第3章 IP 地 址

IP 地址是因特网技术中的一个非常重要的概念，IP 地址在 IP 层实现了底层网络地址的统一，使因特网的网络层地址具有全局唯一性和一致性。IP 地址含有位置信息，反映了主机的网络连接，是因特网进行寻址和路由选择的依据。本章在介绍 IP 地址概念、IP 地址分类的基础上，讨论了与 IP 地址相关的子网技术、超网技术以及无类网络地址。

3.1 IP 地址概述

地址是标识对象所处位置的标识符。传输中的信息带有源地址和目的地址，分别标识通信的源结点和目的结点，即信源和信宿。目的地址是传输设备为信息进行寻址的依据。

不同的物理网络技术（底层网络技术）通常具有不同的编址方式，这种差异主要表现在不同的地址结构和不同的地址长度上。

在一个物理网络中，每个结点都至少有一个机器可识别的地址，该地址叫作物理地址。

物理地址有两个特点：不一致性和不唯一性。不一致性是指不同的物理网络技术采用不同的编址方式；不唯一性是指不同的物理网络中结点的物理地址可能重复。

为了保证寻址的正确性，必须确保一个网络中结点地址的唯一性，这一要求在单一的物理网络中很容易得到满足。但是当多个不同的物理网络进行互联时，这种唯一性就难以得到保证。另外，不同物理网络在地址编址方式上的不统一会给寻址带来极大的不便。因此，在进行网络互联时首先要解决的问题是物理网络地址的统一问题。在第 2 章我们已经提到因特网是在网络级进行互联的，因此，因特网在网络层（IP 层）完成地址的统一工作，将不同物理网络的地址统一到具有全球唯一性的 IP 地址上，IP 层所用到的地址叫作因特网地址，又称为 IP 地址。实现地址统一的概念模式如图 3-1 所示。

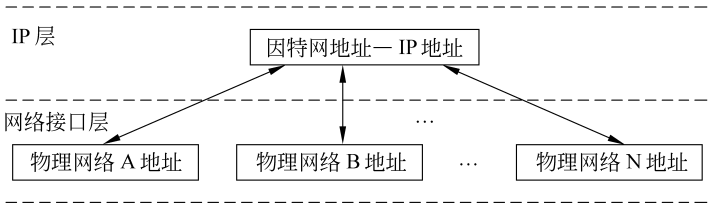

图 3-1 用 IP 地址统一物理网络地址

因特网采用一种全局通用的地址格式，为全网的每一个网络和每一台主机都分配一个因特网地址，以此屏蔽物理网络地址的差异。

早期的 ARPANET 的主机地址就采用了层次型地址（P，N），这种地址体现了网络的层次结构，便于进行寻址。寻址时先找到主机所在的网点 P，然后再根据 N 找到该网点中的主机。因特网沿用了 ARPANET 的思想，仍然采用层次型地址。因特网由网络互联而成，

网络由主机互联而成。因此，IP 地址由网络号和主机号构成，如图 3-2 所示。IP 地址可以表示为：

IP-address :: = {<Network-number>,<Host-number>}

网络号(Network-number)	主机号(Host-number)

图 3-2　因特网 IP 地址结构

其中网络号的长度决定整个因特网中能包含多少个网络，主机号的长度决定每个网络能容纳多少台主机。网络号的长度并不是固定的。通常因特网中的网络数难以确定，但每个网络的预期规模却比较容易确定。

因特网的 IP 协议提供了一种整个因特网通用的地址格式(保证一致性)，并在统一管理下进行 IP 地址的分配(保证唯一性)，确保一个地址对应一台因特网主机(或路由器)，这样，对上层而言物理地址的差异就被 IP 层屏蔽了。

因特网地址是一种层次型地址，它携带了关于对象位置的信息。因特网所要处理的对象比广域网要复杂得多，无结构的地址是不能担此重任的。由于 IP 地址标识了一个主机的位置(所属的网络)，当将一台主机从一个网络移到另一个网络时必须改变这台主机的 IP 地址。

IPv4 规定，因特网地址长度为 32 位(IPv6 规定地址长度为 128 位)。因此，IPv4 的地址空间为 2^{32}，即 4 294 967 296 个 IP 地址。本书中所涉及的 IP 地址若不特别说明，则指 IPv4 地址。

IP 地址一般用点分十进制数表示，例如 202.119.84.120。这 4 个用点分隔的段分别对应 4 个字节。IP 地址也可以用二进制(如 11001010 01110111 01010100 01111000)或十六进制(如 0XCA775478)表示。IP 地址的二进制表示法在讨论地址类别和掩码时经常会用到，而十六进制表示法则很少使用。

3.2　分类 IP 地址

传统的因特网采用分类地址。因特网定义了 5 类 IP 地址：A 类、B 类、C 类、D 类和 E 类，如图 3-3 所示。

	第 1 个字节	第 2 个字节	第 3 个字节	第 4 个字节	第1个字节取值	网络号	主机号
A 类：	0				0~127	1 字节	3 字节
B 类：	10				128~191	2 字节	2 字节
C 类：	110				192~223	3 字节	1 字节
D 类：	1110				224~239		
E 类：	1111				240~255		

图 3-3　因特网 IP 地址类别

其中 A、B 和 C 是 3 个基本的类别，分别代表不同规模的网络。A 类地址由 1 个字节的网络号和 3 个字节的主机号构成，用于少量的大型网络。B 类地址由 2 个字节的网络号和 2 个

字节的主机号构成,用于中等规模的网络。C 类地址由 3 个字节的网络号和 1 个字节的主机号构成,用于小规模的网络。

各类网络所占因特网地址空间的比例如图 3-4 所示。

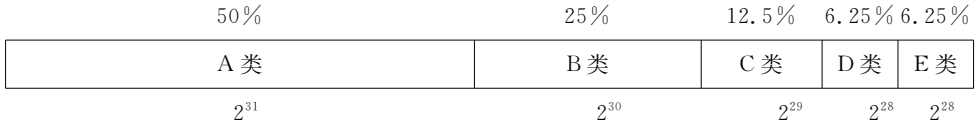

图 3-4　因特网 IP 地址空间

A 类地址第 1 个字节的最高位固定为 0,另外 7 位可变的网络号可以标识 128 个网络(0～127),0 一般不用,127 用作环回地址。所以共有 126 个可用的 A 类网络。A 类地址的 24 位主机号可以标识 1 677 216 台主机(2^{24}=1 677 216),主机号为全 0 时用于表示网络地址,主机号为全 1 时用于表示广播地址,这两个主机号不能用来标识主机。所以,每个 A 类网络最多可以容纳 1 677 214 台主机。A 类地址第 1 个字节的取值范围为0～127。

B 类地址第 1 个字节的最高 2 位固定为 10,另外 14 位可变的网络号可以标识 2^{14}=16 384 个网络。16 位主机号可以标识 65 536 台主机(2^{16}=65 536),由于主机号不能为全 0 和全 1。所以,每个 B 类网络最多可以容纳 65 534 台主机。B 类地址的第 1 个字节的取值范围为 128～191。

C 类地址第 1 个字节的最高 3 位固定为 110,另外 21 位可变的网络号可以标识 2^{21}=2 097 152 个网络。8 位主机号可以标识 256 台主机(2^8=256),由于主机号不能为全 0 和全 1。所以,每个 C 类网络最多可以容纳 254 台主机。C 类地址的第 1 个字节的取值范围为 192～223。

D 类地址用于组播(multicasting)。因此,D 类地址又称为组播地址。D 类地址的范围为 224.0.0.0～239.255.255.255,每个地址对应一个组,发往某一组地址的数据将被该组中的所有成员接收。D 类地址不能分配给主机。D 类地址的第 1 个字节的取值范围为 224～239。有些 D 类地址已经分配用于特殊用途,如 224.0.0.0 是保留地址,224.0.0.1 是指本子网中的所有系统,224.0.0.2 是指本子网中的所有路由器,224.0.0.9 是指运行 RIPv2 路由协议的路由器,224.0.0.11 是指移动 IP 中的移动代理。另外,还有一些 D 类地址留给了网络会议,如 224.0.1.11 用于 IETF-1-AUDIO,224.0.1.12 用于 IETF-1-VIDEO。

E 类地址为保留地址,可以用于实验目的。E 类地址的范围为 240.0.0.0～255.255.255.254,E 类地址的第 1 个字节的取值范围为 240～255。

在分类地址网络中每个网络占用一个地址块。各类网络地址块的示例如表 3-1 所示。

表 3-1　各类网络地址块的示例

类别	起始地址	结束地址	网络地址	主机地址范围	广播地址
A 类	86.0.0.0	86.255.255.255	86.0.0.0	86.0.0.1～86.255.255.254	86.255.255.255
B 类	188.6.0.0	188.6.255.255	188.6.0.0	188.6.0.1～188.6.255.254	188.6.255.255
C 类	206.8.2.0	206.8.2.255	206.8.2.0	206.8.2.1～206.8.2.254	206.8.2.255

从表 3-1 中可看出,每个网络都要占用两个 IP 地址,一个用于标识网络,另一个用于网

络广播。每个网络使用该网络地址块的起始地址作为网络地址，该地址仅作为网络的标识，主要用在网络路由中。网络地址块的结束地址被用作该网络的广播地址。

在因特网的地址中包含了网络信息。当一个路由器或网关连到多个网络上时，每个网络都会给路由器或网关分配一个 IP 地址，设备有多少个网络连接，就有多少个 IP 地址。而且这些 IP 地址分别属于不同的网络，这对于路由选择来说是非常有用的。一台主机也可以连接多个网络，这种主机叫作多宿主主机(multi-homed host)。多宿主主机拥有多个 IP 地址，每个地址对应一条物理连接。由此可见，因特网地址的本质是标识主机的网络连接。图 3-5 给出了多宿主设备的地址配置。

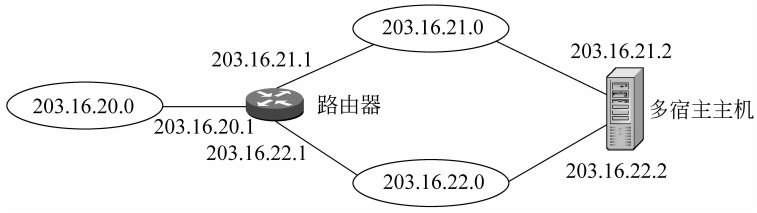

图 3-5　IP 地址标识网络连接

因特网地址是由中央管理机构分配的。一个组织加入因特网时，将会从因特网的网络信息中心 InterNIC 获得网络前缀，然后负责组织内部的地址分配。这样，既解决了全局唯一性问题，又分散了管理负担。

3.3　特殊 IP 地址

在 IP 地址中有些地址并不是用来标识主机的，这些地址具有特殊意义。这些地址包括网络地址、直接广播地址、受限广播地址、本网络地址、环回地址等。

1. 网络地址

因特网上的每个网络都有一个 IP 地址，其主机号部分为 0。

网络地址的一般表达式为：

{<Network-number>,<Host-number>}={<Network-number>,0}

该地址用于标识网络，不能分配给主机，因此不能作为数据的源地址和目的地址。网络地址的使用可以减小路由表的规模。

A 类网络的网络地址为：Network-number.0.0.0。例如 120.0.0.0。

B 类网络的网络地址为：Network-number.0.0。例如 139.22.0.0。

C 类网络的网络地址为：Network-number.0。例如 203.120.16.0。

2. 直接广播地址

直接广播(direct broadcast)是指向某个网络上的所有主机发送报文。TCP/IP 规定，主机号各位全部为 1 的 IP 地址用于广播，称为直接广播地址。路由器在目标网络处将 IP 直接广播地址映射为物理网络的广播地址，以太网的广播地址为 6 个字节的全 1 二进制位，即 ff:ff:ff:ff:ff:ff。

直接广播地址的一般表达式为：

{<Network-number>,<Host-number>}={<Network-number>, −1}

这里的－1 表示全 1。

直接广播地址只能作为目的地址。

A 类网络的直接广播地址为：Network-number. 255. 255. 255。例如 120. 255. 255. 255。

B 类网络的直接广播地址为：Network-number. 255. 255。例如 139. 22. 255. 255。

C 类网络的直接广播地址为：Network-number. 255。例如 203. 120. 16. 255。

3. 受限广播地址

直接广播要求发送方必须要知道信宿网络的网络号。但有些主机在启动时，往往并不知道本网络的网络号，这时候如果想要向本网络广播，只能采用受限广播地址(limited broadcast address)。

受限广播地址是在本网络内部进行广播的一种广播地址。TCP/IP 规定，32 位全为 1 的 IP 地址用于本网络内的广播。

受限广播地址的一般表达式为：

{<Network-number>,<Host-number>}={－1, －1}

受限广播地址的点分十进制表示为：255. 255. 255. 255。

受限广播地址只能作为目的地址。

路由器将隔离受限广播，不对受限广播分组进行转发。也就是说因特网不支持全网络范围的广播，这也是为了对网络进行保护，以防网络带宽被过多地占用。

4. 本网络地址

TCP/IP 协议规定，网络号各位全部为 0 时表示的是本网络。本网络地址分为两种情况：本网络特定主机地址和本网络本主机地址。

本网络特定主机地址的一般表达式为：

{<Network-number>,<Host-number>}={0, <Host-number>}

本网络特定主机地址只能作为源地址。

A 类网络的本网络特定主机地址为：0. Host-number。例如 0. 10. 130. 12。

B 类网络的本网络特定主机地址为：0. 0. Host-number。例如 0. 0. 135. 12。

C 类网络的本网络特定主机地址为：0. 0. 0. Host-number。例如 0. 0. 0. 12。

本网络本主机地址的一般表达式为：

{<Network-number>,<Host-number>}={0, 0}

本网络本主机地址的点分十进制表示为：0. 0. 0. 0。

本网络本主机地址只能作为源地址。

若主机启动时不知道自己的 IP 地址(或因为是无盘工作站，或未配 IP 地址)，则采用网络号和主机号都为 0 的本网络本主机地址作为源地址。

5. 环回地址

环回地址(loopback address)是用于网络软件测试以及本机进程之间通信的特殊地址。A 类网络地址 127 被用作环回地址。

环回地址的一般表达式为：

{<Network-number>,<Host-number>}={127, <any>}

但习惯上采用 127. 0. 0. 1 作为环回地址，并将其命名为 localhost。

当使用环回地址作为目的地址发送数据时，数据将不会被发送到网络上，而是在数据离开网络层时将其回送给本机的有关进程。环回接口对 IP 数据报的处理过程如图 3-6 所示。

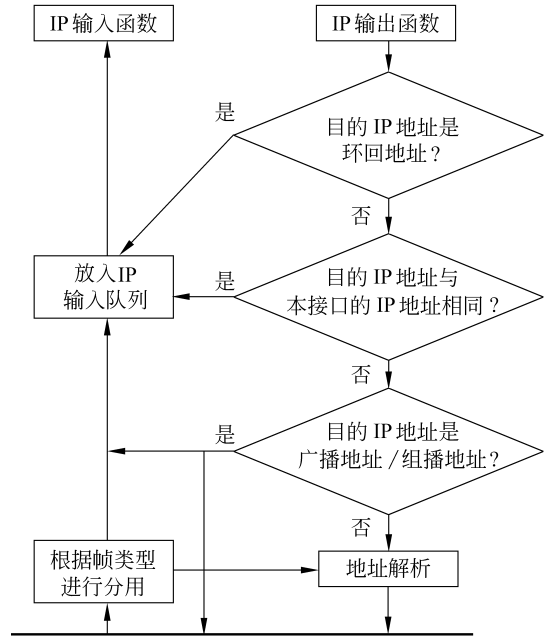

图 3-6　环回接口对 IP 数据报的处理

在发送 IP 数据报时，首先要判别该数据报的目的 IP 地址是否为环回地址，如果是环回地址，则直接将 IP 数据报放入 IP 输入队列实现环回。对于直接以本机地址作为目的地址的 IP 数据报也要回送给本机。对于广播或组播数据报，则在回送给本机的同时还要向网络发送。

3.4　私有网络地址

因特网地址分配机构为私有网络保留了 3 组 IP 地址(RFC 1918)，任何位于防火墙和代理服务器后面的私有网络都可以使用这 3 组地址。这 3 组保留地址如下：

A 类：10.0.0.0～10.255.255.255

B 类：172.16.0.0～172.31.255.255

C 类：192.168.0.0～192.168.255.255

这些地址是专门提供给那些没有连接到因特网上的网络使用的，这些 IP 地址与现在因特网上所使用的所有地址都不冲突。

从理论上讲，没有连接到因特网的私有网络可以使用从因特网地址分配机构申请到的 IP 地址，但这样做无疑是对地址的一种浪费。

当然，没有连接到因特网的私有网络也可以使用任意的 IP 地址块，但如果有朝一日该网络要通过代理服务器连接到因特网时，内网地址不变，利用 NAT 将内网地址转换为申请到的合法 IP 地址上因特网，就可能无法正常访问因特网上的某些服务器。

图 3-7 中代理服务器后面的私有网络采用了不是申请来的地址块 202.119.86.0,因此,无法访问因特网上合法的 202.119.86.0 网络提供的服务。每当该私有网络中的主机试图访问因特网上的 202.119.86.0 网络提供的服务时,代理服务器都会将该访问看作是对该私有网络内部的访问,而不会将信息转发到因特网上。

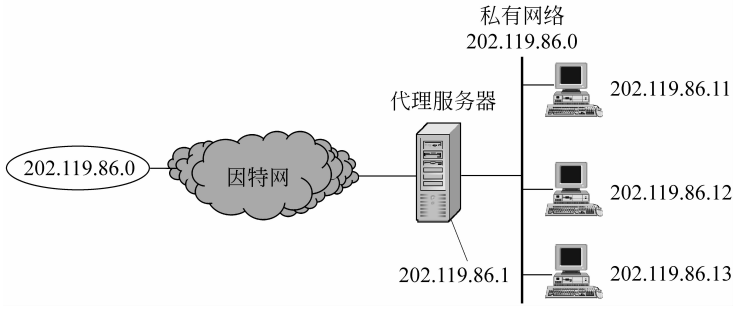

图 3-7　采用不合适 IP 地址的私有网络

使用保留的私有网络地址的网络通过代理服务器连接到因特网时,完全不用担心和因特网上的其他网络发生地址冲突。

使用私有网络地址不仅可以节省大量的 IP 地址,缓解 IP 地址不足的问题,而且还可以借助于代理服务器的网络地址转换(NAT)功能,隐藏私有网络的地址框架,保证私有网络的安全。

另外,还有一块为 Windows 系统所专用的 IP 地址块:自动专用 IP 寻址(APIPA)地址。这块保留地址的范围是 169.254.0.0～169.254.255.255。这块私有地址用于支持 DHCP 故障转移处理机制。当设置为 DHCP 客户端的 Windows 启动时,如果 DHCP 服务器不可用,则无法从 DHCP 服务器获得 IP 地址等配置信息,此时,DHCP 客户机会自己自动配置 IP 地址和子网掩码。这就是自动专用 IP 寻址,具体过程是 APIPA 在 169.254.0.1 到 169.254.255.254 的私有地址空间内随机选择地址分配,并使用默认的网络掩码 255.255.0.0。DHCP 客户机还会通过使用 ARP 测试地址冲突,以确保所选择的 IP 地址未在本网络中使用。如果发现冲突,则客户机会选择试用另一个 IP 地址。客户机将重试最多 10 个地址的自动配置。

即使自动配置了 IP 地址,DHCP 客户机每隔 5 分钟还会尝试与 DHCP 服务器联系一次,直到它可以与 DHCP 服务器通信为止。此时,DHCP 客户机放弃它的自动配置信息,而去使用由 DHCP 服务器提供的地址(以及它提供的任何其他 DHCP 选项信息)来更新其 IP 配置。

APIPA 也可以用于为没有 DHCP 服务器的独立网络提供自动配置 TCP/IP 协议的功能。

3.5　IP 地址配置

为了确保网络上的主机能够正常工作,在为主机配置 IP 地址时,应遵守以下原则:

- 同一网络上的所有主机应该采用相同的网络号;

- 一个网络中的主机号必须是唯一的；
- 主机号不能为全 1(主机号为全 1 是广播地址)；
- 主机号不能为全 0(主机号为全 0 表示网络)；
- 因特网上的每个网络的网络号具有唯一性；
- 网络号不能为全 1；
- 网络号不能为全 0(全 0 表示一个本地网)；
- 网络号不能以 127 开头(127 是环回地址)。

IP 地址配置得是否正确将直接影响到网络的运行。所以，通常由熟知 IP 地址分配规则的管理员进行 IP 地址的管理和配置。

两类最常见的 IP 地址配置问题是：错误的 IP 地址和重复的 IP 地址。

如果一台主机的网络号与本地网络号不匹配，那么，本网络中的其他主机将假定这个不正常的主机是远程网络上的一台主机，从而强制它们把消息发送给路由器，而不是发给本网络内的计算机。图 3-8 给出了错误 IP 地址的一个示例。

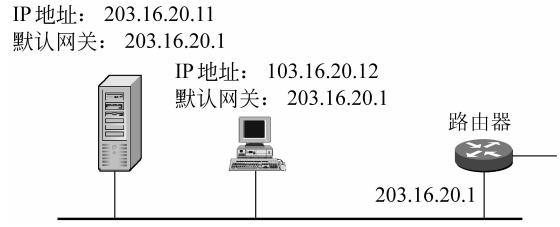

图 3-8　错误的 IP 地址

当网络上有两台或多台主机的 IP 地址出现重复时，通信可能无法正常进行。

使用 Windows 操作系统的计算机在启动期间将对 TCP/IP 进行初始化，此时，会发送一条 ARP 广播，借此检查本网络中是否存在与本机地址相同的 IP 地址。如果存在重复地址，则不加载本机的 TCP/IP 协议，同时显示一条带有对方 MAC 地址的地址重复出错消息。但有些其他类型的网络操作系统并未对重复地址进行检查，这给以后的查错工作带来了麻烦。

一种避免地址冲突的方法是使用动态主机配置协议 DHCP(dynamic host configuration protocol)。该协议自动进行 IP 地址分配，确保不会出现地址重复。动态主机配置协议将在第 10 章进行讨论。

3.6　子网及子网掩码

一个标准的 A 类、B 类和 C 类网络可以进一步划分为子网。子网划分技术能够使单块网络地址横跨几个网络，这样，一台路由器所连接的多个网络就可以是同属于一个网络地址块下的不同子网了。

划分子网的原因主要有以下几点：

(1) A 类网络和 B 类网络的地址空间都很大，不进一步划分，很难得到有效的利用；

(2) 将一个大型网络划分为多个与单位的部门相对应的小网络更便于管理；

(3) 通过使用路由器连接子网,可以隔离广播和通信,减少网络拥塞;

(4) 出于安全方面的考虑,希望利用子网技术将管理网络和服务网络分开;

(5) 由于历史的原因和应用的需要使得一个单位可能拥有不同的物理网络,利用子网技术可以方便地实现互联。

划分子网的方法是将 IP 地址的主机号部分划分成两部分,拿出一部分来标识子网,另一部分仍然作为主机号。带子网标识的 IP 地址结构如图 3-9 所示。

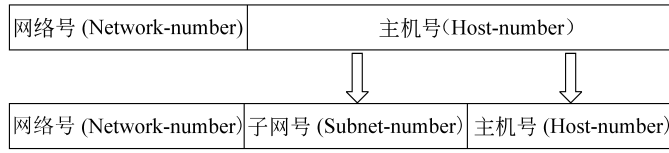

图 3-9 带子网的 IP 地址结构

划分后 IP 地址由三部分组成:网络号、子网号以及主机号。因此,IP 地址可以表示为:

IP-address ::= {<Network-number>,<Subnet-number>,<Host-number>}

IP 地址的网络号加子网号可以唯一地标识一个子网,因此,我们将这两部分合起来再加上为 0 的主机号部分称为子网地址。

在未划分子网时,我们可以根据网络的类别(由 IP 地址的第 1 个字节确定)得到网络号和主机号的长度。在划分子网后,我们如何知道网络号、子网号以及主机号的长度呢? 为此,TCP/IP 采用了子网掩码。

子网掩码是一个 32 位的二进制数字,它告诉 TCP/IP 主机,IP 地址的哪些位对应网络号和子网号部分,哪些位对应主机号部分。TCP/IP 协议使用子网掩码判断目的主机是位于本地子网上,还是位于远程子网上。

子网掩码指定了子网标识和主机号的分界点。子网掩码中对应网络号和子网号的所有位都被设为 1,而对应主机号的所有位都被设为 0。子网掩码是由连续的 1 加连续的 0 所构成的 32 位二进制位串。

获得子网地址的方法是将子网掩码和 IP 地址进行按位“与”运算,如图 3-10 所示。

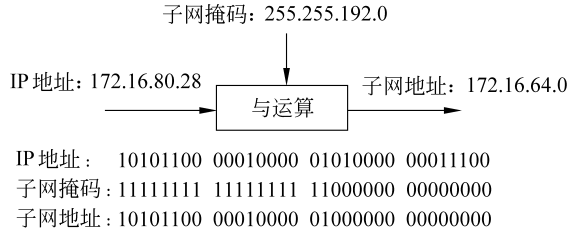

图 3-10 由 IP 地址和子网掩码获得子网地址

究竟拿出多少位作为子网号来标识子网,取决于子网的数量和子网的规模。

各类网络的主机号的位数用 p 表示,如果从 p 位主机号中拿出 m 位来划分子网,则剩下的 $n=p-m$ 位用于标识主机。

A 类网络、B 类网络和 C 类网络的 p 值分别为 24、16 和 8。

m 位可以标识 2^m 个子网,但在子网概念出现的早期是不使用 m 位子网号为全 0 和全 1

的子网的，原因是早期的路由协议并不同时发布网络地址和子网掩码，这样会导致 IP 地址的二义性。对于未划分子网的原主网络的网络号和划分完子网后的第 1 个子网的网络号是相同的；原主网络的广播地址和划分完子网后的最后一个子网的广播地址也是相同的。因此，不使用全 0 和全 1 的子网号的子网，以免发生 IP 地址二义性问题。直到 RFC 1878 才废除了这一规定。这里的前提条件是路由协议都是支持子网掩码的。但在后来的一段时间里还是不建议使用子网号为全 0 和全 1 的子网，主要是可能考虑还存在一些老的路由协议还在使用。比如，在 Cisco 路由器上，默认可以使用子网号为全 1 的子网，但是不能使用子网号为全 0 的子网，如果想要使用全 0 的子网，须输入相关命令开启全 0 子网的使用。

如果不使用子网号为全 0 和全 1 的子网，m 位用来划分子网，实际可以划分 2^m-2 个可用的子网。

n 位可以标识 2^n 台主机，但 n 位为全 0 时用于标识子网，为全 1 时用于表示子网广播地址。这样，n 位主机号实际可以标识 2^n-2 台主机。

以 B 类网络 172.16.0.0 为例，当 $m=1$ 时，第 3 个字节的最高位被拿出来划分子网。此时子网掩码为 255.255.128.0，两个子网为：

172.16.0.0　　(10101100 00010000 0<u>0</u>000000 00000000　子网号：0)

172.16.128.0　(10101100 00010000 1<u>0</u>000000 00000000　子网号：1)

这两个子网一般不建议使用。

当 $m=2$ 时，第 3 个字节的最高两位被拿出来划分子网。此时子网掩码为 255.255.192.0，4 个子网为：

172.16.0.0　　(10101100 00010000 <u>00</u>000000 00000000　子网号：00)

172.16.64.0　　(10101100 00010000 <u>01</u>000000 00000000　子网号：01)

172.16.128.0　(10101100 00010000 <u>10</u>000000 00000000　子网号：10)

172.16.192.0　(10101100 00010000 <u>11</u>000000 00000000　子网号：11)

当 $m=8$ 时，可以划分为 256 个子网：172.16.0.0、172.16.1.0、…、172.16.255.0。子网掩码为 255.255.255.0。

通常在规划一个网络时划分子网的步骤如下：

(1) 确定需要多少个子网号来唯一标识每一个子网；

(2) 确定需要多少个主机号来标识每个物理网络(子网)上的每台主机；

(3) 综合考虑子网数和子网中的主机数后，确定一个符合要求的子网掩码；

(4) 确定标识每个子网的网络号；

(5) 确定每个子网上可以使用的主机号的范围。

例如：假设已经得到一个 A 类网络地址 86.0.0.0。现在想把这个网络划分成 4 个子网。该网络中最大的网段要求 9000 个可供主机寻址的地址，但在未来两年内可供寻址的主机数将增至 20 000 台。什么样的子网掩码值可以用于这个网络的子网规划呢？

从主机号中拿出 3 位可以划分 8 个子网，去除不建议使用的子网号为全 0 和全 1 的子网之后，还可以有 6 个子网。这样，子网掩码为：255.224.0.0，每个子网可以容纳的主机数为 $2^{21}-2$。表 3-2给出了各个子网的地址、子网中主机 IP 地址的范围以及子网的直接广播地址。

表 3-2　86.0.0.0 的 8 个子网划分

子网地址	起始地址	结束地址	广播地址
86.0.0.0	—	—	—
86.32.0.0	86.32.0.1	86.63.255.254	86.63.255.255
86.64.0.0	86.64.0.1	86.95.255.254	86.95.255.255
86.96.0.0	86.96.0.1	86.127.255.254	86.127.255.255
86.128.0.0	86.128.0.1	86.159.255.254	86.159.255.255
86.160.0.0	86.160.0.1	86.191.255.254	86.191.255.255
86.192.0.0	86.192.0.1	86.223.255.254	86.223.255.255
86.224.0.0	—	—	—

满足上述题目要求的方案不止一个,增加子网号的位数或减少主机号的位数可以得到其他方案。

例如:假设已经得到一个 B 类网络地址 160.46.0.0。要求把整个网络划分成 18 个不同的子网,该网络中最大的网段要求 1800 个可供主机寻址的地址。

要提供 18 个子网,必须占用主机地址的 5 位。去除不建议使用的子网号为全 0 和全 1 的子网之后,5 位可以提供 30 个可用的子网(2^5-2)。这样,子网掩码为:255.255.248.0。每个子网可以容纳的主机数为 $2^{11}-2$,可以满足要求。表 3-3 给出了各个子网的地址、子网中主机 IP 地址的范围以及子网的直接广播地址。

表 3-3　160.46.0.0 的 32 个子网划分

子网地址	起始地址	结束地址	广播地址
160.46.0.0	—	—	—
160.46.8.0	160.46.8.1	160.46.15.254	160.46.15.255
160.46.16.0	160.46.16.1	160.46.23.254	160.46.23.255
160.46.24.0	160.46.24.1	160.46.31.254	160.46.31.255
160.46.32.0	160.46.32.1	160.46.39.254	160.46.39.255
…	…	…	…
160.46.240.0	160.46.240.1	160.46.247.254	160.46.247.255
160.46.248.0	—	—	—

A 类网络的默认掩码(default mask)是 255.0.0.0,B 类网络的默认掩码是 255.255.0.0,C 类网络的默认掩码是 255.255.255.0。

引入子网概念后,由于路由器对广播的隔离作用,受限广播数据被限制在子网中。

针对某一子网的直接广播可以表示为:

{< Network-number >, < Subnet-number >, < Host-number >} = {< Network-number>, <Subnet-number>, −1}

针对某一网络内所有子网的直接广播可以表示为：

{＜Network-number＞，＜Subnet-number＞，＜Host-number＞}＝{＜Network-number＞，－1，－1}

在上面所讨论的子网划分中，各个子网的地址空间是一样大的，各个子网的掩码也是一样的。但为了提高地址空间的利用率，可能需要将子网进一步划分为更小的子网，此时，可以从主机号中再拿出一些比特来划分子网，这就使得在一个网络中有多个不同规模的子网，每个子网都有其对应的子网掩码，这便是可变长子网掩码 VLSM(variable-length subnet mask)。可变长子网掩码要求路由器支持子网掩码和路由信息的同时发布。当系统中的所有路由协议都支持子网掩码和路由信息的同时发布时，不仅可以使用可变长子网掩码，也可以使用全 0 和全 1 的子网号。采用可变长子网掩码划分子网的一个例子如表 3-4 所示。

表 3-4　用可变长子网掩码划分 86.0.0.0 的例子

子网地址	起始地址	结束地址	广播地址	子网掩码
86.0.0.0	86.0.0.1	86.63.255.254	86.63.255.255	255.192.0.0
86.64.0.0	86.64.0.1	86.95.255.254	86.95.255.255	255.224.0.0
86.96.0.0	86.96.0.1	86.127.255.254	86.127.255.255	255.224.0.0
86.128.0.0	86.128.0.1	86.159.255.254	86.159.255.255	255.224.0.0
86.160.0.0	86.160.0.1	86.191.255.254	86.191.255.255	255.224.0.0
86.192.0.0	86.192.0.1	86.199.255.254	86.199.255.255	255.248.0.0
86.200.0.0	86.200.0.1	86.207.255.254	86.207.255.255	255.248.0.0
86.208.0.0	86.208.0.1	86.223.255.254	86.223.255.255	255.240.0.0
86.224.0.0	86.224.0.1	86.255.255.254	86.255.255.255	255.224.0.0

这里的可变长实际上指的是子网掩码中前面部分连续 1 的位数可以是不同的。表中子网 86.0.0.0 的子网掩码前面部分连续 1 的位数是 10 位，子网 86.64.0.0 的是 11 位，子网 86.192.0.0 的是 13 位，子网 86.208.0.0 的是 12 位，掩码的总长度 32 位是不变的，不同的是前面连续 1 的位数。总长不变的情况下连续 1 的位数越多，主机号部分就越短，网络的规模也就越小。

3.7　超网

由于 A 类网络和 B 类网络较少，而 C 类网络较多，对于拥有较多计算机的单位往往可以获得多个连续的 C 类网络地址块，而不是 A 类或 B 类网络地址块。利用超网技术，可以将这些 C 类网络地址块合并为一个大的地址块。从理论上讲，也可以将多个 B 类地址块合并为一个更大的地址块。

超网技术使用与子网技术正好相反的方法，如图 3-11 所示，构造超网时，从网络号中拿出一些位和主机号拼接在一起形成新的主机号。

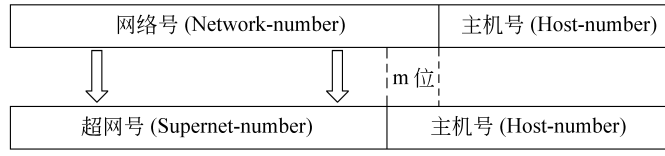

图 3-11　超网的 IP 地址结构

和子网的划分类似,超网通过超网掩码来指定超网号和主机号的分界点。超网掩码中对应于超网号的所有位都被设置为 1,而对应于主机号的所有位都被设置为 0。与子网划分不同的是,子网划分是通过增加掩码中 1 的位数来实现的,而超网划分是通过减少掩码中 1 的位数来实现的。获得超网地址的方法也是将超网掩码和 IP 地址进行按位“与”运算。

一般合并超网大多是 C 类地址块的合并,在构造超网时,须注意以下 3 点:

(1) 地址块必须是连续的。

(2) 待合并的地址块的数量必须是 2^m($m=1,2,\cdots$)。

(3) 被合并的 C 类网络的第一个地址块的地址中第 3 个字节的值必须是待合并的地址块的整数倍。

例如,可以将下列 8 个 C 类地址块合并为一个超网。

192.168.168.0　192.168.169.0　192.168.170.0　192.168.171.0

192.168.172.0　192.168.173.0　192.168.174.0　192.168.175.0

构造超网时,从网络号的最低位起拿出 3 位来合并这 8 个 C 类地址块。此时,超网掩码为:11111111 11111111 11111000 00000000,即 255.255.248.0。通过验算可以发现,上述地址块中的任何 IP 地址与超网掩码运算的结果都是 192.168.168.0,也就是说这些地址块中的所有主机都认为它们位于同一个网络 192.168.168.0 上。所构造的超网的示意图如图 3-12 所示。

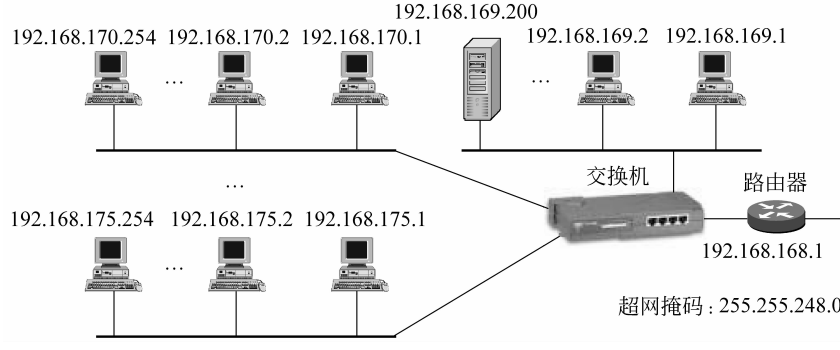

图 3-12　超网的一种连接方案

超网技术将多个网络地址合并成单个网络地址,这样可以减小路由表。

3.8　无类地址

通过前面对子网和超网的介绍，我们看到利用掩码中 1 的位数的增加或减少可以方便地控制网络的规模。在实际应用中许多单位都只需要很少的 IP 地址，为了方便 IP 地址的分配和提高 IP 地址的利用率，1993 年因特网组织机构发布了无类别域间路由选择 CIDR (classless interdomain routing)。

CIDR 去掉了 A 类地址、B 类地址和 C 类地址的概念，采用了无类地址的概念，不再由地址的前几位来预先定义网络类别。每一个地址仅仅包含网络号部分和主机号部分，网络号部分被称为网络前缀。整个 IP 地址空间被分割为一些大小不同的块。每一个块对应一个网络。

和子网所使用的方法相同，无类地址也是利用掩码来划分网络号和主机号的分界点。只要给出了起始地址和掩码，就可以确定整个地址块。只不过这里的网络号不再与网络的数量相关，只是标识这个网络，因为此时已经是可变长子网掩码了。各个网络的掩码前面连续 1 的位数都可以不同，只取决于网络的规模(主机号的位数)。

对每个无类地址块的要求是：

(1) 地址块必须由连续的 IP 地址构成。

(2) 地址块所含 IP 地址的数量必须是 2^n。

(3) 地址块的起始地址必须能够被 2^n 整除。

第(1)条是显而易见的，因为是一块，而不是多块；第(2)条是由主机号的位数 n 决定的；第(3)条则是保证这一地址块不会跨网络，即保证这一地址块中的任一地址和这块地址的掩码与运算的结果都会等于这个网络的首地址——网络地址。

由于 IP 地址 X. Y. Z. 0 一定是 2^8 的整数倍，X. Y. 0. 0 一定是 2^{16} 的整数倍，X. 0. 0. 0 一定是 2^{24} 的整数倍，因此我们在考察起始地址是否合法时，可以简化计算过程。当地址块中的地址数小于 2^8 时，只需要考察起始地址的最后 1 个字节是否可以被 2^n 整除；当地址块中的地址数小于 2^{16} 时，只需要考察起始地址的最后 2 个字节是否可以被 2^n 整除；当地址块中的地址数小于 2^{24} 时，只需要考察起始地址的最后 3 个字节是否可以被 2^n 整除即可。

例如，起始地址为 10. 126. 60. 40，掩码为 255. 255. 255. 248 的地址块所对应的地址范围是 10. 126. 60. 40～10. 126. 60. 47。同样，该地址范围的第一个地址作为网络地址，最后一个地址作为直接广播地址。

掩码的点分十进制数表示法较复杂，在无类地址中常采用的一种表示法是斜线表示法 (slash notation)。斜线表示法将地址和掩码一起表示出来，其格式为：W. X. Y. Z/n。斜线前面是 IP 地址，斜线后面是前缀长度。这里的前缀是指 IP 地址中的网络号部分，因此前缀长度是指 IP 地址中的网络号部分的位数，也就是掩码中连续 1 的位数。斜线表示法中的 W. X. Y. Z 可以是网络地址(地址块首地址)，也可以是本网络中的任意一个 IP 地址，只要有这个地址和前缀长度 n，就可以唯一地决定一个网络。

斜线表示法又称为 CIDR 表示法。斜线表示法中的前缀长度与掩码是一一对应的，前缀长度与掩码的对应关系如表 3-5 所示。

表 3-5　前缀长度与掩码的关系

/n	掩　码	/n	掩　码	/n	掩　码	/n	掩　码
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

本章要点

- 一个物理网络中的每个结点都至少拥有一个机器可识别的物理地址。物理地址又称为硬件地址、MAC 地址或第二层地址。
- 因特网在 IP 层(网络层)用 IP 地址实现了地址的统一。
- IP 地址体现了因特网的层次化结构。32 位的 IPv4 地址由网络号和主机号构成,网络号的位数决定网络的数量,主机号的位数决定网络的规模。
- IP 地址的本质是标识设备的网络连接。
- 4 个字节的 IP 地址通常用点分十进制数表示,根据 IP 地址第 1 个字节的值可以知道 IP 地址的类别。
- 因特网上的每个网络都有一个 IP 地址,其主机号部分为 0。
- 直接广播是向某个网络中所有的主机发送信息。
- 受限广播是向本网络内的所有主机发送信息。
- 环回地址是用于网络软件测试以及本机进程之间通信的特殊地址。
- 因特网为私有网络保留了 3 组 IP 地址,任何位于防火墙和代理服务器后面的私有网络都可以使用这 3 组地址。
- 在进行 IP 地址配置时要注意避免重复的 IP 地址和错误的 IP 地址与掩码。
- TCP/IP 协议利用子网掩码可以判断目的主机是位于本地子网上,还是位于远程子网上。
- 在进行子网规划时要综合考虑子网的数量和子网中主机的数量。
- A 类网络的默认掩码是 255.0.0.0,B 类网络的默认掩码是 255.255.0.0,C 类网络的默认掩码是 255.255.255.0。
- 划分子网的方法是将 IP 地址的主机号部分划分成两部分,拿出一部分来标识子网,另一部分仍然作为主机号。
- 利用超网技术,可以将多个网络地址块合并为一个更大的地址块,以便使路由表更小、更有效。通常是将多个 C 类网络地址块合并为一个大的地址块。构造超网时,

从网络号的低位部分拿出一些比特和主机号拼接在一起形成新的主机号。

- 无类地址将整个 IP 地址空间分割为一些大小不同的块。
- 斜线表示法(CIDR 表示法)将地址和掩码一起表示出来,其格式为:W. X. Y. Z/n。斜线前面是 IP 地址,斜线后面是前缀长度。

习题

3-1　直接广播和受限广播有何不同?

3-2　使用私有网络地址有什么好处?

3-3　现有一个 C 类网络地址块 199.5.6.0,需要支持至少 7 个子网,每个子网最多 9 台主机。请进行子网规划,给出各子网的地址、可以分配给主机的地址范围和子网广播地址。

3-4　子网号为 10 位的 A 类地址与子网号为 2 位的 B 类地址的子网掩码有何不同?

3-5　若 IP 地址为 156.42.72.37,子网掩码为 255.255.192.0,其子网地址是什么?

3-6　将以 203.119.64.0 开始的 16 个 C 类地址块构造成一个超网,请给出该超网的超网地址和超网掩码。

3-7　若一个超网的地址是 204.68.64.0,超网掩码是 255.255.252.0,那么下列 IP 地址中哪些地址属于该超网?

204.68.63.26　204.68.67.216　204.68.68.1　204.69.66.26　204.68.66.2

3-8　在下列地址块组中,哪个组可以构成超网?其超网掩码是什么?

a. 199.87.136.0　199.87.137.0　199.87.138.0　199.87.139.0

b. 199.87.130.0　199.87.131.0　199.87.132.0　199.87.133.0

c. 199.87.16.0　199.87.17.0　199.87.18.0

d. 199.87.64.0　199.87.68.0　199.87.72.0　199.87.76.0

3-9　以斜线表示法(CIDR 表示法)表示下列 IP 地址和掩码。

a. IP 地址:200.187.16.0,掩码:255.255.248.0

b. IP 地址:190.170.30.65,掩码:255.255.255.192

c. IP 地址:100.64.0.0,掩码:255.224.0.0

3-10　188.80.164.82/27 的网络地址是什么?

3-11　查阅文档 RFC 1219 和 RFC 4632。

第4章　地址解析

IP地址是网络层(IP层)的地址,IP地址实现了底层网络物理地址的统一。但因特网技术并没有改变底层的物理网络,更没有取消物理网络的地址,最终数据还是要在物理网络上传输,而在物理网络上传输时使用的仍是物理地址。因此,因特网在网络层使用IP地址的同时,在物理网络中仍使用物理地址。这样一来,网络中就同时存在两套地址,而且在这两套地址之间必须建立映射关系。

IP地址又称为逻辑地址,逻辑地址由软件进行处理。建立逻辑地址与物理地址之间映射的方法通常有两种:静态映射和动态映射。

静态映射主要采用地址映射表格来实现逻辑地址与物理地址之间的映射。当主机知道另一台主机的逻辑地址而不知道其物理地址时,可以通过查表的方法获得它。但逻辑地址与物理地址之间的映射关系并不是一成不变的。主机的物理地址可能因为更换网络接口卡(NIC)而发生变化;其逻辑地址也可能因为主机从一个网络移到另一个网络而发生变化。一旦出现上述情况,地址映射表就需要及时更新。由于地址映射表一般以人工方式建立和维护,所以不能适应物理地址和逻辑地址频繁变化的网络和规模庞大的网络。

动态映射是在需要获得地址映射关系时利用网络通信协议直接从其他主机上获得映射信息。因特网采用了动态映射的方法进行地址映射。

在因特网技术中,逻辑地址与物理地址之间的映射称为地址解析(address resolution)。地址解析包括两个方面的内容:从IP地址到物理地址的映射和从物理地址到IP地址的映射。TCP/IP专门提供了两个协议来实现这两种映射,一个是地址解析协议(address resolution protocol, ARP),另一个是反向地址解析协议(reverse address resolution protocol,RARP)。

ARP用于从IP地址到物理地址的映射;RARP用于从物理地址到IP地址的映射。如图4-1所示。

本章分别介绍地址解析协议和反向地址解析协议的工作原理和方法,并给出两者的报文格式及封装方法。

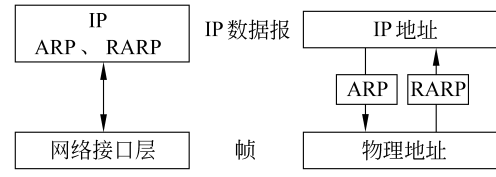

图4-1　用协议实现动态地址映射

4.1　地址解析协议

地址解析协议ARP使IP能够获得与某个给定IP地址相关的主机物理地址。ARP的功能分为两部分:一部分在发送数据包时请求获得目的主机的物理地址;另一部分向请求物理地址的主机发送解析结果。

4.1.1　地址解析原理

当主机 A 需要向同一物理网络中的主机 B 发送 IP 数据报时，主机 A 的 IP 层要将 IP 数据报传给数据链路层进行帧封装，封装时要求给出目的主机的物理地址。因此，IP 层发送 IP 数据报时通常将产生以下事件：

（1）IP 调用 ARP，请求 IP 地址为 I_B 的目的主机 B 的物理地址 P_B。

（2）ARP 创建一个 ARP 请求帧，请求 IP 地址 I_B 对应的物理地址。ARP 请求帧将包括如下信息：

- 请求主机的物理地址 P_A；
- 请求主机的 IP 地址 I_A；
- 目的主机的 IP 地址 I_B。

（3）主机 A 在本地网络中广播 ARP 请求帧，请求帧的目的地址为广播地址（全 1），如图 4-2 所示。但在用于对地址进行验证和确认时也可以用单播地址，此时知道对方的物理地址，用单播进行针对性的解析，以便确认对方地址的正确性。

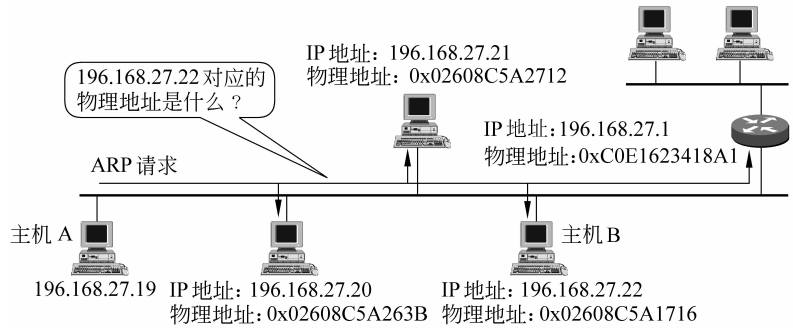

图 4-2　以广播方式发送 ARP 请求

（4）该网络中的所有主机都能接收 ARP 请求帧，并将该帧中的目的主机 IP 地址 I_B 和自己的 IP 地址进行比较。其地址与 I_B 不匹配的主机将忽略这个帧。

（5）如果主机发现请求中的目的主机 IP 地址 I_B 与自己的 IP 地址相同，就产生一个包含其物理地址 P_B 的 ARP 应答帧。

（6）ARP 应答帧直接发回给发送 ARP 请求的主机 A（ARP 应答帧不以广播方式发送）。ARP 应答帧包含以下信息：

- 应答主机的物理地址 P_B；
- 应答主机的 IP 地址 I_B；
- 请求主机的物理地址 P_A；
- 请求主机的 IP 地址 I_A。

ARP 应答帧的发送如图 4-3 所示。

（7）利用从应答帧中得到的目的主机的物理地址 P_B 完成 IP 数据报的帧封装，并将该帧发送给主机 B。

这里需要注意以下两点：

（1）ARP 请求帧在网络中是以广播方式发送的，因为此时还不知道目的主机的物理地

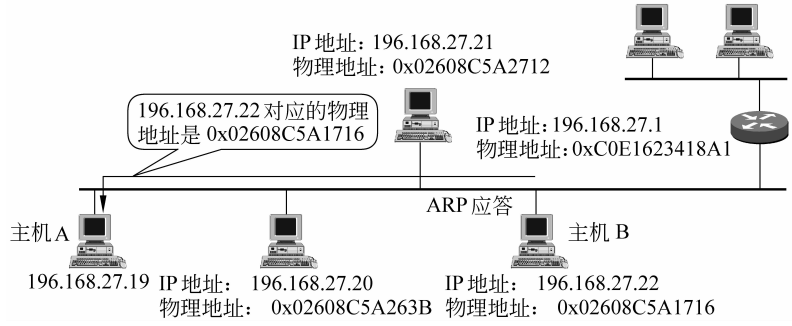

图 4-3 以单播方式发送 ARP 应答

址。ARP 应答帧是以单播方式发送的,因为应答方从请求帧中可以得到对方的物理地址。

(2) 目的主机必须与源主机位于同一网络中。由于 ARP 采用的是物理网络中的广播,IP 路由器不会对该广播帧进行转发,因而不能用 ARP 确定远程网络中主机的物理地址,而且也没有必要知道远程主机的物理地址。如果目的主机位于远程网络中,IP 会将数据报先发送给路由器,然后由路由器进行转发。在这种情况下,IP 只需要利用 ARP 确定路由器的物理地址就可以了,而路由器将逐级向前转发数据报。

4.1.2 ARP 高速缓存

如果每次在发送 IP 数据报前都重复上面的过程,势必会带来较大的开销。广播 ARP 请求不仅要耗费带宽,而且使得本地网络中的每台主机都要处理该广播帧,然后忽略或给出响应帧。

为了使地址解析时的广播尽可能少,每台主机都维护一个名为 ARP 高速缓存的本地列表。ARP 高速缓存中含有最近使用过的 IP 地址与物理地址的映射列表。ARP 请求方和应答方都把对方的地址映射存储在 ARP 高速缓存中。

当发送 IP 数据报需要获取目的主机的物理地址时,首先检查它的 ARP 高速缓存,如果 ARP 高速缓存中已经存在对应的映射表项,那么就可以从 ARP 高速缓存中获得目的主机的硬件地址,主机就可以立即发送 IP 数据报,而不需要发送 ARP 请求去进行地址解析了。只有当 ARP 高速缓存中不存在与该目的 IP 地址对应的映射表项时,才广播 ARP 请求。

由于 ARP 高速缓存位于内存中,因此每次计算机或路由器重新启动时,都必须动态地创建地址映射表。当主机收到一个 ARP 请求帧或响应帧时,都会检查它的 ARP 高速缓存,如果其中不存在对应的映射表项,那么主机就会将 ARP 请求帧或响应帧中的发送方的 IP 地址和物理地址加入到 ARP 高速缓存中。

1. ARP 高速缓存中地址映射表项的超时

由于 IP 地址与物理地址的映射关系可能因网络接口或 IP 地址的变化而发生变化,因此 ARP 高速缓存中的地址映射表项都存在一个过时的问题。解决此问题的办法是给 ARP 高速缓存中的每一个表项都设置一个超时值(又称为老化时间),使得每个地址映射表项都有一个生命期。

不同的 TCP/IP 实现使用不同的超时值,短的仅有几十秒钟,而长的则长达几个小时。超时值越短,系统中出现的 ARP 请求广播就越多。但若超时值过长,主机又不能及时地发

现地址映射关系的改变，也可能会引起问题。

DLINK 默认的超时值是 20 秒；Linux fedora 的默认值是 60 秒；思科 2690 系列交换机的默认值是 4 小时。

对于 Windows 2000/XP 系统，ARP 高速缓存中新加入的表项的超时值是 2 分钟，若在 2 分钟内没有被使用就会超时。如果在 2 分钟内，该高速缓存表项被使用来寻找目的主机的硬件地址，那么该表项的超时值又会被重置为 2 分钟，超时前的每次使用都会被重置为 2 分钟，一直到 10 分钟的最长生命期限制。超过 10 分钟的最大限制后，该表项将被移除，并且通过另一个 ARP 请求/回应解析过程来获得新的对应关系。

除了为 ARP 高速缓存表项设置生命期外，还可以通过设置动态的探测次数来减少地址的解析错误。在将一条动态 ARP 表项删除之前，系统可以先进行探测，如果超过设置的探测次数，被探测的目标主机仍没有应答，则此 ARP 表项将被删除。

2. 控制地址映射表项的超时值

对于 Windows 2000/XP 系统的计算机，还可以利用注册表参数 ArpCacheLife 对高速缓存表项的超时值进行控制。若未设置 ArpCacheLife 参数，则 ARP 高速缓存中的超时值使用默认值 2 分钟(即 120 秒)，当在注册表中添加了 ArpCacheLife 参数后，Arp 表项的超时值取决于注册表中设置的值。

另一个相关的注册表参数是 ArpCacheMinReferencedLife，该参数是被重复使用的表项可以在 ARP 缓存中存放的最长生命期限制时间。也就是前面所提到的 10 分钟(600 秒)。

ArpCacheLife 和 ArpCacheMinReferencedLife 参数的类型为 REG_DWORD，单位为秒，值的有效范围 0-0xFFFFFFFF，两个参数存放在如下的注册表项中：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

如果在注册表中看不到这两个键值，说明当前使用的是默认值，即分别为 120 秒和 600 秒。若要修改，须自行创建这两个键值，修改后重启计算机后生效。

ArpCacheLife 和 ArpCacheMinReferencedLife 的使用规则是：如果 ArpCacheLife 的值大于等于 ArpCacheMinReferencedLife 的值，则被使用和未被使用的 ARP 缓存表项可存储的时间都是 ArpCacheLife；如果 ArpCacheLife 的值小于 ArpCacheMinReferencedLife 的值，则未被使用的 ARP 缓存表项在 ArpCacheLife 秒的时间后过期，被使用的表项的最大生存期为 ArpCacheMinReferencedLife 的值。

3. 静态 ARP 表项

另一种控制地址映射表项超时值的方法是在 ARP 高速缓存中创建一个静态表项。静态表项是永不超时的地址映射表项。静态表项主要用在一台主机经常向另一台主机发送 ARP 请求的情况下。为了提高效率，减少不必要的开销，可以在 ARP 高速缓存中创建一个静态表项，使该地址映射表项始终存在于 ARP 高速缓存中，以避免向某一主机发送 ARP 广播。

静态表项也有可能发生变化，当主机接收到 ARP 广播，而且该广播所含的地址信息与当前 ARP 高速缓存中对应的静态表项不一致时，主机将用新收到的物理地址替代原有的物理地址，并为该表项设置超时值，使其不再是静态表项。使用 arp 实用程序可以人工删除静态表项。重新启动主机也会使静态表项丢失。