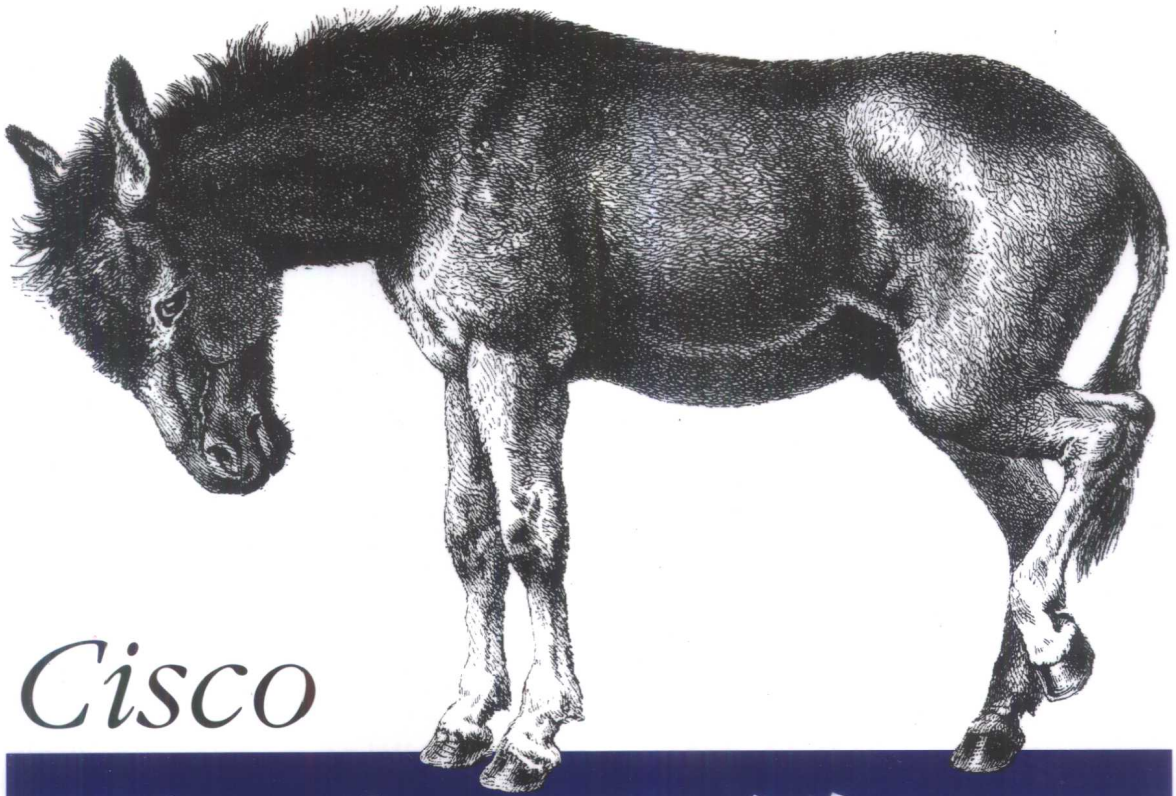
Managing IP Networks with Cisco Routers



Cisco 路由器管理

O'REILLY®
中国电力出版社

Scott M. Ballew 著
夏昊 洪峰 译

Cisco路由器管理

Scott M. Ballew 著

夏昊 洪峰 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

中国电力出版社

图书在版编目（CIP）数据

Cisco路由器管理：/（美）巴留（Ballew, S. M.）著；洪峰译. - 北京：中国电力出版社，2000.1

书名原文：Managing IP Networks with Cisco Routers

ISBN 7-5083-0196-X

Ⅰ.C… Ⅱ.①巴… ②洪… Ⅲ.计算机通信网-路由器管理 Ⅳ.TN913.2

中国版本图书馆CIP数据核字（1999）第66965号

北京市版权局著作权合同登记

图字：01-1999-3162号

书　　名/ Cisco路由器管理
书　　号/ ISBN 7-5083-0196-X
责任编辑/ 刘江
封面设计/ Ellie Volckhausen、Hanna Dyer，张健
出版发行/ 中国电力出版社
地　　址/ 北京三里河路6号（邮政编码100044）
电　　话/ （010）66412306、68352645（总编室）　（010）68316497（发行部）
经　　销/ 全国新华书店
印　　刷/ 北京市地矿印刷厂
开　　本/ 787毫米×1092毫米　16开本　20.75印张　310千字
版　　次/ 2000年1月第一版　2000年1月第一次印刷
印　　数/ 00001-10000册
定　　价/ 40.00元（册）

Cisco 路由器管理

目录

前言

有关Windows或UNIX的系统管理方面有许多好书，进一步而言，关于各种的网络服务如网络文件系统（Network File System，NFS），域名服务（Domain Name Server，DNS）或WWW都有不少值得推荐的好书。即使是计算机网络背后的基础理论，也有许多好书，但就是很难见到一本书“能够教你如何管理IP路由器构成的网络”。这就是我写作本书的动机，希望本书能对你有所帮助。

本书的读者对象

越来越多的网络管理员必须面对路由器带来的问题，甚至需要从头建立一个这样的网络，这些人是本书最主要的读者群。我假设读者已经具备基本的网络概念，当然不一定要是IP理论的高手。

本书的另一类读者对象是系统信息的主管，他们领导着一群打算建立新网络的网络管理员，或者是打算将原来通过桥接式的IP机器改由路由器来连接。这类读者可能对路由器的配置细节不感兴趣，他们需要的是网络与路由器管理方面的基本知识，让他们在选择网络管理员时具有背景知识，以了解技术人员将会作什么。

最后，本书的目的是从更实际的观点来了解IP网络的运行，而不是关于协议的理论性论述，虽然本书的有些主题并不直接和网络管理有关。

本书讲什么？

这本书到底在讲什么呢？在回答这个问题之前，让我先排除这本书不会讲到的东西。第一，本书不会提到IP协议的内部细节，相关主题的好书已经够多了，我对那些作者们也敬畏有加。这也不是一本Cisco路由器的专门技术文件，它不能取代Cisco本身提供的文件。Cisco互联网操作系统（Internetworking Operating System，IOS）的文件厚达上千页，我可不想自欺欺人。我的目的在于补充其原有的文件，而非取而代之。本书也不是一本技巧大全，来专门教你应付一些网络的疑难杂症，其实这类书籍根本不能达到目的，因为每个网络都有各自独特的状况，其配置方式千奇百怪，不可能全都一致。最后，本书告诉你的并非是唯一的方法，也不见得是最好的方法。本书试图给你的是一个坚实的知识背景，让你在设计一个IP网络时能得心应手。

第一章，IP网络的基础。我粗浅地叙述了IP网络的运行原理。我没有长篇大论地深入讨论协议的细节，只是简单地介绍以后章节所涉及的技术背景。谈到的主题包括IP地址的组成和利用方式、子网、超网与掩码；私有地址和公用地址；IP路由的算法；域名与DNS。

在接下来的第二章和第三章中，我讨论与IP网络设计的相关主题。我猜想你大概已经有了现成的网络架构，所以你可以从标题的名称来寻找你感兴趣的主题，直接找出你的网络效率不佳的原因。第二章的内容包括确立你的目标、网络结构、媒体的选择、描述各种拓扑方式的优劣。这一章比较偏向理论。第三章接着上一章谈到的主题包括集线器（Hub）、交换机（Switch）与路由器（Router）的区别；路由器在网络中安装的位置；网络掩码和子网的设定；代理地址解析协议（Proxy Address Resolution Protocol，代理ARP），它的作用和缺点；网络设计上的冗余性（redundancy）和容错（fault tolerence）。最后，我谈到多重协议路由（multi-protocol routing）对网络设计的影响。

第四章，网络设备的选购。我首先告诉你IP路由器是什么东西，然后再谈形形色色的路由器之优缺点。我的重点是让你在选购这些设备前必须有一个评估标准，包括厂家、功能、互操作性以及可靠性等。

第五章，选择路由器的协议。从这里开始，我们离开了与设计相关的主题。协议的选择是每个网络管理员的必备知识。讨论的主题包括静态路由和动态路由、动态路由协议的分类方式、以及各种方式的优缺点。最后列出一些重要的原则，让你在选择协议时有一个可以遵循的标准。

一旦你决定了采用一种协议，那么第六章，“路由协议的配置方式”让你实际深入协议配置的细节。我利用“路由信息协议”（Routing Information Protocol，RIP）、“增强内部网关路由协议”（Enhanced Interior Gateway Routing Protocol，EIGRP）与“开放最短路径优先”（Open Shortest Path First，OSPF）举了几个例子，涵盖了几种常见的情况。虽然我举的例子不是很多，但应付一般的情况却绰绰有余。范例包括静态路由的广播、定义备份静态路由、利用长度可变的子网掩码、压缩与过滤路由信息、多重路径路由，以及同时利用多重动态协议的路由。

第七章，网络管理的非技术层面。这一章开始讨论一些与你的路由器网络管理有关的非技术方面的问题。主题包括怎样考察你的网络、其边界在哪里、管理人员需要具备一些什么样的素质、涉及的成本有哪些，以及怎样预计这些成本、怎样建立技术支持中心。

第八章，网络管理的技术层面。这一章将主题转入讨论一些与你的路由器网络管理有关的技术方面的问题，例如怎样监控你的网络，排除故障的技巧，并考察了几种能完成这些任务的工具。最后，我们探索了几种一开始就能使你避免陷入麻烦的注意事项，例如仔细保留记录，并规划配置的更改。

第九章谈的是与外界连接时，所可能产生的任何以外状况与陷阱，Internet只是外界定义中的一种，也不是本章的重点。当我谈到Internet的时候，重点放在外部路由。我也谈到了如何通过“边界网关协议”（Boarder Gateway Protocol，BGP）进行外部路由的配置。

第十章，网络安全。我们谈到网络在其相连主机的安全性上所扮演的角色。谈到的主题包括安全性定义、关于安全性的需求、通过防火墙与口令所达到的安全目标、以及秘密保护的设计观点。

附录包括路由器界面的配置，取得RFC，取得Internet草案，如何获得IP地址。在讨论界面配置的章节中，我举了几个例子，分别涵盖了以太网、令牌环、光纤分布式数据互联（Fiber Distributed Data Interconnect，FDDI）、串口线路（租用专线与拨号线路）、帧中继与异步传输模式（Asynchronous Transmission Model，ATM）。

本书没有谈到IP多播路由（Multicast Routing）与多播主干网（MBONE），我从本书写作的开始就为是否加入这些主题而摇摆不定，但最后，我觉得这些主题目前还是太虚幻。虽然某些网络已经提供了MBONE的服务，但是Mutilcast Routing显然还处在研究阶段，所以，我们不提也罢。

虽然本书偏重Cisco路由器，范例采用的也是Cisco的IOS指令，但本书绝对不是Cisco产品的广告性文档。别误会我的意思，我自己也使用Cisco产品，而且相当满意，但市场上也同样有许多产品值得你考虑。我以Cisco产品为主是基于实际的理由，因为我需要举出实际的范例，而Cisco无疑是目前业界领导性的厂商，在市场上占有绝对的优势，而我自己又熟悉他们的产品。我尽量不让本书带上偏袒性，所以书中以IOS为范例的技巧同样也能在其他厂家的机器上使用。

欢迎评论

尽管我们尽了自己最大努力检查并确保本书内容的正确性，但缺点和错误仍在所难免，如果您发现了任何错误或需要改进的地方，请告诉我们，以便我们在将来的版本中采纳您的建议。

奥莱理软件（北京）有限公司设立了专门的站点，回答用户提出的关于本书的问题：

cisco1e@mail.oreilly.com.cn

致谢

一本书不可能靠一个人单独完成（如果你不信的话，自己写一本书看看）。我付出了相当大的代价才学到这一点，但我无怨无悔。我享受了写作带来的乐趣，这份享受部分来源于O'Reilly公司朋友们的工作态度。

在一长串的感谢名单中，我首先要提到的是我的技术编辑Mike Loukides，他让我的写作成为一种乐趣。每当我拖稿的时候，他从不会恶言相向，反而都是在我快丧失信心的时候，给我一点提示，让我继续前进。他时常提出一些关键性的问题，例如，某些主题是否放进来很适合、这些问题看上去很单纯、但是当局者迷，反而让我有时举棋不定。

我要感谢Dave Curry，他一开始介绍Mike当我的技术编辑。我从没有自己写一本书的念头，当Mike问Dave谁能够写一本类似主题的书的时候，Dave就给他我的名字，我得感谢Dave促成此事。

Cisco公司的Alex Bochannek给了我许多技术上的指导，修正了一些关于Cisco IOS技术说明上的错误。Eric Pearce指出了我的初稿中需要补充的地方。Karl Friesen提供我关于校园网络与ISP的实际经验。普渡大学（Purdue University）的Larry Billado在本书的可读性与完整性方面提供了意见。

我必须感谢我的教授Douglas Comer，让我有机会管理他的实验室网络。配合他在课堂上教授的理论，我之后真正迷上了网络。我必须感谢Gary的耐心校稿、忍受了我不断的修改。最后，我必须向我可爱的狗Rascal说声抱歉，过去两年为了这本书，我真的没时间陪过它。

原书空白页

本章内容

- 地址与网络
- 私有地址与公开地址
- IP路由算法
- 域名与域名系统

第一章

IP网络技术的基础

近年来，随着Internet的飞速发展和日益普及，IP网络技术获得了前所未有的成功。然而，训练有素且能足以管理这些网络的网管技术人员却供不应求。情况往往是这样，早已疲于应付现有工作的计算机技术支持人员被任命为IP网络管理员，除了管理主机、服务器的责任外，再加上了路由器、交换机和其他构成网络基础架构的各类设备。很多人对此准备不足。

本书试图填补IP网络技术流行形势下不少计算机专业人士知识上新形成的空白点。作者希望本书能对有效地管理IP路由器、组建稳定可靠的网络过程中所牵涉的任务、问题和工具作出有用的介绍。

因为目前网络管理员的技术背景各不相同，有时您可能会觉得本书内容过于浅显，不言自明。这是一件好事，说明您的技术背景已经比较完善。然而作者希望您还是花时间阅读那些一眼看上去觉得是老生常谈的章节，而不要略过。您可能从中发现其中有新的观点帮助您理解以前不甚明了、不明所以然的东西，甚至以前所忽略掉的全新信息。

譬如本章探讨了一些IP网络技术的基本概念，包括地址分配，子网、超网与网络掩码，IP路由算法，使用域名系统（Domain Name System，DNS）实现域名和地址之间的映射。这不是一本试图提供对IP网络技术面面俱到的参考书籍，也不适用于完全不熟悉IP网络的读者。本章的作用在于保证我们在下文的探讨中有基

本的共识。如果跳过本章，您也许会发觉以后的章节用到本章提供的信息。如果您需要更详尽地了解IP协议组工作的内部机制，请阅读由Douglas Comer著，Prentice Hall公司出版的《Internet Networking with TCP/IP, Vol 1》。如果您需要对IP网络技术建立一个坚实的基础，则请阅读由Craig Hunter所著，O'Reilly公司出版的《TCP/IP网络管理》。

在保证大家具备一定的共识之后，下面几章将探讨如何设计网络（事实上这往往意味着纠正您现有网络中所存在的设计问题）：选择路由器的注意事项；如何选择动态路由协议以及如何配置动态路由协议。其后的几章涵盖的主题包括维护、运行您的网络；与其他的网络包括Internet互联；最后还有如何增强您网络的安全并协助网上主机抵挡来自网络的威胁。

本书中贯穿了许多与Cisco互联网操作系统（Internet Operation System, IOS）直接相关的范例、技术和技巧，但这并不说明本书提供的信息对其他厂商的设备无效。绝大多数的范例和技术都适用于所有的路由器，只要它们支持必要的协议。有些技巧虽然可能无法直接用于您的路由器，但它们也应能对您有所启发。

地址与网络

无论在任何网络中，所有节点都必须拥有一个唯一的标识符，以便其他机器向它传送信息。这个标识符通常称作“地址”。在有些网络技术中，地址标识一台特定机器；而在IP网络中，地址标识着一个网络接入点，更普及的说法是“网络界面”。由此一台拥有多个网络界面的机器可以有多个IP地址——每个网络界面分别对应一个IP地址。网络界面通常是独立的物理连接（例如，一个您用以插入网线的实际上的插座），但它们也可以是共享同一个下层物理连接的逻辑接口。您在ATM网络接入中可以看到上述第二种情况。正式的说法是“界面复用”（interface multiplexing）。将ATM网络上的主机逻辑上划分为多个群组，可使您把每个组作为一个物理网络来区别对待，尽管所有的主机事实上都是连接到同一物理网络。连接到这个网络的任何设备，只要建立相应的逻辑连接，就可加入几个这样的逻辑网络，每个逻辑网络对应一个IP地址。

拥有多个地址的主机称作“多穴主机”（multi-homed machines）。所有的路由器都是多穴的；按照定义，它们实现在多个网络中的路由、为分组包提供路由。然而，并非所有的多穴主机都是路由器。一台机器具有多个网络连接，但不为任一个网络提供IP路由服务，这种情况完全有可能也不罕见。例如，一台被多个网络共享的文件服务器。

IP 地址的结构

IP地址的长度是32比特。我们把这地址视为四个字节的序列，或者使用网络工程师的说法，称之为四个 octets。在书写 IP 地址时，您把每个字节转换为十进制，并用实心圆点将四个字节连起来。这样，32 比特的 IP 地址：

```
10101100 00011101 00100000 01000010
```

应被写作：

```
172.29.32.66
```

这种格式，称作“点分四元组”（dotted quad）格式，就容易为人所接受；在本书余下的讨论中我们就将使用这种格式。但在某些情况下，使用对32比特的十六进制表示会使某些运算更易实现或更显而易见。若用十六进制表示，上述地址就写为：

```
0xac1d2042
```

尽管所有IP地址都是32比特，但一切IP地址的集合却并不属于统一的空间。与其相反，IP地址分作两部分，分别标识网络和该网络中的主机，构成一个两层的层次系统。在IP协议中网络号标识一组在ISO/OSI网络参考模型第二层能够直接相互通信的主机。该层称为数据链路层。包括以太网、令牌环、FDDI以及点对点连线。无论是只有一根物理电缆线，还是由重复器，网桥，交换机所连接起来的多个网段，IP把它们都看作同一网络。

自然地，主机号就定义了属于该网络的一台特定机器。图 1-1 显示了这样一个范例。

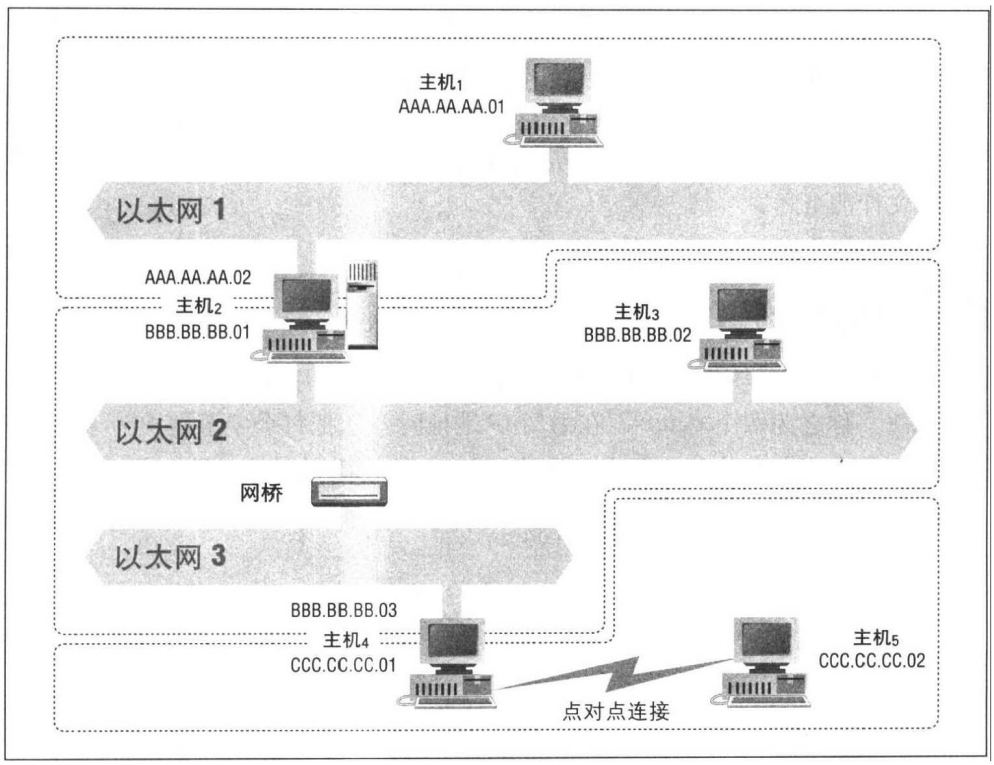


图 1-1 以太网 2 和 3 是同一个网络

在图 1-1 中，尽管以太网 2 和 3 由网桥分隔开，它们构成一个共同的 IP 网络，因为网桥对 IP 这样的网络层协议是透明的，主机 2，主机 3 和主机 4 都包含这个桥接网络中的 IP 地址。主机 4 和主机 5 之间的串行链路构成又一个 IP 网络，主机 4 和主机 5 也就包含这个串行网络中的 IP 地址。最后，以太网 1 是第三个 IP 网络，并且包括主机 1 和主机 2。由此，主机 2 和主机 4 各有两个 IP 地址；它们是多穴主机，可能是路由器。IP 地址的两层结构在以后有关路由的讨论中非常重要。而在此，我们只需能够区分 IP 地址中哪一部分是网络号，哪一部分是主机号。

网络号作为 IP 地址的一部分，有一个重要的后果：一个主机的 IP 地址取决于它所连接的网络。这意味着，任何主机移至新的网络时都必须更换地址。

其他网络技术，如 Novell IPX 基于网卡硬件地址，或 Apple 的 AppleTalk 自动选择地址，而 IP 地址本质上是手工分配设定的。当然，存在启动协议（BOOTP）