IP VPN 业务管理中可重用管理组件的划分和应用

夏海涛,孟洛明,邱雪松
(北京邮电大学交换技术与通信网国家重点实验室,北京 100876)

摘 要: IP VPN(基于 IP 的虚拟专用网)业务管理面临的主要难题是,TMN(电信管理网)管理层次模型中业务管理层不断扩展的业务需求,可重用业务管理组件是降低动态变化的业务需求带来的业务管理复杂度、灵活地定制和提供 IP VPN 业务的有效途径. 本文首先分析了 IP VPN 的基本业务需求,提出了 IP VPN 业务属性的概念. 在此基础上,从 IP VPN 业务属性的视点对 IP VPN 业务管理功能进行了划分,形成可重用的业务管理组件. 最后,本文给出了一个业务管理功能向业务管理组件映射的实例.

关键词: IP VPN; 软件重用; 管理组件; 业务属性
中图分类号: TN915.07 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0576-04

Partition and Application of Reusable Management Components in IP VPN Service Managenent

XIA Hai-tao, MENG Luo-ming, QIU Xue-song
(Nation Lab. Of Switching Technology and Telecommunication Network, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: The main trouble that IP VPN (Virtual Private Network) service management has to face is the continuously developing requirements of service management layer in TMN (Telecom Management Network) model. It is an effective approach to reduce management complexity and neatly customize IP VPN services by providing reusable service management components. In this paper, we first analyze the basic service requirements of IP VPN, then bring forward and conclude the concept of "IP VPN service feature". On this foundation, we design a partition of IP VPN service management functions from the viewpoint of service features and form some reusable service management components. Finally, a mapping instance is given from service management functions to service management components.

Key words: IP VPN; software reuse; management component; service feature

1 引言

IP VPN 业务的提供和管理已经成为新一代 IP 网络的研究热点[1]. 在未来的"面向用户基于业务"的管理体系结构下,业务的可扩展性需求增加了 IP VPN 业务管理的复杂性. 这一点将导致在 IP VPN 业务管理的层次功能结构中,网元管理层和网络管理层的功能可以做到相对稳定,而业务管理层的功能却不断地扩展,成为 IP VPN 业务管理变数最大、管理最难的一层.

软件重用是降低计算机应用实现的复杂性,缩短系统开发周期的一个基本方法. 面对需求动态变化的业务管理层,提取 IP VPN 业务管理功能中独立于各业务模型的操作,分解成可重用的业务管理组件,是简化 IP VPN 业务管理的难度、灵活地定制满足用户特定需求的 IP VPN 业务的有效途径. 目前,国外关于组件在业务管理中的应用已有一些研究和原型系统[2,3],但这些研究与具体的组件实现技术相关,组件功能的定义都是基于特定的系统实现框架(如: Enterprise Java Beans),很难在其它的操作环境下重用. 在网络管理体系结构中设计业务管理层的功能,最为重要的原则是做到管理功能与具体的业务模型和实现环境无关,即具有一个标准化的业务管理功能. 本文首先分析了 IP VPN 的基本业务需求,从中归纳了反映不同 IP VPN 业务模型所共有的本质特征的业务属性. 然后基于软件重用的思想,从业务属性的视点对公共的 IP VPN 业务管理功能进行了可重用的业务管理组件划分. 最后通过具体的 IP VPN 业务模型介绍了如何将业务管理功能映射到业务管理组件集合.

2 IP VPN 业务属性

"业务属性"的概念在业务工程领域被普遍应用,它的提出旨在细化业务的共有特性和反映网络的支持能力,从而帮

收稿日期:2001-11-15;修回日期:2002-04-27
基金项目:国家杰出青年科学基金(No. 60025104);国家自然科学基金(No. 60202003);国家自然科学基金重大研究计划项目(No. 90204002)

助业务开发商和业务用户理解业务的内涵. 业务属性本身不是组成业务的功能构件,它更多地体现了从底层网络支持能力中提取的业务所包含的特征. 本文提出的 IP VPN 业务属性是从另外一个视点进行定义的,它面向业务用户,反映了业务用户对业务的基本需求,以一种自顶向下的方法归纳了 IP VPN 业务的本质特征. 在 IP 网络配置能力不变的情况下,通过这种方法定义的 VPN 业务属性能够适应不同 IP VPN 业务模型的业务配置需求.

IP VPN 业务属性是和 IP VPN 业务需求密切相关的. 虽然业务需求的确定存在着多个视点,如:业务用户视点、业务提供商视点等,但是这里存在一个基本的业务需求集合[4],能被不同的视点和业务模型所包容. 最基本的业务需求是功能需求,即:通过建立 IP VPN 业务站点之间的隧道连接以及复用于其上会话连接,向 IP VPN 业务用户提供可访问的网络资源的功能,这是提供 IP VPN 业务的前提条件,不涉及在 IP 网络中对 VPN 业务质量的控制和管理. 除了功能需求之外,这个基本业务需求集合还包括:

1) 能够支持用户定义的任意网络拓扑,IP VPN 业务的提供应该与具体的网络拓扑无关.

2) 提供一种能够分布和交换网络中的路由可达信息的机制,能够限制业务数据只访问路由数据或配置规定的业务站点.

3) 寻址能力:同一 VPN 内部的 IP 地址必须唯一地标识业务站点,而不同 VPN 的 IP 地址可以重叠.

4) 安全性:要求涵盖用户数据的机密性、完整性和源端认证,路由数据免受未授权实体的篡改,对业务用户的访问权限控制,VPN 之间的隔离以及端节点的认证和授权等方面.

5) 可管理性:激活 TMN 的网络管理功能域,建立业务提供商和业务用户之间的业务等级协定 SLA(Service Level Agreement)以及对 SLA 参数进行测量.

6) 互操作性:对于同一解决方案的不同实现,在网元级、网络级和业务级的多厂商环境的互操作性应该得以保证,这是业务提供商和业务用户最为关注的业务需求.

以上的 IP VPN 基本业务需求可以归为三类:第一类是基本的业务连接需求,主要目标是面向 IP VPN 业务数据流而建立 VPN 逻辑路径,包括对网络路由/连接的配置以及对 VPN 业务数据转发处理方法的确定;第二类是安全性需求,保证业务数据在 VPN 中传递的私密性以及防止非授权用户对 VPN 的访问;第三类是业务质量 QoS(Quality of Service)需求,对 VPN 网络的传输能力进行优化,提高业务数据在网中交换或转发的效率.

这个基本业务需求集合决定了 IP VPN 的业务属性. 一个新创建的 IP VPN 业务也相应地具备如下的三类共九个业务属性:

1) 基本业务连接属性,包括了业务站点的地址信息(IP 地址和端口号)、VPN 路由信息的分布策略和用户数据包的处理策略等三个业务属性. 基本业务连接属性是在 IP 公共基础网络中开通一个 VPN 业务所必需的连接配置,它们确定了一个 VPN 的逻辑拓扑以及拓扑中的业务数据可达的路径.

2) 安全属性,包括了数据加密算法、端用户认证方法、隧道对等体认证方法和站点访问控制等四个业务属性. 安全属性是区分普通的 IP 业务和 IP VPN 业务的重要标志,是 IP VPN 业务的核心要求. 用于支持安全属性的机制应该尽可能地对业务用户透明,以防止远程的业务用户通过多种方式接入 VPN 形成冲突.

3) QoS 属性,包括了业务带宽和服务优先级两个业务属性. QoS 属性决定了 IP VPN 业务管理系统的流量控制能力,反映了 VPN 业务性能优化的程度. 与这两个属性相关的带宽管理和分级服务(DiffServ)是解决 VPN 中数据拥塞的有效措施.

应当说明的是,这三类业务属性是由 IP VPN 基本业务需求集合自然归纳形成的,它们并不完全满足语义的"正交无关性". 安全属性类和 QoS 属性类中的属性彼此无关,而它们都或多或少地和基本业务连接属性类中的 VPN 路由分布策略和用户数据包的处理策略两个属性相关,因为在配置业务连接的时候需要根据相关的安全属性或 QoS 属性来决定策略中的行为.

3　IP VPN 业务管理组件划分

面向组件的网络管理系统[3]的产生主要来自网络业务的迅速发展,业务提供的时效性显得更加突出. 将网络管理功能映射到高可重用的管理组件可以改善网络管理系统对网络业务的支持能力,降低网络管理软件的开发成本. 根据软件工程对可重用的软件模块的可靠性、独立性和完备性设计要求,IP VPN 业务管理组件的划分应具有较好的抽象性和通用性,通过增大内聚和减小耦合而适于重用.

如何确定 IP VPN 业务管理组件划分的标准(尺度)是我们面临的主要问题. 在目前已经出现的多种 IP VPN 业务模型中,我们研究了三种具有代表性的 IP VPN 业务模型:基于 L2TP(Layer 2 Tunneling Protocol)的拨号 VPN、基于 IPSec(IP Security)的专线 VPN 和基于 MPLS(Multiple Protocol Label Switching)的 VPN[5],总结了各自的业务提供流程,得出的结论是这些业务模型都覆盖了本文给出的基本业务需求集合. 因此,虽然不同的业务模型能形成不同的业务需求,而不同的业务需求又可以定义面向具体业务模型的业务管理功能,但是从基

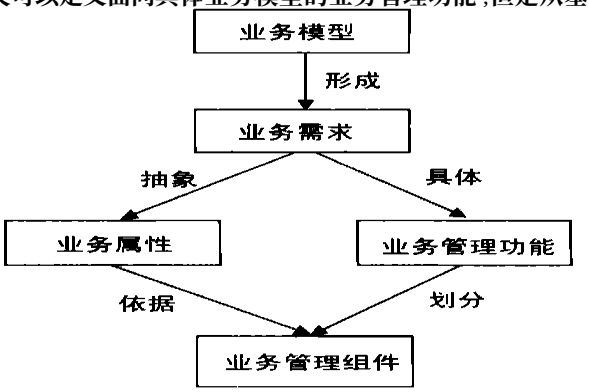

图 1　IP VPN 业务模型、业务属性、业务管理功能和业务管理组件的关系

本业务需求部分抽象出 IP VPN 的业务属性出发,以此来划分业务管理功能,可以有效地实现组件级重用的业务管理目标.以上描述的关系如图 1 所示.表 1 列出了我们研究的三种 IP VPN 业务模型和 IP VPN 业务属性之间的关联程度比较,这是由业务模型所采取的技术实现所决定的.除了业务站点地址信息是各业务模型必备的业务属性之外,各业务模型在保证 VPN 业务质量的技术实现中所侧重的业务属性不同:基于 L2TP 的拨号 VPN 侧重于对连接(包括隧道和端用户)两端的身份认证;基于 IPSec 的专线 VPN 侧重于保证业务数据的安全和完整;基于 MPLS 的 VPN 侧重于提高网络性能.

表 1 几种 IP VPN 业务模型及业务属性的关联

	基于 L2TP 的拨号 VPN	基于 IPSec 的专线 VPN	基于 MPLS 的 VPN
业务站点地址信息	必备	必备	必备
VPN 路由信息分布策略	弱关联	弱关联	强关联
用户数据包处理策略	弱关联	强关联	强关联
数据加密	弱关联	强关联	弱关联
端用户认证	强关联	弱关联	弱关联
隧道对等体认证	强关联	弱关联	弱关联
站点访问控制	弱关联	强关联	强关联
业务带宽	弱关联	弱关联	强关联
服务优先级	弱关联	弱关联	强关联

根据 IP VPN 业务属性划分的业务管理组件具有较好的稳定性和可扩展性,彼此功能相对独立,宜于在业务管理层业务管理组件功能的基础上灵活地配置面向特定业务模型的业务管理功能.VPN 路由分布策略和用户数据包处理策略本身所包含的语义比较复杂和易变,而从业务管理组件功能独立性的角度看,和这两个业务属性相关的业务管理功能不宜划分管理组件,以避免组件之间耦合度的增加.因此,在根据业务属性划分业务管理功能时,我们对这两个业务属性进行了弱化(即忽略不计),将其语义分解为更为独立的子属性是未来需要改进的工作.由 IP VPN 业务属性导出的可重用管理组件的划分表示为:

{基本隧道连接管理组件、数据加密管理组件、端用户认证管理组件、隧道对等体认证管理组件、站点访问控制管理组件、带宽管理组件、分级服务管理组件}

IP VPN 业务管理的目标是满足业务用户需求的拨号 VPN 业务或专线 VPN 业务.这个业务用户需求包含两个层面:基本的业务开通以及在此基础上的安全性和 QoS 的保证.因此,这里给出的功能划分覆盖了 IP VPN 基本业务需求,它适用于本文介绍的三种 IP VPN 业务模型.用自然语言描述各管理组件的功能如下:

1) 基本隧道连接管理组件 这一组件包括了 IP VPN 隧道连接的创建、删除、隧道连接参数的修改和查询等功能.对于隧道连接的建立,需要指明目标 VPN 标识和它所包含的隧道端点,也就是隧道两端的 PE(Provider Edge)路由器地址;另外也要指明每个隧道端点的邻接关系(即相邻的 PE 路由器地址).由于拨号 VPN 业务生成的是一个点到点的隧道连接,因此邻接关系就简化为隧道对等体端点的直连关系;而在专线 VPN 业务中,隧道连接的建立形成了一个网状的 VPN 拓扑结构.本组件在配置业务管理功能时为必选项.

2) 数据加密管理组件 这一组件包括了 IP VPN 业务数据加密的配置、去配和查询功能.加密配置需要指明目标 VPN 标识、加密算法和密钥长度,有时也需要指明压缩算法.本组件提供了网络传输中业务数据流的安全保证,是可选项.

3) 端用户认证管理组件 这一组件包括了 IP VPN 端用户认证的配置、去配和查询功能.认证配置需要指明目标 VPN 标识、端用户的身份(一般用域名表示)和用户认证算法(如:CHAP —Challenge Handshake Authentication Protocol、PAP —Proxy Authentication Protocol 等).本组件提供了 IP VPN 端到端访问的可靠性,是可选项.

4) 隧道对等体认证管理组件 这一组件包括了 IP VPN 隧道两端端点认证的配置、去配和查询功能.认证配置需要指明目标 VPN 标识、隧道两端端点的地址和隧道认证算法.本组件提供了 IP VPN 网段到网段访问的可靠性,是可选项.

5) 站点访问控制管理组件 这一组件包括了 IP VPN 业务站点访问控制策略的配置、去配和查询功能.策略配置需要指明目标 VPN 标识和业务数据包的过滤或分类算法,主要应用于外联网的业务模型中.本组件提供了对 IP VPN 业务站点限制访问的功能,是可选项.

6) 带宽管理组件 这一组件包括了 IP VPN 业务带宽的分配、去配、修改和查询的功能.带宽的分配可以使业务提供商预留出 IP VPN 业务所需的带宽,预防网络中出现业务数据拥塞.本组件是可选项.

7) 分级服务管理组件 这一组件包括了 IP VPN 业务优先级的配置、去配、修改和查询功能.在 IP 网络中提供分级服务借鉴了 ATM 交换网络中业务类型的思想,目前可提供的分级服务粒度较粗,可以分成实时业务、非实时业务和最大努力(*best effort*)业务.分级服务管理组件对 IP VPN 路由中数据流量分配的优化起到了重要的作用,本组件是可选项.

4 业务管理功能映射实例

目前,可提供的 IP VPN 业务主要分为拨号 VPN 业务和专线 VPN 业务两类.其中,拨号 VPN 业务作为最常用的 VPN 接入模型,而专线 VPN 业务则是内联网模型和外联网模型的总称.其它的 IP VPN 业务模型可以被视为这两种基本业务模型之上的扩展模型.

本节通过拨号 VPN 业务模型介绍 IP VPN 业务管理功能向业务管理组件的映射.拨号 VPN 提供了企业远程用户和企业网关之间的一条会话连接.会话连接的建立是通过远程用户拨号连接到本地的网络接入服务器 NAS,再由 NAS 通过 IP 网络建立起和网络另一端的企业网关的隧道连接.会话连接拓展了 IP 网络中实际存在的隧道连接,在连接建立的各个阶段对连接对等端的身份进行了有效的认证,为远程用户接入企业网提供了安全的端到端连接.目前,用于实现这一业务模型的隧道技术主要包括第二层隧道协议 L2TP、第二层转发协议 L2F 和点到点隧道协议 PPTP.

根据研究分析的结果,参考国际电信联盟 ITU-T 制定的关于 VPN 业务管理标准[6,7],我们提出基于 L2TP 的拨号 VPN

业务管理功能需求如下:

1) 业务管理系统对 L2TP 协议的隧道域信息的配置和管理. 隧道域指一个或一组隧道端点,在这里定义为业务管理系统管理范围内的 LAC (L2TP Access Concentrator) 和 LNS (L2TP Network Server) 端点对集,即:隧道域信息的配置和管理总是以 LAC 和 LNS 成对出现的. 功能主要包括指配隧道域信息、删除隧道域信息、修改隧道域信息和查询隧道域信息功能. 此外,还包括隧道域状态监控功能子集 (如隧道域的创建、删除、改变的报告功能). 以上的配置和管理均对隧道两端的 LAC 和 LNS 进行. 该功能集给出了业务管理系统对网络管理系统隧道连接管理的配置环境.

2) 业务管理系统对 L2TP 协议的拨号 VPN 业务用户信息的配置和管理. 拨号 VPN 业务用户信息是指端用户为了和企业网前端的 LNS 建立起端到端的拨号 VPN 业务而提供的业务相关信息,对网络管理系统要映射为会话连接的管理. 功能主要包括指配拨号 VPN 业务用户信息,删除拨号 VPN 业务用户信息,修改拨号 VPN 业务用户信息和查询拨号 VPN 业务用户信息等功能. 此外,还包括拨号 VPN 业务用户信息监控功能子集 (如拨号 VPN 业务用户信息的创建、删除、改变的报告功能);会话信息的查询作为一个辅助功能. 以上的配置和管理均对会话两端的 LAC 和 LNS 进行. 该功能集给出了业务管理系统对网络管理系统会话连接管理的配置环境.

实现这样的业务管理功能可以通过组合本文设计的三个业务管理组件来完成,它们分别是:基本隧道连接管理组件、端用户认证管理组件和隧道对等体认证管理组件. 其中,第一个和第三个组件用于实现 L2TP 协议隧道域信息的配置和管理;第二个组件用于实现 L2TP 协议的拨号 VPN 业务用户信息的配置和管理. 实际上,在这个业务模型中,端用户认证和隧道对等体认证决定了 L2TP 用户数据包的处理策略. 图 2 给出了 L2TP 业务管理功能和业务管理组件之间的映射关系.

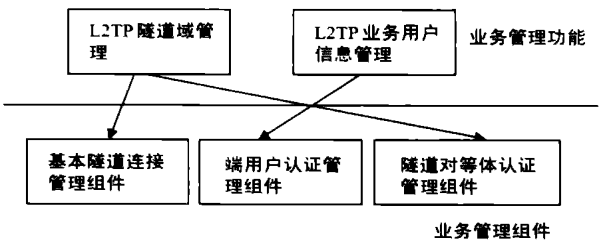

图 2　2TP 业务管理功能和业务管理组件之间的映射

通过组件综合形成的业务管理功能满足基于 L2TP 的拨号 VPN 业务提供的基本需求,但是仍然需要在业务管理层进行功能适配,以满足业务用户特定的业务管理需求.

5　结束语

本文从业务属性的角度对 IP VPN 业务管理的可重用管理组件划分进行了探讨和研究,并结合一个特定的 IP VPN 业务模型给出了业务管理功能向业务管理组件映射的实例. 可以说,在已经成熟而且定型的 IP VPN 业务模型 (如:L2TP、IPSec 隧道技术实现的业务模型) 中,这一划分覆盖了业务管理的功能需求,具有通用性,而且还可以灵活地制定满足业务用户特定需求的管理功能. 而对于尚处于发展变化中的 IP VPN 业务模型 (基于 MPLS 的 IP VPN),这一划分基本满足了目前的功能需求.

另一方面,IP VPN 业务管理是 IP 网络领域一个较新的研究课题,功能需求并不十分清晰,本文对所划分组件的功能描述粒度较粗,没有采用形式化的组件描述模板. 但是,这一划分方法具有较好的可扩展性,能够方便地增加组件来适应新的业务管理功能需求.

参考文献:

[1] Torsten Braun, Manuel Guenter, and Ibrahim Kualil. Management of quality service enabled VPNs [J]. IEEE Communications Magazine, May 2001:90 - 98.

[2] James W Gish, James F Tremlett. Building a service provisioning system using the enterprise javabean framework [A]. Proceedings of NOMS [C]. Honolulu, Hawaii, USA. 2000, 4:367 - 380.

[3] Taichi KAWABATA, et al. Component-oriented network management system development [A]. Proceedings of NOMS [C]. Honolulu, Hawii, USA. 2000, 4:395 - 408.

[4] IETF draft. Service Requirements for Provider Provisioned Virtual Private Networks [S]. February 2001.

[5] Panos Trimintzios, et al. A management and control architecture for providing IP differentiated Services in MPLS-Based networks [J]. IEEE Communications Magazine, May 2001:80 - 88.

[6] ITU-T Recommendation M. 3208. 3, TMN Management Services for Dedicated and Reconfigurable Circuits network: Virtual Private Network Services [S]. 1999.

[7] ITU-T Recommendation M. 3108. 3, Information Model for Management of Virtual Private Network Service [S]. 2000.

作者简介:

夏海涛　男,1972 年 8 月生于吉林省长春市,北京邮电大学交换技术与通信网重点实验室博士研究生,1993 年毕业于吉林大学计算机科学系,1996 年 5 月在华北计算技术研究所获得工学硕士学位,同年 6 月到北京邮电大学计算机学院工作,2000 年 9 月考入北京邮电大学攻读博士研究生,目前研究方向是电信/网络业务管理、新一代运营支撑系统和工作流程管理.

孟洛明　男,1955 年出生于河南洛阳市,北京邮电大学教授、博士生导师,程控交换与通信网国家重点实验室主任,主要从事网络管理、通信网、通信软件方面的研究、教学工作. 主持完成了 10 余项国家级的重大项目,获 10 余次国家和省部级科技进步奖.