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

【实验学时】

2 学时

【实验环境配置】

采用网络结构二

节点	IP 地址	MAC 地址
A	171.16.1.2/24	00-E0-4C-54-A1-B6
B(端口 1)	172.16.1.1/24	00-E0-4C-54-A1-95
B(端口 2)	172.16.0.1/24	F0-4D-A2-32-BB-AF
C	172.16.1.3/24	00-E0-4C-61-4C-29
D	172.16.1.4/24	00-E0-4C-54-A1-88
E	172.16.0.2/24	00-E0-4C-C5-18-89
F	172.16.0.3/24	00-25-64-91-DE-88

【实验原理】

一、 IP 报文格式

IP 数据报是由 IP 首部加数据组成的。IP 首部的最大长度不超过 60 字节。 IP 数据报文格式如下图所示：

<table>
<tr><td>4 位版本</td><td>4 位首部长度</td><td>8 位服务类型</td><td colspan="2">16 位总长度（字节数）</td></tr>
<tr><td colspan="3">16 位标识</td><td>3 位标志</td><td>13 位片偏移</td></tr>
<tr><td>8 位生存时间</td><td colspan="2">8 位协议类型</td><td colspan="2">16 位首部检验和</td></tr>
<tr><td colspan="5">32 位源 IP 地址</td></tr>
<tr><td colspan="5">32 位目的 IP 地址</td></tr>
<tr><td colspan="5">选项（如果有）</td></tr>
</table>

数据

二、 IP 分片

链路层具有最大传输单元（MTU）这个特性，它限制了数据帧的最大长度。不同的网络类型都有一个上限值。以太网通常是 1500 字节。 如果 IP 层有数据包要传输，而数据包的长度超过了 MTU，那么 IP 层就要对数据包进行分片操作。使每一片长度都小于 MTU。 IP 首部中“16 位标识”、“3 位标志”和“13 位片偏移”包含了分片和重组所需的信息。另外，当数据被分片后，每个片的“16 位总长度” 值要改为该片的长度值。

三、 IP 路由表

大部分网络层设备都存储着一张记录路由信息的表格，称为路由表。它由许多条项目组成。网络层设备收到数据报后，根据其目的 IP 地址查找路由表确定数据报传输的最佳路径(下一跳)。然后利用网络层的协议重新封装数据报，利用下层提供的服务把数据报转发出去。路由表的项目一般含有五个基本字段：目的地址、网络掩码、下一跳地址、接口、度量。

路由表按如下顺序匹配：

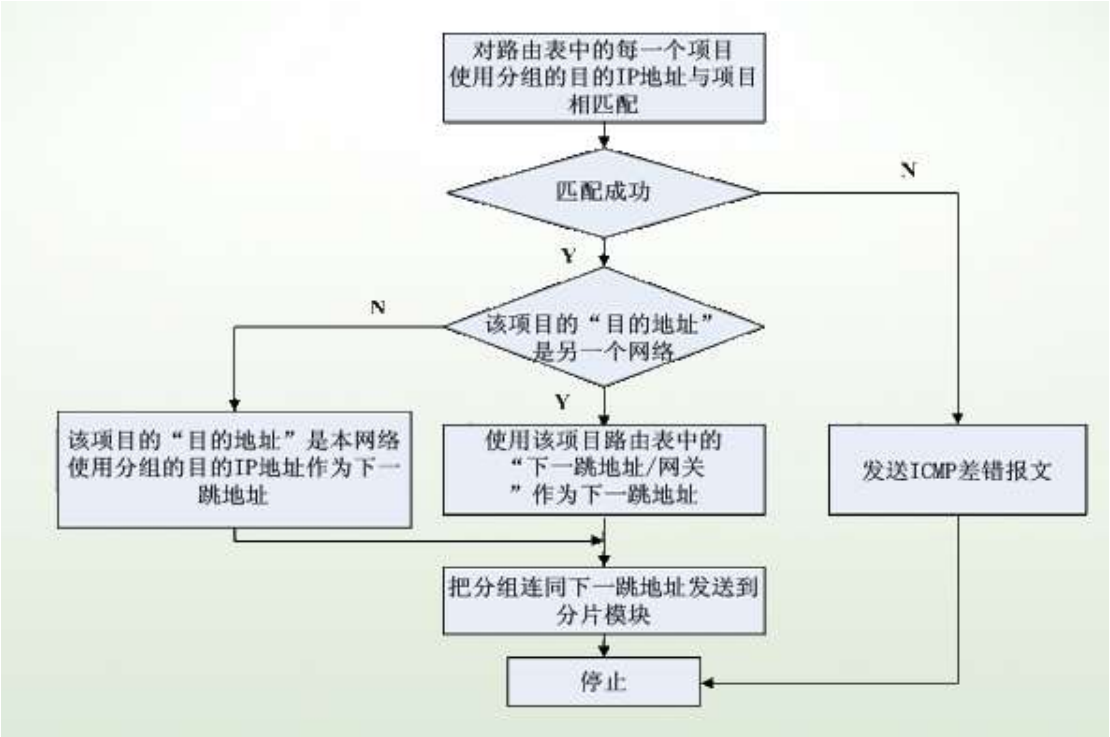
- 直接交付：路由表表项的“目的地址”字段是交付主机的本网络地址。
- 特定主机交付：路由表表项的“目的地址”字段是某台特定主机的 IP 地址。
- 特定网络交付：路由表表项的“目的地址”字段是另一个网络的地址。
- 默认交付：路由表表项的“目的地址”字段是一个默认路由器（默认网关）。

四、 路由选择过程

路由选择模块从 IP 处理模块接收到 IP 分组后，使用该分组的目的 IP 地址同路由表中的每一个项目按特定的顺序（按照前面介绍的“路由表匹配顺序”）查找匹配项，当找到第一个匹配项后就不再继续寻找了，这样就完成了路由选择过程。

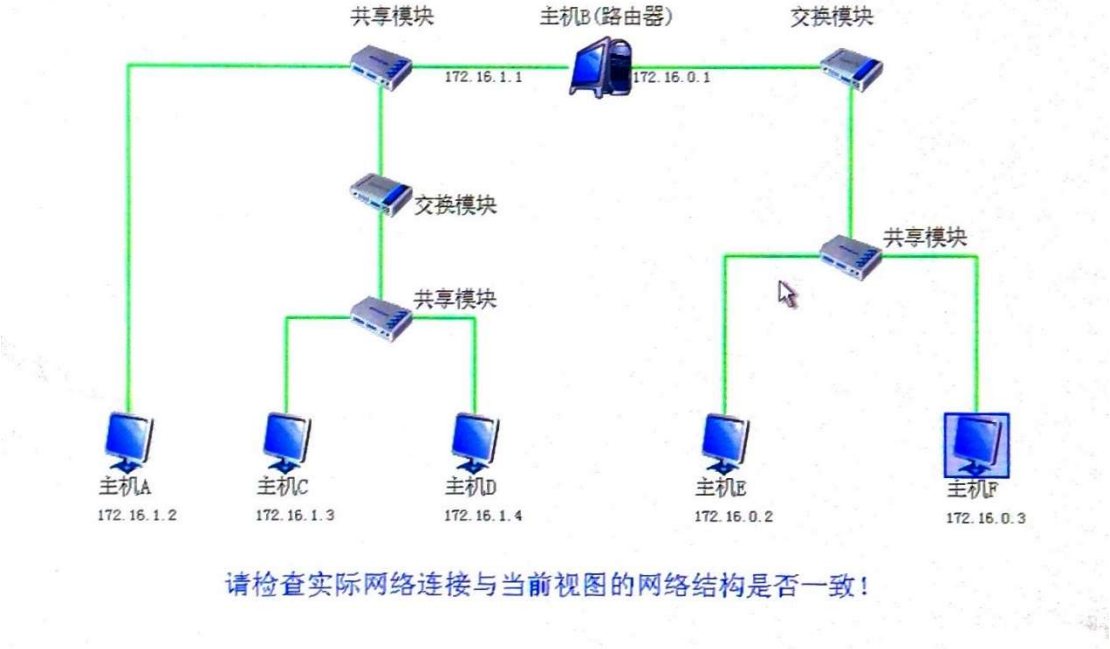
匹配路由表项的方法是将 IP 地址与路由表中的一个项目的“子网掩码”进行按位“与”操作，然后判断运算结果是否等于该项目的“目的地址”，如果等于，则匹配成功，否则，匹配失败。

路由选择模块的工作过程：



【实验步骤】

主机 B 启动静态路由服务（方法：在命令行方式下，输入“staticroute_config”）。 按照拓扑结构图连接网络，使用拓扑验证检查连接的正确性。



练习一：编辑并发送 IP 数据报

1. 主机 A 启动仿真编辑器，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：在其他所有字段填充完毕后计算并填充。

   IP 在计算校验和时包括那些内容？

   【说明】先使用仿真编辑器的“手动计算”校验和，再使用仿真编辑器的“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 计算校验和仅计算 IP 数据报首部的内容，而不计算数据部分。

2. 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。

3. 主机 A 发送第 1 步中编辑好的报文。
4. 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。

   发生了变化，变化的字段为以太网帧中的源 MAC 地址(变成了 B（E 所在子网的端口）的 MAC 地址即 F0-4D-A2-32-BB-AF)和目标 MAC 地址(变成了 E 的 MAC 地址即 00-E0-4C-C5-18-89)，IP 数据报中的 TTL 和首部校验和字段。MAC 地址发生了变化是因为 IP 数据报经过了路由器(B)的转发，需要设置新的首地址和源地址，TTL 是每过一个路由器自动递减的。

5. 将第 2 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。
6. 主机 B、E 重新开始捕获数据。
7. 主机 A 发送第 5 步中编辑好的报文。
8. 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。

   B 捕获到了主机 A 所发送的报文，E 没有捕获到，因为 TTL 的初始值为 1，在经过路由器后，TTL 递减为 0，遂丢弃。

练习二：特殊的 IP 地址

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：172.16.0.255。
校验和：在其他字段填充完毕后，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。
校验和：在其他字段填充完毕后，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 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	A、B、C、D、E、F
收到 IP 数据报 2	B、E、F

结合实验结果，简述直接广播地址的作用。

直接广播地址(IP 地址)的作用是对某一个特定的子网进行广播，本网收到的 IP 数据报受到目的 MAC 地址的影响。同时，若目的 MAC 地址没有设置成 B 或者广播地址，子网 172.16.0.0/24 将不再能够受到 IP 数据报。

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”设置为 FFFFFF-FFFFFF。
“目的 IP 地址”设置为 255.255.255.255。

(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，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	A、B、C、D
未收到主机 A 发送的 IP 数据报	E、F

结合实验结果，简述受限广播地址的作用。

受限广播地址(IP 地址)仅对本子网进行广播，即路由器会截止转发这个 IP 数据报，因此，最后只有和 A 同处于本子网的主机(A、B、C、D)收到了 A 发送的 IP 数据报。

3. 环回地址。

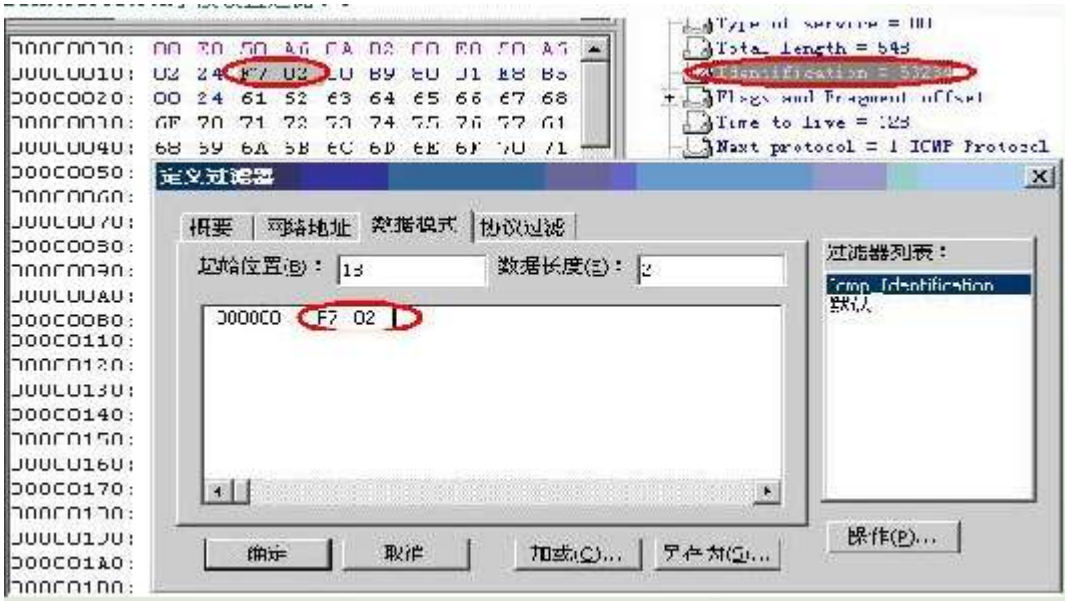
主机 F 重新启动协议分析器开始捕获数据并设置过滤条件（提取 IP 协议）。
主机 E ping 127.0.0.1。
主机 F 停止捕获数据。

- 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？

并没有，环回地址仅在主机内部转发，不会经过网卡进入子网。

练习三：IP 数据报分片

1. 在主机 B 上使用“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、E 停止捕获数据。主机 E 如下图所示，重新定义过滤条件（取一个 ICMP 数据包，按照其上层协议 IP 的 Identification 字段设置过滤）。



将 ICMP 的报文分片信息填入下表：

字段名称	分片序号 1	分片序号 1	分片序号 1
Identification 字段值	49237	49237	
More fragments 字段值	1	0	

Fragment offset 字段值	0	97	
传输的数据量	776	224	

分析表格内容，理解分片的过程。

5. 主机 E 恢复默认过滤器。主机 A、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、E 停止捕获数据。察看主机 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 1	分片序号 1
Identification 字段值	32876	32876	32876
More fragments 字段值	1	1	0
Fragment offset 字段值	0	97	194
传输的数据量	776	776	448

分片时，IP 数据报取不大于 MTU，以 8 字节为整数倍的最大整数+20（适配 Fragment offset），。可以得到单次最大的 IP 数据报长度为 796（20+776），单次片偏移为 97。除最后的片段外，其他片段的 More fragments 均置为 1。

8. 主机 B 上使用“开始\程序\网络协议仿真教学系统 通用版\工具\MTU 工具”恢复以太网端口的 MTU 为 1500 字节。

练习四：子网掩码和路由转发

1. 所有主机取消网关
2. 主机 A、C、E 设置子网掩码为 255.255.255.224,主机 B、D、F 设置子网掩码为 255.255.255.240。
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	
主机 C----主机 D	
主机 E----主机 F	

请问什么情况下两主机的子网掩码不同，却可以相互通信？

4. 主机 A 设置子网掩码为 255.255.255.252，主机 C 设置子网掩码为 255.255.255.254，用主机 A ping 主机 C（172.16.1.3）。 记录实验结果

	是否 ping 通
主机 A----主机 C	

【思考问题】

1. 试说明 IP 地址与硬件地址的区别。为什么要使用这两种不同的地址？
2. 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？
3. IP 数据报中的首部检验和并不检验数据报中的数据。这样做的最大好处是什么？坏处是什么？