HZ BOOKS

Microsoft Press

Microsoft
核心技术丛书

Windows Server 2008
网络互联和网络访问保护参考手册

Windows Server 2008 Networking and Network Access Protection (NAP)

（美） Joseph Davies
Tony Northrup 著
Microsoft网络团队

侯彦娥 贾笑明 党兰学 等译

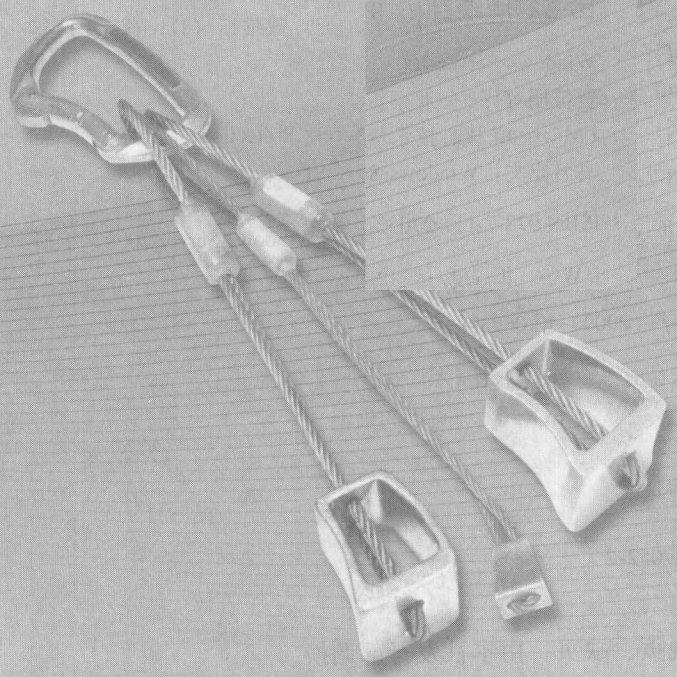
机械工业出版社
China Machine Press

Microsoft
核心技术丛书

Windows Server 2008 网络互联和网络访问保护参考手册

Windows Server 2008 Networking and Network Access Protection (NAP)

Joseph Davies
(美) Tony Northrup 著
Microsoft网络团队
侯彦娥 贾笑明 党兰学 等译



机械工业出版社
China Machine Press

本书分为四部分。第一部分提供部署指南构建寻址和数据流基础结构。第二部分利用域名系统（DNS）和 Windows Internet 名称服务（WINS）来构建名称解析基础结构。第三部分讨论如何构建一个网络访问基础结构，包括活动目录域服务、公钥基础结构、组策略等。第四部分介绍网络访问保护（NAP）。

本书提供的部署方案并没有针对任何具体类型的组织或者特定的网络，从基本原理出发，为读者提供通用的部署指导。本书不仅可以作为 Windows 网络管理员学习部署网络基础结构以及排除网络故障的参考书，同时也可以作为教材供教师和学生使用。

Joseph Davies：Windows Server 2008 Networking and Network Access Protection（NAP）
（ISBN：978-0-7356-2422-1）

版权登记号：图字：01-2009-1601

图书在版编目（CIP）数据

Windows Server 2008 网络互联和网络访问保护参考手册/（美）戴维斯（Davies, J.）等著；贾笑明等译. —北京：机械工业出版社，2009.7
（Microsoft 核心技术丛书）
书名原文：Windows Server 2008 Networking and Network Access Protection

ISBN 978-7-111-27052-2

Ⅰ. W… Ⅱ. ①戴… ②贾… Ⅲ. 服务器－操作系统（软件），Windows Server 2008－手册
Ⅳ. TP316.86-62

中国版本图书馆 CIP 数据核字（2009）第 069398 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：陈佳媛
北京慧美印刷有限公司印刷
2009 年 7 月第 1 版第 1 次印刷
186mm×240mm · 35.5 印张
标准书号：ISBN 978-7-111-27052-2
定价：85.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

译 者 序

作为网络管理员，可能你正打算部署组织的专用网络，或者正在为如何确保连接到专用网络的计算机能正常运行而深感苦恼。部署组织的专用网络，总需要对涉及到的基础结构进行必要的了解，并掌握其部署方案；在完成部署之后，为了保证网络的正常运行所要进行的维护也会耗费你相当多的精力。作者对本书的内容进行了精心组织，不仅让读者了解到网络和网络访问保护的基础知识，同时以图文并茂的方式指导读者部署各种组件和基础结构。除此之外，针对每个环节可能出现的常见问题，作者都给出了疑难解答工具以及使用这些工具进行故障排除的解决方案。

本书提供的部署方案并没有针对任何具体类型的组织或者特定的网络，而是从基本原理出发，为读者提供通用的部署指导。本书不仅可以作为 Windows 网络管理员学习部署网络基础结构，以及排除网络故障的参考书，同时也可以作为教材供教师和学生使用。

参与本书翻译的人员有：侯彦娥（第 9、11、13 章）、贾笑明（第 1、3、4 章）、党兰学（第 14、15 章）、付征叶（第 10、12 章以及词汇表）、闵林（第 5、6、7、8 章）、赵亮（第 2 章）、史苇杭（第 16、17 章）和牛现云（第 18、19 章）。侯彦娥、贾笑明和党兰学对全书译稿进行统一整理。

虽然我们本着精益求精、锲而不舍的态度，尽力保证本书翻译的准确性，但由于能力、时间有限，书中出现错误与不妥之处在所难免。非常欢迎任何相关的批评、建议和指正（联系 E-mail：houyane@foxmail.com）。

译 者

2009 年 2 月于开封

前　言

欢迎阅读这本《*Windows Server* 2008 网络互联和网络访问保护参考手册》。

通过在本书第一部分提供的部署指南，你可以使用 Internet 协议版本 4（IPv4）和 Internet 协议版本 6（IPv6）、动态主机配置协议（DHCP）、基于主机的防火墙和 Internet 协议安全（IPsec）、基于策略的服务质量（QoS）和可伸缩网络技术构建寻址和数据流基础结构。

你可以通过本书第二部分提供的部署指南，利用域名系统（DNS）和 Windows Internet 名称服务（WINS）来构建名称解析基础结构。

你也可以通过本书第三部分提供的指南部署一个网络访问基础结构，包括活动目录域服务、公钥基础结构、组策略、并使用远程身份验证拨入用户服务（RADIUS）进行集中的身份验证、授权和记账。这种网络访问基础结构支持各种身份验证和授权的网络接入方式，包括 IEEE 802.11 无线网络，带有身份验证的交换机和虚拟专用网络（VPN）连接。

一旦寻址和数据包流、名称解析以及网络访问基础结构就位，就可以使用本书第四部分提供的指南部署网络访问保护（NAP），来对受到 IPsec 保护的通信、通过 IEEE 802.1X 进行身份验证的无线和有线接入、远程访问 VPN 连接和 DHCP 地址配置强制系统健康要求。

编写体例

本书使用了以下约定以突出特定功能或用法：

读者助手

本书使用了以下读者助手来指出有帮助的细节：

读者助手	用途
注意	强调特定概念的重要性，或突出某一特例可能不适用于所有的情况
更多信息	指出补充信息的其他资源
在线内容	提醒注意相关链接，可以帮助完成文中描述的任务

补充内容

本书使用了以下补充内容来提供有关联网和网络访问保护（NAP）的其他见解、技巧和建议：

补充内容	用途
起源	由 Microsoft 专家提供，从源头洞察这些技术的工作机制、最佳实践和疑难解答技巧
工作机制	提供独特的功能视角以及它们的工作机制

命令行示例

书中的命令行示例格式使用以下约定：

格式	用途
粗体	表示用户输入（输入与所见的字符完全一致）
斜体	表示需要提供特定值的变量（例如，file_name 可以指任意有效的文件名）
固定间距字体	用于示例代码或命令行输出
% SystemRoot%	环境变量

其他联机内容

当本书有补充的新资料或更新的内容时，它会发布在 Microsoft Press Online 的 Windows Server and Client 网站。根据 Windows Server 2008 的最终版本，你所找到的更新可能包括本书的内容、文章、参考内容链接、勘误表、样章等。该站点位于 http：//www. microsoft. com/learning/books/online/serverclient 并将定期更新。

致　谢

Joseph Davies 和 Tony Northrup 要感谢 Windows Server 2008 产品团队的众多成员，以及 Microsoft 在这个项目中奉献了数百个小时宝贵时间的其他专家，当我们在这个项目上工作时，他们仔细审查了章节内容中技术的准确性，贡献内容，并不厌其烦地提供他们的意见、鼓励和支持。

特别要感谢 Microsoft 的以下参与人员，他们编写了补充内容中的“起源”部分，这一部分提供了只有这些专家才可能知道的深层知识（按章节顺序）：

- Dmitry Anipko，Windows Core Networking Group 的一位开发人员。
- Sean Siler，Windows Core Networking Group 的一位 IPv6 程序经理。
- Santosh Santosh，Enterprise Networking Group 的资深程序经理。
- Ian Hameroff，Security and Access Product Marketing 的高级产品经理。
- Gabe Frost，Windows Core Networking 的产品经理。
- Rade Trimceski，Windows Networking and Devices and Devices Group 的程序经理。
- Jeff Westhead，Enterprise Networking Group 的一位高级软件开发工程师。
- Anthony Witecki，Microsoft Services，Public Sector 的一位高级顾问。
- Chris Irwin，Premier Field Engineering Group 的一位高级现场工程师。
- Clay Seymour，Enterprise Platform Support 的一位升级支持工程师。
- Tim Quinn，Enterprise Platform Support 的一位升级支持工程师。
- James McIllece，Windows Server User Assistance Group 的一位技术作家。
- Samir Jain，India Development Center 的一位资深程序经理。
- Greg Lindsay，Windows Server User Assistance Group 的一位技术作家。
- John Morello，Windows Server Customer Connection Group 的一位高级程序经理。

当我们在编写本书时，Windows Server 2008 还处于开发阶段，Microsoft 许多卓越的工作人员审查了我们的初稿并提出更正意见，提醒我们注意操作系统中的变动，并建议补充内容。在此多谢我们的审稿人（按章节顺序）：

Mike Barrett，Dmitri Anipko，Ben Shultz，Thiago Hirai，Mahesh Narayanan，Santosh Chandwani，Jason Popp，Hermant Banavar，Osama Mazahir，Ian Hameroff，Rade Trimceski，Alireza Dabagh，Chandra Nukala，Arren Conner，Jeff Westhead，Sudhakar Pasupuleti，Yi Zhao，Subhasish Bhattacharya，Tim Quinn，Clay Seymour，Chris Irwin，Greg Lindsay，James MacIllece，Anthony Leibovitz，Sreenivas Addagatla，Arvind Jayakar，Brit Weston，Lee Gibson，Drew Baron，Brit Weston，Dhiraj Gupta，Samir Jain，Puja Pandey，Tushar Gupta，Manu Jeewani，Jim Holtzman，Kevin Rhodes，Steve Espinosa，Tom Kelnar，Kedar Mohare，Pat Fetty，Gavin Carius，Wai - O Hui，Harini Muralidharan，Richard Costleigh，Ryan Hurst，Chris Edson，Chandra Nukala，Abhishek Tiwari，Aanand Ramachandran，John Morrello 和 Barry Mendonca。

另外，感谢 Microsoft Security Review Board 对本书所有内容的细心审阅。

如果上述列表有所遗漏，敬请谅解。

Joseph 个人特别要向 Greg Lindsay 表示感谢，对于本书的网络访问保护（NAP）各章，他在会议、讨论、技术审查和多篇补充资料上投入了大量的时间。

Tony 个人也要向 Bob Hogan 表示感谢，他所做的已经超出了作为技术编辑所需要的份内工作，还有 Hayley Bellamy，感谢他帮助解决了一个关键的硬件故障。

最后，我们要共同感谢我们出色的编辑团队，包括 Microsoft Press 对于该项目的 Martin DelRe，Jenny Moss Benson，Maureen Zimmerman，Maria Gargiulo，以及 Interactive Composition Corporation 的 Susan McClung，Joel Rosenthal，Bob Hogan，Mary Rosewood，Seth Maislin，本书的成功来自他们充沛的精力和不懈的努力。

——*Joseph*，*Tony*

目　录

译者序
前言
致谢

第一部分　寻址和数据流基础结构

第 1 章　IPv4 …… 1
1.1　概念 …… 1
1.1.1　网络层 …… 1
1.1.2　IPv4 寻址 …… 1
1.1.3　私有 IPv4 地址 …… 4
1.1.4　自动专用 IP 地址（APIPA） …… 4
1.1.5　多播地址 …… 4
1.1.6　网络地址转换 …… 5
1.1.7　第 2 层和第 3 层寻址 …… 6
1.1.8　第 4 层协议：UDP 和 TCP …… 7
1.2　规划和设计要点 …… 8
1.2.1　设计 Internet 连接 …… 8
1.2.2　创建 IPv4 寻址方案 …… 10
1.2.3　规划主机地址 …… 10
1.2.4　使用 VPN …… 11
1.2.5　规划冗余 …… 12
1.2.6　使用多宿主计算机 …… 13
1.3　部署步骤 …… 13
1.3.1　手动配置 IPv4 客户端 …… 14
1.3.2　配置 DHCP 服务器不可用时的客户端行为 …… 14
1.3.3　增加路由到路由表 …… 14
1.4　日常维护 …… 15
1.5　疑难解答 …… 15
1.5.1　ARP …… 15
1.5.2　Ipconfig …… 15
1.5.3　Netstat …… 16
1.5.4　PathPing …… 17
1.5.5　性能监测器 …… 18
1.5.6　Ping …… 18
1.5.7　任务管理器 …… 19
1.5.8　Windows 网络诊断 …… 20
1.6　本章小结 …… 20
1.7　其他信息 …… 20
第 2 章　IPv6 …… 21
2.1　概念 …… 21
2.1.1　IPv4 到 IPv6 的变化 …… 21
2.1.2　IPv6 寻址 …… 22
2.1.3　IPv6 自动配置 …… 26
2.1.4　DHCPv6 …… 27
2.1.5　邻居发现 …… 28
2.1.6　IPv6 安全性 …… 28
2.1.7　IPv6 过渡技术 …… 28
2.2　规划和设计要点 …… 33
2.2.1　迁移到 IPv6 …… 34
2.2.2　获得 IPv6 地址 …… 35
2.2.3　规划网络基础结构升级 …… 35
2.2.4　规划 IPv6 过渡技术 …… 35
2.3　部署步骤 …… 36
2.3.1　禁用 IPv6 …… 36
2.3.2　手动配置 IPv6 …… 37
2.3.3　从脚本配置 IPv6 …… 37
2.3.4　启用 ISATAP …… 37
2.3.5　启用 6to4 …… 38
2.3.6　启用 Teredo …… 39
2.3.7　配置 IPv6 计算机为 IPv6 路由器 … 40
2.4　日常维护 …… 43
2.5　疑难解答 …… 43
2.5.1　Netsh …… 43
2.5.2　Ipconfig …… 44
2.5.3　Nslookup …… 44
2.5.4　Teredo 疑难解答 …… 44

2.6 本章小结 …… 45
2.7 其他信息 …… 45
第3章 动态主机配置协议 …… 46
3.1 概念 …… 46
3.1.1 DHCP 地址分配过程 …… 46
3.1.2 DHCP 生命周期 …… 47
3.2 规划和设计要点 …… 47
3.2.1 DHCP 服务器 …… 48
3.2.2 DHCP 中继代理 …… 48
3.2.3 DHCP 租期 …… 49
3.2.4 规划作用域 …… 49
3.2.5 DHCP 服务器群集 …… 50
3.2.6 动态 DNS …… 50
3.3 部署步骤 …… 51
3.3.1 DHCP 服务器 …… 51
3.3.2 DHCP 中继代理 …… 57
3.3.3 DHCP 客户端配置 …… 58
3.4 日常维护 …… 58
3.4.1 监视 DHCP 服务器 …… 59
3.4.2 手动备份和还原 DHCP 服务器 … 60
3.5 疑难解答 …… 60
3.5.1 DHCP 客户端疑难解答 …… 60
3.5.2 DHCP 服务器疑难解答 …… 61
3.5.3 使用审核日志分析 DHCP 服务器行为 …… 61
3.6 本章小结 …… 62
3.7 其他信息 …… 62
第4章 高级安全 Windows 防火墙 …… 63
4.1 概念 …… 63
4.1.1 使用 Windows 防火墙筛选通信 … 63
4.1.2 使用 IPsec 保护通信 …… 64
4.2 规划和设计要点 …… 67
4.2.1 规划 Windows 防火墙策略 …… 67
4.2.2 使用 IPsec 保护通信 …… 69
4.3 部署步骤 …… 74
4.3.1 使用组策略配置防火墙设置 …… 74
4.3.2 IPsec 连接安全规则 …… 79
4.4 日常维护 …… 81
4.5 疑难解答 …… 82
4.5.1 Windows 防火墙日志 …… 83
4.5.2 监视 IPsec 安全关联 …… 85
4.5.3 使用 Network Monitor …… 85
4.6 本章小结 …… 85
4.7 其他信息 …… 86
第5章 基于策略的服务质量 …… 87
5.1 概念 …… 87
5.1.1 产生网络性能问题的根源 …… 87
5.1.2 QoS 提供的帮助 …… 88
5.1.3 出站流量的 QoS …… 89
5.1.4 入站流量的 QoS …… 90
5.1.5 QoS 实现 …… 91
5.2 规划和设计要点 …… 91
5.2.1 设置 QoS 目标 …… 91
5.2.2 规划 DSCP 值 …… 91
5.2.3 规划流量调节 …… 93
5.2.4 硬件和软件需求 …… 93
5.2.5 规划 GPO 和 QoS 策略 …… 94
5.2.6 用于 Windows Vista 便携式计算机的 QoS 策略 …… 95
5.3 部署步骤 …… 95
5.3.1 使用组策略配置 QoS …… 95
5.3.2 配置系统范围 QoS 设置 …… 98
5.4 日常维护 …… 99
5.4.1 删除 QoS 策略 …… 99
5.4.2 编辑 QoS 策略 …… 100
5.4.3 监视 QoS …… 100
5.5 疑难解答 …… 102
5.5.1 分析 QoS 策略 …… 102
5.5.2 验证 DSCP 恢复能力 …… 103
5.5.3 隔离网络性能问题 …… 104
5.6 本章小结 …… 105
5.7 其他信息 …… 105
第6章 可伸缩网络 …… 106
6.1 概念 …… 106
6.1.1 TCP 烟囱卸载 …… 106
6.1.2 接收端缩放 …… 108
6.1.3 NetDMA …… 109
6.1.4 IPsec 卸载 …… 110
6.2 规划和设计要点 …… 110
6.2.1 评估网络可伸缩性技术 …… 110
6.2.2 负载测试服务器 …… 111
6.2.3 监视服务器性能 …… 112

6.3 部署步骤 …… 114
6.3.1 配置 TCP 烟囱卸载 …… 114
6.3.2 配置接收方缩放 …… 114
6.3.3 配置 NetDMA …… 115
6.3.4 配置 IPsec 卸载 …… 115
6.4 日常维护 …… 115
6.5 疑难解答 …… 116
6.5.1 TCP 烟囱卸载疑难解答 …… 116
6.5.2 IPsec 卸载疑难解答 …… 117
6.6 本章小结 …… 117
6.7 其他信息 …… 118

第二部分 名称解析基础结构

第 7 章 域名系统 …… 119
7.1 概念 …… 119
7.1.1 DNS 层次结构 …… 119
7.1.2 DNS 区域 …… 120
7.1.3 DNS 记录 …… 120
7.1.4 动态 DNS 更新 …… 120
7.1.5 DNS 名称解析 …… 121
7.2 规划和设计要点 …… 122
7.2.1 DNS 区域 …… 122
7.2.2 DNS 服务器位置 …… 123
7.2.3 DNS 区域复制 …… 124
7.2.4 DNS 安全性 …… 125
7.2.5 GlobalNames 区域 …… 126
7.3 部署步骤 …… 127
7.3.1 DNS 服务器配置 …… 127
7.3.2 DHCP 服务器配置 …… 134
7.3.3 DNS 客户端配置 …… 135
7.3.4 配置冗余 DNS 服务器 …… 136
7.4 日常维护 …… 136
7.4.1 添加资源记录 …… 136
7.4.2 维护区域 …… 137
7.4.3 自动监视 …… 137
7.4.4 提升辅助区域为主要区域 …… 139
7.5 疑难解答 …… 140
7.5.1 事件日志 …… 140
7.5.2 使用 Nslookup …… 140
7.5.3 服务器调试日志 …… 143
7.5.4 使用 DNSLint …… 143
7.5.5 使用 DCDiag …… 144
7.5.6 使用 Network Monitor …… 146
7.6 本章小结 …… 146
7.7 其他信息 …… 146
第 8 章 Windows Internet 名称服务 …… 147
8.1 概念 …… 147
8.1.1 历史 …… 147
8.1.2 NetBIOS 名称 …… 148
8.1.3 WINS 名称解析 …… 148
8.1.4 WINS 客户端注册 …… 149
8.2 规划和设计要点 …… 149
8.2.1 WINS 服务器位置 …… 150
8.2.2 WINS 复制 …… 150
8.3 部署步骤 …… 151
8.3.1 配置 WINS 服务器 …… 151
8.3.2 配置 WINS 复制 …… 152
8.3.3 WINS 客户端配置 …… 152
8.4 日常维护 …… 154
8.4.1 备份 WINS 服务器数据库 …… 154
8.4.2 压缩 WINS 数据库 …… 155
8.4.3 执行一致性检查 …… 155
8.4.4 监视 WINS 服务器 …… 156
8.4.5 添加静态 WINS 记录 …… 157
8.4.6 删除 WINS 记录 …… 158
8.5 疑难解答 …… 158
8.5.1 WINS 服务器疑难解答 …… 158
8.5.2 WINS 客户端疑难解答 …… 160
8.6 本章小结 …… 162
8.7 其他信息 …… 163

第三部分 网络访问基础结构

第 9 章 身份验证基础结构 …… 165
9.1 概念 …… 165
9.1.1 活动目录域服务 …… 165
9.1.2 公钥基础结构 …… 168
9.1.3 组策略 …… 171
9.1.4 RADIUS …… 173
9.2 规划和设计要点 …… 177
9.2.1 活动目录 …… 177
9.2.2 PKI …… 178

9.2.3 组策略 …… 179
9.2.4 RADIUS …… 179
9.3 部署步骤 …… 185
9.3.1 部署活动目录 …… 185
9.3.2 部署 PKI …… 185
9.3.3 组策略 …… 191
9.3.4 RADIUS 服务器 …… 191
9.3.5 使用 RADIUS 代理实现跨林身份验证 …… 196
9.3.6 使用 RADIUS 代理扩展身份验证 …… 202
9.4 日常维护 …… 205
9.4.1 活动目录 …… 205
9.4.2 PKI …… 205
9.4.3 组策略 …… 205
9.4.4 RADIUS …… 206
9.5 疑难解答工具 …… 207
9.5.1 活动目录 …… 207
9.5.2 PKI …… 207
9.5.3 组策略 …… 207
9.5.4 RADIUS …… 207
9.6 本章小结 …… 208
9.7 其他信息 …… 209
第 10 章 IEEE 802.11 无线网络 …… 211
10.1 概念 …… 211
10.1.1 对 IEEE 802.11 标准的支持 …… 212
10.1.2 无线安全 …… 213
10.1.3 802.11 无线网络的组件 …… 215
10.2 规划和设计要点 …… 216
10.2.1 无线安全技术 …… 217
10.2.2 无线身份验证模式 …… 218
10.2.3 Intranet 基础结构 …… 219
10.2.4 无线 AP 布局 …… 220
10.2.5 身份验证基础结构 …… 224
10.2.6 无线客户端 …… 224
10.2.7 PKI …… 232
10.2.8 使用 NAP 的 802.1X 强制 …… 234
10.3 部署受保护的无线访问 …… 234
10.3.1 部署证书 …… 234
10.3.2 配置活动目录的用户账户和组 …… 236
10.3.3 配置 NPS 服务器 …… 236
10.3.4 部署无线 AP …… 237
10.3.5 配置无线客户端 …… 239
10.4 日常维护 …… 243
10.4.1 管理用户账户和计算机账户 …… 243
10.4.2 管理无线 AP …… 244
10.4.3 更新无线配置文件 …… 244
10.5 疑难解答 …… 244
10.5.1 Windows 中的无线疑难解答工具 …… 245
10.5.2 Windows 无线客户端疑难解答 …… 250
10.5.3 无线 AP 疑难解答 …… 251
10.5.4 身份验证基础结构疑难解答 …… 254
10.6 本章小结 …… 258
10.7 其他信息 …… 258
第 11 章 IEEE 802.1X 身份验证有线网络 …… 260
11.1 概念 …… 260
11.2 规划和设计要点 …… 261
11.2.1 有线身份验证方法 …… 261
11.2.2 有线身份验证模式 …… 263
11.2.3 身份验证基础结构 …… 264
11.2.4 有线客户端 …… 265
11.2.5 PKI …… 269
11.2.6 使用 NAP 的 802.1X 强制 …… 271
11.3 部署 802.1X 身份验证有线访问 …… 271
11.3.1 部署证书 …… 271
11.3.2 配置活动目录的账户和组 …… 273
11.3.3 配置 NPS 服务器 …… 273
11.3.4 配置支持 802.1X 的交换机 …… 274
11.3.5 配置有线客户端 …… 275
11.4 日常维护 …… 278
11.4.1 管理用户账户和计算机账户 …… 278
11.4.2 管理支持 802.1X 的交换机 …… 278
11.4.3 更新有线 XML 配置文件 …… 279
11.5 疑难解答 …… 279
11.5.1 Windows 中的有线疑难解答工具 …… 279
11.5.2 Windows 有线客户端疑难解答 …… 283
11.5.3 支持 802.1X 的交换机疑难解答 …… 284
11.5.4 身份验证基础结构疑难解答 …… 286
11.6 本章小结 …… 290
11.7 其他信息 …… 290

第 12 章 远程访问 VPN 连接 …… 292
12.1 概念 …… 292
12.2 规划和设计要点 …… 294
12.2.1 VPN 协议 …… 295
12.2.2 身份验证方法 …… 298
12.2.3 VPN 服务器 …… 299
12.2.4 Internet 基础结构 …… 302
12.2.5 Intranet 基础结构 …… 303
12.2.6 VPN 客户端并发访问 Intranet 和 Internet …… 306
12.2.7 身份验证基础结构 …… 307
12.2.8 VPN 客户端 …… 308
12.2.9 PKI …… 311
12.2.10 使用 NAP 的 VPN 强制 …… 313
12.3 其他安全要点 …… 314
12.3.1 强链路加密 …… 314
12.3.2 VPN 服务器上的 VPN 通信包筛选 …… 314
12.3.3 用于 VPN 通信的防火墙包筛选 …… 314
12.3.4 多用途的 VPN 服务器 …… 321
12.3.5 阻止 VPN 客户端的通信路由 … 322
12.3.6 并发访问 …… 322
12.3.7 未使用的 VPN 协议 …… 323
12.4 部署基于 VPN 的远程访问 …… 323
12.4.1 部署证书 …… 323
12.4.2 配置 Internet 基础结构 …… 325
12.4.3 配置活动目录的用户账户和组 …… 326
12.4.4 配置 RADIUS 服务器 …… 326
12.4.5 部署 VPN 服务器 …… 327
12.4.6 配置 Intranet 网络基础结构 …… 331
12.4.7 部署 VPN 客户端 …… 332
12.5 日常维护 …… 336
12.5.1 管理用户账户 …… 337
12.5.2 管理 VPN 服务器 …… 337
12.5.3 更新 CM 配置文件 …… 338
12.6 疑难解答 …… 338
12.6.1 疑难解答工具 …… 338
12.6.2 远程访问 VPN 疑难解答 …… 342
12.7 本章小结 …… 346
12.8 其他信息 …… 346
第 13 章 站点间 VPN 连接 …… 348
13.1 概念 …… 348
13.1.1 请求拨号路由概述 …… 348
13.1.2 Windows 站点间 VPN 的组件 … 352
13.2 规划和设计要点 …… 352
13.2.1 VPN 协议 …… 353
13.2.2 身份验证方法 …… 355
13.2.3 VPN 路由器 …… 356
13.2.4 Internet 基础结构 …… 359
13.2.5 站点网络基础结构 …… 360
13.2.6 身份验证基础结构 …… 362
13.2.7 PKI …… 364
13.3 部署站点间 VPN 连接 …… 366
13.3.1 部署证书 …… 366
13.3.2 配置 Internet 基础结构 …… 369
13.3.3 配置活动目录的用户账户和组 …… 370
13.3.4 配置 RADIUS 服务器 …… 370
13.3.5 部署应答路由器 …… 371
13.3.6 部署呼叫路由器 …… 376
13.3.7 配置站点网络基础结构 …… 380
13.3.8 配置站点间网络基础结构 …… 382
13.4 日常维护 …… 383
13.4.1 管理用户账户 …… 384
13.4.2 管理 VPN 路由器 …… 384
13.5 疑难解答 …… 385
13.5.1 疑难解答工具 …… 385
13.5.2 站点间 VPN 连接疑难解答 …… 385
13.6 本章小结 …… 391
13.7 其他信息 …… 392

第四部分 网络访问保护基础结构

第 14 章 网络访问保护概述 …… 393
14.1 网络访问保护的必要性 …… 393
14.1.1 恶意软件及其对企业计算的影响 …… 393
14.1.2 企业网恶意软件防护 …… 394
14.1.3 NAP 的角色 …… 397
14.1.4 NAP 的商业收益 …… 398
14.2 NAP 的组件 …… 399

14.2.1 系统健康代理和系统健康验证程序 …… 400
14.2.2 强制客户端和强制服务器 …… 401
14.2.3 NPS …… 401
14.3 强制方法 …… 402
14.3.1 IPsec 强制 …… 402
14.3.2 802.1X 强制 …… 402
14.3.3 VPN 强制 …… 403
14.3.4 DHCP 强制 …… 403
14.4 NAP 的工作机制 …… 403
14.4.1 IPsec 强制的工作机制 …… 404
14.4.2 802.1X 强制的工作机制 …… 405
14.4.3 VPN 强制的工作机制 …… 405
14.4.4 DHCP 强制的工作机制 …… 406
14.5 本章小结 …… 407
14.6 其他信息 …… 407
第 15 章 准备网络访问保护 …… 409
15.1 评估当前网络的基础结构 …… 409
15.1.1 Intranet 计算机 …… 409
15.1.2 第 2 层接入 Intranet …… 410
15.1.3 网络支持基础结构 …… 411
15.2 NAP 健康策略服务器 …… 411
15.2.1 规划和设计要点 …… 412
15.2.2 部署步骤 …… 413
15.2.3 日常维护 …… 414
15.3 健康要求策略配置 …… 414
15.3.1 健康要求策略的组件 …… 415
15.3.2 NAP 健康评估工作机制 …… 420
15.3.3 健康要求策略的规划和设计要点 …… 423
15.4 更新服务器 …… 424
15.4.1 更新服务器和 NAP 强制方法 … 425
15.4.2 更新服务器的规划和设计要点 …… 426
15.5 本章小结 …… 426
15.6 其他信息 …… 427
第 16 章 IPsec 强制 …… 428
16.1 了解 IPsec 强制 …… 428
16.1.1 IPsec 强制逻辑网络 …… 429
16.1.2 使用 IPsec 强制的通信建立过程 …… 429
16.1.3 IPsec 强制的连接安全规则 …… 432
16.2 规划和设计要点 …… 433
16.2.1 活动目录 …… 433
16.2.2 PKI …… 434
16.2.3 HRA …… 438
16.2.4 IPsec 策略 …… 442
16.2.5 NAP 客户端 …… 443
16.3 部署 IPsec 强制 …… 444
16.3.1 配置活动目录 …… 444
16.3.2 配置 PKI …… 445
16.3.3 配置 HRA …… 447
16.3.4 配置 NAP 健康策略服务器 …… 452
16.3.5 在边界网络上配置更新服务器 …… 455
16.3.6 配置 NAP 客户端 …… 455
16.3.7 报告模式的 IPsec 强制部署检查点 …… 458
16.3.8 配置和应用 IPsec 策略 …… 458
16.4 日常维护 …… 462
16.4.1 添加 NAP 客户端 …… 462
16.4.2 添加新的 SHA 和 SHV …… 462
16.4.3 管理 NAP CA …… 463
16.4.4 管理 HRA …… 464
16.5 疑难解答 …… 465
16.5.1 疑难解答工具 …… 465
16.5.2 IPsec 强制疑难解答 …… 467
16.6 本章小结 …… 471
16.7 其他信息 …… 471
第 17 章 802.1X 强制 …… 473
17.1 802.1X 强制概述 …… 473
17.1.1 使用 ACL …… 475
17.1.2 使用 VLAN …… 476
17.2 规划和设计要点 …… 476
17.2.1 NAP 免除安全组 …… 476
17.2.2 802.1X 身份验证方法 …… 477
17.2.3 802.1X 强制类型 …… 477
17.2.4 802.1X 访问点 …… 477
17.2.5 NAP 客户端 …… 478
17.3 部署 802.1X 强制 …… 479
17.3.1 配置活动目录 …… 479
17.3.2 配置基于 PEAP 的身份验证方法 …… 480

17.3.3 配置 802.1X 访问点 …… 480
17.3.4 配置受限网络上的更新服务器 …… 481
17.3.5 配置 NAP 健康策略服务器 …… 481
17.3.6 配置 NAP 客户端 …… 487
17.3.7 报告模式的 802.1X 强制部署检查点 …… 490
17.3.8 测试受限访问 …… 490
17.3.9 为不相容 NPA 客户端配置用于延迟强制模式的网络策略 …… 491
17.4 日常维护 …… 492
17.4.1 添加 NAP 客户端 …… 492
17.4.2 添加新的 SHA 和 SHV …… 493
17.4.3 管理 802.1X 访问点 …… 493
17.5 疑难解答 …… 493
17.5.1 疑难解答工具 …… 493
17.5.2 802.1X 强制疑难解答 …… 495
17.6 本章小结 …… 497
17.7 其他信息 …… 497
第 18 章 VPN 强制 …… 499
18.1 了解 VPN 强制 …… 499
18.2 规划和设计要点 …… 501
18.2.1 网络访问隔离控制的使用 …… 501
18.2.2 NAP 免除安全组 …… 502
18.2.3 包筛选类型 …… 502
18.2.4 VPN 身份验证方法 …… 503
18.2.5 VPN 服务器 …… 503
18.2.6 NAP 客户端 …… 503
18.3 部署 VPN 强制 …… 505
18.3.1 配置活动目录 …… 505
18.3.2 配置 VPN 服务器 …… 506
18.3.3 配置基于 PEAP 的身份验证方法 …… 506
18.3.4 配置更新服务器 …… 506
18.3.5 配置 NAP 健康策略服务器 …… 507
18.3.6 配置 NAP 客户端 …… 512
18.3.7 配置报告模式的 VPN 强制部署检查点 …… 513
18.3.8 测试受限访问 …… 513
18.3.9 配置延迟强制 …… 514
18.3.10 配置强制模式的网络策略 …… 515
18.4 日常维护 …… 516
18.4.1 添加 NAP 客户端 …… 516
18.4.2 添加新的 SHA 和 SHV …… 516
18.5 疑难解答 …… 516
18.5.1 疑难解答工具 …… 516
18.5.2 VPN 强制疑难解答 …… 518
18.6 本章小结 …… 520
18.7 其他信息 …… 520
第 19 章 DHCP 强制 …… 522
19.1 了解 DHCP 强制 …… 522
19.2 规划和设计要点 …… 523
19.2.1 NAP 免除安全组 …… 524
19.2.2 DHCP 服务器 …… 524
19.2.3 NAP 健康策略服务器 …… 525
19.2.4 用于特定 DHCP 作用域的健康要求策略 …… 525
19.2.5 NAP 客户端的 DHCP 选项 …… 525
19.2.6 NAP 健康策略服务器不可达时 DHCP 强制的动作 …… 525
19.2.7 NAP 客户端 …… 525
19.3 部署 DHCP 强制 …… 527
19.3.1 配置更新服务器 …… 527
19.3.2 配置 NAP 健康策略服务器 …… 527
19.3.3 配置 NAP 客户端 …… 531
19.3.4 配置 DHCP 服务器 …… 532
19.3.5 报告模式的 DHCP 强制部署检查点 …… 534
19.3.6 测试受限访问 …… 535
19.3.7 配置延迟强制 …… 536
19.3.8 配置强制模式的网络策略 …… 536
19.4 日常维护 …… 537
19.4.1 添加 NAP 客户端 …… 537
19.4.2 添加新的 SHA 和 SHV …… 537
19.5 疑难解答 …… 538
19.5.1 疑难解答工具 …… 538
19.5.2 疑难解答 DHCP 强制 …… 539
19.6 本章小结 …… 541
19.7 其他信息 …… 542
术语表 …… 543

第一部分　寻址和数据流基础结构

第 1 章　IPv4

目前，绝大部分联网计算机都在使用 Internet 协议版本 4（IPv4）和传输控制协议/Internet 协议（TCP/IP）协议族进行通信。而要对 Microsoft Windows 网络进行规划、部署、维护和疑难解答，首先必须了解 TCP/IP 的基本原理。

本章提供了如何对 IPv4 网络进行设计、部署、维护和疑难解答相关的信息。本章中的大部分信息同样适用于 Windows Server 2008、Windows Vista 和 Windows Server 2003 以及其他最新版本的 Windows 操作系统。对于 IPv6 相关的信息，请参见第 2 章。本章假定读者已经对 TCP/IP 有了大体的认识，并具有一定的网络经验。

1.1　概念

本节简要概括了重要的 TCP/IP 概念，包括 IPv4 寻址、多播、用户数据报协议（UDP）和 TCP。

1.1.1　网络层

网络协议通过分层进行组织，每一层只与直接相邻的上一层或下一层进行交互。最为常用的模型就是开放系统互连（OSI）的 7 层模型。表 1-1 列出了 7 个 OSI 分层以及各个层的协议示例。

表 1-1　OSI 分层

层	名称	示例
第 1 层	物理层	有线电缆或无线频率标准
第 2 层	数据链路层	以太网（Ethernet），无线网（Wi-Fi）
第 3 层	网络层	IPv4、IPv6、Internet 控制消息协议（ICMP）
第 4 层	传输层	TCP、UDP
第 5 层	会话层	NetBIOS
第 6 层	表示层	极少使用
第 7 层	应用层	超文本传输协议（HTTP）、简单邮件传输协议（SMTP）、邮局协议（POP）、域名系统（DNS）

本章的重点是 IPv4，它是一个第 3 层协议，但是本章也会讨论到 IPv4 如何与第 2 层和第 4 层协议相互作用。

1.1.2　IPv4 寻址

IPv4 地址的长度为 4 字节，也就是 32 位（1 字节 = 8 位）。每个字节（称作是 1 个 8 位组）写为十进制数就是 0 ~ 255，之间用一个句点（发音为“点”）隔开。例如，以下 IP 地址是有效的：

- 192. 168. 1. 32
- 10. 1. 1. 1
- 127. 0. 0. 1

IP 地址的开始部分是网络地址，余下的部分是主机地址，它标识了子网上的一个计算机。路由器使用网络地址转发数据包到正确的目标网络，计算机使用主机地址确定哪些数据包是发给它们的。图 1-1 给出了路由器如何将数据包穿过网络传送到目标计算机。

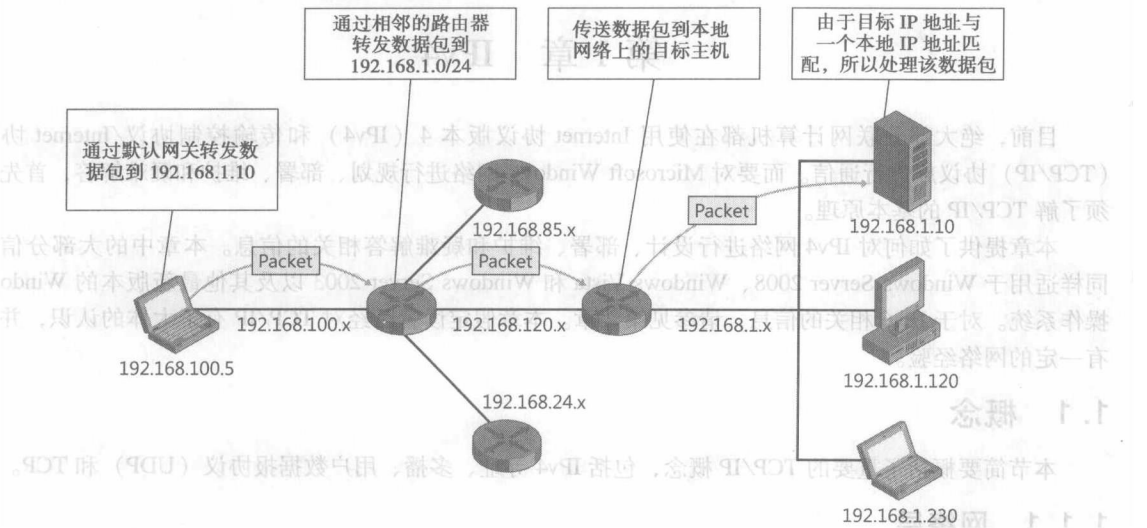


图 1-1　IPv4 路由

在图 1-1 中，IP 地址的前 3 个 8 位组是网络地址（例如 192. 168. 1 或 192. 168. 10），最后一个 8 位组是主机地址（例如 . 5 或 . 10）。虽然这是拆分 IP 地址的主机和网络部分的最为常见的方法，但是也可以：

- 使用更短的网络地址（例如 192. 168）让主机地址使用更多的位。虽然网络数量减少了，但是每个网络可以有更多的主机数量。
- 网络地址使用更多的位而让主机地址使用的位减少。这样可以提供更多的子网，但在每个网络上的惟一主机数量减少了。

主机使用子网掩码指示 IP 地址中有多少位用作网络地址。子网掩码 255. 255. 255. 0 表示 IP 地址中的前 3 个 8 位组用作网络地址，通常称作是一个 C 类网络。子网掩码 255. 255. 0. 0 表示 IP 地址中的前两个 8 位组用作网络地址，通常称作是一个 B 类网络。A 类网络很少使用，它的子网掩码是 255. 0. 0. 0，表示 IP 地址中只有第一个 8 位组用作网络地址。

起源：网络分类

基于“A”、“B”、“C”这样的分类网络已经过时了。由 RFC 1519 带来的无类型域间路由（CIDR）不仅仅是一种表示法，它与地址空间的实际划分方法也息息相关。它与分类网络之间的其中一个区别就是，分类网络中只需要给出地址，中间路由器就可以确定子网掩码，从而确定该地址是否为子网广播地址。在 CIDR 中，通常只有直接连接该子网的路由器可以确定实际的子网掩码。

Dmitry Anipko, Developer

Windows Core Networking