Cisco专业技术丛书

HZ BOOKS

Cisco

访问表配置指南

Cisco Access Lists Field Guide

(美) Gil Held　Kent Hundley(CCNA)　著

前导工作室　译

机械工业出版社
China Machine Press

McGraw-Hill

Cisco

访问控制列表配置指南

Cisco Access Lists Field Guide

Cisco专业技术丛书

Cisco访问表配置指南

(美) Gil Held
Kent Hundley (CCNA) 著
前导工作室 译

机械工业出版社
China Machine Press

本书详细讲解了配置Cisco路由器访问表的方法，内容包括网络基础知识、访问控制的基础知识、Cisco路由器的软硬件知识以及Cisco路由器的一般配置方法。重点介绍了Cisco的访问控制表，包括动态访问表、自反访问控制表、基于时间的访问表以及基于上下文的访问控制等，并对其他一些安全知识进行了阐述。

本书叙述清晰，实用性强，是网络管理员和对Cisco安全策略感兴趣的读者不可多得的一本好书。

本书版权登记号：图字：01-2000-1732

图书在版编目(CIP)数据

Cisco访问表配置指南/ (美)海尔德(Held,G.)，(美）亨得利(Hundley, K)著；前导工作室译. －北京：机械工业出版社，2000.9

（Cisco专业技术丛书）

书名原文：Cisco Access Lists Field Guide

ISBN 7-111-08214-1

Ⅰ.C… Ⅱ.①海… ②亨… ③前… Ⅲ.通信网－路由选择－指南 Ⅳ.TN915.05-62

中国版本图书馆CIP数据核字(2000)第43594号

机械工业出版社 (北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑：郭东青

北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行

2000年9月第1版第1次印刷

787mm × 1092mm 1/16 · 11.5印张

印数：0 001-7 000册

定价：25.00元

译 者 序

近几年来，网络的发展非常快。网络底层的带宽正在快速增加。与此同时，网络软环境（网络管理和网络安全）的发展却相对落后于带宽的发展，就如同计算机软件的发展落后于硬件的发展一样。

政府上网工程以来，国内对网络安全的呼声越来越高。译者认为，对于进行网络安全方面工作的工程人员和研究人员而言，首先要了解现有网络设备的安全情况，才能够对网络的漏洞进行补救。译者很幸运地参加了网络安全方面的一些研究工作，近两年的时间里，也花费了很多时间研究Cisco和3COM网络设备的安全结构，对网络安全有一定的认识和见解。对于用户（网络管理员）而言，熟练掌握所使用设备的安全特征是必要的，只有这样才能较好地保护自己所在单位的网络安全。

目前，我国使用得最多的路由器是Cisco公司生产的，大量的随机文档虽然对管理员有一定的帮助，但阅读英文毕竟是一件让人心烦的事情，我们希望本书能满足用户对网络安全的需要。

本书全面地介绍了Cisco在访问表方面的思想，以及这些思想在Cisco设备中的应用。作者首先简单明了地说明了对Cisco路由器的操作和使用，然后对各种访问表进行了分别介绍，并介绍了一些非访问表的安全控制方法。书中还包含了大量现实生活中的示例，以便读者可以参照进行设备配置。书中还提到了一些可以用来增强网络安全的要点和技术。

本书由前导工作室的胡平、李化组织翻译，前导工作室的全体人员共同完成了本书的录入、校对等工作。本书的出版是集体智慧的结晶。

译者在翻译的过程中，对原书存在的一些明显错误进行了修改，以便进行正确的翻译。

如果书中仍然存在疏忽与错误之处，恳请读者批评指正。

译　者

2000年6月

前　言

本书集中阐述Cisco IP访问表，主要讲述访问表的操作和使用，并提供100多个示例，以便读者能够参考本书以满足自己特殊操作的需要。

访问表是网络防御外来攻击的第一关。另外，访问表还是一种控制信息流通过路由器接口的机制。这样，读者可以使用访问表设计网络操作和控制网络数据流。反过来，通过使用路由器的访问表，读者也可以建立特定的网络规划策略。

本书是Cisco专业技术丛书中的一本，本系列丛书沿用先介绍相关知识，而后给出应用的具体实例的方法。我们将回顾一下不同类型的访问表，进而介绍其格式、关键字的使用、创建方法以及如何应用到接口上。另外，每章集中讨论一种特定的访问表，并给出大量的标准应用实例。这种组织形式先概述网络应用或需求，而后借助于访问表、网络方案图解以及必要的Cisco Internet online service（IOS）语句来实现网络应用或需求，最后提供IOS语句的应用实例。作者力图给读者提供一些现实生活中的实例，以便使读者能够轻松地对其进行改造以满足特定的需求。

作为职业作家，我们很期望读者能够给出反馈意见。如果读者愿意与我们分享自己对本书中所涉及领域的见解，或者在本书未来版本中希望了解哪些专题，或者希望作者在某个更专业的领域中介绍有关Cisco的其他专题，那么读者可以通过出版社与我们联系，或者通过电子邮件直接与我们联系。

Gilbert Held
Macon, Georgia
gil_held@yahoo.com

Kent Hundley
Stanford, Kentucky
kent.hundley@prodigy.net

目　录

译者序
前言
第1章　引言 ……1
1.1 Cisco专业参考指南 ……1
1.2 路由器的任务 ……1
1.3 全书预览 ……2
1.3.1 路由器的软硬件 ……2
1.3.2 Cisco访问表基础 ……2
1.3.3 动态访问表 ……2
1.3.4 基于时间的访问表 ……3
1.3.5 自反访问表 ……3
1.3.6 基于上下文的访问控制 ……3
1.3.7 TCP拦截和网络地址转换 ……3
1.3.8 IPSec ……3
1.3.9 流量整形 ……4
第2章　路由器软硬件概述 ……5
2.1 硬部件 ……5
2.1.1 中央处理单元 ……5
2.1.2 闪存 ……6
2.1.3 只读存储器 ……6
2.1.4 随机存取存储器 ……6
2.1.5 非易失的RAM ……6
2.1.6 输入/输出端口和特定介质转换器 ……6
2.1.7 路由器的初始化过程 ……8
2.2 基本的软部件 ……10
2.2.1 操作系统映像 ……10
2.2.2 配置文件 ……11
2.2.3 数据流 ……11
2.3 路由器配置过程 ……12
2.3.1 线缆的考虑 ……12
2.3.2 控制台访问 ……12
2.3.3 设置考虑 ……14
2.3.4 命令解释器 ……16
2.3.5 用户模式的操作 ……16
2.3.6 特权模式的操作 ……17
2.3.7 配置命令的种类 ……19
2.4 安全管理的考虑 ……22
2.4.1 口令管理 ……22
2.4.2 访问表 ……23
第3章　Cisco访问表基础 ……24
3.1 概述 ……24
3.1.1 目的 ……24
3.1.2 应用 ……24
3.2 访问表类型 ……25
3.2.1 标准IP访问表 ……25
3.2.2 扩展的IP访问表 ……28
3.3 IP访问表的表项注解 ……30
3.4 创建和使用访问表 ……31
3.4.1 指定接口 ……31
3.4.2 使用IP访问组命令 ……31
3.5 命名的访问表 ……32
3.5.1 概述 ……32
3.5.2 标准的命名IP访问表 ……32
3.5.3 标准的命名IP访问表应用 ……32
3.5.4 扩展的命名IP访问表 ……33
3.5.5 扩展的命名IP访问表应用 ……33
3.5.6 编辑 ……34
3.5.7 编辑处理过程 ……35
3.6 需要考虑的规则 ……36
3.6.1 自上而下的处理过程 ……36
3.6.2 添加表项 ……36
3.6.3 标准的访问表过滤 ……36
3.6.4 访问表位置 ……36
3.6.5 语句的位置 ……37
3.6.6 访问表应用 ……37
3.6.7 过滤方向 ……37
3.6.8 路由器产生的报文 ……37

第4章 动态访问表 ……38
4.1 概述 ……38
4.2 使用指南 ……40
4.3 动态访问表应用：示例1 ……41
4.3.1 概述 ……41
4.3.2 解决方案 ……42
4.3.3 分析 ……42
4.4 动态访问表应用：示例2 ……43
4.4.1 概述 ……43
4.4.2 解决方案 ……44
4.4.3 分析 ……44
4.5 动态访问表应用：示例3 ……45
4.5.1 概述 ……45
4.5.2 解决方案 ……45
4.5.3 分析 ……46
4.6 动态访问表应用：示例4 ……46
4.6.1 概述 ……46
4.6.2 解决方案 ……46
4.6.3 分析 ……47
第5章 基于时间的访问表 ……48
5.1 理论基础 ……48
5.2 概述 ……48
5.2.1 定义时间范围 ……48
5.2.2 time-range命令 ……49
5.2.3 absolute语句 ……49
5.2.4 规则 ……49
5.2.5 periodic语句 ……50
5.2.6 示例 ……50
5.3 注意事项 ……51
5.4 时间范围应用：示例1 ……51
5.4.1 概述 ……51
5.4.2 解决方案 ……52
5.4.3 分析 ……52
5.5 时间范围应用：示例2 ……52
5.5.1 概述 ……52
5.5.2 解决方案 ……53
5.5.3 分析 ……53
5.6 时间范围应用：示例3 ……54
5.6.1 概述 ……54
5.6.2 解决方案 ……55
5.6.3 分析 ……55
5.7 时间范围应用：示例4 ……55
5.7.1 概述 ……55
5.7.2 解决方案 ……56
5.7.3 分析 ……57
第6章 自反访问表 ……58
6.1 概述 ……58
6.2 操作 ……58
6.2.1 术语来源 ……58
6.2.2 特征 ……59
6.2.3 数据流 ……59
6.3 创建访问表 ……60
6.3.1 permit语句 ……60
6.3.2 evaluate语句 ……61
6.3.3 ip reflexive-list timeout命令 ……61
6.3.4 接口选择过程 ……61
6.3.5 观察自反访问表的操作 ……63
6.4 局限性 ……63
6.4.1 语句位置 ……63
6.4.2 应用支持 ……64
6.5 自反访问表应用：示例1 ……64
6.5.1 概述 ……64
6.5.2 解决方案 ……64
6.5.3 分析 ……65
6.6 自反访问表应用：示例2 ……66
6.6.1 概述 ……66
6.6.2 解决方案 ……66
6.6.3 分析 ……67
6.7 自反访问表应用：示例3 ……67
6.7.1 概述 ……67
6.7.2 解决方案 ……68
6.7.3 分析 ……68
6.8 自反访问表应用：示例4 ……68
6.8.1 概述 ……68
6.8.2 解决方案 ……69
6.8.3 分析 ……69
6.9 自反访问表应用：示例5 ……69
6.9.1 概述 ……69

6.9.2 解决方案 ……70
6.9.3 分析 ……70
第7章 基于上下文的访问控制……71
7.1 概述 ……71
7.2 特征 ……72
7.3 操作 ……72
7.4 配置 ……73
7.4.1 第1步——选择接口 ……74
7.4.2 第2步——配置访问表 ……74
7.4.3 第3步——定义超时和门槛值 ……75
7.4.4 第4步——定义检测规则 ……75
7.4.5 第5步——应用检测规则 ……76
7.4.6 其他命令 ……76
7.5 日志 ……78
7.6 CBAC示例 ……79
7.6.1 CBAC应用：示例1 ……79
7.6.2 解决方案 ……80
7.6.3 分析 ……81
7.6.4 CBAC应用：示例2 ……83
7.6.5 解决方案 ……83
7.6.6 分析 ……84
7.6.7 CBAC应用：示例3 ……86
7.6.8 解决方案 ……86
7.6.9 分析 ……87
7.6.10 CBAC应用：示例4……87
7.6.11 解决方案……88
7.6.12 分析……89
第8章 TCP拦截和网络地址转换……91
8.1 TCP拦截概述 ……91
8.1.1 开启TCP拦截 ……92
8.1.2 设置模式 ……93
8.1.3 主动门槛值 ……93
8.1.4 其他命令 ……93
8.2 TCP拦截应用：示例1 ……94
8.2.1 解决方案 ……94
8.2.2 分析 ……94
8.3 TCP拦截应用：示例2 ……95
8.3.1 解决方案 ……95
8.3.2 分析 ……95
8.4 网络地址转换概述 ……95
8.4.1 特征 ……96
8.4.2 局限性 ……96
8.5 NAT的术语 ……97
8.6 启用NAT ……97
8.7 其他命令 ……99
8.8 NAT应用：示例1 ……100
8.8.1 解决方案……101
8.8.2 分析……101
8.9 NAT应用：示例2 ……102
8.9.1 解决方案1 ……102
8.9.2 解决方案2 ……102
8.9.3 分析……103
8.10 NAT应用：示例3……104
8.10.1 解决方案 ……104
8.10.2 分析 ……105
8.11 NAT应用：示例4……105
8.11.1 解决方案 ……106
8.11.2 分析 ……107
8.12 NAT应用：示例5……107
8.12.1 解决方案 ……108
8.12.2 分析 ……108
8.13 NAT应用：示例6……109
8.13.1 解决方案 ……109
8.13.2 分析 ……110
第9章 Cisco加密技术与IPSec……111
9.1 概述……111
9.2 基本的密码学……111
9.2.1 理论上的加密 ……111
9.2.2 实际中的加密 ……112
9.2.3 加密范例 ……112
9.2.4 优秀密钥的重要性 ……113
9.3 加密学定义……114
9.3.1 基础知识 ……114
9.3.2 对称密钥加密 ……114
9.3.3 非对称密钥加密 ……115
9.3.4 Hash函数 ……116
9.3.5 数字签名 ……116
9.3.6 授权认证 ……117

9.3.7 数据加密标准 ……117
9.3.8 数字签名标准 ……117
9.3.9 互连网安全联盟及密钥管理协议 ……117
9.3.10 互连网密钥交换 ……118
9.3.11 RSA算法 ……118
9.3.12 Diffie-Hellman ……118
9.3.13 MD5 ……118
9.3.14 SHA ……118
9.4 CET概述 ……118
9.4.1 定义 ……118
9.4.2 实现 ……119
9.5 IPSec概述 ……121
9.5.1 IPSec的目标 ……121
9.5.2 IPSec基本特征 ……122
9.5.3 IPSec实现 ……125
9.6 加密应用：示例1 ……128
9.6.1 解决方案 ……128
9.6.2 分析 ……129
9.7 加密应用：示例2 ……129
9.7.1 解决方案 ……129
9.7.2 分析 ……130
9.8 加密应用：示例3 ……131
9.8.1 解决方案 ……132
9.8.2 分析 ……133
9.9 加密应用：示例4 ……133
9.9.1 解决方案 ……134
9.9.2 分析 ……135
第10章 流量整形与排队 ……136
10.1 排队技术 ……136
10.2 排队方法 ……136
10.3 排队应用：示例1 ……141
10.3.1 解决方案 ……141
10.3.2 分析 ……142
10.4 排队应用：示例2 ……142
10.4.1 解决方案 ……142
10.4.2 分析 ……142
10.5 流量修正 ……143
10.6 CAR应用示例 ……144
10.6.1 解决方案 ……144
10.6.2 分析 ……144
10.7 流量整形 ……145
10.7.1 配置GTS ……145
10.7.2 配置FRTS ……146
10.8 流量整形应用：示例1 ……147
10.8.1 解决方案 ……148
10.8.2 分析 ……148
10.9 流量整形应用：示例2 ……148
10.9.1 解决方案 ……148
10.9.2 分析 ……149
附录A 决定通配符屏蔽码的范围 ……150
附录B 建立访问表 ……158
附录C 标准的访问表 ……160
附录D 扩展的访问表 ……161
附录E 术语 ……162
附录F 缩写词 ……170

第1章 引 言

我们在序言中讲过，路由器的访问表是网络防御的前沿阵地。我们还讲过，访问表提供了一种机制，可以控制通过路由器的不同接口的信息流。这种机制允许用户使用访问表来管理信息流，以制定公司内网络相关策略。这些策略可以描述安全功能，并且反映流量的优先级别。例如，某个组织可能希望允许或拒绝Internet对内部Web服务器的访问，或者允许内部局域网（Local Area Network，LAN）上一个或多个工作站能够将流量发到广域网（Wide Area Network，WAN）的ATM骨干网络上。这些情形，以及其他的一些功能，都可以通过访问表来达到目的。

本章的目标是让读者了解全书的内容。首先，向读者介绍Cisco专业领域的一些概念，先简要描述路由器的功能，以及Cisco访问表的一些基本知识。然后，对全书提供一个概括性的描述，主要是讲述后续章节中将介绍的知识内容。

1.1 Cisco专业参考指南

Cisco专业参考指南系列提供了操作Cisco设备的一些信息和一系列的实践实例，读者可以使用这些知识来满足自己单位的特别需要。参考指南系列的第一本书集中阐述访问表，并提供了各种类型的访问表的使用方法、访问表的创建和格式，以及应用到接口和进行操作的详细信息。我们为各种截然不同的访问表类型提供了一系列的实例，在实例中，先给出一个通用的格式，包括应用场景或问题的一个概括性描述，用来说明路由器LAN或WAN接口的网络示意图。然后，再讲述访问表的IOS语句，这些IOS语句可以用来解决应用或问题。每一个访问表实例都包括用来实现的访问表的基本原理。

1.2 路由器的任务

从操作的观点上看来，路由器的作用是将报文（Packet）从一个网络传输到另外一个网络。路由器工作于网络层，根据开放式系统互连（Open Systems Interconnection，OSI）参考模型，它实现的是第三层的功能。通过检测报文的网络地址，路由器可以用来决定报文流的去向，并且创建和维护路由表。在过去的20年中，人们开发了50多种路由协议，而路由信息协议（Routing Information Protocol，RIP）、开放式最短路径优先（Open Shortest Path First，OSPF）、边界网关协议（Border Gateway Protocol）只是这50多种协议中的3种。从安全的角度上看来，路由器是保护网络的“前沿阵地”。这种保护措施是通过创建访问表来允许或拒绝报文通过路由器的接口来实现的。

Cisco公司的路由器支持两种类型的访问表：基本访问表和扩展访问表。基本访问表控制基于网络地址的信息流。扩展访问表通过网络地址和传输中的数据类型进行信息流控制。尽管访问表可以认为是保护网络的第一关，当前实现的路由器并不实际检验报文中的信息域，也不维护关于连接状态的信息。换句话说，每一个报文被分别检验，路由器并不判断某个报文是否为一个合法对话流中的一部分。

在过去的两年中，Cisco系统公司对访问表的能力进行了一些重要的功能增强，包括根据某天的某个时间、某星期的某一天对向内或向外的流量进行检测的新功能，在标准和扩展访问表中插入动态表项的能力，以及防止黑客攻击Web服务器和其他网络设备的能力。

我们将讲述Cisco访问表的类型和特征，包括基于上下文的访问控制表（Context-Based Access Control list，CBAC）和自反访问控制表（reflexive ACL）。CBAC是Cisco防火墙特征集（Firewall Feature Set，FFS）的核心。FFS是某些Cisco路由器模型中特定代码的修订版本。从IOS 12.0T开始，CBAC出现在800、1600、1720、3600和7200系列路由器中。其特征是能够维护一个已有连接的状态信息，对有限的TCP和UDP协议进行应用层信息检验，它比传统的访问表增加了更高的安全性。自反访问控制表是Cisco IOS 11.3开始出现的新特征。Reflexive ACL维护一定程度的“伪状态（pseudostate）”信息，一旦合法的对话建立起来，它就在传统ACL中创建动态的表项。以后的报文与自反ACL中的动态表项进行比较评估，以确定这些报文是否为已存在连接的一部分。会话结束后，ACL中的动态表项被删除。但是，反访问控制表不能理解高层协议，并且不适宜于与文件传输协议（File Transfer Protocol，FTP）等多通道协议一起使用。CBAC和自反访问控制表将在本书稍后章节中进行详细阐述。

1.3 全书预览

本节将对全书的后续章节做一个概括性的描述。作者建议那些对IOS的基础知识和如何使用访问表不太熟悉的读者，应该按照本书的顺序首先阅读前面一些章节。最后五章采用的是模块化结构，每一章集中阐述一种类型的访问表，所以，如果读者对开始的章节比较熟悉的话，就可以根据自己的需要阅读后面五章中的信息和特定类型的访问表实例。

1.3.1 路由器的软硬件

编写和应用访问表需要读者对Cisco路由器的软硬件有基本的认识。了解路由器的硬件便于读者了解路由器如何工作，以及如何配置路由器。第2章将简单介绍Cisco路由器的基本软硬件，包括如何通过EXEC操作模式配置一台路由器。

1.3.2 Cisco访问表基础

读者理解了路由器的基本软硬件之后，将讨论Cisco访问表的基础知识。第3章定义和阐述了各种类型的访问表及其格式，以及阐述了在各种类型的访问表格式中如何使用关键字，并且介绍了在一系列的实例和ISO语句中，如何通过标准访问表和扩展访问表达到预期的功能。

1.3.3 动态访问表

第4章讨论路由器的高级报文过滤技术，并且讨论如何使用动态访问表，动态访问表通常又称为lock-and-key安全。使用动态访问表允许用户在路由器中编写IOS语句，从而将动态表项插入到标准访问表或扩展访问表中。在用户认证过程中，动态访问表将会被开启。相比而言，普通的访问表关于报文过滤能力是固定的，而lock-and-key安全特性比普通访问表更具有灵活性。

1.3.4 基于时间的访问表

传统的访问表存在一个缺陷，一旦访问表应用到某个接口，如果不删除，它们就一直保持有效。这样，如果希望根据某一天的不同时间、某一星期的不同天来实现不同的规则和策略，用户就必须删除当前的访问表，然后使用新的访问表。路由器管理员可能不大愿意老是做这样的事情，尤其是要在星期五的下午五点使用一种新的过滤机制的时候。Cisco系统公司现在解决了这个问题，在IOS中增加了基于时间的访问表，所以现在，安全策略和其他报文过滤可以基于一天中的某个时间段和/或一星期中的某天产生作用。第5章讲述基于时间的访问表的操作，并包含了一些能够满足某些单位特殊需要的访问表实例。

1.3.5 自反访问表

自反访问表是动态访问表更加灵活的一个版本。我们将讲述如何让访问表根据需要进行动态的开启，自反访问表适应于单通道的应用程序。其他章中也包含了一系列的访问表配置实例，读者可以直接引用这些实例，或者进行一些简单的修改以满足特殊的操作需要。

1.3.6 基于上下文的访问控制

尽管基于上下文的访问表是对传统访问表的一种功能增强，但是它只能支持单通道应用程序。也就是说，读者不能使用自反访问表来支持FTP等多通道应用程序。

第7章将学习基于上下文的访问控制，这种技术类似于自反访问表，但是它能够支持多通道应用程序和Java模块，并且能够提供实时警告和审核跟踪功能。在讲述CBAC的过程中，将讲述一系列用来管理报文过滤的超时命令。

1.3.7 TCP拦截和网络地址转换

第8章讨论两种相对较新的路由器功能，一种功能用来访问一种比较普遍的黑客攻击（称为SYN泛洪），另一种则用于基于安全的需要，或者某个组织需要更多的有效地址而必须让路由器进行地址转换的情形。首先将讨论TCP的三阶段握手过程，在Web服务器负载过重时，这个过程对Web功能能够产生一定的影响，Web服务器可能会拒绝合法的服务请求。在理解了SYN泛洪如何吞食计算机的资源之后，将阐述TCP拦截的任务，包括其拦截过程和监视模式、配置每一种模式的步骤，以及让该特征得以体现的IOS语句。第8章其他部分讨论网络地址转换（Network Address Translation，NAT），包括将组织的内部IP地址转换成可以在Internet上进行路由的IP地址等内容。

1.3.8 IPSec

第9章讨论的是那些希望实现基于路由器的虚拟专用网络（Virtual Private Network，VPN）的人所感兴趣的内容。IP安全（IP Security，IPSec）是在任何（而不管其物理拓扑结构如何）基于IP的网络中创建加密通道的技术集合。IPSec可以让用户在运行Windows 95/98、NT或者甚至Linux的工作站中建立加密通道。在Cisco路由器上建立IPSec通道可以在路由器之间建立通信关系。

1.3.9 流量整形

最后一章讲述Cisco路由器处理报文流的不同方法，包括扼杀通过某些接口的流量，或者基于流量的类型选择性地丢弃一些报文的能力。这些技术统称为流量整形（Traffic Shapping），而它们是第10章要讲述的内容。

第2章　路由器软硬件概述

本章提供对Cisco路由器软硬件的一个概括性描述。首先将集中阐述Cisco路由器的硬部件，然后讨论路由器的软件模型。再后，我们将转向路由器的操作模式，并介绍不同路由器功能的使用。

希望通过阅读本章，读者可以了解Cisco路由器的一般操作方式，以及如何对其进行配置。本章包含大量EXEC命令的使用示例，为熟悉Cisco产品的读者提供了一个温习的机会。对于缺少Cisco使用经验的读者，则能提供一些与路由器配置相关的必要信息。本章中还包含一些专用的指导性知识和提示，这些指导性知识都是建立在作者几年以来配置和使用Cisco路由器的经验之上的。这些提示和指导性知识将节约读者很多时间，并使得路由器的配置过程变得有意思起来。

2.1　硬部件

Cisco系统公司生产了大量的、各种类型的路由器产品。尽管这些产品在处理能力和所支持的接口数上有所不同，但它们都使用一些核心的硬件部件。图2-1展示了Cisco路由器的关键部件，其CPU（或微处理器）的类型、ROM与RAM的大小，以及I/O端口的数目和介质转换器根据产品的不同各有相应的变化，但每一个路由器都有图中所示的各个硬部件。通过分析各硬部件的功能，我们就能了解路由器整体上的工作方式及其所提供的功能。

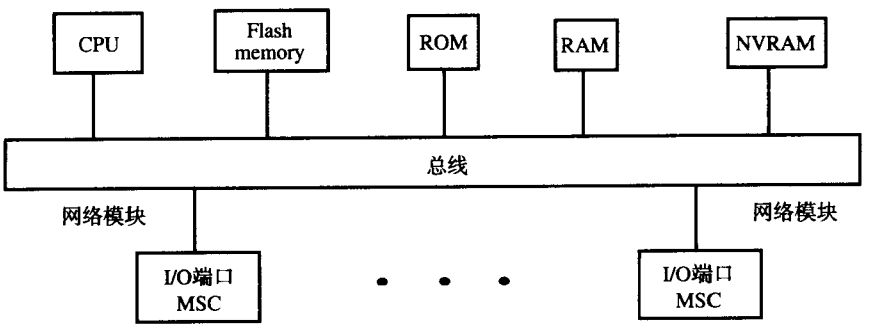

图2-1　Cisco系统公司生产的路由器的关键部件，CPU=中央处理单元；MSC=特定介质转换器；NVRAM=非易失的RAM；RAM=随机存取存储器；ROM=只读存取存储器

2.1.1　中央处理单元

中央处理单元（Central Processing Unit，CPU），或者称为微处理器，负责执行组成路由器操作系统（OS）的指令，以及执行通过控制台（Console）和Telnet连接输入的用户命令。因此，CPU的处理能力与路由器的处理能力直接相关。

2.1.2 闪存

闪存（Flash Memory）是一种可擦写的、可编程类型的ROM。在许多路由器上，Flash Memory作为一种选择性的硬部件，负责保存OS的映像（image）和路由器的微码（microcode）。因为修改Flash Memory无需更换和移动芯片，在要定期修改存储内容的情况下，其代价低，且使用方便。用户可以在Flash Memory中存储多个OS的映像，只要空间允许。这项功能对于测试新的映像十分有用。路由器的Flash Memory还能通过使用普通文件传输协议（trival file transfer protocol，TFTP）将OS的映像加载到另一个路由器上。

2.1.3 只读存储器

ROM中所包含的代码执行加电检测，这一点与许多PC所执行的加电自检（Power On Self-Test，POST）是相同的。ROM中的启动程序还负责加载OS软件。尽管许多路由器需要软件升级时，只能通过更换路由器系统板上的ROM芯片才能做到，但另一些路由器可能使用不同类型的存储方式来保存OS。

2.1.4 随机存取存储器

随机存取存储器（Random Access Memory，RAM）用来保存路由表，进行报文缓存等，在许多流量流向一个通用接口时，报文可能不能直接输出到接口，此时RAM可以提供报文排队所需的空间。在设备操作期间，RAM还能提供保存路由器配置文件所需的存储空间。当RAM为缓存ARP信息而提供空间时，它能减少ARP的流量，并增强多个LAN连接到路由器时的传输能力。路由器关电时，RAM中的内容被清除。

2.1.5 非易失的RAM

非易失的RAM（Nonvolatile RAM，NVRAM）在路由器关电时，仍能保持其内容。通过在NVRAM中保存配置文件的一个拷贝，路由器在电源故障时可以快速地恢复。使用NVRAM后，路由器就不再需要硬盘或软盘来保存其配置文件了。因此，在Cisco路由器中没有移动部件，从而增强了各部件的使用寿命。计算机系统的许多故障都是因为对移动部件的拆装，如硬盘故障等引起的。

因为路由器没有了硬盘和软盘，所以通常的方法是将配置文件存储在一台PC上，这样，用户可以使用文本编辑器方便地进行修改。配置文件可以通过网络使用tftp直接加载到NVRAM中。

当通过路由器来加载配置时，路由器相当于一个客户机，而文件所在的PC相当于一台服务器。这意味着用户要在PC上安装tftp服务器软件操作PC，以便将文件在计算机上进行移入或移出。本章稍后，将讨论tftp服务器软件。

2.1.6 输入/输出端口和特定介质转换器

输入/输出（Input/Output，I/O）端口是报文进出路由器的连接装置。每一个I/O端口都连到一个特定介质转换器（Media-Specific Converter, MSC）上，MSC提供物理接口到特定类型介质，如以太网、令牌环网、RS-232连接或V.35 WAN接口等。

在Cisco中，访问表要应用到某个接口上。而接口要产生作用的话，就需要通过interface命令进行I/O端口配置。因为单个路由器内部或者不同路由器之间的I/O端口各不相同，所以理解如何引用端口是十分重要的。

如果在路由器上加入了一个端口，则可以通过其编号进行直接引用。例如，串行端口1可以通过下面的接口命令进行引用：

```
interface serial0
```

插入到路由器槽中的适配卡通常拥有一组端口，因此引用端口需要使用槽号和端口号。这样，在Cisco 7200或者Cisco 7500路由器中，用户可以使用下面的格式指定某个特定的串行端口：

```
interface serial slot #/port #
```

在Cisco 7200系列设备中，这种格式有一些变化，因为多个端口可以在一个端口适配卡上，而多个端口适配卡可以插在一个槽上。在这种情形下，可以使用下面的命令格式引用某个特定的串行端口。

```
interface serial slot #/port adapter/port #
```

按照路由器的数据流，当路由器从LAN上接收到数据后，报文的第2层报文头被丢掉，并进入RAM中。此时，CPU检查路由表，以决定报文的输出端口及报文的封装方式。

前面所描述的处理过程称为过程式交换模式（Process Switching Mode）。每一个报文都必须被CPU处理，CPU要查询路由器并决定往何处发送报文。Cisco路由器还有一种交换模式称为快速交换（Fast Switching）。在快速交换模式中，路由器维护着一个内存缓冲区，其中包含目的IP地址与下一跳的接口信息。

路由器通过存储以前从路由表中获取的信息而创建这样的缓存。去往特定目标的第一个报文需要CPU查询路由表。一旦路由信息被得到之后，在决定去往特定目标的下一跳时，其信息就已经存储在快速交换缓存中。当新的发往该目标的报文到达时，就不再需要查询路由表。这种机制使得路由器交换报文的速度更快，并且路由器CPU的负载也会相应降低。

快速交换的变种存在于特殊硬件结构中，它只在高端路由器模型，如7200和7500系列中才存在。但快速交换的变种与快速交换两者的原理在本质上是一样的，对于所有的交换模式都需要一个包含目的地址到接口映射的缓存。还有一种交换模式称为网络流交换（Netflow Switching），这种方式不仅缓存目的IP地址，还缓存源IP地址和上层的TCP或UDP端口等。在IOS版本12.0以前，这种交换模式也只在高端路由器平台上才存在。从12.0T开始，Cisco将这种交换模式引入到了低端平台，如2600中。

对于快速交换还有一些要点需要指出。首先，任何对路由表或ARP缓存的修改都会导致强制清除快速交换缓存中的内容。该动作一般发生在拓扑结构发生改变时，此时快速交换缓存要重建。而且，快速交换缓存中的项会随着路由表中内容的改变而改变。快速交换缓存中的项与路由表中的相应项要能匹配。例如，如果路由器有一个到10.1.1.0/24网络的路由，路由器将会缓存目标10.1.1.0/24。如果路由器只有一个到10.1.0.0/16网络的路由，路由器将会缓存目标10.1.0.0/16。如果路由表中没有网络或子网的项，路由器就使用缺省路由，并使用缺省主网络屏蔽码，路由器将缓存目标10.0.0.0/8。

这种方式只工作在对特定的目标只有一个路由的情况下。如果有多个代价相同的路径，且无缺省路径，路由器就会缓存整个32位的目标。例如，若目的IP地址为10.1.1.1，而路由器