维普资讯 http://www.cqvip.com

这是一种相当简单的封装技术，一个外层的IP报头被加在原始的IP报头之前，它们之间可以是其他任何有关路径的报头，例如，针对隧道配置的安全报头。外层IP报头的源和目的确定隧道的端点，内部IP报头的源和目的确定报文的原始发送者和接收者。封装格式如图5所示。

外层IP报头	隧道头	内层IP报头	IP有效载荷

图5 IP-in-IP封装格式

2.5 L2TP(第二层隧道协议)

L2TP是IETF结合Cisco的第二层转发(L2F)和Microsoft的点对点隧道协议(PPTP)开发出来的，可用于建立强制型隧道(Compulsory Tunneling)和自发型隧道(Voluntary Tunneling)。L2TP协议扩展了PPP协议模型。它使得与用户建立第2层链路的设备不需要具备NAS(Network Access Server)的功能，NAS服务器可以位于IP网络上的其它主机中。在这里，第2层链路设备只需要从第2层链路上获取用户的PPP数据包，然后通过L2TP隧道转发给NAS服务器。因此，PPP会话的路径显然延长了，不再仅仅限制在第2层链路上。L2TP的协议模型如图6所示。

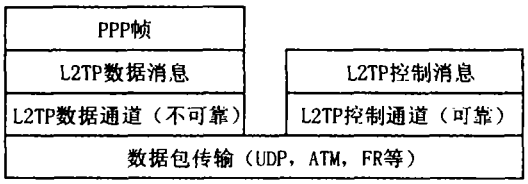

图6 L2TP协议模型

3. 隧道技术比较

3.1 隧道复用

为了减小隧道建立的时延和降低处理开销，可能让多个VPN共用一条隧道，但需要区分不同VPN的数据包和传输要求，所以，在隧道协议中需要有一个复用域。

MPLS作为VPN的隧道机制时，采用了两层标记堆栈的LSP，上层标记用于穿过MPLS骨干网，底层标记用于区分不同的VPN，所以，MPLS支持隧道复用。IPSec通过AH和ESP的SPI(安全参数索引)域在两个对等设备间复用安全联盟或隧道。L2TP有Tunnel-id和Session-id，通过Tunnel-id可以在两端点间建立多条L2TP隧道，通过Session-id可以在一条隧道中建立多个会话。GRE的描述中没有明确支持复用，但可以扩展GRE的关键字(KEY)域而作为复用域。IP-in-IP不能支持隧道复用。

3.2 多协议支持

一个VPN建立起来以后，不能限制VPN中传输的只能是IP包，作为传送VPN数据的隧道应该能够支持各种网络协议，如IP，IPX，AppleTalk等等。

MPLS可以承载IP数据包和其他协议的数据包。GRE支持任何类型的载荷协议。IPSec需要进行扩展才能携带IP之外的数据报，例如GRE可以与它一起使用，得到如(IP(IPSec(IP(GRE(非IP协议)))))的结构。IP-in-IP只能支持IP数据。L2TP传输的是PPP数据包，因为PPP是多协议的，所以L2TP也能支持多协议。

3.3 对QoS的支持

支持QoS是专用网的特点，所以，QoS也是VPN的基本要求。一般与QoS相关的因素是带宽、时延和时延抖动的保证，峰值速率，不同的服务水平协商(SLA)等。

MPLS本身没有QoS或SLA的管理机制，但其他的技术如DiffServ可以与MPLS一起使用来支持QoS。GRE的QoS能力依赖于传送协议。IPSec本身没有QoS或SLA能力，其他的机制如DiffServ可以与IPSec一起使用。IP-in-IP没有QoS或SLA能力。L2TP报头包含1-bit的优先级域，可以为需要优先级处理的数据包所使用。

3.4 对安全的支持

安全是构建VPN的重要因素，VPN业务提供商和客户都会对VPN解决方案的安全提出他们的要求，所以，隧道协议应该提供一定程度的安全机制。

MPLS具有与ATM或FR相同级别的安全能力。根据前面的概述可知，IPSec提供的安全级别是最高的，能够提供数据完整性认证、数据来源鉴别和防重传保护，保证数据机密性和通信流的机密性等各种级别的安全服务。而其它隧道技术的安全能力要弱得多，如L2TP只能继承PPP协议的认证和加密；GRE有一个可选的4字节关键字域，可用来进行数据源的认证；IP-in-IP没有提供安全机制。

3.5 隧道的建立和维护

可以通过网络管理，采用手工的方法来实现隧道的建立和维护，但这只适应于规模较小的网络，所以，一般使用专门的信令协议或控制协议来实现隧道的建立和维护，这样，可以提高VPN的可扩展性。

MPLS可以通过标记分发协议LDP[7]或资源预留协议RSVP[8]来建立和维护LSP，扩展的BGP也能携带标记信息[9]。GRE没有具备建立和维护GRE隧道的标准方法。IKE用于IPSec隧道的建立和维护。IP-in-IP利用IP协议的ICMP消息进行隧道的建立和维护，不需要额外的带宽开销。L2TP控制协议用于建立隧道，L2TP另外定义了一些管理和维护操作，如周期性地发送Hello消息来判断隧道的连通性和使用Next Sent(Ns)和Next Received(Nr)域来实现隧道的流量控制和拥塞控制等。

3.6 对最大传输单元(MTU)的要求，隧道开销的最小化和帧的有序性

MPLS对MTU的大小没有限制；标记交换的开销很小；MPLS能够保证有序的包传输。GRE对MTU的要求依赖于传送协议；GRE包头的开销被设计得比较小；序列域可以用来完成数据的有序传输。IPSec对MTU的大小没有限制；IPSec的设计可能会加重处理的开销；IPSec有一个序列码域被接受者用来进行防止报文重传检验，不是用来保证有序的报文传输，即IPSec不能保证数据的有序传输。IP-in-IP完全依赖于IP协议。L2TP本身没有分割和重组的能力，如果运行于UDP/IP之上，分割可以在需要的时候进行，也可以通过PPP协商MTU来防止分割；数据平面的开销包括UDP、L2TP和PPP报头，控制面的开销在于L2TP和PPP的控制协议；L2TP支持有序的数据包传输。

4. 隧道技术综合分析

通过对上述隧道技术的比较，可以发现不同的隧道技术具有各自不同的特点，现在对它们作一些综合性的分析。

MPLS是对IP现有组网模式的革新，包括路由和转发体系结构。MPLS提供了传统路由器与IP现有组网模式不具备的解决方案，如显示路由、流量工程。MPLS既保护了现有电

维普资讯 http://www.cqvip.com

信网的投资，也保护了现有因特网上传统路由器的投资，又实现了两者的融合并向宽带分组化网络平滑演进和升级，使网络运营商能在业务量快速增长和QoS要求的外部因素、网络资源优化的内部因素间找到了合适的平衡点。因此，MPLS已经发展成为一种被普遍认同的理想的骨干网技术。在MPLS网络上构建的VPN，由于标记堆栈的运用，使得VPN具有了很好的可扩展性，另外，MPLS在流量工程方面的优势，将会为VPN QoS问题的解决提供良好的解决方案。

IPSec是IETF为了解决Internet没有任何安全保障的现实，经过几年的努力，开发出来的一种基于IP协议层的网络安全体系结构。IPSec提供了一种标准的、健壮的和内容广泛的安全机制，通过对网络层IP协议的扩展，增加了安全协商、数据包和通信流的加密、数据完整性和数据来源认证以及面向主机的访问控制等安全措施，为IP及上层协议(如TCP和UDP)提供安全保证。由于IPSec提供了高级别的安全保障，加上它是IETF制定的标准，所以，IPSec是解决VPN数据安全和网络安全的首要选择。

GRE的突出特点就是它的通用性，适合任何的网络协议。它本身并不具有传送能力，但它是传送协议和被传送协议之间的桥梁，它使得在任何网络环境下，都能够实现隧道技术，实现数据包的透明传输。例如，它能实现在IP上封装一个IP载荷数据包。

IP-in-IP的特点就是简单，而且它直接利用IP协议的ICMP消息，实现隧道的建立和维护，不需要额外的开销。它的局限性就是许多功能都要依赖于IP协议，制约了它的使用。

L2TP最显著的作用就是将NAS服务器与第2层链路设备分离，不再要求NAS服务器必须是第2层链路终端。由于L2TP可以建立在ATM、FR或IP网络上，因此NAS服务器可以是ATM网络、FR网络或IP网络上的任何一台主机。对VPN而言，L2TP是实现VPDN(虚拟专用拨号网)[10]的重要技术，已经在电信网中广泛使用。

经过以上的分析可知，各种隧道技术的功能差异显著，优势明显，如MPLS VPN有良好的可扩展性，IPSec能提供高级别的安全保证等，所以，结合它们各自的优势是势在必行，可以看出，VPN的发展有这样的趋势：(1)在MPLS网络上构建VPN；(2)利用MPLS的流量工程优势实现VPN的QoS保证；(3)通过IPSec实现VPN的数据安全和网络安全；(4)远程访问企业网采用L2TP隧道技术。

结束语 通过对比分析，不同的隧道技术各有特点，功能差异比较大，所以，希望在VPN中只采用一种隧道技术是不可能的，VPN领域中势必是各种隧道技术共存，特别是MPLS、IPSec和L2TP之间的相互融合有可能会成为VPN发展中的一个重要研究方向。本文只对相关的隧道技术进行了宏观上的分析比较，具体的融合方案有待进一步研究。

参考文献

1 Callon R, Suzuki M, Gleeson B, et al. A Framework for Provider Provisioned Virtual Private Networks. Internet-draft (draft-ietf-ppvpn-framework-01.txt), July 2001

2 Rosen E, Viswanathan A, Callon R. Multiprotocol Label Switching Architecture. RFC3031, Jan. 2001

3 Hanks S, Li T, Farinacci D, et al. Generic Routing Encapsulation (GRE). RFC1701, Oct. 1994

4 Kent S, Atkinson R. Security Architecture for the Internet Protocol. RFC2401, Nov. 1998

5 Simpson W. IP in IP Tunneling. RFC1853, Oct. 1995

6 Townsley W, Valencia A, Rubens A, et al. Layer Two Tunneling Protocol "L2TP". RFC2661, Aug. 1999

7 Andersson L, Doolan P, Feldman N, et al. LDP Specification. RFC3036, Jan. 2001

8 Braden R, Zhang L, Berson S, et al. Resource ReSerVation Protocol (RSVP) --Version 1 Functional Specification. RFC2205, Sep. 1997

9 Rekhter Y, Rosen E C. Carrying Label Information in BGP-4. Internet-draft (draft-ietf-mpls-bgp4-mpls-05.txt), Jan. 2001

10 Gleeson B, Lin A, Heinanen J, et al. A Framework of IP Based Virtual Private Networks. RFC2764, Feb. 2000

(上接第130页)

加密算法，加密数据分组长度为1024比特。选定的消息认证码(MAC)方案是HMAC_SHA-1_160。

F_{2^m}上基于ONB的椭圆曲线加密软件的实现，归根结底是通过基于ONB的F_{2^m}上的域元素运算、椭圆曲线点的运算、点及域元素间的转换等基本算法来实现上面提出的加密方案。这些基本算法在第2、3节已进行了说明和分析。

实现中，我们采用Turbo C 2.0作为开发工具，并将开发的软件以动态链接库(ECC.dll)的形式提供给用户使用。目前，该软件包已应用在成电领先软件有限公司研发的"用户身份识别"项目中，其基本思想是在客户端通过指纹传感器采集用户的活体指纹，然后通过该加密软件包将指纹信息加密传输到服务器端，最后在服务器端解密指纹信息并进行匹配，达到身份认证的目的。通过实际测试，该软件的安全性、运行效率完全合乎要求。

结束语 由于椭圆曲线密码体制与其他公开密码体制相比，在安全性和执行效率上具有独特的优势，因此基于ECC的安全应用正成为密码学界研究的热点。

本文设计的加密软件既保持了ECC的安全性，同时具有对称密钥加密体制的速度。我们下一阶段的工作：一是对开发的软件包进行严格的测试；二是从事基于ECC的门限密码体制的研究。由于门限密码体制一般采用同态密码算法(如RSA)来实现，因此基于ECC的门限密码体制研究中尚有许多难点需要解决。

参考文献

1 张险峰，秦志光，刘锦德. 椭圆曲线加密体制的性能分析. 电子科技大学学报，2001

2 Ceiticom Corporation Whitepaper. Canada: Ceiticom Corporation, 1997

3 IEEE P1363. Standard Specifications for Public Key Cryptography Draft Version 13, 1999

4 Agnew G B, Mullin R C, Vanstone S A. An implementation of elliptic curve cryptosystems over $F_{2^{155}}$. IEEE journal on selected areas in communications, 1993, 11(5): 804～813

5 Lopez J, Dahab R. An O verview of Elliptic Curve Cryptography. http://citeseer.nj.nec.com/333066.html

6 Menezes A J. Elliptic Curve Public Key Cryptosystems. USA: Kluwer Academic Publishers, 1993

7 Desmedt Y. Some Recent Research Aspects of Threshold Cryptography. http://www.cs.fsu.edu/~desmedt/ISW97.ps