

中国海洋大学

硕士学位论文

基于L2TP的隧道协议技术在VPN中的应用研究

姓名：邵然

申请学位级别：硕士

专业：计算机技术

指导教师：姚文琳

20070601

基于 L2TP 的隧道协议技术在 VPN 中的应用研究

摘 要

由于目前对远程接入服务质量要求越来越高,经济性、安全性、数据传输可靠性成为远程接入网络发展所必需考虑的问题。本文针对目前多数企业总部与外地分支机构间高成本的远端接入服务费用的现状,提出应用基于L2TP(Layer 2 Tunneling Protocol)的隧道协议技术替代原有的通过PSTN网接入技术,应用朗讯MaxTNT远端接入服务器实现稳定可靠的VPN网络结构,

文章前面章节通过解析 VPN 技术,重点解析二层隧道协议技术,将以下 L2TP 的特点优势逐一展开研究;中间部分着重分析了 L2TP 的技术,并引入作为 L2TP 技术实现软硬件的朗讯 MaxTNT 远端接入服务器介绍;后半部分阐述了基于 L2TP 的 MaxTNT 组网结构、方案配置、源代码设置,并通过昆明电信的实际案例分析了基于 L2TP 的隧道协议技术在 VPN 改造工程中的实际应用价值。

本文从协议原理、协议结构等方面说明L2TP在VPN二层隧道协议技术中的重要性,从L2TP的自身特点及同其他二层隧道协议技术PPTP、L2F相比的优势出发,得出L2TP在二层隧道协议中的下列优点,结合朗讯MaxTNT远端接入服务器,在文章最后给出实际网络工程实例,说明基于L2TP的隧道协议技术在构建低成本,高可靠性的VPN网络中的可行性,为当前大量的大型企业信息中心部门及网络服务提供商在选择远程接入服务上提供参考。

L2TP 结合了 L2F 和 PPTP 的优点,可以让用户从客户端或接入服务器端发起 VPN 连接, L2TP 定义了利用公共网络设施封装传输链路层 PPP 帧的方法。目前用户拨号访问因特网时,必须使用 IP 协议,并且其动态得到的 IP 地址也是合法的, L2TP 的好处就在于支持多种协议,用户可以保留原来的 IPX、AppleTalk 等协议或企业原有的 IP 地址,企业在原来非 IP 网上的投资不致于浪费。另外, L2TP 还解决了多个 PPP 链路的捆绑问题, PPP 定义了多协议跨越第二层点对点链接的一个封装机制,通过对网络数据的封包和加密传输,在公网上传输私有数据、达到私有网络的安全级别,提高信息通信可靠性。

在对二层隧道协议技术及 L2TP 进行详细的技术解析后, 文章中后部分结合 L2TP 应用平台朗讯 MaxTNT 远程接入服务器, 详细地说明了实现构建、配置 L2TP 功能的方案配置, 对源代码设置进行详细解释, 给出经作者实际配置并验证的源代码方案; 最后, 通过一个实际实施的 L2TP 改造方案来说明 L2TP 在 VPN 网络改造中的可行性及有效性。

关键词: VPN, L2TP, PPTP, L2F, 二层隧道协议技术, PSTN

The Application and Research of L2TP(Layer 2 Tunneling Protocol) in VPN

Abstract

More and more people needs higher requirement of service quality on remote access now, economy, security and data transmission reliability will be new question on remote access network development. This article focuses on the current status of huge remote access service expense between most HQ and branches, provides using L2TP(Layer 2 Tunneling Protocol) technology instead of PSTN access, applying on Lucent MaxTNT to realize stable and reliable VPN network structure.

The front part of this article analyses VPN technology, especially for layer 2 tunneling protocol, discusses the following character and advantage of L2TP; The middle part analyzes L2TP technology and quotes Lucent MaxTNT which is L2TP application HW/SW environment; The rear part provides the MaxTNT to set up network structure base on L2TP, schema plan and source code configuration, using KunMing Telecom as a real case to analyze the real application value of L2TP in VPN optimization.

From the protocol principle and structure aspect, this article illuminates the importance of L2TP in VPN, compares with PPTP, L2F etc. other layer 2 tunneling protocols and explains the advantage of L2TP, provides real site network engineering case which using Lucent MaxTNT and shows the feasibility of constructing low cost and high reliability network using L2TP. Gives a reference to corporation IT dept. and ISP when choose remote access service.

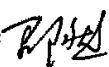
L2TP combines the advantage of PPTP and L2F, it can originate VPN connection by clients or server. L2TP defines how to encapsulate transmission link layer PPP frame using common network facility. The current way of dial up to internet is using IP protocol and its dynamic IP address is valid, L2TP supports multi protocol, users can remain the former IPX, AppleTalk etc. protocol or former IP address, so the IP address will not be wasted. On the other hand, L2TP has also solved multi-PPP binding issue. PPP is a encapsulated protocol which defines multi protocol over layer2 point to point link, via encapsulates network data and encryption transmission, transmits private data over public network, and reaches the security class of private network to improve the information telecommunication reliability.

After detailed analysis of L2TP, in the middle and rear part of this article, specifies how to set up and config L2TP feature on MaxTNT, also provides the detailed explanation on L2TP source code which is verified on real site; at last, using a real L2TP deployment case to illuminate the feasibility and validity of L2TP in VPN improvement.

Key Words: VPN, L2TP, PPTP, L2F, Layer 2 tunneling protocol, PSTN

独 创 声 明

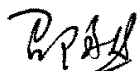
本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含未获得_____（注：如没有其他需要特别声明的，本栏可空）或其他教育机构的学位或证书使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名: 

签字日期: 2007年 6月2 日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权学校可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。（保密的学位论文在解密后适用本授权书）

学位论文作者签名: 

导师签字: 

签字日期: 2007年 6月2 日

签字日期: 2007年 6月2 日

学位论文作者毕业后去向:

工作单位: 阿尔卡特朗讯（中国）有限公司

电话: 532-88615771

通讯地址: 青岛市松岭路 169 号朗讯公司

邮编: 266000

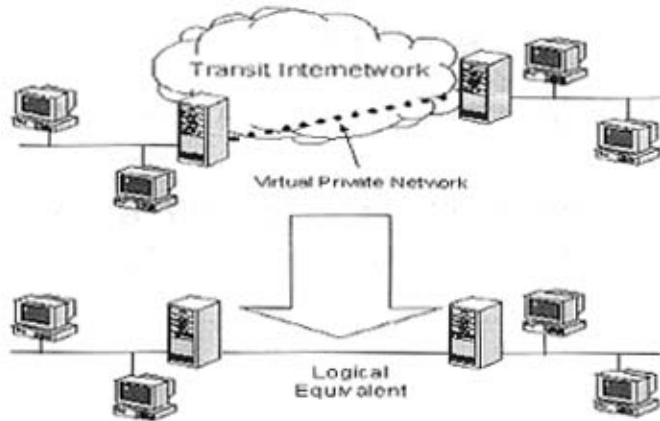
1 VPN 的现状及技术分析

全球信息化建设都处于一个高速发展的阶段，信息孤岛和信息共享安全是信息化建设过程中两个比较突出的问题，传统的专线方式，其高昂的建造费用和每月产生的运营费用，使得大量企事业单位望而却步，于是 VPN（虚拟专用网）技术成为性价比最高的解决方案。使用 VPN 技术可以解决在当今远程通讯量日益增大，企业全球运作广泛分布的情况下，员工需要访问中央资源，企业相互之间必须进行及时和有效通讯的问题。

1.1 VPN 技术

VPN（虚拟专用网）是指在公众数据网络上建立属于自己的私有数据网络。VPN 具有两个方面的含义：首先它是“虚拟”的，不再使用长途专线建立私有数据网络，而是将其建立在分布广泛的公用网络，尤其是因特网上；其次它又是一个“专网”，每个 VPN 的用户都可以临时从公用网络中获得一部分资源供自己使用。VPN 是网络基础设施，它的应用没有局限性，可以用于各个行业。主要应用于良好发展前景而且具备先进管理理念的现代企业。除了传统意义的远程连接访问以外，现代企业在享受建立内部资源共享基础上高效率的协同工作的成果或 WEB 上传下载的同时，也要面临保护内部网络及其数据安全性稳定性的严峻挑战，包括网络反病毒、防入侵、防黑客、数据丢失等。同时，基于 VPN 的应用越来越多，用户对 VPN 产品的安全稳定性能要求越来越高，对于 VPN 服务的概念要求越来越高。VPN 的发展的确能代表远程接入服务今后的发展趋势，其综合了传统数据网络的安全和服务质量，以及共享数据网络结构的简单和低成本，建立安全的数据通道。VPN 在降低成本的同时满足了用户对网络带宽、接入和服务不断增加的需求，因此，VPN 必将成为未来远程接入服务发展的主要方向【1】。

VPN 可以实现不同网络的组件和资源之间的相互连接。VPN 能够利用 Internet 或其它公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。如下图所示：



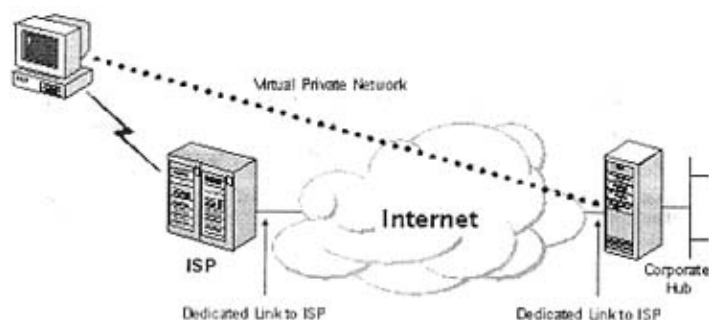
虚拟专用网络允许远程通讯方，销售人员或企业分支机构使用 Internet 等公共互联网的路由基础设施以安全的方式与位于企业局域网端的企业服务器建立连接。虚拟专用网络对用户端透明，用户好象使用一条专用线路在客户计算机和企业服务器之间建立点对点连接，进行数据的传输。虚拟专用网络技术同样支持企业通过 Internet 等公共互联网络与分支机构或其它公司建立连接，进行安全的通讯。这种跨越 Internet 建立的 VPN 连接逻辑上等同于两地之间使用广域网建立的连接。

1.2 VPN 的基本用途

下面介绍 VPN 的基本用途。

1.2.1 通过 Internet 实现远程用户访问

虚拟专用网络支持以安全的方式通过公共互联网络远程访问企业资源。



与使用专线拨打长途电话连接企业的网络接入服务器（NAS）不同，虚拟专用网络用户首先拨通本地 ISP 的 NAS，然后 VPN 软件利用与本地 ISP 建立的连接在拨号用户和企业 VPN 服务器之间创建一个跨越 Internet 或其它公共互联网络的虚拟专用网络。

1.2.3 通过 Internet 实现网络互连

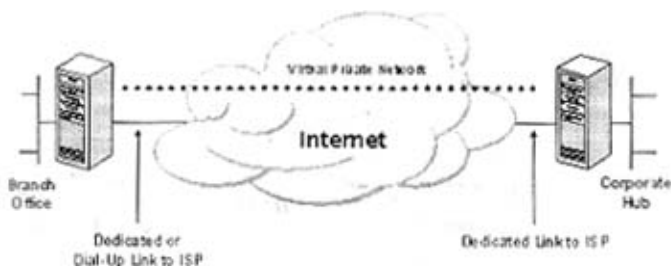
可以采用以下两种方式使用 VPN 连接远程局域网。

1. 使用专线连接分支机构和企业局域网。

不需要使用价格昂贵的长距离专用电路，分支机构和企业端路由器可以使用各自本地的专用线路通过本地的 ISP 连通 Internet。VPN 软件使用与本地 ISP 建立的连接和 Internet 网络在分支机构和企业端路由器之间创建一个虚拟专用网络。

2. 使用拨号线路连接分支机构和企业局域网。

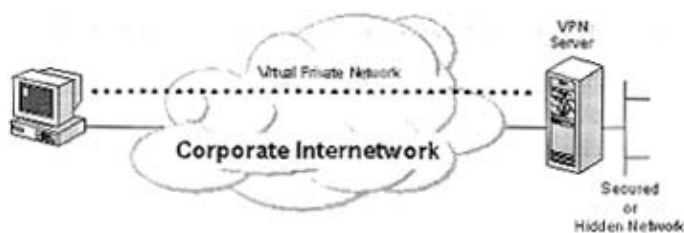
不同于传统的使用连接分支机构路由器的专线拨打长途电话连接企业 NAS 的方式，分支机构端的路由器可以通过拨号方式连接本地 ISP。VPN 软件使用与本地 ISP 建立起的连接在分支机构和企业端路由器之间创建一个跨越 Internet 的虚拟专用网络。



应当注意在以上两种方式中，是通过使用本地设备在分支机构和企业部门与 Internet 之间建立连接。无论是在客户端还是服务器端都是通过拨打本地接入电话建立连接，因此 VPN 可以大大节省连接的费用。建议作为 VPN 服务器的企业端路由器使用专线连接本地 ISP。VPN 服务器必须一天 24 小时对 VPN 数据流进行监听。

1.2.3 连接企业内部网络计算机

在企业的内部网络中，考虑到一些部门可能存储有重要数据，为确保数据的安全性，传统的方式只能是把这些部门同整个企业网络断开形成孤立的小网络。这样做虽然保护了部门的重要信息，但是由于物理上的中断，使其他部门的用户无法，造成通讯上的困难。



采用 VPN 方案，通过使用一台 VPN 服务器既能够实现与整个企业网络的连接，又可以保证保密数据的安全性。路由器虽然也能够实现网络之间的互联，但是并不能对流向敏感网络的数据进行限制。使用 VPN 服务器，但是企业网络管理人员通过使用 VPN 服务器，指

定只有符合特定身份要求的用户才能连接 VPN 服务器获得访问敏感信息的权利。此外，可以对所有 VPN 数据进行加密，从而确保数据的安全性【2】。

1.3 VPN 的基本要求

一般来说，企业在选用一种远程网络互联方案时都希望能够对访问企业资源和信息的要求加以控制，所选用的方案应当既能够实现授权用户与企业局域网资源的自由连接，不同分支机构之间的资源共享；又能够确保企业数据在公共互联网络或企业内部网络上传输时安全性不受破坏因此【3】。最低限度，一个成功的 VPN 方案应当能够满足以下所有方面的要求：

1. 用户验证

VPN 方案必须能够验证用户身份并严格控制只有授权用户才能访问 VPN。另外，方案还必须能够提供审计和计费功能，显示何人在何时访问了何种信息。

2. 地址管理

VPN 方案必须能够为用户分配专用网络上的地址并确保地址的安全性。

3. 数据加密

对通过公共互联网络传递的数据必须经过加密，确保网络其他未授权的用户无法读取该信息。

4. 密钥管理

VPN 方案必须能够生成并更新客户端和服务器的加密密钥。

5. 多协议支持

VPN 方案必须支持公共互联网络上普遍使用的基本协议，包括 IP，IPX 等。以点对点隧道协议（PPTP）或第 2 层隧道协议（L2TP）为基础的 VPN 方案既能够满足以上所有的基本要求，又能够充分利用遍及世界各地的 Internet 互联网络的优势。其它方案，包括安全 IP 协议（IPSec），虽然不能满足上述全部要求，但是仍然适用于在特定的环境。

1.4 VPN 的具体实现

VPN 的具体实现是采用隧道技术，在公网中建立企业之间的链接，将用户的数据封装在隧道中进行传输。隧道技术与接入方式无关，它可以支持各种形式的接入，如拨号方式接入、CABLE Modem、xDSL 以及 ISDN、E1 专线和无线接入等。一个隧道协议通常包括以下几个方面：

乘客协议——被封装的协议，如 PPP、SLIP；

封装协议——隧道的建立、维持和断开，如 L2TP、IPSec 等；

承载协议——承载经过封装后的数据包的协议，如 IP 和 ATM 等。

目前因特网上较为常见的隧道协议大致有两类：第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 GRE、IPSec。第二层和第三层隧道协议的区别主要在于用户数据在网络协议栈的第几层被封装。其中 GRE 和 IPSec 主要用于实现专线 VPN 业务，L2TP 主要用于实现拨号 VPN 业务，也可用于实现专线 VPN 业务。本文的其余部分分别介绍这些隧道协议。

1.5 小结

本章节重点介绍了 VPN 技术。从 VPN 技术的定义、组网结构、基本用途、基本要求以及具体实现方面介绍 VPN 技术，阐明其在远程接入服务中的作用及广泛的应用需求。在 VPN 的具体实现部分提出隧道协议技术，为下一章二层隧道协议技术的分析做好理论基础。

2 基于 L2TP 的隧道协议技术研究

本章节对二层隧道协议技术进行分析，并重点分析二层隧道协议技术中的 L2TP 技术。

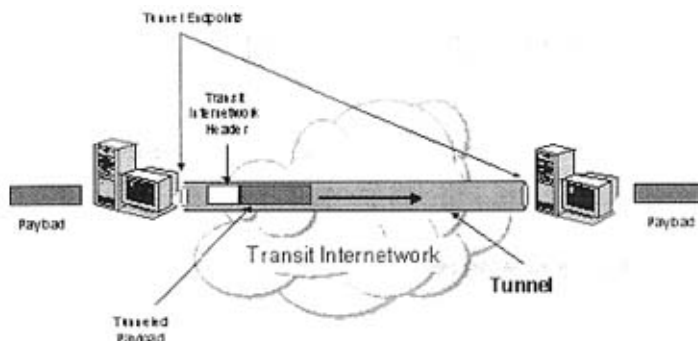
2.1 二层隧道协议技术综述

二层隧道协议技术区别于三层隧道协议技术广泛应用于 VPN 网络中，下面从隧道协议技术基础，逐步介绍隧道协议及二层隧道协议技术。本部分内容包括：隧道技术基础，二层隧道协议技术，隧道协议，隧道技术的实现，隧道协议和基本隧道要求，点对点协议，隧道类型，高级安全功能。

2.1.1 隧道技术基础

隧道技术【4】是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将这些其它协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点，数据将被解包并转发到最终目的地。注意隧道技术是指包括数据封装，传输和解包在内的全过程。



隧道所使用的传输网络可以是任何类型的公共互联网络，本文主要以目前普遍使用 Internet 为例进行说明。此外，在企业网络同样可以创建隧道。隧道技术在经过一段时间的发展和完善之后，目前较为成熟的技术包括：

1. IP 网络上的 SNA 隧道技术

当系统网络结构（SystemNetworkArchitecture）的数据流通过企业 IP 网络传送时，SNA 数据帧将被封装在 UDP 和 IP 协议包头中。

2. IP 网络上的 Novell NetWare IPX 隧道技术

当一个 IPX 数据包被发送到 NetWare 服务器或 IPX 路由器时，服务器或路由器用 UDP 和 IP 包头封装 IPX 数据包后通过 IP 网络发送。另一端的 IP-TO-IPX 路由器在去除 UDP 和 IP 包头之后，把数据包转发到 IPX 目的地。

2.1.2 二层隧道协议技术

二层隧道协议可以支持多种路由协议，如 IP、IPX 和 AppleTalk；也可以支持多种广域网技术，如帧中继、ATM、X.25 或 SDH / SONET；还可以支持任意局域网技术，如以太网、令牌环和 FDDI 等。二层隧道协议包括 PPTP、L2F 和 L2TP。

1. PPTP (Point to Point Tunneling Protocol)

点到点隧道协议 (PPTP) [5] 是由 PPTP 论坛开发的点到点的安全隧道协议, 为使用电话上网的用户提供安全 VPN 业务, 1996 年成为 IETF 草案。PPTP 是 PPP 协议的一种扩展, 提供了在 IP 网上建立多协议的安全 VPN 的通信方式, 远端用户能够通过任何支持 PPTP 的 ISP 访问企业的专用网络。PPTP 提供 PPTP 客户机和 PPTP 服务器之间的保密通信。PPTP 客户机是指运行该协议的 PC 机, PPTP 服务器是指运行该协议的服务器。

通过 PPTP, 客户可以采用拨号方式接入公共的 IP 网。拨号客户首先按常规方式拨号到 ISP 的接入服务器 (NAS), 建立 PPP 连接; 在此基础上, 客户进行二次拨号建立到 PPTP 服务器的连接, 该连接称为 PPTP 隧道, 实质上是基于 IP 协议的另一个 PPP 连接, 其中 IP 包可以封装多种协议数据, 包括 TCP / IP, IPX 和 NetBEUI。对于直接连接到 IP 网的客户则不需要第一次的 PPP 拨号连接, 可以直接与 PPTP 服务器建立虚拟通路。

PPTP 可以用于在 IP 网络上建立 PPP 会话隧道。在这种配置下, PPTP 隧道和 PPP 会话运行在两个相同的机器上, 呼叫方充当 PNS。PPTP 使用客户机-服务器结构来分离当前网络访问服务器具备的一些功能并支持虚拟专用网络。PPTP 作为一个呼叫控制和管理协议, 它允许服务器控制来自 PSTN 或 ISDN 的拨入电路交换呼叫访问并初始化外部电路交换连接。PPTP 只能通过 PAC 和 PNS 来实施, 其它系统没有必要知道 PPTP。拨号网络可与 PAC 相连接而无需知道 PPTP。标准的 PPP 客户机软件可继续在隧道 PPP 链接上操作。PPTP 使用 GRE 的扩展版本来传输用户 PPP 包。这些增强允许为在 PAC 和 PNS 之间传输用户数据的隧道提供低层拥塞控制和流控制。这种机制允许高效使用隧道可用带宽并且避免了不必要的重发和缓冲区溢出。PPTP 没有规定特定的算法用于低层控制, 但它确实定义了一些通信参数来支持这样的算法工作。

PPTP 的最大优势是 Microsoft 公司的支持。NT4.0 已经包括了 PPTP 客户机和服务器的功能, 并且考虑了 Windows95 环境。另外一个优势是它支持流量控制, 可保证客户机与服务器间不拥塞, 改善通信性能, 最大限度地减少包丢失和重发现象。PPTP 把建立隧道的主

动权交给了客户，但客户需要在其 PC 机上配置 PPTP，这样做既会增加用户的工作量，又会造成网络的安全隐患。另外，PPTP 仅工作于 IP，不具有隧道终点的验证功能，需要依赖用户的验证。

协议结构

16	32 bit
Length	PPTP Message Type
Magic Cookie	
Control Message Type	Reserved 0
Protocol Version	Reserved 1
Framing Capability	
Bearing Capability	
Maximum Channels	Firmware Revision
Host Name (64 Octets)	
Vendor String (64 Octets)	

- Length — 该 PPTP 信息的八位总长，包括整个 PPTP 头。
- PPTP Message Type — 信息类型。可能值有：1、控制信息；2、管理信息。

- Magic Cookie — Magic Cookie 以连续的 0x1A2B3C4D 进行发送，其基本目的是确保接收端与 TCP 数据流间的正确同步运行。
- Control Message Type — 可能值有：1、开始—控制—链接—请求 (Start-Control-Connection-Request)；2、开始—控制—链接—答复 (Start-Control-Connection-Reply)；3、停止—控制—链接—请求 (Stop-Control-Connection-Request)；4、停止—控制—链接—答复 (Stop-Control-Connection-Reply)；5、回音—请求 (Echo-Request)；6、回音—答复 (Echo-Reply)；
- Call Management — 可能值有：1、导出—呼叫—请求 (Outgoing-Call-Request)；2、导出—呼叫—答复 (Outgoing-Call-Reply)；3、导入—呼叫—请求 (Incoming-Call-Request)；4、导入—呼叫—答复 (Incoming-Call-Reply)；5、导入—呼叫—链接 (Incoming-Call-Connected)；6、呼叫—清除—请求 (Call-Clear-Request)；7、呼叫—断开链接—通告 (Call-Disconnect-Notify)；8、广域网—错误—通告 (WAN-Error-Notify)；
- PPP Session Control — 设置—链路—信息 (Set-Link-Info)。
- Reserved 0 & 1 — 必须设置为 0。
- Protocol Version — PPTP 版本号。
- Framing Capabilities — 指出帧类型，该信息发送方可以提供：1、异步帧支持 (Asynchronous Framing Supported)；2、同步帧支持 (Synchronous Framing Supported)。
- Bearer Capabilities — 指出承载性能，该信息发送方可以提供：1、模拟访问支持 (Analog Access Supported)；2、数字访问支持 (Digital access supported)。
- Maximum Channels — 该 PAC 可以支持的个人 PPP 会话总数。
- Firmware Revision — 若由 PAC 出发，则包括发出 PAC 时的固件修订本编号；若由 PNS 出发，则包括 PNS PPTP 驱动版本。
- Host Name — 包括发行的 PAC 或 PNS 的 DNS 名称。

Vendor Name — 包括特定供应商字符串，指当请求是由 PNS 提出时，使用的 PAC 类型或 PNS 软件类型。

2. L2F (Level 2 Forwarding)

L2F [6] 是由 Cisco 公司提出的，可以在多种介质（如 ATM、帧中继、IP）上建立多协议的安全 VPN 的通信方式。它将链路层的协议（如 HDLC、PPP、ASYNC 等）封装起来传送，因此网络的链路层完全独立于用户的链路层协议。1998 年提交给 IETF，成为 RFC2341。L2F 远端用户能够通过任何拨号方式接入公共 IP 网络。首先，按常规方式拨号到 ISP 的接入服务器（NAS），建立 PPP 连接；NAS 根据用户名等信息发起第二次连接，呼叫用户网络的服务器。这种方式下，隧道的配置和建立对用户是完全透明的。L2F 允许拨号服务器发送 PPP 帧，并通过 WAN 连接到 L2F 服务器。L2F 服务器将包去封装后，把它们接入到企业自己的网络中。与 PPTP 和 PPP 所不同的是，L2F 没有定义客户。

L2F 用于建立跨越公共网络（如因特网）的安全隧道来将 ISP POP 连接到企业内部网关。这个隧道建立了一个用户与企业客户网络间的虚拟点对点连接。L2F 允许高层协议的链路层隧道技术。使用这样的隧道，使得把原始拨号服务器位置和拨号协议连接终止与提供的网络访问位置分离成为可能。L2F 允许在其中封装 PPP/SLIP 包。ISP NAS 与家庭网关都需要共同了解封装协议，这样才能在因特网上成功地传输或接收 SLIP/PPP 包。

协议结构

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	16	24	32 bit
F	K	P	S	0	0	0	0	0	0	0	0	0	C	Version	Protocol	Sequence		
Multiplex ID																Client ID		
Length																Offset		

Key

- Version — 用于创建数据包的 L2F 软件的主修版本。
- Protocol — 协议字段，规定 L2F 数据包中传送的协议。
- Sequence — 当 L2F 头部的 S 位设置为 1 时的当前序列号。
- Multiplex ID — 数据包 Multiplex ID 用于识别一个隧道中的特殊链接。
- Client ID — Client ID (CLID) 支持解除复用隧道中的终点。
- Length — 整个数据包的长度大小（八位形式），包括头、所有字段以及有效负载。
- Offset — 该字段规定通过 L2F 协议头的字节数，协议头是有效负载数据起始位置。如果 L2F 头部的 F 位设置为 1 时，就会有该字段出现。
- Key — Key 字段出现在将 K 位设置在 L2F 协议头的情况。这属于认证过程。
- Checksum — 数据包的校验和。Checksum 字段出现在 L2F 协议头中的 C 位设置为 1 的情况。

3. L2TP (Layer 2 Tunneling Protocol)

L2TP【7】协议由 Cisco、Ascend、Microsoft、3Com 和 Bay 等厂商共同制订，1999 年 8 月公布了 L2TP 的标准 RFC 2661。上述厂商现有的 VPN 设备已具有 L2TP 的互操作性。L2TP 结合了 L2F 和 PPTP 的优点，可以让用户从客户端或接入服务器端发起 VPN 连接，L2TP 定义了利用公共网络设施封装传输链路层 PPP 帧的方法。目前用户拨号访问因特网时，必须使用 IP 协议，并且其动态得到的 IP 地址也是合法的，L2TP 的好处就在于支持多种协议，用户可以保留原来的 IPX、AppleTalk 等协议或企业原有的 IP 地址，企业在原来非 IP 网上的投资不致于浪费。另外，L2TP 还解决了多个 PPP 链路的捆绑问题，PPP 定义了多协议跨越第二层点对点链接的一个封装机制。特别地，用户通过使用众多技术之一

(如: 拨号 POTS、ISDN、ADSL 等) 获得第二层连接到网络访问服务器 (NAS)，然后在此连接上运行 PPP。在这样的配置中，第二层终端点和 PPP 会话终点处于相同的物理设备中 (如: NAS)。

L2TP 扩展了 PPP 模型，允许第二层和 PPP 终点处于不同的由包交换网络相互连接的设备来。通过 L2TP，用户在第二层连接到一个访问集中器 (如: 调制解调器池、ADSL DSLAM 等)，然后这个集中器将单独得的 PPP 帧隧道到 NAS。这样，可以把 PPP 包的实际处理过程与 L2 连接的终点分离开来。对于这样的分离，其明显的一个好处是，L2 连接可以在一个 (本地) 电路集中器上终止，然后通过共享网络如帧中继电路或英特网扩展逻辑 PPP 会话，而不用在 NAS 上终止。从用户角度看，直接在 NAS 上终止 L2 连接与使用 L2TP 没有什么功能上的区别。L2TP 协议也用来解决“多连接联选组分离”问题。多链接 PPP，一般用来集中 ISDN B 通道，需要构成多链接捆绑的所有通道在一个单网络访问服务器 (NAS) 上组合。因为 L2TP 使得 PPP 会话可以出现在接收会话的物理点之外的位置，它用来使所有的通道出现在单个的 NAS 上，并允许多链接操作，即使是在物理呼叫分散在不同物理位置的 NAS 上的情况下。

L2TP 主要由 LAC (接入集中器) 和 LNS (L2TP 网络服务器) 构成。LAC 支持客户端的 L2TP，用于发起呼叫，接收呼叫和建立隧道。LNS 是所有隧道的终点。在传统的 PPP 连接中，用户拨号连接的终点是 LAC，L2TP 使得 PPP 协议的终点延伸到 LNS。在安全性考虑上，L2TP 仅仅定义了控制包的加密传输方式，对传输中的数据并不加密，并不能完全满足用户对安全性的需求。如果需要安全的 VPN，则依然需要 IPSec。

L2TP 使用以下两种信息类型，即控制信息和数据信息。控制信息用于隧道和呼叫的建立、维持和清除。数据信息用于封装隧道所携带的 PPP 帧。控制信息利用 L2TP 中的一个可靠控制通道来确保发送。当发生包丢失时，不转发数据信息。

协议结构

L2TP 命令头:

12												16	32 bit
T	L	X	X	S	X	0	P	X	X	X	X	VER	Length
Tunnel ID												Session ID	
Ns (opt)												Nr (opt)	
Offset Size (opt)												Offset Pad (opt)	

- T — T 位表示信息类型。若是数据信息，该值为 0；若是控制信息，该值为 1。
- L — 当设置该字段时，说明 Length 字段存在，表示接收数据包的总长。对于控制信息，必须设置该值。
- X — X 位为将来扩张预留使用。在导出信息中所有预留位被设置为 0，导入信息中该值忽略。
- S — 如果设置 S 位，那么 Nr 字段和 Ns 字段都存在。对于控制信息，S 位必须设置。
- — 当设置该字段时，表示在有效负载信息中存在 Offset Size 字段。对于控制信息，该字段值设为 0。
- P — 如果 Priority (P) 位值为 1，表示该数据信息在其本地排队和传输中将会得到优先处理。
- Ver — Ver 位的值总为 002。它表示一个版本 1 L2TP 信息。
- Length — 信息总长，包括头、信息类型 AVP 以及另外的与特定控制信息类型相关的 AVPs。

- Tunnel ID — 识别控制信息应用的 Tunnel。如果对等结构还没有接收到分配的 Tunnel ID，那么 Tunnel ID 必须设置为 0。一旦接收到分配的 Tunnel ID，所有更远的数据包必须和 Tunnel ID 一起被发送。
- Call ID — 识别控制信息应用的 Tunnel 中的用户会话。如果控制信息在 Tunnel 中不应用单用户会话（例如，一个 Stop-Control-Connection-Notification 信息），Call ID 必须设置为 0。
- Nr — 期望在下一个控制信息中接收到的序列号。
- Ns — 数据或控制信息的序列号。
- Offset Size & Pad — 该字段规定通过 L2F 协议头的字节数，协议头是有效负载数据起始位置。Offset Padding 中的实际数据并没有定义。如果 Offset 字段当前存在，那么 L2TP 头 Offset Padding 的最后八位字节后结束

2.1.3 隧道协议

为创建隧道，隧道的客户机和服务器双方必须使用相同的隧道协议。

隧道技术可以分别以第 2 层或第 3 层隧道协议为基础。上述分层按照开放系统互联（OSI）的参考模型划分。第 2 层隧道协议对应 OSI 模型中的数据链路层，使用帧作为数据交换单位。PPTP、L2TP 和 L2F（第 2 层转发）都属于第 2 层隧道协议，都是将数据封装在点对点协议（PPP）帧中通过互连网络发送。第 3 层隧道协议对应 OSI 模型中的网络层，使用包作为数据交换单位。IP over IP 以及 IPSec 隧道模式都属于第 3 层隧道协议，都是将 IP 包封装在附加的 IP 包头中通过 IP 网络传送。

2.1.4 隧道技术的实现

对于象 PPTP 和 L2TP 这样的第 2 层隧道协议，创建隧道的过程类似于在双方之间建立会话；隧道的两个端点必须同意创建隧道并协商隧道各种配置变量，如地址分配，加密或

压缩等参数。绝大多数情况下，通过隧道传输的数据都使用基于数据报的协议发送。隧道维护协议被用来作为管理隧道的机制。

第 3 层隧道技术通常假定所有配置问题已经通过手工过程完成。这些协议不对隧道进行维护。与第 3 层隧道协议不同，第 2 层隧道协议（PPTP 和 L2TP）必须包括对隧道的创建，维护和终止。

隧道一旦建立，数据就可以通过隧道发送。隧道客户端和服务端使用隧道数据传输协议准备传输数据。例如，当隧道客户端向服务器端发送数据时，客户端首先给负载数据加上一个隧道数据传送协议包头，然后把封装的数据通过互联网络发送，并由互联网络将数据路由到隧道的服务器端。隧道服务器端收到数据包之后，去除隧道数据传输协议包头，然后将负载数据转发到目标网络。

2.1.5 隧道协议和基本隧道要求

因为第 2 层隧道协议（PPTP 和 L2TP）以完善的 PPP 协议为基础，因此继承了一整套的特性。

1. 用户验证

第 2 层隧道协议继承了 PPP 协议的用户验证方式。许多第 3 层隧道技术都假定在创建隧道之前，隧道的两个端点相互之间已经了解或已经经过验证。一个例外情况是 IPSec 协议的 ISAKMP 协商提供了隧道端点之间进行的相互验证。

2. 令牌卡（TokenCard）支持

通过使用扩展验证协议（EAP），第 2 层隧道协议能够支持多种验证方法，包括一次

性口令 (one-timepassword), 加密计算器 (cryptographic calculator) 和智能卡等。

第 3 层隧道协议也支持使用类似的方法, 例如, IPSec 协议通过 ISAKMP/Oakley 协商确定公共密钥证书验证。

3. 动态地址分配

第 2 层隧道协议支持在网络控制协议 (NCP) 协商机制的基础上动态分配客户地址。

第 3 层隧道协议通常假定隧道建立之前已经进行了地址分配。目前 IPSec 隧道模式下的地址分配方案仍在开发之中。

4. 数据压缩

第 2 层隧道协议支持基于 PPP 的数据压缩方式。例如, 微软的 PPTP 和 L2TP 方案使用微软点对点加密协议 (MPPE)。IETF 正在开发应用于第 3 层隧道协议的类似数据压缩机制。

5. 数据加密

第 2 层隧道协议支持基于 PPP 的数据加密机制。微软的 PPTP 方案支持在 RSA/RC4 算法的基础上选择使用 MPPE。第 3 层隧道协议可以使用类似方法, 例如, IPSec 通过 ISAKMP/Oakley 协商确定几种可选的数据加密方法。微软的 L2TP 协议使用 IPSec 加密保障隧道客户端和服务端之间数据流的安全。

6. 密钥管理

作为第 2 层协议的 MPPE 依靠验证用户时生成的密钥, 定期对其更新。IPSec 在 ISAKMP 交换过程中公开协商公用密钥, 同样对其进行定期更新。

7. 多协议支持

第 2 层隧道协议支持多种负载数据协议，从而使隧道客户能够访问使用 IP，IPX，或 NetBEUI 等多种协议企业网络。相反，第 3 层隧道协议，如 IPSec 隧道模式只能支持使用 IP 协议的目标网络。

2.1.6 点对点协议

因为第 2 层隧道协议在很大程度上依靠 PPP 协议【8】的各种特性，因此有必要对 PPP 协议进行深入的探讨。PPP 协议主要是设计用来通过拨号或专线方式建立点对点连接发送数据。PPP 协议将 IP，IPX 和 NETBEUI 封装在 PP 帧内通过点对点的链路发送。PPP 协议主要应用于连接拨号用户和 NAS。PPP 拨号会话过程可以分成 4 个不同的阶段。分别如下：

阶段 1：创建 PPP 链路

PPP 使用链路控制协议（LCP）创建，维护或终止一次物理连接。在 LCP 阶段的初期，将对基本的通讯方式进行选择。应当注意在链路创建阶段，只是对验证协议进行选择，用户验证将在第 2 阶段实现。同样，在 LCP 阶段还将确定链路对等双方是否要对使用数据压缩或加密进行协商。实际对数据压缩/加密算法和其它细节的选择将在第 4 阶段实现。

阶段 2：用户验证

在第 2 阶段，客户会 PC 将用户的身份明发给远端的接入服务器。该阶段使用一种安全验证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。大多数的 PPP 方案只提供了有限的验证方式，包括口令验证协议（PAP），挑战握手验证协议（CHAP）和微

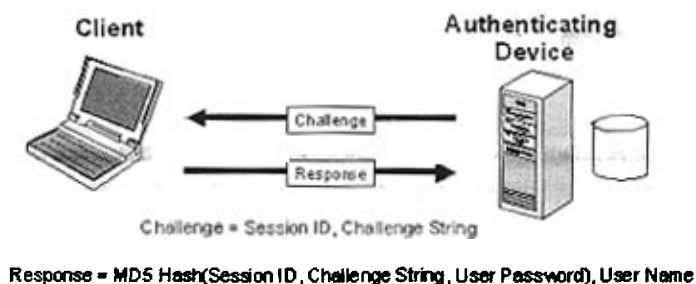
软挑战握手验证协议 (MSCHAP)。

1. 口令验证协议 (PAP)

PAP 是一种简单的明文验证方式。NAS 要求用户提供用户名和口令, PAP 以明文方式返回用户信息。很明显, 这种验证方式的安全性较差, 第三方可以很容易的获取被传送的用户名和口令, 并利用这些信息与 NAS 建立连接获取 NAS 提供的所有资源。所以, 一旦用户密码被第三方窃取, PAP 无法提供避免受到第三方攻击的保障措施。

2. 挑战-握手验证协议 (CHAP)

CHAP 是一种加密的验证方式, 能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令 (challenge), 其中包括会话 ID 和一个任意生成的挑战字符串 (arbitrary challengestring)。远程客户必须使用 MD5 单向哈希算法 (one-wayhashingalgorithm) 返回用户名和加密的挑战口令, 会话 ID 以及用户口令, 其中用户名以非哈希方式发送。



CHAP 对 PAP 进行了改进, 不再直接通过链路发送明文口令, 而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令, 所以服务器可以重复客户端进行的操作, 并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字符串来防止受到再现攻击 (replay attack)。在整个连接过程中, CHAP 将不定时的向客户端重复发送挑战口令, 从而避免第 3 方冒充远程客户 (remoteclient impersonation) 进行攻击。

3. 微软挑战-握手验证协议 (MS-CHAP)

与 CHAP 相类似, MS-CHAP 也是一种加密验证机制。同 CHAP 一样, 使用 MS-CHAP 时, NAS 会向远程客户发送一个含有会话 ID 和任意生成的挑战字串的挑战口令。远程客户必须返回用户名以及经过 MD4 哈希算法加密的挑战字串, 会话 ID 和用户口令的 MD4 哈希值。采用这种方式服务器端将只存储经过哈希算法加密的用户口令而不是明文口令, 这样就能够提供进一步的安全保障。此外, MS-CHAP 同样支持附加的错误编码, 包括口令过期编码以及允许用户自己修改口令的加密的客户-服务器 (client-server) 附加信息。使用 MS-CHAP, 客户端和 NAS 双方各自生成一个用于随后数据加密的起始密钥。MS-CHAP 使用基于 MPPE 的数据加密, 这一点非常重要, 可以解释为什么启用基于 MPPE 的数据加密时必须进行 MS-CHAP 验证。

在第 2 阶段 PPP 链路配置阶段, NAS 收集验证数据然后对照自己的数据库或中央验证数据库服务器 (位于 NT 主域控制器或远程验证用户拨入服务器) 验证数据的有效性。

阶段 3: PPP 回叫控制 (callbackcontrol)

微软设计的 PPP 包括一个可选的回叫控制阶段。该阶段在完成验证之后使用回叫控制协议 (CBCP) 如果配置使用回叫, 那么在验证之后远程客户和 NAS 之间的连接将会被断开。然后由 NAS 使用特定的电话号码回叫远程客户。这样可以进一步保证拨号网络的安全性。NAS 只支持对位于特定电话号码处的远程客户进行回叫。

阶段 4: 调用网络层协议

在以上各阶段完成之后, PPP 将调用在链路创建阶段 (阶段 1) 选定的各种网络控制协议 (NCP)。例如, 在该阶段 IP 控制协议 (IPCP) 可以向拨入用户分配动态地址。在微软的 PPP 方案中, 考虑到数据压缩和数据加密实现过程相同, 所以共同使用压缩控制协议协商数据压缩 (使用 MPPC) 和数据加密 (使用 MPPE)。

2.1.7 隧道类型

1. 自愿隧道 (Voluntarytunnel)

用户或客户端计算机可以通过发送 VPN 请求配置和创建一条自愿隧道。此时，用户端计算机作为隧道客户方成为隧道的一个端点。

2. 强制隧道 (Compulsorytunnel)

由支持 VPN 的拨号接入服务器配置和创建一条强制隧道。此时，用户端的计算机不作为隧道端点，而是由位于客户计算机和隧道服务器之间的远程接入服务器作为隧道客户端，成为隧道的一个端点。

目前，自愿隧道是最普遍使用的隧道类型【9】。以下，将对上述两种隧道类型进行详细介绍。

自愿隧道

当一台工作站或路由器使用隧道客户软件创建到目标隧道服务器的虚拟连接时建立自愿隧道。为实现这一目的，客户端计算机必须安装适当的隧道协议。自愿隧道需要有一条 IP 连接（通过局域网或拨号线路）。使用拨号方式时，客户端必须在建立隧道之前创建与公共互联网络的拨号连接。一个最典型的例子是 Internet 拨号用户必须在创建 Internet 隧道之前拨通本地 ISP 取得与 Internet 的连接。

对企业内部网络来说，客户机已经具有同企业网络的连接，由企业网络为封装负载数据提供到目标隧道服务器路由。

大多数人误认为 VPN 只能使用拨号连接。其实，VPN 只要求支持 IP 的互联网络。一些

客户机（如家用 PC）可以通过使用拨号方式连接 Internet 建立 IP 传输。这只是为创建隧道所做的初步准备，并不属于隧道协议。

强制隧道

目前，一些商家提供能够代替拨号客户创建隧道的拨号接入服务器。这些能够为客户端计算机提供隧道的计算机或网络设备包括支持 PPTP 协议的前端处理器（FEP），支持 L2TP 协议的 L2TP 接入集线器（LAC）或支持 IPSec 的安全 IP 网关。本文将主要以 FEP 为例进行说明。为正常的发挥功能，FEP 必须安装适当的隧道协议，同时必须能够当客户计算机建立起连接时创建隧道。

以 Internet 为例，客户机向位于本地 ISP 的能够提供隧道技术的 NAS 发出拨号呼叫。例如，企业可以与某个 ISP 签定协议，由 ISP 为企业在全国范围内设置一套 FEP。这些 FEP 可以通过 Internet 互联网络创建一条到隧道服务器的隧道，隧道服务器与企业的专用网络相连。这样，就可以将不同地方合并成企业网络端的一条单一的 Internet 连接。

因为客户只能使用由 FEP 创建的隧道，所以称为强制隧道。一旦最初的连接成功，所有客户端的数据流将自动的通过隧道发送。使用强制隧道，客户端计算机建立单一的 PPP 连接，当客户拨入 NAS 时，一条隧道将被创建，所有的数据流自动通过该隧道路由。可以配置 FEP 为所有的拨号客户创建到指定隧道服务器的隧道，也可以配置 FEP 基于不同的用户名或目的地创建不同的隧道。

自愿隧道技术为每个客户创建独立的隧道。FEP 和隧道服务器之间建立的隧道可以被多个拨号客户共享，而不必为每个客户建立一条新的隧道。因此，一条隧道中可能会传递多个客户的数据信息，只有在最后一个隧道用户断开连接之后才终止整条隧道。

2.1.8 高级安全功能

虽然 Internet 为创建 VPN 提供了极大的方便，但是需要建立强大的安全功能以确保企业内部网络不受到外来攻击，确保通过公共网络传送的企业数据的安全。

1. 对称加密与非对称加密（专用密钥与公用密钥）

对称加密，或专用密钥（也称做常规加密）由通信双方共享一个秘密密钥。发送方在进行数学运算时使用密钥将明文加密成密文。接受方使用相同的密钥将密文还原成明文。RSA RC4 算法，数据加密标准（DES），国际数据加密算法（IDEA）以及 Skipjack 加密技术都属于对称加密方式【10】。

非对称加密，或公用密钥，通讯各方使用两个不同的密钥，一个是只有发送方知道的专用密钥，另一个则是对应的公用密钥，任何人都可以获得公用密钥。专用密钥和公用密钥在加密算法上相互关联，一个用于数据加密，另一个用于数据解密。

公用密钥加密技术允许对信息进行数字签名。数字签名使用发送方一方的专用密钥对所发送信息的某一部分进行加密。接受方收到该信息后，使用发送方的公用密钥解密数字签名，验证发送方身份。

2. 证书

使用对称加密时，发送和接收方都使用共享的加密密钥。必须在加密通讯之前，完成密钥的分布。使用非对称加密时，发送方使用一个专用密钥加密信息或数字签名，接收方使用公用密钥解密信息。公用密钥可以自由分布给任何需要接收加密信息或数字签名信息的一方，发送方只要保证专用密钥的安全性即可。

为保证公用密钥的完整性，公用密钥随证书一同发布。证书（或公用密钥证书）是一种经过证书签发机构（CA）数字签名的数据结构。CA 使用自己的专用密钥对证书进行数字

签名。如果接受方知道 CA 的公用密钥, 就可以证明证书是由 CA 签发, 因此包含可靠的信息和有效的公用密钥。

总之, 公用密钥证书为验证发送方的身份提供了一种方便, 可靠的方法。IPSec 可以选择使用该方式进行端到端的验证。RAS 可以使用公用密钥证书验证用户身份。

3. 扩展验证协议 (EAP)

如前文所述, PPP 只能提供有限的验证方式。EAP 是由 IETF 提出的 PPP 协议的扩展, 允许连接使用任意方式对一条 PPP 连接的有效性进行验证。EAP 支持在一条连接的客户和服务器两端动态加入验证插件模块。

4. 交易层安全协议 (EAP-TLS)

EAP-TLS 已经作为提议草案提交给 IETF, 用于建立基于公用密钥证书的强大的验证方式。使用 EAP-TLS, 客户向拨入服务器发送一份用户方证书, 同时, 服务器把服务器证书发送给客户。用户证书向服务器提供了强大的用户识别信息; 服务器证书保证用户已经连接到预期的服务器。

用户方证书可以被存放在拨号客户 PC 中, 或存放在外部智能卡。无论那种方式, 如果用户不能提供没有一定形式的用户识别信息 (PIN 号或用户名和口令), 就无法访问证书。

5. IPSEC

IPSEC [11] 是一种由 IETF 设计的端到端的确保基于 IP 通讯的数据安全性的机制。IPSEC 支持对数据加密, 同时确保数据的完整性。按照 IETF 的规定, 不采用数据加密时, IPSEC 使用验证包头 (AH) 提供验证来源验证 (source authentication), 确保数据的完

完整性；IPSEC 使用封装安全负载（ESP）与加密一道提供来源验证，确保数据完整性。IPSEC 协议下，只有发送方和接受方知道秘密密钥。如果验证数据有效，接受方就可以知道数据来自发送方，并且在传输过程中没有受到破坏。

可以把 IPSEC 想象成是位于 TCP/IP 协议栈的下层协议。该层由每台机器上的安全策略和发送、接受方协商的安全关联（security association）进行控制。安全策略由一套过滤机制和关联的安全行为组成。如果一个数据包的 IP 地址，协议，和端口号满足一个过滤机制，那么这个数据包将要遵守关联的安全行为。

6. 协商安全关联（Negotiated Security Association）

上述第一个满足过滤机制的数据包将会引发发送和接收方对安全关联进行协商。ISAKMP/OAKLEY 是这种协商采用的标准协议。在一个 ISAKMP/OAKLEY 交换过程中，两台机器对验证和数据安全方式达成一致，进行相互验证，然后生成一个用于随后的数据加密的共享密钥。

7. 验证包头

通过一个位于 IP 包头和传输包头之间的验证包头可以提供 IP 负载数据的完整性和数据验证。验证包头包括验证数据和一个序列号，共同用来验证发送方身份，确保数据在传输过程中没有被改动，防止受到第三方的攻击。IPSEC 验证包头不提供数据加密；信息将以明文方式发送。

8. 封装安全包头

为了保证数据的保密性并防止数据被第 3 方窃取，封装安全负载（ESP）提供了一种对 IP 负载进行加密的机制。另外，ESP 还可以提供数据验证和数据完整性服务；因此在 IPSEC 包中可以用 ESP 包头替代 AH 包头。

9. 用户管理

在选择 VPN 技术时，一定要考虑到管理上的要求。一些大型网络都需要把每个用户的目录信息存放在一台中央数据存储设备中（目录服务）便于管理人员和应用程序对信息进行添加，修改和查询。每一台接入或隧道服务器都应当能够维护自己的内部数据库，存储每一名用户的信息，包括用户名，口令，以及拨号接入的属性等。但是，这种由多台服务器维护多个用户帐号的作法难以实现及时的更新，给管理带来很大的困难。因此，大多数的管理人员采用在目录服务器，主域控制器或 RADIUS 服务器上建立一个主帐号数据库的方法，进行有效管理。

10. RAS 支持

微软的远程接入服务器（RAS）⁴使用域控制器或 RADIUS 服务器存储每名用户的信息。因为管理员可以在单独的数据库中管理用户信息中的拨号许可信息，所以使用一台域控制器能够简化系统管理。⁵

微软的 RAS 最初被用作拨号用户的接入服务器。现在，RAS 可以作为 PPTP 和 L2TP 协议的隧道服务器（NT5 将支持 L2TP）。这些第 2 层的 VPN 方案继承了已有的拨号网络全部的管理基础。

11. 扩展性

通过使用循环 DNS 在同属一个安全地带（securityperimeter）的 VPN 隧道服务器之间进行请求分配，可以实现容余和负荷平衡。一个安全地带只具有一个对外域名，但拥有多个 IP 地址，负荷可以在所有的 IP 地址之间进行任意的分配。所有的服务器可以使用一个共享数据库，如 NT 域控制器验证访问请求。

12. RADIUS

远程验证用户拨入服务 (RADIUS) 协议【12】是管理远程用户验证和授权的常用方法。RADIUS 是一种基于 UDP 协议的超轻便 (lightweight) 协议。RADIUS 服务器可以被放置在 Internet 网络的任何地方为客户 NAS 提供验证 (包括 PPP PAP, CHAP, MSCHAP 和 EAP)。另外, RADIUS 服务器可以提供代理服务将验证请求转发到远端的 RADIUS 服务器。例如, ISP 之间相互合作, 通过使用 RADIUS 代理服务实现漫游用户在全球各地使用本地 ISP 提供的拨号服务连接 Internet 和 VPN。如果 ISP 发现用户名不是本地注册用户, 就会使用 RADIUS 代理将接入请求转发给用户的注册网络。这样企业在掌握授权权利的前提下, 有效的使用 ISP 的网络基础设施, 使企业的网络费用开支实现最小化。

13. 计费, 审计和报警

为有效的管理 VPN 系统, 网络管理人员应当能够随时跟踪和掌握以下情况: 系统的使用者, 连接数目, 异常活动, 出错情况, 以及其它可能预示出现设备故障或网络受到攻击的现象。日志记录和实时信息对计费, 审计和报警或其它错误提示具有很大帮助。例如, 网络管理人员为了编制帐单数据需要知道何人在使用系统以及使用了多长时间。异常活动可能预示着存在对系统的不正确使用或系统资源出现不足。对设备进行实时的监测可以在系统出现问题时及时向管理员发出警告。一台隧道服务器应当能够提供以上所有信息以及对数据进行正确处理所需要的事件日志, 报告和数据存储设备。

NT4.0 在 RAS 中提供了对计费, 审计和报警的支持。RADIUS 协议对呼叫-计费请求 (call-accountingrequest) 进行了规定。当 RAS 向 RADIUS 发送呼叫-计费请求后由后者建立计费记录分别记录呼叫开始, 结束以及预定中断的情况。

2.2 二层隧道协议 L2TP 的技术解析

如上一节所述, L2TP 同 PPTP 及 L2F 相比有其优点, 本小节从 L2TP 的协议结构、网络结构、L2TP 隧道协议方面详细解析 L2TP。

2.2.1 综述

隧道技术是建立安全 VPN 的基本技术之一, 类似于点对点连接技术, 在公用网建立一条数据隧道, 让数据包通过这条隧道传输。隧道是由隧道协议形成的, 分为第二、三层隧道协议。第二层隧道协议有 L2F、PPTP 和 L2TP 等, 是先把各种网络协议封装到 PPP 中, 再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第三层隧道协议有 GRE、IPSEC 等。第二层隧道协议和第三层隧道协议的本质区别在于在隧道内用户的数据包是被封装在何种数据包中进行传输的【13】。

L2TP 隧道协议是典型的被动式隧道协议, 它结合了 L2F 和 PPTP 的优点, 可以让用户从客户端或访问服务器端发起 VPN 连接。L2TP 是把链路层 PPP 帧封装在公共网络设施如 IP、ATM、帧中继中进行隧道传输的封装协议。

L2TP 主要由 LAC(L2TP Access Concentrator) 和 LNS(L2TP Network Server) 构成, LAC 支持客户端的 L2TP, 用于发起呼叫、接收呼叫和建立隧道; LNS 是所有隧道的终点, LNS 终止所有的 PPP 流。在传统的 PPP 连接中, 用户拨号连接的终点是 LAC, L2TP 使得 PPP 协议的终点延伸到 LNS。

L2TP 的好处在于支持多种协议, 用户可以保留原有的 IPX、Appletalk 等协议或公司原有的 IP 地址。L2TP 还解决了多个 PPP 链路的捆绑问题, PPP 链路捆绑要求其成员均指向同一个 NAS(Network Access Server), L2TP 可以使物理上连接到不同 NAS 的 PPP 链路, 在逻辑上的终结点为同一个物理设备。L2TP 还支持信道认证, 并提供了差错和流量控制。

L2TP 利用 IPsec 增强了安全性，支持数据包的认证、加密和密钥管理。L2TP/IPsec 因此能为远程用户提供设计精巧并有互操作性的安全隧道连接。这对安全的远程访问和安全的网关之间连接来说，它是一个很好的解决方案。因此，安全的 VPN 需要同时解决好 L2TP 和 IPsec 这两个不同的问题。L2TP 协议解决了穿过 IP 网络的不同用户协议的转换问题；IPsec 协议（加密/解密协议）解决了通过公共网络传输信息的保密问题【14】。

2.2.2 应用 L2TP 技术的网络拓扑结构

该网络结构中将 IPsec SGW(安全网关)和 LNS 合并成一个系统，即安全远程访问服务器 SRAS (Secure Remote Access Server)。这样，远程访问客户将访问唯一的节点 SRAS，该节点既是 NAS 服务的 PPP 终端，也是进入企业的安全网关节点。

至于远程访问，好处是对于穿过 Internet 的端到端 IP 包，将 IPsec 安全性当作适合企业请求的可信任模型。这样，你可以简单地使用 AH，它不存在对外来窃听的担心，你只需要验证包数据（包括包的来源）；你也可以使用 ESP（包括 ESP 验证），它不考虑对网络的信任以及任何人对公司活动窃听的问题。

SRAS 的操作要求配置防火墙允许 UDP 包进入 SRAS 节点，该节点将依次只处理 L2TP 包并丢弃其它包。而且，SRAS 将要求所有嵌入在 PPP 内的 IP 包封装成 AH 和 ESP 包之一，并指向它自身。另外，为了执行 IKE 协商和动态生成 IPsec 密钥，SRAS 也将允许 IKE UDP 包指向它自身。企业通过只允许安全远程访问包进入企业来实施安全策略，它将丢弃所有其它嵌入 PPP 内的 IP 包。当一个 PPP 会话被丢弃时，与远程访问用户相关的 IPsec 和 ISAKMP 的 SAs（安全关联）也从 SRAS 内被丢弃。这样，在捆绑 SRAS 后，SGW 和 LNS 相分离的网络结构的所有缺点都不存在了。

图 1 给出了应用 L2TP 技术的网络拓扑结构。

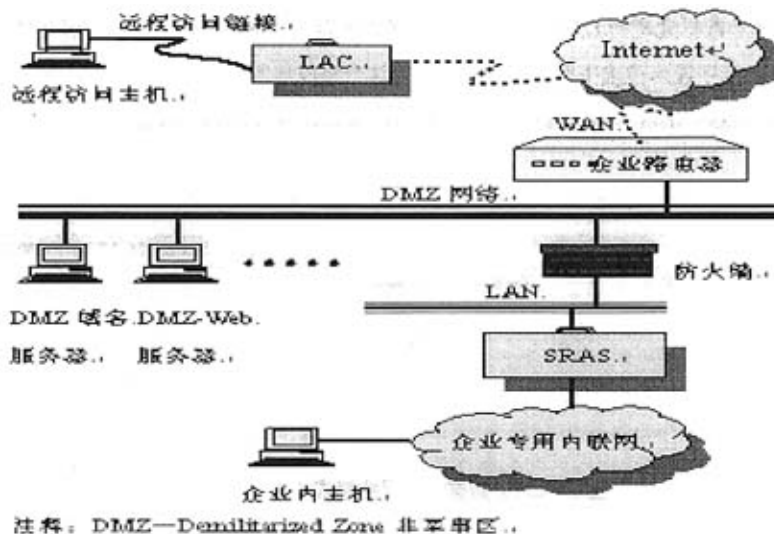


图 1 应用 L2TP 技术的网络拓扑结构

2.2.3 L2TP 报头格式

L2TP 使用两种类型的消息：控制消息和数据消息。控制消息用于隧道和呼叫的建立、维护和清除，它使用 L2TP 内的可靠控制通道来保证传送。数据消息用于封装隧道传输的 PPP 帧，当发生包丢失时不再传送数据消息。

PPP 帧先由 L2TP 报头封装，再由一种包传输机制（如 UDP、帧中继、ATM 等）封装之后在一个不可靠的数据通道上传输。但是，控制消息在一个可靠的 L2TP 控制通道上传送，这个控制通道在同一包传输机制上传送包。在所有的控制消息中都需要有序列号，序列号还用于提供控制通道上的可靠传送。数据消息可以使用序列号来重新排序数据包和检测包的丢失。

控制通道和数据通道的 L2TP 数据包的报头格式相同（如图 2 所示）。在该报头格式中，当一个可选字段未被选中时，在消息中不为这个字段预留空间。注意：当数据消息的可选项 Ns 在消息中出现（即被选中）则可选项 Nr 必须出现在所有控制消息中。

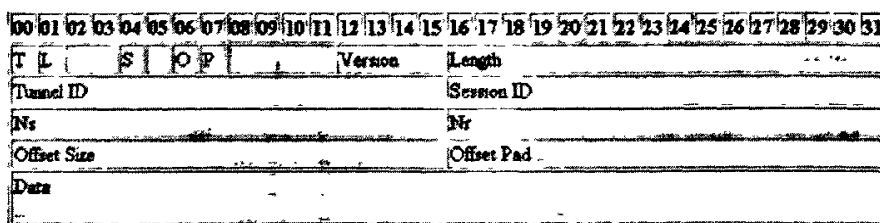


图2 L2TP数据包的报头格式

T: 消息类型，1 bit。0 数据消息；1 控制消息。

L: 长度字段出现，1 bit，可选。如果设置了这一位，则长度字段出现。控制消息中必须设置这一位。

S: 序列号出现，1 bit。如果设置了这一位，则 Ns 和 Nr 字段出现。控制消息中必须设置这一位。

O: 偏移字段出现，1 bit。如果设置了这一位，则 Offset Size 字段出现。控制消息中必须设置这一位。

P: 优先权，1 bit。这一特征只是对数据消息而言，控制消息都必须设置这一位。如果设置了这一位，则在本地排队和传输中将优先处理这个数据消息。

Version: 4 bits。指明 L2TP 协议的版本，必须被设置为 2。保留值 1 用作允许对 L2F 数据包的检测，判断是否与 L2TP 数据包一起到达。当接收到一个版本值未知的数据包时，必须丢弃这个数据包。

Length: 16 bits。指明消息的总长度，用字节表示。

Tunnel ID: 16 bits。指明控制连接的标识符。L2TP 隧道由只有本地意义的标识符命名；即，同一隧道在隧道的每一端都有不同的 Tunnel IDs。每一个消息中的 Tunnel ID 都是预定接收者而不是发送者的 Tunnel ID。在隧道创建期间，Tunnel IDs 的选择和交换都是作为 Assigned Tunnel ID AVPs (Attribute-Value Pair) 进行的。

Session ID, 16 bits. 指明一个隧道内的一次会话的标识符。L2TP 会话由只有本地意义的标识符命名；即，同一个会话在会话的每一端有不同的 Session IDs。每一个消息中的 Tunnel ID 都是预定接收者而不是发送者的 Session ID。在会话创建期间，Session IDs 的选择和交换都是作为 AssignedSession ID AVPs 进行的。

Ns: 16 bits, 可选。指明数据消息或控制消息的序列号。从 0 开始每发送一个消息加 1。

Nr: 16 bits, 可选。表明所要收到的下一个控制消息中“预定”的序列号 0。因此，Nr 被设为所接收到的最后一个消息的 Ns 加 1。若在数据消息中保留 Nr，则接收时必须忽略。

Offset/Size: 16 bits, 可选。如果出现，则指定了 L2TP 报头之后的字节数，因为载荷数据从这里开始（即载荷数据的字节数）。如果 offset 字段出现，则 L2TP-header 在 offset padding 的最后一个字节之后结束。

Offset Pad: 偏移填充，可变长度，可选。

Data: 可变长度。

2.2.4 相关技术与应用

1. 用 L2TP 控制消息维护隧道

与 PPTP 不同，L2TP 隧道的维护不在独立的 TCP 连接上进行。L2TP 呼叫控制和管理业务在 L2TP 客户和服务器之间以 UDP 消息的形式发送。在 Windows 2000 中，L2TP 客户和服务器都使用 UDP 端口 1701。值得注意的是，Windows 2000 的 L2TP 服务器也支持使用的其他 UDP 端口（UDP 端口不为 1701）的 L2TP 客户 [15]。

IP 上的 L2TP 控制消息以 UDP 数据包的形式发送。在 Windows 2000 实现中，这样的 L2TP 控制消息作为 IPSec ESP 的加密载荷发送，如图 3 所示：

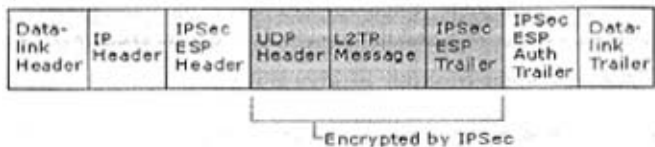


图3 Windows2000 中 L2TP 控制消息结构

因为没有使用 TCP 连接，L2TP 使用消息序列确保 L2TP 消息的传输。L2TP 控制消息中，Nr 和 Ns 字段都用于保持控制消息的次序，违反次序的数据包将被丢弃。Nr 和 Ns 字段也可用于隧道数据的顺序传送和流控制。

L2TP 的每一个隧道都支持多个呼叫。L2TP 控制消息和报头中有隧道数据的 Tunnel ID—用于指定隧道和 Call ID—用于指定这个隧道中的一次呼叫。

2. L2TP 数据的隧道传输

L2TP 数据的隧道传输是通过多级封装实现的【16】。图 4 为 IPSec 隧道数据进行 L2TP 封装之后产生的结构。

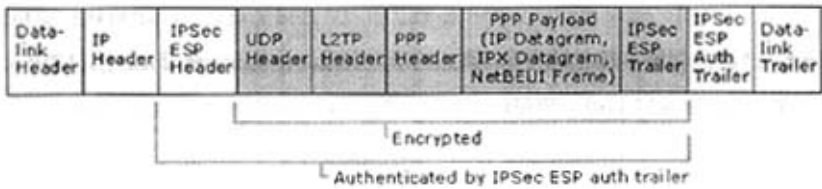


图4 L2TP 数据包的封装结构

其中, Data-Link Layer 封装是为了在 LAN 或 WAN 连接上传送, IP 数据包用数据链路层的报头和报尾封装。例如, 以太网接口上发送的 IP 数据报用以太网报头和报尾封装。当 IP 数据报在点到点 WAN 链路 (如模拟电话线或 ISDN) 上传送时, IP 数据报用一个 PPP 报头和报尾来封装。

接收到 L2TP 封装的 IPSec 隧道数据后, L2TP 客户或 L2TP 服务器将进行 L2TP 的分离处理, 过程如下:

处理并剥去数据链路层报头和报尾;

处理并剥去 IP header;

使用 IPSec ESP Auth trailer 认证 IP 载荷和 IPSec ESP 报头;

使用 IPSec ESP header 解密数据包的加密部分;

④ 处理 UDP header 并将 L2TP 数据包发给 L2TP;

L2TP 使用 L2TP header 中的 Tunnel ID 和 Call ID 确定特定的 L2TP 隧道;

使用 PPP header 确定 PPP 载荷, 并将它转发给适当的协议驱动器进行处理。

3. Windows 2000 网络体系结构中利用 L2TP 技术实现 VPN

图 5 说明了隧道传输数据在 Windows 2000 网络体系结构中从一个 VPN 客户使用一个模拟 MODEM 在远程访问 VPN 经过的过程【17】:

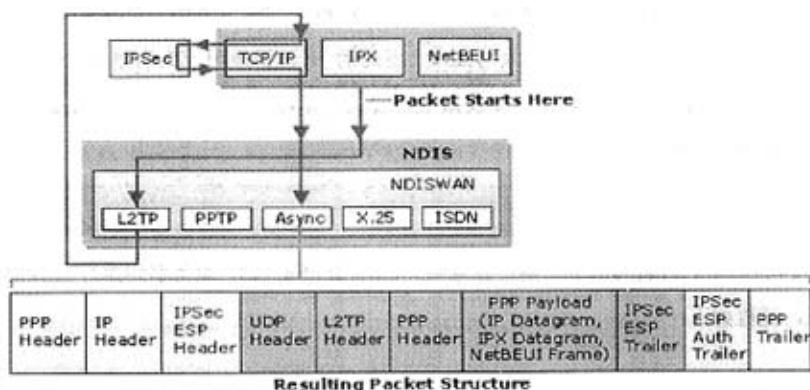


图 5 Windows 2000 中利用 L2TP 实现 VPN 的结构。

一个 IP 数据报、IPX 数据报、或 NetBEUI 帧由适当的协议发送到虚拟接口上，使用 NDIS（网络驱动器接口标准）表示 VPN 连接。NDIS 向 NDISWAN 提交一个数据包（可以是压缩过的）并提供一个只包含 PPP 协议 ID 字段的 PPP 报头，不添加 Flag 和 FCS 字段。NDISWAN 向 L2TP 协议驱动器提供 PPP 帧，由 L2TP 协议驱动器用一个 L2TP 报头封装 PPP 帧。在 L2TP 报头中，将 Tunnel ID 和 Call ID 设置成适当的值以确定 L2TP 隧道。

然后 L2TP 协议驱动器向 TCP/IP 协议驱动器提交产生的数据包，同时还要提交将 L2TP 数据包以 UDP 消息形式从 UDP 端口 1701 发送到 UDP 端口 1701，同时提交的还有 VPN 客户和服务器的 IP 地址。TCP/IP 协议驱动器用适当的 IP 报头和 UDP 报头构建一个 IP 数据包；然后 IPsec 分析这个 IP 数据包找出与之相匹配的 IPsec。IPsec 根据这个策略的设置，使用适当的 ESP 报头和报尾封装和加密 IP 数据包中的 UDP 消息部分；将 Protocol 字段设为 50 的源 IP header 添加到 ESP 数据包前面。

然后 TCP/IP 协议驱动器向使用 NDIS 表示到本地 ISP 的拨号连接的接口提交所产生的数据包。NDIS 向 NDISWAN 提交这个数据包。NDISWAN 提供 PPP 报头和报尾，并将产生的 PPP 帧提交给适当的、表示拨号硬件的 WAN miniport 驱动器。

应当注意到, 拨号连接可以和 ISP 协商一个加密的 PPP 连接, 但是不必要也不推荐这样做, 因为所发送的专用数据或隧道传输的 PPP 帧已经用 IPSec 加密了, 不需要其他层的加密, 而且这些加密会影响性能。

2.3 小结

作为论文的重点部分, 本章节对二层隧道协议技术进行详细分析, 并着重分析二层隧道协议技术中的 L2TP 协议技术。二层隧道协议技术区别于三层隧道协议技术广泛应用于 VPN 网络中, 本章从隧道协议技术基础, 逐步介绍隧道协议及二层隧道协议技术, 并对 L2TP 进行详细解析。本部分内容为了对二层隧道协议及 L2TP 进行详细说明, 从隧道技术基础、二层隧道协议技术、隧道协议、隧道技术的实现、隧道协议和基本隧道要求、点对点协议、隧道类型以及高级安全功能方面分析介绍隧道协议, 并从 L2TP 的协议结构、网络结构、L2TP 隧道协议方面详细解析 L2TP。

通过本章节的介绍, 说明了 L2TP 的技术优势和在远程接入网中的重要地位, 为远程接入网的技术改造阐明技术可行性。

3 朗讯 MaxTNT 远程接入服务器

朗讯 MaxTNT 作为远程接入服务器，可应用 L2TP 构建 VPN 网络，下面介绍朗讯 MaxTNT。

3.1 朗讯 MaxTNT 远端接入服务器简介

朗讯 MAXTNT 以其功能强劲的多协议广域网访问交换器将远程网络工业全面革新，使网络服务供应商和大企业能建立高密度的网络。这个可延伸、电信业级的交换器可同时处理多达 672 个接连以中央场点的呼叫，或在不同的动态组合访问线路，如模拟、ISDN 和 T1 或 T3 帧中继线路上使用 MegaPOP。它可被设定为多达三个格层，每个格层能提供 16 个扩展模组，以支援数码调制解调器 (Digital Modem)，混合型访问 (Hybrid Access) 或帧线模组 (Frame Line)。

采用这个模组工架构，用户可按个别应用方案和带宽的需要来制定网络基制。MAX 列软件和工业标准协议使用户能天衣无缝地将 MAXTNT 综合于现有网络环境中。而由于 MAXTNT 兼备高效能的硬件和软件功能，不但可将系统容量增至极限，同时亦可节省花在初始设备及操作上的费用。

MAXTNT 产品可以满足提供 Internet, Intranet 接入的电信运营商和大型 ISP 对用户拨号接入的要求。MAXTNT 支持 E1 接入。一台 MAXTNT 最多支持 32 根 E1/PRI 线路，能同时支持 960 个 PSTN 接入或 ISDN 接入。在满负荷的情况下，MAXTNT 的系统效率基本不受影响。MAXTNT 支持主叫号码识别，通过 Radius 协议和计费软件可以实现按主叫号码计费，用户不需要事先申请帐号，用户拨号上网后输入缺省用户名和 password，即可访问由 Radius 过滤器属性定义的网络资源，MAXTNT 也支持预付费卡业务。

MAXTNT 支持中国 7 号信令，可实现 163/169 的中继合群和 PSTN/ISDN 的中继合群。支持多种增值电信业务如：端口出租，VoIP 等 [18]。

3.2 性能特点

MAXTNT 是一项电信级的广域网接入服务器产品，它能使电信公司、Internet 服务提供商及大型企业能提供各种网络访问服务，包括模拟、ISDN、T1/E1、帧中继等，它是同级产品中最高密度的系统，能有效的节省空间及每端口的成本。

MAXTNT 的每个机架能够达到 672 个数字信道的接入能力，通过高速的数码调制解调器实现 288 个 PSTN 接入能力。采用高速的数码调制解调器，通过数码线路，如 E1 或 PRI，向拨入 MAX 的模拟用户提供全面的访问功能。MAXTNT 采用 48 端口的数码调制解调器模块来保障系统的可靠性，同时消除模拟噪音、系统失灵及使用独立的模拟调制解调技术的操作成本。

MAXTNT 支持多种协议的路由及桥接功能，如 RIP2、OSPF、IGMP 路由协议，TCP/IP 及 IPX 网络协议，所有桥接协议，PPP、SLIP、C-SLIP 终端服务，Telnet、ARA、动态 IP 地址分配服务等。可以通过不同的物理接口，连接到本地或远程的主干网上。通过 10Mbps 的以太网连接主干网。通过 V.35 串口的帧中继，达到 8MB 的连接。通过集成 CSU 的 T1/E1/PRI，实现与远程主干网的连接。

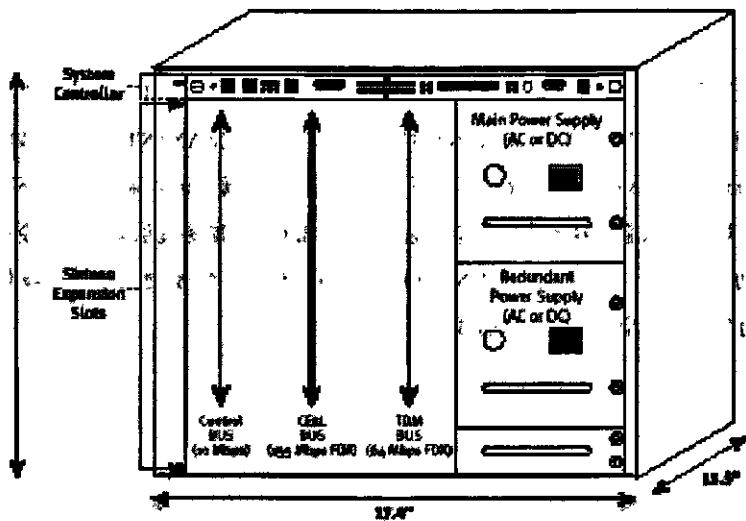
MAXTNT 通过混合访问的功能，使用户在各种访问线路上，如 PSTN、ISDN、Switched，都可获得远程访问服务。MAXTNT 支持标准的用户认证系统，如 PAP、CHAP、RADIUS、TACACS 和 TACAS+，它采用以服务器为基础认证技术使从中央站点管理大规模远程访问更为简便。扩展的 RADIUS 功能容许服务提供商和网络管理员在网络中融入记帐、认证及授权等功能。MAXTNT 还可采用安全防火墙选件，为企业网络提供全面、综合的安全方案。

MAXTNT 可选用 VPN 软件来实现 VPN 功能，可达到在 Internet 上建立安全而私有的网络效果。它采用 PPTP、ATMP、Direct IP、Direct FR 等技术来实现 VPN，作为 L2TP 标准的建立者之一，同时支持 L2TP。

MAXTNT 支持模块热插拔功能，同时提供双电源，以保证网络的可靠性。支持工业管理标准，使网络管理员可采用管理工具来监控网络，它支持标准及专用的 MIBs，同时配合简单网络管理协议(SNMP)管理软件使用，如 HP OPENVIEW。更可采用 Ascend 公司的网管软件 Netclarity 来完成对 MAXTNT 的管理。

3.3 系统硬件结构和软件结构

MAXTNT 系统采用分布式处理，每一张介质卡上都有处理能力，整个 MAXTNT 系统由控制卡加上 16 个扩展槽组成，在内部有三条总线连接介质卡和主控卡，如下图所示：



三条总线分别为控制总线，TDM 总线，CELL 总线，其中，控制总线为 10M 用来传递主控卡与接口卡的信息；TDM 总线为处理 E1 信息的 TDM 通道，最多可处理 960 个 DS0；CELL 总线为数据总线，为传递网络数据之用。两个独立的电源，可提供电源的容余备份和负载均担，可保证很强的安全性和连续有效性。

对于介质卡，每块都带有 CPU，可实现分布处理，以路由为例，主控卡计算出路由表，下载到介质卡，如以太网卡，当去往相同路径的网络流到该介质卡上时，可在该卡上完成查寻，而不用再由主控卡处理。分布式处理大大提高了系统的可靠性，提高了系统的总体性能。

MAXTNT 所采用的系统软件称为 TAOS(True Access Operation System)，是专门为接入应用而设计的软件，该软件的系统功能经过 MAX4000，MAX6000，MAXTNT 在世界各地的使用，在软件结构和系统功能方面都全面满足接入设备的服务要求。TAOS 利用 MAXTNT 高性

能的硬件，实现分布式处理功能。在软件的设计上，采用多文件、层次化设计，在 MAXTNT 的系统软件里包含两套执行映像，一个为控制卡映像，另一个为一组文件，其中每个文件驱动一种类型的介质卡，TAOS 的执行代码存在 MAXTNT 控制卡的 FLASHRAM 中，在系统引导时，控制卡经过解压缩通过系统的控制总线进入介质卡的 RAM 之中，由于采取单独的文件存储，使得 MAXTNT 任何软件模块的维护更新不会影响其它软件。

3.4 小结

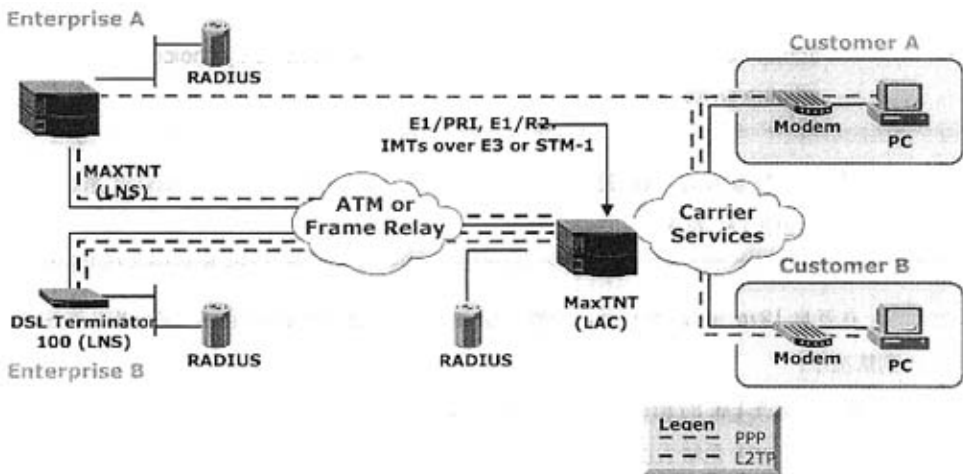
本章介绍 L2TP 应用服务器朗讯 MaxTNT，通过介绍 MaxTNT 的硬件、软件和性能特点，为下一章 L2TP 结合 MaxTNT 的应用做准备。MAXTNT 产品可以满足提供 Internet/Intranet 接入的电信运营商和大型 ISP 对用户拨号接入的要求，MAXTNT 是一项电信级的广域网接入服务器产品，它能使电信公司、Internet 服务提供商及大型企业能提供各种网络访问服务，包括模拟、ISDN、T1/E1、帧中继等，它是同级产品中最高密度的系统，能有效的节省空间及每端口的成本。

4 基于 L2TP 的 MaxTNT 组网结构及其在 VPN 工程应用中的实现

下面部分结合 L2TP，通过朗讯 MaxTNT 接入设备，介绍基于 L2TP 的二层隧道协议的组网结构以及在 VPN 工程中的具体实现。

4.1 基于 L2TP 的 MaxTNT 组网结构

如 2.2.2.1 所述，L2TP 主要由 LAC（接入集中器）和 LNS（L2TP 网络服务器）构成【19】。下图用 2 台朗讯 MaxTNT 作为 LAC 和 LNS 设备，通过配置相应的参数数据，实现 L2TP 的功能。LAC 支持客户端的 L2TP，用于发起呼叫，接收呼叫和建立隧道。LNS 是所有隧道的终点。在传统的 PPP 连接中，用户拨号连接的终点是 LAC，L2TP 使得 PPP 协议的终点延伸到 LNS【20】。



4.2 方案配置及源代码设置

下面介绍通过 L2TP 在 MaxTNT 上构建 VPN 的方案配置，并给出源代码设置。

4.2.1 方案配置

1. 激活 L2-Tunnel-Global 参数

为了启用 MaxTNT 的 LAC 功能，必须设置 L2TP 参数并配置一些全局隧道协议参数。L2-Tunnel-Global 参数是系统中用于控制 L2TP 和 PPTP 开关，下面通过设置 L2-Tunnel-Global 中的 `l2tp-mode` 参数将一台 MaxTNT 设置为 LAC，开启该台 MaxTNT 的 LAC 功能。L2-Tunnel-Global 参数下的所有子参数用于定义 LAC 的操作，不特指某一台 LNS。

```
admin> new l2-tunnel-global
admin> list
[In L2-TUNNEL-GLOBAL (new)]
pptp-enabled = no
server-profile-required = no
l2tp-mode = disabled
l2tp-auth-enabled = no
l2tp-rx-window = 0
admin> set l2tp-mode = lac          (LAC is the only choice as of 7.0.0)
admin> write
```

`l2tp-mode` 参数为开启/关闭 L2TP 的参数开关，缺省为关闭，用于 MaxTNT 系统指定 LAC 启用 L2TP LAC 操作。

在开启 `l2tp-mode` 参数后，一般还要定义 MTU（最大传送单元），定义 MTU 需注意下列情况中：

- 需定义 LAC 的 MTU 同 LNS 的 MTU 一致，
- 定义 MTU 足够大以避免数据包破碎

MTU 参数在 connection profile 中的子参数 atm-options profile 定义，用来设定 MaxTNT 在异步传输模式 ATM 的永久性虚链路 PVC 上能够传送单包的数量。可设置 128 到 1600 byte，缺省设置为 1560 byte，在此我们设置为缺省值即可。

2. 配置 Tunnel-Server

通过配置 Tunnel-Serve 参数来定义 LNS，当隧道功能被全部打开后，MaxTNT 能够向有效配置的 Tunnel-Server 发起隧道初始化请求。下面的参数通过定义 tunnel-server 的 IP 地址来指定 LNS，并通过 set enabled = yes 来激活 tunnel-server 功能。

```
admin> new tunnel-server 1.1.1.1      (IP address or the name of the LNS)
admin> list
[In TUNNEL-SERVER/1.1.1.1 (new)]
server-endpoint* = 1.1.1.1
enabled = yes
shared-secret = ""
admin> set enabled = yes
admin> write
```

tunnel-server 参数值可以是 LNS 的主机名（最多 253 字节）或 IP 地址，通常地，该项值与 tunnel-server-endpoint RADIUS 属性值相同，但是也可以不同。一旦主机名被指定了，MaxTNT 将通过 DNS 查找来得到主机地址。

3. 在 LNS 中配置 Connection Profile

LNS 的 Connection profile 定义与 LAC 呼叫连接相关的参数信息，包括鉴权设置，数据压缩及过滤设置等。MaxTNT 用 answer-defaults profile 来应答呼叫并确定是否建立一个呼叫，然后再进行查找 Connection profile 或外部鉴权服务器 RADIUS 进一步进行用户验证。

```
admin> new connection
admin> set station = MaxTNT            (name of the endpoint LNS)
admin> set active = yes
admin> set encapsulation = ppp
admin> set ip-options remote = 1.1.1.1
admin> set telco-options call-type = ft1
admin> set telco-options nailed-group = 1
admin> write
```

如上面参数设置 LNS 中配置 Connection profile 的步骤。新建 Connection profile，设置设备名称为 MaxTNT，激活 Connection profile 功能，设置数据封装协议为 PPP，远端主机地址为 1.1.1.1，呼叫类型为 ft1，nailed-group 为 1，保存。

4. 配置用户 Connection profile

配置用户 Connection profile 用来对拨入用户进行连接相关信息的设置。如果 PPP 用户 profile 被配置来发起 L2TP 隧道请求, MaxTNT 在验证鉴权连接后将会打开隧道; 具体为在使用 CLID (Calling Line ID) 主叫号码服务或 DNIS(Dialed Number Information Service)被叫号码服务用户名和密码进行预鉴权或后, 打开隧道。

如果 LAC 对用户呼叫进行预鉴权通过, 将打开隧道同 LNS 进行连接, LNS 进行所有 PPP 协商并终结 PPP 连接。即使 LAC 通过密码认证认为一个呼叫合法, 考虑到安全原因, LNS 也能够进行二次认证。LAC 和 LNS 可以使用不同的 PPP 认证协议。

```
admin> new connection
admin> set station = l2tp-client1
admin> set active = yes
admin> set clid = 555-1212 (the actual calling number)
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options tunneling-protocol = l2tp
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
admin> write

admin> new connection
admin> set station = l2tp-client2
admin> set active = yes
admin> set calledNumber = 111-2222 (the actual called number)
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options tunneling-protocol = l2tp-protocol
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
admin> write
```

5. 配置 RADIUS

对用户进行鉴权认证，除了通过定义 connection profile，还可以在 RADIUS 服务器上进行认证。如果用户数量多，在 MaxTNT 上通过定义 connection profile 需要定义大量用户数据，不便于 MaxTNT 系统维护及管理，如果将用户认证方式改为外部服务器进行认证，通过在 RADIUS 上定义用户文件，实现大量用户的有效管理，同时实现计费功能。

如果使用 RADIUS 进行认证及计费，必须在 MaxTNT 上通过下列命令定义 external-auth profile。

```
admin> new external-auth
EXTERNAL-AUTH read
admin> set auth-type = radius
admin> set acct-type = radius
admin> set rad-auth-client auth-server-1 = 2.2.2.3
admin> set rad-auth-client auth-port = 1645
admin> set rad-auth-client auth-key = key
admin> set rad-auth-client auth-timeout = 5
admin> set rad-acct-client acct-server-1 = 2.2.2.3
admin> set rad-acct-client acct-port = 1646
admin> set rad-acct-client acct-key = key
admin> set rad-acct-client acct-timeout = 5
admin> write
EXTERNAL-AUTH written
```

配置完成后，RADIUS 上用户 1112222 的认证信息如下：

```
1112222      Password=Ascend-DNIS, User-Service=Dialog-Framed-User
Tunnel-Type=L2TP,
Tunnel-Medium-Type=IP,
Tunnel-Server-Endpoint=1.1.1.1
```

Example of name and password authentication in MAXTNT unit Connection profile:

```
admin> new connection
admin> set station = l2tp-client3
admin> set active=yes
admin> set encapsulation = ppp
admin> set ppp recv-password = password
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options tunneling-protocol = l2tp-protocol
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
```

```
admin> write
```

Following is a comparable RADIUS profile using name and password authentication:

```
l2tp-client4 Password="password"
    User-Service=Framed-User,
    Framed-Protocol=PPP,
    Framed-Netmask=255.255.255.255,
    Tunnel-Type=L2TP,
    Tunnel-Medium-Type=IP,
    Tunnel-Server-Endpoint=1.1.1.1
```

4. 2. 2 源代码设置

在 MaxTNT 上实现 L2TP 功能的源代码设置如下:

```
; configuration
; saved from tntsr 11.0.6
; saved Tue Nov 14 15:48:31 2006

; saving all profiles
; saving profiles of type QOS
new QOS
write -f
;
; saving profiles of type SS7-M2UA
; saving profiles of type SS7-MTP2
; saving profiles of type SLOT-PCCTRL
; saving profiles of type APS-CONFIG
; saving profiles of type PCTFI
; saving profiles of type STM-PATH
; saving profiles of type STM
; saving profiles of type PRIVATE-ROUTE-TABLE
; saving profiles of type TRANSACTION-SERVER
new TRANSACTION-SERVER
write -f
;
; saving profiles of type SECURE-HASH
; saving profiles of type IPSEC
; saving profiles of type VOIP
; saving profiles of type DNIS
; saving profiles of type MULTI-LINK-FR
; saving profiles of type CALL-SWITCHING
```

```
new CALL-SWITCHING
write -f
;
; saving profiles of type SS7-GATEWAY
; saving profiles of type TRUNK-GROUP-PARAMS
; saving profiles of type MEDIA-GATEWAY
new MEDIA-GATEWAY
write -f
;
; saving profiles of type VROUTER
; saving profiles of type CALL-LOGGING
new CALL-LOGGING
write -f
;
; saving profiles of type ATMP
new ATMP
write -f
;
; saving profiles of type TUNNEL-SERVER
new TUNNEL-SERVER
set server-endpoint = 135.252.141.152
set shared-secret = l2test
set client-auth-id = tntlac
set server-auth-id = lns
write -f
;
new TUNNEL-SERVER
set server-endpoint = 135.252.141.153
set shared-secret = l2test
set client-auth-id = tntlac
set server-auth-id = lns
write -f
;
; saving profiles of type L2-TUNNEL-GLOBAL
new L2-TUNNEL-GLOBAL
set l2tp-mode = lac
set l2tp-system-name = tntlac
set l2tp-config default-tunnel-server = lns
set l2tp-config max-calls-per-tunnel = 50
write -f
;
; saving profiles of type EXTERNAL-AUTH
new EXTERNAL-AUTH
write -f
;
; saving profiles of type CALL-ROUTE
new CALL-ROUTE
set index device-address physical-address slot = slot-1
set call-route-type = voice-call-type
```

```
write -f
;
new CALL-ROUTE
set index device-address physical-address slot = slot-1
set index entry-number = 1
set call-route-type = digital-call-type
write -f
;
; saving profiles of type LOG
new LOG
set save-level = debug
set software-debug = yes
set call-info = end-of-call
set syslog-enabled = yes
set host = 135.252.141.130
set facility = local2
set log-call-progress = yes
set log-software-version = yes
write -f
;
; saving profiles of type IDSL
; saving profiles of type E3-ATM
; saving profiles of type OC3-ATM
; saving profiles of type ATMSVC-ROUTE
; saving profiles of type ATM-INTERFACE
; saving profiles of type DS3-ATM
; saving profiles of type UDS3
; saving profiles of type ADSL-DMT
; saving profiles of type ADSL-CAP
; saving profiles of type SDSL
; saving profiles of type SWAN
; saving profiles of type T3
; saving profiles of type DS1-CLOCK-ERROR
new DS1-CLOCK-ERROR
write -f
;
; saving profiles of type T1
new T1
set name = 4399600
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 1
set line-interface enabled = yes
set line-interface frame-type = esf
set line-interface encoding = b8zs
set line-interface clock-priority = high-priority
set line-interface signaling-mode = isdn
set line-interface channel-config 24 channel-usage = d-channel
write -f
```

```
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 2
write -f
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 3
write -f
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 4
write -f
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 5
write -f
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 6
write -f
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 7
write -f
;
new T1
set physical-address shelf = shelf-1
set physical-address slot = slot-11
set physical-address item-number = 8
write -f
;
; saving profiles of type USER-GROUP
; saving profiles of type USER
new USER
set name = admin
set password = Ascend
set allow-termserv = yes
```



```
set allow-system = yes
set allow-diagnostic = yes
set allow-update = yes
set allow-password = yes
set allow-code = yes
set allow-debug = yes
set prompt = "tnt2> "
set log-display-level = info
write -f
;
new USER
set name = default
write -f
;
; saving profiles of type IPX-SAP-FILTER
; saving profiles of type IPX-ROUTE
; saving profiles of type IP-ROUTE
new IP-ROUTE
set name = default
set gateway-address = 135.252.141.129
set metric = 1
set private-route = yes
write -f
;
; saving profiles of type SERIAL
new SERIAL
set physical-address shelf = shelf-1
set physical-address slot = controller
set physical-address item-number = 2
write -f
;
; saving profiles of type TERMINAL-SERVER
new TERMINAL-SERVER
set modem-configuration v8bis-enabled = no
write -f
;
; saving profiles of type IPX-GLOBAL
new IPX-GLOBAL
write -f
;
; saving profiles of type IPX-INTERFACE
new IPX-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 1
write -f
;
new IPX-INTERFACE
set interface-address physical-address shelf = shelf-1
```

```
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 2
write -f
;
new IPX-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 3
write -f
;
new IPX-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 4
write -f
;
new IPX-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = controller
set interface-address physical-address item-number = 1
write -f
;
; saving profiles of type LOAD-SELECT
new LOAD-SELECT
write -f
;
; saving profiles of type IP-GLOBAL
new IP-GLOBAL
set system-ip-addr = 135.252.141.132
set pool-base-address 1 = 10.10.10.1
write -f
;
; saving profiles of type IP-INTERFACE
new IP-INTERFACE
write -f
;
new IP-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 1
write -f
;
new IP-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 2
write -f
;
new IP-INTERFACE
```

```
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 3
write -f
;
new IP-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = slot-5
set interface-address physical-address item-number = 4
write -f
;
new IP-INTERFACE
set interface-address physical-address shelf = shelf-1
set interface-address physical-address slot = controller
set interface-address physical-address item-number = 1
set ip-address = 135.252.141.132/26
set netmask = 255.255.255.192
write -f
;
; saving profiles of type ETHERNET
new ETHERNET
set interface-address shelf = shelf-1
set interface-address slot = slot-5
set interface-address item-number = 1
write -f
;
new ETHERNET
set interface-address shelf = shelf-1
set interface-address slot = slot-5
set interface-address item-number = 2
write -f
;
new ETHERNET
set interface-address shelf = shelf-1
set interface-address slot = slot-5
set interface-address item-number = 3
write -f
;
new ETHERNET
set interface-address shelf = shelf-1
set interface-address slot = slot-5
set interface-address item-number = 4
write -f
;
new ETHERNET
set interface-address shelf = shelf-1
set interface-address slot = controller
set interface-address item-number = 1
write -f
```

```
; saving profiles of type BGP-POLICY
; saving profiles of type BGP-SUMMARIZATION
; saving profiles of type BGP-PEER
; saving profiles of type BGP-GLOBAL
; saving profiles of type OSPF-NBMA-NEIGHBOR
; saving profiles of type OSPF-AREA-RANGE
; saving profiles of type OSPF-VIRTUAL-LINK
; saving profiles of type CONNECTION
new CONNECTION
set station = l2test
set active = yes
set encapsulation-protocol = ppp
set ppp-options send-password = l2test
set imp-options enabled no
set calledNumber = 9600
set tunnel-options profile-type = mobile-client
set tunnel-options tunneling-protocol = l2tp-protocol
set tunnel-options max-tunnels = 4
set tunnel-options primary-tunnel-server = 135.252.141.152
set tunnel-options secondary-tunnel-server = 135.252.141.153
set tunnel-options password = l2test
set tunnel-options client-auth-id = tntlac
set tunnel-options server-auth-id = lns
write -f
;
; profiles saved
```

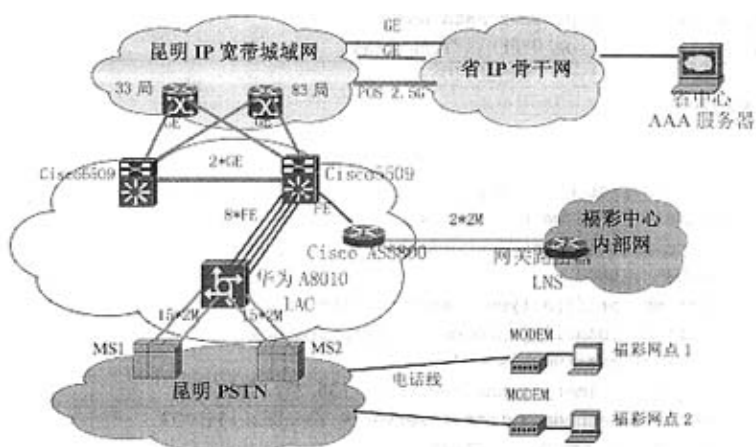
4.3 基于 L2TP 的隧道协议技术在 VPN 工程中的应用

下面以本人负责实施的昆明 VPN 改造扩容工程为例说明基于 L2TP 的隧道协议技术在 VPN 中的应用 [21]。

4.3.1 昆明 IP 网（窄带部分）VPN 网络现状

目前昆明 IP 网（窄带部分）VPN 网络 PSTN/ISDN 使用一台华为 A8010 接入服务器负责接入，与本地交换网络 MS1、MS2 局之间各有 15 条 2M 中继相连，信令采用 SS7，可同时接入 500 个 VPN 拨号用户。数据网络侧接入昆明 163 平台。用户接入号码为 16306，组网使用 L2TP 协议及强制隧道方式，即由电信运营商的接入服务器（A8010）根据 AAA 服务器返回的隧道参数与客户中心路由器建立 L2TP 隧道。AAA 服务器位于省数据网管中心，并由其负责制作客户的相关隧道参数。客户中心路由器使用 2

个 2M 专线与电信 IP 网络相连，用户接入内网的第二次认证目前（如福彩）也是由电信的 AAA 服务器进行的。网络示意图如下：



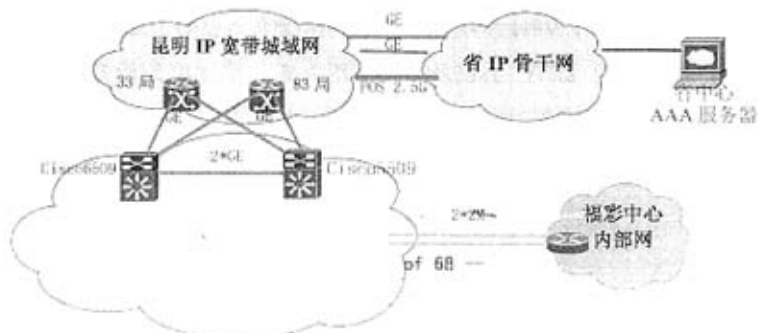
4.3.2 本次升级改造满足的业务需求及 L2TP 改造的优势

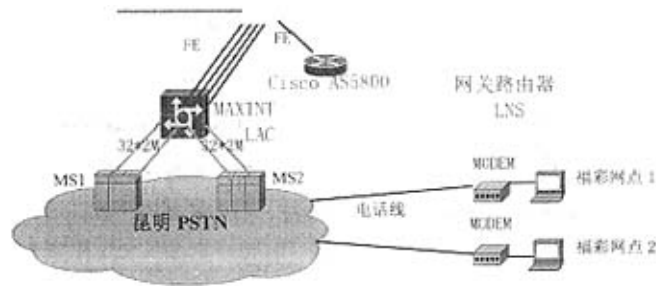
2007 年 VPN 业务仍将保持一定需求增长，根据昆明市电信分公司的预测将有 1500 个用户分支点使用 VPN 组网，本次 VPN 扩容改造后的 VPN 容量，可以满足以上业务需求。

同时从安全角度考虑，本次改造后网络结构由 L2TP 取代以前用户通过 PSTN 拨号接入的方法，利用 L2TP 的隧道技术，增强了网络接入的安全性。

4.3.3 网络升级改造方案

升级改造后的网络图如下：





根据目前本地网内窄带 NAS 设备端口利用率较低的现状, 建议使用 53 局已有的两台朗讯 MAXTNT 拨号服务器 (共计 1920 个拨号端口) 上通过系统软件升级方式, 仅需要加载 VPN 功能并适当的修改配置即可解决网络扩容问题。

本方案建议采用原有 MAXTNT 上的 2*32 共 64 条 E1 中继 (共计 1920 个拨号端口), 优势在于不需对现有 ASG 信令网关做任何配置修改。也可采用新增 64 条 E1 中继方式, 但这种方式将涉及对 ASG 配置修改, 还要根据现有网络状况考虑是否需要新增新的信令码。建议采用 16306 作为中继接入号码, 这样可以保证 VPN 用户可以呼到指定的 MAXTNT (L2TP Enabled)。VPN 用户采用带有域名的用户帐号认证, 如 l2tp@VPN.yn.cn, 电信的 AAA 认证服务器将对用户帐号的域名进行第一次认证并根据域名返回相应的 L2TP 隧道建立信息, 由电信运营商的接入服务器 (MAXTNT) 根据 AAA 服务器返回的隧道参数与客户中心路由器建立 L2TP 隧道。AAA 服务器位于省数据网管中心, 并由其负责制作客户的相关隧道参数。客户中心路由器使用 2 个 2M 专线与电信 IP 网络相连, 用户接入内网的第二次认证目前 (如福彩) 也是由电信的 AAA 服务器进行的。

L2TP 协议是现行的 VPN 的标准, MAXTNT 通过 L2TP 协议, 可以实现不同厂家设备间互通。在 L2TP 协议中, VPN 用户是通过 LAC (L2TP Access Concentrator) 与 LNS (L2TP Network Server) 建立 L2TP Tunnel 将用户接入私有网络。用户接入 LAC, LAC 根据被叫号码或用户的主叫号码或对用户进行认证的方式与 LNS 建立 IP 连接, 通过该 IP 连接建立一个控制连接。在 LNS 对用户做认证后, LAC 与 LNS 建立 L2TP Tunnel。VPN 用户就是通过该 Tunnel 经过公网与私有网络通讯。

在基于 Line 的 VPN 应用中, MAXTNT 与 LNS 之间采用如下过程建立 VPN 的连接: VPN 用户接入 MAXTNT (LAC), MAXTNT (LAC) 将根据用户的主叫或被叫号码及该主叫或被叫号

码在 Radius 上的用户 VPN 属性与 LNS 建立一个 IP 连接。通过这个 IP 连接, MAXTNT (LAC) 与 LNS 建立一个控制通道, MAXTNT (LAC) 发一个 Inbound Call Request 给 LNS, 接着 LNS 将对 VPN 用户作认证, 如认证通过则建立一个 Tunnel。通过这个 Tunnel, VPN 用户与私有网进行数据交换。当 VPN 用户从 MAXTNT (LAC) 上断开, 则 MAXTNT (LAC) 向 LNS 发送 Call Disconnect Notify 消息, MAXTNT (LAC) 与 LNS 断开 Tunnel。

在基于用户的 VPN 应用中, MAXTNT 与 LNS 之间采用如下过程建立 VPN 的连接: VPN 用户接入 MAXTNT (LAC), MAXTNT (LAC) 将用户认证信息包递交给 Radius 服务器, Radius 服务器认证完成后将用户的 VPN 属性传给 MAXTNT (LAC)。MAXTNT (LAC) 根据这些属性与 LNS 建立一个 IP 连接。通过这个 IP 连接, MAXTNT (LAC) 与 LNS 建立一个控制通道, MAXTNT (LAC) 发一个 Inbound Call Request 给 LNS, 接着 LNS 将对 VPN 用户再一次作认证, 如认证通过则建立一个 Tunnel。通过这个 Tunnel, VPN 用户与私有网进行数据交换。当 VPN 用户从 MAXTNT (LAC) 上断开, 则 MAXTNT (LAC) 向 LNS 发送 Call Disconnect Notify 消息, MAXTNT (LAC) 与 LNS 断开 Tunnel。

通过 Radius 对用户的识别, 完成了对 VPN 用户的认证和计费。

4.3.4 实施方案:

因为在升级过程中, 需要 MAXTNT 重新启动, 为了避免给网上用户带来过多的影响, 建议在升级前先将这 64 条 E1 中继端口屏蔽, 逐渐将用户转移到其他的远程接入设备上, 禁止用户的呼入。

1. 在升级前, 应备份现有 MAXTNT、RADIUS 等相关设备配置。
2. 登陆到欲升级的 MAXTNT 设备上, 用 user stat 命令观察用户状态, 直至没有用户使用的情况下, 即可升级。
3. 升级前, 首先通过 get base 命令检查

```
admin>get base
[inBASE]
shelf-number=1
```

```
software-version=9
software-revision=0
software-level=""
manufacturer=dba-ascend-mfg
d-channel-enabled=yes
aim-enabled=no
switched-enabled=yes
multi-rate-enabled=no
tl-pri-conversion-enabled=no
frame-relay-enabled=no
maxlink-client-enabled=disabled
data-call-enabled=yes
atmp-enabled=disabled
l2tp-enabled=disabled
pptp-enabled=disabled
```

4. 执行朗讯提供 MAXTNT 的 L2TP 的升级命令, 如 `update`。

执行后可以通过 `get base` 检查 `l2tp-enabled` 选项是否 `enabled`。

```
admin>get base
[inBASE]
shelf-number=1
software-version=9
software-revision=0
software-level=""
manufacturer=dba-ascend-mfg
d-channel-enabled=yes
aim-enabled=no
switched-enabled=yes
multi-rate-enabled=no
tl-pri-conversion-enabled=no
frame-relay-enabled=no
maxlink-client-enabled=disabled
data-call-enabled=yes
atmp-enabled=disabled
l2tp-enabled=enabled
pptp-enabled=disabled
```

5. 重新启动 MAXTNT

6. 将 MAXTNT 配置为 LAC, 方法如下:


```
admin>new l2-tunnel-global
admin>list

[ inL2-TUNNEL-GLOBAL (new) ]
pptp-enabled=no
server-profile-required=no
l2tp-mode=disabled
l2tp-auth-enabled=no
l2tp-rx-window=0

admin>set l2tp-mode=lac      (LAC is the only choice as of 7.0.0)
admin>write
```

7. 在 RADUIS 上添加相应 VPN 域名以及 VPN 用户认证的帐号。

RADIUS 需根据用户帐号的域名返回认证信息时添加如下属性指定 Tunnel-end-point:

```
Tunnel-Type=L2TP,
Tunnel-Medium-Type=IP,
Tunnel-Server-Endpoint=1.1.1.1
```

8. 程控交换机方面在相应的 E1 中继上添加 16306 的新的被叫中继号。如果采用新增 64 条 E1 中继的方案, 这时还要同时对 ASG 的配置做相应的改动。

9. 用拨号机呼叫 16306 测试 VPN 用户帐号是否成功。

4.4 小结

本章重点介绍了基于 L2TP 的 MaxTNT 组建 VPN 的组网结构、方案配置以及源代码设置, 并通过实际案例说明基于 L2TP 的隧道协议技术在 VPN 中的应用。

在基于 L2TP 的 MaxTNT 组建 VPN 的组网结构、方案配置以及源代码设置部分, 提出基于 L2TP 的提出者原 Ascend 公司的方案设计思想, 结合 MaxTNT 远程接入服务器所设计 L2TP 组建 VPN 的方案配置, 详细说明了每一步的设计依据、实现方法及参数定义, 最后提供经实际案例证实有效的源代码设置, 为实际工程中组建基于 L2TP 的 VPN 网提供方案设计参考。

在实际案例部分说明基于 L2TP 的隧道协议技术在 VPN 中的应用过程中，引用昆明电信 VPN 改造扩容工程的案例，说明 L2TP 改造的优点及带来的好处，即降低接入费用，扩容接入点和增加安全性，最后给出改造方案和实施方案，说明基于 L2TP 的隧道协议技术在 VPN 中的应用的可操作性。

5 总结

全球信息化建设都处于一个高速发展的阶段，信息孤岛和信息共享安全是信息化建设过程中两个比较突出的问题，传统的专线方式，其高昂的建造费用和每月产生的运营费用，使得大量企事业单位望而却步，于是 VPN 技术成为性价比最高的解决方案。除了传统意义的远程连接访问以外，现代企业在享受建立内部资源共享基础上高效率的协同工作的成果或 WEB 上传下载的同时，也要面临保护内部网络及其数据安全性稳定性的严峻挑战，包括网络反病毒、防入侵、防黑客、数据丢失等。同时，基于 VPN 的应用越来越多，用户对 VPN 产品的安全稳定性能要求越来越高，对于 VPN 服务的概念要求越来越高。VPN 的发展的确能代表远程接入服务今后的发展趋势，其综合了传统数据网络的安全和服务质量，以及共享数据网络结构的简单和低成本，建立安全的数据通道。VPN 在降低成本的同时满足了用户对网络带宽、接入和服务不断增加的需求，因此，VPN 必将成为未来远程接入服务发展的主要方向。

下面从 L2TP 的技术优势及在远程接入网络应用的必要性和 L2TP 在 VPN 网络改造中的意义和价值方面对本文进行总结如下：

L2TP 技术优势及在远程接入服务网应用的必要性：

本文从 L2TP 的自身特点及同其他二层隧道协议技术 PPTP、L2F 相比的优势出发，从协议原理、协议结构等说明 L2TP 在 VPN 二层协议技术中的重要性。文章前面章节通过解析 VPN 技术，重点解析二层隧道协议技术，将以下 L2TP 的特点优势逐一展开研究；中间部分着重分析了 L2TP 的技术，并引入作为 L2TP 技术实现软硬件的朗讯 MaxTNT 远端接入服务器介绍；后半部分阐述了基于 L2TP 的 MaxTNT 组网结构、方案配置、源代码设置，并通过昆明电信的实际案例分析了基于 L2TP 的隧道协议技术在 VPN 改造工程中的实际应用价值。

L2TP 协议由 Cisco、Ascend、Microsoft、3Com 和 Bay 等厂商共同制订，1999 年 8 月公布了 L2TP 的标准 RFC 2661。上述厂商现有的 VPN 设备已具有 L2TP 的互操作性。L2TP 结合了 L2F 和 PPTP 的优点，可以让用户从客户端或接入服务器端发起 VPN 连接，L2TP 定义了利用公共网络设施封装传输链路层 PPP 帧的方法。目前用户拨号访问因特网

时, 必须使用 IP 协议, 并且其动态得到的 IP 地址也是合法的, L2TP 的好处就在于支持多种协议, 用户可以保留原来的 IPX、AppleTalk 等协议或企业原有的 IP 地址, 企业在原来非 IP 网上的投资不致于浪费。另外, L2TP 还解决了多个 PPP 链路的捆绑问题, PPP 定义了多协议跨越第二层点对点链接的一个封装机制。

L2TP 协议是现行的 VPN 的标准, MAXTNT 通过 L2TP 协议, 可以实现不同厂家设备间互通。在 L2TP 协议中, VPN 用户是通过 LAC (L2TP Access Concentrator) 与 LNS

(L2TP Network Server) 建立 L2TP Tunnel 将用户接入私有网络。用户接入 LAC, LAC 根据被叫号码或用户的主叫号码或对用户进行认证的方式与 LNS 建立 IP 连接, 通过该 IP 连接建立一个控制连接。在 LNS 对用户做认证后, LAC 与 LNS 建立 L2TP Tunnel。VPN 用户就是通过该 Tunnel 经过公网与私有网络通讯。

基于 L2TP 的二层协议技术的 VPN 网络相比较传统的 PSTN 拨号网络及其他三层隧道协议技术, 有下列优点:

- 对于 GRE 及 IPSec 这些三层隧道协议, 区分用户将比较困难; 因为在三层 (IP 层), 一般只能通过 IP 地址来区分用户。对于 VPN 来说, 用户的地址是可以重复的, 这样, 三层隧道协议不适合区分用户。
- L2TP 是二层 (链路层) 的隧道协议, 是作为 PPP 的扩展提出来的。PPP 适合区分不同的用户, 比如拨号用户、采取专线直连的对端路由器等等, 因为 PPP 可以得到对端的用户名。对于拨号用户接入这种情况来说, 需要区分不同的 VPN 用户, 使用 L2TP 协议进行 VPN 组建。
- L2TP 隧道协议, 并且只分配企业网内部 IP 地址。
- L2TP 是由 IETF 起草, 结合了 PPTP 与 L2F 的优点, 成为一种标准, L2TP 还支持信道认证, L2TP 具有 IPSec 选项。
- 而 PPTP 等第二层的隧道协议, 要求有正式的 IP 地址, 在拨入拨号服务器时, 由拨号服务器提供, 再二次拨入企业网关时, 由企业网关分配内部网地址。

L2TP 在 VPN 网络改造中的意义和价值:

在远程接入服务中, 通信成本和安全性是衡量一项技术的重要标准。

相比较传统 PSTN 拨号实现远程接入服务, 用 L2TP 构建 VPN 网络节省的通信成本是巨大的。L2TP 节省了昂贵的远程拨入长途费用, 用户只需花费较低的市话接入费用或网络接入费用即可实现远程连接。在本文介绍的利用朗讯 MaxTNT 实现 L2TP 的 VPN 网络中, 在用户接入侧就是只需要本地市话接入费用。

另外用 L2TP 构建 VPN 网络, 其网络安全性也大大增强。对于构建 VPN 来说, 网络隧道(Tunneling)技术是个关键技术。网络隧道技术指的是利用一种网络协议来传输另一种网络协议, 也就是将现有的透明网络信息进行再次封装, 从而保证网络信息传输的安全性。

本文所介绍使用朗讯 MaxTNT 设备基于 L2TP 所构建的 VPN 网络, 该 VPN 网络将用户接入端的 LAC 和远程访问端的 LNS 利用 L2TP 结合在一起, 可实现二次认证。用户远程访问按如下步骤进行。

1. 用户认证

用户端通过在拨号软件中输入用户名和密码, 向用户接入端的 LAC 提出远程访问请求, LAC MaxTNT 和 VPN Server (Raidus) 交互用户名和密码。对用户进行认证, 认证后则向用户反馈认证结果。

2. 建立隧道

如果认证成功 VPN Server (Raidus) 则向远程网络的 LNS 提出隧道建立申请, 并将用户信息提交给 LNS, LNS 对用户进行第二次身份认证, 如认证通过则给用户 ID、动态 IP 地址和访问权限, 并将此反馈给用户。

3. 远程访问

用户通过两次认证后则能够以所给的用户 ID、IP 地址和权限进行远程访问, 同时用户接入端的 LAC 把用户上网时间和流量提交给 VPN Server (Raidus) 开始对用户进行计费。

在第一次用户认证时可采用 PPPOE 方式,网络数据信息从用户电脑到接入网设备 LAC 之间经过 IP-PPP-PPPOE-MAC 四层封装,在通过第一次用户认证后,接入网设备 LAC 除掉了网络信息的 PPPOE 和 PPP 封装,封装格式成为 IP-MAC,即在接入网设备 LAC 上实现了 PPPOE 的终结。在隧道建立起后,将从接入网设备 LAC 出来的数据信息作为一个整体封装在基于 PPP 协议的 L2TP 数据的最低层,其格式为 IP-PPP-L2TP-UDP-IP-MAC,这里最上层的 IP 已经不是原有的 IP,即 IP 地址已经更改成远程网络 LNS 分配和认可的 IP 地址,到达目的远程网络后,经过远程网络 LNS 的解封装,除去了中间的 PPP、L2TP、UDP 和 IP 封装,数据封装格式重新成为 IP-MAC,新数据信息里的 IP 地址仍然是远程网络 LNS 认可的 IP 地址而不是用户原有的 IP 地址。因此在网络数据传输过程中,用户原始数据经过 L2TP 封装到最低层,因为 L2TP 封装的复杂性,就算有人能够截获数据流,也很难按照原有的网络 ISO 模型对其进行分析以获取有用信息;在远程网络端,用户的 IP 信息被分配和认可的 IP 信息取代,即用户的信息是相对保密,从而保护了用户不被侵犯;整个传输过程对用户而言是非透明的,用户无法知晓 L2TP 传输机制,从而保证了传输过程的安全性。

L2TP 构建 VPN 除了上述的意义价值外还有如下实际价值:

1. 灵活的身份验证机制以及高度的安全性

L2TP 是基于 PPP 协议的,因此它除继承了 PPP 的所有安全特性外,还可以对隧道端点进行验证,这使得通过 L2TP 所传输的数据更加难以被攻击。而且根据特定的网络安全要求,还可以方便地在 L2TP 之上采用隧道加密、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

2. 内部地址分配支持

LNS 可以放置于企业网的防火墙之后,它可以对于远端用户的地址进行动态的分配和管理,可以支持 DHCP 和私有地址应用。远端用户所分配的地址不是 Internet 地址而是企业内部的私有地址,这样方便了地址的管理并可以增加安全性。

3. 网络计费的灵活性

可以在 LAC 和 LNS 两处同时计费，即 ISP 处（用于产生帐单）及企业处（用于付费及审记）。L2TP 能够提供数据传输的出入包数，字节数及连接的起始、结束时间等计费数据，可以根据这些数据方便地进行网络计费。

4. 可靠性

L2TP 协议可以支持备份 LNS，当一个主 LNS 不可达之后，LAC（接入服务器）可以重新与备份 LNS 建立连接，这样增加了 VPN 服务的可靠性和容错性。

5. 统一的网络管理

L2TP 协议将很快地成为标准的 RFC 协议，有关 L2TP 的标准 MIB 也将很快地得到制定，这样可以统一地采用 SNMP 网络管理方案进行方便的网络维护与管理。

相信在不远的未来，基于 L2TP 的隧道协议技术将会应用到各类 VPN 工程中，同时将会引发新一轮的技术更新。

参 考 文 献

- 【1】. 高海曲、薛元星、辛阳等著, VPN 技术, 机械工业出版社, 2004-4;
- 【2】. 韩杰编著, 计算机网络与通信, 人民邮电出版社, 2002-2;
- 【3】. 卢昱、林琪编著, 网络安全技术, 中国物质出版社, 2001-2;
- 【4】. 阎梦天、董德存著, VPN 隧道技术的探讨, 广东通信技术 2004-7;
- 【5】. RFC2637, Point-to-Point Tunneling Protocol “PPTP”, in IETF1999;
- 【6】. RFC2341, Cisco Layer Two Forwarding (Protocol) “L2F”, in IETF1998;
- 【7】. RFC2661, Layer Two Tunneling Protocol “L2TP”, in IETF1999;
- 【8】. RFC2153, The Point-to-Point Protocol “PPP”, in IETF 1994;
- 【9】. 何宝宏著, IP 虚拟专用网技术, 人民邮电出版社, 2002;
- 【10】. 杨璐, 刘云玲, VPN 及其安全技术研究, 计算机工程与设计, 2000-12;
- 【11】. Cisco System Inc., Cisco Systems Acomparison between IPSec and Multiprotocol Label Switching, 2000;
- 【12】. RFC2865, Remote Authentication Dial In User Service (RADIUS), in IETF 2000;
- 【13】. 王达著, 虚拟专用网 (VPN) 精解, 清华大学出版社, 2004-1;
- 【14】. B. Patel. RFC 3193 Securing L2TP using IPSec, Cisco System, 2001;
- 【15】. 郝辉, 钱华林, VPN 及其隧道技术研究, 微电子学与计算机, 2004-11;
- 【16】. 陈恺, 吴国新, VPN 中隧道交换技术的研究, 数据通信, 2003-5;
- 【17】. Mark Norris 著, 局域网设计—INTRANET、VPN 及企业网, 电脑报出版社, 2001-7;
- 【18】. Ascend Inc., MAXTNT Technical Backgrounder, Version 1.07, Ascend Technologies, 2000-1;
- 【19】. Lucent Technologies, APX and MAXTNT Administration Guide, Version 11.01, Lucent Technologies, 2005-3;
- 【20】. Lucent Technologies, APX and MAX TNT WAN, Routing, and Tunneling Configuration Guide, Version 11.01, Lucent Technologies, 2003-6;
- 【21】. 邵然, L2TP 在 VPN 工程中的应用, 朗讯科技交换与数据应用技术季刊, 2006-6;

致 谢

本论文是在姚文琳导师的全面指导下完成的。在我读工程硕士的二年半时间里，导师在学术上给予了细致入微的指导和关怀，在此我要向他致以衷心地感谢！导师以他丰富的知识和精辟的见解来指导我的学业和研究，使我深刻感受到了导师在学术上对学生的厚望和期待。导师严谨的治学精神，科学的思考方式，平易近人的处世风范，对我现在以及今后的人生必将产生深远的影响。

我要深深感谢中国海洋大学提供给我这一个宝贵的学习机会。在两年多的工程硕士学习过程中，海洋大学老师们渊博的学识、严谨的治学态度、孜孜不倦忘我工作的精神、宽广灵活的思路都使我受益非浅，并将成为我今后工作过程中努力的目标和方向。

最后要向我攻读工程硕士期间所有关心我、帮助我的老师和同学们表示衷心的感谢！向大力支持我们家人，朋友，公司领导和同事表示衷心地感谢！

