云南大学学报（自然科学版），2005，27（5）：387~391　　CN 53-1045/N　ISSN 0258-7971
Journal of Yunnan University

基于 VPN 技术的云南强震观测高速远程通信实用方案*

周　挚[1]，刘琼仙[1]，梁　虹[2]，全海燕[3]，旷昆萍[4]，崔建文[1]，周　晖[5]
（1. 云南省地震局，云南 昆明　650041；2. 云南大学 信息学院，云南 昆明　650091；
3. 昆明理工大学 信息工程与自动化学院，云南 昆明　650051；4. 云南省通信管理局，云南 昆明　650011；
5. 云南电信网信集团，云南 昆明　650041）

摘要：在充分利用现有国家通信网络基础设施的前提下，基于 VPN 技术提出了 2 套适用于强震远程观测的高速远程通信实用方案. 方案 1 把 VPN 技术性工作交给了网络运营商，方案 2 把 VPN 技术性工作留给了用户. 但方案 2 在安全性和经济性均优于方案 1.

关键词：VPN 技术；强震观测；远程通信；L2TP VPN；IPSec VPN
中图分类号：TN 915.61　　文献标识码：A　　文章编号：0258-7971(2005)05-0387-05

随着云南省城市化建设、基础设施和生命线工程（如大型水电站、高速公路、大型桥梁）等基础建设的步伐加快，地震的社会影响和经济影响更显突出[1~5]. 建设高密度数字强震台网和地震烈度速报系统已经成为减轻地震灾害的重要举措，并受到政府的高度重视[2,6].

“十五”期间，云南省地震局拟在全省范围内新建固定强震台 70 个，在昆明地区范围内新建固定强震台 50 个，在昆明建设一个强震观测监控中心. 全省范围内的 70 个强震台用于增加全省强震定点观测台网的密度，扩大台网的监控范围，提高台网的监测能力；昆明地区范围内的 50 个强震台用于新建一个具有烈度速报功能的昆明市数字化强震及烈度速报系统，该系统的强震仪分布密度将达到每 50 km^2 1 台仪器的水平. 120 台强震仪、昆明强震观测监控中心将和原有强震仪共同组成现代化的云南强震观测网络系统.

观测仪器数量较多，原有的原始通信手段已不能适应新形势的需要. 为此迫切需要启用新的通信技术手段. 卫星通信等技术虽然有其优越性，但是成本太高. 所以“十五”规划中的地震监测信息化建设发展目标强调“充分利用国家通信网络基础设施，建设中国地震信息服务网络系统，进一步推动地震系统的信息化进程”. 分析研讨如何充分利用国家通信网络基础设施所能提供的最新通信技术手段，就显得非常重要，非常迫切[7]. 本文在充分利用现有国家通信网络基础设施的前提下，基于 VPN（Virtual Private Network，虚拟专用网络）技术的最新进展和市场所能提供的高速通信技术，提出了 2 套适用于强震远程观测的经济型高速远程通信实用方案.

1　通信需求分析

1.1　通信节点规模　全省范围内 **70** 个观测点，昆明市区范围内 50 个观测点. 每个观测点安置 1 台强震仪，构成 1 个独立的远程用户终端，各连接 1 个通信节点. 合计有 120 余个通信节点.

1.2　通信业务类型　仅含数据业务，不含话音业务和图像业务.

1.3　连接时间和数据流量规模　当强震仪触发阈值选为 5 伽时，单台记录数量一般不大于每日 100 条记录. 云南省 5 级以上地震频度约为每年 5 次. 仅在有地震时生产强震数据. 每条记录的数据包不大于 100 kbyte. 平时仅有极少量仪器工作状态数据需要传送.

1.4　强震仪通信功能（协议需求和接口需求）　数

* 收稿日期：2005-03-21
基金项目：云南省自然科学基金资助项目（2003D0084M）；云南省“十五”重点科研资助项目.
作者简介：周　挚（1954-　），男，湖北人，高级工程师，主要从事电子信息工程与数字信号处理方面的工作.

字强震仪支持常见的数据通信协议. 如 XMODEM, YMODEM, ZMODEM 或 TCP/IP 等协议. 数字强震仪具有一个以上的 RS232 全双工异步通信接口.

2 VPN 技术

VPN 的主要功能是在公用网络上传输私有数据,即在 IP 网或 MPLS 网的基础上形成虚拟专用通道[8]. VPN 采用了 4 项主要技术[9~12]: 分别是隧道技术(Tunneling)、加解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication). VPN 主要特点有四: ① 安全保障; ② 服务质量保证; ③ 可扩充性和灵活性; ④可管理性.

2.1 VPN 运行原理 VPN 的基本原理是采用复杂的算法来加密需传输的信息,使得敏感的数据不会被窃听. VPN 的处理过程大体如下: ① 主机发送明文信息到连接公共网络的 VPN 设备; ② VPN 设备根据网管设置的规则,确定是否需要对数据进行加密或让数据直接通过; ③ 对需要加密的数据, VPN 设备对整个数据包进行加密并附上数字签名; ④ VPN 设备加上新的数据报头,其中包括目的地 VPN 设备需要的安全信息和一些初始化参数; ⑤VPN 设备对加密后的数据、鉴别包、源 IP 地址、目标 VPN 设备 IP 地址进行重新封装. 重新封装后的数据包通过虚拟通道在公网上进行传输. ⑥ 当数据包到达目标 VPN 设备时,数据包被解封装. 数字签名经核对无误后,数据包被解密[13].

2.2 VPN 技术分类 传统 VPN 技术基于专线形式(第 2 层 VPN),用户通过租用专用电路组建内部专用网络. 专线方式的内部网具有带宽资源独享、安全性高、运行费用高、组网不灵活等特点. 现阶段所说的 VPN 指的是 IP- VPN 技术,它是利用公共 IP 网的网络资源,在网络层(第 3 层)上为 VPN 用户提供类似于企业专网的服务. 一般而言, IP- VPN 技术可以归纳为基于网络型与基于用户设备型的 2 种[14].

对基于网络型的 VPN 而言,业务的关键特性将集中于运营商网络的边缘设备,采用端到端模型. 其业务管理和网络管理需要进行全网一体化管理,在数据报文穿透公网时采用 IP 隧道技术.

对基于用户设备型的 VPN 而言,业务处理功能全部由用户设备完成. 用户设备之间建立端到端的 IP 隧道,核心网设备只需要完成标准的 IP 转发功能,不需要也不可能知道 VPN 用户的存在.

综合比较 2 种 IP- VPN 网络的实现模式,基于网络型的 VPN 模型侧重于运营商网络业务的提供,故对运营商网络的要求较高,而对接入用户的要求(包括设备、技术、接入手段、业务需求等方面)比较灵活. 而基于用户设备型的 VPN 模型侧重于用户自身网络应用的实现. 客户需要特殊的设备来建设自己的网络及业务的需求. 因此, 2 种 VPN 实现模式的根本区别在于是谁提供 VPN 网络的建立与维护.

3 基于 ADSL 接入 Internet 的 L2TP VPN (方案 1)

ADSL(非对称数字用户线)是 DSL 系列中应用比较成熟的一种技术. 从总体上看, ADSL 采用了较好的调制解调码型,通过普通电话线为客户提供了宽带数据传输的业务[15].

3.1 系统方案 系统网络拓扑见图 **1**.

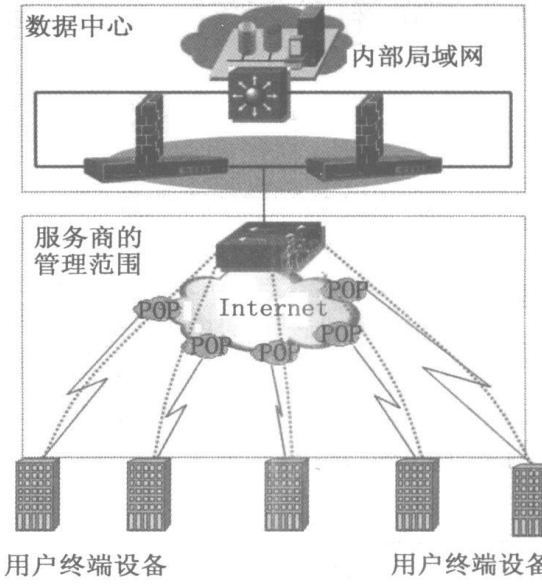

图 **1** **L2TP VPN** 系统网络拓扑

Fig. 1 Network topology of L2TP VPN system

120 个独立的强震仪远程用户终端通过本地 ADSL 接入 Internet,每一个远程用户终端都有自己的动态 IP 地址. 监控中心用户终端通过 IP 宽带专线接入 Internet,大约 10 个固定 IP 地址. 强震仪用户终端可要求与监控中心用户终端建立路由连接,建立连接后可双向数据通信. 基于上述 ADSL 接入 Internet 的基础,由服务商提供全部 VPN 通

道. 整个系统成为一个高速数据通信专用网络. 由于 L2TP 对全部数据提供一般的可靠传送服务, 故这种模式较适应于那些不希望购买 VPN 设备, 又短缺 IT 人员、技术水平不足、资金能力有限的中小型企业用户. 本方案特点是由网络服务商提供 VPN 服务, 而不用添加 VPN 硬件设备.

3.2 方案的优点和缺点　ADSL 接入 Internet 的主要优点有: ① 所有远程用户终端都保持全天候在线; ② 数据流量和通信功能的可挖掘潜力很大; ③ 绝大部分线路维护工作都交给电信服务商.

在 ADSL 接入 Internet 的基础上, L2TP VPN 还有以下优点: ① 设置好的 VPN 可以自动连接; ②安全性和保密性与专线传输效果相当; ③ 强震仪端不需要 IP 地址, 直接作为拨号终端使用; ④不必增加硬件投资; ⑤VPN 维护工作交给电信服务商.

主要缺点是目前的运行费用太高.

3.3 **L2TP** 协议　L2TP 协议是 IETF(Internet 工作任务组) 在 2 层转发协议(L2F) 以及点到点隧道协议(PPTP) 2 个协议的基础上发展出来的[16].

L2TP 协议可以运行在 ATM, AR 及 IP 网等协议环境下. 通常一个用户可以利用拨号电路(如 PSTN, ISDN, ADSL 专线等) 接入网络访问服务器(NAS), 先建立物理连接, 进而建立用户主机与 NAS 之间的点到点第 2 层 L2 链路. 为了在该链路上能用多协议传送数据, 需用 PPP 协议对多协议的数据封装, 建立 PPP 会话. 此时 L2 链路终结点和 PPP 会话端点位于同一物理设备内. 使用 L2TP 可使 PPP 模块延伸, 延伸后的 PPP 端点可通过包交换网络与 L2 端点互联, 从而使 L2 端点与 PPP 端点配置在不同的物理设备内. 例如: 利用 L2TP, 1 个用户有 1 个 L2TP 连接到接入集中器(如 MODEM Pool、ADSL 集中器等), 然后该集中器通过所建隧道把 PPP 帧传至 NAS, 该 NAS 不在本地而在远端. 这样做的明显好处是: 用户的 L2 连接只需连接到就近的本地集中器, 无需通过长距离的专用线路连接到远端的 NAS, 从而可以用共享的网络代替专线, 节省线路费用.

L2TP 协议包含 2 种类型的消息, 即控制消息与数据消息. 前者用于隧道和呼叫的建立、维持、拆除; 后者用于在域内放置待传送的 PPP 帧. 控制消息要利用可靠的控制通道, 以保障可靠投送. 数据消息没有此要求, 数据包丢失时不采取重发等纠错措施.

L2TP 协议对全部控制消息提供低级别的可靠传送服务. 它是通过其字头中的序列编号 Ns, Nr, 用滑动窗口法实施的. 其工作原理是: 发送每一个 L2TP 控制消息包按顺序编号(Ns), 接收端对每一个收到的包检查其 Ns 的顺序及其值, 并用向相反方向传输的 L2TP 控制消息包中的 Nr 来通知原发端. 根据收到的 Nr 值可确定对方已收到值为 Ns= Nr- 1 及其前面的包. 对丢失的包采用重发方式予以纠正.

3.4 总费用　ADSL 接入 Internet 的建设费用约 25 万元人民币, 运行费用约每年 29.6 万元人民币.

在 ADSL 接入 Internet 所需线路费用基础上, L2TP VPN 方案的服务费用: 远程用户终端需增加 0.6 万元人民币的服务费用; 监控中心的宽带专线接入需要每年 10 万元人民币的中心平台使用费用.

总体看, 本方案的建设费用约 25 万元人民币, 运行费用约每年 40.2 万元人民币.

4 基于 ADSL 接入 Internet 的 IPSec VPN (方案 2)

4.1 系统方案　基于 ADSL 接入 Internet 的基础上, 用户在自有设备上硬件实现基于 IPSec 协议的 VPN. 每一个服务商提供的用户端口处都连接一个带有 VPN 功能的防火墙. 数据中心的用户终端处有一个带有 VPN 功能且安全功能很强的防火墙. 整个系统构成一个安全级别很高的高速数据传输专用网络. 虽然在基于 ADSL 接入 Internet 的基础上增加了 VPN 的建设费用; 但对于安全性非常敏感的数据和信息, 可以使用安全性最高的 IPSec 封装技术来建立安全 VPN 隧道. 故这种方案比较适合那些对安全要求极高的用户. 本方案的特点是由用户自己建立和维护 VPN. 系统网络拓扑见图 2.

4.2 方案的优点和缺点　在 ADSL 接入 Internet 的基础上, IPSec 安全 VPN 还有下述优点: ① 提供了目前最完善的安全性; ② 设置好的 VPN 可以自动连接; ③ 强震仪端不需要固定 IP 地址, 直接作为拨号终端使用; ④配置方便.

主要缺点是: ① 增加了 VPN 的设备投资; ② IPSec 的加密和认证会消耗系统资源, 降低系统的吞吐量.

4.3 IPSec VPN IPSec 是目前唯一能为任何形式的 Internet 通信提供安全保障的协议[16~18]. 由于 IPSec 允许提供逐个数据流或者逐个连接的安全,所以能实现非常细致的安全控制. 用户可以根据不同的需要选择不同强度的 IPSec 通道,实现不同级别的安全保护.

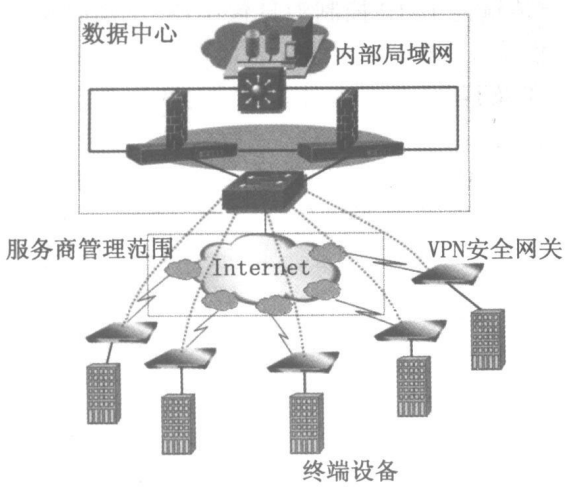

图 2 IPSec VPN 系统网络拓扑

Fig. 2 Network topology of IPSec VPN system

为了实现 IP 层安全, IETF 于 1994 年开始了一项 IP 安全工程,成立了专门的工作组,制定和推广一套称之为 IPSec 的 IP 安全协议标准. 其目标是把安全机制集成到 IP 层,以便对 Internet 的安全业务提供 IP 层的支持. IETF 于 1995 年 8 月开始公布了一系列关于 IPSec 的 RFC 建议标准,并于随后陆续公布了一系列草案供人们协商探讨. 1999 年底, IETF 安全工作组完成了 IPSec 的扩展,在 IPSec 协议中加上了 ISAKMP 协议、部分 Oakley 协议密钥交换机制. ISAKMP/IKE/Oakley 支持自动建立加密、认证信道、密钥的自动安全分发和更新. IPSec 定义了一套用于保护私密性和完整性的标准协议,支持一系列加密算法,检查传输数据包的完整性,确保数据没有被修改,具有数据源认证功能. IPSec 可以确保运行在 TCP/IP 协议上的 VPN 之间的互操作性.

IPSec 协议提供一种标准的、健壮的机制,可为 IP 及其上层协议提供安全保证;通过加密、认证、封装等手段为所有高层协议提供透明的安全保护,从而保证了数据传输的可靠性、完整性和保密性. IPSec 体系是一个开放性的标准框架,其中的 3 个基本模块是: AH(Authentication Header,认证报头)、ESP(Encapsulating Security Payload,负载安全封装)、IKE(Internet Key Exchange, Internet 密钥交换协议). AH 提供了可靠的数据源、数据完整性和避免消息重放的保护措施. ESP 实现了 AH 的所有功能,同时还对携带的数据加密. IKE 负责密钥交换和安全关联 SA 的协商.

IPSec 协议可以设置在 2 种工作模式下运行:一种是隧道模式(tunnel mode),另一种是传输模式(transport mode). 隧道模式下, IPSec 把 IPv4 数据包封装在安全的 IP 帧中. 传输模式下,不隐藏路由信息,只保护端到端的安全性. 隧道模式最安全,但会带来较大的系统开销. 2 种模式的区别就在于保护的内容不同,一个是 IP 包,一个是 IP 载荷.

IPSec 现行的密钥交换协议是 IKE,它是一种混合型协议,由 ISAKMP/OAKLEY/ SKEME 组成. IKE 创建在 ISAKMP 定义的框架上,沿用了 OAKLEY 的密钥交换模式和 SKEME 的共享与密钥更新技术,还定义了自己的 2 种密钥交换方式.

4.4 防火墙集成 VPN 单独的 VPN 网关主要保证数据包的加密解密处理和身份认证,没有很好的访问控制功能. 独立防火墙加 VPN 的部署方式下,防火墙无法对 VPN 的数据流量进行任何访问控制. 由此带来安全、性能、管理上的一系列问题[19]. 而防火墙安全网关上集成 VPN 则能提供一个灵活、高效、完整的安全方案,是当前网络安全产品的发展趋势. 它可以保证加密的流量在解密后,同样需要经过严格的访问控制策略之检查,以保护 VPN 网关免受 DoS 攻击和入侵威胁;提供更好的处理性能,简化网络管理的工作量,快速适应动态变化的网络环境. 因此, VPN 技术已经成为安全网关产品的重要组成部分. 防火墙集成 VPN 后,原始的数据经过加密封装在另外一个 IP 通道内,通道头部地址就是防火墙外部端口 IP 地址,用以实现公网链路上的传输,利用高强度、动态变换的密钥保证数据安全. 168 位的 3DES 算法、AES 算法,提供了业界极高的安全防御体系.

4.5 总费用 在 ADSL 接入 Internet 的基础上,所有的远程用户终端(含监控中心)都必须接入一个集成 VPN 的防火墙. 建设费用:强震仪端的集成 VPN 防火墙共约 24 万元人民币,监控中心端的集成 VPN 防火墙约 10 万元人民币. 在 ADSL 接入 Internet 的基础上,服务费用不必增加.

方案 2 的建设费用约 59 万元人民币, 运行费用约每年 29.6 万元人民币.

5 结　语

目前, VPN 属于一项正在不断发展的技术, 市场前景广阔, 正在为越来越多的企业所采用. 根据预测, 美国和加拿大近年的 VPN 业务将以每年 34% 的速度增长; 全球的 VPN 业务在近 5 年将高达 360 亿美元[20]. 本文在充分利用现有国家通信网络基础设施的前提下, 基于 VPN 技术和市场所能提供的最新高速通信技术, 提出了 2 套经济型高速远程通信实用方案, 它们各有其特点. 从技术上看, 方案 1 把 VPN 的技术性工作交给了网络运营商, 方案 2 把 VPN 的技术性工作留给了用户. 从安全性看, 方案 2 高于方案 1. 从经济性看, 方案 1 的建设费用小于方案 2, 但其运行费用远高于方案 2. 如果用 5 年的运行周期来比较, 运行费用和总费用的差异则更明显. 总体而言, 方案 2 优于方案 1, 但有一定的实现难度.

远程通信网络建设不仅包括上述远程通信的问题, 而且还包含有许多其它重要问题: 监控中心的网络系统集成、防火墙安全措施、双机备份、线路备份、实时监控组态软件、网络系统管理、技术队伍建设等. 这些工作首先会牵涉到费用问题, 而且有些工作需要在较高的层面上统筹解决. 这些工作拟另文讨论.

参考文献:

[1] 高光伊, 于海英, 李山有. 中国大陆强震观测[J]. 世界地震工程, 2001, 17(4): 13－18.

[2] 周雍年. 强震观测的发展趋势和任务[J]. 世界地震工程, 2001, 17(4): 19－26.

[3] 赵永庆, 崔建文, 乔　森, 等. 施甸地震强震观测记录及其初步分析[J]. 地震研究, 2001, 24(3): 245－250.

[4] 崔建文, 任增云, 赵永庆, 等. 大姚 6.0 级地震的强地震动观测研究[J]. 地震研究, 2004, 27(2): 133－139.

[5] 周光全, 毛　燕, 施伟华. 云南地区地震受灾人口与经济损失评估[J]. 地震研究, 2004, 27(1): 88－93.

[6] 崔建文, 王　彬, 乔　森, 等. 云南施甸、永胜地区强地震动观测与研究[M]. 昆明: 云南科技出版社, 2004.

[7] 周　挚, 山秀明, 崔建文, 等. 基于 Internet 的强震仪监测网络系统的设计[J]. 云南民族大学学报(自然科学版), 2005, 14(1): 61－63.

[8] 孔　雷, 刘云新. 虚拟私用网络技术[M]. 北京: 清华大学出版社, 2000.

[9] Ivan Pepelnjak, Jim Guichard. MPLS 和 VPN 体系结构[M]. 赵　斌, 陈文飞, 徐鸿文译. 北京: 人民邮电出版社, 2003.

[10] 王　晶. VPN 关键技术研究[J]. 网络安全技术与应用, 2003, (5): 61－65.

[11] 叶　盛. VPN 的实现机制和系统评价[J]. 小型微型计算机系统, 2002, 23(9): 1 053－1 058.

[12] 刘云玲, 杨　璐. VPN 及其安全技术研究[J]. 计算机工程与设计, 2003, 24(12): 82－85.

[13] 王传林. VPN 网关的设计与实现[J]. 高性能计算技术, 2003, (3): 52－56.

[14] 阎宝刚, 阎民正. IP－VPN 在政府及行业网络中的应用——以地震行业为例[J]. 山西地震, 2003, (2): 35－37.

[15] 郭士秋. ADSL 宽带网技术[M]. 北京: 清华大学出版社, 2001.

[16] 陈锦章. 宽带 IP 网络技术[M]. 北京: 清华大学出版社, 2003.

[17] 屈长青, 魏大宽. 基于 IPSec 的 VPN 技术[J]. 计算机技术与自动化, 2001, (4): 63－66.

[18] 徐凤华, 胡　敏. IPSec VPN 关键技术研究与应用分析[J]. 武汉工程职业技术学院学报, 2003, 15(4): 30－33.

[19] Paul Serrano. 如何选择适宜的防火墙和 VPN 解决方案[J]. 信息网络安全, 2003, (11): 60－61.

[20] 蔡　康, 李　洪, 朱英军. IP 宽带业务与运营[M]. 北京: 人民邮电出版社, 2003.

The practical scheme of high-speed telecommunication of Yunnan strong earthquake observations based the VPN1

ZHOU Zhi[1], LIU Qiong-xian[1], LIANG Hong[2], QUAN Hai-yan[3], KUANG Kun-ping[4], CUI Jian-wen[1], ZHOU Hui[5]

(下转第 396 页)

表1 网络课堂组播通信方式下系统性能测试结果

Tab. 1 The test data of network class under group broadcasting transmission

学生机数量/台	服务器流量/kbps		质量评价
	DL	UL	
1	160.1	138.5	优
5	171.2	153.4	优
10	168.3	149.6	优
20	177.3	152.4	优
50	169.5	154.6	优

参考文献:

[1] 张美枝, 贺思德. 基于IP组播的校园网多媒体教学系统模型的设计与实现[J]. 云南大学学报(自然科学版), 2003, 25(6A): 62—66.

[2] 杜常青, 贺思德. 基于组播通信的多媒体系统扩展[J]. 云南大学学报(自然科学版), 2004, 26(5A): 89—91.

[3] ALTHUN B. Streaming services: Specification and implementation based on XML and JMF[J]. Scientific Engineering of Distributed Java Applications Lecture Notes in Computer Science, 2004, 2952: 23—32.

Application study of the JMF in network teaching system

HE Si-de, ZHANG Mei-zi

(Department of Telecommunication Engineering, Yunnan University, Kunming 650091, China)

Abstract: JMF (Java Media Framework) is a socket that introduce multimedia audio and video stream into JAVA and Applet programs. The major difference between network based multimedia teaching system and ordinary multimedia application is that it contains not only audio and video streams, but also the screen and the teachers hand writing data stream. The realizations of JMF API and JMF RTP API in network based teaching system is discussed, it is a better solution in network class recording system.

Key words: multimedia telecommunication network; JMF (Java Media Framework); JMF API; JMF RTP API

* *

(上接第391页)

(1. Yunnan Earthquakes Administration, Kunming 650041, China;
2. College of Information, Yunnan University, Kunming 650091, China;
3. Faculty of Information engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China;
4. Yunnan Communications Administration, Kunming 650011, China;
5. Yunnan Telecom Netit Group, Kunming 650041, China)

Abstract: Being fully used the national communicational facilities available, it is presented two high-speed telecommunication schemes for the remote strong earthquake observation based the VPN. The network runners take the responsibility for the VPN in the first scheme while the users for it in the other scheme. However, scheme 2 is much better than scheme 1 as for safe and economical sake.

Key words: VPN-Technology; strong earthquake observations; remote telecommunication; L2TP VPN; IPSec VPN