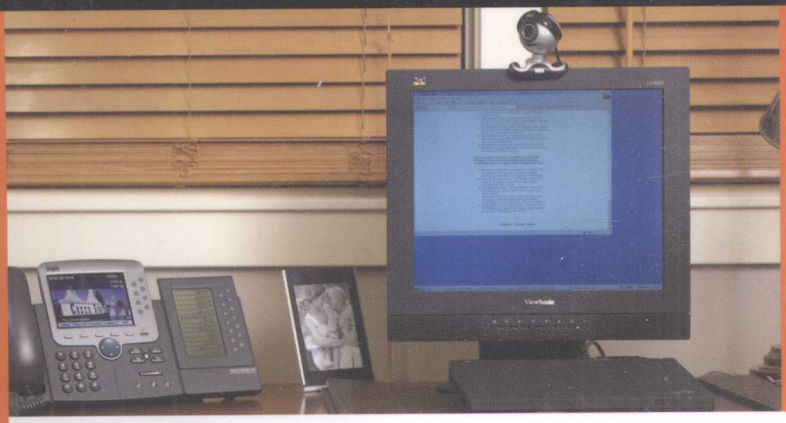
CISCO



SECURITY

局域网交换机安全

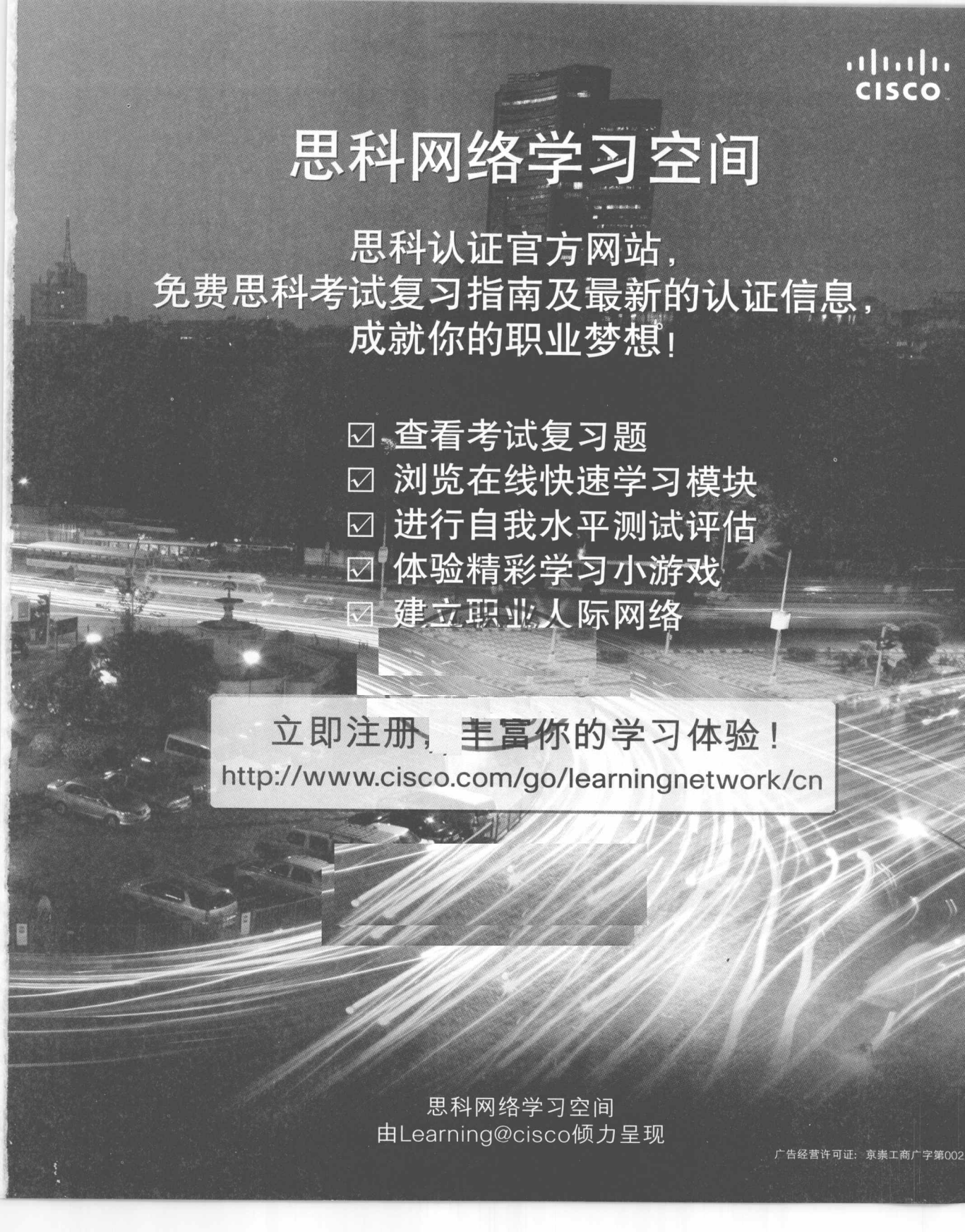
LAN Switch Security

What Hackers Know About Your Switches

A practical guide to hardening Layer 2 devices and stopping campus network attacks

〔美〕 Eric Vyncke
Christopher Paggen, CCIE #2659 著
孙余强 孙剑 译

人民邮电出版社
POSTS & TELECOM PRESS


cisco
思科网络学习空间
思科认证官方网站，
免费思科考试复习指南及最新的认证信息，
成就你的职业梦想！
☑ 查看考试复习题
☑ 浏览在线快速学习模块
☑ 进行自我水平测试评估
☑ 体验精彩学习小游戏
☑ 建立职业人际网络
立即注册，丰富你的学习体验！
http://www.cisco.com/go/learningnetwork/cn
思科网络学习空间
由Learning@cisco倾力呈现
广告经营许可证：京崇工商广字第002

图书在版编目（CIP）数据

局域网交换机安全 /（美）维恩克（Vyncke, E.），（美）培根（Paggen, C.）著；孙余强，孙剑译. -- 北京：人民邮电出版社，2010.7
ISBN 978-7-115-22990-8

Ⅰ. ①局… Ⅱ. ①维… ②培… ③孙… ④孙… Ⅲ. ①局部网络－信息交换机－安全技术 Ⅳ. ①TN915.05

中国版本图书馆CIP数据核字(2010)第086898号

局域网交换机安全

◆ 著 [美] Eric Vyncke Christopher Paggen, CCIE#2659
译 孙余强 孙 剑
责任编辑 傅道坤

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：20.5
字数：444 千字 2010 年 7 月第 1 版
印数：1－3 500 册 2010 年 7 月北京第 1 次印刷

著作权合同登记号 图字：01-2010-0302 号
ISBN 978-7-115-22990-8

定价：55.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书是迄今为止国内引进的第一本专门介绍第二层交换环境安全技术的图书。作者在书中通过一个个鲜活的第二层攻击场景，以及针对这些攻击的化解之策，来强调第二层安全的重要性。这些针对第二层协议的攻击场景，囊括了读者所知的任何一种第二层协议（STP、VRRP/HSRP、LACP/PagP、ARP 等）。书中给出了针对上述攻击的各种反制措施。

除了攻击与对抗攻击之外，作者还高屋建瓴般地展望了未来以及正在流行的第二层安全体系结构及技术，这包括线速的ACL、IEEE 802.1AE、Cisco INBS 以及结合IPSec与 L2TPv3 的安全伪线。读完本书之后，读者将会加深对网络整体安全性的理解：网络安全并不能只靠防火墙、入侵检测系统甚至是内容过滤设备。如果没有上述这些设备，在网络的第二层利用交换机同样可以实施网络安全。

本书适合从事计算机网络设计、管理和运维工作的工程技术人员阅读，可以帮助网络（安全）工程师、网络管理员快速、高效地掌握各种第二层网络安全技术。本书同样可以作为高校计算机和通信专业本科生或研究生学习网络安全的参考资料。

关于作者

Eric Vyncke 获得比利时列日大学计算机科学工程系硕士学位后在该校任助理研究员。随后进入比利时网络研究院，出任研发部门的领导。之后加盟西门子出任多个安全项目（包括一个代理防火墙项目）的项目经理。自 1997 年起，他被 Cisco 公司委以杰出咨询工程师一职，担当公司欧洲地区的安全技术顾问。20 年来，Eric 从事的专业领域一直在从第二层到应用层的网络安全方面。Eric 还是几所比利时大学安全研讨班的客座教授，经常参加各种安全活动（如 Cisco Live 的 Networkers、RSA 大会）并发言。

Christopher Paggen 于 1996 年加入 Cisco，一直从事以局域网交换和安全方面为主的工作。之后，转而负责公司当前和未来高端防火墙的产品需求定义。Christopher 持有几项美国专利，其中一项与动态 ARP 检测（Dynamic ARP Inspection，DAI）有关。除 CCIE 证书（CCIE #2659）外，Christopher 还曾获得 HEMES 大学（比利时）计算机科学学士学位，并继续在 UMS 大学（比利时）学习了两年经济学。

关于特约作者

Rajesh Bhandari 是一名 Cisco 网络安全解决方案架构师。作为 Cisco“自防御（Self Defending）网络”计划的一部分，他负责定义一种安全架构，该安全架构集成了各种用以构建安全网络的标准技术。在 Cisco，Rajesh 还曾担任存储网络的技术领导人、Catalyst 6000 平台的软件工程师。1999 年加盟 Cisco 前，Rajesh 曾是北电网络（Nortel Networks）光网络领域的一名软件工程师。他在加拿大维多利亚大学获得了荣誉数学学士学位。Rajesh 合写了本书第 18 章。

Steinthor Bjarnason 在冰岛大学得了计算机科学学位。2000 年加入 Cisco 前，他为世界范围的金融公司设计、实现在线交易系统。他现在是 Cisco 的一名咨询工程师，专注于集成安全解决方案和攻击预防。Steinthor 经常在诸如 Cisco Live 的 Networkers 之类的活动上发表演讲。Steinthor 撰写了本书第 12 章和第 13 章。

Ken Hook，CCNA、CCNP、CISSP，Cisco 基于身份的网络服务（IBNS）的共同创始人和最早的解决方案经理，也曾是 Cisco 内容交付网络和 Catalyst 6500 的产品经理。加入 Cisco 前，Ken 在应用系统开发、网络集成咨询和企业级项目程序管理等领域拥有 15 年的从业经历。如今，Ken 是 Cisco 集成交换安全服务计划的一名解决方案经理。Ken 合写了本书第 18 章。

Jason Fraizer 是 Cisco 技术系统工程组的一位技术领导人。他是 Cisco 基于身份网络服务计划的系统架构师和共同创始人。Jason 撰写了众多 Cisco 解决方案指南，并经常参加 Cisco Networkers 之类的行业论坛。他从事网络设计和安全已有 8 年。Jason 为本书撰写了第 17 章。

关于技术审稿人

Earl Carter 是 Cisco 的一名安全研究工程师，也是其安全技术评估团队的成员之一。他对数种 Cisco 产品进行了安全评估，这其中包括 PIX 防火墙、Cisco CallManager 的 VPN 解决方案以及其他一些 VoIP 产品。Earl 还是 Cisco Press 几本技术书籍的作者，包括《CCSP SNPA Official Exam Certification Guide Third Edition》、《Intrusion Prevention Fundamentals》、《CCSP IPS Exam Certification Guide)》以及《CCSP Self-Study: Cisco Secure Intrusion Detection System (CSIDS), Second Edition》。

Hank Mauldin 是 Cisco 安全部门的一位企业咨询工程师，在网络领域有超过 25 年（后 13 年在 Cisco）的从业经验。Hank 致力于通过与产品研发、工程、市场部门、客户以及标准组织展开跨职能协作来增强 Cisco 技术和解决方案的安全性。除了本职工作之外，Hank 还是一名为发展中国家的学生提供 Internet 路由和安全培训的 Cisco 团队成员，该团队在美国国家技术培训协会（USTTI）的指导下工作。这一为期 3 周的项目每年举办 2 次，每次 20 人。加盟 Cisco 前，Hank 曾就职于多家集成公司，专攻美国联邦和国防部的网络设计和集成。Hank 持有华盛顿特区乔治华盛顿大学信息系统技术专业的硕士学位。

致谢

本书得以出版，我们要向以下人士致谢：我们的雇主 Cisco 公司；还有我们的经理们，他们是 Jane Butler、Steve Steinhilber、Colin McMillan、Axel Clauberg、Jonathan Donaldson、Neil Anderson、Ron Tisinger，以及 Cecil Christie。没有他们的支持，本书不可能成稿。

我们也对本书的技术审稿人致谢，是他们保证了内容的质量：Earl Carter、Hank Mauldin，还有 Paul Oxman。他们为改善本书的质量投入了大量时间和精力。

另外，我们要感谢为本书作出贡献的以下 Cisco 员工：Greg Abelar、Max Ardica、Michael Behringer、Benoit Claise、Ronald Ducomble、Chris Lonvick、Fabio Maino、Francesca Martucci、David McGrew、Paddy Nallur、Troy Sherman、Dale Tesch，还有 Cisco 以外的人员：Sean Convery、Michel Fontaine、Yves Wesche（来自列日大学），以及 Michael Fine。

最后，我们要感谢我们的编辑和 Cisco Press 团队——Brett Bartow、Christopher Cleveland，以及 Dan Yang——感谢他们与我们共同工作并使本书得以按时出版。

献辞

Eric Vyncke：

献给我的妻子 Isabella，你是本书的第一个评论者，给予了我极大的支持。献给我的孩子 Pierre 和 Thibault，你们总是那样活力四射，滔滔不绝。

Chris Paggen：

献给 Nathalie、Leo 和 Nils。

Jason Frasier：

Christy，你是我的灵魂。Davis，你是我的生命之光。能和你们俩在一起，我是多么的幸运。现在我只能想象即将到来的成员会怎样充实我们的生活。献给我在 Cisco 的同事和朋友，感谢你们多年来对我的支持。

Ken Hook：

献给我的父亲 Don Hook，让我帮着出版他的近著（当然，还为了很多别的事情）。献给我的多年挚友 Shawn Wiggins。他们是我工作中灵感的源泉，激励我前进。献给我的继母 Eleanor Hook，还有 Ira Barth。仅凭文字不足以表达我对以上 4 位的感激和感谢。另外，我要感谢 Doug Gourlay、Cecil Christie，还有 Bob Gleichauf，感谢你们提供的宝贵指导和支持。

Rajesh Bhandari：

纪念我的父亲 Vijay Bhandari。我生命中取得的任何成就，都源自于他的不懈努力、爱和奉献精神。献给我的女儿 Ria：我不可能找到比你更好的朋友了。

译者序

From 孙剑

需要声明的是：本人虽然一直从事 IT 行业，但对网络的理解至多也就是“临渊羡鱼”的境界，更遑论精通了。参与本书的翻译工作，大半是因为禁不住朋友的蛊惑，还有一点沽名钓誉的私心。工作中侧重的是对原文的理解以及文字的润色，艰深一点的技术都是由搭档来把握。

本书在第二层网络安全领域的地位，读者可以自行去亚马逊网站了解，这里不再赘述。但翻译中的几点体会，还是想拿出来和大家分享。

虽然本书问世已有相当的年份，Cisco Press 却并没有为其维护勘误表。我们在翻译中发现的疑点只能通过邮件与两位作者沟通。而他们的工作异常繁忙，大部分问题都无法回应。这不能不说是本书翻译工作的一大遗憾。由于作者的母语并非英文，又都不是专职作家，用词常有失严谨，行文的逻辑性时有欠妥之处，也算是白璧微瑕吧。折腾有暇，常使我怀念起 Richard Stevens 和 Donald Knuth 等老一代专业图书作者。毕竟，“擅技术，能著文”是我们前进的方向。虽然尽了最大的努力，译文中的疏漏和错误仍是在所难免，也请有心的读者能不吝赐教。

孙剑
ahjf@msn.com
2010 年 5 月

From 孙余强

本无意翻译此书，但经不住编辑傅道坤先生的再三鼓励，这也算是对我从事网络技术工作十余年以来的一次检验。在这十余年以来，一直看人民邮电出版社引进的 Cisco Press 图书学习网络技术。可以说，自己所拥有的专业技能大多要归功于人民邮电出版社。在此一并感谢。

正如我的翻译搭档孙剑所言，本书作者的母语并非英文，行文起来晦涩难懂。但是，本书在第二层网络安全领域的地位仍然不容怀疑。当然，我们在翻译本书之时也发现了原文中的许多疏漏之处——至少也是值得推敲之处，我们也一一做注。不过，由于所注的篇幅过大，可能未必会全部收录于本书之中。如果在本书付梓之际，我们的译注没有被全部收录，请读者去人民邮电出版社的官方网站上自行下载。

最后，限于种种原因，书中难免存在疏漏和错误。读者在阅读本书的过程中如有疑问，请通过信箱与我沟通。在本书的流通周期以内，我会全力维护本书的勘误校正工作，并且在本书再版时进行一一更正。

孙余强
sunlengxie@gmail.com
2010年5月

致谢：

From 孙剑

感谢我的父母，是你们的督促让我没有放弃对英语的学习。

感谢我的妻子，许渝，你让我尝试宽容、尝试从别人的角度来看问题。

感谢我的儿子，孙晓凡，你的出现使我对人生的认识出现了转折。

From 孙余强

首先，要感谢祖国！

其次，要感谢我的搭档孙剑。没有他，本书绝不会让人读来趣味盎然。有时，我拿到他刚修改过我翻译的译稿，我都会情不自禁地哑然失笑。当年一起同事之时，若不是他鼓励我学英语，我也不会拥有现在的专业技能。在此处我同样建议读者：今天读翻译版图书，目的为了将来直接读英文版图书，做网络技术（IT技术）学好英文是第一步。

然后，要感谢我现任的领导胡国宏先生，没有他的宽宏大量，在上班时对我睁一只眼闭一只眼，本书的进度绝不会如此之快。

最后，要感谢我的父母。

本书中使用的图标


PC
终端
文件服务器
Web
服务器
路由/交换
处理器
笔记本电脑
路由器
多层交换机
Catalyst
交换机
ATM
交换机
网络云
以太网连接
串行链路连接
交换式串行连接
认证服务器
(AS)
防火墙
管道
黑客

命令语法惯例

本书命令语法遵循的惯例与 IOS 命令手册使用的惯例相同。命令手册对这些惯例的描述如下。

- **粗体字**表示照原样输入的命令和关键字，在实际的设置和输出（非常规命令语法）中，粗体字表示命令由用户手动输入（如 **show** 命令）。
- *斜体字*表示用户应提供的具体值参数。
- 竖线（|）用于分隔可选的、互斥的选项。
- 方括号（[]）表示任选项。
- 花括号（{}）表示必选项。
- 方括号中的花括号（[{}]）表示必须在任选项中选择一个。

前言

人们常认为局域网和以太网交换机与管道系统很相似，易于安装、配置。但恰恰是看似简单的东西，往往容易忽略对其安全性的关注。

以太网交换机存在着多个安全隐患[①]。利用这些隐患的攻击工具几年前就已经问世（例如著名的 dsniff 软件包）。运用这些工具，黑客可以打破交换机的所谓安全神话："不可能用嗅探和包截取技术来攻击交换机"。的确，使用 dsniff、Cain 或者其他 Windows、Linux 系统下界面友好的工具，黑客可以轻而易举地将任何流量转向他的个人计算机，从而破坏了这些流量的保密性和完整性。

对于第二层协议，从生成树协议到 IPv6 邻居发现，这些隐患中的绝大部分都是与生俱来的。一旦第二层被攻陷，再使用诸如"中间人"（MITM）攻击之类的技术在更高层协议上构建攻击手段是轻而易举的事。由于能够截取任意流量，黑客可以在明文通信（例如 HTTP 和 Telnet）和加密通道（例如 SSL 或 SSH）里做手脚。

要利用网络第二层的隐患，攻击者常常必须与攻击目标在第二层相邻。尽管听起来有些不可思议，但实际上外部黑客是可以连接到一个公司的局域网的。他可以运用社交工程出入公司场所，或是假扮成一名电话约来的工程师，来现场解决"机械故障"。

另外，很多攻击来自于公司内部员工，比如由一个在现场工作的雇员发起攻击。传统上，企业一直存在着不成文的和在某些场合是书面的规则，即认定雇员是受信任的个体。然而，过去数 10 年中无数的案件和统计数据证明，这一假设是错误的。2006 年 CSI/FBI 计算机犯罪与安全调查报告显示，受调查公司 68%的损失都部分地或完全归结于内部员工的行为不端。

一旦进入大多数组织的场所内部，取得未经授权的网络连接相对来说就容易多了：找到一个墙上闲置的以太网插口，或者一部可以断开的网络设备（例如，一台网络打印机）。考虑到 DHCP 的广泛部署，基于局域网的端口中仅有很低比例需要认证（例如 IEEE 802.1X），用户的计算机可以获得一个 IP 地址，且在绝大多数情况下，拥有了和其他合法授权用户同样的网络访问级别。获取网络中的一个 IP 地址后，恶意用户就可以尝试各种攻击手段。

有了针对网络用户的信任假定，在这一新观点的审视之下，敏感和秘密信息在网络上的流转成为不容忽视的事实。如非全部，绝大多数组织都会在其应用系统和众多文档容器中设计访问安全机制。然而，这并非万无一失。它们仅仅有助于确保适当授权的用户访问应用系统或文档容器中的信息。这些访问控制技术并不能阻止恶意用户在信息的运转过程中用在线窥探来获得信息访问权。目前，大部分在网络上流转的信

① vulnerabilities，该词在正文中，随着上下文的不同还有另外译法。——译者注

息都没有经过加密。聪明而常常是好奇的网络用户，借助于简单的脚本工具就可以轻松地在线探测到任何明文信息。这些可能是无关痛痒的会议通知，或是敏感信息：诸如用户名和密码、人力资源密或健康记录、保密客户信息、信用卡信息、合同、知识产权，甚至机密的政府信息。不言而喻，一个公司信息资产有多么重要，有时甚至是公司的中枢所在。信息的曝光、泄露对公司都是极其不利的，有时会造成严重的经济后果。公司可能在一夜间名誉扫地，随之失去忠实的客户基础。

随着设计用来暴露或者利用网络协议弱点的工具的大量涌现（诸如 Yersinia 和 Cain），在线窥探所需的知识在过去 10 年来发生了巨大的变化。在很多情况下，这些工具对内容敏感并提供了帮助菜单，这使得针对在线流转信息的窃听、篡改和回放行为更加普遍。同样，一旦获取了用户访问权限，黑客们可以利用操作系统和应用程序存在的隐患来获取或篡改信息，引发“拒绝服务”。

反言之，以太网交换机及其相关协议、特性通过采用用户识别、强制实施线速安全策略（wire speed security policy）、第二层加密等措施可以改善局域网环境的安全状态。

目的和方法

在讨论基于交换机的网络安全隐患时，首先对协议进行描述，提供隐患列表，并解释了如何防止或缓解这些隐患。由于还涵盖了运用其他特性来增强网络安全的技术，本书也会阐述这些技术并给出运用场景，并在必要时提供配置实例和屏幕截图。

读者对象

本书主要适于有以太网交换技术知识和安全基础常识的网络结构师阅读。

本书的另一类读者是信息安全主管，他们只需要对网络有最低程度的了解。由于本书对所有隐患和防范技术做了详细解释，因此不要求读者在以太网交换机方面具备专业知识。

商业机构和服务提供商也可以从本书获取有用的信息。

本书的组织结构

本书由 4 个独立部分组成。

- **第 1 部分，“安全隐患和缓解技术”**，详细解释了第二层协议中存在的几个安全缺陷以及如何防止针对这些缺陷的攻击。

  第 1 部分的各章结构相似，开篇先给出协议描述，随之是对该协议安全缺陷的细

节描述，最后以预防或缓解技术结尾。

— **第 1 章，“安全导论”**，针对网络人群给出“安全性”的介绍，对诸如保密性、完整性、可用性之类的概念给出定义，还解释了加密机制和其他密码系统。

— **第 2 章，“挫败学习型网桥的转发进程”**，重点介绍了 IEEE 802.1d 网桥的学习进程和内容寻址型内存（CAM），以太网帧就是通过它们被发往指定目的地。该进程存在着安全隐患，本章也展示了一种称作“端口安全”的缓解技术。

— **第 3 章，“攻击生成树协议”**，阐明 IEEE 802.1d 生成树是可以被攻击的，但利用诸如网桥协议数据单元防护（BPDU guard）和根防护（root guard）之类的特性能防止此类攻击。

— **第 4 章，“VLAN 安全吗”**，涵盖了 IEEE 802.1Q VLAN 标记，驳斥了“默认配置下，VLAN 之间是相互隔离”的谬论。本章演示了攻击手段，详细解释了如何通过一种安全的配置将谬论转变成为现实（例如，不允许任何从一个 VLAN 到另一个 VLAN 的跳转）。

— **第 5 章，“利用 DHCP 缺陷的攻击”**，解释了 DHCP 的一些安全隐患，以及如何运用 DHCP 窥探（DHCP snooping）特性防范网络上的恶意 DHCP 服务器。

— **第 6 章，“利用 IPv4 ARP 的攻击”**，本章首先对称为“ARP 欺骗”的 ARP（地址解析协议）安全缺陷进行了说明，接着展示了结合 DAI，如何使用 DHCP 窥探（DHCP snooping）来拦截这种攻击。

— **第 7 章，“利用 IPv6 邻居发现和路由器通告协议的攻击”**，讨论的是 IPv6 中新的辅助协议：邻居发现协议（neighbor discovery）和路由器通告协议（router advertisement），思想上很具前瞻性。这些协议中存在着与生俱来的弱点，并已被一种新协议所解决：安全邻居发现协议（secure neighbor discovery）。

— **第 8 章，“以太网上的供电呢”**，描述了以太网电力传送是什么以及该特性是否存在安全隐患。

— **第 9 章，“HSRP 适应力强吗”**，讨论了高可用性协议：热备路由器协议（Hot Standby Routing Protocol），解释了热备路由协议的安全隐患并展示了相应的缓解技术。

— **第 10 章，“能打败 VRRP 吗”**，针对基于标准的虚拟路由器冗余协议（Virtual Router Redundancy Protocol，VRRP）做了同样的分析：描述、安全性隐患和相应的缓解技术。

— **第 11 章，“Cisco 辅助协议与信息泄露”**，提供了所有辅助协议的相关信息，诸如 Cisco 发现协议（CDP，Cisco Discovery Protocol）。

■ **第 2 部分，“交换机如何抵抗拒绝服务（Denial of Service）攻击”**，深度展示了如何发现又如何缓解 DoS 攻击。

— **第 12 章，“拒绝服务攻击简介”**，介绍了 DoS 攻击，它们从哪里来，对网络有

什么实际影响。

— **第 13 章，“控制平面的监管”**，侧重于控制平面（即路由协议和管理协议运行所在的平面）的讨论。由于该平面可能遭到攻击，必须对其进行保护。控制平面的监管则被证明是实施保护的最佳技术。

— **第 14 章，“屏蔽控制平面协议”**，讨论了当无法使用控制平面的监管时（例如在老的交换机上），可以运用的技术。

— **第 15 章，“用交换机发现数据平面拒绝服务攻击（DoS）”**，利用 NetFlow 和网络分析模块（Network Analysis Module，NAM）在网络中发现拒绝服务攻击或急剧繁殖的蠕虫。早期发现（甚至在用户感知之前）的目的是更有效地应对拒绝服务攻击。

■ **第 3 部分，“用交换机来增强网络安全”**，讲述如何利用以太网交换机来实际提升局域网的安全级别。

— **第 16 章，“线速访问控制列表”**，描述了在交换机上使用访问控制列表（ACL）的场合：端口层面、VLAN 内部，或者（通常是）第三层的端口上。这些 ACL 以线速来强制实施了一种简单的安全策略。本章还对隐含在这些 ACL 背后的技术进行了阐述。

— **第 17 章，“基于身份的网络服务与 802.1X”**，讲述了在交换机上如何有效地运用 IEEE 802.1X 来实现基于端口的身份验证。文中给出了针对该协议的注意事项，以及用来避免这些限制的特性。

■ **第 4 部分，“局域网安全的下一步”**，介绍了一种新的 IEEE 协议将如何允许在第二层通信上加密。

— **第 18 章，“IEEE 802.1AE”**，描述了能以线速加密所有以太网帧的 IEEE 的新协议。

— **附录，“结合 IPSec 与 L2TP v3 实现安全伪线”**，阐明了如何结合两种比较老的协议（第二层隧道协议（L2TP）和 IP 安全协议（IPSec）），对两台交换机之间的第二层流量进行加密。

目　录

第 1 部分　安全隐患和缓解技术