第 3 章

网络层

网络层是 OSI 模型中介于运输层和数据链路层之间的第三层，通过网络层可以实现源计算机和目标计算机之间的通信建立、维护和终止网络连接，并通过网络连接交换网络服务的数据单元。

当两个终端计算机系统的传输实体之间在进行通信时，并不必考虑建立和操作一个指定的网络连接时有关的路径选择及中转等细节，只需把要交换的数据单元交给它们的网络层便可实现。

本章学习目的：

- 网络层设计要点
- 网际协议
- 子网掩码
- 地址解析协议和逆地址解析协议
- IPv6 协议及寻址

3.1 网络层设计要点

为了让网络层更好地实现其功能，必须对网络层进行严谨的设计。因此，设计人员在进行网络层设计过程中，需要注意的存储—转发分组交换、向传输层提供的服务、连接服务的实现以及子网的内部设计实现。

3.1.1 向传输层提供的服务

网络层通过网络层与传输层接口，为传输层提供服务。这一接口相当重要，因为它通常是载体与用户的接口，也是通信子网的边界。载体往往决定直接通往网络层的各种协议和接口，它主要负责传输由其用户提供的分组，基于这个原因，对接口的定义必须

非常完善。

网络层的服务是按以下目标进行设计的。

- 服务应与通信子网技术无关。
- 通信子网的数量、类型和拓扑结构对于传输层来说是不可见的。
- 传输层所能获得的网络地址应采用统一的编号方式，甚至可以跨越多个 LAN 和 WAN。

在考虑到这些目标后，设计者便有相当大的自由度来编写提供给传输层的服务的详细规范，这种自由度往往会导致两个竞争派别之间的激烈冲突，而冲突的焦点是网络层应该提供面向连接的服务还是无连接的服务。

一类是以 Internet 委员会为代表的认为：通信子网的工作是在网上传送分组，除此之外，不再做其他的事。按照这样的观点，无论怎样来设计通信子网，它总是不可靠的。因此，主机应接受这个事实即必须自己来完成差错控制（错误检测和纠正）和流量控制的任务。

提　示

这种观点很快导致了这样的结论：网络层提供的服务应该用原语是 SEND PACKET 和 RECEIVE PACKET 及少许其他原语构成的无线连接方式。特别是，由于分组排序和流量控制并不在网络层完成，而在主机完成。因此，在网络层中不必再设置分组排序和流量功能。此外，由于每个被发送的分组在其传输过程中独立于它前面的那些分组。因此，每个分组必须带有完整的目标地址。

另一类以电信公司为代表的认为：子网应该提供一种可靠（合理）的、面向连接的服务。按照这一观点，其连接应该具有如下特性。

- **发送数据前**　发送端网络层进程必须与接收端网络层对等进程建立连接，这是一个具有特殊标识符的连接，一直到数据传输完毕后才能释放。
- **建立连接时**　两个进程可就其服务参数、服务质量和服务开销进行协商。
- **通信是双向的**　分组按次序进行递交。
- **能自动提供流量控制功能**　以防止一个快速发送者以高于接收者取出分组的速率将分组堆积在队列中，从而导致溢出。

这两类都有很好的例证来说明他们的观点。Internet 提供了无连接的网络层服务，ATM 网络提供了面向连接的网络层服务。但是，随着服务质量变得越来越重要，Internet 现在也正在努力获得与面向连接服务有关的一些特性。

3.1.2　无连接服务和面向连接服务的实现

如果网络层提供的是无连接的服务，那么所有的分组都被独立地传送到子网中，并且独立于路由，还不需要预先建立任何辅助设施。在这样的情况下，分组通常被称为数据报（Data Gram），子网被称为数据报子网（Datagram Subnet）。

而如果网络层提供的是面向连接的服务，那么在发送数据分组之前，必须建立一条从源路由器到目标路由器之间的路径。这条连接路径通常被称为 VC（Virtual Circuit，虚电路），子网则被称为虚电路子网（Virtual-circuit Subnet）。

1．数据报子网

如图 3-1 所示，进程 1 要发送一个长消息给进程 2，它先将该消息递交给传输层，

并告诉传输层将该消息递交给主机 2 上的进程 2。于是，传输层便在该消息的前面加上一个传输头，然后将结果交给网络层。

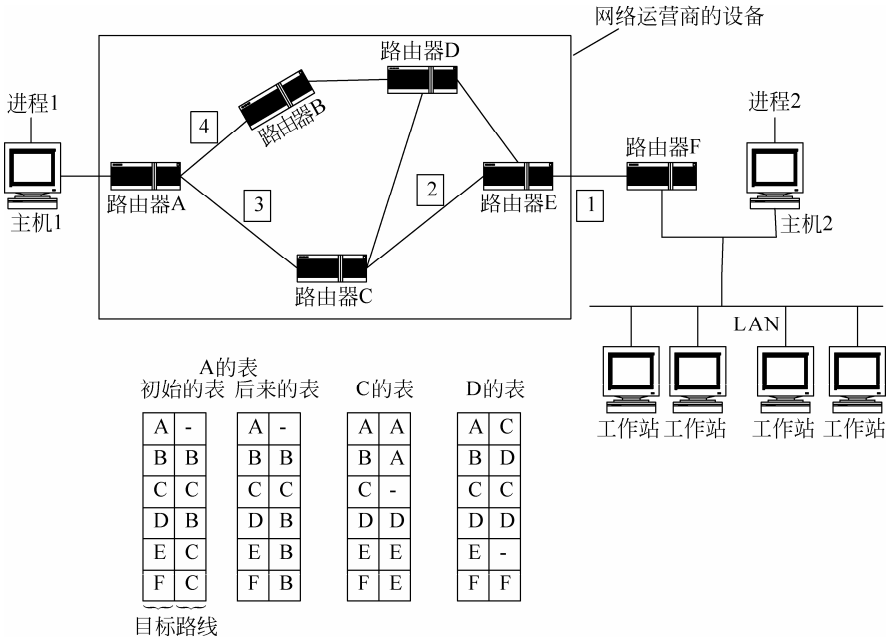


图 3–1　数据报子网的路由

若该消息的长度是最大分组长度的 4 倍，那么网络层应该先将这个消息分成 4 个组，然后选择一种点到点协议（比如 PPP）将这些分组依次发送给路由器 A。

这时，网络运营商便将传输任务接管过来。每台路由器中的内部表指明了每个目标地址应该将分组送到哪里去。每一个表项包含两个元素：一个是目标地址，另一个是针对该目标地址所使用的输出线路。

在这里，路由器只允许使用直接连接的线路。如图 3-1 所示，路由器 A 只有两条输出线路路由器 B 和路由器 C，因此，每一个进来的分组必须被发送给这两台路由器之一，即使它的目标地址是另外一台路由器。路由器 A 的初始路由表如图 3-1 所示中的“初始表”所示。

当分组 1、2 和 3 到达路由器 A 时，它们被暂时保存起来（以便检验它们的校验和）。然后，根据路由器 A 的路由表，再把每一个分组被转发给 C。然后分组 1 被转发给 E，下一步被转发给 F。当它到达 F 的时候，它被封装到一个数据链路层的帧中，通过 LAN 被发送给主机 2。分组 2 和 3 也经过了同样的路径。再看分组 4，当它到达路由器 A 之后，虽然其目标地址是路由器 F，但是它却被发送给路由器 B。而路由器 A 因为某种原因，便采用不同于前三者的路径来发送分组 4。管理这些路由表并做出路由选择的算法称为路由算法（Routing Algorithm）。

2．虚电路子网

在虚电路中，不需要每次都为一个分组重新选择路径，而是当一个连接被建立起来的时候，从源地址到目标地址间的这条路径被选择作为连接的一部分，并保存在经过的

路由器的内部表中，所有在这个连接上通过的流量，都使用这条路径。这跟电话系统的工作方式一样，当连接被释放后，虚电路也随之结束。在面向连接的服务中，每个分组的标识符都指明了它所属的虚电路。

如图 3-2 所示，主机 1 已经与主机 2 之间建立了一条连接 1。该连接被记录在每个路由表中的第一个表项中，如在路由器 A 的路由表中的第一行表明：如果一个分组包含了来自于主机 1 的连接标识符 1，那么它将被发送到路由器 C，并且赋予连接标识 1。

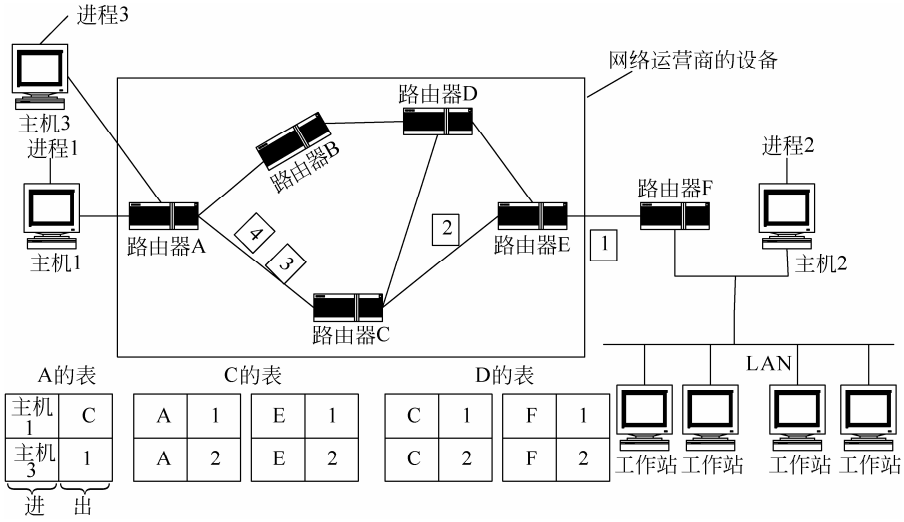


图 3-2 虚电路子网内的路由

同样，路由器 C 中的第一个表项将该分组路由到路由器 E，也赋予连接标识符 1。此时，如果主机 3 再与主机 2 建立连接，主机 3 也只能选择标识符 1，并且要在子网中建立虚电路，即路由表中的第二行。

但在这里会产生一个冲突，因为虽然路由器 A 能很容易区分出来自于主机 1 的连接 1 分组和来自于主机 3 的连接 1 分组，但是，路由器 C 却并不能区分出这两个分组。

因此，路由器 A 只能给主机 1 与主机 3 之间的连接分配一个不同的连接标识符。这说明了路由器需要具备“在输出分组中替换连接标识符”的能力，在这里也被称为标签交换（Label Switching）。

3．虚电路子网和数据报子网的比较

虚电路和数据报都有其支持者和反对者，下面将从多个角度来总结有关的争议。表 3-1 列出了通信子网内部采用数据报和采用虚电路的不同之处。

表 3-1 数据报和虚电路子网的比较

项目类型	数据报子网	虚电路子网
电路设置	不需要	需要
地址信息	每个分组包含完整的源地址和目标地址	每个分组包含一个很短的虚电路号
状态信息	路由器不保留任何有关连接的状态信息	每个虚电路都要求路由器为每个连接建立表项
路由选择	对每个分组独立选择	当虚电路建立时选择路径，所有的分组都沿着这条路径

续表

项目类型	数据报子网	虚电路子网
路由器失效的影响	除了在崩溃时全丢失分组外，无其他影响	所有经过此失效路由器的虚电路都将终止
服务质量	较难实现	如果有足够的资源可以提前分配给每一个虚电路，则很容易实现
拥塞控制	较难实现	如果有足够的资源可以提前分配给每一个虚电路，则很容易实现

在通信子网内部，虚电路和数据报之间有好几个需要权衡的因素，一个是路由器的内存空间和带宽之间的权衡。虚电路允许分组可以只包含虚电路号即可，而不用包含完整的目标地址。如果分组很短，那么各分组中的完整目标地址可能会成为一个不小的负担，造成带宽浪费。内部使用虚电路的代价是在路由器中占用空间。根据通信电路和路由器存储空间的相对开销，可能虚电路更合算，也可能数据报更合算。

另一个因素是建立虚电路所需要的时间和地址解析的时间的比较。使用虚电路时，它要求有一个建立阶段，该阶段既花费时间，也消耗资源。但是，要搞清楚数据分组在虚电路通信子网中如何运行却很简单，即路由器只要利用虚电路号作为索引，就可以在内部表中找到该分组的目标去向。在数据报子网中，路由器需要执行一个相对复杂的查找过程，才能确定分组的目标去向。

还有一个问题是在路由器内存中所要求的表空间的数量。在数据报子网中，每个目标地址都要求有一个表项，而在虚电路子网中，只要为每一个虚电路提供一个表项即可。但是，这也并不是绝对的，如建立连接的分组也需要路由选择，它们也使用目标地址，就同数据报子网一样。

从服务质量和拥塞控制的角度来讲，虚电路有一些明显的优势，因为连接已建立起来的资源可以提示保留下来，一旦分组开始到来，所需的带宽和路由器资源已准备就绪。对于数据报子网避免拥塞则更困难。

对于事务处理系统，如打电话来验证信用卡购物的商家，需要建立和清除虚电路的开销有可能会妨碍虚电路的使用。如果系统中大量的流量都是这样，那么在通信子网内部采用虚电路就会变得毫无意义。

虚电路还具有脆弱性，即若一台路由器崩溃或内存中的数据丢失，那么，所有从该路由器经过的虚电路都将被中断。相反，若一台数据报路由器停止，则只有当时还有分组且留在路由器队列中的用户会受到影响，而且，在分组没被确认的情况下，这些用户并不会受到影响。一条通信线路的失效对于使用该线路的虚电路来说是无可挽回的，但如果使用了数据报的话，则这种损失就很容易得到补偿。对于数据报子网来讲，路由器还可以平衡通信流量，因为在传输一个很长的分组序列过程中，路由器可以在中间改变传输路径。

3.2 网际协议

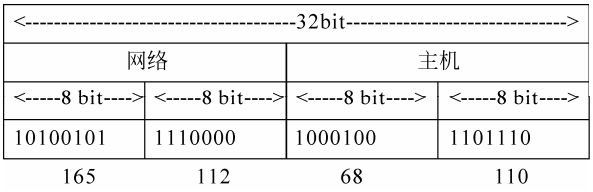
网际协议（IP）是开放系统互联模型（OSI Model）的一个主要协议，也是 TCP/IP 中完整的一部分。IP 完成什么工作呢？它主要的任务有两个：一是寻址；二是管理分割

数据片（Datagrams）。

3.2.1 IP 地址分类

IP 地址的长度为 32 位（4 个字节）无符号的二进制数，它通常采用点分十进制数表示方法，即每个地址被表示为 4 个以小数点隔开的十进制整数，每个整数对应 1 个字节，如 165.112.68.110 就是一个合法的 IP 地址。

32 位的 IP 地址由网络号和主机号两部分构成。其中，网络号就是网络地址，用于标识某个网络。主机号用于标识在该网络上的一台特定的主机。位于相同物理网络上的所有主机具有相同的网络号，如图 3-3 所示。



网络		主机	
<-----8 bit---->	<-----8 bit---->	<-----8 bit---->	<-----8 bit---->
10100101	1110000	1000100	1101110
165	112	68	110

图 3-3 IP 地址的表示

为了适应于不同的规模的物理网络，IP 地址分为 A、B、C、D、E 五类，但在 Internet 上可分配使用的 IP 地址只有 A、B、C 三类。这三类地址统称为单目传送（Unicast）地址，因为这些地址通常只能分配给唯一的一台主机。D 类地址被称为多播（Multicast）地址，组播地址可用于视频广播或视频点播系统，而 E 类地址尚未使用，保留给将来的特殊用途。

不同类别的 IP 地址的网络号和主机号的长度划分不同，它们所能识别的物理网络数不同，每个物理网络所能容纳的主机个数也不同，如图 3-4 所示。

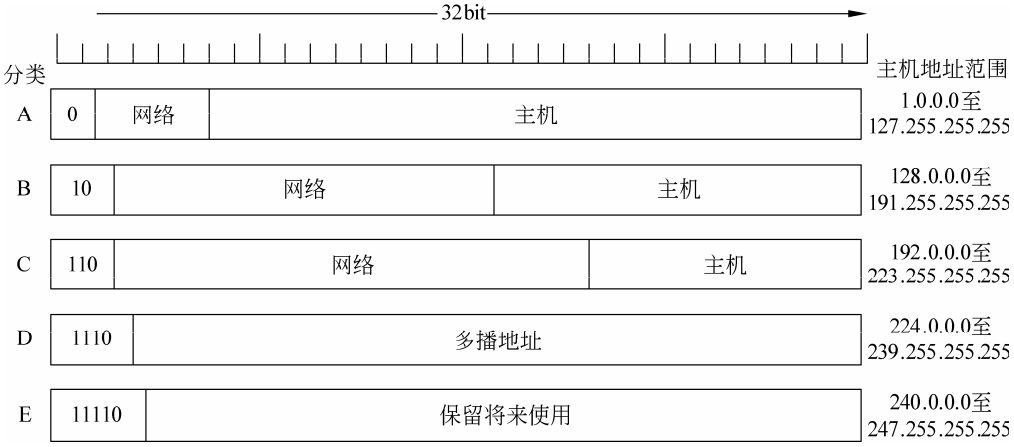


图 3-4 IP 地址的格式与分类

A 类地址用 7 位表示 IP 地址的网络部分，而用 24 位表示 IP 地址的主机部分。因此，它可以用于大型网络。B 类地址用 14 位表示 IP 地址的网络部分，而用 16 位表示 IP 地址的主要部分。它可以用于中型规模的网络。C 类地址用 21 位表示 IP 地址的网络部分，而用 8 位表示 IP 地址的主机部分，在一个网络中最多只能连接 256 台设备，因此，只适用于较小规模的网络。D 类地址为多播的功能保留。E 类地址为将来使用而保留。

根据 A、B、C、D、E 的高位数值，可以总结出它们的第一个字节的取值范围，如

A 类地址的第一个字节的数值为 1～126。表 3-2 给出了每种地址类别第一个字节的取值范围及其规模。

表 3-2 各类地址的取值范围

高　位	第一个字节的十进制数	地址类别
0	1～126	A
10	128～191	B
110	192～223	C
1110	224～239	D
11110	240～254	E

3.2.2 IP 地址与 MAC 地址

MAC（Media Access Control）地址，或称为 MAC 位址、硬件地址，用来定义网络设备的位置。

在 OSI 模型中，第三层网络层负责 IP 地址，第二层链接层则负责 MAC 位址。因此，一个主机会有一个 IP 地址，而每个网络位置会有一个专属于它的 MAC 位址。

MAC 地址是收录在 NIC（Network Interface Card，网卡）里的 MAC 地址，是由 48 位（6B/byte，1Byte=8bit）十六进制的数字组成。0～23 位叫做组织唯一标志符（Organizationally Unique identifier），是识别 LAN 结点的标识。24～47 位是由厂家自己分配。其中，第 40 位是组播地址标志位。

提　示

网卡的物理地址通常是由网卡生产厂家烧入网卡的 EPROM（闪存芯片），它存储的是传输数据时真正赖以标识发出数据的计算机和接收数据的主机的地址。

形象地说，MAC 地址就如同身份证上的身份证号码，具有全球唯一性。

1．MAC 地址的作用

IP 地址就如同一个职位，而 MAC 地址则像是去应聘这个职位的人。职位既可以由甲担任，也可以由乙担任。同理，一个结点的 IP 地址对于网卡是不做要求的，基本上什么样的厂家都可以用，也就是说 IP 地址与 MAC 地址并不存在着绑定关系。

如果一个 IP 主机从一个网络移到另一个网络，可以给它一个新的 IP 地址，而无须换一个新的网卡。

无论是局域网，还是广域网中的计算机之间的通信，最终都表现为将数据包从某种形式的链路上的初始结点出发，从一个结点传递到另一个结点，最终传送到目的结点。数据包在这些结点之间的移动都是由 ARP（Address Resolution Protocol，地址解析协议）负责将 IP 地址映射到 MAC 地址上来完成的。

2．MAC 地址的应用

身份证就是用来证明一个人的身份。平日身份证的作用并不是很大，但是到了一些关键时刻，必须由身份证来说明一个人的一切。

那么，IP 地址与 MAC 地址绑定，就如同在日常生活中一个人与身份证的关系。因为，IP 地址可以随意的，但 MAC 地址是唯一说明 IP 地址身份的。例如，为防止 IP 地址被盗用，通常交换机的端口绑定（端口的 MAC 表使用静态表项）可以在每个交换机端口只连接一台主机的情况下防止修改 MAC 地址的盗用，如果是三层设备，则还可以提供交换机端口、IP 地址和 MAC 地址三者的绑定。

提　示

一般绑定 MAC 地址都是在交换机和路由器上配置的，是网管人员才能接触到的。对于一般计算机用户来说，只要了解了绑定的作用就可以了。

3.2.3　IP 数据报的格式

要进行传输的数据在 IP 层首先需要加上 IP 头信息，封装成 IP 数据报。IP 数据报包括一个报文头以及与更高层协议相关的数据。图 3-5 所示为 IP 数据报的具体格式。

IP 数据报的格式可以分为报头区和数据区两大部分。其中，数据区包括高层需要传输的数据，报头区是为了正确传输高层数据而增加的控制信息，这些控制信息包括以下几种。

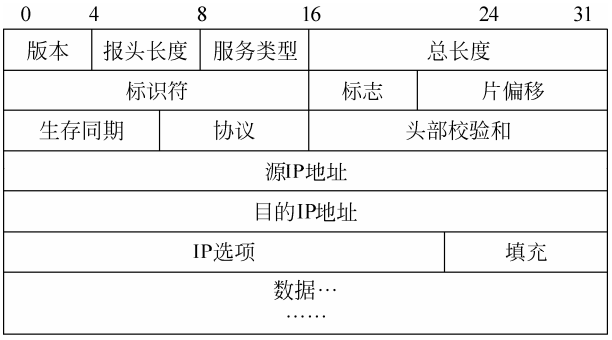


图 3-5　IP 数据报格式

1．版本

长度为 4bit，表示与数据报对应的 IP 协议版本号。不同的 IP 协议版本，其数据报格式有所不同。当前的 IP 协议版本号为“4”。所有 IP 软件在处理数据报之前都必须检查版本号，以确保版本正确。IP 软件将拒绝处理版本不同的数据报，以避免错误解释其中内容。

2．报头长度

长度为 4bit，指出以 32bit 长计算的报头长度，IP 数据报头中除 IP 选项域外，其他各域均为定长域，各定长域长度为 20 个字节，这样一个不含选项域的普通 IP 数据报其头标长度域值为“5”。总的来说，头标长度应为 32bit 的整数位，假如不是，在头标尾部添“0”凑齐。

3．服务类型

服务类型（Service Type）规定对本数据报的处理方式。该域长度为一个字节，被分为 5 个子域，其子域结构如表 3-3 所示。

表 3-3　服务类型子域结构

0　1　2	3	4	5	6　7
优先权	D	T	R	未用

其中，3bit 的“优先权”（Precedence）子域指示本数据报的优先权，表示本数据报的重要程度。优先权取值为 0～7，“0”表示一般优先权，“7”表示网络控制优先权，优先权值是由用户指定的。大多数网络软件对此不予理睬，然而它毕竟提供了一种手段，允许控制信息享受比一般数据较高的优先权。DTR 三位数据表示本数据报所要的传输类型。其中，D 代表低延迟（Delay）；T 代表高吞吐率（Throughput）；R 代表高可靠性（Reliability）。上述 3 位只是用户的请求，不具有强制性，Internet 在寻找路径时可能以它们为参考。

4．总长度

总长域为 16bit，指示整个 IP 数据报的长度，以字节为单位，其中包括报头长度及数据区长。因此，IP 数据报总长可达 2^{16}–1（即 65535）个字节。

5．标识

标识是信源机赋予数据报的标识符，目的主机利用此域和信源地址判断收到的分组属于哪个数据报，以使数据报重组。分片时，该域必须不加修改地复制到新片头中，数据报标识符的实现原则是对于同一信源机各标识符必须是唯一的。

6．标志

标志为 3bit，用于控制分片和重组。Bit0：保留，必须为“0”。Bit1：0=可以分片，1=不分片。Bit2：0=最后一个分片，1=还有分片。

7．片偏移

它指出本片数据在初始数据报数据区中的偏移量，以 8 个字节为单位。由于各片按独立数据报的方式传输，其到达信宿机的顺序无法保证，因此，重组的片顺序由片偏移域提供。

8．生存周期

数据报传输的一大特点是随机寻径，因此，从信源机到信宿机的传输延迟也具有随机性。当路由器的路由表出错时，数据报可能会进入一条循环路径，无休止地在 Internet 中流动。为避免这种情况，IP 协议对数据报传输延迟要进行控制。

为此，每生成一个数据报，它都带有一个生存时间，该时间以秒为单位，每个处理该数据报的结点必须至少把 TTL 值减 1，即使处理时间小于一秒。假如数据报在路由器中因等待服务而被延迟，则从 TTL 中减去等待时间，一旦 TTL 减至 0，该数据报将被丢弃。

9．协议

协议为 1 个字节，指创建数据报数据区数据的高级协议类型，如 TCP、OSPF 等。

10．头部校验和

校验为 2 个字节，用于保证头部数据的完整性，其算法很简单，设“头部校验和”初值为 0，然后对头部数据每 16 位求异或，结果取反，便得到校验和。

11．选项

主要用于控制和测试两个目的。

3.2.4 IP 数据报的分片与组装

当一个 IP 数据报从一个主机传输到另一个主机时，它可能通过不同的物理网络。每个物理网络有一个最大的帧大小，即所谓的 MTU（Maximum Transmission Unit，最大传输单元）。它限制了能够放入一个物理帧中的数据报长度。

IP 用一个进程来对超过 MTU 的数据报进行分片。这个进程建立了一个最大数据量以内的数据报集合。接收主机重新组合原始的数据报。IP 要求每个链路至少支持 68 个 8 位字节的 MTU。这是最大的 IP 报文头长度（60 个 8 位字节）和非最后分片中可能的最小数据长度（8 个 8 位字节）的总和。如果任何一个网络提供了一个比这个还小的值，则必须在网络接口层实现分片和分片重组。这个过程对于 IP 必须是透明的。IP 实现不必处理大于 576 字节的未分片的数据报。

一个未分片的数据报的分片信息字段全为 0，即多个分片标志位为 0，并且片偏移量为 0。分片一个数据报，须执行以下几个步骤。

- ❑ 检查 DF 标志位，查明是否允许分片。如果设置了该位，则数据报将被丢弃，并将一个 ICMP 错误返回给源端。
- ❑ 基于 MTU 值，把数据字段分成两个部分或多个部分。除了最后的数据部分外，所有新建数据选项的长度必须为 8 个字节的倍数。
- ❑ 每个数据部分被放入一个 IP 数据报。这些数据报的报文头略微修改了原来的报文头。
- ❑ 除了最后的数据报分片外，所有分片都设置了多个分片标志位。
- ❑ 每个分片中的片偏移量字段设为这个数据部分在原来数据报中所占的位置，这个位置相对于原来未分片数据报中的开头处。
- ❑ 如果在原来的数据报中包括了选项，则选项类型字节的高位字节决定了这个信息是被复制到所有分片数据报，还是只复制到第一个数据报。
- ❑ 设置新数据报的报文头字段及总长度字段。
- ❑ 重新计算报文头部校验和字段。

此时，这些分片数据报中的每个数据报如一个完整 IP 数据报一样被转发。IP 独立地处理每个数据报分片。数据报分片能够通过不同的路由器到达目的。如果它们通过那些规定了更小的 MTU 网络，则还能够进一步对它们进行分片。

在目的主机上，数据被重新组合成原来的数据报。发送主机设置的标识符字段与数据报中的源 IP 地址和目的 IP 地址一起使用，分片过程不改变这个字段。

为了重新组合这些数据报分片，接收主机在第一个分片到达时分配一个存储缓冲区。这个主机还将启动一个计时器。当数据报的后续分片到达时，数据被复制到缓冲区存储器中片偏移量字段指出的位置。当所有分片都到达时，完整的未分片的原始数据包就被恢复了。处理如同未分片数据报一样继续进行。

如果计时器超时并且分片保持尚未认可状态，则数据报被丢弃。这个计时器的初始值称为 IP 数据报的生存期值。它是依赖于实现方式的。一些实现方式允许对它进行配置。

在某些 IP 主机上可以使用 netstat 命令列出分片的细节，如 TCP/IP for OS/2 中的 netstat-i 命令。

3.2.5 IP 数据报路由选项

IP 数据报选项字段为 IP 数据报源站提供了两种显式提供路由信息的方法。它还为 IP 数据报提供了一种确定传输路由的方法。

1．不严格的源路由

不严格的源路由选项也称为不严格的源和记录路由选项，它为 IP 数据报提供了一种显式地提供路由信息的方法。路由器在把数据报转发到目的站时使用该信息，同时还用它来记录路由。

2．严格的源路由

严格的源路由选项也称为 SSRR（Strict Source and Record Route，严格的源和记录路由）选项，除了中间路由器必须通过一个直接连接的网络把数据报发送到源路由中的下一个 IP 地址外，它使用与不严格的源路由相同的原则。它不能使用中间路由器。如果不能实现这点，它就发出 ICMP 目的不可达的错误消息。

3．记录路由

这个选项提供了一种记录 IP 数据报通过的路径的方法。它的功能类似于源路由选项。但是，这选项提供了一个空的路由数据字段，这个字段在数据报通过网络时被填入。

源主机必须为这个路由信息提供足够的空间。如果数据字段在数据报到达目的主机之前被填充，则在不记录这个路径的情况下继续转发这个数据报。

4．网际时间戳

该选项强制目的路由上的一些或所有路由器把一个时间戳放入选项数据中。时间戳按秒度量，并且可以用于调试的目的。但由于大多数 IP 数据在不到 1s 的时间内就被转发及 IP 路由器不需要有同步的时钟，导致时间戳不精确。因此，它不能用于性能度量。

3.3 子网掩码

子网掩码（Subnet Mask）又叫网络掩码、地址掩码，是一种用来指明一个 IP 地址的哪些位标识的是主机所在的子网以及哪些位标识的是主机的位掩码。子网掩码不能单独存在，它必须结合 IP 地址一起使用。子网掩码只有一个作用，就是将某个 IP 地址划分成网络地址和主机地址两部分。

3.3.1 子网掩码概述

互联网是由许多小型网络构成的，每个网络上都有许多主机，这样便构成了一个有

层次的结构。IP 地址在设计时就考虑到地址分配的层次特点，将每个 IP 地址都分割成网络号和主机号两部分，以便于 IP 地址的寻址操作。

IP 地址的网络号和主机号各是多少位呢？如果不指定，就不知道哪些位是网络号、哪些是主机号，这就需要通过子网掩码来实现。

子网掩码不能单独存在，它必须结合 IP 地址一起使用。子网掩码只有一个作用，就是将某个 IP 地址划分成网络地址和主机地址两部分。子网掩码的设定必须遵循一定的规则。

子网掩码也是由 32 位的二进制数构成，其左边用若干个连续的二进制数字“1”表示，右边用若干个连续的二进制数字“0”表示，其格式如图 3-6 所示。这样通过左边若干连续个数的“1”及右边连续个数的“0”能够区分 IP 地址的网络号和主机号部分。

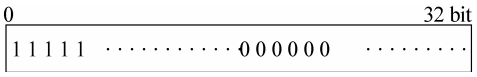


图 3-6 子网掩码格式

子网掩码也通常使用点分十进制数的方法来表示。例如，255.255.255.0 就表示一个子网掩码，与转后的二进制数关系如图 3-7 所示。并且它是 C 类 IP 地址的默认子网掩码。

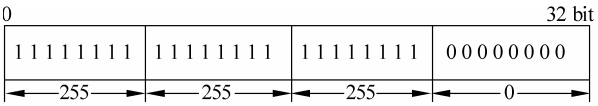


图 3-7 子网掩码十进制与二进制对应关系

常用的子网掩码有数百种，这里只介绍最常用的两种子网掩码，它们分别是 255.255.255.0 和 255.255.0.0。

- **子网掩码是 255.255.255.0 的网络** 最后面一个数字可以在 0～255 范围内任意变化，因此可以提供 256 个 IP 地址。但是实际可用的 IP 地址数量是 256–2，即 254 个，因为主机号不能全是“0”或全是“1”。
- **子网掩码是 255.255.0.0 的网络** 后面两个数字可以在 0～255 范围内任意变化，可以提供 255^2 个 IP 地址。但是实际可用的 IP 地址数量是 255^2–2，即 65023 个。

为了使读者更容易理解子网掩码的相关知识，读者还应该明白什么是掩码，什么是子网。

1．子网

对于企业所有主机位于同一网络层次中，不方便管理员对其进行管理。因此，提出了将大网络进一步划分成小网络，而这些小网络就称为“子网”。

IP 地址的子网掩码设置不是任意的。如果将子网掩码设置过大，也就是说子网范围扩大。根据子网寻径规则，很可能发往和本地机不属于同一子网内的计算机，会因为错误的判断而认为目标计算机是在同一个子网内中。

那么，数据包将在本子网内循环，直到超时并抛弃，使数据不能正确到达目标的计算机，导致网络传输错误。

如果将子网掩码设置得过小，那么会将本来属于同一子网内的机器之间的通信当作跨子网传输，数据包都交给默认网关处理，这样势必增加默认网关的负担，造成网络效率下降。

因此，子网掩码应该根据网络的规模进行设置。如果一个网络的规模不超过 254 台

计算机，则采用 255.255.255.0 作为子网掩码就可以了。

2．掩码

掩码与 IP 地址相对应，具有 32 位地址，当用掩码与 IP 地址进行逐位“逻辑与”（AND）运算后，就能够得知该 IP 地址的网络地址（网络号）。例如，一个 IP 地址为 221.180.60.15，其默认掩码为 255.255.255.0，与 IP 地址进行 AND 运算后，可得知其网络地址为 201.180.60.0，如图 3-8 所示。

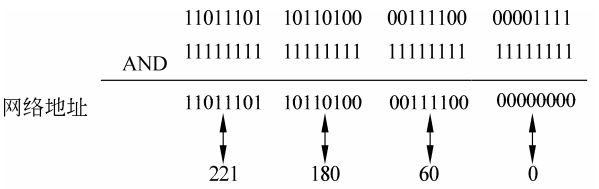


图 3-8 掩码的作用

通常 A 类、B 类和 C 类 IP 地址都有其默认掩码，如图 3-9 所示。

地址类别	默认掩码（十进制）	默认掩码（二进制）
A	255.0.0.0	11111111 .00000000 .00000000 .00000000
B	255.255.0.0	11111111 .11111111 .00000000 .00000000
C	255.255.255.0	11111111 .11111111 .11111111 .00000000

图 3-9 各类地址的默认掩码

提　示

二进制数字“与”运算是对应位数字进行相与，其运算公式为，1 与 1 得 1、1 与 0 得 0、0 与 0 得 0。简而言之，二进制数字的“与”运算公式为：遇 0 得 0。

3.3.2　子网掩码的计算

在对子网进行划分时，需要使用子网掩码，通过子网掩码，能够表明网络中一台主机所在的子网与其他子网的关系，这就需要计算子网掩码。计算子网掩码的方法有利用划分的子网个数和计算子网中主机的数量两种。

1．利用子网数计算子网掩码

在利用子网数计算子网掩码之前，需要了解具体要划分的子网个数，其具体步骤如图 3-10 所示。

例如，现将一网络地址为 129.65.0.0 的网络划分为 27 个子网，其子网掩码的计算方法为：

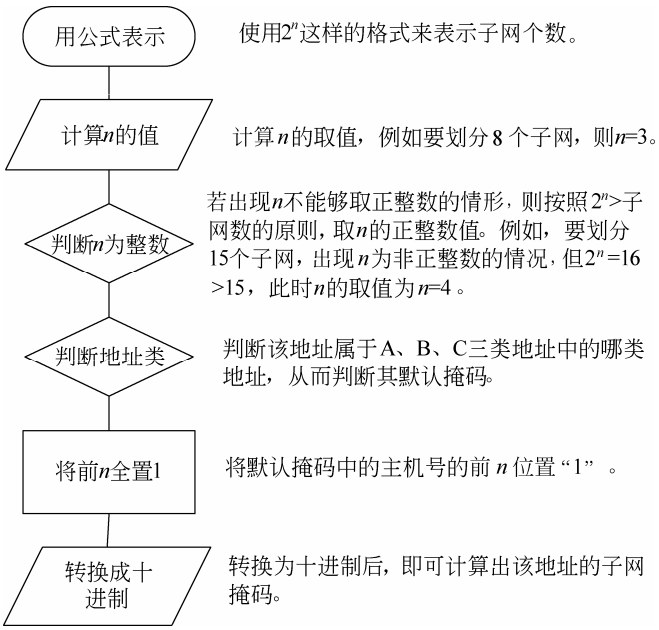


图 3-10 计算子网掩码流程

首先由(2^n=32)>27 确定 n 的取值为 5，然后根据 129.65.0.0 的网络地址，判断其属于 B 类 IP 地址，其默认掩码为 255.255.0.0。最后，将默认掩码中主机号的前 5 位置为 1，即“11111000”，转换为十进制为 248，所以划分子网的子网掩码为 255.255.248.0。

通过前面的介绍，从划分子网的个数就能够判断出其子网掩码，对于 B 类网络来讲，其子网划分个数与子网掩码即每一个子网的主机数有如下关系，如图 3-11 所示。

对于 C 类网络来讲，其划分子网个数与子网掩码及每个子网所能够容纳的主机数量，如图 3-12 所示。

子网个数	子网掩码
2	255.255.128.0
4	255.255.192.0
8	255.255.224.0
16	255.255.240.0
32	255.255.248.0
64	255.255.252.0
128	255.255.254.0
256	255.255.255.0

图 3-11 B 类网络子网个数与子网掩码对应关系

子网个数	子网掩码
2	255.255.255.128
4	255.255.255.192
8	255.255.255.224
16	255.255.255.240
32	255.255.255.248
64	255.255.255.252

图 3-12 C 类网络子网个数与子网掩码对应关系

2．利用主机数计算子网掩码

在利用主机数计算子网掩码时，必须知道每个子网所需容纳的主机个数，而不必知道其需要划分的子网个数，其主要步骤如图 3-13 所示。

例如，要将网络号为 180.195.0.0 的网络划分成若干子网，要求其每个子网能够容纳的主机数量为 900 台，那么其子网掩码计算方法为：首先由(2^n=1024)>900，可以确定 n 的取值为 10，然后根据 180.195.0.0 的网络，判断属于 B 类 IP 地址，其默认掩码为 255.255.0.0，最后，将默认掩码中主机号的所有位全部转换为 1，即“11111111 11111111”，接着按照由低位到高位的顺序将 n=10 位全部转换为 0，即“11111100

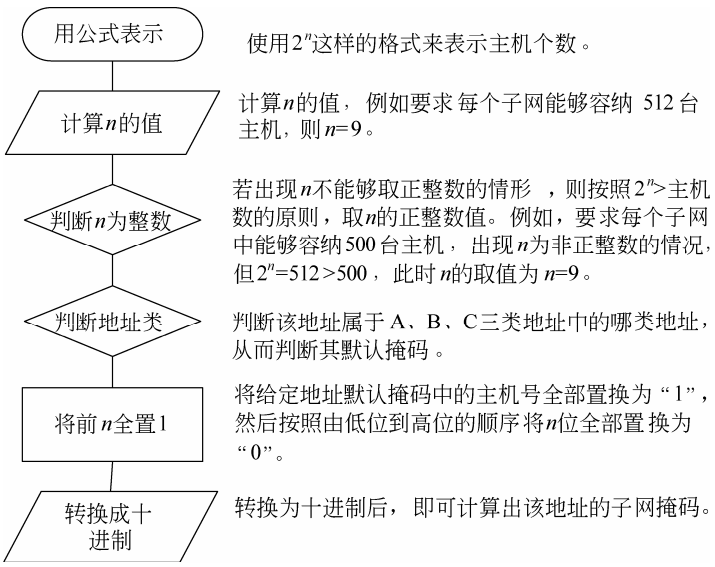


图 3-13 利用主机数计算子网掩码流程

000000”转换成十进制为 252，因此其划分子网的子网掩码为 255.255.252.0。

同过前面的计算，可以得出一个规律，即按照子网能够容纳的主机数量也能够计算出其子网掩码。对于 B 类网络来讲，其子网能够容纳主机数量与子网掩码有如下关系，如图 3-14 所示。

对于 C 类网络来讲，其子网掩码每个子网所能够容纳的主机数量的对应关系，如图 3-15 所示。

每子网容纳主机数量	子网掩码
32766	255.255.128.0
16382	255.255.192.0
8190	255.255.224.0
4094	255.255.240.0
2046	255.255.248.0
1022	255.255.252.0
510	255.255.254.0
254	255.255.255.0

图 3-14 B 网子网掩码与每个子网

每子网容纳主机数量	子网掩码
126	255.255.255.128
62	255.255.255.192
30	255.255.255.224
14	255.255.255.240
6	255.255.255.248
2	255.255.255.252

图 3-15 C 网子网掩码与每个子网

3.3.3 网络号与广播地址

在 IP 地址中，除了人们已经知道的 IP 地址的五类划分及私有地址外，还有网络号和广播地址这两种特殊的 IP 地址。网络地址和广播地址主要用于一些网络协议中，在主机中一般是不允许使用这样的地址的。

1．网络地址

网络号即网络标识，通常表示一个网络。在网络规划或子网划分中，有时需要了解某主机地址属于哪个网络，以便于管理网络，因此读者需要掌握网络地址的计算方法。

IP 地址与默认掩码做“与”运算或与子网掩码做“与”运算，就能够得到网络号。例如，现有一个主机地址为 202.100.10.130，其子网掩码为 255.255.255.224，那么计算该主机地址的所处网络号的方法为：首先，将 202.100.10.130 转换为二进制表示为“11001010 01100100 00001010 10000010”，子网掩码转换为二进制表示为“11111111 11111111 11111111 11100000”。然后将其进行“与”运算可得结果为“11001010 01100100 00001010 10000000”。

其中，计算格式如图 3-16 所示。最后将其使用十进制表示为 202.100.10.128，即 202.100.10.128 就是网络地址。

```
        11001010  01100100  00001010  10000010
AND     11111111  11111111  11111111  11100000
-------------------------------------------------
        11001010  01100100  00001010  10000000
```

图 3-16 计算网络地址

技　巧

在计算主机地址的网络地址时，若给出的是默认掩码，则可立刻得知其网络地址为“网络号+0”，若为非默认掩码时，只需使用该地址的主机号与子网掩码的主机号做“与”运算，得出结果即可，此时网络地址为“网络号+该结果”。

2．广播地址

广播地址是指用来同时向网络上的所有主机发送报文的地址，而不考虑物理网络的特性如何。广播地址又分为有限广播地址和直接广播地址两种。

有限广播地址：它不能被路由但是能够被传送到相同物理网络段上的所有主机，其地址的网络号和主机号全为“1”，即 255.255.255.255，它是一个本网内的广播地址。

直接广播地址：网络中的广播能够被路由，且能够被传送到该地址网络上的每一台主机。其地址的主机号部分全为“1”，如 136.80.255.255 就是一个 B 类地址中的一个广播地址，将信息发送到该地址，就是指将信息发送给网络地址为 136.80 上的所有主机。

在知道了什么是广播地址后，读者还需要了解广播地址是如何计算的。广播地址的计算与默认掩码或子网掩码密切相关。

❑ **利用默认掩码计算广播地址**

这种方法由于没有考虑子网问题，因此其计算较为简单。

例如，IP 地址为 202.100.10.130，默认掩码为 255.255.255.0，计算广播地址。

首先，可计算出其网络地址为 202.100.10.0，那么它的广播地址为 202.100.10.255。即此时广播地址为网络地址与最大主机号之和。

❑ **利用子网掩码计算广播地址**

在使用子网掩码计算广播地址时，由于考虑了子网划分，就不能再使用广播地址为网络地址与最大主机号之和这样的方法来计算广播地址了。此时广播地址为该主机号所属子网段的最后一个地址。

3．计算网络地址

例如，现有一主机地址为 200.100.50.190，子网掩码为 255.255.255.240，那么计算该主机所在网络的广播地址的方法如下所示。

❑ **进制转换**

首先，将主机地址 200.100.50.190 转换为二进制表示为“11001000 01100100 00110010 10111110”，子网掩码转换为二进制表示为“11111111 11111111 11111111 11110000”。然后，将主机地址与子网掩码做“与”运算，计算出它的网络地址为“11001000 01100100 00110010 10110000”，如图 3-17 所示。最后，将该结果转换为十进制为 200.100.50.176。

```
          11001000  01100100  00110010  10111110
AND       11111111  11111111  11111111  11110000
-------------------------------------------------
          11001000  01100100  00110010  10110000
```

图 3-17　计算网络地址

❑ **计算子网掩码所能容纳的主机 IP 地址数**

子网掩码 255.255.255.240 能够容纳的主机 IP 地址数有 $2^4=16$ 个（包括网络地址和广播地址从 0 到 15）。

❑ **地址分段**

按照子网掩码所能容纳主机数量（16 个）将主机 IP 地址进行分段，其分段结果如

下所示：

200.100.50.0～200.100.50.15；
200.100.50.16～200.100.50.31；
200.100.50.32～200.100.50.47；
200.100.50.48～200.100.50.63；
200.100.50.64～200.100.50.79；
200.100.50.80～200.100.50.95；
200.100.50.96～200.100.50.111；
200.100.50.112～200.100.50.127；
200.100.50.128～200.100.50.143；
200.100.50.144～200.100.50.159；
200.100.50.160～200.100.50.175；
200.100.50.176～200.100.50.191；
200.100.50.192～200.100.50.207；
200.100.50.208～200.100.50.223；
200.100.50.224～200.100.50.239；
200.100.50.240～200.100.50.255。

❑ 计算结果

当对其进行分段完成后，能够查看到主机地址 200.100.50.190 属于分段 200.100.50.176～200.100.50.191。因此可以得知其广播地址为 200.100.50.191。

提　示

按照子网掩码所能容纳主机数量将主机 IP 地址分段，其中包括网络地址和广播地址，每个分段的第一个地址为该子网的网络地址，最后一个地址为广播地址。

3.4　地址解析协议和逆地址解析协议

地址解析协议 ARP 和反地址解析协议 RARP 都是特定网络的标准协议。ARP 协议负责把 IP 地址转换为物理网络地址，在 RFC826 中对它进行了描述。而 RARP 协议则是把物理网络地址转换为 IP 地址，在 RFC903 中对它进行了描述。本节将对 ARP 协议和 RARP 协议的相关内容进行详细介绍。

3.4.1　地址解析

在一个单独的物理网络上，通过物理硬件地址识别网络上的各个主机。IP 地址以符号地址的形式对目的主机进行编址。

当这样的一个协议想要把一个数据报发送到目的 IP 地址时，设备驱动程序将不能理解这个目的 IP 地址。因此，必须提供这样一个模块，它能将 IP 地址转换为目的主机的物理地址。通常将一台计算机的 IP 地址转换为物理地址的过程称为地址解析。

地址解析也叫地址之间的映射，它包括两个方面的内容：一种是从 IP 地址到物理地

址的映射；另一种是从物理地址到 IP 地址的映射。

关于这两种地址间的映射，TCP/IP 专门提供了两个协议：ARP 地址解析协议，用于从 IP 地址到物理地址的映射；RARP 反向地址解析协议，用于从物理地址到 IP 地址的映射。

3.4.2 IP 地址与物理地址的映射

实现从 IP 地址到物理地址的映射是非常重要的，任何一次从 IP 层以上（包括 IP 层）发起的数据传输都使用 IP 地址，一旦使用 IP 地址，必然涉及这种映射，否则物理网络便不能识别地址信息，无法进行数据传输。

IP 地址到物理地址映射有表格方式和非表格方式两种方式。

1．表格方式

事先在各主机中建立一张 IP 地址，物理地址映射表。这种方式很简单，但是映射表需要人工建立及人工维护，由于人的速度太慢，因此该方式不适应大规模和长距离网络或映射关系变化频繁的网络。

2．非表格方式

采用全自动技术，地址映射完全由机器自动完成。根据物理地址类型的不同，非表格方式又分为两种，即直接映射和动态联编。

❑ 直接映射

物理地址可分为固定物理地址和可自由配置的物理地址两类，对于可自由配置的物理地址，经过特意配置后，可以将它编入 IP 地址码中，这样，物理地址的解析就变得非常简单，即将它从 IP 地址的主机号部分取出来便是。这种方式就是直接映射。

直接映射直截了当，但适用范围有限，当 IP 地址中主机号部分容纳不下物理地址时，这种方式就会失去作用。

另外，像以太网这样的物理网络，其物理地址是固定的，一旦网络接口更换，物理地址随之改变，采用直接映射也会有问题。

❑ 动态联编

像以太网这样的物理网络具备广播能力。针对这种具备广播能力、物理地址固定的网络，TCP/IP 设计了一种巧妙的动态联编方式进行地址解析，并制定了相应标准，这就是 ARP。动态联编 ARP 的原理是，在广播型网络上，一台计算机 A 欲解析另一台计算机 B 的 IP 地址 BP，计算机 A 首先广播一个 ARP 请求文，请求 IP 地址为 BP 的计算机回答其物理地址。网上所有主机都将收到该 ARP 请求，但只有 B 识别出自己的 IP 地址，并做出应答，向 A 发回一个 ARP 响应，回答自己的 IP 地址。这种解析方式就是动态联编。

为提高效率，ARP 使用了高速缓存技术（Caching），在每台使用 ARP 的主机中，都保留了一个专用的内存区（即高速缓存），存放最近获得的 IP 地址——物理地址联编。一收到 ARP 应答，主机就将信宿机的 IP 地址和物理地址存入缓存。欲发送报文时，首先去缓存中查找相应联编，若找不到，再利用 ARP 进行地址解析。这样就不必每发一个

报文都要事先进行动态联编。实验表明，由于多数据网络通信都需要持续发送多个报文，所以高速缓存大大提高了 ARP 的效率。

3.4.3 反向地址解析协议 RARP

反向地址解析协议（Reversed Address Resolution Protocol，RARP），可以实现物理地址到 IP 地址的转换。无盘工作站在启动时，只知道自己的物理地址，而不知道自己的 IP 地址。它首先使用 RARP 协议得到自己的 IP 地址后，才能和服务器通信。

在一台无盘工作站启动时，工作站首先以广播方式发出 RARP 请求。同一网络上的 RARP 服务器就会根据 RARP 请求中的物理地址为该工作站分配一个 IP 地址，生成一个 RARP 响应包发送回去。RARP 数据包和 ARP 数据包的格式几乎完全一样。唯一的差别在于 RARP 请求包中是由发送者填好源端物理地址，而源端 IP 地址为空（需要查询）。在同一个子网上的 RARP 服务器接收到请求后，填入相应的 IP 地址，然后发送回源工作站。

RARP 与 ARP 相比，有如下几个方面的改变。

- ARP 只假定所有主机知道它们各自的硬件地址和协议地址之间的映射。RARP 要求网络上的一个或者多个主机来维护硬件地址和协议地址间映射的数据，以便它们能够回答客户主机的请求。
- 由于这个数据库能够采用的最大容量。服务器的部分功能通常在适配器的微代码处实现，在微代码中有选择地实现一个小型缓存。然后，微代码部分仅仅负责 RARP 帧的接收和传输，RARP 映射本身由服务器软件处理，作为主机中的一个普通进程运行。
- 这个数据库的性质还需要用某些软件来人工建立和更新数据库。
- 在网络上有多个 RARP 服务器的情况下，RARP 请求主机只使用它的广播 RARP 请求所接收到的第一个 RARP 应答，而丢弃所有其他应答。

3.5 IPv6 协议及寻址

IPv6（Internet Protocol version 6，互联网通讯协议第 6 版）是被指定为 IPv4 继任者的下一代互联网协议版本，互联网中最先出现的应用到现在依然占有优势。

3.5.1 什么是 IPv6

IPv6 在 1998 年 12 月由互联网工程任务小组（Internet Engineering Task Force，IETF）通过公布互联网标准规范（RFC 2460）的方式定义出台。

IPv6 具有比 IPv4 大得多的地址空间。这是因为 IPv6 使用了 128 位的地址，而 IPv4 只用 32 位。

IPv6 中可能的地址有 $2^{128} \approx 3.4\times10^{38}$ 个。也可以考虑为 16^{32} 个，因为 32 位地址每位可以取 16 个不同的值。

在很多场合，IPv6 地址由两个逻辑部分组成：一个 64 位的网络前缀和一个 64 位的主机地址，主机地址通常根据物理地址自动生成，叫做 EUI-64（或者 64 位扩展唯一标识）。

3.5.2 IPv6 格式

IPv6 二进位制下为 128 位长度，以 16 位为一组，每组以冒号（:）隔开，可以分为 8 组，每组以 4 位十六进制方式表示。例如，“2001:0db8:85a3:08d3:1319:8a2e:0370:7344”是一个合法的 IPv6 位址。

同时 IPv6 在某些条件下可以省略，以下是省略规则。

1．省略规则一

每项数字前导的 0 可以省略，省略后前导数字仍是 0 则继续，如下组 IPv6 是等价的。

2001:0DB8:02de:0000:0000:0000:0000:0e13
2001:DB8:2de:0000:0000:0000:0000:e13
2001:DB8:2de:000:000:000:000:e13
2001:DB8:2de:00:00:00:00:e13
2001:DB8:2de:0:0:0:0:e13

2．省略规则二

若有连贯的 0000 的情形出现，可以用双冒号（::）代替。

如果 4 个数字都是零，可以被省略。例如下组 IPv6 是等价的。

2001:DB8:2de:0:0:0:0:e13
2001:DB8:2de::e13

遵照以上省略规则，下面这组 IPv6 都是等价的。

2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab

不过请注意有的情形下省略是非法的，例如“2001::25de::cade”IPv6 地址是非法的。因为，它有可能是以下几种情形之一，造成无法推断。

2001:0000:0000:0000:0000:25de:0000:cade
2001:0000:0000:0000:25de:0000:0000:cade
2001:0000:0000:25de:0000:0000:0000:cade
2001:0000:25de:0000:0000:0000:0000:cade

如果这个地址实际上是 IPv4 的地址，后 32 位可以用十进制数表示；因此，“::ffff:192.168.89.9”等价于“::ffff:c0a8:5909”，但不等价于“::192.168.89.9”和“::c0a8:5909”。

“::ffff:1.2.3.4”格式叫做 IPv4 映射位址。而“::1.2.3.4”格式叫做 IPv4 一致位址，目前已被取消。

IPv4 地址可以很容易地转化为 IPv6 格式，如 IP 地址为 135.75.43.52（十六进制为 0x874B2B34），它可以被转化为“0000:0000:0000:0000:0000:ffff:874B:2B34”或者“::ffff:874B:2B34”。同时，还可以使用混合符号（IPv4-Compatible Address），则地址可以为“::ffff:135.75.43.52”。

3.5.3 IPv6 的特性

IPv6 协议改进了 IPv4 协议报头，并提供了一些新的机制，从而很好地解决了诸如移动性、安全性、多媒体传输等问题。

1．新的报文结构

IPv6 使用了全新的协议头格式，在 IPv6 报文头中包括基本报头和可扩展报头两部分，其格式如图 3-18 所示。

图 3-18 报文结构

其中，基本报头与原 IPv4 报头类似，但在 IPv6 报头中添加了一些新的字段，以及改变了某些字段，如图 3-19 所示。

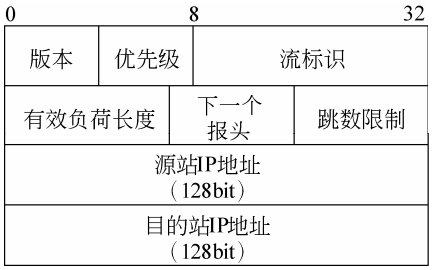


图 3-19 IPv6 报头

扩展报头中提供了许多额外信息，共分为 6 种扩展报头，且它们是可选的。当有多个扩展报头时，这些扩展报头必须按照一定的排列次序跟在基本报头之后，如表 3-4 所示。

IPv6 采用 128 位 IP 地址，其地址空间为 2^{128}。此外，一些非根本性的和可选择的字段被移动到了 IPv6 协议头之后的扩展协议中，从而简化了路由器的选择过程，使得网络中的中间路由器在处理 IPv6 协议头时，有更高的效率。

表 3-4 报头所包含信息

类　型	描　述
站到站选项	用于描述路由器的各种信息
源路由报头	指明数据报到达目换站所必须经过的路由器
分片报头	用于数据报的分片管理
身份验证报头	用于接收端对发送端身份的验证
加密报头	用于传输经过加密的报文信息
目的地选项	有关数据报接收端的附加信息

2．新的地址配置方式

随着网络技术的发展，在 Internet 上的结点不再单单是计算机了，它将发展成为包括个人数字助理（PDA）、移动电话（Mobile Phones），甚至包括冰箱、电视等家用电器，这就要求 IPv6 主机地址配置更加简化。

因此，为了达到简化地址配置的目的，在 IPv6 中除了支持手动地址配置和有状态自动地址配置（使用专用的地址分配服务器动态分配地址）外，还支持一种无状态的地址配置技术。

在该技术中，网络上的主机能够给自己自动配置 IPv6 地址，在同一链路上，所有主机不需人工干涉就可以进行通讯。

3．QoS（服务质量）保证

在 IPv6 的基本报头中新定义了一种被称为流标识的全新字段。它使得网络中的路由器能够对属于一个流标识的数据包进行识别并提供特殊处理。

IPv6 的流标识字段，使得路由器可以在不打开传输的内层数据包的情况下就可以识别流，这就是说即使数据包有效负荷已经进行了加密，但仍然可以实现对 QoS 的支持。

提　示

QoS（服务质量）是指网络提供更高优先服务的一种能力，它包括专用带宽、抖动控制和延迟（用于实时和交互式流量的情况）、丢包率的改进以及不同 LAN、MAN 和 WAN 技术下的指定网络流量等，同时确保为每种流量提供的优先权不会阻碍其他流量的进程。

4．支持实时音频和视频传输

在 IPv6 的报头结构中取消了服务类型字段，增加了流标识字段。该字段除了能提供 QoS 外，还使得源主机可以请求对数据做出特殊的处理，如能够支持实时音频和视频的传输。

5．移动性

在 IPv6 的可扩展报头中，采用了 Routing Header（路由报头）和 Destination Option Header（目的地选项报头）报头类型，使得 IPv6 对移动性提供了内在的支持。

在 IPv6 中能够给移动结点分配一个本地地址，通过此地址总可以访问到它。在移动结点位于本地时，它连接到本地链路并使用其本地地址。在移动结点远离本地时，本地代理（通常是路由器）在该移动结点和正与其进行通信的结点之间传递消息。

这样就达到了设备能够在 Internet 上随意改变位置但仍能够维持现有连接的目的。

3.5.4　IPv6 地址分类

IPv6 地址根据接口不同可以分为单播 IPv6 地址、多播 IPv6 地址和任播 IPv6 地址，其具体介绍如下所述。

1．单播 IPv6 地址

单播 IPv6 地址是指具有单一接口的地址，其中一个单接口有一个标识符。发送给一个单播地址的数据包被送到由该地址标识的接口。

通常，单播地址在逻辑上划分为子网前缀和接口 ID 两部分，如图 3-20 所示。其中接口 ID 用于标识链路接口，在

n bit	(128-*n*) bit
子网前缀	接口 ID

图 3-20　单播地址格式

该链路中其值必须是唯一的，一个接口标识符应与该接口的链路层地址相同，该链路通常由子网前缀来标识。

在 IPv6 单播地址中，如果所有位全部为“0”，那么称该地址为未指定地址，用文本形式表示为“::”，它不能分配给任何结点。另外，IPv6 单播地址“::1”或“0:0:0:0:0:0:0:1”称为环回地址，常用于结点向自己发送数据包，它不能分配给任何物理接口。

2．多播 IPv6 地址

多播 IPv6 地址是指一组接口的地址（通常分属不同结点），其中这一组接口具有一个标识符，如图 3-21 所示。发送到一个多播地址的数据包被送到由该地址标识的每个接口上。简单地说，多播地址就是一组结点的标识符。

8 bit	4	4 bit	112 bit
11111111	Flag	Extent	Group ID

图 3-21　多播地址格式

第一字段是标识字段，共占 8 位，所有位全部为“1”，用于标识该地址是一个多播地址。

Flag（标志字段），共占 4 位，其格式为“000T”。其中前 3 位为高位是保留位，其初始值为 0；T 的取值包括 0 和 1。若 T=0，则表示一个永久分配的多播地址，由全球 Internet 编号机构进行分配；若 T=1，则表示一个非永久的多播地址。

Extent（范围字段），共占 4 位，主要用于限制多播组的范围。该字段的可能取值。

Group ID（组标识），共占 112 位，主要用于标识多播组，可以是永久的也可以是临时的。

3．任播 IPv6 地址

任播 IPv6 地址也称为任意点播 IPv6 地址，它是指一组接口的地址（一般属于不同结点）具有一个标识符，发送到任播地址的数据包被送到由该地址标识的、根据路由选择距离度量最近的一个接口上。

任播地址是从单播的地址空间分配而来，可用任何一种规定的单播地址格式。因此，在语法上是无法区别单播地址和任播地址的。当一个单播地址分配给多个接口时，如果把它转为任播地址，那么被分配该地址的结点，必须显示地配置，以便知道这是一个任播地址。

对于任何一个已经分配的单播地址，有一个最长的地址前缀 P 用来标识拓扑地区。在该区域中，所有接口均属于该任播地址。

在前缀 P 内，任播组的每个成员，被告知在选录系统中作为一个独立实体（主机路由）；在前缀 P 以外，任播地址可以集合在前缀 P 的选路通告中。假如，出现 P 为 0 的前缀，那么说明该组成员可能没有拓扑位置。

此时，任播地址将在整个 Internet 上，被告知作为一个分离的选路实体，这样对于任播地址的使用将带来限制。其限制包括：任播地址不能用作 IPv6 包的源地址；任播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。其中，预定的子网路由器任播地址格式如图 3-22 所示。

n bit	(128-*n*) bit
子网前缀	00000000000000

图 3-22　任播地址格式

在该格式中，子网前缀用来标识一条特定链路；接口标识为“0”的链路上的一个接口，其任播地址与单播地址在语法上是相同的。

3.5.5 主机和路由器地址

在 IPv6 协议中，不仅主机 IP 地址有所不同，网络设备路由器地址也与 IPv4 协议中的路由器地址不同。

1．主机地址

在 IPv6 中，一台主机可同时拥有的单点传送地址有每个接口的链路本地地址、每个接口的单点传送地址和环路接口的环路地址（::1）。

另外，每台 IPv6 主机至少有接收本地链路信息的链路本地地址和路由的站点本地地址或全球地址。同时每台主机还需要时刻保持收听包括以下几个方面的多点传送地址上的信息：

- 结点本地范围内所有结点组播地址（FF01::1）。
- 链路本地范围内所有结点组播地址（FF02::1）。
- 请求结点（Solicited-node）多播地址（如果主机的某个接口加入请求结点组）。
- 多播组多点传送地址（如果主机的某个接口加入任何多播组）。

2．路由器地址

在 IPv6 中，一台路由器可被分配以下几种类型的单播地址。

- 每个接口的链路本地地址。
- 每个接口的单点传送地址（包括一个站点本地地址和一个或多个可聚集全球地址）。
- 子网-路由器任播地址。
- 其他任播地址（可选）。
- 环路接口的环路地址（::1）。

此外，与主机地址类似，路由器同样需要时刻保持收听多点传送地址上的信息。

- 结点本地范围内的所有结点多播地址（FF01::1）。
- 结点本地范围内的所有路由器多播地址（FF01::2）。
- 链路本地范围内的所有结点多播地址（FF02::1）；链路本地范围内的所有路由器多播地址（FF02::2）。
- 站点本地范围内的所有路由器多播地址（FF05::2）。
- 请求结点（Solicited-Node）多播地址（如果路由器的某个接口加入请求结点组）。
- 多播组多点传送地址（如果路由器的某个接口加入任何多播组）。

3.6 练习：子网划分

为了提高 IP 地址的使用效率，可将一个个网络划分为子网。采用借位的方式，从主机位最高位开始借位变成新的子网位，所剩余的部分仍为主机位。

1. 实验目的

- ❑ 查看 IP 地址
- ❑ 划分子网

2. 实验步骤

1 按下 Windows+R 键，打开【运行】对话框，在文本框中输入“cmd”命令，单击【确定】按钮，如图 3-23 所示。

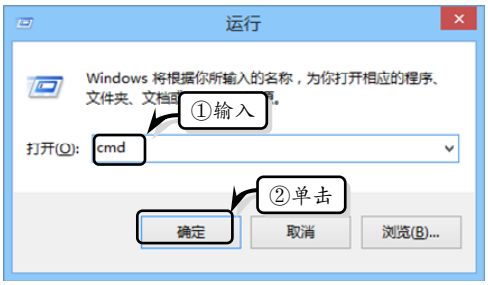


图 3-23 输入运行命令

2 在弹出的窗口中输入 ipconfig 命令，按下 Enter 键，即可查看 IP 地址，如图 3-24 所示。

图 3-24 查看 IP 地址

3 下载并运行“子网计算机工具”软件，在界面中激活【主机 IP->本子网 IP】选项卡，并输入主机 IP 地址，如图 3-25 所示。

4 激活【网络 IP->各子网 IP】选项卡，输入网络地址。然后，单击【要划分的子网数量】下拉按钮，选择数量 8，如图 3-26 所示。

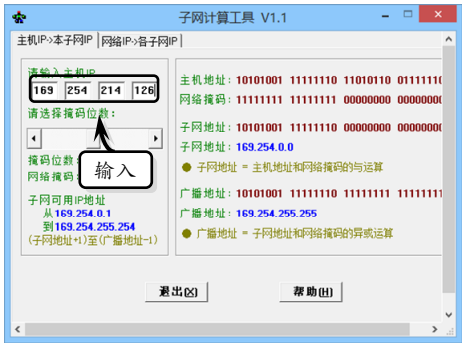


图 3-25 输入 IP 地址

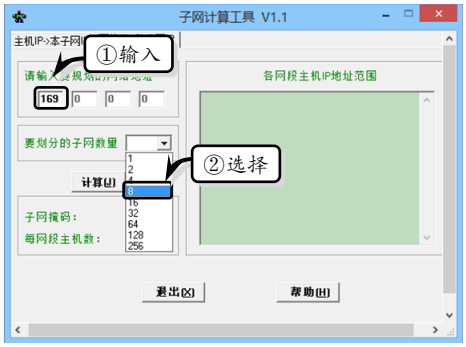


图 3-26 输入规划网络地址

5 单击【计算】按钮，在右侧【各网段主机 IP 地址范围】栏下方的列表框中，将显示出规划的子网 IP，如图 3-27 所示。

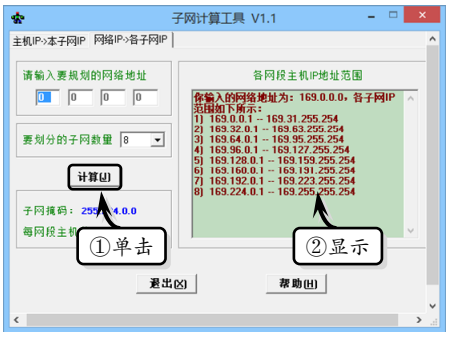


图 3-27 规划子网 IP

3.7 练习：安装协议

IPX/SPX 协议即 IPX 与 SPX 协议的组合，它是 Novel 公司为了适应网络的发展而开发的通信协议，具有很强的适应性，安装方便，同时还具有路由功能，要以实现多网络间的通信。IPX/SPX 协议一般可以应用于大型网络和局域网游戏环境内中，下面将以 Windows 8 系统为例，详细介绍安装 IPX/SPX 的操作方法。

1. 实验目的

- ❑ 打开网络连接
- ❑ 添加网络协议

2. 实验步骤

1 右击任务栏托盘中的【网络】图标，执行【打开网络和共享中心】命令，在弹出的窗口中选择【更改适配器设置】选项，如图 3-28 所示。

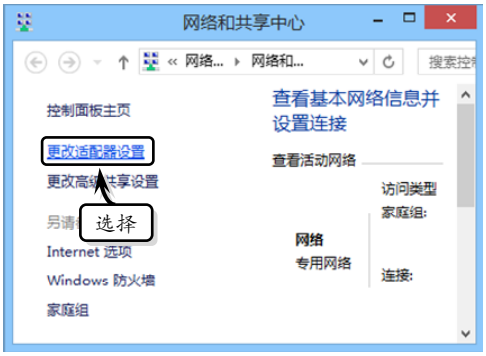


图 3-28 【网络和共享中心】对话框

2 在弹出的【网络连接】对话框中，右击【以太网】图标，执行【属性】命令，如图 3-29 所示。

图 3-29 选择连网方式

3 在弹出的【以太网 属性】对话框中，选择【此连接使用下列项目】列表框中的【Internet 协议版本 4（TCP/IPv4）】选项，并单击【安装】按钮，如图 3-30 所示。

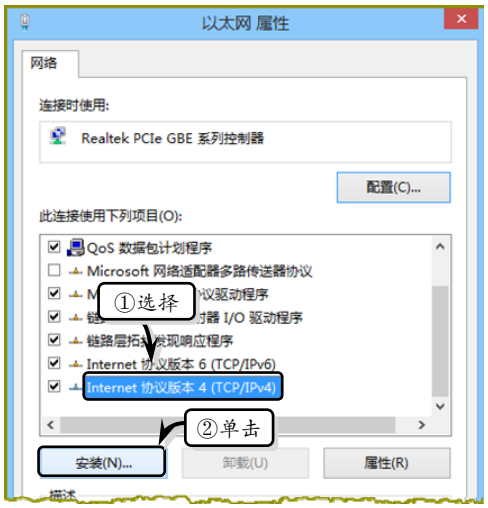


图 3-30 选择安装协议

4 在弹出的【选择网络功能类型】对话框中，选择【协议】选项，并单击【添加】按钮，如图 3-31 所示。

5 在弹出的【选择网络协议】对话框中，根据自身计算机的安装需求选择相应的协议，并单击【确定】按钮，如图 3-32 所示。

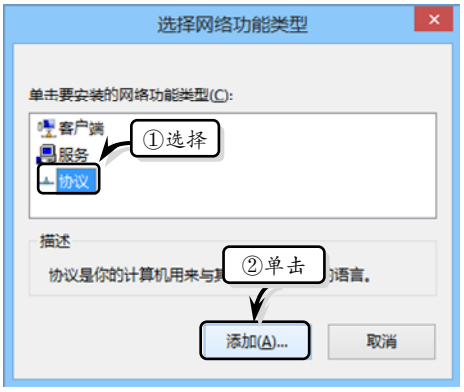


图 3-31 选择网络功能类型

图 3-32 选择网络协议

3.8 思考与练习

一、填空题

1. _____是 OSI 参考模型中的第三层，TCP/IP 中的第二层。

2. 网络层的目的在源和目的子网结点之间选择路由，主要功能是_____。

3. 虚电路表示这只是一条_____，分组都沿着这条逻辑连接按照存储转发方式传送，而并不是真正建立了一条物理连接。

4. 网络层向上只提供简单灵活的、无连接的、尽最大努力交付的_____。

5. TCP/IP 的网络层被称为网际层或 IP 层，其以数据报的形式向_____提供面向无连接的服务。

6. 路由算法是提高_____功能，尽量减少路由时所带来的开销的算法。

7. 关于路由器如何收集网络的结构信息以及对之进行分析来确定最佳路由，有两种主要路由算法，分别为_____和_____。

二、选择题

1. _____是网络层的通信设备之一。

A. 网桥　　B. 中继器

C. 路由器　　D. 网关

2. 假如一台连接到网络上的计算机的网络配置为：IP 地址=136.62.2.55，子网掩码=255.255.192.0，网关地址=136.62.89.1。这台计算机在网络中不能与其他主机进行通信，其中_____设置导致了问题的产生。

A. 子网掩码　　B. 网关地址

C. IP 地址　　D. 其他配置

3. 下列最好的描述了循环冗余检验特征的是_____。

A. 逐个地检查每一个字符

B. 查出 99%以上的差错

C. 查不出有偶数上位出错的差错

D. 不如纵向冗余检查可靠

4. 在虚电路方式中，_____。

A. 能保证每个分组正确到达，但分组的顺序发生了变化

B. 能保证每个分组正确到达，且分组的顺序与原来的一样

C. 不能保证每个分组正确到达，且分组的顺序发生了变化

D. 不能保证每个分组正确到达，而且有的分组会丢失

5. 网络层的主要功能中不包括_____。

A. 路径选择

B. 数据包交换

C. 实现端与端的连接

D. 网络连接的建立与拆除

三、简答题

1. 网络层有哪些协议？

2. 路由算法的优化原则是什么？

3. 子网划分的概念是什么？

四、上机练习

1．添加简单网络管理协议

如果用户需要通过 IIS（Internet 信息服务）建立一个本地站点，首先应该先安装 IIS 组件。首先，打开【控制面板】窗口，选择【程序】选项，并选择【启用或关闭 Windows 功能】选项。然后，在弹出的【Windows 功能】对话框中，启用【简单网络管理协议（SNMP）】复选框，单击【确定】按钮即可，如图 3-33 所示。

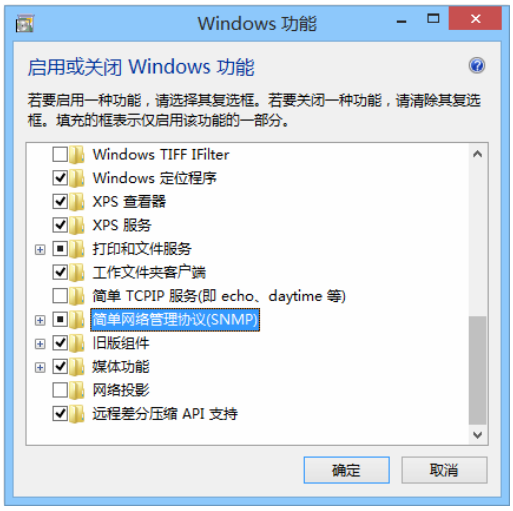


图 3-33　添加 Hyper-V

2．卸载已安装的协议

当计算机上安装的协议与计算机中的另一个协议发生冲突时，用户需要删除一个协议，以保证计算机正常运行。如果用户需要删除安装的 IPX/SPX 协议，右击任务栏托盘中的【网络】图标，执行【打开网络和共享中心】命令，选择【更改网络适配器】选项。然后，右击【以太网】图标，执行【属性】命令。在弹出的【以太网 属性】对话框中，选择【此连接使用下列项目】列表框中的一种协议，单击【卸载】按钮即可，如图 3-34 所示。

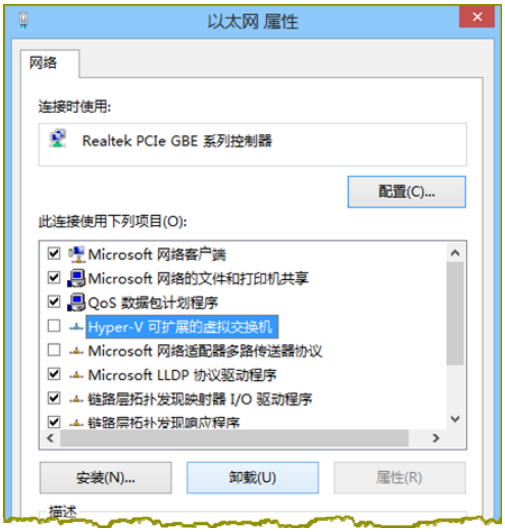


图 3-34　卸载已安装的协议