万水计算机组装与维护系列

Windows 企业网络应用案例精解

（Windows Server 2003 R2）

陶英华 等编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书共分为 15 章，系统地讲解了各种企业网络需求在 Windows Server 2003 R2 操作系统上的实现，并且遵循微软的初衷，介绍了和 UNIX 网络的混合应用。内容包括企业网络基础知识、动态主机配置互联网访问方案、一点对多点网络连接方案、企业域名解析方案、建立集中管理的网络方案、企业加密远程访问方案、企业网站组建方案、内部网络数据加密解决方案、三种 FTP 认证模式的解决方案、用 ISA 构建企业安全方案、NetBIOS 快速名称解析方案、企业邮件通信方案、企业内部时间同步方案、企业文件资源集中共享方案、企业信息共享协同工作方案。在讲解这些应用时，力求符合微软的设计要领，即将各种服务和活动目录服务相集成的观点，不单单讲解这些服务在单机服务器上的配置，而是着重讲解了和活动目录集成的配置方法与管理方法。

本书适合 Windows Server 2003 R2 的初学者、网络管理员、计算机教师以及 Windows Server 2003 R2 的爱好者学习参考，在内容上兼顾 Windows Server 2003 R2 的初中级使用者，对于网络管理员来说，它可以作为日常网络管理的参考书。

图书在版编目（CIP）数据

Windows 企业网络应用案例精解：Windows Server 2003 R2 / 陶英华等编著. —北京：中国水利水电出版社，2007

（万水计算机组装与维护系列）

ISBN 978-7-5084-4249-5

Ⅰ. W… Ⅱ. 陶… Ⅲ. 服务器—操作系统（软件），Windows Server 2003 R2 Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2006）第 143323 号

书　　名	Windows 企业网络应用案例精解（Windows Server 2003 R2）
作　　者	陶英华　等编著
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm　16 开本　33 印张　815 千字
版　　次	2007 年 1 月第 1 版　2007 年 1 月第 1 次印刷
印　　数	0001—4000 册
定　　价	55.00 元

前　言

在微软的 Windows Server 2003 发布之后，由于现阶段后续版本还没有开发成熟，所以微软推出了一个 SP1 和一个升级版本，也就是 R2，重点加强了服务器系统的安全性和与 UNIX 系统的互访问性。本书以笔者做过的网络方案为基础，在 Windows Server 2003 R2 上重现了这些方案的配置。主要内容包括：企业网络基础知识、动态主机配置互联网访问方案、一点对多点网络连接方案、企业域名解析方案、建立集中管理的网络方案、企业加密远程访问方案、企业网站组建方案、内部网络数据加密解决方案、三种 FTP 认证模式的解决方案、用 ISA 构建企业安全方案、NetBIOS 快速名称解析方案、企业邮件通信方案、企业内部时间同步方案、企业文件资源集中共享方案、企业信息共享协同工作方案。重点介绍了比较难的知识点，例如 IPSec 的使用、FTP 的活动目录隔离以及与 UNIX 的 NFS 的互操作等内容。笔者希望这些配置方案能起到抛砖引玉的作用，将来能有更多的著作介绍 Windows 和 UNIX 的互相操作和融合。对于涉及 UNIX 的操作，书中均给出了详尽的截图说明。另外，书中还介绍了一些现在网络管理过程中很实用的应用程序，以及笔者自己编写的小程序等。

针对现在一些网友抱怨介绍网络配置的书不注重安全性的问题，本书最后还介绍了 Windows Server 2003 R2 的安全配置向导，其实也就是 SP1 带的安全配置向导。这样，用户在享受服务器提供的各项优秀服务的同时，还可以配置出一个比较安全的操作系统，减少了用户的后顾之忧。

最后，感谢在本书写作过程中为笔者审稿的翟宏颖、林小杰、韩美琦，感谢对本书进行校对的宋萍、陶思言、唐宇、韩德成、陶景生、高鹤、侯锋、韩英伟、于航、陶英轩、刘建等同志。

作　者

2006 年 8 月

目　　录

第 1 章　企业网络基础知识

1.1　OSI 模型

OSI 模型是由国际标准化组织（ISO）于 1984 年发布的，在每册讲解互连网络设计的专业书籍中都必不可少地要讲到这个参考模型。为什么都要讲解这个模型呢？因为在 1984 年以前，建立计算机网络都以不同的硬件设备和软件来设计组建，在局域网络内，计算机之间的访问是畅通的，但是不同的局域网络之间的通讯就成了问题。因为它们使用了不同的硬件和软件结构来架设，这样就导致了它们之间的难以沟通。解决它们之间的兼容性问题很困难。ISO 认识到开发一种被众多厂商都采用的网络模型的需要，因此 ISO 研究了众多的网络结构，例如 DECnet、SNA 和 TCP/IP 等网络方案，最终发布了 OSI 网络模型。OSI 模型如图 1-1 所示。

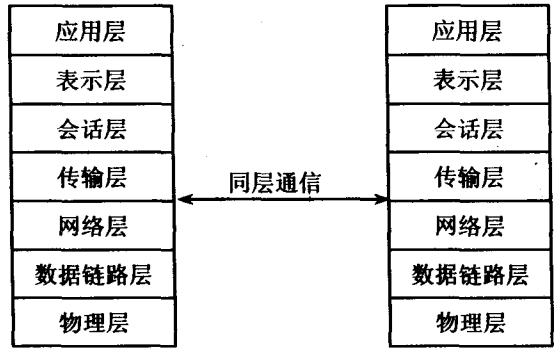

图 1-1　OSI 模型

那么，OSI 模型的具体表现形式是什么呢？OSI 模型对应到现实世界中来就是网络协议和物理网络设备。

OSI 模型开发出来以后并未得到广泛的实际采纳，但是绝大多数公司在他们开发出来的产品中所实现的协议都是以 OSI 模型为参照而建立的。所以说，OSI 模型是一个参考模型，虽然它并未被严格应用在开发领域，但是它却起到了一个模板的作用。在网络领域的标准统一方面做出了巨大的贡献。

那么，什么是协议呢？协议是计算机之间共同遵守的一套信息传输规则。如果计算机之间想要成功地进行通信，就必须共同遵守这套规则。两台主机要进行通信，必须使用相同的协议。一个开发出来的协议一般覆盖了 OSI 模型中的某几层，通常是一个协议集合，称为协议栈或协议族。OSI 模型各层的功能就是这个协议族中的各个协议的作用，而物理层的功能就是网络设备的作用，如网卡或网络适配器。

数据在网络上传输时是以帧的形式穿越 OSI 模型的各层以及通过网络传输介质。怎样理解帧呢？帧也叫数据包，它在传输时就像上学时我们在课堂上传递的小纸条。例如我想约另一

个同学下课一起去学校的机房，但是现在正在上课，我们相隔了好几张桌的距离。我只好写一张纸条，首先需要写上那个同学的名字，也就是纸条要传给谁，然后写上我的名字。如果类比数据帧的传输，我还需要在我名字的后面再写上“如果纸条破损了，请传给我纸条告之，我给你重发。”，然后写上正文，最后传出去。而经过的每一位同学，可以看作网络介质。我的手和各位传递的同学都可以看作物理层设备。而接受我的纸条的同学的思想就可以看作 OSI 模型的物理层以上各层的协议。数据帧的确可以类比为传递的纸条。数据帧的结构如图 1-2 所示。

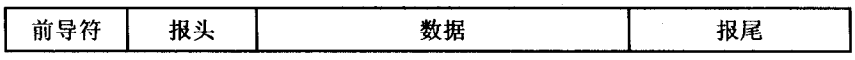

图 1-2 数据帧的结构

前导符通知接收方包即将到达。报头部分包括数据帧的目的地址、来源地址，还有 OSI 各层附加的报头信息。数据就是帧所携带的数据，这才是真正要传达的正文。报尾包括帧的 CRC 校验码以及包的结束符。

每块网卡都有一个 MAC 地址，这个地址是全球惟一的，用以识别和定位这个网络实体。MAC 地址的长度是 48 位，用 12 个十六进制数表示。前 6 个十六进制数由 IEEE 管理，用来识别生产者，构成组织的惟一标识符，后 6 个十六进制数包含了网卡的序列号。这个序列号是预烧到网卡的只读存储器中的。网卡被初始化时，这个地址被复制到计算机的内存中。

了解了网络实体的定位以后，下面介绍一下数据帧在穿越 OSI 模型的各层以及在网络上传输的过程。首先介绍一下 OSI 模型各层的功能。

1. *应用层*

应用层在实际的网络工作中负责与用户使用的应用程序的交互。也就是说，用户的应用程序使用计算机网络功能时需要调用应用层协议，如 HTTP、FTP、SMTP、POP3、IMAP 等。用户的应用程序有 IE、Netscape、Outlook 等。应用层负责创建最初的网络数据帧，如果某种协议的功能是从无到有创建网络数据帧，那么这个协议通常是应用层协议。应用层协议是网络应用程序使用网络功能时的基础，并且产生最初的数据帧。

2. *表示层*

表示层负责解决用户信息的语法表示问题，它的功能是修改数据格式。例如在设置邮件服务器时通常要设置一种协议叫做 MIME。MIME 是“多用途互联网邮件扩充协议”，其功能是在一封邮件中可以传输图像、声音等多媒体信息。我们知道，SMTP 协议只支持纯文本格式，如果要想传输多媒体信息，就需要将多媒体信息转化为纯文本格式，然后在接收端再将其转化回来。这就需要表示层协议，而 MIME 就是这样一种表示层协议。表示层还负责数据的压缩、加密、解密等工作。

表示层的协议所完成的功能位于应用层之下，可以看成是应用层的基础，主要完成的工作是数据格式转换以及数据的加解密和压缩等。它可以补充应用层的功能。

3. *会话层*

会话层为表示层实体提供建立、维护、结束会话连接的功能，允许不同计算机上的应用程序建立、使用会话，并提供名字识别和安全性等功能。它首先通过传输层服务连接到远程处理上，然后再为上一层管理会话。因此，尽管传输层可能只提供非连接式服务，但会话层能为上一层提供连接式服务。典型的会话层协议有 RPC、LDAP、NETBIOS 等。

会话层的特点是在两个应用程序之间执行、维持和终止会话，但是也并不总是这样，例

如在 TCP/IP 协议中，这一功能由传输层完成。

4. 传输层

传输层的主要功能是数据传输过程中的差错检验、出错恢复以及流量控制等。传输层向上一层提供一个可靠的端到端的连接通信，使上一层看不见下面几层的通信细节。在传输层的通信分为两种：面向连接的通信和无连接通信。面向连接的通信在通信双方开始通信前在双方建立一条可靠的连接。首先发送方将通信报文发送到目标以便目标知道数据将要到达，然后目标方会回馈给发送方一条报文，让发送方知道目标方已经收到通知并且做好了接收准备。

无连接通信和面向连接通信的区别是，无连接通信不产生最初的信任连接，所以信息发出后，发送方并不知道信息是否到达了目标方。但是无连接通信的速度要快于面向连接通信的速度。传输层协议有 TCP、UDP 等。

传输层最主要的功能是提供一个可靠的端到端通信，并且实现数据的流量控制等。流量控制功能对于路由器之间的通信是异常重要的。

5. 网络层

网络层负责处理网络寻址和路由。在网络上定位主机或网络设备的功能由网络层协议来实现。经常使用的网络层协议有 IP 和 IPX 等。从网络层开始以下三层都和网络通信有关，称为通信子网。它们负责将数据报文从一个地方可靠地传递到另一个地方，并且网络层向数据帧的报头添加网络地址。

6. 数据链路层

数据链路层的作用是把相邻两个节点间不可靠的物理链路变成可靠的无差错的逻辑链路，包括把原始比特流分帧、排序、设置检错、确认、重发、流控等功能。数据链路层传送信息的单位是帧（Frame），每帧包括一定数量的数据和一些必要的控制信息，在每帧的控制信息中，包括同步信息、地址信息、差错控制信息、流量控制信息等。同物理层相似，数据链路层负责建立、维护和释放数据链路。数据链路层协议附加本地地址（MAC 地址）到数据链路报头。

数据链路层协议有 802 协议、LAPB、LLC 等。

7. 物理层

物理层的作用是负责网络传输中大多数实质性的东西，例如信号标准、布线、电压等。物理层的另一个重要作用是为进行传输而将数据帧转换为比特以在网络介质上进行传输。物理层协议有 EIA/TIA568A、568B、100BaseT 等。物理层负责实际存在的网络设备以及网络传输标准和方法，并且将上层建立的数据帧转化为比特流进行传输。

下面介绍一下数据在网络上传输的过程。数据在网络上传输经历了一个封装和解封装的过程。首先从应用层开始，应用程序创建了要传输的数据，然后应用层在数据前面添加了应用层报头。然后由表示层协议将数据分为表示层信元并将表示层报头添加进来。接下来会话层协议将数据分为会话层信元并且将会话层报头添加进来。在传输层，数据分为数据报并将传输层报头添加进来。在网络层，网络层协议将数据分为数据包，网络层报头添加进来。在数据链路层数据分为数据帧，数据链路层报头添加进来。在物理层，数据分为原始比特流，添加物理控制报头。这是数据的封装过程。在接收端，相应层协议将相应层报头去掉，然后提供给上一层处理，最后提取出最终的数据。这称为解封装过程。数据帧如图 1-3 所示。

物理层报头	数据链路层报头	网络层报头	传输层报头	会话层报头	表示层报头	应用层报头	数据
物理层创建	数据链路层创建	网络层创建	传输层创建	会话层创建	表示层创建	应用层创建	应用程序创建

图 1-3 数据帧格式

现在用一个在互联网上进行邮件发送的例子来说明 OSI 模型各层的作用。首先用 Outlook 创建一封邮件，同时还想将我的照片一起发送给我的朋友 tyh99@126.com，于是照片以 JPG 的格式装入了附件。邮件写完后，填入了朋友的邮箱地址，然后单击“发送”按钮。这时一个邮件 API 报头加到数据的前面。接下来在表示层，因为图像格式是不能直接传送的，因此表示层协议将图像附件的格式转化为纯文本格式，这样一来数据就可以在网络上传递了。接下来就是会话层执行 DNS 解析操作，将 126.com 的 IP 地址解析出来，这样就知道了存储在 126.com 域名服务器上的 MX 记录。会话层为本地 IP 和 MX 的 IP 地址之间建立了一个联系。接下来在传输层，消息被分成了一个个的小块，建立了一个 TCP 会话，并且进行流量控制。建立会话的过程是在网络层进行路由的。具体的寻址是 IP 地址由 ARP 协议转化为网络实体的 MAC 地址，在数据链路层就可以使用 MAC 地址进行寻址通信了。在数据链路层再一次对报文分段，将报文分割为符合介质传输要求的最大传输单元的帧。在物理层，帧转化为比特流进行传输。在另一端的主机执行相反的操作将最终数据提取出来提交给用户使用。

1.2 TCP/IP 协议

TCP/IP 协议是传输控制协议/互联网协议的缩写，是目前使用最广泛的协议之一，并且它是现在的互联网协议标准。

TCP/IP 协议共分为 4 层：应用层、传输层、网际层和网络接口层。它和 OSI 模型的对比如图 1-4 所示。

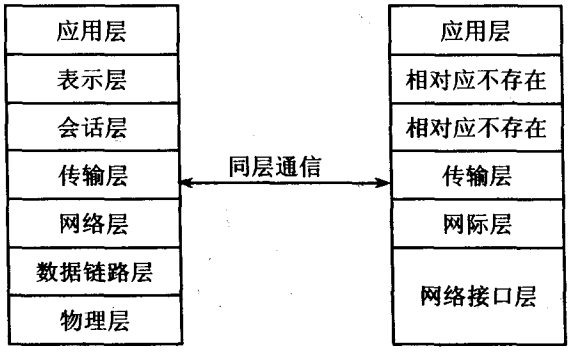

图 1-4 TCP/IP 与 OSI 模型的比较

1. *应用层*

应用层的作用是应用程序通过此层访问网络。这一层的协议有 FTP、HTTP、DNS 等。可见与 OSI 模型相比，TCP/IP 协议将 OSI 模型的前 3 层合并为了应用层。

2. 传输层

传输层负责在网络上相互通信的主机之间提供通信会话。这一层包括两个协议：TCP 协议和 UDP 协议，分别对应面向连接的通信和无连接通信。其中 TCP 使用著名的三次握手的机制为应用程序提供可靠的通信连接，而 UDP 不对包的传输进行可靠保证，发出数据后，它并不保证接收端能够完整地接收到这个数据包，数据的可靠传输只好由应用层来负责。

3. 网际层

网际层协议将数据包封装成数据报，并且运行路由算法。在网际层主要有 4 个协议：IP、ARP、ICMP 和 IGMP。其中，IP 协议负责在网络之间寻址和路由；ARP 用于 IP 地址到 MAC 地址的解析；ICMP 负责发送消息并报告错误；IGMP 被用来向本地多路广播路由器报告主机组成员。

4. 网络接口层

网络接口层是 TCP/IP 模型的最底层，这一层负责数据包的发送和接收。在一个广域网络中，主机与主机之间是如何寻址的呢？首先是使用主机的 IP 地址，这是由网际层的 IP 协议来实现的。IP 协议首先要判断目标主机和本主机是否在一个子网内，判断的方法是将目标主机的 IP 地址和本地子网的子网掩码进行与操作，如果相与后得到的网络地址和本地子网的网络地址相同，则主机会认为目标主机和本地主机在一个子网内，于是开始查询本机的 ARP 表，如果有目标主机的 MAC 地址，则使用这个地址作为数据帧的目的地址给目标主机发送数据帧；如果在本机的 ARP 表中没有目标主机的 MAC 地址，则使用一个全为 F 的广播 MAC 地址发出一条广播，询问目标 IP 地址的 MAC 地址。目标主机会给予应答，于是这条 IP 地址和对应的 MAC 地址就会被存入主机的 ARP 表。如果目标主机的 IP 地址在另一个子网内，也就是说要发送数据的主机用本地子网的掩码和目标主机的 IP 地址相与操作后得到的网络地址和本地子网的网络地址不相同，这个数据帧将被发送到路由器，这时在数据帧中的目的 MAC 地址被替换为路由器的 MAC 地址，但是网络层地址不变，也就是目的和源 IP 地址不变，变化的仅仅是二层 MAC 地址。如果没有路由器的 MAC 地址也将通过 ARP 协议的 ARP 广播得到。然后路由器将会使用下一跳路由器的 MAC 地址替换数据帧中的目的 MAC 地址，最后在目标网络内将数据帧传递给目标主机。

1.3　基本 IP 寻址

下面对上面讲到的记忆点中涉及到的概念做一下介绍。首先介绍一下主机的 IP 地址，在互联网上有两种方式可以惟一地标识主机，一种是主机的 IP 地址，注意这里说的是公网地址；另一种是网卡的 MAC 地址。这两种地址都是全球惟一的。IP 地址的形式如图 1-5 所示，这是一个私有地址。

实际的 IP 地址是由 32 位二进制数来表示的，但是在操作系统的实际配置过程中通常使用十进制来表示，因为十进制易于记忆。将十进制数换算为二进制数的方法如图 1-6 所示。

将余数从下向上排列就成为换算后的二进制数，图中是将十进制数 192 换算为二进制数 11000000。下面介绍将二进制数换算为十进制数的方法，如图 1-7 所示。

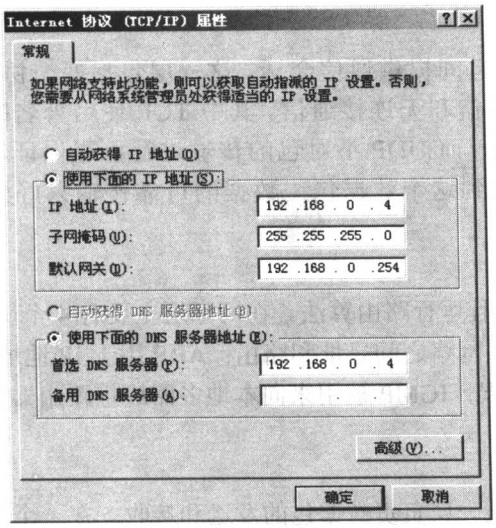

图 1-5 IP 地址的形式

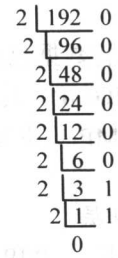

图 1-6 十进制数换算为二进制数

$$\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \end{array}$$

$$1\times128+1\times64+0\times32+0\times16+1\times8+1\times4+0\times2+1\times1$$

图 1-7 二进制数转换为十进制数

二进制数转换为十进制数的方法是将二进制数的最低位定为 2 的 0 次幂，然后用每位二进制数和相应位的 2 求幂相乘，最后把每一位的结果相加，得出的结果就是十进制数。

理解了十进制数和二进制数的关系后，下面介绍一下 IP 地址结构。IP 地址结构如图 1-8 所示。

网络部分	主机部分
192. 168. 0.	4
255. 255. 255.	0

图 1-8 IP 地址结构

整个 IP 地址共分为两个部分：网络部分和主机部分。网络部分表明这台主机位于哪个子网，主机部分标识子网内的具体主机。可以看到，在 IP 地址后面附加了子网掩码，子网掩码的作用就是确定主机位于哪个子网内。

确定网络位置的方法就是使用子网掩码，具体方法是用子网掩码和 IP 地址做与操作，如图 1-9 所示。

11000000. 10101000. 00000000. 00000100

11111111. 11111111. 11111111. 00000000

11000000. 10101000. 00000000. 00000000

192 . 168 . 0 . 0

图 1-9 取网络地址

如果对两个 IP 地址用子网掩码进行与操作后得到的网络地址相同，则这两台主机可以直接进行通信。如果相与操作后得到的网络地址不同，则它们之间的通信要通过路由器进行转发。

不要以子网掩码 255 来判断网络位置，而是要用与操作来判断。例如 192.168.1.1/255.255.255.0 和 192.168.1.2/255.255.0.0 两个 IP 地址如果仅仅依靠子网掩码的位数来判断，得

到的子网位数是不同的，但是进行与操作后得到的网络地址却是相同的，因此这两台主机可以进行通信。

在网络上主机的 IP 地址必须被转化为烧录在网卡只读存储器中的 MAC 地址才能进行通信，由 IP 地址到 MAC 地址的解析是由 ARP（地址解析协议）负责进行的。在每台主机上都维护着一张动态的 ARP 表，如图 1-10 所示，在主机上使用 arp -a 命令。

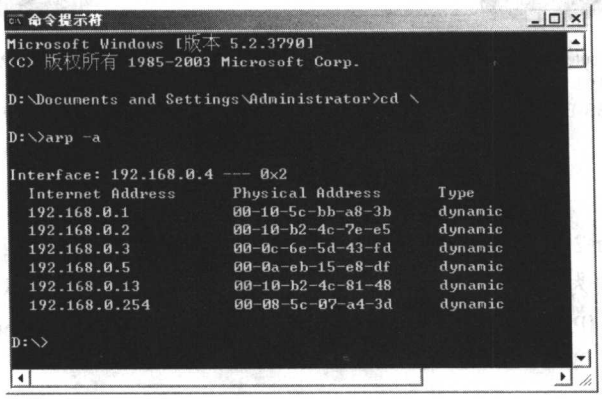

图 1-10　ARP 表

在这张表上记录着本地子网上的主机与它们的 MAC 地址的对应关系，并且列表项是动态添加的。如果与一台没有在这张表上列出的主机通信，并且主机在本地子网上，则通过 ARP 协议的广播会收到目标主机的应答，然后目标主机的 IP 地址和 MAC 地址的对应关系又会添加到这张表中。下面再以图解的方式描述前面讲过的通信过程。整体网络拓扑图如图 1-11 所示。

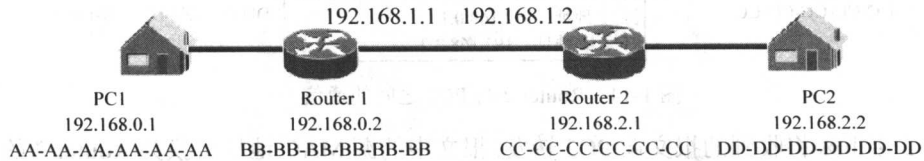

图 1-11　实验网络

实验网络中各个主体之间的连接采用以太网络连接，现在假设 PC1 要发送一个数据包给 PC2。首先来看 PC1 与 Router 1 之间的通信，如图 1-12 所示。

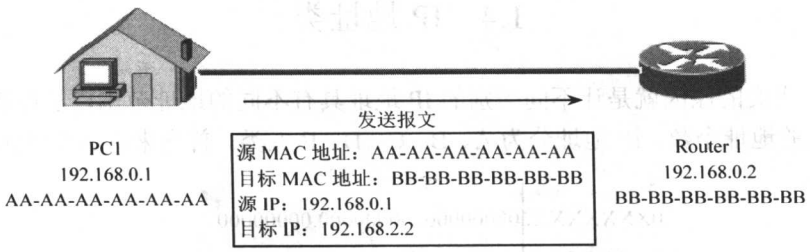

图 1-12　PC1 与 Router 1 之间的通信

PC1 首先用子网掩码和目标 IP 相与，相与的结果表明目标 IP 和 PC1 不在一个子网内，因此这个报文将通过路由器进行转发。如果 PC1 的 ARP 表内没有 Router 1 的 MAC 地址，则 PC1

通过 ARP 协议发送 ARP 广播来获取 Router 1 的 MAC 地址。然后报文内的目标 MAC 地址被替换为 Router 1 的 MAC 地址，但是网络层的源 IP 地址和目标 IP 地址都不变。报文被发送到 Router 1。接下来的通信如图 1-13 所示。

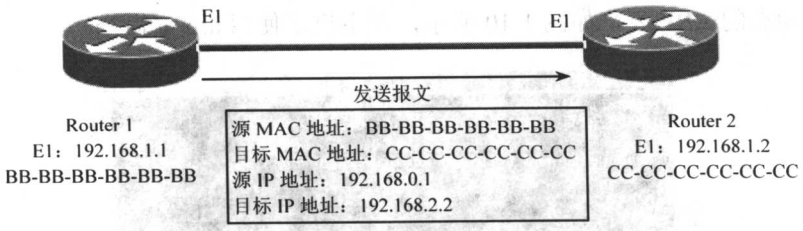

图 1-13 Router 1 与 Router 2 之间的通信

Router 1 与 Router 2 之间连接的端口分别为 192.168.1.1 和 192.168.1.2，Router 1 将报文中的目标 MAC 地址更改为 Router 2 的 MAC 地址，源 MAC 地址更改为 Router 1 的 MAC 地址，但是源 IP 地址和目标 IP 地址仍然不变。报文发送到 Router 2 之后由 Router 2 转发到 PC2。通信过程如图 1-14 所示。

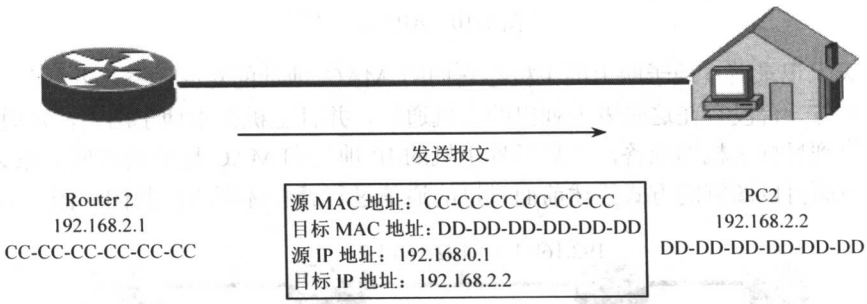

图 1-14 Router 2 与 PC2 之间的通信

Router 2 接下来将收到的报文向 PC2 转发。报文中的源 MAC 地址替换为 Router 2 的 MAC 地址，目标 MAC 地址替换为 PC2 的 MAC 地址，但是源 IP 地址和目标 IP 地址都不变。如果 Router 2 的 ARP 表内没有 PC2 的 MAC 地址，则 Router 2 通过 ARP 协议获得 PC2 的 MAC 地址从而将报文发送给 PC2。这就完成了一次通信过程。

1.4 IP 地址类

IP 地址分成类的原因就是让不同类别的 IP 地址具有不同的地址范围，从而让不同规模的机构使用不同的地址个数。IP 地址分为 A、B、C、D、E 五类。首先来看 A 类地址，如图 1-15 所示。

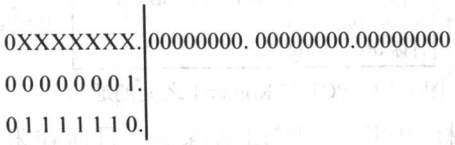

图 1-15 A 类地址

A 类地址的网络地址部分是头 8 个二进制数，并且第一个二进制数为 0，其余部分为主机位。可以看出 A 类地址的主机部分范围特别大。A 类地址用在哪里呢？

A 类地址每个网络的主机数超过 1600 万台，通常用在最高级别的 ISP。

现在来看图 1-15，可以看到，前 8 位最小为 1，最大为 01111111。但是 01111111 换算为十进制后是 127，这个地址用来表示自身，也叫做回送或环回，通常在对其本身执行测试时使用。

网络地址不能全为 0 或全为 1。如果 32 位 IP 地址都为 1，则向本地子网广播；如果知道其他子网的网络地址，那么主机位全为 1 则向其他子网广播。如果 32 位 IP 地址都为 0，则报文送到默认路由。IP 地址中主机地址全为 0 的地址表示网络地址，IP 地址中主机地址全为 1 的地址是广播地址。

因此，A 类网络的网络地址为 1～126，总网络数为 126 个，每个网络的主机数是 1670 万个，默认子网掩码是 255.0.0.0。

B 类 IP 地址的网络地址是 32 位 IP 地址中的头 16 个二进制数，如图 1-16 所示。

10XXXXXX. XXXXXXXX .00000000. 00000000
10000000.00000000 .
10111111.11111111 .

图 1-16　B 类地址

可以看到，B 类网络地址是以 10 开头的，所以最小的网络地址是 10000000.00000000，最大的网络地址是 10111111.11111111。这样满足网络地址不全为 0 也不全为 1。换算为十进制数就是 128.0-191.255。注意这里第二段地址可以是 255，这是因为看网络地址要看整个 16 位，整个网络地址不全为 1。

B 类地址的网络地址范围是 128.0～191.255，B 类地址的每个网络拥有 65534 台主机，总网络数为 16384，默认子网掩码为 255.255.0.0。

现在再来讨论一下 B 类地址的主机范围。因为 B 类地址的后 16 位为主机地址，所以最小的主机地址应该是 00000000.00000001，最大主机地址应该是 11111111.11111110。因为主机地址也不应该全为 0 和 1，全为 0 代表的是主机所在的网络地址，全为 1 代表的是主机所在网络的广播地址，所以换算成十进制数得出的主机地址范围是 XXXXXXXX.XXXXXXXX.0.1～XXXXXXXX.XXXXXXXX.255.254，主机数是 65534 台。

计算主机数量的方法是首先计算出主机地址共有多少位，例如 B 类地址共有 16 位，所以计算方法是 2^{16}-2。为什么要减去 2 呢？因为主机地址不能全为 0 或者全为 1，所以要将这两个地址去掉。这样得出的结果就是 65534。

C 类地址的网络地址部分是 32 位 IP 地址的前 24 位，如图 1-17 所示。

110XXXXX . XXXXXXXX . XXXXXXXX . 00000000
11000000.00000000 .00000000 .
11011111.11111111 .11111111 .

图 1-17　C 类地址

C 类地址的网络部分是以 110 开始的，因此最小网络地址是 11000000.00000000.00000000.，