虚拟专用网实现的统一框架

刘桂开
(中国联通广州分公司数据部　广州510630)

摘　要　虚拟专用网(VPN)是一个在公共网上建立的逻辑网,它的链路就是隧道。本文通过对VPN隧道建立的分析,构筑了实现VPN的一个统一的框架,并讨论了其对VPN QoS及安全的影响。

关键词　虚拟专用网,隧道模式,隧道代理,统一框架

Unified Framework for Realization of Virtual Private Network

LIU Gui-Kai
(Data Department,China Unicom,Guangzhou 510630)

Abstract　Virtual private network is a logic network established over public network and its 'links' are tunnels. This paper constructs a unified framework for realization of virtual private network (VPN)by analyzing establishment of VPN's tunnels, and discusses the effects to VPN QoS and security.

Keywords　Virtual private network (VPN), Tunneling mode, Tunneling broker, Unified framework

"网络"就是一个能够以某些方式进行通信的设备的集合,这些设备可以是交换机、路由器、主机、打印机等,它们之间能够实现数据的接收和传送。其中连接这些通信设备的链路(Link)是网络的重要组成部分,它们决定着网络的拓扑结构、路由以及流量分布等许多重要的方面。由此联想到虚拟专用网在逻辑上也是一个"网络",它的链路就是"隧道",因此,"隧道"同样决定着虚拟专用网的许多重要方面。本文希望从分析VPN隧道的建立出发,对VPN实现体系作一个一般化的描述,并阐明隧道的建立对其它技术以及VPN实现的影响,即从体系结构的层面上来考虑隧道在VPN实现中的地位关系。

图1是采用统一建模语言UML对基于网络的VPN系统进行描述的用例图,从中可以看出,如果要实现VPN,需要的功能单元(用例)包含隧道技术、数据加密技术、流量工程技术和VPN管理等,但隧道是VPN数据的传输通道,所以VPN数据的安全和QoS保证都与隧道密切相关,由此可见,隧道的建立是VPN实现的最关键部分,是其它VPN技术得以展开的基础。

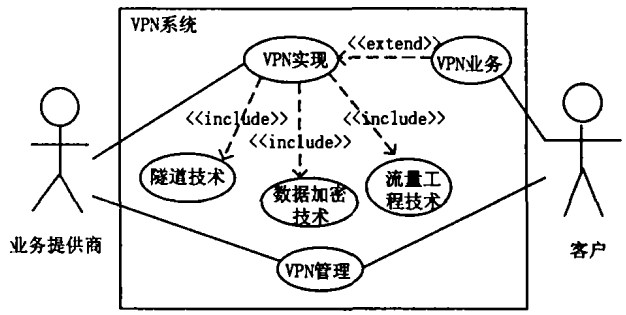
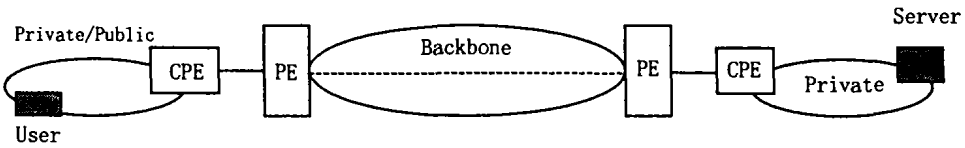


图1　基于网络的VPN系统用例图

1. 隧道的跨度

首先来讨论一下在构建VPN时,由隧道起点和终点的不同所呈现出的各种隧道情形。



PE: Provider Edge device
CPE: Customer Premises Equipment

图2　VPN的网络结构

图2表示的是VPN的一般网络结构(当User经过公用网络接入时,User端没有CPE设备)。假设需要建立User和Server之间的连接,根据穿过骨干网隧道的起点和终点,可以组合出如下一些隧道模式,其中User和Server都是终端系统,用End表示:

PE-to-PE;PE-to-CPE;PE-to-End;
CPE-to-PE;CPE-to-CPE;CPE-to-End;
End-to-PE;End-to-CPE;End-to-End;

总共有九种可能的隧道模式,其中PE-to-PE和CPE-to-CPE分别是业界讨论较多的基于网络的VPN和基于CPE的VPN,可以看出,如果从实现VPN设备的位置来对VPN进行分类,则VPN的类型不会超过九种,如图3所示。

刘桂开　工学博士,主要研究方向为宽带ATM和IP技术。

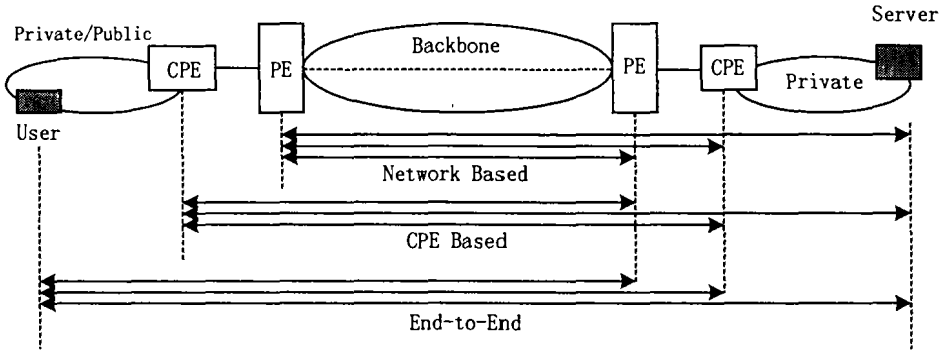


图3 九种可能的隧道模式

隧道的建立，一般是由一端发起建立。在建立 User 和 Server 之间的隧道时，假设由 User 端发起，最常见的情况是 User 是一个移动用户，他需要访问自己公司内部的站点。这种情况下，End-to-PE、End-to-CPE 和 End-to-End 都有可能，只是 End-to-PE 隧道需要 User 向 SP(Service Provider)提出申请才能建立。

当由 PE 发起建立时，最有可能，也是最常见的情形是 PE-to-PE，因为这是在它自己的管理域进行操作。如果要建到 CPE，即 PE-to-CPE 模式，CPE 可能是专用网中的通信服务器，这时需要跨越不同的管理域，只有在专用网有这样的要求时才会允许建立。至于 PE-to-End 隧道模式一般情况下不会有这样的需求。

当由 CPE 发起建立时，CPE-to-PE、CPE-to-CPE 和 CPE-to-End 三种情形都有可能。CPE-to-CPE 和 CPE-to-End 隧道的起点和终点都是在专用网内，完全可以由客户自己决定。CPE-to-PE 隧道需要客户向 SP 提出申请才有可能建立。

当 User 通过公用网接入时，End-to-End、End-to-CPE 和 End-to-PE 都是自发型隧道(Voluntary Tunneling)，PE-to-PE 和 PE-to-CPE 是强制型隧道(Compulsory Tunneling)。

2. VPN 的拓扑结构

一个 VPN 的拓扑结构由 VPN 节点之间隧道的全连接或任意的拓扑结构组成的。对应不同的隧道实现模式，VPN 的拓扑结构是不同的。例如，当建立的隧道都是 End-to-End 或 CPE-to-CPE 时，VPN 的拓扑结构是位于同一平面(VPN 级)的全连接拓扑结构，而当建立的隧道都是 PE-to-PE 时，VPN 的拓扑结构是分级的全连接拓扑结构，只是在 SP 级是全连接的，就整个 VPN 来说，并不是全连接的。很明显，它们的可扩展性是：PE-to-PE 优于 CPE-to-CPE，CPE-to-CPE 优于 End-to-End。这也是为什么基于网络的 VPN 成为研究热点的重要原因之一。

对于 Hub-and-Spoke 这样的拓扑结构可能有多种隧道模式共存，如图4所示。

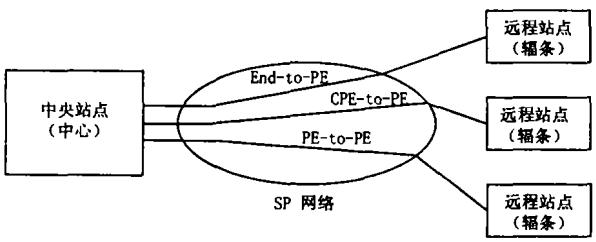


图4 中心和辐条式拓扑

在全连接或部分连接拓扑结构中，一般情况下，很少出现多种隧道模式共存的情形，但并不是说不能建立多种隧道模式，只要有需求，建立哪种隧道模式都是可能的，如图5所示，三个 Site 属于同一个 VPN，假设客户只与 SP1间有服务级协商(SLA)，而与 SP2没有，这样，Site1与 Site2之间的隧道可以是 PE-to-PE 的，而 Site1与 Site3之间的隧道不可能是 PE-to-PE 模式，只可能是其它的模式，如 CPE-to-CPE 或 End-to-End。有了以下介绍的综合实现平台的支持，就可以根据需要建立最适合需求的隧道。

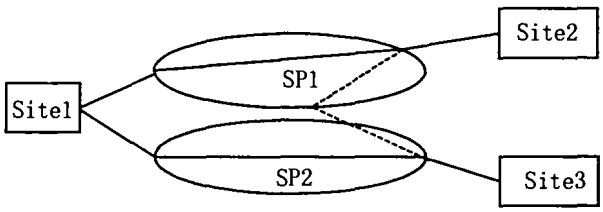


图5 全连接拓扑

3. VPN 实现的综合平台

VPN 实现的目的就是要在公用网络上建立一个能够进行私有通信的逻辑网络，再分细一些，就是要建立许许多多端到端的私有通信，如图2中的 User 和 Server。连接 User 和 Server 的 VPN 连接需要跨越三个网络，即 User 的接入网(可以是专用网或公用网)、SP 骨干网和 Server 所在的专用网。隧道是这条连接中必不可少的部分，图3显示了所有可能的隧道模式，隧道模式的不同就会产生不同的 VPN 实现，如基于网络的 VPN(PE-to-PE)和基于 CPE 的 VPN(CPE-to-CPE)。因此，只要把不同隧道模式的建立综合起来，就相当于综合了各种不同的 VPN 实现，将 VPN 的实现集成在一个统一的框架之中。

为了建立最适合需求的隧道(即最佳的 VPN 实现方式)，VPN 实现中需要引入一定的机制来控制不同隧道的建立。这样的控制的方法可能有许多种，这里提出一种称为“隧道代理(Tunneling Broker)”的方法，即由专门的代理服务器来控制隧道的建立。实施控制所依赖的是我们首先定义的一系列规则，也可以称为策略。假设所有的规则都存放在规则数据库中，规则的选择和隧道建立信息的下达都由隧道代理服务器来进行，如图6所示。

规则定义：任何适合网络环境和要求的规则或策略都可以动态生成，这可以由客户专用网的管理系统执行。例如，当客户与 SP 达成了服务级的协商(SLA)，隧道可以由 SP 来负责建立，可以是 PE-to-PE 模式或 PE-to-CPE 模式；如果客户

与 SP 没有达成服务级的协商(SLA),那么隧道就只能由 CPE 或 User 发起建立起来,SP 就不会参与隧道的建立。当然,规则的定义可能还包括更为复杂的细节,最起码生成的规则必须体现 VPN 的安全级别和 QoS 保障程度。

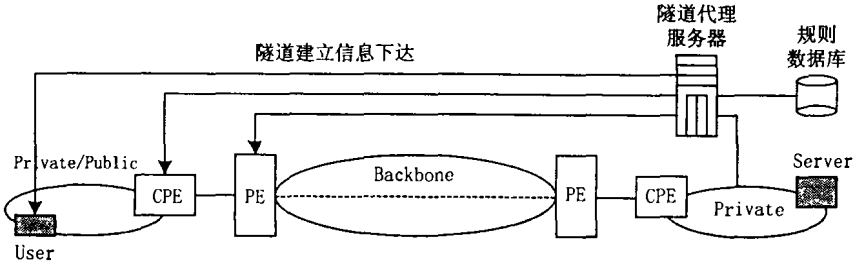


图6 代理服务器指示隧道的建立

隧道建立信息下达:

(1)User 向隧道代理服务器提出建立到 Server 连接的申请;

(2)隧道代理服务器对 User 的身份进行认证(身份认证也可能由专门的认证服务器来进行);

(3)认证通过后,代理服务器根据 User 提供的信息从规则数据库中提取相应的规则;

(4)作出选择后,代理服务器将隧道建立指示信息下达到相应的设备(PE 或 CPE),指示它们建立何种类型、达到什么要求的隧道,某些相关的信息也会通告给 User。如果代理服务器指示由 User 自己建立隧道,那么 PE 或 CPE 就不会收到建立隧道的指示信息。

VPN 实现的综合平台其实就是一个统一的 VPN 实现框架。通过对隧道建立规则的动态定义和更新,可以根据网络环境变化灵活建立最适合 VPN 要求的隧道,建立最能满足客户要求的 VPN,而且能够支持实时灵活的配置和管理。

4. VPN 安全

这里主要讨论隧道的建立对 VPN 安全的影响。我们说隧道可以将 VPN 数据流与公用网上其它的流量隔离开来,所以,隧道能够为 VPN 数据流提供一定级别的安全保障。可以这样说,通过隧道传输的数据流的安全至少不会低于那些不通过隧道而直接在公用网上传输的数据流。所以,在同等的隧道技术条件下,End-to-End 隧道模式所具有的安全保护是最高的,而 PE-to-PE 模式是最低的。当然,不同的隧道技术会提供不同的安全级别。

当 VPN 实现建立是 PE-to-PE 模式的隧道时,VPN 安全会变得较为复杂,因为它涉及到客户专用网的安全和 SP 网络的安全,由于 SP 网络是公用网,不可避免地会受到来自各个方面的攻击,对 SP 网络的任何安全威胁都会给 VPN 带来安全风险,特别是当 VPN 需要跨越多个 SP 网络时,VPN 的安全风险会大幅度地增加。由此可见,采用 PE-to-PE 隧道模式建立 VPN 时,SP 网络对 VPN 的安全起着决定性的作用。所以,这样实现的 VPN 虽然给 SP 带来了商机,减轻了客户的配置管理负担,但同时也承受着很大的安全风险。

当隧道的端点是 End 或 CPE 时,VPN 的实现是在客户专用网内部进行,受到攻击的可能性也是存在的,但与 SP 网络相比,所承担的风险要小得多,至少 VPN 的配置管理信息没有暴露在公共的网络环境中。

5. QoS 保证

在 VPN 中,QoS 保证指的是对 VPN 业务提供 QoS 保证,落实到网络中,就是要对 VPN 数据流传输的完整性、时延、时延抖动提供保证。因为隧道是传输 VPN 数据的通道,所以,VPN 数据的 QoS 保证是与隧道密不可分的。

网络中 QoS 的保证一般是通过流量工程的方法来实现,可以说流量工程是 VPN 业务的重要组成部分,而流量工程的目的就是要优化资源的利用和提高网络的性能,归根结底是要如何控制流经网络的数据流。VPN 数据是通过隧道来传输,所以控制 VPN 数据流的传输就是相当于要控制 VPN 隧道的建立。由此可见,VPN 业务的 QoS 保证,VPN 内的流量工程都将是针对 VPN 隧道来进行。例如,流量监测、业务分级、控制负载等。

结束语 隧道在 VPN 的实现中是最基本的部分,同时也是最重要的部分,可以说,隧道支撑着整个 VPN 的实现体系,对 VPN 的拓扑结构、安全级别和 QoS 保证都有着至关重要的影响。由于隧道是 VPN 连接中必不可少的组成部分,所以可以通过控制建立不同的隧道模式来满足相应的 VPN 要求,VPN 实现的综合平台就是一个统一的 VPN 实现框架,将许多不同类型的 VPN 实现集成到了一起。在 VPN 发展的初始阶段,VPN 实现主要集中在如何搭建 VPN 上,规则定义可能主要集中在建立不同的隧道模式上,但是,隧道对 VPN 安全和 QoS 保证都起着至关重要的作用,因此,随着 VPN 研究的发展,VPN 安全、QoS 保证将都会被包含在隧道建立规则定义的范围之内。在隧道建立对 VPN 其他技术的影响方面,本文只讨论了隧道对 VPN 安全和 QoS 保证产生的影响,但隧道在 VPN 实现的其它方面的作用也是相当重要的,如 VPN 管理,VPN 数据的转发等,均可以进行进一步的探讨。

参 考 文 献

1 OMG. OMG Unified Modeling Language Specification (draft v1.3). January 1999

2 UML 参考手册. www.China-pub.com

3 Gleeson B, et al. A Framework of IP Based Virtual Private Networks. RFC2764, 2000-02

4 Rosen E, Rekhter Y. BGP/MPLS VPNs. RFC2547, 1999.3

5 Braun T, Guenter M, Khalil I. Management of Quality of Service Enabled VPNs. IEEE Communications Magazine, May 2001

6 刘桂开,雷振明. 虚拟专用网隧道技术分析. 计算机科学,2003,30(1):99~101