第17章　远程访问协议

作者：Mark Kadrich

本章内容包括：

- 远程互联
- 远程认证拨入用户服务(RADIUS)
- 使用SLIP、CSLIP和PPP传送IP报文
- 隧道远程访问

随着Internet的增长，需要从任何位置访问 Internet的需求也在增长。开始时，访问是通过连接以放在公司核心中的大型机终端来完成。这种访问方法相当不错，只要用户在桌前，或至少在办公室里就能进行。随着预算的增加，支持人员的减少，急需提供给系统管理员一种访问权，使他们能在家里管理提供服务的系统。因此，产生了远程访问。这种简单的访问通过当时的慢速调制解调器来实现，通常是 110波特(波特率和位/秒非常接近，可以互换使用)。现在系统管理员可以在家中比较方便地监控系统行为并按需要进行一些系统相关的修改。为组织带来的好处是通过个人在紧急情况下的监控，关键性系统能达到 24×7的指标。也就是说只要紧急情况不中止服务，服务就照样可以进行。

70年代末80年代初技术进步使调制解调器的吞吐量每隔几年就增长一次。就像集成电路存储器芯片所遵从的摩尔定律一样每隔几年容量就增长一倍。

今天的调制解调器波特率为 56K或更高，但实际的吞吐量受限于老式的公用电话交换网(PSTN)中的铜线结构，这种过时的基础设施，通过引入更先进的可靠性和安全性要求，对于开发有效的传输和接收数字信息协议起了重要作用。

17.1　远程互联

前面已经指出，远程访问的主要设备是调制解调器。调制器 /解调器(mo-dem)可以以多种不同类型的设备形式出现。基本上讲，调制解调器把用户计算机产生的数字信号转变为 PSTN能传输的信息。每个端系统必须有一个兼容的调制解调器才能正常工作 (参见图17-1)。一旦到达接收端，模拟信号解调为数字信号并输入给接收计算机。

图17-1　基本的调制解调器和PSTN网络

17.1.1 ISDN

并不是所有的这些设备都兼容。标准调制解调器允许用户连接到综合业务数字网（ISDN），而NT-1(网络终端)将不允许用户连接到除ISDN之外的任何网络。ISDN提供了一些非常有用的特点。基本速率接口(Basic Rate Interface，BRI)允许用户使用模拟电话并进行数据的纯数字传输。在美国，BRI由两条64K信道和一条16K信道组成，这些信道是时分多路复用(TDM)的，总共144Kbps。(见图17-2)。

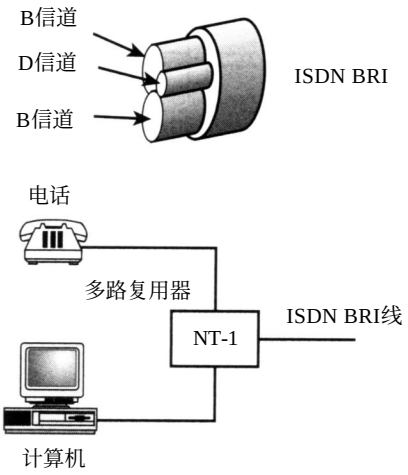

图17-2 ISDN BRI配置

ISDN的功能多样性来源于如下事实：在任何时候，所有的三个信道能够单独使用，或者两个64K信道合起来使用提供总共128K的吞吐量。ISDN一个令人感兴趣的优点是ISDN能使用已有的进出大多数公司和家庭的双绞线。对于公司和提供ISDN服务的电话公司而言，这是很重要的一个考虑。这意味着无须升级已有的PSTN。虽然这样会延长已有PSTN的寿命，但是随着成百万的计算机连接Internet，Internet革命会给ISDN施加更多的压力。ISDN存在的时间不长了。

17.1.2 电缆调制解调器

电缆调制解调器已经使用了多年(见图17-3)。电缆调制解调器利用了如下事实：许多消费者在家中有基带传输媒体——电视电缆。

利用有线电缆带宽中不用的部分并且使用一些调制技巧，电缆调制解调器能提供给用户大约1Mbps的访问速度。在家庭环境中这样的速度非常诱人。最新软件和操作系统的发展允许多台计算机利用这单一访问点。

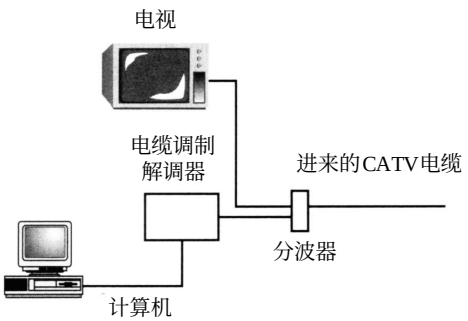

图17-3 电缆调制解调器

电缆调制解调器把计算机和相邻有线电缆连接的方式非常类似于把计算机通过同轴电缆与以太网相连的方式，每个人在一条数据总线上。这意味着相邻用户能彼此访问计算机，应该小心不要让这种情况发生。一种解决方法是通过网络地址转换(Network Address Translation，NAT)。

通过利用RFC 1918“私人网络地址分配技术”的软件，家庭网络现在能为网络上的每台计算机提供到Internet的访问和安全。如果管理员想按年龄把用户分开(如父母与青少年)，可以很方便地做到这一点。已经证明，今天的计算机受到的重视就如同昨天的电话一样。

像@Home这样的公司已经在许多地区率先开始这种访问类型，用户可以看一下本地有线公司是否提供这种功能。

17.1.3 数字用户环(DSL)

数字用户环(Digital Subscriber Loop，DSL)是一项比较新的服务，DSL提供许多令人感兴

趣的实质上是相同功能的东西。使用基于价格的服务级模型，付款越多， DSL提供的吞吐量就越大。一条56K的链路大约每月需付费50美元，3倍的容量要付费100美元。表17-1列出了基于吞吐量的一般DSL价格。这些是平均列表价格，其中不包括任何折扣或其他服务。

表17-1 一般的DSL价格列表

数据速率	高	低
144	$124.00	$90.00
160	$149.00	$80.00
192	$169.00	$90.00
384	$199.00	$130.00
768	$359.00	$180.00
1.1	$399.00	$200.00
1.5	$359.00	$290.00

有许多不同类型的DSL，不对称DSL(ADSL)是最常见的类型。ADSL基于如下考虑：典型的用户通常下载比上载多。当浏览站点时，用户会以图片形式下载页面，而上载却很少。一般说来，绝大多数用户只上载简单应答查询。当用户点击 Web页面上的一个按钮时，会向服务器发送一个简单的消息，告诉服务器返回一个图片或文本。例外情况是电子邮件。然而，即使考虑电子邮件，下载和上载仍为 10:1的比率。

DSL的发明是为了解决随着 Internet增长而出现的许多特殊问题，特别是容量问题。已有的PSTN基于如下想法建造：绝大多数对话 10分钟左右，一般家庭至多有两条线。这种情况允许中心局(CO是电话术语)的大小按某种比例。也就是说，如果只有 10%的用户同时使用电话，中心局(CO)就只须支持这么多的电话交换。

注意 DSL仍不是很完美的。当DSL线路是ISDN线路来的一部分时，线路之间的串扰就会降低DSL线路的效果。在使用DSL线路之前要与供应商谈妥。

DSL比电缆调制解调器一个让人更感兴趣的好处是其吞吐量维持不变。由于电缆调制解调器用户要与相邻用户共享电缆段，因此相邻用户越多，所得到的有效吞吐率就越少。由于DSL是用户和服务提供者之间点到点连接，就不受这个问题的影响。然而， DSL仍受限于中心局到Internet可获得的带宽。

17.1.4 无线网络

许多技术支持无线网络，从蜂窝网络到 Ricochet和Metricom提供纯无线调制解调器技术。通过位于附近光极 (light pole)上的收发器通信， Ricochet允许适当装备的计算机通过无线与Internet通信；但这种通讯方法的不足之处是不安全。

17.2 远程认证拨入用户服务(RADIUS)

远程认证拨入用户服务 (Remote Authentication Dial-In User Service，RADIUS)即RFC 2138，为远程用户提供了许多重要的服务。 RADIUS是一个客户机/服务器类型的协议，最初由Livingston公司在1992年开发。毫无疑问， RADIUS是为了满足为安全设备提供一种加强的用户认证方法的需要。

RADIUS已经成为使系统管理员对认证过程更加自信的一个重要组成部分。

RADIUS配置通常由一个中心数据库服务器和一个或多个拨入服务器组成 (参见图17-4)。

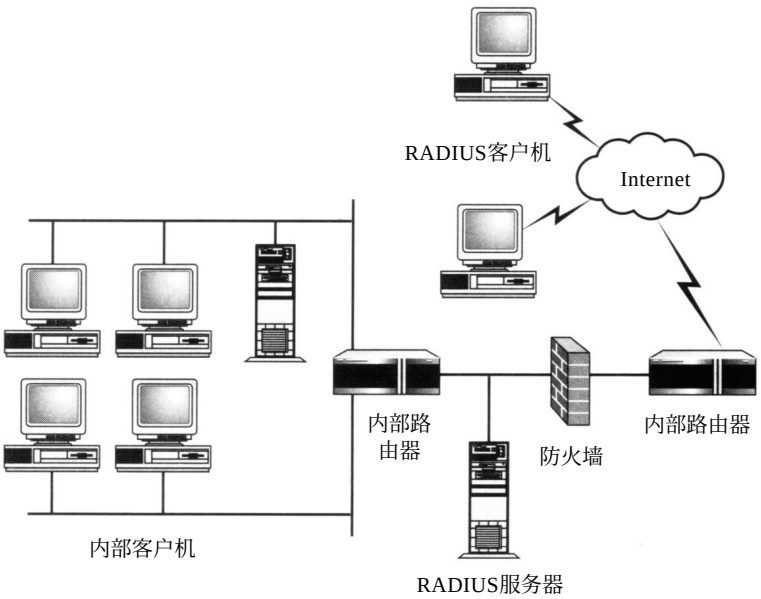

图17-4 RADIUS客户机服务器模型

数据库中包含三种信息 —— 认证、授权和记账。认证信息使网络能识别系统的用户。虽然认证信息通常存储在文本文件中，但是 RADIUS服务器能够和口令文件及 NIS+进行通信，授权信息赋予用户对服务器和数据的访问权，如可以对公司内部服务器或电话列表进行访问。记账信息用于记录用户的访问次数、失败访问次数、连接时间等等。

17.2.1 RADIUS认证

RADIUS交流信息是非常直接的。一旦用户和远程访问服务器相联，RAS服务器会提示用户输入用户名和口令，这个过程使用口令认证协议 (Password Authentication Protocol，PAP)，RFC 1334描述了PAP，或挑战握手认证协议 (Challenge Handshake Authentication Protocol，CHAP)，见RFC 1994。

1. 口令认证协议(PAP)

PAP是一个老式协议，依赖于口令和用户 ID。用户在建立远程连接之后，用户 ID和口令对就送到RADIUS服务器。如图 17-5所示，访问服务器不断地发送口令和用户 ID至认证服务器，直到这个过程发生超时。如果读者对安全重视，就不应选择这样的协议。口令以“明码”传送。换句话说，用户信

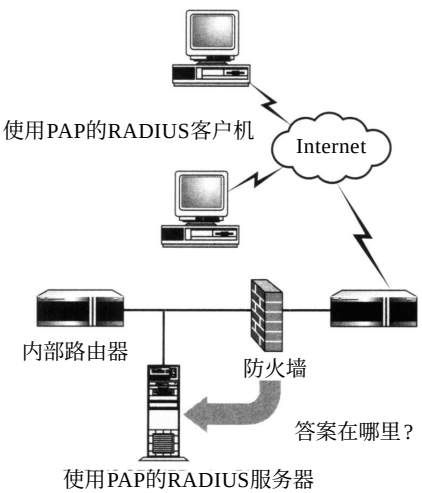

图17-5 PAP协议互换信息

息没有经过加密处理。这意味着别人可以记录事务，并在以后重复这一过程达到访问用户关键服务的目的。PAP通常作为回调协议使用，在一些协议如CHAP失败后才使用PAP。

2. 挑战握手认证协议(CHAP)

CHAP的特别之处在于它提供了认证用户更强的方法。 CHAP是一个三路握手过程，首先发一个Challenge码到用户并期望用户作出合适的“ 握手 ”应答。在用户建立连接之后，服务器会给客户机发一个“ challenge ”报文。客户机使用一路 hash函数如MD5计算出应答。客户机把应答发给服务器，服务器已计算出所期望的应答。如果从客户机发送来的应答与服务器计算出的应答相吻合，客户机就被允许访问网络。如果应答和服务器计算出的应答不相吻合，访问就被拒绝。为了保证会话过程不被劫获，可以配置 CHAP协议周期性地重新对客户进行认证。与PAP不一样，认证方控制整个 CHAP过程，很少允许重试。

这种类型的认证能防止重复 (Replay)型攻击，如上一节所讨论的。由于每个 Challenge不相同，计算出的每个应答也不相同。应该注意到这个协议依赖于一个共享的密钥(secret)。密钥作为hash函数的键字(参见图17-6)，所以它应受到保护。 Challenge值应遵循两个标准：惟一且不可预测。

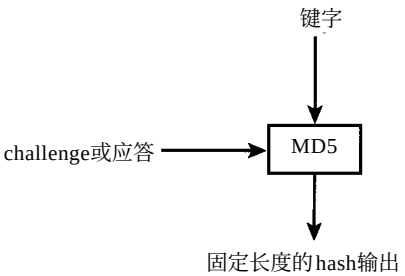

图17-6 hashing方法示意图

CHAP认证方法应该用于对敏感网络资源的访问或者出于安全考虑时采用。作为事实，和 CHAP RFC相比，当使用PPP时实际上已经抛弃了作为口令协议的PAP。

17.2.2 记账信息

记账信息可以采用多种形式，包括用户 ID、口令、访问限制、服务授权以及审查信息。

我们已经熟悉UID和口令信息。RADIUS允许加入审查信息。审查信息可以用于确定是否某个人试图访问其不该访问的信息。也可以利用审查信息来控制何时允许某人访问网络。如果有一个接待员只要求上午 9点到下午5点之间访问网络，就可以设置记账信息来反映这一要求。任何超过这个限制的访问都不允许。实际上这种方法减少了网络被访问时间，从而增加了安全性。

通过使用数据库来限制对各种服务的访问可以达到相似的效果。通过输入允许服务列表，就能阻止对非授权服务的访问。当用户访问没被授权的服务时，会被 RADIUS服务器拒绝。这是基本的策略管理，并且支持集中式的用户数据库，集中式的用户数据库能够使更新容易。

17.3 用SLIP、CSLIP和PPP传输IP数据报文

已经开发出许多协议用于把信息从一个地方传到另一个地方。协议的选择依赖于功能要求的大小。以下各节讨论远程访问协议的历史及其现在的状况。

17.3.1 串行线路接口协议(SLIP)

SLIP是用于远程用户和本地主机互联的早期协议。 RFC 1055作为信息规范只是由于SLIP被认为是实际上的标准。 SLIP是第一批远程访问协议之一， SLIP提供了到远程网络的IP互联，

这出现在80年代早期。图17-7显示了伯克利和Sun(升阳)公司操作系统使用SLIP的方式。

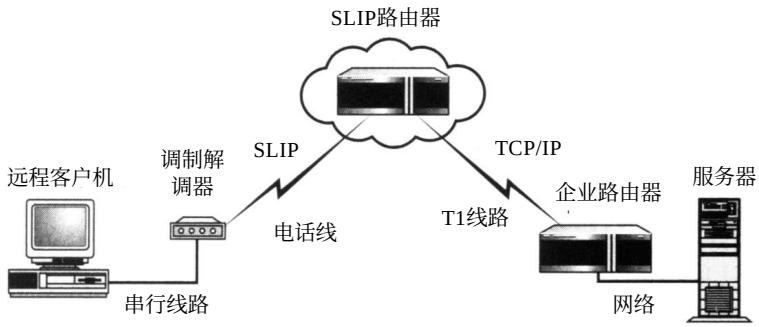

图17-7 SLIP协议

SLIP是非常简单的协议，因为设计SLIP时网络还很简单。整个RFC，包括代码，也仅有5页纸。SLIP所做的全部事情是定义在串行线路上组帧的方式。 SLIP没有纠错和检测、寻址、报文标识或压缩。SLIP的惟一目的是在串行线路上发送报文。

由于SLIP的简单性造成了其低效率，因此在大型网络实现中并不希望使用 SLIP。最麻烦的是在SLIP会话过程中，会话双方必须知道彼此的 IP地址。如果不知道，就没法处理路由问题。在现代网络中，这会成为问题，特别是在基于 DHCP的环境中。然而又是 SLIP的简单性使其实现很容易。

SLIP数据报文通常小于1006字节，大大低于大多数机器的MTA限制。RFC中关心的另一个问题是最大调制解调器速率，建议 SLIP的连接小于19.2Kbps。实际上这是个很好的限制。更快速度的互联由PPP提供，但PPP要引入额外的错误检查机制。

17.3.2 压缩的SLIP(CSLIP)

CSLIP协议通过使用VanJacobsenTCP头压缩来减小传输开销，使TCP头从40字节减为7个字节。实质上，压缩采用如游程长度编码那样的机制用一个字符和一个计数值代替由重复字符形成的字符串。当用户发送大量小报文的时候压缩和不压缩会有很大区别，协议如 Telnet正是这种情况。正如名字所指出的， TCP头压缩，对非TCP头如UDP和SNMP没有影响。

17.3.3 点到点协议(PPP)

由于SLIP协议的问题和限制，很显然需要一种新的工具，这就是 PPP协议。

RFC 1134在1989年由卡内基·梅隆大学的Drew Perkins起草。PPP协议非常通用，它支持数据报在点到点的链路上和 Internet上的传输。数据报是一块类似于报文的数据。通过封装数据报，PPP保持与媒体的无关性并且支持多个非 IP协议。诸如UDP/IP，IPX/SPX甚至Appletalk这样的协议都可以利用PPP。

1. PPP操作模式

为了确保能支持任何类型的用户会话， PPP内嵌的许多功能提供了不同的操作模式。对应于连接请求，PPP具有三种基本的操作模式：

- 立即式PPP链路
- 自动检测

• 交互式操作

(1) 立即式链路

正如其名所示，立即式 PPP在应答请求后就提供 PPP通信。任何认证在 PPP协议自身之内进行。因为必须关闭认证，所以这是一种带有危险性的连接方法。这种方法允许任何人联到网络。

(2) 自动检测

在自动检测方法中，服务器会在PPP、SLIP、交互式或其他系统配置的协议之中进行选择。这种方法的好处是多样性。由于能够支持广泛的协议选择，网络能有效地处理升级和迁移问题。不必slash cutover，就能进行用户和服务的逐渐迁移。 slash cutover是指配置所有系统在同一时间迁移到相同的服务。这就如在深夜里轻拨一下开关，置许多系统管理员于“ 死地 ”一样，因为系统一定是出了一些故障，故障原因通常是 VP计算机，并且经常发生在早晨 6点钟。

(3) 交互式操作

对哑终端和必须访问网络的终端仿真用户的支持是其另一个优点。一些数据库访问程序仍然要求访问合法系统，所以要小心这一功能。

在会话开始时， PPP确定是在进行处理主动会话还是被动会话。主动站点会发送帧来试图与对等方进行握手过程。配置出向 (outbound)节点为主动站点是标准过程，而入向 (inbound)节点既可以配置为主动节点，也可以配置为被动节点。自动检测拨入服务器应该设置为被动的，以便确定远程节点所使用的线路协议。

为了使PPP成功开始握手过程，一个节点必须是主动节点。注意，不是所有的软件都支持模式选择。NT RAS是一个被动服务器，然而 Sun公司的Solaris PPP是主动服务器。如果使用的是PPP 2.3，用户就能选择主动模式或被动模式。

PPP通过使用加密控制协议 ECP(RFC 1962、RFC 1968)支持加密。PPP支持许多加密算法，包括DES。两个端节点必须都要支持加密且必须使用相同的算法。注意，并不是所有的产品都支持加密，因为加密是 PPP的扩展。

和SLIP相比，PPP支持许多服务，包括：

• 同时支持多个协议
• 链路配置
• 错误检测
• 压缩
• 加密
• 网络信息
• 认证

如图17-8所示，PPP位于协议栈中的数据链路层上，和物理层和网络层接口。

以这种方式使用协议栈，能使 PPP支持多协议。比如， IP数据报能封装在PPP帧中，如图17-9所示。

IPX也以完全相同的方式进行封装。 IPX数据报，不是IP数据报，由支持 PPP的数据链路层处理。这种方式维持了栈的一致性，但却为今天多协议网络环境提供了所需的多样性。

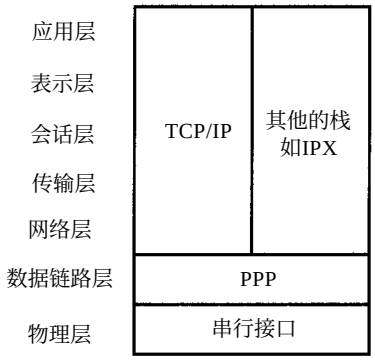

图17-8 具有PPP连接服务的TCP/IP栈

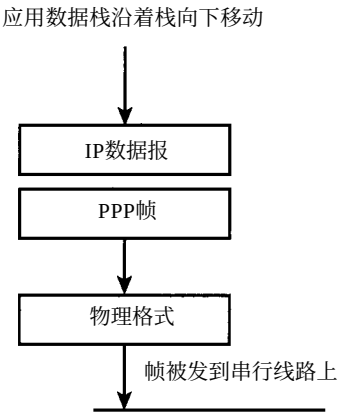

图17-9 IP数据报封装进PPP帧并发送到线路上

PPP的灵活性也表现在可以修改操作参数上。为了使链路功能达到最大， PPP能设置许多链路配置参数，如：

- 最大接收单元(MRU)
- 异步控制字符映像(Async Control Character Map，ACCM)
- 认证协议
- 扩展的认证协议(EAP)
- 质量协议
- 魔数
- 协议域压缩
- 地址控制域压缩
- FCS 选择

2. 最大接收单元(MRU)

MRU告诉其他节点，本节点作为接收端时能处理的最大传输单元尺寸不同于缺省的 1500字节。应该注意所有的实现要求在任何时候都接收 1500字节的PPP信息。这个值与连接时协商的值无关。因为使用压缩协议会使一些类型的数据由于置换算法而增大，所以计算 MRU是个复杂的过程。一些PPP实现以连接速度为基础计算 MRU。高于1.44Mbps的T1速度对TCP/IP而言没有价值。

3. 异步控制字符映像(ACCM)

ACCM在RFC 1662中描述，告诉对方数据流中的什么字符应该“消失 (escape)”以保证不破坏数据，通过设置能否使用从 18到IF的32个ASCII码控制字符来完成此功能。通常用于中止和开始流的控制字符 CONTROL-S和CONTROL-A(XON和XOFF)会以奇怪的令人惊讶的方式破坏数据。

4. 认证协议

认证协议在RFC 1161中描述，用于告诉对等方在开始进一步通信之前需要对方证实自己。缺省选择是不认证。发送方可以发出一个配置请求报文，指示对方需要使用指定的协议证实自己。接收方能发送一个无应答配置报文 (Configure-Nak)来请求使用另一个协议，如图 17-10所示。

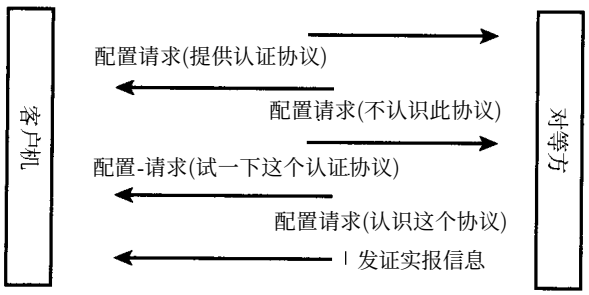

图17-10 认证过程

此时，发送方能中止会话，或发送使用不同认证协议的报文。允许的认证协议包括 RFC 1334 PAP、RFC 1994 MD5 CHAP、MSCHAP 、EAP或SPAP。一旦对方发送了配置应答(Configure-Ack)，本方就必须使用一个上述协议进行回复。

CHAP和PAP前面已描述过，下面会简单地描述剩下的协议。

(1) 扩展的认证协议(EAP)

扩展的认证协议(EAP，RFC 2284、RFGC 2484)是1999年之后建议使用的认证协议。

在链路控制阶段 (LCP)，PPP建立连接后，才进行认证算法选择。之后，在认证阶段，EAP与客户机相互协商，获得与特定认证协议相关的信息。 EAP的主要优点是具有支持后端(back-end)系统认证和加密的能力。这样使得 PPP与RADIUS服务器或其他基于硬件和软件的安全令牌更容易集成。

(2) Shiva PAP

Shiva PAP同样也具有使用硬件令牌的功能，但Shiva PAP好像并不把令牌释放到公共域中，而是把令牌赋给选中的生产商。几乎没有关于 Shiva PAP的文档。

(3) MS CHAP

MS CHAP基本上是一般的 CHAP，但却使用了不同的 hashing算法。MS CHAP不使用MD5，而是使用 DES或MD4。使用哪一个将依赖于是使用 LAN形式(DES)，还是NT形式(MD4)。两种情况下，应答都是使用 DES。这一点类似于CHAP的标准形式，只是标准 CHAP使用MD5。

5. 质量协议

PPP一个令人感兴趣的方面是其具有测量服务质量 (QoS)参数的能力。通过告诉对方想要接收QoS信息，就能达到监控数据丢失情况和错误率的目的。缺省的设置是“ 无协议 ”。提供的信息是关于链路及其状态的简单统计。

6. 魔数

魔数在QoS请求、抛弃请求及链路质量报文中使用。这是一个随机选取的数用于节点彼此标识，并帮助进行错误检测和闭环 (loopback)检验。缺省设置是“ 无魔数 ”。

7. 协议域压缩

协议域压缩执行简单的功能，把 16位的协议域压缩为 8位。最高字节必须为 0以保证工作正确。只有最低字节被传送。缺省情况下不使用这种功能。

8. 地址控制域压缩

另一个压缩域是地址控制域，告诉对等方和这个域相关的固定 HDLC值0xff和0x33可以被

忽略。如果是其他值，缺省设置为“ off ”。在对延迟敏感的应用中(如实时应用程序)可以以这种方式忽略无用的地址域。最后的效果可以节省报文传输中的几个字节。

9. FCS选择

这里讨论的最后一个选项是FCS选择，这个选项告诉对方，本方想接收非标准的缺省帧校验序列域。这是一个链路控制协议配置选项，选项一般被忽视，因为并不是在所有的 PPP实现中都可以配置它。这一选项允许对等方协商使用 32位的循环冗余校验 (CRC)而不是通常的16位CRC。

PPP支持一些扩展功能，但这些扩展或者有漏洞或者过时，使用这些选项时应该小心，并且在可能的情况下使用其他的解决方法。这些选项在 RFC 1570、RFC 1663、RFC 1976和RFC 1990中有描述。包括：

- 编号模式
- 多链路规程
- 回调
- 连接时间
- 组合
- Nominal数据封装
- 多链路MRRU
- 多链路短序列号头格式
- 多链路端点鉴别
- 独占权
- DCE标识
- 多链路+规程(Multi-Link-Plus Procedure)
- 链路鉴别
- LCP认证选项

17.4 隧道远程访问

在许多情况下，为了把数据从一个网络传送到另一个网络必须使用专门的技术。有时把一个协议打包到另一个协议之中是件简单的事情，图 17-11显示了把IPX报文封装到IP中的情况。

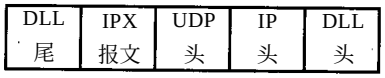

图17-11 IPX报文封装到IP中

原本的协议(在这里是IPX)不具有在互联网络之间传送数据的功能。为了解决这一问题， IPX报文前附加一IP头，给出路由器所需的信息，以便指导路由器把报文发送到最终目的地。这是一个常用方法，从Appletalk年代就使用这种方法，而且证明这种方法非常有效。

然而，这种解决方法并不是没有缺点。一些应用程序被设计成直接处理自己的原本(native)应用。在上面的例子中，是指Novell Netware。IP的各种实现具有不同的特点，这使得实现起来不直接。这样的一个例子是在微软网络上运行 IPX。在一些MS网络上运行IPX的例子中，会发生和超时及幻相效应相关的奇怪事情。幻相效应是指网络资源时隐时现的效应。这种现象一般发生在打印机上，原因是由于网络和打印机驱动程序的不正确分布。

问题就出现在这里。必须保持对细节的特别关注，因为这实际上是使用两个或多个网络

协议来支持用户应用。一个不正确安装或陈旧的驱动程序很难被检查出来且不容易修复。更重要的一点是使得网络看起来不可靠。

针对这个问题有一些解决方法，并且在过去证明很有效。首先，使用远程管理产品让系统管理员能安装、管理远程站点。来自 Vector Networks (www.vector-networks.com)和Traveling Software (www.traveling software.com)公司的产品，提供了额外功能，这些功能并不是为桌面环境而设计的。这些产品的特征具有远程控制、远程管理、远程软件及硬件报表功能。通过这些功能可以提供可靠的网络环境，但应注意这些产品有其自身的不足。错误配置会导致对敏感信息的非授权访问。必须使用强口令，并且管理访问权只赋那些需要的人。

在有些情况，可能需要比较高的安全级。在这些特殊环境下，可以使用加密协议如 PPTP和L2TP。

17.4.1 点到点隧道协议(PPTP)

PPTP是Ascend通信公司、ECI电话公司、微软、3com以及US Robotics公司共同合作的成果。这个工作组称为PPTP论坛。PPTP的基础是很好绑定且相互区别的函数。之所以这样做是因为这样可以使用户和生产商能利用 Internet的普遍特性。通过支持一种标准，用户可以通过本地ISP拨号并能够安全地通过Internet隧道连接到他们的公司网络。这样可以使公司减少产生和支持自身远程访问硬件的要求。

这种新的体系结构可以使公司利用 Internet结构——让ISP做自身擅长的工作：把个人用户和Internet连接起来。之后，公司可以自由地购买连到城域网 (MAN)或广域网的设备，通过本地环路多路分解到达的远程访问连接。对他们而言，远程呼叫看起来像是到另一个 Internet站点的连接。图17-12显示了体系结构的区别。

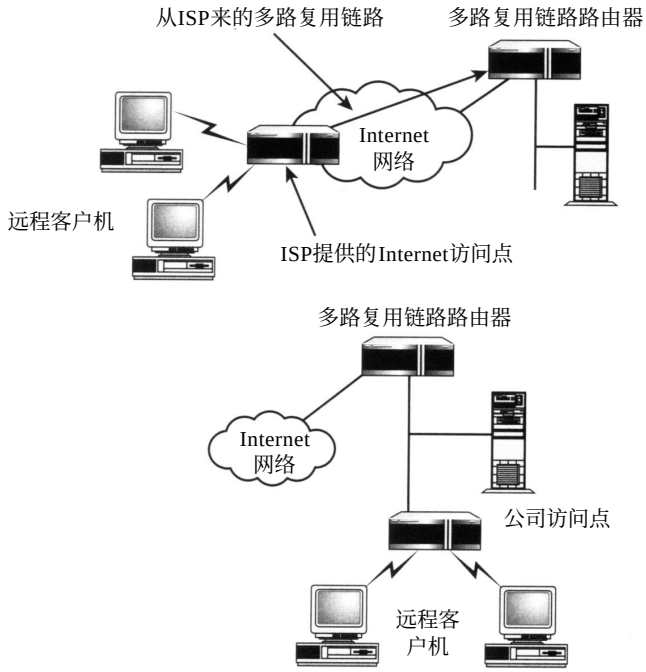

图17-12 使用远程访问设备的网络和一个使用远程ISP和多路复用器、多路分解器的网络

1. PPP会话汇聚

PPTP是基于客户机/服务器模型的协议，专门设计用于使用 PPP和第二层协议通过IP网络进行隧道传输。 PPTP能通过一条PPTP隧道支持多PPP连接。 PPTP在ISP模型中可以很好地工作，在这种模型中，多个远程用户必须导向一个特殊的公司实体 (参见图17-13)，这些隧道通常称为虚拟私人网(VPN)。

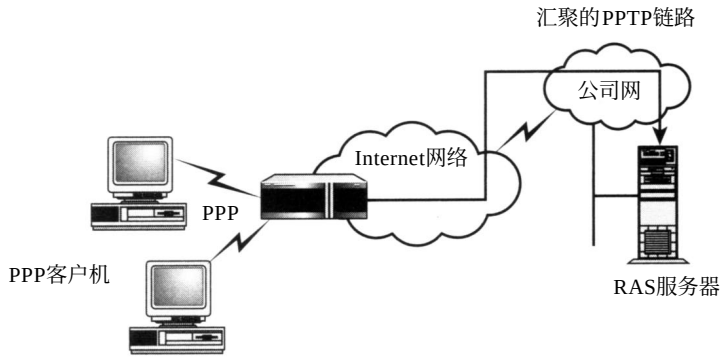

图17-13 PPTP支持多用户

对绝大多数ISP而言，这看起来好像不错，因为 PPTP需要带外控制用于TCP端口1723，这个端口由通用路由封装 (GRE)协议使用。然而GRE不像TCP或UDP那样普遍，所以许多 ISP不支持它。没有这个连接， PPTP将无法操作。

最常见的实现是在拨入存在点(Point of Presence， POP)之间提供服务。在这种方式中， ISP仅提供IP服务，而客户机和私有路由器协商 PPTP链路。应该注意并不是所有的 PPP软件都支持PPTP，因为PPTP不是标准协议。微软的视窗98和NT操作系统是支持这种服务的一个例子。

在LCP功能完成之后，物理连接就建立了，这时可以认证用户， PPTP依赖于PPP构造数据报。之后PPTP封装PPP报文，通过IP隧道发送报文。

2. 分离的控制信道

如前所述， PPTP使用两条信道来支持连接：一条数据信道和一条控制信道。控制信道在TCP端1723上运行。这个信道包含与链路状态和管理消息相关的信息。这些管理信息用于建立、管理、中止PPTP隧道。管理信道使PPTP具有控制数据传输速率的功能。这一功能对如下两种情况是很方便的： 1) 线路噪声很大； 2) 网络拥塞导致报文丢失现象。

封装进IP的数据流在节点之间传输，路由控制由 GRE来完成。并不是所有的 ISP都支持GRE，所以需要客户端和服务器建立自己的隧道。

3. 多协议支持

PPTP的另一个特点是支持多协议：如 NetBEUI、IPX，以及还在使用的 AppleTalk。因为PPTP是一个二层协议，它也包括和媒体相关的头，使它能在以太网或 PPP上操作。

4. 认证和保密

加密和密钥管理不是 PPTP规范的一部分。 PPTP依赖于PPP提供的认证协议并且依赖于PPP对数据进行加密。为了加强 PPP/PPTP的保密性，微软引入了一种新的加密方法称为微软点到点加密算法，这个算法以RSA RC4加密标准为基础。

PPTP使用CHAP、PAP、EAP及PPP支持的MS-CHAP进行认证。

5. PPTP隧道类型

PPTP能支持一些基本的隧道连接配置，如前面所述。隧道类型依赖于一些能力。首先也是最重要的是ISP支持GRE的能力，GRE是PPTP的要求。其次是客户机支持PPTP连接的能力。用户的计算机会决定隧道的端点；端点可以是 ISP的远程访问服务器(RAS)也可以是其自身的计算机。这两种连接类型分别称为主动隧道 (voluntary tunnel)和被动隧道(compulsory tunnel)。

(1) 主动隧道

在主动隧道中，用户初始化至公司计算机的 PPTP连接。然而，这意味着用户必须有一个可操作的PPTP客户机，如视窗9X或NT操作系统提供的一样。在这种情况下 ISP只需提供基本的IP服务(如图17-14所示)而无需提供其他任何服务。

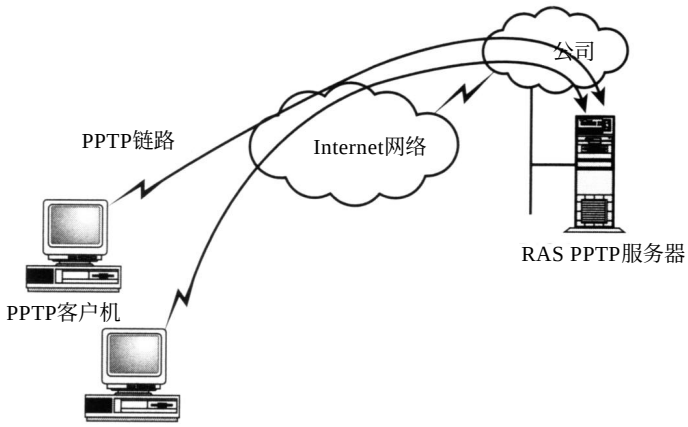

图17-14 用户通过Internet和服务器的PPTP连接

在ISP提供RAS服务器的情况下，客户机无需 PPTP客户程序；只需一个PPP客户程序。在被动隧道中，用户连接到ISP的RAS服务器，但却不控制隧道(见图17-15)。在绝大多数情况下，用户甚至不知道PPTP隧道的存在。

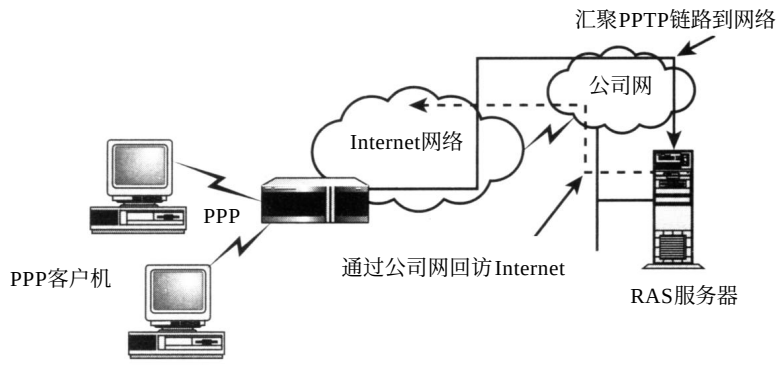

图17-15 被动隧道

(2) 被动隧道

被动隧道又分成两个子类：静态的和动态的。静态隧道使用指定的设备，也被称为基于域的，或手工的隧道。一个域是用户名的一部分并与用户的域联系起来。 RAS服务器会使用这个信息确定PPTP连接的终点位置。 RAS服务器必须手工配置来支持这种连接类型。这种类型的优点是公司可以控制用户使用 Internet的情况。这种方法允许用户连接到公司的内部网以

使用其服务。访问Internet要通过公司网络参见图(17-15)。

动态隧道更有效，因为隧道只是在需要时才存在。 RAS服务器连接到一台RADIUS服务器以便获得用户信息。隧道以用户存储的信息为基础构造。与使用和访问控制有关的信息存储在RADIUS服务器中，由RAS服务器在需要时获取。

被动隧道的另一个好处是其具有汇聚流量的功能。多个 PPP客户机能组合成一条至公司内部网的PPTP连接，因而降低了带宽要求，节约了相关成本。

被动隧道的一个缺点和安全相关。从客户机到 RAS服务器的链路不安全。然而，对于使用主动隧道的用户，也存在安全问题，因为没有方法可以阻止用户连接到 Internet下载一段恶意的代码。之后，再连接到公司网络上。

安全性是一门系统科学，必须在系统级找到解决方案。单纯的依赖于技术不能防止安全漏洞。

17.4.2 两层隧道协议(L2TP)

L2TP与PPTP在许多方面有非常相似之处。它结合了 PPTP和Cisco的二层转发 (L2F)。L2TP胜过PPTP的地方是L2F不依赖于GRE。这意味着L2TP兼容于其他媒体类型如 ATM或其他基于报文的网络如X.25。但是，规范必须要说明L2F报文的处理过程。最初的工作使用UDP，把L2F置于PPTP后面。

1. L2F

和PPTP使用方式相似， L2F使用PPP作为初始连接和服务(如认证)的提供者，和PPTP不一样，一开始L2F就使用终端访问控制器访问控制系统 (TACACS)。TACACS是另一个必要的服务。TACACS是Cisco的私用协议，为其路由器产品提供认证、授权和记账功能。 TACACS有一些限制，这将在本章后面讨论。

L2F也利用隧道连接概念，使其在L2F连接之内支持多条隧道。在加强安全级别的努力中，L2F支持额外的认证级。不仅仅在PPP级别认证，L2F还加入了在公司网关或防火墙一级的认证。

L2TP规范阐述了L2F的优点。L2TP使用相同的方法通过PPP支持远程用户。利用L2F工作，L2TP使用自己的隧道协议。当用户考虑迁移到 ATM和帧中继网络时，这个特性非常重要。

2. 认证

和PPTP一样， L2TP支持通过PPP的认证。使用PAP、CHAP及EAP建立到RADIUS服务器的连接， L2TP和PPTP具有相同的效果。为了加强这一级的效果， L2TP加入了 TACACS、TACACS+以及基于IPSec的服务。

3. IPSec支持

IPSec区别于其他服务之处在于IPSec是一个开放规范，它不仅支持认证，同时也支持保密。IPSec是比简单PPP模型更强的安全实现方法。从图 17-16可以看出， L2TP具有支持公共密钥结构(PKI)的功能， L2TP利用了LDAP和强认证服务。简而言之， PKI是一种管理公钥及其所支持证书的方法。IPSec支持使用许多不同的认证和加密工具，如 PKI依赖的非对称加密算法。虽然，本章会讨论这些安全机制，然而 PKI超出了本章范围，不在这里作讨论。

和PPTP一样， L2TP依赖于PPP建立连接。L2TP希望PPP建立物理连接，执行初始认证过程，构造PPP数据报，并且在中止时，关闭连接。其他就没有相似之处。 L2TP会和其他节点通信确定呼叫节点是否被授权，端节点是否希望支持 L2TP连接。如果是否定的，会话过程就

被中止。

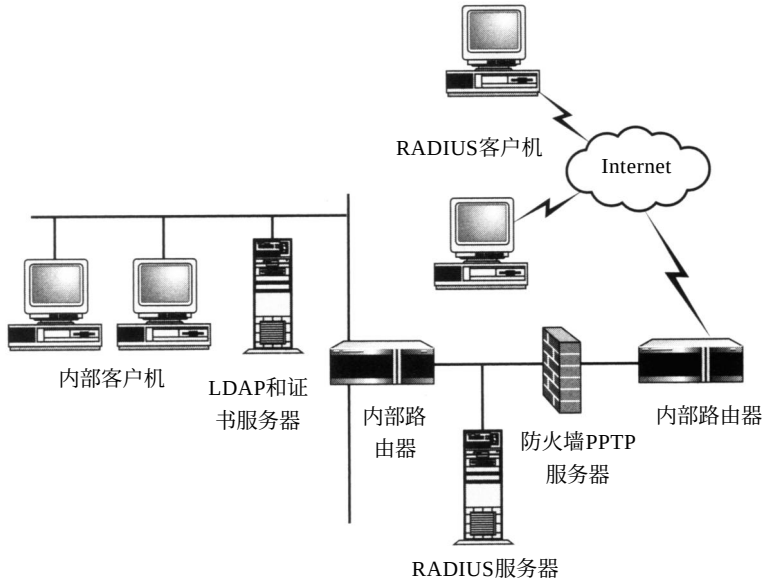

图17-16 L2TP和PKI

和PPTP一样，L2TP定义了两种不同类型的消息：控制消息和数据消息。控制消息用于建立和维护隧道并且控制数据的发送和接收。和PPTP需要两条信道不一样，L2TP把数据和控制信道组合成一条数据流。在IP网络中，就是把数据和控制封装进一个UDP报文，如图17-17所示。

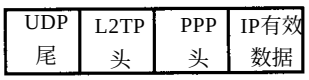

图17-17 封装数据和控制

有效数据实际上是PPP报文减去和媒体相关的帧元素。因为L2TP是2层协议，必然包括媒体头以指示下一层如何传输报文。这可以是以太网、帧中继、X..25、ATM或原始的PPP链路。如读者所见，非常多样。

为了减少网络拥塞，L2TP支持流控。流控在L2TP访问集中器(LAC)和L2TP网络访问服务器(LNS)之间实现；LAC的功能是作为网络访问服务器，LNS提供对公司网络的访问。控制消息包含与传送速率和缓冲参数有关的信息。通过交换这些信息 LAC和LNS能调整数据流，达到控制拥塞的目的(见图17-18)。

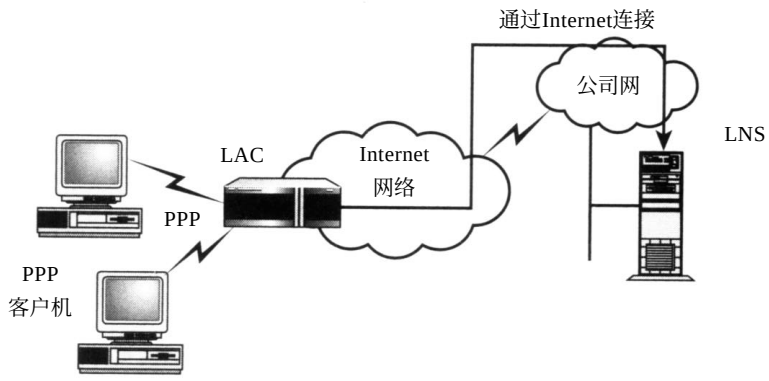

图17-18 LAS和LNS

L2TP实现的另一个减小网络开销的方法是压缩报文头。读者能想起PPTP具有相似的功能。

和PPTP相似，L2TP也支持两种连接类型——主动隧道和被动隧道。

在主动隧道中，用户从本机初始化L2TP连接。然而这意味着用户必须有一个能操作的L2TP客户程序。在这种情况下ISP只需提供基本服务(见图17-19)。

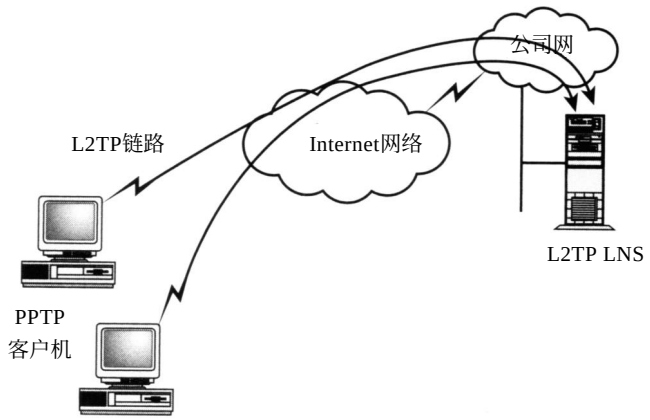

图17-19 用户到服务器的L2TP主动隧道

在ISP提供LAC的情况下，客户机不需要L2TP客户程序；而只需要PPP客户程序。在被动隧道中，用户联到ISP的LAC，但对隧道没有控制权(见图17-20)。在绝大多数情况下，用户甚至不知道隧道的存在。

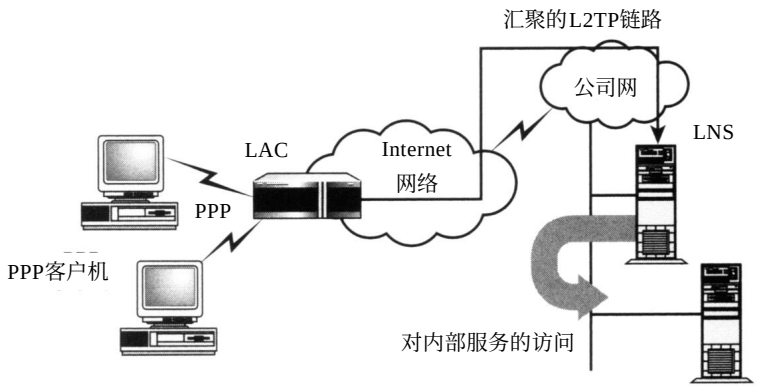

图17-20 通过ISP LAC的被动隧道

被动隧道有两个子类：静态的和动态的。静态隧道使用指定的设备。这种使用方法不利于使用资源，因为即使当隧道不再需要时，也不能使用设备。而且，LAC必须手工配置来支持这种连接类型。

动态隧道更有效一些，因为隧道只是在用户需要时才建立。LAC从认证服务器(如RADIUS或TACACS服务器)获得用户信息。被动式动态隧道与认证服务器一起使用会带来很大好处。隧道可以基于用户信息如电话号码和认证方法来定义。认证方法包括令牌和智能卡。在安全管理和金融事务中，可以执行额外的检查和记账处理，审查信息是部门变化之后仍使用原来服务的基础或者帮助协商ISP的速率。

这一优点与上一节描述的一样。用户连接到公司内部网以便得到相应服务，如果允许，

还可以通过公司网络访问Internet(见图17-21)。

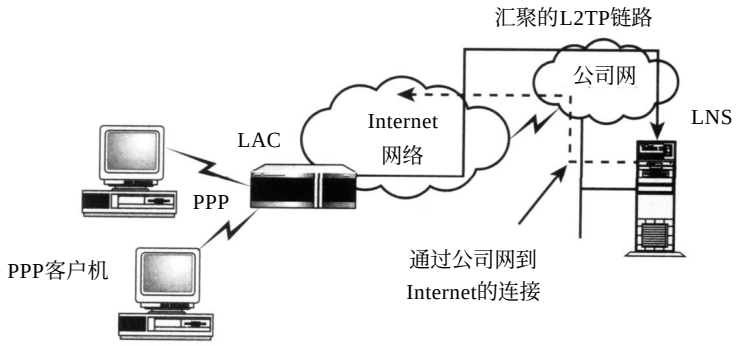

图17-21 到Internet的被动L2TP连接

使用被动隧道的优点是流量汇聚。多连接能组合到一条 L2TP隧道连到公司的内部网，这样带宽利用率更高，费用更低。

必须清楚被动隧道的缺点是从客户机到 LAS服务器的链路不安全，因为它仅使用简单的PPP链路。如前所述，使用主动隧道的用户也有安全问题。因为无法阻止用户联到 Internet，下载一段恶意代码，之后再联到公司网络。

和PPTP实现中的情况相同，安全性是一门系统科学，必须在系统一级找到解决方法。不能仅仅依赖于技术提供安全性。忽略文化上的问题和解决方法不会杜绝安全漏洞的出现。

L2TP通过ISP的认证，比PPTP使用的认证复杂。在和 ISP的初始联系过程中， ISP使用以下三个元素之一标识用户：

- 呼入的电话号码
- 被呼叫的电话号码
- 用户名或ID

这一步完成之后， ISP LAC会产生一个新的呼叫 ID标识隧道内的会话，并把信息转发到公司网络的LNS上(参见图17-22)。

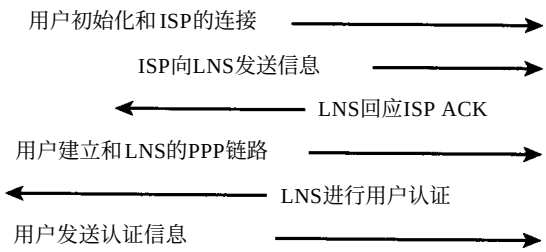

图17-22 L2TP认证过程

之后，公司网络负责检查提供的信息并决定是否接受还是拒绝连接请求。如果接受呼叫请求，下一步是PPP认证。虽然端点已经被标识和认证，需要格外注意消息仍以名文传送。任何运行的监听程序都能劫获用户数据。同时，报文也能插进报文流来试图迷惑或误导接收方。通过提供保密机制， IPSec能解决这一问题。

PPP提供加密，但是PPP使用共享的密钥来对数据进行加密。双方必须知道这一密钥才能

工作。这意味着必须使用带外方法进行密钥分发。 L2TP隧道认证也是这样。而且，即使使用PPP加密，L2TP也不保护控制信息。IPSec能解决这一问题。

17.4.3 IPSec

由于TCP/IP实际上不提供任何保护机制，因此过去这些年出现了许多方法来弥补这一不足。然而，这些方法不具有跨平台能力，也不能可靠地工作。为了解决这一问题， IETF设计了一组协议，即IPSec。虽然本节不讲述虚拟专用网 (VPN)，但是L2TP能非常有效地利用大量IPSec函数，所以本节会简要地看一下 IPSec特性。

IPSec最初设计用于IPv6标准的出现，在1995年出现的RFC 1825-1829讨论了如何在IP数据报上进行认证和加密。之后不久，这些 RFC被修改，解决Internet IPv4地址模式问题。这些规范把解决方案分成两类：

- 认证
- 加密

认证部分由认证头(AH)标识，加密部分由封装安全数据 (ESP)标识。每一种功能由不同的头表示，如图17-23所示。

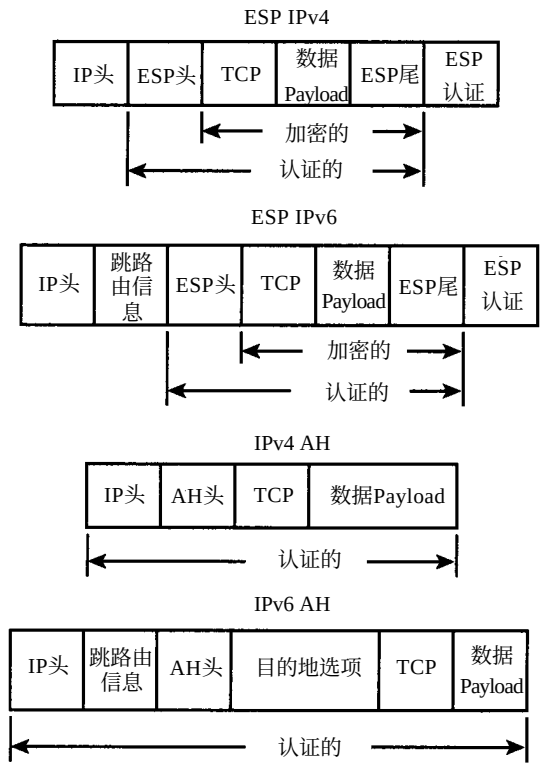

图17-23 IPSec报文头信息

1. 基于标准的加密

一起使用时，两个功能可以提供认证和保密。除了认证和保密之外，不像到目前为止讨论的其他认证，IPSec也能提供数据完整性功能。数据完整性是指确定数据在传输过程中是否

被修改过。如果这些数据恰好是公司合同或用户的工资存单，数据完整性就是很重要的，

为了确保兼容性，IPSec标准建造于许多密码标准之上：

- D-H或Diffie-Hellmann，用于密钥交换。
- 公钥密码算法，用于D-H密钥交换签名。
- DES加密。
- MD5、SHA以及HMAC(基于Hash的消息认证码)，用于带密钥的hash算法。
- 数字证书。

这种方法的主要强大之处是其多样性。一个新算法开发出来之后可以插入IPSec体系结构中，如图17-24所示。

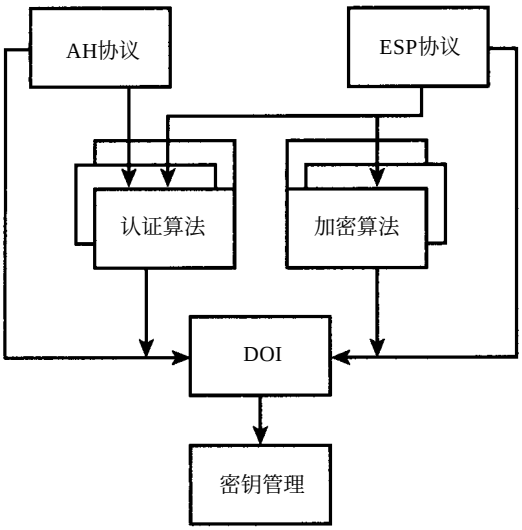

图17-24 IPSec体系结构

2. 建立安全联合

为了开始安全通信过程，双方必须建立一个安全联合（SA)。虽然有建立安全通信信道的缺省设置，但IPSec提供了不同密钥值、算法及计时设置协商功能。为了对各种值进行解释，IPSec使用解释域(DDI)概念来标准化这些元素。这样使得建立SA更容易。SA确定以下各项：

- 认证算法模式以及AH中使用的密钥。
- 加密算法模式以及ESP中使用的密钥。
- 密码同步参数。
- 通信认证过程中使用的协议、算法和密钥。
- 通信私有过程中所有的协议、算法和密钥。
- 认证和私有密钥交换的频率。
- ESP使用的认证算法、模式、转换和密钥。
- 密钥生命周期。
- SA生存时间。
- SA源地址。

3. 认证

AH提供了一种很强的认证报文发送者及其包含信息的方法。使用密码 hash函数产生一个校验和，校验和与其他控制信息一起插到IP头和其他报文头之间(见图17-23)。

4. ESP

由于AH所做的全部工作就是验证报文的发送者以及报文没有被修改过， AH不能防止内容被监听。这就是提出ESP的目的， ESP会在IP头和报文其他部分之间插入自身信息，这个信息使用安全参数索引(SPI)进行了加密。应该注意许多不同的操作模式会产生令人感兴趣的功能。其中一个操作模式是隧道(见图17-25)。

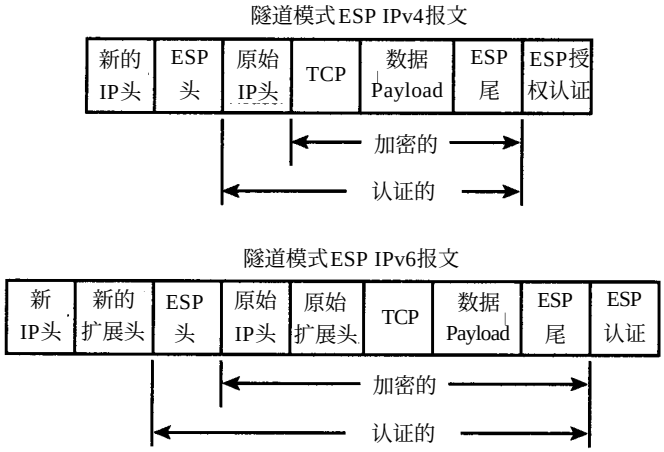

图17-25 隧道化IPSec

5. 隧道

在隧道模式中，整个报文被加密、被认证，并且报文前面加上中介网关如防火墙的地址。这样可以防止目的地址暴露给偷窥者。

正如读者所看到的， IPSec对PPTP或L2TP安全性进行了很大的改进。然而，现在产品中IPSec仍然不长见。

17.5 小结

有许多方法可以把远程用户和本地局域网连接起来。 SLIP、PPP、PPTP以及L2TP提供了不同程度的功能和保护。

PPP提供了连接到服务器所需的基本服务，并且比早期的 SLIP功能强很多。PPP具有控制链路和支持多协议功能，成为优于 SLIP的远程连接选择。 SLIP，功能简单，可能适合于指定的终端连接但SLIP缺少PPP的健壮性和多样性。

为PPP增加功能， PPTP使ISP和公司能更有效地利用 Internet。通过支持更多的协议，PPTP能使内部网服务扩展到家庭和远程用户的膝上电脑。利用远程认证机制如 PAP、CHAP以及RADIUS，PPTP增强了组织对使用网络资源用户的控制。

再为PPP添加上功能， L2TP在使用Internet资源及其相关的、多样化的介质时，组合了许多最好的协议。通过使用强的安全模型如 IPSec，L2TP更好地限制了远程访问客户机的能力。为网络加上更多的功能，必须有新的方法来适应，以保证这些功能不被错误使用或滥用。当人类进入新千年时， L2TP有希望支持这些功能，并有希望支持 IPv6。