

网管实战宝典

Windows Server 2003 服务器架设与管理

张伍荣 主编

清华大学出版社

北 京

第 1 章 构建 Windows Server 2003 网络 服务环境

Windows Server 2003 作为网络操作系统或服务器操作系统，具有高性能、高可靠性、高安全性和配置方便等特点，在任意规模的应用中都可以成为理想的服务器平台。尤其是在日趋复杂的企业应用和 Internet 应用中，Windows Server 2003 更是经济划算的优质服务器操作系统。

通过本章的学习，读者应该掌握以下内容。

- ✧ Windows Server 2003 的应用场合，以及可以担当的服务器角色。
- ✧ IP 地址的组成、表示及分类，以及如何通过子网掩码进行子网划分。
- ✧ 虚拟机技术概念，以及如何利用虚拟机技术构建 Windows Server 2003 实验环境。

1.1 Windows Server 2003 所提供的网络功能

1.1.1 Windows Server 2003 应用场合

Windows Server 2003 提供了许多网络技术与服务，可以在不同的网络结构或应用场合中使用。

1. Internet 环境

Internet 是一个以 TCP/IP 网络协议连接各个国家、各个地区、各个机构的计算机网络的数据通信网，它将数万个计算机网络、数千万台主机互联在一起，覆盖全球。从信息资源的角度讲，Internet 是一个集各个部门、各个领域的信息资源为一体的，供网络用户共享的信息资源网。

2. Intranet 环境

- ✧ Intranet 是建立在企业内部的 Internet，又称内联网。它是一种基于 Internet 的 TCP/IP 协议，使用 WWW 等工具，采用防止外界侵入的安全措施，为企业内部服务并有连接 Internet 功能的企业内部网络。实际上，它将 Internet 技术运用到企业内部的信息系统中去，以企业内部员工为服务对象，以促进公司内部各个部门的沟通、提高工作效率、增加企业竞争力为目的，使用 Web 协议构建企业级的信息集成和信息服务。

3. Extranet 环境

Extranet, 又称外联网, 它往往被看作企业网的一部分, 是现有 Intranet 向外的延伸。它是一个使用公共通信设施和 Internet 技术的私用网, 也是一个能够使其客户和其他相关企业(如银行、贸易合作伙伴、运输企业等)相连以完成共同目标的交互式合作网络。

4. 远程访问环境

远程访问环境用来为远程办公人员、外出人员, 以及监视和管理多个部门办公室服务器的系统管理员提供远程网络。运行 Windows 操作系统并拥有网络连接的用户可以拨号远程访问他们的网络来获得服务, 例如文件和打印机共享、电子邮件及 SQL 数据库访问。

1.1.2 Windows Server 2003 的服务器角色

Windows Server 2003 是一个多任务操作系统, 它能够按照用户的需要, 以集中或分布的方式处理各种服务器角色。我们在安装 Windows Server 2003 后首先要做的就是配置服务器角色, 这些服务器角色主要包括以下几种。

1. 文件服务器角色

文件服务器提供和管理文件访问权限。如果要使用计算机上的磁盘空间存储、管理和共享诸如文件和网络访问的应用程序的信息, 请将该计算机配置为文件服务器。

2. 域控制器角色

域控制器可以存储目录数据, 管理用户和域之间的通信, 包括用户登录过程、身份验证和目录搜索。如果要提供 Active Directory 目录服务以管理用户和计算机, 请将该服务器配置为域控制器。

3. WINS 服务器角色

WINS (Windows Internet 名称服务) 服务器可以实现 IP 地址与 NetBIOS 计算机名之间的映射。通过组织中的 WINS 服务器, 可以按照计算机名而不是按照 IP 地址检索资源, 计算机名更容易记住。如果要将 NetBIOS 名称映射到 IP 地址或集中地管理名称(地址数据库), 请将该服务器配置为 WINS 服务器。本书的第 2 章将介绍 WINS 服务器的配置与管理。

4. DNS 服务器角色

DNS(Domain Name System, 域名系统)是在 Internet 上使用的 TCP/IP 名称解析服务。DNS 服务允许网络上的客户端计算机注册和解析用户友好的 DNS 名称。如果要使网络上的资源在 Internet 上可用, 请将该服务器配置为 DNS 服务器。本书的第 3 章将介绍 DNS 服务器的配置与管理。

5. DHCP 服务器角色

DHCP(Dynamic Host Configure Protocol, 动态主机配置协议)是设计用于简化管理地址配置的 TCP/IP 标准,旨在通过服务器计算机来集中管理网络上使用的 IP 地址和其他相关配置信息,以减少管理地址配置的复杂性。如果要执行多播地址分配,动态获得客户端 IP 地址和相关的配置参数,请将该服务器配置为 DHCP 服务器。本书的第 4 章将介绍 DHCP 服务器的配置与管理。

6. 终端服务器角色

使用“终端服务器”可提供单点安装,该安装赋予了多个用户对运行 Windows Server 2003 操作系统的任意计算机的访问权。用户可从远程位置运行程序、保存文件并使用网络资源,仿佛这些资源都安装在他们自己的计算机上一样。本书的第 5 章将介绍终端服务器的配置与管理。

7. Web 服务器和 Web 应用程序服务器角色

Web 服务器和 Web 应用程序服务器角色,其中包含该功能的全部以及用于 XML Web 服务、Web 应用程序和分布式应用程序的开发、部署和运行时管理的服务。如果要将服务器配置为应用程序服务器,就要将 Internet 信息服务(IIS)与其他可选技术和服务(例如 COM+ 和 ASP.NET)一起安装。IIS 和 Windows Server 2003 家族通过 Intranet、Internet 或 Extranet,一起提供集成的、可靠的、灵活的、安全的且可管理的 Web 服务器。IIS 还可用于创建动态网络应用程序的强通信平台。本书的第 6 章将介绍 Web 服务器和 Web 应用程序服务器的配置与管理。

8. FTP 服务器角色

FTP(File Transfer Protocol, 文件传输协议)是 TCP/IP 协议族的应用协议之一,主要用来在计算机之间传输文件。若要向用户提供文件的下载或上传服务,可以使用 Windows Server 2003 IIS 组件中的 FTP 子组件,来架设一个 FTP 站点。本书的第 7 章将介绍 FTP 服务器的配置与管理。

9. 邮件服务器角色

若要向用户提供电子邮件服务,可以使用 Windows Server 2003 提供的邮局协议 3 (POP3) 和简单邮件传输协议 (SMTP) 组件。POP3 服务实施标准的 POP3 协议,用于邮件检索,可以将它与 SMTP 服务配对以启用邮件传输。如果要让客户端与该 POP3 服务器连接,并使用适于 POP3 的邮件客户端将电子邮件下载到本地计算机上,请将该服务器配置为邮件服务器。本书的第 8 章将介绍邮件服务器的配置与管理。

10. 证书服务器角色

证书服务器是 PKI 公共密钥安全体系中的关键设备,注册、发放和管理网络系统中各种设备和用户的证书,用于建立和保障网络安全通信中的身份认证和相互信任体系。若要在组织内部建立 PKI 公共密钥安全体系为用户提供服务,可以使用 Windows Server 2003 的

证书服务组件,来架设一个 CA 证书服务器。本书的第 9 章将介绍证书服务器的配置与管理。

11. 流式媒体服务器角色

流式媒体服务器可为组织内部提供 Windows Media Services。Windows Media Services 通过 Intranet 或 Internet 对 Windows Media 内容进行管理、交付和存档,包括流式音频和视频。如果您计划通过拨号连接 Internet 或局域网 (LAN) 实时地使用数字媒体,请将该服务器配置为流式媒体服务器。本书的第 10 章将介绍流式媒体服务器的配置与管理。

12. NAT 服务器和基本防火墙角色

随着 Internet 的迅速发展,IP 地址短缺已成为一个十分突出的问题。如果组织的合法的 IP 地址不够用时,可以使用网络地址转换(NAT)功能,将内部用户设置为私有 IP 地址。本书的第 10 章将介绍 NAT 服务器和基本防火墙角色的配置与管理。

13. 远程访问/VPN 服务器角色

“路由和远程访问”服务为远程计算机提供了功能完备的软件路由器以及拨号和虚拟专用网(VPN)连接,为局域网(LAN)和广域网(WAN)环境提供路由服务。另外,还允许远程和移动人员通过拨号连接或者使用 VPN 连接通过 Internet 访问公司网络,就好像直接连接一样。如果要将远程人员(或网络)与公司网络连接,请将该服务器配置为远程访问 VPN 服务器。本书的第 12 章将介绍远程访问 VPN 服务器的配置与管理。

 **点评与拓展:**除了通过 Windows Server 2003 自身包含的服务组件实现上述服务器角色外,还可以通过第三方软件来实现。例如通过 Apache Web Server 来实现 Web 服务器和 Web 应用程序服务器角色,通过 Serv-U FTP 来实现 FTP 服务器角色等。

1.2 IP 地址及 IP 子网划分

不论是 Internet,还是 Intranet、Extranet、远程访问应用环境中,都是以 TCP/IP 网络协议为基础。在 TCP/IP 协议网络中,每一台连接到网络中的计算机(或网络设备)都称为一台“主机(host)”。为了标识这些主机,每一台主机都要拥有一个唯一的 IP 地址。

1.2.1 IP 地址

1. IP 地址的组成

一个 IP 地址由网络号和主机号两部分组成。同一个物理网络中的所有主机都用同一个网络号,网络中的每一台主机(包括网络中的工作站、服务器和路由器等)都有一个主机号与其对应。据此把 IP 地址划分为两个部分,一部分用以标明具体的网络段,即网络号(net-id);另一部分用以标明具体的节点,即主机号(host-id)。

2. IP 地址表示

一个 IP 地址由 4 个字节共 32 位的数字串组成，这 4 个字节通常用小数点分隔，每个字节都可用十进制表示，如 192.45.8.22。IP 地址也可以用二进制和十六进制表示，如图 1-1 所示。

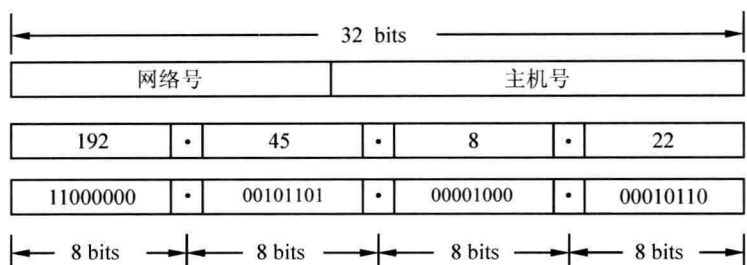


图 1-1 IP 地址的组成与表示

3. IP 地址的分类

IP 协议的寻址方式支持 5 种不同的网络类型：A 类、B 类、C 类、D 类和 E 类。其中，A、B、C 类地址是基本的 Internet 地址，是用户使用的地址。D 类地址被称为组播地址(多点播送地址)，而 E 类地址尚未使用，以保留给将来的特殊用途。IP 地址最左边的 1 个或多个二进制位通常用来指定网络的类型。例如，A 类地址的第一位为“0”，B 类地址的前两位为“10”，C 类地址的前三位为“110”。图 1-2 和表 1-1 说明了 5 种不同网络类型 IP 地址的特征和地址容量。

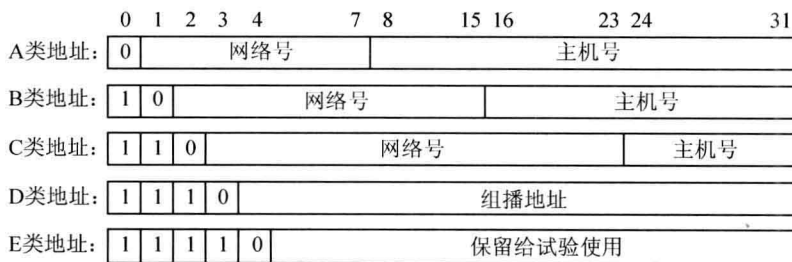


图 1-2 IP 地址的分类

(1) A 类：一个 A 类 IP 地址由 1 个字节的网络地址和 3 个字节主机地址组成，网络地址的最高位必须是“0” (每个字节有 8 位二进制数)。7 位作为网络号，24 位作为主机号，最多可以表示 126 个网络号(0 和 127 用作特殊地址)，每个 A 类地址主机数可以有 $2^{24}-2(16777214)$ 个，适用于大型网络。

(2) B 类：一个 B 类 IP 地址由 2 个字节的网络地址和 2 个字节的主机地址组成，网络地址的最高两位必须是“10”。16 位作为网络号，14 位作为主机号，最多可以表示 $2^{14}(16384)$ 个网络号，每个 B 类地址主机数最多可有 $2^{16}-2(65534)$ 个，适用于中等规模的网络。

(3) C 类：一个 C 类地址由 3 个字节的网络地址和 1 个字节的主机地址组成，网络地

址的最高三位必须是“110”。21 位作为网络号，8 位作为主机号。共有 2^{21} (2097152) 个网络号，每个 C 类地址主机数少于 $2^8 - 2$ (254) 个，适用于小规模局域网。

(4) D 类：用于多点播送。第一个字节以“1110”开始。因此，任何第一个字节大于 223 小于 240 的 IP 地址都是组播地址。

(5) E 类：以“11110”开始，保留给试验用的地址。

表 1-1 Internet 的 IP 地址空间容量

类型	第一字节范围	网络地址长度	网络数	主机地址长度	主机数	用途
A 类	0~127	7 位	126	24 位	16777214	大型网络
B 类	128~192	14 位	16384	16 位	65534	中型网络
C 类	192~223	21 位	2097152	8 位	254	小型网络
D 类	224~239	组播地址				
E 类	240~255	保留给试验使用				

4. 几种特殊的 IP 地址形式

1) 网络地址

主机号各位全为“0”的 IP 地址不能分配给主机使用，它是用来标识本网络的网络地址。例如，C 类 202.102.192.68，网络号占 24 位，主机号占 8 位，因此它的网络地址是 202.102.192.0，主机号是 68。

2) 广播地址

IP 具有两种广播地址形式，即直接广播地址和有限广播地址。

✧ 直接广播地址：主机号各位全为“1”的 IP 地址，用于将一个分组发送给特定网络上的所有主机，即对全网广播。例如，一个 C 类网络的网络地址是 202.102.192.0，则该子网的直接广播地址是 202.102.192.255。

✧ 有限广播地址：网络号和主机号都为 1 的 IP 地址(即 255.255.255.255)，也是对当前网络进行广播，多数是用在当一台主机在运行引导程序但又不知道其 IP 地址时向服务器获取 IP，这时用该地址作为目的地址发送分组。

3) 回送地址

A 类网络地址 127.0.0.0 是一个保留地址，用于网络软件测试以及本地机进程间通信，叫做回送地址。任何一个 IP 数据报，若它的目的地址是回送地址，TCP/IP 协议软件将不会将该数据报在网络传播，而直接返回本机。

1.2.2 子网掩码与子网划分

1. 为什么要划分子网

划分子网的原因主要有以下几点。

(1) IP 地址空间利用率很低。由于 Internet 的 IP 采用两级结构，即网络号和主机号，这样的设计有不够合理的地方。IP 地址中的 A 至 C 类地址，可供分配的网络号码超过 211 万个，而这些网络上的主机号的总数则超过 37.2 亿个，初看起来，似乎 IP 地址足够全世界

来使用(在 20 世纪 70 年代初期设计 IP 地址时就是这样认为的)。其实不然。第一,当初没有预计到微机会普及得如此之快,各种局域网和局域网中的主机数目急剧增长。第二,IP 地址在使用时有很大的浪费。例如,某个单位申请到了一个 B 类地址,但该单位只有 1 万台主机。于是,在这个 B 类地址中的其余 5 万 5 千多个主机号码就白白地浪费了,因为其他单位的主机无法使用这些号码。

(2) 大的网络将影响网络性能。从网络吞吐量考虑,将大量主机安装在一个网络上往往会影响网络的性能。当网络上工作的主机数小于一定数值时,网络的吞吐量和网络上工作的主机数大约成正比。但是当网络上工作的主机数超过一定数量时,拥塞就可能产生,这就导致网络的吞吐量增长缓慢,甚至会随着主机数的增加而下降。

(3) IP 的两级结构也不够灵活。有时情况紧急,一个单位需要新的地点马上开通一个新网络。但是在申请到一个新的 IP 地址之前,新增加的网络不可能连接到因特网上工作。我们希望有一种方法,使用户能随时灵活地增加本单位的网络,而不必事先到因特网管理机构去申请新的网络号。原来的两级 IP 地址无法做到这一点。

2. 从两级 IP 地址到三级 IP 地址

为了解决上述问题,在 IP 地址中又增加了一个“子网号”字段,使原来两级的 IP 地址变成三级的 IP 地址,它能够较好地解决上述问题,并且使用起来也很灵活。划分子网的基本思路如下。

(1) 一个拥有许多物理网络的单位,可将所有物理网络划分为若干个子网(subnet)。划分子网纯属一个单位内部的事情,本单位以外的网络看不见这个网络是由多少个子网组成的,对外仍表现为一个没有划分子网的网络。

(2) 划分子网的方法是从网络的主机号借用若干比特作为子网号 subnet-id,而主机号 host-id 也就相应减少了若干比特。于是两级的 IP 地址在本单位内部就变为三级 IP 地址:网络号 net-id、子网号 subnet-id 和主机号 host-id,如图 1-3 所示。

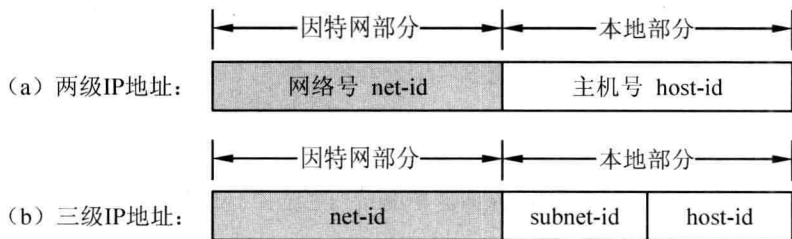


图 1-3 从两级 IP 地址到三级 IP 地址

(3) 从其他网络发送给本单位某个主机的 IP 数据报,仍然是根据 IP 数据报的目的网络号 net-id 找到连接在本单位网络上的路由器。但此路由器在收到 IP 数据报后,再按目的网络号 net-id 和子网号 subnet-id 找到目的子网,将 IP 数据报交付给目的主机。

下面用一个例子来说明划分子网的概念。图 1-4 表示一个单位拥有一个 B 类 IP 地址,网络地址是 141.14.0.0(net-id 是 141.14)。凡目的地址为 141.14.x.x 的数据报都被送到这个网络上的路由器 R1。

现将图 1-4 的网络划分为三个子网，如图 1-5 所示。这里假设子网号 subnet-id 占用 8 位，因此在增加了子网号后，主机号 host-id 就只有 8 位。所划分的三个子网分别是：141.14.2.0、141.14.7.0 和 141.14.99.0。在划分子网后，整个网络对外部仍表现为一个网络，其网络地址仍然是 141.14.0.0。此时，路由器 R1 收到数据报后，再根据数据报的目的地址将其转发到相应的子网。

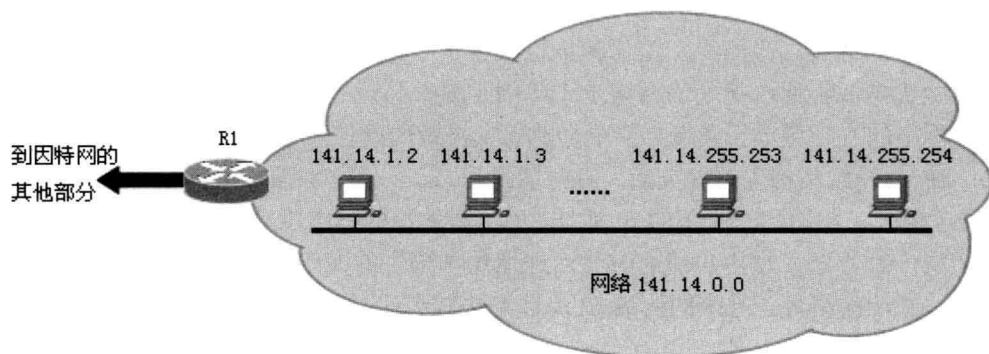


图 1-4 从两级 IP 地址到三级 IP 地址

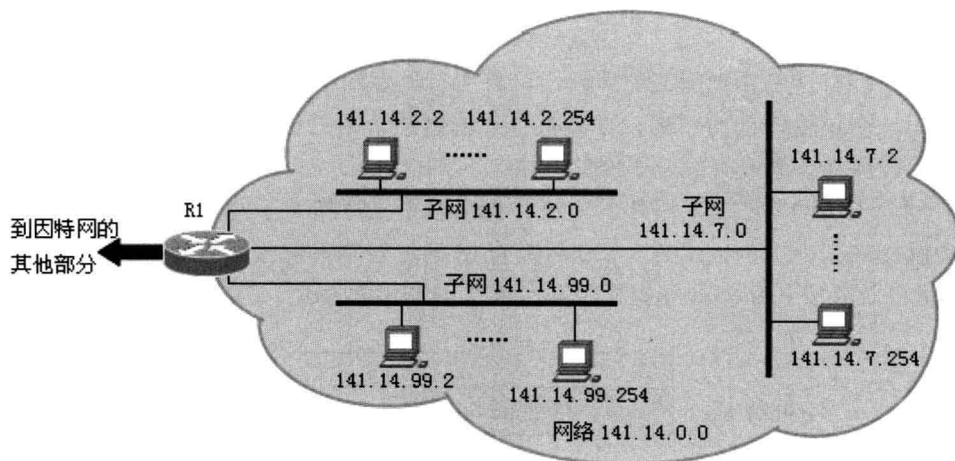


图 1-5 从两级 IP 地址到三级 IP 地址

3. 子网掩码

虽然上面已经把—个网络划分成为若干个子网，但路由器 R1 必须知道数据报中目的 IP 地址的网络号 net-id、子网号 subnet-id 和主机号 host-id 各是多少位，这就需要通过子网掩码(Subnet mask)来实现。

子网掩码和 IP 地址—样，也是 32 位，由—串 1 和跟随的—串 0 组成。子网掩码中的 1 对应于 IP 地址中的网络号 net-id 和子网号 subnet-id，而子网掩码中的 0 对应于 IP 地址中的主机号 host-id。要得到网络或子网地址，只需将 IP 地址和子网掩码按位进行“与”(AND)

运算就可以得到。图 1-6 说明了子网掩码是如何工作的。

图 1-6(a)表示在没划分子网的情况下,网络地址是 IP 地址与它的默认的子网掩码(255.255.0.0)逐位相“与”(AND)的结果,即将主机号 host-id 置为 0 的 IP 地址。图 1-6(b)表示在划分子网情况下,在主机号借用 8 位作为子网号 subnet-id,子网掩码中的“1”个数相应地增加 8,即 255.255.255.0。这时将子网掩码和 IP 地址逐位相“与”(AND)就得到了子网地址。这里要注意:网络地址(在划分子网时常称为子网地址)并不仅仅是一个子网号 subnet-id,而是将主机号 host-id 置为 0 的 IP 地址。可以看出,子网掩码不能单独存在,它必须结合 IP 地址一起使用。

141.14.2.21				
IP地址:	10001101	00001110	00000010	00010101
255.255.0.0				
子网掩码:	11111111	11111111	00000000	00000000
141.14.0.0				
网络地址:	10001101	00001110	00000000	00000000
(a) 不划分子网				
141.14.2.21				
IP地址:	10001101	00001110	00000010	00010101
255.255.255.0				
子网掩码:	11111111	11111111	11111111	00000000
141.14.2.0				
网络地址:	10001101	00001110	00000010	00000000
(b) 划分子网				

图 1-6 按位进行“与”(AND)运算可得到网络地址

与 IP 地址相同,子网掩码也通常使用点分十进制表示法,例如 255.255.255.0、255.255.255.240 等。有时为了表示方便,通常在 IP 地址后加一个“/网络号和子网号位数”。例如,210.45.12.58/28 就表示该 IP 地址的网络号 net-id 和子网号 subnet-id 共占用 28 位,主机号占用 $32-28=4$ 位,如果用点分十进制表示法表示,则子网掩码为 255.255.255.240 (11111111.11111111.11111111.11110000)。

使用子网掩码的好处就是,不管网络有没有划分子网,不管 IP 地址中的网络号 net-id 和子网号 subnet-id 是多少位,只要将子网掩码和 IP 地址逐位相“与”(AND),就能立即得出网络地址,这样在路由器处理到来的 IP 分组时就可采用同样的算法。

如果一个网络不划分子网,那么该网络的子网掩码就使用默认的子网掩码。默认子网掩码中 1 比特的位置和 IP 地址的网络号 net-id 正好相对应。因此默认子网掩码和不划分子网的 IP 地址逐位相“与”(AND),就能得出该 IP 地址的网络地址,这样做就可以不用查找该地址的分类位就能知道这是哪一类的 IP 地址。显然,A 类、B 类和 C 类网络默认子网掩码分别是 255.0.0.0(/8)、255.255.0.0(/16)、255.255.255.0(/24),如图 1-7 所示。

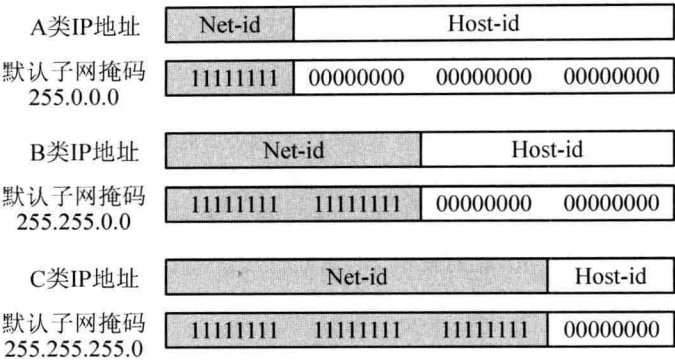


图 1-7 A 类、B 类和 C 类网络默认子网掩码

4. 划分子网实例

1) B 类地址的子网规划示例

B 类地址由两个字节的网络号 net-id 和两个字节的主机号 host-id 组成。一个得到 B 类地址的组织可以有一个单独的物理网络，在此网络上连接的计算机可达 $65534(2^{16}-2)$ 个。但是，若该组织愿意有更多的物理网络，则这个大的范围可划分成许多更小的范围，表 1-2 说明了一个 B 类地址可以有多少种子网划分方法。在采用固定长度子网时，划分的所有子网的子网掩码都是相同的。

表 1-2 B 类地址的子网划分选择(使用固定长度子网)

子网位数	子网掩码	子网数	主机数
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

例如，一个具有 B 类地址的组织，网络号为 X.Y.0.0($128 \leq X \leq 191$)，至少需要 12 个子网，试找出子网掩码和每个子网的配置。因为至少需要 12 个子网，划分时至少要有 14 个子网，其中 12 个是可用的，两个保留为特殊地址，不可用，因此至少需要向主机号 host-id

借 4 位($2^3-2 \leq 14 \leq 2^4-2$)来构造子网, 网络号 net-id 和子网号 subnet-id 共 12 位($8+4=12$), 所以子网掩码为 11111111.11111111.11110000.00000000, 即 255.255.240.0。每个子网有 4096 个($2^{12}=4096$)地址, 其中第一个地址用来定义子网(子网地址), 而最后一个地址用于子网内广播(广播地址), 这就表明连接到每一个子网上的计算机数是 4094。表 1-3 是每一个子网的地址范围。

表 1-3 B 类地址的子网划分实例(使用固定长度子网)

子 网	子网地址	地址范围	广播地址	说 明
第 0 个子网	X.Y.0.0	X.Y.0.1 ~ X.Y.15.254	X.Y.15.255	保留, 不可用
第 1 个子网	X.Y.16.0	X.Y.16.1 ~ X.Y.31.254	X.Y.31.255	可用
第 2 个子网	X.Y.32.0	X.Y.32.0 ~ X.Y.47.254	X.Y.47.255	可用
.....				可用
第 14 个子网	X.Y.224.0	X.Y.224.0 ~ X.Y.239.254	X.Y.239.255	可用
第 15 个子网	X.Y.240.0	X.Y.224.1 ~ X.Y.239.254	X.Y.255.255	保留, 不可用

点评与拓展: 根据 RFC950 规定, 进行子网划分时, 子网号 subnet-id 为全 0 和全 1 的子网不允许使用, 因此表 1-3 中, 第 0 个子网和第 15 个子网是不能使用的。但随着无分类域间路由选择 CIDR 的广泛使用, 现在全 0 和全 1 的子网也可以使用, 但一定要谨慎使用, 要弄清所使用的路由器是否支持子网号全 0 和全 1 的子网。

2) C 类地址的子网规划

C 类地址由三个字节的网络号 net-id 和一个字节主机号 host-id 组成。一个得到 C 类地址的组织可以有一个单独的物理网络, 在此网络上连接的计算机可达 $254(2^8-2)$ 个。但是, 若该组织愿意有更多的物理网络, 则这个大的范围可以划分成许多更小的范围, 表 1-4 说明了一个 C 类地址可以有多少种子网划分方法 (在采用固定长度子网时, 划分的所有子网的子网掩码都是相同的)。

表 1-4 C 类地址的子网划分方法(使用固定长度子网)

子网位数	子网掩码	子 网 数	主 机 数
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

例如, 一个具有 C 类地址的组织, 网络号为 X.Y.Z.0($192 \leq X \leq 223$), 至少需要 5 个子网, 试找出子网掩码和每个子网的配置。因为至少需要 5 个子网, 划分时至少要有 7 个子网, 5 个是可用的, 两个保留为特殊地址, 不可用, 因此至少需要向主机号 host-id 借 3 位($2^2-2 \leq 7 \leq 2^3-2$)来构造子网, 网络号 net-id 和子网号 subnet-id 共 27($24+3$)位, 所以子网掩码为 11111111.11111111.11111111.11100000, 即 255.255.255.224。每个子网有 32 个($2^5=32$)地址, 其中第一个地址用来定义子网(子网地址), 而最后一个地址用于子网内广播(广播地址), 这

就表明连接到每一个子网上的计算机数是 30。表 1-7 是每一个子网的地址范围。

表 1-5 C 类地址的子网划分实例(使用固定长度子网)

子网	子网地址	地址范围	广播地址	说明
第 0 个子网	X.Y.Z.0	X.Y.Z.1 ~ X.Y.Z.30	X.Y.Z.31	保留, 不可用
第 1 个子网	X.Y.Z.32	X.Y.Z.33 ~ X.Y.Z.62	X.Y.Z.63	可用
第 2 个子网	X.Y.Z.64	X.Y.Z.65 ~ X.Y.Z.94	X.Y.Z.95	可用
.....				可用
第 6 个子网	X.Y.Z.192	X.Y.Z.193 ~ X.Y.Z.222	X.Y.Z.223	可用
第 7 个子网	X.Y.Z.224	X.Y.Z.225 ~ X.Y.Z.254	X.Y.Z.255	保留, 不可用

A 类地址的子网规划的方法和 B 类、C 类相似, 因篇幅所限, 这里不做介绍。

5. 变长子网掩码 VLSM

因特网允许一个地点使用变长子网划分。下面举例说明什么时候有这种需要。考虑有一个具有 C 类地址的地点需要划分为 5 个子网, 其连接的主机数分别为: 60、60、60、30 和 30。这个地点不能给子网分配两位的掩码, 因为这样只有 4 个可连接 62 台主机($256/4-2=62$)的子网。在这个地点给子网部分分配三位掩码也不行, 因为这样将有 8 个可连接 30 台主机($256/8-2=30$)的子网(应注意, 这里放松了对特殊地址的要求, 即子网号全 0 和全 1 可用)。

解决这个问题的一种方法是使用变长子网划分。在这种配置中, 路由器使用两个不同的掩码, 使用一个以后再使用另一个。它先使用具有 26 个 1 的掩码(11111111.11111111.11111111.11000000 或 255.255.255.192), 将网络划分为 4 个子网。然后再对其中的一个子网使用具有 27 个 1 的掩码(11111111.11111111.11111111.11100000 或 255.255.255.224), 将其划分为两个更小的子网, 如图 1-8 所示。

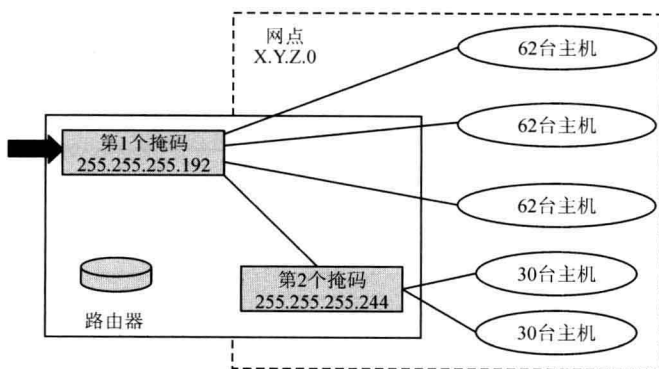


图 1-8 变长子网划分

6. 超网(Supernet)

虽然 A 类和 B 类地址几乎已经用完了, C 类地址目前还能申请到。然而 C 类地址空间最多只能容纳 254 台主机, 这可能无法满足一个组织的需要。

一种解决方法是构成超网(supernet)。为此, 一个组织可申请一块而不是只申请一个 C

类地址。例如，一个需要 1000 个地址的组织可申请 4 个 C 类地址。这个组织就可以在一个超网中、在 4 个网络中或在超过 4 个子网中使用这些地址。在图 1-9 中，4 个 C 类地址合并为一个超网。

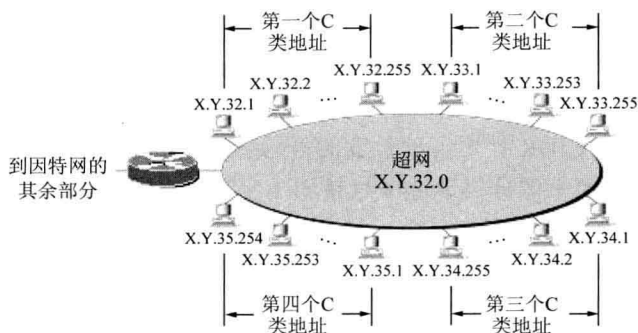


图 1-9 超网

可以给超网掩码指派一块 C 类网络地址，只要地址数是 2 的整数次方(2, 4, 8, 16...)。C 类地址的默认掩码是 255.255.255.0，即 24 个 1 后面跟上 8 个 0。如果将其中的某些 1 改变为 0，就可得到一组 C 类地址的掩码。如图 1-10 所示，超网掩码与子网掩码不同。在子网掩码中，我们将默认掩码中的 host-tid 部分的某些 0 改变为 1。在超网掩码中，我们将 net-id 部分中的某些 1 改变为 0。要注意，在超网掩码中全 1 的位置定义了最低地址。例如，如图 1-10 所示的超网掩码，开始地址可以是 X.Y.32.0，但不能是 X.Y.33.0。将最低地址与超网掩码组合起来就能唯一地定义属于一个超网的地址范围，另一个定义地址范围的方法是使用最低地址和在此范围内的地址数。

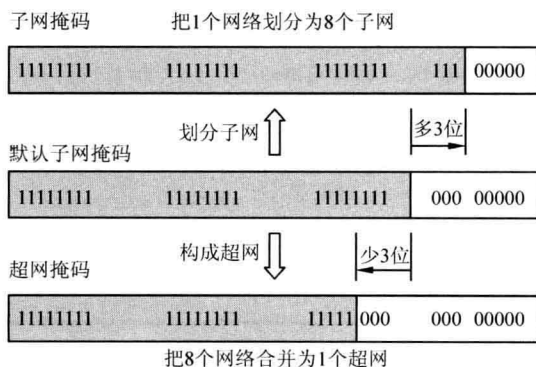


图 1-10 超网掩码

例如，用超网掩码 255.255.252.0 可以将 4 个 C 类地址合并成为一个超网。如果选择第一个地址是 X.Y.32.0，则其他三个地址就是 X.Y.33.0、X.Y.34.0 和 X.Y.35.0。当路由器收到一个分组时，就将超网掩码应用到目的地址，并与最低地址相比较。若结果与最低地址一致，则该分组就属于这个超网。

假定一个分组到达目的地址 X.Y.33.4。在应用掩码 255.255.252.0 后，结果为 X.Y.32.0，它与最低地址一致，因此该分组属于这个超网。

现在假定具有目的地址为 X.Y.39.12 的分组到达。在应用掩码 255.255.252.0 后，结果为 X.Y.36.0，它与最低地址不一致，因此该分组不属于这个超网。

7. 无分类编址(CIDR)

在 VLSM 的基础上又进一步研究出无分类编址方法，它的正式名字是无分类域间路由选择(CIDR, Classless Inter-Domain Routing)。CIDR 最主要的特点有两个。

一是 CIDR 消除了传统 A 类、B 类和 C 类地址以及划分子网的概念，从而更加有效地分配 IPv4 的地址空间。CIDR 使用各种长度的“网络前缀”(network-prefix)来代替分类地址中的网络号和子网号，而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀，使 IP 地址从三级编址(使用子网掩码)又回到两级编址，但这是一个无分类的两级编址。CIDR 使用“斜线记法”，它又称为 CIDR 记法，即在 IP 地址后面加上一条斜线“/”，然后写上网络前缀所占的位数(这个数值对应于三级编址子网掩码中 1 的个数)。例如，128.14.146.158/20，表示在这 32 位中，前 20 位表示网络前缀，而后面 12 位为主机号。

二是 CIDR 将网络前缀都相同的、连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块是由地址块的起始地址(即地址块中地块数值最小的一个)和地址块中的地址数来定义的。CIDR 地址块也可用斜线记法来表示，例如，128.14.32.0/20 表示的地址块共有 2^{12} 个地址，而这个地址的起始地址是 128.14.32.0。

1.2.3 私有 IP 地址的使用

如果一个组织不需要接入因特网，但需要在其网络上运行 TCP/IP 协议，最佳选择是使用本地地址。本地地址不需要从因特网管理机构申请，任何组织都可以使用这些地址。这些地址在一个组织内部是唯一的，但从全局来看却不是唯一的。同时因特网的路由器也不转发目标地址为本地地址的数据包。表 1-6 所示的是私有 IP 地址。

表 1-6 Internet 的保留 IP 地址空间

类 型	网 络 号	网 络 数
A 类	10.0.0.0	1
B 类	172.16.0.0 至 172.32.0.0	16
C 类	192.168.0.0 至 192.168.255.0	256

1.3 利用虚拟机技术构建 Windows Server 2003 实验环境

对于 Windows Server 2003 学习者来说，最大困难可能是没有一个实验环境。自从有了虚拟机，这个问题就解决了。下面简要介绍什么是虚拟机、虚拟机的特点，以及如何利用虚拟机技术构建 Windows Server 2003 实验环境。

1.3.1 虚拟机简介

1. 什么是虚拟机

虚拟机本质上讲是一套软件，通过对计算机硬件资源的管理和协调，在已经安装了操作系统的计算机上虚拟出一台计算机来。虚拟机让用户可以在一台实际的机器上同时运行多套操作系统和应用程序，这些操作系统使用的是同一套硬件装置，但在逻辑上各自独立运行、互不干扰。虚拟机软件将这些硬件资源映射为本身的虚拟机器资源，每个虚拟机器看起来都拥有各自的 CPU、内存、硬盘、I/O 设备等。

虚拟机与主机、虚拟机与虚拟机间可以通过网络进行连接，在软件层上和真实的网络并没有区别。甚至可以通过桥接的方式将虚拟机接入实际的局域网中，这台虚拟机就成为网络中的一员，与网络中其他计算机地位一样。还可以使用这台虚拟机上网，安装应用软件，完全和一台真实的计算机一样。

2. 虚拟服务器

虚拟服务器是不久前才发展出来的一个概念。什么是虚拟服务器呢？就是在计算机上建立一个或多个虚拟机，由虚拟机来做服务器的工作。将服务器的功能包括操作系统从硬件上剥离出来，使得服务器看起来就像一个软件或者文件，因而具有良好的移植性和可恢复性。

在哪些地方可以用到虚拟服务器呢？在某些场合下，一个局域网中只有一台服务器，但需要提供多个功能，将所有的服务功能都放在同一个服务器上不便于管理，也不安全。比如有的服务本身存在漏洞，容易被恶意控制，这个时候其他关键的服务也会受到牵连。将不同安全级别的服务安放在不同的虚拟服务器上是个不错的主意。

又比如有些服务程序只能运行在特定的操作系统上，单独为这个服务配置一台服务器过于昂贵，这个时候虚拟机就能经济简单地解决这个问题。

另外，虚拟服务器的移植和恢复都非常快。我们可以为虚拟服务器建立快照，就是将服务器当前的状态用一个文件保存下来。如果虚拟服务器出现故障，只需要几十秒钟载入快照就能让它重新运行起来。如果虚拟机所在的真实计算机不能使用了，将快照文件复制到别的计算机上就能马上重新运行服务器了。

点评与拓展：虚拟机只有在运行时才占用系统资源，如果只是建立了虚拟机而没有运行它，除了占用小部分硬盘空间外它不会占用别的东西。您尽可在一台计算机上建立多个虚拟机，只要控制同时运行的虚拟机的数量就行了。

3. 常用的虚拟机软件

目前常用的虚拟机软件主要有三种，分别如下。

(1) VMware，使用非常简便，但没有模拟显卡，需要在虚拟机中安装虚拟机工具 VMware-tools 才能使虚拟机具有高分辨率和真彩色，否则只能工作在 VGA 模式下。VMware 通过模拟网卡与主机进行网络连接。

(2) Virtual PC，微软公司的产品，对 Windows 系列操作系统的支持非常好，但其他方面就没这么出色了。Virtual PC 是通过在现有网卡上绑定 Virtual PC emulated switch 服务来实现网络共享的。

(3) Bochs，一套免费的开源软件，可以自行修改编译源代码，而前面两个都是商业软件。Bochs 对 Linux 系统的支持非常好，但操作略显复杂，多用于 Linux 平台上。

1.3.2 安装 VMWare Workstation

本节以 VMware Workstation 5.5 版本为例，说明虚拟机软件 VMware 的安装与配置过程。

- 1 在 VMware 官方网站下载 VMware 安装文件并申请注册序列号，其网址是 <http://www.vmware.com>。
- 2 双击 VMware Workstation 的安装文件，安装文件解压缩后，将启动欢迎界面，单击 Next 按钮继续，如图 1-11 所示。

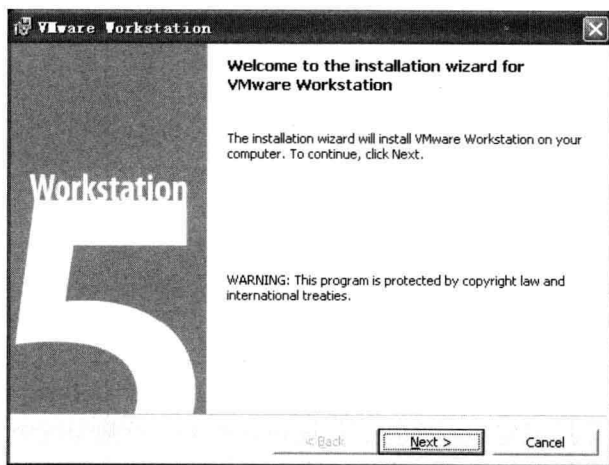


图 1-11 VMware 安装向导

- 3 在 License Agreement 向导页中，询问是否同意最终用户许可协议，选择 Yes, I accept the terms in the license agreement 单选按钮，单击 Next 按钮继续，如图 1-12 所示。
- 4 在 Destination Folder 向导页中，选择虚拟机软件安装的路径。可单击 Change 按钮更改默认路径，修改完成后，单击 Next 按钮继续，如图 1-13 所示。
- 5 在 Configure Shortcuts 向导页中，选择是否创建桌面图标、开始菜单选项和快速启动图标。用户可根据习惯自行确定来勾选相应的复选框，单击 Next 按钮继续，如图 1-14 所示。
- 6 在 Configure Product 向导页中，选择是否禁用光驱自动播放功能。Windows 下的光驱自动播放功能可能会使虚拟机产生意想不到的错误，因此选中 Yes disable autorun 复选框禁用该功能，单击 Next 按钮继续，如图 1-15 所示。