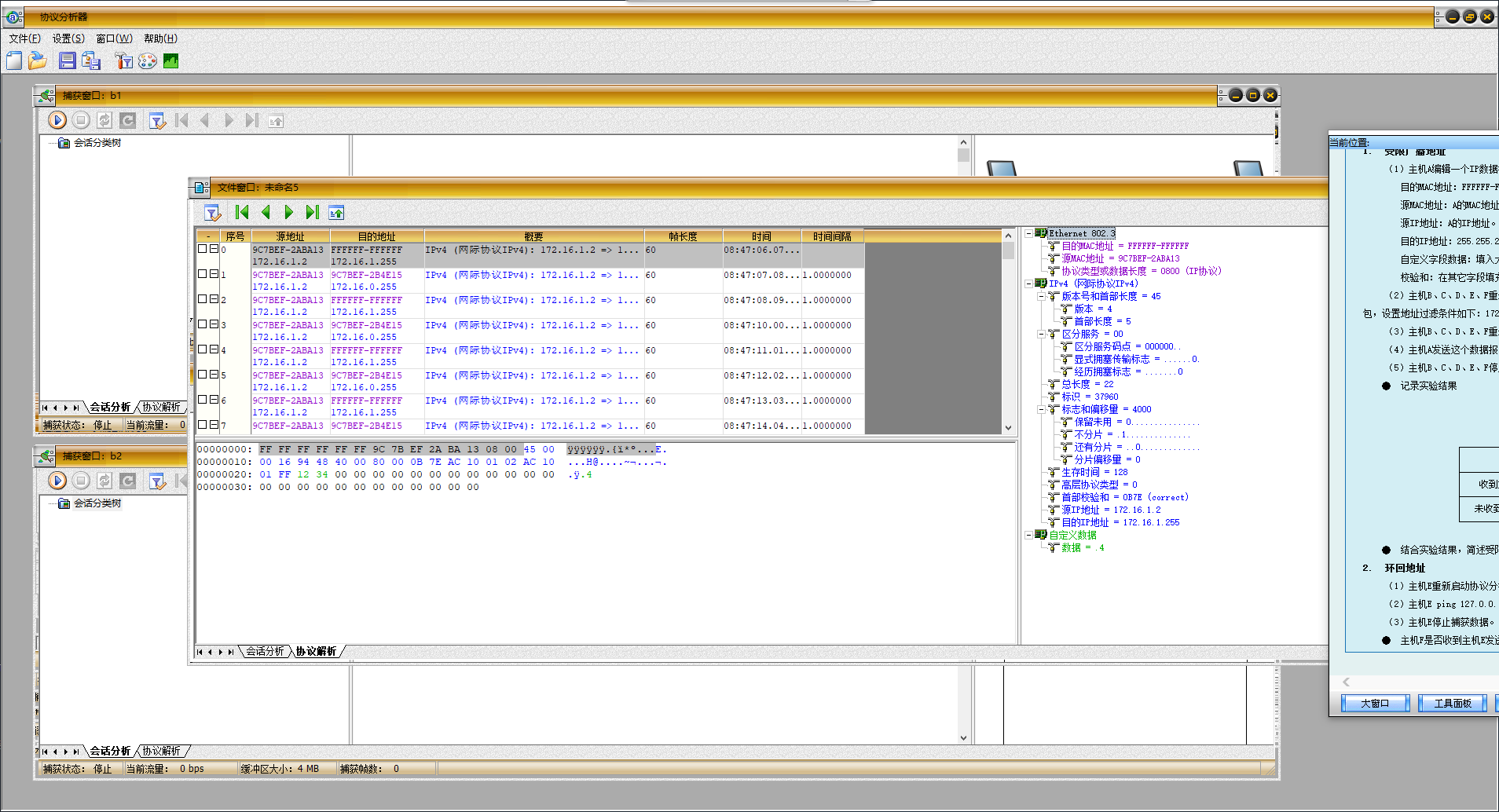
（4）主机B、C、D、E、F开始捕获数据。

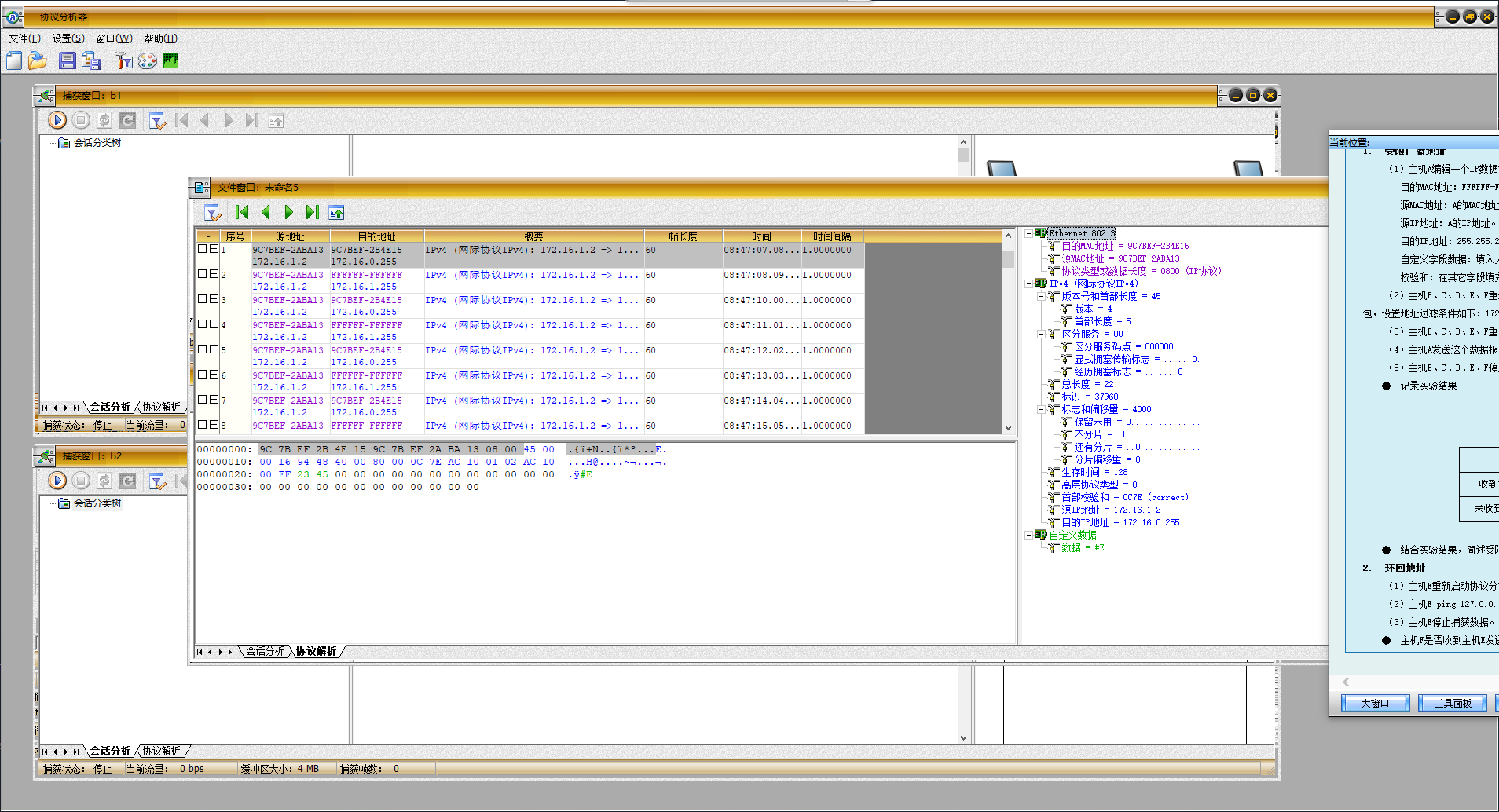
（5）主机A同时发送这两个数据报。

（6）主机B、C、D、E、F停止捕获数据。

● 记录实验结果

|  |  |
| --- | --- |
|  | 主机号 |
| 收到IP数据报1 | B（172.16.1.1）、C、D |
| 收到IP数据报2 | B（172.16.1.1）、B（172.16.0.1）、E、F |





（主机B）

● 结合实验结果，简述直接广播地址的作用。

**直接广播地址，指定了一个特定网络的“所有主机”，一个直接广播的单一拷贝被发送到一个指定的网络，在那里他被广播到所有网络终端。**

2. 受限广播地址

（1）主机A编辑一个IP数据报，其中：

目的MAC地址：FFFFFF-FFFFFF。

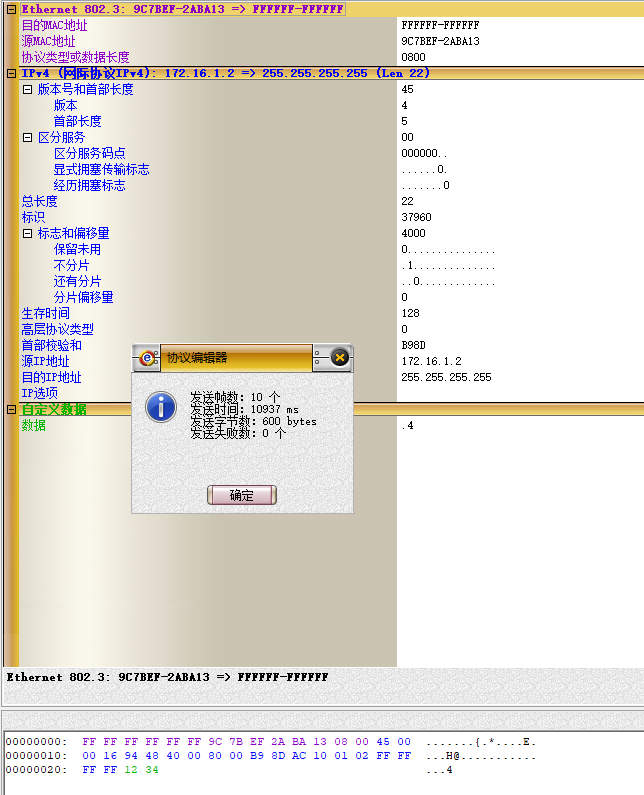
源MAC地址：A的MAC地址。

源IP地址：A的IP地址。

目的IP地址：255.255.255.255。

自定义字段数据：填入大于1字节的用户数据。

校验和：在其它字段填充完毕后，计算并填充。



（2）主机B、C、D、E、F重新启动协议分析器并设置过滤条件（提取IP协议，捕获172.16.1.2接收和发送的所有IP数据包，设置地址过滤条件如下：172.16.1.2<->Any）。

（3）主机B、C、D、E、F重新开始捕获数据。

（4）主机A发送这个数据报。

（5）主机B、C、D、E、F停止捕获数据。

● 记录实验结果

|  |  |
| --- | --- |
|  | 主机号 |
| 收到主机A发送的IP数据报 | B（172.16.1.1）、C、D |
| 未收到主机A发送的IP数据报 | B（172.16.1.1）、C、D |

● 结合实验结果，简述受限广播地址的作用。

**受限的广播地址是255.255.25.255（全1），路由器不转发目的地址为受限的广播地址的数据报，这样的数据报仅出现在本地网络中。所以只有本局域网内的B、C、D主机收到了A主机发送的IP数据报。**

3. 环回地址

（1）主机F重新启动协议分析器开始捕获数据并设置过滤条件（提取IP协议）。

（2）主机E ping 127.0.0.1。

（3）主机F停止捕获数据。

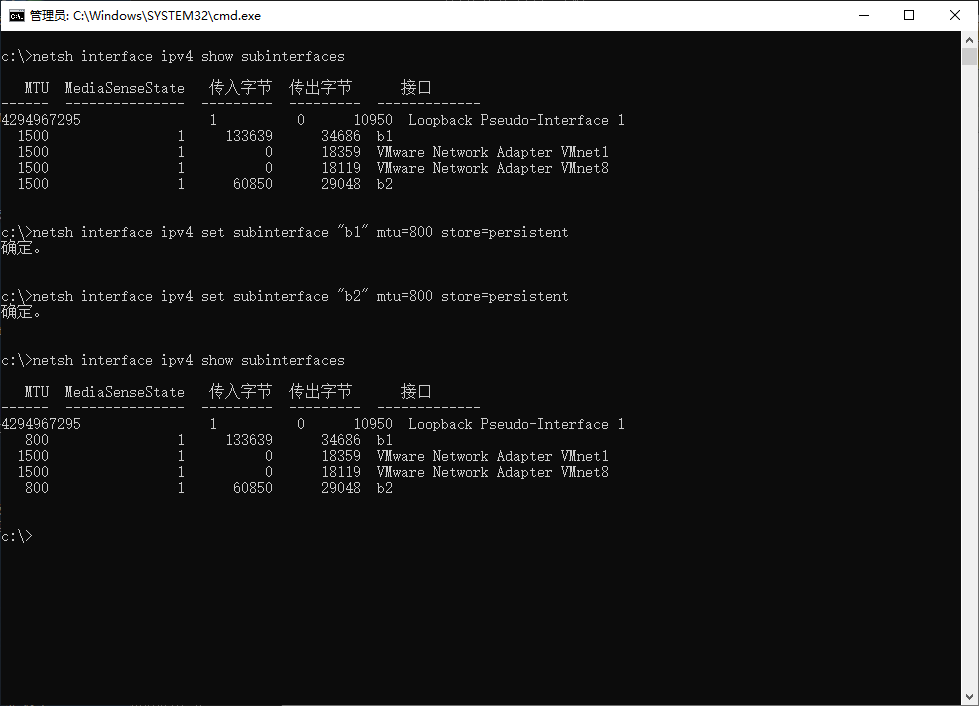
● 主机F是否收到主机E发送的目的地址为127.0.0.1的IP数据报？为什么？

**主机F没有收到E发送的IP数据报，因为若主句发送一个目的地址以为环回地址（127.0.0.1）的IP数据报，则本主机中的协议软件就处理数据报中的数据，而不会把数据报发送到任何网络。所以F主机不会收到E主机发送的目的地址为127.0.0.1的数据报。**

**练习3：IP数据报分片**

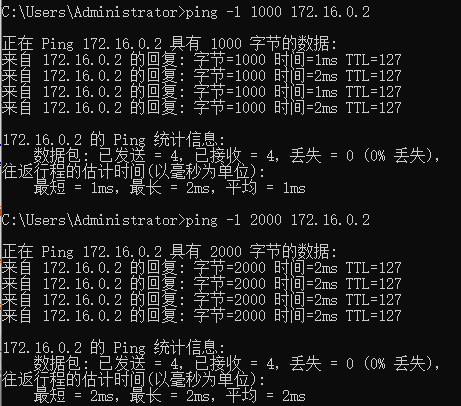
本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 在主机B上使用“实验平台上工具栏中的MTU工具” 设置以太网端口的MTU为800字节（两个端口都设置）。

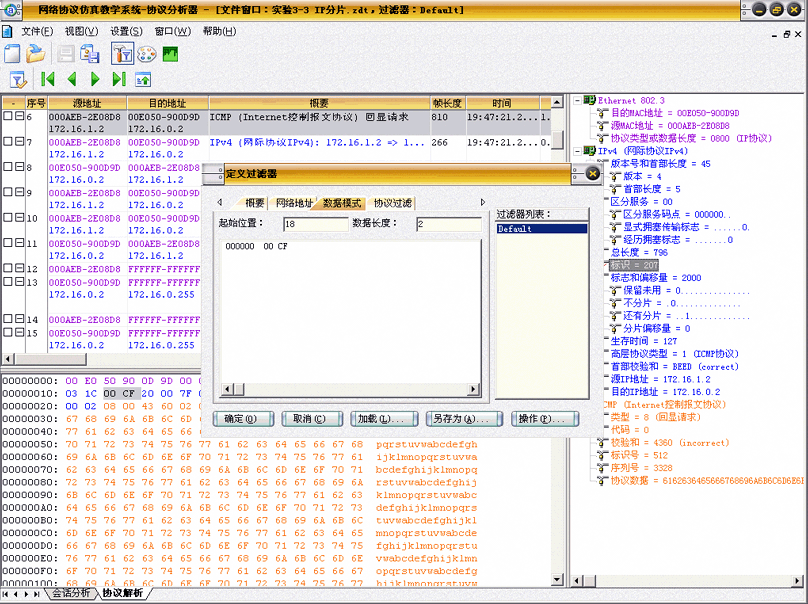


2. 主机A、B、E启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件(提取ICMP协议)。

3. 在主机A上，执行命令ping -l 1000 172.16.0.2。



4. 主机A、B、E停止捕获数据。在主机E上重新定义过滤条件（取一个ICMP数据包，按照其IP层的标识字段设置过滤），如图所示：

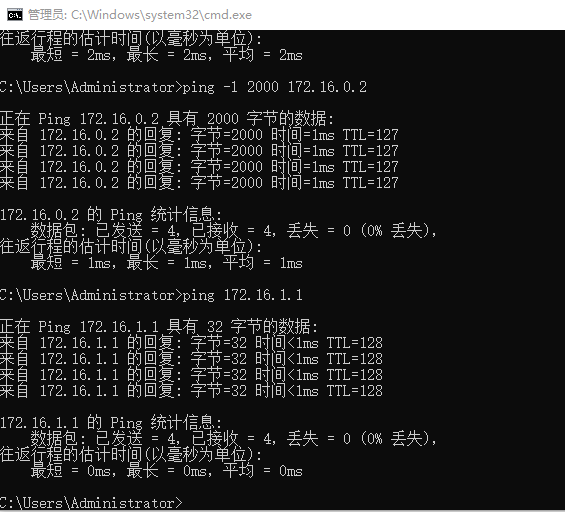


● 将ICMP报文分片信息填入下表，分析表格内容，理解分片的过程。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 分片序号1 | 分片序号2 | 分片序号3 |
| “标识”字段值 | 13628 | 13628 |  |
| “还有分片”字段值 | 1 | 0 |  |
| “分片偏移量”字段值 | 0 | 97（8字节） |  |
| 传输的数据量 | 796字节 | 252字节 |  |

5. 主机E恢复默认过滤器。主机A、B、E重新开始捕获数据。

6. 在主机A上，执行命令ping -l 2000 172.16.0.2。



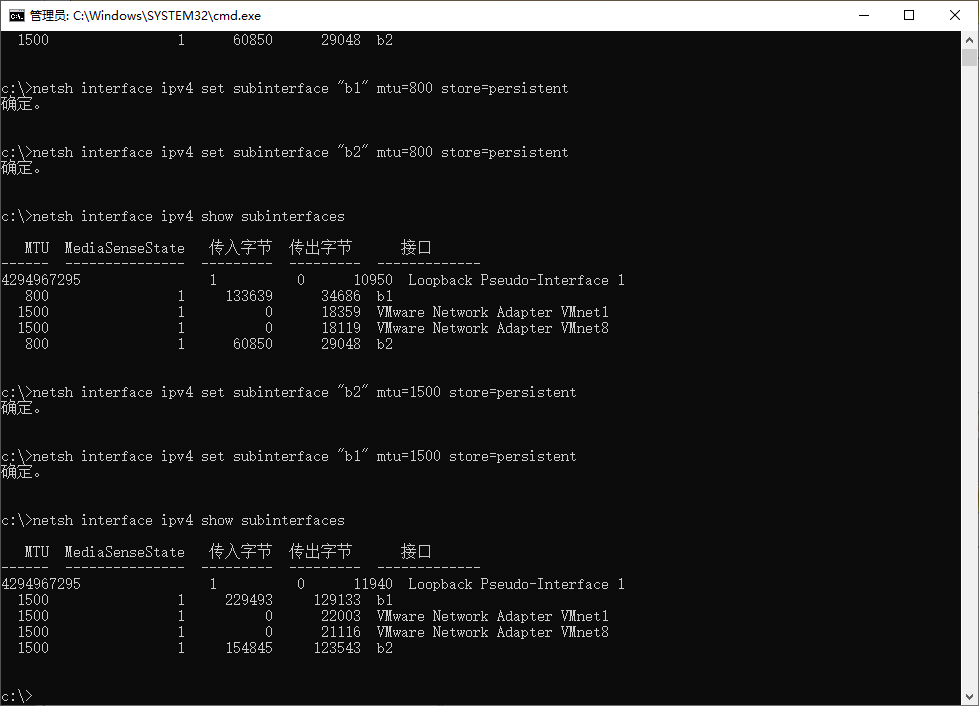
7. 主机A、B、E停止捕获数据。查看主机A、E捕获到的数据，比较两者的差异，体会两次分片过程。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 分片序号1 | 分片序号2 | 分片序号3 |
| “标识”字段值 | 13829 | 13829 | 13829 |
| “还有分片”字段值 | 1 | 1 | 0 |
| “分片偏移量”字段值 | 0 | 97（8字节） | 185（8字节） |
| 传输的数据量 | 796字节 | 724字节 | 528字节 |

第一次A主机发送的数据报（13628）总长度为1028字节（A主机捕获），则数据部分1028-20=1008字节，分片数为1。E主机收到2个分片。分片1总长度796字节，数据部分长度为776字节，分片偏移量为0,。分片2总长度252字节，数据部分长度232字节，分片偏移量97（8字节）=776字节。由于主机B的MTU被设置成了800字节，所以B在转发数据时重新分片，分片长度不超过800字节，除去固定部分20字节，数据部分不超过780字节而分片长度必须是8字节的整数倍，所以分片1数据长度为776字节，加上20字节固定首部长度，所以分片1的长度为796字节。剩余数据组成分片2。

第二次A主机发送的数据报（13829），有2个分片，总长度分别为1500字节、548字节（A主机捕获）。A主机分片1，数据部分长度1480，在经过B主机分割后成为2个分片，1480-776=704字节，加上20字节固定首部长度，E主机捕获的分片2总长度为724。A主机分片2总长度548字节，分片偏移量185（8字节）。E主机捕获分片3总长度548字节，分片偏移量185（8字节）。

8. 主机B上使用“实验平台上工具栏中的MTU工具”恢复以太网端口的MTU为1500字节。



**练习4：子网掩码的作用**

本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 所有主机取消网关。

2. 主机A、C、E设置子网掩码为255.255.255.192，主机B（172.16.1.1）、D、F设置子网掩码为255.255.255.224。

3. 主机A ping 主机B（172.16.1.1），主机C ping 主机D（172.16.1.4），主机E ping 主机F（172.16.0.3）。

● 记录实验结果

|  |  |
| --- | --- |
|  | 是否ping通 |
| 主机A----主机B | 能ping通 |
| 主机C----主机D | 能ping通 |
| 主机E----主机F | 能ping通 |

● 请问什么情况下两主机的子网掩码不同，却可以相互通信？

A按位与结果 172.16.1.0

B按位与结果 172.16.1.0

C按位与结果 172.16.1.0

D按位与结果 172.16.1.0

E按位与结果 172.16.0.0

F按位与结果 172.16.0.0

可以看到A与B、C与D、E与F在同一网段，故可以相互通信。

4. 主机B在命令行方式下输入recover\_config命令，停止静态路由服务。

5. 所有主机恢复到网络结构二的配置。