第 23 卷 第 2 期 电 子 与 信 息 学 报 Vol.23 No.2
2001 年 2 月 JOURNAL OF ELECTRONICS AND INFORMATION TECHNOLOGY Feb. 2001

ATM 网中 VPN 业务管理的研究与实现 [1]

邱雪松 孟洛明 陈俊亮

(北京邮电大学程控交换技术与通信网国家重点实验室 北京 100876)

摘 要 基于 TMN 的逻辑分层体系结构，提出 VPN 业务管理的体系结构，分析了体系结构中各个子系统的功能．在此基础上，提出 VPN 业务管理所需的管理信息模型及其与 ATM 网络层 / 网元层的管理对象的映射关系，并详细讨论了系统中的安全管理功能．

关键词 电信管理网，虚拟专用网，逻辑分层体系结构

中图号 TN919.3

1 引 言

虚拟专用网(VPN)业务的提供与管理方式近年来已成为网络和业务管理的研究热点 [1]．欧盟的 RACE II 计划中有三个项目与 VPN 业务管理相关 (R2004PREPARE, R2041 PRISM, R2059 ICM)．这三个项目，基于电信管理网 (TMN)[2] 的框架，研究了 ATM 公众网中 VPN 业务管理的各个方面．PRISM 研究了 VPN 业务的带宽管理 [3,4]，ICM 研究了虚路经 (VP) 连接 (VPC) 和路由管理 [5]，而 PREPARE 则研究了多管理域环境下的业务管理，其中包括了 VPN 业务的管理 [6]．文献 [7, 8] 研究了客户网管理 (CNM), 着重于客户如何管理他们的 VPN 业务。

以上的研究工作或是仅仅着重于 CNM 系统和 ATM 公众网管理系统 (PNMS) 间的基于 SNMP 的 M3 接口 [7−9], 或是仅仅着重于 CNM 系统和业务提供者管理系统 (SPMS) 间的接口 $X^{[6]}_{\text{vpncust}}$，对 M3 或 X_{vpncust} 接口和 PNMS(或 SPMS) 与其管理的网络间的接口 M4[10] 间的关系则缺少相应的研究．本文在研究了基于 ATM 网 VPN 业务管理体系结构的基础上，提出基于通用管理信息协议 (CMIP, Common Management Information Protocol) 的 M3 接口信息模型，并仔细分析了 M3 和 M4 两个接口 的关系，提出它们间的映射关系．文章最后对我们实现的 VPN 业务管理原型系统的安全管理功能进行了详细的讨论．

2 VPN 业务管理的体系结构

ATM 网上的 VPN 业务 [3,4] 一般是基于 VP 网络的，即 VPN 业务客户租用若干条半固定的 VPC，形成自己的 VPN 网络，然后在半固定 VPC 的基础上，向用户提供虚信道 (VC) 连接 (VCC) 服务．

基于 ATM 的 VPN 业务的管理主要可划分为两个方面：(1) 配置和管理 VPN 业务，即在 ATM 物理网络之上如何向 VPN 业务客户提供 VPN 业务，主要包括创建 VPN 业务、删除 VPN 业务、修改有关 VPN 业务参数、增加 VPN 业务接入点 (SAP) 到 VPN 、从 VPN 移去 VPN SAP 和 VPN 业务参数查询功能及 VPN 业务状态监控功能 (如 VPN 业务的创建、

[1] 1999-04-14 收到，1999-10-06 定稿
国家 “95” 攻关项目 (96-742-03-01) 资助课题

删除、配置改变的报告功能)。(2) 对 VPN 业务客户的 VPN 网络中的 VCC 如何管理，即 VPN 业务客户如何能够有效地管理其 VPN 网络。如何管理 VPN 业务客户的 VPN 网络的租用电路，主要包括创建 VPN 租用电路、删除 VPN 租用电路、修改 VPN 租用电路参数和查询 VPN 租用电路参数功能以及 VPN 租用电路状态监控功能 (包括 VPN 租用电路创建报告、删除报告、配置改变的报告)。

为了能够在异构环境下提供 VPN 业务及对 VPN 业务进行有效的管理，基于 TMN 逻辑分层原则 [2] 及我们所研究开发的 ATM PNMS，我们提出 VPN 业务管理体系结构。图 1 给出此管理体系结构的示意图。

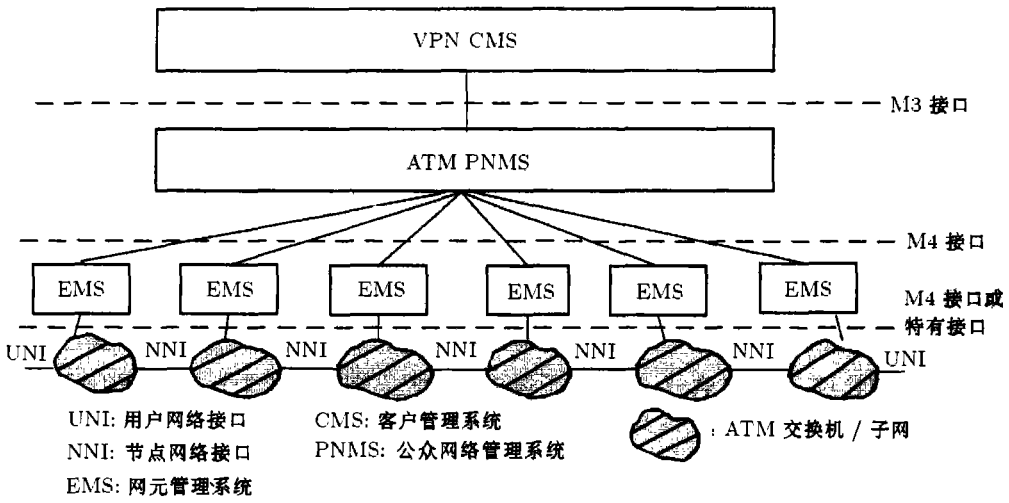

图 1 VPN 业务管理体系结构

图 1 显示了与 VPN 业务管理相关的不同子管理系统间以及下层网络和网元间的关系。VPN 业务管理的体系结构包括以下子管理系统：网元管理系统 (EMS)、ATM PNMS、VPN CNM 系统。下面具体分析各个子管理系统在 VPN 业务管理的作用。

EMS 属于 TMN 逻辑分层结构中的网元管理层，负责管理单个或一系列独立的网元，并在网络管理层与网元层间提供协调功能。其主要功能有：

(1) 接受 ATM 网络管理系统的 VP/VC 连接的配置命令。

(2) 将配置命令转换成与 ATM 网元相关的配置命令，完成与 ATM 网元的交互，并将配置结果上报。

(3) 接受 ATM 网元的告警或其它类型的事件，分析后向 ATM 网络管理系统上报。

ATM PNMS 包括管理网络中的所有网元及网元间的关系并提供 VPN 业务，即完成 VPN 业务提供者的功能。它同时有 TMN 逻辑分层结构中的网络管理层和业务管理层的功能。其主要功能有：

(1) 完成 VPN 业务提供者或 VPN 客户管理系统的与 VPN 相关的配置命令。

(2) 将配置命令映射成对 EMS 的相应操作，完成与 EMS 的交互，并将配置结果上报。

(3) 接受 EMS 的告警或其它类型的事件，分析转换成与 VPN 业务相关的事件向 VPN 业务客户管理系统上报。

(4) 对 VPN 业务客户管理系统的请求进行安全控制。

VPN 业务客户管理系统，它完成管理客户 VPN 网络，包括客户本身私有网络及其拥有的公众网的资源．其主要功能有：

(1) 完成与 ATM PNMS 的交互．

(2) 接受操作者的与 VPN 业务相关的请求，完成后报告结果．

(3) 对与 VPN 业务管理的相关功能进行安全接入控制．

(4) 接收与 VPN 相关的事件如告警等信息给 VPN 并进行相应处理．

从以上各个子管理系统与 VPN 业务管理相关的功能可知，EMS 的功能和 ATM PNMS 中的部分功能与 VPN 业务管理无直接关系，只是配合 VPN 业务管理，对 ATM 网络和 ATM 网元进行直接的控制．与 VPN 管理直接相关的是 VPN CMS 管理子系统和 ATM PNMS 中充当代理的部分． VPN CMS 和 ATM PNMS 间更加具体的关系如图 2 ．

从图 2 可知， VPN 业务管理主要是通过位于 VPN CMS 侧的 VPN 管理者功能与位于 ATM PNMS 侧的 VPN 代理功能交互完成．在 ATM PNMS 中，为了在 ATM 公众网中建立支持 VPN 业务的 VPC ，需要在 VPN 业务管理信息模型和 ATM 网络层或网元层的管理信息模型 M4 进行相互映射， VPN 代理模块的信息模型映射功能块完成以上功能．

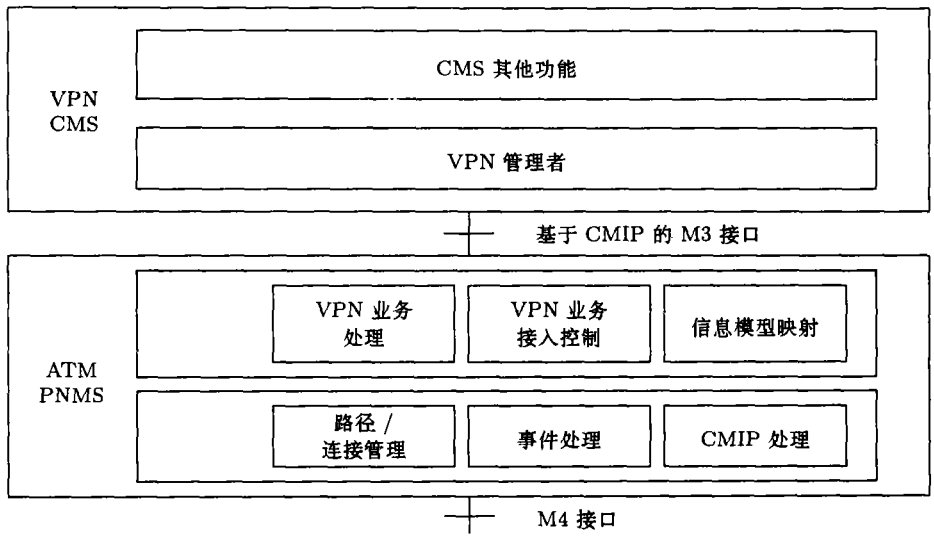

图 2　ATM PNMS 和 VPN CMS 间的关系

3 VPN 管理的信息模型

从上一节的讨论和图 2 可知，在 VPN CMS 和 ATM PNMS 两个管理系统间，采用基于 Q3/CMIP 的 M3 接口．这主要考虑以下几点理由：

(1) CMIP 能够通过面向连接的方式传递数据，比较可靠．

(2) CMIP 支持定界和过滤功能，这样有利与选择多个管理对象一起完成某项操作．

(3) 选择 CMIP 可以使我们设计的系统基于 TMN 的管理对象．

(4) 使用 CMIP 可以比较方便地实现安全管理功能．

(5) CMIP 支持大容量网络管理系统，而这一点正是通信网的主要特点．

(6) 我国 ATM 网元管理层和网络管理层的技术规范均采用 CMIP，使用 CMIP，将保证 VPN 业务管理的标准化程度.

对 ATM PNMS，它可以从两个角度去看待整个 ATM 物理网络，一个采用网络管理层(即以子网的概念) 的角度；另一个采用网元管理层 (即以网元的概念) 的角度去抽象 ATM 物理网络. 而对 VPN CMS 而言，它属于业务管理层，它关心的是更抽象的管理信息，如 VPN 客户的相关信息. 通常情况下，VPN 业务客户并不关心 ATM 实际网络的配置信息的. 所以，可以将整个 ATM 物理网络从子网的角度抽象，将其看作一个大型的交叉连接系统. 按照以上分析，参照 I-ETS 300 653[11] 和 ATM 论坛关于 ATM 管理的网络层管理 M4 标准 [12,13]，并根据 VPN 管理功能需求，确定 VPN 管理所需管理对象类如图 3 所示.

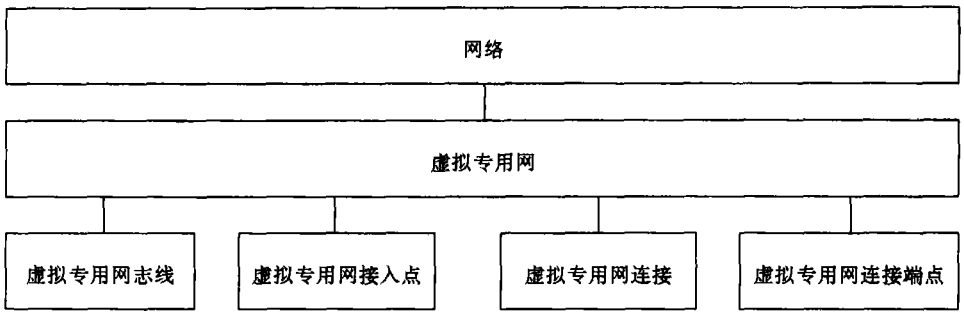

图 3 VPN 管理所需的管理对象类

图 3 中，VP 层的管理对象类 (MOC，Managed Object Class) 为虚拟专用网专线 (vpnLeasedLine) 和虚拟专用网接入点 (vpnAccessPoint)，VC 层的 MOC 为虚拟专用网连接 (vpnConnection) 和虚拟专用网连接端点 (vpnConnectionTP)，VPN CMS 所关心的管理信息是业务客户的信息和点到点连接的管理. 管理对象 vpnLeasedLine 表示 VPN 业务客户申请的 VPN 网的虚拟专用线路，即半固定的 VPC. vpnAccessPoint 表示 VPN 业务接入点. vpnConnection 表示 VPN 业务用户所要求的 VCC，它在 vpnLeasedLine 之上建立. vpnConnectionTP 表示 VCC 的端点. 虚拟专用网 (virtualPrivateNetwork) 对象表示业务客户的 VPN.

显然，VPN CMS 所需的管理对象和 ATM PNMS 所需的管理对象如端点，路径和连接和交叉连接是不同的，这样，在 ATM PNMS 中，需要有不同管理信息间相互映射的机制. 图 4 给出 VPN CMS 和 ATM PNMS 管理对象 (MO，Managed Object) 间的映射关系.

ATM PNMS 管理网络层的管理对象，如 VP 路径 (vpTrail)，VP 连接 (vpConnection)，适配层路径 (tcTrail). 而 TP 类的管理对象 (如 VP 路径端点 vpTTP，VP 连接端点 vpCTP) 的管理对象实际上存在于 EMS 中. 但在 ATM PNMS 中有虚的对象与之对应. ATM PNMS 管理对象类的定义是参照 ITU-T 的关于 ATM 管理的相关标准 I.751(与 ATM M4 等同) 和 ITU-T 定义的通用的管理对象类定义的. vpTrail 和 vpnLeasedLine 的信息实际上基本一致 (当然，vpnLeasedLine 中包括 VPN 业务客户的信息).

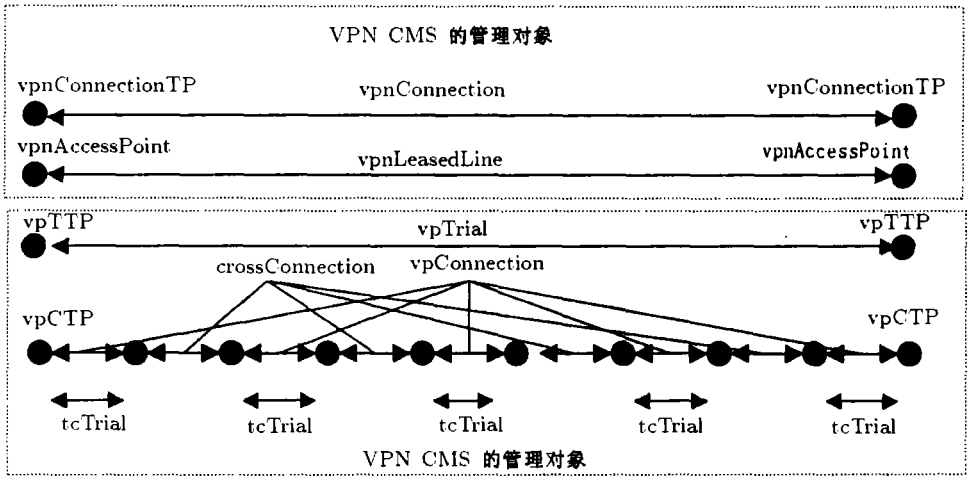

图 4　VPN CMS 与 ATM PNMS 的管理对象间的映射关系

在 VPN CMS 中，故障管理是一项重要功能．这在管理信息的映射中也应得到体现．当 ATM 物理网络发生告警时，ATM PNMS 可以通过映射，将告警的信息映射到 VPN 业务管理的某个管理对象上．然后 VPN 代理以及在 VPN 代理中配置的 EFD 对象，将告警信息发送到 VPN CMS．

通过以上分析，VPN 代理中的管理信息可分为两类：

(1) 与 ATM 物理网络无关而与 VPN 业务客户相关的静态管理信息．

(2) 通过映射处理可以从 ATM PNMS 所管理的管理对象中得到的管理信息．

VPN 业务管理所需的管理信息模型的映射方法可在其管理对象定义指南 (GDMO) 描述 [14] 的行为包中定义，具体映射处理在 VPN 代理模块的信息模型映射功能块中进行．

4 安全方面的问题

对于 ATM PNMS，它有两种类型的使用者，一种是面向 VPN 业务提供者的，主要是在 ATM 物理网络上向 VPN 业务客户提供 VPN 业务．另一种是面向 VPN 客户的，主要是 VPN 业务客户管理其定购的 VPN 业务，向其用户提供连接服务．为了防止 ATM 物理网络资源或 VPN 业务定购者的资源不被非法占用，ATM PNMS 必须有安全管理功能．

对 ATM PNMS 而言，除了系统本身的安全以外，还要考虑以下两个方面：

(1) VPN 业务提供者应该按照与 ATM 网络提供者之间的合同使用属于自己的可用的物理资源．

(2) VPN 业务定购者只能管理或接入属于自己的 VPN 资源．

从以上可知，访问控制是 ATM PNMS 中一项主要的安全管理功能．从图 1 VPN 业务管理体系结构中可知，ATM PNMS 管理系统的安全管理有两个层次的访问控制，如图 5 所示．

图 5　VPN 安全管理的两层访问控制

从图中可知，VPN 业务提供者通过图形用户界面向 ATM PNMS 发出命令请求．对不同的 VPN 业务提供者可以使用的功能及能访问的资源在 ATM PNMS 中需定义，这是网管系统本身的安全控制，我们称之为第一层访问控制．VPN CMS(即 VPN 管理者) 向 VPN 代理发的命令请求，是以 CMIS 原语形式发出的，命令的目标是特殊的管理对象或管理对象的特殊属性，这是 TMN 中安全管理域内的访问控制，我们称之为第二层访问控制．

对 VPN 管理者与 VPN 代理间的访问控制问题，可以通过 X.741 中的方法 [15] 来定义和实现．管理者与代理间的访问控制，可以分为 4 个级别：

(1) 允许连接的建立，即特定的管理者才能与代理建立连接．

(2) 允许对代理的访问，即当管理者发送的信息被 AGENT 鉴权有效时，管理者才能访问代理．

(3) 允许对特殊对象的访问．

(4) 允许对特殊对象的特殊属性的访问．

对第 (1) 级别，使用 ACSE(Association Control Service Element) 中的 AE title 域来识别特定的管理者．对第 (2) 级别，使用 CMIP 的 access control 域来进行鉴权．对第 (3) 和第 (4) 级别，使用 X.741 中定义的关于访问控制管理对象和 CMIP 的 access control 域来实现．

5 结论和展望

如何在 ATM 网络上提供 VPN 业务和怎样使定购者对其申请的 VPN 业务进行有效的管理是 ATM 网在使用中亟待解决的问题．本文应用 TMN 的体系结构和相关的方法，提出了 VPN 的管理体系结构和相应的管理信息模型，并详细讨论了其中安全管理功能的实现方法．对于已有的 ATM 网络管理系统，通过本文提出的方法，可以比较方便地实现 VPN 业务的提供和管理．支持 VPN 业务的 ATM PNMS 已经实现了原型系统 [16]，此原型系统采用 SUN 公司提供的 TMN 网络管理开发平台 SEM 开发，底层采用基于 TCP/IP 的 CMIP 通信协议栈，并将在中国多媒体公众网的骨干网上试运行．

对于 VPN 业务管理问题，还有以下两个问题需要进一步研究：

(1) 本文的 VPN 业务管理是在单个 ATM PNMS 的条件下的，如何在多个 ATM PNMS 的条件下提供 VPN 业务，及其管理体系结构问题需要进一步研究．

(2) 性能管理功能方面的问题需进一步研究．

参 考 文 献

[1] Virtual Private Network, Volume 1: VPN state-of-the-art. RACE R2004 PREPAER deliverable R2004/GMD/WP6/DS/P/016/b1.

[2] ITU-T Rec. M.3010, Principles for a telecommunication management network, 1995.

[3] Saydam T, Gaspoz J P, Etique P A. Object-oriented design of a VPN bandwidth management system. Proc. of ISINM'95, London: Chapman and Hall, 1995, 344–355.

[4] Gaspoz J P, Saydam T, Hubaux J P. Object-oriented specification of a bandwidth management system for ATM-based virtual private networks. Proc. of the Third ICCCN Conference, San Francisco, USA: 1994, 28–32.

[5] Griffin D P, Georgatsos P. A TMN system for VPC and routing management in ATM networks. Proc. of ISINM'95, London: Chapman and Hall, 1995, 356–369.

[6] Bjerring L H, Lewis D, Thorarensen I H. Inter-domain services management of broadband virtual private networks. J. of Network and System Management, 1996, 4(4): 355–373.

[7] Hanaki M,*et al.* LAN/WAN management integration using ATM CNM interface. Proc. IEEE/IFIP 1996 Network Operations and Management Symposium Conference, Kyoto: 1996, 12–21.

[8] Chan M C,*et al.* An architecture for broadband virtual network under user control. Proc. IEEE/IFIP 1996 Network Operations and Management Symposium Conference, Kyoto: 1996, 135–144.

[9] ATM Forum, M3 Specification: Customer Network Management for ATM Public Network Services, 1994.

[10] ATM Forum, CMIP Specification for the M4 (NE View) Interfaces, Sept., 1995.

[11] I-ETS 300 653, Generic managed object class library for the network level view, 1996.

[12] ATM Forum af-nm-0058.000, M4 Network View Requirements and Logical MIB, June, 1996.

[13] ATM Forum, M4 Network View CMIP MIB Specification Version 1.0, November, 1996.

[14] ITU-T Rec. X.722, Guidelines for Definition of Managed Objects, 1992.

[15] ITU-T Rec. X.741, Objects and Attributes for Access Control, 1993.

[16] Qiu Xuesong, Duo Zhuangzhi, Meng Luoming. The design and implementation of the TMN-based ATM NMS. Proc. of ICCT'98, Beijing: 1998, S43-04-01–S43-04-5.

THE STUDY AND IMPLEMENTATION OF VPN SERVICE MANAGEMENT FOR ATM NETWORK

Qiu Xuesong　Meng Luoming　Chen Junliang

(*Nat. Lab. of Switching Tech. and Telecom. Networks, BUPT, Beijing* 100876)

Abstract The VPN service management architecture is proposed based on the logical layer architecture of the TMN and the function of the subsystem in the architecture is analyzed. Based on this, the management information model of the VPN service management is presented and the mapping relationship between this model and ATM network/network element layer managed object classes is also given. The security function of the system is discussed in detail.

Key words Telecommunication management network (TMN), Virtual private network (VPN), Logical layer architecture

邱雪松：　男，1973 年生，博士生，研究方向：通信软件与网络管理体系结构.

孟洛明：　男，1955 年生，教授，博士生导师，研究方向：TMN、通信软件及网络管理.

陈俊亮：　男，1927 年生，教授，博士生导师，中科院院士和中国工程院院士，研究方向：通信软件与智能网.