华东师范大学计算机科学技术系上机实践报告

课程名称：计算机网络	**年级：**2022	**上机实践成绩：**
指导教师：洪道诚	**姓名：**朱宇笑	**创新实践成绩：**
实验名称：网际协议(IP)	**学号：**10225001410	**上机实践日期：**2023/12/8
座位编号：F	**组号：**6	**上机实践时间：**2 学时

一、 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

二、 实验设备

1. PC机
2. 仿真编辑器和协议分析器

三、 实验原理

本实验采用网络结构二，如下图所示

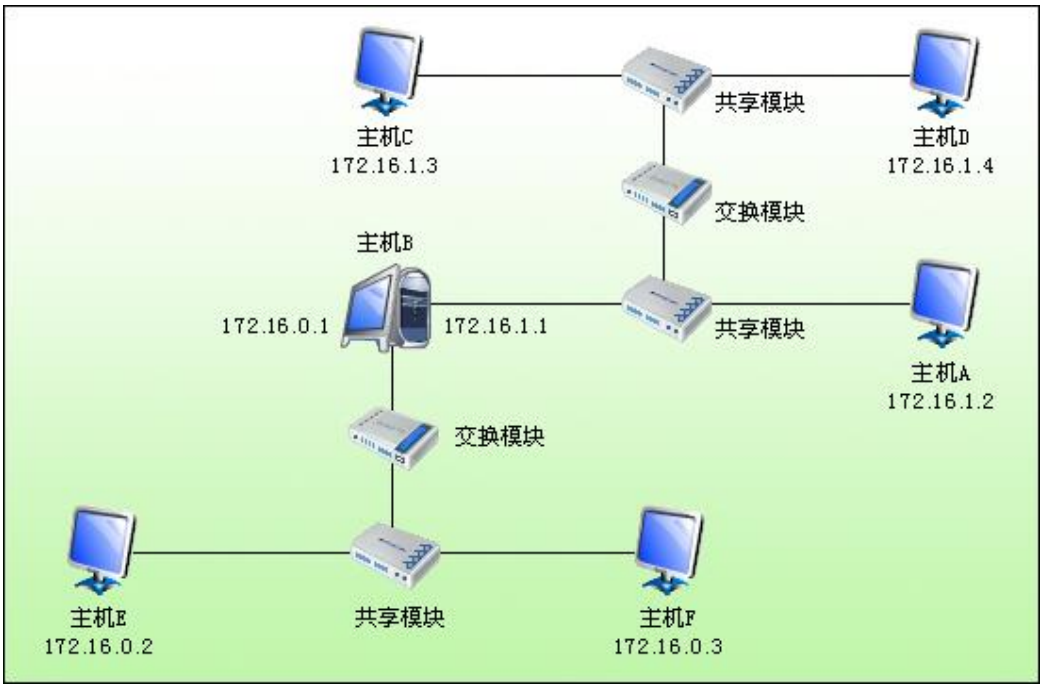


图1 网络结构二

（一）IP 协议简介

IP（网际协议）是 TCP/IP 协议族中最核心的协议，它负责将数据包从源点交付到终点。所有的 TCP、

UDP、ICMP 及 IGMP 数据都以 IP 数据报格式传输。IP 协议提供不可靠、无连接的数据报传送服务，即它对数据进行“尽力传输”，只负责将数据包发送到目的主机，不管传输正确与否，不做验证、不发确认、也不保证 IP 数据包到达顺序，将纠错重传问题交由传输层来解决。

（二）IP 地址及其表示方法

IP 地址是网际协议地址（InternetProtocoladdress）的简称。一个 IP 地址惟一地标识了 Internet 上的一台主机。通信时要使用 IP 地址来指定相应的目的主机。

1. 地址空间

地址空间就是协议所使用的地址总数。如果协议使用 N 位来定义地址，每一位可以有两种不同的值（1 或 0），那么地址空间就是 2^N。

IP 使用 32 位地址，这表示地址空间是 2^{32}，或 4294967296（超过 40 亿个）。从理论上讲，可以有超过 40 亿个设备连接到 Internet。但是，实际的数字要远小于这个数值。

2. IP 地址的表示方法

IP 地址有三种常用的表示方法：二进制表示方法、点分十进制表示方法和十六进制表示方法。

●二进制表示方法：

在二进制表示方法中，用一个 32 位的比特序列表示 IP 地址，为了使这个地址有更好的可读性，通常在每个字节（8 位）之间加上一个或多个空格做分隔。例如：

10000001000011100000011000011111

●点分十进制表示方法：

为了使 32 位地址更加简洁和更容易阅读，Internet 的地址通常写成用小数点把各字节分隔开的形式。每个字节用一个十进制数表示，这个数小于 256。例如：

129.14.6.31

●十六进制表示方法：

有时会见到十六进制表示方法的 IP 地址。每一个十六进制数字等效于 4 个位。例如：

0x810E061F

3. IP 地址的分类

IP 地址分成 5 类：A 类，B 类，C 类，D 类和 E 类。其中 A 类、B 类和 C 类地址是基本的 Internet 地址，是用户使用的地址，D 类地址用于广播，E 类地址为保留地址。

下图描述了 IP 地址的二进制表示方法的分类：

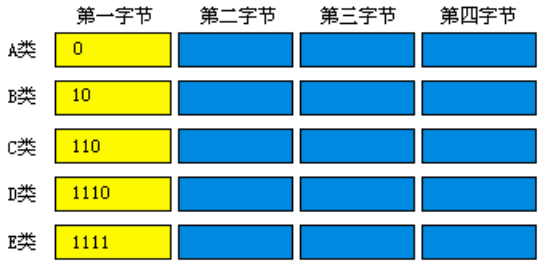


图 3-1 在二进制记法中找出 IP 地址的类别

下图描述了 IP 地址的十进制表示方法的分类：

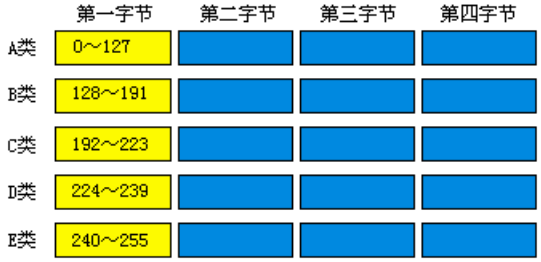


图 3-2 在点分十进制记法中找出 IP 地址的类别

4. 网络号和主机号

在分类编址的 A 类，B 类和 C 类地址中，IP 地址可划分为网络号（net-id）和主机号（host-id）。这两部分长度都是可变的，取决于地址的类型。下图给出了网络号和主机号所占的字节。应该注意的是，D 类地址和 E 类地址不划分网络号和主机号。

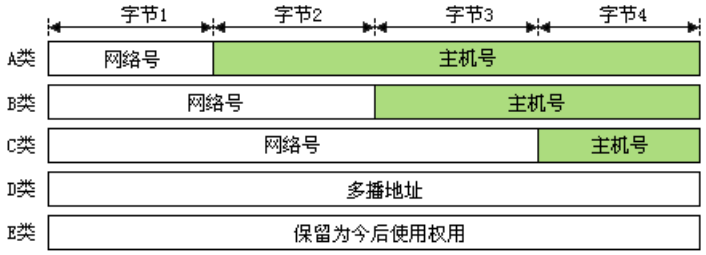


图 3-3 网络号和主机号

5. 地址类和地址块

分类编址将每一类地址都划分为固定数目的地址块，并且每一个地址块的大小都是固定的。

A 类地址共分为 128 个地址块，每个地址块都包含有 16777216 个地址。这表明要使用这类地址的机构一定是一个非常庞大的机构。但是，每个地址块中的地址数比机构的地址需求大的多，所以，在这类地址中，许多地址都被浪费了。

B 类地址共划分为 16384 个地址块，每个地址块都包含有 65536 个地址。这个地址数往往大于中等规模机构的地址需求，所以，在这类地址中，也有许多地址被浪费了。

C 类地址共划分为 2097152 个地址块，每个地址块都包含有 256 个地址。这类地址中的地址数对大多数机构来说是不够用的，因此许多机构不太愿意要这类地址。

D 类地址只有一个地址块。它用来进行多播。

E 类地址只有一个地址块。它是保留地址。

（三）特殊的 IP 地址

1. 特殊的 IP 地址

●网络地址：主机号为全“0”的 IP 地址不分配给任何主机，而是作为网络本身的标识。

例：主机 202.198.151.136 所在网络地址为 202.198.151.0。

●直接广播地址：主机号为全“1”的 IP 地址不分配给任何主机，用作广播地址，目的地址为直接广播地址的数据包传递给该网络中的所有节点（能否执行广播，则依赖于支撑的物理网络是否具有广播功能）。

例：202.198.151.136 所在网络的广播地址为 202.198.151.255。

●有限广播地址：32 位为全“1”的 IP 地址（255.255.255.255）称为有限广播地址，通常由无盘工作站启动时使用，希望从网络 IP 地址服务器处获得一个 IP 地址。

●主机本身地址：32 位全“0”的 IP 地址（0.0.0.0）称为主机本身地址。

●回环地址：127.0.0.1 称为回环地址，常用于本机上软件测试和本机上网络应用程序之间的通信地址。

2. 专用 IP 地址

随着 Internet 的飞速发展，IP 地址资源已经开始告急，专用 IP 地址的使用是解决 IP 地址紧缺的一种方法。原理是定义两类 IP 地址：

●全局 IP 地址：用于 Internet 上的公共主机；

●专用 IP 地址：仅用于专用网内部的本地主机。

公共主机和本地主机可以共存于同一网络并进行互访，而大多数路由器不转发携带专用 IP 地址的数据包。本地主机必须经网络地址转换服务器（NAT 或代理服务器）才能访问 Internet。专用 IP 地址为：

10.0.0.0-10.255.255.2551 个 A 类网络

172.16.0.0-172.31.255.25516 个连续的 B 类网络

192.168.0.0-192.168.255.255256 个连续的 C 类网络

（四）子网划分

为了便于网络的管理、提高系统的可靠性、改进系统性能、克服简单局域网的技术条件限制、通过设置不同访问权限来增强系统的安全保障，人们采用了划分子网的办法将网络进一步划分成独立的组成部分。

现在的主机都要求支持子网编址。不是把 IP 地址看成由单纯的一个网络号和一个主机号组成，而是把主机号再分成一个子网号和一个主机号。例如，把一个 B 类网络地址的 16 位主机号分成 8 位子网号和 8 位主机号如下图所示：

16 位	8 位	8 位
网络号	子网号	主机号

图 3-4 子网划分

这样就允许有 254 个子网，每个子网可以有 254 台主机。对 A 类和 B 类网络，许多管理员采用自然的划分方法，即以 8 位为单位划分子网地址和主机号。这样用点分十进制方法表示的 IP 地址就可以比较容易确定子网号。但是，并不要求 A 类或 B 类地址的子网划分都要以字节为分界限。子网对外部路由器来说隐藏了内部网络组织的细节。

主机除了知道 IP 地址以外，还需要知道 IP 中有多少位用于子网号，多少位用于主机号。这是通过使用一个称为“子网掩码”的 32 位值来完成的。其中值为 1 的位留给网络号和子网号，为 0 的位留给主机号。

给定 IP 地址和子网掩码以后，主机就可以确定 IP 数据包的目的是本子网中的主机、本网络中其它子网中的主机还是其它网络上的主机。

如果知道本机的 IP 地址，那么就知道它是否为 A 类、B 类或 C 类地址（从 IP 地址的高位可以得知），也就知道网络号和子网号之间的分界线。而根据子网掩码就可知道子网号与主机号之间的分界线。

子网掩码除了可以如 IP 地址一样用“点分十进制”方式表示外，还可以在 IP 地址后用一个斜线（/）后面写明子网掩码的位数的方法来表示。如：192.168.1.25/24 表示 IP 地址 192.168.1.25 的掩码为 255.255.255.0。

（五）IP 报文格式

IP 数据报格式如下图所示，它是由 IP 首部与数据组成的。IP 首部长度通常为 20 字节。如果含有选项字段，IP 首部长度将会大于 20 字节，但不会超过 60 字节。

<table>
<tr><td>版本号（4 位）</td><td>首部长度（4 位）</td><td>区分服务（8 位）</td><td colspan="2">总长度（16 位）</td></tr>
<tr><td colspan="3">标识（16 位）</td><td>标志（3 位）</td><td>偏移量（13 位）</td></tr>
<tr><td>生存时间（8 位）</td><td>高层协议类型（8 位）</td><td colspan="3">首部校验和（16 位）</td></tr>
<tr><td colspan="5">源 IP 地址（32 位）</td></tr>
<tr><td colspan="5">目的 IP 地址（32 位）</td></tr>
<tr><td colspan="5">IP 选项（如果有）</td></tr>
<tr><td colspan="5">数据</td></tr>
</table>

图 3-5IP 报文格式

在 IP 首部中各个字段的意义如下：

●版本号：这个字段定义了 IP 的版本。目前主流的是版本 4（IPv4），但它正逐渐地被版本 6（IPv6）所替代。

●首部长度：由于 IP 选项字段的存在，所以 IP 首部长度是可变的。该字段用 4 位来定义首部长度。将该值乘 4 可得到用字节表示的长度，所以 IP 首部长度为 20～60 个字节。

●区分服务：该字段以前叫做服务类型（在 RFC791 中定义），是由 3 位优先域、4 位服务类型域和 1 位未用位(该位必须置为 0)组成，其中 4 位服务类型分别代表：最小时延、最大吞吐量、最高可靠性和最小费

用。该字段在 RFC2474 中被重新定义,在新的定义中将该字段命名为区分服务，其中包含一个 6 位的区分服务码点(DSCP)字段和一个 2 位的未用位（CU）字段。如下图所示：

区分服务码点（6 位）	未用位（2 位）

图 3-6RFC2474 定义的区分服务字段

前 6 位的区分服务码点的值用来映射一个底层的服务，它决定了每一跳行为。在 RFC3168 中，将区分服务字段中的未用位字段定义为显示拥塞通告（ECN）字段，ECN 字段包括 2 个子字段，分别为：ECT 字段和 CE 字段，如下图所示：

区分服务码点（6 位）	ECT（1 位）	CE（1 位）

图 3-7RFC3168 定义的区分服务字段

ECN 字段用于指定发送数据的主机是否支持拥塞通告以及指示网络中是否有拥塞发生。ECN 通过两个子字段的不同值组合来做到这一点：

00：发送主机不支持 ECN。

01 或 10：发送主机支持 ECN。

11：路由器正在经历拥塞。

●总长度：该字段以字节为单位定义 IP 数据报的总长度（首部加上数据）。要得到 IP 上层数据的长度，只需从总长度中减去首部长度即可。

●标识：每一个 IP 数据包在发送时被给定特有的标识值。如果数据包必须被分割成碎片以适应支持小型数据包的网络，那么每一个碎片中都设置相同的标识号码。

●标志：标志由 3 位组成，第 1 位保留；第 2 位为不分片标志，表示此数据包不可以被分片；第 3 位为更多分片标志，表示在分片包之后还有分片，即此包不是最后分片。

●偏移量：如果数据包是一个分片包，该域指明了当前分片包在与其它分片包被重新组装成一个单独数据包时，应该位于数据包的什么位置。该域的值以 8 字节为单位。

●生存时间：该字段表明数据包保存的生存时间，单位为秒，在实际的应用中，生存时间是按照数据包经过路由器的跳数计算的。通常生存时间的值是 32、64、128。

●高层协议类型：该字段定义了使用 IP 层服务的较高层协议。一个 IP 数据报能封装来自诸如 TCP、UDP、ICMP 和 IGMP 等较高层协议的数据。

●首部校验和：IP 首部校验和只对首部内容进行错误检测，并不包括数据包的其它内容。校验和采用 16 位反码求和的算法。

●源 IP 地址：该字段定义了源主机的 IP 地址。在 IP 数据包从源主机传送到目的主机期间，该字段保持不变。

●目的 IP 地址：该字段定义了目的主机的 IP 地址。在 IP 数据报从源主机传送到目的主机期间该字段保持不变。

●IP 选项：这个字段是可选项。它们通常用于网络测试和调试。虽然可选项不是 IP 头部所必需的部分，但要求 IP 软件能够处理它们。目前，这些选项定义如下：

(1)安全和处理限制（用于军事领域）；

(2)记录路径（让每个路由器记下它的 IP 地址）；

(3)时间戳（让每个路由器都记下它的 IP 地址和时间）；

(4)宽松的源站选路（为数据报指定一系列必须经过的 IP 地址）；

(5)严格的源站选路（与宽松的源站选路类似，但是要求只能经过指定的这些地址，不能经过其它的地址）。

（六）IP 封装

IP 数据报直接封装到数据链路层帧中，其封装方法如下图所示：

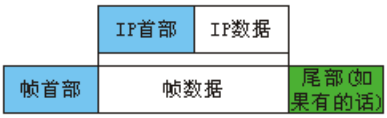


图 3-8IP 封装

（七）IP 数据报分片

数据包可能通过多个不同的网络。每一个路由器把收到的帧进行拆装，再进行处理，然后又封装成另一个帧。收到帧的格式与长度取决于这个帧刚刚经过的物理网络所使用的协议。发送出去的帧格式与长度则取决于这个帧将要经过的物理网络所使用的协议。例如，如果路由器把以太网连接到一个广域网，那么这个路由器收到的帧是以太网的格式，而发送的帧是广域网的格式。

1. 最大传送单元（MTU）

不同的网络所能传送的数据包的最大长度是不同的，这个最大长度叫做最大传送单元（MTU），这是由网络所使用的硬件与软件所决定的。每种网络的数据链路层都有自己的帧格式，其中有一个字段是“数据字段最大长度”。当数据包封装成帧时，数据包的总长度必须小于这个数据字段最大长度，如下图所示。

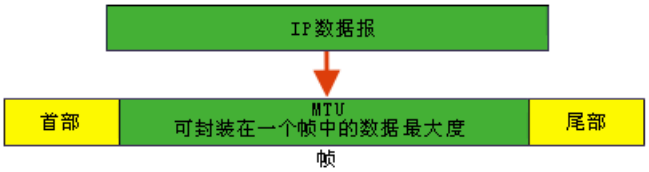


图 3-9MTU

对于不同的物理网络协议，MTU 的值是不同的。下表给出了不同协议的 MTU 值。

表 3-1 不同网络的 MTU 值

协议	MTU	协议	MTU
超级通道（Hyperchannel）	65535	以太网	1500
令牌环（16Mbps）	17914	X.25	576
令牌环（4Mbps）	4464	PPP	296
FDDI	4352	——	——

为了使 IP 协议与物理网络无关，IP 协议不考虑底层网络的 MTU，只是规定 IP 数据包的最大负载长度为 65535 字节。对于物理网络，如果数据包的长度超过了 MTU，就要把数据包进行分割，使它们能够通过这些网络，这就叫做分片。源主机的传输层会自动对数据包进行分片工作，把数据包划分成 IP 协议和数据链路层都可接受的大小。

当数据包被分片时，每一个数据包片有它自己的首部，其中大部分的字段都是重复的，但有些是不同的。如果已经分片的数据包要经过更小 MTU 的网络，那么这些已经分片的数据包还可再进行分片，数据包在到达最后终点之前可以经过多次的分片。

数据包可以被源主机或在其路径上的路由器进行分片。但是数据包的重装却只能在目的主机上进行。由于被分片的数据包可能会通过不同的路由到达目的主机，所以应当在最后的目的主机上进行重装。

当数据包被分片时，首部中的一些字段会被复制到所有的分片中（选项字段可以被复制，也可不被复制）。有三个字段是与数据包分片相关的，这三个字段是：标识字段、标志字段和偏移量字段。当然，不管是否进行分片，校验和的值总是要重新计算的。

对于最大传输单元（MTU）还可以理解为某层协议报文可携带数据的最大长度，对于不同协议，对应的 MTU 可能会有不同的值和计算方法。如我们常说的“以太网 MTU 为 1500”，说的是以太网 MAC 帧可封装的最大数据长度，其只包含 IP 报头及其上层协议数据的总长度。对于 IP 协议的 MTU 值应为 65535-20，也只是说一个 IP 数据报（包含 IP 包头的长度和 IP 上层协议数据的长度），最多可以携带 65535 个字节的数据。

2. 与分片有关的字段

与数据包的分片和重装有关的三个字段是：标识字段、标志字段和偏移量字段。

●标识：IP 数据包的标识字段值与源 IP 地址惟一地确定了一个数据包。IP 协议使用一个计数器来保证每个数据包标识的惟一性。当 IP 协议发送数据包时，就把这个计数器的当前值复制到标识字段中，并把这个记数器的值加 1。当数据包被分片时，标识字段的值就复制到所有的分片中。这样所有的分片具有相同的标识。这个标识号在终点重装数据包时很有用。终点会将所有具有相同标识号的分片组装成一个数据包。

●标志：这是一个长度为 3 位的字段。第一位保留。第二位是不分片位。若这个位为 1，就表示不能把该数据包进行分片。若无法把这个数据包通过任何可用的物理网络进行转发，就丢弃这个数据包，并向源主机发送 ICMP 差错报文（关于 ICMP 差错报文，参见实验 4）。若这个位为 0，则在需要时可把这个数据包进行分片。第三位是还有分片位。若这个位是 1，则表示这个数据包不是最后的分片，在这个分片后面还有其它分片。若这个位是 0，则表示这是最后的分片。标志字段如下图所示：

图 3-10 标志字段

●偏移量：偏移量字段表示一个分片在整个数据包中的相对位置。以 8 字节为度量单位。下图表示具有 4000 字节长度的数据包被划分为三个分片。在原始数据包中的数据编号是 0～3999。第一个分片携带的数据是字节 0～1399。对于这个数据包，偏移量是 0 / 8＝0。第二个分片携带的数据是字节 1400～2799；对于这个数据包，偏移量是 1400 / 8＝175。最后，第三个分片携带的数据是字节 2800～3999。对于这个数据包，偏移量是 2800 / 8＝350。如下图。

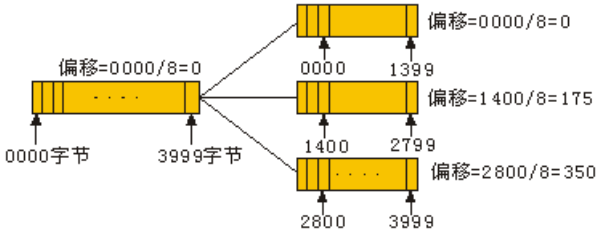


图 3-11 分片举例

偏移量字段的长度只有 13 位，它不能表示超过 8191 的字节数，所以偏移量是以 8 字节为单位的。因此，把数据包进行分片的主机或路由器必须选择一个能够被 8 整除的长度来为数据包分片。

（八）IP 数据报校验和

大多数 TCP/IP 协议族中的协议采用的差错检测方法是校验和。校验和能够识别数据包在传输过程中是否受到损伤。校验和是在数据包上附加的信息。

在发送端先计算校验和，并把得到的结果与数据包一起发送出去。接收端对整个数据包重复进行同样的计算。若得到的结果正确则接受这个数据包；否则就把它丢弃。

1. 在发送端计算校验和

在发送端，将数据包按 16 位长度分段。把这些段用反码算数运算相加，将相加后得到的和再取反码就得出了校验和。

2. 在接收端计算校验和

接收端把收到的数据包按 16 位长度分段，并把这些段相加。把得到的和取反码。若结果为 0，则接受这个数据包；否则就拒绝这个数据包。

下图用图解的方法描述了发送端和接收端计算校验和的过程。

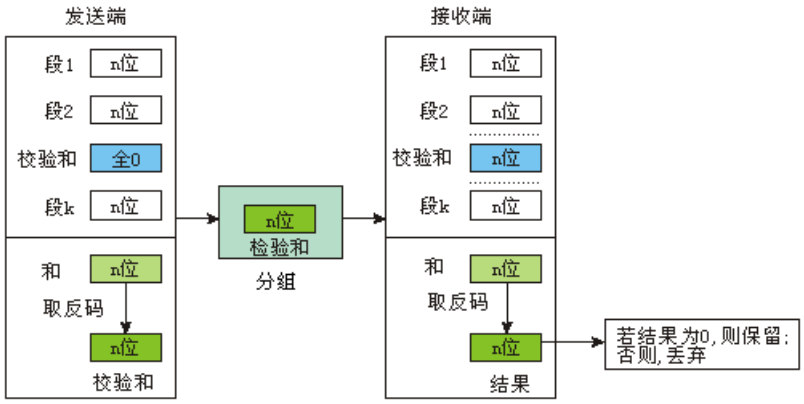


图 3-12 校验和的概念

3. IP 数据包中的校验和

IP 数据包的校验和只校验 IP 首部部分而不校验 IP 数据部分。这是因为所有将数据封装在 IP 数据报中的高层协议，都有覆盖整个数据包的校验和。因此，IP 数据报的校验和就不必再检验所封装的数据部分。其次，每经过一个路由器，IP 数据包的首部就要改变一次，但数据部分不改变。因此若校验和包含数据部分，这就意味着路由器要花费很多时间计算没有改变的数据部分的校验和。

（九）交付与转发

所谓交付，是指在网络层的控制下，一个数据包被底层网络处理的方式。例如，面向无连接的服务和面向连接的服务，以及直接交付和间接交付等。

所谓转发是指数据包被交付到下一站的方式。

1. 交付

网络层控制底层物理网络对数据包的处理过程，这种过程叫做交付。在交付过程中有几个重要概念，即连接类型，直接与间接交付。

2. 连接类型

数据包在网络层的交付可以用面向连接的服务或无连接服务来完成。

(1)面向连接服务

在面向连接服务的情况下，本地网络层协议在发送数据包之前先要和远地网络层协议建立一条连接。当连接建立后，一系列的数据包就从源点一个接一个地发送到终点。在这种情况下，各个数据包之间存在着一种关系。它们都沿着同一条路径按序发送。一个数据包与走在它前面的数据包以及与走在它后面的数据包在逻辑上是连接在一起的。若报文中的所有数据包都已被交付，连接就终止了。

在面向连接服务的情况下，对从同一个源点到同一个终点的一系列数据包来说，其路由的确定只需进行一次。路由器不需要对每一个单个的数据包重新计算路由。

(2)无连接服务

在无连接服务的情况下，网络协议独立地对待每一个数据包，而每一个数据包与任何其它数据包都没有关系。一个报文中的各数据包到它们的终点可以走相同的路径也可以走不同的路径。在无连接服务的情况下，对一个数据包的路由是由每一个路由器单独地确定。IP 协议是无连接协议，它提供无连接服务。

3. 直接交付与间接交付

把一个数据包交付到它最后的终点有两种方式：直接交付和间接交付。

(1)直接交付

在直接交付的情况下，数据包的最后终点是与交付者连接在同一个网络上的主机。当数据包的源点和终点都在同一个物理网络上时，或者交付是在最后一个路由器与目的主机之间进行时，就为直接交付，如下图所示。

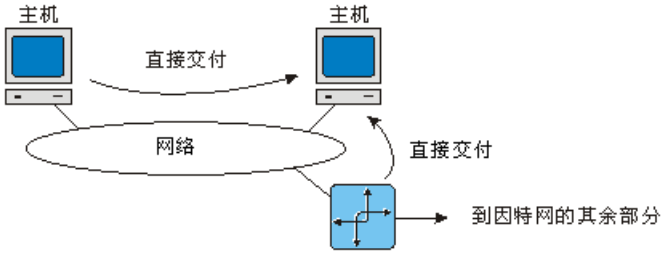


图 3-13 直接交付

发送端很容易确定交付是否为直接交付。发送端可以提取出终点的网络地址（使用掩码），并与它所连接的网络的网络地址相比较。若匹配，交付就是直接的。

在直接交付时，发送端使用目的 IP 地址找出目的物理地址。然后把目的 IP 地址和目的物理地址一起交付给数据链路层，以便进行实际的交付。这个过程叫做把 IP 地址映射到物理地址。地址解析协议（ARP）可以动态地把 IP 地址映射到相应的物理地址。

(2)间接交付

如果目的主机与交付者不在同一个网络上，数据包就要进行间接交付。在间接交付时，数据包从一个路由器传送到另一个路由器，直到这个数据包到达与最后的终点连接在同一个网络上的路由器为止。如下图所示。

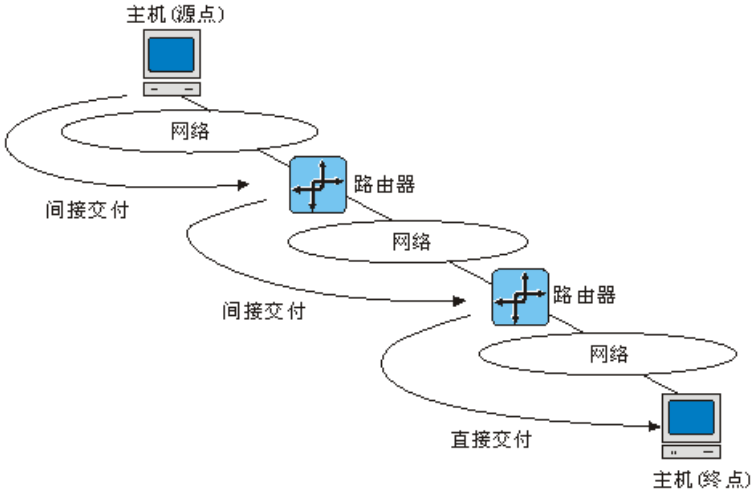


图 3-14 间接交付

交付永远包括一个直接交付，以及零个或多个间接交付。最后的交付就是直接交付。

在间接交付中，发送端使用目的 IP 地址和路由表来找出下一个路由器的 IP 地址。然后使用 ARP 协议找出下一个路由器的物理地址。在直接交付时，地址的映射是在终点的 IP 地址与终点的物理地址之间进行的。在间接交付时，地址的映射是在下一个路由器的 IP 地址与下一个路由器的物理地址之间进行的。

4. 转发

转发表示把数据包放到去终点的路由上。进行转发就要求主机或路由器装有路由表。当主机有数据包要发送时，或路由器收到数据包要进行转发时，就要查找路由表，以便找出到达最后终点的路由。但是，这种简单的转发方法，在今天的互联网中已经变得不可能了，因为路由表中的项目数已使得路由表的查找效率非常低。

5. 转发技术

使用一些转发技术可以减小路由表的大小，同时还能够处理一些安全问题。下面为三种简单的转发技术。

(1)下一跳方法

下一跳方法就是在路由表中只保留下一跳的地址，而不是保留完整路由信息。下图所描绘的例子说明了路由表如何被简化。

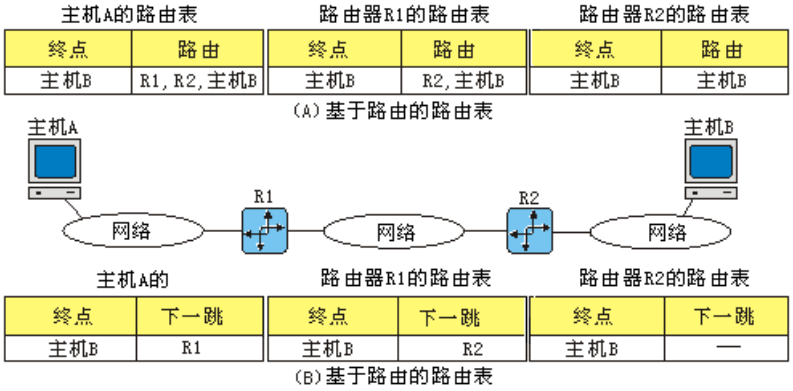


图 3-15 下一跳方法

(2)特定网络方法

特定网络方法不是对连接在同一个物理网络上的所有主机都设置一个路由表项，而是仅用一个路由表项来代表这个目的网络本身的地址。换言之，这种技术把连接在同一个网络上的所有主机看成是一个路由表项。如下图所示：

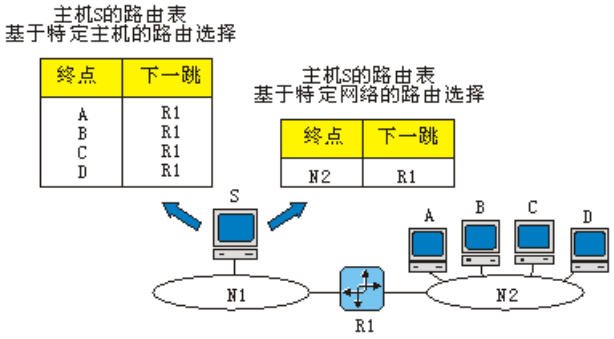


图 3-16 特定网络方法

(3)特定主机方法

特定主机方法将目的主机地址在路由表中全部给出。这种方法与特定网络方法的思想相反。这是用牺牲效率来换取其它一些优点的方法。虽然把主机地址放在路由表中会降低效率，但有时管理员还是想对路由选择作出更多的控制。如下图所示：

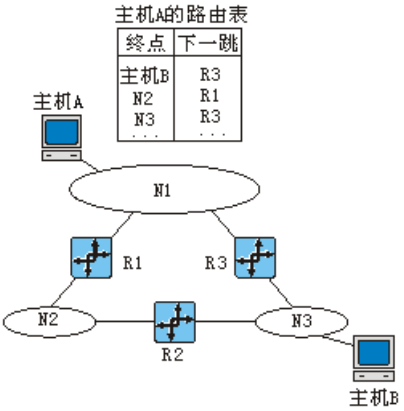


图 3-17 特定主机方法

（十）路由选择

路由选择涉及的问题是创建和维护路由表。

1. 静态和动态路由选择

主机或路由器要转发 IP 数据包就要有一个路由表，并给每一个终点或一组终点设置一个路由表项。路由表可以是静态的，也可以是动态的。

(1)静态路由表

静态路由表中的路由信息是由管理员手动设置的。管理员把到达每一个终点的路由输入到路由表中。路由表的更新由管理员手动完成。

静态路由表用在不会经常变动的小型互联网中，或用在故障查找的试验互联网中。在大的互联网中很少使用静态路由表。

(2)动态路由表

动态路由表使用一种动态路由选择协议，如 RIP、OSPF（关于这两个协议，请参考实验十六，实验十七）。当网络中发生变化时，动态路由选择协议就更新所有路由器中的路由表。

为了有效地交付 IP 数据包，规模较大的网络一般使用动态路由表。

2. 路由表

下图给出了路由表中常用的一些列：

掩码	网络地址	下一跳地址	接口号	标志	引用计数	使用
……	……	……	……	……	……	……

图 3-18 路由表中常用的列

●掩码：这列定义应用到路由表项的掩码。

●网络地址：这列定义数据包要交付到的网络地址。在特定主机路由选择中，这个字段定义目的主机的地址。

●下一跳地址：这列定义了数据包要交付到的下一跳路由器的地址。

●接口：这列指出接口的名字。

●标志：这列定义了五个标志：U（Up，工作），G（网关），H（特定主机），D（因改变路由而增加的）和 M（因改变路由而修改的）。

路由选择过程如下图所示：

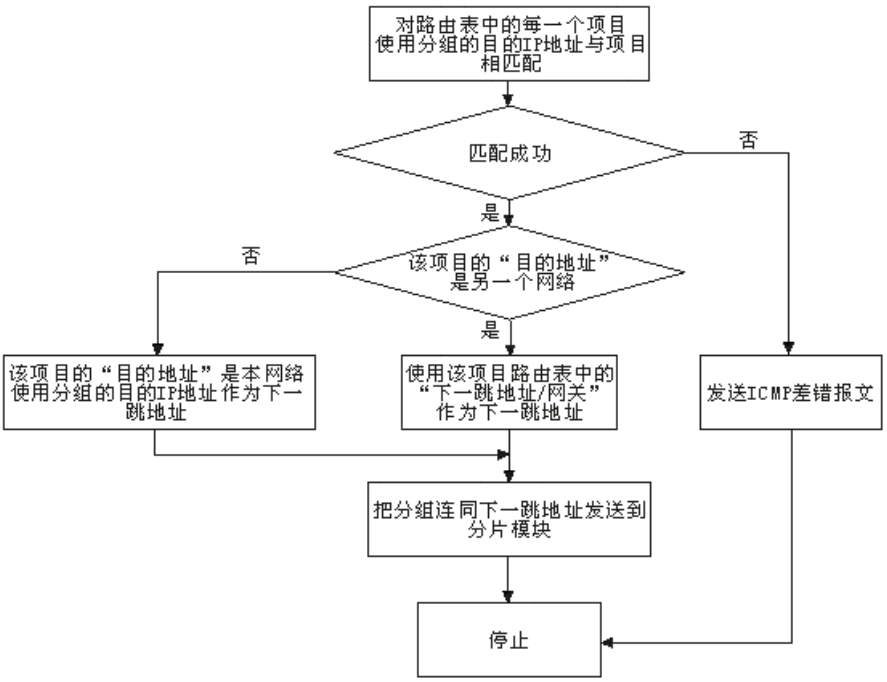


图 3-19 路由表使用过程

（十一）协议栈实现代码解析

本实验将通过对安装目录 JLCSS\ExpCNC\Work\NPL\ExpNPL_student\netproto_ip_student\netproto_ip_student 下的 netproto_ip_student.h、netproto_ip_shudent.c 和安装目录 JLCSS\ExpCNC\Work\NPL\ExpNPL_student\netproto_ip_student\netproto_iproute_student 下的 netproto_iproute_student.h、netproto_iproute_student.c 四个文件进行编码，完成协议栈中 IP 协议的实现。

netproto_ip_student.h 和 netproto_ip_shudent.c 文件用于实现 IP 数据包发送和接收。其中，netproto_ip_student.h 文件中定义了 IP 协议实现相关数值以及 IP 的负载内容、负载长度，关键代码如下所示：

```
#defineIP_VERSION4
#defineIP_HEADERLEN5
#defineIP_TTLNETP_TTL
#defineIP_DSNETP_DS
#defineIP_CUS_PROTO93//IP 自定义高层协议
#defineIP_DEST_ADDR"0.0.0.0"


#definePAYLOAD_DATA"Hello,World!"
#definePAYLOAD_LENsizeof(PAYLOAD_DATA)
```

这段代码定义了 8 个宏，他们代表的含义如下表所示：

表 3-2netproto_ip_student.h 中定义的宏

宏	值	描述
IP_VERSION	4	定义 IP 包头中“版本号”字段的值，必须为 4
IP_HEADERLEN	5	定义 IP 包头中“首部长度”字段值，一般为 5
IP_TTL	NETP_TTL	定义 IP 包头中“生存时间”字段值，默认为 128
IP_DS	NETP_DS	定义 IP 包头中“区分服务”字段值，默认为 0
IP_CUS_PROTO	93	定义 IP 包头中“高层协议类型”字段值，该值为自定义数值，学生可以更改
IP_DEST_ADDR	″0.0.0.0″	定义 IP 请求数据包头中“目的 IP 地址”字段值
PAYLOAD_DATA	″Hello,World!″	自定义 IP 负载内容
PAYLOAD_LEN	sizeof(PAYLOAD_DATA)	自定义 IP 负载的长度

在实验的编码过程中，应该使用这些宏对相应的变量进行赋值。

netproto_ip_shudent.c 文件是协议栈中 IP 数据包发送和接收的实现部分，其中定义了 2 个函数。下面介绍这些协议栈的实现部分。

函数 netp_ip_output_student 的功能是构造并发送一个 IP 数据包，其高层协议为自定义协议类型，负载内容为自定义负载。这个函数的编码工作需要由学生完成。

当有数据到达本机网络接口时，函数 netp_ip_input_student 将被调用，并传递给这个函数原始数据。在该函数中，需要判断一些条件值来确定接收到的数据包为自定义 IP 数据，如果是自定义 IP 数据包，则输出负载内容，如果不是，则返回 NETP_PUSH_TO_LWIP 交给协议栈继续处理。

netproto_iproute_student.h 和 netproto_iproute_shudent.c 文件用于实现 IP 路由表的管理。其中 netproto_iproute_student.h 文件的内容与 netproto_ip_student.h 相似，只是添加了 netp_create_iproute_table() 和 display_iproute_table()函数的声明。

netproto_iproute_shudent.c 文件是协议栈中 IP 路由表的管理的实现部分，其中定义了 1 个全局数组和

5 个函数。

全局数组 iproute_table 用来存储 IP 路由表，数组元素为 netp_iproute_table_item 结构对象，netp_iproute_table_item 结构的定义如下：

```
structnetp_iproute_table_item{
structip_addrdest_network;
structip_addrnetmask;
intinterface;
intflag;
};
```

函数 display_iproute_table 的功能是显示 IP 路由表的内容，该函数功能已经完成，学生不需要修改。

函数 netp_create_iproute_table 完成 IP 路由表的创建，该函数需要学生完成，实现 IP 路由表的创建。

函数 query_iproute 完成 IP 路由表的查询功能，该函数需要学生完成，实现 IP 路由表的查询。

函数 netp_iproute_output_student 通过查询 IP 路由表完成 IP 数据包的发送功能。该函数功能已经完成，学生不需要修改。

函数 netp_iproute_input_student 处理输入数据包，显示负载内容，该函数功能已经完成，学生不需要修改。

在编码过程中可能会设计到一些结构体、宏和函数，下表是对他们进行和介绍：

表 3-3 实验涉及的结构体和函数

结构体/函数	声明或定义	描述

structnetp_ip_header	structnetp_ip_header{
	u8_theaderlen:4;
	u8_tversion:4;
	u8_tdiff_services;
	u16_ttotal_length;
	u16_tidentification;
	u16_tflags_offset;
	u8_ttime_to_live;
	u8_tprotocol;
	u16_theader_checksum;
	structip_addrsource_address;
	structip_addrdestination_address;
	};
		ipv4 包头结构

structin_addr	structin_addr{
	u32_ts_addr;
	};
		32 位地址

structnetp_eth_header	structnetp_eth_header{
	u8_tdest_address[ETH_ADDRESS_LEN];
	u8_tsour_address[ETH_ADDRESS_LEN];
	u16_ttype;
	};
		以太网帧头结构

IP_HEADER_LEN	#defineIP_HEADER_LEN20	IP 包头长度
PAYLOAD_DATA	#definePAYLOAD_DATA"Hello,World!"	IP 负载内容
PAYLOAD_LEN	#definePAYLOAD_LENsizeof(PAYLOAD_DATA)	IP 负载长度
ETH_HEADER_LEN	#defineETH_HEADER_LEN14	以太网帧头长度
netp_current_ip_addr	u32_tnetp_current_ip_addr();	获取当前正在使用的网络接口的 IP 地址
htons	u16_thtons(u16_tn);	将 16 位数值由主机字节序转换为网络字节序
inet_addr	u32_tinet_addr(constchar*cp);	将 ASCII 编码的 Internet 地址转

结构体/函数	声明或定义	描述
		换成为网络字节序地址
inet_chksum	u16_tinet_chksum(void*dataptr,u16_tlen)	计算校验和
netp_ip_output	err_tnetp_ip_output(void*buffer,intbuff_len, intadapterID)	发送 IP 数据包，需要构造 IP 头部

（十二）各模块推荐流程

1. IP 数据包发送流程

编码实现 IP 数据包发送推荐使用如下流程：

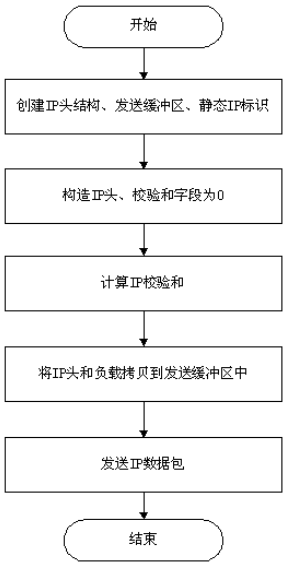


图 3-20IP 数据包发送推荐流程

2. 输入 IP 数据包处理流程

编码实现处理 IP 输入数据包推荐使用如下流程：

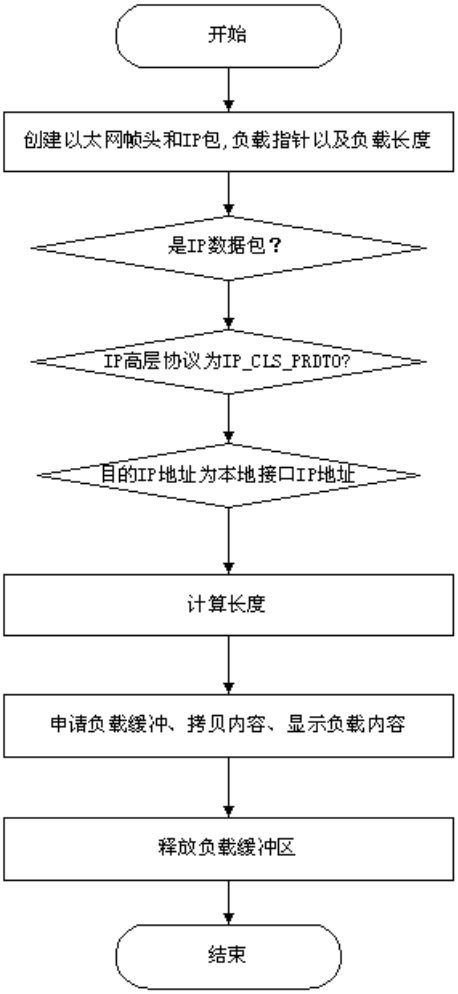


图 3-21 处理 IP 输入数据包推荐流程

3. IP 路由表创建流程

编码实现 IP 路由表创建推荐使用如下流程：

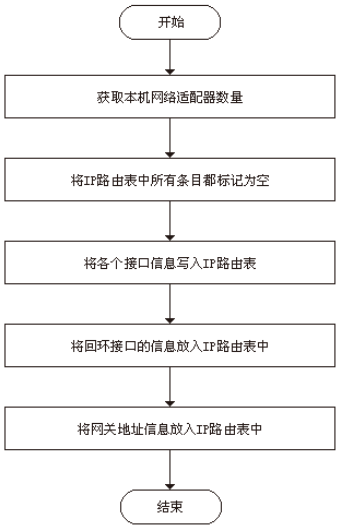


图 3-22IP 路由表创建推荐流程

4. IP 路由表查询流程

编码实现 IP 路由表查询推荐使用如下流程：

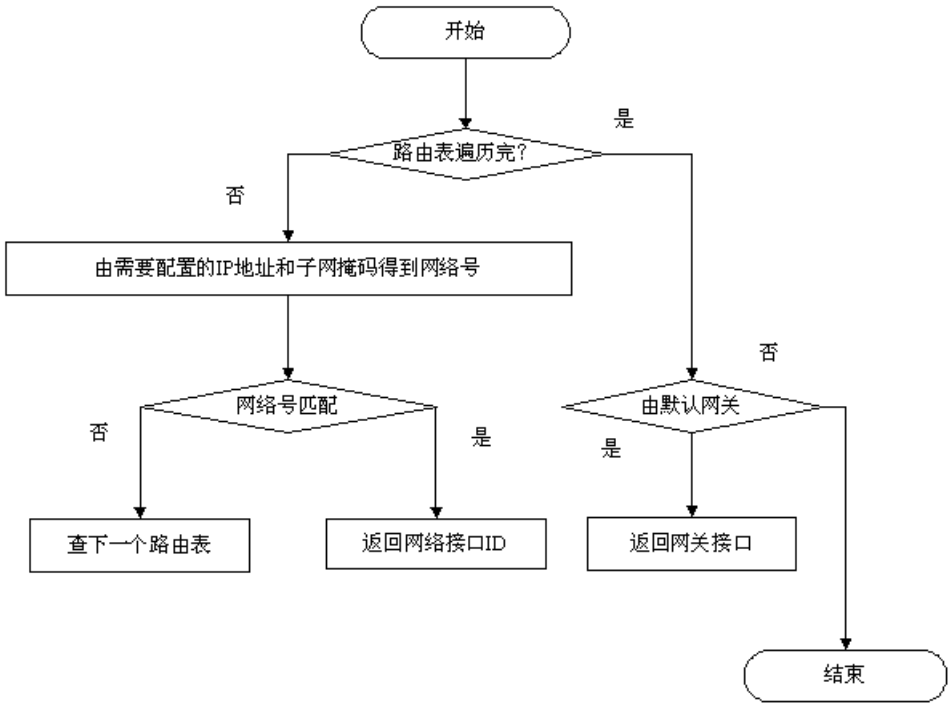


图 3-23IP 路由表查询推荐流程

四、 实验步骤

练习 1 编辑并发送 IP 数据报

首先按照附录 A 关于网络拓扑结构二的要求为每组的 A~F 各主机设置 IP 地址、子网掩码、默认网关等参数。

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。

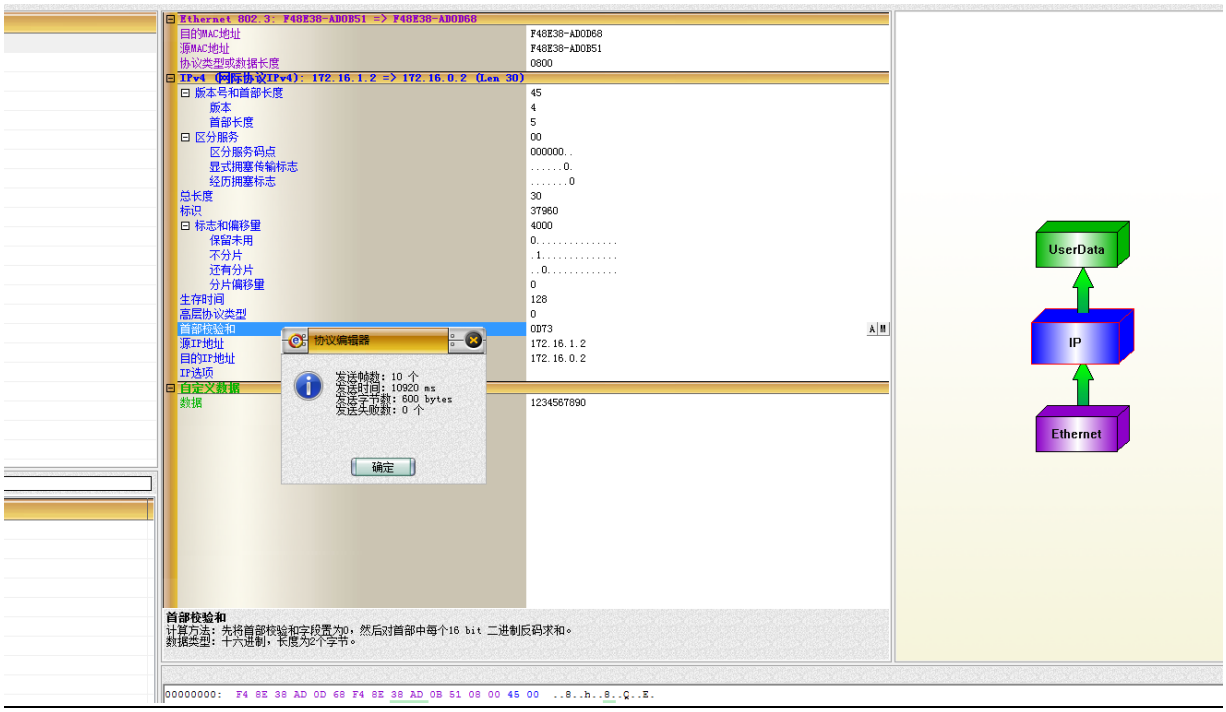
源 IP 地址：主机 A 的 IP 地址（172.16.1.2）。

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。



●IP 在计算校验和时包括哪些内容？

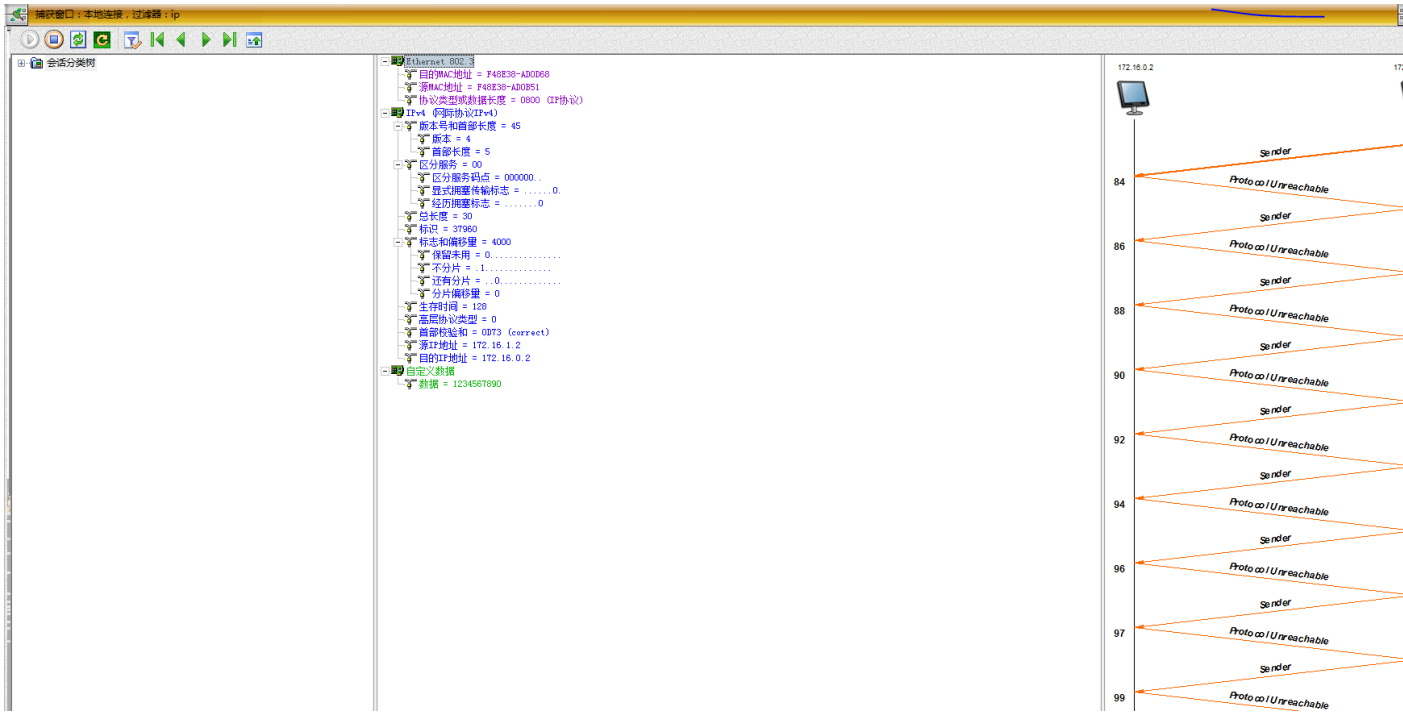
答：IP 在计算校验和时只检验数据报的首部，而不包括数据部分。

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。

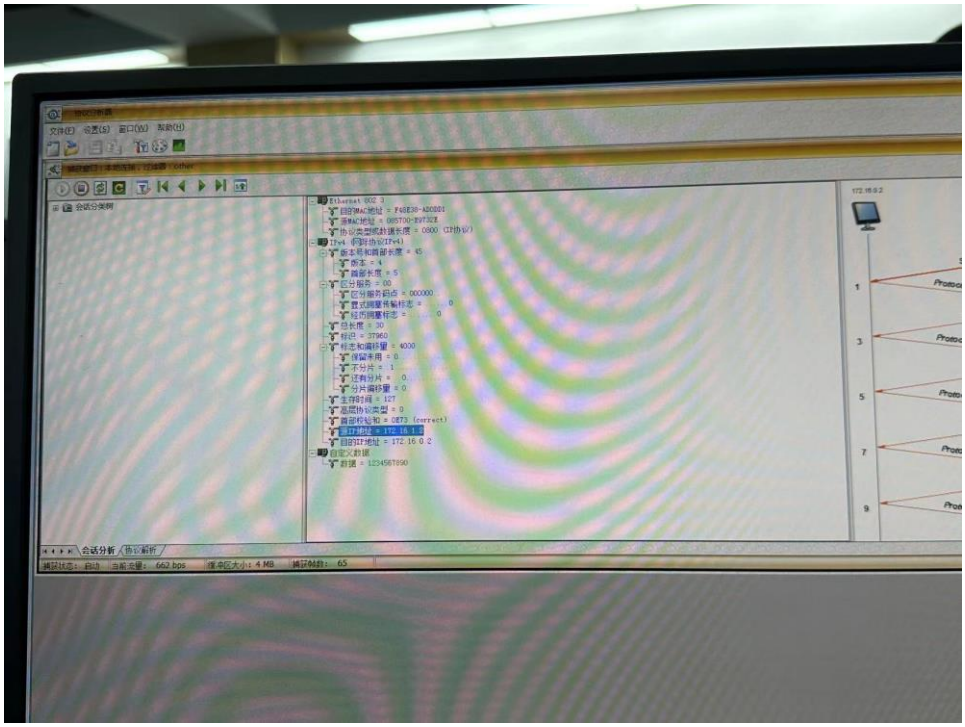
4. 主机 A 发送第 1 步中编辑好的报文。

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：

主机 B：



主机 E:



●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。

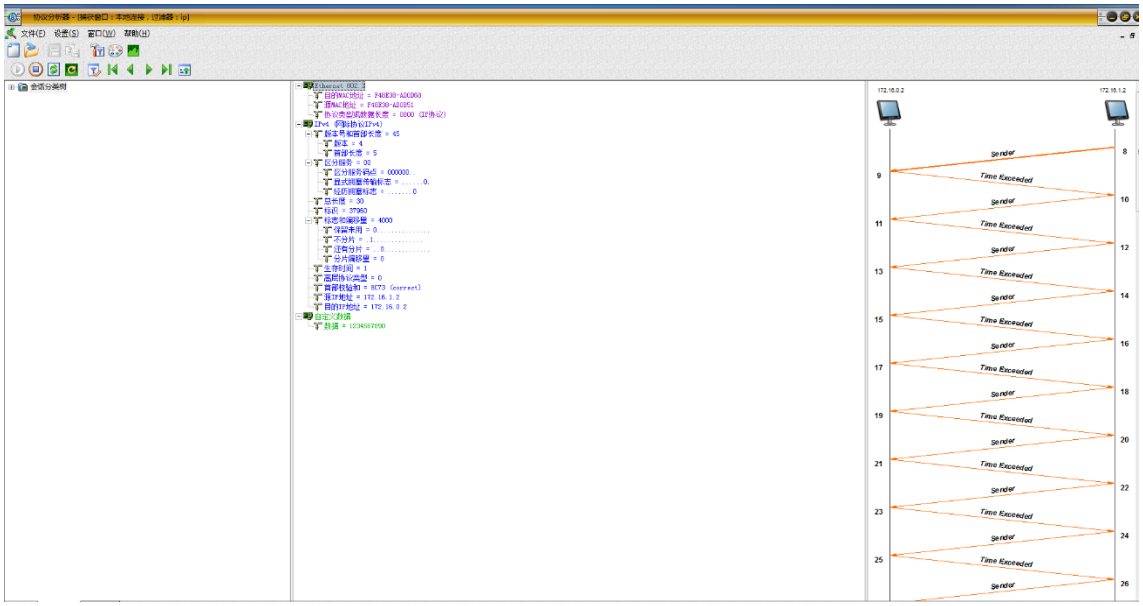
答：报文数据发生变化：TTL 由 128 变为 127，校验和由 0D73 变为 0E73。
原因：经过一次路由器，数据报的生存时间就会减一；内容发生变化，因此校验和发生改变。

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。

答：主机 B 能收到，主机 E 收不到。因为 A、E 处于不用的子网内，B 充当了路由器的角色，当报文经过主机 B 后 TTL 减 1 变为 0，此报文之后将被丢弃，因此 E 收不到报文。

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. 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。

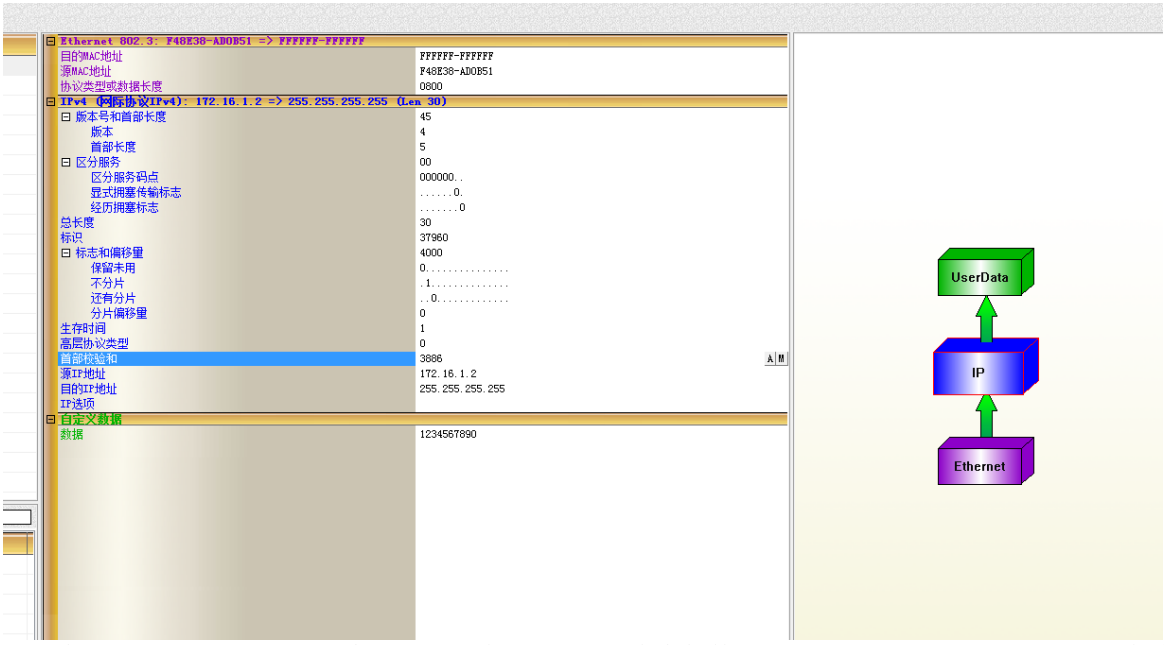
源 MAC 地址：A 的 MAC 地址。

源 IP 地址：A 的 IP 地址。

目的 IP 地址：255.255.255.255。

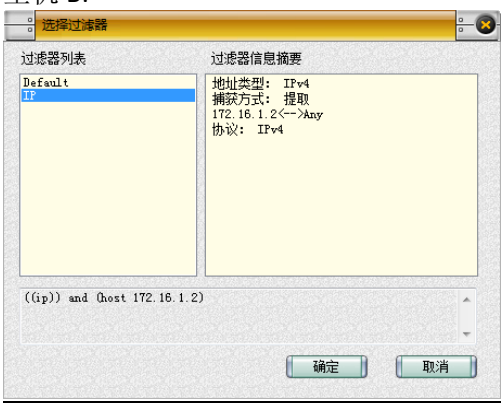
自定义字段数据：填入大于 1 字节的用户数据。

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）。

主机 B:



(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

表 3-5 实验结果

	主机号
收到主机 A 发送的 IP 数据报	B、C、D
未收到主机 A 发送的 IP 数据报	E、F

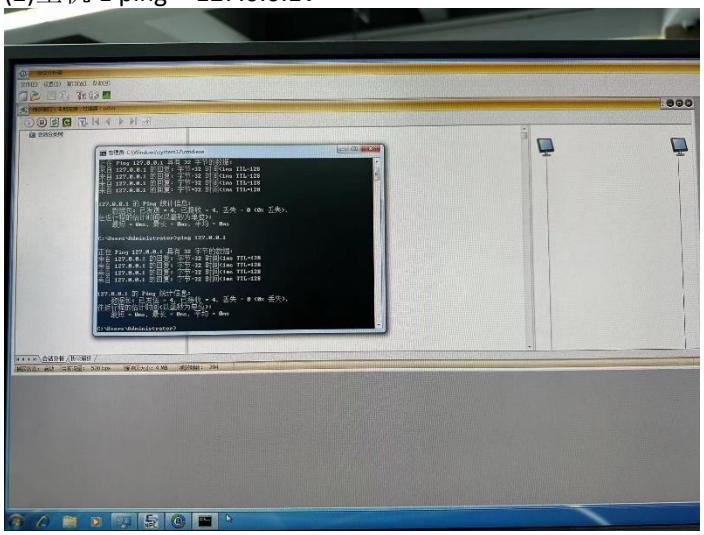
●结合实验结果，简述受限广播地址的作用。

答：用于主机配置过程中 IP 数据报的目的地址.这种也称之为本地广播地址，它的目标地址为 255.255.255.255. 意思是只在本网络进行广播，而不会被路由器转发到其他网络。

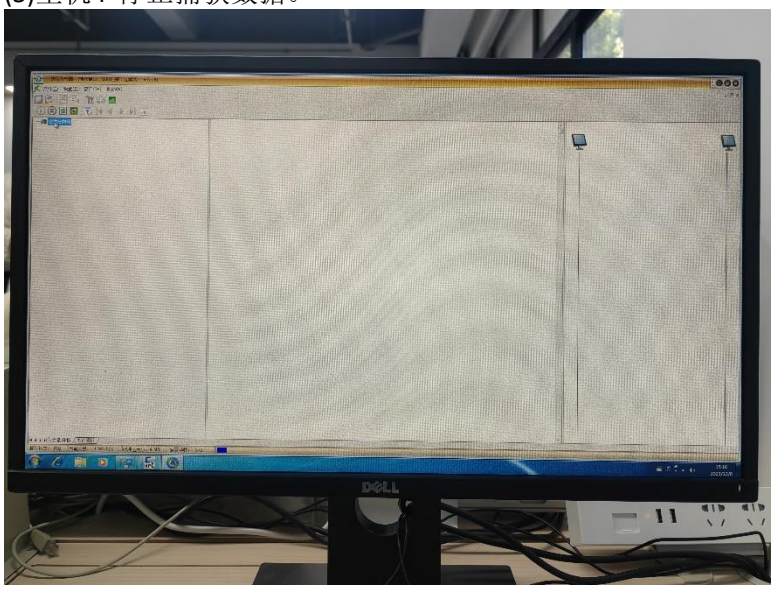
2. 环回地址

(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？

答：主机 F 不会收到主机 E 发送的 IP 数据报，127.0.0.1 为环回地址，此时主机向自己发送数据报，此报文不会经过其他主机。

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。

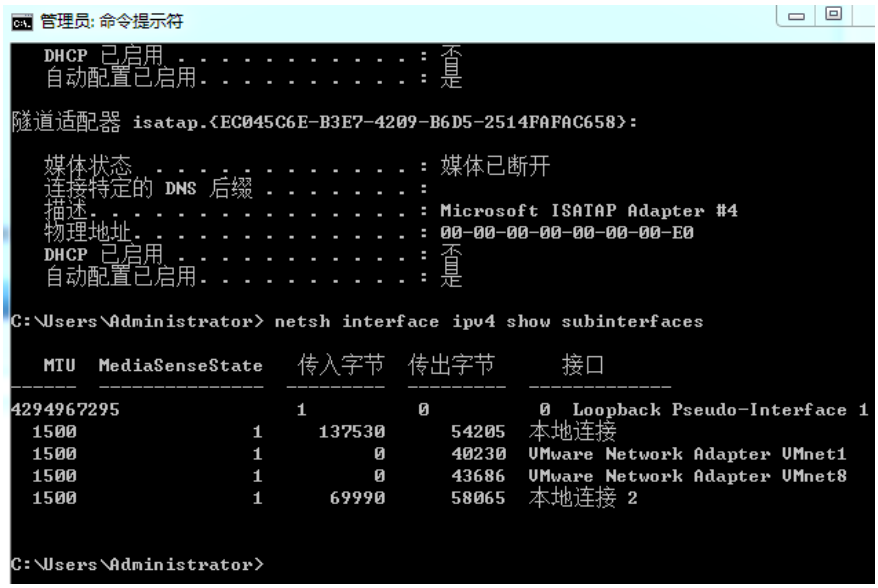
1. 主机 B 设置以太网端口的 MTU 为 800 字节（两个端口都设置），执行命令如下（进入 cmd 控制台）：

查看以太网端口当前 MTU 值

```
netsh interface ipv4 show subinterfaces
```

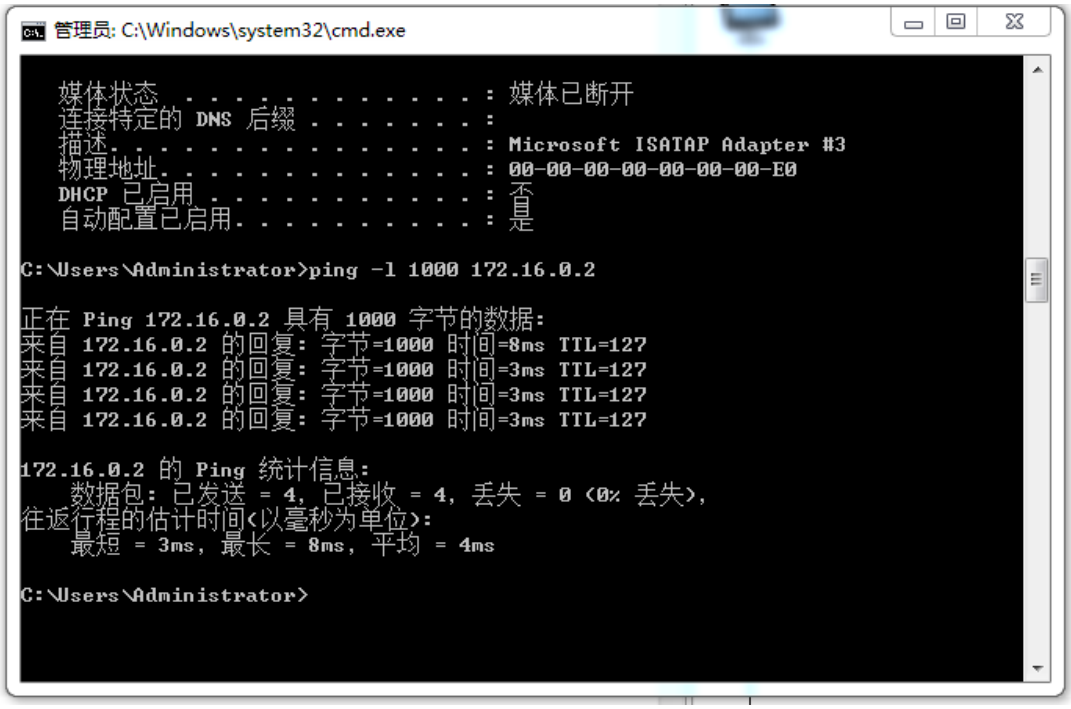
修改指定以太网端口的 MTU 值，按实际情况指定网络连接名称

```
netsh interface ipv4 set subinterface "网络连接名称" mtu=800 store=persistent
```



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：

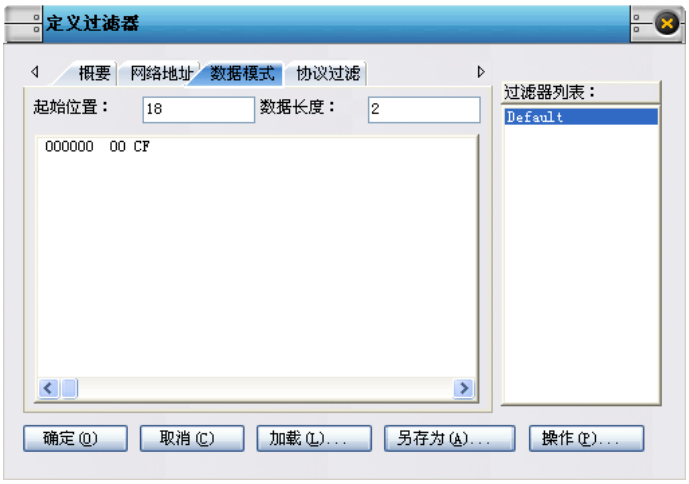
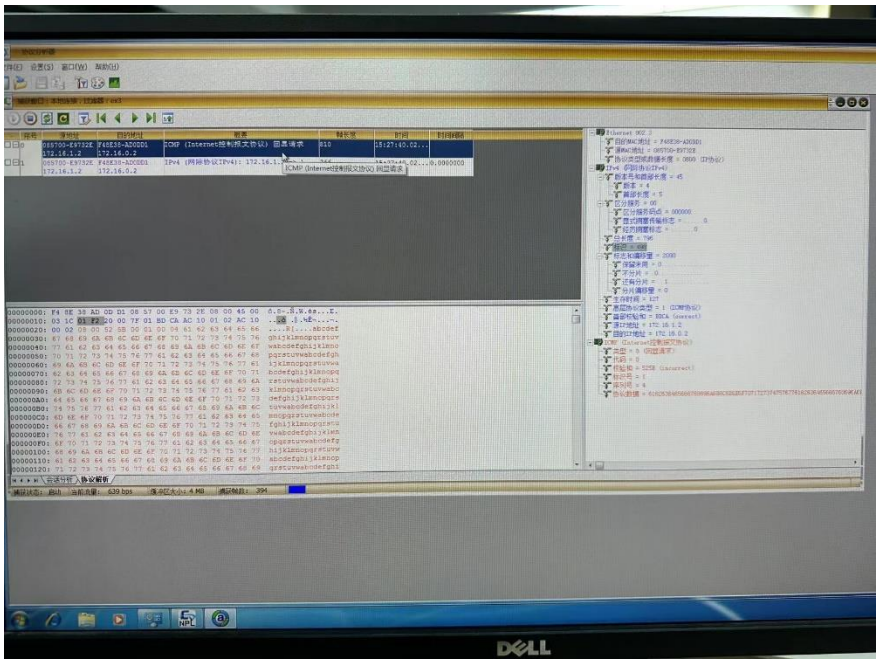
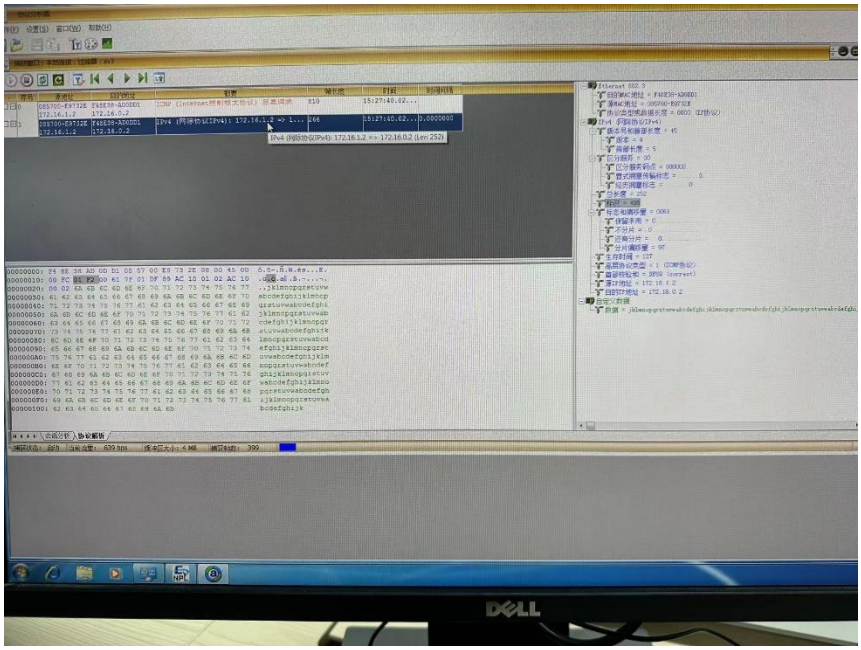

定义过滤器
概要
网络地址
数据模式
协议过滤
起始位置：
18
数据长度：
2
过滤器列表：
Default
000000 00 CF
确定(O)
取消(C)
加载(L)...
另存为(A)...
操作(P)...

图 3-24 过滤条件设置





●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。

表 3-6 实验结果

字段名称	分片序号 1	分片序号 2	分片序号 3
“标识”字段值	498	498	\
“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	776	232	\

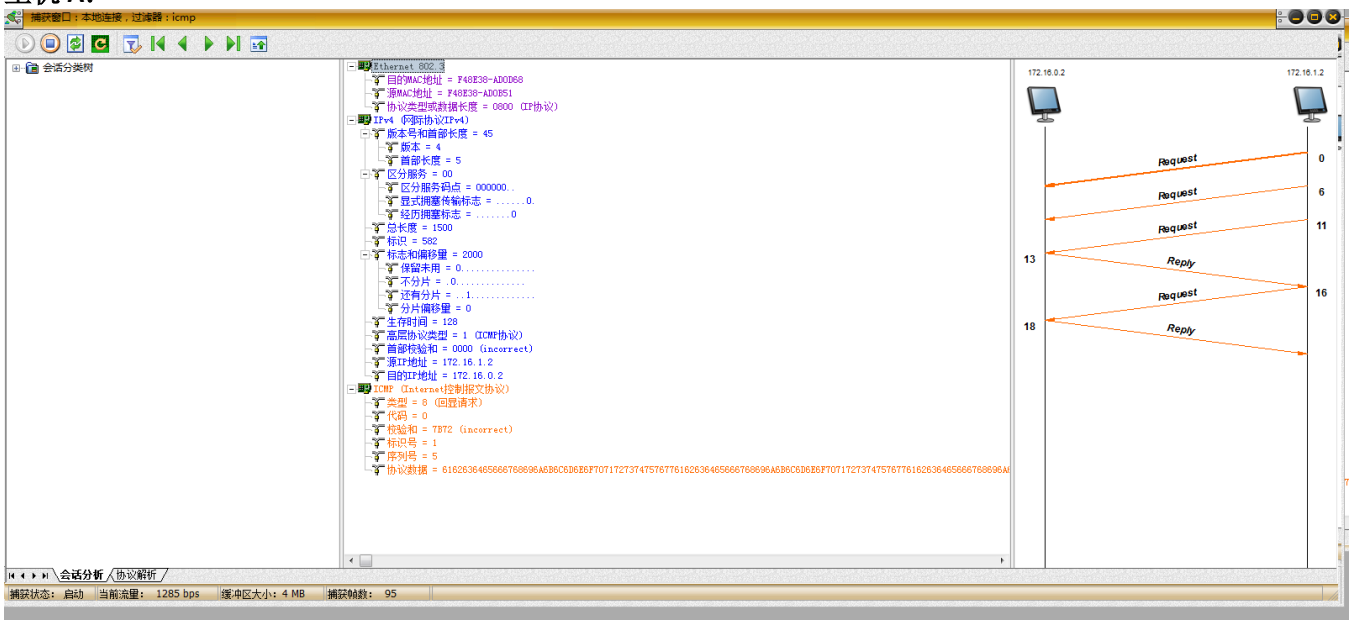
5. 主机 E 恢复默认过滤器。主机 A、B、E 重新开始捕获数据。

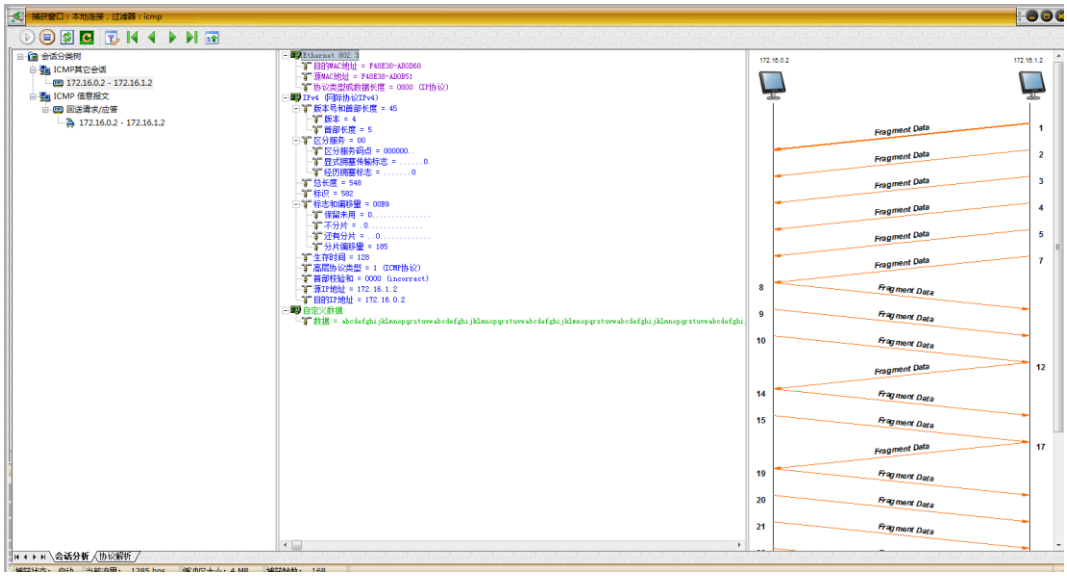
6. 在主机 A 上，执行命令 ping -l 2000 172.16.0.2。

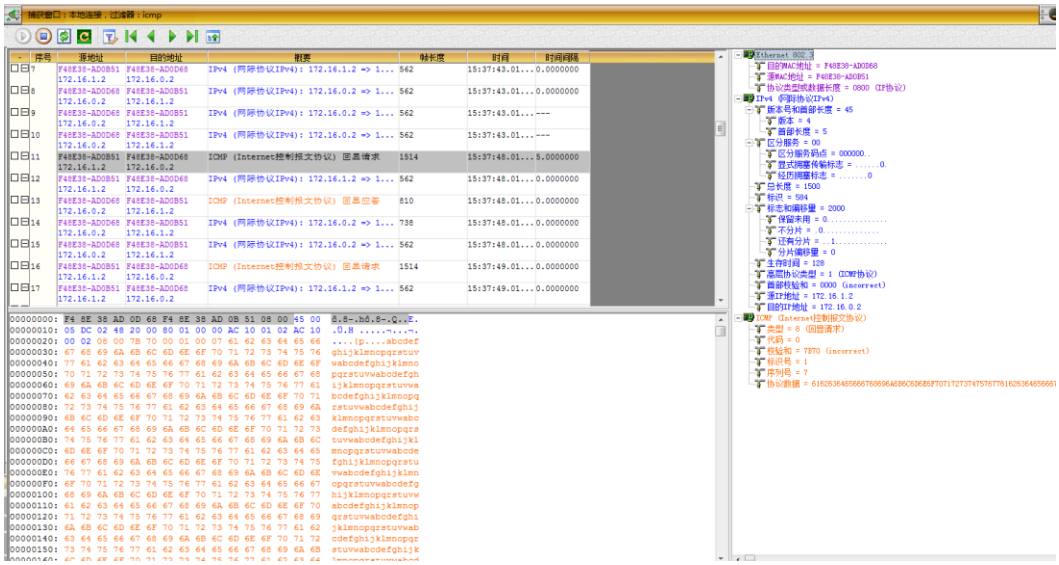
```
C:\Users\Administrator>ping -l 2000 172.16.0.2

正在 Ping 172.16.0.2 具有 2000 字节的数据:
来自 172.16.0.2 的回复: 字节=2000 时间=3ms TTL=127
来自 172.16.0.2 的回复: 字节=2000 时间=3ms TTL=127
来自 172.16.0.2 的回复: 字节=2000 时间=3ms TTL=127
来自 172.16.0.2 的回复: 字节=2000 时间=3ms TTL=127

172.16.0.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms, 最长 = 3ms, 平均 = 3ms
```

7. 主机 A、B、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。

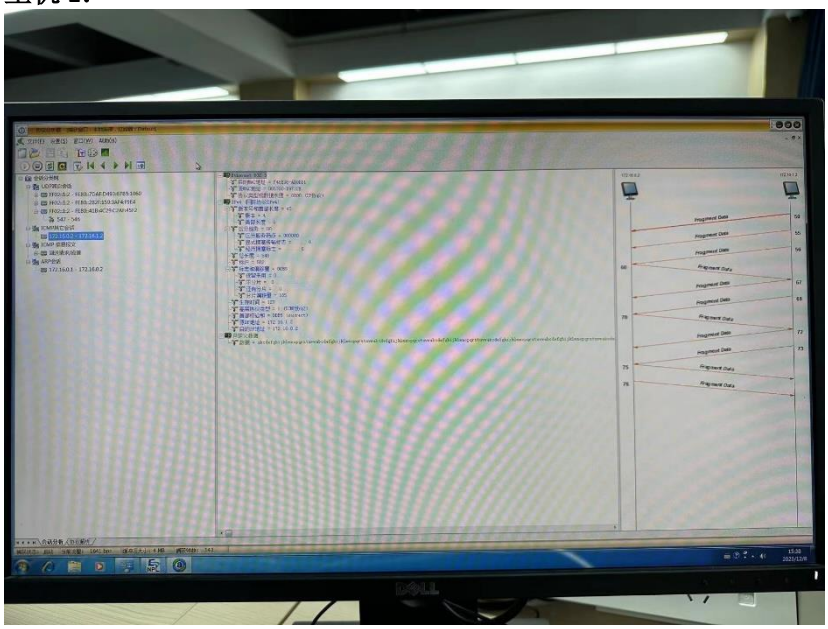
主机 A：

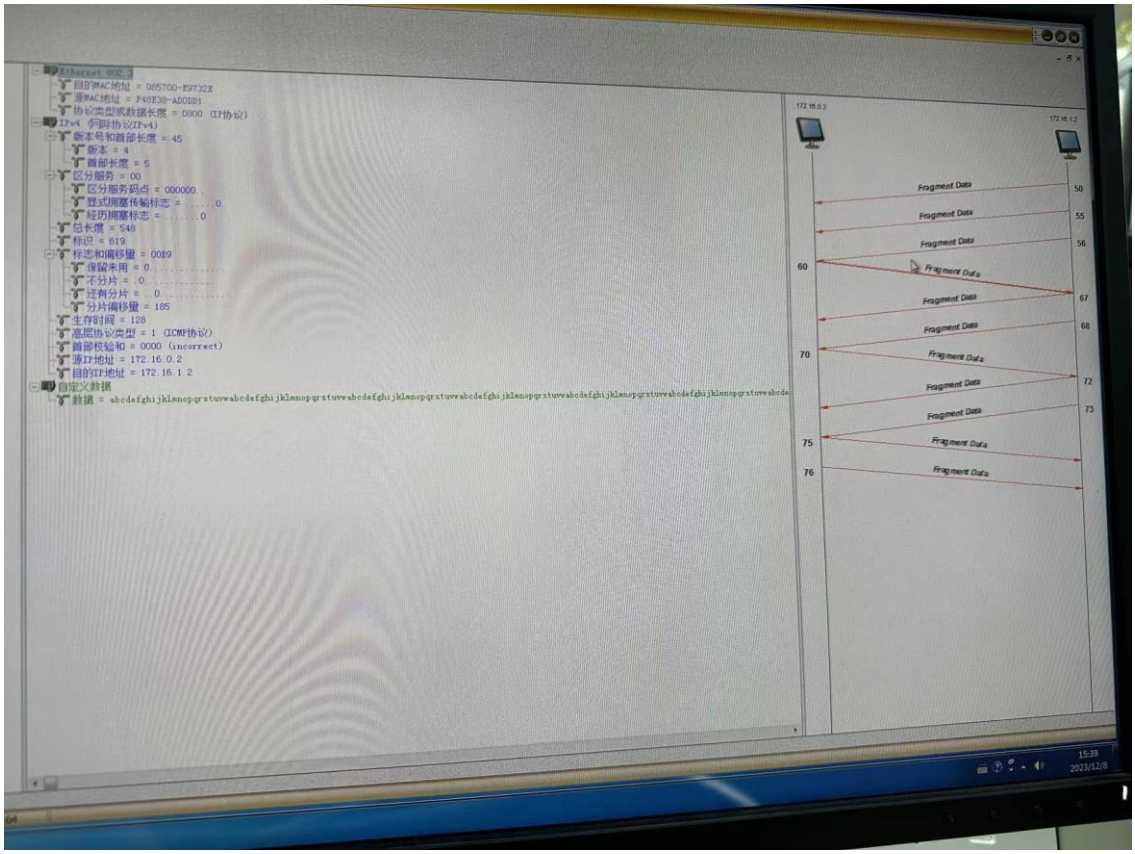






主机 E：





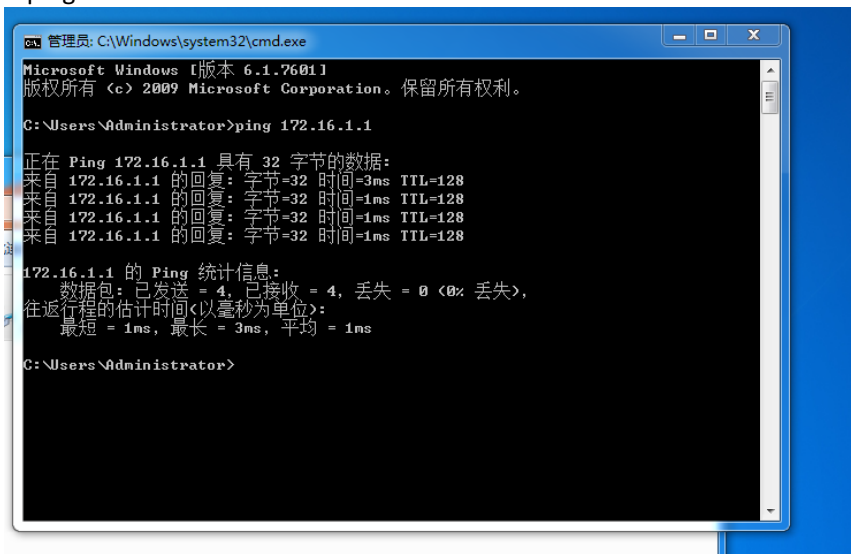
8.主机 B 恢复以太网端口的 MTU 为 1500。

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)。

A ping B：



●记录实验结果

表 3-7 实验结果

	是否 ping 通
主机 A----主机 B	**是**
主机 C----主机 D	**是**
主机 E----主机 F	**是**

●请问什么情况下两主机的子网掩码不同，却可以相互通信？

答：当两台主机的子网掩码分别与其 IP 地址进行逻辑与，得到的子网 IP 地址相同时，认为两台主机位于同一子网，能够相互通信。

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拓扑结构二的 IP 参数配置。

五、 实验结果总结

思考问题:

1. (练习 1)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？

答：

① 区别1：长度区别。IP地址由32bit组成，是逻辑地址；物理地址即硬件地址，由48bit构成。

区别2：放置位置的区别。IP地址放在IP数据报的首部，而硬件地址则放在MAC帧的首部。

区别3：使用的区别。在网络层和网络层以上使用IP地址，数据链路层和物理层使用硬件地址。

② 使用这两种不同的地址的原因：在 IP 层抽象的互联网上，我们看到的只是 IP 数据报，路由器根据目的站的 IP 地址进行选路。在具体的物理网络的链路层，我们看到的只是 MAC 帧，IP 数据报被封装在 MAC 帧里面。MAC 帧在不同的网络上传送时，其 MAC 帧的首部是不同的。这种变化，在上面的 IP 层上是看不到的。每个路由器都有 IP 地址和硬件地址。使用 IP 地址与硬件地址，尽管连接在一起的网络的硬件地址体系各不相同，但 IP 层抽象的互联网却屏蔽了下层这些很复杂的细节，并使我们能够使用统一的、抽象的 IP 地址进行通信。

2. (练习 2)受限广播地址的作用范围？

答：受限广播地址为 255.255.255.255。该地址用于主机配置过程中 IP 数据包的目的地址，此时主机可能还不知道它所在网络的网络掩码和 IP 地址。路由器并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。

3. (练习 2)受限广播地址和直接广播地址的区别？

答：在主机不知道本机所处的网络时，只能采用受限广播方式。TCP/IP 协议规定 32 位全为 1 的 IP 地址（255.255.255.255）为受限广播地址，用于本网广播。有限广播的数据包里不包含自己的 IP 地址。

当广播地址包含一个有效的网络号和一个全“1”的主机号，技术上就称为直接广播地址，如 202.198.151.255。直接广播地址里包含自身的 IP 地址。

4. (练习 2)路由器转发受限广播吗？

答：在任何情况下，路由器都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。

5. (练习 3)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？

答：数据部分为 3000 字节，MTU 为 1500 字节，IP 数据报首部长为 20 字节，传输数据部分 1480 字节，3000/1480=2.03，因此被分为 3 片。

6. (练习 3)数据部分长度为多少时报文正好被分为 2 片？

答：考虑 MTU 减去 IP 首部 20 字节，数据长度为[MTU-19, (MTU-20)*2] 时被分为 2 片。

7. (练习 3)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？

答：使用大的 MTU 可以在较少的报文中包含较多的数据，报文数量的减少可以降低路由器的负荷。小的 MTU 更能保证 pkt 的可信度，和实时性（较小的等待时间），更适合远距离传输和即时类软件。

8. (练习 4)IP 数据报中的首部校验和并不检验数据报中的数据，这样做的最大好处是什么？缺点是什么？

答：好处：可以减少 IP 数据报的处理复杂度，提高数据报的处理速度。

首先，所有将数据封装在 IP 数据报中的高层协议（如 TCP），都有覆盖整个分组的校验和。因此，IP 数据报的校验和就不必再检验所封装的数据部分。其次，每经过一个路由器，IP 数据报的首部就要改变一次，但数据部分不改变。因此校验和只对发生变化的部分进行检验。若检验包含数据部分，则每个路由器必须重新计算整个分组的校验和，这就表示每一个路由器要花费更多的处理时间。

最大缺点：数据部分出现差错时不能及早发现。

在数据报转发过程中不能及时发现数据报中的数据部分错误，只有在数据报交付到目的地后才发现数据报中的数据部分错误。