Cisco Systems

ciscopress.com

第二层 VPN 体系结构

Layer 2 VPN Architectures

A complete guide to understanding, designing, and deploying Layer 2 VPN technologies and pseudowire emulation applications

[美] Wei Luo, CCIE #13291
Carlos Pignataro, CCIE #4619
Dmitry Bokotey, CCIE #4460
Anthony Chan, CCIE #10266
著

刘伟琴 米 强 译

人民邮电出版社
POSTS & TELECOM PRESS

第二层 VPN 体系结构

[美] Wei Luo，CCIE #13291
Carlos Pignataro，CCIE #4619
Dmitry Bokotey，CCIE #4460
Anthony Chan，CCIE #10266 著

刘伟琴 米 强 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

第二层 VPN 体系结构 /（美）罗（Luo,W.）等著；刘伟琴，米强译.
—北京：人民邮电出版社，2006.8

ISBN 7-115-14973-9

Ⅰ. 第… Ⅱ. ①罗…②刘…③米… Ⅲ. 虚拟网络 Ⅳ. TP393.01

版 权 声 明

第二层 VPN 体系结构

◆ 著 [美] Wei Luo，CCIE#13291
Carlos Pignataro，CCIE#4619
Dmitry Bokotey，CCIE#4460
Anthony Chan，CCIE#10266

译 刘伟琴 米 强

责任编辑 李 际

◆ 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
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：31
字数：771 千字 2006 年 8 月第 1 版
印数：1－4 000 册 2006 年 8 月北京第 1 次印刷
著作权合同登记号 图字：01-2006-0304 号
ISBN 7-115-14973-9/TP・5535

定价：65.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223

内容提要

本书介绍了第二层虚拟专用网（VPN）的概念，并通过介绍性的案例研究和广泛的设计场景，描述了第二层 VPN 技术。书中通过解释 Cisco 统一 VPN 套件中可用的两种技术——对基于 MPLS 核心的 AToM 和对本地 IP 核心的 L2TPv3——的历史和实现细节，为期望满足那些要求的读者提供帮助。本书的结构是先着重介绍第二层 VPN 的优点和实现要求，并将它们与基于第三层的 VPN 进行比较，然后以循序渐进的方式更加详细地介绍了当前可用的每种解决方案。

本书适用于从事计算机网络设计、管理和维护工作的工程技术人员阅读，可以使网络工程师和管理员快速、高效地学习 AToM 和 L2TPv3 技术。本书也可以作为高等院校计算机和通信专业的本科生和研究生学习第二层 VPN 的参考资料。

关于作者

Wei Luo（CCIE#13291）是 Cisco Systems 公司的一名技术负责人。自从 1998 年加盟 Cisco Systems 公司以来，他已经领导提出了远程访问网络、WAN 和 MPLS 等技术的许多产品设计和开发倡议。他是 Cisco 伪线仿真和第二层 VPN 产品（例如，AToM 和 VPLS）的总设计师和开发者。他积极参与 IETF 标准化过程，致力于并撰写了 IETF 工作组中的各种 RFC 和 Internet 草案。他获得了计算机科学学士学位和硕士学位。

Carlos Pignataro（CCIE#4619）在 Cisco Systems 公司升级小组担任高级工程师。在此期间，他负责处理困难而复杂的升级问题，解决关键的或者被迫停止的软件缺陷，并参与新的产品和开发过程。他获得了电子工程学学士学位和电信网络硕士学位。他致力于 IETF Internet 草案，是网络工作者大会上的一名积极演讲者。他已经为 Cisco Press 撰写了 *Cisco Multiservice Switching Networks* 一书。

Dmitry Bokotey（CCIE#4460）在路由与交换、ISP 拨号、安全和服务提供商等 4 个领域拥有 CCIE 证书。他在 Cisco Systems 公司的中心工程和 Metro 以太网小组担任网络咨询工程师。在过去的 12 年中，他为各种大型企业和服务提供商客户设计并实施了各种不同的网络环境。在其职业生涯中，他出席过许多高级网络技术主题的研讨会。他是由 Cisco Press 出版的另外两本书 *CCIE Practical Studies:Security* 和 *CCNP Practical Studies: Remote Access* 的著作者之一。

Anthony Chan，服务提供商（CCIE#10266），他为 Cisco Systems 公司的高级服务中心工程组织担任网络咨询工程师。他是 MPLS 和路由选择技术等小组的成员，为服务提供商和企业客户提供令人关注的设计和售前支持。他获得了美国西北大学的电子工程学士学位，曾供职于福特汽车公司和国际网络服务公司。

关于技术审稿人

Archana Sharma（CCIE#3080）具有 5 年以上园区交换网络的故障诊断经验。从 Cisco Systems 公司最开始发布 Catalyst 交换机以来，她就一直从事于 Catalyst 交换机的工作。自从 1995 年作为 RTP TAC 小组（该小组职能是支持 Cisco 园区交换产品线）的一名支持工程师加盟 Cisco Systems 公司以来，她一直致力于诊断和解决客户问题。在第二层交换和第三层交换方面，她都拥有丰富的故障诊断经验，而且，作为小组负责人和 Cisco 诊断工程师，她在自己的岗位上，为这些方面提供升级支持。

Aamer Akhter（CCIE#4543）1998 年毕业于佐治亚理工学院，获电子工程学学士学位，之后加盟 Cisco Systems 公司，供职于 Cisco Systems 的技术辅助中心（TAC）小组。然后在 NSA（美国国家安全局）从事对 Cisco Systems 的大型企业客户的支持工作，在此期间，他帮助设计并部署了几个大型第二层网络。后来，他又调到 Cisco Systems 的网络解决方案集成测试工程（NSITE）小组，在那里经过短暂地从事 IPSec VPN 之后，又调到一个新的小组，从事 MPLS-VPN 的测试工作。4 年之后，MPLS-VPN 已经成熟了许多，但是与 MPLS 相关技术的测试工作却仍然在继续。Aamer 目前领导着一个团队，从事于跨 Cisco 的第三层 VPN 和相关技术的测试工作。

John Chang（CCIE#2736）是 Cisco Systems 公司的一名解决方案测试主管工程师。在此岗位上，他主管在技术上对远程接入和 IP VPN 解决方案的功能、可缩放性和性能的验证工作。他拥有 20 多年的网络工程经验，已经设计、开发和支持了多种 LAN 和 WAN。他获得了电子工程学学士学位和硕士学位。

Wen Zhang（CCIE#4302）是 Cisco Systems 公司 TAC 升级小组的一名成员。目前致力于 VPN 和安全技术。自从 1997 年加盟 Cisco Systems 公司以来，他一直是 Cisco 开放论坛的一名定期撰稿人。他获得了美国克莱姆森大学电子工程学学士和硕士学位。

献　辞

Wei Luo：谨以此书献给我的母亲 Ximen，感谢她对我永远无私的热爱和信任。也将此书献给我的父亲 Jiyang Luo、我的姐姐 Michelle 和姐夫 Tong Ge，以及我可爱的外甥 Jesse 和外甥女 Lauren，感谢他们多年来为我做出的牺牲和支持以及给予我长久的爱。

Carlos Pignataro：谨以此书献给我的儿子 Luca 和妻子 Veronica，感谢他们使我的生活充满快乐。也将此书献给我记忆中的母亲 Elena Renee Goenaga，并献给我的父亲 Juan Carlos，对他们充满了衷心的感激和深深的爱。

Dmitry Bokotey：谨以此书献给我亲爱的朋友 Tom Kladek、Kevin Taylor 和 Carlos Pignataro，感谢他们为我打开了所有方便之门。

Anthony Chan：谨以此书献给我优秀的父母亲 Foon 和 Sin Ying Chan、我的哥哥 Johnny Chan 和嫂子 Diana Chu，并献给记忆中的祖母 Fung Yu Choy，感谢他们为我提供的指导和赋予我的智慧。也将此书献给我的侄女 Alicia。祝她前途光明并充满生机。

致　谢

Wei Luo：感谢 Cisco Press 所有对此书出版提供过帮助的人，特别感谢执行编辑 Brett Bartow 对我们工作的容忍。

感谢 Greg Burns、Gary Green 和 Cisco Systems 公司的其他同事，他们提供了毫无保留的支持以及特有的智慧和见识。如果不是他们的聪明才智使得第二层 VPN 成为现实，那么也就不可能有本书。

本书是真正的合作产物。感谢我的合著者们，感谢他们的艰苦劳动和无私的投入。特别要感谢的是合著者 Dmitry Bokotey，感谢他为我打开方便之门，并始终陪伴在我的身边。

Carlos Pignataro：感谢我的合著者们，感谢他们协同工作的精神和集体智慧才使得本书得以完成。感谢我们的技术审稿人，感谢他们提出了有帮助的意见。也要感谢 Cisco Systems 公司这一大家庭中想方设法实现这些技术的所有人们。

特别感谢 W. Mark Townsley，感谢他最有价值的见识与无私奉献，他给了我很多学习机会；也要特别感谢我的同事 Wen Zhang，他总是以自己的专业技术和经验帮助我找到问题的答案。

也要感谢我们的执行编辑 Brett Bartow 和开发编辑 Dayna Isley，感谢他们的敬业精神，同时也要感谢整个 Cisco Press 团队。

最后，感谢使第二层 VPN 网络保持平稳运行的所有设计工程师、网络构架师和 NOC 工程师。

Dmitry Bokotey：本书是集体努力的产物。感谢我的合著者 Anthony Chan、Wei Luo 和 Carlos Pignataro，他们的过人才能和丰富的专业知识得以使本书顺利完成。

一如继往，感谢我的妻子 Alina，感谢她帮助记录和编辑我撰写的那几章。

也要感谢 Brett Bartow 和 Cisco Press 的其他人，感谢与他们另一次富有成效的合作。真诚地感谢他们。

非常感谢 Cisco Systems 公司这一大家庭，感谢为我提供了探索和实现这一技术的机会，这成为撰写本书的基础。

最后，感谢我的母亲和父亲，感谢在我的生活中有他们的帮助；也感谢我的小 Alyssa，感谢她使得我能够出现在她的生活中。

Anthony Chan：感谢我的合著者们，感谢他们在整个过程中始终坚定不移。

感谢 Brett Bartow 和 Dayna Isley 以及 Cisco Press 的其他人员，感谢他们对我的耐心，尽管我在此过程中提出了许多额外的要求。

也要感谢 Cisco Systems 公司开发和支持 L2TPv3 和 UTI 的所有工程和体系结构小组，感谢他们创建了等效的 IP 伪线解决方案。

前　言

直到最近，VPN 前景已相当复杂，因为服务提供商已经努力致力于如何以最好的方式在公共网络基础设施上适应传统的接入技术（例如，拨号、帧中继和 ATM）和新的接入技术（例如，以太网接入和无线接入）以及第三层 VPN。一种新的解决方案，可以使服务提供商将第二层服务和第三层服务融合起来，并提供基于 IP 或者 MPLS 骨干网的遗留数据服务，此方案承诺可以使事情变得简单化，服务提供商和企业双方均可以从中受益。

遗留的第二层和第三层 VPN 解决方案在历史上的分离，使得服务提供商不得不构建、运作和维护分离的基础设施，以适应各种不同的 VPN 接入技术。但是，现在不再需要做这么昂贵的事情了。作为其新的统一 VPN 套件（Unified VPN Suite）的一部分，Cisco Systems 公司现在提供了下一代第二层 VPN 服务，例如第二层隧道协议版本 3（L2TPv3）和 MPLS 上的任意传输（AToM），它们使得服务提供商可以在公共 IP/MPLS 核心网络上提供帧中继、ATM、以太网和租用线路服务。通过统一多个网络层，并在此基础设施上提供一组集成的软件服务和管理工具，Cisco 第二层 VPN 解决方案使得传统运营商、面向 IP 的 ISP/CLEC 以及大型企业客户（LEC）能够到达范围广泛的一组潜在 VPN 客户，并提供真正的全球 VPN。

虽然第三层 MPLS VPN 可以完成某些客户的市场需求，但是，它们也存在一些缺点。那就是，第三层 MPLS VPN 只处理 IP 流量，它们要求客户将他们常用的 CPE/订户模型从第二层对等模型改变为在第三层与服务提供商对接。理想情况下，现已有遗留的第二层和第三层网络的运营商愿意向单一的骨干网移动，而新的运营商则喜欢在他们已有的第三层核心上出售有利可图的第二层服务。

这些情况的解决方案就是允许在第三层基础设施上实现第二层传输的一种技术。本书通过解释 Cisco 统一 VPN 套件中可用的两种技术（对基于 MPLS 核心的 AToM 和对本地 IP

核心的 L2TPv3）的历史和实现细节，为期望满足那些要求的读者提供帮助。

目的和方法

本书的目的是要向大家介绍与第二层 VPN 体系结构和伪线仿真相关的技术和实践，包括下面这些内容：

- 第二层 VPN 应用。
- 比较第三层与第二层提供商所提供的 VPN。
- 讨论 IETF 对伪线仿真边缘到边缘和第二层 VPN 的标准化活动。
- 描述了对控制平面信令和数据平面伪线分组进行解码所使用的机制。
- 详述并举例说明如何维护 AToM 和 L2TPv3 伪线环境中的服务质量（QoS）。
- 提供高级 AToM 主题，例如，负载共享、AS 间场景以及 VCCV。
- 描述 L2TPv3 网络中的路径 MTU 发现机制和问题。
- 介绍 VPLS 的概念、设计和配置。
- 详细介绍如何实现安全和认证。

除了描述与第二层 VPN 相关的概念外，本书还提供了一组广泛的案例研究集，向大家展示了技术和体系结构是如何工作的。这些案例研究包括 AToM 和 L2TPv3，并用实用的配置范例和实现细节揭示了现实世界服务提供商及企业设计问题和解决方案。这些案例研究包括使用 AToM 和 L2TPv3 伪线传输的所有第二层技术（包括以太网、以太网 VLAN、HDLC、PPP、帧中继、ATM AAL5 和 ATM 信元）和高级案例。

阅读完本书之后，大家应该能够理解、描述和解释第二层体系结构，并能够对使用 AToM 和 L2TPv3 的复杂网络场景进行设计、配置和故障诊断。

本书的组织结构

虽然本书可以从头到尾按顺序阅读，但是，它的设计很灵活，允许读者在各章节之间轻松地移动，找到自己所需要的内容。因此，本书遵循模块化设计。本书的几个主要部分和各章划分如下。

- **第一部分：基础知识**——本书从解释第二层 VPN 的现有市场驱动力入手，探讨了各种类型的 VPN 各自存在于什么地方。这一部分介绍了第二层 VPN 的体系结构框架和选择，并深入研究了伪线仿真的实现和细节。这一部分也描述了第二层 VPN 和伪线技术的体系结构参考模型和标准化过程，并介绍了 AToM 和 L2TPv3。
  - **第 1 章：“理解第二层 VPN”**——本章介绍了 L2VPN 和它的推动力。另外也对第二层与第三层 VPN 进行了比较。
  - **第 2 章：“伪线仿真框架和标准”**——本章展示了伪线仿真参考模型和体系结构组件，定义了关键技术，并解释了 IETF 中伪线仿真的历史和标准化过程。
  - **第 3 章：“第二层 VPN 体系结构”**——本章介绍了 AToM 和 L2TPv3，并介绍了当选择第二层 VPN 技术时要考虑的商业和技术因素。
- **第二部分：第二层协议入门知识**——这一部分完整地概述了第二层 LAN 和 WAN 技术。
  - **第 4 章：“LAN 协议”**——本章概述了 LAN 协议，例如，以太网 II 和 802.3、

以太网 dot1Q、以太网 QinQ、生成树以及相关技术。

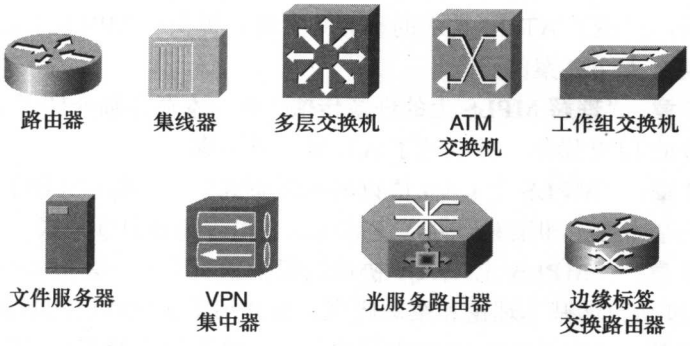
— **第 5 章：“WAN 数据链路协议”**——本章概述了不同的 WAN 协议，包括 HDLC、PPP、帧中继和 ATM。

- **第三部分：MPLS 上的任意传输**——这一部分中的几章涵盖了与 AToM 有关的 MPLS 和 LDP 在理论和操作上的细节，分析了控制平面（伪线信令）和数据平面（数据封装），描述了 AToM 技术的设计和实现，提供了 MPLS 上的 LAN 和 WAN 协议以及高级 AToM 案例研究。
  - — **第 6 章：“理解 MPLS 上的任意传输”**——本章详细介绍了 AToM 以及对伪线信令的 LDP 操作，并描述了 AToM 伪线封装。
  - — **第 7 章：“MPLS 上 LAN 协议的案例研究”**——本章介绍了 MPLS 上 LAN 协议的基本理论和案例研究，包括端到端模式和 dot1Q 模式。
  - — **第 8 章：“MPLS 上 WAN 协议的案例研究”**——本章介绍了 MPLS 上所有 WAN 协议的基本理论和案例研究，也介绍了这些协议的各种操作模型。
  - — **第 9 章：“高级 AToM 案例研究”**——本章用高级案例研究结束了 AToM 部分，例如，负载共享、优先路径选择、具有流量工程（TE）的 AToM、GRE 上的 AToM、AS 间 AToM、VCCV 和 QoS。
- **第四部分：第二层隧道技术协议版本 3**——这一部分讨论了在 IP 网络中基于第二层隧道协议版本 3（L2TPv3）的第二层协议的理论，分析了控制平面 L2TPv3 协议交互和数据平面封装细节，并提供了 LAN 和 WAN 协议以及高级案例研究。
  - — **第 10 章：“理解 L2TPv3”**——本章开始先介绍了通用传输接口（UTI）的历史和到L2TPv3的演化，然后详细介绍了L2TPv3控制平面（包括隧道、会话、cookie、AVP、控制平面消息和消息格式）和L2TPv3数据平面（包括数据分组格式）。
  - — **第 11 章：“基于 L2TPv3 的 LAN 协议案例研究”**——本章介绍了基于 L2TPv3 的 LAN 协议的基本理论和案例研究，包括对带有和不带 VLAN 重写特性的以太网端到端模式和 VLAN 模式的静态会话、带有 keepalive 的静态会话以及动态会话。
  - — **第 12 章：“基于 L2TPv3 的 WAN 协议案例研究”**——本章介绍了基于 L2TPv3 的所有 WAN 协议的基本理论和案例研究，包括 HDLC、PPP、帧中继（DLCI 模式和端口模式）和 ATM（AAL5 模式和各种信元中继模式）。
  - — **第 13 章：“高级 L2TPv3 案例研究”**——本章详细介绍了 L2TPv3 网络的高级案例研究，包括路径 MTU 发现、ATM OAM 仿真和信元打包，以及 QoS。
- **第五部分：扩展第二层 VPN 体系结构**——这一部分介绍了任意到任意（any-to-any）第二层 VPN 互通（interworking）、本地交换技术以及虚拟专用 LAN 服务（VPLS）。这一部分包括体系结构和理论上的框架，也包括配置和设计的案例研究。
  - — **第 14 章：“第二层互通与本地交换技术”**——本章介绍了第二层 IP 和以太网互通（分别为路由和桥接互通）的相关第二层 VPN 体系结构、第二层本地交换技术，以及与本地交换技术互通的组合。这一章包括 AToM 和 L2TPv3 的细节信息和案例研究。
  - — **第 15 章：“虚拟专用 LAN 服务”**——本章通过理论、配置和多个案例研究对 VPLS 应用做了介绍。

本书最后的附录部分总结了 Cisco 和 IETF L2TPv3 AVP 属性类型。

本书使用的图标

Cisco Systems 公司使用下面这些标准图标来表示不同的网络设备。在本书中将会遇到其中的一些图标。



命令语法约定

本书中用来表示命令语法的约定与 Cisco IOS 命令参考中使用的约定是相同的。命令手册中采用如下表示法：

- **粗体字** 表示按照显示的字面内容输入的命令和关键字。在实际的配置范例和输出（非命令语法）中，**粗体字**表示由用户手工输入的命令（例如 **show** 命令）。
- *斜体字* 表示需要用户提供其实际值的参数。
- 竖线（|）分开可选的、相互排斥的选项。
- 方括号（[ ]）表示可选项。
- 大括号（{ }）表示必选项。
- 方括号内的大括号（[{ }]）表示可选项中的必选项。

目　录

第一部分　基础知识

第二部分 第二层协议入门知识

第三部分 MPLS 上的任意传输

第四部分 第二层隧道技术协议版本 3