

<<IP虚拟专用网技术>>

图书基本信息

书名：<<IP虚拟专用网技术>>

13位ISBN编号：9787115174840

10位ISBN编号：7115174849

出版时间：2008-7

出版时间：人民邮电出版社

作者：何宝宏 等著

页数：324

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<IP虚拟专用网技术>>

### 内容概要

《IP虚拟专用网技术(第2版)》根据国内外最新标准和研究状况,结合目前应用和实施情况,系统地介绍了基于IP的虚拟专用网(IPVPN)技术的特点、典型隧道协议和各种VPN业务的实现方式等内容。

通过阅读《IP虚拟专用网技术(第2版)》,读者能够全面地了解IPVPN技术的原理与应用。

《IP虚拟专用网技术(第2版)》重点内容包括IPVPN的起源、概念与类型,L2TP、IPSec和MPLS等典型隧道协议,用于二层VPN(L2VPN)和一层VPN(L1VPN)的端到端伪线仿真(PWE3)协议,接入VPN、L1VPN、L2VPN和L3VPN的需求和典型实现机制,以及IPVPN应用现状和测试评估技术等,几乎覆盖了IPVPN技术和应用的各个方面以及最新进展。

## &lt;&lt;IP虚拟专用网技术&gt;&gt;

## 书籍目录

第1章 IP VPN基础1.1 VPN的起源1.1.1 专网1.1.2 ATM/FR虚拟专网1.1.3 IP VPN1.2 VPN的含义1.3 IP VPN的含义1.3.1 不透明分组传输1.3.2 数据的安全性1.3.3 服务质量保证1.3.4 隧道技术1.4 IP VPN的优势1.5 IP VPN的安全性1.6 IP VPN与隧道技术1.7 IP VPN的接入方式1.8 IP VPN的实现位置1.9 IP VPN的实施主体1.10 IP VPN业务1.11 IP VPN的典型应用1.11.1 远程接入VPN ( Access VPN ) 1.11.2 内联网VPN ( Intranet VPN ) 1.11.3 外联网VPN ( Extranet VPN ) 1.12 IP VPN的类型第2章 IP VPN业务2.1 概述2.2 通用业务要求2.2.1 客户对VPN业务的要求2.2.2 运营商对VPN业务的要求2.2.3 工程技术要求2.3 VPN业务类型2.4 L3VPN业务2.4.1 叠加模型与对等模型2.4.2 L3VPN2.4.3 基于PE的L3VPN2.4.4 基于CE的L3VPN2.5 L2VPN业务2.5.1 L2VPN的发展2.5.2 L2VPN2.5.3 VPWS2.5.4 VPLS2.5.5 IPLS2.6 L1VPN业务2.7 VPDN业务第3章 隧道协议3.1 概述3.2 二层隧道协议3.2.1 点对点隧道协议 ( PPTP ) 3.2.2 第二层转发 ( L2F ) 3.2.3 二层隧道协议 ( L2TP ) 3.2.4 多协议标记交换 ( MPLS ) 3.3 三层隧道协议3.3.1 IP中的IP ( IP in IP ) 3.3.2 通用路由封装 ( GRE ) 3.3.3 IP安全 ( IPSec ) 3.4 高层隧道协议3.4.1 安全套接层 ( SSL ) 3.4.2 SOCKS3.5 隧道协议的比较3.5.1 复用3.5.2 信令协议3.5.3 数据安全3.5.4 多协议传输3.5.5 帧排序3.5.6 隧道维护3.5.7 MTU问题3.5.8 最小隧道开销3.5.9 流量和拥塞控制3.5.10 QoS/流量管理第4章 L2TP协议4.1 概述4.2 基本协议4.2.1 协议概述4.2.2 拓扑结构4.2.3 消息类型4.2.4 报头格式4.2.5 控制消息4.2.6 属性值对4.2.7 工作流程4.2.8 数据转发4.2.9 保序机制4.2.10 连通性检测4.2.11 会话的拆除4.2.12 控制连接的拆除4.2.13 控制消息的可靠传递4.3 承载技术4.3.1 TCP/IP4.3.2 IP4.3.3 帧中继4.3.4 ATM4.4 L2TP扩展4.4.1 服务质量4.4.2 ATM接入4.4.3 多播4.4.4 隧道交换4.5 L2TPv34.6 安全性4.6.1 隧道终点的安全4.6.2 数据包级安全4.6.3 端到端安全4.6.4 L2TP与IPSec4.6.5 代理PPP认证第5章 IPSec协议5.1 概述5.2 IPSec框架结构5.2.1 协议族组成5.2.2 基本工作原理5.2.3 实现方式5.2.4 运行模式5.3 安全联盟5.3.1 定义5.3.2 功能5.3.3 SA的组合5.3.4 SA数据库5.3.5 SA的密钥管理5.4 IP流量处理5.4.1 出流量管理5.4.2 入流量管理5.5 认证头协议5.5.1 AH的目标5.5.2 AH头格式5.5.3 AH处理5.6 封装安全载荷协议5.6.1 ESP的目标5.6.2 ESP包格式5.6.3 ESP处理5.7 Internet密钥交换协议5.7.1 IKE消息格式5.7.2 IKE的密钥交换技术5.7.3 IKE的认证方式5.7.4 IKE的交换模式5.7.5 IPSec解释域5.8 IPSec最新动态第6章 MPLS技术6.1 概述6.2 MPLS技术起源6.2.1 IP/ATM融合6.2.2 融合模型6.2.3 发展简史6.2.4 多协议支持6.3 MPLS技术原理6.3.1 重要概念6.3.2 体系结构6.3.3 工作原理6.3.4 LSR结构6.3.5 MPLS与路由协议6.4 MPLS封装技术6.4.1 通用标记栈格式6.4.2 确定网络层协议6.4.3 生存期处理6.4.4 分片和路径MTU发现6.4.5 ATM标记封装6.4.6 FR标记封装6.4.7 PPP标记封装6.4.8 LAN标记封装6.5 标记分发协议6.5.1 LDP基本概念6.5.2 LDP消息类型6.5.3 LDP消息格式6.5.4 LDP基本操作6.5.5 LDP工作模式6.6 MPLS流量工程6.6.1 流量工程 ( Traffic Engineering , TE ) 6.6.2 MPLS TE6.6.3 MPLS TE概念6.6.4 约束路由6.6.5 MPLS TE实现6.6.6 CR-LDP协议6.6.7 RSVP-TE协议6.6.8 快速重路由6.6.9 CR-LSP备份6.7 MPLS技术应用6.7.1 MPLS服务质量6.7.2 MPLS VPN6.7.3 通用MPLS6.8 MPLS扩展性6.9 MPLS运维管理6.9.1 MPLS OAM概述6.9.2 MPLS OAM报文类型6.9.3 MPLS OAM主要功能第7章 PWE3技术7.1 概述7.2 协议分层模型7.2.1 PWE3框架7.2.2 分层模型7.2.3 PW分类7.3 网络参考模型7.3.1 单跳PWE3参考模型7.3.2 多跳PWE3参考模型7.3.3 预处理7.4 PWE3载荷类型7.4.1 分组业务7.4.2 信元业务7.4.3 比特流业务7.4.4 结构化比特流业务7.5 PWE3封装7.5.1 通用封装7.5.2 PWE3 over IP7.5.3 PWE3 over MPLS7.6 控制平面7.6.1 建立和拆除7.6.2 状态监视7.6.3 状态改变通知7.6.4 保活机制7.6.5 本地业务控制消息7.7 PWE3与L2VPN的关系7.7.1 控制平面的扩展7.7.2 数据平面的扩展7.8 典型业务实现7.8.1 Ethernet业务仿真7.8.2 ATM业务仿真7.9 异种介质互连7.10 PWE3拥塞控制7.10.1 IP网中的PWE3拥塞控制7.10.2 关于PW拥塞的讨论第8章 接入VPN8.1 概述8.2 VPDN优势8.3 用户管理协议8.3.1 AAA概念8.3.2 RADIUS简介8.3.3 TACACS简介8.3.4 域用户管理8.3.5 双因素认证8.4 基于RADIUS认证8.4.1 强制隧道8.4.2 基于域的隧道8.4.3 认证流程8.5 基于RADIUS计费8.6 VPDN业务8.6.1 发起方式8.6.2 系统组成8.6.3 典型流程实例第9章 L3VPN业务要求9.1 概述9.2 通用业务要求9.2.1 流量类型9.2.2 拓扑结构9.2.3 数据与路由隔离9.2.4 安全性9.2.5 地址分配9.2.6 服务质量9.2.7 服务等级规范9.2.8 管理9.2.9 互操作性9.2.10 互联互通9.3 客户的要求9.3.1 VPN成员9.3.2 运营商独立9.3.3 地址分配9.3.4 路由协议9.3.5 服务质量9.3.6 服务等级规范9.3.7 客户管理9.3.8 数据与路由隔离9.3.9 安全9.3.10 演进影响9.3.11 网络接入9.3.12 业务访问9.3.13 混合VPN9.4 运营商网络的要求9.4.1 扩展性9.4.2 地址分配9.4.3 标识符9.4.4 VPN信息学习9.4.5 服务等级规范9.4.6 服务质量9.4.7 路由9.4.8 数

## &lt;&lt;IP虚拟专用网技术&gt;&gt;

据与路由隔离9.4.9 安全9.4.10 跨域VPN9.4.11 VPN批发9.4.12 隧道封装9.4.13 接入网/骨干网9.4.14 保护恢复9.4.15 互操作性9.4.16 演进支持9.5 运营商管理的要求9.5.1 差错管理9.5.2 配置管理9.5.3 计费管理9.5.4 性能管理9.5.5 安全管理9.5.6 管理信息库9.6 安全考虑9.6.1 系统安全9.6.2 接入控制9.6.3 端点认证9.6.4 数据完整性9.6.5 保密性9.6.6 保护控制数据9.6.7 跨运营商VPN第10章 BGP/MPLS IP VPN10.1 概述10.2 网络模型10.3 基本概念10.4 VPN-IPv4地址族10.4.1 地址重叠10.4.2 地址结构10.4.3 RD编码10.4.4 RD类型10.5 VPN实例10.5.1 VRF与AC10.5.2 IP包关联10.5.3 VRF路由传播10.6 VPN目标属性10.7 VPN路由发布10.7.1 本地CE到入口PE10.7.2 入口PE到出口PE10.7.3 出口PE到远端CE10.7.4 VPN路由反射10.7.5 VRF间路由分发10.7.6 BGP AS号替换10.8 VPN数据转发10.8.1 隧道数据转发10.8.2 VPN隔离10.8.3 LDP隧道实例10.9 VPN访问控制10.9.1 Full mesh组网10.9.2 Hub&Spoke组网10.9.3 部分网状组网10.10 跨域VPN10.10.1 VRF-to-VRF跨域10.10.2 MP-EBGP跨域10.10.3 Multi-hop MP-EBGP跨域10.11 访问Internet10.11.1 非VRF访问10.11.2 VRF访问10.11.3 VRF存储非VPN路由10.11.4 VRF存储因特网路由10.12 运营商的运营商10.12.1 组网概念10.12.2 CE要求10.12.3 实现原理10.13 分层VPN10.13.1 平面/分层模型10.13.2 分层VPN原理10.13.3 SPE-UPE接口10.13.4 分层的嵌套10.13.5 多归路UPE10.13.6 UPE后门连接10.14 服务质量10.14.1 考虑因素10.14.2 资源隔离10.15 可扩展性10.15.1 VPN数量10.15.2 PE数量10.15.3 VPN接口10.15.4 VPN路由10.15.5 LSP隧道10.15.6 扩展性规划10.16 安全性10.16.1 控制平面安全10.16.2 数据平面安全10.16.3 访问控制10.16.4 安全措施第11章 L2VPN业务要求11.1 概述11.2 通用业务要求11.2.1 业务范围11.2.2 流量类型11.2.3 拓扑结构11.2.4 安全11.2.5 服务质量11.2.6 服务等级协定11.2.7 寻址11.2.8 CE到PE的链路要求11.2.9 保护和恢复11.2.10 管理11.2.11 互操作性11.2.12 互通11.3 客户要求11.3.1 独立于运营商11.3.2 支持L3流量11.3.3 QoS和业务参数11.3.4 业务等级规定11.3.5 安全性11.3.6 网络接入11.3.7 用户流量11.3.8 支持L2控制协议11.4 运营商要求11.4.1 扩展性11.4.2 标识符11.4.3 L2VPN相关信息发现11.4.4 支持SLS11.4.5 QoS11.4.6 流量和转发信息的隔离11.4.7 安全性11.4.8 跨越多个AS ( SP ) 的L2VPN11.4.9 L2VPN批发11.4.10 隧道机制要求11.4.11 接入技术的支持11.4.12 网络资源的分割和共享11.4.13 互通性11.4.14 测试11.4.15 运营商管理需求11.5 安全考虑11.5.1 运营商网络安全性问题11.5.2 运营商-用户网络安全问题11.5.3 用户网络的安全问题11.6 工程实施11.6.1 控制平面要求11.6.2 数据平面要求第12章 L2VPN的实现12.1 概述12.2 L2VPN参考模型12.2.1 L2VPN的参考模型12.2.2 VPWS的参考模型12.2.3 VPLS参考模型12.2.4 分布式VPLS-PE和VPWS-PE的参考模型12.3 VPWS业务的实现12.3.1 基于MPLS的VPWS12.3.2 Martini VPWS12.3.3 Kompella VPWS12.3.4 小结12.4 VPLS业务的实现12.4.1 VPLS-LDP ( V.Kompella ) 方式12.4.2 VPLS-BGP ( Kompella ) 方式12.4.3 两种实现的简单比较12.5 IPLS的实现12.5.1 IPLS概述12.5.2 VPLS和IPLS的对比12.5.3 IPLS的实现方式第13章 MPLS IP VPN的部署13.1 服务质量13.1.1 MPLS DiffServ13.1.2 MPLS TE13.1.3 MPLS DS-TE13.2 安全性13.2.1 安全威胁13.2.2 安全模型13.2.3 控制平面安全13.2.4 数据平面安全13.2.5 管理平面安全13.3 可靠性13.3.1 关键技术13.3.2 应用部署13.4 IPv6应用13.4.1 PE13.4.2 VPE13.4.3 两种技术对比13.5 流量统计13.5.1 系统结构13.5.2 报文格式13.5.3 输出方式13.5.4 流量提取输出13.6 小结第14章 L1VPN业务与应用14.1 概述14.2 L1VPN业务类型14.2.1 参考模型14.2.2 业务类型14.3 L1VPN业务需求14.4 L1VPN业务场景14.4.1 内容分发14.4.2 视频会议14.4.3 多业务骨干网14.4.4 运营商的运营商14.5 L1VPN参考模型14.6 L1VPN体系结构14.6.1 运营商网络侧14.6.2 用户网络侧14.7 与其他VPN的关系14.7.1 L1VPN嵌套14.7.2 L2/L3与L1的多点连接14.7.3 L2/L3与L1的C/U平面附录A IP VPN测试应用附录B MPLS VPN市场应用附录C 缩略语附录D 参考文献及网址

## <<IP虚拟专用网技术>>

### 章节摘录

第1章 IP VPN基础 1.1 VPN的起源 随着社会的进步和技术的发展，信息的分布式处理趋势越来越明显。

从20世纪70年代末期开始，在基础科学和工程领域开始使用个人计算机处理信息，这些都是在本机完成的。

在个人计算机普及和发展的基础上，局域网（LAN）技术应运而生，它在本地将公司内的多台个人计算机连接起来，实现信息在本地的共享和分布式处理。

随着局域网技术的不断发展，信息处理的应用范围也不断扩大，从本地开始延伸到跨地区、跨城市甚至是跨国家，于是出现了将地理上异地分布的计算机或LAN连接起来的广域网（WAN）技术的市场需求。

连接站点的WAN技术有两类：拨号方式和专线方式。

对于那些需要临时性接入的用户（如远程接入用户），通过拨号方式把他们与其他站点连接起来，实现“按需访问（Access On Demand）”；对于那些需要永久连接的用户（如放置企业服务器的LAN），使用租用来的专线加以连接，以保持“永远在线（Always on Line）”。

拨号方式一般使用公众交换电话网（PSTN）或综合业务数字网（ISDN）将远程用户连接到企业网。

一般而言，这是通过在一个或多个中心站点部署接入服务器（NAS）来实现的。

用户（计算机）首先拨号接入某个NAS，该NAS与认证、授权和计费（AAA）服务器交互，验证用户身份，并根据验证结果授权使用站点中的某些资源和服务。

拨号方式一般用于计算机与LAN之间或计算机与计算机之间的连接。

## <<IP虚拟专用网技术>>

### 编辑推荐

《IP虚拟专用网技术(第2版)》侧重原理性说明,力求具有理论性、实用性和系统性,适用于信息技术领域的广大工程技术人员以及大学高年级学生或研究生阅读,并可供希望系统了解IPVPN知识的其他人员参考。

<<IP虚拟专用网技术>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>