**《Internet协议分析实验报告》**

**实验单元： 网络层(5/6)**

**传输层(4/6)**

学号:\_\_\_\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 实验机位:\_\_\_\_\_\_\_\_\_

小组成员:

学号：\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_

学号: \_\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_

学号：\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_

学号: \_\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_

学号：\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_

学号：\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_\_\_

实验时间：\_\_\_\_\_\_\_\_\_年\_\_\_\_\_\_\_月\_\_\_\_\_\_\_日

实验目录

**第3部分 网络层(5/6) (5个任务)**

**实验9 网际协议(ipv4)分析**

*练习二 子网掩码与特殊IP地址分析*

任务一 子网掩码作用验证

*练习三 IP数据报分片*

任务一 IP数据报分片

**实验11 Internet控制报文协议（ICMP）分析**

*练习三 ICMP差错报文编辑与分析*

任务一 差错报文编辑与分析

**实验15 路由协议分析**

*练习一 静态路由配置与路由表分析*

任务一 静态路由配置与路由表分析

*练习二 动态路由协议RIPv2分析*

任务一 动态路由协议RIPv2分析

**第4部 传输层(4/6) (4个任务)**

**实验18 用户数据报协议(UDP)分析**

*练习二 UDP单播和广播通信*

任务一 UDP单播通信

任务二 UDP广播通信

**实验19 传输控制协议(TCP)分析**

*练习一 TCP数据传输过程分析*

任务一 TCP连接建立与释放过程

任务二 编辑并发送TCP数据包

# 实验9 网际协议(ipv4)分析

## 练习二 子网掩码与特殊IP地址分析

### 实验学时

0.5学时

### 实验目的

● 掌握子网掩码

● 理解特殊IP地址的含义

### 实验环境

网络拓扑结构二

### 实验工具

协议分析器

协议编辑器

命令行

### 实验任务

任务一 子网掩码作用验证

### 任务一 子网掩码作用验证

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。

本任务将主机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B在命令行方式下输入staticroute\_config命令，开启静态路由服务。

3. 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。

4. 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 |
| 主机C------主机D | 能 |
| 主机E------主机F | 能 |

● 请问什么情况下两主机的子网掩码不同，却可以相互通信？

两台主机都在同一网段，能相互通信

5. 所有主机恢复到网络结构二的配置。

## 练习三 IP数据报分片

### 实验学时

0.5学时

### 实验目的

● 掌握IP数据报分片

● 理解最大传送单元MTU

● 了解与数据报分片有关的字段

### 实验环境

网络拓扑结构二

### 实验工具

MTU工具

协议分析器

命令行

### 实验步骤

任务一 IP数据报分片

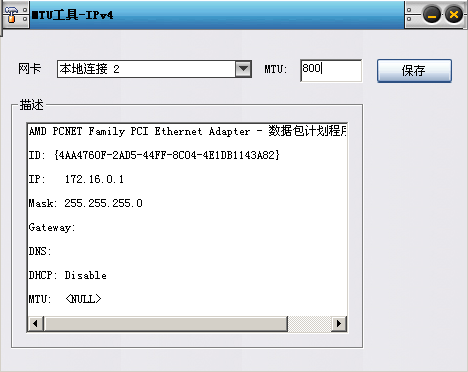
### 任务一 IP数据报分片

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。

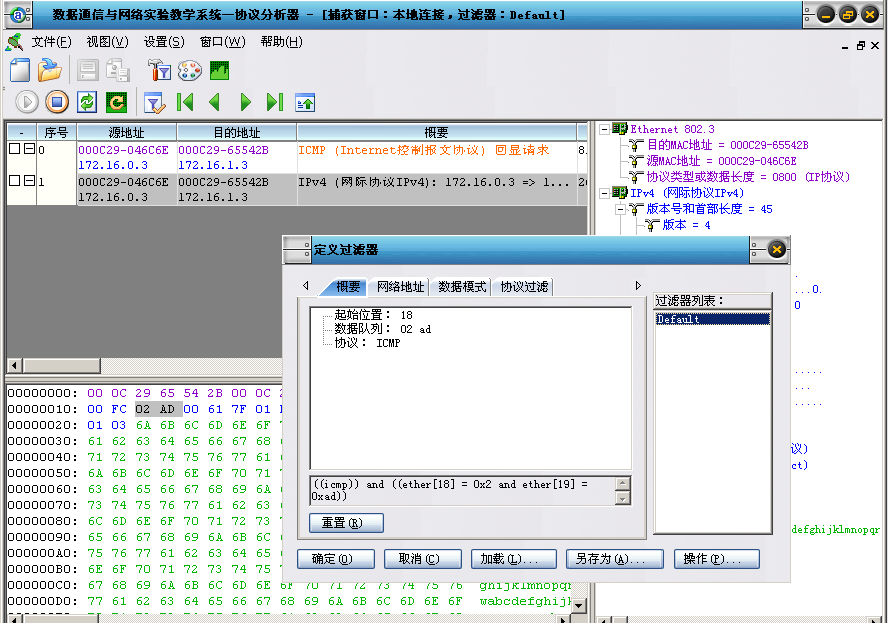
本任务将主机A、B、C、D、E、F作为一组进行实验。

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. 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）。

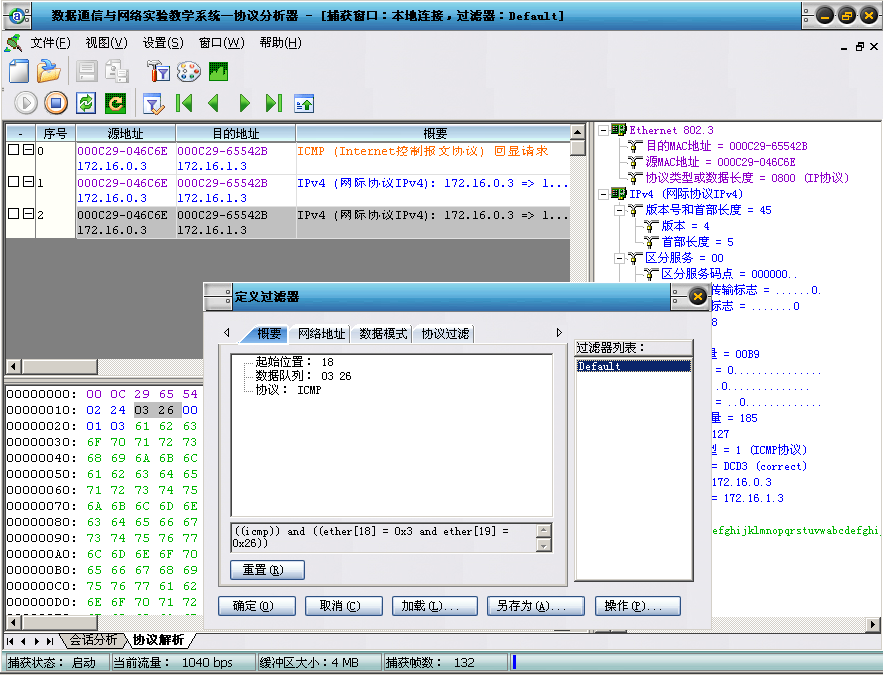


3. 主机A、C、D启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件(提取ICMP协议)。



4. 在主机E上，执行命令ping -l 1000 172.16.1.2；主机F执行命令ping -l 1000 172.16.1.3。

5. 主机A、C、D停止捕获数据。在主机A、C、D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(此图仅是示例，请替换成实验实际的截图)：



● 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 | 685 | 685 |  |
| “还有分片”字段值 | 1 | 0 |  |
| “分片偏移量”字段值 | 0 | 97 |  |
| 传输的数据量 | 768字节 | 232字节 |  |

6. 主机A、C、D恢复默认过滤器。主机A、C、D重新开始捕获数据。

7. 在主机E上，执行命令ping -l 2000 172.16.1.2；主机F执行命令ping -l 2000 172.16.1.3。

8. 主机A、C、D停止捕获数据。察看主机A、C、D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 | 806 | 806 | 806 |
| “还有分片”字段值 | 1 | 1 | 0 |
| “分片偏移量”字段值 | 0 | 97 | 185 |
| 传输的数据量 | 768字节 | 768字节 | 464字节 |

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

做完实验后，请同学考虑以下问题：

◆ Ping的数据部分为3000字节，回显请求报文为何被分为3片而不是2片？

MTU是指IP数据报的首部与数据部分之和，直观看上去3000/1500=2，但是要算上IP数据报的首部，所以分片数3000/（1500-首部长度）>2。

◆ 数据部分长度为多少时报文正好被分为2片？

假设IP首部采用固定长度20字节，那么数据部分就是1500-20=1480字节，1480\*2=2960字节。

◆ 不同协议的MTU的范围从296到65535，使用大的MTU有什么好处？使用小的MTU有什么好处？

大的MTU可以一次性传输更多的数据，适用于网络无阻塞的情况。

小的MTU将大文件分成多片传送，投有助于缓慢的数据传输。

# 实验11 Internet控制报文协议（ICMP）分析

## 练习三 ICMP差错报文编辑与分析

### 实验学时

0.5学时

### 实验目的

● 了解ICMP差错报文的类型

● 掌握目标不可达报文

● 掌握时间超时报文

### 实验环境

网络拓扑结构二

### 实验工具

协议分析器

协议编辑器

命令行

### 实验任务

任务一 差错报文编辑与分析

### 任务一 差错报文编辑与分析

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。

本任务将主机A、B、C、D、E、F作为一组进行实验。

实验开始前主机B首先执行命令“staticroute\_config”启动静态路由。

1. 目的端不可达

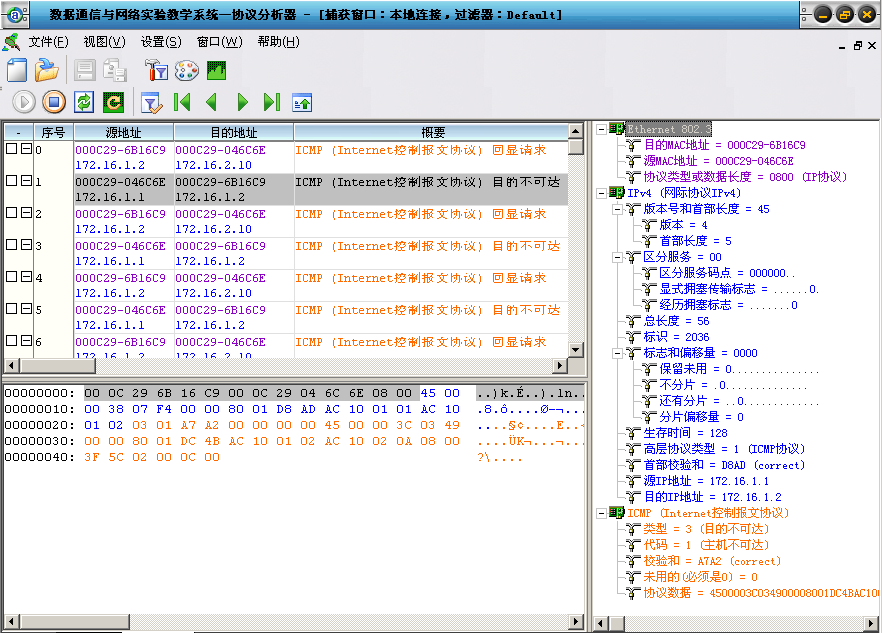
（1）主机A、C、D、E、F启动协议分析器捕获数据，并设置过滤条件（提取ICMP）。

（2）在主机A、C、D、E、F上ping 172.16.2.10（不存在的IP）。

（3）主机A、C、D、E、F停止捕获数据。察看捕获到的数据，并回答以下问题：

● 捕获到的是哪一种目的端不可达报文？

(截图并说明答案)



2. 超时

（1）在主机E上启动协议编辑器，编写一个发送给主机A（172.16.1.2）的ICMP数据帧；主机F启动协议编辑器编写发送给主机C（172.16.1.3）。其中主机E编辑如下的数据帧：

MAC层：

目的MAC地址：主机B的MAC地址（172.16.0.1接口的MAC）。

源MAC地址：E的MAC地址。

协议类型或数据长度：0800。

IP层：

总长度：包含IP层和ICMP层长度。

生存时间：0。

高层协议类型：1。

校验和：在其它字段填充完毕后，计算并填充。

源IP地址：E的IP地址。

目的IP地址：A的IP地址。

ICMP层：

类型：8。

代码字段：0。

校验和：在ICMP其它字段填充完毕后，计算并填充。

其它字段使用默认值。

主机F编辑如下数据帧：

MAC层：

目的MAC地址：主机B的MAC地址（172.16.0.1接口的MAC）。

源MAC地址：F的MAC地址。

协议类型或数据长度：0800。

IP层：

总长度：包含IP层和ICMP层长度。

生存时间：0。

高层协议类型：1。

校验和：在其它字段填充完毕后，计算并填充。

源IP地址：F的IP地址。

目的IP地址：C的IP地址。

ICMP层：

类型：8。

代码字段：0。

校验和：在ICMP其它字段填充完毕后，计算并填充。

其它字段使用默认值。

◆ 为什么要设置“生存时间”字段？

防止差错报文一直被转发，造成不必要的网络负载。

（2）主机A、B(两块网卡)、C、D启动协议分析器捕获数据，并设置过滤条件（提取ICMP协议）。

（3）主机E和F发送已编辑好的数据帧。

（4）主机A、B、C、D停止捕获数据，察看并分析捕获到的数据。

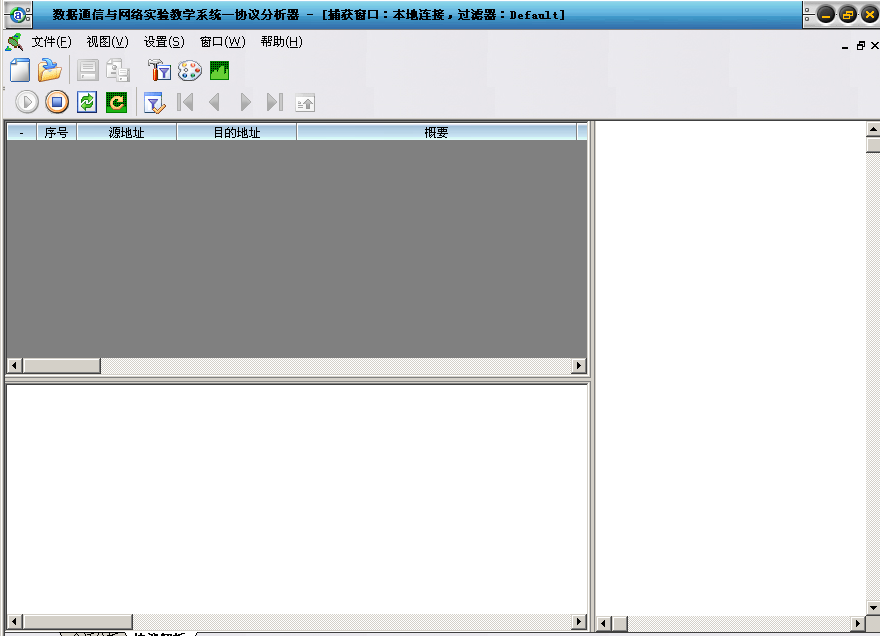
● 哪些主机能捕获到超时报文，哪些主机捕获不到超时报文？

(截图，并说明答案)

B可以捕获



ACD不能



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

# 实验15 路由协议分析

## 练习一 静态路由配置与路由表分析

### 实验学时

0.5学时

### 实验目的

● 掌握路由协议的分类，理解静态路由和动态路由

### 实验环境

网络拓扑结构三

### 实验工具

协议分析器

命令行

### 实验任务

任务一 静态路由配置与路由表分析

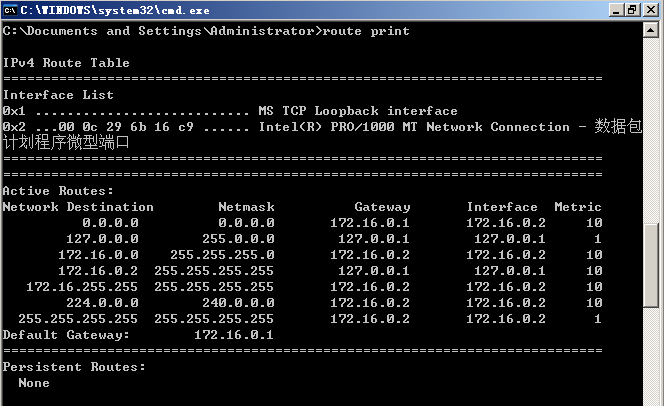
### 任务一 静态路由配置与路由表分析

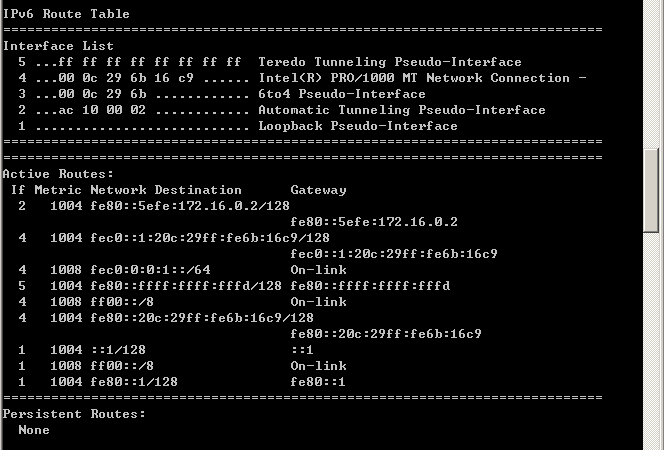
各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。

本任务将主机A、B、C、D、E、F作为一组进行实验。

1. 主机A、B、C、D、E、F在命令行下运行“route print”命令，察看路由表，并回答以下问题：

● 路由表由哪几项组成？

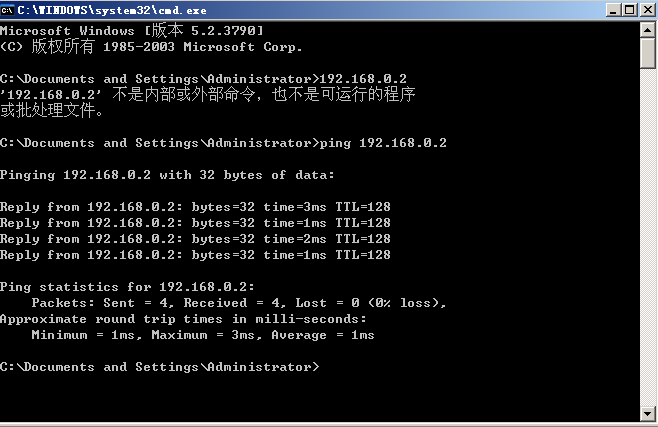


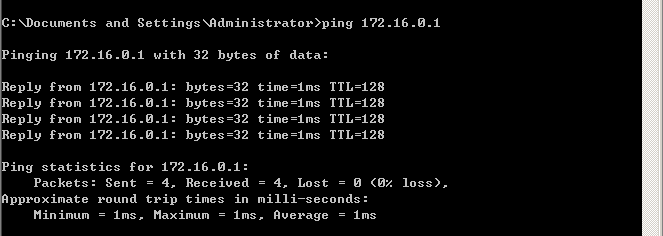


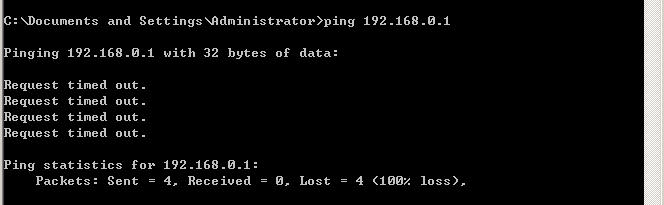
destination 目的网段  
mask 子网掩码  
interface 到达该目的地的本路由器的出口ip  
gateway 下一跳路由器入口的ip，路由器通过interface和gateway定义一调到下一个路由器的链路

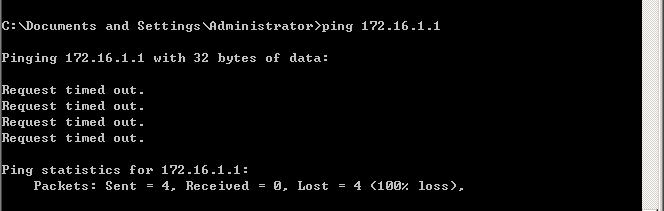
metric 跳数，该条路由记录的质量，如果有多条到达相同目的地的路由记录，路由器会采用metric值小的那条路由

2. 主机A、C、D和F依次ping 主机B（192.168.0.2）、主机B（172.16.0.1）、主机E（192.168.0.1）、主机E（172.16.1.1），观察现象，记录结果。通过在命令行下运行route print命令，察看主机B和主机E路由表，结合路由信息回答问题：









● 主机A的默认网关在本次练习中起到什么作用？

用于向其他IP网络转发IP数据报的IP地址。

● 记录并分析实验结果，简述为什么会产生这样的结果？

「注」表格以主机A为例，主机C、D和F参照主机A。

|  |  |  |
| --- | --- | --- |
|  | 是否ping通 | 原因 |
| 主机A---主机B (192.168.0.2) | 是 | 默认网关是主机B的一个物理接口地址，而目标地址为主机B的另一个物理接口地址 |
| 主机A---主机B (172.16.0.1) | 是 | 默认网关是主机B的一个物理接口地址，而目标地址为主机B的另一个物理接口地址 |
| 主机A---主机E (192.168.0.1) | 否 | AE之间要通过B进行路由，但是B中没有路由条目 |
| 主机A---主机E (172.16.1.1) | 否 | AE之间要通过B进行路由，但是B中没有路由条目 |

3. 主机B和主机E启动静态路由。

（1）主机B与主机E在命令行下使用“staticroute\_config”命令来启动静态路由。

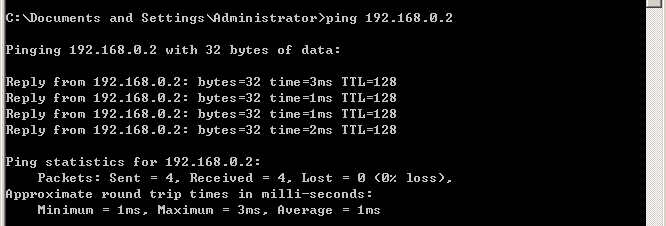
（2）在主机B上，通过在命令行下运行route add命令手工添加静态路由（“route add 172.16.1.0 mask 255.255.255.0 192.168.0.1 metric 2”）。

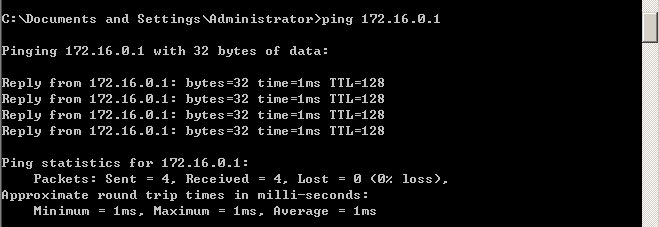
（3）在主机E上，也添加一条静态路由（“route add 172.16.0.0 mask 255.255.255.0 192.168.0.2 metric 2”）。

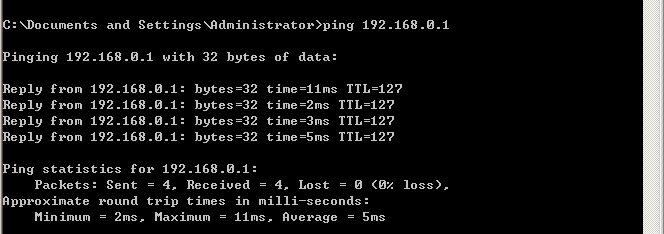
（4）从主机A依次ping主机B（192.168.0.2）、主机B（172.16.0.1）、主机E（192.168.0.1）、主机E（172.16.1.1），观察现象，记录结果。

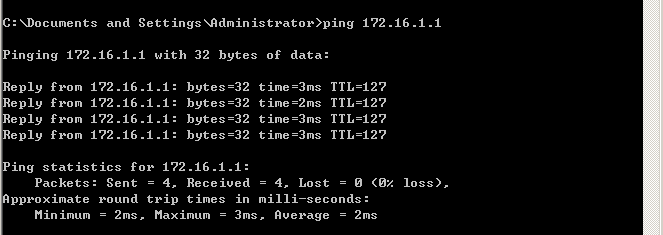
（5）通过在命令行下运行route print命令，察看主机B和主机E路由表，结合路由信息回答问题：

● 记录并分析实验结果，简述手工添加静态路由在此次通信中所起的作用。









|  |  |  |
| --- | --- | --- |
|  | 是否ping通 | 原因 |
| 主机A---主机B (192.168.0.2) | 是 | 默认网关是主机B的一个物理接口地址，而目标地址为主机B的另一个物理接口地址 |
| 主机A---主机B (172.16.0.1) | 是 | 默认网关是主机B的一个物理接口地址，而目标地址为主机B的另一个物理接口地址 |
| 主机A---主机E(192.168.0.1) | 是 | 加入路由条目后，可以把A的ICMP报文抓发给E |
| 主机A---主机E(172.16.1.1) | 是 | 加入路由条目后，可以把A的ICMP报文抓发给E |

**手工添加静态路由在此次通信中所起的作用:**

加入路由后，B可以通过查找路由表，把A的ICMP报文抓发给E所在网络。

4. 在主机B上，通过在命令行下运行route delete命令（“route delete 172.16.1.0”）；在主机E上，运行route delete命令（“route delete 172.16.0.0”）删除手工添加的静态路由条目。

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

● 简述静态路由的特点以及路由表在路由期间所起到的作用。

静态路由是一种特殊的路由，有网络管理员采用手工方法在路由器中配置而成这

种方法适合在规模较小、路由表也相对简单的网络中使用。它比较简单，容易实现；可

以精确控制路由选择，改进网络的性能；减少路由器的开销，为重要的应用保证带宽。

但对于大规模的网络而言，如果网络拓扑结构发生改变或网络链路发生故障，用手工的方法配置及修改路由表，对管理员会形成很大压力。每台运行 TCP/IP 的计算机根据 IP 路由表的决定作出路由决定。

## 练习二 动态路由协议RIPv2分析

### 实验学时

0.5学时

### 实验目的

●掌握动态路由协议RIP的报文格式、工作原理及工作过程

### 实验环境

网络拓扑结构三

### 实验工具

协议分析器

命令行

### 实验步骤

任务一 动态路由协议RIPv2分析

### 任务一 动态路由协议RIPv2分析

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。

本任务将主机A、B、C、D、E、F作为一组进行实验。

1. 在主机A、B、C、D、E、F上启动协议分析器，设置过滤条件（提取RIP和IGMP），开始捕获数据。



2. 主机B和主机E启动RIP协议并添加新接口：

（1）在主机B上启动RIP协议：在命令行方式下输入“rip\_config”。

（2）在主机E上启动RIP协议：在命令行方式下输入“rip\_config”。

（3）添加主机B的接口：

① 添加IP为172.16.0.1的接口：在命令行方式下输入“rip\_config "172.16.0.1的接口名" enable”。

② 添加IP为192.168.0.2的接口：在命令行方式下输入“rip\_config "192.168.0.2的接口名" enable”。

（4）添加主机E的接口：

① 添加IP为192.168.0.1的接口：在命令行方式下输入“rip\_config "192.168.0.1的接口名" enable”。

② 添加IP为172.16.1.1的接口：在命令行方式下输入“rip\_config "172.16.1.1的接口名" enable”。

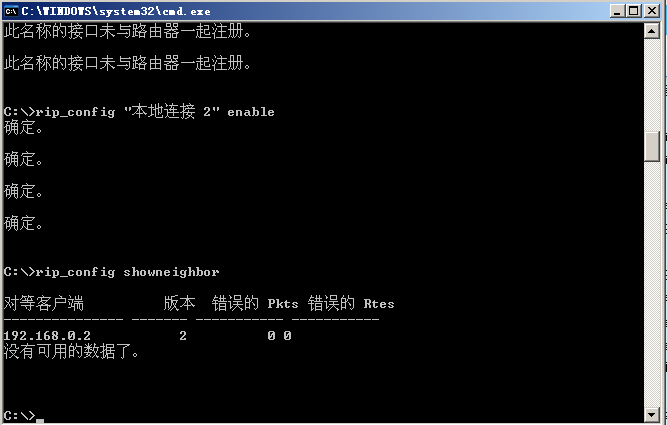
3. 主机B在命令行方式下，输入“rip\_config showneighbor”察看其邻居信息。

(贴图)



主机E在命令行方式下，输入“rip\_config showneighbor”察看其邻居信息。

(贴图)



4. 所有主机通过协议分析器观察报文交互，直到两台主机的路由表达到稳定态。

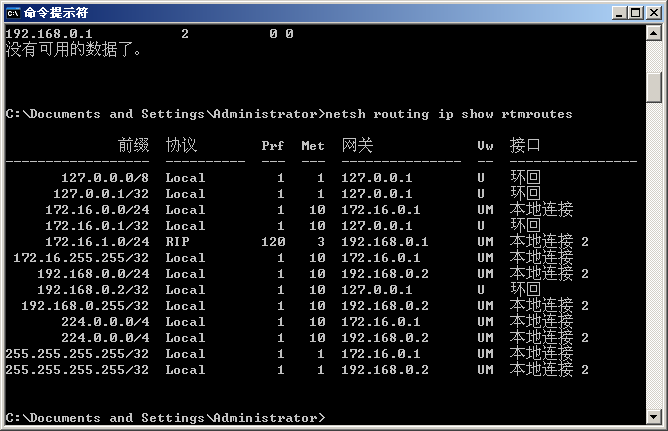
● 如何判定路由表达到稳定态？

方法1：主机A ping主机F，若ping通则路由表达到稳定态；

方法2：如果主机B的路由条目中出现172.16.1.0网络的信息，同时主机E的路由条目中出现172.16.0.0网络的信息，则路由表达到稳定态。

● 在主机B、E上使用“netsh routing ip show rtmroutes”察看路由表，记录稳定状态下主机B和主机E的路由表条目。

(贴图)



主机B的路由表中除了具有172.16.0.0和192.168.0.0网络信息外，还具有

172.16.1.0网络信息。



主机E的路由表中除了具有172.16.1.0和192.168.0.0网络信息外，还具有

172.16.0.0网络信息。

5. 主机B和主机E在命令行下输入命令“recover\_config”，停止RIP协议。观察协议分析器报文交互，并回答问题：

● IGMP报文在RIP交互中所起的作用是什么？

启动RIP协议的路由器受限使用IGMP组成员报告报文加入多播组，从而减轻以后RIP交互报文对网络的负载。

● 通过以上5步，绘制主机B和主机E的RIP交互图（包括IGMP报文）。

加入多播组（发送IGMP组成员报告报文）-->路由信息请求（发送RIP请求报

文）-->路由信息应答（发送RIP应答报文）。

# 实验18 用户数据报协议(UDP)分析

## 练习二 UDP单播和广播通信

### 实验学时

1学时

### 实验目的

● 了解单播、广播和多播的概念

● 掌握单播、广播通信方式

● 了解广播和多播的区别

### 实验环境

网络拓扑结构一

### 实验工具

UDP工具

协议分析器

协议编辑器

### 实验任务

任务一 UDP单播通信

任务二 UDP广播通信

### 任务一 UDP单播通信

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。

本任务将主机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。

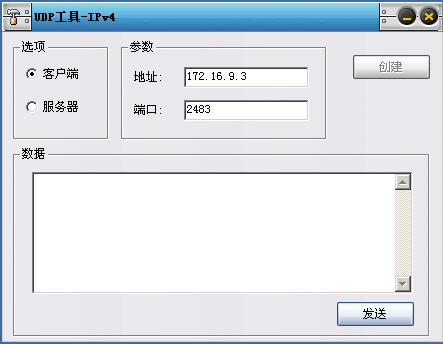
2. 主机C、E上启动协议分析器开始捕获数据，并设置过滤条件（提取UDP协议）。

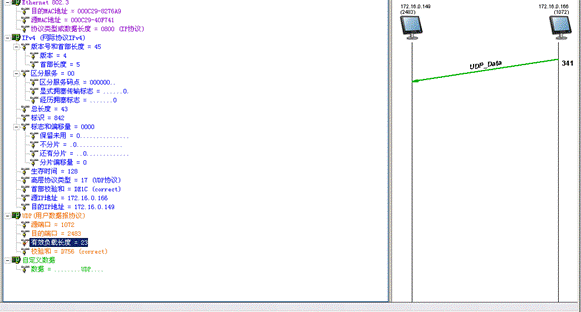
3. 主机A上启动“实验平台工具栏中的UDP工具”，作为客户端，以主机C的IP为目的IP地址，以2483为端口，填写数据并发送。

4. 察看主机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？

(贴图说明)





主机C可以收到

5. 察看主机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：传输效率高，不需进行编号，不必进行连接建立和连接终止；

缺点：使用UDP的进程不能向UDP发送数据流，也不能期望UDP将这个数据流分割成为许多不同的相关联的用户数据报。相反，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。

不含有

优点：提高传输效率；

缺点：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可以收到数据包。UDP可以使用0作为校验和进行通信。

7. 主机B、C、D、E、F关闭服务端，主机A关闭客户端。

### 任务二 UDP广播通信

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。

本任务将主机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。

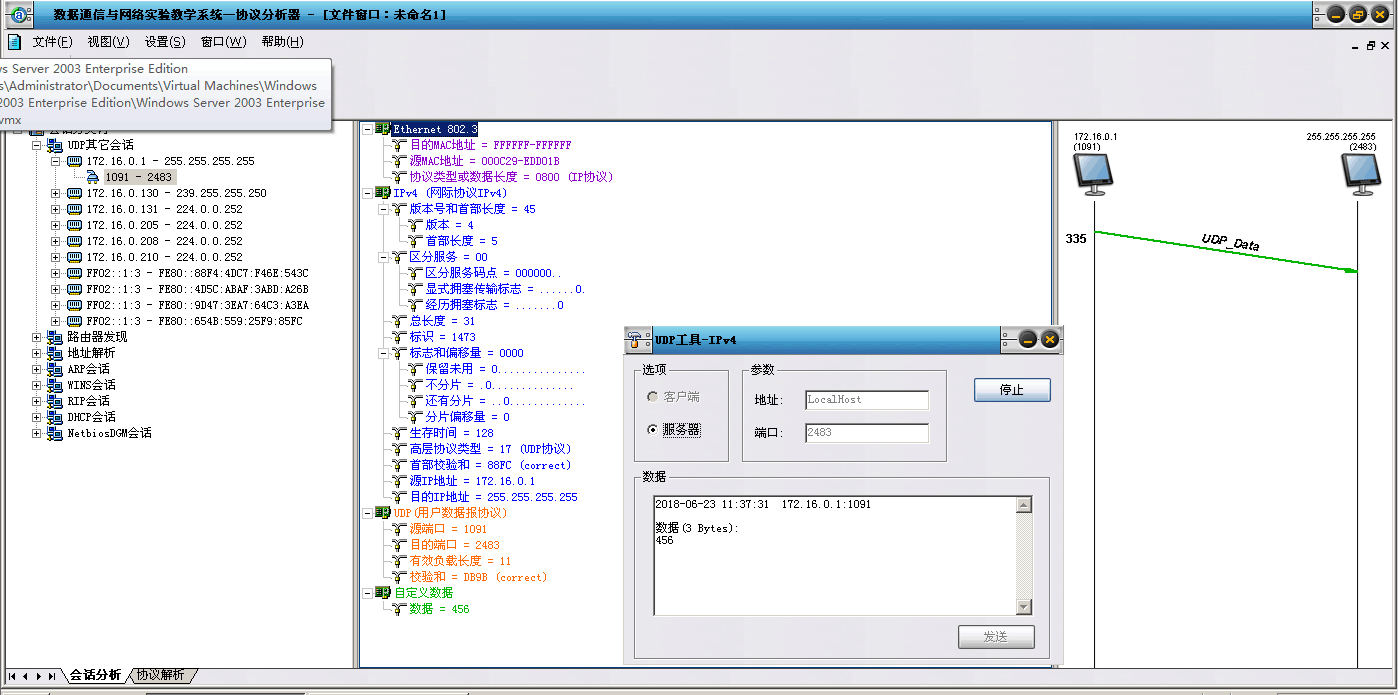
2. 主机B、C、D、E、F启动协议分析器捕获数据，并设置过滤条件（提取UDP协议）。

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. 察看主机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？

(贴图说明)



主机B、C、D、E、F都收到了主机A发送的UDP报文。

5. 察看协议分析器上捕获的UDP报文，并回答以下问题：

● 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？

目的MAC地址为FFFFFF-FFFFFF，是广播地址；

目的IP地址为255.255.255.255，是受限广播地址。

◆ 如果将任务一中所编辑数据包的目的MAC地址换成某一个主机的MAC地址，是否所有主机还会收到这种报文？

主机A发送的报文的目的MAC地址为某一主机的MAC地址，而目的IP地址无论是某一主机的IP地址，还是255.255.255.255，结果都是只有目的MAC地址所对应的主机可收到主机A发送的报文。因为目的MAC地址对应主机才是真正接收数据的主机（前提是目的IP是有效的）。

◆ 如果将任务一中所编辑数据包的目的MAC地址设成广播地址，目的IP设成某一主机的IP地址，结果怎样？

如果目的MAC为广播地址，则结果为所有主机都可接收主机A的报文；

如果目的MAC为某一主机的MAC，则主机A发送的数据只能被该主机接收。

因为目的MAC地址对应主机才是真正接收数据的主机。

6. 所有主机断开与UDP工具的连接。

# 实验19 传输控制协议(TCP)分析

## 练习一 TCP数据传输过程分析

### 实验学时

1学时

### 实验目的

● 掌握TCP协议的报文格式

● 掌握TCP连接的建立和释放过程

● 掌握TCP数据传输中编号与确认的过程

● 掌握TCP协议校验和的计算方法

### 实验环境

网络拓扑结构一

### 实验工具

地址本工具

协议分析器

协议编辑器

TCP工具

启动TCP屏蔽

停止TCP屏蔽

命令行

### 实验任务

任务一 TCP连接建立与释放过程

任务二 编辑并发送TCP数据包

### 任务一 TCP连接建立与释放过程

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。

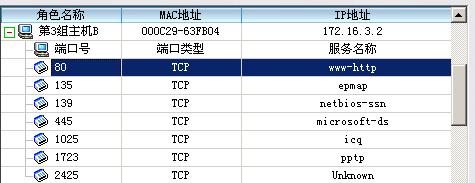
本任务将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B所在组为例，其它组的操作参考主机A、B所在组的操作。

1. 主机B启动协议分析器捕获数据，并设置过滤条件（提取TCP协议）。

2. 主机A启动TCP工具连接主机B。

（1）主机A启动“实验平台工具栏中的地址本工具”。点击[主机扫描]按钮获取组内主机信息，选中主机B点击[端口扫描]按钮获取主机B的TCP端口列表。

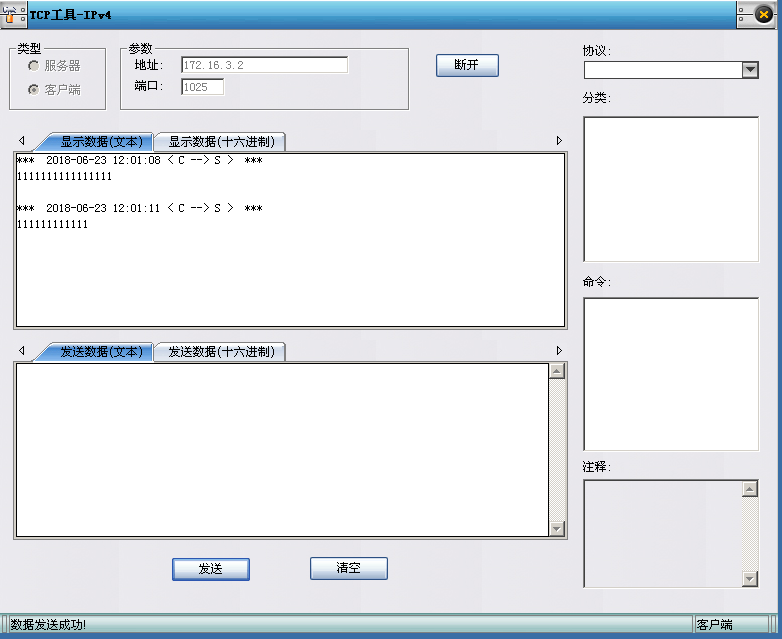
(贴图)



（2）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。

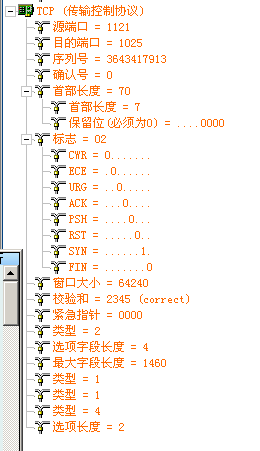
「注」建议使用1024以后的端口。

(贴图)

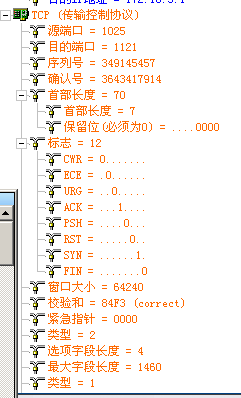


3. 察看主机B捕获的数据，填写下表。

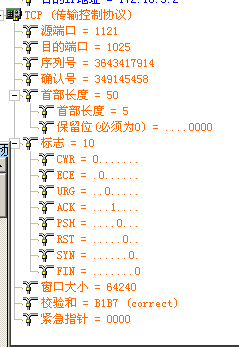
(报文1 贴图)



(报文2 贴图)



(报文3 贴图)



● 记录实验结果。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 报文1 | 报文2 | 报文3 |
| 序列号 | 3643417913 | 349145457 | 3643417913 |
| 确认号 | 0 | 3643417914 | 349145458 |
| 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“最大字段长度”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。

它的值是1460；由发送端指定，表明了能在网络上传输的最大的段的尺寸；

MSS=MTU-20(IP首部)-(20TCP首部)

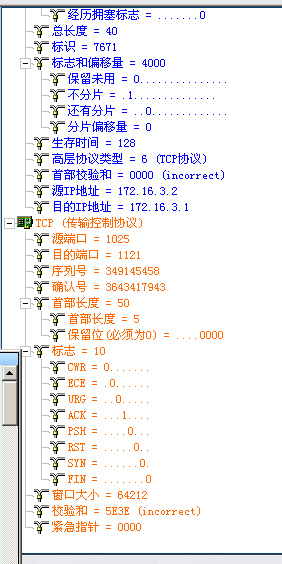
4. 主机A断开与主机B的TCP连接。

5. 察看主机B捕获的数据，填写下表。

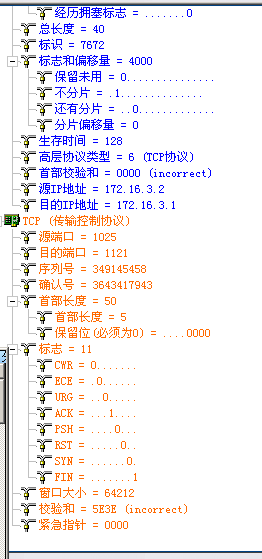
(报文4 贴图)



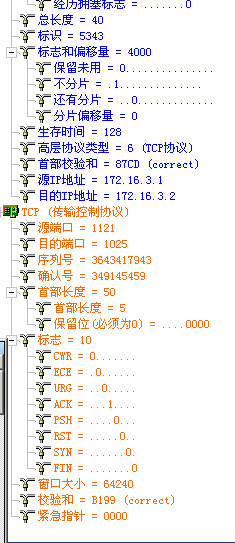
(报文5 贴图)



(报文6贴图)



(报文7 贴图)



● 记录实验结果。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 报文4 | 报文5 | 报文6 | 报文7 |
| 序列号 | 3643417942 | 349145458 | 349145458 | 3643417943 |
| 确认号 | 349145458 | 3643417943 | 3643417943 | 349145459 |
| 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。

（说说你的理解）

为了确保可靠性，发送的报文都有递增的序列号。序号和确认号用来确保传输的可靠性。

### 任务二 编辑并发送TCP数据包

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。

本任务将主机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。

在本任务中由于TCP连接有超时时间的限制，故协议编辑器和协议分析器的两位同学要默契配合，某些步骤（如计算TCP校验和）要求熟练、迅速。

为了实现TCP三次握手过程的仿真，发送第一个连接请求帧之前，编辑端主机应该使用TCP屏蔽功能来防止系统干扰（否则计算机系统的网络会对该请求帧的应答帧发出拒绝响应）。

通过手工编辑TCP数据包实验，要求理解实现TCP连接建立、数据传输以及断开连接的全过程。在编辑过程中注意体会TCP首部中的序列号和标志位的作用。

首先主机B上的一个进程作服务器进程，并向该服务器进程发送一个建立连接请求报文，对应答的确认报文和断开连接的报文也编辑发送。其步骤如下：

1. 主机B启动协议分析器捕获数据，设置过滤条件（提取HTTP协议）。

2. 主机A上启动协议编辑器，在界面初始状态下，程序会自动新建一个单帧，可以利用协议编辑器打开时默认的以太网帧进行编辑。

3. 填写该帧的以太网协议首部，其中：

源MAC地址：主机A的MAC地址

目的MAC地址：主机B的MAC地址

协议类型或数据长度：0800（IP协议）

4. 填写IP协议头信息，其中：

高层协议类型：6（上层协议为TCP）

总长度：40（IP首部 + TCP首部）

源IP地址：主机A的IP地址

目的IP地址：主机B的IP地址

其它字段任意。

应用前面学到的知识计算IP首部校验和。

5. 填写TCP协议信息，其中：

源端口：任意大于1024的数，不要使用下拉列表中的端口

目的端口：80（HTTP协议）

序列号：选择一个序号ISN（假设1942589885），以后的数据都根据它来填写

确认号：0

首部长度：50（长度20字节）

标志位：02（标志SYN=1）

窗口大小：任意

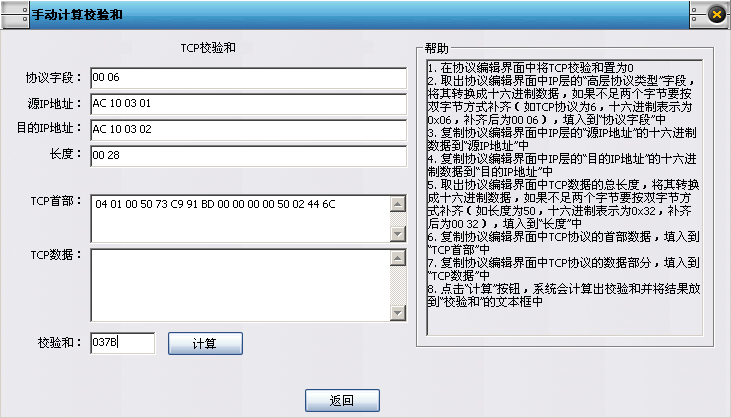
紧急指针：0

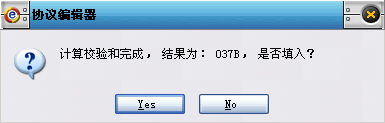
使用协议编辑器的“手动计算”方法计算校验和；再使用协议编辑器的“自动计算”方法计算校验和。将两次计算结果相比较，若结果不一致，则重新计算。

(对编辑结果贴图)









● TCP在计算校验和时包括哪些内容？

[TCP](https://www.baidu.com/s?wd=TCP&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)校验和的范围包括首部和数据这两部分。和[UDP](https://www.baidu.com/s?wd=UDP&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)用户数据报一样，在计算校验和时，要在[TCP](https://www.baidu.com/s?wd=TCP&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)报文段的前面加上12字节的伪首部。

6. 将设置完成的数据帧复制3份。

修改第二帧的TCP 层的“标志”位为10（即标志位ACK=1），TCP层的“序列号”为1942589885+1。

修改第三帧的TCP层的“标志”位为11（即标志位ACK=1、FIN=1），TCP层的“序列号”为1942589885+1。

7. 在发送该TCP连接请求之前，先ping一次主机B，让主机B知道自己的MAC地址。

8. 启动“实验平台工具栏中的启动屏蔽”，为TCP/IP协议栈过滤掉收到的TCP数据。

9. 点击菜单栏中的[发送]按钮，在弹出对话框中选择发送第一帧。

10. 在主机B上捕获相应的应答报文，这里要求协议分析器一端的同学及时准确地捕获应答报文并迅速从中获得应答报文的接收字节序列号，并告知协议编辑器一端的同学。

(贴图并说明)



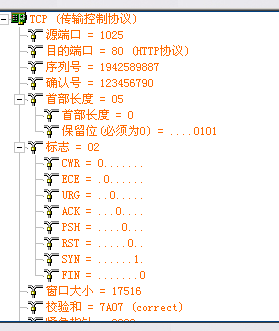
11. 假设接收字节序号为：3246281765，修改第二帧和第三帧TCP层的“确认号”的值为：3246281766。

12. 计算第二帧的TCP校验和，将该帧发送。对主机B的应答报文进行确认。

13. 计算第三帧的TCP校验和，将该帧发送。

14. 在主机B上观察应答报文，要及时把最后一帧“序列号”告知协议编辑器一端的同学。

(贴图并说明)

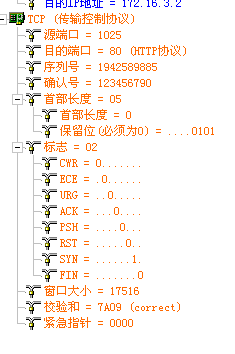


15. 修改第四帧的TCP层“确认号”为接收的序列号+1（即3246281767）。

16. 计算第四帧的TCP校验和，将该帧发送。断开连接，完成TCP连接的全过程。

17. 协议分析器一端截获相应的请求及应答报文并分析，注意观察“会话分析”中的会话过程。

(贴图并分析说明)



18. 编辑端主机启动“实验平台工具栏中的停止屏蔽”，恢复正常网络功能。

## 